FACULTAD DE INGENIERÍAS Y CIENCIAS AGROPECUARIAS

"HACKING ÉTICO PARA EL CENTRO DE OPERACIÓN DE LA RED PARA LA ZONA 8 DE LA EMPRESA C.N.T. CON SOFTWARE DE CÓDIGO ABIERTO."

Trabajo de titulación presentado en conformidad a los requisitos establecidos para optar por el título de Ingeniero en Redes y Telecomunicaciones.

Profesora Guía:

Ing. Víctor Ulloa

Autor:

Oscar Milton Sánchez Robayo

Año

2012

DECLARACIÓN DEL PROFRESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el/la estudiante, orientando sus conocimientos para un adecuado desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan a los Trabajos de Titulación.”

Víctor Ulloa
Ing. Networking.
170802979-6

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi auditoría, que se ha citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que se protegen los derechos de autor vigentes”.

Oscar Milton Sánchez Robayo
171546930-8

AGRADECIMIENTO

A mis padres

A mis hermanos

A mis profesores

Al Instituto de Crédito Educativo.

A The hacking blog

DEDICATORIA

A mis Padres por sus incontables esfuerzos por terminar mi carrera y un especial agradecimiento a mi madre que siempre estuvo para apoyarme y darme ánimos en cada etapa de mi vida.

RESUMEN

Dentro del presente proyecto se revisarán temas como introducción al hackeo ético, el cual nos indicará sobre dos temas controversiales como son la ética y el hackeo, software de código abierto, sistemas de hackeo, extracción de información y seguridades en redes de información, se mencionará sobre una metodología que se hace referencia para nuestro tema y una breve explicación sobre la red de la C.N.T.

Posteriormente se procederá a desarrollar un conjunto de pruebas para la zona 8 de la empresa C.N.T con software de código abierto, utilizando hacking ético con programas como: Wireshark, Metasploit, SET, Fasttrack, SSLstrip, nmap, dsniff, netcat, nikto, nbtscan, scapy, etc., en base de los lineamientos ya establecidos.

Se considerará accesos no autorizados a información sensible o crítica, y se elaborará un informe de evaluación de la red de la zona 8 de la CNT.

ABSTRACT

Within this project will be reviewed as an introduction to issues ethical hacking, which will indicate on two controversial issues like ethics and hacking, open source software, hacking systems, information extraction and security in information networks, will be mentioned on a methodology referred to our topic and a brief explanation of the CNT network

Then proceed to develop a test suite for the enterprise zone 8 CNT with open source software, using ethical hacking programs such as Wireshark, Metasploit, SET, Fasttrack, sslstrip, nmap, dsniff, Netcat, Nikto, nbtscan, scapy, etc., based on the guidelines already established.

Be considered unauthorized access to sensitive or critical information, and prepare a report listing the network vulnerabilities of the area 8 of the CNT.

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

CAPITULO I

MARCO TEÓRICO

Descripción de la situación actual de la empresa y estudios sobre diferentes tipos de seguridad que son usados en la red de la zona 8 perteneciente a C.N.T

La CNT EP cuenta con un amplio portafolio, basado en la RED de última generación IP/MPLS TE y DWDM. Basándose en los más altos estándares de calidad y ajustándose a cada uno de los requerimientos específicos de empresas, compañías y negocios, esta red está orientada a cubrir necesidades y brindar la seguridad que necesitan.

1.1. Recopilación de la información

Para entender qué servicios vamos a poner a prueba tenemos que saber qué servicios actualmente está ofreciendo la empresa.

Los servicios que pone a disposición del empresario ecuatoriano son:

1.1.1. BackBone

La red de fibra óptica más grande a nivel nacional, con más de 10.000 Km de fibra óptica, instalada en todo el territorio ecuatoriano. La mayor red de microonda del país para un triple respaldo en la información.

1.1.2. IP/MPLS TE y DWDM.

Es una red de última tecnología y a la vanguardia en todo el mundo, está conformada por una columna vertebral ‘backbone' de alta disponibilidad, con distribución y acceso de cobertura nacional, con enlaces redundantes, evitando pérdidas del servicio; permite conectar todo el equipamiento de la red de acceso de la empresa (MSAN, DSLAM, WIMAX, CDMA 450), para proporcionar servicios de telefonía fija alambica e inalámbrica, transmisión de datos, Internet y video de alta calidad.

La red de CNT fue reconocida por Cisco con el premio "CISCO Innovation

Awards" como el proyecto de mayor impacto social de la región.

1.1.3. Red de Acceso

Mediante la aplicación de las tecnologías, ADSL 2+, GPON y FTTB, G.SHDSL, WIMAX, DTH la empresa está en capacidad de brindar todas las soluciones de telecomunicaciones que sus clientes requieren.

1.1.4. Acceso a la red de Internet

La CNT EP es propietaria de la red de acceso más grande del Ecuador. 10.000 Km de Fibra óptica, mono modo con anillos redundantes y soportados en Tecnología IP/MPLS TE

1.1.5. Convergencia

Las profundas transformaciones tecnológicas y administrativas emprendidas por la CNT EP han incrementado su rentabilidad y liquidez, siendo este el mejor momento para la absorción de Alegro. Así la empresa completará el círculo, y estará en capacidad de ofrecer a sus clientes servicios de convergencia.

"Gracias a la fusión entre CNT EP y Alegro, la empresa contará con servicios móviles y ofertas comerciales convergentes, unidos a una cultura organizacional de servicio y un mejoramiento integral en los centros de atención al cliente" señaló César Regalado en su intervención[1].

1.1.6. Conectividad Internacional.

CNT posee nivel de TIER 2, por lo tanto la mejor conectividad internacional del País con una capacidad de transporte internacional de datos de 192 STM-1.

Ofrece conectividad con más de 1000 destinos en el mundo entero,

La empresa posee actualmente 5 salidas para conexión internacional:

Dos cables submarinos (Cable Panamericano + Américas II y_ Emergía).

Dos cables terrestres (una salida por Colombia y la otra por Perú).

---

[1] Revista buscando la noticia, http://revistabuscandolanoticia.com/produccion.html

1.1.7. Servicios Satelitales

Transmisión de datos y acceso a Internet, sin ningún tipo de limitación geográfica. Cubre el 100% de la República del Ecuador, incluyendo las islas Galápagos.

1.2. Introducción a la Ética Hacker

La ética hacker no es un programa de **seguridad de redes.** Tampoco es un programa de entrenamiento de **análisis de seguridades,** ni de probar seguridades.

La ética Hacker se refiere a los profesionales de la seguridad que **aplican sus habilidades** de hacker **para fines defensivos**, el 100% de sus esfuerzos va dedicado a programas ofensivos hacia una red (programas) que miden el nivel de confiabilidad en un sistema dado, en este caso la red de la zona 8 perteneciente a C.N.T.

1.2.1. Clases de Hacker

Sombrero Negro

Individuos con habilidades extraordinarias para la computación, recurriendo a maliciosas y destructivas actividades. También conocidos como crackers.

Sombrero Blanco

Las personas que profesan habilidades de un hacker y el uso de ellos paracon fines defensivos. También conocido como los analistas de seguridad.

Sombrero Gris

Las personas que trabajan tanto ofensiva como defensivamente en varias ocasiones.

Hacker Suicidas

Las personas que tienen como objetivo reducir la infraestructura crítica de una "causa" y no están preocupados por enfrentar 30 años de cárcel por sus acciones.

1.2.2. Hackers Éticos.

Ex Sombreros Negros

- Crackers reformados
- Personas con experiencia de primera mano
- Menor credibilidad percibida

Sombrero Blanco

- Consultores independientes de seguridad (pueden ser grupos como hat White también)
- Demanda a ser informados sobre las actividades black hat.

Consultoría de Empresas

• Parte de las empresas TIC

• Las buenas credenciales.

1.2.3. Como llegar a ser un Hacker Ético

Para convertirse en un hacker ético, debe cumplir con los siguientes requisitos:

- Debe ser competente con habilidades de redes de comunicación y lenguajes de programación.
- Debe estar familiarizado con la investigación de vulnerabilidades
- Dominio en las diferentes técnicas de hacking
- Seguir un estricto código de conducta

1.2.4. Cómo llevar a cabo un Ethical Hacking

Paso 1: Hable con su cliente sobre las necesidades de las pruebas

Paso 2: Preparar los documentos de NDA y pedir al cliente que los firme

Paso 3: Prepare un equipo de hacking ético y elaboración de calendario para las pruebas

Paso 4: Realizar la prueba
Paso 5: Analizar los resultados y preparar un informe.
Paso 6: Entregar el informe al cliente

1.2.5. Enfoques de Ethical Hacking

De red remota:
• Este enfoque intenta simular un intruso, lanzar un ataque a través de Internet
Remoto de acceso telefónico de red:
• Lanzar un ataque contra las listas del módem del cliente

Red local
• Este método simula un empleado con legal acceso sobre la redlocal.
Los equipos robados:
• Este método simula el robo de una información de recurso crítica, como un ordenador portátil propiedad de un estratega que fue sacado de su dueño y dado a la ética hacker.

La ingeniería social:
• Este enfoque trata de comprobar la integridad de los empleados de la organización.
• Este enfoque trata de comprometer físicamente laorganización de infraestructura de TIC.

1.2.6. Pruebas de Ethical Hacking

Hay diferentes formas de las pruebas de seguridad. Los ejemplos incluyen el escaneo de vulnerabilidades, hacking ético, y las pruebas de penetración.
Enfoques de la prueba se muestran a continuación:
Caja Negra
• Sin el conocimiento previo de la infraestructura

Caja blanca

• Con un conocimiento completo de la infraestructura de red.

Caja gris

También se conoce como prueba interna. Se examina el grado de acceso por laspersonas internas dentro de la red.

1.2.7. Hacking ético Entregables

Un informe de Hacking Ético:

• Detalles de los resultados de la actividad de la piratería.

• Se detallan las vulnerabilidadesy se sugieren medidas de prevención. Por lo general se entregan en formato escrito, por razones de seguridad.

1.2.8. Cuestiones a considerar:

El equipo, sensibilidad de la información, cláusula de no divulgación en el contrato legal (que haga uso de la información correcta a la persona adecuada), integridad de la evaluación.

1.3. Leyes para Hacking

1.3.1. ECUADOR

Según la fiscalía general del Estado actualmente tipifica los siguientes delitos:

- Apropiación ilícita de bienes ajenos
- Defraudación tributaria:
    - Alteración dolosa de contabilidad, anotaciones, asientos y registros contables en perjuicio del acreedor tributario
    - Destrucción de respaldos contables para evadir obligaciones tributarias
    - Doble contabilidad con distintos asientos o registros
- Producción, comercialización y distribución de imágenes pornográficas.

Se está estudiando para que los delitos informáticos tengan sanciones penales ya que el aumento de este tipo de actividades se han incrementando; con pérdidas de 100 usd hasta miles de dólares y también con los recientes ataques a páginas web del estado y ataques a cuentas bancarias utilizando medios como el **phishing**[2] suplantación de identidad, el **skimming**[3] que clona tarjetas de débito y crédito y el **carding**[4] que utiliza los números de tarjetas de crédito para hacer compras en el extranjero.

En otros países existen leyes establecidas que tipifican claramente este delito como: Estados Unidos y México, ver anexos.

1.4. Pasos para el hackeo ético.

Lo básico que realiza un hacker (experto en informática) es: 1.Reconocimiento Activo Pasivo2. Escaneo 3. Como ganar acceso – a niveles de sistema operativo – a niveles de aplicaciones – Nivel de Red – Por denegación de Servicios 4. Mantener el acceso – bajando –subiendo – alterando programas o datos. 5. Por último Limpiando las Pistas (referente al acceso no autorizado).

1.4.1. Reconocimiento Activo Pasivo

Un Reconocimiento Activo Involucra adquirir información sin directamente interactuar con el objetivo.Por ejemplo buscar registros o noticias emitidas.
Un Reconocimiento Pasivo involucra interactuar con el objetivo directamente por cualquier medio. Por ejemplo, llamadas de teléfono al departamento técnico o help desk.

---

[2] Phishing .- conocida por la falsificación de sitios web

[3] Skimming .- la suplantación de tarjetas de débito y de crédito.

[4] Carding .- la utilización de tarjetas de crédito para compras en el exterior.

1.4.2. Escaneo

Se refiere a la fase de pre-ataque cuando el hacker escanea la red para obtener información específica sobre la base de información recopilada durante el reconocimiento.
Los escaneos pueden incluir el uso de marcadores (telefonía hacia otros o un mismo país), analizadores de puertos, escáneres de barrido, etc.

1.4.3. Como ganar acceso

– Niveles de sistema operativo
– Niveles de aplicaciones
– Nivel de Red
– Por denegación de Servicios

El acceso se refiere a la fase de penetración. El atacante explota la vulnerabilidad en el sistema. El exploit puede ocurrir en una red LAN, Internet o robo. Los ejemplos incluyen desbordamientos de buffer, denegación de servicios, secuestro de sesiones y craqueo de contraseñas.

Los factores que influyen son la arquitectura y la configuración del sistema de destino, el nivel de habilidad del autor, y el nivel inicial de acceso obtenidos.
Riesgos de Negocio: La más alta - El atacante puede obtener acceso a la nivel de sistema operativo, nivel de aplicación, o nivel de red

1.4.4. Mantener el acceso – Bajando –subiendo – alterando programas o datos.

Mantener el acceso se refiere a la fase en la que el atacante trata de mantener su propiedad en la red. Los atacantes pueden evitar que el sistema pase a ser propiedad de otros atacantes para asegurar su acceso exclusivo con puertas traseras, rootkits, troyanos, etc.

Los atacantes pueden subir, descargar, o manipular los datos, aplicaciones yconfiguraciones en el sistema de propiedad de ellos.

1.4.5. Por último Limpiando Pistas (referente al acceso no autorizado).

Cubriendo pistas, se refieren a las actividades llevadas a cabo por un atacante para ocultar sus fechorías.
Las razones incluyen la necesidad de estancia prolongada, el uso continuo de los recursos, eliminación de pruebas de hacking o evitar una acción legal
Los ejemplos incluyen esteganografía, un túnel, y la modificación de los archivos de registro

1.5. Metodología osstmm

La metodología osstmm (open source security test methodology manual), es un manual que nos indica como realizar un pentesting o ethical hacking que consiste en una serie de pruebas para verificar que tan segura o confiable es nuestra red ayudándonos con indicadores como es el **RAV** que nos indica en que porcentaje nuestra red es segura.

1.5.1. RAV

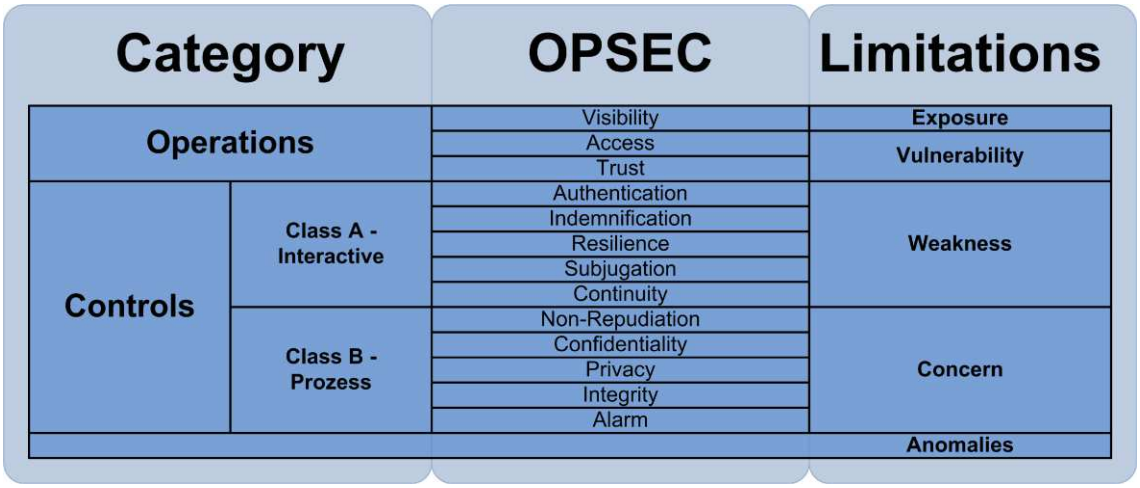
El **rav** es una medida a escala de la superficie de ataque, la cantidad de interacciones sin control con un objetivo, que se calcula por el balance cuantitativo entre limitaciones y controles. Tener la Ravs es comprender cómo gran parte de la superficie de ataque se expone.

En esta escala, 100 rav (también se muestra como 100% rav por la simplicidad de comprensión, aunque no precisamente en porcentaje) es un equilibrio perfecto y un valor menos de 100 nos indica muy poco control y por lo tanto una mayor superficie de ataque. Más de 100 rav muestra más controles que

son necesarios y que puede ser un problema, ya que los controles suelen añadir las interacciones dentro de un ámbito, así como la complejidad y los problemas de mantenimiento.

El Rav se deriva de tres categorías definidas en el ámbito: seguridad operacional (Opsec), controles y limitaciones. Con el fin de empezar, debemos primero agregar y asociar a todos los de nuestra información de entrada en las categorías apropiadas para cada variable de entrada.

Figura 1. 1 Categorías definidas en el ámbito de seguridad operacional



Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Para elegir el tipo de prueba adecuado, lo mejor es entender primero cómo los módulos están diseñados para trabajar. Dependiendo de la minuciosidad, la empresa, asignación de tiempo, y los requisitos de la auditoría, el analista puede programar los detalles de la auditoría de fase.

1.5.2. Hay cuatro fases en la ejecución de esta metodología:

A. Inducción

B. Fase de Interacción

C. Fase indagatoria

D. Fase de Intervención

Cada fase da una profundidad diferente a la auditoría, pero no hay una sola fase que es menos importante que otra en términos de seguridad real.
Poner todos los módulos entre sí proporciona una metodología para conocer y trabajar con ellos. Esta es una metodología que es aplicable a cualquiera y todos los tipos de pruebas de seguridad. Ya sea que el objetivo sea un sistema en particular, un lugar, una persona, un proceso, o miles de ellos, esta metodología nos asegurará la prueba más completa y eficiente posible.
Para una explicación máscompleta véase el anexo sobre metodología OSSTMM.

1.6. Descripción de la red

Actualmente la Corporación Nacional de Telecomunicaciones está divida por regiones en todo el Ecuador. En lo que se refiere a Quito, está dividido por zonas; conformando 8 que dividen internamente a la ciudad de Quito. Nuestro estudio va dedicado particularmente a la zona 8 perteneciente a la zona de Tumbaco.

1.7. Centros de Operación de red (NOC) y Centros de Seguridad (SOC)

1.7.1. NOC (NETWORK OPERATIONS CENTER)

DEFINICIÓN

Entidad de trabajo encargada de la administración de una red, de su infraestructura física y lógica, con la finalidad de mantener adecuados índices de rendimiento y disponibilidad.

La RFC[5] 1302 (Building a Network Information Services Infrastructure), define como: “Un Centro de Operaciones de Red es una organización cuyo objetivo es supervisar y mantener las operaciones diarias de una red.”

1.7.2. OBJETIVOS DE UN NOC

Entre los objetivos que un NOC persigue se encuentran:

- Mantener la correcta operación de la red y de sus enlaces**.**
- Implementar herramientas que otorguen un adecuado funcionamiento de la red.
- Monitorear todos los enlaces de backbone y dispositivos de red. Monitorear, identificar y resolver irregularidades encontradas.
- Solucionar fallas de la red en el mínimo tiempo posible.
- Establecer normas y procedimientos para la gestión de la red. Implantar nuevas tecnologías dentro de la infraestructura de red.
- Verificar la continua operación de servidores y servicios.
- Operar las 24 horas del día, 7 días a la semana.
- Disponer de personal adecuadamente preparado para su operación.
- Proveer soporte de calidad a los usuarios de la red.

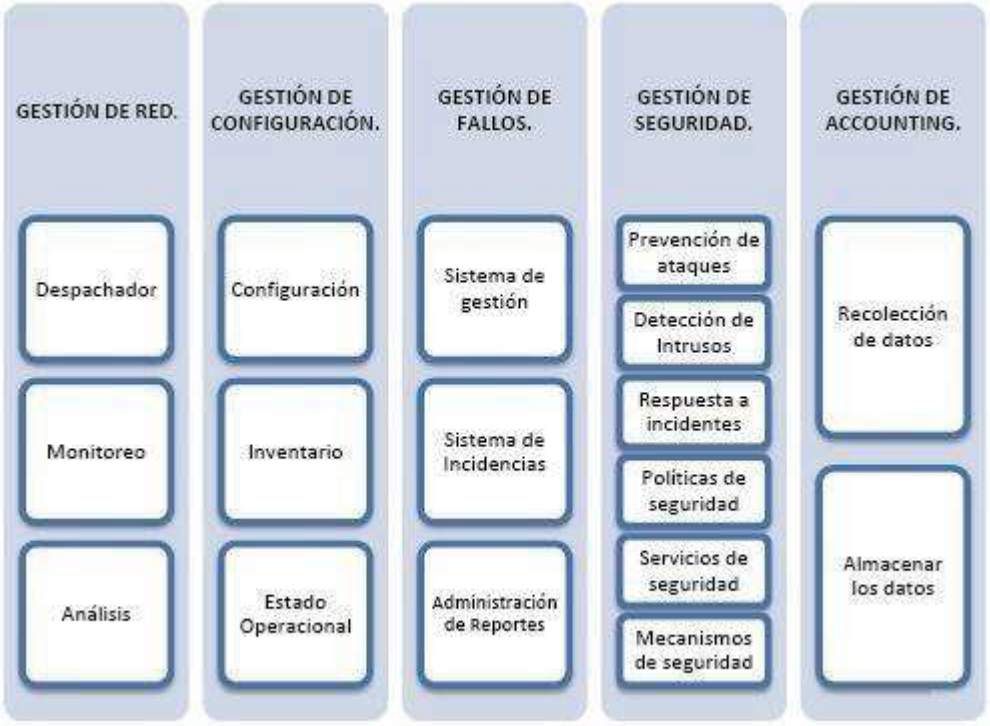
1.7.3. FUNCIONES DE UN NOC.

Las diferentes áreas funcionales del NOC son determinadas en base a recomendaciones del modelo FCAPS y adaptadas según las necesidades y características de la red a fin de cumplir los objetivos de un NOC.

La Figura 1.2, muestra los distintos elementos existentes en un NOC dentro de cada área funcional.

[5] RFC .- son comentarios enviados a la organización IETF, la cúal decide si se convierte o no en RFC.

Figura 1. 2Áreas funcionales del NOC



Fuente: Danny Alexander Bastidas Flores, Daniel Santiago Ushiña Gusque (2010), Estudio para la implementación de un centro NOC en la intranet de Petroproducción y realización de un proyecto piloto para la matriz Quito, disponible en línea http://dspace.epn.edu.ec/bitstream/15000/9980/1/T11768.pdf. Página 15

El NOC se ocupa de mantener las cosas en movimiento de manera eficiente y la SOC se refiere a la seguridad, prestados a través de análisis en el ESM.
Enterprise Security Management (ESM) es un término general que se ha aplicado a soluciones de monitorización de eventos de seguridad y análisis.

La recopilación de registros, es importante para aumentar la eficiencia operativa, reducir los riesgos y mejorar la postura de una organización de seguridad.Un mecanismo de recopilación de registros debe ser escalable, extensible y flexible
ESM tiene que ser capaz de procesar los datos de registro bruto y convertirlo en información procesable.

En la normalización de registro, cada campo de registro de datos se convierte en una particular representación de datos y consistentemente clasificado.
Cada fuente de registro puede tener un nivel de gravedad único asignado a él.
Un factor importante en el análisis de registros es el tiempo.
La convergencia de Seguridad puede aprovechar la tecnología para mejorar el desempeño de la función de seguridad. La convergencia de Seguridad es la identificación de riesgos de seguridad e interdependencias entre las funciones y procesos de negocio dentro de la empresa.

1.8. Centros de Seguridad (SOC)

Son un conjunto de servicios entre los que podemos encontrar la administración y supervisión de forma remota de los siguientes elementos entre otros:
Servidores, Firewalls, Control de acceso a la red, Antivirus, Sistemas Anti-Spam, Sistemas de Detección de Intrusiones (IDS),Tráfico de red, Ancho de banda, Copias de Seguridad.

Aspectos positivos

La especialización del personal: siempre que se externaliza un servicio se obtiene un beneficio directo proveniente del conocimiento del personal que realiza la tarea.

Servicio 24/7: estaríamos contratando un servicio que respondería las 24 horas del día durante los 7 días de la semana, hecho que resulta de especial relevancia , un servicio expuesto a Internet no entiende de horarios por lo que un incidente de seguridad puede surgir en cualquier momento.

Relación Coste/Resultado: estos servicios permiten tener a disposición de la organización a un equipo de expertos en seguridad informática por un precio muy inferior a lo que costaría mantenerlos a nivel interno.

Velocidad de Respuesta: Aquí se debería distinguir entre medidas preventivas y correctivas, sobre todo cuando se opere con sistemas que se encuentran dentro del entorno de producción.

CAPITULO II

2. Herramientas utilizadas para el Hackeo Ético.

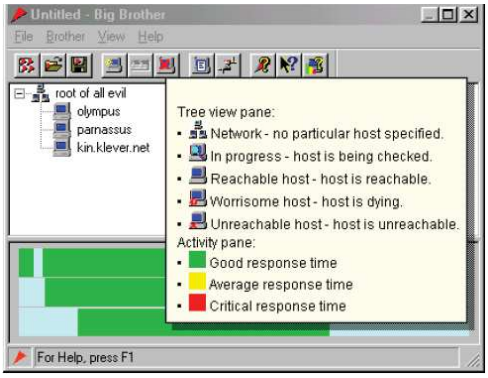
Tenemos varias herramientas que se utilizan para realizar un hackeo ético que a continuación vamos a listar con una breve descripción de las mismas. Las herramientas que utilizaremos en nuestro trabajo serán opensource y algunas versiones de prueba ya que debido a los costos, herramientas opensource nos ayudan a relizar el mismo trabajo que las pagadas; la empresa a la que se hace este tipo de pruebas no debe estar preocupada por licencias, renovaciones, contratos, etc.

2.1. Algunas herramientas para el Footprinting :

2.1.1. Big Brother

Está diseñada para ver como la red está actuando en tiempo real desde cualquier página web. Muestra información de estado en páginas web para dispositivos WAP.Incluye soporte para las pruebas de ftp, http, HTTPS, SMTP, POP3, DNS, Telnet, IMAP, NNTP yservidores ssh.

Figura 2.1 Big Brother



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1, http://www.eccouncil.org

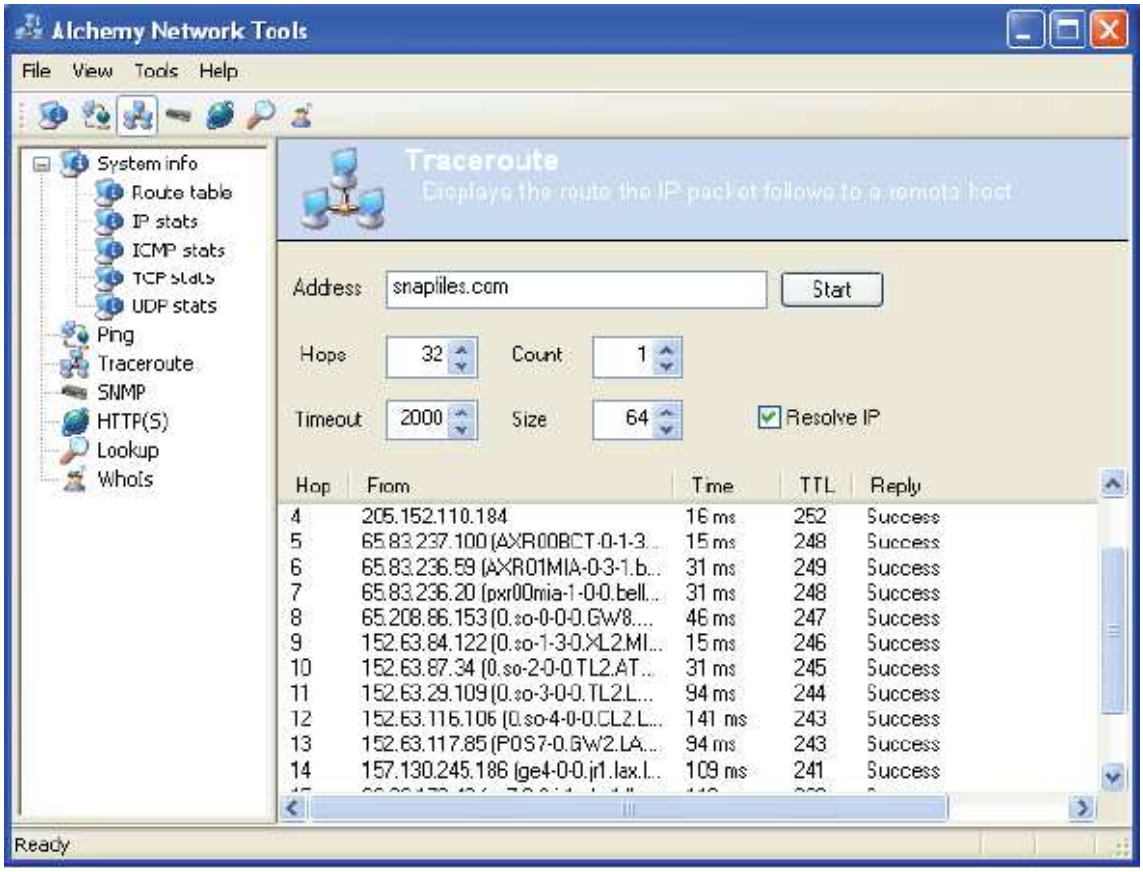
2.1.2. Alchemy Network Tools

Alchemy Network Tools es un paquete de software que contiene un conjunto de análisis de redes y herramientas de diagnóstico que ayuda a los administradores a mantener y gestionar sus redes en una interfaz gráfica agradable.

Alchemy Network contiene las siguientes utilidades de red:

• Ping, Traceroute, NSLookup, Whois, HTTP / HTTPS remitente de la petición, SNMP remitente de la petición.

Figura 2. 2Alchemy Network Tools



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1, http://www.eccouncil.org

2.1.3. Advanced Administrative Tools

Advanced Administrative Tools es una red de hilos múltiples y una herramienta de diagnóstico del sistema que está diseñado para recopilar información detallada y estado de disponibilidad de equipo de red.

Combina 12 utilidades:

• Port Scanner, Analizador de Proxy, Localizador, Analizador de CGI, EmailVerifier, Analizador de Enlaces, Monitor de red, Process Monitor, Whois, Sistemade Información, Visor de recursos, Registry Cleaner.

Figura 2. 3 AATools

Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1, http://www.eccouncil.org

2.1.4. Whois Lookup

Conwhois lookup, puede obtener datos de carácter personal y el contactoinformación sobre el dominio

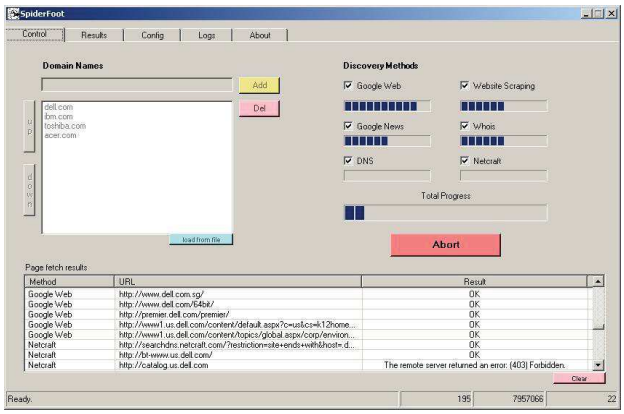
Figura 2. 4 Whois Lookup

Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.1.5. SpiderFoot

SpiderFoot es una herramienta, de código abierto, y de footprinting[6] de dominio que va a tocar los sitios web de ese dominio, así como búsqueda en Google, Netcraft, Whois y DNS para acumular información de subdominios.

Figura 2.5 SpiderFoot



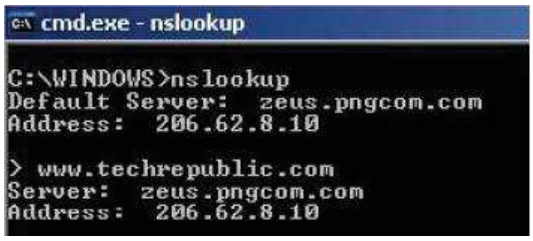
Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.1.6. Nslookup

Nslookup.-Ayuda a encontrar las direcciones IP de varios dominios. Revela la IP del servidor de correo, Unix y Windows.

[6]Footprinting .- utilizados para seguir huellas de nuestro objetivo (target) .

Figura 2. 6 Nslookup

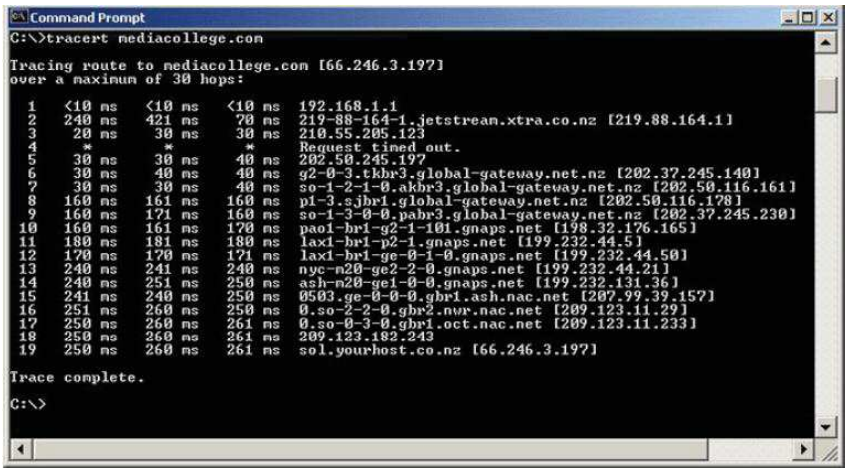


Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.1.7. Traceroute

Traceroute funciona mediante la explotación de una característica del protocolo de Internet llamado TTL o Time To Live, revela la ruta de los paquetes IPentre dos sistemas mediante el envío de series consecutivas de paquetes UDP o ICMP, con incrementos de TTL.

Figura 2. 7 Tracert



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.1.8. Dogpile (Motor de Búsqueda Meta)

Dogpile es un motor de búsqueda de meta, obtiene resultados de los múltiples motores de búsqueda y directorios, y luego los combina y presenta al usuario.

Dogpile proporciona el código para añadir a su herramienta de búsqueda sitio web, se persigue a los mejores resultados de la parte superior de Internet, motores de búsqueda, como Google, Yahoo! Search, MSN,Ask Jeeves, About, MIVA, LookSmart, etc.

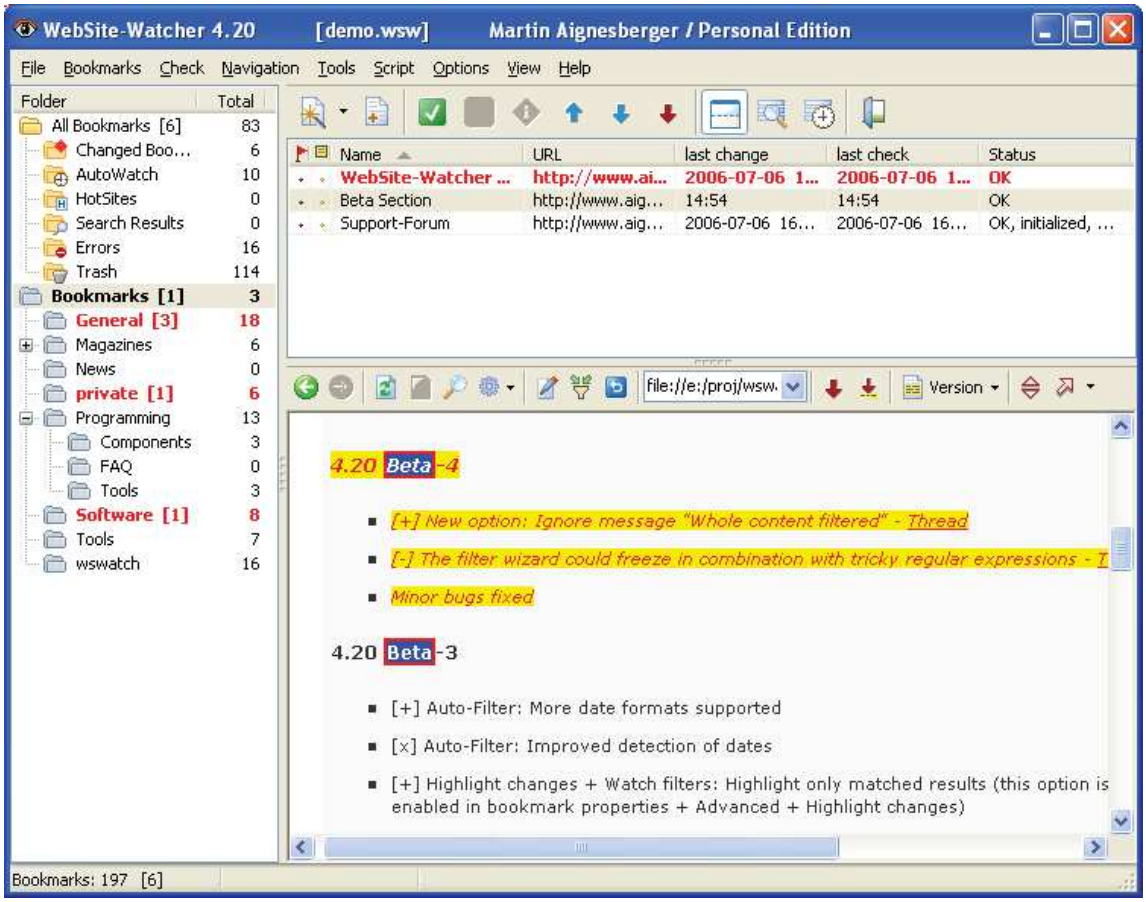
Figura 2.8 DOGPILE

Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.1.9. Website watcher

Los Website watcher pueden ser utilizados para obtener las actualizaciones en el sitio web, se puede utilizar para obtener ventajas competitivas.
Con esta herramienta podemos obtener la versión actual en la cual está corriendo nuestra aplicación y si esta o no actualizada.

