PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

"IMPLEMENTACIÓN DE UN MODELO DE SEGURIDAD PARA CONTROL DE ACCESOS A LA RED DE DATOS, EVALUANDO HERRAMIENTAS DE HACKING ÉTICO, EN LA EMPRESA BLENASTOR"

AUTORES:

RICARDO GONZALO AVILÉS GUZMAN

MIGUEL ANGEL SILVA URÍA

DIRECTOR:

DR. GUSTAVO CHAFLA

QUITO, ENERO 2017

RESUMEN

Hoy en día, no se puede navegar por Internet sin una protección eficaz. Incluso con el software adecuado, nadie está a salvo de cualquier daño. Virus, la suplantación de identidad, troyanos, intrusiones en su sistema, ataques pishing, etc. La imaginación de los piratas informáticos no tiene límites. La única solución es protegerse de manera efectiva. Un usuario informado es una debilidad menos.

Los hackers están empujando constantemente los límites, para explorar lo desconocido y para desarrollar su ciencia. Saber cuáles son sus técnicas no sólo a tomar conciencia de consecuencias insospechadas, tales como errores de codificación, sino también para resolver problemas de programación complejos. Es por eso que se ha incrementado últimamente la ingeniería social, o la manipulación social, dada por los defectos humanos, representan más del 60% de los ataques con más éxito que los defectos físicos ya que un error humano representa permitir el acceso directo a las computadoras y las redes.

La información es un recurso valioso que puede contribuir tanto a la puesta en peligro o el éxito del usuario, empresa, etc. Cuando se gestiona bien, le permiten actuar con confianza a la empresa o usuario. Los sistemas de información son omnipresentes estos días en todos los negocios. El software de seguridad de estos sistemas debe proteger contra numerosas amenazas de diversos orígenes. El análisis de riesgos puede determinar, en función de la vulnerabilidad del sistema, la criticidad de cada una de estas amenazas. Estos análisis permiten proponer las soluciones necesarias y suficientes para reducir el riesgo a un nivel residual aceptable.

DEDICATORIA

La siguiente disertación, es dedicada a nuestros padres y hermanos, los cuales siempre han estado dándonos un apoyo incondicional y siempre nos han mostrado una guía para ser personas de bien y de esta manera poder cumplir todas nuestras metas.

AGRADECIMIENTOS

Queremos agradecer nuevamente a nuestros mayores apoyos que son nuestros padres, ya que sin ellos no estaríamos en el lugar en el que estamos, no solo nos apoyaron moral y éticamente, sino que también nos brindaron todo su apoyo económico para alcanza nuestra meta actual.

También agradecemos a nuestro director de tesis, Gustavo, que nos guio como maestro y también como nuestro director, a nuestros correctores por sus sugerencias y enseñanzas, y a todos nuestros profesores que nos ayudaron con sus conocimientos a lo largo de nuestra formación en la carrera y como personas.

Finalmente agradecemos a todos nuestros amigos y compañeros que estuvieron a nuestro lado y nos brindaron su apoyo. Y sobre todo también a nuestra universidad PUCE por todo lo que nos brindó y pudimos lograr gracias a esta.

CONTENIDO

INTRODUCCION

Cada vez más está creciendo la era digital, las empresas de hoy en día, ya sean pequeñas, medianas o grandes, son objeto de amenazas significativas en cuanto a la piratería. espionaje industrial, el robo de datos, el costo de la piratería es ahora lo suficientemente pequeño como para que sea económicamente interesante para cortar en el sistema informático o un sitio web de negocios. Para estos últimos, el riesgo es muy importante, el punto puede comprometer su sostenibilidad. Ante tal amenaza, muchas empresas utilizan los servicios de "hacking ético".

ANTECEDENTES

Actualmente la mayoría de la información se guarda en dispositivos de almacenamiento y en redes de datos, con los avances tecnológicos, es estos últimos años se ha empezado a utilizar con fuerza la nube (cloud), que se encuentra sujeta a riesgos e inseguridades ya sean internas y externas a las organizaciones. Es por esto que muchas empresas tanto públicas como privadas han decido priorizar la protección de su información, sin embargo, los presupuestos asignados a esta gestión son limitados, por esta razón es necesario mantener implementados controles de seguridad para afrontar los riesgos a que está sometida la información en forma continua y no hacer inversiones grandes cuando ya se enfrenta a ataques informáticos.

En la prensa se puede ver artículos que no hablan acerca de problemas que tienen varias empresas de todo tipo, un ejemplo en el Ecuador, el robo de información fue el principal incidente del 2012 en materia de seguridad informática. Entre los casos de fuga de información más resonantes pueden mencionarse la filtración de datos de más de 56.000 cuentas de tarjetas de crédito, la exposición de 6.5 millones de contraseñas de LinkedIn y 450.000 credenciales robadas de Yahoo! Voice.

Para el Gobierno Ecuatoriano la seguridad es una prioridad, su nuevo enfoque está de manifiesto en el Plan Nacional de Seguridad Integral, aprobado en diciembre del 2011, donde articula políticas transversales alineadas a La Constitución, La Ley de Seguridad Pública y del Estado y al Plan Nacional para el Buen Vivir. Además, manifiesta que la Seguridad Integral no se alcanza con esfuerzos aislados, sino, que se requiere del compromiso de todos desde los diversos ámbitos.

Y no solo para los gobiernos es importante la seguridad integral, las empresas privadas también tienen sus prioridades de protección de todos sus recursos, incluyendo la información por ser uno de los principales activos de las organizaciones, en este ámbito como ejemplo podemos mencionar a los bancos tanto públicos como privados, han tomado conciencia sobre la necesidad de gestionar la seguridad de la información para garantizar la continuidad de sus servicios, disminuyendo al máximo los riesgos para los clientes.

El hacking ético es una herramienta de prevención y protección de datos. En la cual lo más importante que se pretende conocer es de los nuevos ataques y amenazas que están en nuestro entorno por lo cual se pretende estar constantemente más adelante de aquellos que nos intentan agredir haciendo pruebas y ataques propios con la ayuda de programas especiales y expertos informáticos los cuales con sus herramientas y conocimientos de seguridad en información pueden revisar en el sistema, redes o dispositivos electrónicos vulnerabilidades, con el fin de reportarlas para que la empresa o persona pueda tomar medidas para que no esté en riesgo el sistema.

JUSTIFICACIÓN

La seguridad informática ha ganado popularidad en los últimos años y ha pasado de ser considerada un gasto, a ser vista como una inversión por parte de los directivos de las empresas y organizaciones a nivel mundial.

En algunos países esto ha sucedido de forma acelerada, en otros el paso ha sido más lento; pero en última instancia hemos convergido todos en un mundo digital en el que la información es el activo intangible más valioso con el que contamos.

Y al ser un activo, debemos protegerlo de posibles pérdidas, robos, mal uso, etc. Es aquí en donde juega un papel importante el ingeniero en sistemas.

El rol del hacker ético es efectuar - desde el punto de vista de un cracker - un ataque controlado hacia la infraestructura informática de un cliente, detectando vulnerabilidades potenciales y explotando aquellas que le permitan penetrar las defensas de la red objetivo, pero sin poner en riesgo los servicios y sistemas auditados. Y todo esto con el solo propósito de alertar a la organización contratante de los riesgos de seguridad informática presentes y cómo remediarlos.

El formulario de evaluación considera:

La seguridad informática es un punto importante para las empresas y organizaciones para el cuidado de información.

Es un avance tecnológico y de crecimiento en todo el mundo, ya que la información es el activo más valioso con el que contamos.

Se tiene que considerar mucho más a la información y su seguridad para que esta tenga un buen uso y no pueda ser robada o manipulada para ser usada de una forma inadecuada.

Desde el punto de vista de un hacker/cracker la mejor manera de ver debilidades y percatarse de las vulnerabilidades potenciales es hacer ataques controlados, de esta manera se planea hacer esto para descubrir las fallas de seguridad que la empresa u organización tiene.

ALCANCE

El presente proyecto de disertación de grado concluirá con la entrega de un documento con la investigación de las herramientas de hacking ético, el análisis de resultados de la ejecución de las mismas, selección de la o las herramientas que se ajustan a la empresa caso de estudio y el modelo validado de seguridad para la red de datos de la empresa.

OBJETIVOS

Objetivo General

Implementar un modelo de seguridad para control de accesos a la red de datos, evaluando herramientas de hacking ético y seleccionado la herramienta que más se ajuste a la empresa Blenastor.

Objetivos Específicos

- Investigar las herramientas de hacking ético indicadas, sus beneficios y utilidad.
- Analizar la situación actual de la empresa especialmente el tema se seguridades en la red de datos.
- Configurar y evaluar las herramientas de hacking ético investigadas.
- Analizar resultados y seleccionar la o las herramientas que más se ajusten a la empresa caso de estudio.
- Desarrollar el modelo o metodología de seguridad para ver debilidades en la red.
- Describir conclusiones y recomendaciones.

CAPÍTULO 1

MARCO TEÓRICO

1.1. Seguridad Informática

Según la Real Academia Española la Seguridad es Calidad de seguro, donde Seguro es Libre y exento de Peligro, por lo que podríamos concluir que Seguridad Informática es "la cualidad de un sistema informático exento de peligro". (Real Academia Española, 2017)

Refiriéndonos a la seguridad informática, una definición apropiada. “es la práctica de proteger los recursos y todos los datos de un sistema de computadoras y redes, incluyendo la información guardada en dispositivos de almacenamiento y en su transmisión”. (Sheldon, 1997)

1.2. Objetivo de la Seguridad Informática

La seguridad informática tiene como principal objetivo el proteger todos los recursos que la empresa o la persona tiene y considera como valiosos, tales como datos, software o hardware. Esto se da gracias a que la seguridad informática adopta medidas para que las organizaciones, empresas o personas puedan cumplir sus objetivos, esto permite que se puedan proteger todos los recursos, sistemas, datos financieros, situación legal y tanto bienes intangibles como tangibles. (Toribio, 2016)

Para que un sistema sea seguro tiene que cumplir con estos elementos principales de la seguridad informática, los cuales son:

- **Integridad:** Garantiza que los datos y la información no sean alterados o modificados, ni destruidos o borrados de modo no autorizado. (López, 2010)

- **Confidencialidad:** Garantiza que los datos y la información solo puedan estar al alcance de las personas, entidades u organizaciones autorizadas. (López, 2010)
- **Disponibilidad:** Es disponibilidad de la información, datos u componentes del sistema a las personas, entidades u organizaciones autorizadas. (López, 2010)
- **Autentificación:** Es la manera en la cual se garantiza que los diferentes recursos estén disponibles solo para las personas, entidades u organizaciones autorizadas. (López, 2010)
- **Trazabilidad:** Esta determina el qué, cuándo, cómo y quién realiza acciones al sistema. (López, 2010)

En general, se puede recordar que la metodología de la seguridad informática es la siguiente:

- **Realizar un análisis de riesgos:** Debido a que es posible protegerse contra el riesgo del que se sabe. Dicho esto, es para cada empresa para evaluar el riesgo, es decir, la medida de acuerdo a la probabilidad de su apariencia y sus posibles efectos. Las empresas harían bien en evaluar, aunque toscamente estos riesgos y las maneras de poner en práctica, en función de sus costes. El concepto de riesgo puede ser entendida como el producto de perjuicio por la probabilidad de ocurrencia de los mismos. El concepto de riesgo definido por los especialistas de acuerdo con la siguiente ecuación:

  Riesgo = Daño x Probabilidad de ocurrencia

  Esta fórmula supone que un evento cuya probabilidad es bastante alta, pero es posible prevenir el daño que puede causar, representa un riesgo aceptable. Es lo mismo para un evento en la gravedad imparable (por ejemplo, colapso del edificio), pero con baja probabilidad de ocurrencia. Es obvio que, en el primer caso, el riesgo es aceptable si las medidas preventivas contra los daños son eficaces y eficientes. (López, 2010)

- **Establecer una política de seguridad:** Una vez que el análisis de riesgos, la política de seguridad está en su lugar. Esta función consiste en:
    - Definir el alcance del uso de los recursos del sistema de información;
    - Identificar las técnicas de seguridad para poner en práctica en diferentes departamentos de la organización;
    - Educar a los usuarios en la seguridad informática
- **Aplicar técnicas de seguridad:** Estas técnicas son la respuesta a las necesidades fundamentales de la seguridad de TI se ha definido anteriormente. Su función es garantizar la disponibilidad, integridad, confidencialidad y, en algunos casos, la durabilidad de la información en los sistemas de información. métodos de seguridad incluyen:
    - La vulnerabilidad de auditoría y pruebas de penetración (Pen-Test)
    - Seguridad de datos: encriptación, autenticación, control de acceso
    - Seguridad de red: Firewall, IDS
    - Seguimiento de la información de seguridad o la educación del usuario
    - Las actividades del plan de recuperación.

1.3. Tipos de Seguridad Informática

1.3.1. Seguridad Física: Son las medidas o planes que se tienen para la protección de todos nuestros recursos de amenazas externas. Estas amenazas pueden ser:

- Desastres naturales como incendios, terremotos, tornados, inundaciones, etc.
- Acciones hostiles como robos, fraude, sabotaje.
- Amenazas ocasionadas por el hombre o control de acceso.

(Segu.Info, 2010)

Estos peligros físicos pueden ser accidentales o provocados y las consecuencias son fácilmente identificables. Este tipo de incidentes pueden dañar los recursos o materiales del sistema de información y pueden tener un impacto directo en los activos de información que contienen los sistemas informáticos.

Los riesgos físicos están en el concepto tradicional de seguridad, las principales fuentes de preocupación en términos de directivos de la empresa de seguridad, aunque en la práctica sólo representan un pequeño porcentaje.

(Segu.Info, 2010)

1.3.2. Seguridad Lógica: Esta se divide en dos.

- **Activa:** Son todas las medidas de seguridad cuyo objetivo es prevenir y reducir los riesgos que pueden amenazar la integridad del sistema.

  Ejemplo: Los accesos de usuario, antivirus, encripta miento de datos, etc.
- **Pasiva:** Son todas las medidas que se tienen para poder controlar el riesgo o la amenaza, es decir los planes que se tienen para minimizar los riesgos una vez que un ataque se da.

  Ejemplo: Copias de seguridad de la información o base de datos.

(Segu.Info, 2010)

Con el rápido desarrollo de la informática distribuida, los datos y las aplicaciones han adquirido mayor importancia. De hecho, estamos en presencia de una migración gradual del valor del equipo al valor de los datos y aplicaciones. El desarrollo de Cloud Computing es uno de los ejemplos más

expresivos de esta tendencia. La cuestión principal es cómo evaluar y analizar el valor de la que no es físico, tan intangible, es decir los datos.

Es para responder a esta pregunta surgió el concepto de accidente, error y la malicia, directamente de los métodos de análisis de riesgos desarrollados en los últimos años.

- **El accidente:** Este es un evento que afecta el flujo de datos o datos, en ausencia de daño físico a los equipos (alteración física del material).
- **El error:** Esto puede ser un error de diseño, la programación, la configuración o la manipulación de datos y sus soportes. El error se refiere a las pérdidas consecutivas a la intervención humana en el tratamiento automatizado de datos. Ellos son los riesgos más comunes en el ciclo de vida de un sistema de información empresarial.
- **Malicia:** Esto es para todos los actos que reflejan la clara voluntad del autor de usar con malas intenciones y sin autorización de un sistema de información.

(Segu.Info, 2010)

1.4. Vulnerabilidades

Las vulnerabilidades son debilidades de un sistema o software. Estas debilidades son explotadas por los hackers para obtener acceso a un recurso (CPU redes, etc.) o información. Las debilidades están en servicios, aplicaciones y usuarios:

- Servicios: En general, estos servicios son el correo electrónico, la Web u otra aplicación que se comunica con otra aplicación. Los ejemplos incluyen los ataques contra IIS en 2001 que permitió la propagación del gusano CodeRed. Las vulnerabilidades de los servicios son muy peligrosas debido a que no requieren la intervención humana.

- Aplicaciones: Vulnerabilidades de las aplicaciones a menudo requieren intervención humana: por ejemplo, el usuario activa un virus mediante un clic del ratón. ¿Qué podría ser más atractivo que los correos electrónicos con el tema “Te amo” o con contenido para demostrar que es el afortunado ganador de una gran suma de dinero? Un simple clic y usted se encuentra la víctima de un virus gusano o software espía.
- Acciones del usuario: Los usuarios pueden crear vulnerabilidades en los sistemas o software por configuraciones incorrectas o malas. Un usuario puede volver a configurar un sistema o software y por lo tanto las puertas abiertas para los hackers. En este caso, incluso el sistema de seguridad más eficiente, si está mal configurado, ofrece una violación de la seguridad.

1.5. Fases de un Ataque Informático

- **Reconocimiento:** El propósito de esta encuesta es conocer las vulnerabilidades del sistema, incluyendo información de identificación, versiones de software y las configuraciones de red de inicio del sistema.
- **Enumeración:** El segundo paso en cualquier tipo de ataque cibernético es la detección de datos de reconocimiento. Servicio de escaneo y los archivos de marcado son muy populares durante la fase de enumeración.
- **Compilación:** Un método para recopilar esta información es a través de la ingeniería social, engañando a los usuarios finales para proporcionar información privada. A menudo son perpetrados por phishing (correo electrónico fraudulento), pharming (sitios web fraudulentos) y drive-by pharming (redirección de DNS y configuración de puntos de acceso inalámbrico).

- **Guerra de Marcación:** Marcación guerra implica el uso de un sistema automatizado para llamar a cada uno de los números de teléfono pertenecientes a una empresa con la esperanza de encontrar un módem que puede proporcionar acceso directo a los recursos internos de la empresa.
- **Ataques de intrusos y avanzados:** Una vez que los atacantes han sido identificados y se correlacionó vulnerabilidades conocidas, que pueden usarlos para entrar en la red.
- **Denegación de servicio (Denial of Service):** Hay otra forma de intrusión maliciosa avanzada, denegación de servicio (DoS), cuyo objetivo es que las redes se mantienen las solicitudes de bombardeo inoperantes o aplicaciones para la comunicación externa.
- **Inserción de malware:** Tras infiltrarse en una red, el siguiente paso es insertar ataque de malware en secreto mantener un control permanente sobre los sistemas remotos y luego ejecutar el código dentro de la red para lograr un objetivo particular. Una vez insertado, el malware puede ser una molestia (por ejemplo, la comercialización de pistas de audio), el controlador (proporcione la pasarela o el mando a distancia) o destructiva (para causar daño o para cubrir las huellas del atacante).

1.6. Hacking ético

El Hacking Ético llega gracias a la necesidad que se da para poder tener un control sobre nuestros sistemas y sobre todo nuestra información personal o de gran importancia, ya que existen vulnerabilidades las cuales pueden ser explotadas para mal, estas no solo se pueden dar de manera interna sino también de manera externa, tal es el caso de redes inalámbricas o redes locales. El hacking Ético busca demostrar y encontrar todas estas vulnerabilidades las cuales son encontradas para que están se puedan arreglar o buscar una manera de protegerlas.

Una definición que tiene, es el proceso por el cual se busca deficiencias o daños en la seguridad, red, o sistemas y de esta manera poder analizar, calibrar y ver el riesgo que estas tienen para que de esta manera se pueda brindar y recomendar soluciones factibles o las más apropiadas para poder arreglar, combatir o mejorar cada una de estas y no tener riesgos futuros. (Gómez, 2011)

Los proyectos de Hacking Ético no buscan dañar los equipos o sistemas, estos como bien se ha dicho buscan ver las debilidades para que de esta manera poder ayudar a mejorarlos, los informes que se presentan después de realizar este proceso de ver vulnerabilidades de los ordenadores, redes, servidores, etc. Indican los resultados mostrando los detalles de en qué parte se encuentra el problema. (Gómez, 2011)

1.6.1 Tipos de hacking ético.

1.6.1.1. Hacking Ético Externo: Este hacking es realizado desde la red hacia una infraestructura de red pública del usuario, de tal manera en la que los ordenadores de una empresa o compañía que están conectados a una red de internet pueden ser atacados. Por decir routers, firewalls, servidores, etc. (Astudillo, 2013)

1.6.1.2. Hacking Ético Interno: Este tipo de hacking es realizado de manera interna en la que alguien que tiene acceso puede ingresar y atacar la red. Por lo general en estos casos se suele encontrar más debilidades en la seguridad ya que los encargados de las áreas de seguridad prestan más atención a poner una fuerte estructura de seguridad externa que interna. Por ejemplo, en el Reino Unido, cuando se realizó encuestas de seguridad por lo general los ataques eran 25% externos y 75%internos. (Astudillo, 2013)

1.6.2. Beneficios del Hacking Ético.

Existen muchos beneficios a nivel de seguridad los cuales se pueden obtener realizando un informe de Hacking Ético, pero el principal de todos es poder ver el estado en el cual se encuentra nuestros sistemas en seguridad, también podemos tener: (Malagón, 2010)

- Conocimiento de los riesgos que se tiene y a su vez mediante esto poder reducirlos.
- Ahorro de tiempos y gastos al poder obtener los datos de los riesgos que se presentan para poder afrontarlos con tiempo o de estar mejor preparados.
- Mejora de la calidad de la empresa en los marcos de seguridad.
- Detección temprana de futuros fallos o ver las brechas de seguridad.

1.6.3. Que es un Hacker.

Hacker es el nombre que se le da a una persona la cual sabe cosas específicas en una o varias ramas técnicas, también estas están relacionadas con las nuevas tecnologías informáticas, electrónicas o de telecomunicaciones tales como los sistemas, redes, etc. Se podría decir que esta persona es un informático el cual está especializado en poder romper o pasar seguridades. (Michelena, 2005)

Los hackers siempre buscan estar actualizados a las nuevas tecnologías por lo cual casi siempre están tratando de conocer todos los terrenos y novedades en la cual se mueve el crecimiento tecnológico en parte de software y hardware. Su búsqueda por el conocimiento siempre está en ansias para poder estar al día y de esta manera mediante la investigación poder realizar inmediatamente o de manera más sencillo lo que resulta difícil de descifrar. (Michelena, 2005)

Los hackers siempre buscan de una manera poder entender primero los sistemas tanto internamente como externamente para que de esta manera resulte más fácil poder modificar, robar o copiar la información, servicios, etc. (Michelena, 2005)

1.7. Tipos de Hackers.

1.7.1. ***Gray Hats:*** Se los conoce como los hackers de sombrero gris, estos hackers son personas las cuales actúan de manera ofensiva y defensiva, esto quiere decir que no atacan por atacar, pero si están preparados para todo, son personas las cuales solo actúan cuando lo ameritan o actúan de una buena manera. (Quispe, 2013)

1.7.2. ***Black Hats:*** Se los conoce como hackers de sombrero negro o también como crackers. Estos hackers tienen grandes habilidades, pero se enfocan en violar seguridades, vulnerabilidades de los sistemas, etc. (Quispe, 2013)

1.7.3. ***White Hats:*** Estos también son conocidos como hackers de sombrero blanco, son los hackers que tienen habilidades iguales a los hackers de sombrero negro con la diferencia que las ocupan para mejorar la seguridad o ayudar para detectar problemas. Ellos son comúnmente contratados por empresas para realizar auditorías o consultorías para ver las debilidades que esta tenga. (Quispe, 2013)

1.7.4. ***Suicide Hackers:*** Conocidos como los hackers suicidas, estos hackers son las personas revolucionarias que por hacer algo por un bien común no tienen miedo de enfrentar los cargos que se les puedan dar o que puedan recibir. (Quispe, 2013)

1.7.5. ***Script Kiddies:*** Se los conoce como los hackers los cuales atacan mediante programas creados por otros para poder penetrar los sistemas, redes, paginas, etc. No tienen mucho conocimiento sobre el código o la programación. (Quispe, 2013)

1.7.6. ***Newbie:*** Son los hackers que no tienen conocimiento previo, pero bajan toda la documentación junto a programas para realizar ataques para aprender. También se los conoce como los que recién están empezando o la gente nueva en la informática. (Quispe, 2013)

1.8. Ataques Informáticos.

Existen muchos tipos de ataques informáticos los cuales circulan por la red, los cuales cuando ingresan a nuestro ordenador pueden robar, dañar, modificar, borrar nuestra información o incluso hacer que nuestras computadoras dejen de funcionar o hacer acciones específicas que el atacante desea. A continuación, vamos a ver los distintos tipos de ataques que hay o archivos dañinos para nuestros ordenadores.

1.8.1. ***Virus:*** Es un malware el cual se enfoca principalmente en cambiar el funcionamiento de nuestras computadoras sin el permiso o conocimiento del usuario. Estos archivos por lo general cambian o remplazan a los ejecutables originales para poder así meter el código dañino o infectado. Algunos virus no alteran mayormente el sistema y estos solo hacen que sean molestosos para el usuario, pero por otra parte hay otros que dañan y hacen que las computadoras dejen de funcionar. (Kaspersky Lab, 2017)

1.8.2. ***Gusanos Informático:*** Es similar a los virus, pero la diferencia es que el gusano solo necesita una conexión a internet o a la red para contaminar el equipo, aparte los gusanos se propagan por el computador automáticamente. Hay muchos tipos de gusanos, uno de los más comunes es el gusano de correo electrónico el cual manda links o archivos adjuntos para poder contaminar el ordenador una vez que este se abre. (Kaspersky Lab, 2017)

1.8.3. ***Troyanos:*** Los troyanos son programas maliciosos los cuales modifican, elimina y roban información. Estos también hacen que la computadora se haga lenta y cambie su rendimiento normal, diferentemente de los virus y los gusanos, los troyanos no se pueden multiplicar por el computador. (Rivero, 2008)

1.8.4. ***Rootkit:*** Son herramientas las cuales facilitan a los atacantes acceder a los sistemas. Estos programas ocultan los rastros de la persona que está atacando el sistema, también puede acceder a los Backdoors del sistema y puede usar Exploits para atacar otros sistemas. (Rivero, 2008)

1.8.5. ***Scripts:*** Son código dañino que se encuentra en las páginas web por lo general en su estructura interna, estos códigos alterados se procesan como página normal ya que el explorador no los detecta. De esta manera se puede robar la información. (Rivero, 2008)

1.8.6. ***Archivos Compartidos:*** Se usa para poder mandar archivos infectados los cuales se enfocan en atacar las ubicaciones de los archivos principales del sistema. (Rivero, 2008)

1.8.7. ***Archivos Masivos:*** Son los archivos los cuales se encargan de entrar en tu libreta de contactos para así poder mandar el correo y seguir infectando. (Rivero, 2008)

1.8.8. ***Web Brosing:*** Este ataque se da cuando el sistema que está infectado tiene acceso a la red, infecta a todos los archivos de contenido web de tal manera en la que los usuarios que pasan por las páginas que están infectadas se infectan. (Rivero, 2008)

1.8.9. ***Exploit:*** Este tipo de ataque malicioso se enfoca en explotar las deficiencias, bugs o vulnerabilidades del sistema. El enfoque de este tipo de ataque es tratar de dañar permanentemente el sistema al cual es designado para atacar. (Kaspersky Lab, 2017)

1.8.10. ***Simple Network Management Protocol:*** Estos protocolos son los más usados para el intercambio de información entre dispositivos por la red, de esta manera se los puede

administrar y supervisar. El ataque que ocurre por este medio busca los protocolos vulnerables y lo que hace es que genera a tareas muchas respuestas y también engañar haciendo solicitudes falsas para poder engañar.

1.8.11. ***Trackware:*** Se le llama así a todo programa que realiza un seguimiento de todo lo que realiza el usuario mientras esta en la red, tales como su historial, los clicks que da, descargas, etc. Este ataque genera un perfil del usuario el cual se usa para pasar publicidad. (Rivero, 2008)

1.8.12. ***Spear Phishing:*** Este es un tipo de estafa en la cual generalmente ocurre por medio del mail para poder robar los datos personales. Se diferencia del Phishing este es enfocado a grupos específicos. (Kaspersky Lab, 2017)

1.8.13. ***Joke:*** Son los programas que hacen simulación a un virus destructivo. Estos programas simulan que destruyeron archivos, pero son simples simulaciones que se pueden detectar.

1.8.14. ***Backdoors:*** Se la conoce comúnmente como puerta trasera, se basa en poder evitar los sistemas de seguridad del ordenador mediante código. Estas puertas están en los sistemas no por error si no para poder tener una forma secreta de acceso. Los primeros y más conocidos backdoors son NetBus y Back Orifice.

1.8.15. ***Hoaxes:*** También se los conoce como mensajes engañosos, estos mensajes ocurren por correo y es enviado de manera masiva, constan de contenido falso. Estos mensajes son comúnmente los de ayuda para un niño enfermo, o los que indican que ganaste la lotería. Su objetivo es más para poder saturar la red o servidores de correo.

1.8.16. ***Password Crack:*** Este ataque es el intento de descifrar las contraseñas ocupando métodos de recuperación de contraseñas, las cuales comúnmente aparecen o se brindan al usuario para poder recuperar su contraseña.

1.8.17. ***Man In the Middle:*** El MITM o en español hombre en el medio, este ataque ocupa un intermediario, por decir si te conectas a una red libre el atacante puede interceptar las comunicaciones que tienes y de esta manera poder tener acceso a lo que estas realizando.

1.8.18. ***Spam:*** El spam son los mensajes basuras los cuales el usuario no los solicita o no son de parte de conocidos. Estos mensajes suelen ser estorbosos y su fin es re direccionar a links o paginas basura para contaminar de virus, robo de datos o simplemente dañar el rendimiento del computador. (Kaspersky Lab, 2017)

1.8.19. ***Mail Bombing:*** Consiste en mandar varios correos con el mismo mensaje un sin número de veces con el fin de poder saturar la bandeja del mail.

1.8.20. ***Ransomwear:*** Se lo conoce como secuestro digital, este es un ataque el cual mediante un código dañino roba la información del usuario para después con eso poder pedir dinero para recuperar la información robada. (Rivero, 2008)

1.8.21. ***Fragmentación IP:*** Los ataques que se pueden dar en la fragmentación de IP es intentar la interrupción o negación de acceso del computador o red, esto se da mediante transmisión de datos los cuales se rompen en fragmentos pequeños, los datos se hacen más difíciles de ensamblar o armar, ocasionando que en este proceso se quede sin memoria intermedia.

1.8.22. ***Negación de Servicios****:* Estos ataques tienen el objetivo principal el negar el acceso a un servicio de la red de la empresa, estos ataques se dan por tiempos indefinidos. Los ataques se enfocan en ir al servidor para que de esta manera no se puedan ocupar. Estos ataques son sencillos de hacer, pero ocupan muchos recursos.

1.8.23. ***Spoofing****:* En este tipo de ataque la persona que lo realiza por una maquina pirata simula que es otra máquina de la red para que de esta manera pueda conseguir el acceso. Estos

ataques se pueden realizar de formas diferentes pero la más común es por cambio de IP. (Kaspersky Lab, 2017)

1.9. Ingeniería Social

La ingeniería social es una de las técnicas más usadas para el robo de información u obtención de datos, también es una de las que más se da en empresas o para usuarios por eso hay que estar preparados, también en empresas se capacita al personal, porque este método de ataque se basa en atacar a la persona y su mente. No importa cuanta seguridad se tenga para la protección de información ya que el dar el acceso a una persona siempre tendrá su riesgo, el riesgo humano, y por lo tanto este es vulnerable a la ingeniería social. (Castellanos, Revista .Seguridad - UNAM, 2011)

1.9.1. Que es la Ingeniería Social.

Su objetivo se basa en un principio "el usuario es el eslabón más débil", la manipulación se da por técnicas psicológicas y habilidades sociales las cuales tienen como fin, el robo de información de una persona para que de esta manera se pueda entrar a sistemas y hacer lo que el atacante desee.

Este método se puede considerar un arte ya que es una manera complicada en la que pocos pueden llegar a desarrollar, ya que tienes que entrar a la mente del usuario mediante actitudes que presentar o formas que das para que el humano pueda entregarte información sin que él lo perciba o se dé cuenta. (Castellanos, Revista .Seguridad - UNAM, 2011)

1.9.2. Formas de Ataques.

Existen varias maneras de atacar a la persona para poder obtener la información, pero principalmente se centran en:

1.9.2.1. ***Ataque telefónico*****:** Este ataque es uno en el que el atacante este persistente para robar la información, se realiza una llamada a la víctima y el atacante se hace pasar por otra persona, por lo general dicen que son de entidades bancarias, ofertas, soporte técnico, encuestas, etc. De esta manera se saca información básica del usuario la cual se puede usar para poder robar la contraseña de correo o recuperar claves las cuales te dan acceso a información valiosa del usuario. (Castellanos, Revista .Seguridad - UNAM, 2011)

1.9.2.2. ***Ataque por Internet*****:** Los ataques que se dan en la red más comunes llegan a darse mediante correo electrónico por el cual se enfocan en obtener datos personales mediante malware, también los otros ataques que se pueden dar son mediante páginas web falsas o links de redirección para que mediante esto se simula formularios para que se ingresen datos personales o si es el otro caso es el simular una web para que el usuario pueda hacer un login y obtener sus datos. Otro tipo de ataque de red es el que se da mediante un chat virtual que su afán es simular que es una persona conocida que quiere sacarte información. (Castellanos, Revista .Seguridad - UNAM, 2011)

1.9.2.3. ***Dumpster Diving, Trashing*****:** Esto ya no es muy común pero este ataque se enfoca en buscar información personal en la basura de la persona, como: agendas, cuadernos, etc. También buscan CD's o USB o chatarra informática del usuario para ver si encuentran datos útiles. (Castellanos, Revista .Seguridad - UNAM, 2011)

1.9.2.4. ***Ataque SMS*****:** Estos ataques se enfocan en mandar mensajes los cuales quieren aparentar ser promociones, cupones, o quieren brindar un servicio, luego de esto si

es que el usuario acepta o responde hace que se envíen datos importantes o personales. (Castellanos, Revista .Seguridad - UNAM, 2011)

1.9.2.5. ***Ataque Cara a Cara*:** Este método es uno de los más difíciles pero muy efectivo. En este ataque la persona se acerca a la víctima para sacar información de manera en que esta trata de hacerse buen amigo para que de este modo la victima entre información con facilidad. El atacante tiene que ser muy social y agradable para por lograr esto, aparte este método lleva largos periodos de tiempo. (Castellanos, Revista .Seguridad - UNAM, 2011)

1.9.2.6. ***Exploit de Familiaridad*:** Este método se basa en acercarse a los familiares y amigos de la víctima para que mediante esto llegar a sacar información y con esto también entra en el ambiente en el que se maneja la persona atacada dándole facilidad al atacante el control y el conocimiento de la situación. (Castellanos, Revista .Seguridad - UNAM, 2011)

1.9.2.7. ***Entrar a su Ambiente de Trabajo*:** Consiste en que el atacante intenta pertenecer al ambiente en el que se mueve el usuario tal es el caso de llegar a entrar al mismo trabajo para poder acercarse a la víctima y a los datos que desea robar con mayor facilidad. (Castellanos, Revista .Seguridad - UNAM, 2011)

1.9.2.8. ***Explotar la Sexualidad*:** Este ataque se basa en jugar con los deseos de la víctima para que de esta manera el hombre o mujer se pueda acercar más y por actos de manipulación sacar la información deseada. (Castellanos, Revista .Seguridad - UNAM, 2011)

1.9.3. Defenderse de la Ingeniería Social.

La ingeniería social es de gran riesgo para las empresas ya que se enfocan en las fallas humanas que en las fallas de software o hardware. De esta manera los Ingenieros Sociales expertos tienen muchas maneras de poder lograr ataques o lo propuesto como objetivo con facilidad. (Izaskun Pellejero, 2006)

Las empresas u organizaciones tienen que aprender a enfrentar estos problemas de manera que dan capacitaciones a los empleados para que conozcan los tipos de ataques y las distintas formas que pueden llegar a acercarse los Ingenieros Sociales a las víctimas.

