
ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA
TELECOMUNICACIONES Y REDES

# "PROPUESTA DE BEST PRACTICE PARA EL ANALISIS DE VULNERABILIDADES, MÉTODOS DE PREVENCIÓN Y PROTECCIÓN APLICADOS A LA INFRAESTRUCTURA DE RED DEL LABORATORIO DE SISTEMAS"

## TESIS DE GRADO

PREVIA A LA OBTENCIÓN DEL TÍTULO DE:

**INGENIERO EN ELECTRÓNICA TELECOMUNICACIONES Y REDES**

**Presentado por:**

JORGE BOLIVAR ORELLANA PAZMIÑO

CRISTIAN FABRICIO VILLARROEL VILLARROEL

RIOBAMBA – ECUADOR

2012

**DERECHOS DE AUTORÍA**

Nosotros, Jorge Bolívar Orellana Pazmiño y Cristian Fabricio Villarroel Villarroel, declaráramos ser los autores del presente trabajo de tesis “PROPUESTA DE BEST PRACTICE PARA EL ANALISIS DE VULNERABILIDADES, MÉTODOS DE PREVENCIÓN Y PROTECCIÓN APLICADOS A LA INFRAESTRUCTURA DE RED DEL LABORATORIO DE SISTEMAS-FIE”, que fue elaborada en su totalidad por nosotros, bajo la dirección del Ingeniero Diego Ávila, haciéndonos totalmente responsables por las ideas, criterios, doctrinas y resultados expuestos en esta Tesis, y el patrimonio de la misma pertenece a la Escuela Superior Politécnica de Chimborazo.

_____ _____

**Jorge Bolívar Orellana Pazmiño** **Cristian Fabricio Villarroel Villarroel**

**CI. 060367824-4** **CI. 060380275-2**

**AGRADECIMIENTO**

Expresamos nuestro más sincero agradecimiento a las Autoridades y maestros de la Escuela Superior Politécnica de Chimborazo y de manera especial al Ingeniero Diego Ávila y a nuestro compañero y amigo Ingeniero Luis Pazmiño, quienes con sus valiosos aportes ayudaron a la consecución del presente trabajo.

**Jorge y Cristian**

**DEDICATORIA**

Dedico este trabajo a mi familia, de manera muy especial a mi madre, que ha sido soporte en los momentos mas difíciles y en la luz que me ha iluminado durante el desarrollo de mi carrera.

**Cristian**

**DEDICATORIA**

Dedico el presente trabajo a mi familia por su apoyo constante en el transcurso de mi vida, de manera muy especial a mi querida hija Oderay Cristina y mi esposa Gabriela.

Agradezco infinitamente a mis amigos del Grupo 24 Horas Chimborazo por que sin ellos no podría haber culminado esta etapa de mi vida.

**Jorge**

# FIRMAS RESPONSABLES

| | FIRMA | FECHA |
|---|---|---|
| **ING. IVÁN MENES**<br>**DECANO FAC. INFORMÁTICA Y ELECTRÓNICA** | _____ | _____ |
| **ING. PEDRO INFANTE**<br>**DIRECTOR ESC. ELECTRÓNICA TELECOMUNICACIONES Y REDES** | _____ | _____ |
| **ING. DIEGO ÁVILA**<br>**DIRECTOR DE TESIS** | _____ | _____ |
| **ING. WILSON BALDEON**<br>**MIEMBRO DEL TRIBUNAL** | _____ | _____ |
| **TEC. CARLOS RODRÍGUEZ**<br>**DIRECTOR CENTRO DOCUMENT.** | _____ | _____ |
| **NOTA DE TESIS** | _____ | |

# ÍNDICE DE CONTENIDOS

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

# CAPÍTULO I
# MARCO REFERENCIAL

## 1.1 INTRODUCCIÓN

Los datos son un bien invaluable de las empresas e instituciones, para lo cual los administradores de la red, deben identificar mecanismos y herramientas que les permita transportarlos de una manera segura.

La seguridad debería ser el aspecto más importante dentro de cualquier organización ya sean esta públicas, privadas o de cualquier índole, ya que la información que las mismas poseen constituye el activo más importante para el desarrollo de sus actividades, por lo que se deben tomar todas las medidas necesarias para precautelar esta información y no ser víctimas de intrusos o delincuentes informáticos. El ahorro dentro del diseño de la seguridad de una intranet puede costar a la empresa su credibilidad y su viabilidad, para lo cual es necesario tener un equilibrio respecto a la relación del costo con la seguridad.

La despreocupación por el control y manejo de la información está haciendo que las empresas sean cada vez más vulnerables ante el robo de información que es vital para el funcionamiento de las mismas y que puede ser utilizada de una manera mal intencionada. Generalmente pensamos que esto sólo le sucede a grandes compañías que son hackeadas por delincuentes especializados, pero nunca pensamos que la mayoría de los casos que ocurren tanto en grandes como pequeñas empresas, son realizados por “enemigos internos”, que aprovechan formar parte de la organización para realizar los ataques.

Para poder mitigar las fallas de seguridad existentes en una organización es necesaria la realización de pentest para poder determinar las vulnerabilidades existentes, con lo que podremos realizar una guía de prevención basándonos en los estándares existentes.