Figura 2. 9 Website watcher



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.1.10. Google Earth

Google Earth muestra información de todo el planeta y otros derechos de información geográfica, imágenes tomadas desde el satélite.

La ubicación de un lugar con GoogleEarth es una herramienta valiosa para los atacantes que permite ubicar nuestro objetivo de una manera rápida y sencilla.

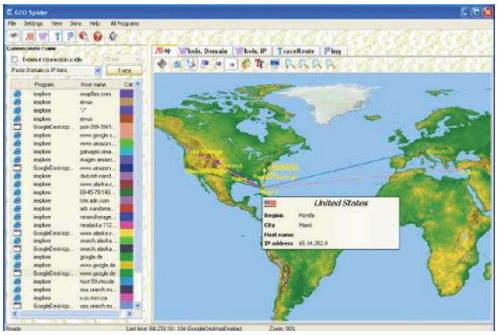
Figura 2. 10 GoogleEarth

Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.1.11. GEO Spider[7]

GEO Spider le ayuda a detectar, identificar y supervisar la actividad de la red en el mapa mundial. Usted puede ver la ubicación de la dirección IP de una página web en la Tierra, GEO Spider puede trazar e investigar un sitio web, y buscar un nombre de dominio mostrando su ubicación.

Figura 2. 11 GEO Spider



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

[7]Spider .- programa usado para búsquedas específicas de páginas web.

Y tenemos má s herramientas para realizar el footprinting como: ARIN,Neo Trace,VisualRoute Trace, SmartWhois, eMailTrackerPro, Website watcher, GEO Spider, HTTrack Web Copier, E-mail Spider que casi tienen las mismas funciones que las herramientas anteriormente mencionadas.

2.2. Herramientas para el Scanning

2.2.1. Angry IP Scanner

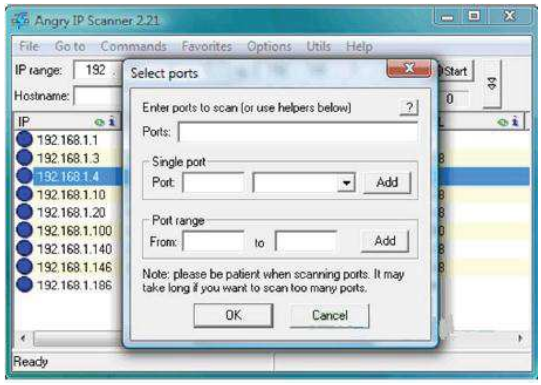
Angry IP Scanner o simplemente scan es una herramienta código abierto y además es un escaneador de red.

Esto simplemente realiza un ping a cada dirección Ip para verificar si están activas.

Proporciona información NETBIOS tales como:

- Nombre de la Computadora, nombre del Grupo de trabajo, direcciones MAC.

Figura 2. 12 Angry Ip Scanner



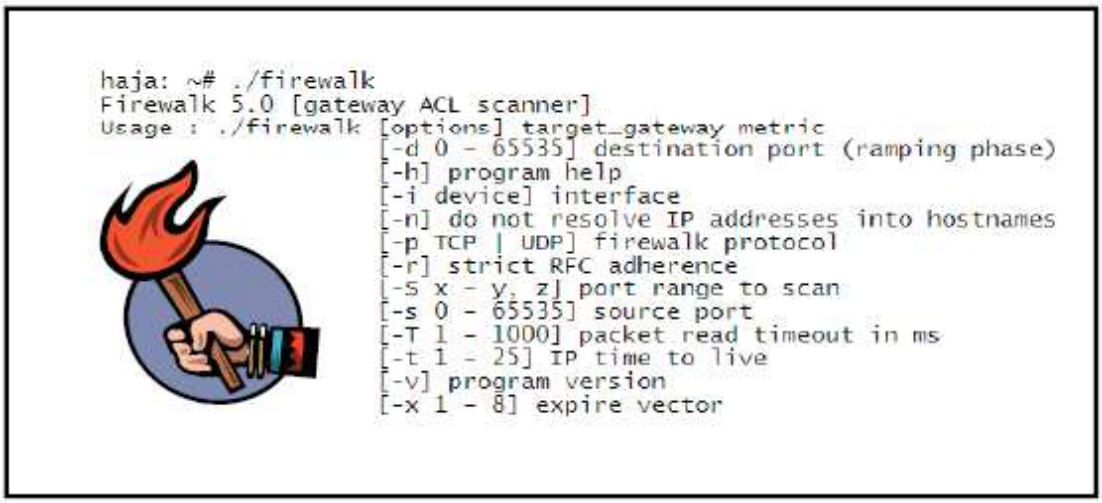
Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1 http://www.eccouncil.org

2.2.2. Firewalk

Firewalk es una herramienta que emplea técnicas como traceroute para analizar respuestas de paquetes IP, para determinar filtros, ACL y mapas de red.

Esta herramienta emplea la técnica para determinar las reglas de filtrado. Trabaja con paquetes TCP, UDP paquetes con un valor alto de TTL.

Figura 2. 13 Comandos de Firewalk



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1 http://www.eccouncil.org

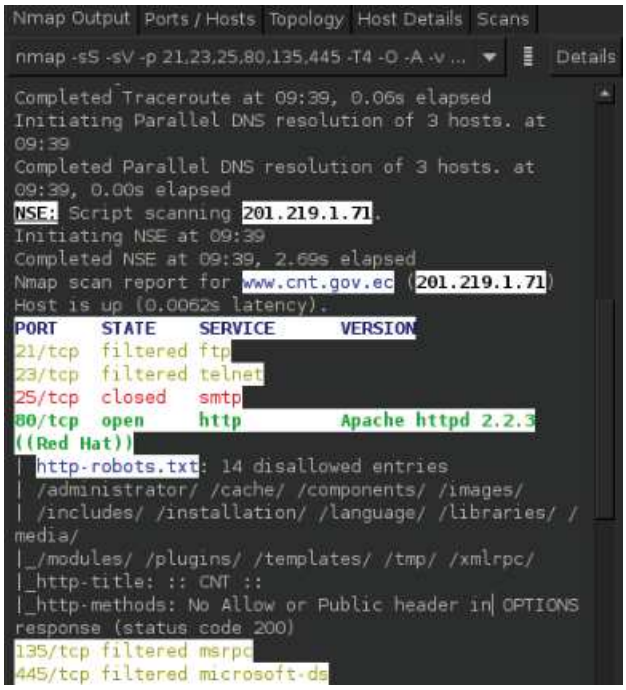
2.2.3. Nmap

Nmap es una herramienta libre (open source)[8] que es utilizada para la exploración de la red. Está diseñada para escanear redes grandes.

Nos ofrece varias tipos de escaneo lo que nos permite identificar puertos abiertos, versiones de software, aplicaciones que se están ejecutando, sistemas operativos, listar computadores remotos que están activos, dependiendo del tipo de escaneo usado podemos conectarnos no solo en computadoras objetivo (target) sino en diferentes dispositivos switch, hubs, routers ydesde allí escanear la red.

[8] Open Source .- software distribuido libremente.

Figura 2. 14 Nmap



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

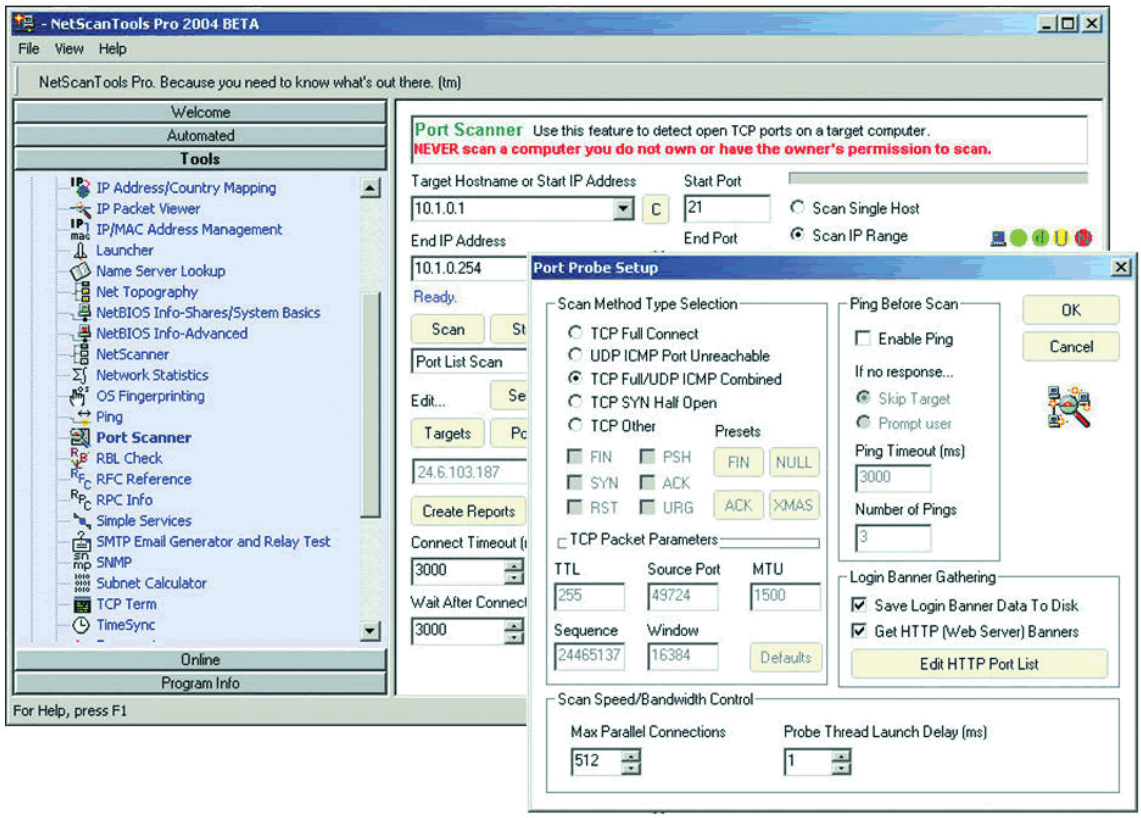
2.2.4. Windows Scan

Esteherramienta es similar al escaneo ACK, excepto que este a veces detecta puertos abiertos, filtrados y no, debido a anomalías en el tamaño de la ventana TCP reportada por algunos sistemas operativos.

2.2.5. NetScan Pro

NetScan Pro es usado para determinar las direcciones Ip, traducirlas a sus respectivos nombres, escanear redes, probar puertos, validar direcciones de correo, determinar los usuarios de los dominios, listar computadoras en un dominio.

Figura 2. 15 NetScan pro



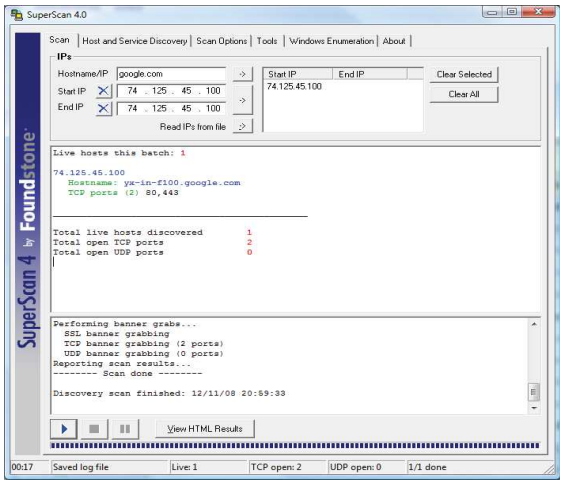
Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.2.6. Super Scan

Es un escaneador de puertos usando el pinger y resolviendo los nombres de pc's, usando cualquier rango Ip y escanea cualquier puerto desde una lista especificada.

Con esta herramienta podemos usar varias opciones de configuración, probando desde una Ip hasta un grupo de direcciones.

Figura 2. 16 SuperScan



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1

http://www.eccouncil.org

2.2.7. Net Tools Suite Pack

Net Tools Suite Pack, es una colección de herramientas de escaneo.

Figura 2.17 Net Tools Suite Pack

Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1

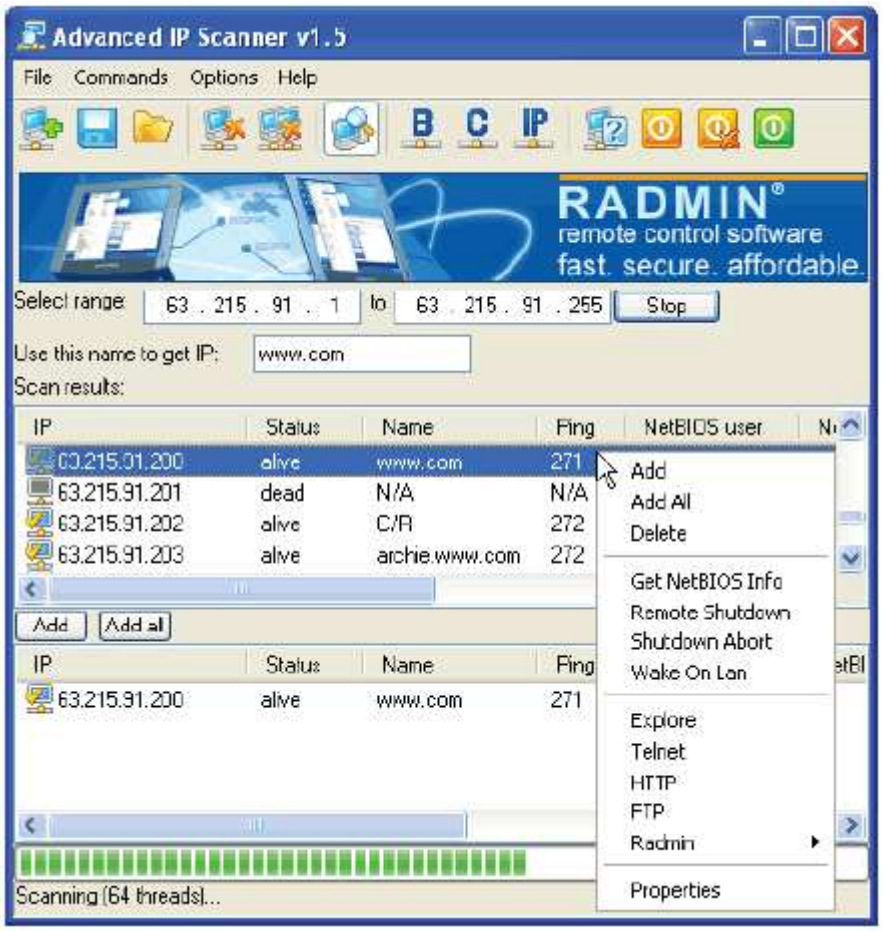
http://www.eccouncil.org

2.2.8. Advance Ip scanner

Advance Ip scanner es rápido, robusto y fácil de usar para escanear una red LAN, el cuál colecciona varios tipos de información sobre la red local de computadores.

Esto proporciona muchas funciones útiles tales como el apagado remoto. Las direcciones pueden ser almacenadas en una lista para su uso posterior.

Figura 2. 18 Advanced IP Scanner



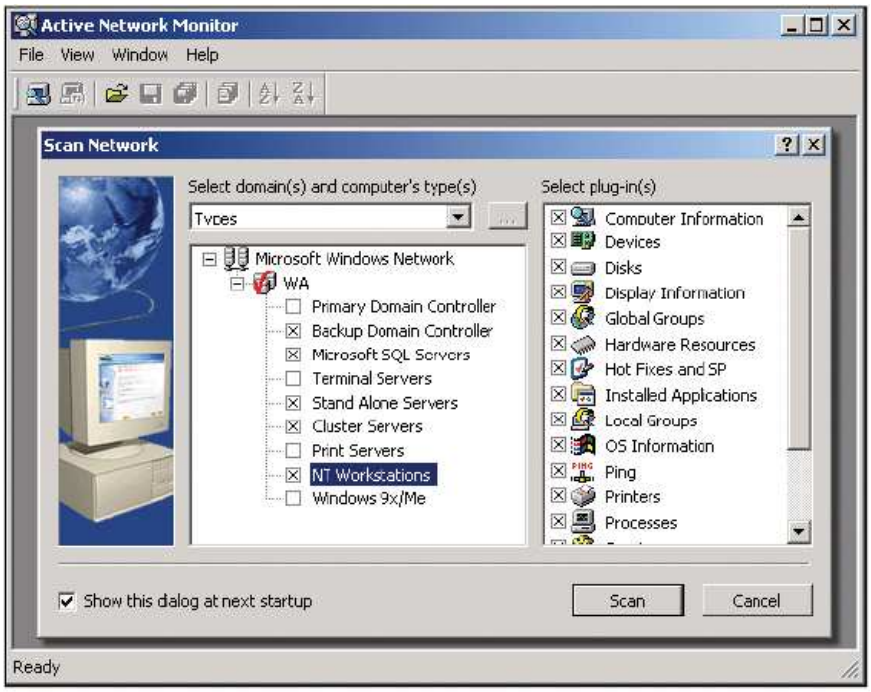
Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.2.9. Active Network Monitor

Active Network Monitor permite al administrador del sistema coleccionar información de todas las máquinas que están en la red sin instalar aplicaciones de servidor en esas computadoras.

Selecciona una variedad de artículos como: aplicaciones instaladas, como hardware, recursos, información del sistema operativo y aplicaciones instaladas.

Figura 2. 19 Active Network Monitor



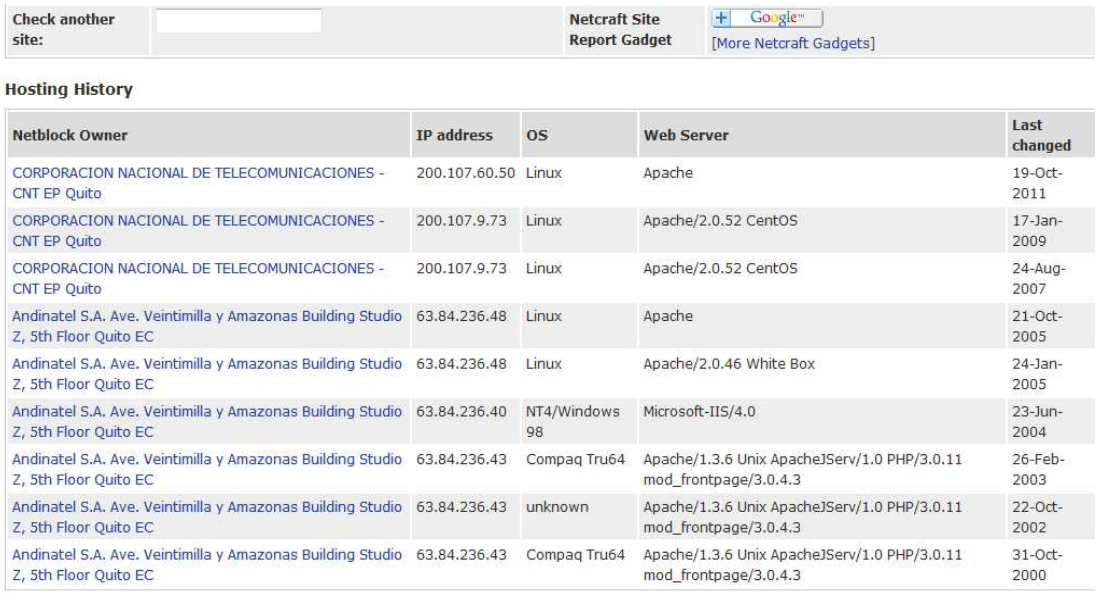
Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.2.10. Netcraft

Puede ser usada para identificar pasivamente un sistema operativo remoto de una empresa.

La información desplegada por esta página es importante ya que como podemos observar en la Figura 2.20 nos muestra su dirección, su sistema operativo, sus aplicaciones con fechas de actualización.

Figura 2. 20 Netcraft[9]



Check another site:

Netcraft Site Report Gadget

[More Netcraft Gadgets]

Hosting History

Netblock Owner	IP address	OS	Web Server	Last changed
CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP Quito	200.107.60.50	Linux	Apache	19-Oct-2011
CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP Quito	200.107.9.73	Linux	Apache/2.0.52 CentOS	17-Jan-2009
CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP Quito	200.107.9.73	Linux	Apache/2.0.52 CentOS	24-Aug-2007
Andinatel S.A. Ave. Veintimilla y Amazonas Building Studio Z, 5th Floor Quito EC	63.84.236.48	Linux	Apache	21-Oct-2005
Andinatel S.A. Ave. Veintimilla y Amazonas Building Studio Z, 5th Floor Quito EC	63.84.236.48	Linux	Apache/2.0.46 White Box	24-Jan-2005
Andinatel S.A. Ave. Veintimilla y Amazonas Building Studio Z, 5th Floor Quito EC	63.84.236.40	NT4/Windows 98	Microsoft-IIS/4.0	23-Jun-2004
Andinatel S.A. Ave. Veintimilla y Amazonas Building Studio Z, 5th Floor Quito EC	63.84.236.43	Compaq Tru64	Apache/1.3.6 Unix ApacheJServ/1.0 PHP/3.0.11 mod_frontpage/3.0.4.3	26-Feb-2003
Andinatel S.A. Ave. Veintimilla y Amazonas Building Studio Z, 5th Floor Quito EC	63.84.236.43	unknown	Apache/1.3.6 Unix ApacheJServ/1.0 PHP/3.0.11 mod_frontpage/3.0.4.3	22-Oct-2002
Andinatel S.A. Ave. Veintimilla y Amazonas Building Studio Z, 5th Floor Quito EC	63.84.236.43	Compaq Tru64	Apache/1.3.6 Unix ApacheJServ/1.0 PHP/3.0.11 mod_frontpage/3.0.4.3	31-Oct-2000

Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

La información mostrada arriba, para la persona que está haciendo un reconocimiento de la red es muy importante ya que nos da una idea por donde empezar nuestras pruebas y verificar si tienen o no actualizado las aplicaciones que están corriendo en los servidores.

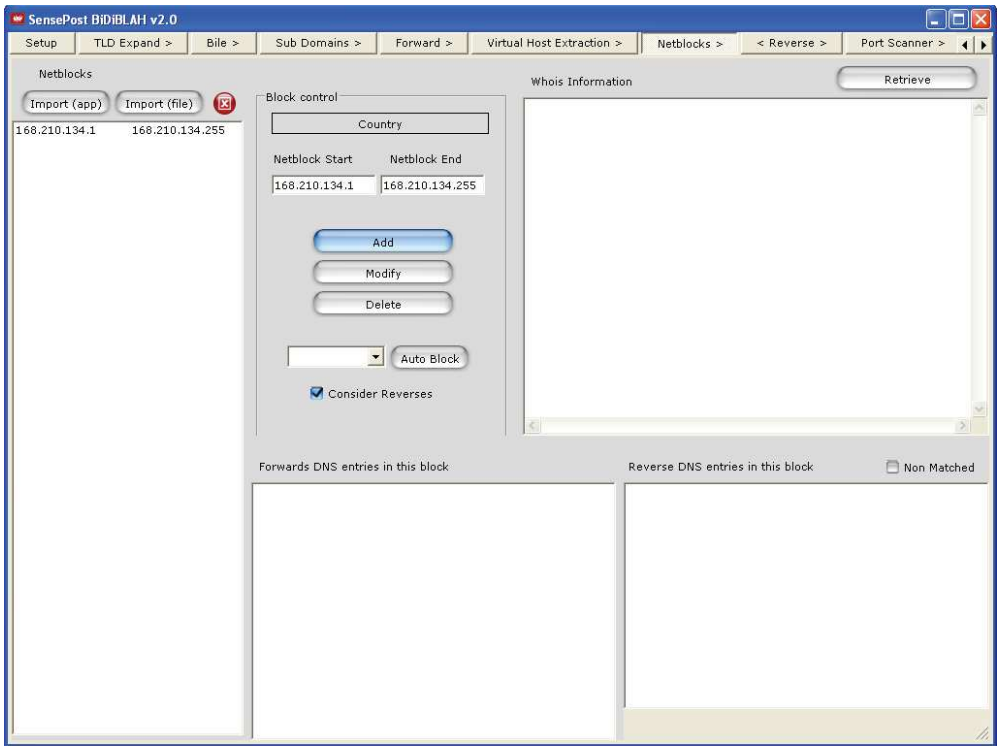
2.2.11. Bidiblah Automated

Bidiblah Automated automatiza el footprinting, enumeración DNS, escaneo de puertos y acceso a las vulnerabilidades dentro de un solo programa.

Nos permite ver el número de máquinas que están conectadas en nuestra red, mostrándonos sus DNS y también indicándonos sus puertos abiertos.

[9] Página web http://toolbar.netcraft.com/site_report?url=http://www.andinanet.net

Figura 1 Bidiblah Automated



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1

http://www.eccouncil.org

2.2.12. Saint

Saint es también conocido como herramienta de red integrada a un administrador. Esta detecta vulnerabilidades en la red.

Figura 2. 21 Saint

Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1

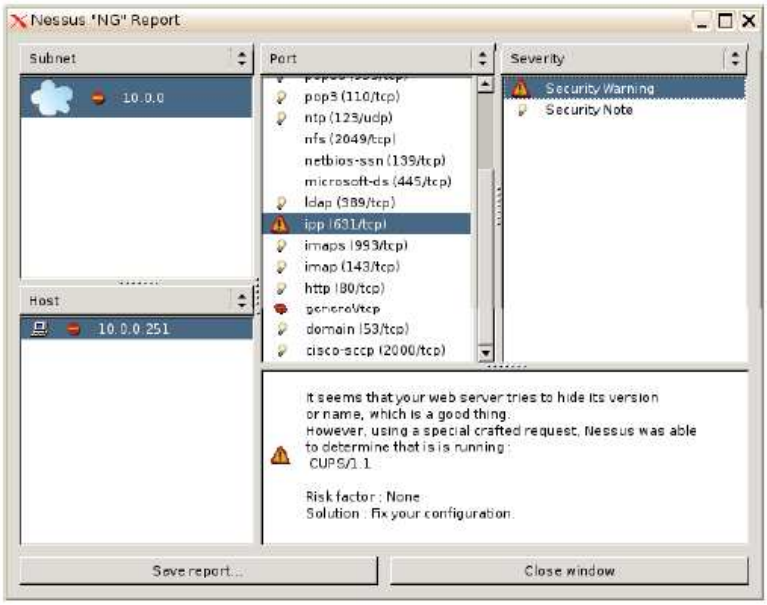
http://www.eccouncil.org

2.2.13. Nessus

Nessus es un escáner que busca vulnerabilidades en lo que se refiere a errores en el software. Un atacante puede usar esta herramienta para violar los aspectos de seguridad de un producto de software.

Esta herramienta nos lista las vulnerabilidades encontradas, nos describe el problema mostrando su versión y también indica a que versión debemos actualizar para corregir este problema.

Figura 2. 22 Nessus



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.2.14. Nagios

Nagios es un computador y monitor de servicios diseñados para informar problemas sobre la red ante los clientes, usuarios finales y administradores de la red. Monitorea servicios como: SMTP, POP3, HTTP, NNTP, PING.

Figura 2. 23 Nagios

Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

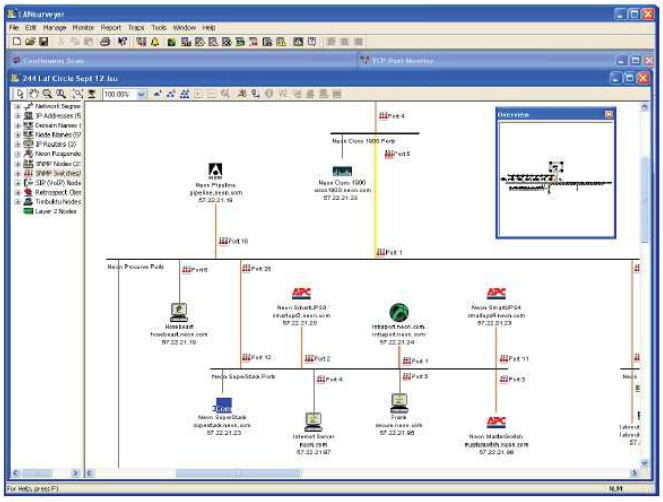
2.2.15. Nikto

Es una herramienta de código abierto escaneador de servidores web. Este realiza comprensivos test de seguridad en contra de servidores web.
El test que realiza este servidor web es en el menor tiempo posible.

2.2.16. LANsurveyor

LANsurveyor automáticamente descubre la red y produce comprensivos y fáciles mapas de red que pueden ser exportados a Microsoft Office. Automáticamente descubre y diagrama la topología de la red, genera reportes para office.

Figura 2. 24LANsurveyor



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.3. Herramientas para Enumeración.

La enumeración es definida como un proceso de extraer nombre de usuarios, nombres de máquinas, recursos de red y servicios.

Las técnicas de enumeración son conducidas en un ambiente de intranet, esto involucra conexiones activas al sistema y consultas dirigidas.

El tipo de información enumerada por los intrusos:

- Recursos de red y compartidos.
- Usuarios y Grupos
- Aplicaciones y configuraciones de auditoría.

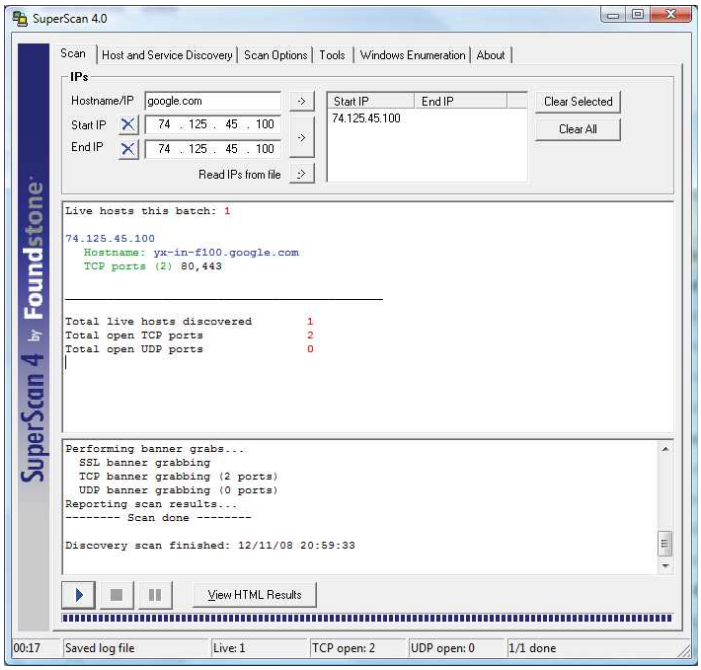
Algunas técnicas para enumeración son: Win2k, SNMP, IDS, Fuerza Bruta del árbol de directorio.

2.3.1. SuperScan

SuperScan es una conexión poderosa basada en un escaneador de puertos TCP, tiene pinger y resuelve nombres de computadoras.

Realiza escaneos de pings y de puertos usando rangos de direcciones IP.

Figura 2. 25 SuperScan



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1

http://www.eccouncil.org

Herramientas PS fue desarrollado por Mark Russinovich de SysInternals y contiene una colección de herramientas de enumeración.

Algunas herramientas requieren la autenticación del usuario al sistema:

• PsExec - ejecuta procesos de forma remota

• PsFile - Muestra los archivos abiertos de forma remota

• PsGetSid - Muestra el SID de un equipo o un usuario

• PsKill - Mata procesos por su nombre o identificador de proceso

• PsInfo - Muestra información sobre un sistema

• PsList - Muestra información detallada sobre los procesos

• PsLoggedOn - muestra quién está conectado de forma local y través de recursos compartidos

• PsLogList - Vuelca los registros de eventos

• Los PsPasswd - Cambia las contraseñas de cuentas

• PsService - servicios de Vistas y controles

• PsShutdown - Apaga y opcionalmente reinicia una computadora

• PsSuspend - Suspende los procesos

PsUptime - Muestra el tiempo que un sistema ha estado funcionando desde su último reinicio.

2.3.2. PsExec

PsExec es una herramienta ligera que reemplaza a telnet, permitiendo ejecutar procesos en otros sistemas, completamente con bastante interactividad para aplicaciones por consola. Inclusive lanza comandos interactivos en sistemas remotos.

Figura 2. 26 PsExec

Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.3.3. SNMP

SNMP significa Protocolo simple de administración de red. Los administradores envían solicitudes a los agentes y estos envían respuestas. Las peticiones y las respuestas se refieren a las variables accesibles al Agente de software.

Los administradores también pueden enviar solicitudes para establecer los valores para ciertas variables.

Las trampas que se hacen al administrador de que algo importante se produjo al final del agente son:

• Un reinicio.

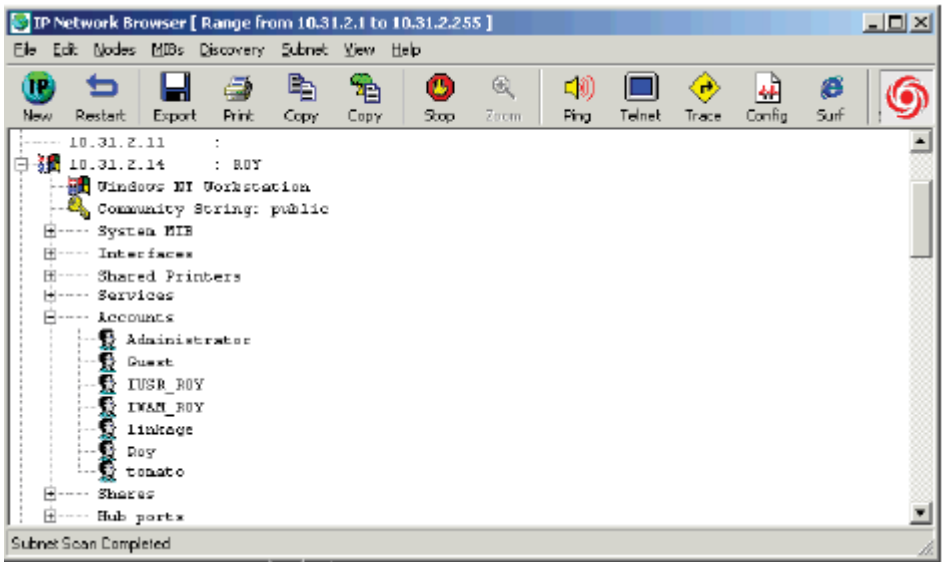
• Una interfaz caída de una.

• O bien, otra cosa que potencialmente esta mal, ha ocurrido.

2.3.4. SOLAR WINDS

Es un conjunto de administración de herramientas de red. Consisten en lo siguiente: Discovery, Herramientas Cisco, Ping, Administración de direcciones, monitoreo, seguridad, etc.

Figura 2. 27 SolarWinds



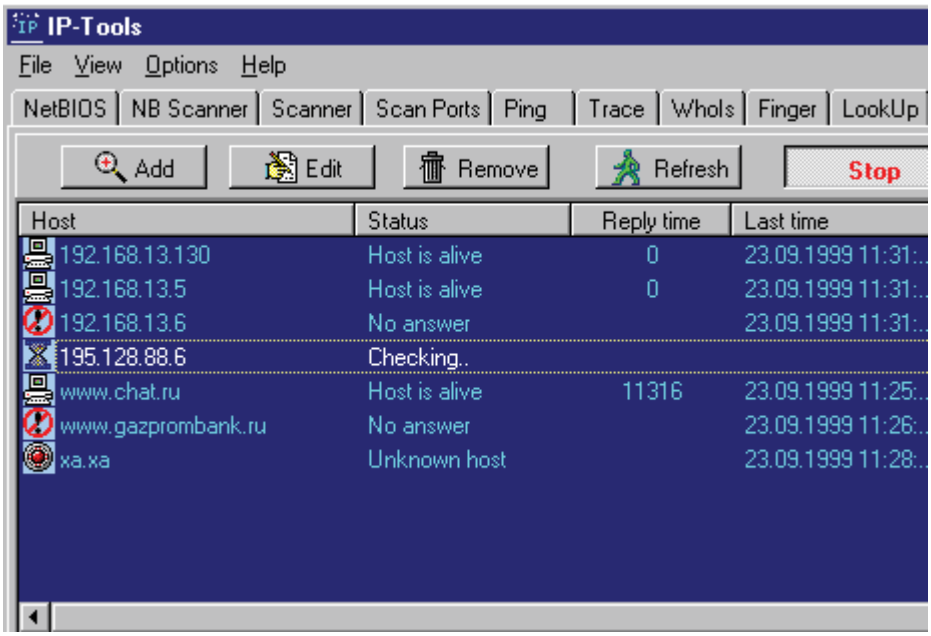
Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1 http://www.eccouncil.org

2.3.5. IP TOOLS

IP TOOLS es un conjunto de 19 servicios que incluyen:

• Información local, Conexiones del monitor, NetBIOS Scanner, recursos compartidos, SNMP, HostName, Escáner de Puertos, Escáner de UDP, Escáner de Ping, Trace, Lookup, dedo, WHOIS, Cliente Telnet El cliente HTTP, IP-Monitor, Hosts Monitor y SNMP Trap Watcher.

Figura 2. 28 Ip TOOLS



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.3.6. Enumeración de sistemas utilizando contraseñas por defecto.