Estos problemas se resuelven afrontándolos mediante medidas preventivas, algunas sugeridas son:

- Nunca hablar de la información personal o confidencial en lugares públicos o con personas que no son de confianza.
- Si se sospecha de alguien informar al respecto para que se puedan tomar medidas o se realicen investigaciones.
- Implementar medidas de seguridad, tanto dando charlas y educando al personal.
- Efectuar controles de seguridad rutinarios como auditorias o pentest en la empresa.

(Castellanos, Revista .Seguridad - UNAM, 2011)

1.10. Redes

1.10.1. Que es una Red de Ordenadores.

Una red de computadoras u ordenadores, o simplemente "la red" es un conjunto de equipos interconectados con el fin de intercambiar información o datos. Pero para entrar más en detalle una red de ordenadores, es un conjunto de hardware y software que se utiliza para asegurar la comunicación entre ordenadores, estaciones de trabajo y ordenadores.

1.10.2. Tipología de las Redes .

Probablemente la clasificación más simple y básica. Son distinguidos tres principales redes:

- **LAN:** Local Area Network o más conocida como red de área local. Los equipos están conectados a través de cables o dispositivos inalámbricos en un área geográfica más pequeña.
- **MAN:** Metropolitan Area Network, por su parte una red más grande geográficamente normalmente cubre una metrópolis (ciudad).
- **WAN:** Wide Area Network, es una red aún más grande (varios cientos de kilómetros) y permite interconectar LANs remotas. Internet es el mejor ejemplo de una WAN muy grande.

1.10.3. Tipos de Arquitecturas de Red.

1.10.3.1. ***Cliente / Servidor Arquitectura*****:** La arquitectura cliente / servidor se refiere a un modo de comunicación entre varios ordenadores en una red. Uno o más clientes por lo general solo un servidor puede distinguirse allí. De este modo, cada cliente puede enviar peticiones a un servidor cuyo papel es el de ser una espera pasiva para una petición de cliente.

1.10.3.2. ***Arquitectura Multi Niveles*****:** A diferencia de cliente / servidor que tiene sólo dos tipos de equipos de una red: clientes y servidores. La arquitectura de múltiples niveles divide el servidor en varias entidades especializadas que crean más de dos tipos de ordenadores, de ahí el término "multi niveles".

1.10.3.3. ***Arquitectura Par a Par*:** Este tipo de arquitectura se opone radicalmente al modelo cliente / servidor. De hecho, en P2P, todos los elementos de red son iguales y son alternativamente cliente y el servidor.

1.10.4. Clasificación de Redes por Servicio.

Una red se puede clasificar de acuerdo a su uso y los servicios que ofrece. Esta división también se solapa con la noción de escala. Por lo tanto, para redes que utilizan tecnologías de Internet (familia TCP / IP), la nomenclatura es la siguiente:

1.10.4.1. ***Intranet*:** Red interna de una entidad organizativa. A diferencia de Internet, intranet es una red privada que se puede acceder por vía interna de ahí el prefijo "Intra". Esto es típicamente sitios de la empresa que son accesibles solamente a los empleados cuando están en el trabajo.

Una intranet se basa en una infraestructura técnica muy similar a la de Internet, excepto que el tamaño es mucho menor, y el acceso está limitado a personal de la empresa que conecta desde un ordenador de la red local (LAN) de los negocios y el uso de un nombre de usuario y una contraseña.

Una intranet es útil para comunicarse con los empleados, lo que les permite ser pagados casos administrativos o incluso el uso del sistema de información de la compañía a través de una interfaz web. (Miguel, 2015)

1.10.4.2. ***Extranet*:** La red externa a una unidad organizativa. Es nada menos que la extensión de la intranet al exterior de la empresa.

De hecho, cuando la empresa quiere proporcionar a sus empleados son de intranet, que debe ser accesible desde fuera de la empresa a la que el prefijo "Extra".

En este caso, el cableado utilizado para conectarse a Internet que el empleado o estudiante usa para ver los sitios de intranet, pero debe identificarse necesariamente (usuario y contraseña) y utilizar la mayoría de las veces una conexión segura para cifrar los datos y evitar intrusiones, mientras que en una Intranet hay poco riesgo porque el que se conecta necesariamente estar en el negocio. (Miguel, 2015)

1.10.4.3. ***Internet*:** La red de redes interconectadas a nivel mundial. También es conocida como la red global la cual está compuesta por sitios web alojados en servidores de todo el mundo y los cuales están al alcance de todos a través de un simple navegador y una conexión a Internet. (Miguel, 2015)

1.11. Protocolos

1.11.1. Que es un Protocolo.

Un protocolo es un conjunto de reglas y procedimientos estándares que deben observarse para enviar y recibir datos a través de una red. Esta estandarización tiene el objetivo principal de permitir que dos programas por lo general se ejecutan en máquinas diferentes para comunicarse y entenderse entre sí.

También se puede decir que un protocolo es un método estándar que permite la comunicación entre procesos (posiblemente se ejecutan en máquinas diferentes), es decir un conjunto de reglas y procedimientos a seguir para transmitir y recibir datos a través de una red.

Podemos ver un cuadro comparativo con las similitudes entre OSI y TCP/IP con sus protocolos:

Tabla 1: Servicios y Protocolos

TCP/IP	Servicios y Protocolos	OSI
Aplicación	NTP, PING, HTTP, TELNET, FTTP.	Aplicación
		Presentación
		Sesión
Transporte	UDP, TCP	Transporte
Network	ICMP, IP, IGMP, ARP	Network
Interface de Red	Ethernet	Red de Datos
		Físico

Autor: R Avilés, M Silva, enero 2017

1.11.2. Protocolos de Aplicación.

Los protocolos de la categoría de aplicación aseguran la interacción y el intercambio de datos:

- APPC (Programa Avanzado de Programa de Comunicación) es la extensión del protocolo SNA al elemento que IBM utiliza principalmente en los equipos AS / 400.
- FTAM (File Transfer acceso y gestión) es un protocolo de acceso a archivos OSI.
- X.400 es un protocolo CCITT (Comité Consultivo Internacional de Telegrafía y Telefonía) para la transmisión internacional de correo electrónico.
- X.500 del CCITT es un protocolo que ofrece servicios de archivos y directorios que abarcan múltiples sistemas.
- SMTP (Simple Mail Transfer Protocol) es un protocolo de Internet para transferir correo electrónico.
- FTP (File Transfer Protocol) es un protocolo de Internet para la transferencia de archivos.
- SNMP (Simple Network Management Protocol) es un protocolo de Internet para redes de vigilancia y sus componentes.

- Telnet es un protocolo de Internet para conectarse al host remoto y el procesamiento de datos local.
- SMB (Server Message Blocks) es el redirector de cliente (shell) MICROSOFT.
- PNC (Novell NetWare Core Protocol) es el redirector de cliente (shell) de Novell.
- APPLETALK AppleShare y está siguiendo el protocolo MANZANA.
- AFP (AppleTalk Filing Protocol) es un protocolo de APPLE (para los ordenadores Macintosh) para el acceso remoto a archivos.
- DAP (Protocolo de Acceso de Datos) es un protocolo para el acceso a archivos DECnet.

1.11.3. Protocolos de Transporte.

Los protocolos de la categoría de transporte proporcionan conexiones y transferencias de datos de control:

- TCP (Protocolo de control de transmisión) es parte del protocolo de Internet TCP / IP que garantiza la entrega de datos de la secuencia.
- SPX (Sequential Packet Exchange) es una parte del protocolo IPX / SPX NOVELL que garantiza la entrega de datos de secuencias. Es un protocolo de reducción, rápido y enrutable. SPX / IPX es un derivado del protocolo XNS (Xerox Network System), que fue desarrollado por la empresa XEROX para redes Ethernet locales. La pila XNS es un protocolo que ha sido ampliamente distribuido en la década de 1980 pero fue sustituido gradualmente por la pila TCP / IP. La pila XNS genera muchos mensajes de difusión general (broadcast), que hizo que la lenta además de ser voluminoso.
- NWLink es la versión de Microsoft del protocolo IPX / SPX de Novell.

- NetBEUI (NetBIOS Extended User Interface) es un protocolo que crea sesiones NetBIOS (Red Basic Input Output System) y proporciona servicios de transporte de datos (NetBEUI). NetBEUI se basa en el protocolo de transferencia de SMB.
- ATP (Protocolo de Transacción AppleTalk) y NBP (Nombre Binding Protocol) son protocolos para ordenadores Apple Macintosh.
- X.25 es un conjunto de protocolos para redes de conmutación de paquetes utilizados para conectar los terminales remotos a los sistemas host de gran tamaño (en servidor).

1.11.4. Protocolos de Red.

Los protocolos de red Categoría proporcionan enlaces a servicios (direccionamiento, enrutamiento, la comprobación de errores y solicitud de retransmisión) y definen la red de reglas de comunicación Ethernet, Token Ring, etc.

- IP (Protocolo de Internet) es la parte del protocolo de Internet TCP / IP que rutas y enrutar paquetes.
- IPX (Intercambio de paquetes de Internet working) es la parte del protocolo IPX / SPX NOVELL que las rutas y encaminar los paquetes.
- NWLink es la versión de Microsoft del SPX / IPX NOVELL.
- NetBEUI es un protocolo que proporciona servicios de transporte a las aplicaciones y sesiones NetBIOS.
- DDP (Protocolo de datagramas de entrega) es un protocolo AppleTalk para el transporte de datos (para los ordenadores Macintosh).

1.11.5. Protocolos Direccionables o de Routing.

Hasta mediados de los años 80, las redes locales se componen de un único segmento de cable, y la mayoría se aislaron las redes. La evolución de la tecnología y los requisitos han dado lugar a una apertura y conexión de las redes. Las redes locales se convertirían en subconjuntos de redes más grandes, una parte integral de una "red de área amplia".

La complejidad de las redes ha aumentado con el tiempo. Las rutas posibles para que un paquete alcance su objetivo crece según el número de nodos de la red. Era necesario no sólo garantizar que el paquete llegara a su destino, sino también hacerlo en un plazo razonable. Algunos protocolos permiten que el paquete pase por varias rutas, que se llaman "protocolos enrutables". Los protocolos enrutables permiten que el paquete alcance su objetivo lo más rápido posible:

- El uso de la ruta más corta
- Mediante la ruta menos congestionada, dependiendo del tráfico de red

Los protocolos direccionables permiten que los paquetes "a través de" routers.

1.11.6. Protocolos TCP/IP.

TCP / IP (Transmission Control Protocol / Internet Protocol) es el más conocido del protocolo, ya que es la que se utiliza en la red de redes, por ejemplo, Internet. Históricamente, TCP / IP tenía dos desventajas principales, su tamaño y lentitud. El protocolo TCP / IP es parte del sistema operativo UNIX desde mediados de la década de 1970 (antes es el UUCP (Unix to Unix Copy Program) que fue utilizado para copiar archivos y mensajes de correo electrónico entre dos máquinas).

TCP / IP es un estándar abierto, es decir, los protocolos que componen la pila TCP / IP fueron desarrollados por diferentes proveedores sin consulta. El IETF (Internet Engineering Task Force) reunió a los diferentes protocolos en la pila TCP / IP para que sea un estándar. El trabajo de la IETF es regularmente objeto de toda la "comunidad de Internet" en los documentos llamados RFC (Request For Comments). RFC se consideran corrientes de aire porque las especificaciones que contienen podrían en cualquier momento ser revisados y reemplazados. El IETF está tratando de decidir en este momento en un estándar (calendario de Internet, Programación de Protocolo simple de transferencia) para las agendas de transporte de datos y horarios.

TCP / IP es una gran pila relativamente de protocolos, lo que puede causar problemas con un cliente como MS-DOS. Sin embargo, los sistemas operativos de red con interfaz gráfica de usuario como Windows 95 o Windows NT no tienen limitación de memoria para cargar la pila TCP / IP. En cuanto a la velocidad de ejecución y la transmisión de paquetes, el TCP / IP asciende a IPX / SPX.

Tabla 2: Protocolos de Pila TCP/IP

Los Protocolos de la Pila de TCP / IP	
Nombre	**Función**
FTP	FTP (File Transfer Protocol) se encarga de la transferencia de archivos.
TELNET	TELNET establece una conexión con un host remoto y gestionar los datos locales.
TCP	TCP (Transmission Control Protocol) asegura que se establecen y mantienen las conexiones entre dos ordenadores.
IP	IP (Protocolo de Internet) gestiona las direcciones lógicas de los nodos.
ARP	ARP (Address Control de la Resolución) coincide con las direcciones lógicas (IP) a las direcciones físicas (MAC).
RIP	RIP (Routing Information Protocol) es la ruta más rápida entre dos ordenadores.
OSPF	OSPF (Open Shortest Path First) es una mejora a RIP, más rápido y más fiable.
ICMP	ICMP (Internet Control Message Protocol) controla los errores y envía mensajes de error.
BGP / EGP	BGP / EGP (Border Gateway Protocol / Exterior Gateway Protocol) gestiona la transmisión de datos entre redes.
SNMP	SNMP (Simple Network Protocolo de Gestión) permite a los administradores de red gestionar sus equipos de red.
PPP	PPP (Point to Point Protocol) se utiliza para establecer una conexión remota por teléfono. PPP (después de SLIP) es utilizado por los proveedores de servicios de Internet.
SMTP	SMTP (Simple Mail Transport Protocol) para enviar correos electrónicos.
POP3 e IMAP4	POP3 (Post Office Protocol versión 3) e IMAP4 (Internet Message Protocol version 4 Publicidad) se utilizan para conectarse a un servidor de correo y recuperar su correo electrónico.

Autor: R Avilés, M Silva, enero 2017

1.12. Firewall

1.12.1. Que es el Firewall.

Podemos definir como firewall a los sistemas de seguridad que conforman una parte vital de una red corporativa, son los encargados de permitir o denegar accesos, sus principales funciones son la de bloquear paquetes que vienen de determinados rangos de IP, bloqueo de paquetes por aplicaciones no autorizadas, bloqueo de paquetes que son identificadas como ataques informáticos, integra sistemas de defensa con virus, spam y malware. (Ramos, 2015)

Una forma de clasificar los firewalls es por modo de empleo:

Modelo de arquitectura: si existe uno o más firewall implementados en una red, el que se encuentra más externo y tiene comunicación con otras redes se lo denomina firewall de contención, los que se encuentran más internamente y protege las redes internas se llama firewall bastión, en cambio cuando solo existe un firewall protegiendo la red se lo denomina bastión. (Ramos, 2015)

Instaladores de software vs appliance: Algunos firewalls se los implementa mediante instaladores, tal es el caso como los Iptables de Linux, Isa server de Microsoft. Existe otro tipo de implementación como es el appliance, estos requieren de la instalación del software lo único que requiere es que conecte y se reinicie el dispositivo, una vez iniciado se podrá procederá realizar el proceso de configuración, un ejemplo de este tipo son PIX Firewall de Cisco, Netscreen de Juniper, etc. (Ramos, 2015)

Muchos fabricantes ofrecen sus soluciones de firewall en formato appliance, ya que a los fabricantes de hardware les gusta trabajar con otros fabricantes terceros de software, para integrar sus soluciones de antivirus o antispam, y así poder ofrecer un dispositivo "todo en uno". (Ramos, 2015)

1.10.2. Características de los Firewalls.

1.10.2.1. Características de Firewalls en Software.

- Soportados por varios sistemas operativo.
- Pueden ser instalados en varias plataformas hardware.
- Altamente configurables.

1.10.3. Firewall de Host vs Firewall de Red.

Su principal diferencia está en el entorno que se desea proteger. Mientras uno lo hace solo en los sistemas donde se encuentran instalados, otros protegen la red o redes donde se han implementado.

1.10.3.1. Características de firewall de red.

- Protege redes completas.
- Sistema dedicado a la función de Firewall.
- Módulos adicionales como IDS/IPS, antivirus o anti-spam.
- Requieren recursos dedicados de CPU y memoria RAM.

(Ramos, 2015)

1.10.3.2. Características de Firewall en el ordenador personal.

- Firewalls personales.
- En algunos casos ya están embebidos en el sistema operativo.
- Fabricantes de antivirus proveen soluciones "todo en uno" para los usuarios, donde incluyen módulos de firewall.

(Ramos, 2015)

1.11. Proxys

Los servidores Proxy se ejecutan en unos pocos programas que pueden ser seguros y confiables. Estos programas son aplicaciones específicas, cada protocolo soportado tiene su propio servicio proxy gestionado por un Proxy genérico. Realiza conexiones punto a punto de vista técnico el proxy es servidor y cliente al mismo tiempo ya que tiene funciones de listener y de iniciador. La comunicación a través de un proxy requiere varios niveles de autenticación. (Ramos, 2015)

1.11.1. Características de una conexión Proxy.

- Usuario realiza petición de un servicio de Internet, como HTTP, FTP. Telnet, etc.
- El software instalado en el sistema del cliente lanza la petición de acuerdo con la política de seguridad a utilizar para el servicio de Internet requerido.
- El proxy provee conexión actuando como Gateway de servicio remoto.

- El proxy realiza las comunicaciones necesarias para establecer la conexión con los sistemas externos, mientras protege los sistemas que se ubican detrás de él.
- Todo el tráfico se encamina entre el usuario interno y el sistema externo a través del Proxy Gateway.
- Ejemplo: servicios Proxy para correo. El servicio en el firewall acepta todos los correos con dirección interna y entonces realiza un forward a los sistemas internos o al servidor de correo central interno.
- Al realizarse la comunicación entre el usuario interno y el servicio externo a través del Proxy, éste protege la dirección IP del usuario, el sistema operativo que ejecuta en su sistema (a través de técnicas de identificación como las de passive fingerprint).
- EL sistema Proxy debe ser implementado para ser usado por un solo servicio (si es posible), no configurar cuentas de usuario, no instalar en ellos compiladores ni otros programas innecesarios, etc.

(Ramos, 2015)

1.11.2. Tipos de Proxy.

1.11.2.1. *Proxy Inverso*: es utilizado normalmente fuera del firewall para implementar un servidor de contención seguro para los clientes externos, previniendo directamente los accesos no monitorizados de los servidores internos por parte de los usuarios externos. Se puede usar también para mejorar el rendimiento, ya que múltiples proxies pueden ser implementados en un frontal para realizar load balancing de los usuarios con accesos pesados. (Ramos, 2015)

1.11.2.2. *Proxy de Aplicación*: son programas cliente servidor implementados para cada servicio. El ejemplo más notable son los proxies de HTTP. (Ramos, 2015)

1.11.2.3. *Proxy de Circuito*: además de filtrar por dirección IP, número de puerto u otro tipo de información contenida en las cabeceras, puede validar y monitorizar cada una de las sesiones que se establecen en la comunicación. El proxy de circuito determina que la sesión es válida basándose en reglas como la dirección IP de destino/origen, el puerto de destino/origen, protocolo, usuario ID, password, fecha. Etc… pudiendo gestionar el tráfico UDP. (Ramos, 2015)

1.11.3Conceptos

Antes de implementar cualquier firewall se van a definir una serie de conceptos o técnicas básicas con los que trabajan la mayoría de firewalls.

(Ramos, 2015)

1.12.1. **NAT:** (Network Address Translation), es básicamente el método por el cual la dirección IP es mapeada desde un grupo a otro, que a su vez es transparente a los otros usuarios. Otro método de mapeo es el de NAPT (Network Adress Port Translation), donde un conjunto de puertos asociados a direcciones IP son trasladados a otros puertos de una dirección IP. Hay dos tipos básicos de NAT:

1.12.2. NAT estático: cada dirección IP se enmascara en otra dirección IP, de modo que la relación es uno a uno. Este tipo de NAT se utiliza, por ejemplo, para ocultar los servidores de acceso público a Internet, ya que se oculta detrás de una dirección IP del firewall.

1.12.3. NAT dinámico: varias direcciones IP se enmascaran detrás de una dirección IP de firewall. Este tipo de NAT se implementa en redes que se ocultan detrás de la IP del firewall, siendo la relación varios a uno.

(Ramos, 2015)

1.12.4. Spoofing: Es la técnica de envío de paquetes con información falsa, donde puede parecer que el origen del paquete proviene de una red que se encuentra protegida por el firewall. En este caso, las direcciones IP de origen son del rango de las direcciones privadas de una red interna, pero el flujo de los paquetes es "hacia el interior del firewall, con entrada por la tarjeta externa de éste". Si penetran este tipo de paquetes, uno de los hosts que se encuentran en la red interna puede llegar a determinar que provienen de un sistema confiable y que puede acceder a su información. (Ramos, 2015)

Esto se realiza con herramientas de crafting de paquetes como hoping o scapy. Establecer reglas anti-spoofing, como las de no permitir entradas al firewall cuyas direcciones IP de origen sean privadas además de deshabilitar el enrutamiento de origen, protege de este tipo de ataques. (Ramos, 2015)

1.12.5. Fragmentación: Los ataques de fragmentación fueron diseñados para contrarrestar el filtrado de paquetes. En principio las tecnologías de filtrado dejaban pasar todos los fragmentos, pero se implementaron mejoras donde se verificaba el primer fragmento, y si pasaba los filtros, se permitía pasar los siguientes. La verificación de la cabecera del primer fragmento dio lugar a la división de la información de los puertos TCP y UDP en fragmentos más pequeños La RFC 1858 define los métodos para detener la fragmentación. (Ramos, 2015)

1.12.6. Sistema de Detección de Intrusos (IDS): IDS o sistemas de detección de intrusos son sistemas de software o hardware diseñado para ser capaz de automatizar los eventos de monitoreo que se producen en una red o en una máquina en particular, y que informe al administrador del sistema, todos los rastros actividad anormal en él o en la máquina monitoreada. Los IDS es un sistema de detección pasivo. El administrador puede decidir

si desea bloquear esta actividad. Estos sistemas de monitorización de red se han vuelto casi indispensable debido a la cada vez mayor en número y peligrosidad de los ataques a la red en los últimos años.

(Larrieu, 2013)

Existen diferentes métodos para identificar ataques:

1.13. Modelo De Análisis

El más simple y más comúnmente utilizado para detectar intrusiones. Una base de conocimientos contiene todas las cadenas alfanuméricas característicos de una intrusión. (Larrieu, 2013)

1.14. Investigación Genérica

Adaptado a los virus. Mirando en los comandos de código ejecutables que son potencialmente peligrosos. Por ejemplo, se detecta un comando de DOS sin referencias, las emisiones de los centros comerciales, las instrucciones relacionadas con los ataques conocidos. (Larrieu, 2013)

1.15. El Control De Integridad

Enfoque de comportamiento a los sistemas consisten en la detección de las diferentes anomalías en la red. El administrador define el funcionamiento "normal" de los elementos monitorizados, así que hay una curva de aprendizaje para establecer ese nivel. A continuación, el IDS será capaz de informar al administrador de cualquier situación que divergen desde el nivel operativo de referencia. La operación de referencia puede ser desarrollada por los diferentes análisis estadísticos del elemento a ser monitoreados. Este sistema de detección tiene una ventaja en comparación con el anterior: detecta nuevos tipos de ataques. Sin embargo, a veces se hará cambios en la explotación de referencia corresponde mejor a la actividad normal del usuario y por lo tanto reducir las falsas alarmas que resultarían. (Larrieu, 2013)

CAPÍTULO 2

DATOS DE LA EMPRESA

2.1. Misión

Blenastor C. A. es la más importante empresa ecuatoriana fabricante de productos de cuidado oral cuyo objetivo es satisfacer los requerimientos de los consumidores con productos especializados de la más alta calidad y el aporte de un grupo humano competente y alineado a los objetivos y valores institucionales.

2.2. Visión

Ser líderes en la fabricación y comercialización de productos especializados para el cuidado oral y afines.

2.3. Giro de Negocio

El giro de negocio de la empresa Blenastor C.A. es la de industria de transformación, ya que es un establecimiento de una industria que se dedique a la transformación de materia prima en productos terminados.

2.4. Análisis de la infraestructura tecnológica y red de datos.

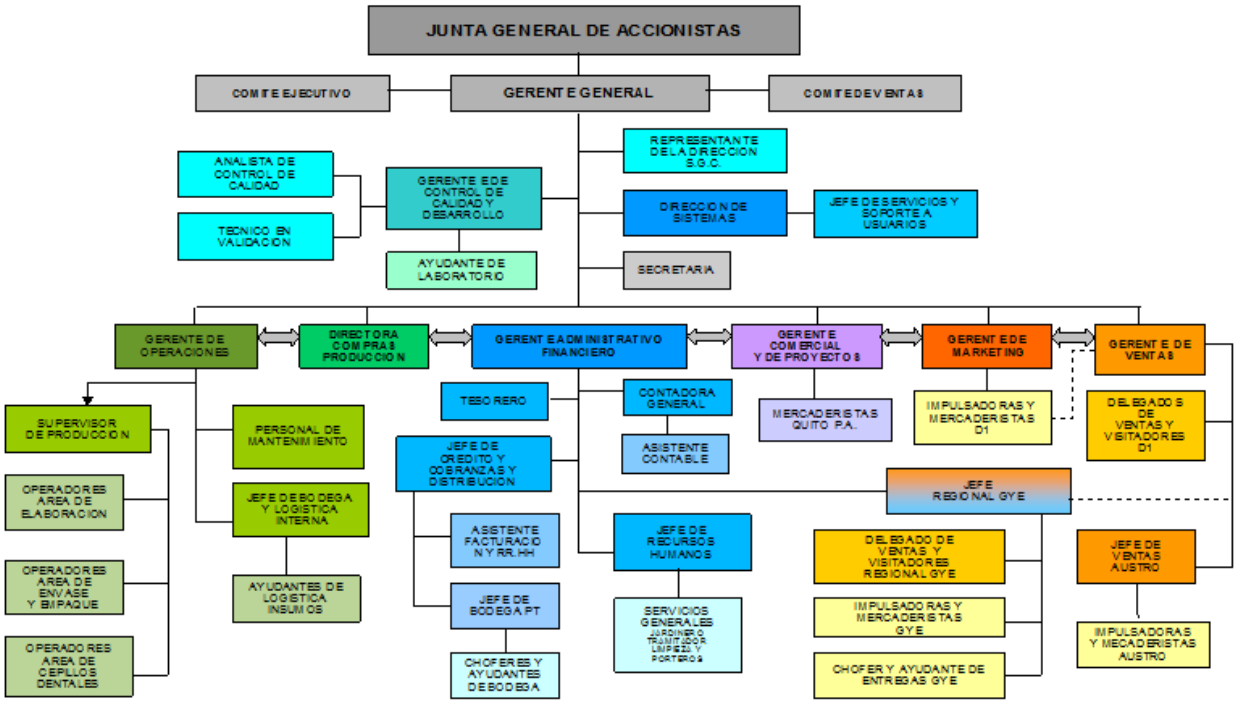
La empresa dejó de utilizar sus propios servidores hace un año y medio, desde entonces otra empresa se hizo cargo de los servidores de la empresa.

Blenastor cuenta con un firewall para la protección de sus archivos.

- La empresa consta de 25 computadoras, marca Dell.
- 9 impresoras Epson.
- Router Wi Fi marca Cisco.
- El Sistema operativo que utilizan es Windows 8.
- El sistema que utilizan en sistemas Windows Server 2012.
- Utilizan programas como as400 y Cpp.
- También utilizan un módulo de compras.

2.5. Mapa de procesos de la empresa Blenastor.

2.6. Diagrama de Jerarquía.



CAPÍTULO 3

CONFIGURAR LAS HERRAMIENTAS DE HACKING ÉTICO

3.1. Nmap

Ilustración 1: Logo Nmap

Network Mapper, 2016

El Nmap o "mapeador de redes" es una herramienta de código abierto para exploración de red y auditoría de seguridad, escrito originalmente por Gordon Lyon (Fyodor Vaskovich), que es un experto en seguridad de redes, escritor de varios libros y hacker. Inicialmente se lo diseñó para analizar grandes redes de una forma rápida y eficiente, pero funciona muy bien contra equipos individuales. (ConectaBell, 2015)

Sus inicios fueron en el año 1997, el lenguaje original en el cual fue programa o codificado fue en C, principalmente cuando recién surgió, este programa era solo soportado por sistemas Linux, es un inicio era un programa básico y solo cumplía las funciones principales que le dio el programador. Después de un tiempo el programa fue modificado y reescrito en C++ añadiéndole más funcionalidades, una de las más importantes en ese entonces era el soporte del protocolo IPv6. (ConectaBell, 2015)

La forma de trabajar de Nmap, es utilizar paquetes IP "crudos" que ayuda a mostrar que ordenadores se encuentra conectados a una Red. Básicamente Nmap es muy utilizado en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios

y la monitorización del tiempo que los equipos o servicios se mantiene activos. (Lyon, Nmap Network Scanning, 2008)

En lo referente a la seguridad, este es utilizado para poder realizar pruebas de intrusión, poder encontrar servicios abiertos, saber la versión en la cual se encuentra el sistema operativo de un ordenador y a su vez también de todos los programas. (ConectaBell, 2015)

La característica principal de esta herramienta es la de permitir determinar los puntos débiles de una red, los cuales pueden ser aprovechados por individuos de malas intenciones que quieran perjudicar a una empresa, institución y las personas que lo integran.

Como sabemos este programa viene para distintos sistemas operativos, tales como Mac OS X, Debian, Fedora, Windows. En nuestro caso nos vamos a enfocar solamente en la instalación de Windows, debido a que es el sistema operativo más usado por las empresas a nivel nacional.

Los puertos TCP descendentes en orden de accesibilidad:

Tabla 3: Puertos y Servicios

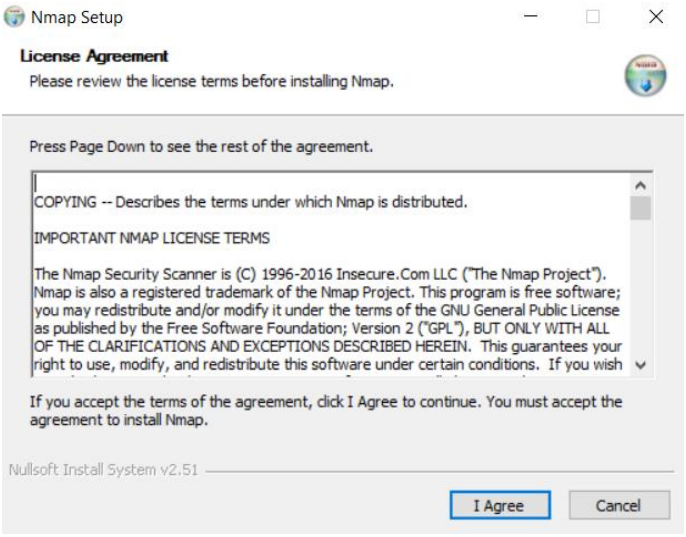
Número de Puerto	Servicio	Razón
80	http	La prevalencia de los servidores web en Internet lleva a muchos novatos a creer que la Web es Internet
25	smtp	Mail es otro "killer app" de Internet que las empresas permiten a través de sus firewalls
22	ssh	SSH parece haber superado finalmente Telnet como el estándar para la administración terminal remota.
443	https	SSL es una forma popular para que los sitios web protejan la información confidencial del directorio.
21	ftp	Este protocolo de transferencia de archivos continua activo, ya no es muy utilizado.
113	auth	El servicio auth permite a los servidores solicitar el nombre de usuario de los clientes conectados a ellos. Los administradores suelen dejar este puerto sin filtrar para evitar largos tiempos de espera que pueden ocurrir cuando las reglas de firewall impiden que los servidores se conecten de nuevo al puerto 113. El uso de este puerto para la exploración de ping puede dar lugar a falsos positivos, ya que algunos administradores han configurado sus firewalls para forjar RST en respuesta a las consultas de autenticación a cualquier IP de su red, incluso cuando no exista ninguna máquina en esa IP. El administrador hace esto para evitar los tiempos de espera del servidor mientras se impide que se accedan a los puertos.
23	Telnet	Muchos dispositivos todavía ofrecen esta interfaz administrativa, aunque es una pesadilla de seguridad.
53	domain	Los servidores de nombres de dominio están muy extendidos
554	rtsp	Real Time Stream Control Protocol es utilizado por los servidores de medios, incluyendo QuickTime y RealServer
3389	ms-term-server	Microsoft Terminal Services permite a los usuarios (ya veces a los hackers) acceder a aplicaciones y datos en una computadora remota
1723	pptp	Protocolo de túnel punto a punto se utiliza a menudo para implementar soluciones VPN en Microsoft Windows
389	ldap	El protocolo ligero de acceso a directorios se utiliza a menudo para almacenar directorios de contactos y similares.
636	ldapssl	LDAP sobre SSL es popular para acceder a información confidencial
256	FW1-securemote	Los dispositivos Firewall de Checkpoint-1 suelen tener este puerto de administración abierto.