Se puede tener en cuenta que con el desarrollo de los sistemas informáticos siempre existirá un constante cambio con respecto a las seguridades de tal o cual sistema, lo cual debe ser previsto y de la misma forma atendido, por lo que la persona encargada de la administración de la red debe estar en una constante actualización de conocimientos para de esa manera evitar nuevas vulnerabilidades.

## 1.2 JUSTIFICACIÓN

El presente proyecto de investigación tiene como finalidad la contribución al fortalecimiento de un ámbito tan importante como es el campo de seguridad en Redes de Área Local, por medio de la utilización de herramientas de software libre, a la vez demostrar las diversas vulnerabilidades que posea la red a ser analizada, realizando pruebas de penetración en un entorno controlado que nos permita señalar efectivamente las deficiencias de seguridad para poder analizarlas y realizar una guía de best practice basándonos en el estándar ISO/IEC 17799.

La seguridad no solo se trata de un programa antivirus o de un firewall, más bien se trata de normas del comportamiento que todos los que hacemos utilidad de la red debemos conocer y aplicar.

Para poder realizar este análisis de vulnerabilidades es necesario contar con las herramientas necesarias para lo cual hemos escogido Backtrack por las prestaciones que nos brinda. Backtrack es una distribución de GNU/Linux diseñada para la auditoria de seguridad y relacionada con la seguridad informática en general. BackTrack es una de las distribuciones GNU/Linux más famosas orientada a la seguridad informática, diseñada por las personas de remote-exploit, con un gran número de herramientas para realizar test de penetración (exploits, todo tipo de escáneres de puertos y vulnerabilidades, auditoria wireless, herramientas de análisis forense, sniffers, entre otras) ya que esta distribución se presenta como LiveCD (no hay necesidad de instalar) podemos utilizar todas las herramientas en tan solo unos minutos.

## 1.3 OBJETIVOS

### 1.3.1 OBJETIVO GENERAL

- Proponer las best practice para el análisis de vulnerabilidades, métodos de prevención y protección aplicados a la infraestructura de red del laboratorio de Sistemas-FIE.

### 1.3.2 OBJETIVOS ESPECÍFICOS

- Estudiar la metodología de hacking ético, que proporciona una guía sistemática de cómo realizar ataques a la integridad de la red.
- Aplicar el método de hacking ético para el análisis de vulnerabilidades, prevención y protección de fallos de seguridad encontrados en la red, de esta manera realizar la corrección de los mismos y especificarlos en la guía de best practice propuesta basada en el Estándar Internacional ISO/IEC 17799.
- Analizar de las diferentes herramientas que provee Backtrack para el pentest de la red, basado en el método de hacking ético.
- Desarrollar ataques controlados en la red del laboratorio de Ingeniería en Sistemas de la FIE de la Escuela Superior Politécnica de Chimborazo con las herramientas que posee Backtrack.

- Evaluar los resultados obtenidos en la realización de las pruebas de penetración y determinar soluciones para los fallos encontrados.

## 1.4 HIPÓTESIS

El análisis de vulnerabilidades mediante la aplicación de Hacking ético permitirá conocer las deficiencias que en materia de seguridad que existan en los laboratorios de la Escuela de Ingeniería en Sistemas, a la vez permitirá generar una guía de prevención y mejores prácticas de seguridad de red, que dote un mayor nivel de seguridad adecuado a este tipo de redes.

# CAPÍTULO II
# MARCO TEÓRICO
## CONCEPTOS DE SEGURIDAD

### 2.1 INTRODUCCIÓN

La Información es si, un bien invaluable como cualquier otro de los bienes del negocio, tiene un valor para la organización y consecuentemente necesita de protección debidamente planificada. La seguridad informática, protege la información de una vasta gama de amenazas con la finalidad de perpetuar la continuidad del negocio, minimizar los daños del mismo y maximizar el retorno de inversión.

Sintetizando se puede entender como seguridad una característica de cualquier sistema que indica que efectivamente ese sistema está libre peligro, esto significa protegerse de adversarios, aquellos que harán daño intencional o circunstancial y que es, en cierta manera infalible. Como esta característica, particularizando

para el caso de sistemas operativos, software o redes de computadores, es muy difícil de conseguir y para la mayoría de expertos, imposible, se suaviza la definición de seguridad y se pasa a hablar de fiabilidad que es la probabilidad de que un sistema se comporte tal y como se espera de él más que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

Alcanzar el nivel apropiado de seguridad para una organización depende de un sistema multifacético y que no solo involucra al administrador de red, sino a un profundo conciencia miento de las amenazas a las que se está expuesto, desde los altos ejecutivos o autoridades de dichas organizaciones hasta alcanzar a todo el personal.