Muchos de los dispositivos tales como switches, hubs y routers pueden estar habilitados con “contraseñas por defecto”. Se las puede utilizar para ganar acceso.

En la mayoría de dispositivos vienen configurados las contraseñas por defecto el administrador tiene que vigilar que estos usuarios sean eliminados ya que existen varias personas que conocen de estos usuarios y podrían sin ningún problema acceder a nuestra red sin nuestro consentimiento.

Figura 2. 29 Contraseñas por defecto

ROUTERPASSWORDS

Welcome to the **DRPD (Default Router Password Database)**. This is the internets most complete default router password database available. Simply select the *Router Make* from the dropdown list and click the *Find Password* button.

If you cant find the make/model you are looking for or would like to add your a new password to the list, click here.

Router Make 3COM

Find Password

Vendor	Model	Protocol	Username	Password
3COM	COREBUILDER *Rev. 7000/6000/3500/2500*	TELNET	debug	synnet
3COM	COREBUILDER *Rev. 7000/6000/3500/2500*	TELNET	tech	tech
3COM	HIPERARC *Rev. V4.1.X*	TELNET	adm	(none)
3COM	LANPLEX *Rev. 2500*	TELNET	debug	synnet
3COM	LANPLEX *Rev. 2500*	TELNET	tech	tech
3COM	LINKSWITCH *Rev. 2000/2700*	TELNET	tech	tech
3COM	NETBUILDER	SNMP		ANYCOM
3COM	NETBUILDER	SNMP		ILMI
3COM	NETBUILDER	MULTI	admin	(none)
3COM	OFFICE CONNECT ISDN ROUTERS *Rev. 5X0*	TELNET	n/a	PASSWORD
3COM	SUPERSTACK II SWITCH *Rev. 2200*	TELNET	debug	synnet

Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.4. Escalando Privilegios

Escalando Privilegios, si un atacante gana accesos a la red usando una cuenta que no es la de administrador, el siguiente paso es obtener una cuenta con mayores privilegios.

2.4.1. Active @ Password Changer.

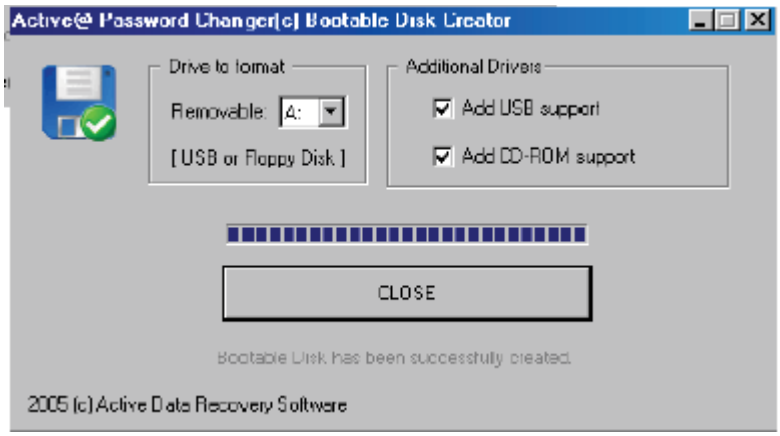
Active @ Password Changer es una solución DOS-basada y diseñada para restablecer el administrador local y contraseñas de usuario en Windows XP / 2003/2000 / NT.

Inicie el equipo objetivo utilizando un disquete formateado o/ CD-ROM y cambiar la contraseña que se encuentra en el archivo SAM.

Otras restricciones de seguridad de la conexión de Windows como 'la cuenta esta deshabilitada', 'La contraseña nunca expira "," La cuenta está bloqueada', 'El usuario debe cambiar la contraseña en el siguiente inicio de sesión "y" Logon Hours " se pueden cambiar o restablecer.

Con Active @ Password Changer, se puede iniciar sesión como un usuario particular con una contraseña en blanco.

Figura 2. 30 Active @ Password Changer

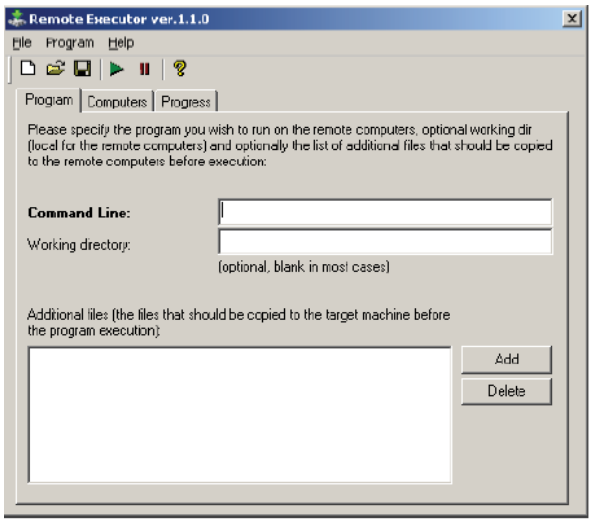


Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.4.2. Alchemy Remote Executor

Alchemy Remote Executor es una herramienta que permite a los administradores de red, ejecutar programas en computadoras remotas.

Figura 2. 31Alchemy Remote Executor



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.4.3. Keystroke Loggers

Keystroke Loggers, si todos los intentos de otros para rastrear los privilegios de dominio fallan, entonces un keystroke loggers es la solución.

Keystroke Loggers son los paquetes de software de sigilo que se colocan entre el hardware del teclado y el sistema operativo, para que puedan registrar cada pulsación de tecla.

Existen dos tipos: **basado en software y basado en hardware,** estos capturan toda la información que se ingresa por el teclado y finalmente los resultados lo envían por correo.

La ventaja con estos dispositivos es que son casi imperceptibles para personas y administradores de red que por ser portables puede pasar algún tiempo para que puedan ser detectados.

Figura 2. 32 Keylogger

Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.4.4. Handy Key Logger

Handy Key Logger, registra todo lo tecleado en un sistema de monitoreo de las teclas del ordenador, graba y resalta automáticamente en los registros y se sustituye con fotos de las teclas.

Captura todas las pulsaciones de teclado, monitorea la actividad de Internet, fotos de los registros de actividad de escritorioy envía los registros a su correo electrónico.

Características:

• Captura todas las contraseñas

• Registra el chat y la mensajería instantánea

• Monitores de la actividad en Internet.

Figura 2. 33 Handy Key Logger

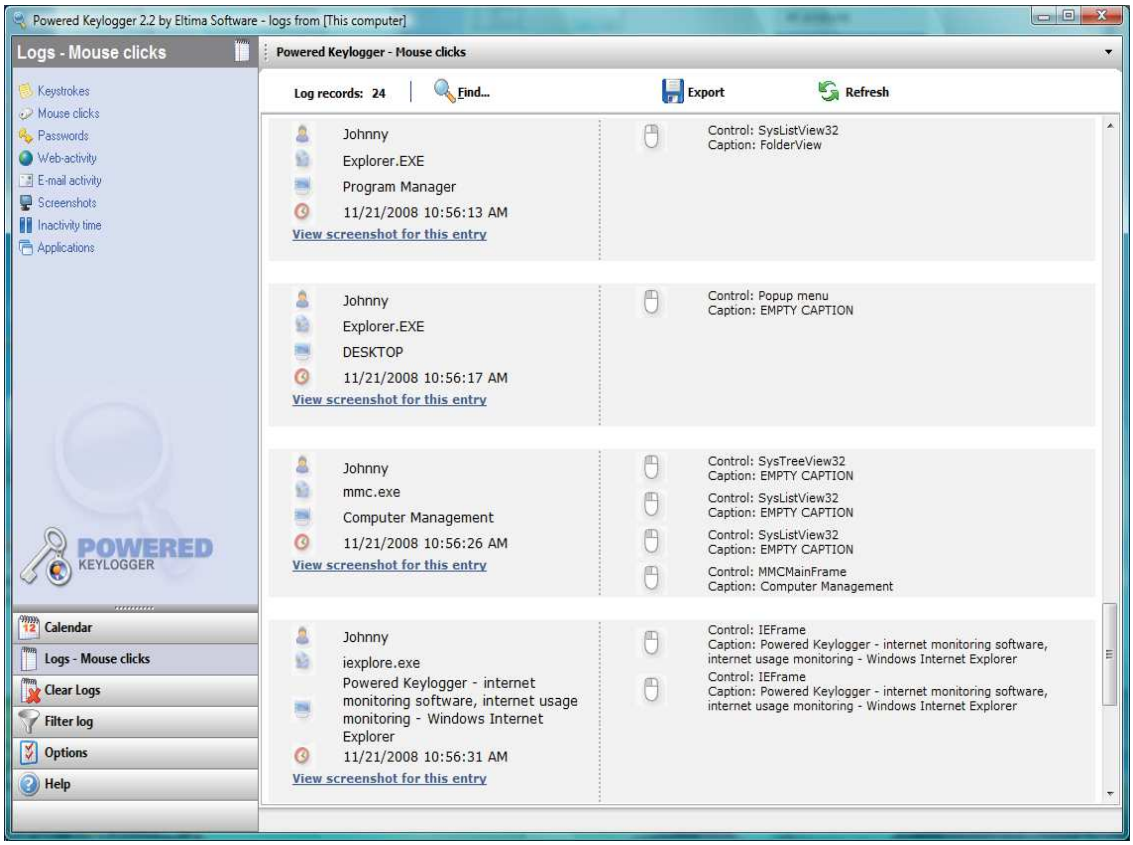
Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.4.5. Powered Keylogger

Powered Keylogger es un controlador basado en software keylogger que secretamente captura las pulsaciones de teclado, clics de ratón, y contraseñas.

Realiza un seguimiento de correos electrónicos enviados y recibidos, los monitores de la actividad de Internet y los registros de aplicaciones iniciadas. Powered Keylogger es indetectable por una lista de firewalls y software antivirus.

Figura 2. 34 Powered Keylogger



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

Basado en Hardware

2.4.6. Hardware Keylogger

Hardware Keylogger es un pequeño dispositivo de hardware que puede ser añadido entre el teclado y la computadora. Este mantiene un registro de todas las teclas presionadas en el teclado.

El proceso que se lo realiza con este software es transparente al usuario final, y pude ser muy útil para pruebas posteriores.

Figura 2. 35 Hardware Keylogger

Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.4.7. AceSpy

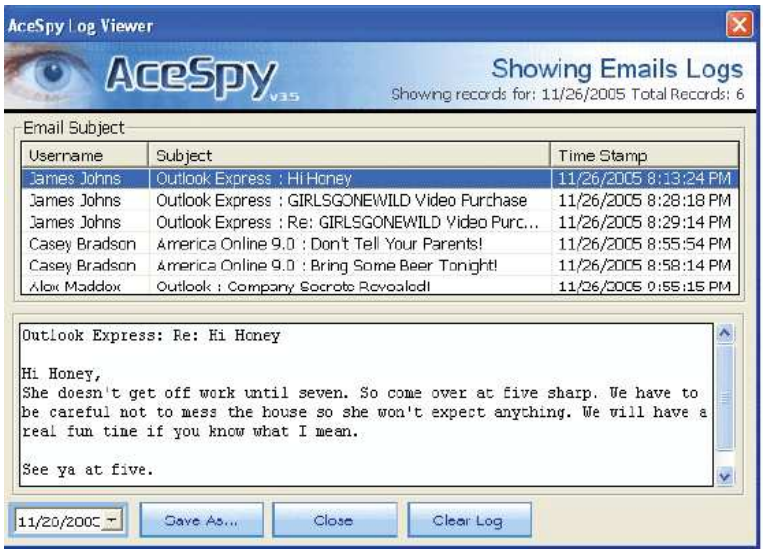
AceSpy registra secretamente todo lo que se hace en el ordenador y también puede bloquear determinados sitios web o programas.

Este software espía de inmediato enviará todos los correos electrónicos y mensajes instantáneos directamente a su dirección de correo electrónico personal.

Se ingresa una lista de programas o sitios web que desea ser bloqueado, AceSpy envia una alerta opcional a su teléfono móvil.

AceSpy registra por separado correos electrónicos, conversaciones de chat, sitios web y sitios web de las pulsaciones de teclado, las pulsaciones de teclado, instantáneas webcam.

Figura 2. 36 AceSpy



Fuente: EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1
http://www.eccouncil.org

2.5. **Cubriendo Pistas**

Si el visitante que entra sin autorización sabe lo que hace, tratará de no dejar evidencia de su paso por el Sistema Operativo, borrar rastro sería una acción muy burda en el caso a que se refieran a la eliminación de archivos enteros de registros en win c:\windows\system32\LogFiles\W3SVC1 para el registro de webserver IIS o /var/log para el registro de sistema en LINUX. Eliminar el registro completo del servidor despertaría una fuerte sospecha de intrusión en el personal de administración de servidores y el intruso hábil lo sabe. Modificar los logs (de servicios, aplicaciones, de usuarios y de sistema) es más sutil que borrarlos directamente.

Existe una forma simple de cambiar la ubicación de los logs del sistema en Windows. Para eso, tendremos que modificar la clave del registro en HKEY_LOCAL_MACHINE \CurrentControlSet\Services\Eventlog.

CAPITULO III

3. En este capítulo se va a realizarpruebas de hackeo ético y emitir un informe.

Antes de realizar cualquier prueba se debe firmar un acuerdo en donde especifique que las pruebas sólo van hacer de tipo no destructivo y que se van a realizar con el propósito de estar preparado ante cualquier evento que pueda suceder.
Se utilizarán algunas de las herramientas antes descritas y se realizará un informe el cuál indicará el nivel de penetración de nuestro ataque simulando como cliente externo e interno.

Con reconocimiento **activo** se lo hace dentro de las oficinas mientras que el **pasivo** se lo hace desde cualquier computador.

El tipo de hackeo ético que se está realizando es el denominado **Black Box** en el cual no se recibe ninguna información por parte del administrador de la red y la persona que está ejecutando la prueba descubre la red en base a diferentes pruebas con software y algunas de ingeniería social.

3.1. Pruebas realizadas a la Corporación Nacional de Telecomunicaciones.

Por medio de direcciones electrónicas y con diferentes dominio de la empresa.

3.1.1. Digitando Página www.kartoo.com

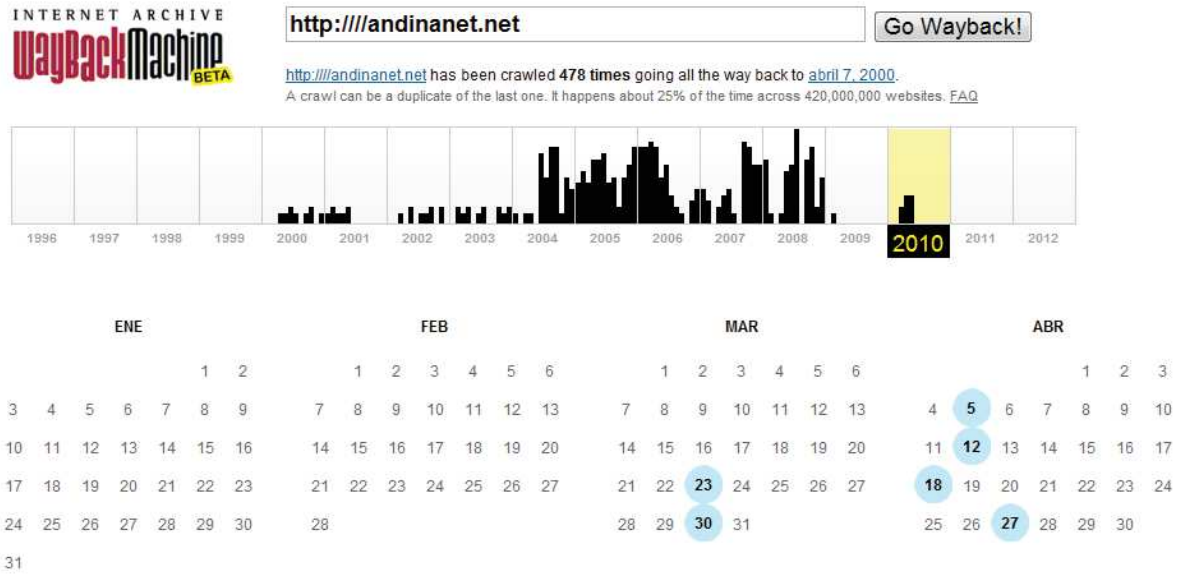
Digitando la palabra Corporación Nacional de Telecomunicaciones, nos da los siguientes resultados.

Figura 3. 1 Información sobre la C.N.T

Cabe indicar que tenemos información básica como la dirección, teléfonos.

3.1.2. Con página:http://wayback.archive.org/web/20110101000000*/http:////andinanet.net

Figura 3. 2 Nos indica un registro de todos los cambios hecho de algunos años.



3.1.3. Con página:http://whois.arin.net/ui/query.do

No tenemos ningún resultado con las direcciones www.cnt.com.ec.

Con andinanet:

Nos da dos direcciones 205.240.152.0 - 205.240.155.255, otro rango más 206.231.68.0 - 206.231.71.255.

Con página http://whois.domaintools.com nos da los siguientes resultados:

Una dirección de correo. noc@andinanet.net

Para andinanet nos da la siguiente dirección de servidores de dominio:

Pichincha 200.107.10.46

Tungurahua 200.107.60.46

Para cnt.com.ec nos da algo parecido a los anteriores resultados.

Muestra siguientes correos: rodolfo.lara@cnt.com.ec ; jhon.benalcazar@cnt.gob.ec

Para www.andinatel.com

3.1.4. Descubriendo DNS

Tenemos la siguiente dirección:

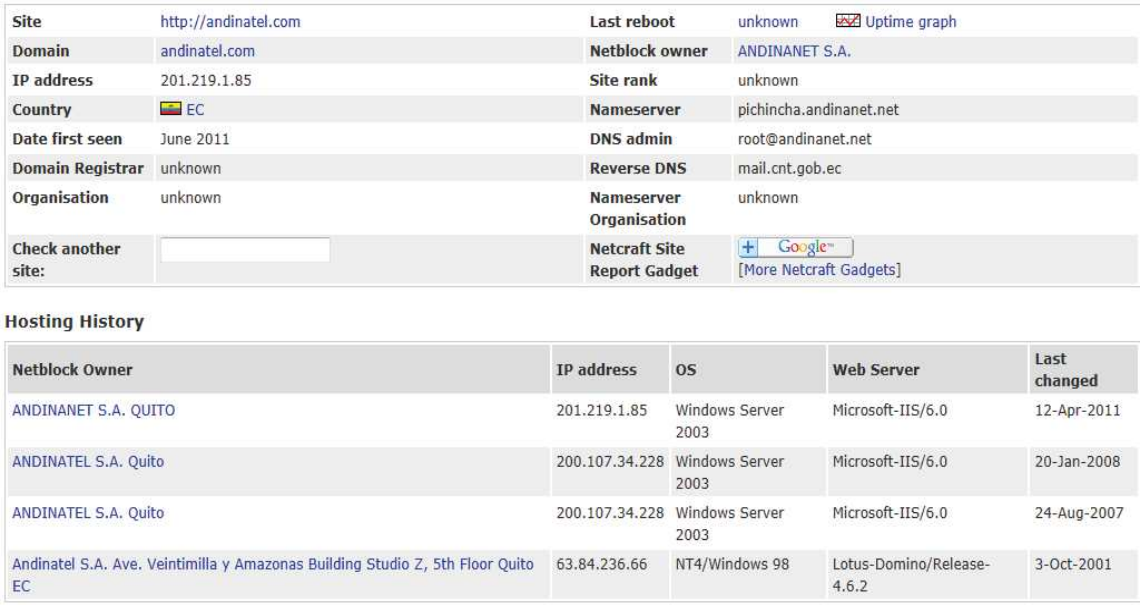
http://toolbar.netcraft.com/site_report?url=andinatel.com

Nos despliega:

Figura 3. 3 Lista los Dns con susSistemas Operativos

Para andinatel.com

Figura 3. 4 Otras direcciones con sus aplicaciones



Site	http://andinatel.com	**Last reboot**	unknown Uptime graph
Domain	andinatel.com	**Netblock owner**	ANDINANET S.A.
IP address	201.219.1.85	**Site rank**	unknown
Country	EC	**Nameserver**	pichincha.andinanet.net
Date first seen	June 2011	**DNS admin**	root@andinanet.net
Domain Registrar	unknown	**Reverse DNS**	mail.cnt.gob.ec
Organisation	unknown	**Nameserver Organisation**	unknown
Check another site:		**Netcraft Site Report Gadget**	Google [More Netcraft Gadgets]

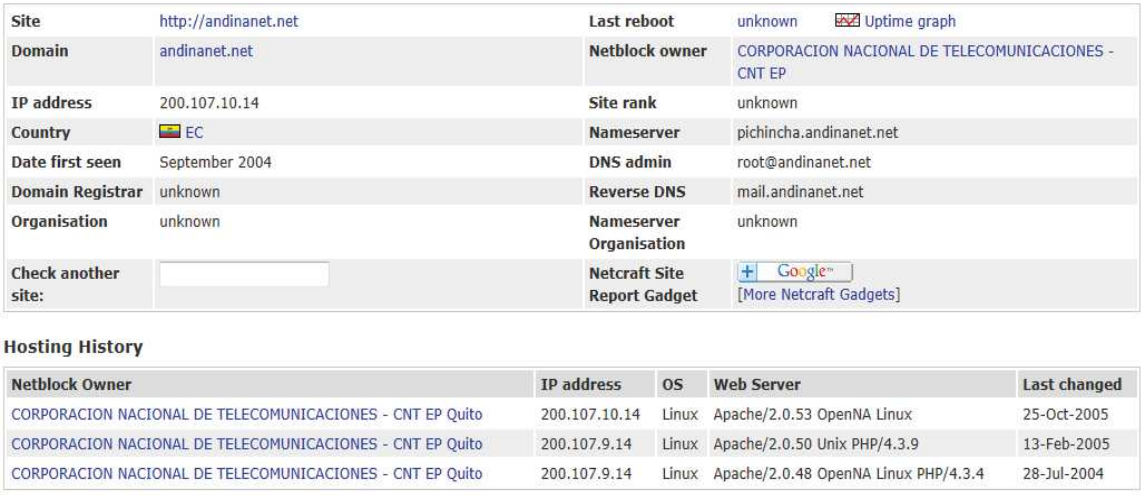
Hosting History

Netblock Owner	IP address	OS	Web Server	Last changed
ANDINANET S.A. QUITO	201.219.1.85	Windows Server 2003	Microsoft-IIS/6.0	12-Apr-2011
ANDINATEL S.A. Quito	200.107.34.228	Windows Server 2003	Microsoft-IIS/6.0	20-Jan-2008
ANDINATEL S.A. Quito	200.107.34.228	Windows Server 2003	Microsoft-IIS/6.0	24-Aug-2007
Andinatel S.A. Ave. Veintimilla y Amazonas Building Studio Z, 5th Floor Quito EC	63.84.236.66	NT4/Windows 98	Lotus-Domino/Release-4.6.2	3-Oct-2001

Lista a los servidores, con el sistema operativo y sus respectivas aplicaciones.

Para andinanet.net

Figura 3. 5 Detalla aplicaciones con sus sistemas operativos



Site	http://andinanet.net	**Last reboot**	unknown Uptime graph
Domain	andinanet.net	**Netblock owner**	CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP
IP address	200.107.10.14	**Site rank**	unknown
Country	EC	**Nameserver**	pichincha.andinanet.net
Date first seen	September 2004	**DNS admin**	root@andinanet.net
Domain Registrar	unknown	**Reverse DNS**	mail.andinanet.net
Organisation	unknown	**Nameserver Organisation**	unknown
Check another site:		**Netcraft Site Report Gadget**	Google [More Netcraft Gadgets]

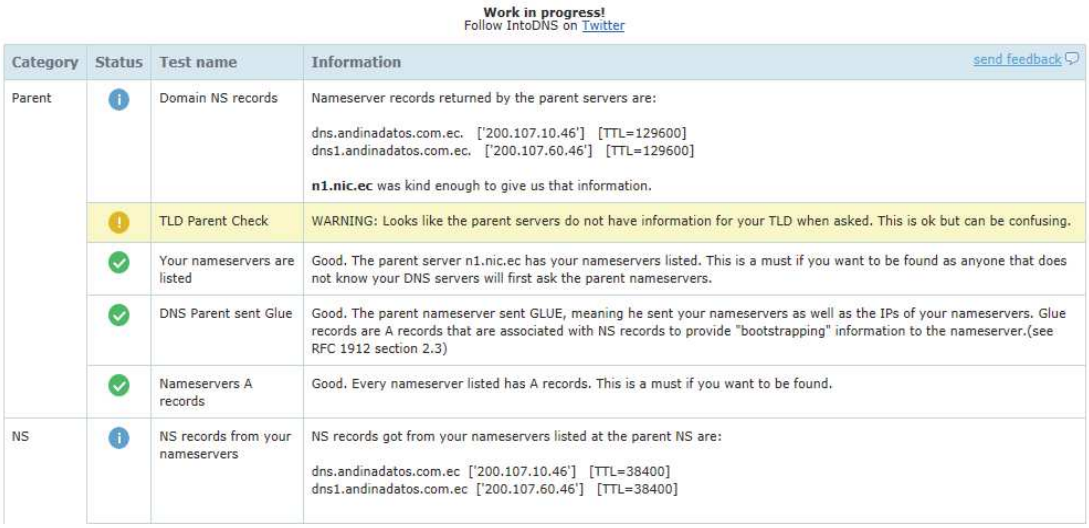
Hosting History

Netblock Owner	IP address	OS	Web Server	Last changed
CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP Quito	200.107.10.14	Linux	Apache/2.0.53 OpenNA Linux	25-Oct-2005
CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP Quito	200.107.9.14	Linux	Apache/2.0.50 Unix PHP/4.3.9	13-Feb-2005
CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP Quito	200.107.9.14	Linux	Apache/2.0.48 OpenNA Linux PHP/4.3.4	28-Jul-2004

3.1.4.1. Con la siguiente página http://www.intodns.com

Para cnt

Figura 3. 6 Lista direcciones de los dns y muestra información sobre servicios

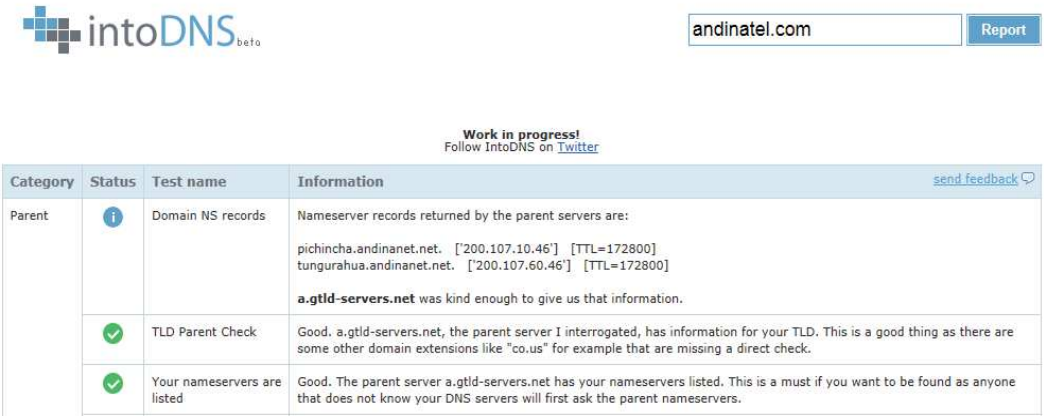


Work in progress!
Follow IntoDNS on Twitter

Category	Status	Test name	Information	send feedback
Parent	i	Domain NS records	Nameserver records returned by the parent servers are: dns.andinadatos.com.ec. ['200.107.10.46'] [TTL=129600] dns1.andinadatos.com.ec. ['200.107.60.46'] [TTL=129600] **n1.nic.ec** was kind enough to give us that information.	
	!	TLD Parent Check	WARNING: Looks like the parent servers do not have information for your TLD when asked. This is ok but can be confusing.	
	✓	Your nameservers are listed	Good. The parent server n1.nic.ec has your nameservers listed. This is a must if you want to be found as anyone that does not know your DNS servers will first ask the parent nameservers.	
	✓	DNS Parent sent Glue	Good. The parent nameserver sent GLUE, meaning he sent your nameservers as well as the IPs of your nameservers. Glue records are A records that are associated with NS records to provide "bootstrapping" information to the nameserver.(see RFC 1912 section 2.3)	
	✓	Nameservers A records	Good. Every nameserver listed has A records. This is a must if you want to be found.	
NS	i	NS records from your nameservers	NS records got from your nameservers listed at the parent NS are: dns.andinadatos.com.ec ['200.107.10.46'] [TTL=38400] dns1.andinadatos.com.ec ['200.107.60.46'] [TTL=38400]	

Para andinatel y andinanet

Figura 3. 7 Lista direcciones de los dns y muestra información sobre servicios



intoDNS beta

andinatel.com Report

Work in progress!
Follow IntoDNS on Twitter

Category	Status	Test name	Information	send feedback
Parent	i	Domain NS records	Nameserver records returned by the parent servers are: pichincha.andinanet.net. ['200.107.10.46'] [TTL=172800] tungurahua.andinanet.net. ['200.107.60.46'] [TTL=172800] **a.gtld-servers.net** was kind enough to give us that information.	
	✓	TLD Parent Check	Good. a.gtld-servers.net, the parent server I interrogated, has information for your TLD. This is a good thing as there are some other domain extensions like "co.us" for example that are missing a direct check.	
	✓	Your nameservers are listed	Good. The parent server a.gtld-servers.net has your nameservers listed. This is a must if you want to be found as anyone that does not know your DNS servers will first ask the parent nameservers.	

3.1.4.2. Con http://centralops.net/co/

Figura 3. 8 Para cnt, andinatel.com (no existe resultados) y para andinanet

Network Whois record

Queried **whois.lacnic.net** with "**201.219.1.85**"...

```
inetnum:     201.219.1.64/27
status:      reallocated
owner:       ANDINANET S.A.
ownerid:     EC-ANSA1-LACNIC
responsible: Marco Sancho
address:     Jorge Drom y Gaspar de Villarroel, 0, 0
address:     0 - QUITO - PI
country:     EC
phone:       +593 2 2941981 []
owner-c:     FBM
tech-c:      FBM
abuse-c:     FBM
created:     20080215
changed:     20080215
inetnum-up:  201.219.1/24
inetnum-up:  201.219.0/19

nic-hdl:     FBM
person:      Pablo Zapata
e-mail:      pablo.zapata@CNT.GOB.EC
address:     9 de octubre y Cordero Edf Droira, 124,
address:     17211446 - Quito - NA
country:     EC
phone:       +593 9 6184685 []
created:     20050107
changed:     20110818
```

Network Whois record

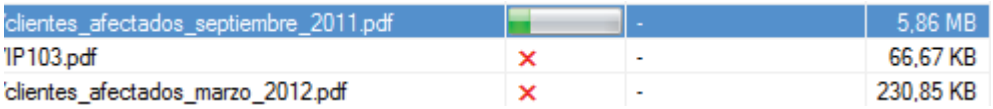
Queried **whois.lacnic.net** with "**200.107.10.14**"...

```
inetnum:     200.107.0/19
status:      allocated
owner:       CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP
ownerid:     EC-ANSA-LACNIC
responsible: Evelin Gavilanes
address:     Jorge Drom y Gaspar de Villaroel, 954, 1 er Piso
address:     3110 - Quito - EC
country:     EC
phone:       +593 2 2941963 []
owner-c:     VMR
tech-c:      VMR
abuse-c:     ALD12
inetrev:     200.107.10/24
nserver:     PICHINCHA.ANDINANET.NET
nsstat:      20120227 AA
nslastaa:    20120227
nserver:     TUNGURAHUA.ANDINANET.NET
nsstat:      20120227 AA
nslastaa:    20120227
created:     20030707
changed:     20080729

nic-hdl:     ALD12
person:      Soporte Técnico
e-mail:      abuse_report@ANDINANET.NET
address:     Jorge Drom y Gaspar de Villaroel, s/n, esquina
address:     3110 - Quito - EC
country:     EC
phone:       +593 2 2941866 []
created:     20080729
changed:     20080730
```

Con el reconocimiento pasivopodemos escanear las direcciones que queramos y encontrar información que sea confidencial para la empresa. Con el programa FOCA, con su autor Chema Alonso Cebrián, podemos capturar información que está en la red sin muchos problemas.

Figura 3. 9 Datos confidenciales de la empresa

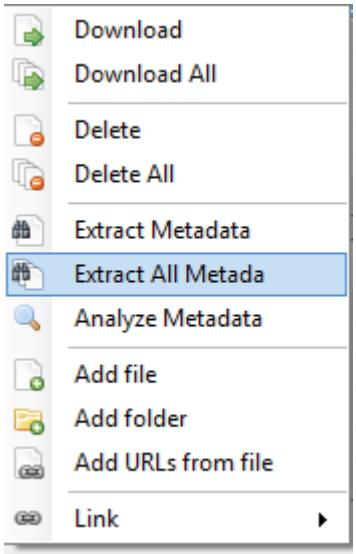


Fuente: Chema Alonso Cebrián

En la Figura 3.9 se muestra que se puede capturar información desde la web para cualquier empresa que deseamos conocer.

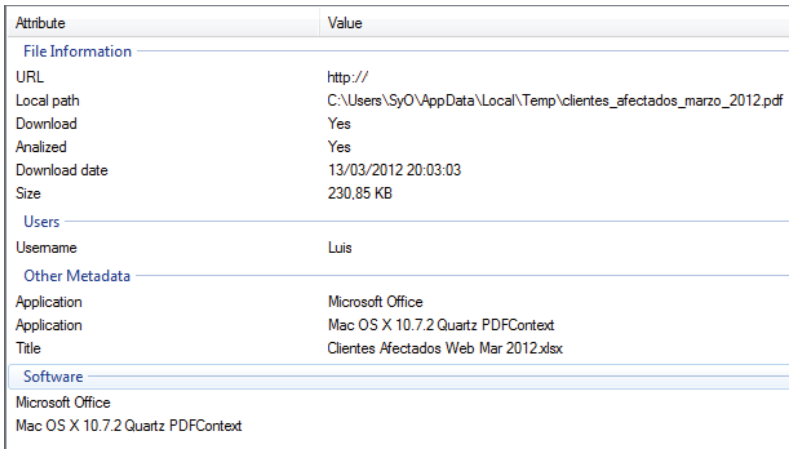
Con el programa anteriormente mencionado, obtenidos los datos podemos utilizar una opción que es la de extraer los metadatos del archivo que hemos bajado, después de realizar este paso procedemos a extraer más información. Recordemos que los metadatos son como huellas que pueden dar más información de la que tiene actualmente.

Figura 3. 10 Extrayendo los metadatos



Fuente: Chema Alonso Cebrián

Figura 3. 11 Obtenido más información de la habitual



Attribute	Value
File Information	
URL	http://
Local path	C:\Users\SyO\AppData\Local\Temp\clientes_afectados_marzo_2012.pdf
Download	Yes
Analized	Yes
Download date	13/03/2012 20:03:03
Size	230,85 KB
Users	
Username	Luis
Other Metadata	
Application	Microsoft Office
Application	Mac OS X 10.7.2 Quartz PDFContext
Title	Clientes Afectados Web Mar 2012.xlsx
Software	
Microsoft Office	
Mac OS X 10.7.2 Quartz PDFContext	

Fuente: Chema Alonso Cebrián

En la figura 3.11 tenemos lo que es nombre de usuario, software usado, fechas de creación.

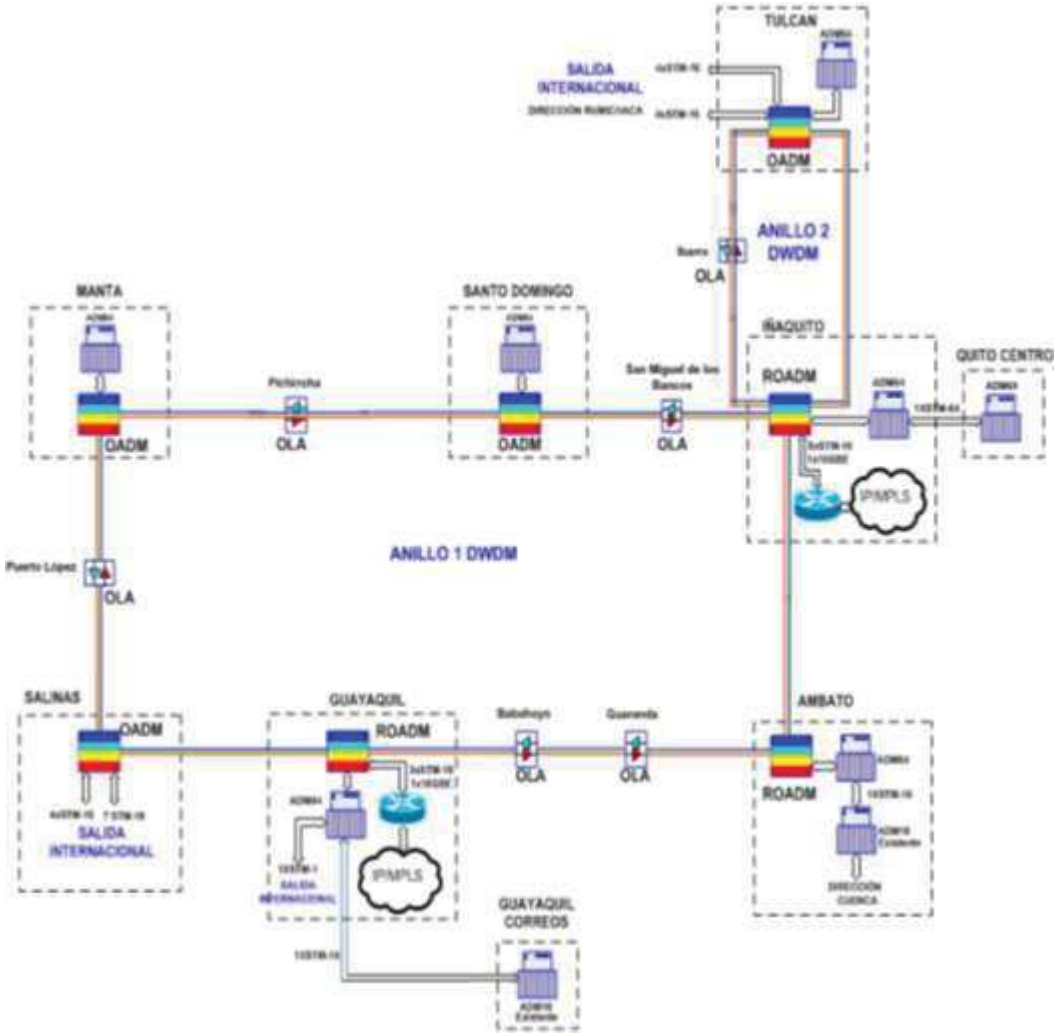
3.2. Información recopilada sobre la red de la Corporación Nacional deTelecomunicaciones E.P.

