DEPARTAMENTO DE INVESTIGACIÓN Y POSGRADOS

TEMA:

"APLICACIÓN DE HERRAMIENTAS HONEYPOT PARA LA DETECCIÓN Y CORRECCIÓN DE VULNERABILIDADES DE SEGURIDAD DE LA RED INFORMÁTICA DEL HOSPITAL MUNICIPAL NUESTRA SEÑORA DE LA MERCED EN EL PERÍODO 2013"

Tesis de grado previo a la obtención del título de

Magister en Gerencia Informática

Línea de Investigación:

Seguridad de redes

Autor:

Diego Fabián Rubio Lana

Director:

Ing. Mg. Javier Wilfrido Cóndor Cruz

Ambato - Ecuador

Abril 2014

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

TEMA:

"APLICACIÓN DE HERRAMIENTAS HONEYPOT PARA LA DETECCIÓN Y CORRECCIÓN DE VULNERABILIDADES DE SEGURIDAD DE LA RED INFORMÁTICA DEL HOSPITAL MUNICIPAL NUESTRA SEÑORA DE LA MERCED EN EL PERÍODO 2013"

Línea de Investigación:

Seguridad de redes

Autor:

Diego Fabián Rubio Lana

Javier Wilfrido Cóndor Cruz, Ing. Mg. f. _____
CALIFICADOR

López Andrade Andrés Rubén, Ing. Mg. f. _____
CALIFICADOR

Jaime Bolívar Ruiz Banda, Ing. Mg f. _____
CALIFICADOR

Juan Ricardo Mayorga Zambrano, PhD f. _____
DIRECTOR DEL DEPARTAMENTO
DE INVESTIGACION Y POSGRADOS

Hugo Rogelio Altamirano Villarroel, Dr. f. _____
SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Abril 2014

DECLARACION DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, Diego Fabián Rubio Lana, portador de la cédula de ciudadanía N° 1802942597 declaro que los resultados obtenidos en la investigación que presento como informe final, previo a la obtención del título de Magister en Gerencia Informática son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola y exclusiva responsabilidad legal y académica

_____

Diego Fabián Rubio Lana

C.I. 1802942597

AGRADECIMIENTO

Mi agradecimiento a mis padres, que han guiado mi vida con amor, paciencia, honestidad y ejemplo de trabajo.

A mi hermano por estar siempre dispuesto a extenderme la mano en los momentos difíciles de la vida.

A esa persona especial en mi vida JR, que me acompaña en los momentos buenos y malos y me brinda su apoyo.

Al Hospital municipal Nuestra Señora de la Merced, por brindarme las facilidades necesarias para el desarrollo de este trabajo tan importante para la seguridad e integridad de su información.

A todos mis familiares y amigos que de alguna manera colaboraron con el desarrollo de esta investigación.

A la Pontificia Universidad Católica del Ecuador por ser una fuente de nuevas oportunidades para la transferencia del conocimiento.

DEDICATORIA

A mi padre, quien ha sido la guía de mi vida, ejemplo de honestidad y trabajo

A mi madre, la persona que más quiero en esta vida, quien a la distancia me da las fuerzas necesarias para alcanzar la superación personal.

RESUMEN

El uso de las Nuevas Tecnologías Informáticas se ha incrementado de manera exponencial durante la última década, lo que ha incidido directamente en la generación de gran cantidad de información por parte de las empresas, llegando a ser considerada como uno de los activos más importantes en la actualidad. La conectividad de redes a gran escala, producida por el desarrollo del Internet y las nuevas tecnologías de comunicación, ha incrementado en gran nivel las amenazas que pueden afectar a los activos de información de las empresas que están expuestos. Actualmente existe la necesidad de proteger la información de las empresas de los ataques provenientes de personas u organizaciones que al margen de la ley intentan dañar u obtener su preciada información mediante la utilización de técnicas y herramientas informáticas que han evolucionado tanto en su eficiencia como en la capacidad de mantenerse ocultas dentro de las redes de datos. La tecnología Honeypot, ofrece a los administradores de red las herramientas necesarias para alertar y conocer de manera oportuna los ataques producidos y las técnicas utilizadas, las mismas que serán analizadas para implementar las medidas de seguridad necesarias y evitar futuros ataques.

ABSTRACT

The use of new information technologies has increased exponentially in the last decade, which has led directly to the generation of a great quantity of information from companies, and is being considered as one of the most important assets at present time. The large-scale connectivity of networks which was produced by the development of the Internet and new communication technologies has greatly increased the threats that can affect the company´s information assets are exposed to. Nowadays there is the need to protect the information of companies from attacks coming from people or organizations which illegally try to damage or obtain its precious information through the use of techniques and computer tools that have evolved as much in its efficiency as in the capacity to stay hidden within the data networks. The Honeypot technology offers network administrators the necessary tools to alert and know the attacks that were produced and the techniques that were used in a timely manner. These will be analyzed in order to implement the necessary security measures and avoid future attacks.

TABLA DE CONTENIDOS

TABLA DE GRAFICOS

GRÁFICOS

TABLAS

CAPITULO I

PROYECTO DE INVESTIGACION

1.1 Antecedentes

El Hospital Municipal Nuestra Señora de la Merced de ahora en adelante denominado El Hospital, cuenta con una Red de Datos a través de la cual se brinda diferentes servicios.

Actualmente la Red de Datos del Hospital, se encuentra interconectada a diferentes redes externas como la Red Informática del Gobierno Autónomo Descentralizado Municipalidad de Ambato con el fin de consumir determinados servicios de datos y al Internet mediante de varios de enlaces de fibra óptica, y ADSL.

La red informática del Hospital no cuenta con un sistema de detección de intrusos, estando expuesta a amenazas externas que afecten la integridad, disponibilidad y confidencialidad de la información.

1.2 Significado del Problema

El Hospital Municipal Nuestra Señora de la Merced, se encuentra inmerso en un proceso de renovación tecnológica, siendo uno de los puntos importantes en esta evolución la digitalización de la información generada en todos los procesos administrativos y productivos, por lo que se debe detectar y corregir las vulnerabilidades físicas y lógicas de la plataforma tecnológica sobre la cual se ejecutan los sistemas informáticos de la institución.

1.3 Definición del problema

No existe un Sistema de Detección de Intrusos en la Red de Datos del Hospital Municipal Nuestra Señora de la Merced que permita detectar ataques, intromisiones y vulnerabilidad externos e internos.

1.3.1 Preguntas Básicas

¿Cómo aparece el problema que se pretende solucionar?

- No existe un análisis de vulnerabilidades de la Red de datos del Hospital municipal Nuestra Señora de la Merced.
- Red de datos conectada al internet.
- Caídas del sistema de sin razón técnica aparente.

¿Por qué se origina?

- Inadecuado control de acceso a la red
- No existe un sistema de detección de intrusos
- Poca capacitación a nivel de usuario sobre las políticas de seguridad informática.

¿Quién o qué lo origina?

- Despreocupación de autoridades por aplicar políticas de seguridad informática.
- Falta de implementación de un sistema de detección de intrusos a nivel de red.
- Malas prácticas de seguridad a nivel de usuarios de los sistemas informáticos

¿Cuándo se origina?

- Cuando no existe una determinación de las vulnerabilidades actuales de la red informática.
- Cuando no se utiliza las tecnologías existentes para la detección de intrusos en la red informática

¿Dónde se origina?

- En las Red de Datos del Hospital Municipal Nuestra Señora de la Merced

¿Qué elementos o circunstancias lo originan?

- Poco control de seguridad sobre la red informática.
- Accesibilidad a la red informática desde el Internet.
- Malas prácticas de seguridad por parte de los usuarios.

1.4 Planteamiento del Tema

Aplicación de herramientas honeypot para la detección y corrección de vulnerabilidades de seguridad de la red informática del Hospital Municipal Nuestra Señora de la Merced en el período 2013

1.5 Delimitación del Problema

La aplicación de herramientas honeypot se la realizará en la red informática del edificio del Hospital Municipal Nuestra Señora de la Merced.

1.5.1 Delimitación Espacial

País: Ecuador

Provincia: Tungurahua

Ciudad: Ambato

Espacio: Hospital Municipal Nuestra Señora de la Merced

Área: Seguridad Informática

Unidad Experimental: Red de datos

1.5.2 Delimitación Temporal

Período: 2013

1.6 Justificación

El desarrollo del presente proyecto es importante ya que no se conoce las vulnerabilidades de la Red de Datos del Hospital, lo cual la convierte en potencial objetivo de ataques de tipo informático.

A nivel de la ciudad de Ambato, es un proyecto necesario, por cuanto no se tiene un conocimiento documentado del tipo de ataques, intromisiones y vulnerabilidades reales dentro de una red informática institucional pública, tomando en cuenta además que nunca antes se ha realizado este tipo de investigación dentro del Hospital Municipal, siendo de vital importancia para mantener la seguridad, confiabilidad. disponibilidad y confidencialidad de la información institucional.

Desde el punto de vista económico, el presente trabajo se justifica ya que la detección y corrección de las vulnerabilidades de la plataforma informática evitará el robo o adulteración de los datos institucionales y por consiguiente los posibles costos que devengan en la recuperación o reparación de la información comprometida.

La elaboración de un documento con normas básicas de seguridad informática para los usuarios finales de sistemas informáticos permitirá dar a conocer a todo el personal involucrado cuales son las mejores prácticas de seguridad y así elevar la confiabilidad de los niveles de protección de la información generada por éstos sistemas.

1.7 Objetivos

1.7.1 Objetivo General

Aplicar herramientas Honeypot para la detección, análisis y corrección de las vulnerabilidades de la Red del Hospital Municipal Nuestra Señora de la Merced.

1.7.2 Objetivos Específicos

Implementar la tecnología Honeypot para la detección de vulnerabilidades de la red de datos del Hospital.

Estudiar los diferentes tipos de ataques a una red de datos.

Analizar las vulnerabilidades detectadas en la red de Datos de la Institución.

Crear una guía para la corrección de las vulnerabilidades detectadas en la red de datos del Hospital Municipal Nuestra Señora de la Merced.

Elaborar un instructivo de seguridad para prevenir futuros ataques y así mejorar los niveles de seguridad de la red de datos del Hospital Municipal Nuestra Señora de la Merced.

1.8 Hipótesis

Con la aplicación de herramientas Honeypot para la detección y análisis en la Red del Hospital Municipal Nuestra Señora de la Merced, se implementará un plan de correcciones y políticas de seguridad, lo cual mejorará los niveles de seguridad Informática, simulando objetivos informáticos con bajos niveles de seguridad.

1.9 Variables

1.9.1 Variable Independiente

Herramientas Honeypot

1.9.2 Variable Dependiente

Seguridad Informática

CAPITULO II

MARCO TEORICO

2.1 Antecedentes

Una sociedad basada en el conocimiento exige la utilización de nuevas herramientas y tecnologías que tengan un mayor impacto en la generación, administración, transferencia y aplicación de la información que se genera a partir del conocimiento para la toma de decisiones, la innovación y la competitividad.

En la actualidad el mundo ha evidenciado el impresionante desarrollo de la tecnología, en especial la referente a la creación de información, su procesamiento y transporte, lo cual ha sido beneficioso para la vida de las personas.

Actualmente la comunicación es instantánea entre personas o equipos electrónicos sin importar su ubicación geográfica, siendo necesario únicamente un medio de transporte de información.

El gran avance de las tecnologías de comunicación y procesamiento de datos trae consigo grandes beneficios para sus usuarios así como desventajas producidas por el robo de información, daños o ataques a infraestructuras de comunicación que soportan los sistemas informáticos que hoy en día son vitales para el normal desenvolvimiento de las actividades humanas, en este sentido actualmente se utiliza un conjunto de elementos, herramientas y servicios orientados al tratamiento, procesamiento y administración de datos e información de una manera organizada disponibles para su consumo y creado para satisfacer una necesidad o requerimiento.

Estos elementos, herramientas o servicios forman parte de algunas de las siguientes categorías:

- Personas
- Datos (Información)
- Actividades (Procesos)
- Recursos (equipo informáticos, de comunicación, servicios).

Debido a la gran cantidad de datos que actualmente se genera en los diferentes sistemas informáticos es necesario aplicar procesos de seguridad informática, con el fin de resguardar y proteger la información a fin de mantener su confidencialidad, integridad y disponibilidad, mediante la aplicación de medios tecnológicos, y políticas diseñadas para el efecto

La seguridad de la información durante todas las etapas de generación, transporte, procesamiento y almacenamiento juega un papel relevante en la infraestructura tecnológica, teniendo igual o mayor importancia que la seguridad física ya que aparte de proteger el Hardware de daños físicos o desaparición, se debe eliminar los riesgos de robo y pérdidas de información de todo tipo desde datos personales, información financiera y bancaria, académica, telecomunicaciones hasta información sensible de seguridad nacional.

Al hablar de Seguridad de la Información se debe tomar en cuenta los siguientes términos:

Amenaza.- Es la probabilidad de ocurrencia de un evento potencialmente desastroso, asociado a un evento físico de origen natural, socio - natural o provocado por los seres humanos, durante cierto período de tiempo (wordpess.com, 2009) que pueda producir un daño físico o virtual sobre los elementos de un sistema de información.

Vulnerabilidad.- Es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño. (wordpess.com, 2009)

Riesgo.- Es la materialización de las vulnerabilidades detectadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el grado de impacto negativo que ocasione a las operaciones de la organización.

Seguridad.- Consiste en asegurar que los recursos de los Sistemas de Información de una organización sean utilizados de la manera planificada.

Por lo tanto la seguridad es una característica de cualquier sistema (informático o no) que nos indica que ese sistema esté libre de peligro, daño o riesgo (Withman, 2012).

Una correcta gestión de la Seguridad de la Información debe establecer programas, controles y políticas que tengan como fin mantener la confidencialidad, Integridad y Disponibilidad de la Información de manera conjunta.

Confidencialidad.- La información de una organización solo puede ser accedida por personas u organizaciones que cuentan con la debida autorización.

Integridad.- Es la característica que busca mantener la información libre de alteraciones o modificaciones no autorizadas, es decir mantener con exactitud la información tal cual fue creada o generada, sin ser objeto de manipulación o alteración por personas o procesos no autorizados.

Disponibilidad.- Es la característica o condición de la información de mantenerse disponible para las personas, servicios u organizaciones autorizadas a acceder a la misma al momento que así lo requieran.

2.2 Hacking Ético

Dentro de la filosofía, la ética se define como la disciplina que se encarga del estudio de la moral, la virtud, el deber, la felicidad y el buen vivir dentro de los parámetros que la sociedad considera moralmente aceptados (Singer, 1994).

Por otro lado definamos al termino Hacking como la búsqueda permanente de información y conocimientos relacionados al área informática, sus mecanismos de seguridad, vulnerabilidades, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellas personas que saben hacerlo.

En términos generales los término Hacking y Ético parecerían ser antagonistas, ya que por un lado, la palabra Hacking para el común de la población está fuertemente relacionado a delincuentes comunes, personas de dudosa moral que utilizan sus conocimientos informáticos para delinquir y por otro lado la palabra ético se refiere a lo que moralmente se considera correcto.

La ética implica que el trabajo y la intervención del profesional en seguridad informática o Hacker Ético no comprometen de ningún modo los activos de la organización que son los valiosos datos con los que ella cuenta (Tori, 2008).

Es por esto que la demostración de técnicas de penetración a los diferentes sistemas deben ser realizados con mucho cuidado para no ser catalogados como intentos de intrusión en sistemas de otras organizaciones diferentes a las que estemos examinando como una tarea legítima propia de expertos informáticos con el único fin de poder estar prevenidos ante ataque de intrusos que carecen de moral en sus actos.

Existen dos tipos de Hacker éticos: los independientes y los profesionales de consultoría.

Un Hacker ético de consultoría está dedicado a prestar sus servicios de seguridad informática a empresas que así lo requieran, todo esto bajo la tutela

de un contrato remunerado, es decir realiza pruebas de hacking ético con fines de lucro y en ambientes controlados.

En todo caso la principal tarea de un hacker ético es evidencias y reportar las fallas de seguridad en las redes organizativas, para que el personal encargado de su administración tome las acciones necesarias para corregir dichas fallas y así poder minimizar el riesgo inherente a ellas.

2.2.1 Ataques Informáticos

Existen diferentes tipos de ataque informático, los mismos que dependiendo del lugar de origen pueden ser ataque internos o externos; los ataque internos son los que se originan dentro de la propia red y los ataque externos son los que se originan fuera del perímetro de seguridad de la Red.

Los ataques informáticos también deben catalogarse de acuerdo a su intencionalidad en ataques activos y ataques pasivos.

Ataques pasivos son aquellos en los que se afecta la confidencialidad de la información, sin afectar su integridad ni disponibilidad, es decir la información solo es observada por el atacante principalmente con la finalidad de conocer la infraestructura tecnológica, descubrir vulnerabilidades, todo esto sin afectar los recursos de la red.

Son considerados ataques activos aquellos que tienen fines dolosos, dañar u apropiarse de la información comprometida, afectar el desempeño de la infraestructura o finalmente paralizar servicios.

Entre los principales ataques activos tenemos:

Spoofing.- Este término hace referencia al uso de técnicas para suplantar la identidad generalmente con fines maliciosos o de investigación.

De acuerdo a la tecnología utilizada, los ataques Spoofing se los puede clasificar de la siguiente manera:

IP spoofing.- Consiste en sustituir la dirección IP ORIGEN de un paquete TCP/IP otra dirección IP a la cual se desea suplantar.

ARP Spoofing (ARP poisoning).- Consiste en la falsificación de tablas ARP mediante la construcción de tramas solicitud y respuesta ARP modificadas con el objetivo de falsear la tabla ARP de una víctima y forzarla a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo.

DNS Spoofing (DNS cache poisoning).- Consiste en la provisión de manera maliciosa de datos de Servidor de Nombres de Dominio que no se originan de fuentes autoritativas de DNS. Este ataque se lo utiliza para reemplazar arbitrariamente el contenido de una serie de victimas con contenido elegido por el atacante.

WEB Spoofing.- Es la suplantación de un sitio web real. Encamina la conexión de una víctima a través de una página falsa hacia otros sitios WEB con el objetivo de apropiarse de información.

La página web falsa actúa a modo de proxy solicitando la información requerida por la víctima a cada servidor original y evadiendo protecciones SSL, pudiendo modificar cualquier información desde y hacia cualquier servidor que la víctima visite. Se debe diferenciar el Web Spoofing del Phishing.

Ataques de Denegación de Servicio (DoS).- Este tipo de ataque consiste en dejar inhabilitado uno o varios servicios de una red por un tiempo determinado mediante la utilización de diferentes técnicas entre las que se destacan:

- Inundación SYN (SYN FLOOD)
- Inundación ICMP (ICMP FLOOD)
- Inundación UDP (UDP FLOOD)

2.3 Pruebas de penetración de sistemas

En la actualidad las organizaciones deben tener muy en cuenta la evaluación a los sistemas de seguridad de sus sistemas informáticos, de ahí se obtendrá cual es su nivel de seguridad.

Para determinar el nivel de seguridad de una infraestructura informática se debe recurrir a lo que en tecnología se denomina “Penetration Test” o Pruebas de Penetración que consisten en acciones ofensivas contra los mecanismos de defensa existentes en la infraestructura que se está analizando.

Estas pruebas evalúan la seguridad desde el análisis de los dispositivos físicos y digitales (hardware y Software) hasta el análisis del factor humano utilizando lo que se denomina ingeniería social.

El objetivo principal de este tipo de pruebas es verificar bajo situaciones extremas, de qué manera se comportan los mecanismos de defensa instalados, buscando sus vulnerabilidades y la ausencia de controles que generan brechas de seguridad entre la información crítica y las medidas de control existentes.

Una prueba de penetración comprende varias etapas en cada una de las cuales se realizan actividades en distintos ámbitos y entornos las mismas que se describen a continuación (gdp.sip.ucm, 2010)

2.3.1 Reconocimiento pasivo (Footprinting)

Es el análisis del perfil de seguridad de una organización, el cual se lo hace de manera metodológica buscando información crítica en base a un hallazgo anterior. No existe una sola metodología para efectuar el footprinting, ya que cada persona deberá escoger los caminos necesarios para llegar a la información. Se debe considerar a esta actividad como esencial debido a que toda la información crítica debe ser recolectada para que el analista o hacker pueda decidir las mejores acciones a tomar.

Se debe ser metódico y organizado al momento de realizar este reconocimiento ya que la información recolectada puede pertenecer a diferentes capas de la red tales como direcciones IP, Puertos, Servicios de red, Aplicativos, Usuarios, Sistemas de detección de Intrusos, direcciones de correo la topología de la red, etc.

Se deberá tener los argumentos necesarios para que, en base a la información obtenida determinar la manera como se va a realizar el ataque.

Es importante señalar que mucha de la información disponible de las posibles víctimas se las puede encontrar en el Internet ya que en muchos de los casos las organizaciones exponen demasiada información crítica de sus sistemas de manera involuntaria, a esta búsqueda se la denomina on-line. La búsqueda off-line se refiere a toda la información que puede ser obtenida mediante el recurso de la ingeniería social

2.3.2 Escaneo (Scanning)

En esta fase el atacante reúne toda la información posible de la víctima mediante el inventario de los equipos de la red, los puertos abiertos y los servicios disponibles mediante la utilización de alguna herramienta de escaneo de puertos. Precisamente el escaneo de puertos es una de las actividades básicas utilizadas por los atacantes. Con el conocimiento de los puertos abiertos de un equipo, se detectan las posibles vulnerabilidades las mismas que en fases posteriores podrán ser explotadas.

La fase de escaneo se la puede subdividir en las siguientes etapas:

- Detección de Sistemas Vivos o Activos
- Escaneo de Puertos
- Detección de Sistemas Operativos
- Identificación de Servicios
- Escaneo de Vulnerabilidades
- Planificación del Ataque.

2.3.3 Enumeración e identificación de vulnerabilidades

Las vulnerabilidades son debilidad en el diseño, configuración o implementación de un sistema informático que puede ser explotada con la materialización de una o varias amenazas existentes, que puede provocar un evento que comprometa la seguridad del mismo.

Las vulnerabilidades describen las debilidades y los métodos más frecuentes que se utilizan para efectuar ataques a los dispositivos de seguridad de una plataforma tecnológica.

Una organización deberá establecer prioridades en los niveles de seguridad para la información que necesita proteger, de acuerdo al valor que representan en su operación y de esta forma prevenir ataques detectando cada una de sus vulnerabilidades.

2.3.4 Ganar acceso

Es la Fase en la cual el Hacker logra penetrar a un sistema informático explotando las vulnerabilidades encontradas y enumeradas en fases anteriores

2.3.5 Mantener el acceso

En esta etapa de un ataque informático, el hacker blackhat o hacker malintencionado, intentará por cualquier medio mantener el acceso logrado al sistema comprometido.

En esta etapa se utilizan varias herramientas que garanticen accesos futuros y en muchas de las ocasiones también proteger su logro del ataque de otros hackers mediante la implementación de puertas traseras o backdoors. (gdp.sip.ucm, 2010).

El objetivo de esta etapa de un ataque es el de mantener los privilegios ya ganados y que para la próxima intrusión no se tenga que empezar de cero. Al instalar o configurar una puerta trasera, se debe tener el cuidado de “hacer el menor ruido posible” para evitar ser detectado por los administradores de sistemas, quienes al detectar la presencia de intrusos activarán sus planes de contingencia para contrarrestar el ataque.

2.3.6 Borrado de huellas

El objetivo de esta etapa de una prueba de penetración es el de cubrir todas las huellas dejadas del ataque en el sistema comprometido con la finalidad de no ser descubierto y poder comprometer acceder al sistema en el futuro.

Un ataque debe ser lo más silencioso posible, para evitar activar alarmas en los sistemas atacados, de la misma manera se debe minimizar los posibles rastros del ataque, ya que un administrador de sistemas experimentado y meticuloso podría determinar el como cuando y desde donde fue comprometido sus sistema.

2.4 Honeypots

Se debe entender como tecnología Honeypot al software o conjunto de software y hardware que tienen como objetivo atraer la atención de atacantes, simulando ser sistemas con debilidades y vulnerabilidades frente a intrusiones externas.

Actualmente la tecnología ha sufrido un gran desarrollo principalmente debido a la necesidad de implementar sistemas de seguridad informática.

El término Honeypot hace referencia a “un tarro de miel” que en la naturaleza atrae a los insectos, haciendo una analogía en el mundo tecnológico, este “tarro de miel” atrae mediante señuelos al hacker que descubren estos sitios y sus vulnerabilidades.

Un honeypot es considerado como una herramienta de seguridad informática, por cuanto se lo utiliza para almacenar la información de los ataques recibidos y las técnicas empleadas.

2.4.1 Clasificación de los Honeypots

Los honeypots se pueden clasificar por su nivel de iteracción y por su ambiente de implementación (cybsec.com, 2010).

Por el nivel de iteracción se los denominan Honeypots de baja iteracción y Honeypots de alta Iteracción.

Se denomina Honeypots de baja iteracción a aquellos cuyo trabajo se basa en la emulación de servicios, sobre sistemas operativos no existentes, los cuales son utilizados como medida de seguridad ya que se puede crear servidores falsos que simulan ser reales tales como un servidor FTP completo o un servidor web. La principal desventaja de este tipo de Honeypots es su limitación en la cantidad de información que puede ser obtenida ya que al no ofrecer una alta iteración con el atacante, éste último ve limitado sus opciones de ataque.

Los Honeypots de alta iteracción son sistemas reales no emulados, montados sobre una infraestructura física real hardware y software por consiguiente su complejidad es mayor al momento de su implementación y mantenimiento además de que suponen un mayor riesgo en su uso.

Por ejemplo un servicio web estará implementado en un servidor real sobre una plataforma adecuada el cual estaría en línea sobre un segmento de red conjuntamente con otros sistemas, por lo que un posible atacante interactuaría sobre un sistema real y del cual se podría obtener una gran cantidad de información de acuerdo a lo que el honeypot lo permita.

En un sistema honeypot de alta iteracción es necesario implementar controles más seguros y eficaces para evitar que los ataques que se intentan provocar y estudiar se conviertan en ataques reales.

Entre los honeypots de alta iteracción tenemos las denominadas Honeynets.

Los honeypots por su ambiente de implementación se clasifican en: Honeypots de Investigación y Honeypots de Producción.

Los objetivos de un honeypot de investigación son:

- Detectar nuevas modalidades de ataques y herramientas de hacking.
- Conocer de mejor manera a los atacantes, sus objetivos, actividades y tendencias
- Descubrir nuevas modalidades de comunicaciones encubiertas.
- Detectar y analizar herramientas de DoS desconocidas.

El objetivo de un honeypot de producción es recolectar suficiente evidencia de un ataque y su atacante.

Debido al gran desarrollo de las herramientas utilizadas por los atacantes para romper las seguridades implementadas en los diferentes sistemas informáticos, actualmente la mayoría de ataques se los realiza de manera automatizada, en las que se utiliza herramientas para el escaneo de redes buscando sus vulnerabilidades para luego poderlas explotar.

En este contexto el uso de honeypots para prevenir dichos ataques se ha ido popularizando en todo el mundo, ya que nos ofrecen gran cantidad de información recolectada en tiempo para realizar un adecuado análisis en busca de las vulnerabilidades de la red y así poder implementar los correctivos necesarios a los sitios reales y evitar un ataque que indisponga los sistemas reales.

2.4.2 Tipos de Honeypots

De acuerdo al tipo de implementación, existen dos tipos de Honeypots: Honeypots Físicos y Honeypots Virtuales.

Un Honeypot físico está montado sobre un equipo físico real el cual en la mayoría de casos implica que su funcionamiento sea de alta iteracción.

Este tipo de implementación resulta difícil principalmente por su alto costo de implementación y mantenimiento ya que resulta poco práctico utilizarlos para cubrir un amplio rango de direcciones debido a que sería necesario instalar un servidor honeypot para cada una de las direcciones IP.

Los Honeypots virtuales son aquellos que se encuentran implementados sobre servidores virtuales gracias al avance tecnológico en el campo de la virtualización en el cual podemos instalar varios servidores virtuales en un solo equipo anfitrión mediante la utilización de un software para virtualización.

Actualmente existen varias opciones de herramientas para virtualización entre las que podemos mencionar: VMWare, VirtualBox, entre otros.

Cada servidor virtual puede implementar un honeypot virtual pero que puede actuar como un honeypot físico de alta iteracción compartiendo los recursos físicos del equipo anfitrión con todos los demás servidores virtuales corriendo en paralelo cada uno con su propia identidad y funcionalidad.

Se dispone además de imágenes de máquinas virtuales ya configuradas como honeypots listas para ser utilizadas luego de realizarles ciertos afinamientos en su configuración de acuerdo a la solución particular a implementarse.

2.5 Redes virtuales honey

A este tipo de redes se las denomina Honeynets, las cuales son un conjunto de honeypots de alta iteracción diseñados para brindar diferentes servicios de red sobre uno o varios sistemas operativos diferentes, y que tienen como objetivo investigar y obtener información de los atacantes y sus acciones para evitar en el futuro intrusiones del mismo tipo.

Se debe entender a una honeynet como una arquitectura compleja y no como un producto software listo para su instalación.

Una Honeynet tiene por objetivo hacerle creer al ataque que se encuentra frente a una red real con diferentes tipos de servicios a los cuales atacar.

Al implementar una honeynet en conjunto con otros mecanismos se obtiene una mejor estrategia para detectar fallos o huecos de seguridad y así proveer mejores sistemas de defensa.

Al analizar la información recolectada de los ataques recibidos, podemos conocer amenazas aun no conocidas y documentadas.