Este sistema debe de proporcionar seguridad en las siguientes áreas de la organización desde el punto de vista de la seguridad informática:

- Personal
- Operaciones cruciales de la organización
- Ambiente Físico
- Integridad de la Red
- Acceso a la información

- Dispositivos de comunicaciones

La seguridad de las redes debe ser una parte integral de las redes informáticas. Debe Incluir protocolos, tecnologías, dispositivos, herramientas y técnicas que aseguran los datos para reducir riesgos frente a las constantes amenazas. La seguridad informática se alcanza a través de la aplicación de ciertos controles, los cuales pueden ser prácticas, procedimientos, estructuras organizacionales y funciones de software. Estos controles necesitan ser establecidos para asegurar que los objetivos específicos de seguridad de una organización sean alcanzados.

**ESTÁNDARES DE SEGURIDAD EN REDES**

BS77994 y ISO/17799 son estándares de seguridad que representa una serie de controles basados en las mejores prácticas de seguridad informática. Cubren aspectos de equipos, Políticas, recursos humanos y asuntos legales

**Estándar BS7799**

BS7799 (parte 2) contiene medidas para la eficiente administración del esquema de seguridad. En 1995 surge la parte 1 del estándar BS 7799, establecido por el instituto británico de estándares.

En 1998 surge la parte 2 de este estándar con mejoras de seguridad actualizadas (Callio,2003). BS 7799-2 ayuda a la organización a establecer un sistema de administración de seguridad informática y por lo tanto prepararse para la auditoria de certificación.

En Diciembre del 2000 el estándar británico BS7799 se convierte en un estándar internacional con el nombre de ISO/17799 y fue adoptado bajo un procedimiento de ruta rápida por el comité técnico ISO/IEC JTC 1. (ISO/IEC, 2000)

**Estándar ISO/17799**

ISO/17799 es el que contiene controles y recomendaciones a través de los cuales la organización puede garantizar la seguridad de su información. Sus características son las siguientes:

- Ha sido probado
- Es internacional
- Está asociado a la calidad
- Evolutivo y flexible
- Disponibilidad de herramientas y soporte

La organización internacional de estandarización (ISO) y la comisión internacional electrotécnica (IEC) forman un sistema especializado para la estandarización mundial. Además existen organizaciones internacionales, gubernamentales y no gubernamentales, que están en alianza con ISO e IEC y también forman parte del desarrollo de los nuevos estándares internacionales (ISO/IEC, 2000).

Los anteproyectos de los estándares internacionales son escritos en coordinación con los reglamentos establecidos por las directivos de ISO/IEC.

En el campo de la tecnología de información, ISO e IEC establecen juntos un comité técnico. Los anteproyectos de los estándares internacionales son

examinados por el comité técnico para posteriormente ser distribuidos a los organismos nacionales para que éstos a su vez voten para su aprobación. Para que un estándar internacional sea publicado requiere la aprobación de por lo menos el 75% de los organismos nacionales que intervienen en la votación (ISO/IEC, 2000).

Existen diez puntos claves para el contexto de ISO/17799 y son los siguientes:

- Política de seguridad
- Seguridad organizacional
- Clasificación de bienes
- Personal de seguridad
- Seguridad física
- Administración de operaciones y comunicaciones
- Control de acceso
- Sistema de desarrollo y mantenimiento
- Administración continúa
- Acatamiento

## 2.2 OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

Seguridad informática es el conjunto de procedimientos, estrategias y herramientas que permitan garantizar la integridad, la disponibilidad y la confidencialidad de la información de la entidad.

El objetivo de un hacker es aprovechar las vulnerabilidades de un sistema o red para encontrar una debilidad en una o más de los cuatro elementos de seguridad. Todos los ataques son un intento de violación de la seguridad del sistema informático, principalmente atentan a cuatro elementos básicos:

- Confidencialidad
- Autenticidad
- Integridad
- Disponibilidad
- No repudio

### 2.2.1 CONFIDENCIALIDAD

La confidencialidad asegura que la información no esté disponible para personas, procesos o programas no autorizados, por lo cual solo los usuarios autorizados pueden manipularla.

En si la confidencialidad se refiere a la protección de datos frente a la difusión no autorizada, la perdida de confidencialidad puede resultar en problemas legales, perdida del negocio o de credibilidad.

El robo de información, como el robo de contraseñas u otros datos a medida que viaja sin cifrar a través de redes de confianza, es un ataque de confidencialidad, ya que permite a una persona distinta del destinatario para obtener acceso a los datos.

### 2.2.2 AUTENTICACIÓN.

Es el proceso de verificar la identidad de los actores y autorización por parte de la entidad autorizadora en una comunicación.

Los profesionales de la seguridad en redes son responsables de mantener la seguridad de los datos de una organización y garantizar la integridad, disponibilidad y confidencialidad de la información.

Falsificación de direcciones MAC es un ataque de autenticación, ya que permite que un dispositivo no autorizado a conectarse a la red cuando Media Access Control (MAC) de filtrado está en su lugar, como en una red inalámbrica.

### 2.2.3 INTEGRIDAD

La integridad garantiza que la información no sea modificada por personas, procesos o programas que no sean debidamente autorizados para ello.

Es necesario asegurar que los datos no sufran cambios no autorizados, la perdida de integridad puede acabar en fraudes, decisiones erróneas o como paso a otros ataques.

*Bit-flipping* ataques se consideran ataques integridad, porque los datos pueden haber sido manipulados en tránsito o en reposo en los sistemas informáticos, por

lo tanto, los administradores de sistemas son incapaces de verificar los datos es que el remitente lo previsto.