La Red de la CNT E.P. esta conformada por 2 anillos de fibra óptica. El anillo 1 consiste de 13 segmento: Iñaquito, Latacunga, Ambato, Guaranda, Babahoyo, Guayaquil, Salinas, Puerto Lopez, Manta, Pichincha, Quevedo, Santo Domingo, San Miguel, Iñaquito.

El anillo 2 consiste de 4 segmentos: Iñaquito, Tulcán, Ibarra, Cayambe, Iñaquito.**Topología de Red DWDN C.N.T E.P**[10]

[10] Ref. Tesis de Carlos Luis Hidalgo LLumiquinga, David Alejandro Laguapillo Muñoz (2011), Diseño e Implementación de un laboratorio que permita emular y probar servicios Ip y Mpls de la red de backbone Cisco de la Corporación Nacional de Telecomunicaciones CNT. Páginas Consultadas 126,127.

Figura 3. 12Topología de la RedDWDN C.N.T E.P



Fuente: Tesis de Carlos Luis Hidalgo LLumiquinga, David Alejandro Laguapillo Muñoz (2011), Diseño e Implementación de un laboratorio que permita emular y probar servicios Ip y Mpls de la red de backbone Cisco de la Corporación Nacional de Telecomunicaciones CNT. Páginas Consultadas 126,127.

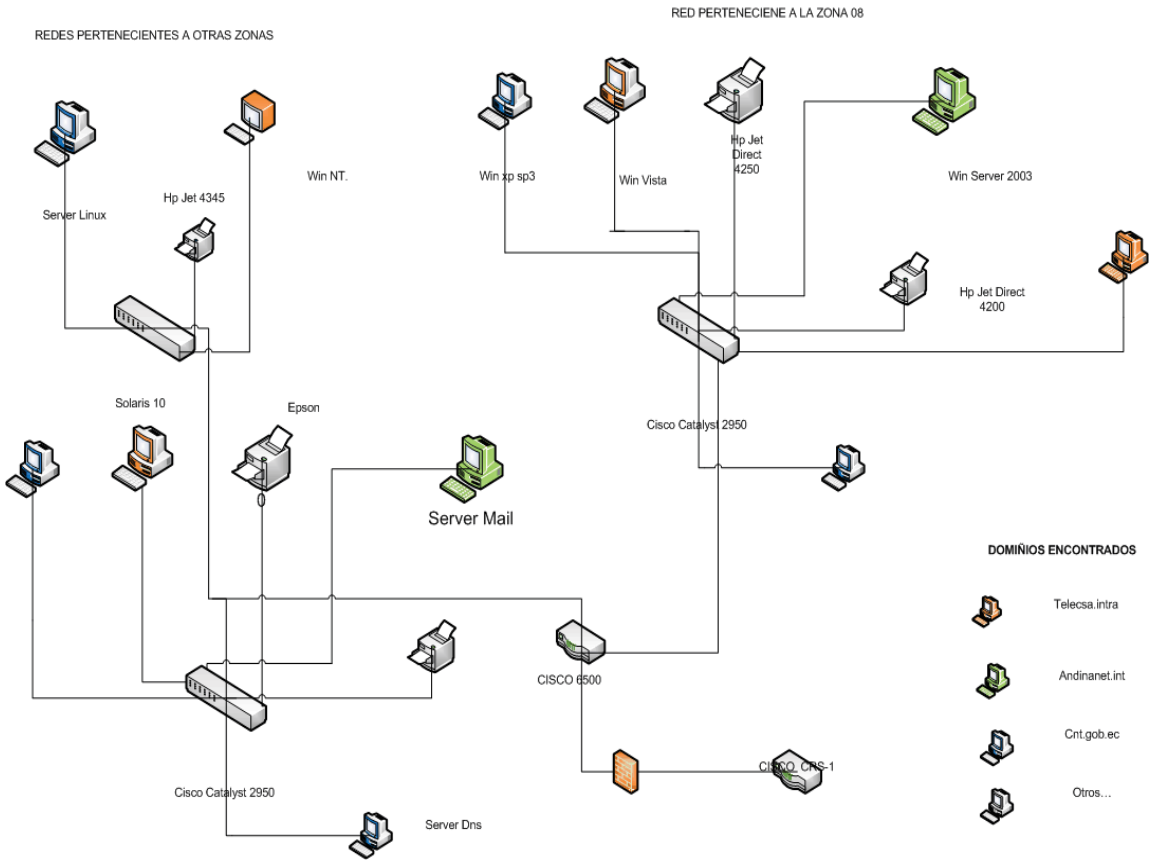
De la Figura 3.12 nos enfocaremos al sector de Iñaquito y Quito-Centro que pertenece a nuestrá área donde se va a realizar las pruebas de hackeo ético.

La red de la Corporación Nacional de Telecomunicaciones es muy extensa ya que está prácticamente en todas las regiones del Ecuador. Nuestro objetivo es centrarnos en la Provincia de Pichincha sector Quito

Dentro de esta ciudad,la Corporación Nacional de Telecomunicaciones estadividida por 8 zonas; dentro de las mismas, se encuentra la zona 8 que es Tumbaco.

Actualmente la red, está conformada por VLAN's las cuales se organizan por departamentos, servicios, servidores, grupos de dominios.

Figura 3. 13 Segmento de Red Zona 08 de Tumbacoperteneciente a la CNT E.P.

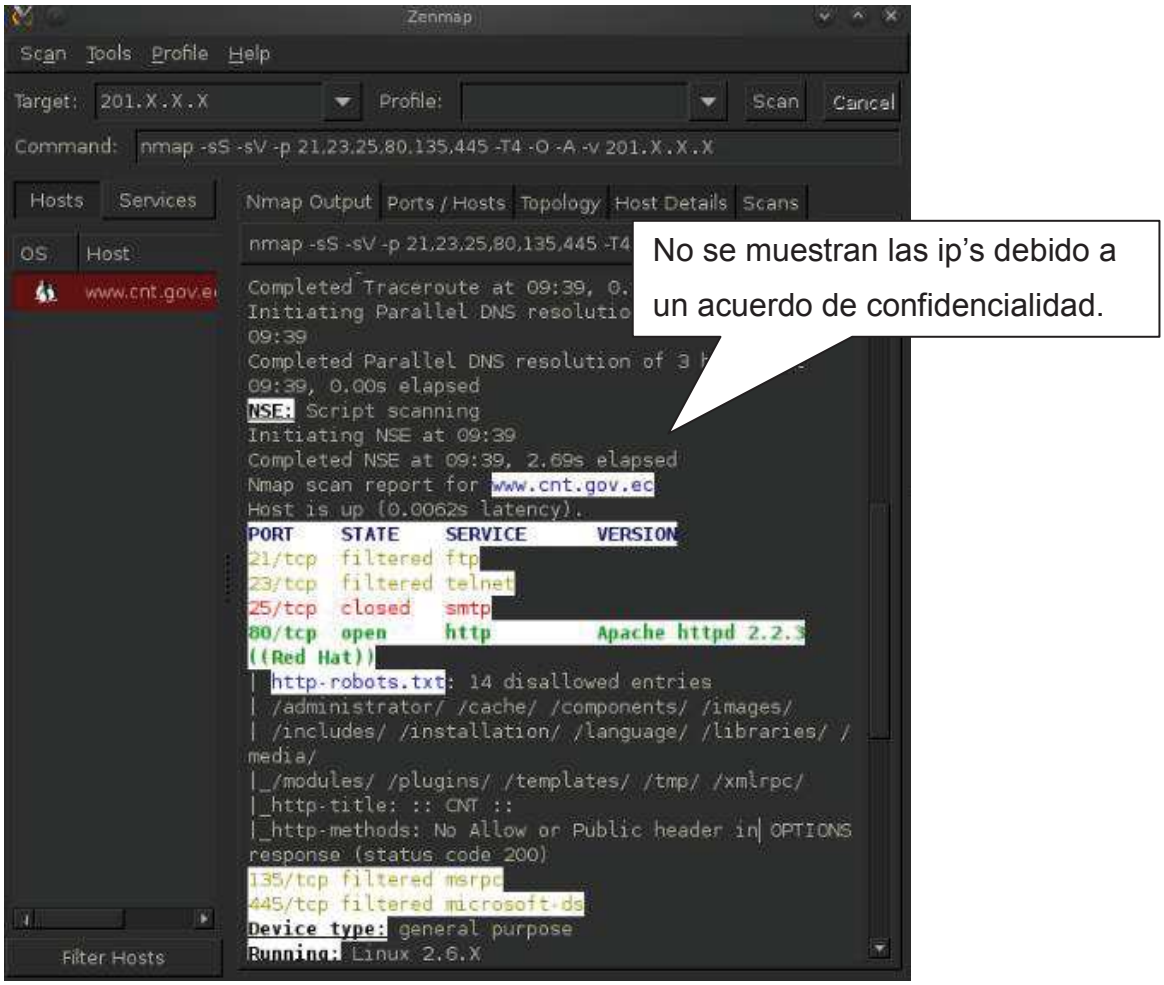


Elaborado por: El Autor

3.3. Conjunto de Pruebas realizadas

Siguiendo con nuestro set de pruebas hemos logrado adquirir direcciones válidas que nos permiten escanear puertos abiertos, con los cuales podemos listarlos y ver que servicios corren sobre los mismos.

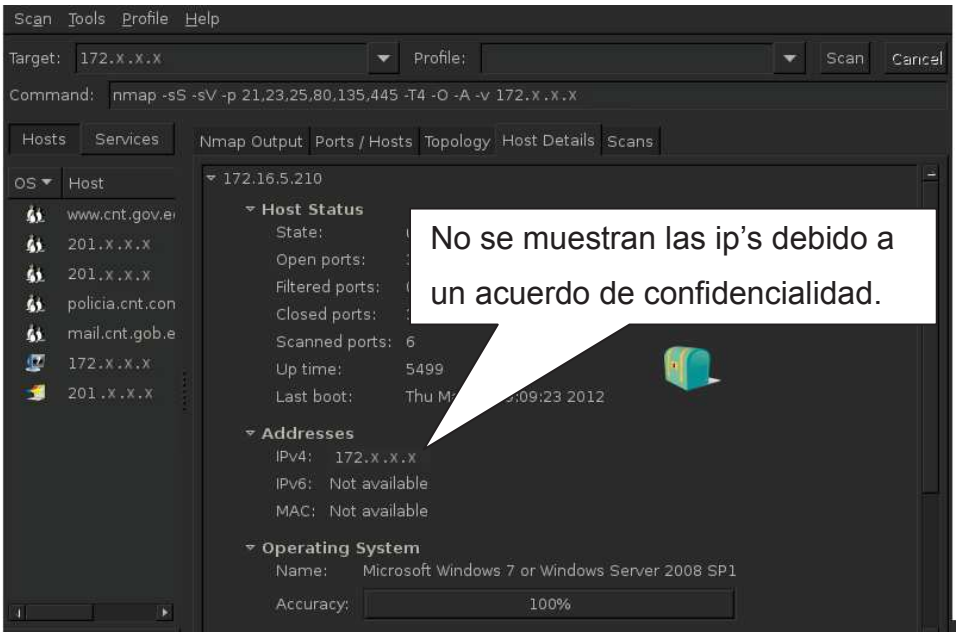
Figura 3. 14Reporte de puertos abiertos



Elaborado por: El Autor

En la figura 3 .14 podemos apreciar que el puerto 80/tcp está abierto y están corriendo servicios como son el de http y apache ver. 2.2.3

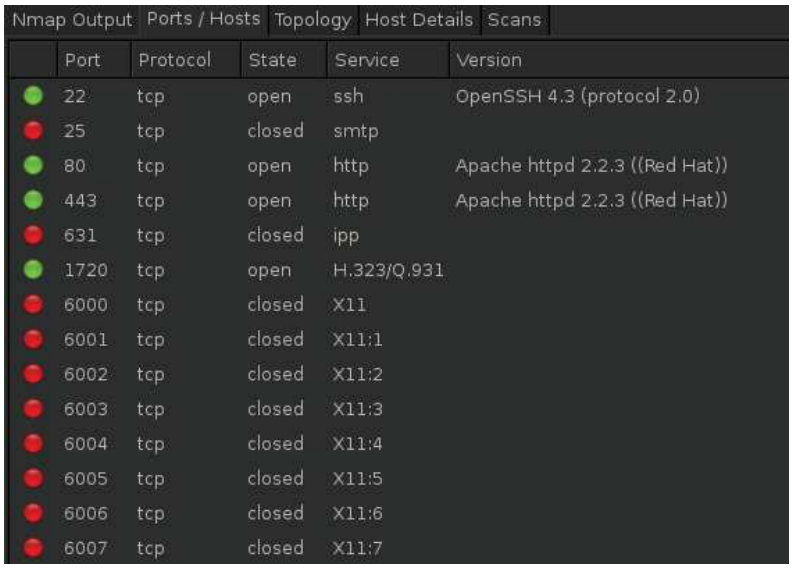
Figura 3. 15Listado de Sistema Operativo que está corriendo



Elaborado por: El Autor

Con herramientas como nmap, hemos logrado escanear nuestro segmento de red perteneciente a la zona 8 de tumbaco dandonos un rango de direcciones, puertos abiertos, servicios que se están corriendo y el sistema operativo sobre los cuales nos esta reportando la herramienta.

Figura 3. 16Listado de puertos disponibles



Elaborado por: El Autor

Una vez enumerada nuestra red seguimos con el siguiente paso que es la **Identificación de vulnerabilidades**, el cuál de todo lo que hemos venido haciendo desde el seguimiento de huellas (footprinting) hasta todos los resultados dados por la herramienta nmap (scanning), vamos a utilizarlos.

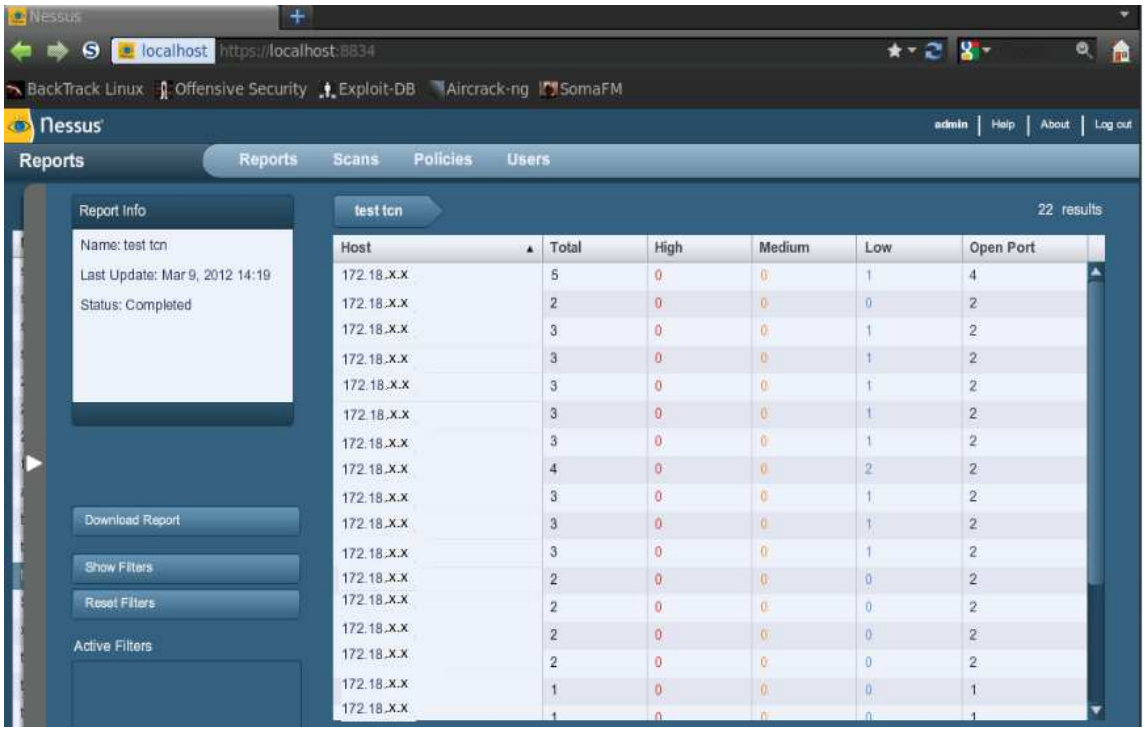
El siguiente paso es listar todos los puertos que tengan la posibilidad de ser atacados utilizaremos la herramienta nessus, el cuál nos indicará mediante un ID si la posibidad es:

Alta (High) Aparte de identificar los puertos, indican el número de vulnerabilidades que pueden ser atacadas y pueden ser utilizados para ingresar en nuestra red.

Mediana (Medium) Identifica vulnerabilidades, que indican un riesgo mediano.

Baja (Low) Identifica vulnerabilidades bajas de poder ser atacados.

Figura 3. 17Listado de Vulnerabilidades existentes



Elaborado por: El Autor

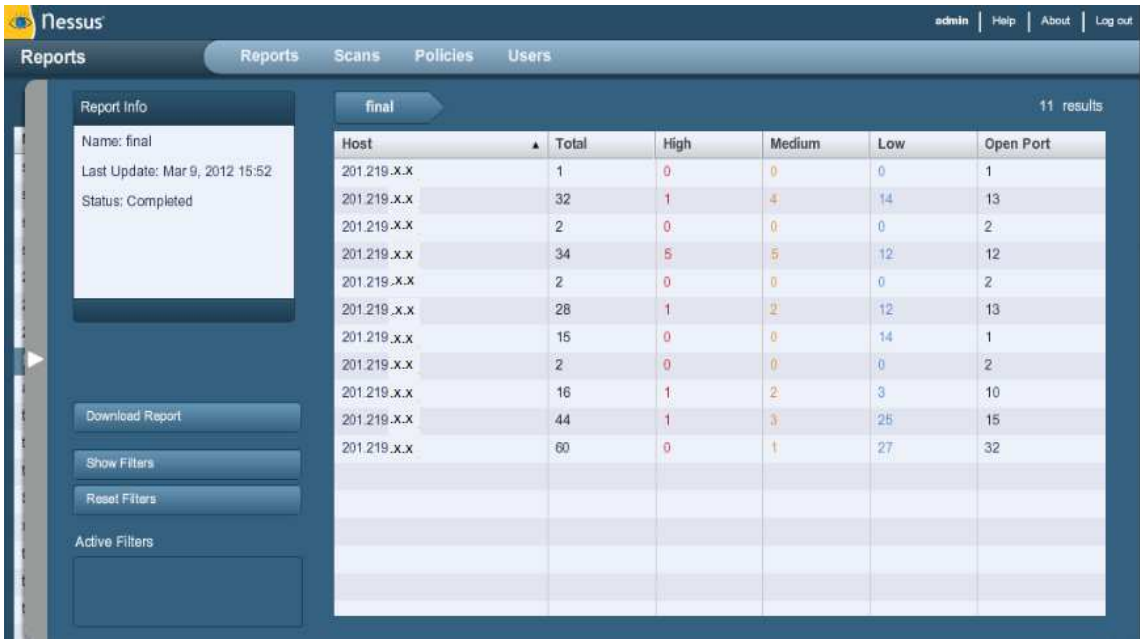
El proceso de verificar las vulnerabilidades en la red es largo ya que dependiendo de toda la información que hemos recopilado y de las especificaciones que le demos a la herramienta nos dará todos los parámetros que queremos encontrar.

En el ejemplo de la figura 3. 17 se realizó el escaneo de 16 ips, dentro de las cuales ninguna mostró un nivel alto de poder ser atacada, con este reporte nuestra prueba no podría ser realizada ya que no existen vulnerabilidades que atacar; como se puede ver también se listan el número de puertos abiertos.

Por razones de seguridad y de confidencialidad no se muestran las Ips que están siendo escaneadas por nosotros.

Se escanean diferentes redes, con el objetivo de buscar una dirección que me indique que tenga vulnerabilidades y así poder explotar[11] las vulnerabilidades que encuentre en esa máquina.

Figura 3. 18 Listado de vulnerabilidades alto

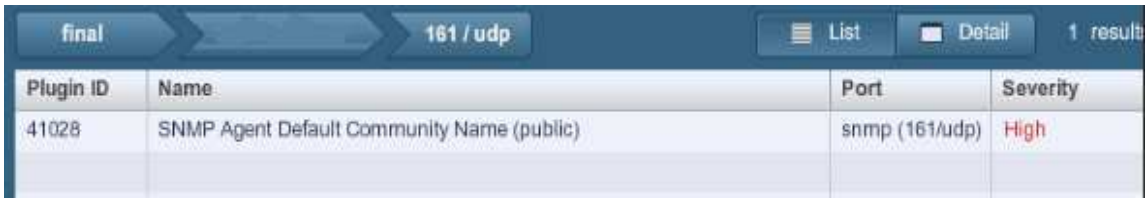


Elaborado por: El Autor

En la Figura 3.18 se encuentran escaneando más direcciones Ips, como podemos observar en la columna **High** se presenta el número 1, el cual nos indica que en esa dirección puede existir una amenaza, posiblemente se puede convertir en ataque, a su lado nos reporta que tiene como alrededor de 13 puertos abiertos con los cuales se podría explotar sus vulnerabilidades y poder tomar control de ese equipo.

[11] Explotar .- encontrar fallas en un sistema.

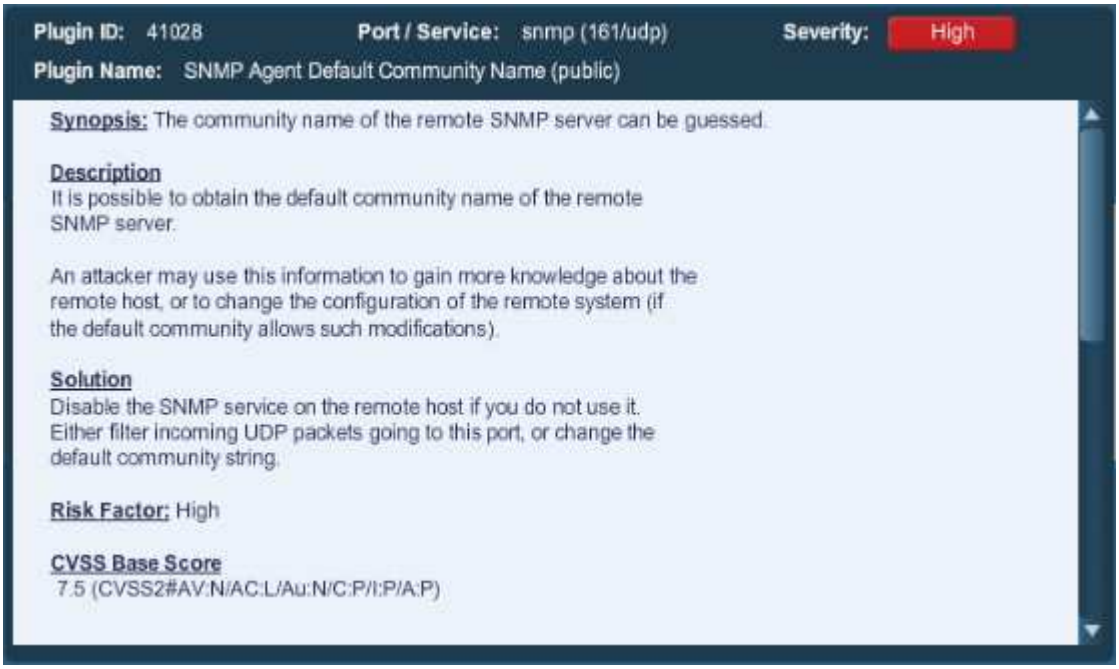
Figura 3. 19 Detalle de la Vulnerabilidad



Elaborado por: El Autor

Además de identificar la vulnerabilidad nos da un ID, un detalle, el número de puerto e indica que el riesgo es alto para ser atacado.

Figura 3. 20 Detalle de la Vulnerabilidad



Elaborado por: El Autor

Como podemos ver en la Figura 3.20 nos da en detalle la vulnerabilidad que se ha encontrado. Siguiendo con el procedimiento detallado en el **capítulo 1** vamos a explotar la vulnerabilidad esto quiere decir que con el ID que hemos encontrado existe páginas donde se listan las vulnerabilidades como son:

http://www.exploit-db.com/ y http://www.securityfocus.com/

Y se pueden ejecutar códigos para poder explotar la misma vulnerabilidad. La herramienta que nos ayuda a explotar esta vulnerabilidad es **Metasploit** que es open-source, la cuál mediante solo unos pocos comandos y con un intérprete como meterpreter nos va a permitir ejecutar el exploit y así tomar control total o parcial de nuestra víctima.

Como nuestro objetivo es el hackeo ético solo se realizará hasta la fase de listar las vulnerabilidades y emitir el informe, debido al acuerdo que se firmó con la Corporación Nacional de Telecomunicaciones E.P, según el anexo 4 Sobre la confidencialidad, en el cuál la persona que se encarga de realizar este tipo de pruebas se compromete a ser custodio de la información y a no divulgarla manteniendo la confidencialidad de la misma, en el caso que no se acate la disposición y el testeador incurra en algún tipo de daño sea material o físico será sancionado de acuerdo a las leyes vigentes estipuladas.

Una vez terminadas las pruebas procederemos a emitir el informe en el que se detalla todo lo que hemos encontrado en nuestra búsqueda.

3.4. INFORME SOBRE EL PENTESTING REALIZADO A LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES

3.4.1. RESUMEN EJECUTIVO

Se ha contratado un servicio para realizar un test de penetración en la Corporación Nacional de Telecomunicaciones E.P.

La evaluación fue conducida en una manera que se simulaba ser un atacante malicioso enfocado a un objetivo (target) de la compañía con el objetivo de:

- Identificar ataques remotos los cuales podrían penetrar las defensas de la Corporación Nacional de Telecomunicaciones E.P.
- Verificar el estado de las configuraciones actuales.
- Preparar a equipos remotos para cualquier anomalía
- Listar las vulnerabilidades encontradas.

3.4.2. Resumen de Resultados

El reconocimiento de la red fue hecho con las herramientas anteriormente mencionadas, como se empezó con el tipo de hackeo black box en el cuál, el administrador de la red no nos proporciona información y nosotros empezamos a descubrir con técnicas como Ingeniería Social. Realizamos el seguimiento de las huellas (footprinting)[12] en la que el testeador, trata de recoger información de cómo está conformada la red.

3.4.3. Servidores Encontrados

Tabla 3. 1 Servidores Encontrados

NOMBRE	ROL	SOFTWARE
Server CNT	Servidor Web	Linux 2.6.9 -2.6.27
WMweb	Servidor HP 4200 PSA de Impresiones.	Linux 2.4.35, Linux 2.4.21
Policía_cnt	Servidor aplicaciones	Linux 2.6.9 -2.6.27
Uiodm_andina		Win Server 2003 SP1-SP2
Mail_cnt	Servidor de base de datos	Linux 2.6.23 / Serv 2008 R2 Standard
63.x.x.x	Lotus, compartición de datos dentro la red interna de una forma eficiente.	nt4/win 98
200.x.x.x	Microsoft IIs 6.0	Win serv 2003

Elaborado por: El Autor

Con las herramientas mencionadas en el capítulo 2 como nmap, autoscan, netifera y angryipscanner encontramos algunas vulnerabilidades como puertos abiertos, sesiones ftp con administrador anonymous habilitados, etc.
Localizados algunos servidores nosotros podemos realizar un escaneo más personalisado como poder hacerlo sobre los puertos que estén abiertos comprobando que actualizaciones existen en ese momento.

[12]Footprinting .- es una herramienta utilizada para seguir rastros.

Tabla 3. 2 Cuadro Resumen de Puertos, Servicios y Sistemas Operativos pertenecientes a Servidores.

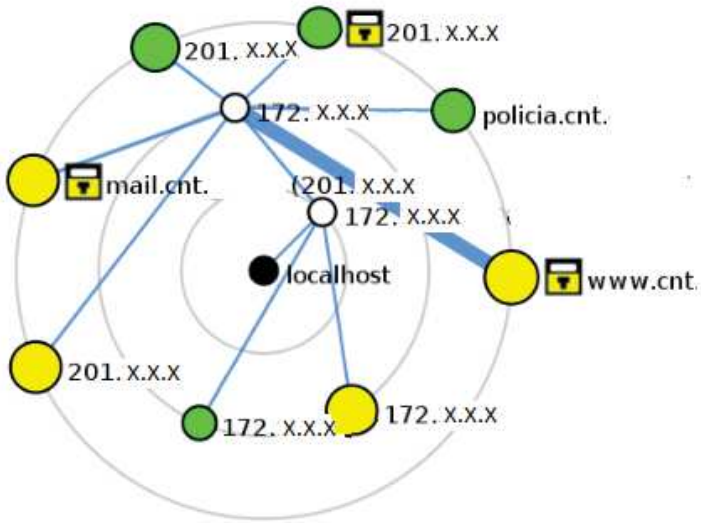
NOMBRE	IP	PUERTO	SERVICIO	VERSIÓN	FUNCIÓN
server_cnt	201.x.x.x	21/tcp filtered	ftp		Servidor Web
		23/tcp filtered	telnet		
		25/tcp closed	smtp		
		80/tcp open	http	Apache httpd 2.23 (Red Hat)	
		135/tcp filtered	msrpc		
		445/tcp filtered	microsoft-ds		
wmweb	201.x.x.x	21/tcp closed	ftp		Servidor Impresión Hp 4200 PSA
		23/tcp closed	telnet		
		25/tcp open	smtp	Sendmail 8.12.10	
		80/tcp open	http	Apache httpd 1.3.33	
		135/tcp closed	msrpc	(Unix) PHP/4.3.9	
		445/tcp closed	microsoft-ds		
	201.x.x.x	21/tcp filtered	ftp		
		23/tcp filtered	telnet		
		25/tcp closed	smtp		
		80/tcp open	http	Apache httpd 2.23 (Red Hat)	
		135/tcp filtered	msrpc		
		445/tcp filtered	microsoft-ds		
policia_cnt	201.x.x.x	21/tcp closed	ftp		
		23/tcp closed	telnet		
		25/tcp closed	smtp		

		80/tcp open	http	Apache httpd 2.23 (Red Hat)	
		135/tcp closed	msrpc		
		445/tcp closed	microsoft-ds		
Uiodm_andin	201.x.x.x	21/tcp open	ftp	Microsoft ftpd	Propósito General
		23/tcp closed	telnet	Anonymous ftp allowed	
		80/tcp closed	http		
		135/tcp open	msrpc		
		445/tcp open	microsoft-ds	Microsoft Win. 2003 or 2008	
Mail_cnt	201.x.x.x	21/tcp filtered	ftp		Open BSD 4.0
		23/tcp filtered	telnet		Win Server 2008 SP2
		25/tcp open	smtp		Acorp w400g adsl modem
		80/tcp filtered	http		microsoft iis 6.0
		445/tcp open	netbios-ssn		

Elaborado por: El Autor

La topología de la red de la CNT, usando la herramienta zenmap es:

Figura 3. 21 Topología de la red CNT E.P.



Elaborado por: El Autor

Se encontró vulnerabilidades con respecto a aplicaciones:

Tabla 3. 3 Vulnerabilidades con respecto a servicios

	Protocolo	Servicio		INFORMACIÓN	SOLUCIÓN
201.x.x.x	161/udp	snmp Agent Default Comunity		El nombre de la comunidad del Servidor Remoto puede ser adivinado	Deshabilitar el servicio snmp si no se lo utiliza
201.x.x.x	80/tcp	www	php < 4.3.11 / 5.03 Multiple Unspecified Vulnerabilitis	El servidor remoto está afectado por varias vulnerabilidades	Actualizar a PHP 5.0.3 o 4.3.11
			php < 4.3.10 / 5.03 Multiple Vulnerabilites	El servidor web remoto es vulnerable a varias fallas	Actualizar a PHP 5.0.3 o 4.3.11
			Obselete Web Server detection	El servidor web está obsoleto	Remover el servicio o actualizarlo
			Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow	La versión Apache del servidor es vulnerable a un ataque de desbordamiento.	Actualizar a 1.3.37
	161/udp	snmp Agent Default Comunity		El nombre de la comunidad del Servidor Remoto puede ser adivinado	Deshabilitar el servicio snmp si no se lo utiliza
201.x.x.x	161/udp	snmp Agent Default Comunity		El nombre de la comunidad del Servidor Remoto puede ser adivinado	Deshabilitar el servicio snmp si no se lo utiliza
201.x.x.x	3636/tcp	Apache HTTP Server Byte Range		El servidor web corriendo en el host remoto está afectado por una vulnerabilidad de	Actualizar a Apache httpd 2.2.21

		DoS		denegación de servicios	
201.x.x.x	161/udp	snmp Agent Default Comunit y		El nombre de la comunidad del Servidor Remoto puede ser adivinado	Deshabilitar el servicio snmp si no se lo utiliza
	21/tcp	ftp			
	81/tcp	www			
	81/udp	host2 -ns			
	161/udp	snmp Agent Default Comunit y			
	232/tcp	unknown			
	135/tcp	epmap			
	445/tcp	Cifs			
	445/udp	microsoft -ds			
	1033/tcp	dce-rpc			
	1045/tcp	dce-rpc			
	3456/udp	vat			
	15000/ud p	hydap			
201.x.x.x		microsoft iis 6.0	win serv 2003	LINUX 2.63	
				Acorp w400g or 422g wireless adsl modem Montavista embedded Linux 2.4.17	
				Win Serv 2008 sp2	
				Open BSD 4.0	
172.x.x.x	4035/tcp	MS09-004 Vulnerability in Microsoft SQL Server		Código arbitrario puede ser ejecutado en el host remoto a través de SQL	Microsft ha entregado parches actualment e

Elaborado por: El Autor

La información arriba detallada es un resumen de todas las herramientas que se mostró en el capítulo 2, también se puede ver en los anexos un escaneo completo en lo que se refiere al segmento de la red de la zona 08 de Tumbaco perteneciente a la Corporación Nacional de Telecomunicaciones.

La **Ip** que por motivo de confidencialidad no se muestra, así como **la dirección mac**, los tipos de dispositivos que la herramienta los identifica, detalla los **puertos** cabe destacar que los mostrados en este informe son los más relevantes de los 65535, los **servicios que prestan**, **el dominio** con las que se identifican los computadores, la versión del **sistema Operativo**con el que están corriendo.

Con las herramientas que nos ayudan a detectar redes se detectó alrededor de 512 tablas de ruteo en la Corporación Nacional de Telecomunicaciones E.P. con esto queremos indicar que la red es muy extensa ya que fue pionera en las telecomunicaciones.

Figura 3. 22 Escaneo de direcciones sin riesgos altos

Host ▲	Total	High	Medium	Low	Open Port
172.16.	2	0	0	0	2
172.16.	2	0	0	0	2
172.16.	2	0	0	0	2
172.16.	2	0	0	0	2
172.16.	1	0	0	0	1
172.16.	1	0	0	0	1
172.16.	2	0	0	0	2
172.16.	2	0	0	0	2
172.16.	9	0	0	5	4
172.16.	26	0	0	14	12
172.16.	20	0	2	4	14
172.16.	16	0	0	11	5
172.16.	24	0	0	14	10
172.16.	21	0	0	13	8
172.16.	25	0	0	14	11
172.16.	11	0	0	4	7

Elaborado por: El Autor

Los puertos que se detallan como abiertos en la Figura 3.22, se puede atacar a través de ellos ya que están en modo de escucha, esto no significa que siempre que encontremos un puerto abierto implica que podamos identificar una vulnerabilidad.

La fase de pententesting es un proceso que requiere de tiempo y paciencia para lograr nuestros objetivo que es el de verificar cuan segura es una red.

En la fase de reconocimiento de vulnerabilidades se probó en el segmento de red de la zona 08 de Tumbaco perteneciente a la Corporación Nacional de Telecomunicaciones y lo que se pudo identificar fue que en el nivel de penetración solo había niveles Medios hacia la red lo cuál no significan una amenaza contra la red, cabe destacar que quizá no se encontró amenazas ya que como es un segmento de la red, no existía servidores en los cuales poder identificar las amenazas.
Siguiendo con el escaneo de la red se pudo identificar a los Servidores que ofrecían diferentes servicios como correo, datos, web, etc.

Figura 3. 23 Vulnerabilidad Encontrada 1

Elaborado por: El Autor

En la Figura 3.23 se puede ver el tipo de riesgo encontrado en**Severity**: High que indica que se ha encontrado un riesgo alto de seguridad.