Actualmente existe el “Honeynet Project” el cua es considerado como la organización de investigación de seguridad líder a nivel mundial cuyo propósito es detectar los nuevos tipos de ataques, desarrollar herramientas de seguridad de código abierto para mejorar los niveles de seguridad del Internet y aprender del comportamiento de los hacker maliciosos o Blackhat.

Entre los principales logros de ésta organización presente en todo el mundo se puede mencionar la lucha contra el malware y la creación de herramientas de seguridad utilizadas por empresas y organizaciones gubernamentales a nivel global, esta organización ha definido los requisitos que garantizan el funcionamiento de manera correcta de una Honeynet, con el fin de lograr un ambiente seguro para los sistemas de red en los que se implementa esta arquitectura.

Los requisitos que una Honeynet debe cumplir para su funcionamiento de manera segura son Control, Captura y Recolección de datos.

Una Honeynet es de gran ayuda para responder a las 5+1 W’s de los incidentes de seguridad:

- **W**hat (Qué)
- **W**here (Dónde)

- **W**hen (Cuándo)
- **W**ho (Quién)
- **W**hy (Por qué), +How (Cómo)
-

Desde el aparecimiento de este tipo de tecnología, la complejidad de las Honeynets ha ido evolucionando de acuerdo a la disponibilidad de las herramientas para el control y captura de los datos por lo que actualmente se hace la diferencia entre Honeynets de 1ra Generación y Honeynets de 2da Generación.

2.5.1 Evolución de las Honeynet

Desde el aparecimiento de la primera honeynet, han ido evolucionando en su infraestructura tecnología utilizada y funcionamiento, el proyecto denominado "*The Honeynet Project"* las agrupa en 2 generaciones, aunque otros autores las agrupan en 3 generaciones (seat.massey.ac.nz, 2009), las mismas que se describen a continuación.

Honeynets de 1ra Generación (GEN I)

Aparecieron en 1999 cuando Honeynet Project la desarrolló a partir de medidas simples pero eficientes para el control y captura de datos de los atacantes. Esta generación de Honeynets representada en el Gráfico #1, consta de un Firewall de capa 3 conectado a tres redes diferentes:

- Internet,
- Honeynet y,
- Red de producción.

Todos los paquetes entrantes o salientes de la Honeynet tienen que obligatoriamente pasar por el Router y el Firewall el cual es la principal herramienta para controla las conexiones de entrada o salida.

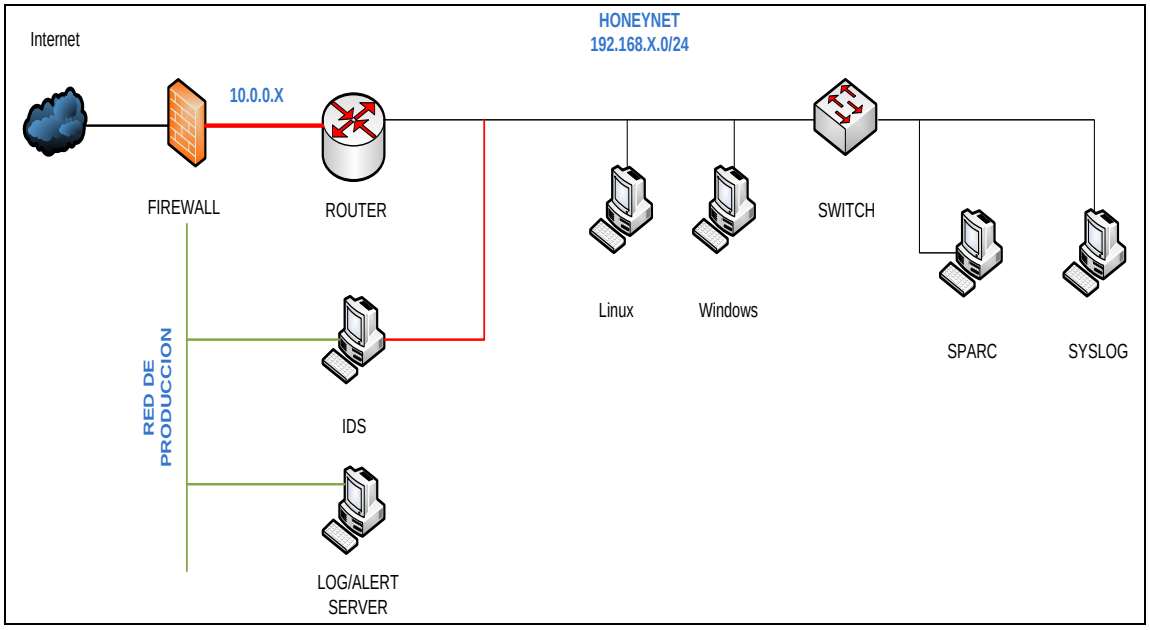


Gráfico # 1: Diagrama de una Honeynet de 1ra Generación

Fuente: El Autor

El firewall debe permitir cualquier conexión entrante pero debe mantener un control sobre todas las conexiones salientes limitando la cantidad permitida de éstas a cada honeypot.

Una vez que un honeypot ha alcanzado el máximo número de conexiones hacia el exterior, el firewall bloqueará cualquier otro intento de salida, facilitando con esto al hacker Blackhat una cierta flexibilidad para efectuar su ataque y de la misma manera nos brinda una adecuada protección frente al abuso.

El número de conexiones permitidas puede variar dependiendo de la funcionalidad que se busque. Si se desea descubrir actividad manual de un

Hacker malintencionado, se deberá permitir un cierto número de conexiones salientes; si al contrario se desea únicamente capturar ataques automáticos como autobotes o gusanos informáticos, lo más probable es que no se necesite permitir conexiones de salida.

El Router se constituye en un suplemento para el filtrado del tráfico en la red, se ubica entre la honeynet y el firewall con la intención de ocultarlo de los atacantes, ofreciéndoles un ambiente más real ya que los atacantes encuentran un Router productivo entre ellos y las redes exteriores.

Adicionalmente el Router actúa como una segunda opción de control de acceso sobre la capa 2, dando un mayor Control de Datos ya que ninguna Honeynet debe depender de una sola opción para este proceso.

El Router solo permitirá el paso de paquetes cuyo origen sea la Honeynet lo cual protege de ataques como el SYN Looping o ataques SMURF, además bloquea el tráfico de ICMP saliente, al limitar el ICMP a este nivel podemos ayudar al firewall en el seguimiento del tráfico con lo cual se protege a la red en la etapa de reconocimiento de la misma previa a un ataque y del ping de la muerte.

Al combinar el firewall con el Router se considera una técnica efectiva para el control del tráfico saliente ya que permite cierta flexibilidad al atacante para que realice su trabajo pero limitándolo al no permitir ataques a otros sistemas fuera de la honeynet.

La captura de los datos se la realiza en varias capas. La primera capa constituye el firewall que es quien registra y emite la alerta de todas las conexiones generadas desde y hacia la honeynet a las cuales se las considera sospechosas.

La siguiente capa en la captura de datos se la realiza en el Sistema de Detección de Intrusos IDS el cual tiene dos objetivos: capturar la actividad de la red es decir capturar y registrar todos y cada uno de los paquetes y su carga en

la infraestructura de red. Esta acción se la realiza a través de la interface de red que se encuentra físicamente unida a los otros sistemas de la honeynet.

El segundo objetivo del IDS es el de emitir las alertas de cualquier actividad sospechosa, muchos IDS realizan el análisis de actividad sospechosa comparando con ciertas “marcas” de los paquetes analizados concuerdan con las almacenadas en una Base de Datos de Marcas ya conocidas.

El IDS utilizado por Honeynet Project es el denominado Snort in Line con el cual se ha obtenido un excelente rendimiento al efectuar estas tareas, sistema que reenvía periódicamente las alertas generadas al servidor de Syslog presente en la Honeynet.

La tercera capa de captura de datos las realizan los propios sistemas de los cuales se quiere capturar la actividad, esto se logra guardando todos los registros de eventos de los servidores tanto localmente como de manera remota a manera de backup en sistemas independientes que pueden ser Unix o Windows a donde se deberán enviar todos los datos capturados.

Esto debido a que un Syslog es fácilmente detectable por el atacante quien entre una de sus estrategias está siempre deshabilitar los procesos encargados de registrar los eventos “syslogd” a través de diversas herramientas disponibles en la actualidad.

Honeynets de 2da Generación (GEN II)

Esta evolución de las Honeynets se las utiliza a partir del año 2002 cuando fue desarrollada por Honeynet Project, la cual introduce varias modificaciones en relación a las Honeynets de 1ra generación. Los objetivos de esta evolución residen en simplificar su implementación y mejorar su seguridad, haciéndolos más difíciles de detectar por parte de los atacantes al ofrecerles mayores

posibilidades de interactuar con los sistemas comprometidos, pero ejerciendo un mayor control sobre sus actividades, con esto se logra una mayor cantidad de datos capturados para su posterior análisis.

La evolución hacia las honeynets de 2da generación tiene como objetivo mejorar los procesos de control de datos y captura de datos con la finalidad de simplificar su implementación y a la vez hacerlos más difíciles de detectar por parte de los atacantes.

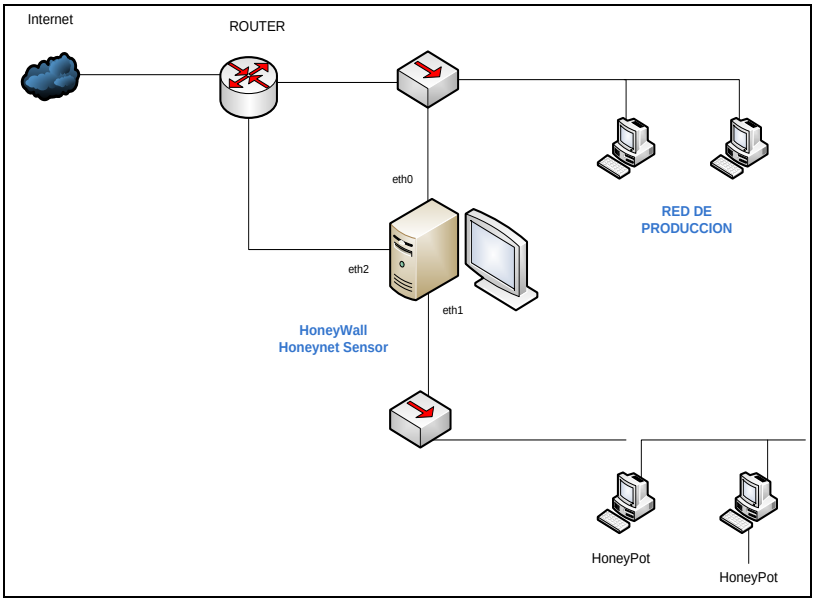


Gráfico # 2: Diagrama de una Honeynet e 2da Generación

Fuente: El Autor

El control de datos de una honeynet de 2da generación ofrece al atacante un mayor margen de interacción con los sistemas vulnerables, pero con un mayor nivel de control sobre sus actividades de una manera más transparente haciendo que este control sea más difícil de ser detectado. Esto se logra ofreciendo al atacante una mayor flexibilidad sobretodo en las conexiones de salida que son las que nos ofrecen mayor información para ser analizada.

Una de las ventajas de una honeynet de 2da generación es que todas las actividades de Control, Captura y Recolección de datos se las puede combinar en un único equipo o dispositivo hardware que actuará como puente o bridge de capa 2, por donde circulará todos los datos a ser analizados. Al ser un dispositivo de capa dos es hace más difícil de detectar por cuanto no dispone de una dirección IP (capa 3), no hay enrutamiento de trafico ni decrementos en la latencia de los paquetes, lo cual lo hace más invisible de los atacantes a quienes le será más difícil detectar si su tráfico está siendo analizadotraduciendose en una ventaja ya que toda la información cruza por el dispositivo con lo cual se puede capturar tanto el tráfico de entrada como el tráfico de salida en este dispositivo.

Además del control del número de conexiones de la actividad no autorizada, este dispositivo será capaz de averiguar qué tipo de tráfico es el que está circulando mediante la identificación del tipo de acciones e intenciones que el atacante ejerce con su actividad. Por ejemplo, el atacante puede realizar unas 20 conexiones FTP de salida, lo cual no representaría peligro alguno, pero si tratara de ejecutar acciones de exploit sobre este mismo protocolo hacia sistemas del exterior que no sean la honeynet (honeypots configurados); ésta actividad se la considerará peligrosa y deberá ser monitorizada y contenida con lo cual se le dota de mayor inteligencia al sistema de control el cual permite la salida del ataque desde la honeynet pero sin ser efectivo; esto se logra modificando los paquetes que atraviesan el bridge de capa 2 alterando la información peligrosa, por lo que el atacante observará que el ataque se realiza pero no entenderá porque no obtuvo éxito con el mismo.

La capacidad de captura de datos mejora sustancialmente con referencia a la generación anterior, ya que antes se realizaba esta actividad a nivel de Red mediante el uso de Sniffers, los mismos que actualmente han sido invalidados ante la generalización del uso de conexiones cifradas. El proceso de captura de datos actualmente se lo realiza a nivel del núcleo del sistema operativo del equipo que actúa como bridge con lo que se asegura la captura de datos a

pesar del protocolo cifrado utilizado para la comunicación los mismos que pueden ser IPSEC, SSL, SSH, entre otros. Una última consideración en la utilidad de esta generación de Honeynet es la económica, ya que son más baratos de implementar.

Honeynets de 3da Generación (GEN III)

Esta versión de Honeynet fue liberada en el año 2004, posee una arquitectura similar a las Honeynets de II generación con algunas mejoras en la interface de administración. La única diferencia entre una Honeynet de 3ra generación con una de 2da generación radica en la implementación dentro del Honeywall de un servidor SEBEK (seat.massey.ac.nz, 2009), diseñado para capturar la mayor parte de información de la actividad de los atacantes en los honeypots implementados de una manera silenciosa e indetectable posible para su posterior envío al servidor de recolección y almacenamiento de datos para su posterior análisis.

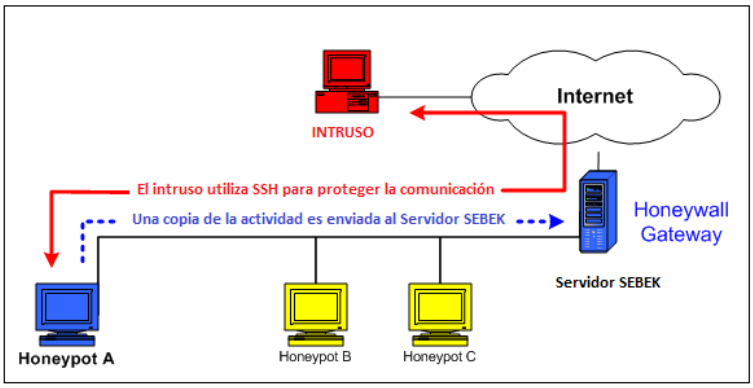


Gráfico # 3: Diagrama del Proceso SEBEK

Fuente: old.honeynet.org, 2006

CAPITULO III

DISEÑO E IMPLEMENTACION

3.1 Antecedentes

Como pasos previos al diseño e implementación de la infraestructura Honeypot en el Hospital Municipal, se realizará un estudio de las conductas informáticas de los Usuarios internos.

También se realiza el análisis lógico y físico de la infraestructura de red actual y pruebas de penetración mediante Hacking ético con la finalidad de detectar sus vulnerabilidades existentes.

3.2 Conducta informática de los usuarios

Se debe conocer la conducta informática de los usuarios de sistemas del Hospital Municipal para establecer los patrones de actuación de éstos respecto a los equipos informáticos, sistemas, servicios y todo tipo de programas o software ofrecidos a través de la Red Institucional para el desempeño de sus funciones.

Es importante determinar los niveles de buenas y malas prácticas informáticas, tanto por usuarios experimentados como por usuarios inexpertos, las buenas prácticas deben ser potenciadas y las malas prácticas deben ser eliminadas pará así minimizar el riesgo informático atribuible a las acciones de los usuarios.

3.2.1 Método de la investigación

Se utiliza el método de investigación Descriptivo – Cuantitativo para determinar los patrones de conducta Informática de los usuarios informáticos y así determinar que conductas deben ser potenciadas y que conductas deben ser corregidas.

3.2.2 Instrumento de recolección

El Instrumento de recolección de información utilizado es una encuesta.

3.2.3 Objetivo General

Determinar los patrones de conducta informática de los Usuarios Internos del Hospital Municipal Nuestra Señora de la Merced.

3.2.4 Objetivos Específicos

N°	OBJETIVO	HIPOTESIS
1	Conocer si los usuarios utilizan una o varias contraseñas para los diferentes sistemas	Utilizan varias contraseñas
2	Determinar si periódicamente se realiza el cambio de contraseñas	Si se cambia periódicamente

3	Conocer si se almacenan las contraseñas en algún medio físico o virtual por parte de los usuarios	Si se almacenan las contraseñas en algún tipo de medio
4	Determinar si existe compartición de contraseñas entre varios usuarios	Si existe compartición de contraseñas
5	Conocer si los usuarios acceden a servicios en línea desde computadores de sitios públicos	Si acceden desde computadores en sitios públicos
6	Conocer si los usuarios acceden a correo no deseado	No acceden a correo electrónico no deseado
7	Conocer si existe reenvío de cadenas de correo electrónico	No existe reenvío de cadenas de correo electrónico
8	Conocer si los usuarios publican información personal en redes sociales	Si publican información personal en redes sociales
9	Conocer si los usuarios instalan software descargado del internet	Si instalan software descargado del internet
10	Conocer si los Usuarios utilizan unidades externas de almacenamiento de información	Si utilizan unidades externas de almacenamiento de información
11	Conocer si los usuarios bloquean su computado como medida de seguridad cuando se ausentan de su estación	Si bloquean su computador

3.2.5 Muestra

Para la realización de este estudio se tomará como población al personal del Hospital Municipal Nuestra Señora de la Merced que utilizan sistemas informáticos

Cálculo de la Muestra

Para calcular la muestra se utilizará la siguiente fórmula:

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}$$

n = el tamaño de la muestra = ?

N = tamaño de la población = 61

σ =Desviación estándar de la población = 0,5.

Z = Valor obtenido mediante niveles de confianza (90%) = 1,65

e = Límite aceptable de error =9% (0,09)

n=36 Usuarios encuestados

3.2.6 Encuesta de patrones de conducta informática de los Usuarios Internos del Hospital Municipal Nuestra Señora de la Merced.

1) ¿Utiliza usted la misma contraseña para varios sistemas o cuentas?

OPCION	PORCENTAJE	CANTIDAD
SI	36,11%	13
NO	63,89%	23
TOTAL	100,00%	36

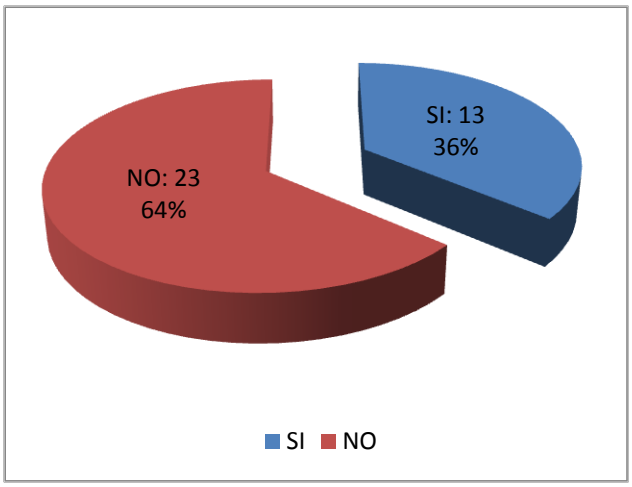


Gráfico # 4: Tabulación Encuesta E01 Pregunta N°1

Fuente: Encuesta. **Elaborado por:** El autor

Hay un 63,89% de usuarios que no utiliza la misma contraseña en varios sistemas o cuentas lo cual constituye una buena práctica de seguridad ya que con ello previenen que la seguridad de sus cuentas se encuentren protegidas de mejor manera en el caso de que alguna de las contraseñas sea descifrada con cual comprometerá solo a un servicio y no a todos, sin embargo es necesario reforzar o dar a conocer esta buena práctica en la totalidad de usuarios.

2) ¿Con que frecuencia cambia la contraseña de sus cuentas de sistemas informáticos?

OPCION	PORCENTAJE	CANTIDAD
SEMANAL	2,78%	1
MENSUAL	25,00%	9
EVENTUAL	58,33%	21
NUNCA	13,89%	5
TOTAL	27,78%	36

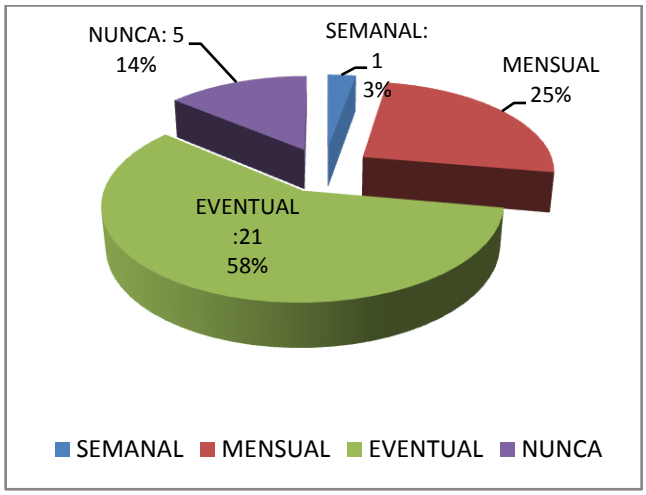


Gráfico # 5: Tabulación Encuesta E01 Pregunta N°2

Fuente: Encuesta. **Elaborado por:** El autor

De acuerdo a los resultados obtenidos solo un pequeño porcentaje de usuarios, 25%, cambia sus contraseñas de manera periódica en un lapso de tiempo aceptable (un mes), y la gran mayoría lo realiza eventualmente 58%, lo cual constituye una debilidad dentro del esquema de seguridad lógica de los sistemas informáticos, así también un 14% de usuarios reconoce que nunca cambia sus contraseñas.

3) ¿Almacena usted los nombres de usuarios y contraseñas en algún medio (papel, archivo de texto, etc.)

OPCION	PORCENTAJE	CANTIDAD
SI	30,56%	11
NO	69,44%	25
TOTAL	100,00%	36

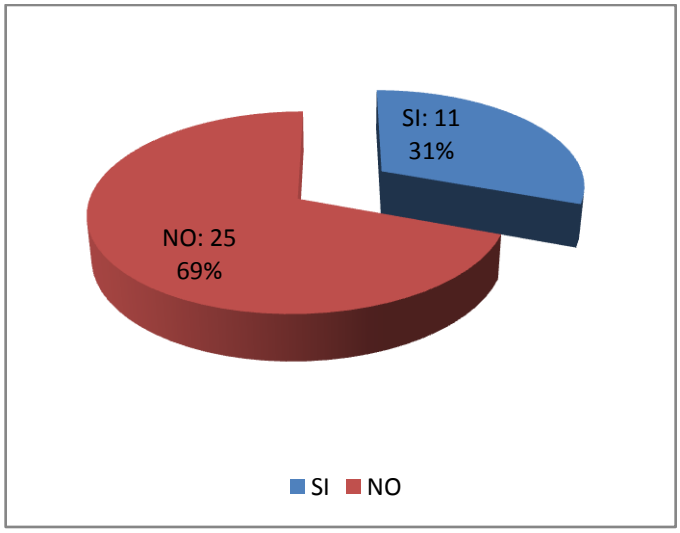


Gráfico # 6: Tabulación Encuesta E01 Pregunta N°3

Fuente: Encuesta. **Elaborado por**: El autor

A pesar de que un 69% de usuarios indica que no almacena de manera física sus contraseñas en algún medio, existe un porcentaje importante que si lo hace, lo cual constituye una falla de seguridad importante que en algún momento puede comprometer algún servicio informático.

4) ¿Ha compartido con compañeros de trabajo o familiares las contraseñas de sus cuentas de servicios informáticos? (Correo Electrónico, Redes sociales, Sistemas Informáticos)?

OPCION	PORCENTAJE	CANTIDAD
SI	27,78%	10
NO	72,22%	26
TOTAL	100,00%	36

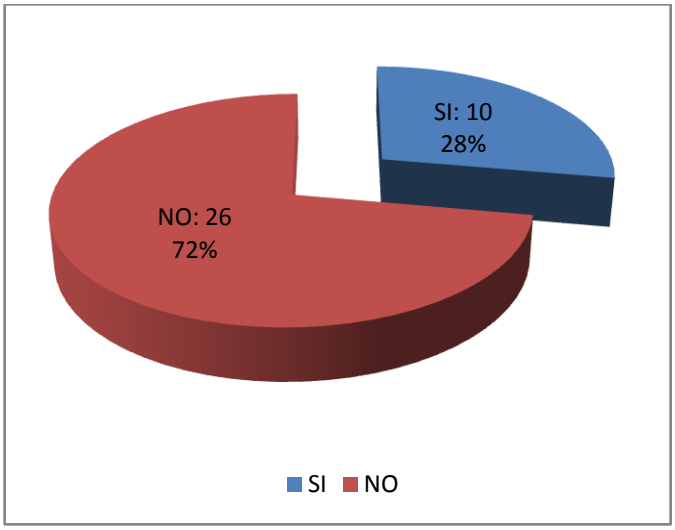


Gráfico # 7: Tabulación Encuesta E01 Pregunta N°4

Fuente: Encuesta. **Elaborado por:** El autor

Un porcentaje importante de usuarios, 28%, afirma compartir las contraseñas de sus cuentas con una tercera persona ya sea en el trabajo o el hogar, lo cual constituye una violación expresa de la normativa interna que indica que las contraseñas de las cuentas de servicios institucionales son de carácter personal e intransferible.

5) ¿Accede a sus cuentas de correo, redes sociales u otros servicios como banca virtual, pago de servicios, etc. desde servicios públicos de internet (cibercafés)?

OPCION	PORCENTAJE	CANTIDAD
SI	19,44%	7
NO	80,56%	29
TOTAL	100,00%	36

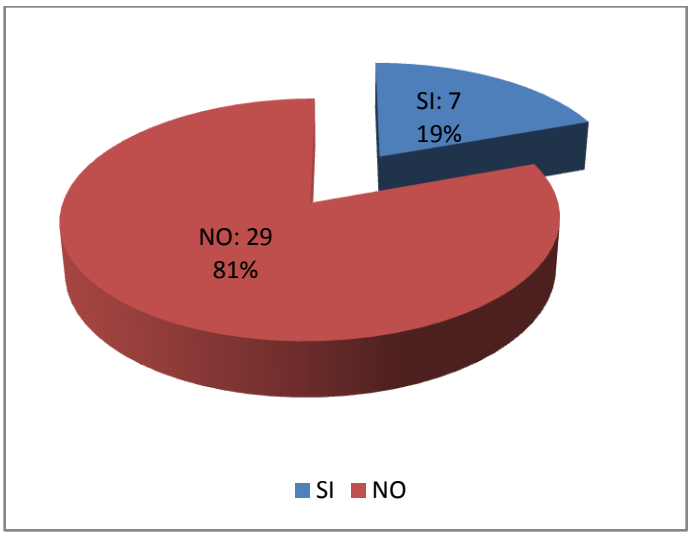


Gráfico # 8: Tabulación Encuesta E01 Pregunta N°5

Fuente: Encuesta. **Elaborado por:** El autor

El 81% de los usuarios encuestados afirma que no accede a sus cuentas de correo, redes sociales y otros servicios desde sitios públicos de acceso a internet, lo cual constituye una buena práctica de seguridad, quedando únicamente un 18% lo cual se considera un porcentaje bajo.

6) ¿Descarga usted archivos adjuntos de un correo electrónico cuando desconoce su remitente o no ha sido solicitado (SPAM)?

OPCION	PORCENTAJE	CANTIDAD
SI	0,00%	0
NO	100,00%	36
TOTAL	100,00%	36

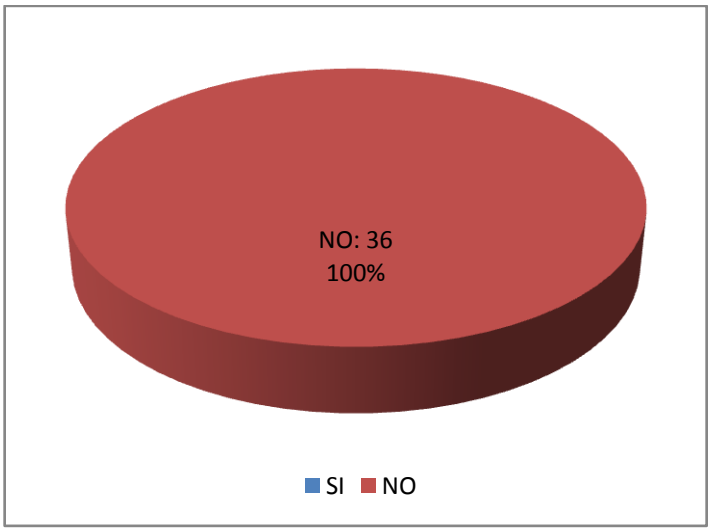


Gráfico # 9: Tabulación Encuesta E01 Pregunta N°6

Fuente: Encuesta. **Elaborado por:** El autor

La totalidad de los encuestados indica que nunca descarga archivos adjuntos de correos de remitentes desconocidos o SPAM, constituyendo una fortaleza en cuanto a buenas prácticas de seguridad.

7) ¿Reenvía Cadenas recibidas en su correo electrónico?