(Official Nmap Project Guide to Network Discovery and Security Scanning, 2008)

3.1.1. Método de instalación

Paso 1. El método de instalación de Nmap en Windows, es similar a cualquier programa que se instala en Windows. Solo se debe estar de acuerdo con los términos de uso.

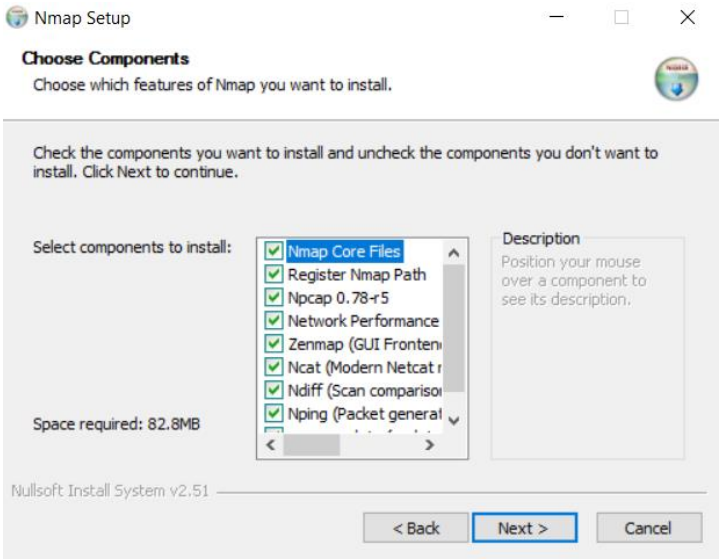
Ilustración 2: Instalación Nmap



Autor: R Avilés, M Silva, enero 2017

Paso 2. Seleccionar los componentes que se vaya a utilizar, en este caso todos.

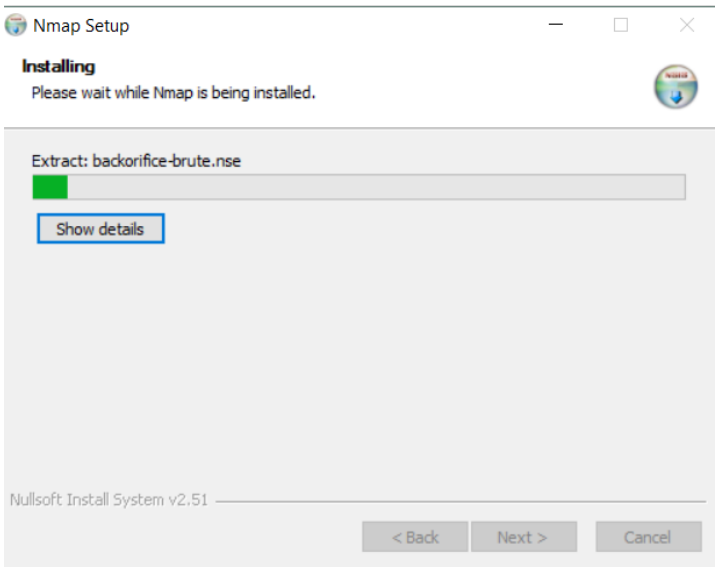
Ilustración 3: Instalación Nmap



Autor: R Avilés, M Silva, enero 2017

Paso 3. Y finalmente se presione instalar y se espera hasta que el programa esté totalmente instalado.

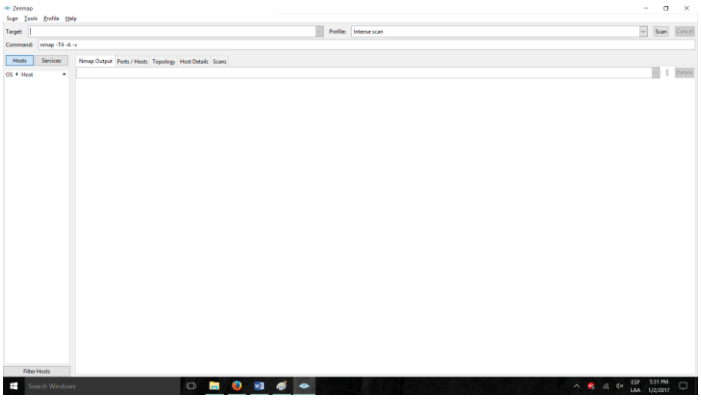
Ilustración 4: Instalación Nmap



Autor: R Avilés, M Silva, enero 2017

Paso 4. Este es la ventana principal de Zenmap.

Ilustración 5: Instalación Nmap



Autor: R Avilés, M Silva, enero 2017

3.2. Nessus

Ilustración 6: Logo Nessus

Tenable Network Security, 2016

Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. El proyecto Nessus comenzó en 1998, cuando Renaud Deraison (es conocido en la comunidad de la seguridad global como el padre del escáner de vulnerabilidades Nessus) quiso que la comunidad de Internet tuviese un escáner remoto de seguridad que fuese libre, aunque a día de hoy su licencia ha cambiado (se ha convertido en software privativo, Renaud co-fundador de Tenable Network Security en el año 2002).

Nessus es una herramienta de escaneo de seguridad remota, que escanea una computadora y genera una alerta si descubre cualquier vulnerabilidad que los hackers maliciosos podrían usar para acceder a cualquier computadora que haya conectado a una red. Esto lo hace corriendo más de 1200 controles en una computadora determinada, probando para ver si alguno de estos ataques podría ser utilizado para entrar en el equipo o dañarlo de otro modo.

Nessus es una gran herramienta que ayuda a mantener sus dominios libres de las vulnerabilidades fáciles que los hackers y los virus comúnmente buscan explotar. Nessus es una herramienta de escaneo de seguridad remota, que escanea una computadora y genera una alerta si descubre cualquier vulnerabilidad que los hackers maliciosos podrían usar para acceder a cualquier computadora que haya conectado a una red. Esto lo hace corriendo más de 1200 controles en una computadora determinada, probando para ver si alguno de estos ataques podría ser utilizado para entrar en el equipo o dañarlo de otro modo.

¿Quién usaría una herramienta como esta?

Si usted es un administrador encargado de cualquier computadora (o grupo de computadoras) conectada a Internet, Nessus es una gran herramienta que ayuda a mantener sus dominios libres de las vulnerabilidades fáciles que los hackers y los virus comúnmente buscan explotar. (Wendlandt, 2008)

Nessus no es una solución completa de seguridad, sino que es una pequeña parte de una buena estrategia de seguridad. Nessus no evita activamente los ataques, es sólo una herramienta que comprueba sus equipos para encontrar vulnerabilidades que los hackers podrían explotar. ES DE

Para saber cómo funcionan Nessus y otras herramientas de seguridad de exploración de puertos, es necesario entender los diferentes servicios (como un servidor web, servidor SMTP, servidor FTP, etc.) se accede en un servidor remoto. La mayoría del tráfico de red de alto nivel, como correo electrónico, páginas web, etc., llega a un servidor a través de un protocolo de alto nivel que es transmitido de forma fiable por un flujo TCP. Para evitar que los diferentes flujos interfieran entre sí, una computadora divide su conexión física a la red en miles de rutas lógicas, llamadas puertos. Por lo tanto, si desea hablar con un servidor web en una máquina determinada, se conectaría al puerto # 80 (el puerto HTTP estándar), pero si desea conectarse a un servidor SMTP en esa misma máquina, en su lugar se conectaría al puerto # 25. (Wendlandt, 2008)

Cada computadora tiene miles de puertos, todos los cuales pueden o no tener servicios (es decir: un servidor para un protocolo de alto nivel específico) escuchando en ellos. Nessus trabaja probando cada puerto en una computadora, determinando qué servicio está ejecutando y luego probando este servicio para asegurarse de que no hay vulnerabilidades en él que pueda ser utilizado por un hacker para llevar a cabo un ataque malicioso. Nessus se llama un "escáner remoto" porque

no necesita ser instalado en una computadora para que pruebe esa computadora. En su lugar, puede instalarlo en un solo ordenador y probar tantos ordenadores como desee. (Wendlandt, 2008)

La versión que vamos a utilizar de Nessus es la 6.9.2, siempre usamos la última versión estable del producto.

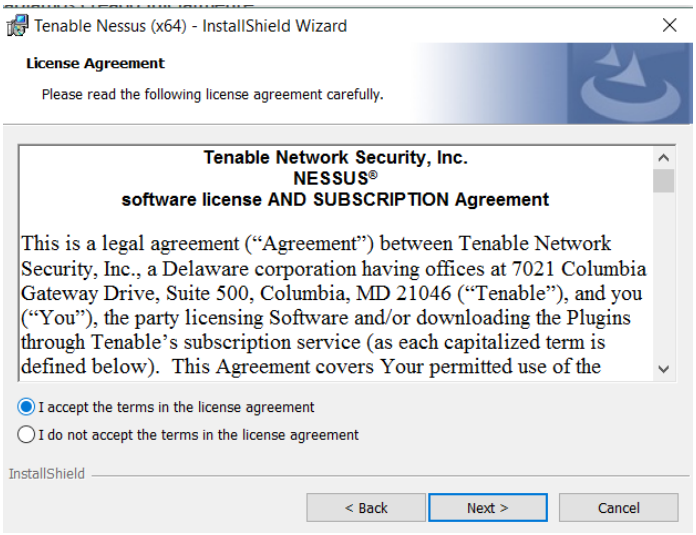
3.2.1. Instalación de Nessus.

Igual que los programas anteriores se lo programa de la misma manera que cualquier programa de Windows, la diferencia es que, desde algunos años Nessus dejó de ser gratuito a pasar a ser privado, por lo que se necesita de una licencia pagada, con un precio de 2190 dólares anuales.

La instalación es sencilla, tenemos que aceptar los términos de la licencia.

Paso 1. Igual que cualquier programa de Windows, exige que se acepte los términos legales de licencia.

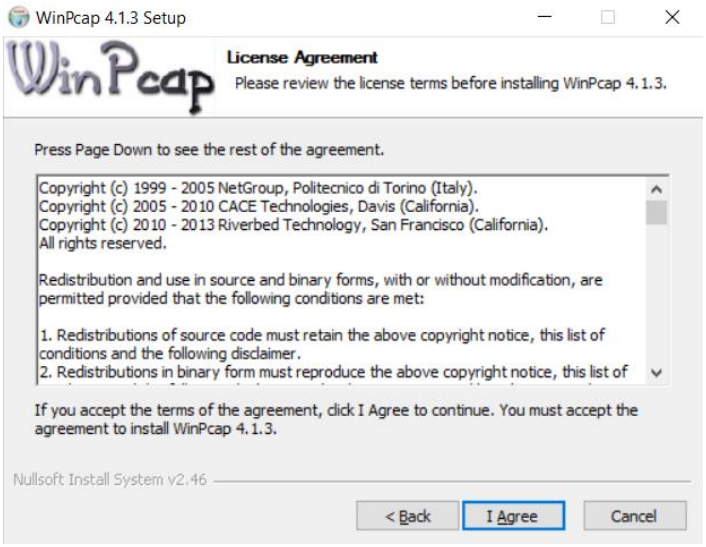
Ilustración 7: Instalación Nessus



Autor: R Avilés, M Silva, enero 2017

Paso 2. Una característica de Nessus, que utiliza WinPcap, la cual sirve para acceder a la conexión entre capas de red en Windows.

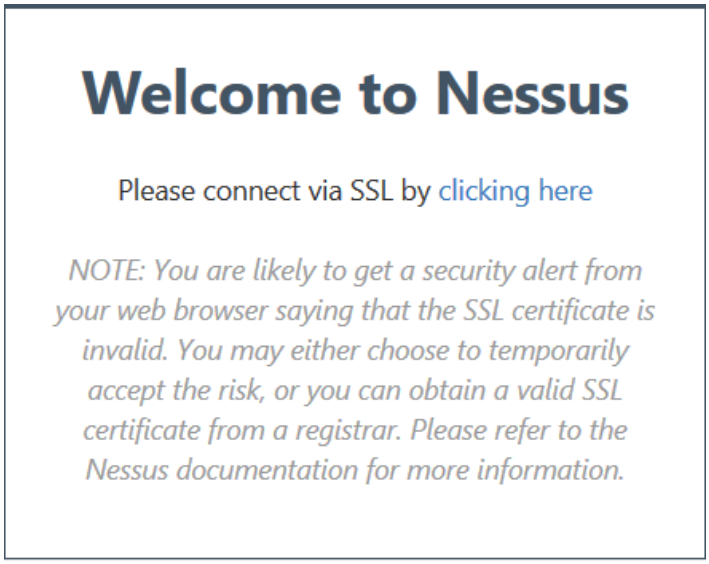
Ilustración 8: Instalación Nessus



Autor: R Avilés, M Silva, enero 2017

Paso 3. Cuando finaliza el programa nos lanza una advertencia, en donde nos comunica que debemos conectarnos vía SSL (Secure Sockets layer) que es un protocolo que perite a las aplicaciones transmitir información de ida y regreso de forma segura.

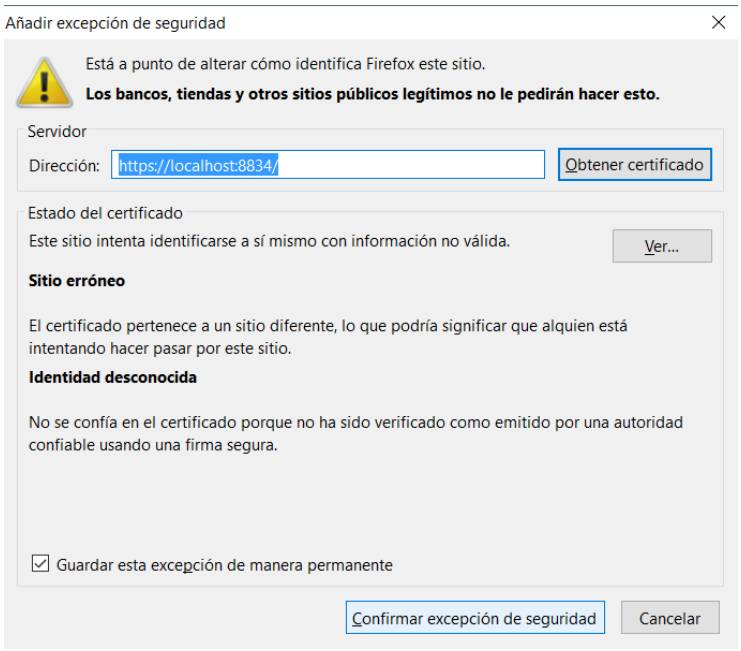
Ilustración 9: Instalación Nessus



Autor: R Avilés, M Silva, enero 2017

Paso 4. Inmediatamente al ingresar nos manda una advertencia en donde se añade el locla hosot de Nessus y confirmar la excepción de seguridad.

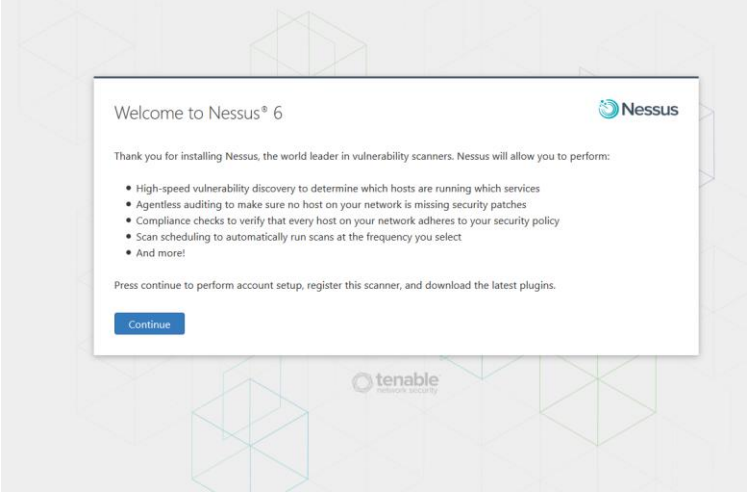
Ilustración 10: Instalación Nessus



Autor: R Avilés, M Silva, enero 2017

Paso 5. Inmediatamente ingresar a Nessus 6.

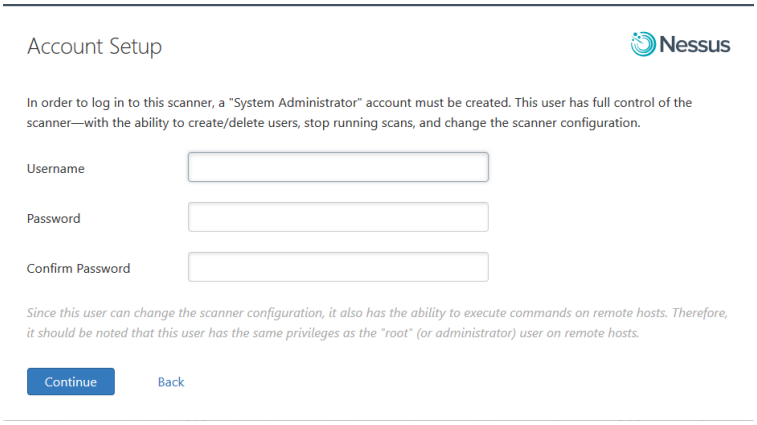
Ilustración 11: Instalación Nessus



Autor: R Avilés, M Silva, enero 2017

Paso 6. Al ingresar se debe poner los datos como el usuario y contraseña.

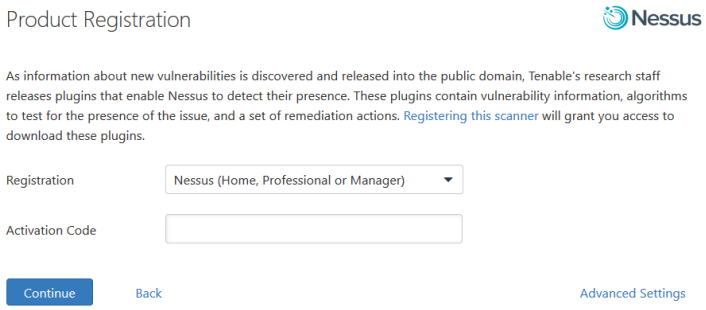
Ilustración 12: Instalación Nessus



Autor: R Avilés, M Silva, enero 2017

Paso 7. Se ingresa el código proporcionado por la empresa para poder usar el programa.

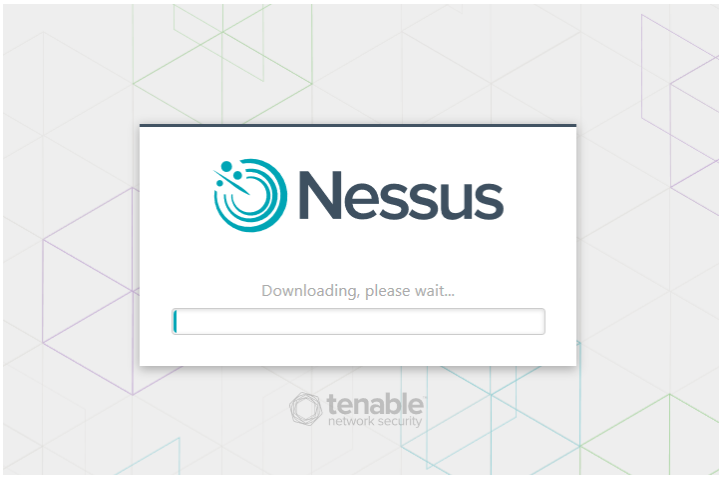
Ilustración 13: Instalación Nessus



Autor: R Avilés, M Silva, enero 2017

Paso 9. Finalmente se descarga los plug ins necesarios para poder usarlo.

Ilustración 14: Instalación Nessus



Autor: R Avilés, M Silva, enero 2017

3.3. Wireshark

Ilustración 15: Logo Wireshark

Wireshark Foundation, 2016

Wireshark es un analizador de protocolo de red. Le permite capturar y explorar de forma interactiva el tráfico que se ejecuta en una red informática. Tiene un conjunto de características ricas y potentes y es la herramienta más popular del mundo de este tipo. Funciona en la mayoría de las plataformas de computación incluyendo Windows, OS X, Linux y UNIX. Profesionales de la red, expertos en seguridad, desarrolladores y educadores de todo el mundo lo utilizan regularmente. Está disponible gratuitamente como código abierto y se publica bajo la licencia GNU General Public License versión 2. (Wireshark, 2014)

Es desarrollado y mantenido por un equipo global de expertos en protocolos, y es un ejemplo de una tecnología disruptiva.

Wireshark solía ser conocido como Ethereal. Consulte la siguiente pregunta para obtener detalles sobre el cambio de nombre. Si aún utiliza Ethereal, se recomienda encarecidamente que actualice a Wireshark ya que Ethereal no es compatible y tiene vulnerabilidades de seguridad conocidas.

Es desarrollado y mantenido por un equipo global de expertos de protocolo, y es un ejemplo de una tecnología de punta.

Wireshark solía ser conocido como Ethereal. Ver el próximo número para obtener detalles sobre el cambio de nombre. Si usted todavía está utilizando etéreo, se recomienda encarecidamente que actualice a Wireshark como Ethereal no es compatible y tiene algunos problemas de seguridad. (Wireshark, 2014)

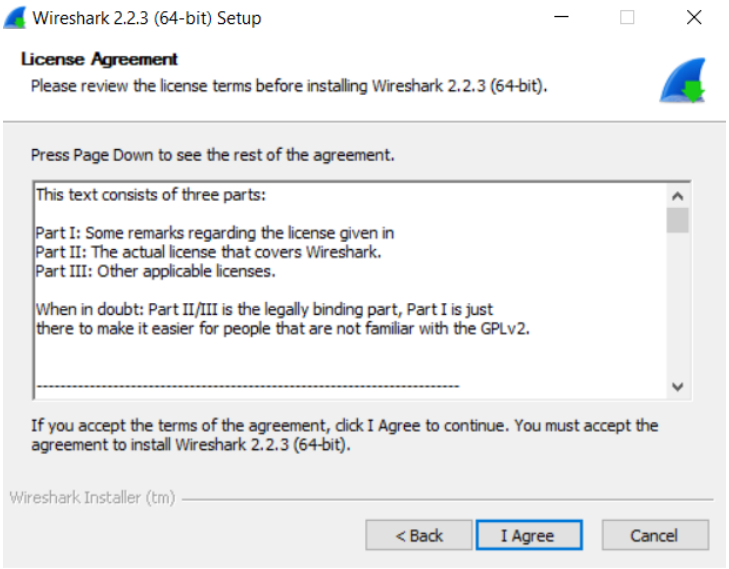
La versión que vamos a utilizar es la 2.2.3, la última estable.

3.3.1. Instalación de Wireshark.

Paso 1. De igual forma su método de instalación es igual a cualquier programa de Windows.

Se acepta la licencia.

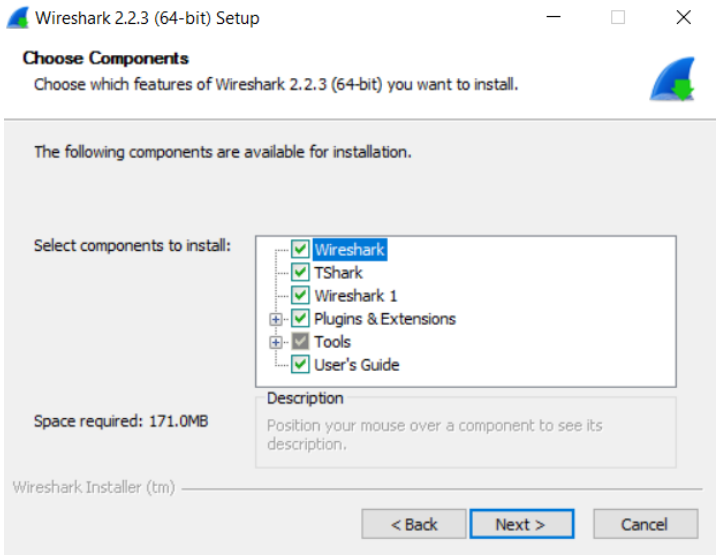
Ilustración 16: Instalación Wireshark



Autor: R Avilés, M Silva, enero 2017

Paso 2. Se escoge los componentes.

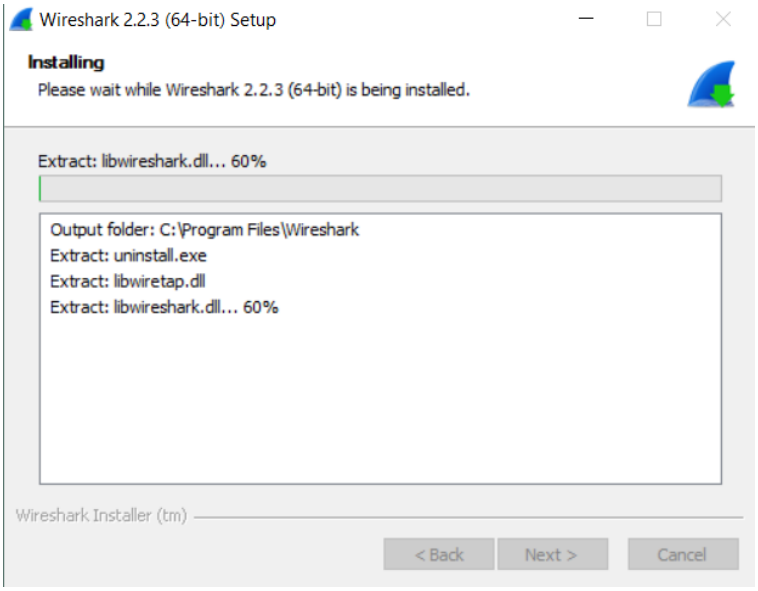
Ilustración 17: Instalación Wireshark



Autor: R Avilés, M Silva, enero 2017

Paso 3. Se pone a instalar el programa.

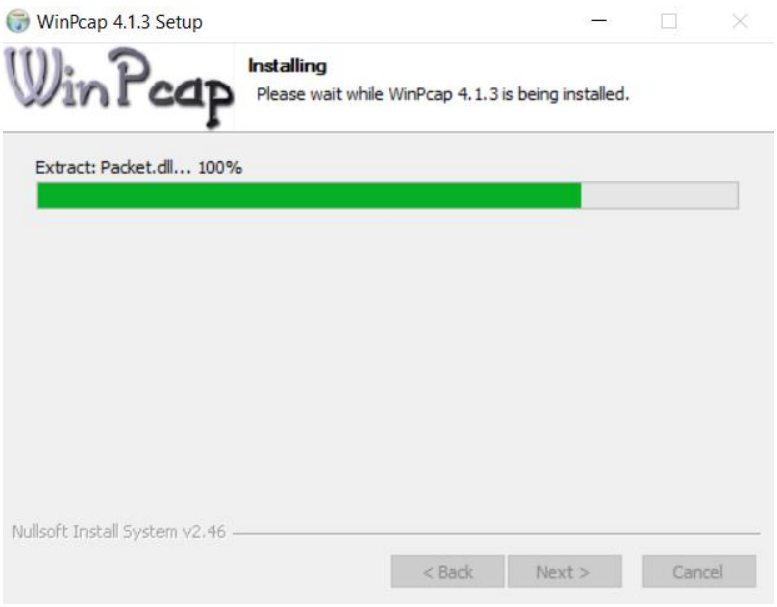
Ilustración 18: Instalación Wireshark



Autor: R Avilés, M Silva, enero 2017

Paso 4. Como Nessus, Wireshark necesita instalar el WinPcap.

Ilustración 19: Instalación Wireshark



Autor: R Avilés, M Silva, enero 2017

3.4. Kali Linux

Kali es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad. Este sistema operativo es gratuito debido a que ese software de código abierto y fue desarrollado con grandes estándares de jerarquía del sistema de ficheros, permitiendo que todos los usuarios de Linux puedan localizar fácilmente archivos binarios, archivos de soporte, bibliotecas, etc. (Kali Linux, 2013)

Kali Linux tiene Kernel personalizado con parches de inyección, esto quiere decir que los desarrolladores realizan evaluaciones inalámbricas en el Kernel, para que siempre tenga los últimos parches de inyección incluidos. (Kali Linux, 2013)

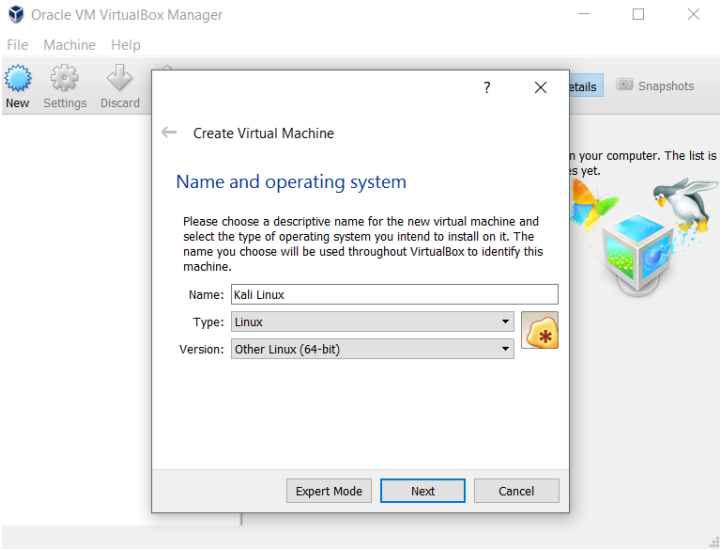
Como es de conocimiento público la mayoría de herramientas de penetración tienden a ser escritas en inglés, por lo que los desarrolladores han programado el Kali Linux en varios idiomas para que los usuarios puedan utilizarlo en su propio leguaje. (Kali Linux, 2013)

3.4.1. Instalación de Kali Linux.

Como es de conocimiento, Kali Linux es un sistema Operativo basado en Linux, Debyan para ser exactos, por lo que para instalarlo debemos usar una máquina virtual, en este caso vamos a usar VirtualBox de Oracle.

Paso 1. Inicialmente lo que se debe hacer es crear una nueva máquina virtual, la cual se debe poner el nombre, el tipo y la versión.

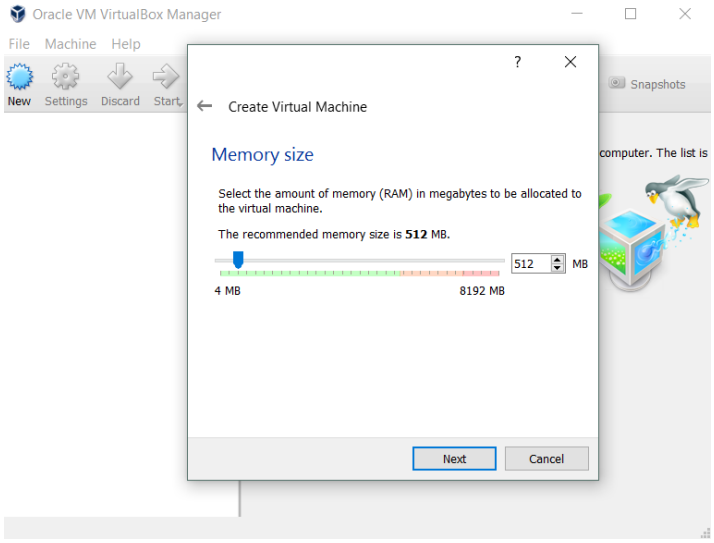
Ilustración 20: Instalación Kali



Autor: R Avilés, M Silva, enero 2017

Paso 2. Se escoge el tamaño de memoria RAM que va a utilizar la máquina virtual.

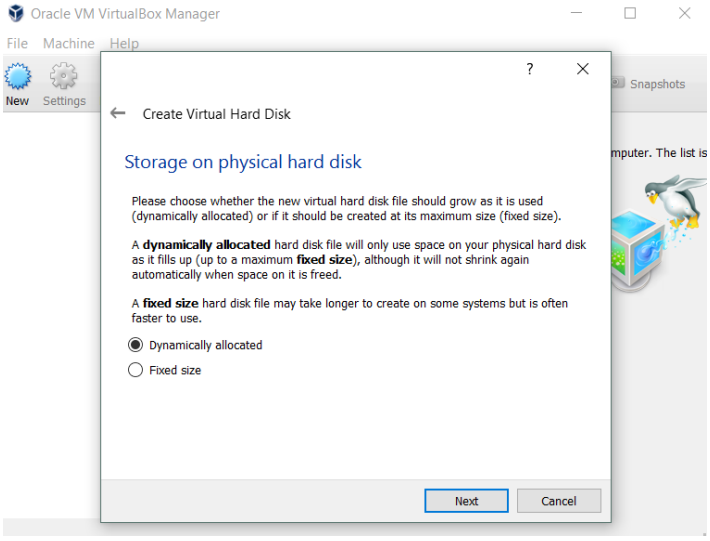
Ilustración 21: Instalación Kali



Autor: R Avilés, M Silva, enero 2017

Paso 3. Crear un disco duro virtual, en el cual se escoge VDI (VirtualBox Disk Image) y que sea reservado dinámicamente.

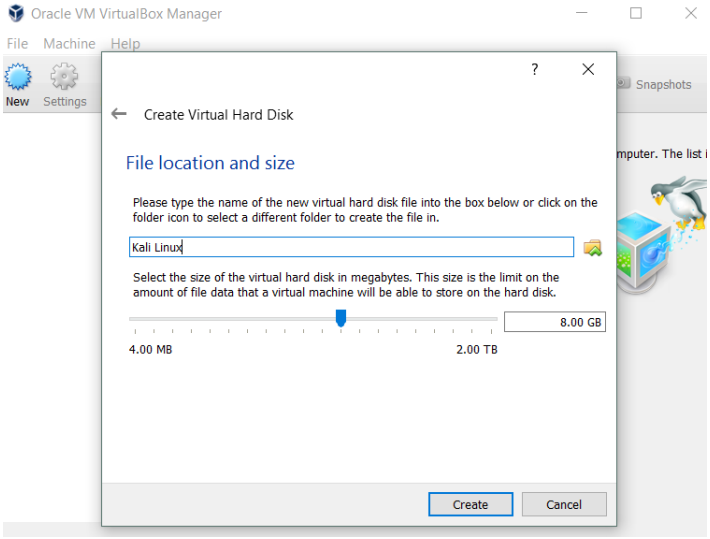
Ilustración 22: Instalación Kali



Autor: R Avilés, M Silva, enero 2017

Paso 4. Seleccionar el tamaño que tendrá el disco duro para la máquina virtual.