### 2.2.4 DISPONIBILIDAD

La disponibilidad significa que la información se encuentra disponible para ser requerida por un usuario, proceso o programa, en todo momento que lo requiera.

También se refiere a la continuidad operativa de la entidad, la perdida de disponibilidad puede implicar, la pérdida de productividad o de credibilidad de la entidad.

En la realización de un ataque de denegación de servicio (DoS), un hacker ataca a los elementos de disponibilidad de sistemas y redes.

### 2.2.5 NO REPUDIO

Proporciona protección contra la interrupción, por parte de alguna de las entidades implicadas en la comunicación, de haber participado en toda o parte de la

comunicación. El servicio de Seguridad de No repudio o irrenunciabilidad está estandarizado en la ISO-7498-2.

No Repudio de origen: El emisor no puede negar que envío porque el destinatario tiene pruebas del envío, el receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario. Prueba que el mensaje fue enviado por la parte específica.

No Repudio de destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor. Prueba que el mensaje fue recibido por la parte específica.

Si la autenticidad prueba quién es el autor de un documento y cual es su destinatario, el “no repudio” prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibió (no repudio en destino).

El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje. Así, cuando se envía un mensaje, el receptor puede comprobar que, efectivamente, el supuesto emisor envió el mensaje. De forma similar, cuando se recibe un mensaje, el emisor puede verificar que, de hecho, el supuesto receptor recibió el mensaje. Definición según la recomendación X.509 de la UIT-T Servicio que suministra la prueba de la integridad y del origen de los datos- ambos en una relación infalsificable que pueden ser verificados por un tercero en cualquier momento.

## 2.3 ATAQUES Y VULNERABILIDADES

Las redes son a menudo victimas de atacantes que utilizan diferentes técnicas para vulnerar la seguridad de las redes. Los ataques más comunes son:

### 2.3.1 DENEGACION DE SERVICIO

Denegación de Servicio es un tipo de ataque cuya meta fundamental es la de negar el acceso del atacado a un recurso determinado o a sus propios recursos.

Algunos ejemplos de este tipo de ataque son:

- tentativas de “floodear” (inundar) una red, evitando de esta manera el tráfico legítimo de datos en la misma;
- tentativas de interrumpir las conexiones entre dos máquinas evitando, de esta manera, el acceso a un servicio;
- tentativas de evitar que una determinada persona tenga acceso a un servicio;
- tentativas de interrumpir un servicio específico a un sistema o a un usuario;

Cabría tener en cuenta que, el uso ilegítimo de recursos puede también dar lugar a la negación de un servicio. Por ejemplo, un “hacker” puede utilizar un área del FTP anónimo como lugar para salvar archivos, consumiendo, de esta manera, espacio en el disco y generando tráfico en la red.

Como consecuencia, los ataques de negación de servicio pueden esencialmente dejar inoperativa una computadora o una red. De esta forma, toda una organización puede quedar fuera de Internet durante un tiempo determinado.

**MODOS DE ATAQUE**

Algunos ataques de negación de servicio se pueden ejecutar con recursos muy limitados contra un sitio grande y sofisticado. Este tipo de ataque se denomina “ataque asimétrico”.

Hay tres tipos de ataques básicos de negación de servicios:

a.- Consumo de recursos escasos, limitados, o no renovables

b.- Destrucción o alteración de información de configuración

c.- Destrucción o alteración física de los componentes de la red

**CONSUMO DE RECURSOS ESCASOS, LIMITADOS, O NO RENOVABLES**

Las computadoras y las redes necesitan para funcionar ciertos recursos: ancho de banda de la red, espacio de memoria y disco, tiempo de CPU, estructuras de datos, acceso otras computadoras y redes, entre otros.

**CONECTIVIDAD**

Los ataques de Negación de servicio se ejecutan, con frecuencia, contra la conectividad de la red. La meta del hacker es evitar que las computadoras se comuniquen en la red. Un ejemplo de este tipo de ataque es el “SYN flood”:

En este tipo de ataque, el hacker comienza el proceso de establecer una conexión TCP a la máquina de la víctima, pero lo hace de manera tal que evita que la conexión se complete. En este tiempo, la máquina del atacado ha reservado uno entre un número limitado de las estructuras de datos requeridas para terminar la

conexión inminente. El resultado es que las conexiones legítimas se rechazan mientras que la máquina del atacado se queda esperando para terminar esas falsas conexiones “medio abiertas”.

Debe tenerse en cuenta que este tipo de ataque no depende del ancho de banda que disponga el atacante. En este caso, el hacker está consumiendo las estructuras de datos del kernel, implicadas en establecer una conexión TCP. Un hacker con una simple conexión dial-up puede realizar este ataque contra una poderosa Workstation (este último es un buen ejemplo de un ataque asimétrico).

**APROVECHAMIENTO DE LOS RECURSOS DEL OTRO**

Un hacker también puede utilizar los recursos que usted dispone contra usted mismo, de maneras inesperadas. Por ejemplo, el caso de Negación de servicio UDP. En este ataque, el hacker utiliza los paquetes “falsificados” de UDP para conectar el servicio de generación de eco en una máquina con el servicio de chargen en otra máquina.