OPCION	PORCENTAJE	CANTIDAD
SI	2,78%	1
NO	97,22%	35
TOTAL	100,00%	36

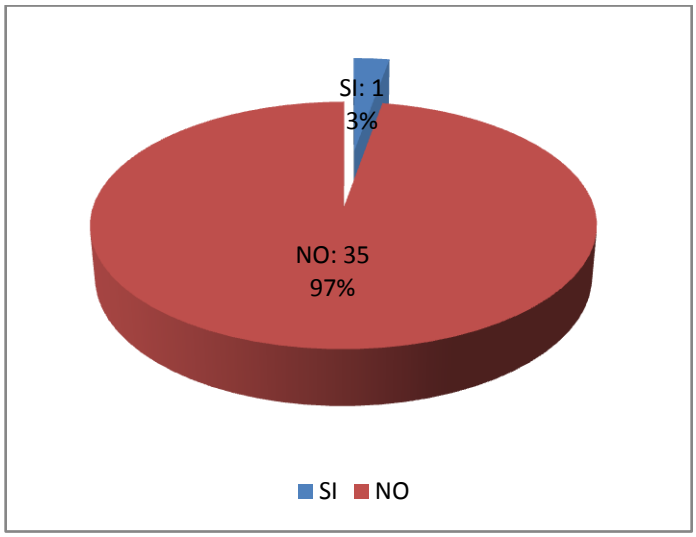


Gráfico # 10: Tabulación Encuesta E01 Pregunta N°7

Fuente: Encuesta. **Elaborado por:** El autor

Prácticamente la totalidad de los encuestados 97% indica que no reenvía cadenas de correo electrónico, lo cual indica que existe cumplimiento a la normativa institucional al respecto.

8) ¿Publica usted información personal en las redes sociales?

OPCION	PORCENTAJE	CANTIDAD
SI	19,44%	7
NO	80,56%	29
TOTAL	100,00%	36

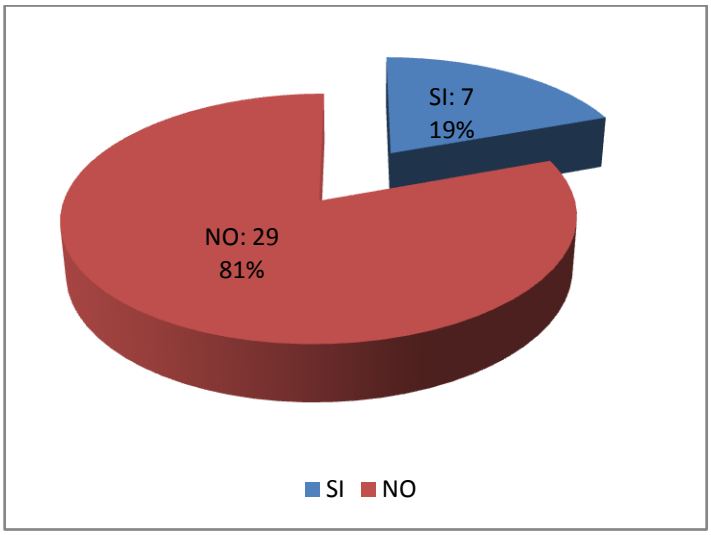


Gráfico # 11: Tabulación Encuesta E01 Pregunta N°8

Fuente: Encuesta. **Elaborado por:** El autor

El 81% de los usuarios encuestados afirma que no publica información personal en las redes sociales, lo cual constituye una buena práctica de seguridad ya que se evita hacer pública información que podría eventualmente ser utilizada para la realización de ingeniería social con fines específicos , quedando únicamente un 18% lo cual se considera un porcentaje bajo.

9) ¿Acepta la instalación de actualizaciones automáticas o software desde el internet en su computador personal o de trabajo?

OPCION	PORCENTAJE	CANTIDAD
SI	22,22%	8
NO	77,78%	28
TOTAL	100,00%	36

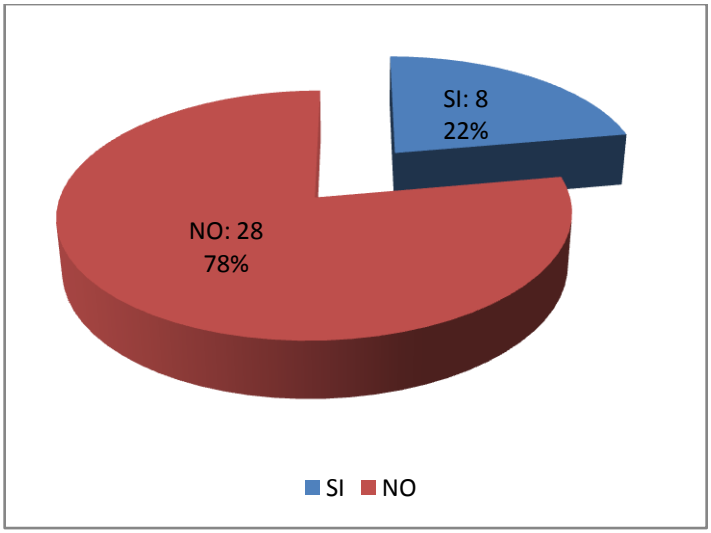


Gráfico # 12: Tabulación Encuesta E01 Pregunta N°9

Fuente: Encuesta**. Elaborado por:** El autor

La mayoría de encuestados 78% no instala actualizaciones ni software sugerido en internet. El porcentaje de usuarios que si lo hace es menor pero no despreciable 22%, lo cual indica que no se ha establecido correctamente los roles y permisos a nivel de usuarios en el sistema Active Directory

10) ¿Utiliza sus unidades de almacenamiento externos (discos externos, memorias flash) en los equipos de computo de la institución

OPCION	PORCENTAJE	CANTIDAD
SI	36,11%	13
NO	63,89%	23
TOTAL	100,00%	36

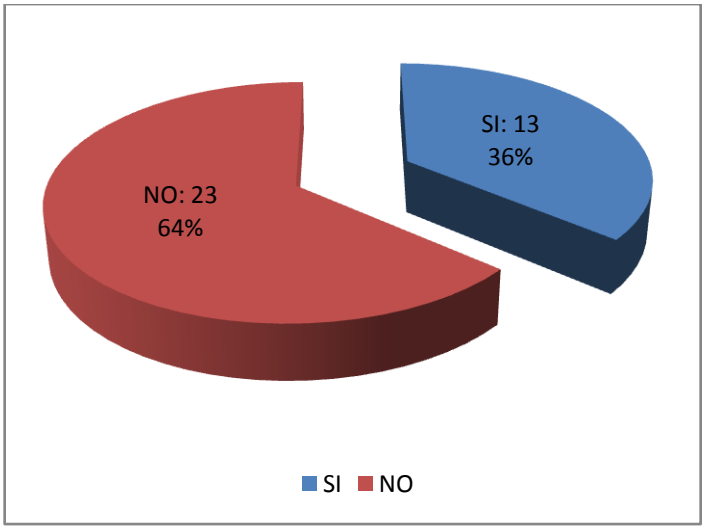


Gráfico # 13: Tabulación Encuesta E01 Pregunta N°10

Fuente: Encuesta. **Elaborado por:** El autor

El porcentaje de usuarios que no utiliza sus unidades de almacenamiento externo 64%es mayor que el porcentaje de los usuarios que si lo hace 36%, se deberá realizar un análisis del grupo de usuarios que por necesidades el desempeño de su trabajo necesite utilizar este tipo de medios de almacenamiento y transporte y cuál es el grupo que no lo necesita.

11) ¿Bloquea su computador antes de ausentarse eventualmente de su estación de trabajo?

OPCION	PORCENTAJE	CANTIDAD
SI	41,67%	15
NO	58,33%	21
TOTAL	100,00%	36

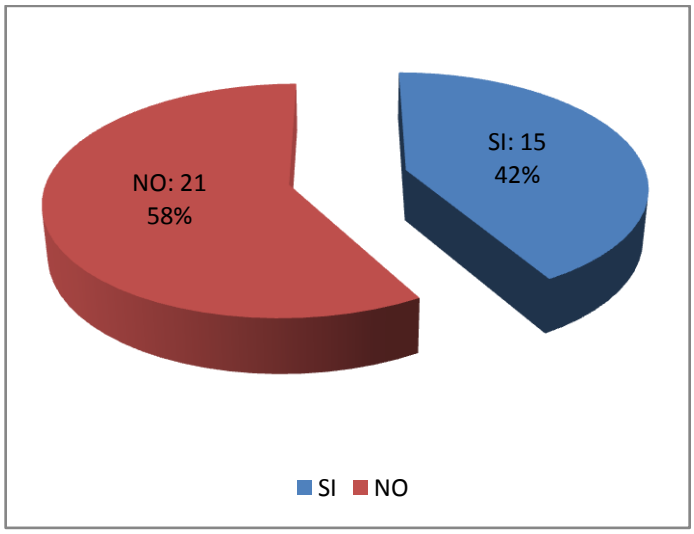


Gráfico # 14: Tabulación Encuesta E01 Pregunta N°11

Fuente: Encuesta. **Elaborado por:** El autor

A pesar de que se ha socializado la necesidad de bloquear el equipo de cómputo cuando por diversas circunstancias los usuarios abandonan su estación de trabajo como medida de seguridad, existe un 42% de usuarios que no lo hace, lo cual constituye un riesgo importante para la seguridad de la información.

3.3 Análisis de la infraestructura existente

El Hospital Municipal Nuestra Señora de la Merced posee una red de datos con una topología de estrella, mediante la implementación de un switch de núcleo y varios centros de distribución interconectados por enlaces de fibra óptica y cobre.

3.3.1 Descripción la red

El Switch de núcleo o Core implementado es un Cisco Catalyst 3560G de Capa 3, en el cual se ha configurado los siguientes servicios:

- Enrutamiento intervlan.
- Protocolo DHCP.
- Enrutamiento Estático.

Jerárquicamente la red tiene un diseño basado en la implementación de VLANS, de acuerdo al estudio realizado se ha determinado que en el Switch de Núcleo se encuentran creadas 5 VLANS (1,10,20,30,40) siendo utilizada la VLAN 1 para la administración de los equipos activos de red y las restantes para producción, a pesar de esto, actualmente todos los equipos de la granja de servidores y equipos clientes se encuentran ubicados en una única VLAN 10, dejando subutilizadas las restantes redes virtuales.

La conexión a Internet se la realiza a través de un Router de Balance de carga con dos interfaces WAN y tres interfaces LAN, las interfaces WAN tienen asignadas las direcciones IP 190.152.3.180 para el enlace ADSL con el ISP CNT EP y 190.95.194.130 para el enlace con el ISP Telconet S.A, este equipo

cumple la función de Gateway o Puerta de enlace a Internet mediante la dirección IP 10.0.0.1/24.

Las interface LAN del Router de Balance de carga se encuentran asignados a un segmento de red privado intermedio, al cual se conecta la interface WAN del Firewall institucional instalado sobre un servidor Appliance NETCYCLON, además se encuentra conectado directamente a este segmento de red un Servidor de Correo Institucional fuera de una zona desmilitarizada y sin un firewall intermedio.

3.3.2 Equipos activos de red

La infraestructura de red del Hospital municipal Nuestra Señora de la Merced cuenta actualmente con un Switch de Núcleo, 5 Switches de distribución administrables y un switch de sub-distribución no administrable, los mismos que se detallan a continuación:

SWITCH N°	CODIGO	DESCRIPCION	MARCA	PTOS OCUP.	PTOS LIBRES	UBICACIÓN
0	SC1	SWITCH CORE	CISCO 3560	19	9	RACK DATACENTER 1
1	SD1	SWITCH DISTRIBUCION 1	3COM 2948	33	15	RACK DATACENTER 1
2	SD2	SWITCH DISTRIBUCION 2	3COM 2924	10	14	RACK EMERGENCIAS
3	SD3	SWITCH DISTRIBUCION 3	3COM 2928	21	7	RACK PB1
4	SD4	SWITCH DISTRIBUCION 4	3COM 2920	11	9	RACK CAJA
5	SD5	SWITCH DISTRIBUCION 5	CISCO 330	6	22	RACK DATACENTER 2
6	SD6	SWITCH DISTRIBUCION 6	DLINK N/A	7	1	RACK PB1

Tabla # 1: Equipos activos de la Red

Fuente: El Autor

3.3.3 Diagrama lógico de la Red

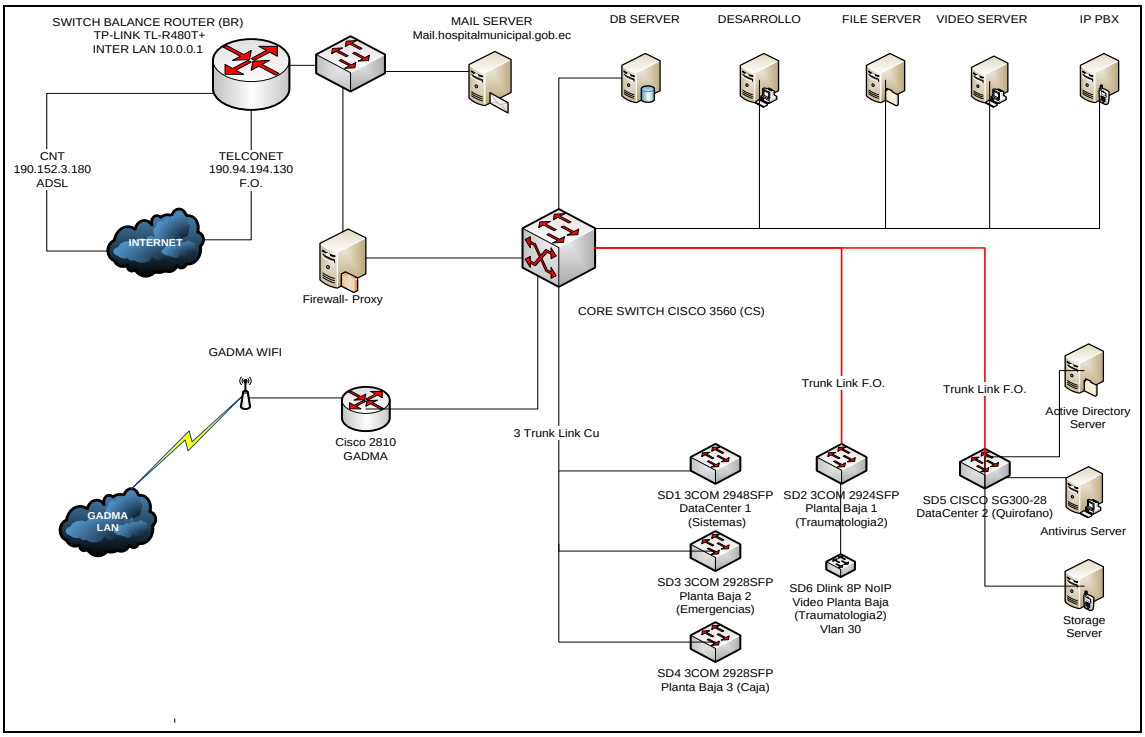


Gráfico # 15: Diagrama Lógico Red

Fuente: El Autor

3.4 Implementación de herramientas Honeypot

Una vez analizado el diseño de la red del Hospital Municipal, y las diferentes generaciones de Honeynets, se ha establecido que una Honeynet de Tercera generación es la más adecuada a ser implementada ya que su implementación y mantenimiento es una tarea más sencilla que para una Honeynet de Primera generación, además de ofrecer mayor seguridad en los procesos de Control de Datos y captura de Datos que evita que esta infraestructura deliberadamente vulnerable sirva como plataforma de ataque a los sistemas de producción del Hospital.

3.4.1 Diseño

Al diseño original de una Honeynet de Tercera generación en la que es necesario un enrutador para poder acceder a la interface de administración del Honeywall, se le ha realizado una modificación que consiste en el incremento de una tarjeta adicional de red al servidor para poder tener acceso a la consola de administración de manera directa.

De acuerdo al diagrama presentado a continuación, se ha escogido el segmento de red 10.0.0.0/24 correspondiente a la red de interconexión entre el router de frontera de internet y el firewall corporativo, en base a esto se ha definido las direcciones IP que serán configuradas en los Honeypots así como la interface de administración.

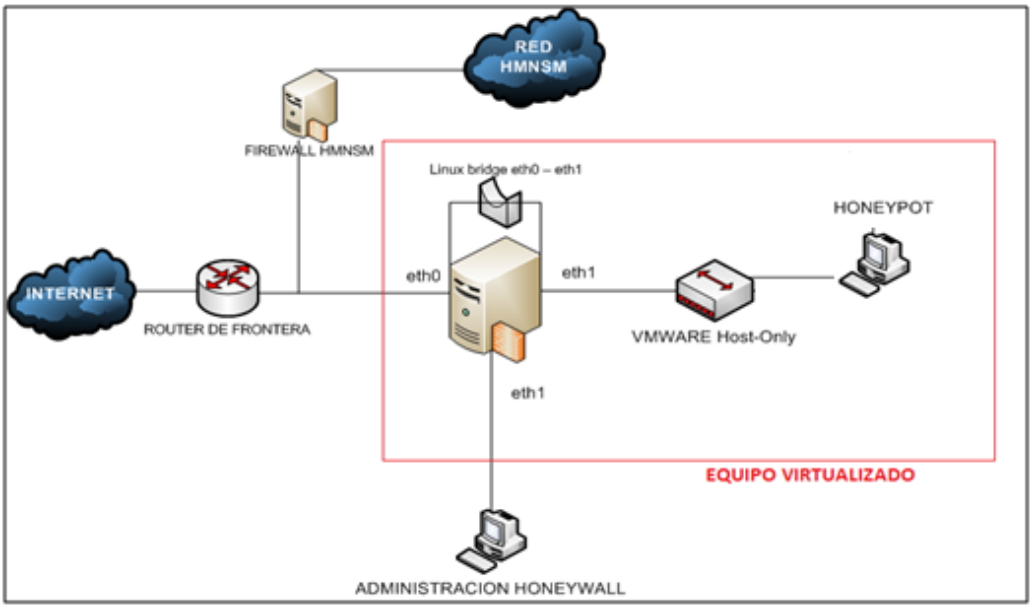


Gráfico # 16: Diagrama Honeynet Propuesto

Fuente: El Autor

A continuación se muestra la información de red para los dispositivos presentes en la Honeynet propuesta.

MAQUINA VIRTUAL	DIRECCION IP	GATEWAY	DNS
M.V. HONEYWALL	10.10.10.66/24	10.0.0.1	10.0.0.1
M.V. WINDOWS X.P	10.0.0.20/24	10.0.0.1	10.0.0.1

Tabla # 2: Direccionamiento IP Honeynet

Fuente: El Autor

3.4.2 Requerimientos de hardware y software

Con la finalidad de realizar esta implementación, y de acuerdo a las experiencias obtenidas por el Honeynet Project se utilizará la herramienta Honeywall proporcionada por el mencionado proyecto denominada ROO, la misma que será complementada por el Honeypot para Windows HoneyBot .

Tanto el honeywall como el Honeypot Windows serán instalados en una máquina virtual; la herramienta de virtualización escogida es WMWARE Workstation para su creación y configuración, posteriormente para su ejecución se utilizará VMWARE PLAYER PLUS por cuestiones de licenciamiento.

Toda la infraestructura de la honeynet se instalará en un computador HP 6000PRO, procesador core i7 con 6 Gb de memoria RAM con dos interfaces físicas de RED

.

3.4.3 Configuración de la Infraestructura virtual

Como pasos previos a la instalación de la honeynet, se deberá tener listo el software de virtualización VMWARE-Workstation, que es en donde se procederá a la instalación y configuración del Honeywall y el Honeypot que luego serán ejecutados en VMWARE PLAYER.

En el software de virtualización VMWARE Workstation se debe configurar las interfaces de red, dos interfaces en modo bridge (VMnet0, VMnet2) y una tercera interface (VMnet1) en modo Host-Only. Las interfaces VMnet0 y VMnet2 deberán ser asociadas a cada una de las interfaces físicas de red del equipo anfitrión. La interface 1 servirá para conectarse al segmento de red en donde se implementa la Honeynet a la cual no se le asignará ninguna dirección IP y la segunda interface VMnet2 la cual servirá para conectarse a la consola de Administración del Honeywall denominado Walleye, por último la interface VMnet1 en modo Host-only servirá para conectar el honeywall con el Honeypot de acuerdo al diagrama propuesto.

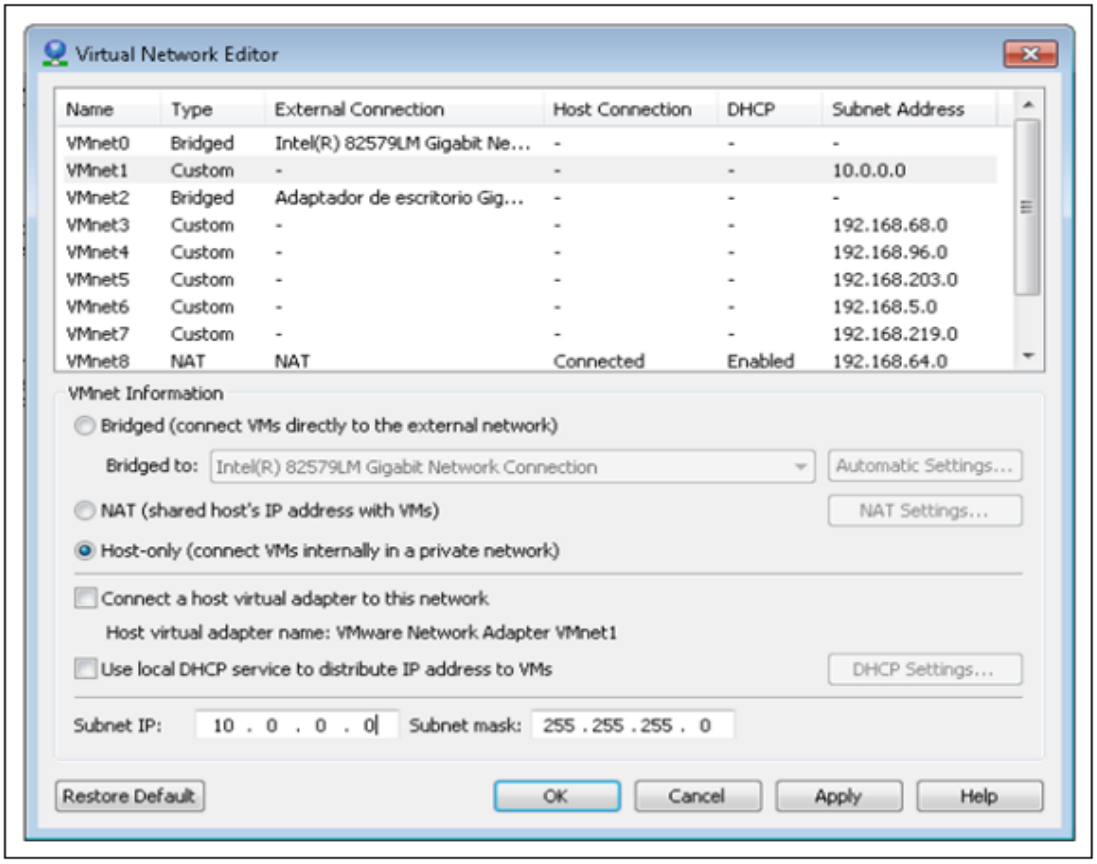


Gráfico # 17: Interfaces virtuales VMWARE

Fuente: El Autor

3.4.4 Instalación y configuración del Honeywall

Para la instalación del Honeywall, se debe iniciar el Asistente de creación de maquinas virtuales de VWWARE, en donde es necesario indicar la ruta de la fuente de instalación del Sistema Operativo virtualizado, en este caso se escoge la opción para instalación desde un archivo de imagen previamente descargado de la página de Honeynet Project, a continuación se seguirá todos los pasos, proporcionando la información solicitada en las secciones de usuario de la máquina virtual, el nombre de la maquina virtual y el tamaño del disco duro virtual.

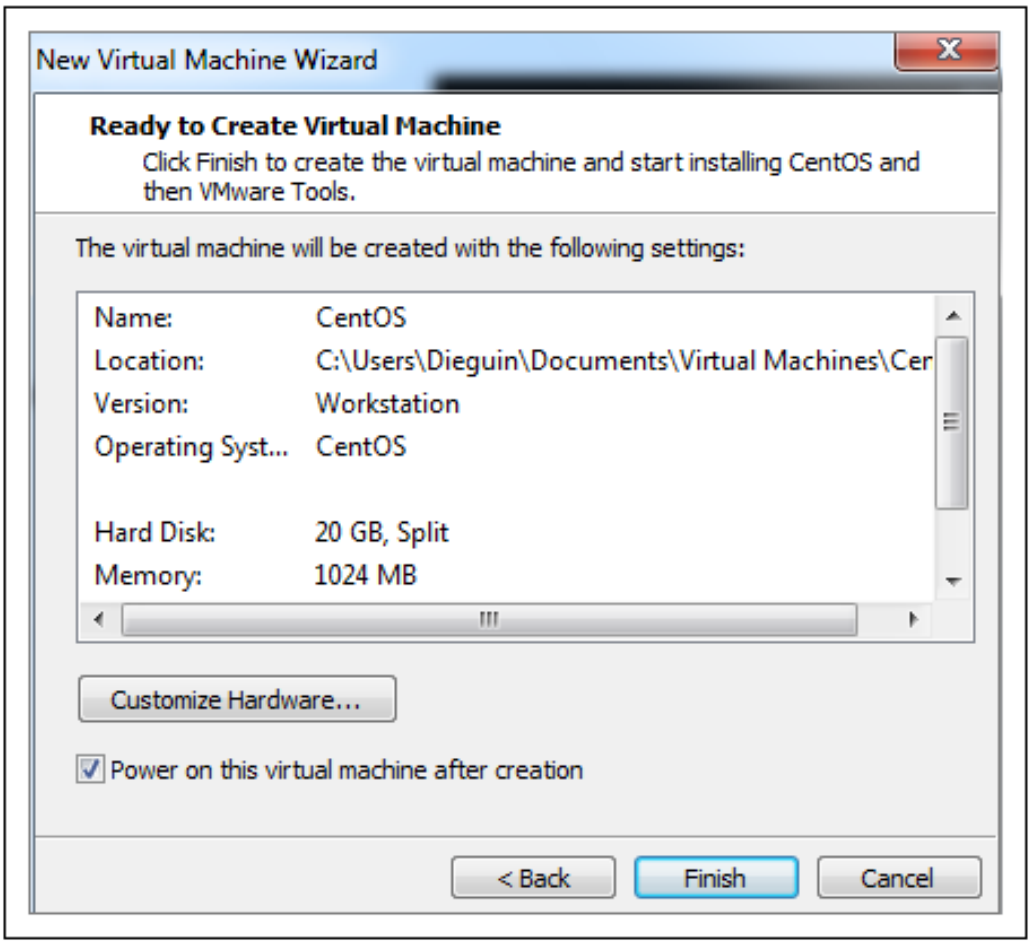


Gráfico # 18: Sección final del asistente de creación de máquinas virtuales

Fuente: El Autor

Una vez que se ha cumplido con todos los pasos del asistente, éste se encuentra listo para realizar la instalación con las configuraciones por defecto, aquí antes de continuar se deberá realizar la personalización del hardware de la máquina virtual mediante la Opción ***"Customize Hardware"*** tal como se muestra en el Gráfico #19, específicamente lo relacionado a las interfaces de red, asociando la interfaz virtual 0 a VMnet0, la interface virtual 1 a VMnet1 y por último la interface virtual 2 a VMnet2.

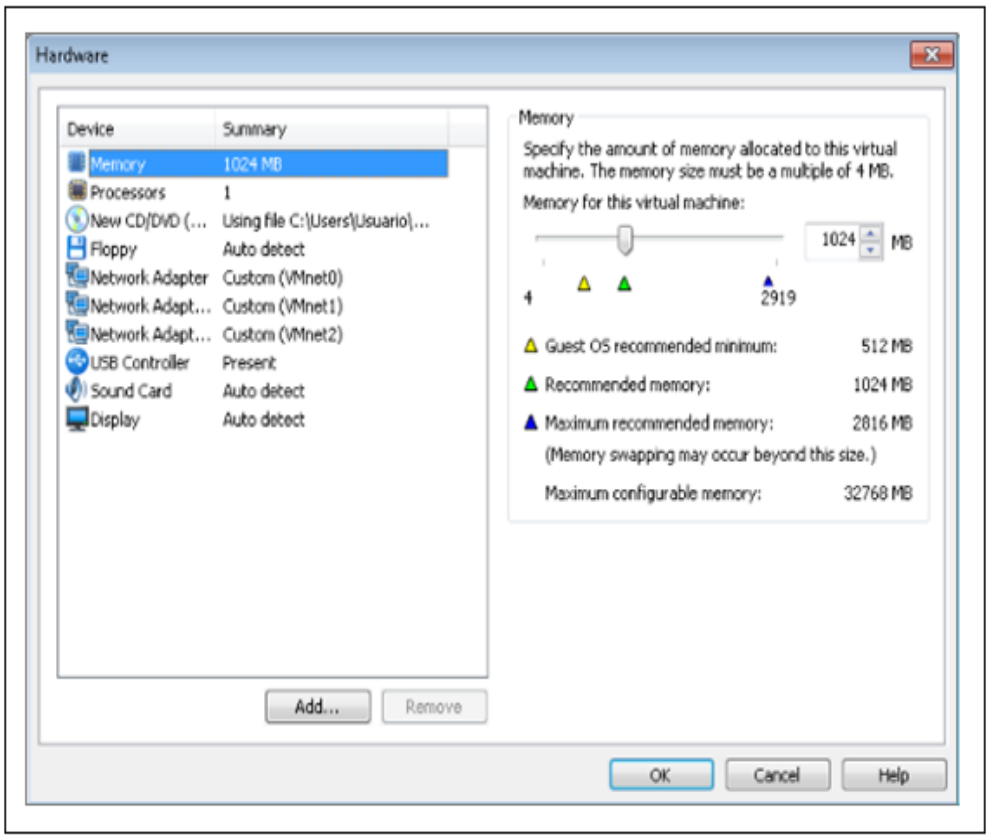


Gráfico # 19: Adición y configuración de las interfaces de red Honeywall

Fuente: El Autor

A continuación se deberá finalizar el asistente para que se inicie el proceso de instalación de la máquina virtual creada.