En un Servidor Apache se encontró una vulnerabilidad en la que indica que se debe actualizar la versión de Apache a una más reciente.
Ya que la versión que se está corriendo actualmente, en el host remoto puede ser afectado por una vulnerabilidad de Denegación de Servicios. Un atacante puede explotar (tomar el control) esta vulnerabilidad haciendo que el sistema sea inestable.

Figura 3. 24 Vulnerabilidad Encontrada 2

Elaborado por: El Autor

En la Figura 3.24, se muestra otra vulnerabilidad encontrada en un diferente servidor, el riesgo es alto de ser atacado. La versión de este software PHP es muy antigua y vulnerable a varios problemas de seguridad, que podrían bajo ciertas circunstancias ejecutar código arbitrario en un host remoto y así dejando pasar código arbitrario a funciones o haciendo un bypass en modo seguro.

En la Figura 3.24 podemos observar que las fechas de publicaciones son actualizadas y no pertenecen a años anteriores. Debemos tener cuidado ya que si no actualizamos nuestro software, el riesgo de una intrusión es muy alto y esto puede comprometer el desempeño de la red.

Figura 3. 25 Vulnerabilidad 3

Elaborado por: El Autor

En la Figura 3.25 informa sobre un problema con el SNMP, reporta que el nombre de la comunidad del servidor puede ser adivinado.

Es posible obtener el nombre de la comunidad de defecto del servidor remoto SNMP. Un atacante puede usar esta información para ganar más conocimiento, sobre el host remoto, o cambiar la configuración. La solución que se presenta aquí, es que si no se utiliza el servicio de SNMP en el host remoto se debe deshabilitar.

De acuerdo a lo antes mencionado solo se listará las vulnerabilidades que tiene la empresa, pero como **ejemplo tomaremos una máquina perteneciente a otra diferente red en la cual se indicará brevemente como se puede hacer una intrusión y tomar el control parcial o total del equipo.**

Siguiendo con los pasos que se mencionó anteriormente, debemos recolectar toda la información que podemos porque por más mínima que sea, siempre nos va a dar una idea sobre como penetrar a un sistema. Podemos encontrar bastante información sobre la empresa C.N.T lo cual nos ayuda a nuestro objetivo.

Con los DNS obtenidos en el internet, por medio de la Ingeniería Social podemos tomar esta información, para futuras pruebas.

Usando el software y los pasos mencionados antes procedemos a buscar computadores activos que nos indican que están en servicio con la red.

Revisando los computadores empezamos a tener una idea de cómo está internamente funcionado nuestra red. Con un simple comando de d.o.s como es el **ping** y **ipconfig** que indican la ip y puerta de enlace que tiene nuestro computador.

Una parte que no debemos olvidar son los puertos sobre los cuales existe mucha información, actualmente existen 65535 puertos algunos escuchan, otros están abiertos, cerrados, filtrados. Nuestro éxito será que podamos encontrar puertos a los cuales nosotros poder ingresar, que estén en estado **open**y podemos intentar conectarnos y probar.

Existen en la actualidad bastantes escaneadores de red que nos permiten visualizar que puertos están abiertos y con esa información poder seguir adelante en nuestras pruebas.

Una vez obtenida toda nuestra información seguimos adelante con nuestro ataque existen programas que nos permiten enumerar nuestra red e identificar vulnerabilidades, hay programas pagados, trial, con código abierto, etc.

Con programas como los mencionados, realizamos las pruebas respectivas encontrando interesantes resultados. Listando vulnerabilidades verificamos que en un tramo de la red existen **altos riegos** listados en nuestro programa.

Nuestro programa nos ha numerado los posibles riesgos que tiene ese puerto con respecto a la intrusión de personas no autorizadas. Fijémonos que los **altos riegos** los etiquetan y pone números con su respectiva información; en la

cual está indicando sobre el año, autor, motivo de cambio, posibles soluciones y parches para que el equipo no esté vulnerable.

Esta información es de suma importancia ya que podemos utilizar la misma y usarla para explotar las vulnerabilidades del sistema.

Usando herramientas como nessus, en las cual se listan las vulnerabilidades y podemos explotarlas si queremos, es decir, podemos tomar el control total o parcial del equipo remoto, realizar cambios si así lo deseamos sin que los administradores se den cuenta, copiar bases de datos que se pueden vender posteriormente, clonar tarjetas de acceso, crédito, tener acceso a información clasificada como sería direcciones, números de cuenta, teléfonos que nos permitirían con la ayuda de la Ingeniería Social poder obtener más de nuestro objetivo (target).

Figura 3. 26 Listado de vulnerabilidades de ejemplo

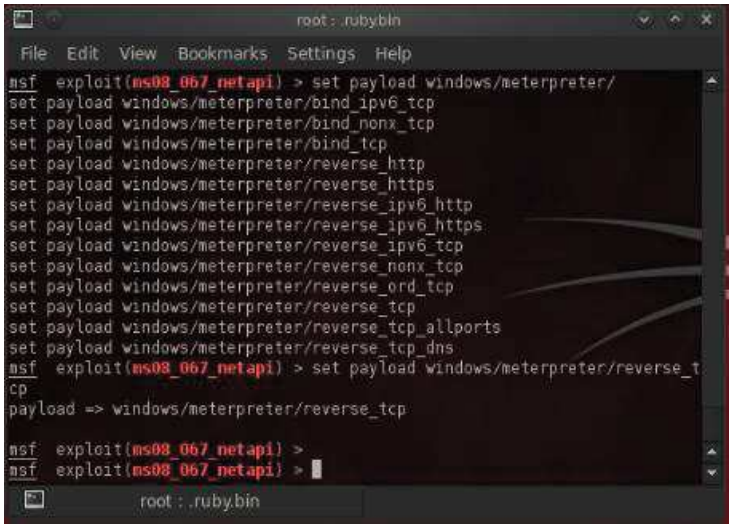
Elaborado por: El Autor

Una vez conocida la vulnerabilidad procedemos a utilizar Metasploit que es una herramienta ofensiva, una vez iniciada esta herramienta, nos ponemos a cargar el exploit[13] que nos identifica la vulnerabilidad y también cargamos el

[13] Exploit .- código que sirve para realizar una específica aplicación..

payload[14]. El payload nos indica que queremos hacer con nuestra vulnerabilidad que en este caso es de Windows.

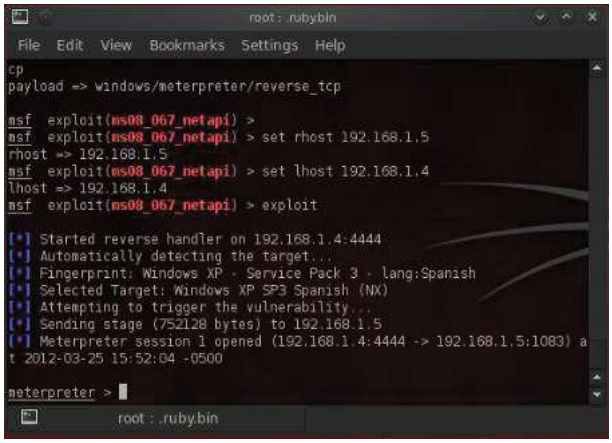
Figura 3. 27 Utilizando Metasploit lanzamos nuestro ataque



Elaborado por: El Autor

Ahora establecemos con el comando **set rhost** la dirección del hots remoto nuestro objetivo, **set lhost** la dirección de nuestra pc. Para ejecutar nuestro ataque digitamos **exploit**y nos aparece como la Figura 3.28 nos despliega un menú de opciones indicándonos que nuestro ataque ha resultado con éxito.

Figura 3. 28 Identificando los host locales y remotos

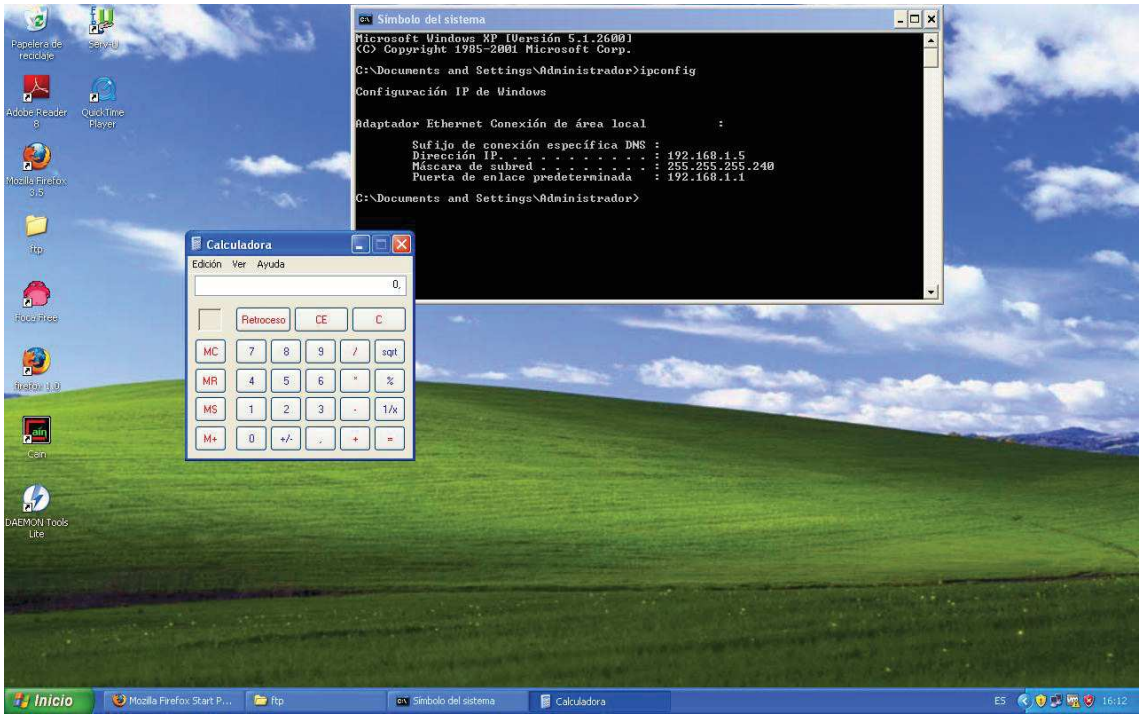


Elaborado por: El Autor

[14]Payload.- sirve para ejecutar un código..

Nos aparece meterpreter que es una poderosa herramienta de metasploit que nos permite ejecutar mediante otros comandos información de nuestra pc objetivo. Digitando comandos como: **Shell** nos podemos ingresar al dos de nuestro equipo, con **PS** podemos listar los procesos que se ejectuan en ese instante. Para verificar que estamos tomando el control del equipo remoto, vamos a mostrar la gráfica del win xp con la calculadora abierta y mediante los comandos mencionados antes vamos a cerrarla desde nuestra ventana de metasploit que se está ejecutando en otro equipo.

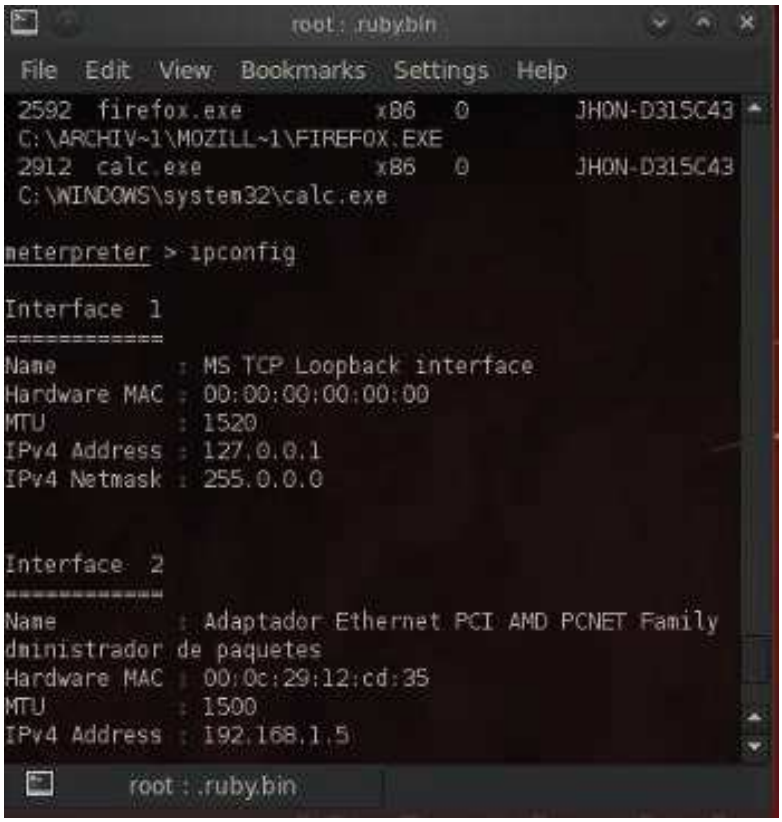
Figura 3. 29 Máquina Objetivo



Elaborado por: El Autor

En nuestra máquina objetivo en la Figura 3.29, verificamos la ip y la calculadora abierta. Con metasploit listamos estos procesos con sus respectivos IDS, y con el comando **kill** podemos remotamente cerrar los procesos que hemos abierto, se puede copiar, bajar archivos, cargar archivos, prácticamente hemos tomado el control de nuestra máquina objetivo.

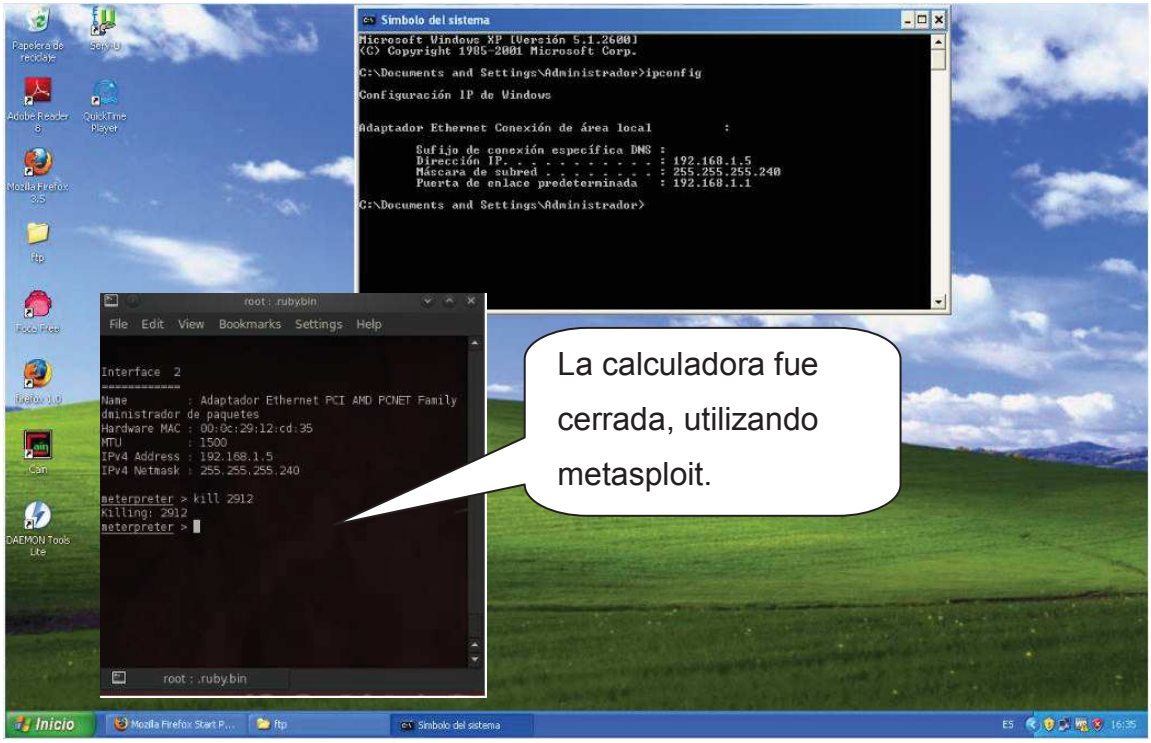
Figura 3. 30 Dirección ip de la máquina objetivo y procesos que corren en Metasploit



Elaborado por: El Autor

Con nuestra máquina podemos listar todos los procesos con su respectivo id, con el id 2912 que en este caso nos asigna la computadora, cerrar la calculadora digitando kill 2912 y verificar en el win xp o desde Metasploit que la calculadora se ha cerrado, verificando que podemos tomar el control del equipo, esto es solo un paso para realizar todo lo que falta deberíamos crearnos una cuenta de administrador, borrar los archivos de registro, copiar información que creamos es importante además deberíamos crear un puerta trasera, que nos permita ingresar al computador objetivo (target) en cualquier momento sin ser detectados por ningún software de última generación.

Figura 3. 31 Tomando Control de la Máquina Objetivo



Elaborado por: El Autor

Queda demostrado que nuestra intrusión en una máquina objetivo ha sido exitosa.

Según varios artículos publicados en CISCO, se sabe que si una persona quiere incursionar en una red podrá hacerlo, lo que podemos hacer con respecto a esto es solo demorar a la persona que quiera hacerlo.

Como medidas para que se eviten la posibilidad de un ataque, se lo hace mediante la aplicación de una Política de Seguridad en la cuál podemos establecer que se mantenga siempre actualizado nuestras versiones de software, con los parches más recientes que nos evitarán de futuros convenientes.

Para una completa descripción sobre todas las políticas que se rigen en la Corporación Nacional de Telecomunicaciones EP véase los anexos.

Cabe mencionar que la Corporación Nacional de Telecomunicaciones, tiene a su servicio gente muy preparada, que se actualizan mensualmente,

Ingenieros, especialistas en diferentes campos de la informática que les ayudan a administrar la red y monitorear ciertos eventos.

Sin embargo se ha podido listar vulnerabilidades que pueden ser atacadas por cualquier persona, este informe se presentará a la parte directiva de la Corporación Nacional de Telecomunicaciones EP,para su respectiva evaluación y correctivos del caso.

.

Valores de la Evaluación de Riesgo (RAVs) y Metodología OSSTMM

Con respecto a la evaluación de riesgos o ravs, no vamos a poder medirla ya que nuestro ataque es solo a nivel de red y el rav se enfoca en todos los parámetros de la seguridad que van desde procesos, personal, políticas, etc. Este a su vez define todos los elementos que interactúan en la seguridad y una vez obtenidos se puede medirlos para establecer que tan segura es nuestra red.

La Metodología OSSTMM fue mencionada para indicar que antes no existían métodos los cuales nos indiquen como proceder a realizar nuestro hackeo ético, pero en la actualidad ya existen varios métodos de los cuales este es uno de los más aceptados, no se aplicó esta metodología, debido a que nuestro ataque solo fue a nivel de red y la metodología abarca todos los procesos como son: personas, políticas, recursos, bienes, etc.

3.5. Costos

Este proyecto es muy realizable gracias al software disponible en el Internet como es el opensource, software de prueba; que nos facilita la ejecución y pruebas sobre nuestro objetivo (target).

Para la elaboración de este informe se utilizó los siguientes materiales:

Tabla 3. 4 TABLA DE COSTOS

HARDWARE Y SOFTWARE UTILIZADOS PARA LAS PRUEBAS					
	Detalle		Cantidad		Precio
1	HP 6710b		1		$ 600
1	Licencia win xp profesional 32 bits		1		$ 100
1	Imagen S.O. para realizar el pentesting		1		$ 10
1	Software Virtualización		1	Uso trial	-------
1	Instalación de Software y hardware para la realización de pruebas.		Aprox. 30 días.		$1500
				TOTAL	**$2210**

Elaborado por: El Autor

CAPITULO IV

4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- En un mundo cambiante y lleno de gente que interactúa con la informática, aprendiendo, investigando e informándose se ha visto la necesidad de tener personal especializado en lo que se refiere a la seguridad en redes quienes colaboran en la administración la red.

- Para ver si nosotros estamos cumpliendo con nuestro objetivo que es el de mantener nuestra red 100% operativa, debemos realizar pruebas que nos indiquen que tan segura es nuestra red, ya que debemos estar siempre preparados para cualquier evento como puede ser desastres naturales, empleados desconformes con la empresa, malas políticas que dan una excesiva restricción a los recursos o a su vez dan una pobre protección con respecto a la seguridad.

- Se ha visto la necesidad de contratar personal especializado de seguridad que realice el Hackeo Ético, el cual nos indicará que tan segura es nuestra red, es muy importante firmar el acuerdo de seguridad, ya que en el mismo indicará que tipo de pruebas se realizará y se indicará el tipo de ataque a realizarse.

- Algunas empresas ven la necesidad de realizar estas pruebas ya que debido al creciente aumento de la tecnología, también se ha incrementado los delitos informáticos y las seguridades tradicionales de antes, se ven impotentes ante el incremento de personas que tratan por cualquier medio de conseguir importante información de cualquier empresa.

- En una parte de las pruebas que se realizaron, se obtuvieron desde la forma más sencillayque se utiliza actualmente, utilizando la Ingeniería Social (se empezó recolectando información con personal de la misma empresa, que sin darse cuenta tenía información muy relevante, la cual nos ayudaría muchísimo más adelante en nuestro objetivo por obtener el acceso hacia un recurso que no nos pertenece), que va desde realizar preguntas simples hasta poder indagar información importante de la empresa, como pudiera ser direcciones de correo, nombres de usuario, fechas de cumpleaños utilizadas muy comúnmente por los empleados para ingresar a sus cuentas.

- Si bien en cierto el Internet nos ofrece mucha información sobre todo lo que realizamos en nuestras labores diarias, accesos, correo, redes sociales, no nos damos cuenta que también estamos dejando huellas, en las cuales cualquier persona que desee puede seguir y darse cuenta que actividades realizadas recientemente fueron hechas.

- Es impresionante ver toda la información que está disponible en la red y en la cual nosotros podemos indagar e informarnos sin tener que estar realizando mucho esfuerzo. Sobre la C.N.T EP que es nuestro objetivo está información sobre quiénes son los administradores, direcciones de correo, direcciones de instalaciones, responsables de gestionar equipos, etc.

- Si bien esto no parece muy importante pero aunque parezca muy limitada la información se puede comenzar con tan poca información como por ejemplo usando la Ingeniería Social podemos hacernos pasar por un administrador de la red, fingir que pasó algún evento como un fallo inesperado del servidor y que tenemos que reiniciarlo para lo cual necesitamos ingresar a los equipos para que se efectúe el cambio.

- La seguridad la realizamos todos, se puede tener bastante información de una persona solo buscando dentro de su basurero el cuál puede tener:

direcciones de correo, fechas importantes, información sobre actualizaciones, nombres de usuario hay personas que por una mala práctica en la seguridad de la información deja anotando las claves en frente a los monitores o simplemente dejan un papel sobre el escritorio o a su vez, dejan por debajo del teclado lo que facilita el acceso a la información.

- El hácking ético que se realizó a la Corporación Nacional de Telecomunicaciones EP, aunque se listaron las vulnerabilidades, no se pudo realizar un ataque ofensivo debido a un acuerdo previamente definido en el cuál se nos declara como custodio de la información razón por la cual esa parte de nuestras pruebas no se pudo realizar.

- A pesar que la Corporación Nacional de Telecomunicaciones, tiene varios sistemas de seguridad actuales como el COBIT[15], se logró listar las vulnerabilidades de la empresa identificando varias vulnerabilidades en las que la empresa deberá tomar más cuidado

.

4.2. Recomendaciones

- Verificar que en el acuerdo de seguridad; se cumpla todo lo que se ha descrito para evitar futuros inconvenientes tanto en la parte que realiza el hackeo ético y la empresa que solicita servicios.

- Para realizar las pruebas de hackeo ético, se debe tomar el tiempo que se necesite ya que si lo realizamos en menos tiempo; los resultados obtenidos no serán reales.
- Una vez revisado el informe sobre hackeo ético, debemos cumplircon los cambios que se indican, para mejorar el desempeño de nuestra red.

[15] COBIT.- Es un conjunto de políticas, procedimientos y soluciones de seguridad

- La confiabilidad con las herramientas que se a trabajado ha sido probada, permitiéndonos tomar el control del equipo. Es recomendable que herramientas que se desconozca sus resultados, realizar pruebas en otras redes y una vez que comprobemos su confiablidad poder usarla para realizar nuestro hackeo ético.

- Las herramientas que se utilicen, siempre tienenque estar actualizadas debido a que en las nuevas versiones se corrigen errores.

- El informe emitido indica que algunas versiones de software no están actualizadas y basándonos en una tesis referenciada en la bibliografía COBIT, en la cual se implementóuna solución referente ala seguridad de Informació mediante COBIT se detectó el mismo problema. Sin la implantación de correctivos, la empresa corre un gran peligro de ser atacada por cualquier persona que tenga algún interés y pueda ocasionar daños a la red y clientes internos que laboran en la misma.

- Se recomienda tener personal dedicado a la seguridad de la red; debido a que los desarrolladores, help desk y demás personal tienen otras tareas que cumplir.

BIBLIOGRAFIA

Libro:

Tori, Carlos, Hacking ético.- 1a ed.- Rosario, 2008, 340 p.

Documentos de Internet:

Fiscalía General del Estado - delitos relacionados con la informática

http://www.cep.org.ec/catalogo/tbl06delitolist.php?t=tbl06delito&psearch=informaticos&Submit=Buscar+%28*%29&psearchtype=

Metodología OSSTMM

http://www.isecom.org/research/osstmm.html

Security Operation Center

http://auditoriasi.blogspot.com/2009/05/soc-ventajas-e-inconvenientes.html

EC-Council Official Curriculum Ethical Hacking & Countermeasures V.6.1

http://www.eccouncil.org

Tésis:

Carlos Luis Hidalgo LLumiquinga, David Alejandro Laguapillo Muñoz (2011), Diseño e Implementación de un laboratorio que permita emular y probar servicios Ip y Mpls de la red de backbone Cisco de la Corporación Nacional de Telecomunicaciones CNT. Páginas Consultadas 126,127.

CRISTIAN ANÍBAL, Romero Zárate Análisis y Diseño de una Estructura de Seguridad Informática empleando COBIT para Andinatel S.A. Trabajo de Grado (Ingeniero). Universidad E.P.N. Facultad de Ingeniería Eléctrica y Electrónica. Disponible en línea http://bibdigital.epn.edu.ec/bitstream/15000/2308/1/CD-3049.pdfpág. consultadas 78,79,80.

Anexos

LISTADO DE ANEXOS

ANEXO 1

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJE DE DATOS[16]

Aquí establece artículos aprobados en Abril del 2002, en el gobierno del ex presidente de la república Gustabo Noboa en los cuales se establece normas y procedimientos para lo que son: archivos y mensajes adjuntos, sobre la información escrita, información original y las copias certificadas, infraestructura de la firma electrónica, duración del certificado de la firma electrónica, revocación de la firma electrónica y suspensión de los servicios de los certificados de firma electrónica y digital, reconocimientos internacionales de la firma electrónica, acreditación de entidades de certificación e información, obligaciones del titular de la firma electrónica y de la seguridad en la prestación de servicios electrónicos.

LEYES VIGENTES EN OTROS PAISES

Si bien en nuestro país no existen reglas para lo que son delitos informáticos en otros países existen ya establecidas leyes para lo que es el hacking, vamos a mencionar brevemente algunas de ellas.

USA[17]

Misión de los Estados Unidos Departamento de Justicia (Departamento de Justicia) es hacer cumplir la ley y defender los intereses de los Estados Unidos, para garantizar la seguridad pública contra las amenazas extranjeras y nacionales, para proporcionar liderazgo federal en la prevención y lucha contra la delincuencia, buscar sólo castigo a los culpables de comportamiento ilegal, y garantizar un trato justo y la administración imparcial de justicia.

---

16 1.- Decreto 3496 (Registro Oficial 735, 31-XII-2002)
2.- Decreto 908 (Registro Oficial 168, 19-XII-2005).
Fuente: FIEL Magister 7.1 (c). Derechos Reservados. 2004.

17 Fuente: http://usdoj.gov

PROHIBICIÓN DE ACTOS O PRÁCTICAS SOBRE SPYWARE.

• (a) **La prohibición** -Es ilegal para cualquier persona, que no es el propietario o usuario autorizado de un ordenador protegido, para participar en injustas o engañosos actos o prácticas que implican cualquiera de las siguientes conductas en relación con el equipo de protección:

- (1) Tomar el control de la computadora.

- (A) como la utilización de equipo para enviar información no solicitada o material

desde el ordenador a otros;

- (B) desviar el navegador de Internet de la computadora, o un programa similar de

el equipo utilizado para acceder y navegar en Internet

(I) sin autorización del propietario o usuario autorizado de la computadora;

y

(Ii) fuera del lugar de que el usuario destina a juicio, a una o más páginas Web, de tal manera que el usuario no pueda ver el contenido de la página Web destinada, a menos que tal desvío está autorizado.

- (C) el acceso, el secuestro, o utilizar el módem o Internet conexión o servicio, para el equipo que cause daños a la computadora o haciendo que el propietario o usuario autorizado o de un Tercero, defraudados por dicha conducta a incurrir en cargos u otros costos para un servicio que no está autorizado por su propietario o usuario autorizado.

- (E) la entrega de los anuncios que un usuario de la computadora no puede cerrar sin un esfuerzo excesivo o conocimiento por parte del usuario o sin apagar el ordenador o el cierre de todas las sesiones de Internet navegador para el ordenador.

- (2) Modificación de ajustes relacionados con el uso de la computadora o al equipo de acceso o el uso de Internet

- (A) la página Web que aparece cuando el propietario o usuario autorizado lanza un navegador de Internet o un programa similar para acceder y navegar por Internet.

- (B) el proveedor predeterminado que se utiliza para tener acceso o de búsqueda de Internet, u otras configuraciones de Internet las conexiones existentes.

- (3) Reunir información de identificación personal mediante el uso de una combinación de teclas función de registro.

- (4) Inducir el propietario o usuario autorizado de la equipo para divulgar información de identificación personal por medio de una página Web que

- (A) es sustancialmente similar a una página Web establecidas o proporcionados por otra persona, y

- (B) induzcan un error al propietario o usuario autorizado, que esta página web es proporcionada por esa otra persona.

WASHINGTON: RCW 9A.52.110[18]

Delitos informáticos en primer grado

(1) Una persona es culpable de delito informático en el primer grado si la persona, sin autorización, intencionalmente obtiene acceso a un sistema informático o base de datos electrónica de otro, y

(A) El acceso se realiza con la intención de cometer otro delito o

(B) La violación implica una computadora o base de datos gestionada por

una agencia del gobierno

(2) Delito Informático en primer grado es un delito mayor clase C[1984 c 273 § 1.]

[18] Fuente : *http://apps.leg.wa.gov/*

MEXICO [19]

Sección 30-45-5 - uso de la computadora no autorizado

Una persona que a sabiendas, voluntariamente y sin autorización, o haya obtenido la autorización, aprovecha la oportunidad de la autorización para los fines que establece que la autorización no se extiende, directa o indirectamente, los accesos, los usos, las tomas, transferencias, oculta, obtiene, copias o retiene la posesión de cualquier ordenador, red informática, los bienes informáticos, equipo servicio, sistema informático o parte de ella, cuando hay

- Daños a la propiedad equipo o servicio informático tiene un valor de doscientos cincuenta pesos ($ 250) o menos, es culpable de un pequeño delito menor;
- daños a la propiedad equipo o servicio informático tiene un valor de más de doscientos cincuenta pesos ($ 250), pero no más de cinco quinientos pesos ($ 500), es culpable de un delito menor;
- daños a la propiedad ordenador o computadora servicio que tiene un valor de más de quinientos dólares ($ 500), pero no más de dos mil cinco cien dólares ($ 2,500), es culpable de un cuarto grado de delito grave;
- Daños a la propiedad ordenador o computadora Servicio tiene un valor de más de dos mil cinco Cien dólares ($ 2,500), pero no más de veinte mil dólares ($ 20.000), es culpable de un tercero grado de delito grave;
- daños a la propiedad ordenador o computadora servicio tiene un valor de más de veinte mil dólares ($ 20.000), es culpable de un delito grave de segundo grado.

[19] Fuente : http://www.gob.mx/

ANEXO 2

METODOLOGÍA OSSTM

Para permitir llevar a cabo esta metodología, se ha creado las certificaciones de Testeador Profesional de Seguridad OSSTMM (OPST) y de Analista Profesional de Seguridad (OPSA).

Un testeador de intrusión sabe que para contrarrestar las defensas, también debe tener una base de datos actualizada sobre los ataques conocidos. Esto ayuda en la rapidez y la efectividad de cada intento. Una y otra vez, determinados "hacks éticos" serán exitosos, y el testeador apreciará mucho estas joyas de su base de datos de ataques, registrando el índice de éxitos.

Armado de esta información, el testeador de intrusión, intentará abusar de la red de su cliente hasta que uno de sus ataques tenga éxito.

Frecuentemente, el cliente es consciente de los riesgos que son necesarios correr para una mejor funcionalidad comercial.

Los tipos de preguntas que debemos hacernos continuamente durante el proceso de testeo son: ¿Qué bienes puedo acceder en qué momento para provocar el máximo riesgo de seguridad? ¿Bajo qué circunstancias encuentro la mayor parte de las vulnerabilidades? ¿Cuándo estoy más propenso a aplicar confidencialidad, integridad y accesibilidad al test? Manteniéndose sistemático y persistente, el efecto acumulativo de estos test dará como resultado un panorama exacto de los riesgos, debilidades, filtraciones de información y vulnerabilidades.

Cuándo testear es tan importante como *qué* testear y *porqué* testear.

Esperar para hacer el test, esperar para reportar los problemas y esperar para solucionarlos, es un error.

Haga las cosas pequeñas, porque en definitiva, todas son cosas pequeñas.

Testear se refiere a los detalles, y muy a menudo los pequeños detalles llevan a las más importantes fallas de seguridad.

Haga más con menos.

Mientras los presupuestos de seguridad sigan siendo bajos, el testeador de seguridad necesita operar con eficiencia y creatividad para hacer más en menos tiempo.

CAPITULO 1

QUE NECESITAMOS SABER

Este manual trata de la seguridad operacional (OPSEC). Se trata de medir qué tan bien funciona la seguridad. Esta metodología le dirá si lo que tienes es lo que queremos que haga y no sólo lo que le dijeron que hiciera.

Para entender mejor cómo OpSec puede trabajar dentro de un entorno operativo, debe ser reducido a sus elementos. Estos elementos permiten cuantificar la superficie de ataque (Attack Surface), que es la falta de específicas separaciones y controles funcionales para ese vector, la dirección de la interacción.

Algunos términos que deberíamos conocer como:

Superficie de Ataque (attack surface).- la falta de especificas separaciones y controles funcionales que existe para ese vector.

Vector ataque (attack vector).- consiste en recursivamente descomponer un problema dentro de dos o más sub problemas del mismo tipo o relacionados, hasta llegar a ser simples para ser resueltos directamente.

Controles (controls).- proporcionan seguridad en las operaciones.

Limitaciones.- los tipos de limitaciones son clasificados por como ellos interactúan con la seguridad en un nivel operacional.

Porosidad (porosity).- todos los puntos interactivos, operaciones, las cuáles son clasificadas como visibilidad, acceso o confianza.

Seguridad (safety).- una forma de protección donde la amenaza o sus efectos son controlados, en orden para ser seguros.

Seguridad (security).- una forma de protección donde una separación es creada entre los bienes y la amenaza.

Rav.- es una escala de medición de un ataque superficial, 100 rav es un perfecto equilibrio en seguridad, menos indica pocos controles. Más de 100 rav muestra más controles delos necesarios que pueden ser un problema ya que los controles suelen añadir las interacciones dentro de un ámbito, así como la complejidad y los problemas de mantenimiento.

Vector.- la dirección de una interacción.

1.1 Seguridad

La seguridad es una función de una separación. Ya sea la separación entre un punto fuerte y las amenazas es que existe o no. Hay 3 formas lógicas y dinámicas para crear esta separación:

1. Mueva el punto fuerte para crear una barrera física o lógica entre él y las amenazas.
2. Cambiar la amenaza a un estado inofensivo.
3. Destruir la amenaza.

La porosidad (**porosity)** reduce la separación entre una amenaza y un acceso. Además, se clasifican como uno de los tres elementos, la visibilidad, el acceso, o la confianza que describe su función en las operaciones que permite, además, los controles adecuados que se añade durante la fase de recuperación de mejorar la protección.

El aumento de la porosidad es la disminución de la seguridad.

Visibilidad.- es un método de cálculo de oportunidad.

Acceso.-la habilidad para interactuar con el bien directamente.
Confianza.- el uso de la métrica se recomienda, lo que permitirá medir qué tan válida es, mediante el cálculo de la cantidad de fiabilidad en la confianza.

1.2 Controles

Los controles son un medio para influir en el impacto de las amenazas y sus efectos cuando una interacción es requerida.

De todos los posibles controles existen 12 principales de las cuales la **identificación,** y la **autorización** no pertenecen.

La razón porque la identificación y la autorización no puede ser expresada operacionalmente se debe a que no se pueden transferir. La identidad existe como es y al mismo tiempo los medios de identificación, como un proceso, es un aspecto operativo,

La autorización como la identificación es otro control de las operaciones que no pueden ser transferidos. Es el control que concede los permisos.

Otra propiedad de la autorización es que requiere identificación para trabajar.

El control de autenticación combina la identificación y la autorización para tener acceso a mapas. El proceso es un simple hecho de saber quién (o qué) es y para qué, dónde, cuándo y cómo se puede acceder antes de que se les conceda el acceso. Dado que la autenticación es un control para la interactividad, es uno de los cinco controles de Clase A, también conocida como la "controles interactivos".

*CONTROLES INTERACTIVOS

La clase A de los controles interactivos forman la mitad de todos los controles de operación.