El resultado es, que los dos servicios consumen todo el ancho de banda de red entre ellos. Así, la conectividad para todas las máquinas en la misma red desde cualquiera de las máquinas atacadas se ve afectada.

**CONSUMO DE ANCHO DE BANDA**

Un hacker puede, también, consumir todo el ancho de banda disponible en su red generando una gran cantidad de paquetes dirigidos a la misma. Típicamente, estos paquetes son de generación de eco de ICMP (ping), pero pueden ser cualquier otra cosa. Además, el hacker no necesita operar desde una sola máquina; él puede poder coordinar varias máquinas en diversas redes para alcanzar el mismo efecto.

**CONSUMO DE OTROS RECURSOS**

Además del ancho de banda de la red, los hackers pueden consumir otros recursos que su sistema necesite para funcionar. Por ejemplo, en muchos sistemas, un número limitado de las estructuras de datos en el kernel está disponible para almacenar información de procesos (identificadores, entradas en tablas de procesos, slots , etc.).

Un hacker puede consumir estas estructuras de datos escribiendo un programa o un script que no haga nada pero que cree en varias ocasiones copias de sí mismo.

Muchos sistemas operativos modernos, aunque no la totalidad de ellos, tienen recursos para protegerse contra este problema. Además, aunque las tablas de

procesos no se llenen, se consume CPU por la gran cantidad de procesos y conmutación entre los mismos.

Un hacker puede también consumir su espacio en disco de otras maneras, por ejemplo:

- Generar miles de mails (Spam, Bombing. Para ampliar este tema, consultar el próximo).
- Generar intencionalmente errores que deben ser logueados. En este tipo de ataque, podemos citar también la utilización indebida del syslog en unix. Es decir, utilizar el proceso syslog de la víctima para que registre eventos de otra máquina, llenando el espacio en disco con el archivo de syslog.
- Colocar archivos en su disco, utilizando ftp anónimo.

En general, se puede utilizar cualquier cosa que permita que los datos sean escritos en su disco para ejecutar un ataque de negación de servicio si no hay límites en la cantidad de datos que se pueden escribir (quotas).

No obstante, muchos sitios tienen esquemas de “lockout” de cuenta después de un cierto número de logins fallados. Un setup típico bloquea el login después de 3 o 5 tentativas falladas. Un hacker puede utilizar este esquema para evitar que los usuarios legítimos entren. En algunos casos, incluso las cuentas privilegiadas, tales como root o administrador, pueden ser víctimas de este tipo de ataque.

Un hacker puede hacer caer su sistema o ponerlo inestable, enviando datos inesperados. Un ejemplo de tal ataque es el “ping flood” o Pings de tamaño demasiado grande. Si su sistema está experimentando caídas frecuentes sin causa evidente, podría deberse a este tipo de ataque.

Hay otros componentes que pueden ser vulnerables a la negación de servicio y que deben vigilar se. Estos incluyen:

- Impresoras
- Unidades de cinta
- Conexiones de red
- Otros recursos limitados importantes para la operación de su sistema.

### 2.3.2 PASSWORD CRACKING

El **password cracking** es un proceso informático que consiste en descifrar la contraseña de determinadas aplicaciones elegidas por el usuario. Se busca codificar los códigos de cifrado en todos los ámbitos de la informática. Se trata del rompimiento o desciframiento de claves (passwords).

Con los métodos de cifrado de hoy en día se hace más difícil el descifrado de claves. En cifrados modernos, como MD5, resulta imposible encontrar una

coherencia lógica entre el texto cifrado y el descifrado, ya que cada clave ha sido generada a partir de una cadena diferente llamada "semilla". Así han tenido que evolucionar los sistemas de rotura de claves (hasta el uso de las increíbles "rainbow tables"), buscando no encontrar una coherencia lógica, sino el cifrado de nuevas cadenas con las que se guarde similitud con el texto cifrado, siendo una tarea ardua y que requiere, habitualmente, un buen equipo para romperlas (algunas pueden tardar incluso años en romperse).

### 2.3.3 E-MAIL BOMBING Y SPAMMING

El e-mail bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando el mailbox del destinatario.

El spamming, que es una variante del e-mail bombing, se refiere a enviar el email a centenares o millares de usuarios e, inclusive, a listas de interés. El Spamming puede resultar aún más perjudicial si los destinatarios contestan el mail, haciendo que todos reciban la respuesta.

Puede, además, ocurrir inocentemente como resultado de enviar un mensaje a la lista y no darse cuenta de que la lista lo distribuye a millares de usuarios, o como resultado de mala configuración de un autorespondedor, por ejemplo el “vacation”.

El e-mail bombing/spamming se puede combinar con el e-mail spoofing – que altera la identidad de la cuenta que envía el mail -, logrando que sea más difícil determinar quién está enviando realmente el mail.

Cuando se proveen los servicios de e-mail los usuarios son, lógicamente, vulnerables al e-mail bombing y spamming.