Gráfico # 20: 17 Inicio de la Instalación del Honeywall

Fuente: El Autor

Luego de dar inicio a la instalación del sistema operativo del honeywall, el proceso tardará algunos minutos. Luego del reinicio automático de la máquina virtual, se deberá ingresar con el usuario por defecto "**roo"** y la contraseña "**honey**" a continuación nos cambiaremos de usuario con el comando "**su –**" y la contraseña "**honey**".

Una vez que se ha ingresado en el honeywall, aparecerá el mensaje que nos indica que aun no se encuentra configurado, antes de continuar es necesario establecer los parámetros necesarios para configurar correctamente el Honeywall.

En la etapa de configuración del honeywall, se establecen todas las direcciones de red de los honeypots, segmentos de red, Interfaces de administración, permisos de acceso, también se configura los parámetros que determinaran los límites a las conexiones salientes para los diferentes protocolos, los permisos de seguridad en el firewall, las acciones del IPS Snort incluido y los parámetros de escucha de los paquetes SEBEK generados en los Honeypots instalados.

En la Tabla #3 se detalla la totalidad de los parámetros que serán ingresados en el asistente de configuración.

PARAMETRO	VALOR	OBSERVACIONES
HONEYPOTS ADDRESS	10.0.0.20	Dirección del honeypots Windows
HONEYNET NETWORK CIDR	10.0.0.0/24	CIDR de la red de la Honeynet
HONEYNET BROADCAST ADDRESS	10.0.0.255	Dirección de broadcast de la red de la honeynet
MANAGEMENT INTERFACE	eth2	Interface física para el acceso a la Interface de administración
MANAGEMENT INTERFACE ADDRESS	192.168.3.66	Dirección IP de la Interface de administración
NETWORK MASK FOR THE MANAGEMENT INTERFACE NETWORK MASK	255.255.255.0	Mascara de Subred de la interface de administración
GATEWAY ADDRESS	192.168.3.254	Dirección del Vlan Gateway
HOSTNAME	administración	Nombre del Host de administración
DOMAIN NAME	hospitalmunicipal.gob.ec	Domino de internet configurado
DNS SERVER ADDRESS	10.0.0.1	Dirección del servidor de DNS a donde apunta la honeynet
ACTIVATE INTERFACE	Yes	Activar la interface de administración
START MANAGEMENT INTERFACE NEXT BOOT	Yes	Iniciar la interface de administración en el siguiente inicio del sistema
CONFIGURE SSH	Yes	Configurar acceso SSH
SSH PERMIT REMOTE ROOT LOGIN	Yes	Acceso remoto SSH con el usuario **root** permitido
CHANGE ROOT PASSWORD	Yes	Cambiar la contraseña del usuario **root**
CHANGE PASWORD FOR ROO USER	Yes	Cambiar la contraseña del usuario **roo**
MANAGEMENT INTERFACE PORT ALLOWED	443	Puerto permitido para administración

LIST OF IP ADDRESS THAN CAN ACCES MANAGEMENT INTERFACE	192.168.0.0/16	Listado de direcciones IP que pueden acceder a la interface de administración
ENABLE WEB INTERFACE FOR DATA ANALYSIS	YES	Habilitar el análisis de datos a través de la interface web de administración
RESTRIC FIREWAAL OUTBOUND COMUNICATIONS	YES	Restringir las conexiones salientes de la honeynet
TCP PORTS ALLOWED OUT	22,25,43,80,443	Puertos de TCP de salida permitidos
UDP PORTS ALLOWED OUT	53,123	Puertos UDP de Salida permitidos
CONNECTION LIMIT SCALE	hour	La escala de tiempo de control de las conexiones de salida es por horas
TCP LIMIT	50	Conexiones de salida TCP permitidas por hora
ICMP LIMIT	50	Conexiones de salida UDP permitidas por hora
OTHER PROTOCOLS	100	Conexiones de salida de otros protocolos permitidas por hora
FIREWALL SEND PACKETS TO SNORT_INLINE	YES	El firewall permite el envío de paquetes al IDS snort_inline
SNORTV RULERSET	DROP	Eliminar paquetes que coinciden con alguna de las reglas de SNORT
ENABLE BLACKLIST, WHITELIST	NO	Habilitar Listas negras y blancas
DISABLE STRICT CAPTURE FILTERING	NO	Deshabilitar el filtro de captura estricto de datos
FENCELIST	NO	No habilitar la lista de defensa
ROACH MOTEL	NO	No habilitar Roach Motel
HONEYNET DNS UNLIMITED ACCESS	YES	
HONEYPOT UNLIMITED DNS ACCES	YES	Acceso DNS ilimitado para la honeynet
WHICH HONEYPOTS HAS UNLIMITED EXTERNAL DNS ACCESS	NO	No determinar que honeypots tienen acceso ilimitado al DNS
RESTRICT WHICH DNS SERVER CAN BE USED FOR UNLIMITED	YES	Restringir que servidores de DNS serán utilizados para el acceso

ACCES		ilimitado
LIST OF DNS SERVERS FOR HONEYPOT USE	10.0.0.1	Servidor DNS
CONFIGURE SEBEK VARIABLES	YES	
DESTINATION IP SEBEK PACKETS	10.0.0.100	Destino de los paquetes SEBEK
SEBEK PORT	6969	Puerto habilitado para los paquetes SEBEK
SEBEK PACKET OPTIONS	4 ACCEPT AN LOG	Acciones sobre los paquetes SEBEK

Tabla # 3: Parámetros de configuración Honeywall

Fuente: El Autor

Al iniciarse por primera vez el Honeywall , automáticamente aparecerá un Menú con las diferentes opciones para administrar, y configurar el Sistema Operativo y Honeywall. En caso de no aparecer esta opción se la puede ejecutar con el comando "**menú"** en la Shell de comandos.

Gráfico # 21: Menú de Opciones para administración del Honeywall

Fuente: El Autor

A continuación se escoge la opción “**Honeywall configuratión”** y se inicia automáticamente el asistente inicial donde inicialmente se debe seleccionar la Opción de configuración “**Interview**” .

Una vez escogido el modo de configuración se presentarán todas las opciones en donde se debe ingresar todos los parámetros previamente definidos en la Tabla #3, el detalle de las pantallas de configuración se lo puede observar en el Anexo E03.

Al finalizar el asistente de configuración el sistema se reiniciará, durante este proceso es posible que se produzcan varios errores en el inicio de algunos servicios, lo cual es normal. Una vez que el aparece la Shell de comando, se procede a ingresar nuevamente al menú de configuración, en donde se puede verificar parámetros establecidos y si es el caso se los puede modificar.

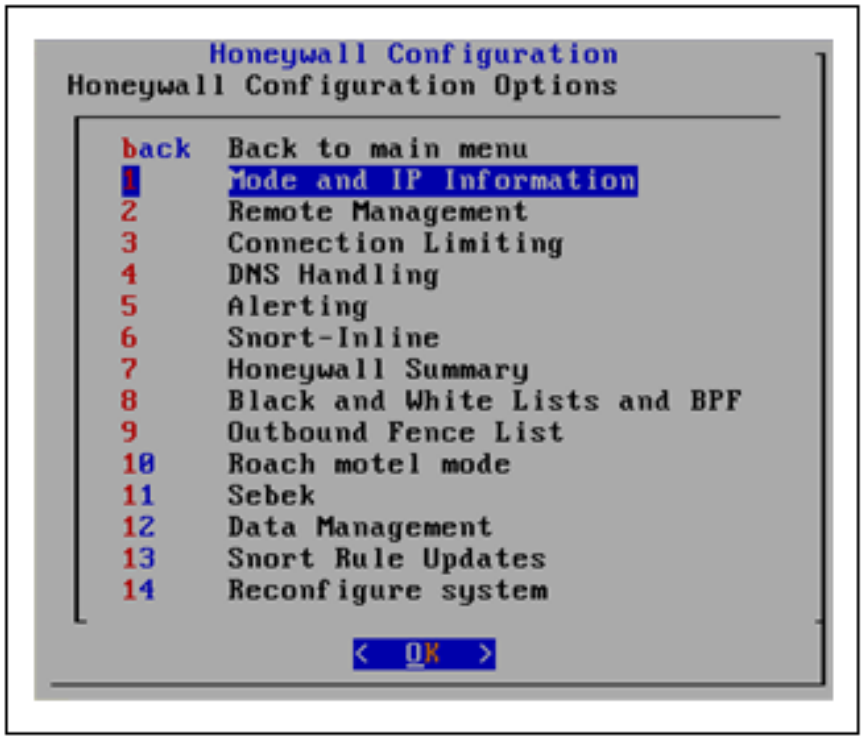


Gráfico # 22: Menú de configuración manual de parámetros del Honeywall

Fuente: El Autor

Concluida la etapa de instalación y configuración del Honeywall, se procede a ingresar a la consola Web de Administración del Honeywall en un computador diferente al utilizado para la implementación de la Honeynet, conectado a la interface eth2 el mismo que estará en el mismo segmento de Red en la que fue configurada la consola de administración.

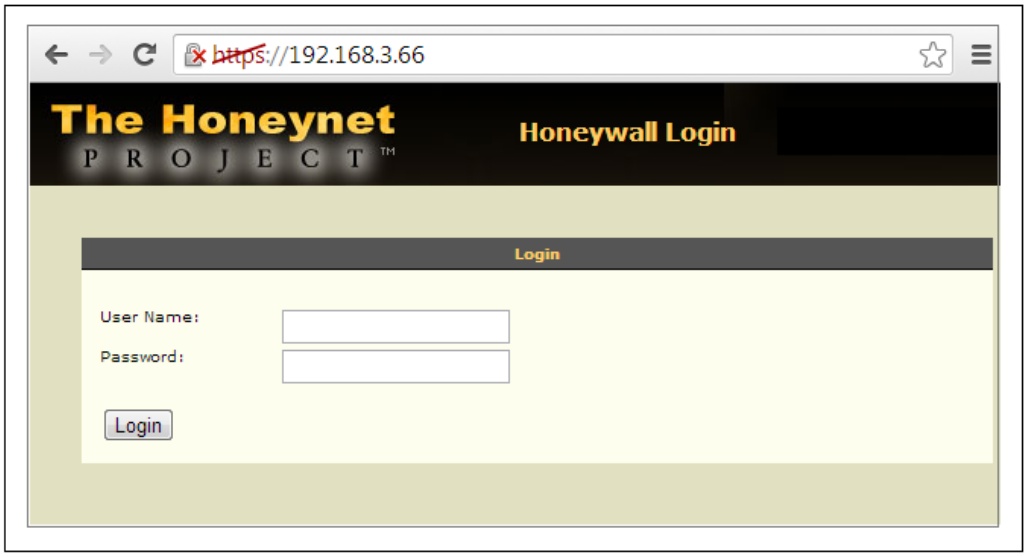


Gráfico # 23: Ingreso a la Consola Web de Administración Honeywall

Fuente: El Autor

3.4.5 Instalación y configuración del honeypot

Para el Honeypot , se deberá realizar los mismos pasos descritos anteriormente para la creación de nuevas máquinas virtual en VMWARE Workstation, con la diferencia que se deberá disponer del Paquetes de Instalación de Windows Xp SP1.

Hay que tener en cuenta que la máquina virtual Windows creada deberá tener instaladas una única interface de red asociada siempre a VMnet1, configurada en modo Host-Only para que de esta forma se comunique con la interface interna del Bridge creado en el Honeywall.

Una vez creada la máquina Virtual Windows XP, se debe configurar los parámetros de red previamente establecidos para este Honeypot, como se muestra a continuación:

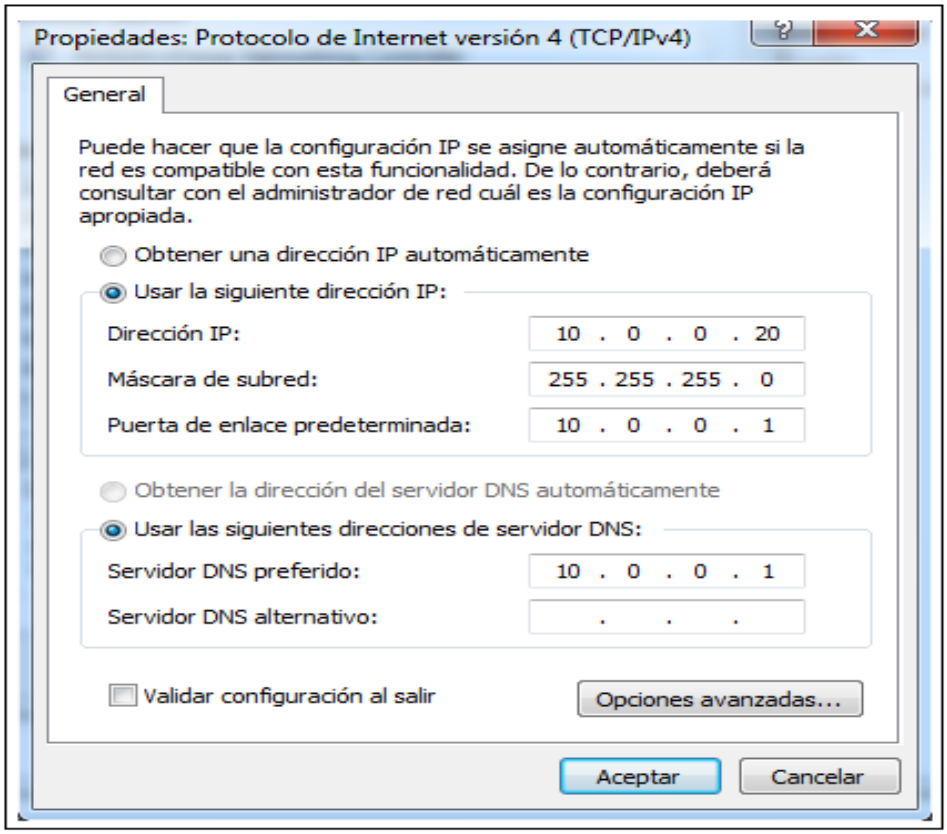


Gráfico # 24: Configuración de RED Honeypot Windows

Fuente: El Autor

A continuación se instala el Software HoneyBot, el cual funciona abriendo un gran número de sockets que los relaciona a servicios, deliberadamente vulnerables a manera de servidores reales, capturando y registrando de manera segura toda la comunicación del atacante para su posterior análisis. (hackplayers.com, 2009)

Una vez instalado HoneyBot, se procede a configurar los parámetros necesarios para su funcionamiento, tal como se observa a continuación.

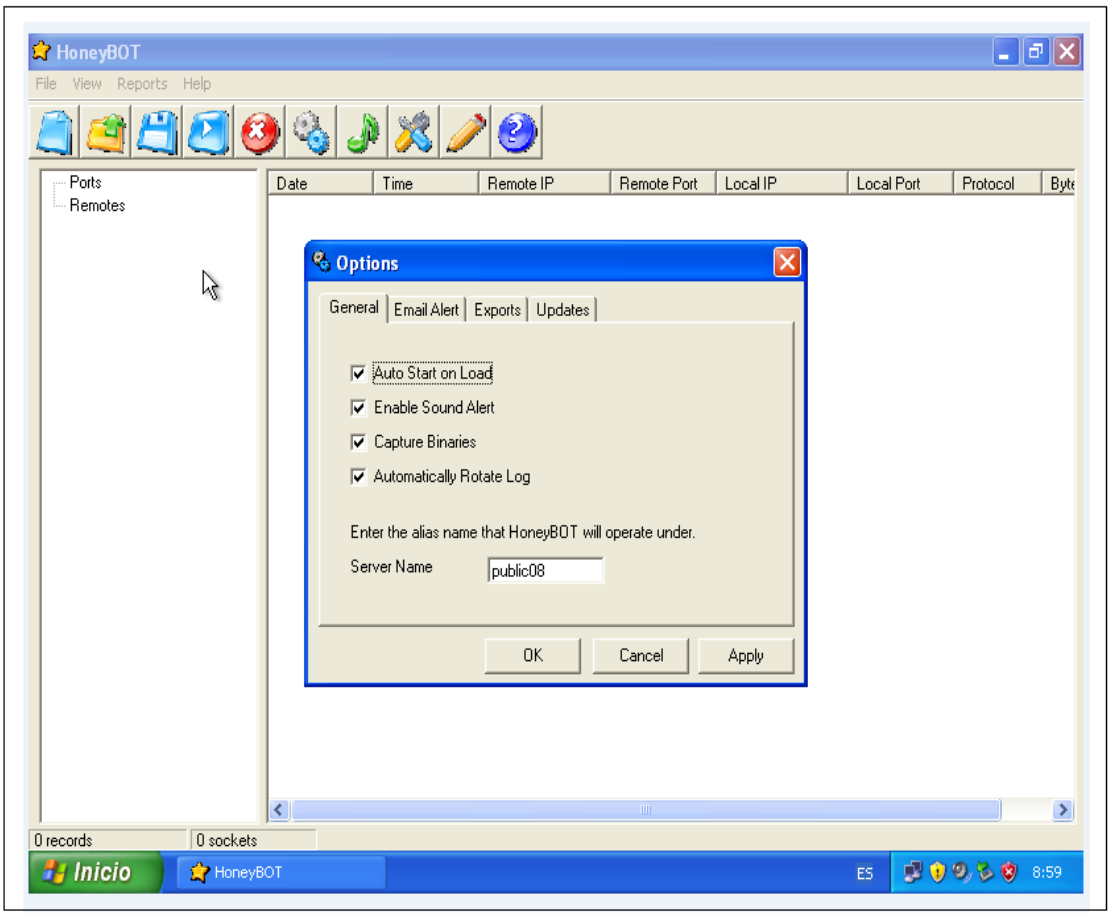


Gráfico # 25: Configuración del honeypot HoneyBot

Fuente: El Autor

Luego se debe instalar el software SEBEK_Client para la captura y envió de datos al servidor; para su configuración se debe ejecutar la aplicación "configuration_Wizard.exe" para iniciar el asistente de configuración en el Gráfico #26 en donde se deberá proporcionar los siguientes datos:

- Dirección MAC de la tarjeta eth1 del Honeywall. 00:0C.29:0A:82:E1
- Dirección IP de destino de los paquetes SEBEK: 10.0.0.100
- Puerto de destino de los paquetes SEBEK: 6969

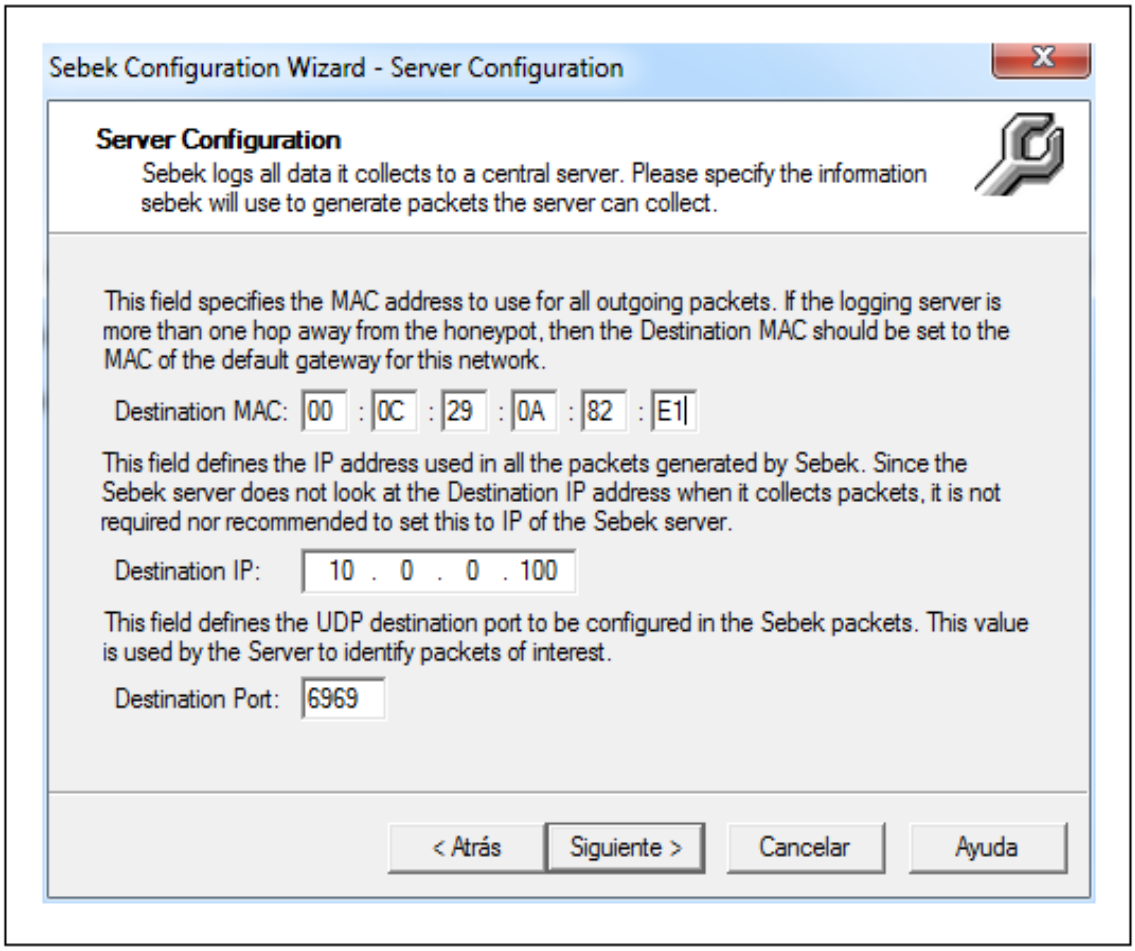


Gráfico # 26: Configuración del cliente SEBEK en el Honeypot

Fuente: El Autor

Los parámetros ingresados, fueron establecidos en la instalación del Honeywall de acuerdo a lo establecido en la Tablas 3.03.

3.4.6 Configuración de reenvío de puertos

Con la finalidad de enrutar todas las peticiones externas hacia el Honeypot se deberán configurar en el router de frontera el reenvío de los puertos necesarios

hacia el Honeypot cuya dirección IP es 10.0.0.20, tal como se muestra a continuación:

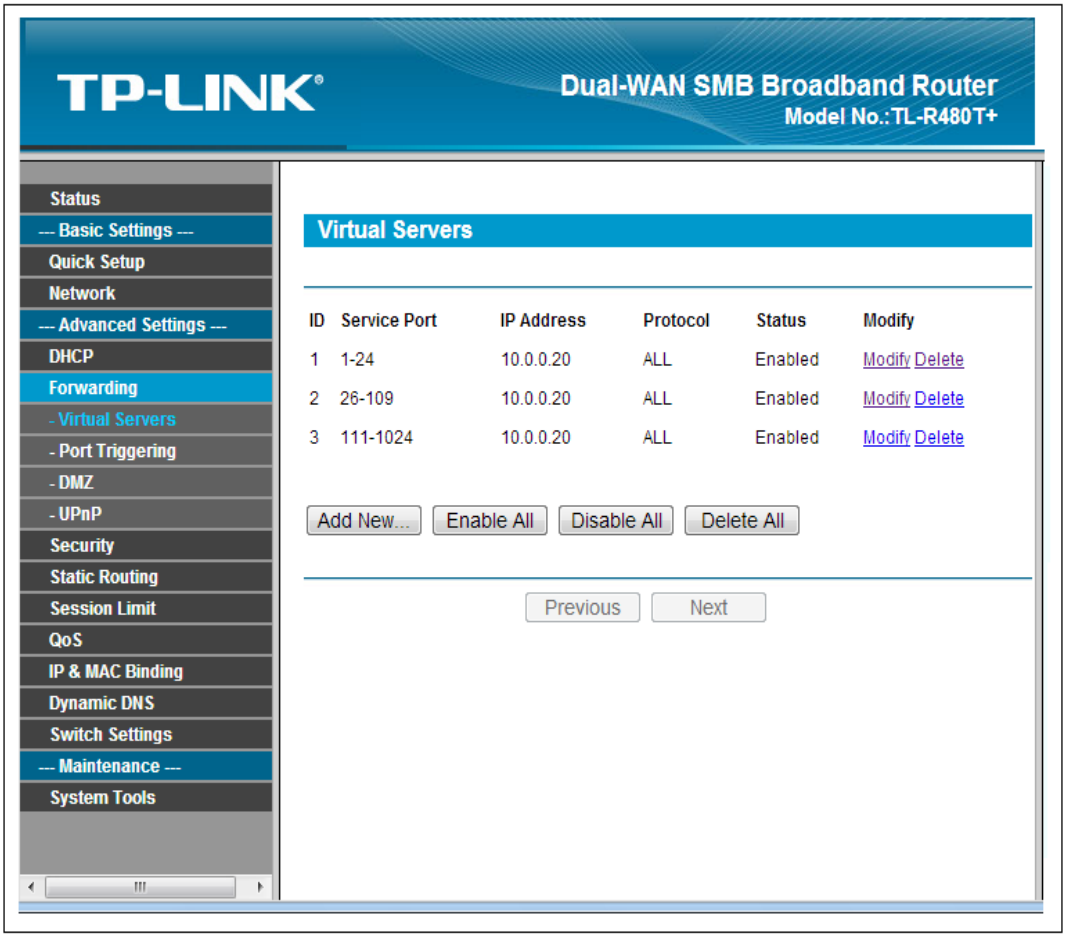


Gráfico # 27: Reenvío de Puertos en el Router de Frontera

Fuente: El Autor

3.5 Prueba de penetración mediante hacking ético

Para el análisis de las vulnerabilidades se realizará un hacking ético en un ambiente controlado el cual constará de los pasos descritos en el capítulo 2.

Para la ejecución de las tareas de penetración al sistema utilizaremos varias herramientas contenidas en la Distribución Kali Linux 1.0 virtualizado en un

equipo conectado a un punto de red conectado al switch de distribución SD1 en la VLAN 10 de producción.

3.5.1 Reconocimiento pasivo o footprinting

Para efectuar el primer paso de un hacker en una prueba de penetración, inicialmente debemos cambiar la MAC-ADDRESS del equipo desde el cual vamos a realizar el ataque para enmascarar la verdadera identidad física.

Para esto se debe utilizar el comando ":#macchanger –m 00:26:5a:11:22:33 eth0" donde 00:26:5a:11:22:33 corresponde a una MAC ADDRESS ficticia de un dispositivo de marca DLink para simular el ataque desde un dispositivo de esa marca.

En la fase de reconocimiento es de mucha utilidad conocer la direcciones IP, mascara de subred, dirección del Gateway, direcciones de DNS, todas éstas son asignadas al equipo atacante mediante un servidor de DHCP existente en la red.

Se obtiene la información de red mediante los comandos:

 # ifconfig eth0

 # nslookup ambato.gob.ec

 # route

La dirección IP obtenida corresponde al segmento de red 192.168.1.0/24, la dirección del servidor de DNS 192.168.1.7 y la dirección de la puerta de enlace

192.168.1.11, además se puede visualizar la nueva dirección MAC falsa, lo cual podemos observar a continuación:

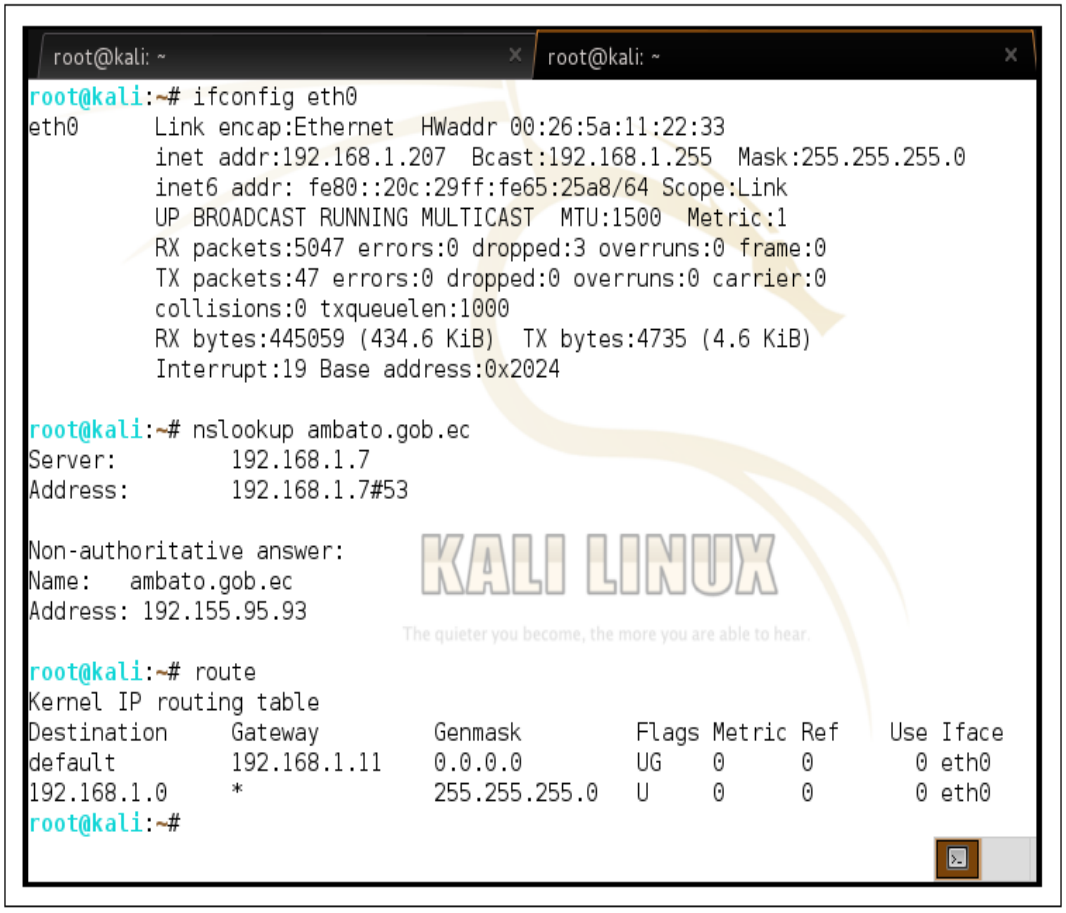


Gráfico # 28: Direccionamiento IP otorgado para prueba de penetración

Fuente: El Autor

A continuación se determina si esta puerta de enlace nos permite el acceso a internet, a una dirección escogida al azar, que en este caso es www.ambato.gob.ec mediante el uso del comando Windows **"tracert ambato.gob.ec"** y así obtener datos de los saltos de un paquete en la red antes de alcanzar su objetivo en el internet el internet.