Tenemos como:

1. Autenticación.- es un control basado en identificación.
2. Indemnización.- es un control a través de un contrato entre el propietario de los activos y la parte que interactúa.
3. Resistencia.- es un control sobre todas las interacciones para mantener la protección de los activos.
4. Subyugación.- es un control asegurando que las interacciones ocurren de acuerdo a procesos definidos.
5. Continuidad.- es un control sobre todas las interacciones.

***CONTROL DE PROCESOS**

Son los controles de la clase B los cuales son usados para crear procesos defensivos.

Tenemos a:

1. No-repudio.- es un control el cuál previene la interacción de la persona denegando su papel en cualquier actividad.
2. Confidencialidad.- un activo mostrado o intercambiado entre partes no puede ser conocido fuera de estas partes.
3. Privacía.- asegurarse que el medio de cómo un activo es accedido, mostrado o intercambiado entre partes no puede ser conocido fuera de estas partes.
4. Integridad.- asegurarse que las partes que interactúan conozcan cuando un activo y un proceso ha cambiado.
5. Alarma.- es un control para notificar que una interacción está ocurriendo o ha ocurrido.

A veces no tener controles es mejor que tener malos controles.

1.3 Objetivos de la Seguridad de Información

Para facilitar el entendimiento tenemos el siguiente cuadro el cuál empareja lo anteriormente hablado.

TABLA A1 1TABLA DE LA SEGURIDAD DE INFORMACIÓN

OBJETIVOS DE LA SEGURIDAD DE INFORMACIÓN	CONTROLES DE OPERACIÓN
Confidencialidad	Confidencialidad Privacia Autenticación Resistencia
Integridad	Integridad No- repudio Subyugación
Disponibilidad	Continuidad Indemnización. Alarma

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

1.4 Limitaciones

Las limitaciones han sido clasificadas dentro de 5 categorías y estas definen el tipo de vulnerabilidad, error, pérdidas en la configuración o deficiencias por operaciones.

Usamos el término de limitaciones para expresar la diferencia de categorizar OpSec cómo falla, más que por el tipo de amenaza.

Con el osstmm la clasificación de las limitaciones son:

1. Vulnerabilidad es la falla o error que: (a) niega el acceso a los activos de las personas o procesos autorizados, (b) permite un acceso privilegiado a los activos a personas no autorizadas o procesos, o (c) permite que

personas no autorizadas o procesos oculten activos o dentro del ámbito de aplicación.

2. Debilidad.- nulifica especialmente los efectos de los 5 controles de interactividad. (autenticación, indemnización, resistencia, subyugación y continuidad.)

3. Preocupación.- es la falla o error que interrumpe, reduce, abusos, o anula los efectos de del flujo o la ejecución de los controles de proceso: el no repudio, confidencialidad, privacidad, integridad y alarma.

4. La exposición.- es una acción injustificada, falla o error que proporciona una visibilidad directa o indirecta de los objetivos o los bienes dentro del canal de ámbito elegido.

5. Anomalía.- es cualquier elemento identificable o no, el cual no ha sido controlado y no puede tenerse en cuenta en las operaciones normales.

Mapeo de las limitaciones

Se tiene la siguiente tabla a1 2 Mapeo de las limitaciones como son su categoría, la seguridad de la operación y las limitaciones.

Todas las categorías que se mencionan en la tabla A12 se explican más adelante en donde se indica la importancia de las mismas sobre cualquier objetivo (target) el cual querramos realizar nuestras pruebas.

Para entender mejor cómo las limitaciones encajan en el marco OpSec, se puede observar:

TABLA A1 2Mapeo de las Limitaciones

CATEGORIA		OpSec	LIMITACIONES
Operaciones		Visibilidad	Exposición
		Acceso	Vulnerabilidad
		Confianza	
Controles	Clase A - Interactiva	Autenticación	Debilidad
		Indemnización	
		Resistencia	
		Subyugación	
		Continuidad	
	Clase B - Procesos	No-repudio	Preocupación
		Confidencialidad	
		Privacia	
		Integridad	
		Alarma	
			Anomalías

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Administrando las limitaciones

Las tres formas más sencillas de manejar las limitaciones es eliminar el área de problema, proveyendo el punto interactivo en conjunto, repararlos, o aceptarlos como parte de los negocios conocidos como la justificación de negocio.

1.5 Seguridad Actual

El papel de los controles es para controlar la porosidad en OpSec. Es como tener diez maneras de controlar las amenazas que vienen a través de un agujero en una pared.

1.6 Conformidad

Son las veces para especificar el uso de las pruebas OSSTMM en un periodo determinado.El gran problema con la conformidad es que requiere una gran cantidad de documentación que tiene que ser versionado y actualizado.

Un test OSSTMM debe dardocumentación que provea un nivel comprensible y verificable de calidad. El uso de la OSSTMM, sin embargo, está diseñado para permitir al analista ver y entender la seguridad. Por lo tanto, con el uso de esta metodología, cualquier cumplimiento es al menos la presentación de pruebas de la gobernabilidad dentro del proceso de negocio de la seguridad.

Capítulo 2 Qué necesitas hacer?

Cuando se realizan pruebas de seguridad, lo que se tiene que hacer es gestionar adecuadamente cualquier complejidad. Esto se hace definiendo apropiadamente los test de seguridad.

2.1 Definiendo un test de seguridad

Estos 7 pasos son los apropiados para definir un test de seguridad.

1. Define qué tú quieres proteger. Allí están los activos. Los mecanismos de protección para estos activos son los **CONTROLES** que se probaría para identificar las **LIMITACIONES.**

2. Identificar el área alrededor de los activos, que incluye los mecanismos de protección, procesos o servicios en torno a los activos. Aquí es donde la interacción con los activos se llevará a cabo. Esta es la zona de combate.

3. Definir todo fuera de la zona de combate que se necesita para mantener los activos operativos. Esto puede incluir cosas que no pueden ser capaces de influir directamente, como la electricidad, alimentos, agua, aire, suelo estable, la información. Este es su ámbito de prueba.

4. Definir cómo interactúa el ámbito dentro de sí mismo y con el exterior. Lógicamente fraccionar los activos en el ámbito a través de la dirección de las interacciones.Estos son los vectores.

5. Identificar qué equipos son necesarios para cada prueba. Dentro de cada vector, las interacciones pueden ocurrir en varios niveles. Estos niveles se pueden clasificar de muchas maneras, sin embargo aquí se han clasificado según su función como cinco canales. Los canales son humanos, físicos, de telecomunicaciones, inalámbricas, y redes de datos. Cada canal debe ser probado por separado para cada vector.

6. Determinar qué información desea aprender de la prueba. El tipo de prueba debe ser definido individualmente para cada prueba, sin embargo, hay seis tipos comunes identificados como: Blind, Double Blind, Gray Box, Double Gray Box, Tandem, and Reversal.

7. Asegurar que las pruebas de seguridad que se han definido, sean de acuerdo a las Reglas de confrontación.

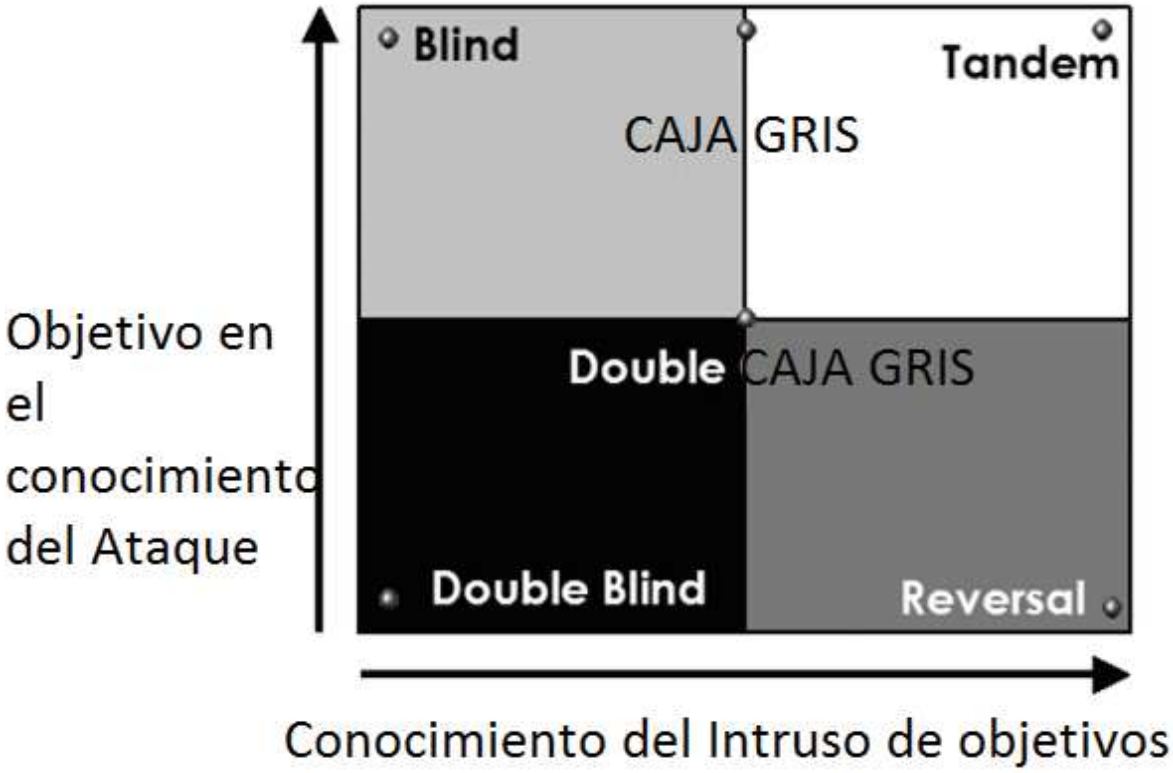
El resultado final será una medición de la superficie de ataque (attack surface). La superficie de ataque es la parte no protegida del Ámbito de un vector definido.

2.2 Ámbito

Los activos pueden ser las propiedades físicas como el oro, la gente, planos, ordenadores portátiles, la típica señal de 900 MHz de frecuencia del teléfono, y el dinero, o de propiedad intelectual, tales como los datos del personal, una relación, una marca, los procesos de negocio, las contraseñas, y algo que se dice sobre los 900 MHz de la señal de teléfono.

2.3 Tipos comunes de pruebas.

Estos seis tipos diferentes, según la cantidad de información que el testeador sabe acerca el objetivo.



Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Blind.- el analista se involucra con el objetivo (target), sin ningún conocimiento previo de sus defensas, activos, o canales.

Double Blind.-el analista se involucra con el objetivo (target), audita las habilidades de prueba del analista. Esto es similar a pruebas Caja Negra Black Box o test de penetración.

Gray Box.- el analista se involucra con el objetivo (target), con limitado conocimiento de sus defensas, activos. La naturaleza de la prueba es la eficiencia. Este tipo de prueba es conocido como **Test de vulnerabilidad.**

Double Gray Box.- el analista se involucra con el objetivo (target), con limitado conocimiento de sus defensas, activos Esta prueba es conocida como **Test Caja Blanca.**

Tandem.- el analista y el objetivo (target) se preparan para la auditoría, tanto sabiendo de antemano todos los detalles de la auditoría. Una auditoríade tándem prueba la protección y los controles del objetivo (target). Esta es una prueba conocida como Caja Cristal o **Crystal Box.**

Reversal.- el analista se involucra al objetivo (target) con conocimiento completo de sus procesos y la seguridad operativa, pero el objetivo no sabe nada de qué, cómo, o cuando el analista estaría testeándolo o probándolo. Esta prueba se llama el ejercicio del equipo rojo o **Red team excercise.**

2.4 Reglas de Compromiso.

Estas normas definen las prácticas aceptables en la comercialización y venta de las pruebas, la realización de trabajos de ensayo y manejo de los resultados.

A. Ventas y Mercadeo.

1. El uso del miedo, la incertidumbre, la duda y el engaño no puede ser utilizado en las ventas o presentaciones de marketing, sitios web, materiales de apoyo, informes o análisis de las pruebas de seguridad con el propósito de vender o proporcionar pruebas de seguridad.
2. El ofrecimiento de libres servicios para penetrar al objetivo (target) está prohibido.
3. Craqueo público, la piratería, y concursos de allanamiento para promover la garantía de seguridad para la venta o comercialización de pruebas de seguridad o de productos de seguridad está prohibido.

4. Se requiere que los clientes se les aconseje la verdad y los hechos en lo que respecta a su seguridad. La ignorancia no es excusa para la consultoría deshonesta.

B. Evaluación / Estimación de entrega

1. La realización de pruebas de seguridad contra cualquier ámbito sin el permiso explícito por escrito del propietario o autoridad competente del objetivo (target) está estrictamente prohibido.
2. Las pruebas de seguridad de los sistemas, obviamente, muy inseguros e inestables, la ubicación y los procesos está prohibida hasta que la infraestructura de seguridad se han puesto en marcha.

C. Contratos y Negociaciones

1. Con o sin un contrato de acuerdo de no divulgación, el analista de Seguridad tiene la obligación para ofrecer confidencialidad y no revelar información de los clientes y resultados de la prueba.
2. Los contratos deben explicar con claridad los límites y peligros de la prueba de seguridad como parte de la declaración de trabajo.
3. El contrato debe incluir permisos claros y específicos para las pruebas que involucran fallas de supervivencia, de denegación de servicio, análisis de procesos e ingeniería social.

D. Definición del Ámbito

1. El ámbito debe estar claramente definido contractualmente antes de verificar los servicios vulnerables.
2. La auditoría debe explicar claramente los límites de las pruebas de seguridad de acuerdo con el ámbito.

E. Plan de Pruebas

1. Las pruebas no puede contener planes, procesos, técnicas o procedimientos que están fuera del área de experiencia del analista.

F. Proceso de Pruebas.

1. El analista debe respetar y mantener la seguridad, la salud, el bienestar y la privacidad del público dentro y fuera de su área a ser testeada.
2. El analista siempre debe operar dentro de la ley de la ubicación física de los objetivos (target), además delas normas o leyes que regulan la ubicación del analista.
3. Pruebas con la gente sólo puede llevarse a cabo en los ámbitos identificados de aplicación y no puede incluir a las personas privadas, clientes, socios, asociados, o de otras entidades externas sin permiso por escrito de la autorización de las entidades.

G. Presentación de informes

1. El analista debe respetar la privacidad de todas las personas y mantener su privacidad por los resultados obtenidos.
2. Los informes deben seguir siendo objetivos y sin mentiras ni maldad dirigidos personalmente.
3. Notificaciones al cliente son necesarias, cada vez que el analista cambia el plan de pruebas, cambia el lugar de prueba de origen.
4. Los informes deben marcar claramente todas las incógnitas y las anomalías.
5. Los informes deben establecer claramente, medidas de seguridad de éxito, fracaso y la pérdida de control.
6. Los informes deben utilizar sólo indicadores cuantitativos para medir la seguridad. Estas métricas deben basarse en hechos carentes de interpretaciones subjetivas.

7. El cliente debe recibir una notificación cuando el informe se envía, como para esperar su llegada y para confirmaracuse de recibo.
8. Todos los canales de comunicación para la entrega del informe debe ser confidencial, de extremo a extremo.

2.5 El proceso de las pruebas de la seguridad operacional

El proceso de pruebas OpSec es una prueba de eventos discretos de un sistema dinámico, estocástico. Esto significa que se van a realizar una secuencia cronológica de las pruebas en un sistema que cambia y no siempre dan el mismo resultado.

El sistema contiene un número finito, pero posiblemente muy grande de variables, y cada cambio en las variables pueden presentar un evento y un cambio de estado. Dado que el entorno es estocástico, hay un elemento aleatorio y no hay medios para predeterminar con certeza todas las variables que afectan el estado del sistema.

Esta metodología de pruebas de seguridad se ha diseñado sobre el principio de la verificación de la seguridad de las operaciones, el objetivo del analista es responder: "¿cómo las operaciones actuales trabajan y cómo funcionan de manera diferente de cómo la administración piensa que trabajan?".

A punto de tener en cuenta es la extensa investigación disponible en el control de cambios en los procesos para limitar la cantidad de eventos indeterminable en un sistema estocástico. Un conocimiento exhaustivo de control de cambios es esencial para cualquier analista.

Una prueba de la seguridad operacional por lo tanto, requiere una comprensión completa del proceso de prueba, elegir el tipo correcto de la prueba, el reconocimiento de los canales de prueba y los vectores, la definición del

alcance de acuerdo con el índice correcto, y la aplicación de la metodología adecuada.

Tenga en cuenta que en una prueba de seguridadcon el proceso de eco, un objetivo que no responde se considera seguro. El proceso eco es de una causa y efecto tipo de verificación.

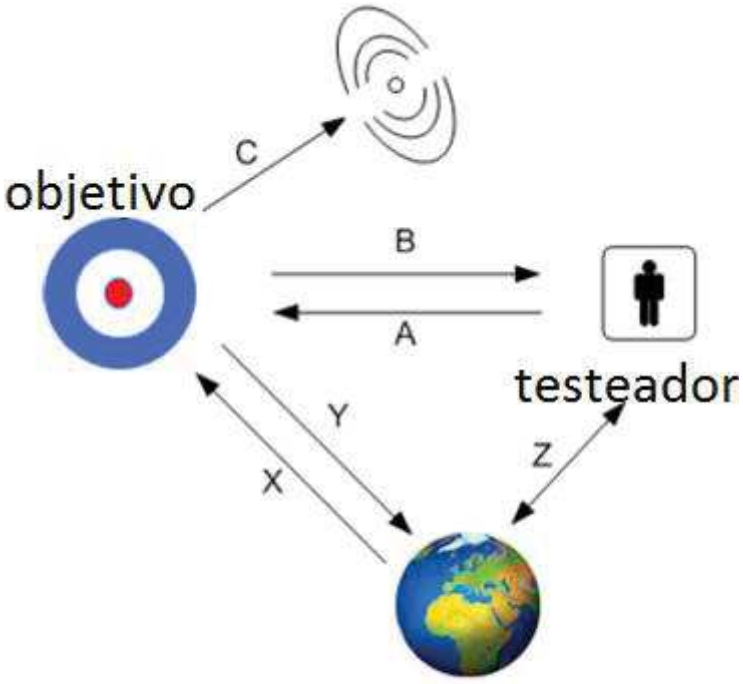
El proceso de prueba de seguridad en esta metodología no recomienda el proceso de eco solo para obtener resultados fiables. Aunque el proceso de eco puede ser utilizado para ciertas pruebas, especialmente cuando el margen de error es pequeño y el aumento de la eficiencia permite un tiempo para ser trasladado a otro intensivo de las técnicas de tiempo, no se recomienda para las pruebas fuera de un entorno determinista. El analista debe escoger cuidadosamente cuándo y bajo qué condiciones aplicar el proceso de eco.

Aunque muchos de los procesos de prueba existen, el **Proceso de cuatro puntos** para las pruebas de seguridad está diseñado para una óptima eficiencia, precisión y rigor para asegurar la validez de la prueba y minimizar los errores en entornos no controlados y estocásticos. Está optimizado para escenarios de prueba en el mundo real fuera del laboratorio. A pesar de que también utilizaagitación, se diferencia del proceso de echo, ya que **permite determinar más de una causa por efecto, y más de un efecto por causa.**

2.6 El proceso de los cuatro puntos

El Proceso de Punto Cuatro (4PP) descompone una prueba desde el inicio hasta su conclusión.Usted no tiene que demostrar cada paso hecho.
Pues bien, el 4PP es las instrucciones específicas y los medios, la información son:

Figura A2 1Interacciones dentro de los cuatro puntos



Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

1. **Inducción.- (z)** establece verdades principales sobre el objetivo del ambiente de leyes y hechos. El analista determina los principios de hecho sobre el objetivo del ambiente donde el objetivo reside. A medida que el objetivo se vera influenciado por su entorno, su comportamiento podrá ser determinado dentro de esta influencia. Donde el objetivo no es influenciado por su entorno, existe una anomalía para ser entendido.
2. **Investigación.- (c)** investigando las emanaciones del objetivo, El analista investiga las emanaciones del objetivo y las pistas o indicadores de las emanaciones. Un sistema o proceso en general, dejará una huella de su existencia a través de interacciones con su entorno.
3. **Interacción.- (A/B)**como las pruebas de eco, estándar y no estándar. El analista se informará o agitara al objetivo para desencadenar respuestas para su análisis.

4. **Intervención.- (X/Y/Z)** cambiando las interacciones de los recursos con el objetivo o entre objetivos. El analista intervendrá con los recursos que el objetivo requiera de su entorno o de sus interacciones con otros objetivos, para comprender los extremos en que se puede seguir operando adecuadamente.

2.7 La trifecta

Esta metodología de pruebas de seguridad tiene una base sólida que puede parecer un poco complicado, pero en realidad es simple en la práctica está diseñado como un diagrama de flujo, sin embargo, a diferencia del diagrama de flujo normal, el flujo, representado por las flechas, puede ir hacia atrás y hacia adelante. De esta manera, es más integral y al mismo tiempo el principio y el fin son claros, la auditoría tiene una mayor flexibilidad. El analista crea un camino único a través de la metodología basada en el destino, el tipo de prueba, el tiempo asignado para la auditoría, y los recursos aplicados a la prueba.

La mejor práctica es sólo lo mejor para algunos, en general, el autor de la práctica. Las operaciones dictan cómo los servicios deben ser ofrecidos y estos dictan los requisitos de la seguridad operacional. Por lo tanto, una metodología que se invoca de forma diferente para cada auditoría y por cada analista puede todavía tener el mismo resultado si el analista completa la metodología. Por esta razón, uno de los fundamentos de la OSSTMM es para registrar con precisión lo que no fue probado, mediante la comparación de lo que fue probado y la profundidad de la prueba con otras, es posible medir la seguridad operativa (OPSEC), basada en los resultados de la prueba.

La aplicación de esta metodología por lo tanto, cumple con el objetivo del analista para responder a las siguientes tres preguntas que componen el Trifecta, la respuesta a las necesidades de OpSec.

1. **Cómo trabajan las operaciones actuales?**

Las métricas derivadas se pueden aplicar para determinar las áreas problemáticas en el ámbito y que los problemas deben ser abordados. Las métricas de esta metodología se han diseñado para mapear los problemas de diferentes maneras a fin de mostrar si el problema es de carácter general o específico.

2. **Cómo trabajan diferente de cómo la administración piensa que ellos trabajan?**

Acceso a las políticas o confianza (o incluso un riesgo) volver a la evaluación del mapa para las diferentes categorías de la métrica. Las categorías proporcionan los valores de estado actual en la que se puede hacer una comparación tanto con un estado óptimo de acuerdo a las políticas y un acuerdo con las amenazas evaluadas.

3. **Cómo tienen que trabajar?**

Donde los indicadores no muestran diferencias entre las políticas o los valores óptimos de confianza (o riesgo) de evaluación de la prueba de seguridad aún muestra que efectivamente existe un problema de protección, independientemente de los controles, tal como se aplica en la política, es posible que claramentedenoten un problema.

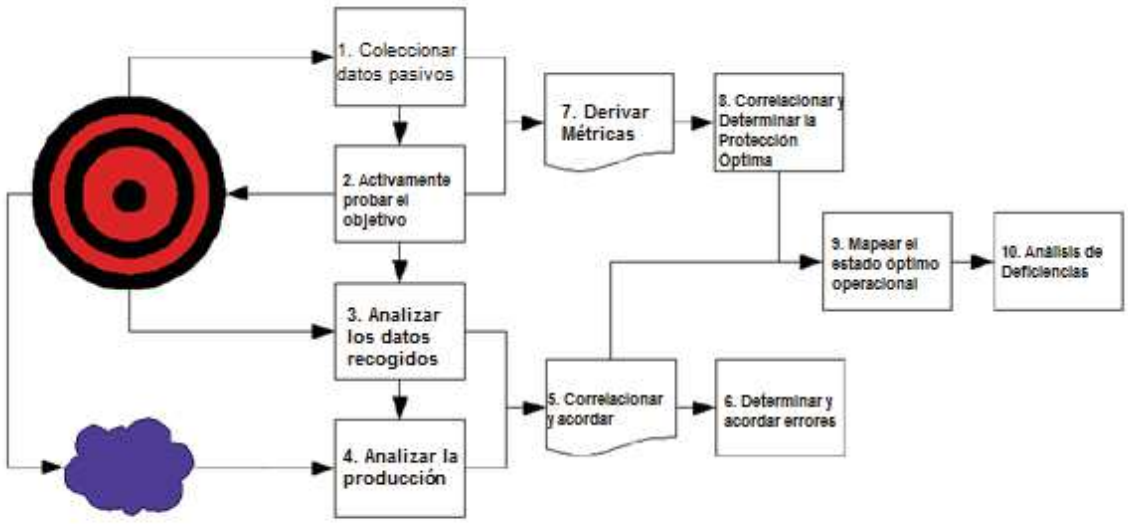
Combinando la trifecta y los cuatro puntos de proceso.

Los pasos se resumen en los siguientes:

1. Pasivamente recoger datos de las operaciones normales para comprender el objetivo (target).
2. Activamente probar las operaciones.
3. Analizar los datos recibidos directamente de las operaciones de prueba.

4. Analizar los datos indirectos de los recursos y los operadores (es decir, los trabajadores, los programas).
5. Correlacionar y conciliar la inteligencia directa (paso 3) e indirecto (paso 4) resultados de las pruebas de datos que determinan los procesos operativos de seguridad.
6. Determinar y reconciliar a los errores.
7. Derivar las métricas de la operación normal.
8. Correlacionar y conciliar la inteligencia entre lo normal y agitado (pasos 1 y 2), las operaciones para determinar el nivel óptimo de protección y control que mejor sería implementado.
9. Mapear el estado óptimo de las operaciones (paso 8) a los procesos (paso 5).
10. Crear un análisis de brecha para determinar qué mejoras son necesarias para los procesos de gobiernonecesarios para la protección y los controles (paso 5), para lograr el estado óptimo de funcionamiento (paso 8),del actual.

Figura A2 2Combinando la trifecta y los 4 puntos de procesos



Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

2.8 Gestión de errores

Al realizar las pruebas los errores no pueden ser culpa del analista, la comprensión de cómo y dónde los errores pueden existir dentro de una prueba es mucho más razonable de esperar que un analista pruebe sin error.

Tenemos los siguientes tipos de errores y su descripción:

1.- **Positivo Falso.-** algo determinado como verdad es en realidad falso.

2.- **Negativo Falso.-** algo determinado como falso es en realidad verdadero.

3.- **Positivo Gris.-** Algunas respuestas verdaderas a todo, incluso si son falsas.

4.- **Negativo Gris.-** Algunas respuestas falsas a todo, incluso si son verdaderas.

5.- **Espectro.-** algunas respuestas verdaderas o falsas, pero la situación real se revela como desconocido. Un espectro puede ser intencional, una anomalía desde el interior del canal, o el resultado del descuido o falta de experiencia del analista. Uno de los problemas más comunes en el proceso de echo es suponiendo que la respuesta es el resultado de la prueba.

6.- **Indiscreción.-** algunas respuestas verdaderas o falsas, dependiendo de cuando se les preguntó. La respuesta indica un particular estado o verdadero o falso pero solo durante un tiempo, el cuál puede seguir un patrón. Si la respuesta no puede ser verificada al mismo tiempo cuando el estado cambia, esta puede prevenir al analista de comprender los otros estados.

7.- **Error de Entropía.-** La respuesta se pierde o se confunde en la señal de ruido, el analista no puede determinar el estado hasta que el ruido se reduce; la entropía puede ser peligrosa, si sus efectos no pueden ser contrarrestados.

8.- **Falsificación.-** los cambios de respuestas dependen en cómo y dónde las preguntas son realizadas.

9.- **Errores de muestreo.-** La respuesta no puede representar al conjunto ya que el ámbito ha sido alterado.El objetivo es una muestra sesgada de un sistema mayor o un mayor número de estados posibles.

10.- **Restricción.-** los cambios de las respuestas dependen de las limitaciones de las herramientas usadas.

11.- **Propagación.-** La respuesta se presume que es de un estado u otro, aunque no se hizo la prueba.

12.- **Error Humano.-** La respuesta cambia dependiendo de la habilidad del analista.

Resultado de las Pruebas

Para medir tanto el rigor de la prueba y la seguridad del objetivo, el uso de esta metodología debe concluir con el **Informe deAuditoría delTest de Seguridad Security Test Audit Report (STAR**), disponible en este manual o en la página web de ISECOM. Requiere de la siguiente información:

1. Fecha y hora de la prueba
2. Duración de la prueba
3. Los nombres de los analistas responsables
4. Tipo de prueba
5. Alcance de la prueba
6. Índice (método de la enumeración de destino)
7. Canal probado
8. Prueba de vectores
9. Ataque métricas superficie
10. ¿Qué pruebas se han completado, terminado o parcialmente completados y en qué medida
11. Cualquier asunto referente a la prueba y la validez de los resultados
12. Todos los procesos que influyen en las limitaciones de seguridad
13. Cualquier producto desconocido, o anomalías

2.9 Declaración

Derechos de divulgación

El contrato de no divulgación, o End User License Agreement (EULA) que niega el derecho a reclamar, anunciar, o distribuir las vulnerabilidades descubiertas.

Responsabilidades

La divulgación completa es útil siempre y cuando no puede hacer daño humano, físico. Además, los consumidores no deberían tener que esperar en la corrección del fabricante para que sus productos sean seguros.

Capítulo 3 Análisis de seguridad.

Análisis de seguridad aquí se refiere a la habilidad para convertir la información en inteligencia de seguridad. En análisis de seguridad, usted produce los hechos aún si los estados no pueden ser conocidos de la información proporcionada. En análisis de riesgos, usted especula y deriva opiniones basadas en información. En análisis de riesgos puede usar análisis de seguridad pero en análisis de seguridad no puede usarse análisis de riesgos.

Analizando la seguridad de todo

La fundamental diferencia entre hacer análisis de riesgos versus un análisis de seguridad es que en **análisis de seguridad, nunca se analiza una amenaza. Debido a que se asume que se conoce que amenazas existen. En análisis de seguridad se estudia y mide los ataques de superficie de y alrededor de un objetivo. Esto permitirá entender donde las amenazas pueden atacar si ellas hacen un ataque.**

3.1 Pensamiento Crítico de Seguridad

La seguridad de pensamiento crítico como se usa aquí es un término para la práctica de usar la lógica y los hechos para formar una idea acerca de la seguridad. Esa idea puede ser una respuesta, una conclusión o una caracterización de algo o alguien para que las pruebas de verificación puedan estar bien definidas. Como una respuesta o una conclusión, el pensamiento crítico de seguridad se establece aquel que tiene más sentido**.**

Técnica de análisis los 6 pasos

Como técnica de análisis se puede reducir a 6 sencillos pasos para determinar los resultados con datos concretos como son:

1. Construir su conocimiento del objetivo de una variedad de recursos.
2. Determinar el nivel global de experiencia para el tipo de objetivo y la cantidad de informaciónposiblemente conocidas.
3. Determinar sus inclinaciones o segundas intenciones en las fuentes de información.
4. Traducir la jerga de las fuentes de información a las palabras similares o conocido para la comparación, porque lo quepuede sonar nuevo o complicado puede ser sólo un truco para distinguir algo en común.
5. Asegúrese de que el equipo de pruebas ha sido debidamente calibrado y el entorno de prueba para asegurar los resultados no están contaminados por la prueba en sí.
6. Asegurar queel estado de las herramientas o procesos de prueba anteriores, se han eliminado lo más antes posiblepara que los resultados no provengan de las mismas.

Falacias como Calificadores

La seguridad no es acerca de los riesgos, essobre la protección y los controles. Para un mejor entendimiento como los calificadores tientan nuestras habilidades para hacer buenos análisis de seguridad, nosotros podemos examinar las falacias como:

1. **Allí no hay tal cosa como 100% seguro.**
2. **Aunque si tú estás seguro, si un atacante quiere ellos ingresarán.**
3. **Allí no hay perfectas seguridades.**
4. **La seguridad es un proceso no un producto.**

Este manual claramente define la seguridad como algo medible.

Un analista está obligado a aplicar el pensamiento crítico de seguridad a la información que se proporciona, así como a las declaraciones que se hacen

acerca de la información analizada de forma objetiva . Inteligencia creada de tal manera que proporciona métricas precisas e imparciales, así como una comprensión clara de cómo la seguridad es deficiente, sin necesidad de calificadores.

Reconociendo el modelo Opsec

Existen dos problemas con la seguridad: La primera es que la tecnología está frecuentemente delante de las habilidades del Analista para entender como todo funciona. La segunda es que irónicamente la deconstrucción de cómo algo trabaja, incluyendo los procesos de negocio pueden ser ilegales para proteger los riegos financieros y la privacidad del fabricante.

Para cada vector y el canal que se analiza, el analista va a guardar una superposición del modelo OpSec sobre los objetivos. Para aplicar el modelo OpSec es simplemente contar con los controles para cada punto de acceso interactivo o confianza, así como el descubrimiento de oportunidades en la forma de visibilidad. Cuando un objetivo es desconocido, comouna caja negra que no se puede abrir, el analista necesita direccionar los controles sobre las interacciones del sistema en su entorno. El proceso se verá así:

1. Lo que es visible en el ámbito de aplicación? ¿Cuál es el valor posible que se sabe? ¿Qué objetivos se puede determinar?
2. ¿Cuáles son los puntos de acceso interactivo a los objetivos y de qué vector o canal?
3. ¿Cuáles son las confianzas dentro del ámbito y sobre qué vector o canal?
4. ¿Cuáles son los controles para esos accesos y confianzas?
5. ¿Son los controles completos o tienen limitaciones?

Incluso una rápida aplicación del modelo OpSec, le dirá si un acceso o confianza se equilibra con los controles.

Esto determinará el tamaño de la superficie de ataque y que los puntos interactivos están abiertos sin ningún tipo de control para gobernarlos.

3.3 Buscar Coincidencias de patrones como un signo de Errores

Si usted comienza buscando exactamente algo en particular, sólo encontrará lo que usted busco. El principal problema se conoce como coincidencia de patrones, el rasgo humano pasa por alto los pasos, a veces sin saberlo, que se consideran innecesarios debido a un "obvio" el resultado.

Para inteligencia aplicable, un resultado es tan bueno como los métodos utilizados para conseguirlos. Sin saber cómo ha llegado a un resultado concreto limitará severamente la acción que puede tomar para solucionarlo.

Para detectar patrones, examine los métodos de prueba y resultados de los datos de los siguientes:

1.Usando pruebas específicasde amenazas en vez de una interacción exhaustiva con la superficie de ataque.

2. La falta de información sobre los procedimientos resultantes detrás de las interacciones con el objetivo.

3. Poca o ninguna información acerca de los controles para varios objetivos.

4. Sólo algunos de los objetivos son presentados para ciertas pruebas y estos tienen resultados completamente negativos.

5. Objetivos no han sido evaluados por razones que son puramente anecdóticos,

6. Pruebas de objetivos que no han sido obviamente asegurados.

3.4 Caracterización de los resultados

El método científico no es una lista de verificación, es un proceso que permite a la inteligencia y la imaginación, una hipótesis que se hace y luego se recogen los datos a través de pruebas y la observación para evaluar esta hipótesis.

El analista se pregunta si se hicieron las pruebas correctas? Se hicieron pruebas suficientes? Fueron los canales o vectores adecuadamente probados?

Se crearon nuevas interacciones que también se prueba?.Para hacer esto debemos caracterizar los resultados.

Para la caracterización de una prueba de seguridad utilizando el método científico consiste en descubrir las propiedades del alcance o ámbito para asegurar que las pruebascorrectas fueron realizadas.

Hay un momento en que una prueba requiere concentración exacta, en un gran número de secuencias repetitivas. En general, tendemos a crear herramientas para manejar este tipo de repetición sin embargo, no siempre es posible debido a la naturaleza dinámica de la prueba como en la interacción con la gente en lugar de objetos inanimados o máquinas. Así como avanza la prueba, el testeador puede usar la intuición para que la presunción de la prueba no seanecesaria. El analista debe prestar especial atención a estas pruebas y buscar signos de intuiciónde parte del testeador.

Las señales de problemas de intuición en pruebas son los siguientes:

1. Las inconsistencias de los tipos de pruebas realizadas a través de múltiples y similaresobjetivos.
2. El número de pruebas disminuyen entre objetivos.
3. La cantidad de tiempo para las pruebas disminuyen entre los objetivos.
4. El mismo objetivo probado más de una vez con las mismas pruebas.

La detección de la intuición en las pruebas muestra un proceso de pruebas inadecuadas y la calidad de los resultados deben ser vistos con sospecha. Volver a las pruebas puede ser necesario.

3.6 Información transparente

Rara vez un análisis de seguridad finalizará con todas las respuestas. Dado que las pruebas dependerán de la OpSec y los controles de un canal en particular y en el vector habrá incógnitas.

El analista debe señalar lo que se ha encontrado con certeza, y no sólo lo que podría ser. Además de información sobre la prueba en sí en cuanto a cómo se hizo, el analista tendrá que informar los siguientes 7 resultados de las pruebas:

1. Incógnitas

Lo desconocido no tiene por qué ser visto como un fracaso del testeador sino que puede ser causada por una protección superior o un ataque que utiliza un gran costo de tiempo o recursos que no es posible en una prueba. Ningún analista debe temer a informar algo que es desconocido.

2. Los objetivos no probados

Al informar lo que no fue probado, es posible hacer comparaciones adecuadas de prueba con las pruebas futuras.

También le ayudará a evitar el engaño por parte de las pruebas sólo el segmento bien protegido de un alcance e ignorando el resto para crear la ilusión de una superficie de ataque pequeño.

3. Limitaciones identificadas y verificadas

Una limitación identificada es la que se ha determinado a través del conocimiento y la correlación.Una limitación verificada es aquel donde ha sido el problema específicamente probado para determinar si existe.