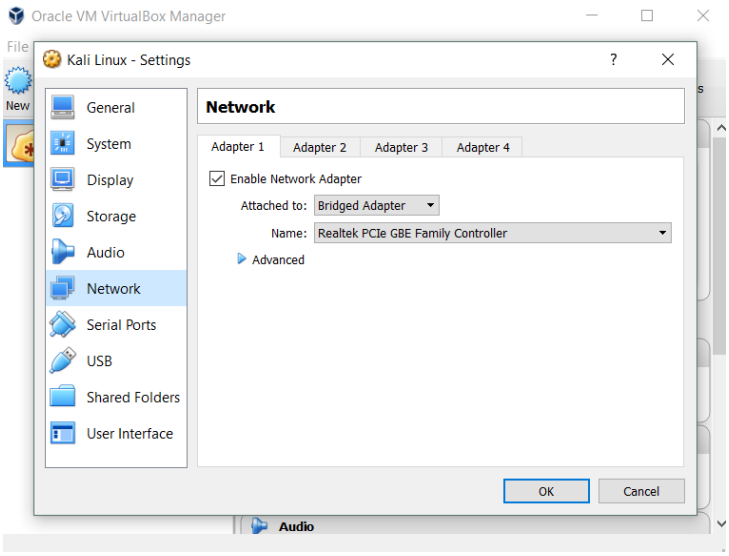
Ilustración 23: Instalación Kali



Autor: R Avilés, M Silva, enero 2017

Paso 5. Ahora se escoge la opción de configuración de Kali Linux, la pestaña de Red, se cambia NAT que viene por default, a Adaptador Puente.

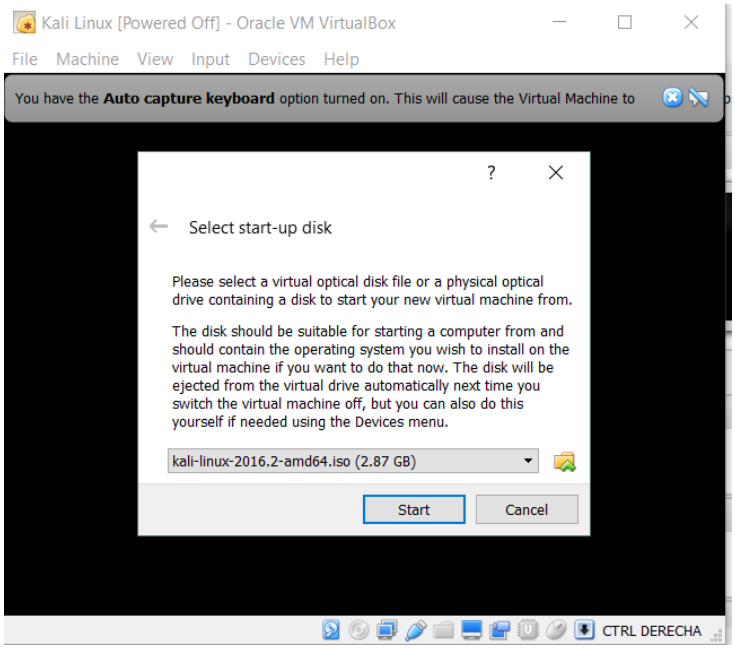
Ilustración 24: Instalación Kali



Autor: R Avilés, M Silva, enero 2017

Paso 6. Se inicia la máquina virtual de Kali Linux y se escoge el formato ISO de Kali Linux.

Ilustración 25: Instalación Kali



Autor: R Avilés, M Silva, enero 2017

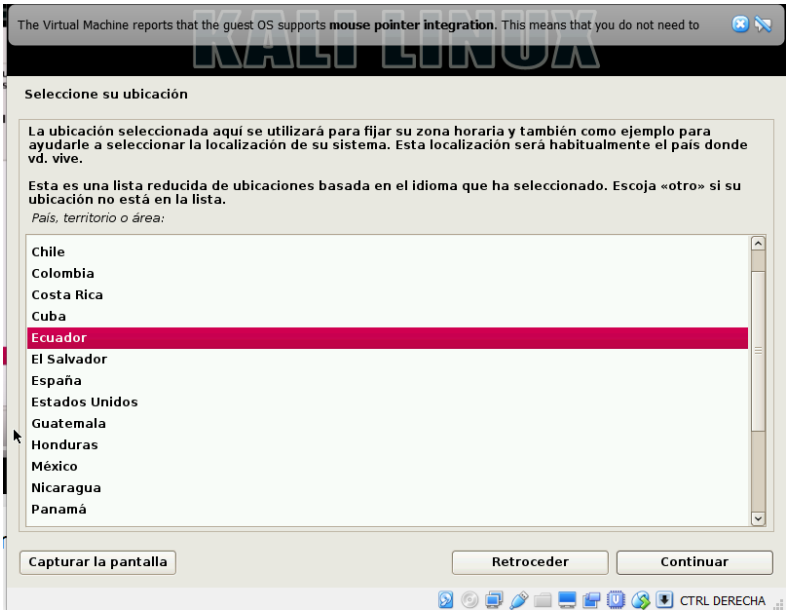
Paso 7. Luego de un momento saldrá el Boot menú de Kali Linux con varias opciones, se escoge la instalación gráfica para mayor facilidad.

Ilustración 26: Instalación Kali

Autor: R Avilés, M Silva, enero 2017

Paso 8. Ahora se escoge el idioma, país y teclado.

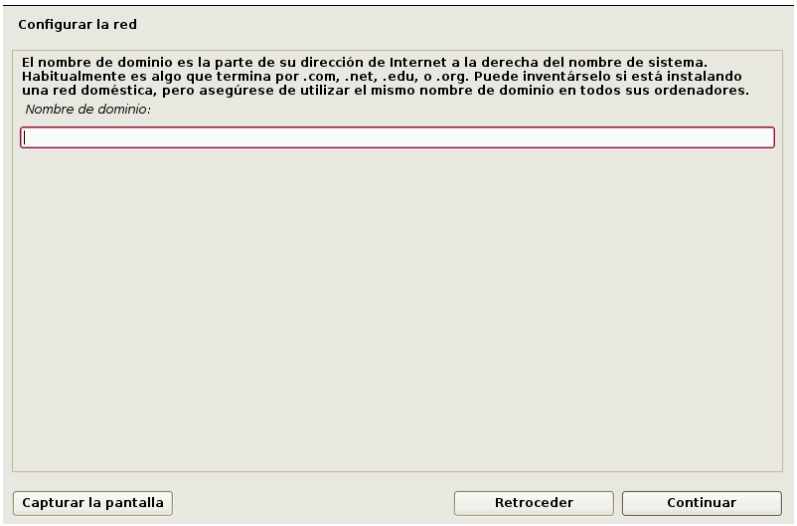
Ilustración 27: Instalación Kali



Autor: R Avilés, M Silva, enero 2017

Paso 9. Se configura la red, al ponerle nombre y una clave.

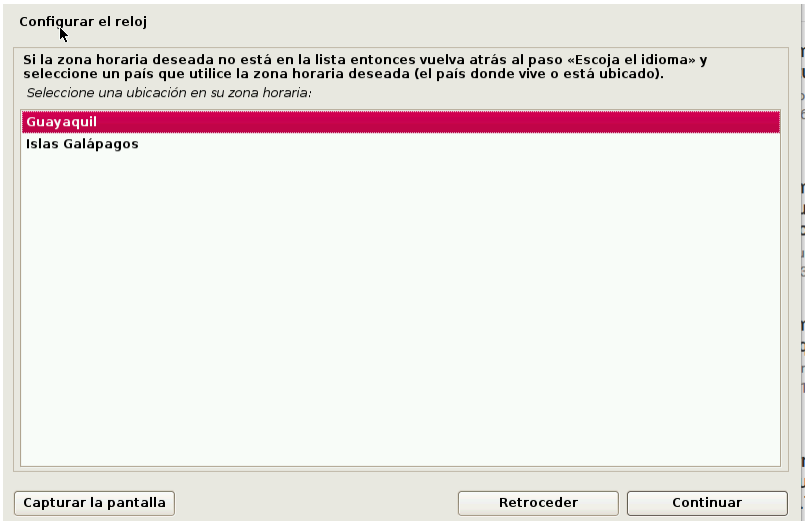
Ilustración 28: Instalación Kali



Autor: R Avilés, M Silva, enero 2017

Paso 10. Se configura el reloj.

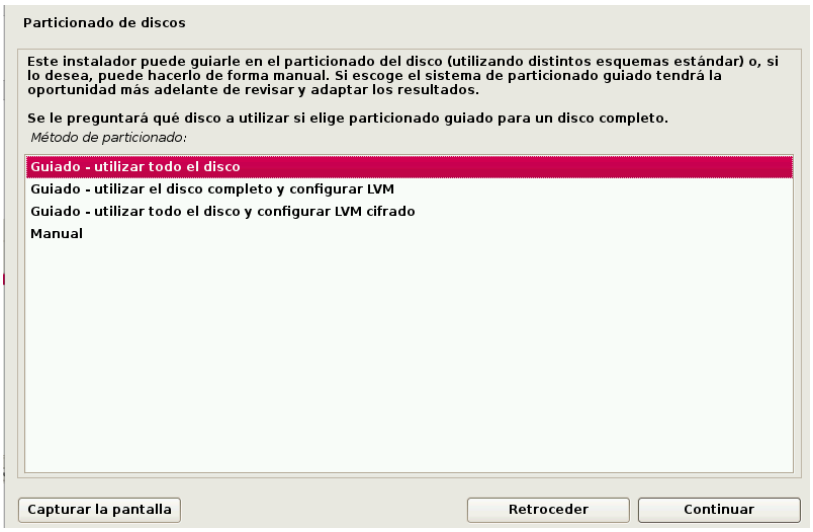
Ilustración 29: Instalación Kali



Autor: R Avilés, M Silva, enero 2017

Paso 11. Muestra la opción de particionar el disco, a lo que se selecciona el de utilizar todo el disco.

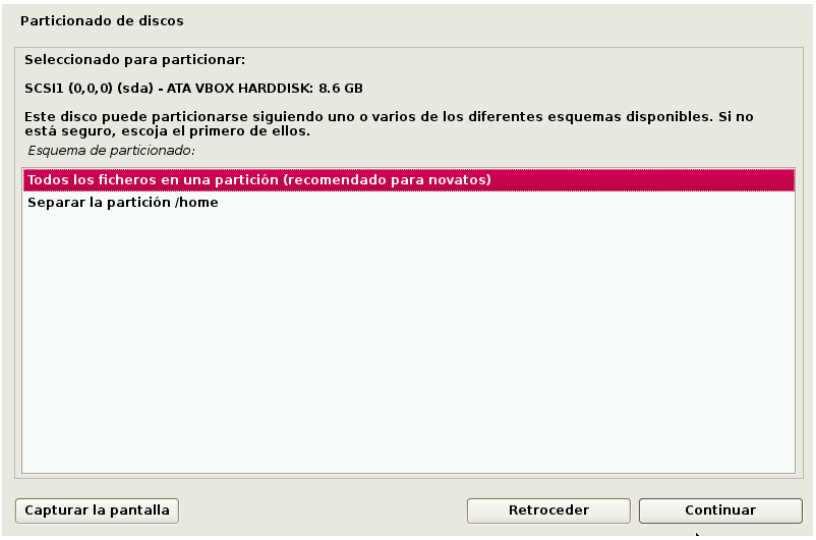
Ilustración 30: Instalación Kali



Autor: R Avilés, M Silva, enero 2017

Paso 12. Seleccionar que todos los ficheros estén en una solo partición.

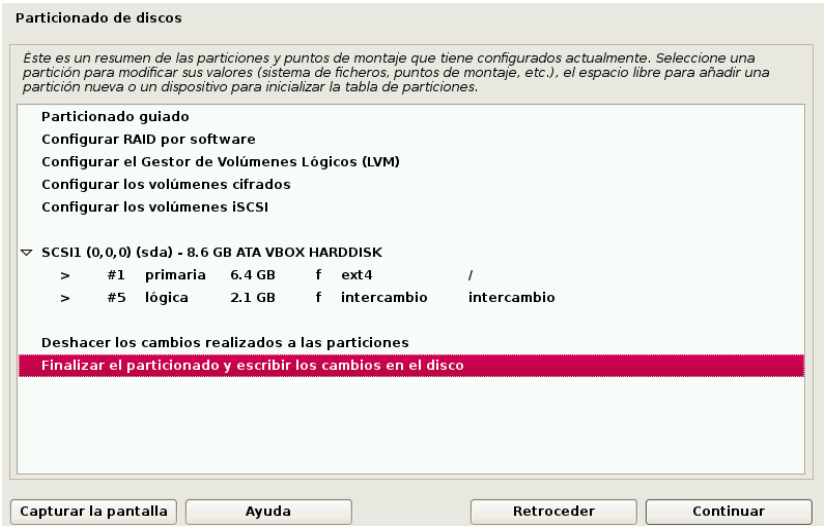
Ilustración 31: Instalación Kali



Autor: R Avilés, M Silva, enero 2017

Paso 13. Finalmente sale una pantalla, con todos los cambios que se ha realizado y damos a continuar, luego pregunta si se quiere formatear algunas particiones a lo que se acepta.

Ilustración 32: Instalación Kali



Autor: R Avilés, M Silva, enero 2017

Paso 14. Comienza a instalar el sistema.

Ilustración 33: Instalación Kali

Autor: R Avilés, M Silva, enero 2017

Paso 15. Se espera un tiempo dependiendo el ordenador para que finalmente el sistema queda completamente funcional

Ilustración 34: Instalación Kali

Autor: R Avilés, M Silva, enero 2017

CAPÍTULO 4

RESULTADOS DE LAS HERRAMIENTAS INVESTIGADAS

4.1. Utilización de Nessus

Nessus es un programa pagado por lo que la licencia gratuita apenas dura 7 días, por lo que en ese lapso de tiempo probamos el programa.

Es un programa enfocado en escaneo de vulnerabilidades en distintos sistemas operativos, además de ser un analizador de seguridad de redes, su forma de realizar el escaneo es usando un daemon, de nombre nesssusd y el programa propiamente el cual es el encargado de mostrar el avance e informar sobre el estado de los escaneos.

Script en informática

Un script informático en el mundo de la Web, comúnmente es un programa de ordenador (o una parte de un programa) es el responsable de realizar una función específica cuando un usuario realiza una acción o cuando una página web está actualmente siendo mostrar en una pantalla. Esta es una serie de instrucciones sencillas y a menudo no estructurada, que permiten la automatización de tareas. Más directamente, el script se encarga de la funcionalidad de un sistema informático.

Para su funcionamiento, el Script siempre debe ser ejecutado por un programa, principalmente en el que fue escrito (o por un servidor dedicado a este lenguaje). Comúnmente los Scripts informáticos o lenguajes de scripting, los cuales son interpretados por el servidor (en el caso de los lenguajes que se utilizan para crear sitios web dinámicos como PHP, Python, etc.), y secuencias de comandos informáticos o lenguajes de scripting, estos se interpretan en el lado del cliente (en el caso de JavaScript entendido por el navegador web). (Alegsa, 2014)

Similar a varios programas que realizan el mismo escaneo, Nessus escanea los puertos con Nmap con la finalidad de encontrar puertos abiertos y después poder intentar varios exploits para atacarlo. Nessus tiene como prueba de vulnerabilidad, una larga lista de plugins, los cuales son escritos en NASL (Lenguaje de Scripting de Ataque Nessus), el cual es un lenguaje scripting optimizado para interacciones personalizadas en redes.

Los resultados obtenidos del escaneo pueden ser exportados en varios formatos, como Latex, Html, XML, etc. Es posible guardar los resultados en una base para referencia en futuros escaneos.

Algunas pruebas que realiza Nessus pueden causar que los servicios se caigan o los sistemas operativos se puedan corromper, por lo que es necesario que se desactive la opción Unsafe test (Pruebas no seguras) antes de realizar el escaneo.

Características Principales

Nessus genera archivos .nessus que son usados por los productos de Tenable como estándar para directivas de análisis y datos de vulnerabilidad.

La interfaz gráfica de Nessus muestra los resultados de los análisis en tiempo real, por lo que facilita el momento de ver los resultados ya que no se debe esperar a que finalice el análisis.

Lo que hace diferente a Nessus de otros programas similares es que no supone que un servicio dado se ejecuta en un puerto fijo, cuando es posible, intenta validar una vulnerabilidad a través de su explosión.

Cada prueba de seguridad está diseñada como plugin externo, y se agrupa en una de 42 familias.

Es posible añadir fácilmente las pruebas, seleccionar plugins específicos o elegir una familia entera sin tener que leer el código del motor de servidores Nessus, nessusd.

Existe varios plugins, aquí un ejemplo de estos:

- SMTP problems
- SNMP
- Solaris Local Security Checks
- SuSE Local Security Checks
- Ubuntu Local Security Checks
- VMware ESX Local Security Checks
- Web Servers
- Windows
- Windows: Microsoft Bulletins
- Windows: User Management

La versión de Apple iTunes que se ejecuta en el host remoto es anterior a 12.5.5 Por lo tanto, está afectada por múltiples vulnerabilidades:

Existen varios problemas de corrupción de memoria en WebKit debido a validación incorrecta de ciertos datos no especificados. Un atacante remoto puede explotar estos, a través de contenido web especialmente diseñado, para corromper la memoria, resultando en la ejecución de código arbitrario.

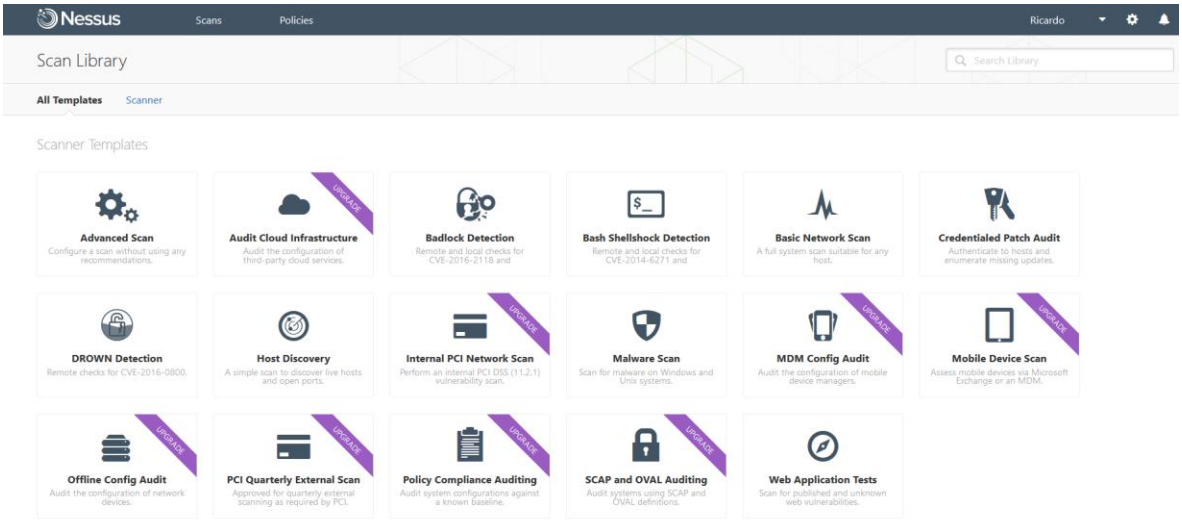
(CVE-2017-2354, CVE-2017-2356, CVE-2017-2366)

Nessus aparte de informar las vulnerabilidades existentes en la red y el nivel de riesgo de cada una de ellas, también notifica sobre como mitigarlas ofreciendo soluciones.

Lo primero que se observa es que el programa trae bastantes opciones para realizar un hackeo, pero varias de ellas están bloqueadas y solo se pueden utilizar en la versión pagada.

A pesar de esto tiene varias opciones básicas de escaneo como son la avanzada y la básica, el escaneo de malwares.

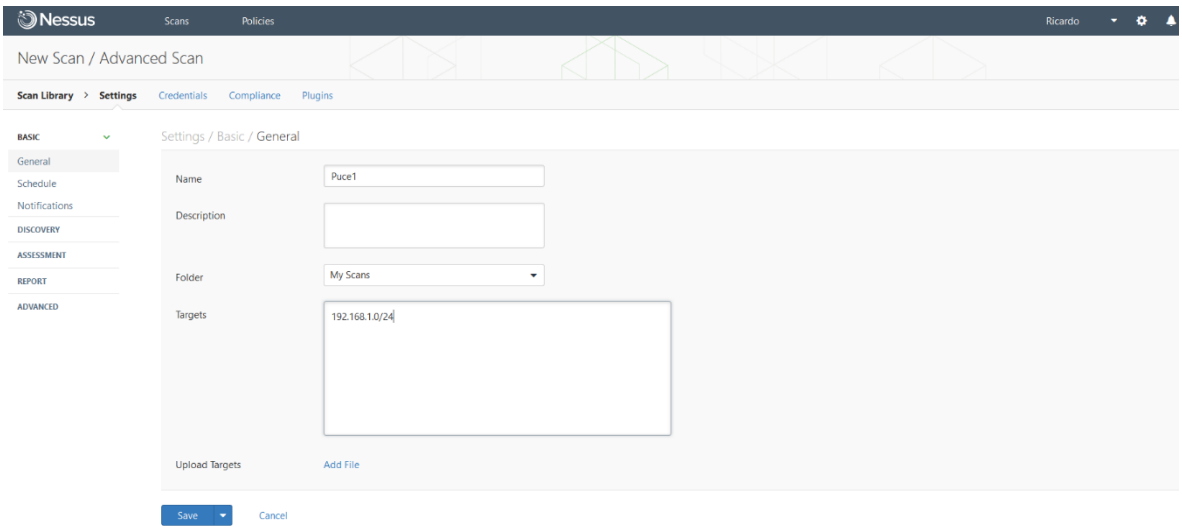
Ilustración 35: Nessus



Autor: R Avilés, M Silva, enero 2017

Para poder verificar el estado de la red, se realiza un escaneo avanzado, al escogerlo nos dice que se debe darle un nombre y escribir el rango de IP que se vaya a escanear.

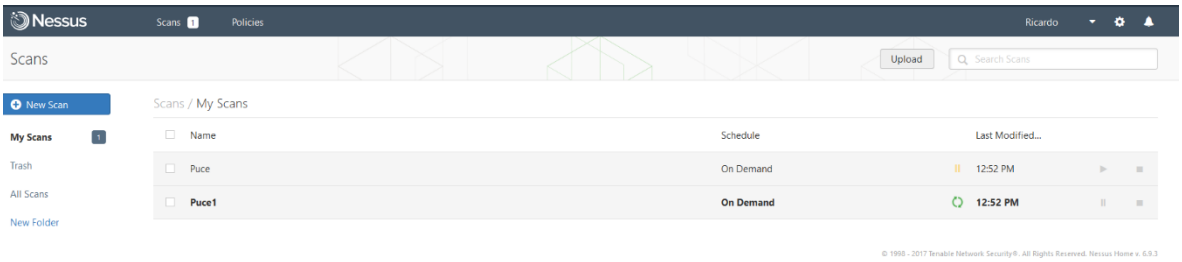
Ilustración 36: Nessus



Autor: R Avilés, M Silva, enero 2017

Nessus nos lleva a una lista en donde se encuentra todos los escaneos previamente ejecutados, se escoge el que se vaya a usar y se espera un tiempo hasta que muestro los resultados.

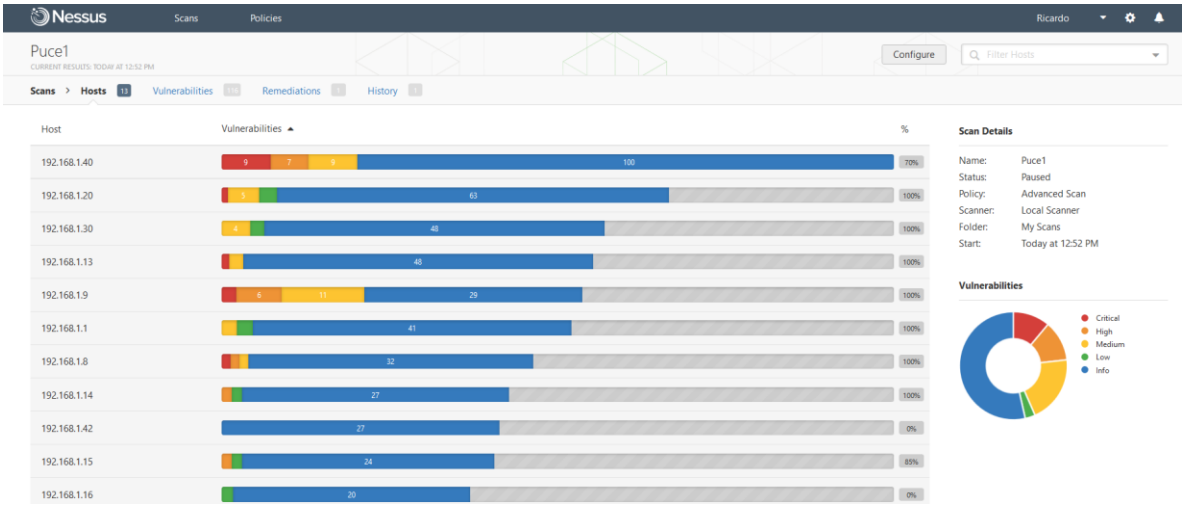
Ilustración 37: Nessus



Autor: R Avilés, M Silva, enero 2017

Cuando termina de escanear, muestra una lista de todas las IP que estén conectadas a la Red, también muestra en un gráfico de anillos, el total de vulnerabilidades encontradas, las divide en vulnerabilidades bajas, medias, altas y críticas con sus respectivos colores.

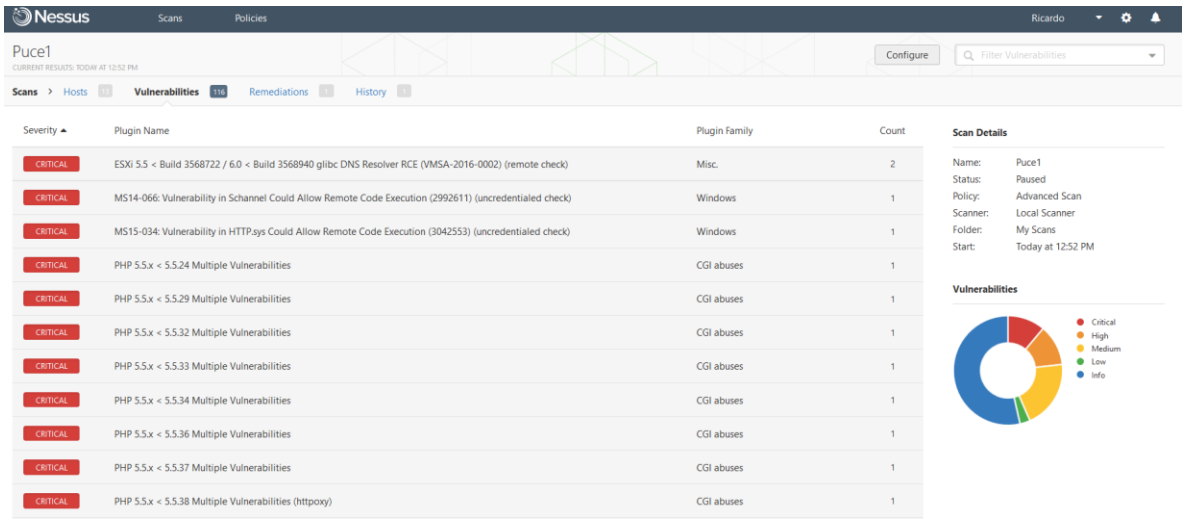
Ilustración 38: Nessus



Autor: R Avilés, M Silva, enero 2017

Al desplazar la lista muestra primero las vulnerabilidades críticas con sus respectivos nombres y también muestra la cantidad de vulnerabilidades iguales que existen.

Ilustración 39: Nessus



Autor: R Avilés, M Silva, enero 2017

Las vulnerabilidades altas y medias igualmente con sus nombres y número que se encuentra.

Ilustración 40: Nessus

HIGH	ESXi 5.5 < Build 1746974 / 5.5 Update 1 < Build 1746018 OpenSSL Library Multiple Vulnerabilities (remote check) (Heartbleed)	Misc.	1
HIGH	ESXi 5.5 < Build 2352327 Multiple Vulnerabilities (remote check) (POODLE)	Misc.	1
HIGH	OpenSSL 'ChangeCipherSpec' MiTM Vulnerability	Misc.	1
HIGH	OpenSSL Heartbeat Information Disclosure (Heartbleed)	Misc.	1
HIGH	PHP 5.5.x < 5.5.22 Multiple Vulnerabilities (GHOST)	CGI abuses	1
HIGH	PHP 5.5.x < 5.5.23 Multiple Vulnerabilities	CGI abuses	1
HIGH	PHP 5.5.x < 5.5.25 Multiple Vulnerabilities	CGI abuses	1
HIGH	PHP 5.5.x < 5.5.26 Multiple Vulnerabilities	CGI abuses	1
HIGH	PHP 5.5.x < 5.5.28 Multiple Vulnerabilities	CGI abuses	1
HIGH	PHP 5.5.x < 5.5.30 Multiple Vulnerabilities	CGI abuses	1
HIGH	PHP 5.5.x < 5.5.35 Multiple Vulnerabilities	CGI abuses	1
HIGH	VMware ESXi Multiple OpenSSL Vulnerabilities (VMSA-2014-0004) (Heartbleed)	Misc.	1
MEDIUM	SSL Self-Signed Certificate	General	5
MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	Windows	3
MEDIUM	SMB Signing Disabled	Misc.	3

Autor: R Avilés, M Silva, enero 2017

Las vulnerabilidades bajas e información.

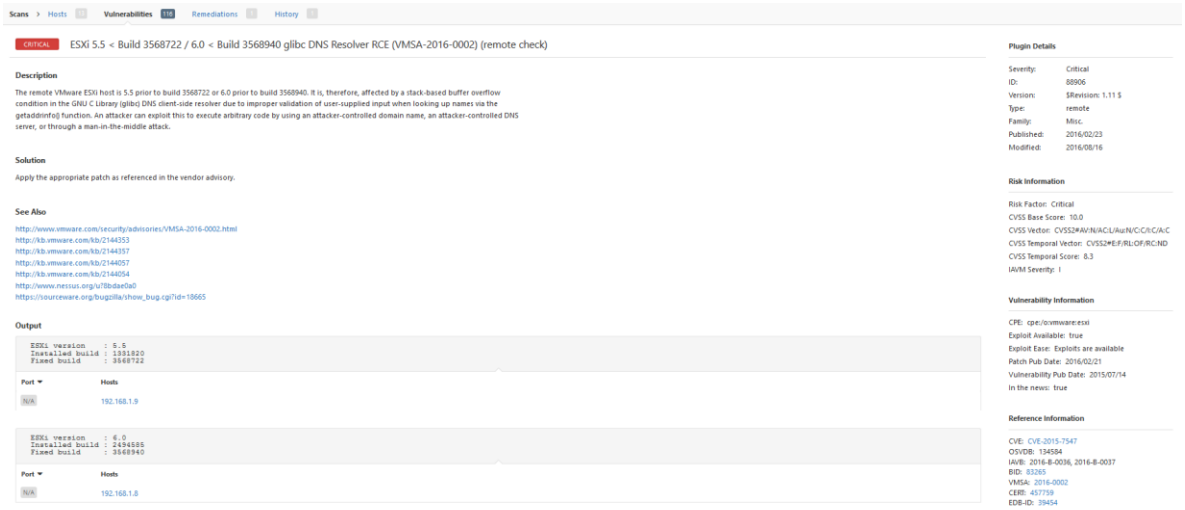
Ilustración 41: Nessus

LOW	Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)	Misc.	3
LOW	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	General	3
LOW	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General	3
LOW	DHCP Server Detection	Service detection	1
INFO	Nessus SYN scanner	Port scanners	114
INFO	DCE Services Enumeration	Windows	64
INFO	Service Detection	Service detection	43
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	18
INFO	HTTP Server Type and Version	Web Servers	16
INFO	Microsoft Windows SMB Service Detection	Windows	12
INFO	HTTP Methods Allowed (per directory)	Web Servers	10
INFO	TCP/IP Timestamps Supported	General	10
INFO	Traceroute Information	General	10
INFO	Common Platform Enumeration (CPE)	General	9

Autor: R Avilés, M Silva, enero 2017

Cuando se selecciona una de ellas muestra una descripción detallada de la vulnerabilidad, al igual que también una solución, también muestra los IP de los ordenadores que tengan esas vulnerabilidades para solucionarlas.

Ilustración 42: Nessus



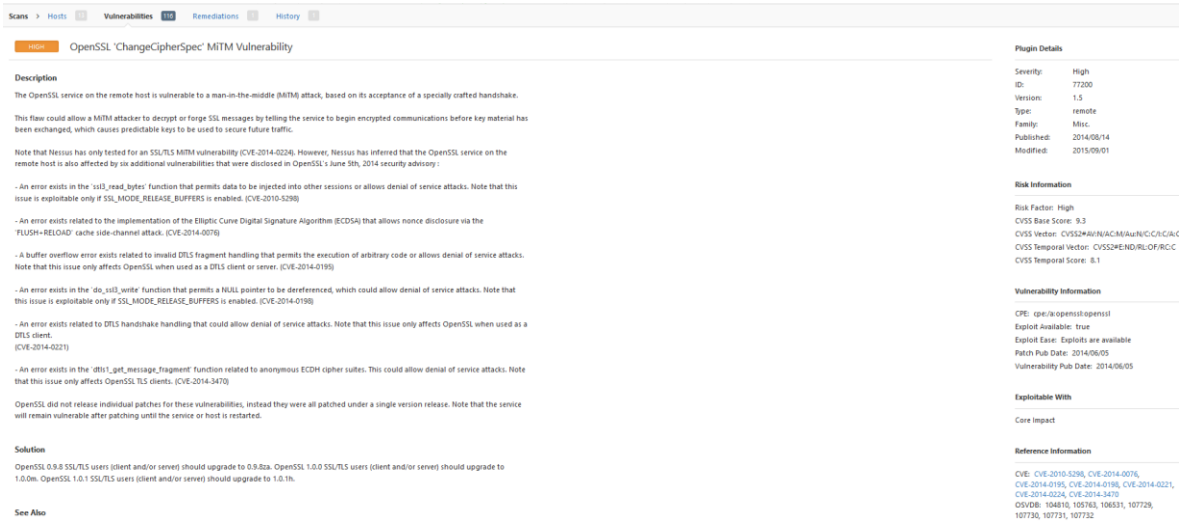
Autor: R Avilés, M Silva, enero 2017

Lo mismo sucede para todas las vulnerabilidades, sean esta de riesgo crítico, alto o bajo.