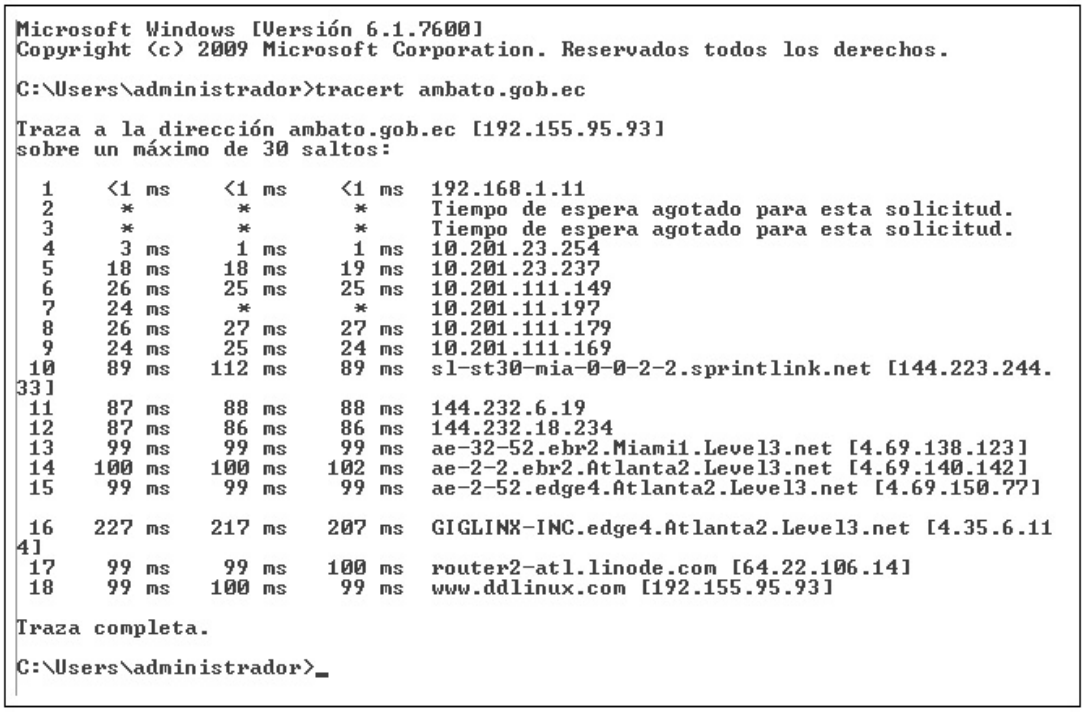


Gráfico # 29: Traza de un paquete enviado al internet

Fuente: El Autor

Como se pudo observar, un paquete realiza varios saltos hasta llegar al internet determinándose que la puerta de enlace al internet es 192.168.1.11 y el siguiente salto es desconocido debido a que el router del proveedor de internet no muestra su dirección.

3.5.2 Escaneo de la infraestructura

Una vez que se ha obtenido información mediante el análisis de reconocimiento o footprinting, procedemos a utilizar herramientas de escaneo activo para así determinar o tener una mejor idea de la topología de la red.

Para esta fase utilizaremos la herramienta Nmap incluida en la suite Kali Linux, la cual nos permite obtener desde un listado de los hosts activos en la red, sus puertos abierto, los sistemas operativos instalados, etc.

Se inicia el escaneo con*":# nmap 192.168.1.0/24 –sP-T4"*

*L*a ejecución de este comando realiza un escaneo de los hosts activos en la red 192.168.1.0 a una velocidad T4 superior a la normal y que los resultados se escriban en el archivo equipos.txt para su posterior análisis tal como se muestra a continuación:

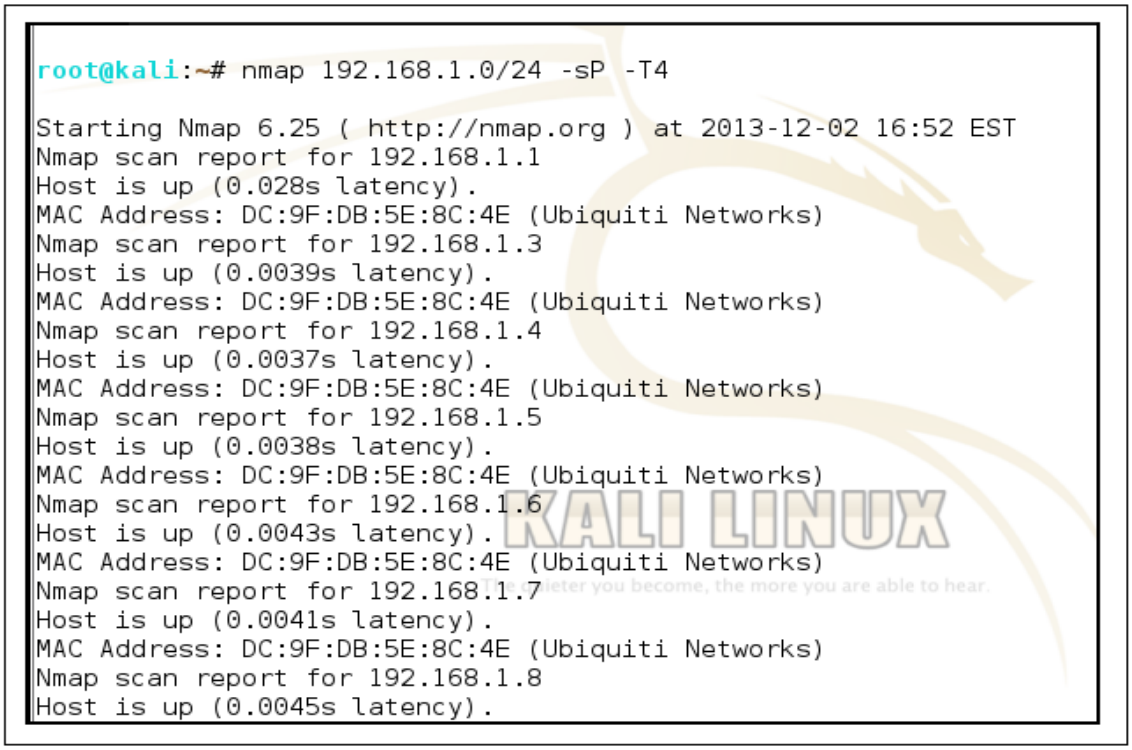


Gráfico # 30: Escaneo de Hosts activos mediante Nmap

Fuente: El Autor

En el archivo generado equipos.txt, encontramos el listado total de los hosts activos en la red al momento de la búsqueda, su dirección IP, la MAC ADDRESS y la marca, con lo cual ya poseemos un listado de las posibles víctimas para el ataque.

Una vez que ya tenemos la información general de puertos y sistemas operativos, se procede a obtener información de NetBIOS de Windows utilizando el comando ":#nbtscan 192.168.1.0/24" para obtener la información de todos los dispositivos de la red.

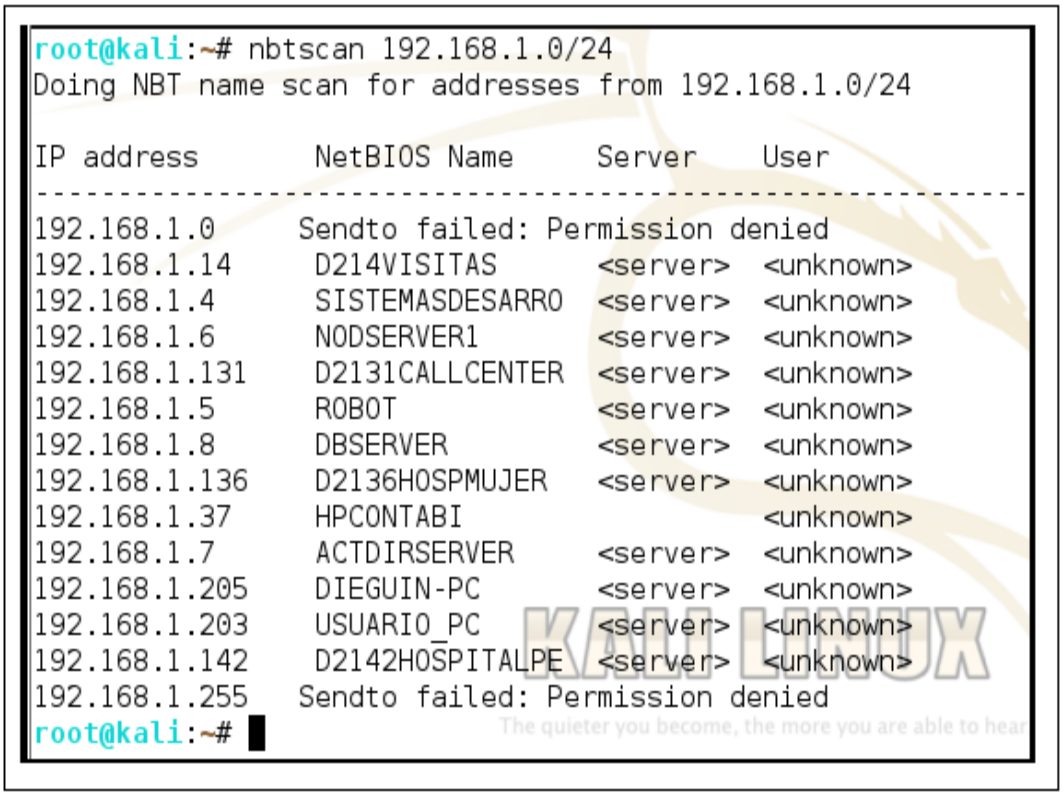


Gráfico # 31: Información de NetBIOS de la red mediante Nbtscan

Fuente: El Autor

La información obtenida es de mucha importancia, ya que podemos tener idea mediante el nombre de NetBIOS, cual es la función o ubicación e cada uno de los Hosts localizados.

Para determinar que puertos se encuentran abiertos en un equipo específico, en este caso DBSERVER que tiene como dirección IP 192.168.1.7 realizaremos un nuevo escaneo con Nmap de la siguiente manera "#nmap 192.168.1.8 –open –O"

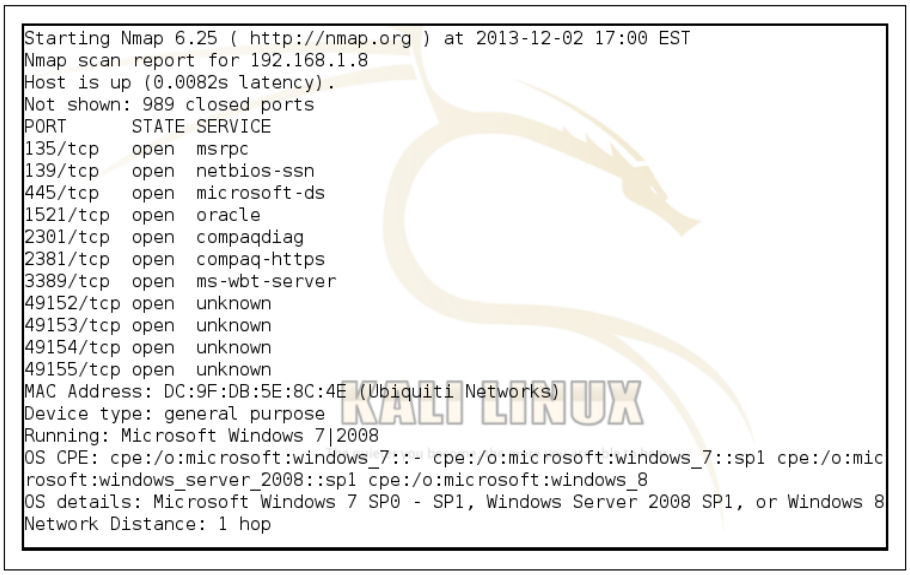


Gráfico # 32: Puertos abiertos Host 192.168.1.8 DBSERVER

Fuente: El Autor

Aquí al analizar los puertos abiertos del Host 192.168.1.8 DBSERVER podemos afirmar que aloja una base de datos Oracle por cuanto tiene abierto el puerto 1521: Oracle

3.5.3 Identificación de vulnerabilidades

Para esta fase del test de penetración al sistema utilizaremos la herramienta Nexpose Security Console en su versión comunitaria, la cual ha sido instalada en un equipo independiente debido a la gran cantidad de recursos que requiere para su funcionamiento. Esta aplicación se la puede descargar en la dirección *http://www.rapid7.com/products/nexpose/compare-downloads.jsp* con la cual podemos realizar solo una tarea de escaneo simultanea de hasta 20 equipos, es por esta razón que se ha subdivido en varias tareas el escaneo de los equipos de la red del Hospital.

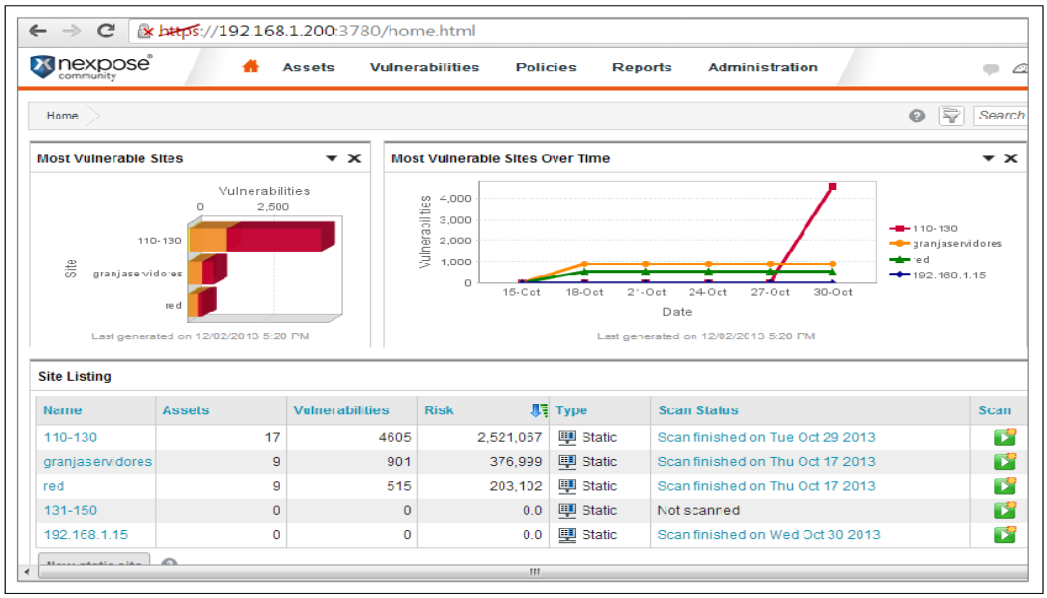


Gráfico # 33: Consola Nexpose Security

Fuente: El Autor

Una vez que se ha ingresado, debemos crear una nueva tarea:

Gráfico # 34: Creación de una Tarea en Nexpose

Fuente: El Autor

En esta etapa de creación de la tarea debemos seguir el asistente de creación en el que básicamente debemos ingresar la información que se detalla a continuación:

- Nombre de la tarea
- Listado de los equipos a ser escaneados (máximo 20)
- El tipo de Escaneo. Es este caso “Full Audit”

Las credenciales de ingreso al equipo. En nuestro caso utilizaremos la cuenta de administrador del dominio de red

Una vez que se ha finalizado el asistente de creación de tareas, la misma aparecerá en la consola principal donde le indicaremos que inicie el proceso de escaneo.

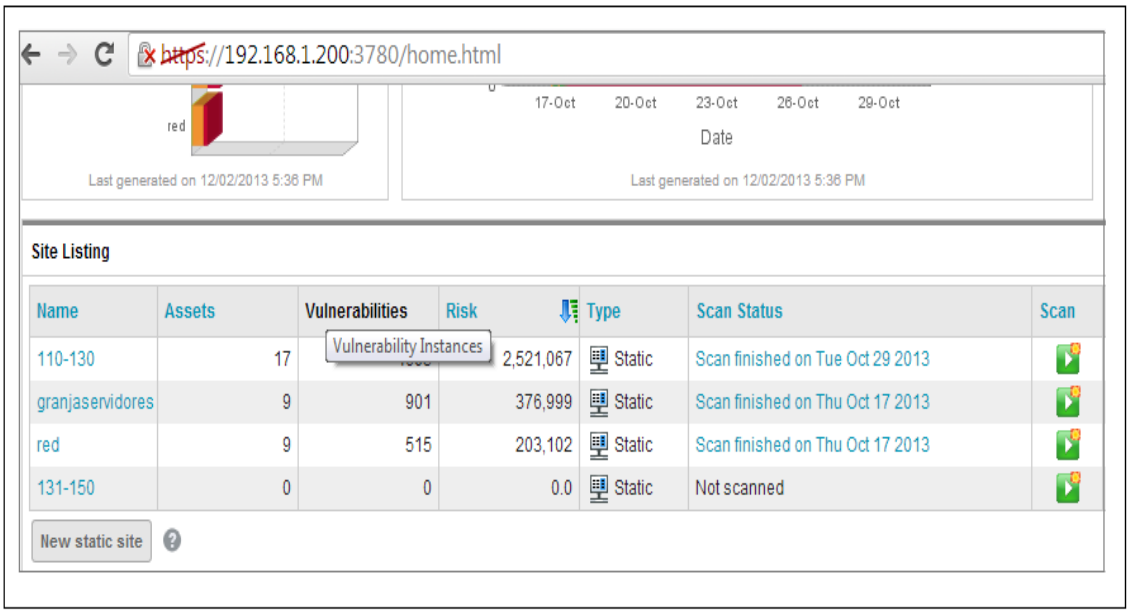


Gráfico # 35: Tareas creadas en Nexpose

Fuente: El Autor

Una vez que ha finalizado el análisis podemos obtener la información de los resultados obtenidos de manera estadística en la parte superior, y de manera específica en la parte inferior de la consola.

Para el ejemplo descrito, escogeremos el análisis realizado a un segmento de equipos de la granja de servidores cuyo rango de direcciones IP es 192.168.1.1-192.168.1.8.

Address	Name	OS			Vulnerabilities
192.168.1.1		Cisco IOS 12	0	0	2
192.168.1.3	ns.hospitalmunicipal.gob.ec	Linux 2.6.5 - 2.6.18	0	12	54
192.168.1.4	Sistemasdesarrollo	Microsoft Windows 7 Professional Edition SP1	13	90	304
192.168.1.5	ROBOT	Microsoft Windows XP	0	20	13
192.168.1.6	nodserver1	Microsoft Windows 7 Professional Edition	0	9	10
192.168.1.7	ACTDIRSERVER	Microsoft Windows Server 2003, Standard Edition SP1	12	72	81
192.168.1.8	dbserver	Microsoft Windows Server 2008 R2, Standard Edition SP1	0	24	134
192.168.1.9	mail.hospitalmunicipal.gob.ec	Linux 2.6.9 - 2.6.30	0	7	13

Gráfico # 36: Resultados Generales Granja de Servidores

Fuente: El Autor

Como se puede observar en la parte superior la información referente a la estadística comparativa de los diferentes análisis en el tiempo realizados sobre esta tarea en la parte inferior nos muestra el listado de los direcciones IP, nombre de NetBios, el sistema operativo, el número de malwares y vulnerabilidades con exploits conocidos detectadas, el total de vulnerabilidades en general, el nivel de riesgo y la fecha del último escaneo realizado de cada equipo incluido en la tarea.

A continuación se obtiene información más detallada de cualquiera de los equipos analizados; en este caso se escoge la IP del servidor de base de datos 19.168.1.8 tal como se observa a continuación:

Title	CVSS	Risk	Published On	Severity
MS08-063: Vulnerability in SMB Could Allow Remote Code Execution (957095)	10	814	Tue Oct 14 2008	Critical
MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution (959807)	10	811	Tue Dec 09 2008	Critical
MS09-013: Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803)	10	804	Tue Apr 14 2009	Critical
KB2607712: Fraudulent Digital Certificates Could Allow Spoofing	10	737	Mon Aug 29 2011	Critical
KB2718704: Unauthorized Digital Certificates Could Allow Spoofing	10	708	Sun Jun 03 2012	Critical
MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)	10	799	Tue Feb 09 2010	Critical
MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	10	785	Tue Aug 10 2010	Critical
MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	10	750	Wed Apr 13 2011	Critical
MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	10	853	Thu Oct 23 2008	Critical
MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	10	824	Tue Jan 13 2009	Critical

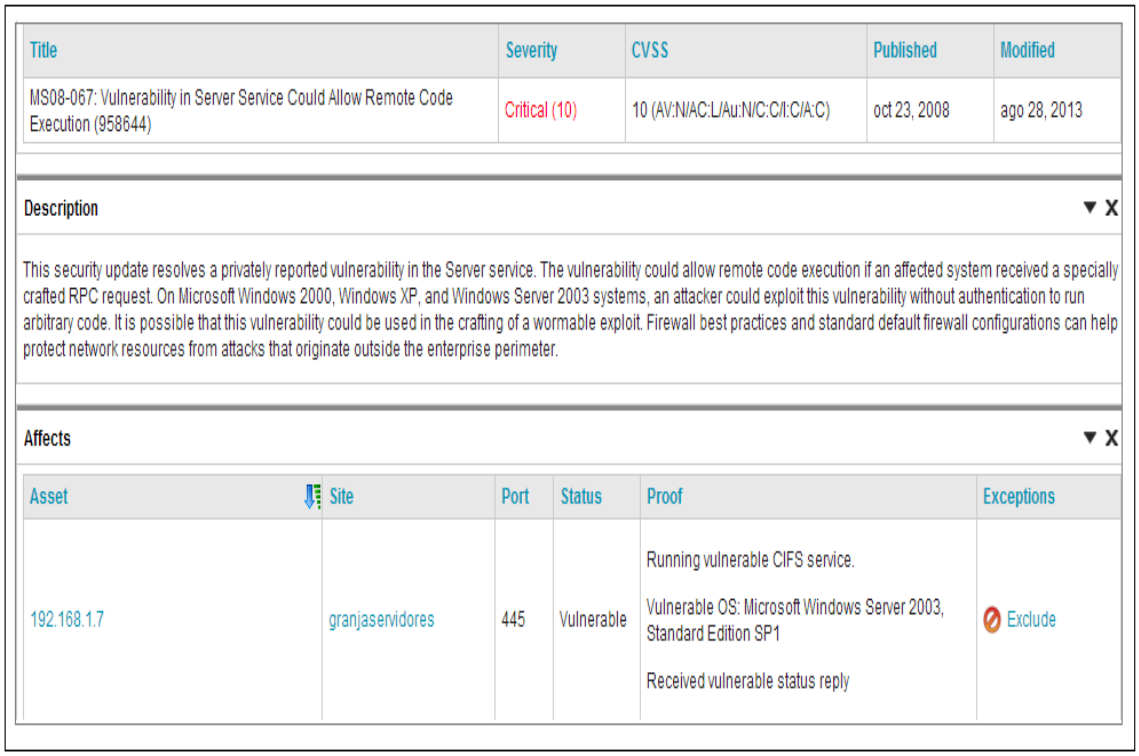
Showing 11 to 20 of 81 | Export to CSV

Gráfico # 37: Información de vulnerabilidades encontradas equipo 192.168.1.8

Fuente: El Autor

Aquí detalla todas las vulnerabilidades encontradas en el equipo en particular, el nombre de la vulnerabilidad también nos indica si existe un malware o exploit conocido para cada una de estas, el riesgo, la fecha de publicación, la severidad, el número de instancias encontradas, etc.

A continuación se detalla la vulnerabilidad MS08_076, una de las más conocidas en sistemas Windows, la cual puede ser explotada mediante Metasploit Framework.



Title	Severity	CVSS	Published	Modified
MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Critical (10)	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	oct 23, 2008	ago 28, 2013

Description

This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter.

Affects

Asset	Site	Port	Status	Proof	Exceptions
192.168.1.7	granjaservidores	445	Vulnerable	Running vulnerable CIFS service. Vulnerable OS: Microsoft Windows Server 2003, Standard Edition SP1 Received vulnerable status reply	Exclude

Gráfico # 38: Detalle vulnerabilidad MS08-067

Fuente: El Autor

La Herramienta Nexpose nos brinda información completa de cada una de las vulnerabilidades encontradas, que incluye una descripción detallada de cada una de éstas, las afectaciones al registro, el listado de exploits y malwares, y el listado de soluciones a seguir para eliminar la vulnerabilidad.

Para obtener un reporte detallado de las vulnerabilidades detectadas por Nexpose, se debe utilizar la herramienta de Reportes, la cual nos brinda algunos tipos de reportes, desde los más completos, hasta reportes gerenciales.

Un Reporte detallado de vulnerabilidades a través de esta herramienta puede llegar a tener más de 500 páginas, lo cual para motivos de estudio se adjunta como un anexo electrónico a este trabajo.

3.5.4 Penetración al sistema

Luego de la fase de escaneo de la red, puertos abiertos y detección de vulnerabilidades a través de la herramienta Nexpose Security, se procederá a realizar el análisis de la vulnerabilidad adecuada para ganar acceso al sistema a través del equipo afectado por la misma.

Como ya se indicó anteriormente, una vulnerabilidad encontrada es la denominada ms08_067_netapi en varios equipos de la red.

Esta vulnerabilidad es una de las más conocidas y explotadas en los equipos afectados alrededor del mundo.

Para realizar un listado más completo de los equipos afectados por la vulnerabilidad mencionada, utilizaremos la herramienta Nmap con el siguiente comando:

":# nmap 192.168.1.0/24 -p445,139,137,135 --script=smb-check-vulns .nse --script-args=unsafe=1 –open > /etc/ms08067netapi.txt",

Esta instrucción indica que se realizará un escaneo nmap a toda la red 192.168.1.0 para buscar vulnerabilidades a través del script smb-check_vulns.nsi en los puertos abiertos 445, 139,137 y 135.

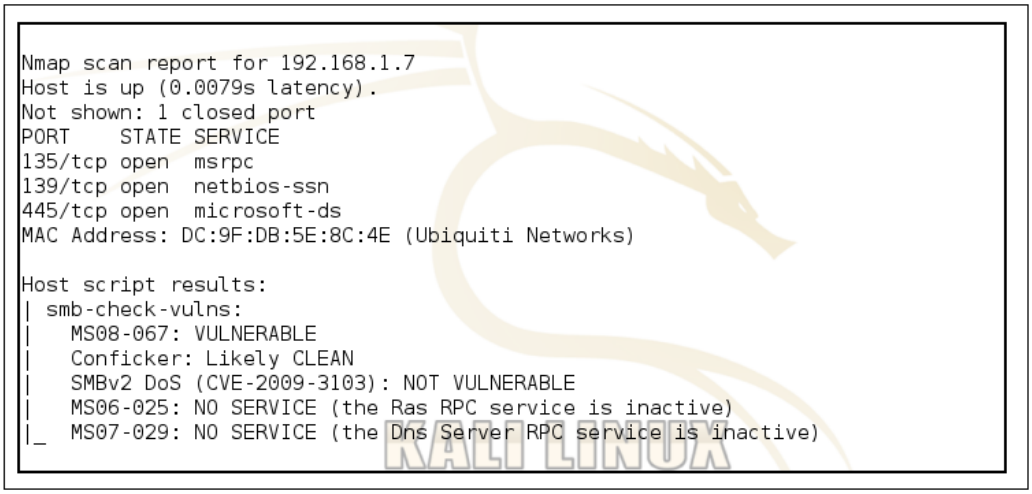


Gráfico # 39: Detección de vulnerabilidad ms08_067_netapi mediante Nmap

Fuente: El Autor

Se pudo verificar que los equipos con dirección IP 192.168.1.7 y 192.168.1.15 mantienen esta vulnerabilidad la misma que puede ser explotada mediante el uso de la herramienta Metasploit incluida en Kali Linux, a la cual se accede mediante el comando : *":# msfconsole".*

3.5.5 Exploit de vulnerabilidades

Para efectuar el exploit de la vulnerabilidad detectada se deberá iniciar el framework Metasploit a través de la instrucción *"# msfconsole"*, una vez iniciado Metasploit se puede visualizar los exploits disponibles mediante el comando ":# show exploits".