4. Falsos positivos y los medios para generar

Durante las pruebas, algunas limitaciones identificadas no serán vulnerables a los ataques en particular durante la verificación. Esto, sin embargo no llega a la conclusión de que el destino no tiene esas limitaciones.

5.Procesos de Seguridad fallidos y su procedimiento

Durante el análisis, los resultados se muestran algo más que el OpSec, tipos de controles, y el número de limitaciones. Cuando un objetivo tiene una limitación muchas veces hay un proceso o procedimiento detrás de él.

6. Buenas prácticas

Explica la mejor forma para una persona u organización para hacer algo. Desafortunadamente, esto ha sido objeto de abusos hasta el punto que ahora significa que es mejor para todos.

7. Conformidad

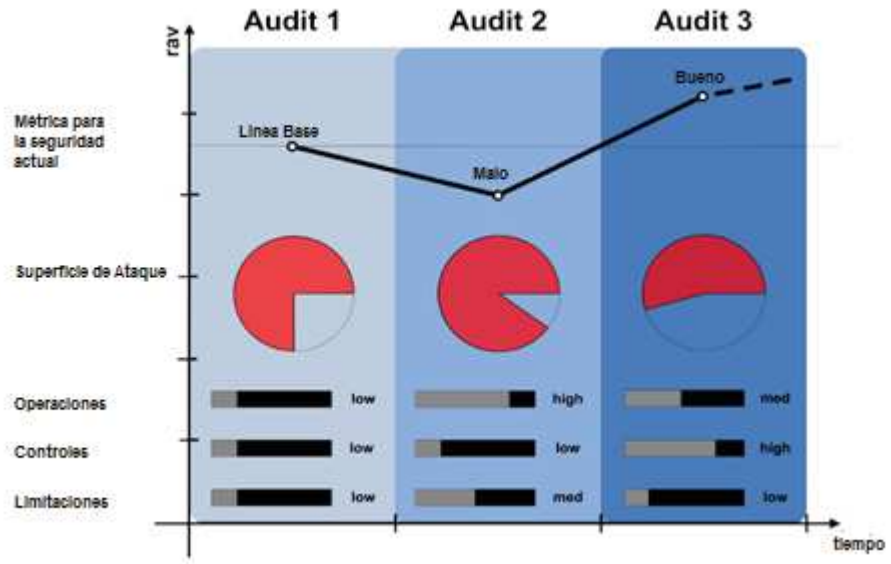
En caso de cumplimiento de los objetivos específicos que deben ser alcanzados, el analista tiene que utilizar los resultados correlacionados para determinar si estos objetivos se han cumplido.

Capítulo 4 - Medidas de Seguridad Operacional

Es una medida constante que nos informa de un recuento de hechos en relación con el mundo físico en el que se vive. Cuando se mide la altura, anchura o longitud de un objeto, estamos utilizando una métrica operacional. Cuando escribimos la fecha, un cumpleaños, o pedir la puntuación de un juego se utiliza métricas operacionales.

Por esta razón, muchas profesionales intentan estandarizar tales cosas como sabores, colores, y las horas de trabajo.De esta forma, los colores se hacen frecuencias, las horas de trabajo se convierten en horas y minutos, los sabores se han convertido en compuestos químicos, y una superficie de ataque se convierte en la porosidad, los controles ylimitaciones.

Figura A4 1Medidas de Seguridad Operacional



Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Utilizando Ravs para medir y rastrear la seguridad de cualquier cosa sobre tiempo.

Por lo tanto, una métrica de seguridad con éxito requiere una prueba que puede ser descrita como la medición de los vectores adecuados.

Estas cualidades se han combinado para crear el Ravs, una descripción imparcial y objetiva de una superficie de ataque.

4.1 Introducción a la RAV

El RAV es una medida a escala de la superficie de ataque, la cantidad de interacciones sin control con un objetivo, que se calcula por el balance cuantitativo entre limitaciones y controles. Tener la RAV's es comprender cómo gran parte de la superficie de ataque se expone. En esta escala, 100 rav (también se muestra como 100% rav por la simplicidad de comprensión, aunque no precisamente en porcentaje) es un equilibrio perfecto y nada menos controla muy pocos y por lo tanto una mayor superficie de ataque. Más de 100 rav muestra más controles que son necesarios y que puede ser un problema, ya que los controles suelen añadir las interacciones dentro de un ámbito, así como la complejidad y los problemas de mantenimiento.

El rav no mide el riesgo de una superficie de ataque, sino que permite la medición de la misma. No puede decir si un objetivo particular será atacado sin embargo, se puede decir que en un objetivo que será atacado, ¿qué tipos de ataques con éxito, el objetivo puede defenderse, la profundidad que un atacante puede obtener, y cuánto daño puede hacer. Con esa información, es posible, entonces, evaluar la confianza (y riesgos) mucho más preciso.

El rav es en realidad varios cálculos por separado de la porosidad, controles y limitaciones, que cuando se combinan muestran el tamaño de la superficie de ataque.

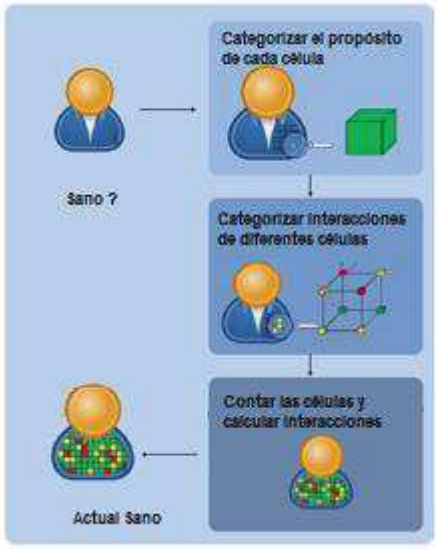
¿Qué es un Rav?

A rav es un poco diferente de otras medidas de seguridad debido a que la cuenta es única del ámbito de aplicación.Para un rav, tanto el número y la

operación se requieren. Esta es la razón por la que rav sólo se puede derivar de las pruebas de seguridad operacional.

Los analistas pueden contar y verificar las operaciones de los objetivos en un ámbito como si fuera un superorganismo. Ellos registran sus interacciones y los controles que rodean esas interacciones. Los clasifican por la operación, recursos, procesos y limitaciones.

Figura A4 2RAV



Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Los Ravs son como el recuento de células y su clasificación por lo que hacen para determinar qué tan bien el organismo se adapta a un medio ambiente.

Ocho respuestas Seguridad Fundamentales

El rav no representan un riesgo cuando este es conocido como:

Riesgo = Amenazas x vulnerabilidad x activos.

El verdadero poder de la RAV sin embargo, es cómo se puede dar respuesta a lassiguientes ocho preguntas fundamentales de seguridad con gran precisión.

1. ¿Cuánto dinero se debe gastar en seguridad?

El Rav indicará la cantidad actual de protección para hacer proyecciones de seguridad ydefinir metas, incluso antes de comprar una solución particular o la aplicación de algunas.

2. ¿Qué debe ser protegido en primer lugar?

Tras el análisis, el RAVmostrará que todo parte del alcance que tiene mayor porosidad y débiles controles.

3. ¿Qué soluciones de protección de lo que necesitamos y cómo debemos prepararlos para una mayor efectividad?

UnRAV completado mostrará los 10 posibles controles operacionales que se aplican paracada objetivo y las limitaciones de los controles. A continuación, puede optar por solucionessobre la base de los tipos de controles que se quieren poner en su lugar.

Esto permite ver los productos para los controles necesarios para ofrecer en las áreas donde los controles son deficientes en la actualidad.

4. ¿Qué tanta mejoría se obtiene por la contratación de seguridad y procesos específicos?

Combinando los mapas a los RAV's del ámbito donde la solución sería colocada, la cantidad de mejoras se puede medir incluso antes de la compra.

5. ¿Cómo podemos medir los esfuerzos de seguridad y mejoras periódicas?

Con auditorías periódicas, el RAV se puede calcular y se compara con el mayor valor.

6. ¿Cómo sabemos si estamos reduciendo nuestra exposición a nuestras amenazas?

Con conocimientos específicos de los controles, se puede deducir fácilmente qué parte o vector del alcance es débil a amenazas específicas y desconocidas.

7. ¿Puede el RAV decirnos lo bien que algo se resiste a los ataques?

Técnicamente, sí, cuanto más se puede controlar el equilibrio de las interacciones, la superficie de ataque y será más capaz el objetivo de controlartipos conocidos y desconocidos de interacciones.

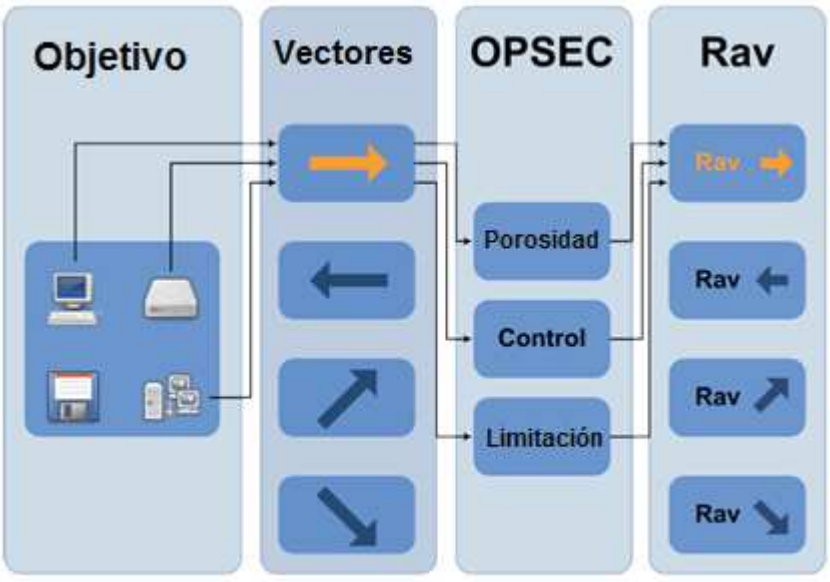
8. ¿Puede el RAV ayudar con el cumplimiento de la normativa?

Cualquier cosa que le ayuda a clasificar todos los controles y puntos de acceso en un ámbito ayudará con las auditorías de cumplimiento. El RAV le ayuda a hacer un buen trabajo en su seguridad bajo el control, incluso puede encontrar fallos en el cumplimiento de reglamentos.

4.2 ¿Cómo hacer un RAV

El RAV requiere una prueba de seguridad con el fin de tener las cosas bien contadas y analizadas las operaciones correctamente. El RAV fue diseñado originalmente para las pruebas de las operaciones, como el OSSTMM, **donde el auditor se centra en el comportamiento del objetivo en lugar de la configuración**. Sin embargo, los experimentos muestran que es posible aplicar el RAV a las pruebas no operativas, así como en análisis de código estático para determinar el nivel de seguridad de software y la complejidad en las auditorías físicas, lista de verificación, de seguridad para determinar el nivel de protección de un espacio físico. El Scare (Análisis de Código Fuente de Evaluación de Riesgos) proyecto hace exactamente esto, mediante la aplicación de la RAV's al código fuente C.

Figura A4 3La sencillez de hacer un test de seguridad



Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

El RAV mínimo se hace calculando la porosidad que son los agujeros en el ámbito de aplicación. El problema con las métricas de seguridad en general, en la determinación de los evaluadores para contar lo que no es posible conocer. Este problema no existe en el RAV.

Usted cuenta con todo lo que está fuera visible e interactivo del ámbito de aplicación y permite la interacción entre autenticado y los objetivos en el ámbito de aplicación. Que se convierte en la porosidad. La siguiente parte es dar cuenta de los controles establecidos por objetivo (target). Esto significa ir objetivo por objetivo y la determinación de que cualquiera de los 10, controles, tales como la autenticación, el sometimiento, no repudio, etc. Cada control tiene un valor de 10% de los poros ya que cada uno proporciona 1/10th de los controles totales necesarias para prevenir todos los tipos de ataque. Esto se debe a que los 10 controles por cada poro es funcionalmente lo mismo que cerrar los poros proporcionan los controles no tienen limitaciones. La tercera parte de la rav es la contabilidad de las limitaciones en la protección y los controles. Estos son también conocidos como "vulnerabilidades". El valor de estas limitaciones proviene de la porosidad y los controles que se establecieron. Con todas las cuentas completadas, el RAV es, básicamente, restando la porosidad y limitaciones de los controles. Esto se hace más fácilmente con la calculadora de hoja de cálculo RAV.

Por desgracia, un analista no calificado puede proporcionar la información incorrecta que se traducirá en un RAV errado.Sin embargo, no hay métrica puede ser inmuney la única manera de asegurar el RAV más preciso es tener pruebas múltiples en el tiempo para hacer la cuenta y estar seguro de que el auditor tendrá la responsabilidad sobre la exactitud de la prueba.

La combinación de canales y vectores

Un requisito importante en la aplicación del RAV es que la verdadera seguridad sólo puede ser calculada por el alcance. Un cambio en el canal, vector, o el índice es un ámbito nuevo y un nuevo cálculo para la verdadera seguridad. Sin embargo, una vez calculado, múltiples campos de acción se pueden combinar

en conjunto para crear una seguridad real que representa una visión más completa de la seguridad operacional de todos los ámbitos.

Calculador RAV

Una manera directa y sencilla para hacer RAV's es utilizar las hojas de cálculo, disponible en la página web de ISECOM. El analista sólo necesita introducir los valores y el resto de los cálculos se realiza automáticamente.

Figura A4 4Calculador RAV

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

4.3 En cuanto a resultados de la prueba en una medición de superficie de ataque

Seguridad Operacional

La medición de la superficie de ataque requiere la dimensión de la visibilidad, confianza y acceso en relación con el ámbito de aplicación. El número de objetivos en el ámbito de aplicación que se puede determinar la existencia de una interacción directa, interacción indirecta, o emanaciones pasiva es su visibilidad. Puesto que la visibilidad está determinada, su valor representa el número de objetivos en el ámbito de aplicación. La confianza es cualquier interacción no autenticadas a cualquiera de los objetivos. El acceso es el número de puntos de interacción con cada objetivo.

CATEGORÍA	DESCRIPCIÓN
Visibilidad	El número de objetivos (targets) en el ámbito de aplicación. Contar con todos los objetivos por el índice de una sola vez y mantener el índice constante de todos los objetivos. Una auditoría HUMSEC emplea a 50 personas, sin embargo, sólo 38 de ellos son interactivos a partir del vector de prueba y de canal. Esta sería una gran visibilidad de 38.
Acceso	Esto difiere de la visibilidad, donde uno, es determinar el número de objetivos existentes. En este caso, el auditor debe contar cada punto de interacción de acceso por la única exploración.
Confianza	Esto difiere de la visibilidad, donde uno está determinando el número de objetivos existentes. En este caso, el auditor debe contar cada confianza de interacción por cada punto de única exploración.

Controles

El siguiente paso en el cálculo de la Rav es para definir los controles, los mecanismos de seguridad puestos en marcha para proporcionar seguridad y protección durante las interacciones.

CATEGORÍA	DESCRIPCIÓN
Autenticación	Cuente cada instancia de autenticación requerida para obtener acceso. Esto requiere que la autorización y la

	identificación hacenal proceso, para el uso adecuado delos mecanismos de autenticación.
Indemnización	Cuente cada instancia de los métodos utilizados para asegurar la responsabilidad y la compensación exacta de todos los bienes dentro del ámbito.
Subjugation	Cuente cada instancia para acceso o confianza en el ámbito estrictamente. Esto difiere de ser una limitación de seguridad en el objetivo ya que se aplica en el diseño o la implementación de controles.
Continuidad	Cuente cada instancia para acceso o confianza en el ámbito que asegura que no hay interrupción en la interacción a través del canal y el vector puede ser causado, incluso en situaciones de fracaso total. La continuidad es el término general para características tales como la supervivencia, equilibrio de carga y redundancia.
Resistencia	Cuente cada instancia para acceso o confianza en el ámbito de aplicación que no deja de abrir o proporcionar nuevos accesos en caso de fallo de seguridad. En lenguaje común, "falla de seguridad".
No-repudio	Cuente cada instancia para el acceso o la confianza que proporciona un mecanismo de no repudio para cada interacción para dar garantías de que la interacción en particular se produjo en un momento determinado entre las partes identificadas. No repudio depende de la identificación y la autorización para establecer adecuadamente la correcta aplicación, sin limitaciones.
Confidencialidad	Cuente cada instancia para acceso o confianza en el ámbito de aplicación que proporciona los medios para mantener el contenido de las interacciones no revelado entre las partes que interactúan. Una herramienta típica para la confidencialidad es el cifrado. Además, la ofuscación de los contenidos de una interacción es también un tipo de confidencialidad, aunque una errónea.
Privacidad	Cuente cada instancia para acceso o confianza en el ámbito de aplicación que proporciona los medios para mantener el método de las interacciones no revelado entre las partes que interactúan. Mientras que "ser privado" es una expresión común, la frase es un mal ejemplo de la privacidad como un control de pérdidas, ya que incluye elementos de confidencialidad. Como un control de pérdidas, cuando algo se hace "en privado", que significa que sólo "el hacer" es privada, pero el contenido de la interacción no puede ser.
Integridad	Cuente cada instancia para acceso o confianza en el ámbito que se puede asegurar que el proceso de interacción y acceso a los activos tiene carácter definitivo y

	no puede estar dañado, parado, continuó, redirigido o revertido sin que se sepa a las partes involucradas. La integridad es un proceso de control de cambios.
Alarma	Cuente cada instancia para acceso o confianza que tiene un registro o hace una notificación cuando se incrementa la porosidad no autorizado y no deseadas para el vector o las restricciones y los controles están en peligro o dañado.

Limitaciones

Finalmente, las limitaciones se verifican siempre que sea posible. Los valores de cada limitación dependen de la porosidad y controles.

Por lo tanto los valores de limitación se calculan en función de la porosidad y los controles del objetivo que se puede encontrar.

CATEGORIA	DESCRIPCIÓN
Vulnerabilidad	Contar por separado cada defecto o error que desafía a la protección de la cual una persona o un proceso puede tener acces, o negar el acceso a los demás, o se oculta activos dentro del ámbito. En telecomunicaciones COMSEC, una vulnerabilidad puede ser una falla en el sistema de teléfono público que permite que los sonidos a través del receptor, una cabina telefónica que permite acceder a cualquier otra persona de la línea de teléfono; un sistema de correo de voz que proporciona mensajes desde cualquier teléfono en cualquier lugar; o una máquina de fax que puede ser consultados a distancia para volver a enviar la última cosa en la memoria para el número del llamante.
Debilidad	Cuenta cada falla o error en los controles de la interactividad: la autenticación, la indemnización, la resistencia, el sometimiento, y continuidad.
Preocupación	Cuenta cada falla o error en los controles de proceso: el no repudio, confidencialidad, privacidad, integridad y alarma.
Exposición	Cuenta cada acción injustificable, defecto o error que proporciona una visibilidad directa o indirecta de los objetivos o los bienes dentro del canal de ámbito elegido.
Anomalías	Cuenta cada elemento identificable o no, sin tener en cuenta en las operaciones normales, por lo general, cuando el origen o el destino del elemento no se pueden entender. Una anomalía puede ser una señal temprana de un problema de

	seguridad. Desde incógnitas son elementos que no se puede controlar, una auditoría adecuada requiere observando todos y todas las anomalías.

4.4 La fórmula de la Seguridad Operacional

El RAV se deriva de tres categorías definidas en el ámbito: seguridad operacional, controles y limitaciones. Con el fin de empezar, debemos primero agregar y asociar a toda nuestra información de entrada en las categorías apropiadas para cada variable de entrada.

La ecuación RAV requiere que cada una de las categorías se le asigna un valor base de la escala logarítmica de los tres factores de la seguridad real de acuerdo con el ámbito.

CATEGORIA		OpSec	LIMITACIONES
Operaciones		Visibilidad	Exposición
		Acceso	Vulnerabilidad
		Confianza	
Controles	Clase A - Interactiva	Autenticación	Debilidad
		Indemnización	
		Resistencia	
		Subyugación	
		Continuidad	
	Clase B - Procesos	No-repudio	Preocupación
		Confidencialidad	
		Privacia	
		Integridad	
		Alarma	
			Anomalías

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Porosidad

La seguridad Operacional, también conocida como la porosidad del ámbito, es el primero de los tres factores de la seguridad real que debe **ser determinada. Inicialmente está se mide como la suma de visibilidad del ámbito (PV), el acceso (PA), y la confianza (PT).**

$$OpSec_{sum} = P_V + P_A + P_T$$

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Al calcular el RAV,sin embargo, es necesario determinar el valor de seguridad de la base operativa, OpSecbase. El valor de seguridad de la base operacional está dada por la ecuación:

$$OpSec_{base} = \log^2(1 + 100 \times OpSec_{sum}).$$

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Ya que el logaritmo de 0 no está definido en el cálculo que teníamos que incluir el 1 +100. El registro de 1 es 0.
Así que si tenemos 0 porosidad y queremos expresar esta falta de interacción como la seguridad perfecta de 100 RAV luego teníamos que añadir uno a la ecuación.

Sin el 1 +100 tendríamos números indefinido en el caso de que las cantidades de cualquiera de esos factores son 0.

Esto es requerido por la metodología debido a la ausencia de interacciones representa una seguridad perfecta y por lo tanto, el logaritmo debe ser igual a 0 para proporcionar el RAV 100.

4.5 La fórmula de los controles

El siguiente paso en el cálculo de la rav es definir los controles de la pérdida, los mecanismos de seguridad establecidos para proteger a las operaciones.

En primer lugar la suma de los controles de la pérdida, la pérdida de 10 categorías de control.

Suma LC, debe ser determinada por la suma.

Controls	**ClassA**		
		Authentication	LC_{Au}
		Indemnification	LC_{Id}
		Resilience	LC_{Re}
		Subjugation	LC_{Su}
		Continuity	LC_{Ct}
	ClassB		
		Non-Repudiation	LC_{NR}
		Confidentiality	LC_{Cf}
		Privacy	LC_{Pr}
		Integrity	LC_{It}
		Alarm	LC_{Al}

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Así, la suma de Control de Pérdidas LC suma i s da como:

$$LC_{sum} = LC_{Au} + LC_{Id} + LC_{\mathrm{Re}} + LC_{Su} + LC_{Ct} + LC_{NR} + LC_{Cf} + LC_{\mathrm{Pr}} + LC_{It} + LC_{Al}.$$

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Pérdidas de Controles

Dado que la combinación de cada uno de los 10 equilibrios de controles que faltan, el valor de una pérdida de OPSEC (visibilidad, accesibilidad, confianza) es necesario determinar la cantidad de controles que faltan, MCsum, con el fin de evaluar el valor de las limitaciones de seguridad. Esto debe hacerse de forma individual para cada una de las 10 categorías de Control de Pérdidas.

La ecuación para determinar los controles de pérdidas para la autenticación (MC_{Au}) es dada por:

$$\text{IF } OpSec_{sum} - LC_{Au} \leq 0$$
$$\text{THEN } MC_{Au} = 0$$
$$\text{ELSE } MC_{Au} = OpSec_{sum} - LC_{Au}.$$

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

El resultado de la falta de control de pérdidas total para cada uno de los 10controles de pérdidas, deben ser añadidos para llegar al valor de un control total de pérdidas (MCsum) como se muestra abajo:

$$MC_{sum} = MC_{Au} + MC_{Id} + MC_{\mathrm{Re}} + MC_{Su} + MC_{Ct} + MC_{NR} + MC_{It} + MC_{\mathrm{Pr}} + MC_{Cf} + MC_{Al}$$

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Controles de verdad

Controles de verdad (TCsum) es el inverso de la pérdida de controles.

La ecuación para la determinación de los controles de verdad para la autenticación es:

$$TC_{Au} = OpSec_{sum} - MC_{Au}$$

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Los totales resultantes para el control verdadero de cada uno de los 10 controles perdidos, deben entonces ser añadidos para llegar al valor total de control True (TCsum) como se muestra abajo:

$$TC_{sum} = TC_{Au} + TC_{Id} + TC_{\mathrm{Re}} + TC_{Su} + TC_{Ct} + TC_{NR} + TC_{It} + TC_{\mathrm{Pr}} + TC_{Cf} + TC_{Al}$$

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Controles de verdad se utilizan para medir la ubicación ideal de los controles. El valor de base también ayuda a eliminarla influencia de la colocación desproporcionada de los controles de seguridad. Los controles de la base real (TCbase)valor se expresa así:

$$TC_{base} = \log^2(1+100\times(OpSec_{sum} - MC_{sum}\times 0.1)).$$

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Basado en la misma idea de los controles de verdad Es cierto que la cobertura real (TCvg) se puede utilizar para medir el porcentaje de controles establecidos en relación con la cantidad óptima y la ubicación de los controles. La cobertura real es entonces a partir de los totales de control de Desaparecidos y la siguiente ecuación:

$$\text{IF } OpSec_{sum} \le 0$$
$$\text{THEN } TCvg = 0$$
$$\text{ELSE } TCvg = 1 - \frac{MC_{sum}}{10\times OpSec_{sum}}.$$

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Controles llenos

Controles llenos, por otra parte, tener en cuenta todos los controles en lugar de una distribución equilibrada. Este valor es importante para medir el valor de la autenticación de dos factores, tenemos la fórmula como:

$$FC_{base} = \log^2(1+10\times LC_{sum})$$

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

4.6 Las limitaciones de la Fórmula

A continuación, las limitaciones son de forma individual ponderado. La ponderación de las vulnerabilidades, debilidades y las preocupaciones se basan en una relación entre la porosidad OpSecsum, los controles de la pérdida y en el caso de las exposiciones y de anomalías de la existencia de otras limitaciones también juega un papel importante.

Una exposición o anomalía no plantea ningún problema a menos que una sola vulnerabilidad, debilidad o preocupación también este presente. Piense en una exposición como un puntero; si hay un puntero que se va a ninguna parte, o en este caso no conduce a nada aprovechable(Vulnerabilidad, debilidad, inquietud) y todos los controles se tienen en cuenta, a continuación, en el momento de la prueba de la exposición no tiene ningún efecto sobre laseguridad y por lo tanto no tiene ningún valor en el RAV.

La tabla siguiente muestra el valor se utiliza para calcular la variable $SecLim_{sum}$, como un paso intermedio entre las entradas de Seguridad Limitación y la variable $SecLim_{base}$la cual es la entrada de la limitación básica para la ecuación RAV.

$$\text{IF } OpSec_{sum} \leq 0$$
$$\text{THEN } MCvg = 0$$
$$\text{ELSE } MCvg = \frac{MC_{sum} \times 0.1}{OpSec_{sum}}$$

Entrada	Valores Pesados	Variables
Vulnerabilidad L_V	$\frac{OpSec + MC}{OpSec_{sum}}$	MC :suma de Pérdida de Controles
Debilidad L_W	$\frac{OpSec + MC}{OpSec_{sum}}$	MC :sumade Pérdida de Controles en Control Clase A
Preocupación L_C	$\frac{OpSec + MC}{OpSec_{sum}}$	MC :sumade Pérdida de Controles enControlClase B
Exposición L_E	$\frac{((P + P)xMCvg+L +L + L)}{OpSec}$	P :sumade Visibilidad P :sumade Acceso $MCvg$:Porcentaje de Pérdida
Anomalías L_A	$\frac{(P x MCvg + L + L + L)}{OpSec_{sum}}$	P :sumade Visibilidad $MCvg$: Porcentaje de Pérdida

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Limitaciones de seguridad Base

A continuación se calcula como el total agregado de cada entrada multiplicada por su correspondiente valor ponderado según se define en la tabla anterior.

$$SecLim_{sum} = \left(L_V \times \frac{(OpSec_{sum} + MC_{sum})}{OpSec_{sum}} \right) + \left(L_W \times \frac{(OpSec_{sum} + MC_A)}{OpSec_{sum}} \right) + \left(L_C \times \frac{(OpSec_{sum} + MC_B)}{OpSec_{sum}} \right) + \left(L_E \times \frac{((P_V + P_A) \times MCvg + L_V + L_W + L_C)}{OpSec_{sum}} \right) + \left(L_A \times \frac{(P_T \times MCvg + L_V + L_W + L_C)}{OpSec_{sum}} \right)$$

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

La ecuación de Seguridad Limitaciones base viene dada por:

$$SecLim_{base} = \log^2(1 + 100 \times SecLim_{sum})$$

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

4.7 La Fórmula actual de la seguridad

Esta es la parte final para el uso de todos los cálculos anteriores en tres aspectos diferentes.

1. Real Delta de Seguridad

El Delta de seguridad actual es útil para comparar productos y soluciones previamente por estimación de los cambios (delta). Podemos encontrar la real Delta Seguridad, ActSec, con la siguiente fórmula:

$$ActSec\Delta = FC_{base} - OpSec_{base} - SecLim_{base}.$$

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

2. Una verdadera protección

Se puede utilizar como una expresión simplificada para la cobertura óptima de un determinado ámbito, donde 100 representa una relación óptima entre la

porosidad, Controles real y las limitaciones de seguridad. Una verdadera protección se calcula:

$$\text{TruPro} = 100 + TC_{base} - OpSec_{base} - SecLim_{base}$$

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

3. Seguridad real

Para medir el estado actual de las operaciones con los controles aplicados y limitaciones descubiertos, un cálculo final es necesario para definir la verdadera seguridad. Como lo indica su nombre este es el valor de la seguridad general que combina los tres valores de la seguridad operacional, controles y limitaciones para mostrar el estado actual.

Seguridad real (total), ActSec, es el verdadero estado de la seguridad proporcionado como un hash de las tres secciones. Una RAV de 100 significa un equilibrio perfecto de la seguridad sin embargo, la seguridad real no es un valor porcentual. Las puntuaciones por encima de 100 indica que el alcance prueba tiene más de lo necesario, que también podría ser la prueba de un gasto excesivo. La última ecuación RAV para la Seguridad reales se presentan como:

$$ActSec = 100 + ActSec\Delta - \frac{1}{100} \times (OpSec_{base} \times FC_{base} - OpSec_{base} \times SecLim_{base} + FC_{base} \times SecLim_{base})$$

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

Capítulo 6 - Flujo de Trabajo

El flujo de OSSTMM comienza con una revisión de la postura del objetivo. La postura es la cultura, reglas, normas, contratos, leyes y políticas que definen el objetivo. Termina con resultados comparativos de las alarmas, alertas, informes o registros de acceso. Este es un concepto de círculo completo en el primer paso es ser consciente de las necesidades de funcionamiento para interactuar con el blanco, y el último paso es la revisión de los registros de la pista de auditoría.

Para el analista, esto es simple: usted sabe lo que tiene que hacer, lo haces, y después de comprobar lo que has hecho.

Esta metodología separa lo que se necesita hacer en este formato jerárquico:

1. CANAL
2. MÓDULO
3. TAREA

El trabajo se describe en la descripción del módulo de auditoría para cada canal en particular. En algunas auditorías se aplican a las tecnologías que pueden tener un carácter de la frontera entre dos o más canales. Por ejemplo, comúnmente se encuentran las redes inalámbricas deben ser probados en tanto los datos del canal y el canal de las redes inalámbricas. Es por eso un plan de pruebas definido correctamente es tan importante. El OSSTMM es plenamente capaz de una revisión de seguridad y por lo tanto, es completamente capaz de aplicar un análisis a un objetivo si los canales son claramente distintos ypor separado o integrado por múltiples canales. Por lo tanto, para todos los objetivos, el analista debe prever la necesidad de definir una auditoría para incluir los canales múltiples. A veces, sólo en investigación que se hacen evidentes si el alcance contiene ningún objetivo en un canal en particular o si el analista se perderá objetivos sólo está disponible en otros canales.

Esta metodología se aplica a los cinco canales. Cuenta con 17 módulos y las mismas propiedades que se aplican a los cinco canales. Mientras que la metodología en sí misma puede ser el mismo, cada canal es diferente en las tareas. Cada módulo tiene una entrada y una salida. La entrada es la información que se utiliza en la realización de cada tarea. La salida es el resultado de las tareas completadas.

Algunas tareas no dan resultado, lo que significa que existen módulos para los cuales no hay entrada. Módulos que no tienen entrada pueden ser ignorados durante las pruebas, pero debe ser documentados. Además, las tareas sin salida no indican necesariamente una prueba inferior, sino que puede indicar una seguridad superior. En detalle, las tareas que no tienen salida resultante pueden significar:

1. El canal fue obstruido de alguna manera durante el desempeño de las tareas.
2. Las tareas no se realizaron correctamente.
3. Las tareas no eran aplicables.
4. Los datos de resultado de la tarea ha sido mal analizados.
5. La tarea revela una seguridad superior.

Es importante que la imparcialidad y la apertura de mente existan en el desempeño de las tareas de cada módulo. El principio primordial de los Estados de auditoría, en relación similar a un sesgo de conformación: ". Cuando uno busca algo, no se espera encontrar, lo que puede llevar a encontrar sólo lo que está buscando".

Unos análisis de confianza anteriores se pueden incorporar para determinar el alcance de acuerdo a los vectores y de canal. Un análisis de la confianza también puede ser utilizado para predeterminar los módulos que deben realizarse como pruebas independientes. Sin embargo, recuerde que los módulos son parte de una prueba de conjunto y la suposición de que cualquier módulo en particular sólo se puede omitir es falso y dará lugar a una prueba inadecuada..

Con las pruebas de detección como un servicio, es importante comunicar a él dueño del ámbito exactamente lo que sería o no probado.

Determinar el ámbito apropiado basado en el vector es importante porque todavía puede haber objetivos fuera del vector y siempre dentro del ámbito de aplicación que no van a compensar el alcance de pruebas actuales. En general, los grandes ámbitos con múltiples canales y múltiples vectores requieren más tiempo dedicado a cada módulo y sus tareas. La cantidad de tiempo permitido antes de volver con los datos de salida no está determinado por esta metodología y depende del analista, el blanco, el entorno de prueba, y el plan de pruebas.

6.1 Metodología de flujo

El OSSTMM no permite una separación entre lo que se considera la recolección de datos activa y verificación a través de la agitación, porque, en

ambos casos, la interacción es necesaria. Ni diferenciar entre las pruebas de activo y pasivo en las pruebas activa es la agitación para crear una interacción con el objetivo y las pruebas pasiva es la grabación, la agregación y el análisis de las emanaciones de el objetivo. Esta metodología requiere de pruebas tanto activa como pasiva. Por otra parte, el analista no puede ser capaz de diferenciar entre los datos recogidos de forma pasiva de las emanaciones de las operaciones y lo que es la respuesta tardía o mal dirigida a la agitación. La introducción de cualquier evento fuera, incluyendo la clase pasiva, tiene el potencial de cambiar la naturaleza de las operaciones del objetivo y bajar la calidad de la prueba sin influencia sobre la seguridad operacional. Sin embargo, esto no representa un fracaso del analista o el proceso de auditoría, sino simplemente un mal inevitable de las pruebas de un sistema en un entorno estocástico en un marco de tiempo lineal. En pocas palabras, el analista a menudo no puede "recuperar" la agitación, una vez que se ha puesto en marcha y las correcciones que hay que hacer, hace que los resultados adicionales no coincidan con el objetivo de la tarea original. Esto es importante porque va a hacer que sea difícil para luego comparar los resultados.

Es importante señalar que cuando la armonización de las normas de ensayo OSSTMM con otros, es importante no restringir el flujo de esta metodología mediante la introducción de normas tan formal e implacable que la calidad de la prueba sufra.

6.2 Los módulos de prueba

Para elegir el tipo de prueba adecuado, lo mejor es entender primero cómo los módulos están diseñados para trabajar. Dependiendo de la minuciosidad, la empresa, asignación de tiempo, y los requisitos de la auditoría, el analista puede programar los detalles de la auditoría de fase.

Hay cuatro fases en la ejecución de esta metodología:

A. Fase de Inducción
B. Fase de Interacción
C. Fase indagatoria
D. Fase de Intervención

Cada fase da una profundidad diferente a la auditoría, pero no hay una sola fase que es menos importante que otra en términos de seguridad real.

A. Fase de inducción
Todo viaje comienza con una dirección. En la fase de inducción, el analista de la auditoría comienza con una comprensión de los requisitos de auditoría, el alcance y las limitaciones a la auditoría de este ámbito.
A menudo, el tipo de prueba se determina mejor después de esta fase.

Módulo		Descripción	Explicación
A.1	**Postura de revisión**	La revisión de la cultura, las reglas, normas, reglamentos, leyes y políticas aplicables a la meta	Conocer el alcance y las pruebas de lo que debe hacerse.
A.2	**Logística**	La medición de la logística de las limitaciones de interacción tales como distancia, velocidad, y la fiabilidad de determinar los márgenes de exactitud en los resultados.	Conozca las limitaciones de la propia auditoría. Esto minimizará los errores y mejorar la eficiencia.
A.3	**Verificación de la detección activa,**	Verificación de la práctica y la amplitud de detección de interacciones, la respuesta, y la previsibilidad de la respuesta.	Conozca las restricciones impuestas a las pruebas interactivas. Esto es necesario para llevar a cabo adecuadamente las fases B y D.

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

B. Fase de Interacción

El núcleo de la prueba básica de seguridad es necesario conocer el ámbito en relación a las interacciones con los objetivos transmitidos a las interacciones con los activos. Esta fase va a definir el alcance.