Ilustración 43: Nessus

Autor: R Avilés, M Silva, enero 2017

Ilustración 44: Nessus



Autor: R Avilés, M Silva, enero 2017

Las observaciones son muy detalladas, para que el momento de reparar no exista confusiones.

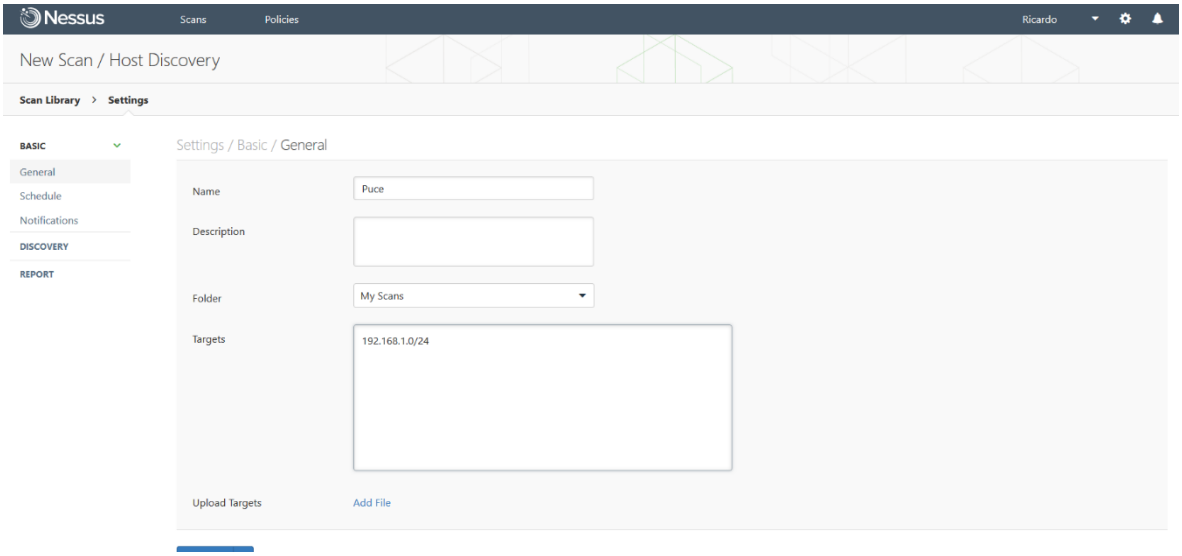
Ilustración 45: Nessus

Autor: R Avilés, M Silva, enero 2017

Una opción muy importante y con lo que realiza pruebas de seguridad en la universidad es la de Host Discovery, en esta se hace un escaneo simple para descubrir los Host que se encuentren activos y los puertos abiertos que tenga la red.

Para utilizarlo se escoge esta opción, luego de ingresar se debe poner como requisito obligatorio un nombre y lo más importante poner el rango de la IP a escanear.

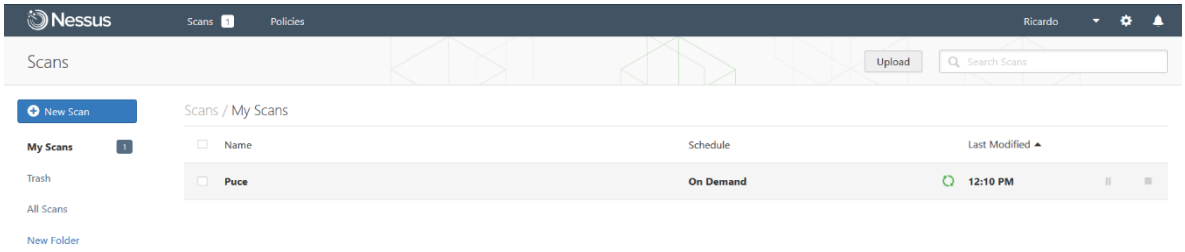
Ilustración 46: Nessus



Autor: R Avilés, M Silva, enero 2017

Inmediatamente se guarda en una lista y le damos a ejecutar para que escanee la red.

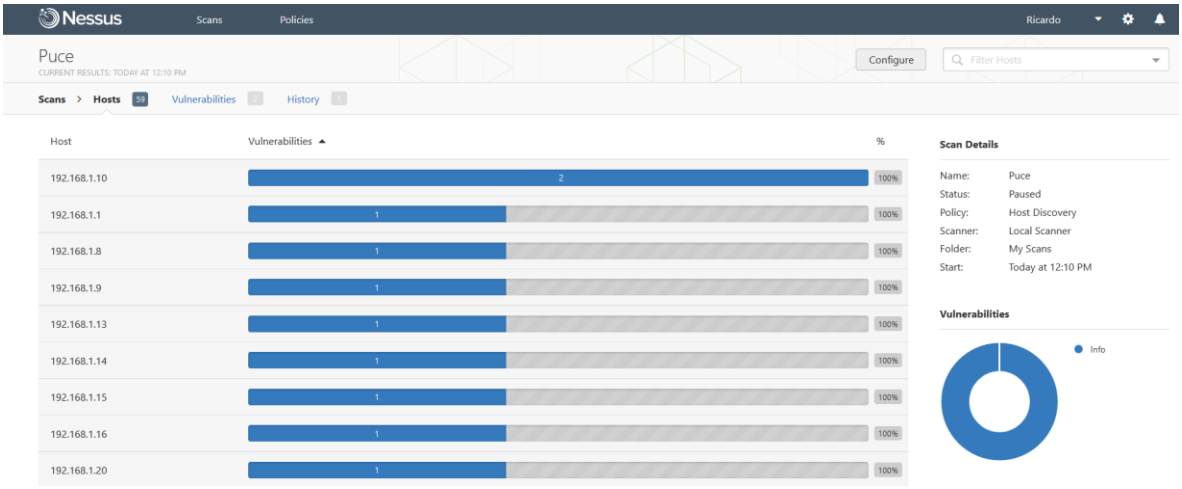
Ilustración 47: Nessus



Autor: R Avilés, M Silva, enero 2017

Dependiendo la cantidad de ordenadores conectadas a la red toma un tiempo entre 2 a 3 horas en realizar el escaneo, luego de eso tiempo, muestra todos los Host que tiene la red. En la universidad están conectadas 59.

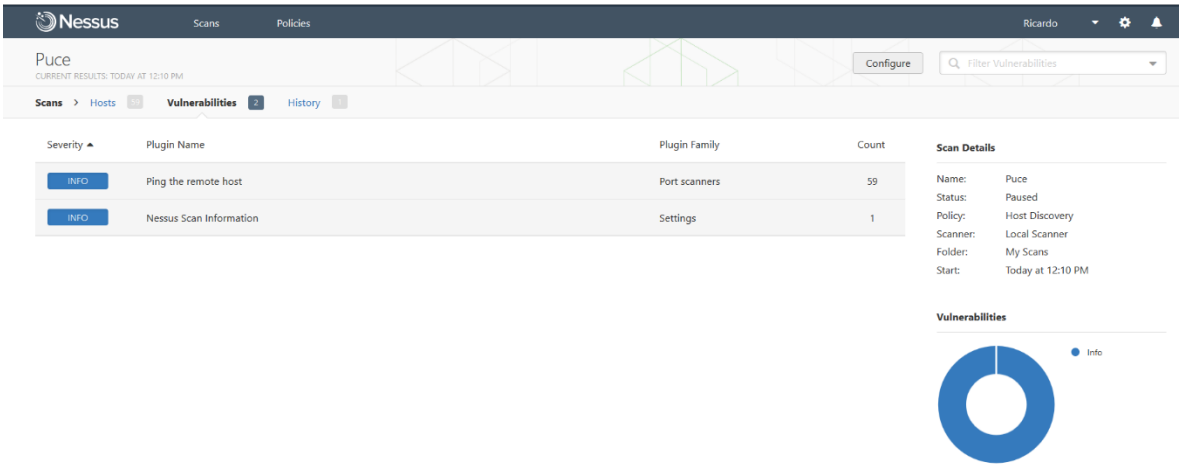
Ilustración 48: Nessus



Autor: R Avilés, M Silva, enero 2017

También da un listado con todas vulnerabilidades que tiene.

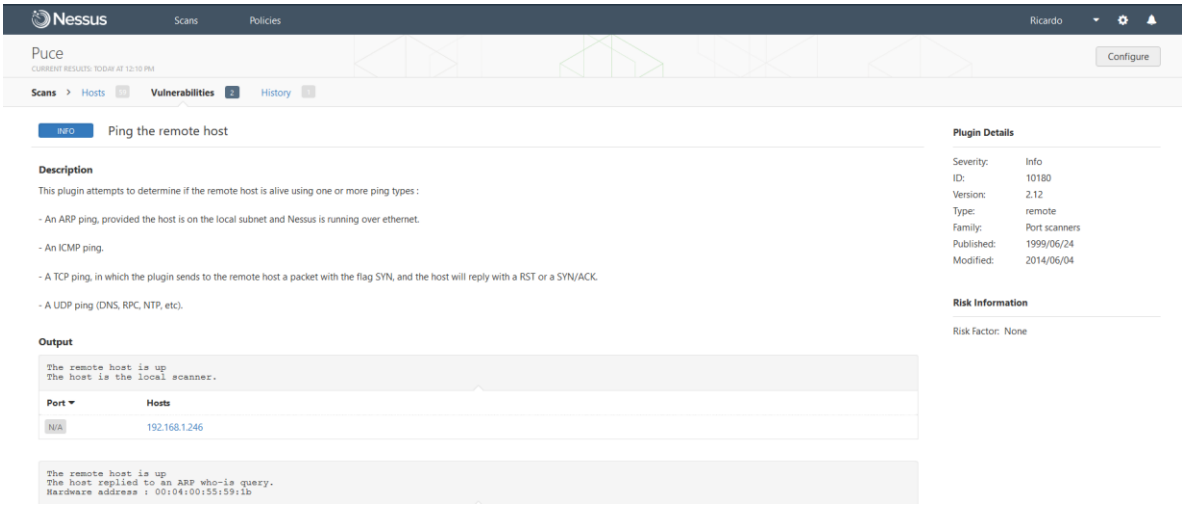
Ilustración 49: Nessus



Autor: R Avilés, M Silva, enero 2017

Incluso da una descripción detallada de cada vulnerabilidad que se haya encontrado.

Ilustración 50: Nessus



Autor: R Avilés, M Silva, enero 2017

Concluyendo, como se observó, es una de las herramientas más completa que se tienen en lo que se refiere a realizar un hackeo ético para una empresa, el mayor inconveniente que encontrado es su precio muy elevado, y que la versión de prueba solo dure 7 días y sea bastante limitado.

Vulnerabilidades Encontradas

En la siguiente tabla se muestran las vulnerabilidades que comúnmente suelen aparecer en cualquier entorno de red. Por lo general estas vulnerabilidades se dan gracias la falta de información sobre la seguridad informática en los usuario o empleados.

Tabla 4: Vulnerabilidades

Vulnerabilidades	Descripción	Notas
Contraseñas (falta de ellas o dejar las predeterminadas que brinda el sistema)	Dejar en blanco las contraseñas administrativas o usar una contraseña predeterminada establecida por el proveedor del producto. Es lo más común en hardware tales como enrutadores y firewall.	Comúnmente asociado con hardware de red, como enrutadores, firewalls, VPNs y dispositivos de almacenamiento conectado a red (NAS). Algunas veces los administradores crean cuentas de usuario privilegiadas de afán y dejan la contraseña en blanco, creando el punto perfecto para que usuarios maliciosos descubran la cuenta.
Suplantación de IP	Una máquina remota actúa como un nodo en su red local, encuentra vulnerabilidades con sus servidores e instala un programa trasero o Caballo de Troya para obtener control sobre los recursos de la red.	La suplantación es bastante difícil ya que el atacante prediga los números de secuencia TCP/IP para coordinar la conexión a sistemas de destino, aunque hay varias herramientas disponibles para que los atacantes realicen dicha agresión.
Vulnerabilidades de servicios	El atacante busca una falla o debilidad en un servicio en la red; a través de esta vulnerabilidad, el atacante compromete todo el sistema y los datos que pueda contener y posiblemente comprometa otros sistemas en la red.	Los servicios basados en HTTP tales como CGI son vulnerables a la ejecución de comandos remotos e incluso al acceso de shell interactivo. Incluso el servicio HTTP se ejecuta como usuario sin privilegios tales como información de "nadie", información tal como archivos de configuración y mapas de redes que pueden leer o el atacante puede iniciar o negar el ataque del servicio que drena los servicios del sistema o los convierte en no disponibles para otros usuarios.
Vulnerabilidades de aplicaciones	Los atacantes buscan fallas en el escritorio y aplicaciones de trabajo (tales como clientes de correo electrónico) y ejecutan código arbitrario, implantan caballos de Troya para compromiso futuro o para dañar sistemas. Otras vulnerabilidades se pueden presentar si la estación de trabajo tiene privilegios administrativos en la parte restante de la red.	Las estaciones de trabajo y escritorios son más propensas a vulnerabilidades ya que los trabajadores no tienen la experiencia para evitar o detectar un compromiso; es imperativo informar a los individuos de los riesgos que corren cuando instalan software no autorizado o abren anexos de correo no solicitado.
Ataques de denegación de servicio (DoS)	El atacante o grupo de atacantes coordina contra una red de organización o recursos de servidor al enviar paquetes no autorizados al host de destino (ya sea servidor, enrutador o estación de trabajo). De esta manera se fuerza al recurso a convertirse en disponible para usuarios legítimos.	Los paquetes de fuente generalmente se falsifican (como también se retransmiten), lo que dificulta la investigación de la fuente verdadera del ataque.

Autor: R Avilés, M Silva, enero 2017

4.2. Utilización de Wireshark

Uno de los usos principales para Wireshark es la de usar filtros para poder detectar actividad maliciosa, es posible detectar conexiones ocultas de malware hacia direcciones remotas para obtener otros archivos, incluso reporta en caso de existir un botnet.

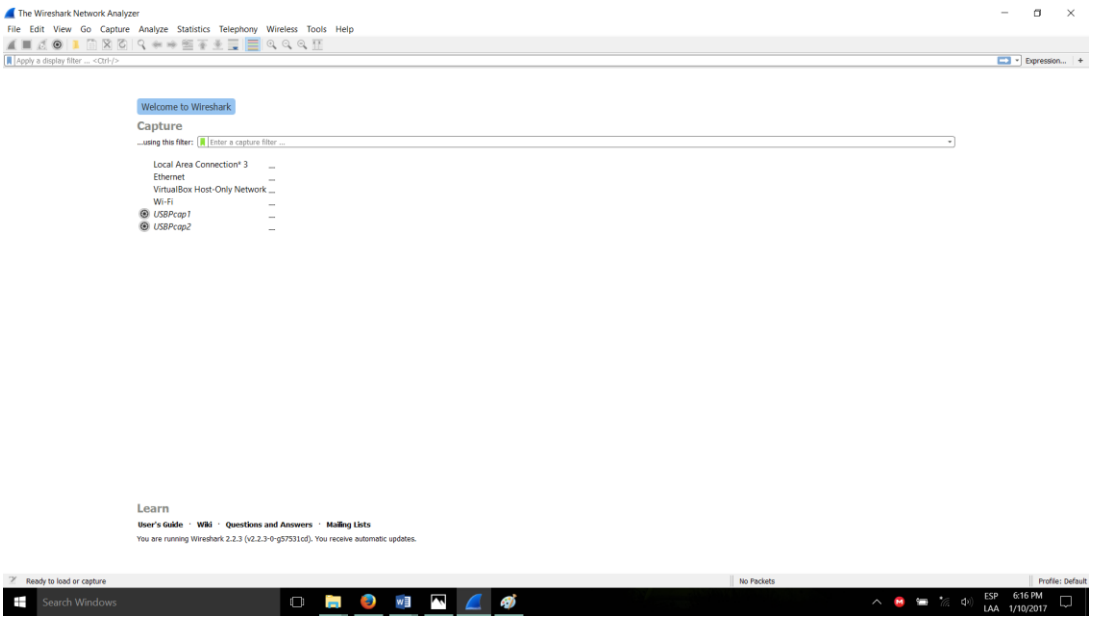
Se puede reconocer a los servidores que ingresan a través de peticiones de DNS. Se hacen visibles todas las IPs, con esto se puede observar en caso de haber malware, se puede ver con que servidor está conectado.

Otra opción muy utilizada es la del filtro http.request, con esta opción es posible obtener todos los GET y POST que fueron hechos en el tiempo en que se ejecutó. Los malware utilizan estas peticiones para enviar información del sistema que haya sido afectado.

Para utilizar el protocolo SMTP, el cual se utiliza para propagarse mediante correo electrónico, mediante filtro se puede observar el remitente del correo, para esto usamos smtp.req.parameter && contains “FROM”. Es posible visualizar los paquetes que tienen el cuerpo del mensaje, cuando se obtiene los paquetes después de los filtros, se puede ver toda la secuencia del paquete completo (si es necesario), tan solo con escoger al que queramos observar y dar en la opción “follow tcp stream”, de esta manera se puede visualizar todo el paquete completo.

Wireshark es una herramienta de análisis de red, principalmente es un sniffer. Para la utilización de Wireshark lo primero que se puede apreciar es el momento de ingresar, que se queda cargando un momento, es en este momento en que está reconociendo todas las redes a las que el ordenador esté conectado en ese momento. Al ingresar a la página principal muestra todas las redes a las que esté conectada la máquina y el uso que se le está dando.

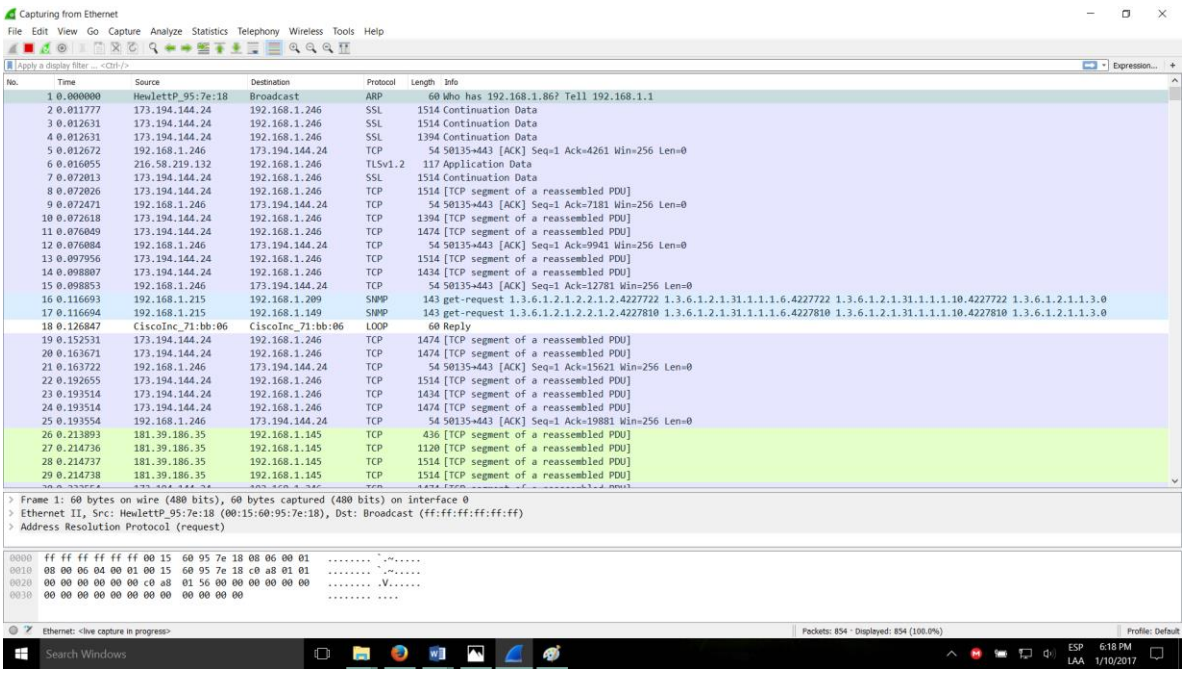
Ilustración 51: Wireshark



Autor: R Avilés, M Silva, enero 2017

Al momento de iniciar con el escaneo, muestra todos los protocolos y todas las actividades que estén realizando todos los ordenadores que estén conectadas a la misma red.

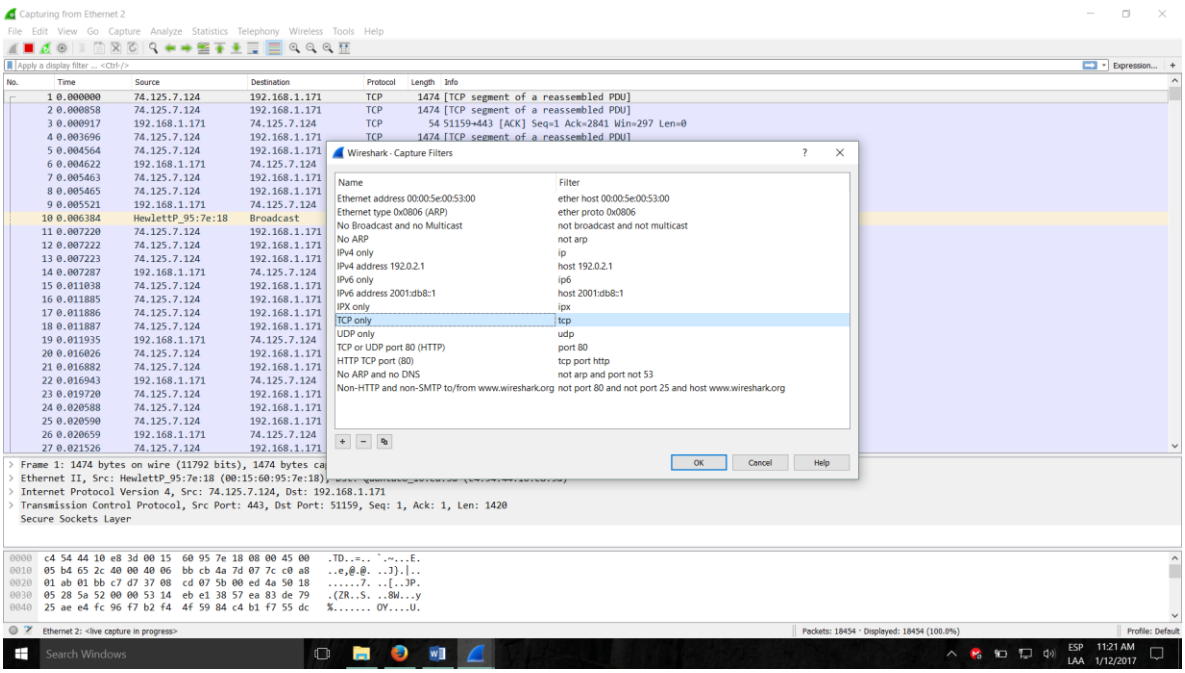
Ilustración 52: Wireshark



Autor: R Avilés, M Silva, enero 2017

Es posible filtrar los protocolos de diferentes maneras, como muestra este caso, se ha filtrado solo TCP.

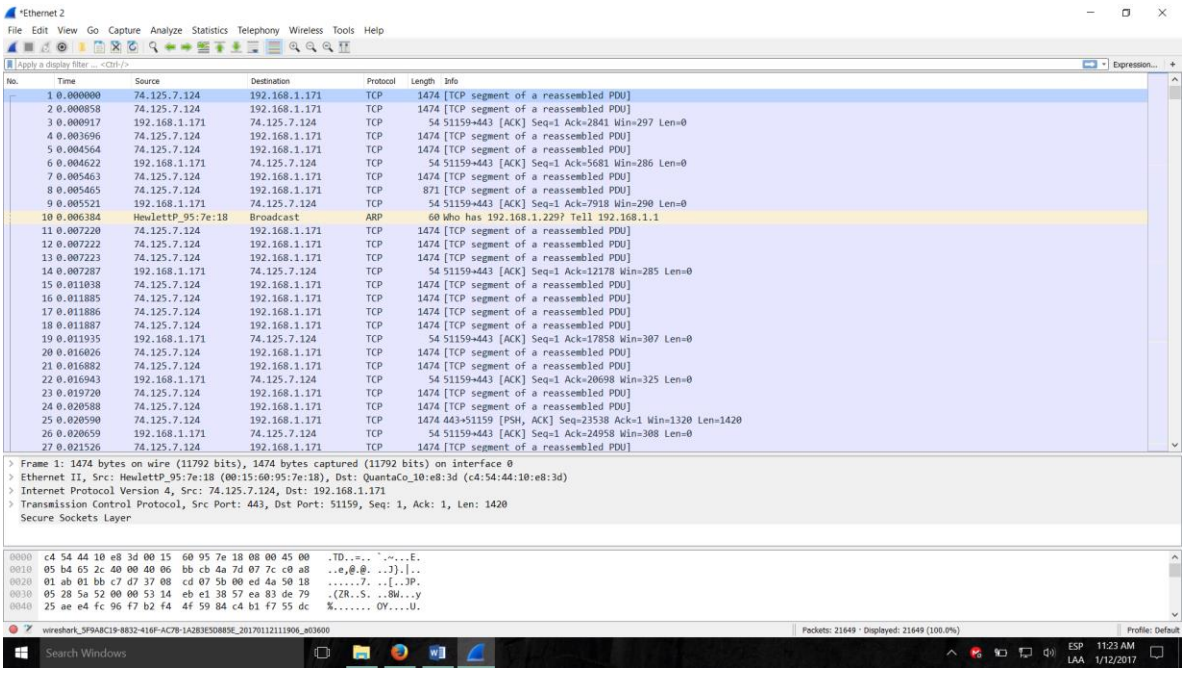
Ilustración 53: Wireshark



Autor: R Avilés, M Silva, enero 2017

Ahora solo muestras todas las actividades de los protocolos TCP.

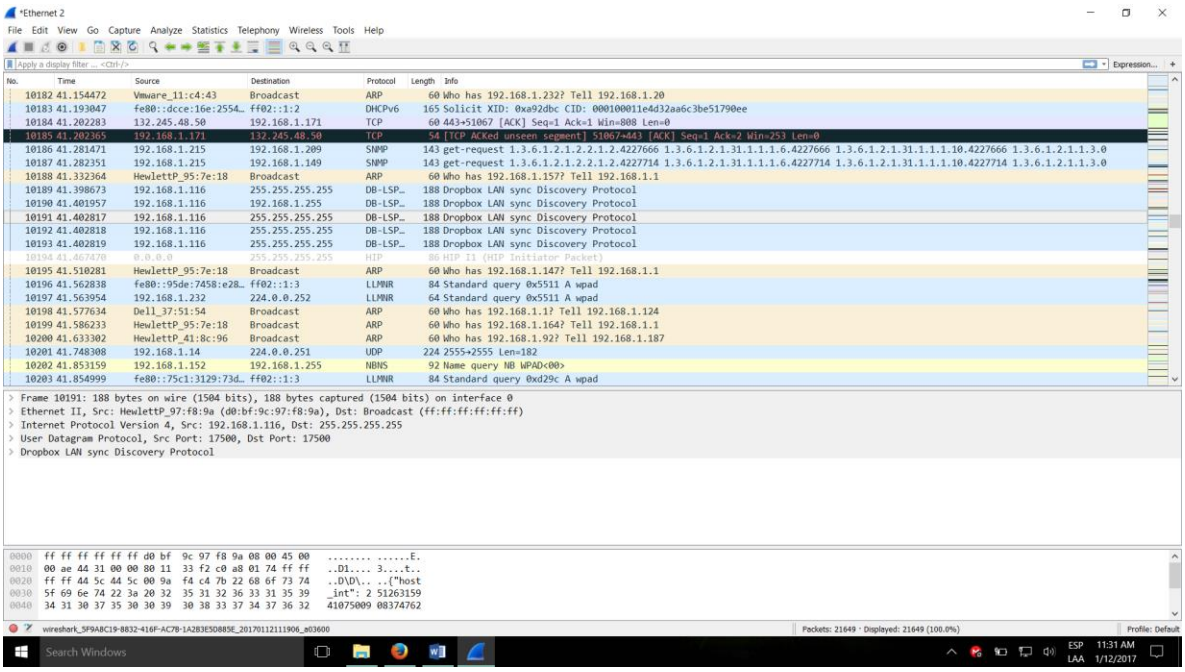
Ilustración 54: Wireshark



Autor: R Avilés, M Silva, enero 2017

Con Wireshark lo que se puede hacer es ver las actividades que estén realizando cualquier ordenador que esté conectado a la Red. Lo característica de Wireshark es que se puede filtrar por protocolos para hacer más fácil la búsqueda de actividades que se estén realizando en esos momentos.

Ilustración 55: Wireshark



Autor: R Avilés, M Silva, enero 2017

Se concluye que utilizar la herramienta de Wireshark es de gran utilidad para verificar actividades maliciosas que se estén ejecutando en la red.

4.3. Utilización de Nmap

Nmap es una herramienta de escaneo de redes, puertos y servicios, al pasar de los años, la herramienta ha ido mejorando en todos sus aspectos, actualmente incorpora el uso de scripts para comprobar varias vulnerabilidades. (Pérez, 2015)

Tabla 5: Scripts

Scripts Incorporados	Descripción
Auth	Este corre todos los scripts que se encuentran disponibles para poder lograr la autentificación.
Default	Mediante este se puede ejecutar todos los scripts básicos que se encuentran por defecto en la herramienta.
Discovery	Mediante esto se puede recuperar la información de la víctima.
External	Este nos permite ocupar los recursos externos.
Intrusive	Este ocupa scripts intrusivos para la víctima.
Malware	Mediante este revisa o chequea si hay conexiones existentes o abiertas por códigos maliciosos o backdoors.
Safe	Este ejecuta scripts los cuales no son intrusivos.
Vuln	Mediante este se pueden encontrar las vulnerabilidades más conocidas.
All	Este ejecuta todos los scripts con una extensión NSE disponible.

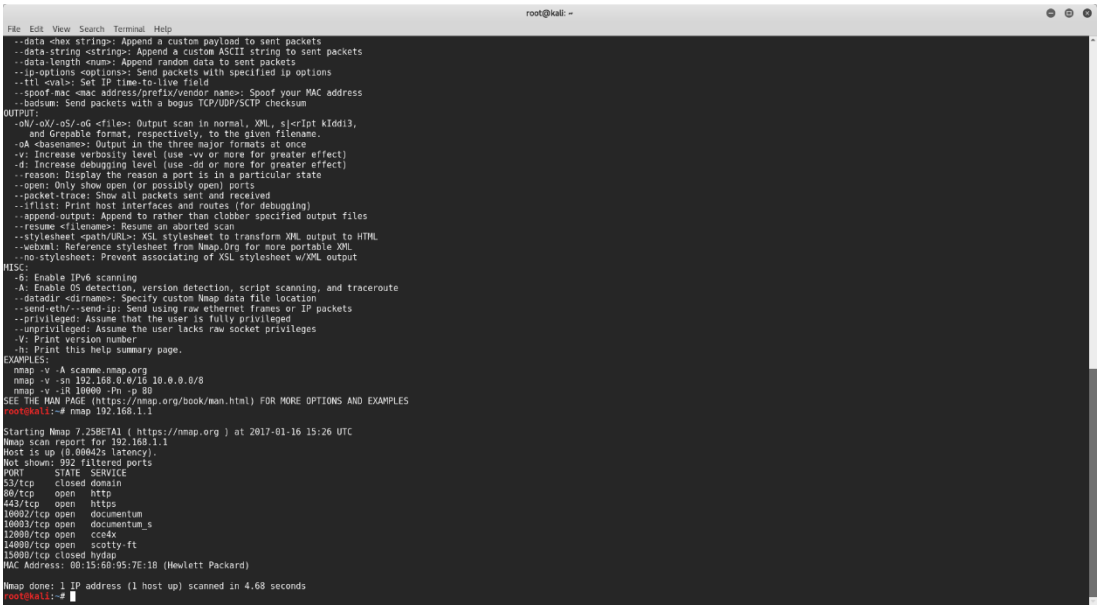
Se puede usar Nmap para comprobar si existen usuarios con contraseñas vacías o usuarios y contraseñas por defecto. Con Nmap se puede observar el ingreso anónimo de usuarios, esto quiere decir sin requerir usuario y contraseña). Se puede obtener información que se recolecta del puerto 80, tal como es el nombre del equipo y su versión de sistema operativo. (Pérez, 2015)

Con vuln, es posible verificar si un equipo presenta algunas de las vulnerabilidades conocidas, como puede ser en el puerto 80 (HTTP), como puede ser la vulnerabilidad CSRF (Cross Site Request Forgery) que es un tipo de exploit malicioso de cualquier página web, su función principal es la de enviar comandos no autorizados sean transmitidos por un usuario a una página web en que confía. Así como también vulnerabilidades de ataques DoS. (Pérez, 2015)

Como podemos observar Nmap tiene varias opciones para poder hacer un escaneo de una red, sabiendo que no es su función principal, podemos usarlo para poder hacer una auditoría de los equipos de una red.

Como ya es de conocimiento, Nmap es un programa que sirve para auditar las redes de seguridad de una empresa. Existen dos formas de utilizarlo, una es la propia Nmap que utiliza la terminal de Linux para ejecutar sus comandos.