En efecto, el e-mail spamming es casi imposible de prevenir. Un usuario con una dirección válida de mail puede realizar " Spam " a cualquier otra dirección de mail, newsgroup, o sistema de BBS.

Cuando gran cantidad de mails son dirigidos a un solo sitio, éste puede sufrir “denial of service” por pérdida de conectividad, caerse el sistema o producirse fallas en el servicio debido a:

- sobrecarga de conexiones de red;
- utilización de todos los recursos de sistema disponibles;
- llenado del disco como resultado de postings múltiples y de entradas en el “syslog”.

## 2.4 POLITICAS DE SEGURIDAD INFORMÁTICA

El propósito de una política de seguridad es describir el uso aceptable de los equipos de la organización. La política de seguridad debe de establecer objetivos claros para cada uno de los equipos utilizados en la defensa de la red, incluyendo los parámetros de seguridad. La política es un documento o una serie de documentos que describen los controles de seguridad que se deben de implementar en la organización, finalmente una política de seguridad no sería efectiva sino se implementa, es por esta razón, que los usuarios de la red deben de firmar un documento claramente detallado que explique qué es lo que se les permite hacer en el sistema de información, por lo menos, una política de seguridad debe de incluir un resumen y una declaración de propósitos.


**FIGURA II.I Esquema Políticas**

Toda política de seguridad implementada debe de estar comprometida para proteger a los empleados, socios de la empresa y a la empresa misma, de acciones ilegales y perjudiciales llevadas a cabo por intrusos internos o externos.

La intención de publicar una política de seguridad no debe de ser para imponer restricciones que son contradictorias al establecimiento de una cultura de disponibilidad, confiabilidad e integridad, una efectiva seguridad requiere del esfuerzo de un equipo que participe y dé soporte a cada empleado que interactúe con la información que se considere confidencial. Es responsabilidad de los usuarios comprender los procedimientos y llevar acabo sus actividades de acuerdo con lo establecido. Los reglamentos deben de definir de alguna manera la protección del empleado y de la organización en caso de alguna mala acción que ponga entre dicho la integridad de la seguridad. Una lista de actividades prohibidas, debe de ser presentada a los empleados antes de que firmen la aceptación de la política, además debe de contener las excepciones a ciertas prohibiciones de acuerdo a la naturaleza del cargo que asumirá el empleado.

La política de seguridad debe de establecer todo un programa que plantee como los usuarios internos y externos, deben de interactuar con las computadoras de la

organización, también debe de plantear como la organización puede implementar la topología de red y determinar dónde deben de estar ubicados sus bienes. La política deberá de evaluar las posibles amenazas en contra de productividad y los bienes tangibles e intangibles de la organización que necesitan diferentes niveles de protección.

El grado de seguridad proporcionado está íntimamente relacionado con la apertura de comunicaciones de las redes, a mayor apertura o alcance de la red, mayor es el grado de seguridad que se requiere. Por ejemplo; las grandes empresas requieren de un nivel de seguridad medio, este nivel debe de satisfacer los requisitos de herramientas de monitoreo como un monitor de referencia que interviene en todos los accesos de usuarios a los objetos, a fin de ser comprobada, y que sea lo bastante pequeña para ser sujeta al análisis y pruebas.

Definir el impacto de la política sobre los usuarios, reconocer los inconvenientes de la seguridad, evitar una complejidad excesiva, hacer uso de las herramientas más comunes de seguridad que han sido probadas y examinadas, decidir si va existir una persecución en contra de los malhechores y en caso de que si exista una persecución entrenar al personal para recolectar información necesaria, decidir el alcance, recordar constantemente y diseminar periódicamente detalles

de seguridad, son parte de las actividades que debe de contemplar una política de seguridad.

Las políticas pueden ser formuladas en un número variado de formas. Se puede escribir una política muy simple y particular, una política general que comprendan varias páginas, se pueden desarrollar una serie de políticas específicas como: política de correo electrónico, de contraseñas, de contabilidad del sistema, de emisión de cuentas de usuario, etc.

Las políticas juegan tres tipos de roles.

- La primera fuente es derivada de la valoración de riesgos de organización. A través de la valoración de riesgos las amenazas a los activos son identificados, la vulnerabilidad y la posibilidad de ocurrencia es evaluada y el impacto potencial es estimado.
- La segunda fuente es la legal, requerimientos establecidos por la ley, reglamentos y contratos que en la organización requieren para negociar con socios, contratistas y proveedores de servicio.

- La tercera fuente son una series de principios, objetivos y requerimientos del procesamiento de información que la organización debe de desarrollar para las etapas de procesamiento que soportan sus operaciones.

La valoración de riesgos de seguridad. Este requiere de una valoración metódica para los riesgos de seguridad, se necesita entonces hacer un balance de las fallas del negocio en relación con los resultados de fallas de seguridad. Las técnicas de valoración de riesgos pueden ser aplicadas a toda la organización, o bien sólo a una parte de ella, así como a los sistemas de información individuales, un componente específico del sistema o un servicio que sea práctico, realístico y de mucha ayuda.