De la lista que se muestra, procedemos a buscar la ruta del exploit necesario para la vulnerabilidad MS08_067 el cual se denomina *"Windows/smb//ms08_067_netapi"*, el cual será utilizado para cargar el PAYLOAD "meterpreter/bind_tcp", tal como se observa a continuación:

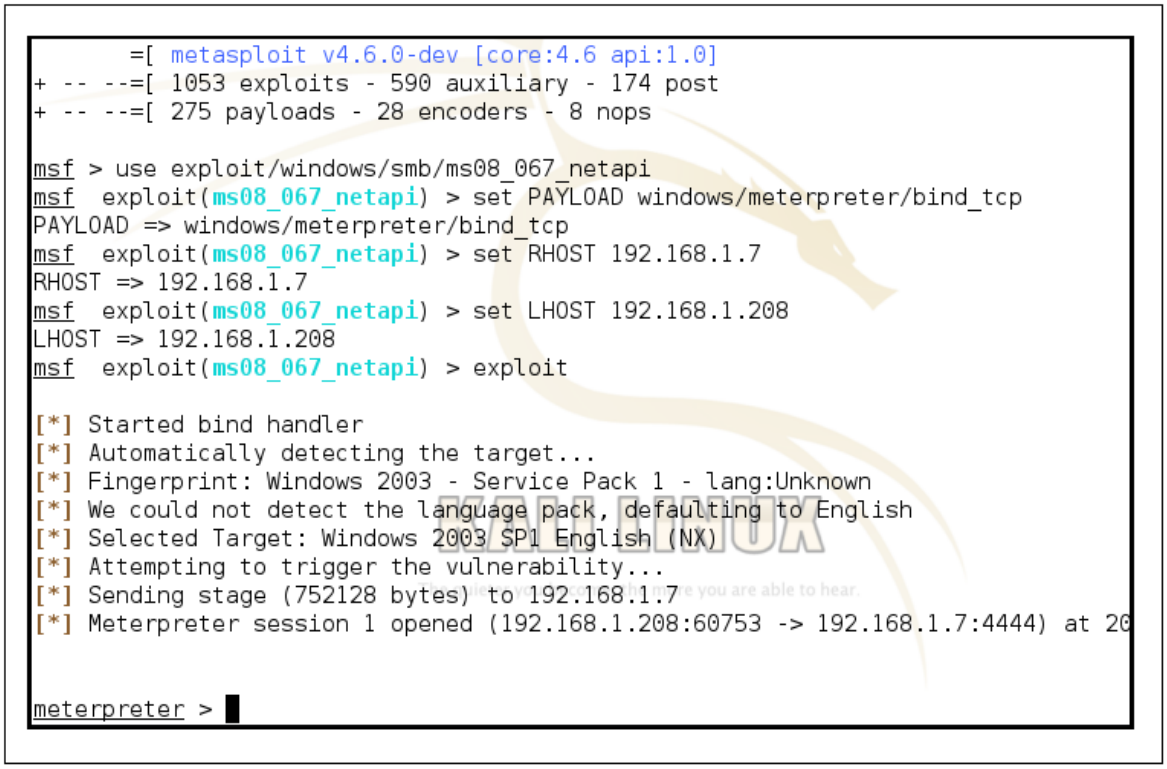


Gráfico # 40: 38 Carga de Exploit y Payload en Metasploit

Fuente: El Autor

El Payload *"meterpreter/bind_tcp"* cargado nos permite establecer una puerta trasera en el equipo a través del cual el atacante puede conectarse y ejecutar comandos para obtener una consola de comandos sobre el equipo atacado, descargarse archivos, migrar procesos, obtener capturas de pantalla de la sesión del usuario del equipo, obtener información de configuración, inclusive apagar remotamente el equipo.

El procedimiento se lo realiza bajo un ambiente controlado ya que el equipo atacado es un servidor de producción.

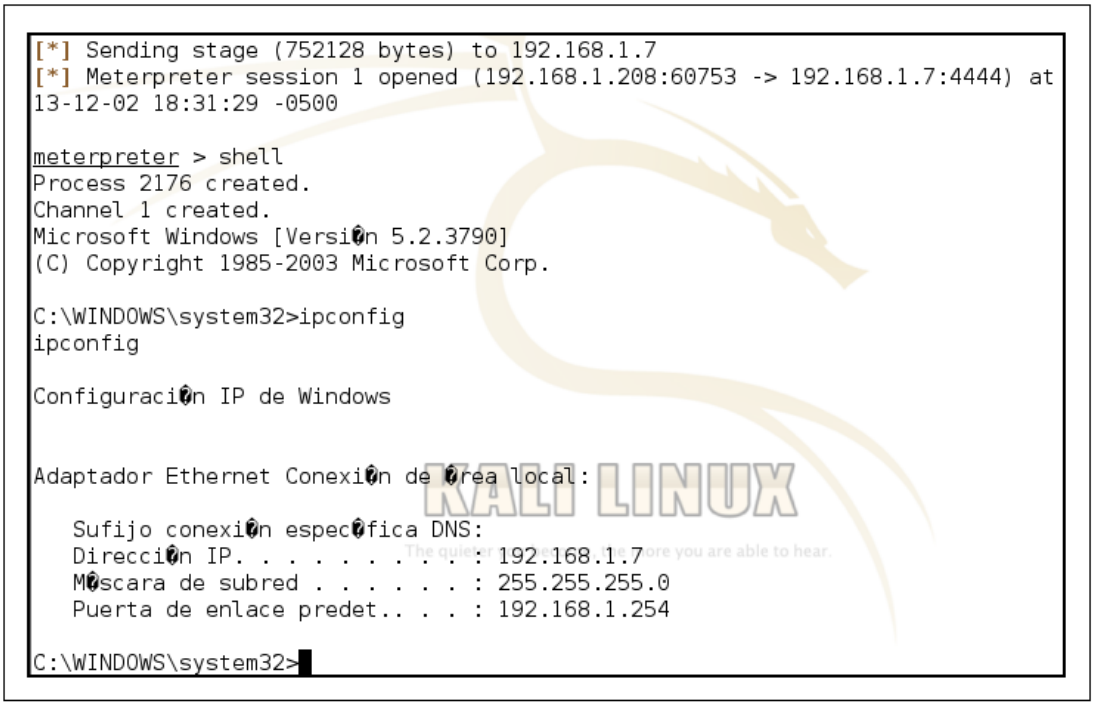


Gráfico # 41: Shell de comandos MS_DOS equipo atacado

Fuente: El Autor

Como se puede observar , el exploit de la vulnerabilidad “ms08_067_netapi” tuvo éxito, porque se pudo obtener una Shell de comandos en la que se puede obtener control total del equipo, cargar y descargar archivos, activar cámaras web y micrófonos, obtener acceso a otros equipos de la red, capturar pantallas, apagarlos, etc. lo cual constituye una gran amenaza a la seguridad de la información.

3.5.6 Ataque por ARP spoofing

Para ejecutar este ataque utilizaremos el comando *“:#arpspoof”* disponible en la suite Kali Linux hacia el equipo víctima de IP 192.168.1.4 y su Gateway de internet 192.168.1.11 de la siguiente manera:

#arpspoof -i eth0 –t 192.168.1.11 192.168.1.4 // (ataque de una vía)

#arpspoof –i eth0 –t 192.168.1.4 192.168.1.11 (ataque de vía contraria)

De esta manera se ha “envenenado” las tablas ARP del equipo atacado y del Gateway con la dirección MAC del equipo atacante, con lo que se logra “introducir un hombre en el medio” o MITM, haciendo que todo el tráfico generado desde el host hacia el Gateway pase primero por el equipo intruso y éste lo retransmita hacia el Gateway y viceversa.

Una forma alternativa para realizar este ataque de una manera más eficiente es utilizando la herramienta Ettercap también disponible en Kali Linux, la cual puede ser invocada mediante siguientes comandos según la necesidad:

#ettercap -T -q -i eth0 –M arp /192.168.1.11/ /192.168.1.4/

#ettercap -T -q -i eth0 –M arp /192.168.100.1/ //

En el primer caso únicamente se “envenena” (ARP poisoning) las tablas ARP de los equipos cuyas direcciones IP son 192.168.1.4 y 192.168.1.11 como en el ejemplo anterior.

En el segundo caso se procede a “envenenar” todos los equipos de ese segmento de red, lo cual resulta poco práctico en un ataque real por cuando se agrega un altísimo tráfico a la red y al equipo atacante ocasionando que la performance de la LAN se vea muy deteriorada lo cual dispararía las “alarmas” a los administradores de red.

Para efectos de este estudio solo se utilizará la primera opción.

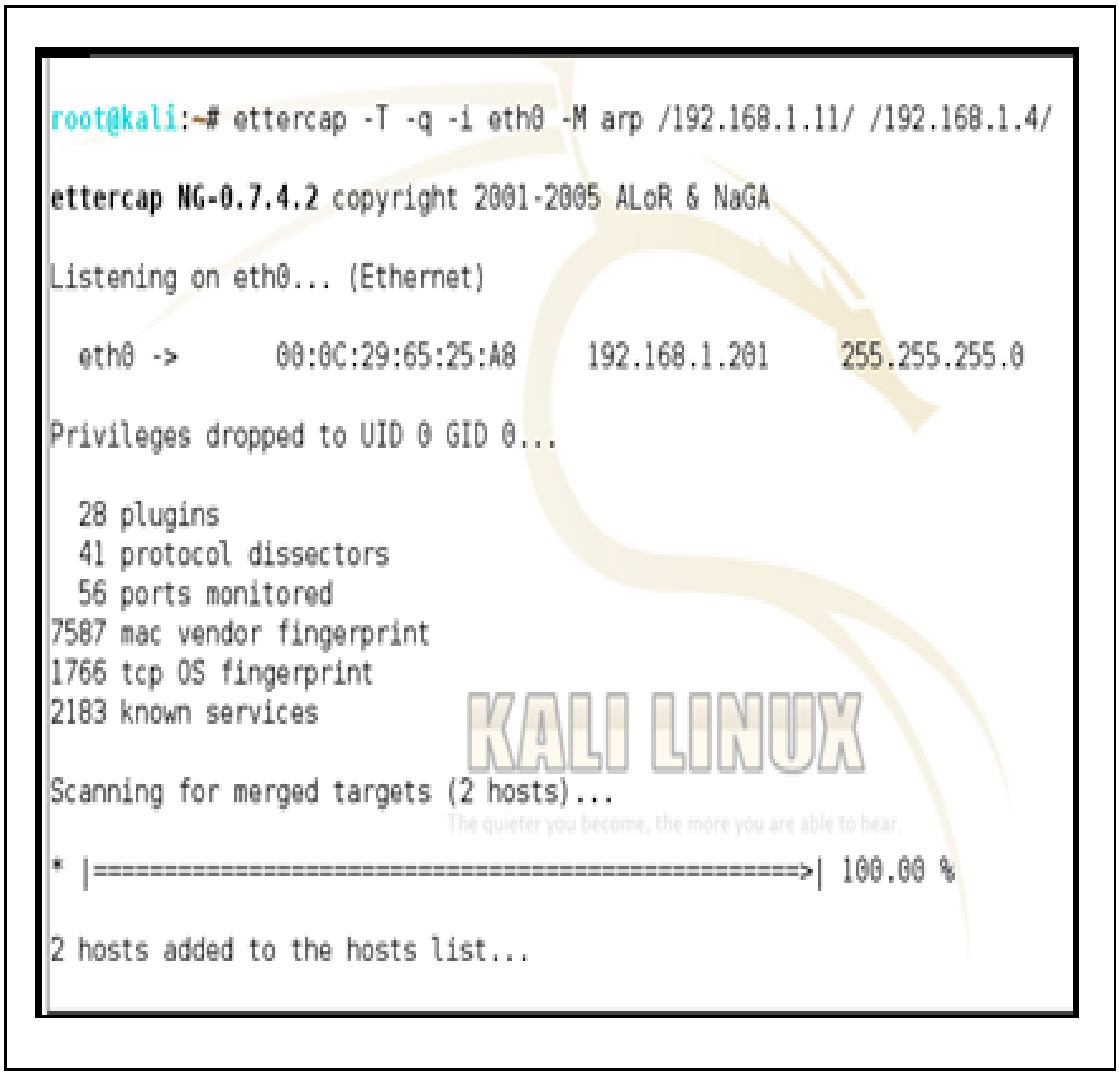


Gráfico # 42: Ejecución de ataque con Ettercap

Fuente: El Autor

Una vez efectuado el ataque, al estar trabajando en un ambiente controlado podemos comprobar que el “envenenamiento” tuvo éxito al comparar las tablas ARP antes y después del ataque en el equipo comprometido.

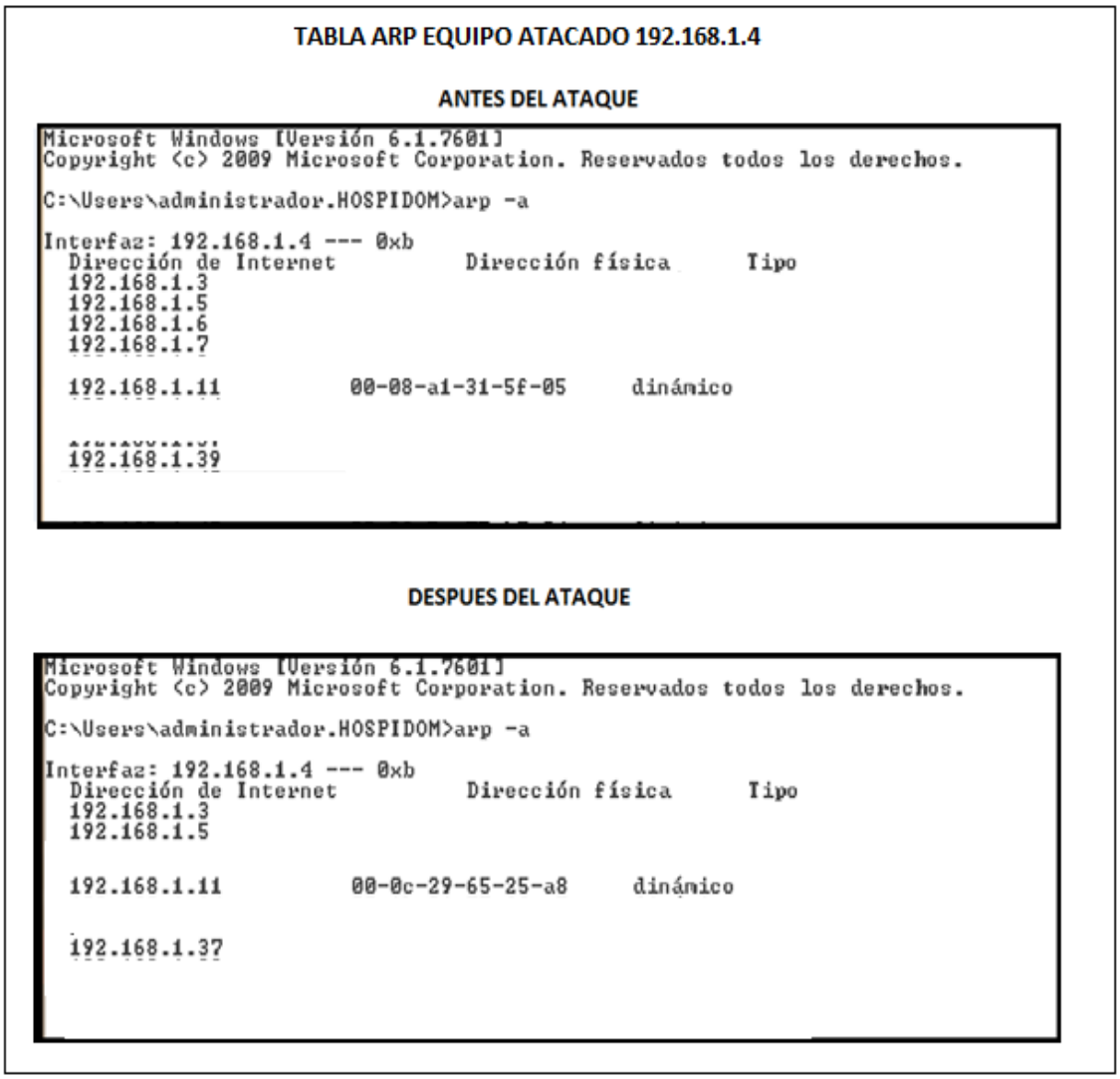


Gráfico # 43: Tablas ARP equipo atacado

Fuente: El Autor

Aquí observamos que la dirección MAC correspondiente a la dirección IP 192.168.1.11 que está asignada al Gateway es diferente antes y después del ataque por ARP spoofing, la primera corresponde a la dirección MAC verdadera de destino y la segunda corresponde a la dirección MAC del equipo atacante. De la misma manera las tablas ARP del Gateway antes y después del ataque serán diferentes.

Una vez realizado el ataque, todos los paquetes que se originen en los equipos comprometidos primero pasarán por el equipo atacante antes de ser re direccionados a su destino con lo cual se posibilita la captura de la información mediante Wireshark.

A continuación se procede a realizar el análisis de paquetes de datos cuyo origen o destino son los equipos atacados, lo cual sería imposible antes del ataque ARP spoofing debido a que un switch crea dominios de colisión diferentes para la comunicación entre pares de equipos por lo tanto esta información no podría ser escuchada por el atacante ya que se encuentra en un dominio de colisión diferente.

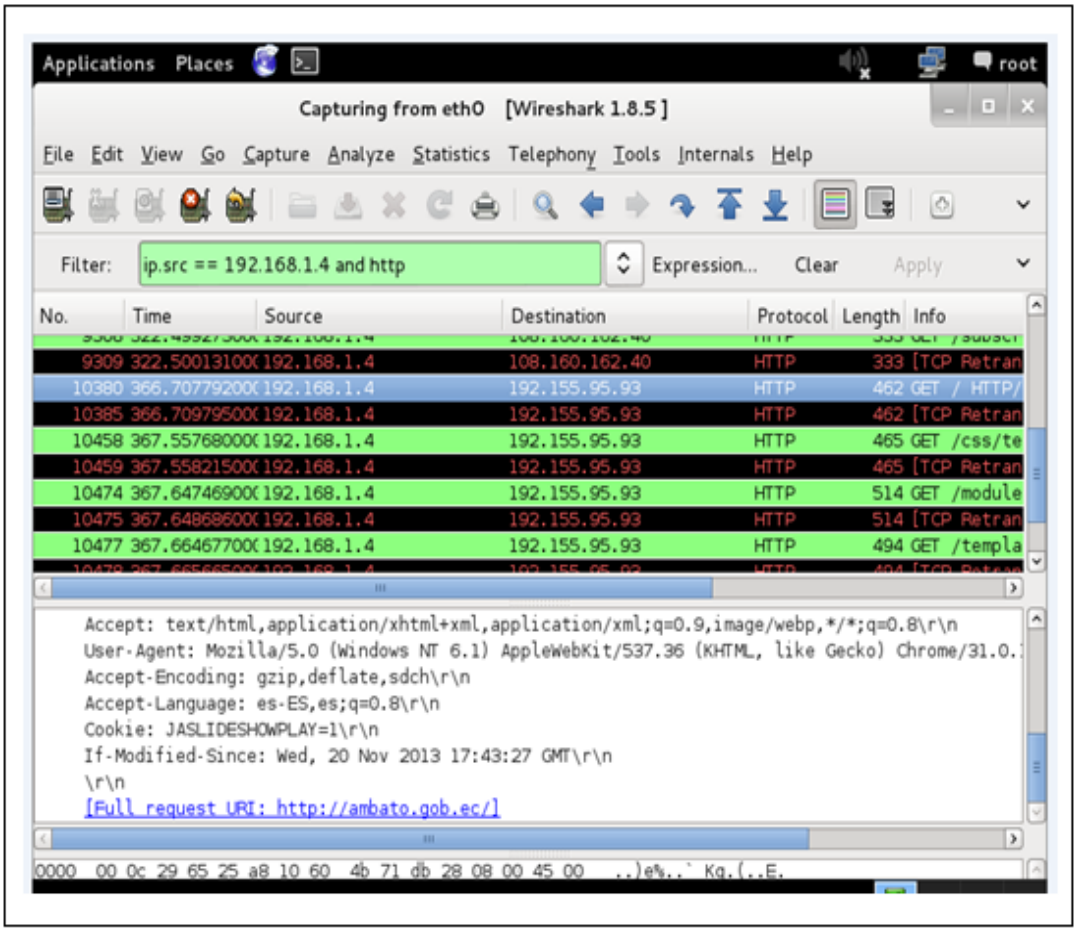


Gráfico # 44: Captura de Paquete HTTP originado en equipo atacado

Fuente: El Autor

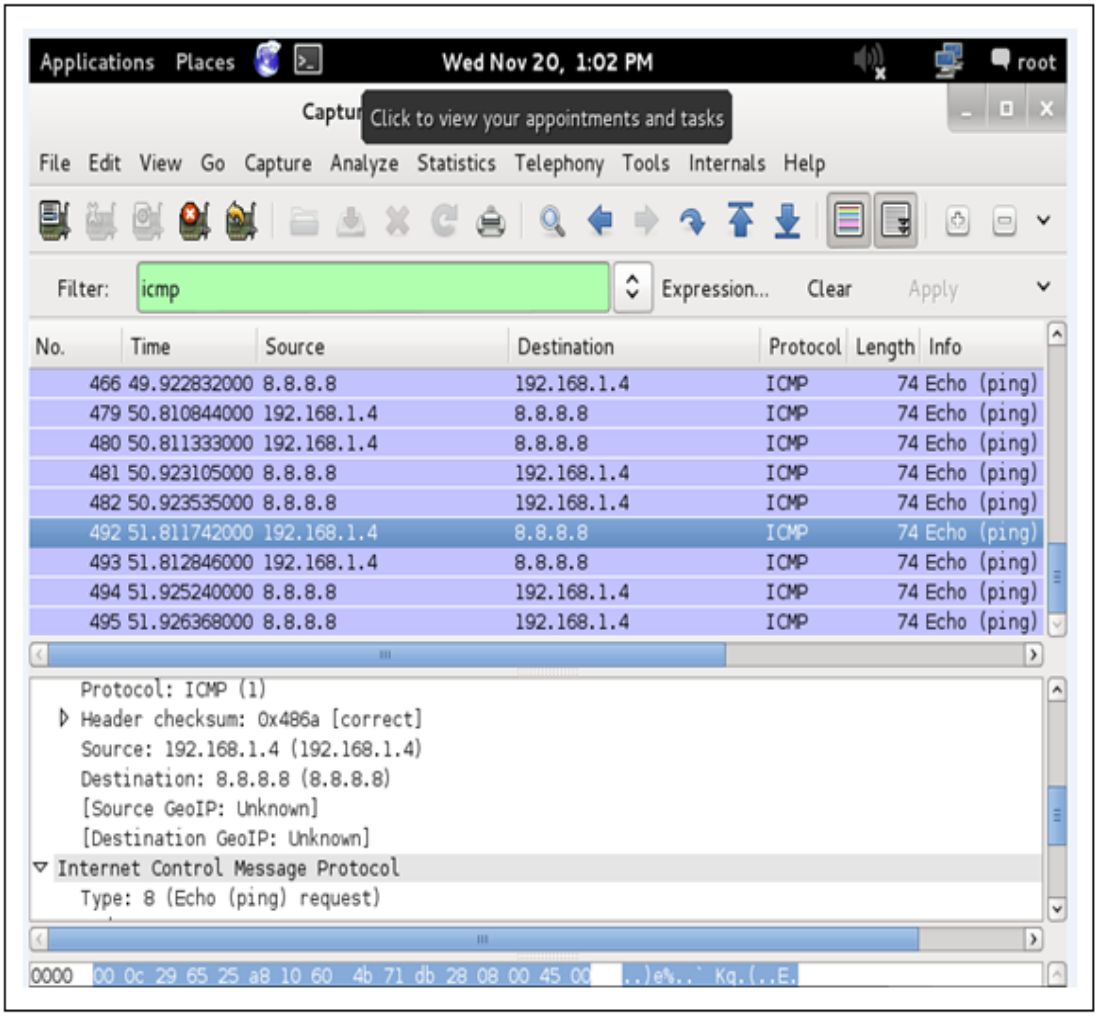


Gráfico # 45: Captura de Paquete ICMP originado en equipo atacado

Fuente: El Autor

Como se puede observar en los gráficos anteriores, se ha capturados dos paquetes de datos cuyo origen fue la IP 192.168.1.4, el primero de ellos un paquete HTTP con una petición hacia el sitio web www.ambato.gob.ec y el segundo paquete correspondía a una petición ICMP hacia la dirección 8.8.8.8, con lo cual se comprueba que el ataque “hombre en el medio” tuvo éxito, al interponer nuestro equipo de ataque entre el computador comprometido y la puerta de enlace seleccionada para el acceso a internet.

3.5.7 Borrado de huellas

Como se pudo observar, los ataques realizados a equipos de la red del Hospital Municipal tuvieron éxito al haberse obtenido acceso a los mismos, cabe indicar que éstos ataque se los realizaron de manera controlada y no se buscaba comprometer la disponibilidad, integridad y confidencialidad de la información almacenada y procesada, por lo que no se generaron rastros que necesiten ser borrados, en el escenario de un atacante real, éste deberá ser lo más cuidadoso posible con la finalidad de evitar ser detectado.

3.6 Políticas de Seguridad Informática

3.6.1 Objetivo general

Mantener segura y legal la red del Hospital Municipal Nuestra Señora de la merced HMNSM.

3.6.2 Objetivos específicos:

Describir todos los mecanismos, normas, políticas y procedimientos a ser implementados para asegurar la red en la Institución.

Difundir al personal las políticas de seguridad adoptadas como modo de protección de la red.

Realizar un seguimiento a los usuarios de la red con el objeto de controlar el cumplimiento de las normas establecidas.

3.6.3 ¿Quién debe leer este documento?

Este documento deberá ser leído por las personas que laboran en el área de TIC's quienes son los encargados de administrar el hardware y software existente en la Institución y todo el personal de otros departamentos que utilicen computadores y consuman servicios de la red al contrario.

Deberá ser difundido a fin de que todos cumplan obligatoriamente con lo estipulado en este manual con el objeto de alcanzar los niveles de seguridad necesarios para preservar el sistema en general.

3.6.4 ¿Quién es el responsable de actualizar este documento?

Deben ser una o varias personas pertenecientes al área de TIC's las encargadas de actualizar este documento, las mismas que deben tener los conocimientos de la estructura y mantenimiento de la red, sujetándose a sugerencias y disposiciones que estén acorde al esquema implantado.

Adicionalmente la actualización de este manual debe ir de la mano conforme avance la tecnología que ayude a encontrar mayores niveles de seguridad.

3.6.5 Normas de seguridad

La presente normativa de seguridad para la red del hospital se basa en las siguientes políticas de aplicación obligatoria:

a) Acceso a los servicios de red.

El personal del HMNSM que necesite trabajar en la red Windows, tendrá asignado un código único de acceso (nombre de usuario) que le permitirá acceder a la red y a los recursos de la misma.

El código de acceso antes mencionado estará compuesto por el nombre del usuario más y la contraseña asignada.

Es imprescindible recalcar que el uso de cada código y clave de usuario será responsabilidad del usuario quien deberá cumplir con la normativa de uso de contraseñas descritas en este manual.

Esta norma aplica a todas las estaciones de trabajo existentes en la Institución.

b) Acceso a los recursos en equipos.

Cada usuario será responsable de permitir el acceso a los recursos (archivos, carpetas, programas e impresoras) que residan en su computador.

El control del acceso a los recursos lo podrá efectuar cada usuario en base al uso de claves de acceso o especificando el/los código(s) de usuario(s) que pueden acceder a algún recurso.

Igualmente es responsabilidad del usuario especificar el nivel de acceso a sus recursos (lectura, total, etc.).

Esta norma aplica para las estaciones de trabajo Windows en sus diferentes versiones.

c) Acceso a internet.

El acceso a Internet está regido por las siguientes normas:

El servicio de Internet debe ser asignado a las personas que de acuerdo a la actividad y requerimientos de su puesto lo necesiten. La información bajada de

Internet debe ser concerniente a las funciones que realiza el HMNSM o se relacionen con la institución.

Cada usuario de internet se le asignará un nombre de usuario y contraseña, controlados por un servidor Proxy, la contraseña de este servicio será personal e intransferible. Toda la actividad de Internet será controlada y registrada por el servidor Proxy.

La seguridad y consecuencias del uso del servicio de internet serán de total responsabilidad del usuario.

d) Uso del correo electrónico

El uso del correo electrónico está regido por las siguientes políticas:

El HMNSM proporciona a todos los usuarios el servicio de correo electrónico institucional a través de un sistema Zimbra propio.

La unidad de TIC´s no dará soporte a cuentas de correo personales.

Los usuarios de correo electrónico están obligados a seguir las siguientes normas:

Está prohibido el envío de correo no solicitado o SPAM. Está prohibido el envío o reenvío de cadenas de correo electrónico a múltiples destinatarios.

Se podrá enviar mensajes no considerados cadenas a un máximo de 20 destinatarios. Si por razones institucionales fuese necesario hacerlo comuníquese con el administrador de la Red.

Está prohibido descargar archivos o abrir enlaces incluidos en correos electrónicos no solicitados, de procedencia dudosa o desconocida. El Sistema no permite la descarga de archivos ejecutables o comprimidos.

El servicio de correo electrónico permite enviar archivos adjuntos por un máximo de 10 Mb.

Cada cuenta de correo tiene asignada una cuota de 250 Mb, la cual podrá ser aumentada de acuerdo a las necesidades del usuario.

Los mensajes enviados y recibitos podrán ser almacenados indefinidamente, salvo los que sean considerados cadenas o SPAM

El servidor de correo electrónico realiza un análisis de virus de los archivos adjuntos, serán eliminados de manera automática cuando se detecte algún tipo de infección

e) Respaldos de la información.

Cada usuario es responsable e independiente de respaldar la información existente en su estación de trabajo y que considere necesario utilizando dispositivos de almacenamiento externo óptico.

Cabe resaltar que no podrá salir fuera de la institución información que se considere como reservada.