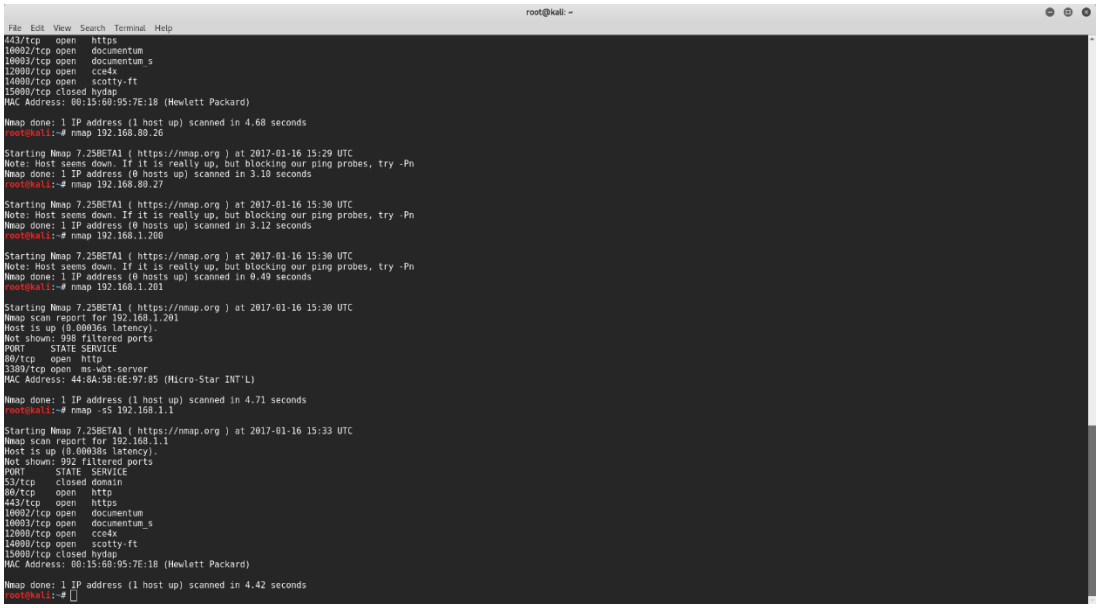
Ilustración 56: Nmap



Autor: R Avilés, M Silva, enero 2017

Nmap tiene varios comandos, la que se utiliza primero es la de escanear con un IP conocido, este es un escaneo simple que hace, nos muestra principalmente los puertos que se encuentra abiertos, utilizando otras opciones como Nmap –sS IP, con esta no dejamos registros en el sistema que se realizó el escaneo.

Ilustración 57: Nmap

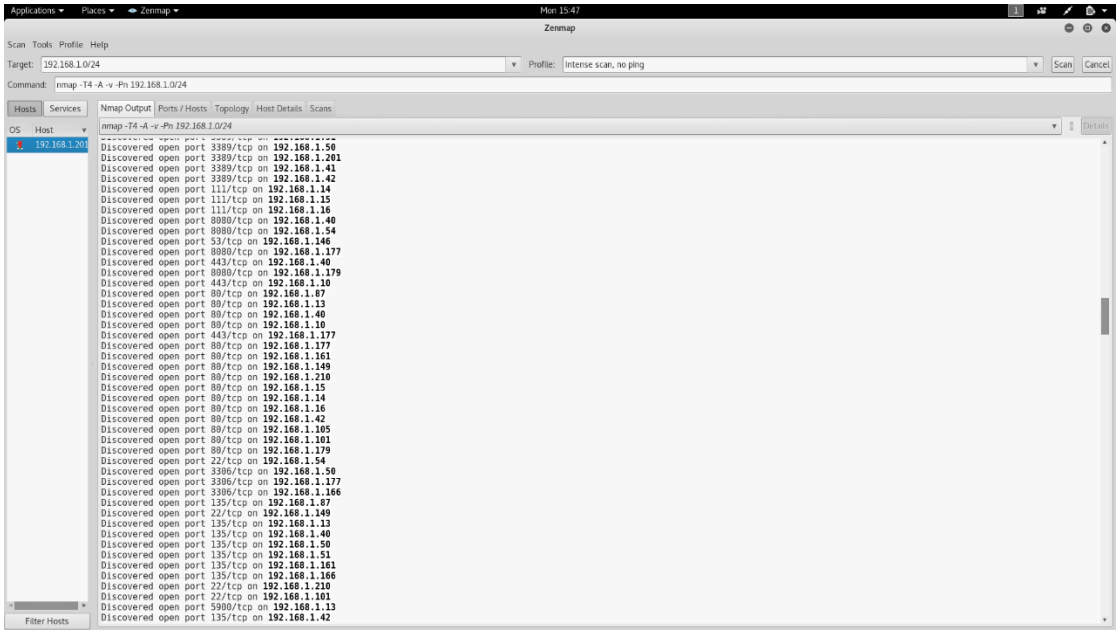


Autor: R Avilés, M Silva, enero 2017

También tiene la forma gráfica que pasa a llamarse Zenmap, este programa se lo puede utilizar en Windows, al ser gráfico no requiere de comandos para ejecutar acciones, lo único que se debe hacer es poner la IP que se tiene y seleccionar el tipo de escaneo que se vaya a utilizar.

En este caso se probó toda la Red de que esté conectado la facultad y utilizó la opción de Escaneo Intenso, pero que no haga Ping en los ordenadores conectados.

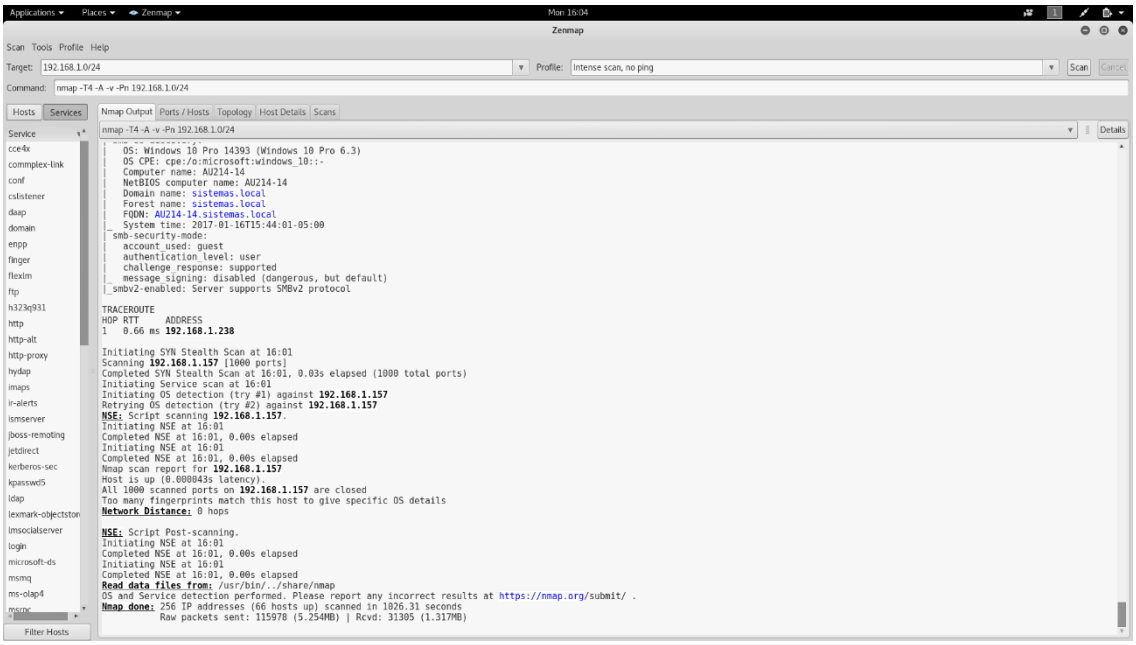
Ilustración 58: Nmap



Autor: R Avilés, M Silva, enero 2017

Conforme va realizando el escaneo, muestra los puertos abiertos que tiene cada una de las computadoras que estén conectadas a la red.

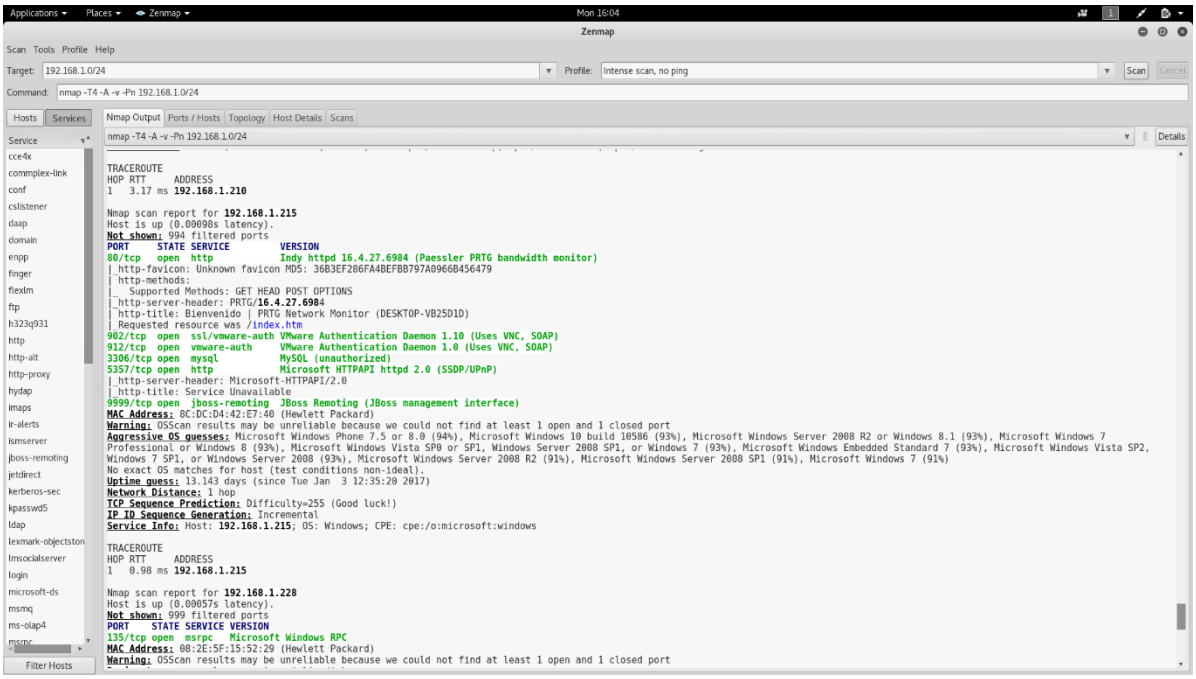
Ilustración 59: Nmap



Autor: R Avilés, M Silva, enero 2017

Cuando finaliza el escaneo, muestra detalladamente los puertos abiertos y los programas que utilizan los puertos que se encuentran abiertos, además de datos privados de cada ordenador.

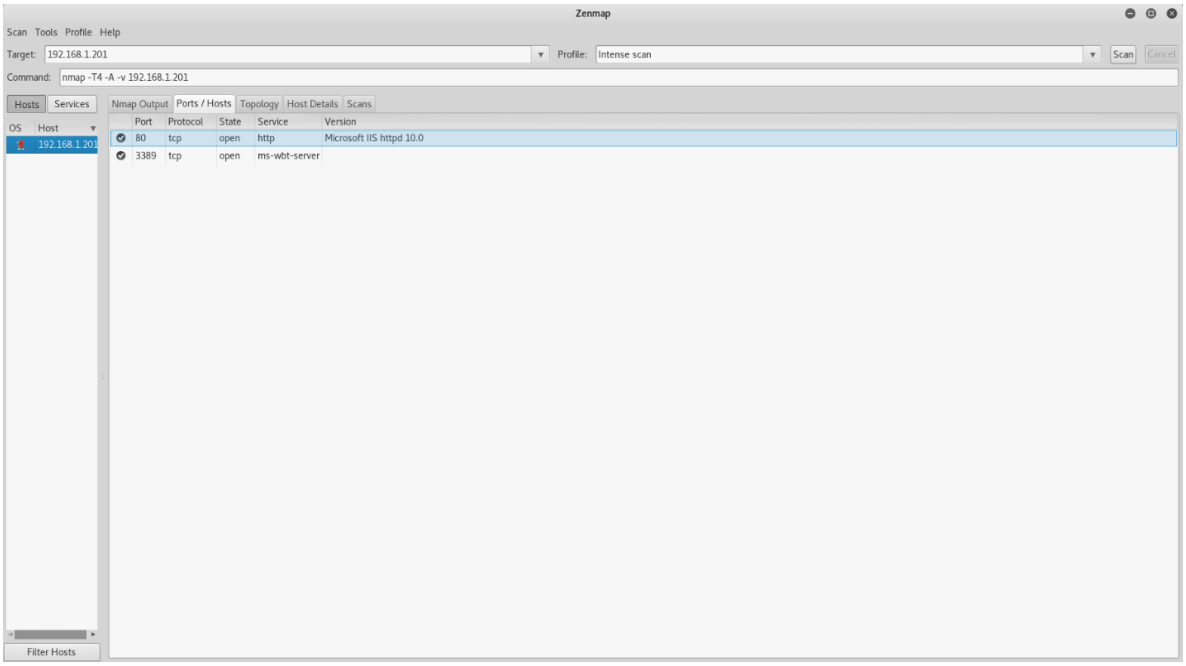
Ilustración 60: Nmap



Autor: R Avilés, M Silva, enero 2017

Otra de las opciones que tiene Zenmap, es lo que se puede observar en detalle los puertos o Host abiertos de cada IP.

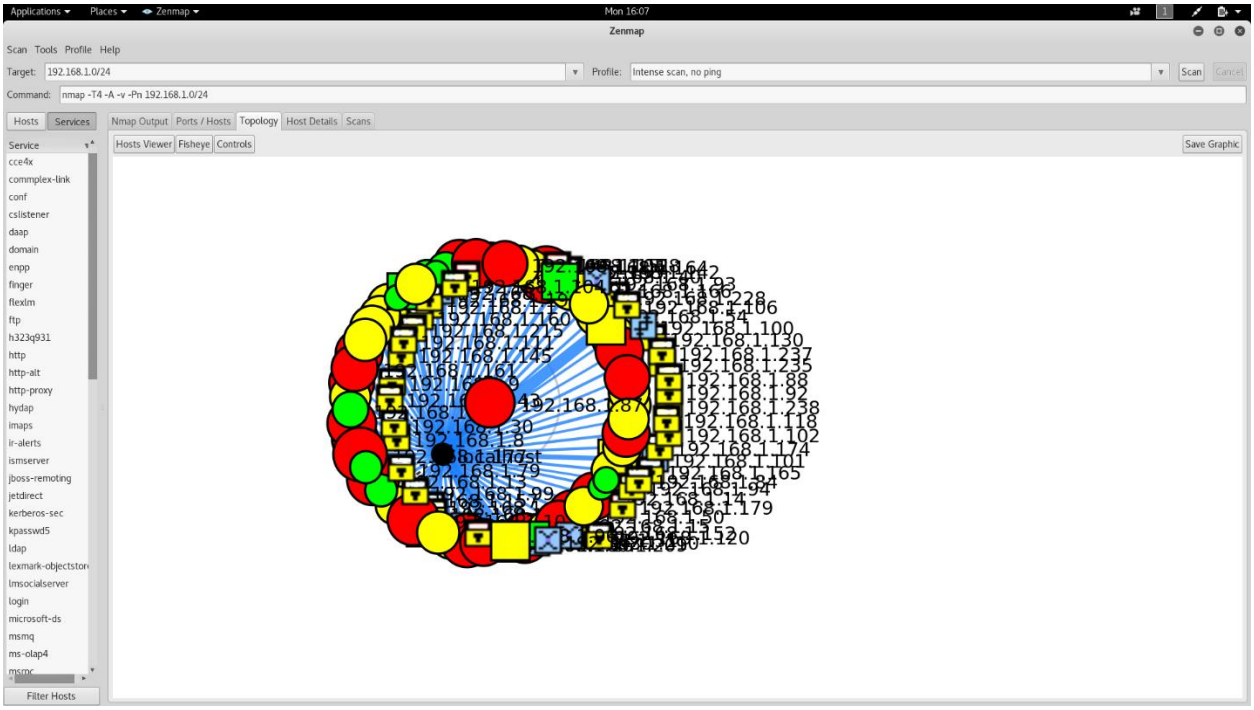
Ilustración 61: Nmap



Autor: R Avilés, M Silva, enero 2017

Otra opción es la de Topología, en donde muestra la topología de cómo está conectada la red, con los colores que nos indican cuáles son lo que mayores vulnerabilidades tienen.

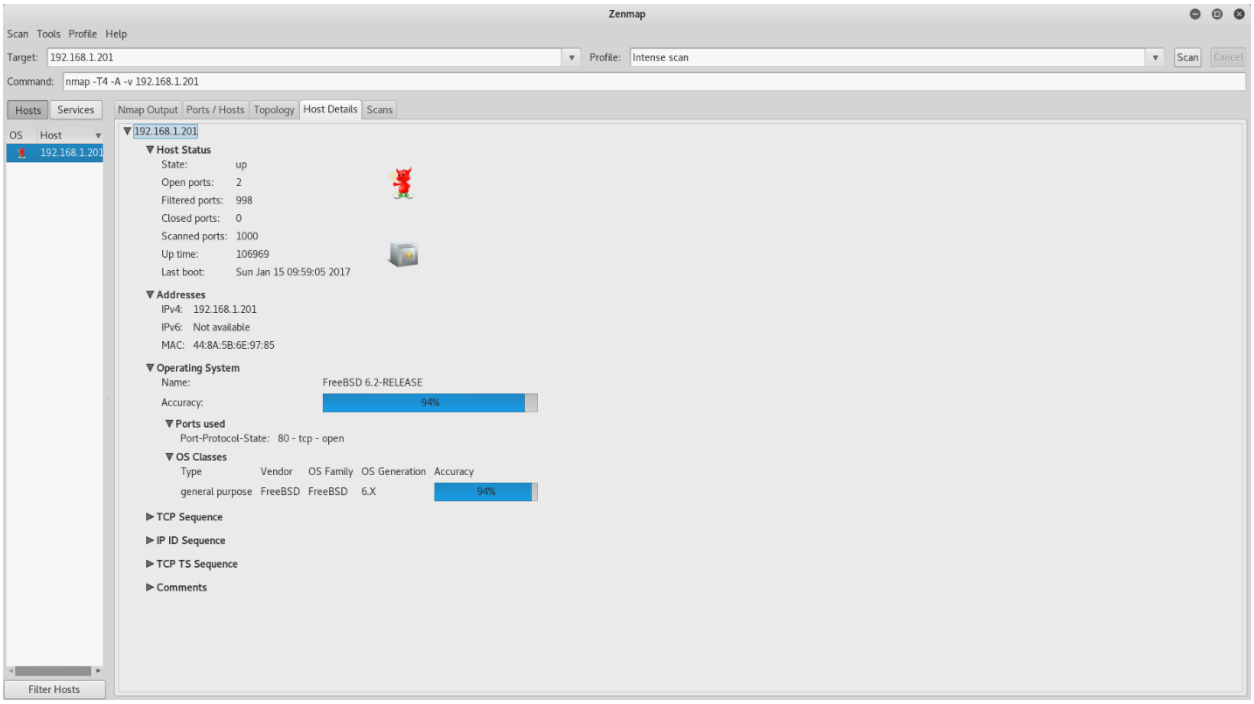
Ilustración 62: Nmap



Autor: R Avilés, M Silva, enero 2017

Detalles del Host con todos los datos.

Ilustración 63: Nmap



Autor: R Avilés, M Silva, enero 2017

4.4. Dentro de Kali Linux

Kali Linux más que una herramienta es un sistema operativo, dentro del cual se encuentran varias herramientas para escaneo y auditoría de redes, dentro de este se encuentra las herramientas como Nmap y Wireshark aparte de muchas opciones como es el caso de Armitage.

Kali Linux viene a ser un sistema operativo basado en Debian 8 “Jessie” que se utiliza para lo que es el Hackeo ético, principalmente, dispone de varias herramientas para realizar todo tipo de actividades.

Ilustración 64: Kali

Autor: R Avilés, M Silva, enero 2017

Armitage

Esta herramienta, la cual va de la mano con Metasploit, ya que junto con esta puede generar y ocupar Scripts los cuales nos pueden permitir la observación de objetivos, exploits y también la muestra de las características avanzadas de post-explotación que tenga el Framework. (Corporación Warez, 2016)

Con Metasploit se puede usar una misma sesión en nuestro equipo, también a su vez nos da la posibilidad de compartir el host, los datos que fueron encontrados y los archivos guardados, este también puede comunicarse a través de un registro de eventos compartidos y ejecutar bots para poder tener todas las tareas del equipo automatizadas. Armitage utiliza Nmap para realizar el

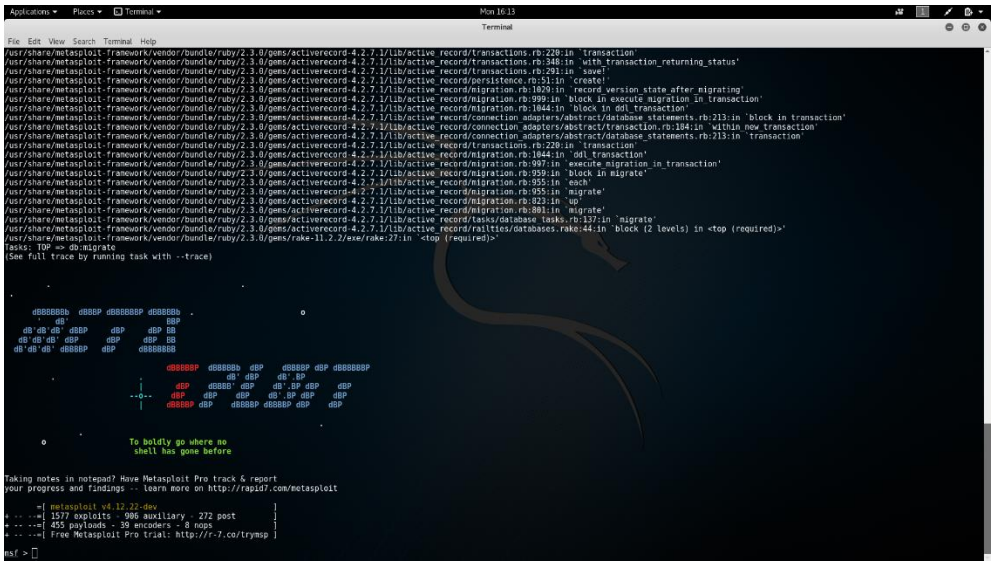
escaneo de la red, por lo que tiene las mismas opciones que tiene Nmap. (Corporación Warez, 2016)

Lo que diferencia a Armitage de todas las herramientas previamente mencionadas, es la posibilidad de realizar exploits mediante Metasploit, al realizar esto podemos escoger en un ordenar de nuestra red los exploits que haya encontrado al usar Nmap, un ejemplo que tienen muchos ordenadores es el de Apache Tomcat en el cual se puede observar que el tomcat_mgr_login el cual es el módulo que buscará la clave y el nombre de usuario que puede utilizar. Una vez que se obtiene y se encuentra esto, pasara a correr el tomcat_mgr_deploy explotándolo para obtener una shell en el host. (Corporación Warez, 2016)

Con Armitage es posible lanzar los exploits a los ordenadores, si tiene éxito, el programa hace que el host comprometido aparezca de color rojo. (Corporación Warez, 2016)

Una herramienta usada frecuentemente para realizar testeos es Armitage, cuyas funciones son muy completas y sobre todo el alcance que llega a tener esta herramienta. Para utilizarlo primero se debe activar el Metasploit.

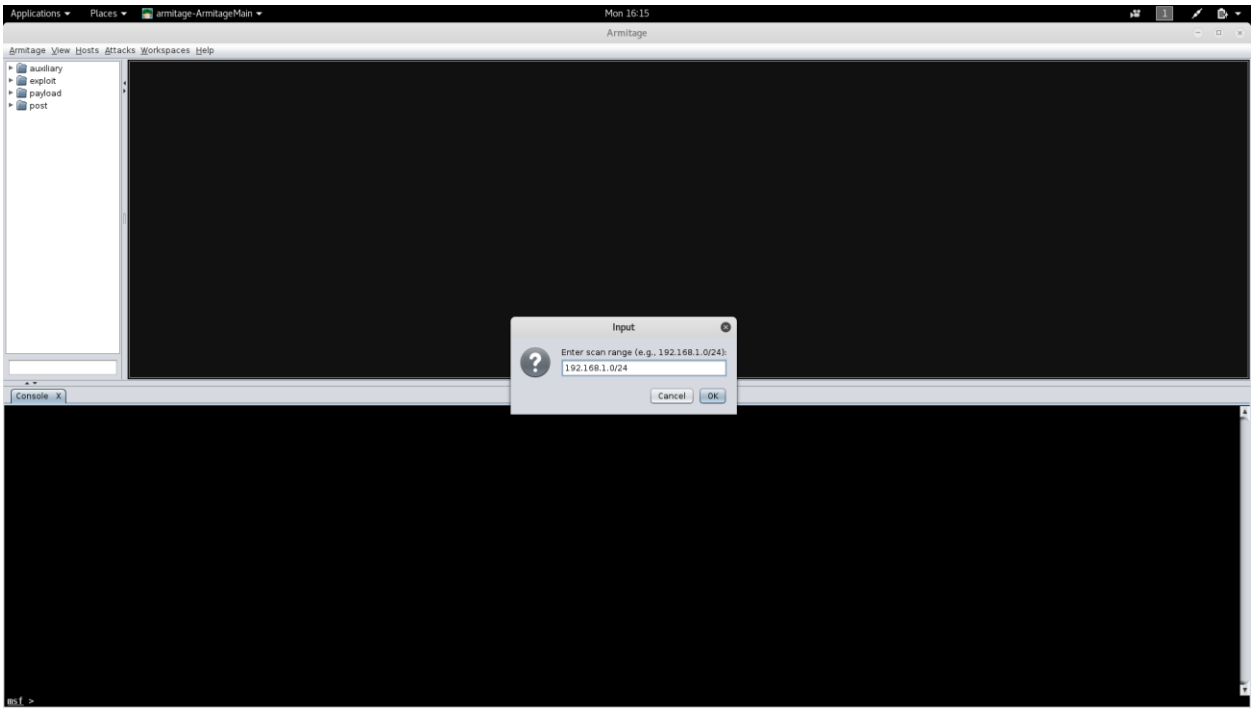
Ilustración 65: Kali



Autor: R Avilés, M Silva, enero 2017

Después de activo el Metasploit se continua con la ejecución del programa propiamente, el momento en que ingresa a la ventana principal, se visualiza con un ambiente gráfico similar al de Zenmap, y esto se debe a que Armitage utiliza Nmap para realizar los escaneos de Red. De igual manera se debe poner el rango que queremos escanear.

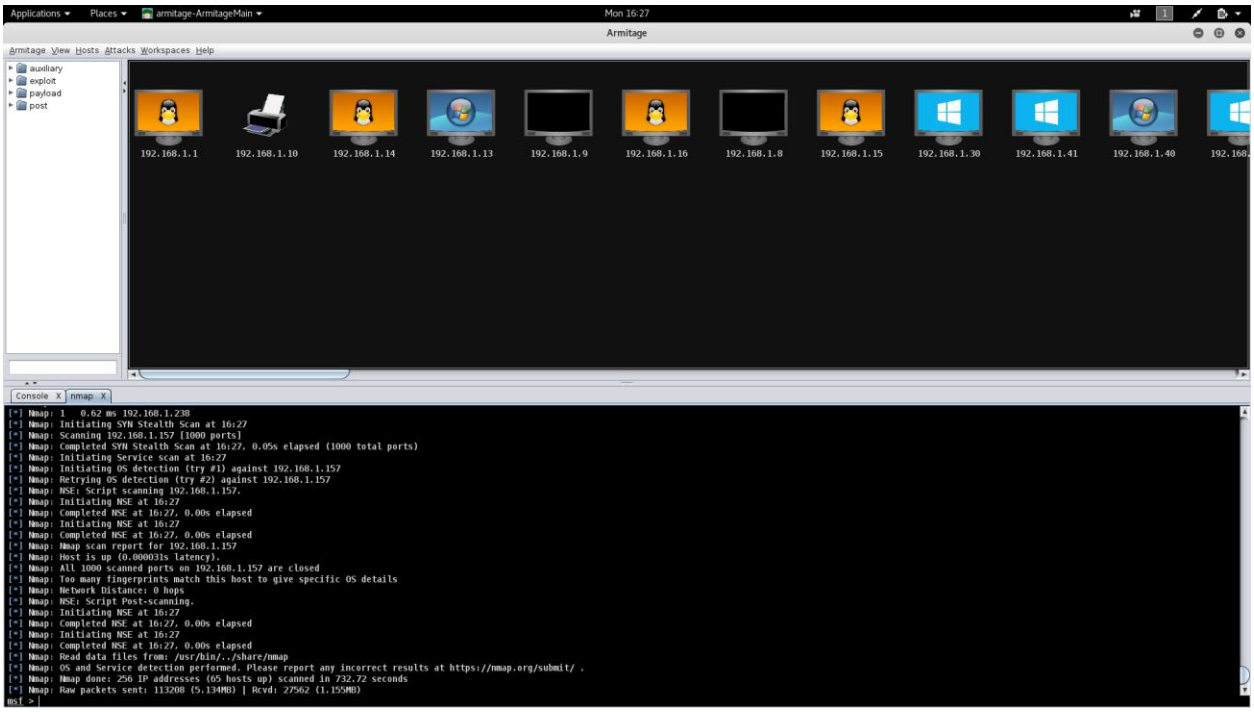
Ilustración 66: Kali



Autor: R Avilés, M Silva, enero 2017

El momento en que finaliza el escaneo, en la pantalla principal, muestra todos los ordenadores conectadas a la Red con sus respectivos Sistemas Operativos.

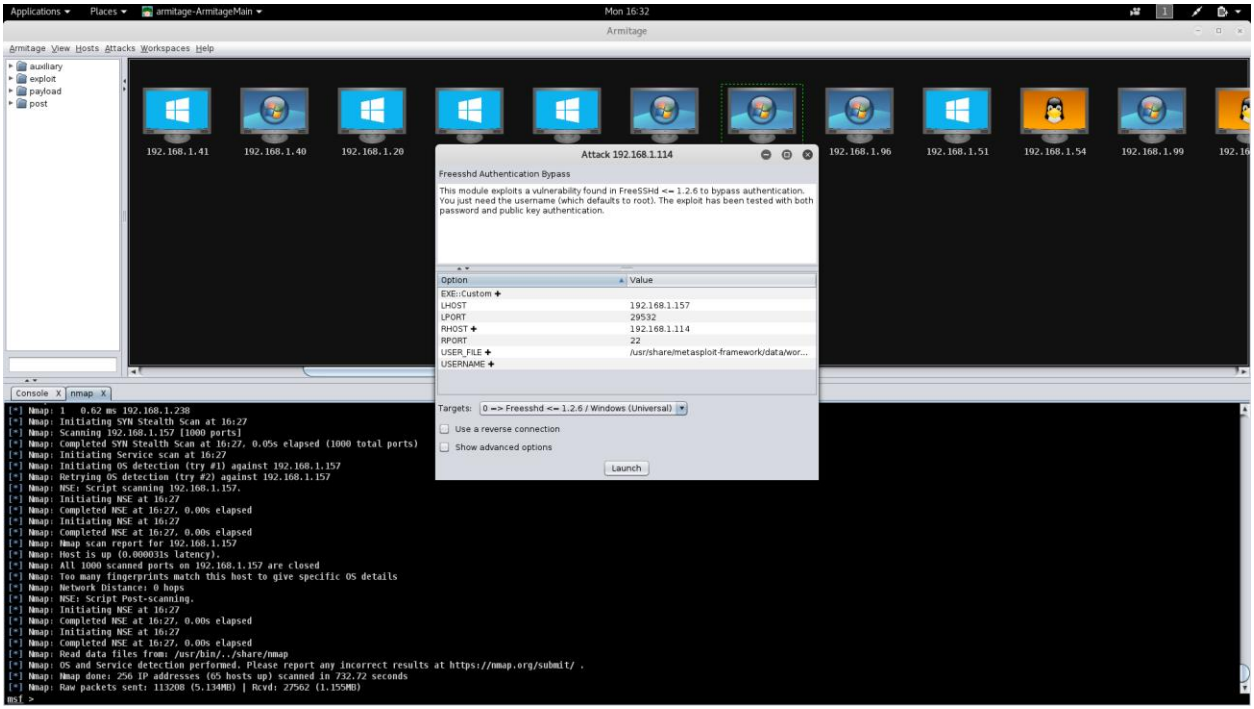
Ilustración 67: Kali



Autor: R Avilés, M Silva, enero 2017

Similar a Nmap se puede realizar diferentes tipos de escaneos para observar los puertos y host abiertos, pero lo interesante de este programa es, que dependiendo el sistema operativo y las vulnerabilidades que tenga cada computador, se puede realizar ataques informáticos de distintas maneras, lo cual ayuda al momento de realizar el documento con todas las vulnerabilidades existente.

Ilustración 68: Kali



Autor: R Avilés, M Silva, enero 2017

CAPÍTULO 5

INFORME DE SEGURIDAD

5.1. Modelo de Seguridad

Para la disertación de grado, se utiliza un test de intrusión informada e interna, esto quiere decir que se utiliza información privada, que fue entregada por la empresa.

Este tipo de pruebas simula ataques hechos por un ente interno en la empresa y con cierto grado de información privilegiada, se lo realiza dentro de las instalaciones de la empresa, su principal enfoque es la de evaluar las seguridades, políticas y mecanismos internos de la empresa.

La importancia de realizar test de penetración, radica en que, en un ambiente de una compañía, esta puede alcanzar niveles óptimos de protección, a ser totalmente penetrable. Cosas como la instalación de nuevos dispositivos de red, o el cambio de configuración en los servidores, pueden aparecer fallos de seguridad en lugares que se creían seguros.

Debido a problemas secundarios con la empresa, no se pudo realizar las pruebes en ésta, debido a esto, las pruebas y resultados fueron obtenidos en la Red de la Universidad Católica de Ecuador.

Es importante mantener los costos de seguridad bajos, ya que, si para realizar un testeo los costos son muy elevados, la empresa puede considerar a esto como un gasto innecesario.

Se debe tener una política de seguridad en la empresa, se sabe que las políticas de seguridad de una organización son complejas y siempre hay personas afectadas, los errores de políticas casi siempre concluyen con efectos negativo.