La política de seguridad en redes traza las reglas de acceso a la red, determina cómo se harán cumplir las políticas y describe la arquitectura básica del ambiente básico de seguridad de la información de la empresa. El documento generalmente consta de varias páginas. Por su amplitud de cobertura e impacto, generalmente es un comité el que lo compila. Es un documento complejo que está diseñado para gobernar temas como acceso a los datos, navegación en la web, uso de las contraseñas, criptografía y adjuntos de correo electrónico.

La política de seguridad de la red establece cuáles bienes deben ser protegidos y da pautas sobre cómo deben ser protegidos. Esto será luego usado para determinar los dispositivos de seguridad y las estrategias y procedimientos de mitigación que deberán ser implementados en la red.

### 2.4.1 ELEMENTOS

Como mencionábamos en el apartado anterior, una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las PSI deben considerar entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.

- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

Las PSI deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios.

De igual forma, las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar

indicaciones sobre la clase de sanciones que se puedan imponer. No debe especificar con exactitud qué pasara o cuándo algo sucederá; no es una sentencia obligatoria de la ley.

Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios entre otros.

### 2.4.2 PARAMETROS

Si bien las características de la PSI que hemos mencionado hasta el momento, nos muestran una perspectiva de las implicaciones en la formulación de estas directrices, revisaremos a continuación, algunos aspectos generales recomendados para la formulación de las mismas.

- Considere efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá afinar las PSI de su organización.

- Involucre a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.
- Comunique a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Recuerde que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los responsables de salvaguardar los activos críticos de la funcionalidad de su área u organización.
- Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas.
- Un último consejo: no dé por hecho algo que es obvio. Haga explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI trazadas.

### 2.4.3 RIESGOS

La autenticación suele realizarse mediante una contraseña, aún cuando sería más lógico - si bien los costes resultan todavía altos para la mayoría de sistemas - que

se pudiera combinar con características biométricas del usuario para impedir la suplantación. Entre éstas pueden estar: la realización de la firma con reconocimiento automático por ordenador, el análisis del fondo de ojo, la huella digital u otras.

Al margen de la seguridad, nos parece que el mayor riesgo, aún teniendo un entorno muy seguro, es que la Informática y la Tecnología de la Información en general no cubran las necesidades de la entidad; o que no estén alineadas con las finalidades de la organización.

Limitándonos a la seguridad propiamente dicha, los riesgos pueden ser múltiples. El primer paso es conocerlos y el segundo es tomar decisiones al respecto; conocerlos y no tomar decisiones no tiene sentido y debiera crearnos una situación de desasosiego.

Dado que las medidas tienen un costo, a veces, los funcionarios se preguntan cuál es el riesgo máximo que podría soportar su organización. La respuesta no es fácil porque depende de la criticidad del sector y de la entidad misma, de su dependencia respecto de la información, y del impacto que su no disponibilidad pudiera tener en la entidad. Si nos basamos en el impacto nunca debería

aceptarse un riesgo que pudiera llegar a poner en peligro la propia continuidad de la entidad, pero este listón es demasiado alto.

Por debajo de ello hay daños de menores consecuencias, siendo los errores y omisiones la causa más frecuente - normalmente de poco impacto pero frecuencia muy alta - y otros, como por ejemplo:

- el acceso indebido a los datos (a veces a través de redes),
- la cesión no autorizada de soportes magnéticos con información crítica (algunos dicen "sensible"),
- los daños por fuego, por agua (del exterior como puede ser una inundación, o por una tubería interior),
- la variación no autorizada de programas, su copia indebida, y tantos otros, persiguiendo el propio beneficio o causar un daño, a veces por venganza.

Otra figura es la del “hacker”, que intenta acceder a los sistemas sobre todo para demostrar (a veces, para demostrarse a sí mismo/a) qué es capaz de hacer, al superar las barreras de protección que se hayan establecido.

Alguien podría preguntarse por qué no se citan los virus, cuando han tenido tanta incidencia. Afortunadamente, este riesgo es menor en la actualidad comparando con años atrás. Existe, de todas maneras, un riesgo constante porque de forma continua aparecen nuevas modalidades, que no son detectadas por los programas antivirus hasta que las nuevas versiones los contemplan. Un riesgo adicional es que los virus pueden llegar a afectar a los grandes sistemas, sobre todo a través de las redes, pero esto es realmente difícil - no nos atrevemos a decir que imposible- por las características y la complejidad de los grandes equipos y debido a las características de diseño de sus sistemas operativos.

En definitiva, las amenazas hechas realidad pueden llegar a afectar los datos, en las personas, en los programas, en los equipos, en la red y algunas veces, simultáneamente en varios de ellos, como puede ser un incendio.

Podríamos hacernos una pregunta realmente difícil: ¿qué es lo más crítico que debería protegerse? La respuesta de la mayoría, probablemente, sería que las personas resultan el punto más crítico y el valor de una vida humana no se puede comparar con las computadoras, las aplicaciones o los datos de cualquier entidad. Ahora bien, por otra parte, podemos determinar que los datos son aún más críticos si nos centramos en la continuidad de la entidad.

Como consecuencia de cualquier incidencia, se pueden producir unas pérdidas que pueden ser no sólo directas (comúnmente que son cubiertas por los seguros) más fácilmente, sino también indirectas, como la no recuperación de deudas al perder los datos, o no poder tomar las decisiones adecuadas en el momento oportuno por carecer de información.