Módulo		Descripción	Explicación
B.4	**Visibilidad de Auditoría**	La determinación de los objetivos que se ha probado dentro del ámbito de aplicación. La visibilidad es considerada como "presencia" y no se limitan a la vista humana.	Saber qué objetivos existen y cómo interactúan con el ámbito, en todo caso. Un objetivo perdido o muerto también es un objetivo que no responde. Sin embargo, un objetivo que no responde no es necesariamente un objetivo perdido.
B.5	**El acceso de Verificación**	La medición de la amplitud y profundidad de los puntos de acceso interactivas dentro del objetivo y la autenticación requerida.	El punto de acceso es el punto principal de cualquier interacción de los activos. Verificación de un punto de acceso existente una parte de la determinación de su propósito. La verificación completa requiere el conocimiento de todo lo que hay que saber sobre el punto de acceso.
B.6	**Verificación de la Confianza**	La determinación de las relaciones de confianza entre los objetivos. Una relación de confianza que existe dondequiera que el objetivo acepta la interacción entre los objetivos en el ámbito.	Conocer las relaciones de confianza entre los objetivos se muestran la edad o el valor de la interacción.
B.7	**Verificación del Control**	La medición del uso y la eficacia de los controles basados en el proceso depérdida (Clase B): el no repudio, confidencialidad, privacidad e integridad.El control de la alarma se verifica al final de la metodología.	La mayoría de los procesos se definen en respuesta a una interacción necesaria y algunos permanecen mucho tiempo después de que la interacción se detiene o ha cambiado.

Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

C. La fase indagatoria

Gran parte de la auditoría de seguridad se trata de la información que el analista descubre.

En esta fase, los distintos tipos de valor o en detrimento de la información fuera de lugar y mal administrado como un bien salen a la luz.

Módulo		Descripción	Explicación
C.8	**El proceso de verificación**	La determinación de la existencia y eficacia del registro y el mantenimiento de los actuales niveles de seguridad o diligencia definidos por la revisión de la postura y los controles de indemnización.	Conocer los controladores y sus rutinas. La mayoría de los procesos tendrá un conjunto definido de reglas, sin embargo, las operaciones reales reflejan ninguna eficiencia, la pereza, o la paranoia que pueden redefinir las reglas. Por lo tanto, no se trata sólo de que el proceso está ahí, pero también la forma en que funciona.
C.9	**Verificación de configuración / Verificación de Entrenamiento**	La investigación del estado estacionario (Funcionamiento normal) de los objetivos, ya que han sido diseñados para funcionar bajo condiciones normales para determinar problemas de fondo fuera de la aplicación de las pruebas de tensión de seguridad.	Este módulo explora las condiciones predeterminadas en las que operan regularmente los objetivos para entender la intención, la justificación de negocio, y las razones de los objetivos. Además, muchas regulaciones necesita información acerca de cómo se planea el trabajo y esto no siempre es evidente en la ejecución de esa obra.
C.10	**Propiedad de validación**	la medición de la amplitud y profundidad en el uso de la propiedad intelectual ilegal o sin licencia o aplicaciones dentro de la meta.	Conozca el estado de los derechos de propiedad.
C.11	**Revisar la Segregación**	Una determinación de los niveles de información de identificación personal definido por la revisión de la postura	Saber que los derechos de privacidad se aplican y en qué medida la información detectada puede ser identificada personalmente puede ser clasificada sobre la base de estos requisitos
C.12	**La exposición de Verificación**	La búsqueda de información libremente disponible que describe la visibilidad indirecta de los objetivos o los activos en el canal elegido del ámbito de aplicación	Descubre información sobre los objetivos y los activos de fuentes públicas, incluida la de los propios objetivos.

C.13	**Inteligencia Competitiva Scouting**	La búsqueda de información libremente disponible, directa o indirectamente, lo que podría perjudicar o afectar negativamente dueño.	Puede haber más valor en la información de los procesos y objetivos de los activos que se protegen.

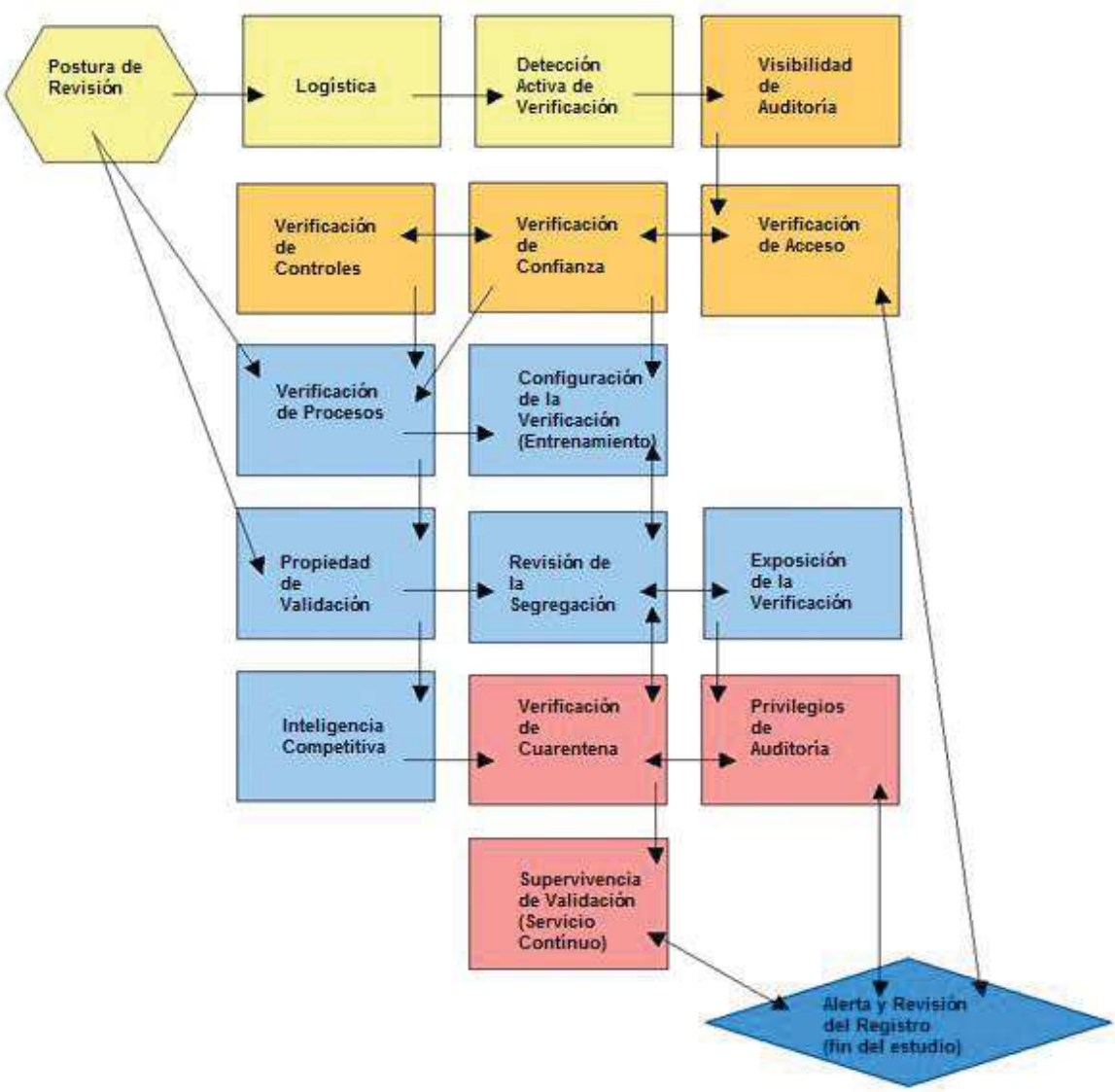
D. Fase de Intervención

Estas pruebas se centran en los recursos de los objetivos requeridos en el ámbito de aplicación. Esos recursos se pueden cambiar, modificar, sobrecargado, para causar la penetración o la interrupción.

Módulo		**Descripción**	**Explicación**
D.14	**Verificación de Cuarentena**	La determinación y la medición de la utilización eficaz de la cuarentena para todos los accesos hacia y dentro de la meta.	Determinar la efectividad de los controles de autenticación y el sometimiento en materia de cuarentenas de la lista en blanco y negro.
D.15	**Privilegios de Auditoría**	El mapeo y medición del impacto de un mal uso de los controles de sometimiento, las credenciales y privilegios, o la escalada de privilegios no autorizada.	Determinar la efectividad de la autorización en los controles de autenticación, indemnización, y el sometimiento en términos de profundidad y los papeles.
D.16	**La supervivencia de validación / Continuidad del Servicio.**	La determinación y la medición de la resistencia del objetivo a los cambios excesivos o adversos en los controles de la continuidad y la resistencia se verían afectadas.	Determinar la efectividad de los controles de continuidad y resistencia.
D.17	**Alerta y Revisión de registro / Fin Encuesta**	Una revisión de las actividades de auditoría llevados a cabo con la verdadera profundidad de las actividades según lo registrado por el objetivo o de un tercero como en el control de la alarma.	Saber qué partes de la auditoría deja un rastro útil y confiable

6.3 Una Metodología

Poner todos los módulos entre sí proporciona una metodología para conocer y trabajar con ellos. Esta es una metodología que es aplicable a cualquiera y todos los tipos de pruebas de seguridad. Ya sea que el objetivo sea de ser un sistema en particular, un lugar, una persona, un proceso, o miles de ellos, esta metodología nos asegurará la prueba más completa y eficiente posible.



Fuente: Metodología OSSTMM, http://www.isecom.org/research/osstmm.html

ANEXO 3

IP	DIRECCION MAC	DISPOSITIVO		PUERTO	SERVICIO	S.O.
172.X.X.2	00:X:X:X:X:e8	Hewlett Packard		21/tcp filtered	ftp	
				23/tcp filtered	telnet	windows xp sp3/2003
				80/tcp filtered	smtp	
				135/tcp filtered	http	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.3	70:X:X:X:X:ea	Cisco Systems		21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.4				3389	TCP	
172.X.X.7	00:X:X:X:X:ef	Hewlett Packard	sisinq2------ .andinatel.int	3389	TCP	
				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp	msrpc	

				open		
				139/tcp open	netbios-ssn	
				445/tcp open	microsoft-ds	
172.X.X.8	00:X:X:X:X:b7	Dell		3389	TCP	
				21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp filtered	http	
				135/tcp filtered	msrpc	
				445/tcp filtered	microsoft-ds	
				139/tcp filtered	netbios-ssn	
172.X.X.9				3389	TCP	
172.X.X.10	70:X:X:X:X:6f			21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				139/tcp closed	microsoft-ds	
				445/tcp closed	microsoft-ds	
172.X.X.11	1c::X:X:X:X:4a	Hewlett Packard	sisinq------.andinatel.int	3389	TCP	
				21/tcp filtered	ftp	

				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp filtered	http	
				135/tcp filtered	msrpc	
				139/tcp open	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.12				21/tcp open	ftp	
				23/tcp open	telnet	
172.X.X.15				3389	TCP	
172.X.X.16	00:X:X:X:X:cb	dell		21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp filtered	http	
				135/tcp filtered	msrpc	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.20	00:X:X:X:X:32	dell	g6------ .andinatel.int	3389	TCP	Win xp/Server 2003
				21/tcp open	ftp	
				23/tcp closed	telnet	
				25/tcp open	smtp	
				80/tcp	http	

				open		
				135/tcp open	msrpc	
				139/tcp open	netbios-ssn	
				445/tcp open	microsft-ds	
172.X.X.21	0c:X:X:X:X:01		sisinq4p------.andinatel.int	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp open	msrpc	
				139/tcp open	netbios-ssn	
				445/tcp open	microsft-ds	
172.X.X.22	d4:X:X:X:X:42	Hewlett Packard	21/tcp closed	ftp		
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp open	msrpc	
				139/tcp open	netbios-ssn	
				445/tcp open	microsft-ds	
172.X.X.23	d4:X:X:X:X:fa	Hewlett Packard	21/tcp filtered	ftp		
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	

				80/tcp filtered	http	
				135/tcp filtered	msrpc	
				139/tcp open	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.25	d4:X:X:X:X:10	Hewlett Packard	3389	TCP		
				21/tcp open	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp open	msrpc	
				139/tcp open	netbios-ssn	
				445/tcp open	microsoft-ds	
172.X.X.26	00:X:X:X:X:4a	Hewlett Packard	3389	TCP		
				21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	
				135/tcp filtered	msrpc	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.27	1c:X:X:X:X:ce	Hewlett	3389	TCP		

		Packard				
				21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp filtered	http	
				135/tcp filtered	msrpc	
				139/tcp open	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.28	00:X:X:X:X:a1	Hewlett Packard	3390	TCP		
				21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp filtered	http	
				135/tcp filtered	msrpc	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.29	00:X:X:X:X:d9	dell	h------ .telecsa.intra	21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp filtered	http	
				135/tcp filtered	msrpc	

				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.32	00:X:X:X:X:a7	dell	7j------ .andinatel.int	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp open	**msrpc**	
				139/tcp open	**netbios-ssn**	
				445/tcp open	**microsoft-ds**	
172.X.X.33	00:X:X:X:X:45	Hewlett Packard	3389	TCP		
				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp open	**msrpc**	
				139/tcp open	**netbios-ssn**	
				445/tcp open	**microsoft-ds**	
172.X.X.34	1c:X:X:X:X:fd	Hewlett Packard	21/tcp closed	ftp		
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp	http	

				open		
				135/tcp open	**msrpc**	
				139/tcp open	**netbios-ssn**	
				445/tcp open	**microsoft-ds**	
172.X.X.35	00:X:X:X:X:cd	Dell		3389	TCP	
				21/tcp open	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp open	msrpc	
				139/tcp open	netbios-ssn	
				445/tcp open	microsoft-ds	
172.X.X.38	00:X:X:X:X:a9	Dell	sisinq4pg------.andinatel.int	3389	TCP	Win xp
				21/tcp open	ftp	
				23/tcp closed	telnet	
				25/tcp open	smtp	
				80/tcp open	http	
				135/tcp open	msrpc	
				139/tcp open	netbios-ssn	
				445/tcp open	microsoft-ds	
172.X.X.41				3389	TCP	
172.X.X.47				80/tcp open	http	Microsoft httpd IIS

						7.5
172.X.X.60	d4:X:X:X:X:47	Hewlett Packard	21/tcp filtered	ftp		
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp filtered	http	
				135/tcp filtered	msrpc	
				139/tcp open	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.61	18:X:X:X:X:ab	Hewlett Packard	21/tcp closed	ftp		
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp open	msrpc	
				139/tcp open	netbios-ssn	
				445/tcp open	microsoft-ds	
172.X.X.63	00:X:X:X:X:37	Hewlett Packard	21/tcp filtered	ftp		
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp filtered	http	
				135/tcp filtered	msrpc	
				139/tcp open	netbios-ssn	

				445/tcp filtered	microsoft-ds	
172.X.X.64	00:X:X:X:X:c1	Hewlett Packard	sisinq4------ .andinatel.int	21/tcp closed	ftp	Win xp
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp open	msrpc	
				139/tcp open	netbios-ssn	
				445/tcp open	microsoft-ds	
172.X.X.66	d4:X:X:X:X:3e	Hewlett Packard	sisinq2p------ .andinatel.int	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp open	msrpc	
				445/tcp open	microsoft-ds	
172.X.X.68	00:X:X:X:X:b1	Hewlett Packard	21/tcp closed	ftp		
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp open	msrpc	
				445/tcp open	microsoft-ds	
172.X.X.70				21/tcp	ftp	

				filtered		
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp filtered	http	
172.X.X.74				139/tcp open	netbios-ssn	win 7/2008
172.X.X.75				139/tcp open		win 7/2008
172.X.X.76				21/tcp open		Hp jet direct
172.X.X.126	00:X:X:X:X:00		Cisco Systems	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.130				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	

172.X.X.131	-			21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.132			sep000dbd4------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.133				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	

				445/tcp closed	microsoft-ds	
172.X.X.134				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.135			sep000dbd4------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.136				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	

				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.137				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.138			sep001a6df-----.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.139				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	

				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.140				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.141			sep0022900-------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.142				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	

				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.143				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.144			sep0014f23------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.146				21/tcp closed	ftp	
				23/tcp closed	telnet	

				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.147				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.148			sep000dbc80-----.telecsa.intra	21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	
				135/tcp filtered	msrpc	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.149				21/tcp closed	ftp	

				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.150				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.151			sep708052-----.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.152				21/tcp	ftp	

				closed		
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.153				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.155			sep000dbda------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp	microsoft-	

				closed	ds	
172.X.X.156				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.157				21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	
				135/tcp filtered	msrpc	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.158			sep000dbcd------.telecsa.intra	21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	
				135/tcp filtered	msrpc	
				139/tcp	netbios-	

				filtered	ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.159				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.160				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.161			sep000dbd------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	

				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.162			sep001360------.teleca.intra	21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	
				135/tcp filtered	msrpc	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.163			sep000db------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.164				21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	
				135/tcp	msrpc	

				filtered		
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.165				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.168				21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	
				135/tcp filtered	msrpc	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.169				21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	

				135/tcp filtered	msrpc	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.171				21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	
				135/tcp filtered	msrpc	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.172				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.173				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp	http	

				open		
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.174			sep000225------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.175			sep00e0752------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.176			sep7081052------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	

				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.177			sep7081052------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.178			sep0008303------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.179				21/tcp	ftp	

				filtered		
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	
				135/tcp filtered	msrpc	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.180				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.181				21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	
				135/tcp filtered	msrpc	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	

172.X.X.182				21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	
				135/tcp filtered	msrpc	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.183			sep000dbcd------.telecsa.intra	21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	
				135/tcp filtered	msrpc	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.184			sep0014f28------.telecsa.intra	21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	
				135/tcp filtered	msrpc	
				139/tcp	netbios-	

				filtered	ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.185			sep0013608------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.186			sepccef484------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.187				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp	msrpc	

				closed		
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.188				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.189			sep001192d------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.190				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp	http	

				open		
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.191			sep000dbd------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.193			sep0022555------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.194			sep0012d9d------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	

				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.195				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.196			sep00136------..telecsa.intra	21/tcp filtered	ftp	
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	
				135/tcp filtered	msrpc	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.197			sep00225------.telecsa.intra	21/tcp closed	ftp	
				23/tcp	telnet	

				closed		
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.198			sep000------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.199			sep000------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.200			sep7081------.telecsa.intra	21/tcp closed	ftp	

				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.201			sep64d98------..telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.202			sep002------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.204			sep000------	21/tcp	ftp	

			.telecsa.intra	filtered		
				23/tcp filtered	telnet	
				25/tcp filtered	smtp	
				80/tcp open	http	
				135/tcp filtered	msrpc	
				139/tcp filtered	netbios-ssn	
				445/tcp filtered	microsoft-ds	
172.X.X.205			sep7081------ .telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.206			sep7081------ .telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	

172.X.X.207			sep7081------ .telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.209			SEP0022------ .telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.210			sep70810------ .telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp	microsoft-	

				closed	ds	
172.X.X.211			sep7081------ .telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.212			sep7081------ .telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.214			sep000------ .telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	

				445/tcp closed	microsoft-ds	
172.X.X.217			sep0008------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.218			sep00------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.220			sep70------.telecsa.intra	21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp	netbios-	

				closed	ssn	
				445/tcp closed	microsoft-ds	
172.X.X.221			sep7081------.telecsa.intra	21/tcp closed	ftp	win2000
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp closed	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	
172.X.X.254				21/tcp closed	ftp	
				23/tcp closed	telnet	
				25/tcp closed	smtp	
				80/tcp open	http	
				135/tcp closed	msrpc	
				139/tcp closed	netbios-ssn	
				445/tcp closed	microsoft-ds	

Elaborado por: El Autor.

ANEXO 4

CONVENIO DE

CONFIDENCIALIDAD PRIMERA.- COMPARECIENTES:

Comparecen a la celebración del presente Convenio de Confidencialidad, por una parte, el Arq. Reinaldo Torres Jaramillo, Gerente Nacional de Desarrollo Organizacional, Delegado para la suscripción del presente Convenio por Representante Legal de la Corporación Nacional de Telecomunicaciones CNT EP, mediante Resolución No. CNTEP-GG-020-2011 de 23 de marzo de 2011; y, por otra parte, el señor Oscar Milton Sánchez Robayo con C.I. 1715469308 a quien para efectos de este convenio, en adelante se le denominará CUSTODIO.

SEGUNDA.- ANTECEDENTES.

13.5. Mediante oficio s/n 17 de junio del 2011, Señorita Andrea Correa Secretaria Académica de Universidad de las Américas solicita se autorice al señor Oscar Sánchez Robayo se facilite el acceso a la información y apoyo técnico, a fin de que el CUSTODIO, realice el proyecto de tesis denominado: “Hacking ético para el Centro de Operación de la Red para la Zona 8 de la Empresa CNT con software DE Código Abierto”.

13.5. Considerando que el tema del proyecto está vinculado con el área de la Gerencia de Accesos específicamente Zona 8 se solicitó la autorización

Tecnóloga. Mónica Estrella quién es Jefe de la Zona 8, mediante Mail de 14 de julio del 2011, indico que es factible realizar el mencionado proyecto previo a la suscripción del respectivo Convenio de Confidencialidad.

TERCERA.- OBJETO.

13.5. Por medio del presente instrumento el CUSTODIO se obliga expresamente para con la CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP a guardar confidencialidad sobre el contenido de toda la información considerada como confidencial, a la que tenga acceso en virtud de los servicios o trabajos que realice y que le sea remitida de manera verbal, visual, por escrito o por cualquier otra forma tangible o intangible para el desarrollo del proyecto, y el resultado del proyecto será de uso exclusivo para la Empresa.

CUARTA.-.OBLIGACIONES DEL CUSTODIO.

El CUSTODIO deberá cumplir a cabalidad las siguientes obligaciones:

13.5. La información confidencial se mantendrá en absoluta reserva y, bajo ningún concepto, podrá ser divulgada a persona natural o jurídica alguna, ajena a CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP, salvo autorización expresa de ésta última u orden de autoridad pública competente. En este último caso el CUSTODIO informará a CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP de la existencia de tal requerimiento en el plazo de un día hábil contado desde la fecha de recepción del mismo.

13.5. Las obligaciones estipuladas en esta Cláusula no alcanzan a aquella información confidencial que:

13.5.4. Sea de dominio público o se convierta en información de dominio público, excepto que lo sea como resultado del incumplimiento a las obligaciones de este Convenio de Confidencialidad;

13.5.4. El CUSTODIO haya tenido acceso o haya producido de modo independiente con anterioridad a este Convenio de Confidencialidad;

13.5.4. Aquella que se torne disponible de modo no confidencial y que provenga de una fuente distinta a CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP y sus representantes; o,

13.5.4. Que la información fuere desarrollada por el CUSTODIO o sus allegados, independientemente de o sin referencia a cualquier información confidencial de CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP En una situación así, el CUSTODIO deberá tener la carga de la prueba de tal desarrollo, independiente.

13.5. El CUSTODIO empleará sus mejores esfuerzos para que la información confidencial de CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP, que esté a su disposición, sea manejada con cautela y para los fines relacionados para los que le haya sido proporcionada dicha información;

13.5. El CUSTODIO se obliga a la custodia de la información confidencial, aplicando las mismas medidas utilizadas en la custodia de la información similar propia;

13.5. El CUSTODIO se obliga a utilizar la información objeto del presente convenio únicamente para los fines para los que le haya sido proporcionada dicha información; y,

13.5. Al darse cuenta de cualquier pérdida, uso no autorizado o revelación de la información confidencial de CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP, el CUSTODIO acuerda adoptar las medidas necesarias para ayudar a CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP a remediar tal uso no autorizado o revelación de la información confidencial.

La aplicación de este principio no exime al CUSTODIO de responder judicial y extrajudicialmente respecto de los perjuicios causados a CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT El?, a causa de la divulgación de información confidencial no autorizada.

13.5. El CUSTODIO expresamente declara que se obliga a no revelar, difundir o hacer uso en beneficio propio o de terceros, de la información confidencial de CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP

QUINTA.- MATERIALES

13.5. Todos los materiales incluyendo, sin estar limitada a: documentos, dibujos, modelos, aparatos, esquemas, diseños, listas y cualquier cuerpo tangible que contenga información confidencial de CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP, a las que tenga acceso, el CUSTODIO, deberán ser devueltos a CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP, de acuerdo con las instrucciones razonables de ésta o deberán ser destruidos, incluyendo sus copias, al momento de la terminación de este Convenio o ante el pedido por escrito de CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP

SEXTA.- ALCANCE DEL CONVENIO

6.1. A más de lo antes referido, se considerará como información confidencial al contenido de todo documento o medio que se haya entregado al CUSTODIO, bajo el presente convenio con la leyenda “CONFIDENCIAL”. Igual condición tendrá la información que se divulgue en cualquier reunión llevada a cabo entre personal de CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP y el CUSTODIO.

SÉPTIMA.- NO LICENCIA

Este convenio no confiere al CUSTODIO ninguna licencia para usar la información confidencial de CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP

OCTAVA.- PLAZO

El presente Convenio, se entiende vigente a partir de la fecha de su suscripción terminará en el momento en que CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP así lo decidiere y lo notificare al CUSTODIO o a la culminación del proyecto, es decir a la presentación de la tesis para la obtención del título de Ingeniería en Redes y Telecomunicaciones. Este Convenio terminará inmediatamente a la recepción de tal notificación, dejándose claramente establecido, que por el hecho de tal terminación, ninguna de las partes deberá a la otra, indemnización alguna, salvo los casos de responsabilidad en que haya incurrido el CUSTODIO.

Ante la terminación de este Convenio o cuando la CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP lo estimare conveniente, el CUSTODIO cesará inmediatamente el uso de la información confidencial

de la CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP y cumplirá inmediatamente con lo dispuesto en la Cláusula Cuarta de este Convenio.

Ante el pedido de la CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP, el CUSTODIO certificará que ha cumplido con sus obligaciones aquí estipuladas.

NOVENA.- DERECHO A INICIAR ACCIONES

En el evento de que se produzca el incumplimiento de lo estipulado en el presente Convenio, la CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP tendrá el derecho a iniciar las acciones legales, civiles o penales, de las que se crea asistido, incluyendo la reclamación de daños y perjuicios.

DÉCIMA.- INDEMNIDAD

El CUSTODIO reconoce que la divulgación no autorizada de la información confidencial de la CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP, que pueda resultar en un perjuicio económico para ésta última, en cuyo caso ésta tendrá derecho al resarcimiento de daños y perjuicios que sea determinado por el Tribunal de Arbitraje o el juez de lo penal, según el caso.

UNDÉCIMA.- CESIÓN DE DERECHOS

El CUSTODIO no podrá ceder sus derechos según este convenio, sin el consentimiento previo y por escrito de la CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP, salvo el caso de disposición de autoridad competente.

DÉCIMA PRIMERA.- DISPOSICIONES GENERALES

12.1. El CUSTODIO reconoce que la solución para cualquier incumplimiento de los términos de este Convenio se realizará en conformidad con la Ley, y se tendrá especial atención a las disposiciones establecidas en la Ley de Propiedad Intelectual, el Código Penal y demás normativa civil y tratados internacionales ratificados por el Ecuador;

12.2. Las partes declaran que, en el evento de incumplimiento o amenaza de los términos de este convenio, la CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP tendrá derecho a iniciar las acciones legales y administrativas que estime del caso y a reclamar por el pago de los correspondientes daños perjuicios;

12.3. Este convenio podrá ser reformado o complementado consensudamente y por escrito; y,

12.4. Si cualquiera estipulación de este Convenio se vuelve invalida o inejecutable, tal estipulación será adecuada por las partes para su ejecución, sin perjuicio de lo cual, el resto del Convenio será mantenido en ejecución total.

DÉCIMA TERCERA.- LEGISLACIÓN, JURISDICCIÓN Y COMPETENCIA

13.1. La Legislación aplicable a este Convenio de Confidencialidad es la ecuatoriana.

13.2. Las partes renuncian a utilizar la vía diplomática para todo reclamo relacionado con este Convenio.

13.3. Para el caso de controversias relacionadas con la aplicación o interpretación de este convenio, que no sean de carácter penal, los comparecientes renuncian fuero y/ o domicilio y se sujetan a la Ley de Arbitraje y Mediación y, en particular, al pronunciamiento de los señores árbitros del Centro de Arbitraje y Mediación de la Cámara de Comercio de Quito, a cuyo efecto realizan, además, las siguientes precisiones:

13.4. El proceso se llevará en la ciudad de Quito, ante el Centro de Arbitraje y Mediación de la Cámara de Comercio de Quito, conforme su reglamentación interna;

13.5. Los árbitros habrán de resolver en derecho;

13.5.1 Los árbitros quedan expresamente facultados para dictar medidas cautelares y para solicitar el auxilio que fuere necesario para ejecutar

. dichas medidas, en los términos previstos en el Art. 9 de la Ley de Arbitraje y Mediación;

13.5.2. Los costos y gastos en que se incurra, incluidos los honorarios profesionales pactados razonablemente, serán cubiertos por la parte que fuere vencida. A pedido de parte realizado antes de dictar el respectivo laudo, el Tribunal tendrá facultades para regular dichos honorarios, si es que le parecieren considerablemente excesivos o exiguos, en consideración a la cuantía y circunstancias del caso que haya sido puesto en su conocimiento;

13.5.3. Las partes se comprometen a aceptar el Laudo Arbitral. Sin perjuicio del derecho conferido por la Ley ecuatoriana para que la parte afectada pueda demandar la nulidad del laudo, en los casos taxativamente permitidos por dicha Ley, las partes

acuerdan que la parte que dedujere un recurso de nulidad que fuere resuelto negativamente para ella, deberá cancelar a la otra parte, a más de todas las obligaciones pendientes o generadas a esa fecha y de aquellas otras obligaciones que, por disposición de la ley, se generasen como efecto de dicha resolución negativa, una indemnización equivalente a la máxima tasa de interés convencional que hubieren generado la suma de todas las citadas obligaciones, desde la fecha de expedición del laudo impugnado, por respectivo órgano o juez ejecutor;

13.5.4. De ser requerido, el respectivo laudo será ejecutado ante los jueces competentes de la ciudad de Quito o del lugar en que se encontraren los bienes del ejecutado.

Para fe y constancia de lo estipulado, las partes suscriben a continuación, en dos ejemplares de igual valor y contenido, en la ciudad de Quito – Ecuador, a

Arq. Reinaldo Torres Jaramillo
GERENTE NACIONAL DE
DESARROLLO ORGANIZACIONAL CNT EP

Sr. Oscar Sánchez Robayo
CUSTODIO
C.I. 1715469308

ANEXO 5

Políticas de Seguridad de la Corporación Nacional de Telecomunicaciones[20]

"Los activos de información y los equipos informáticos son recursos importantes y vitales de nuestra compañía. Sin ellos la CNT EP. Perdería la competitividad y quedaría relegada del negocio de las soluciones integrales de las telecomunicaciones y por tal razón la Presidencia Ejecutiva del directorio y todas las personas que laboran, directa o indirectamente, tiene el deber de preservarlos, utilizarlos y mejorarlos tomando las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de privacidad, intrusos, hackers, interrupción de servicios accidentes y desastres naturales.

Administración de la Seguridad

El Directorio, la Presidencia Ejecutiva, Gerencias y todos los niveles jerárquicos que sean parte de la organización y sea cual fuese su naturaleza de trabajo tienen la obligación de conocer y dar a conocer dentro de su área a su cargo, así como de también cumplir, con estas Políticas de Seguridad.

La Gerencia Nacional de TI es responsable de la custodia de los datos y de la infraestructura informática de la CNT EP, es decir debe tener todo el hardware de servidores de aplicaciones centralizado en sus instalaciones ya sea de manera física y lógica.

La seguridad de información esta delegada a la Gerencia Nacional de TI, a través del Área de Seguridad Informática y será la responsable de la seguridad de la información de la CNT EP, además de asistir al personal de la CNT EP en materia de seguridad y junto con los propietarios de la información se analizará

[20] Tomado de la Tesis: CRISTIAN ANÍBAL, Romero Zárate Análisis y Diseño de una Estructura de Seguridad Informática empleando COBIT para Andinatel S.A. Trabajo de Grado (Ingeniero). Universidad E.P.N. Facultad de Ingeniería Eléctrica y Electrónica. Disponible en línea http://bibdigital.epn.edu.ec/bitstream/15000/2308/1/CD-3049.pdf pág. consultadas 78,79,80

el riesgo de los activos de información de la Compañía y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma. Será además responsable de diseñar e implementar un plan de seguridad de la información que este alineado con los objetivos de negocio y tome en cuenta los riesgos existente s en la compañía. Así mismo se encargará de la revisión, que se dará en un periodo no mayor a un año desde la fecha de aprobación de la misma así como también de emitir cambios cuando así lo amerite.

El Área de Seguridad Informática es la responsable de proveer ayuda y guía en todo lo relacionado con materia de seguridad, pero en última instancia los propietarios de la información[21] son los responsables de la implementación de esta Política de Seguridad sobre los activos bajo los cuales estos tienen control.

La Gerencia Nacional de TI deberá conformar un comité de seguridad de IT de la CNT EP que se encargará principalmente de:

- Difusión y mejoramiento de la Política de Seguridad.
- Revisión y seguimiento de las incidencias en la seguridad de la información.
- Respaldo de las iniciativas principales para mejorar la seguridad de la información.

Este comité deberá estar formado por los Gerentes o delegados de las gerencias que conforman la compañía.

Seguridad en la Red

Red cableada e inalámbrica y uso de sus recursos.

Los recursos de red son recursos que se agotan, como los recursos financieros. Es por tanto que los empleados deben cuidar que estos recursos

[21] Propietarios de la Información en la compañía es la alta Gerencia que se encuentra desde el Directorio de la Presidencia Ejecutiva y Gerentes, ellos son dueños de la información que es procesada dentro de sus áreas de responsabilidad y funciones a cargo

no se agoten con la finalidad que la comunicación en la compañía no sufra de retardos que se vean reflejados en la baja de producción.

El Área de redes deberá velar porque los recursos de la red no sean consumidos de una manera irresponsable por los usuarios y deberá establecer las mejores configuraciones de los equipos, con relación a la seguridad y eficiencia, de manera que la red este siempre en operación.

El Responsable de Redes será un encargado de llevar un diagrama con el perímetro lógico de las redes de la compañía, donde consten los dispositivos que representen las barreras para los intrusos internos y externos, así como las reglas configuradas para cada uno de ellos:

- Firewall
- IPS
- Firewall en las PC's (definido sobre el inventario de software que el área de PC's debe llevar).

Todos los equipos de usuario que se conecten a la red corporativa de datos para utilizar servicios de correo electrónico, intranet, internet, sistemas transaccionales y/o se destinen para realizar las actividades de operación, mantenimiento y gestión de centrales telefónicas o equipos de las redes de servicio público de la CNT EP deberán ser ingresados al dominio de la CNT EP.

Los equipos que no se encuentren bajo la responsabilidad y administración directa de la Gerencia Nacional de TI deberán estar en subredes específicas. En coordinación con el área de redes se analizará y controlará con cuales redes se puede interactuar.

El responsable y/o administrador del área observará que lo adquirido (software y/o hardware), cumpla con las características de compatibilidad de infraestructura y software administrado por la Gerencia Nacional de TI, debe garantizar el correcto funcionamiento de las aplicaciones, el soporte, el

mantenimiento, evitar daños por no compatibilidad, virus y debilidades en acceso a los datos de la compañía.

Previo a todo cambio que se aplique en la red, equipos de comunicación y/o dispositivos, deberá ser analizado en función de medir el riesgo e impacto que este cambio pueda presentar a los servicios, en el caso que este cambio tenga relación o afectación sobre la red interna de la CNT EP deberá coordinarse con la Gerencia Nacional de TI.

El responsable del área que tenga a cargo o bajo su administración red, equipos, deberá mantener al día aplicados los parches y actualizaciones recomendadas por el fabricante.

Está prohibida la utilización de cuentas y contraseñas que vienen configuradas por defecto en los equipos de interconectividad con la red.

Seguridad en la red Inalámbrica

La red inalámbrica debe estar separada de la red de usuarios internos de la compañía y no una extensión de la misma, con ingreso limitado a los servidores y recursos de la red, Debe contar con mecanismos de autenticación y autorización de usuarios registrados para lo cual debe contar son sistemas propietarios o abiertos que garanticen el no ingreso de usuarios no autorizados.

Se debe implementar tipos de encripción como LEAP o WPA2 como sistemas de autenticación y cifrado de datos y el filtrado mediante listas de control de acceso o sistemas de firewall de los recursos disponibles en la red corporativa de datos.

El acceso inalámbrico (Wireless) es autorizado por defecto a todos los jefes de área e inmediatos superiores que se encuentren debidamente registrados dentro del organigrama organizacional.

El área de infraestructura garantizará la entrega de los equipos portátiles, con las opciones Bluetooth, Wireless, dispositivos infrarrojos, y módems deshabilitadas. Solo los usuarios con autorización de acceso Wireless podrán tener habilitada la mencionada opción.

Los puntos de acceso inalámbrico no pueden ser adquiridos o instalados de manera indiscriminada por usuarios y/o áreas diferentes a la infraestructura. En caso de necesidad de instalación y/o ampliación, se debe solicitar el soporte respectivo a la gerencia Nacional de TI.

El área de infraestructura debe asegurar:

a. La existencia de un sistema de autenticación y de autorización que no permita el acceso de usuarios a la red inalámbrica sin que estos estén previamente validados.

b. La implementación de un esquema de cifrado de información que no permita en un corto periodo de tiempo (menor a 5 horas) criptoanalizar el tráfico inalámbrico de manera que comprometa la integridad y confidencialidad de la información transmitida.

c. La existencia de un plan de actualización de firmware de todos los puntos de acceso inalámbrico (Access Point).

d. Está prohibido tener los nombres de red (SSID) que vienen configurados por defecto en los puntos de acceso, de igual manera inhabilitar la emisión broadcast del nombre de red (SSID).

e. Se debe reducir al mínimo la cobertura del alcance de la señal de los puntos de acceso inalámbricos, limitándoles únicamente al edificio donde reside la red.”