5.1.1. Pasos a Seguir

Tabla 6: Pasos de Hacking

Paso	Descripción
Búsqueda de Vulnerabilidad	Se refiere generalmente a las comprobaciones automáticas de un sistema o sistemas dentro de una red.
Escaneo de la Seguridad	Se refiere en general a las búsquedas de vulnerabilidades que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles de la red y análisis profesional individualizado.
Test de intrusión	Se refiere en general a los proyectos orientados a objetivos en los cuales dicho objetivo es obtener un trofeo, que incluye ganar acceso privilegiado con medios pe-condicionales.
Evaluación de Riesgo	Se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación de negocios, las justificaciones legales y las justificaciones específicas de la industria.
Auditoría de Seguridad	Hace referencia a la inspección manual con privilegios administrativos del sistema operativo y de los programas de aplicación del sistema o sistemas dentro de una red o redes.
Hacking Ético	Se refiere generalmente a los test de intrusión en los cuales el objetivo es obtener trofeos en la red dentro del tiempo predeterminado de duración del proyecto.
Test de Seguridad y su equivalente militar, Evaluación de Postura	Es una evaluación de riesgo con orientación de proyecto de los sistemas y redes, a través de la aplicación de análisis profesional mediante 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.

5.2. Recomendaciones Antes de Hacer un Test

Para ejecutar cualquier test de seguridad a una Red cualquiera, es necesario tener un permiso previo, ya sea este oral o escrito por las autoridades pertinentes.

Prohibido el uso de nombres de clientes previos, incluso con el consentimiento de los mismos.

Analista éticamente está obligado a mantener la confidencialidad y no divulgación de información.

En análisis remotos, el contrato debe incluir origen de pruebas por número telefónico y las direcciones IP.

Es importante que los analistas conozcan las herramientas que van a utilizar, origen, uso y haberlas probado.

Cuando se encuentren vulnerabilidades de riesgo crítico, huecos de seguridad y que estas permitan un total acceso sin monitorización, sin dejar rastro, deben ser reportadas inmediatamente al cliente con una solución al problema lo más rápido posible.

Ataques DDOS (Negación del servicio distribuida) están totalmente prohibidos.

Evaluación de Riesgos.

Es necesario recopilar toda la información posible de la empresa para poder realizar un test efectivo.

Todos los test se deben realizar con la mayor precaución posible para evitar los peores escenarios, esto quiere decir, el respeto por la seguridad tanto de los empleados como de los usuarios.

Todos las pruebas que se hayan realizado, deben ser diseñadas para buscar la complejidad mínima, máxima viabilidad y que sean bastante claras.

5.2.1. Tipos de Riesgos

Se identifica los riesgos existentes dividiéndolos por tipos:

Vulnerabilidad: las vulnerabilidades son fallas que vienen en los propios mecanismos de seguridad o pueden ser alcanzados por medio de las protecciones de seguridad, lo que puede causar es el acceso con privilegios a la ubicación, personal o acceso remoto a los procesos, causando generación de datos corruptos o borrados.

Debilidad: viene en la propia plataforma o ambiente en que el mecanismo de seguridad se encuentra, puede venir por una mala configuración, falla de uso, o por una falla en cumplir los requerimientos de las Políticas de Seguridad.

Filtrado de Información: esta se puede dar por errores que se encuentran en el propio mecanismo, o a su vez también estas también pueden ser alcanzadas por medidas de seguridad la cuales hacen que se libere el acceso privilegiado a información privada de la información, datos personales de usuarios o empleados y procesos.

Desconocido: un elemento sin categoría o desconocido en el propio mecanismo, que puede ser alcanzado con medidas de seguridad y se desconoce de su impacto a la seguridad.

En Base al Manual de la "Metodología Abierta de Testeo de Seguridad" (OSSTMM 2.1), se ha realizado un hackeo de forma Ética, siguiendo los diferentes módulos que tiene esta metodología. (Herzog, 2003)

5.3. Revisión de la Inteligencia Competitiva

Es información que se puede recolectar buscando simplemente en Internet, a diferencia de robo de información que se puede hacer mediante hackeo o espionaje empresarial, esta no es invasiva y es muy discreta.

Es de suma importancia poder hacer un diagrama o mapa, mediante el cual se pueda medir la estructura de los servidores web o FTP. Mediante esto se puede medir el precio de todo el TI de la infraestructura de Internet, el costo de soporte de la infraestructura basado en el requerimiento salarial de los profesionales de TI.

5.4. Revisión de Privacidad

Es la parte legal y ética de la información, transmisión y almacenamiento de datos. El uso que se pueda dar a cualquier información, es la reocupación principal de las personas, específicamente a datos privados que se puedan manejar.

Tabla 7:Resultados

Resultados Esperados:	Lista de cualquier revelación
	Lista de fallas de conformidad entre la política pública y la práctica actual
	Lista de los sistemas involucrados en la recolección de datos
	Lista de técnicas de obtención de datos
	Lista de datos obtenidos

Autor: R Avilés, M Silva, enero 2017

5.5. Logística y Controles

El objetivo es eliminar la mayoría de falsos positivos y falsos negativos, haciendo ajustes necesarios en las herramientas de análisis.

Para controlas los paquetes TCP, UDP, ICMP, se utilizó el programa Wireshark, como se pudo comprobar en capítulos anteriores, este programa lo que nos muestra es todas las actividades que estén realizando en ese momento los ordenadores que estén conectadas a la Red.

Dentro del programa se filtra los paquetes eliminando los falsos positivos y falsos negativos, solo quedando con los que se va a utilizar.

Tabla 8:Resultados

Comprobación de Error	Examinar la ruta a la red objetivo en busca de paquetes TCP perdidos.
	Examinar la ruta a la red objetivo en busca de paquetes UDP perdidos.
	Examinar la ruta a la red objetivo en busca de paquetes ICMP perdidos.
	Medir el tiempo utilizado en el recorrido TCP de los paquetes.
	Medir la latencia TCO a través de conexiones TCP.
	Medir el porcentaje de paquetes aceptados y respondidos por la red objetivo.
	Medir la cantidad de paquetes perdidos o rechazos de conexión en la red objetivo.

Autor: R Avilés, M Silva, enero 2017

5.6. Sondeo de Red

El sondeo o escaneo de la red, muestra y ayuda a la introducción de los sistemas que van a ser analizados. Para realizar un sondeo de Red, el mejor programa es Nmap, en este caso Zenmap, que es el programa gráfico de Nmap, el cuál no solo funciona en Kali Linux, también tiene una versión para Windows, el cual funciona de la misma manera.

Se la puede especificar de una mejor manera como una combinación de obtención de información y también recolección de datos. Desde un punto de vista legal, es recomendable definir de una manera exacta y contractualmente los sistemas que se vaya a analizar si la persona que va a realizar el test es un auditor, puede ser de la misma empresa o externo, es posible que no se pueda empezar a realizar un test con los nombres de sistema o IPs en concreto. Es debido a esta razón que es necesario sondear y analizar la Red. Lo indispensable es poder obtener el mayor número de sistemas que deben ser analizados, claro está que no se puede exceder los límites legales de lo que se debe analizar. Debido a esto, escanear una red es una manera de empezar a realizar un test; otra manera es la de recibir el rango de direcciones IP a comprobar. Lo más importante es

la de realizar ningún tipo de intrusión directa en los sistemas, excepto en los sitios considerados un dominio cuasi-público.

Al realizar los escaneos simples nos muestra los nombres de los dominios, nombres de servidores, las direcciones IP de los ordenadores conectados a la Red, Zenmap también nos muestra un mapa de Red.

Tabla 9:Resultados

Resultados esperados:	Nombres de Dominio
	Nombres de Servidores
	Direcciones IP
	Mapa de Red
	Información ISP/ASP
	Propietarios del Sistema y del Servicio
	Posibles limitaciones del Test

Autor: R Avilés, M Silva, enero 2017

5.7. Identificación de los Servicios de Sistemas

Para escanear e identificar puertos usamos el programa Zenmap o Nmap, es la prueba invasiva de los puertos del sistema en los niveles de transporte y red. Cada servidor activo en Internet dispone de 65.536 puertos TCP y UDP. No es necesario realizar un escaneo de todos los puertos. Esto es libre elección de la persona que va a realizar los tests.

Para agilizar el trabajo, se listan los puertos que son importantes.

Para obtener toda la identificación de los servicios de Sistemas, se vuelve a usar Zenmap, pero en esta ocasión, se utiliza un escaneo completo, el cual muestra los puertos abiertos y cerrados, el sistema operativo que utilizan los ordenadores conectados a la Red.

El momento en que los puertos abiertos son identificados, es necesario realizar un análisis de la aplicación que escucha tras dicho servicio. En algunos casos se da que está múltiples aplicaciones las cuales se pueden encontrar detrás de un servicio donde una aplicación es la que realmente esta escuchando dicho puerto y las otras se consideran como parte de los componentes de la aplicación que escucha. (Herzog, 2003)

Tabla 10:Resultados

Resultados Esperados:	Puertos abiertos, cerrados y filtrados
	Direcciones IP de los sistemas activos
	Direccionamiento de los sistemas de la red interna
	Lista de los protocolos descubiertos de tunelizado y encapsulado
	Lista de los protocolos descubiertos de enrutado soportados
	Servicios activos
	Tipos de Servicios
	Tipo y nivel de parcheado de las Aplicaciones de los servicios
	Tipo de Sistema Operativo
	Nivel de parcheado
	Tipo de Sistema
	Lista de Sistemas activos
	Mapa de la Red

Autor: R Avilés, M Silva, enero 2017

5.8. Búsqueda y Verificación de Vulnerabilidades

El objetivo de esto es en sí poder identificar, verificar y comprender las debilidades, los fallos que se encuentran en la configuración y sobre todo la vulnerabilidad que se encuentra en una red ya sea local o externa del servidor o en el mismo.

La búsqueda de vulnerabilidades utilizando herramientas automáticas, como Zenmap en Windows, o Nmap en Kali Linux, es una manera eficaz de poder determinar inseguridades y

parches que se haya realizado en el sistema. También se usa otro tipo de programas, la diferencia es que algunos que son completos en lo que a escanear y verificar vulnerabilidades son programas de pago, se estima que muchas empresas grandes utilizan estos programas debido a que se paga un estimado de 2500 dólares anuales, o que para pequeñas y medianas empresas resulta un costo elevado y a la final terminen por quitar a la seguridad informática de las prioridades de la compañía. Se sabe que estos escáneres actúan tanto en el mercado laboral como en el mundo Hacker, es importante que la persona encargada de realizar el hackeo, identificar y poner en las pruebas los scripts y exploits que se utilizan para hackear. Como ya se ha insistido en pasos anteriores, es importante siempre verificar los falsos positivos y aumentar el conocimiento sobre hackeo, descubrir vulnerabilidades depende mucho de la experiencia y la creatividad de la persona que va a realizar el Hackeo.

Es importante integrar en las pruebas los programas de escaneo que se hayan usado, las herramientas, usar al menos dos tipos diferentes de escáneres para obtener más información o verificar la ya obtenida.

Pode encontrar todas las vulnerabilidades o fallos con similitudes en las aplicaciones, sistemas operativos o sistemas los cuales son similares y pueda de una manera perjudicar al sistema objetivo en general.

Tabla 11:Resultados

Resultados Esperados:	Tipo de aplicación o servicio por vulnerabilidad
	Niveles de parches de los sistemas y aplicaciones
	Listado de posibles vulnerabilidades de denegación de servicio
	Listado de áreas securizadas a través de ocultación o acceso visible
	Listado de vulnerabilidades actuales eliminando falsos positivos
	Listado de sistemas internos o en la DMZ (Zona Desmilitarizada)
	Listado de convenciones para direcciones de e-mail, nombres de servidores, etc…
	Mapa de Red

Autor: R Avilés, M Silva, enero 2017

5.9. Testeo de Control de Acceso

El Firewall es el que controla el flujo de tráfico de red, en la propia empresa, DMZ y también en la Internet. Su funcionalidad es la de seguridad y usa ACL´s (Listas de Control de Acceso). Lo que se hace es asegurar que el Firewall permita el ingreso solo a aquello que puede ser aceptado dentro de la red, lo demás debe ser negado.

La mejor forma de verificar todo esto, es viendo si el Firewall está correctamente ocupándose del filtrado del tráfico de la red local hacia afuera, también esta debe mostrar si está detectando las direcciones de orígenes falsos. Es importante probar las capacidades externas del Firewall desde el interior de la Red.

5.10. Testeo de Medidas de Contingencia

Se trata acerca de lo que es fácilmente atravesable y como saber manejarlo, se refiere a programas maliciosos y a emergencias, medir en lo posible los recursos mínimos necesarios como el Firewall que utiliza la empresa y antivirus que se encuentren instalados en los ordenadores.

5.11. Evaluación de Políticas de Seguridad

Con Políticas de Seguridad se refiere al documento de cualquier empresa, en donde se bosqueja la disminución de riesgos con el uso de tipos específicos de tecnología.

Se debe realizar un testeo de lo que se escribió en las políticas contra el estado actual de las conexiones de la presencia de internet y las no relacionadas a esta. Y asegurar que las políticas estén incluidas dentro de las justificaciones de negocio de la organización, y de los estatutos legales locales, federales e internacionales, en especial en referencia a los derechos y responsabilidades tanto del empleador como de los empleados y la ética de la privacidad personal. (Herzog, 2003)

- Comparar la política de seguridad contra el estado actual de la presencia en Internet.
- Junto a la aprobación de la gerencia permite buscar cualquier signo que revele que la política está aprobada por la gerencia. Ya que, si incumple esto, el personal no tiene la obligación de seguir las reglas establecidas en la política. (Herzog, 2003)
- Cerciórese de que la documentación está adecuadamente almacenada, ya sea electrónicamente o en otros medios, y que la política ha sido leída y aceptada por el personal incluso antes de que ellos obtengan acceso a los sistemas informáticos. (Herzog, 2003)
- Identificar los procedimientos de manejo de incidentes, para asegurar de que las brechas de seguridad son manejadas por las personas adecuadas y que son reportadas de manera apropiada. (Herzog, 2003)
- Identificar los procedimientos de manejo de incidentes, para asegurar de que las brechas de seguridad son manejadas por las personas adecuadas y que son reportadas de manera adecuada. (Herzog, 2003)

- Conexiones Entrantes: verificar los riesgos mencionados que tienen relación directa con las conexiones entrantes de Internet (Internet – DMZ, Internet – red interna), y las medidas que son necesarias implementar para reducir o eliminar dichos riesgos. Esos riesgos pueden ser permitidos en conexiones entrantes, típicamente SMTP, POP3, HTTP, HTTPS, FTP, VPNs y las correspondientes medidas como esquemas de autenticación, encriptación y Listas de Control de Acceso. Específicamente, las reglas que niegan el acceso con estado a la red interna generalmente no son alcanzadas por la implementación. (Herzog, 2003)
- Conexiones Salientes: Las conexiones salientes pueden producirse entre la red interna y DMZ, así como también entre la red interna e Internet. Buscar cualquier regla de conexiones salientes que no se corresponda con la implementación. Las conexiones salientes no pueden ser usadas para introducir código malicioso o revelar las especificaciones de la red interna. (Herzog, 2003)
- Medidas de Seguridad: Las reglas que exigen la implementación de medidas de seguridad, deben ser cumplidas. Aquellas pueden hacer uso de AVS, Firewalls, DMZ´s, routers y las configuraciones/implementaciones adecuadas de acuerdo con los riesgos a contrarrestar.
- Poder asegurar la política de seguridad en lo referente al estado actual de las conexiones que no tienen una relación a Internet o no pertenezcan a ella. (Herzog, 2003)
- Verificar que la política de seguridad establezca las medidas de contención y las pruebas de ingeniería social basados en el uso indebido de Internet por parte de los empleados, de acuerdo con la justificación de negocios y ñas mejores prácticas de seguridad. (Herzog, 2003)

CAPÍTULO 6

RECOMENDACIONES Y CONCLUSIONES

6.1. Conclusiones

- Es necesario tener un ambiente cerrado con ordenadores específicos, para poder saber a detalle los ataques que sufre cada uno de éstos, y, sobre todo, poder comprobar si las recomendaciones que se hace a cada ordenador sean los que, de verdad, mejore la seguridad de los mismos.
- Mediante la investigación del origen, funcionamiento y las funcionalidades de las herramientas de Hacking Ético investigadas se puede ver como su uso puede llegar a ser útil para encontrar vulnerabilidades en los sistemas y de esta manera se pueda tomar cartas en el asusto y mejorar la protección de la organización.
- Sabiendo más acerca de la ingeniería social, se puede asegurar que es un método muy eficaz y peligroso para los empleados y personas particulares de cualquier empresa comprometan la información de la misma. Se puede ver que es diferente a cualquier otra amenaza a la seguridad de una corporación. De esta manera se evitan las tecnologías puestas en su lugar para proteger y detectar la actividad maliciosa. Es una amenaza que siempre existirá, y que no puede ser contenida por software, antivirus, parches completos, firewalls y sistemas de detección de intrusiones. Sólo se necesita de una persona no consciente para hacer un ataque de ingeniería social con éxito. Con la formación adecuada y las políticas establecidas, el riesgo de la ingeniería social puede ser mitigado eficazmente.
- La seguridad de datos privilegiados en una empresa es de vital importancia para las mismas, por lo que la seguridad informática cumple un rol importante, que consiste en la

protección de datos, en los tiempos actuales en donde toda información se traslada a través de Internet, por lo que es primordial proteger el flujo de datos, con esto se da a entender el lugar tan importante que ocupa la seguridad informática.

- Al analizar la situación de la empresa en lo que a seguridad de su información se refiere, se puede realizar un plan para utilizar las herramientas de forma ordenada y sobre todo efectiva. Mediante esto se puede tener un plan más estructurado y poder saber sobre los ataques o futuros ataques que se puedan dar, de esta manera se da información al empleado y se previene de incidentes.
- Después de haber realizado todas las pruebas de Hacking Ético, utilizando las herramientas previamente analizadas e implementadas, se realizó una metodología en base a todos los resultados obtenidos, se habla acerca de todas las fallas de seguridad encontradas y sobretodo como poder defendernos ante estas amenazas para que de esta manera no exista filtración de información u ataques en la empresa.
- El momento en que se evalúa y configura las herramientas, se las hace en base al estudio previo que se hizo a la infraestructura de TI de la empresa y al mapa de Red que esta tiene.
- Al analizar y manipular las herramientas de hackeo, se comprobó y mejoro toda la información que se tenía acerca de ataques informáticos, también se observó cómo estos afectaban a los ordenadores conectados y poder actuar de la mejor manera ante los mismos.

6.2. Recomendaciones

- Debido a que se realizó en un ambiente abierto, no se pudo ver detallada mente los ataques específicos a cada ordenador, por lo que se vio más en general, tampoco se pudo saber a ciencia cierta si las recomendaciones que se hacía para mejorar la seguridad surtían el efecto esperado o requerían de acciones adicionales.
- La pérdida o divulgación de datos pueden tener varios orígenes: error o malicia de un empleado o agente, el robo de un ordenador portátil, un fallo de hardware, o como resultado de daños por agua o fuego. Hay que asegurarse de almacenar datos en servidores de espacios previstos para ello y sin perjuicio de las copias de seguridad regulares. Medios de copia de seguridad deben ser almacenados en una habitación separada que aloja los servidores, a ser posible en una caja fuerte a prueba de fuego.
- El conjunto de reglas para la seguridad informática debe ser formalizado en un documento a disposición de todos los agentes o empleados. Su elaboración requiere el inventario previo de las posibles amenazas y vulnerabilidades que enfrenta un sistema de información. Debe ser regularmente evolucionar este documento, a la luz de los cambios en los sistemas informáticos y las herramientas utilizadas por el organismo en cuestión. Por último, el parámetro de "seguridad" debe tenerse en cuenta corriente arriba de cualquier proyecto relacionado con el sistema de información.
- Uno de los principales problemas fue el momento de realizar el hackeo a la empresa. Inicialmente se tenía planteado realizar un Hackeo Ético a la empresa Blenastor, pero por problemas internos de seguridad (se utiliza una empresa outsourcing para la seguridad de la base de datos), se decidió realizar todas las pruebas en la Facultad de la Universidad Católica del Ecuador.

- El programa de auditoria informática Nessus, anteriormente era de usa libre y gratuito para todos, pero a paso a ser privado con lo que para conseguirlo había que pagar una cifra alta anualmente, otro problema es que existe una versión gratuita la cual, solo sirve por siete días y aparte de eso muchas de las opciones son bloqueadas, y solo se las puede utilizar el momento de adquirir el producto.
- Debido a que los programas utilizados fueron ocupados en los servidores de la universidad, fue fácil acceder y poder realizar las pruebas necesarias, con lo que se recomienda poner mayor seguridad debido a la cantidad de estudiantes que ocupan la Red y están expuestos.
- El principal riesgo en términos de seguridad es un error humano. Los usuarios del sistema de información deben ser especialmente conscientes de los riesgos de TI asociados con el uso de bases de datos. Es importante siempre mantener informados y alertar a los empleados mediante notas, en las cuales se le hable sobre el correcto uso de la Internet, el correo electrónico e incluso e uso del teléfono.
- Fijación de la LAN ya que un sistema de información debe ser seguro cara a cara a los ataques externos. Un primer nivel de protección debe ser garantizada por las características de seguridad lógicas específicas, tales como filtros de paquetes, firewall, etc. Una protección fiable contra virus y software espía asume una vigilancia constante de actualizar estas herramientas, tanto en el servidor y el personal de los puestos. A veces, las conexiones entre sitios remotos de una empresa o de una autoridad local debe hacerse de forma segura a través de conexiones privadas o a través de canales, técnica segura del "túnel" o VPN (red privada virtual). También es esencial para asegurar las redes inalámbricas dada la posibilidad de interceptar la información que circula a distancia: el uso de claves de cifrado, el control de las direcciones físicas de los equipos cliente permitidos, etc. Por último, el

acceso remoto al sistema de información por el trabajo móvil debe estar precedida de una autenticación del usuario y la posición. El acceso a Internet a las herramientas requiere fuertes medidas de seguridad, incluyendo el uso de IPS, SSL / TLS o HTTP.

BIBLIOGRAFÍA

Bibliografía

Alegsa, L. (05 de Junio de 2014). *Alegsa.com.ar*. Obtenido de Alegsa.com.ar: http://www.alegsa.com.ar/Dic/script.php

Astudillo, K. (2013). Hacking Etico 101: Como Hackear Profesionalmente En 21 Dias O Menos! En K. Astudillo, *Hacking Etico* (págs. 12-13). Createspace Independent Pub.

AT&T. (27 de Enero de 2017). *corp.att*. Obtenido de corp.att: http://www.corp.att.com/history/nethistory/switching.html

Castellanos, E. J. (04 de 05 de 2011). *Revista .Seguridad - UNAM*. Obtenido de Revista .Seguridad - UNAM: http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana#_ftn1

Castellanos, E. J. (4 de Junio de 2011). *Seguridad Cultura de prevencion para TI.* Obtenido de Seguridad Cultura de prevencion para TI: http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

Cisco. (10 de Agosto de 2005). *TCP/IP Overview*. Obtenido de Cisco: http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13769-5.html

Cisco. (17 de Octubre de 2014). *cisco.* Obtenido de cisco: https://hacking-etico.com//wp-content/uploads/2014/03/cisco2014_infosec_report.pdf

Cisco. (10 de Enero de 2017). *cisco*. Obtenido de cisco: http://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

Comer, D. E. (1996). *Redes Globales de Información con Internet y TCP/IP.* Pearson Educacion .

ConectaBell. (26 de Junio de 2015). *ConectaBell, Informática, Seguridad, Sistemas y Programación.* Obtenido de ConectaBell, Informática, Seguridad, Sistemas y Programación.: https://conectabell.com/nmap-historia-y-usos-basicos/

Corporación Warez. (30 de Septiembre de 2016). *www.corporacionwarez.com*. Obtenido de www.corporacionwarez.com: http://corporacionwarez.com/armitage-fondo-manual-de-armitage-en/

Gómez, V. Y. (11 de 2011). *Wordpress.* Obtenido de Wordpress: https://viclab.files.wordpress.com/2010/11/docfinal_pub.pdf

Herzog, P. (2003). *Manual de la Metodología Abierta de Testeo de Seguridad .* Institute for Security and Open Methodologies.

Izaskun Pellejero, F. A. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN.* Marcombo.

Kali Linux. (8 de Diciembre de 2013). *Kali Linux.* Obtenido de Official Kali Linux Documentation: http://docs.kali.org/introduction/what-is-kali-linux

Kaspersky Lab. (27 de Enero de 2017). *Kaspersky*. Obtenido de kaspersky: http://latam.kaspersky.com/internet-security-center/definitions

Larrieu, C. (29 de Enero de 2013). *CCM Benchmark Group.* Obtenido de Sistema de detección de intrusos (IDS): http://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids

López, A. (2010). *Seguridad informática.* Editex.

Lyon, G. (2008). *Nmap Network Scanning.* Sunnyvale: Insecure.Com LLC.

Malagón, C. (2010). *Nerbrija Universidad de Madrid.* Obtenido de Nerbrija Universidad de Madrid: http://www.nebrija.es/~cmalagon/seguridad_informatica/transparencias/Modulo_0.pdf

Michelena, A. V. (2005). Los Hackers. En A. V. Michelena, *Enredados / El Mundo de la Internet* (págs. 141- 143). Estudio Ghersi Editores.

Mieres, J. (1 de Enero de 2009). *evilfingers.* Obtenido de evilfingers: https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf

Miguel, J. T. (10 de Julio de 2015). *Implantación de aplicaciones web en entorno internet, intranet y extranet.* Ediciones Paraninfo.

MIRANDA, C. V. (2014). *Redes telemáticas.* Ediciones Paraninfo.

Molist, M. (30 de 04 de 2002). *Ingeniería social - Hack Story*. Obtenido de Ingeniería social - Hack Story: http://ww2.grn.es/merce/2002/is.html

Moreno, W. M. (2003). *Modelo Osi.* Obtenido de Modelo Osi: http://www.ie.itcr.ac.cr/marin/telematica/trd/01_modelo_OSI_v2.pdf

Official Nmap Project Guide to Network Discovery and Security Scanning. (2008). En G. Lyon, *Nmap Network Scanning* (págs. 68-69). Sunnyvale: Insercure.Com LLC.

Pérez, I. (12 de Febrero de 2015). *welivesecurity.com*. Obtenido de welivesecurity.com: http://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/

Quispe, C. A. (2013). *Revistasbolivianas.* Obtenido de Revistasbolivianas: http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a08.pdf

Ramos, B. G. (2015). Firewalls y Detectores de Intrusos. En B. G. Ramos, *Seguridad perimetral, monitorización y ataques en redes* (págs. 65-76). Bogotá: Ra-Ma Editorial.

Real Academia Española. (20 de 01 de 2017). *Real Academia Española*. Obtenido de Real Academia Española: http://dle.rae.es/?id=XTrIaQd

Rivero, M. (22 de Abril de 2008). *infospyware*. Obtenido de infospyware: https://www.infospyware.com/

Segu.Info. (20 de Abril de 2010). *Seguridad de la Informacion*. Obtenido de Seguridad de la Informacion: http://www.segu-info.com.ar/fisica/seguridadfisica.htm

Sheldon, T. (1997). *Manual de Seguridad de Windows NT.* S.A. MCGRAW-HILL / INTERAMERICANA DE ESPAÑA.

Tanenbaum, A. S. (2003). *Redes de computadoras.* Pearson Educacion.

Tenable. (2017). *www.tenable.com*. Obtenido de www.tenable.com: http://www.tenable.com/plugins/index.php?view=single&id=96830

Tolosa, G. (2014). *Protocolos y Modelos OSI.* Obtenido de Protocolos y Modelos OSI: http://www.tyr.unlu.edu.ar/pub/02-ProtocolosOSI.pdf

Toribio, G. (2016). *academia.* Obtenido de academia: https://www.academia.edu/14294410/Seguridad_Informatica

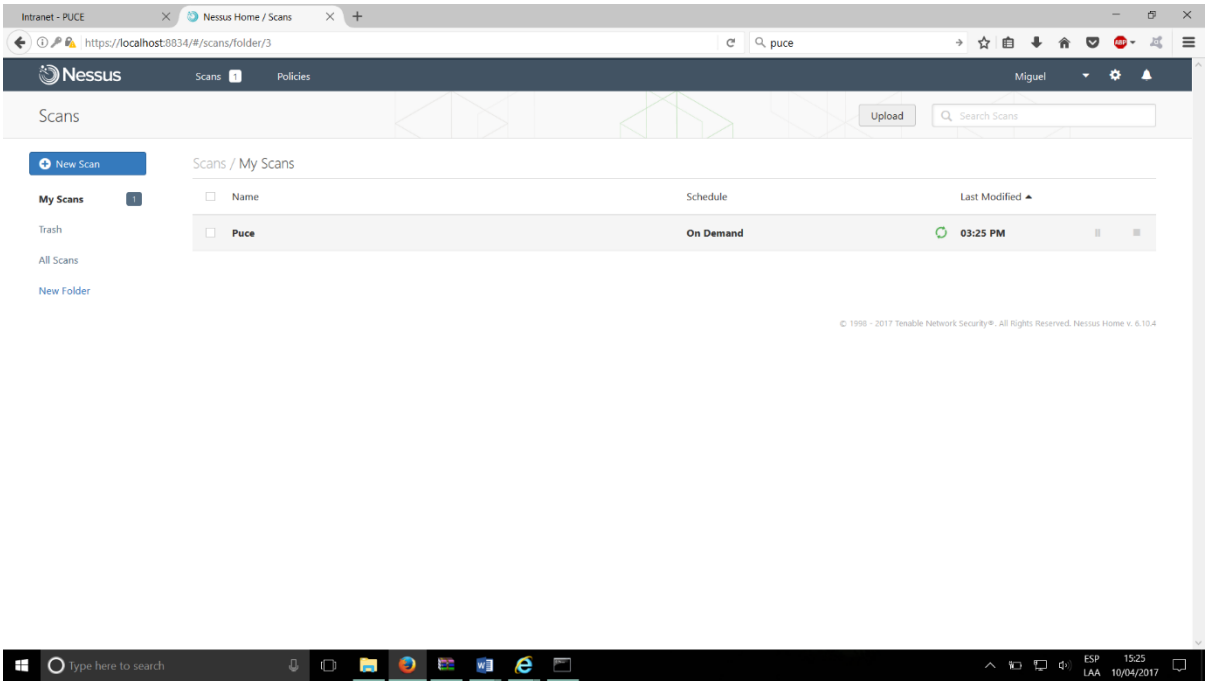
Wendlandt, D. (2008). *Nessus : A security vulnerability scanning tool*. Obtenido de Nessus : A security vulnerability scanning tool: http://www.cs.cmu.edu/~dwendlan/personal/nessus.html

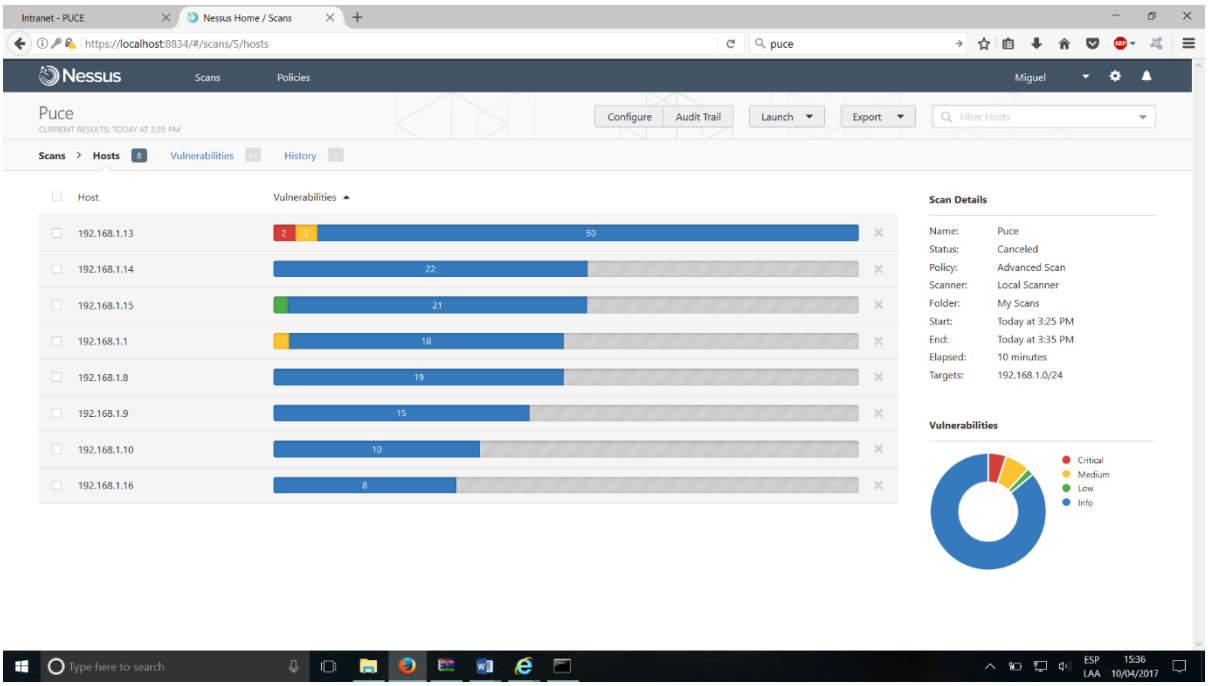
What is Network. (23 de Noviembre de 2016). *whatisnetwork*. Obtenido de whatisnetwork: http://www.whatisnetworks.com/tag/what-are-the-similarities-between-osi-and-tcpip-model/