El área de TIC´s deberá resguardar los respaldos de la información de los servidores, bases de datos y todos los datos considerados importantes y sensibles que contenga información propiedad del patrimonio del HMNSM en medios ópticos y/o sistemas especializados de almacenamiento o Storage.

Se considerará información propiedad del HMNSM, la siguiente:

Toda la información que se encuentra grabada en los discos duros de los equipos propiedad del patrimonio del HMNSM;

Toda la información que se elaboren, desarrollen, produzcan o construyan en los diferentes departamentos, y en los equipos propiedad del HMNSM;

Toda la información que elaboren, desarrollen, produzcan o construyan los empleados en ejercicio de su función.

f) Protección antivirus

El HMNSM cuenta con un sistema antivirus licenciado, centralizado y actualizado a diario, el cual reside en un servidor acondicionado para el efecto.

Todos los servidores Windows y computadores tendrán instalados el sistema antivirus, el cual se actualizará de manera automática con las imágenes descargadas en el servidor.

Es responsabilidad de cada usuario realizar el análisis de sus unidades externas cuando sean conectadas a los puertos USB de los computadores autorizados.

No utilizar software pirata, aún cuando la copia provenga del adquiriente original del software.

Mantenerse informado respecto a la aparición de nuevos virus.

Adquirir un entorno de seguridad a fin de impedir copias de archivos no autorizadas al disco duro, o ejecución de programas a partir de la unidad de discos flexibles.

Para protegerse contra una invasión viral completa de sus respaldos así como la de los archivos del disco duro, hacer un respaldo global periódico, que deberá conservar en forma indefinida. Sin embargo en varias ocasiones no es suficiente, debiéndose adoptar otro tipo de medidas de precaución.

A continuación se detalla un procedimiento a seguir en caso de infección por virus informático:

- Determinar la máquina en problemas.
- Aislar de la red a la estación de trabajo infectada, con el fin de evitar la propagación del virus.
- Suprimir los archivos que no puedan ser desinfectados por el sistema.
- Si el virus se ha extendido, elimínelo reconstruyendo su disco duro o ejecutando un programa de utilería que pueda (óptimamente) eliminarlo.

Adopte prácticas para proteger de cualquier infección sus discos flexibles, y especialmente discos o cintas de respaldo.

Está restringido mediante bloqueo en registro de Windows el uso de unidades de almacenamiento externo. Solo serán desbloqueados los equipos de usuario que, por razones de trabajo lo necesiten. Para realizar el desbloqueo de unidades externas, el usuario interesado deberá realizar una solicitud sustentada.

g) Normas sobre el uso de contraseñas.

El ingreso de los usuarios a los servicios de la Red se controla en base a un Nombre de Usuario y contraseña controlado por un servidor de Active Directory.

El personal con acceso a los servicios de red deberán observar obligatoriamente las siguientes normas generales.

La contraseña entregada a cada usuario es personal e intransferible

La contraseña deberá ser cambiada cada 42 días. El sistema le notificará la proximidad del vencimiento de la contraseña

La contraseña deberá ser lo suficientemente larga y compleja para no ser descifrada

Las contraseñas cumplirán con los siguientes parámetros definidos en la política de contraseñas de Active Directory:

Longitud mínima 10 caracteres y máximo 40 caracteres.

Las contraseñas deberán contar con al menos un carácter de los cuatro grupos siguientes:

- Letras minúsculas (a,b,c,d…..)
- Letras mayúsculas (A,B,C,D…)
- Números (0,1,2,3,4….)
- Símbolos ($,@,-,%,……)

La nueva contraseña deberá ser distinta a las cinco últimas contraseñas utilizadas y no podrá contener el nombre de usuario.

h) Perfiles de usuario

Los usuarios del HMNSM serán de dos tipos:

- Usuarios Estándar
- Usuarios Administradores.

Un usuario estándar podrá realizar uso de los recursos de red establecidos en las políticas de usuario de Active Directory.

Los Usuarios estándar no podrán:

- Instalar aplicativos en el computador.
- Cambiar las configuraciones del Sistema Operativo
- Escribir o modificar archivos en las carpetas que no se encuentren dentro de su respectivo escritorio o “Mis Documentos”.
- Administrar remotamente otros equipos

Solo se asignará usuarios administradores al personal especializado del Área de TIC´s.

i) Instalación de software.

El control sobre la instalación de software es responsabilidad del Área de TIC´s. Todo el software instalado en el HMNSM deberá contar con licencia su licencia respectiva.

Se deberá determinar las necesidades para la instalación de Software en los computadores del HMNSM, para el efecto se deberá realizar usa solicitud sustentada sobre la necesidad de instalar un aplicativo específico.

El Área de TIC´s realizará de forma periódica un inventario de aplicaciones instaladas en los computadores de la institución, para lo cual deberá utilizar herramientas informáticas especializadas para el efecto.

De ser detectado software que no cuente con el respectivo licenciamiento se deberá desinstalarlo inmediatamente, de ser imprescindible el uso de determinado software se deberá iniciar con el proceso de legalización previo un análisis que lo sustente.

j) Acceso a los centros de datos

Los servidores se alojan en los dos centros de datos implementados en áreas separadas dentro del el edificio Institucional.

Las instalaciones físicas del HMNSM están protegidas por una empresa de seguridad 24 horas al día, los centros de datos cuenta con alarmas de seguridad e incendios y vigilancia por video.

El centro de servidores se mantiene permanentemente cerrado y su acceso es controlado por el coordinador TIC´s.

Los accesos a los centros de datos están protegidos por puertas con controles electrónicos.

k) Seguridad lógica

La red informática del HMNSM cuenta con un Sistema Appliance de Seguridad perimetral Firewall, que en conjunto con los procedimientos de seguridad internas, protege la red interna de cualquier acceso no autorizado desde Internet.

El administrador de TIC´s, entregará en un sobre cerrado a la Gerencia del HMNSM el catálogo completo de nombres de usuarios y contraseñas que permitan el acceso y configuración de todos los servicios, servidores y equipos activos de la red, este sobre deberá se mantendrá en una bóveda de seguridad de algún banco y ser abierta únicamente en caso de ausencia no prevista del/los responsables del Área de TIC´s, previa autorización expresa de la gerencia.

3.7 Guía de corrección de vulnerabilidades detectadas.

3.7.1 Vulnerabilidades de Diseño de la red

DESCRIPCION	ESTADO ACTUAL	CORRECCION
Interconexión con Red GADMA	Sin sistema perimetral de seguridad firewall	Implementar Sistema Perimetral de seguridad Firewall para la interconexión con la red del GADMA,

Interconexión con Red GADMA	Enlace WiFi banda libre 5.4 Ghz.	Planificar el reemplazo de la tecnología de comunicaciones en banda libre por tecnología de fibra óptica propietaria o contratada hacia el nuevo edificio municipal.
Servidor de Correo electrónico	Expuesto al internet fuera del perímetro de seguridad	Disponer el servidor de correo electrónico dentro de un perímetro del perímetro de seguridad del firewall
Router de Frontera	Sistema Primario de Seguridad desactivado	Configurar sistema primario de seguridad según las opciones del Router de Balance de Carga TP-LINK dispuesto en la frontera con el internet
VLANS IEEE802.1q	Todos los equipos están dispuestos en una única VLAN	Segmentar la red interna del Hospital en varias VLAN, según su criticidad, sensibilidad y disposición física

Tabla # 4: Corrección de vulnerabilidades de diseño de la Red

Fuente: El Autor

3.7.2 Vulnerabilidades en el Software de los equipos de cómputo

EQUIPO	TIPO	VULNERABILIDAD	CORRECCION
PROXY	SISTEMA OPERATIVO	Sistema Operativo Linux desactualizado	Solicitar actualización del sistema operativo al proveedor del Appliance Netcyclon
DESARROLLO	SISTEMA OPERATIVO	Sistema Operativo Windows 7 desactualizado	Instalar último Service Pack y boletines de seguridad publicados por Microsoft Corp.
DESARROLLO	APLICACIONES	Aplicaciones JAVA, Oracle, Ms_Office desactualizadas	Instalar últimas versiones disponibles, y boletines publicadas por Microsoft Corp.para Ms_office

DESARROLLO	CONFIGURACION	Firewall desactivado	Activar firewall y configurar reglas de confianza
ANTIVIRUS SERVER	SISTEMA OPERATIVO	Sistema Operativo Windows 7 desactualizado	Instalar último Service Pack y boletines de seguridad publicados por Microsoft Corp.
ACTIVE DIRECTORY SERVER	SISTEMA OPERATIVO	Sistema Operativo Windows 2003 Server Obsoleto	Migrar Sistema Operativo y Active Directory a la última versión de Windows 2008 Server, con el último sevicepack y boletines de seguridad publicados por Microsoft Corp.
DB SERVER	SISTEMA OPERATIVO	Sistema Operativo Windows 2008 Server desactualizado	Instalar último Service Pack y boletines de seguridad publicados por Microsoft Corp.
DB SERVER	CONFIGURACION	Firewall desactivado	Activar firewall y configurar reglas de confianza
MAIL SERVER	SISTEMA OPERATIVO	Sistema Operativo Linux Centos 6 64 bits Desactualizado	Realizar actualización mediante ***yum update***
EQUIPOS USUARIOS	SISTEMA OPERATIVO	Sistemas operativos Desactualizado u obsoletos	Actualizar Sistemas operativos con soporte vigente de Microsoft Corp, Migrar sistemas Operativos obsoletos.
EQUIPOS USUARIOS	APLICACIONES	Aplicaciones desactualizadas	Instalar últimas versiones disponibles de aplicativos con licencia, dar de baja o reemplazara aplicativos sin licencia por aplicativos libres
EQUIPOS USUARIOS	CONFIGURACION	Firewall desactivado	Activar firewall y configurar reglas de confianza

Tabla # 5: Corrección de vulnerabilidades de Software de la Granja de Servidores

Fuente: El Autor

CAPITULO IV

ANALISIS Y VALIDACION DE RESULTADOS

Para el análisis de los resultados obtenidos en este estudio, se los ha divido en tres áreas:

- Análisis de los datos obtenidos en las Encuestas
- Análisis de datos de la Honeynet
- Análisis de resultados de la Prueba de Penetración

4.1 Resultados de las encuestas

La encuesta aplicada tuvo como finalidad obtener ciertos patrones generales de conducta informática de los usuarios en áreas como gestión de contraseñas, uso del internet, correo electrónico y seguridad lógica del computador asignado.

Una vez revisados los resultados, en términos generales los usuarios mantienen buenas prácticas de seguridad en la mayoría de temas consultados, sin embargo surgieron datos interesantes respecto a prácticas no seguras en los siguientes que se describen a continuación:

Únicamente el 28% de los encuestados cambia sus contraseñas en períodos aceptables (semanal, mensual), un elevado porcentaje (68%) lo hace de manera eventual y un 14% nunca cambia su contraseña.

Un porcentaje importante de usuarios (31%) almacena sus usuarios y contraseñas en algún medio físico o virtual.

Un porcentaje importante de usuarios (28%) ha compartido eventualmente las contraseñas de de sus cuentas de servicios informáticos con compañeros de trabajo o familiares.

Un porcentaje importante de usuarios (22%) acepta la instalación de actualizaciones automáticas o software sugerido en sitios de internet.

Un porcentaje considerable de usuarios (36%) utiliza unidades de almacenamiento externo en los computadores de la Institución.

Un porcentaje elevado de Usuarios (42%) no bloquea su equipo de cómputo cuando abandona eventualmente su estación de trabajo.

De los resultados presentados, se puede observar que existen ciertas conductas informáticas que deberán ser normadas mediante la aplicación del instructivo de seguridad descrito en el presente trabajo.

4.2 Resultados de la honeynet

Una vez que fue puesta en marcha la Honeynet con la finalidad de registrar los posibles intentos ataques a la infraestructura de red, se procedió a comprobar la funcionalidad del mismo realizando varias pruebas de penetración de manera local y controlada con la utilización de Kali Linux.

Inicialmente se realizó un escaneo de puertos como fase inicial de reconocimiento de la Infraestructura con la herramienta Nmap, lo que nos permitió determinar que la infraestructura se encuentra funcionando de acuerdo a lo previsto, es decir la presencia del Honeypot cuya dirección IP es 10.0.0.20 con sus servicios en funcionamiento, tal como se muestra a continuación:

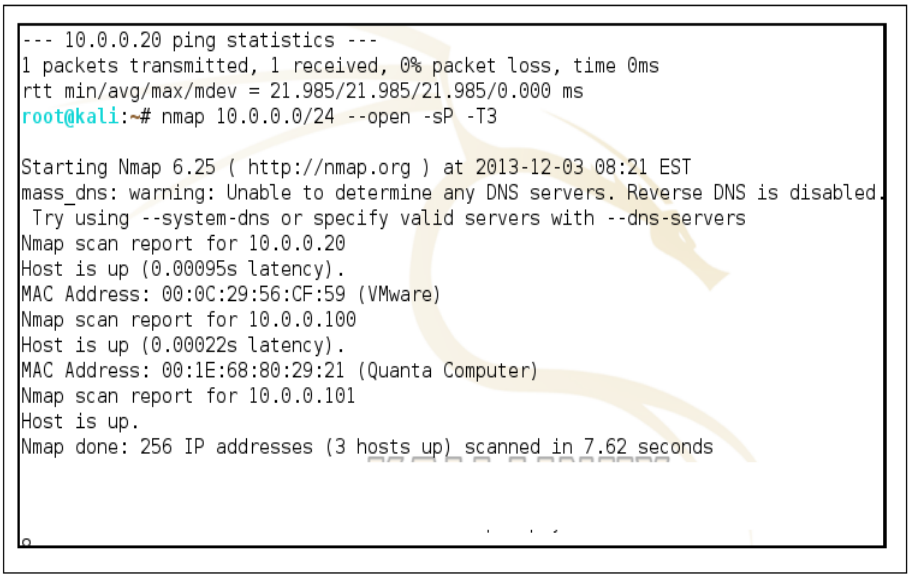


Gráfico # 46: Escaneo Nmap de la Honeynet en producción

Fuente: El Autor

Además se realizó un escaneo Nmap para detectar la vulnerabilidad MS08_067 en los equipos de la Honeynet, tal como se muestra a continuación:

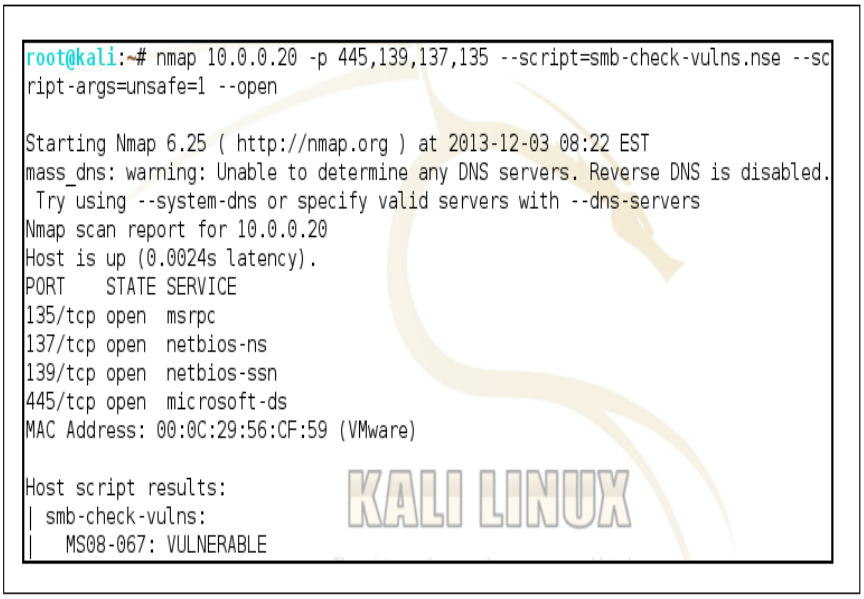


Gráfico # 47: Detección de vulnerabilidad MS08_067 en la Honeynet

Fuente: El Autor

Una vez que se simuló los ataques anteriores, se procede a revisar el analizador de datos del Honeywall a través de su consola de administración.

En el Gráfico # 48 se puede observar la estadística de la actividad capturada.

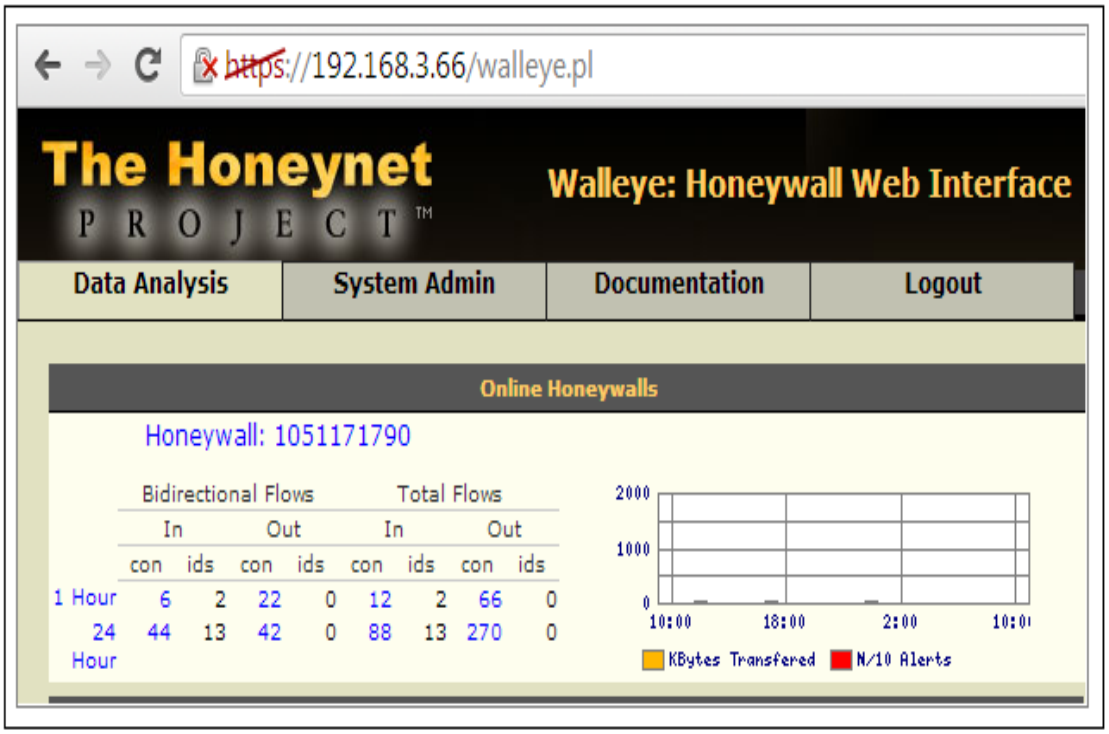


Gráfico # 48: Estadísticas de la Actividad en el Honeywall

Fuente: El Autor

Se puede observar que el honeywall ha registrado actividad de entrada y de salida y en diferentes horarios.

En la consola general en la sección ***Online Honeywalls,*** se procede a seleccionar el sensor “Honeywall: 105117190” para visualizar de manera detallada la actividad capturada por el IDS, los datos se presentan de manera histórica agrupados en rangos de 1 Hora, 24 Horas y por Fechas

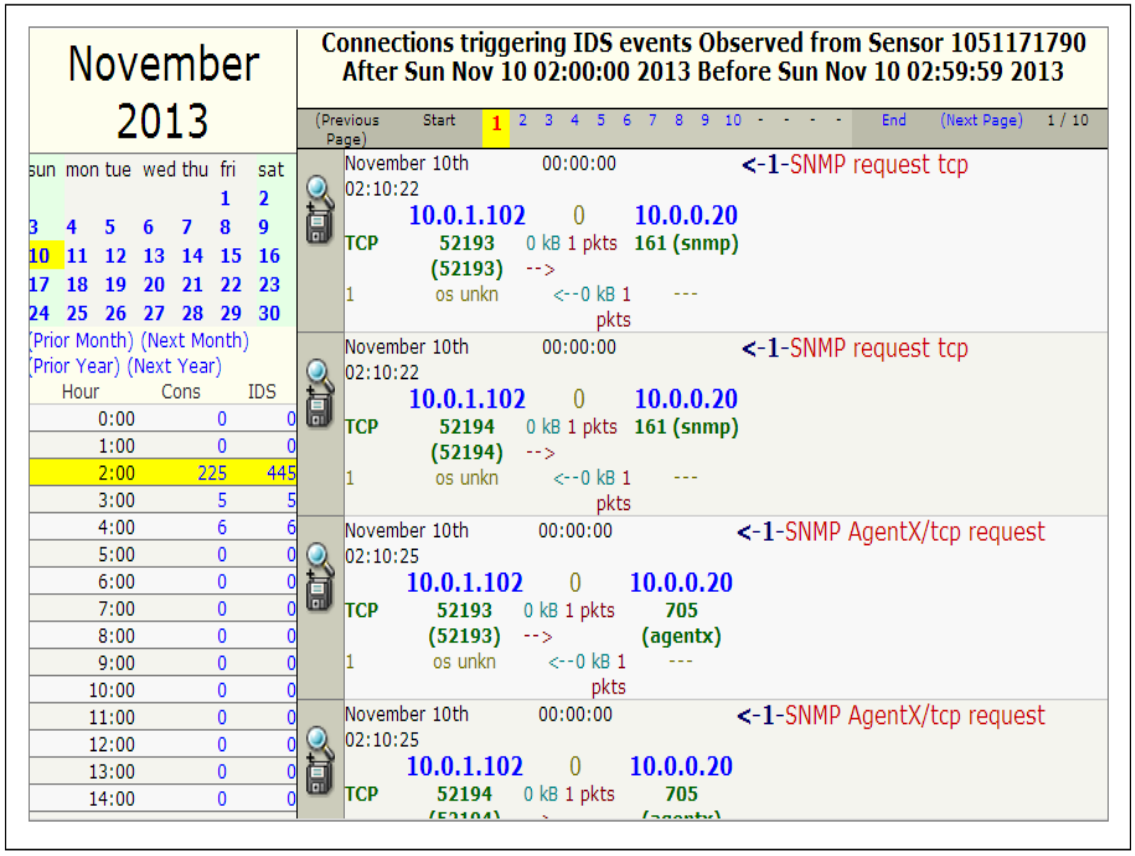


Gráfico # 49: Información capturada por el Honeywall

Fuente: El Autor

En la figura anterior, se puede observar la actividad capturada por el IDS el domingo 10 de noviembre, la cual corresponde a paquetes SNMP generados por el escaneo de puertos realizado con Nmap.

A continuación se realizó un ataque HTTP FLOOD con la herramienta LOIC hacia el servidor web del honeypot. La herramienta LOIC genera un flujo de peticiones HTTP simultáneas hacia el servidor seleccionado con la finalidad de provocar una denegación de servicios DoS por saturación del servidor web atacado.

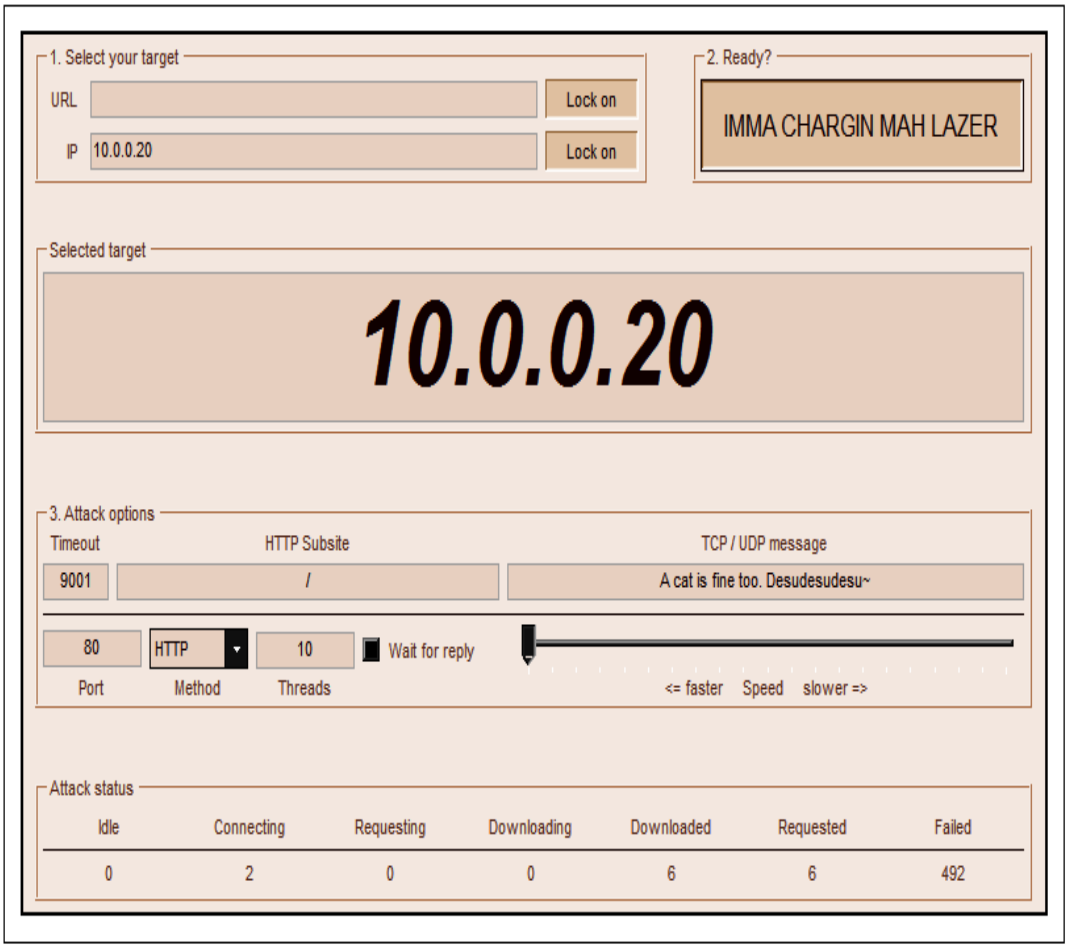


Gráfico # 50: Ataque HTTP-Flood al Honeypot

Fuente: El Autor

Como se observa, LOIC realizó múltiples peticiones http, de las cuales se obtuvo únicamente 6 respuestas y 492 resultaron fallidas, esta prueba tuvo una duración de apenas 30 segundos.

Para complementar las pruebas realizadas, desde una ventana de comando se realiza una petición DNS al servidor simulado en el honeypot mediante el comando ***nslookup*** con el que iniciamos una sesión en el servidor consultado, tal como se muestra a continuación

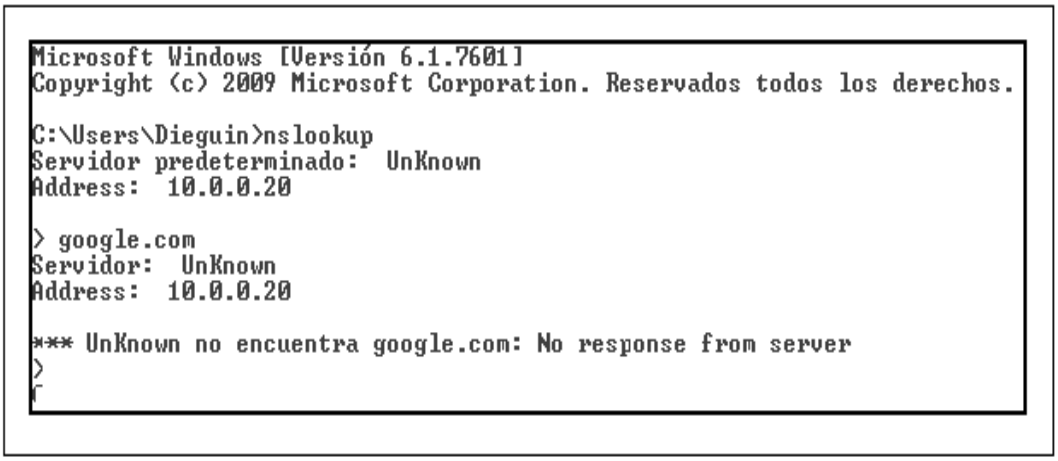


Gráfico # 51: Peticiones DNS y FTP al Honeypot

Fuente: El Autor

La información de los ataques y peticiones realizadas fue capturada por el Honeywall tal como se puede observar a continuación:

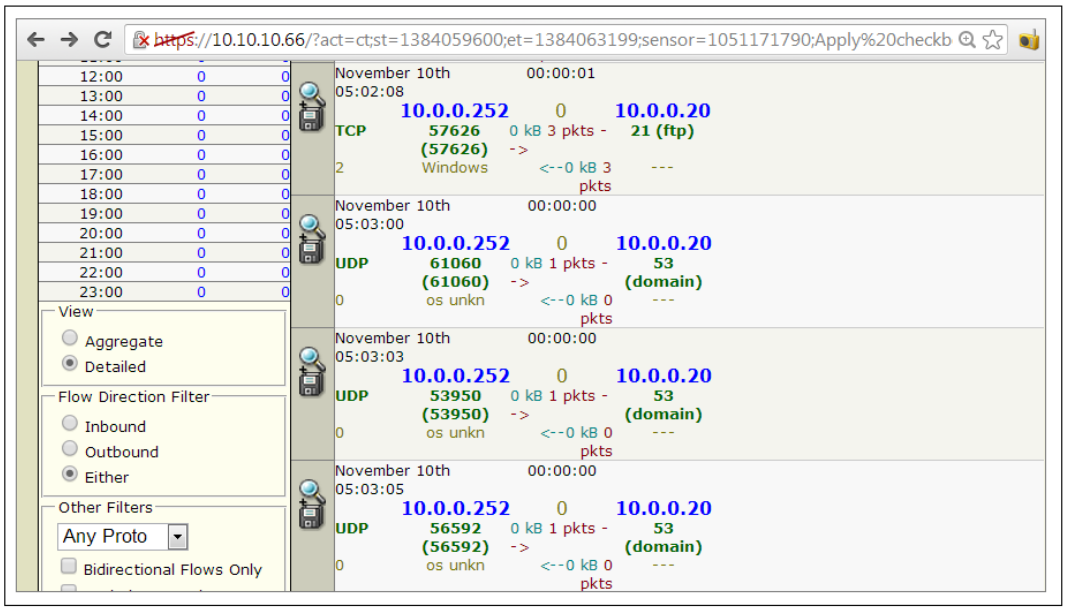


Gráfico # 52: Paquetes DNS capturados por el Honeywall

Fuente: El Autor

4.3 Resultados de la prueba de penetración

Durante las prueba de penetración realizada a la Red del Hospital se detectó que existen varios tipos de vulnerabilidades respecto al Software en los Equipos de cómputo de la red del Hospital, las mismas que afectan tanto al Sistema Operativo como a los aplicativos instalados.