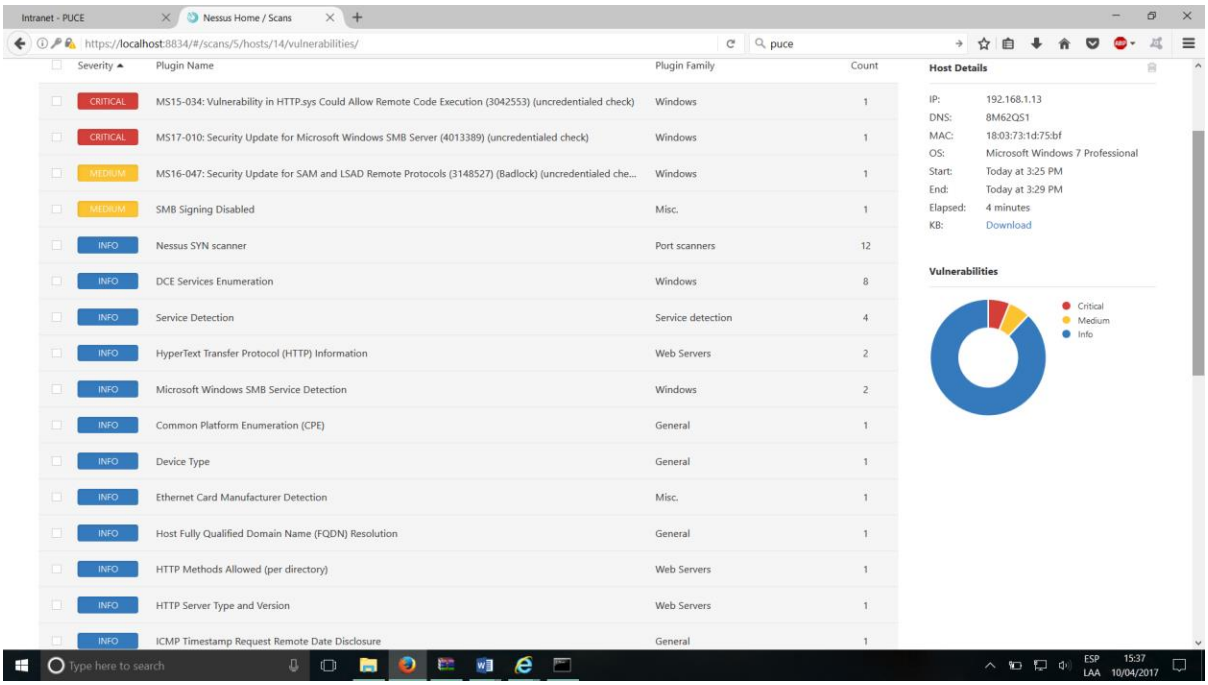
Wireshark. (2014). *Wireshark*. Obtenido de Wireshark: https://www.wireshark.org/faq.html#q1.1

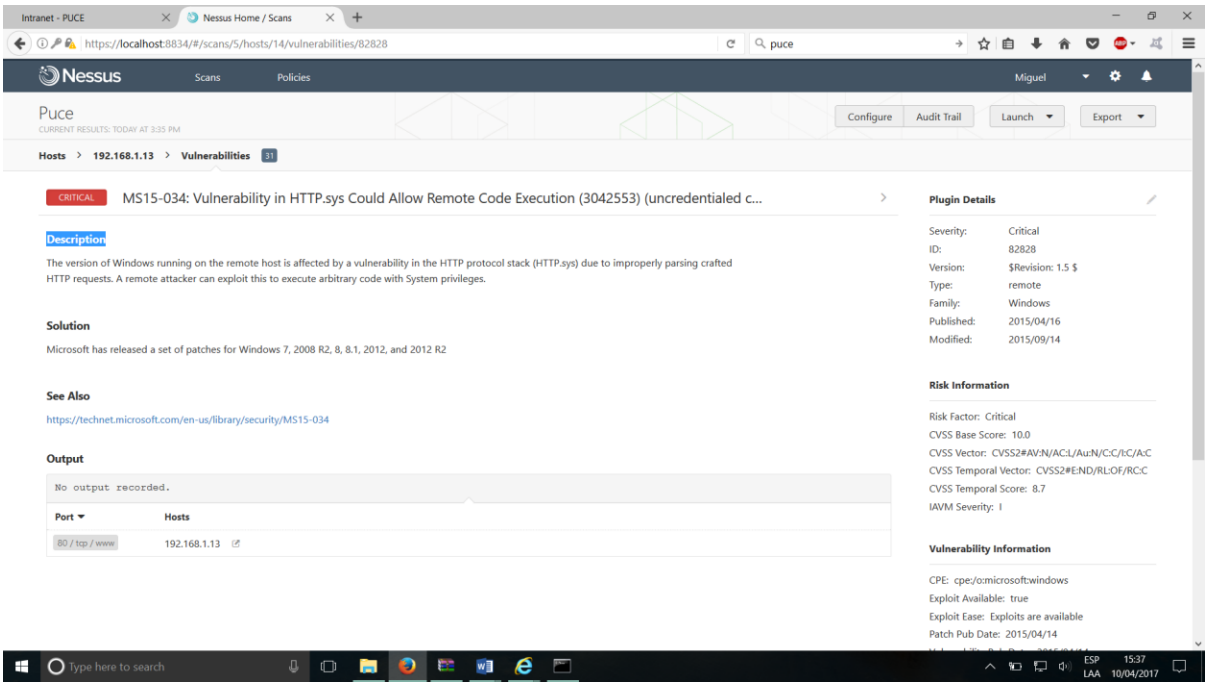
Anexos

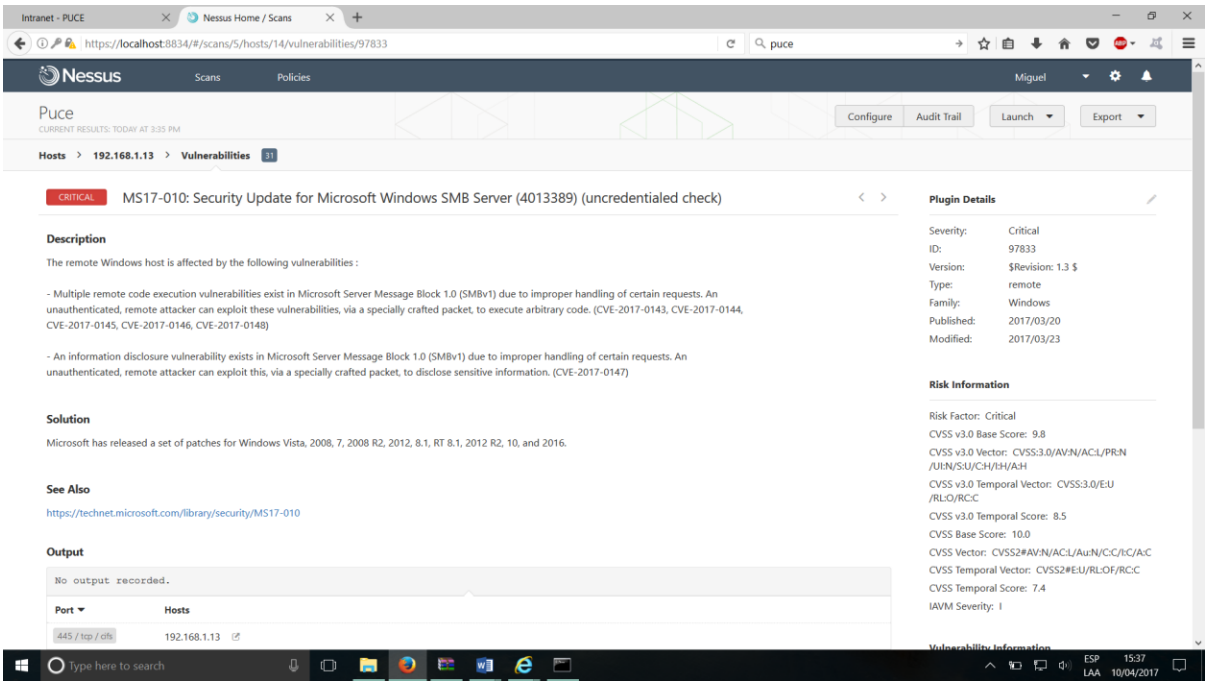
Ataques Comunes Encontrados En las Pruebas

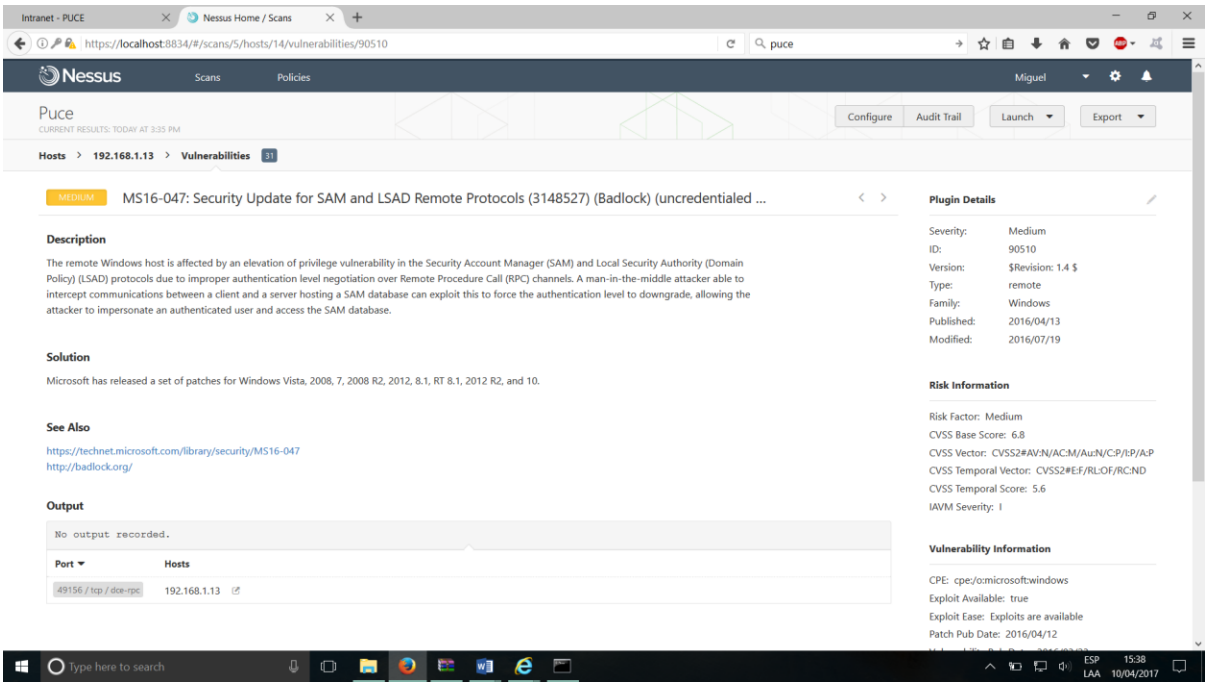


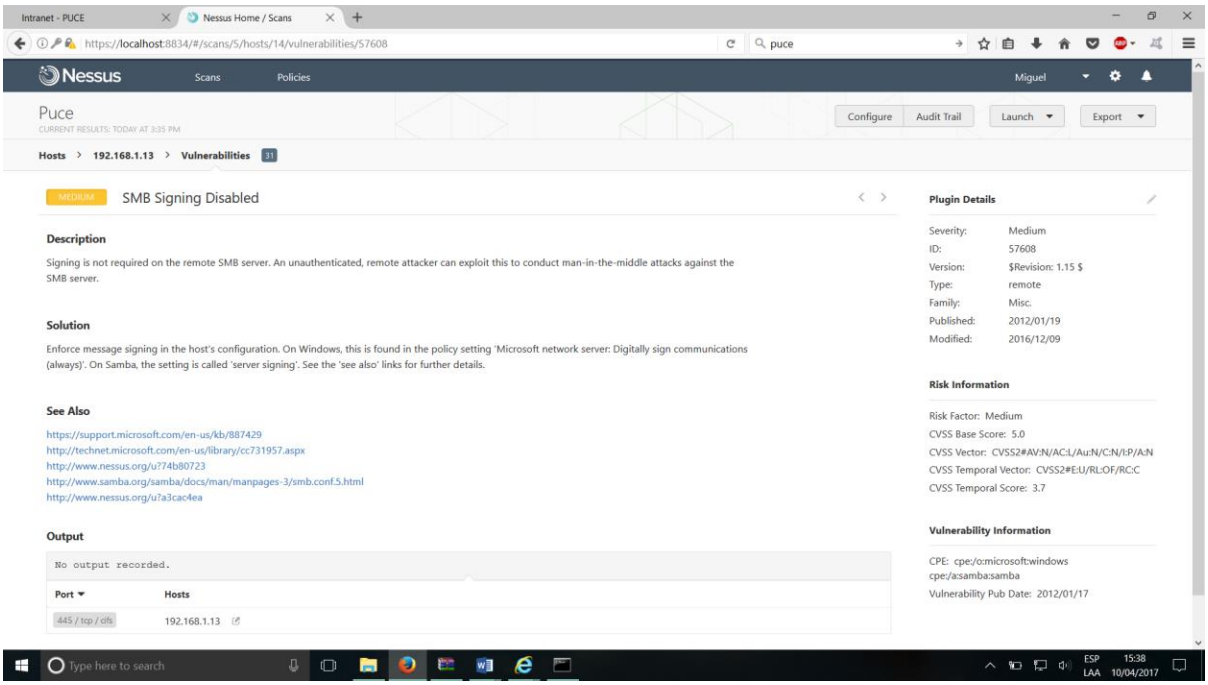


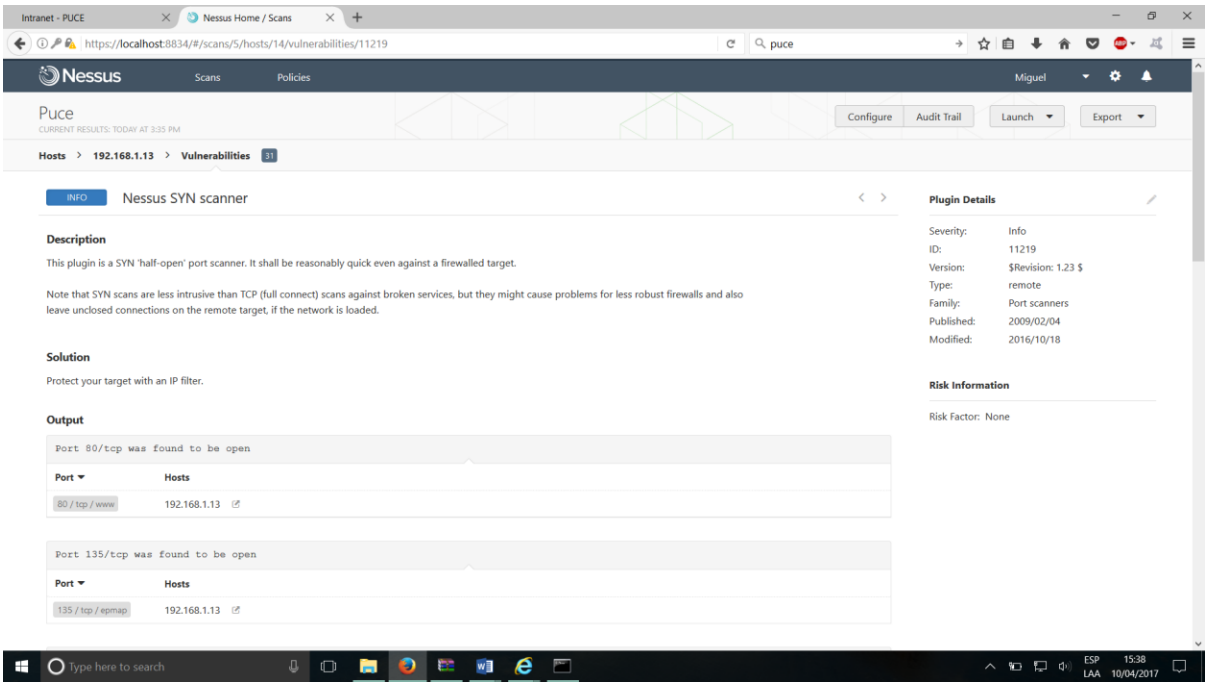

Intranet - PUCE
Nessus Home / Scans
https://localhost:8834/#/scans/5/hosts/14/vulnerabilities/
puce
Severity
Plugin Name
Plugin Family
Count
CRITICAL MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check) Windows 1
CRITICAL MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (uncredentialed check) Windows 1
MEDIUM MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed che... Windows 1
MEDIUM SMB Signing Disabled Misc. 1
INFO Nessus SYN scanner Port scanners 12
INFO DCE Services Enumeration Windows 8
INFO Service Detection Service detection 4
INFO HyperText Transfer Protocol (HTTP) Information Web Servers 2
INFO Microsoft Windows SMB Service Detection Windows 2
INFO Common Platform Enumeration (CPE) General 1
INFO Device Type General 1
INFO Ethernet Card Manufacturer Detection Misc. 1
INFO Host Fully Qualified Domain Name (FQDN) Resolution General 1
INFO HTTP Methods Allowed (per directory) Web Servers 1
INFO HTTP Server Type and Version Web Servers 1
INFO ICMP Timestamp Request Remote Date Disclosure General 1
Host Details
IP: 192.168.1.13
DNS: 8M62QS1
MAC: 18:03:73:1d:75:bf
OS: Microsoft Windows 7 Professional
Start: Today at 3:25 PM
End: Today at 3:29 PM
Elapsed: 4 minutes
KB: Download
Vulnerabilities
Critical
Medium
Info
Type here to search
ESP
LAA
15:37
10/04/2017

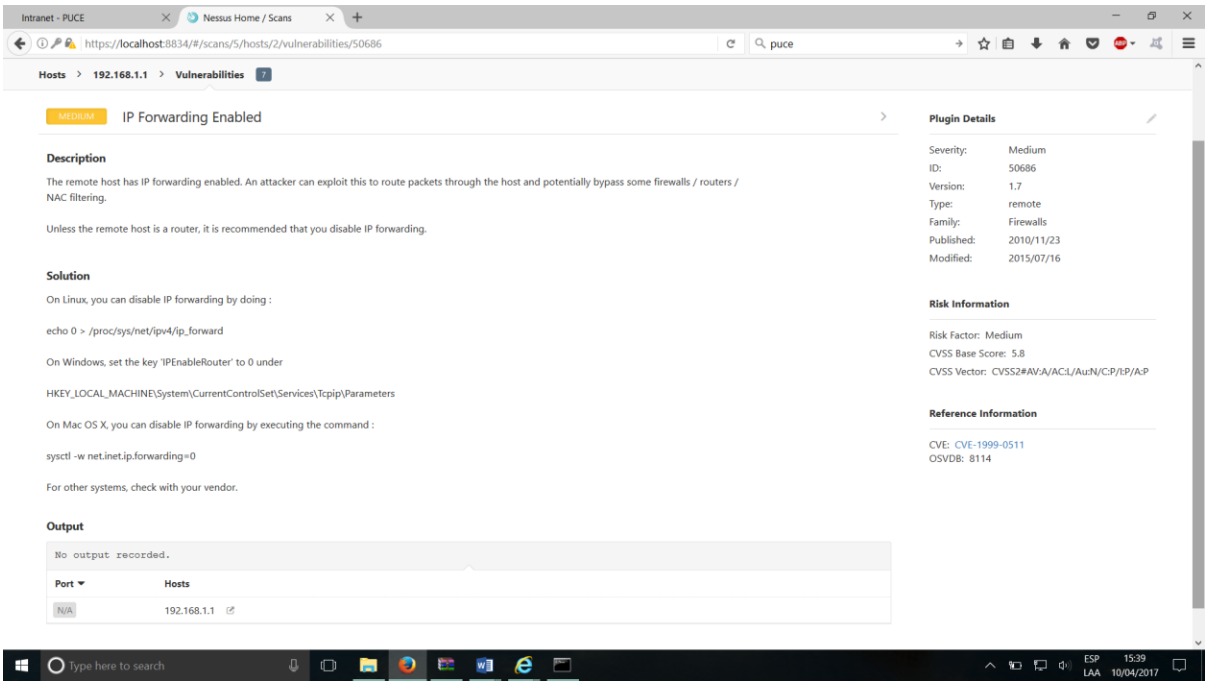

Intranet - PUCE
Nessus Home / Scans
https://localhost:8834/#/scans/5/hosts/14/vulnerabilities/82828
puce
Nessus
Scans
Policies
Miguel
Puce
CURRENT RESULTS: TODAY AT 3:35 PM
Configure
Audit Trail
Launch
Export
Hosts > 192.168.1.13 > Vulnerabilities 31
CRITICAL MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed c...
Description
The version of Windows running on the remote host is affected by a vulnerability in the HTTP protocol stack (HTTP.sys) due to improperly parsing crafted HTTP requests. A remote attacker can exploit this to execute arbitrary code with System privileges.
Solution
Microsoft has released a set of patches for Windows 7, 2008 R2, 8, 8.1, 2012, and 2012 R2
See Also
https://technet.microsoft.com/en-us/library/security/MS15-034
Output
No output recorded.
Port
Hosts
80 / tcp / www
192.168.1.13
Plugin Details
Severity: Critical
ID: 82828
Version: $Revision: 1.5 $
Type: remote
Family: Windows
Published: 2015/04/16
Modified: 2015/09/14
Risk Information
Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:ND/RL:OF/RC:C
CVSS Temporal Score: 8.7
IAVM Severity: I
Vulnerability Information
CPE: cpe:/o:microsoft:windows
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: 2015/04/14
Type here to search
ESP
LAA
15:37
10/04/2017

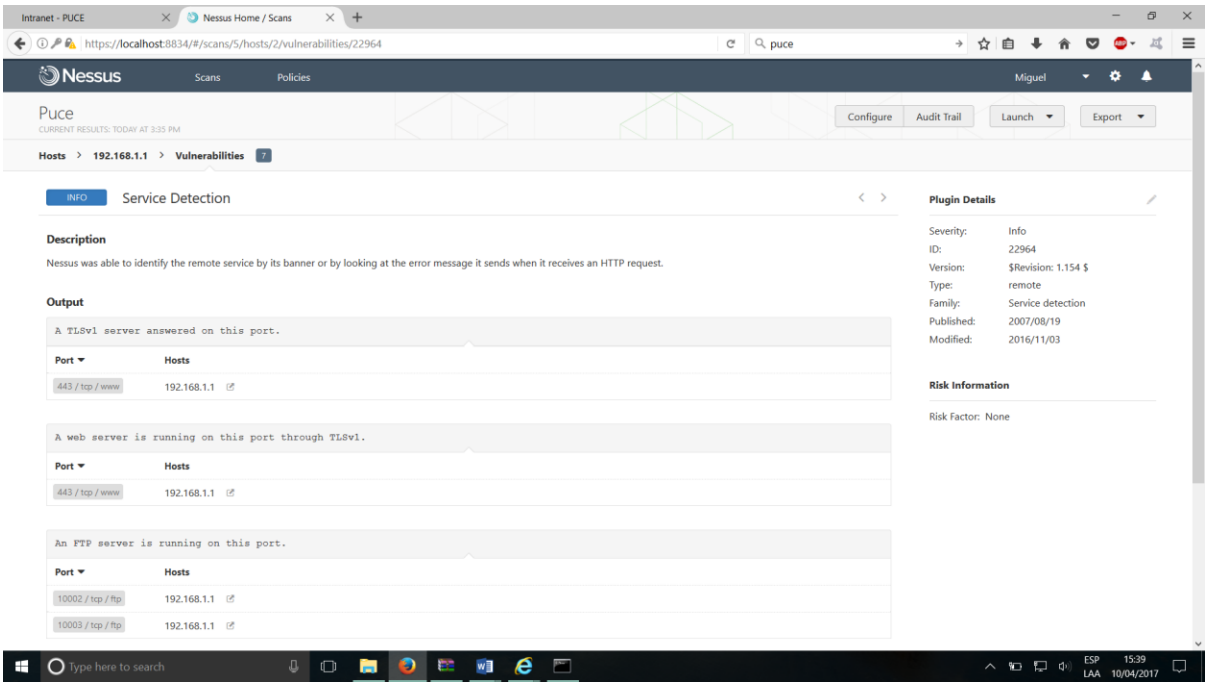

Intranet - PUCE
Nessus Home / Scans
https://localhost:8834/#/scans/5/hosts/14/vulnerabilities/97833
puce
Nessus
Scans
Policies
Miguel
Puce
CURRENT RESULTS: TODAY AT 3:35 PM
Configure
Audit Trail
Launch
Export
Hosts > 192.168.1.13 > Vulnerabilities 31
CRITICAL
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (uncredentialed check)
Description
The remote Windows host is affected by the following vulnerabilities :
- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)
Solution
Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016.
See Also
https://technet.microsoft.com/library/security/MS17-010
Output
No output recorded.
Port
Hosts
445 / tcp / cifs
192.168.1.13
Plugin Details
Severity: Critical
ID: 97833
Version: $Revision: 1.3 $
Type: remote
Family: Windows
Published: 2017/03/20
Modified: 2017/03/23
Risk Information
Risk Factor: Critical
CVSS v3.0 Base Score: 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 8.5
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C
CVSS Temporal Score: 7.4
IAVM Severity: I
Type here to search
ESP
LAA
15:37
10/04/2017

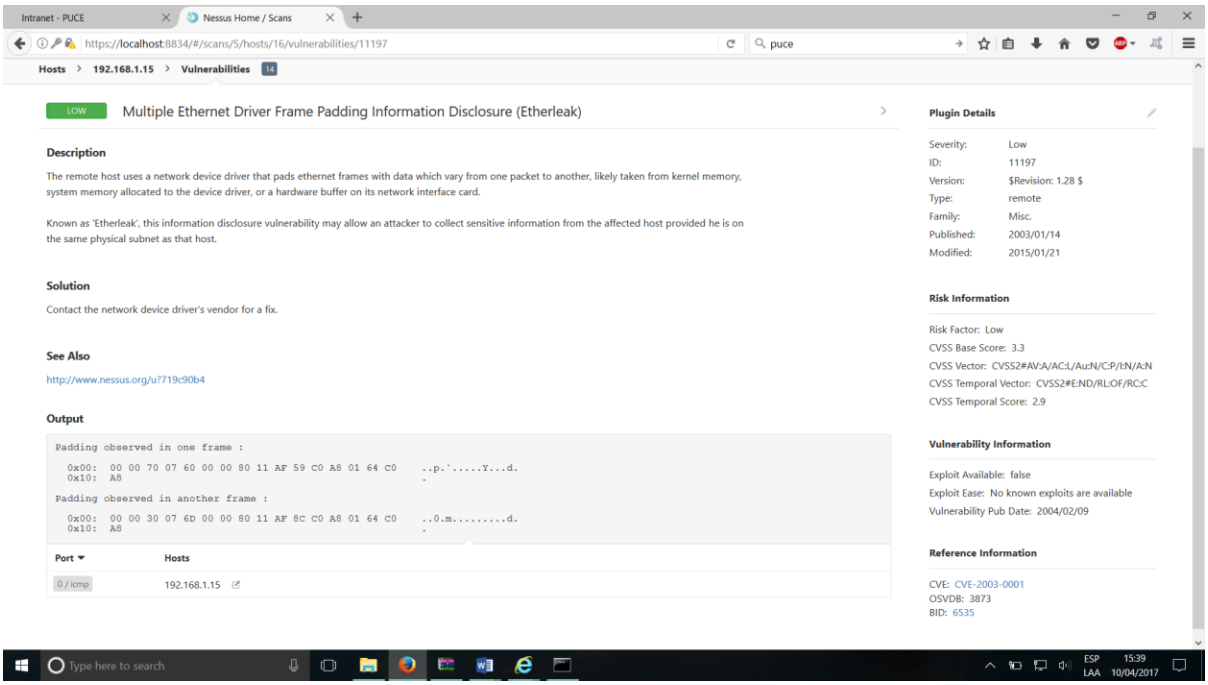

Intranet - PUCE
Nessus Home / Scans
https://localhost:8834/#/scans/5/hosts/14/vulnerabilities/90510
puce
Nessus
Scans
Policies
Miguel
Puce
CURRENT RESULTS: TODAY AT 3:35 PM
Configure
Audit Trail
Launch
Export
Hosts > 192.168.1.13 > Vulnerabilities 31
MEDIUM
MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed ...
Description
The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.
Solution
Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.
See Also
https://technet.microsoft.com/library/security/MS16-047
http://badlock.org/
Output
No output recorded.
Port
Hosts
49156 / tcp / dce-rpc
192.168.1.13
Plugin Details
Severity: Medium
ID: 90510
Version: $Revision: 1.4 $
Type: remote
Family: Windows
Published: 2016/04/13
Modified: 2016/07/19
Risk Information
Risk Factor: Medium
CVSS Base Score: 6.8
CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:ND
CVSS Temporal Score: 5.6
IAVM Severity: I
Vulnerability Information
CPE: cpe:/o:microsoft:windows
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: 2016/04/12
Type here to search
ESP
LAA
15:38
10/04/2017


Intranet - PUCE
Nessus Home / Scans
https://localhost:8834/#/scans/5/hosts/14/vulnerabilities/57608
puce
Nessus
Scans
Policies
Miguel
Puce
CURRENT RESULTS: TODAY AT 3:35 PM
Configure
Audit Trail
Launch
Export
Hosts > 192.168.1.13 > Vulnerabilities 31
MEDIUM
SMB Signing Disabled
Description
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.
Solution
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
See Also
https://support.microsoft.com/en-us/kb/887429
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea
Output
No output recorded.
Port
Hosts
445 / tcp / cifs
192.168.1.13
Plugin Details
Severity: Medium
ID: 57608
Version: $Revision: 1.15 $
Type: remote
Family: Misc.
Published: 2012/01/19
Modified: 2016/12/09
Risk Information
Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C
CVSS Temporal Score: 3.7
Vulnerability Information
CPE: cpe:/o:microsoft:windows
cpe:/a:samba:samba
Vulnerability Pub Date: 2012/01/17
Type here to search
ESP
LAA
15:38
10/04/2017


Intranet - PUCE
Nessus Home / Scans
https://localhost:8834/#/scans/5/hosts/14/vulnerabilities/11219
puce
Nessus
Scans
Policies
Miguel
Puce
CURRENT RESULTS: TODAY AT 3:35 PM
Configure
Audit Trail
Launch
Export
Hosts > 192.168.1.13 > Vulnerabilities 31
INFO
Nessus SYN scanner
Description
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.
Solution
Protect your target with an IP filter.
Output
Port 80/tcp was found to be open
Port
Hosts
80 / tcp / www
192.168.1.13
Port 135/tcp was found to be open
Port
Hosts
135 / tcp / epmap
192.168.1.13
Plugin Details
Severity: Info
ID: 11219
Version: $Revision: 1.23 $
Type: remote
Family: Port scanners
Published: 2009/02/04
Modified: 2016/10/18
Risk Information
Risk Factor: None
Type here to search
ESP
LAA
15:38
10/04/2017


Intranet - PUCE
Nessus Home / Scans
https://localhost:8834/#/scans/5/hosts/2/vulnerabilities/50686
puce
Hosts > 192.168.1.1 > Vulnerabilities 7
MEDIUM
IP Forwarding Enabled
Description
The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.
Unless the remote host is a router, it is recommended that you disable IP forwarding.
Solution
On Linux, you can disable IP forwarding by doing :
echo 0 > /proc/sys/net/ipv4/ip_forward
On Windows, set the key 'IPEnableRouter' to 0 under
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
On Mac OS X, you can disable IP forwarding by executing the command :
sysctl -w net.inet.ip.forwarding=0
For other systems, check with your vendor.
Output
No output recorded.
Port
Hosts
N/A
192.168.1.1
Plugin Details
Severity: Medium
ID: 50686
Version: 1.7
Type: remote
Family: Firewalls
Published: 2010/11/23
Modified: 2015/07/16
Risk Information
Risk Factor: Medium
CVSS Base Score: 5.8
CVSS Vector: CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P
Reference Information
CVE: CVE-1999-0511
OSVDB: 8114
Type here to search
ESP
LAA
15:39
10/04/2017


Intranet - PUCE
Nessus Home / Scans
https://localhost:8834/#/scans/5/hosts/2/vulnerabilities/22964
puce
Nessus
Scans
Policies
Miguel
Puce
CURRENT RESULTS: TODAY AT 3:35 PM
Configure
Audit Trail
Launch
Export
Hosts > 192.168.1.1 > Vulnerabilities 7
INFO
Service Detection
Description
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.
Output
A TLSv1 server answered on this port.
Port
Hosts
443 / tcp / www
192.168.1.1
A web server is running on this port through TLSv1.
Port
Hosts
443 / tcp / www
192.168.1.1
An FTP server is running on this port.
Port
Hosts
10002 / tcp / ftp
192.168.1.1
10003 / tcp / ftp
192.168.1.1
Plugin Details
Severity: Info
ID: 22964
Version: $Revision: 1.154 $
Type: remote
Family: Service detection
Published: 2007/08/19
Modified: 2016/11/03
Risk Information
Risk Factor: None
Type here to search
ESP
LAA
15:39
10/04/2017


Intranet - PUCE
Nessus Home / Scans
https://localhost:8834/#/scans/5/hosts/16/vulnerabilities/11197
puce
Hosts > 192.168.1.15 > Vulnerabilities 14
LOW
Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)
Description
The remote host uses a network device driver that pads ethernet frames with data which vary from one packet to another, likely taken from kernel memory, system memory allocated to the device driver, or a hardware buffer on its network interface card.
Known as 'Etherleak', this information disclosure vulnerability may allow an attacker to collect sensitive information from the affected host provided he is on the same physical subnet as that host.
Solution
Contact the network device driver's vendor for a fix.
See Also
http://www.nessus.org/u?719c90b4
Output
Padding observed in one frame :
0x00: 00 00 70 07 60 00 00 80 11 AF 59 C0 A8 01 64 C0 ..p.`.....Y...d.
0x10: A8 .
Padding observed in another frame :
0x00: 00 00 30 07 6D 00 00 80 11 AF 8C C0 A8 01 64 C0 ..0.m.........d.
0x10: A8 .
Port
Hosts
0 / icmp
192.168.1.15
Plugin Details
Severity: Low
ID: 11197
Version: $Revision: 1.28 $
Type: remote
Family: Misc.
Published: 2003/01/14
Modified: 2015/01/21
Risk Information
Risk Factor: Low
CVSS Base Score: 3.3
CVSS Vector: CVSS2#AV:A/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Vector: CVSS2#E:ND/RL:OF/RC:C
CVSS Temporal Score: 2.9
Vulnerability Information
Exploit Available: false
Exploit Ease: No known exploits are available
Vulnerability Pub Date: 2004/02/09
Reference Information
CVE: CVE-2003-0001
OSVDB: 3873
BID: 6535
Type here to search
ESP
LAA
15:39
10/04/2017