Los ataques perpetrados durante la prueba de penetración tuvieron éxito gracias a la disposición de todos los equipos de cómputo en una única VLAN, lo que inicialmente facilitó el escaneo inicial, además se detectó que los sistemas firewall de la mayoría de computadores se encontró deshabilitado.

Debido a que el análisis de vulnerabilidades de Software fue realizado con la herramienta Nexpose Security en su versión comunitaria la cual limita el número de Tareas permitidas, se procedió a seleccionar un conjunto representativo de Equipos de cómputo compuesto por todos los Servidores Institucionales y varios computadores de la red de producción del Hospital los mismos que mantienen configuraciones similares con los equipos no seleccionados.

Las vulnerabilidades del software instalado en los diferentes equipos de cómputo detectadas se encuentran clasificadas según la criticidad de las mismas en críticas, severas, moderadas y advertencias.

Las vulnerabilidades críticas detectadas en el servidor principal de Base de Datos DBSERVER se describen en la siguiente tabla:

.

VULNERABILIDAD	EXPLOIT DISPONIBLE	NIVEL
IP Source Routing Enabled		**Critical**
Missing Oracle Critical Patch Update (CPU) for October 2009	**metasploit**	**Critical**

MS11-078: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2604930)		**Critical**
MS13-029: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution (2828223)		**Critical**
MS13-037: Cumulative Security Update for Internet Explorer (2829530)	**metasploit**	**Critical**
MS13-038: Security Update for Internet Explorer (2847204)	**metasploit**	**Critical**
MS13-040: Vulnerabilities in .NET Framework Could Allow Spoofing (2836440)		**Critical**
MS13-047: Cumulative Security Update for Internet Explorer (2838727)		**Critical**
MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution (2861561)		**Critical**
MS13-053: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2850851)	**metasploit**	**Critical**
MS13-054: Vulnerability in GDI+ Could Allow Remote Code Execution (2848295)		**Critical**
MS13-059: Cumulative Security Update for Internet Explorer (2862772)	**metasploit**	**Critical**
MS13-062: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)		**Critical**
MS13-063: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2859537)		**Critical**
MS13-069: Cumulative Security Update for Internet Explorer (2870699)		**Critical**
MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)		**Critical**

Tabla # 6: Vulnerabilidades Críticas Servidor de Base de Datos DBSERVER

Fuente: El Autor

A continuación se describen las vulnerabilidades críticas detectadas en el servidor de Active Directory ACTDIRSERVER del Hospital

VULNERABILIDAD	EXPLOIT DISPONIBLE	NIVEL
IP Source Routing Enabled		**Critical**
KB2607712: Fraudulent Digital Certificates Could Allow Spoofing		**Critical**
KB2718704: Unauthorized Digital Certificates Could Allow Spoofing		**Critical**
Microsoft DirectShow Streaming Video ActiveX Control Buffer Overflow	**metasploit**	**Critical**
MS05-026: Vulnerability in HTML Help Could Allow Remote Code Execution (896358)		**Critical**
MS05-051: Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (902400)	**exploitdb**	**Critical**
MS06-002: Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution (908519)		**Critical**
MS06-015: Vulnerability in Windows Explorer Could Allow Remote Code Execution (908531)	**exploitdb**	**Critical**
MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159)	**metasploit**	**Critical**
MS06-036: Vulnerability in DHCP Client Service Could Allow Remote Code Execution (914388)	**exploitdb**	**Critical**
MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883)	**metasploit**	**Critical**
MS06-050: Vulnerabilities in Microsoft Windows Hyperlink Object Library Could Allow Remote Code Execution (920670)	**exploitdb**	**Critical**
MS06-057: Vulnerability in Windows Explorer Could Allow Remote Execution (923191)	**metasploit**	**Critical**

MS06-063: Vulnerability in Server Service Could Allow Denial of Service and Remote Code Execution (923414)	**metasploit**	**Critical**
MS06-066: Vulnerabilities in Client Service for NetWare Could Allow Remote Code Execution (923980)	**metasploit**	**Critical**
MS07-008: Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution (928843)		**Critical**
MS07-020: Vulnerability in Microsoft Agent Could Allow Remote Code Execution (932168)		**Critical**
MS07-034: Cumulative Security Update for Outlook Express and Windows Mail (929123)	**exploitdb**	**Critical**
MS07-046: Vulnerability in GDI Could Allow Remote Code Execution (938829)		**Critical**
MS07-068: Vulnerability in Windows Media File Format Could Allow Remote Code Execution (941569 and 944275)		**Critical**
MS08-007: Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution (946026)		**Critical**
MS08-021: Vulnerabilities in GDI Could Allow Remote Code Execution (948590)	**exploitdb**	**Critical**
MS08-028: Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution (950749)		**Critical**
MS08-046: Vulnerability in Microsoft Windows Image Color Management System Could Allow Remote Code Execution (952954)	**exploitdb**	**Critical**
MS08-049: Vulnerabilities in Event System Could Allow Remote Code Execution (950974)		**Critical**
MS08-063: Vulnerability in SMB Could Allow Remote Code Execution (957095)		**Critical**
MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	**metasploit**	**Critical**
MS08-076: Vulnerabilities in Windows Media Components Could		**Critical**

MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	**metasploit**	**Critical**
MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)		**Critical**
MS09-013: Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803)		**Critical**
MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)	**exploitdb**	**Critical**
MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	**metasploit**	**Critical**
MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)	**metasploit**	**Critical**

Tabla # 7: Vulnerabilidades críticas del Servidor Active Directory ACTDIRSERVER

Fuente: El Autor

4.4 Validación de la hipótesis

Una vez que han sido aplicadas las herramientas Honeypot, se procedió a realizar pruebas de penetración sobre los sistemas, toda esta actividad que fue controlada, capturada y recolectada por el Honeywall.

Algunos de los paquetes TCP capturados que tienen como origen la dirección IP 95.211.217.215 generados desde un equipo ubicado en Holanda (iplocation.net, 2013) como se demuestra en el Gráfico #54, datos que indican que Snort disparó la alerta ***WEB-PHP Setup.php Access*** por el intento de explotar la vulnerabilidad conocida como ***MediaWiki MediaWiki-stable 20031107*** (aldeid.com, 2010).

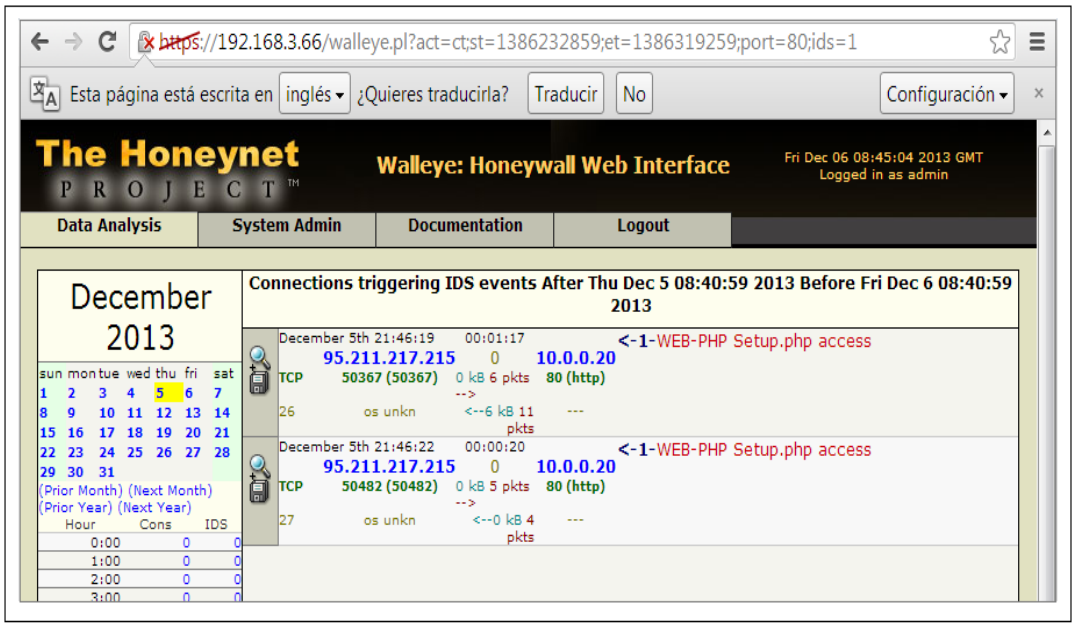


Gráfico # 53: Paquetes TCP capturados ataque desde 95.211.217.215

Fuente: El Autor

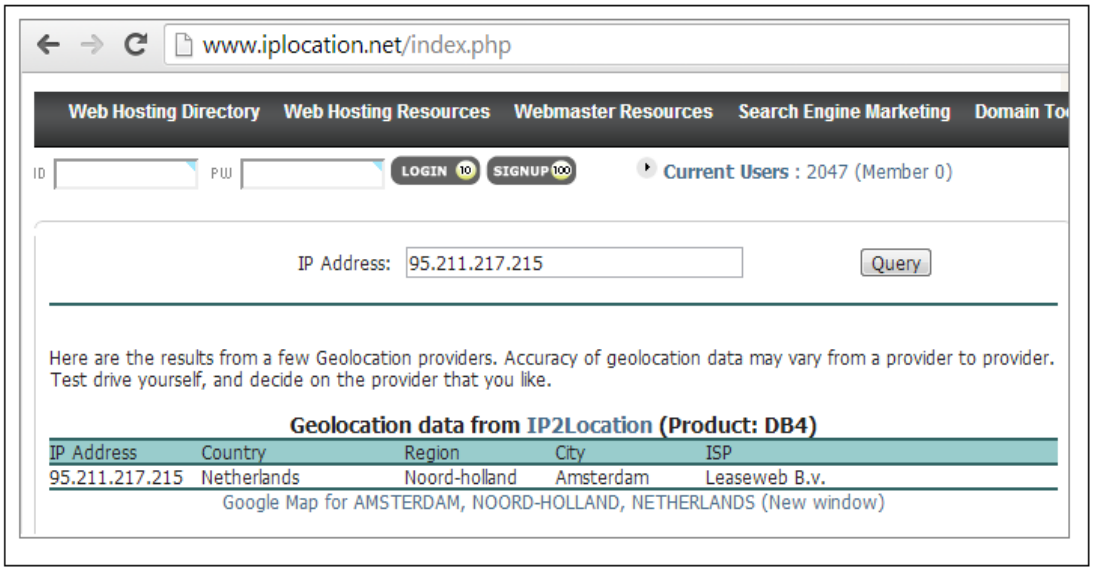


Gráfico # 54: Localización dirección IP del atacante

Fuente: www.iplocation.net

A continuación se puede apreciar la actividad registrada en el Honeypot, que corresponde al ataque registrado, además de otros ingresos no considerados ataques por Snort.

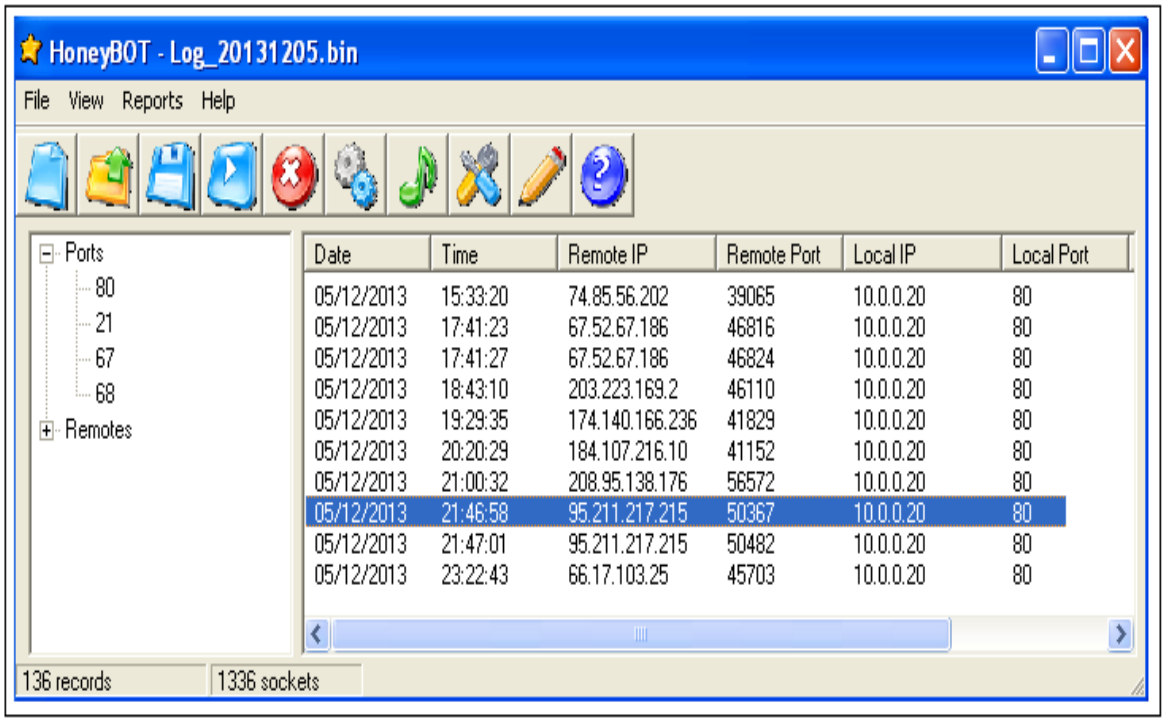


Gráfico # 55: Actividad registrada en el Honeypot

Fuente: El Autor

Finalmente se muestra el resumen de la actividad capturada a través de paquetes SEBEK en donde se puede acceder a cada uno de los paquetes capturados para su análisis, los mismos que se encuentran agrupados por fechas de evento, dirección IP de origen.

Además se muestra la cantidad de conexiones establecidas así como los eventos IDS generados.

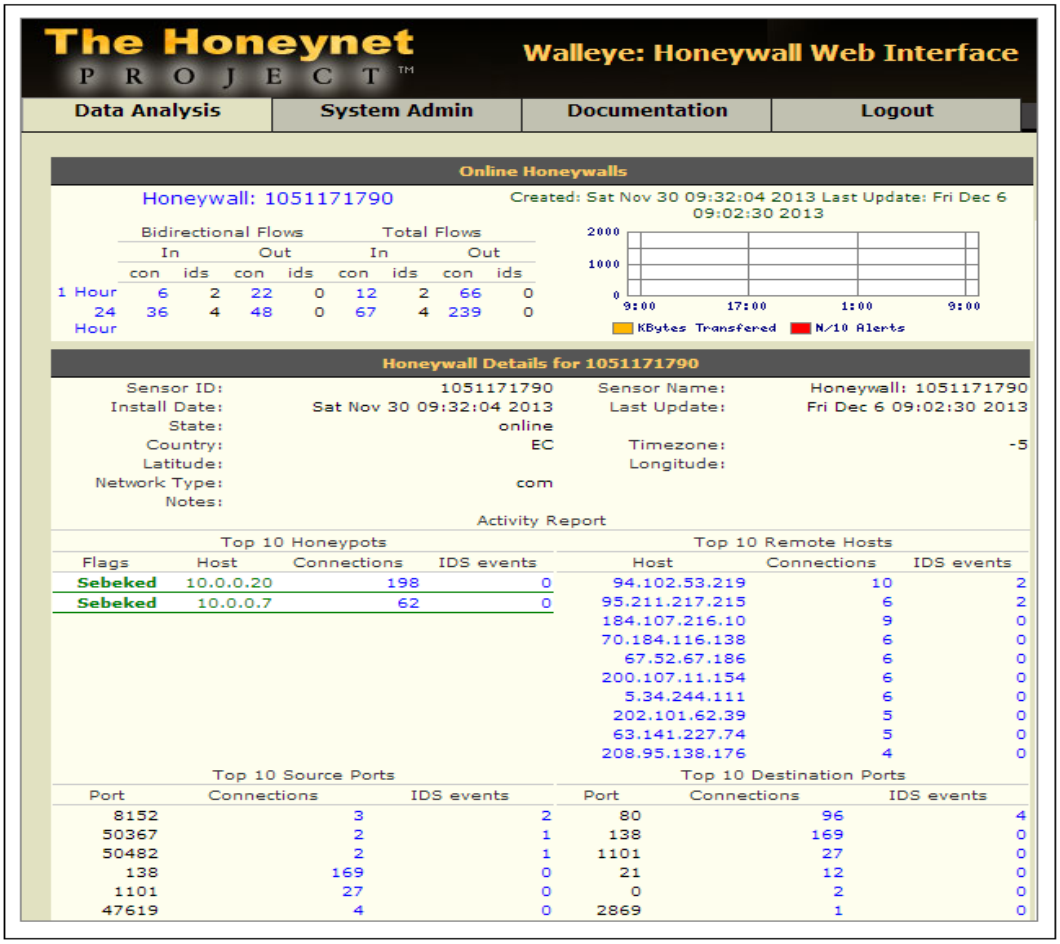


Gráfico # 56: Actividad SEBEK en el IDS del Honeywall

Fuente: El Autor

Con la información presentada, se demuestra el correcto funcionamiento de la infraestructura Honeypot implementada, evidenciado en la efectividad del IDS operativo en el Honeywall en el control, captura y recolección de datos del tráfico generado por los ataques recibidos, que en conjunto con la determinación de las vulnerabilidades de los equipos informáticos de la Red del Hospital Municipal mediante las pruebas de penetración efectuadas, se elaboró la Guía de corrección de vulnerabilidades, la misma que ha sido implementada, luego de lo cual se ejecutó una nueva tarea de análisis de vulnerabilidades

mediante la herramienta Nexpose, en la que se puede evidenciar que las vulnerabilidades críticas han sido corregidas.

Para realizar la validación de la hipótesis se utilizará el enunciado *Modus Ponendo Pones* MPP de la inferencia lógica, el cual indica que “confirmando el antecedente (causa) entonces se confirma el consecuente”.

A ->B

A

_____

B

Para el caso particular de la hipótesis planteada en el presente trabajo, se determino dos premisas dentro de la misma:

A = Detectar y corregir vulnerabilidades

B= Mejorar los niveles de seguridad

Si tomamos como cierto que la corrección de vulnerabilidades de un sistema informático tiene como consecuencia lógica el aumento en los niveles de seguridad del mismo, A -> B, una vez verificado que la premisa A de este estudio se cumple por cuanto se realizó el trabajo de detección y corrección de las vulnerabilidades, la premisa B se afirma como válida ya que es la consecuencia del estudio realizado en la primera variable.

Por lo tanto se verifica que la hipótesis es válida mediante la aplicación del método de comprobación MPP aplicado, en el sentido de que cumpliendo lo enunciado en A tiene como consecuencia B.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Durante el análisis de la infraestructura de Red existente en el Hospital municipal previo a la implementación de una Honeynet se evidenció que existen vulnerabilidades que afectan la seguridad de la información del HMNSM, atribuidas a fallas en el diseño lógico de red especialmente en el perímetro de seguridad externa, entre las fallas de diseño encontradas se estableció la falta de un Sistema Perimetral de Seguridad Firewall en la interconexión entre la Red del Hospital y la Red del Gobierno Autónomo Descentralizado Municipalidad de Ambato más aún cuando se utiliza un este enlace WiFi en una banda libre. La disposición en una zona insegura del Servidor de Correo institucional el mismo que se encuentra expuesto al Internet y la disposición de todos los equipos de cómputo incluidos los servidores en una sola VLAN.

La implementación de herramientas Honeypot en la red del Hospital, conjuntamente con las pruebas de penetración realizadas, permitió detectar un gran número de vulnerabilidades generadas principalmente por la falta de actualización de los Sistemas Operativos y Software de la mayoría de equipos de cómputo del Hospital; causa mucha preocupación el servidor de Active Directory en el cual se detectó gran cantidad de vulnerabilidades fácilmente explotables convirtiéndolo en una gran amenaza para la continuidad, disponibilidad e integridad de los servicios informáticos.

Durante el tiempo de producción de la Honeynet, se evidenció que el honeypot fue accedido en múltiples ocasiones desde diferentes ubicaciones en el planeta, algunas de ellas consideradas por el IDS como intentos de intrusión, lo que indica que la Red del Hospital es considerada como un objetivo para los atacantes.

En la actualidad la tecnología Honeypot aplicada a pesar de ser libre y eficiente, no ha mantenido un desarrollo continuo, lo cual la ha ido relegando frente a nuevas tecnologías propietarias para la detección y prevención de intrusiones disponibles en el mercado.

La cantidad de Software para análisis de redes disponibles en la actualidad correctamente utilizadas ofrece al administrador de redes un gran número de herramientas para conocer el nivel de seguridad de su infraestructura, pero también constituyen una seria amenaza en manos equivocadas.

Actualmente, la sociedad no tiene total conciencia de la importancia de eliminar las malas prácticas en la gestión de la información lo que ocasiona que el nivel de riesgo informático sea elevado en la mayoría infraestructuras de red institucionales.

5.2 RECOMENDACIONES

Es necesario realizar un rediseño de la Red del Hospital Municipal, para eliminar las vulnerabilidades, en el cual se deberá considerar la implementación de un Sistema de Seguridad Perimetral Firewall a fin de corregir la falla de seguridad en la Interconexión con la Red Informática del GADMA.

Se deberá realizar la implementación de VLAN´s con el protocolo IEEE 802.1Q, para distribuir todos los Servidores y computadores de la Red del Hospital en

diferentes redes virtuales según su ubicación e importancia, para dividir el actual dominio de broadcast en segmentos más pequeños.

Planificar la realización de auditorías permanentes del Software instalado en los equipos de cómputo, servidores y estaciones de trabajo, con la finalidad de determinar exactamente los que sistemas operativos y aplicativos necesitan ser actualizados, reemplazados o dados de baja de ser el caso para eliminar nuevas vulnerabilidades.

Ejecutar en el corto tiempo las acciones descritas en la Guía para la Corrección de las Vulnerabilidades detectadas, incluida en el presente trabajo.

Es recomendable mantener y potenciar el sistema Honeypot aplicado, con la finalidad de poder obtener mayor información de los intentos de ataque e intromisión a la Red, ya que resulta más económico y eficiente a realizar una gran inversión financiera en sofisticados sistemas propietarios de Detección de Intrusos.

Planificar la realización periódica de Pruebas de Penetración controladas, con la finalidad de detectar nuevas vulnerabilidades que afecten los niveles de seguridad de la infraestructura Informática de la institución.

La actual maestría en gerencia informática debe potenciar la transferencia de conocimientos en el área de Seguridad Informática, mejorando la aplicación práctica de los conocimientos teóricos mediante la implementación de nueva tecnología en sus laboratorios.

Se debe instruir formalmente a la sociedad en general acerca de la necesidad e importancia de seguir buenas prácticas en la gestión de la información y a los usuarios del Hospital en particular la obligatoriedad del cumplimiento de las normas de seguridad establecidas con la finalidad de establecer altos niveles de seguridad informática.

BIBLIOGRAFIA

aldeid.com (2010). Recuperado el 11 de 11 de 2013, de ALDEID Security: www.aldeid.com/wiki

Acissi. (2011). Seguridad informática: Ethical Hacking. Barcelona. Ediciones ENI.

Ariganello, E. (2010). Redes CISCO: guía de estudio para profesionales. México DF. Alfaomega.

Cobb, S. (1994). Manual de seguridad para PC y redes locales. Madrid. McGraww-Hill

cybsec.com (2010). Recuperado el 05 de 07 de 2013, de CYBSEC S.A. Security Systemas: www.cybsec.com.

De la Cruz Paisig, H. (2013). Hacking & Cracking. Lima. Empresa Editorial Macro.

Gómez Vieites, A. (2007). Enciclopedia de la seguridad informática. México DF. Alfaomega.

gpd.sip.ucm.es (2010). Recuperado el 01 de 07 de 2013, de Departamento de Sistemas Informáticos y Computación of the Universidad Complutense de Madrid: http://gpd.sip.ucm.es

hackplayers.com (2009). Recuperado el 01 de 08 de 2013, de The Hackplayers Blog: www.hackplayers.com

Harrington, J. (2005). Network security. Burlington MT. Morgan Kaufmann Publishers.

honeynet.org (2006). Recuperado el 01 de 08 de 2013, de The Honeynet Project: www.old.honeynet.org

iplocation.net (2013). Recuperado el 10 de 11 de 2013, de IP Location Service: www.iplocation.net

Laet, G. (2005). Network security fundamentals. USA. Cisco Ed.

McClure, S. (2010). Hackers 6: secretos y soluiones de seguridad en redes. Mexico DF. McGraw-Hill Interamericana.

Picouto Ramos, F. (2008). Hacking y seguridad en internet. México DF. Ra-Ma.

seat.massey.ac.nz (2009). Recuperado el 06 de 07 de 2013, de Massey University, New Zeland: www.seat.massey.ac.nz

Singer, P. (1994). Ethics. Chicago IL. Oxford University Press

Stalling, W. (2004). Fundamentos de seguridad en redes: aplicaciones y estándares. Madrid. Pretience Hall.

Stalling, W. (2008). Comunicaciones y redes de computadores. Madrid, Pearson Educación.

Tori, C. (2008). Hacking Etico. Rosario, Argentina. Recuperado de www.4shared.com

Withman, M. (2012). Principles of Information Security. Boston MA: Cengage Learning

wordpress.com (2009). Obtenido del Blog Gestión de Riesgos de la Seguridad Informática de Wordpress: http://protejetefiles.wordpress.com.

GLOSARIO

A

Autorooter Es un troyano que emplea la vulnerabilidad conocida como DCOM-RPC para tomar el control del ordenador afectado, permitiendo que un *hacker* pueda realizar acciones como formatear el disco duro, modificar las páginas web almacenadas, añadir nuevos usuarios, etc.

B

Basilea II.- Segundo de los Acuerdos de Basilea. Dichos acuerdos consisten en recomendaciones sobre la legislación y regulación bancaria y son emitidos por el Comité de supervisión bancaria de Basilea. El propósito de Basilea II, publicado inicialmente en junio de 2004, es la creación de un estándar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios para asegurar la protección de las entidades frente a los riesgos financieros y operativos.

Backdoor.- En la informática, una puerta trasera (o en inglés *backdoor*), en un sistema informático es una secuencia especial dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo (autentificación) para acceder al sistema. Aunque estas puertas pueden ser utilizadas para fines maliciosos y espionaje no siempre son un error, pueden haber sido diseñadas con la intención de tener una entrada secreta

E

Exploit.- **E**xploit, es un programa de prueba de concepto que puede estar en código fuente para compilar o formato binario que sirve para aprovechar o demostrar una vulnerabilidad en una aplicación y puede estar escrita en varios lenguajes de programación.

F

Firewall.- Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

G

Gusano Informático.- Es un **malware** que tiene la propiedad de duplicarse a sí mismo.

H

Hacker.- Un **hacker** es alguien que descubre las debilidades de una computadora o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas.[1] Los hackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta o por el desafío.

Hardware.- Se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Http Flood.- Un *flood* consiste en mandar mucha información en poco tiempo a alguien para intentar que se sature. La manera de aprovechar esto en los chats, consiste en enviar muchas peticiones de información a la víctima, de forma que ésta, al contestar, supere el límite del servidor y éste lo eche.

I

ICMP.- *Internet Control Message Protocol*) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

M

Malware.- código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario

P

Payload.- Parte de un virus informático que realiza una acción malintencionada.

Perl.- Es un lenguaje de programación diseñado por Larry Wall en 1987. Perl toma características del lenguaje C, del lenguaje interpretado bourne shell (sh), AWK, sed, Lisp y, en un grado inferior, de muchos otros lenguajes de programación.

Ping de la muerte.- Es un tipo de ataque enviado a una computadora que consiste en mandar numerosos paquetes ICMP muy grandes (mayores a 65.535 bytes) con el fin de colapsar el sistema atacado

R

Router.- Conocido como router, enrutador, ruteador o encaminador de paquetes— es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes

Ruby.- Lenguaje de programación interpretado, reflexivo y orientado a objetos creado en 1995 por el programador japonés Yukihiro Matsumoto.

S

Snnifer.- Programa informático que captura las tramas en una red de datos.

Software.- Se conoce como *software*[1] *al equipamiento lógico o soporte lógico* de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

V

VLAN.- Una **VLAN** *Virtual LAN*, es un método para crear redes lógicas independientes dentro de una misma red física. es una tecnología que segmenta las redes de forma virtual, una funcionalidad que admiten la mayoría de conmutadores de red. Esto se consigue dividiendo los usuarios de la red en grupos lógicos. Sólo los usuarios de un grupo específico pueden intercambiar datos o acceder a determinados recursos en la red.

ANEXOS

E01 ENCUESTA

E02 DETALLE DE EQUIPOS DE COMPUTO HOSPITAL MUNICIPAL

E03 CONFIGURACION DEL HONEYWALL

E04 REPORTE DE VULNERABILIDADES NEXPOSE