Sabemos que se producen casos similares en gran parte de entidades, pero en general no conocemos a cuáles han afectado (o lo sabemos pero no podemos difundirlo), porque por imagen estos no se hacen públicos y el hecho de que se conozcan muchos más referidos a Estados Unidos y a otros puntos lejanos que respecto de nuestros países no significa que estemos a salvo, sino que nuestro pudor es mayor y los ocultamos siempre que podemos.

# HACKING ETICO

## 2.5 INTRODUCCIÓN

Se describe el Hacker Ético como un profesional de la seguridad, que usa las mismas herramientas de software y técnicas de los hackers para encontrar las debilidades de seguridad en redes y sistemas informáticos, para fines de defensa y protección.

La mayoría de los hackers éticos están en el negocio de la seguridad informática con fines de lucro, una actividad conocida como *pruebas de penetración*, o *pruebas de pentest*, para abreviar las pruebas de penetración son generalmente llevadas a cabo por un profesional de seguridad para identificar riesgos de seguridad y vulnerabilidades de los sistemas y redes. El propósito de identificar riesgos y vulnerabilidades es para encontrar una contramedida y de esta manera mitigar el riesgo en cierta medida, anticipándose a las intenciones del atacante.

Otro componente clave de hacking ético es tener siempre el permiso del titular de los datos antes de acceder al sistema informático. Esta es una de las formas que los hackers éticos pueden superar el estereotipo de los hackers y ganarse la confianza de los clientes.

## 2.6 DEFINICIONES Y TERMINOLOGIA

### 2.6.1 VULNERABILIDAD

Referente a debilidad dentro del sistema; es decir, la existencia de una falla de software, diseño de la lógica, o un error de aplicación que puede llevar a un evento

inesperado y no deseable. El código de explotación está escrito para apuntar a una vulnerabilidad y provocar un fallo en el sistema.

### 2.6.2 AMENAZA

Amenaza de un entorno o situación que podría conducir a una posible infracción de la seguridad. Factor externo que puede suscitar en la explotación de una vulnerabilidad.

### 2.6.3 ATAQUE

Un ataque ocurre cuando un sistema se ve comprometido sobre la base de una vulnerabilidad. Muchos ataques se perpetúan a través de un exploit.

### 2.6.4 VIRUS

Son programas informáticos que se copian automáticamente a un sistema sin el permiso del usuario y que tiene como fin alterar su normal funcionamiento. Los virus informáticos generalmente reemplazan archivos ejecutables por otros

infectados, y pueden llegar a destruir intencionalmente los datos almacenados en un computador.

### 2.6.5 SPOOFS

Los Spoofs o Engaños se manifiestan muy a menudo en redes de información, se trata de una situación en que una persona o software suplantan exitosamente la identidad o la presentación del original; falsificando información y por consiguiente, obteniendo acceso ilegítimo.

### 2.6.6 PORT SCANNING

El escaneo de puertos permite la determinación de las características de una red o sistema remoto, de manera que se pueden identificar los equipos activos, sus servicios, los sistemas que estos poseen y la forma en que están organizados.

### 2.6.7 EXPLOITS

Los Exploits son una vía ya definida para romper la seguridad de un sistema aprovechando una vulnerabilidad. Un exploit se refiere a una parte de software,

herramienta o técnica que se vale de una vulnerabilidad para poder obtener privilegios dentro de un sistema, hacerle perder su integridad, y si es el caso, denegar servicios en el sistema atacado. Los Exploits son peligrosos debido a que todo software tiene vulnerabilidades, los hackers e individuos que tratan de ingresar a los sistemas conocen esas vulnerabilidades y las buscan para tomar ventaja de ellas.

## 2.7 CLASIFICACIÓN HACKER

Mantenerse dentro de la ley es una necesidad para el hacker ético, además deben actuar siempre de manera profesional.

Los hackers pueden ser divididos en tres grupos:

White Hats

Black Hats

Gray Hats

### 2.7.1 WHITE HATS

Hackers de sombrero blanco o White hats hackers, son generalmente profesionales de la seguridad con el conocimiento de la piratería y el conjunto de

herramientas de hacker que utilizan este conocimiento para localizar los puntos débiles y poner en práctica contramedidas. Además los hackers de sombrero blanco son aquellos que cuentan con el permiso del titular de los datos. Es fundamental obtener el permiso antes de comenzar cualquier actividad hacking. Esto hace la diferencia entre un profesional de la seguridad o hacker de sombrero blanco frente a un hacker malicioso en el que no se puede confiar.

### 2.7.2 BLACK HATS

Hackers de sombrero negro o black hats son hackers maliciosos o crackers que utilizan sus habilidades para fines ilegales o dañinos. Irrumpen o violan la integridad del sistema de o sistemas remotos, con mala intención. Después de haber obtenido acceso no autorizado, hackers de sombrero negro destruyen datos vitales, niegan el servicio a los usuarios legítimos, y sólo crea problemas a sus objetivos. Black hats hackers y crackers pueden ser fácilmente diferenciados de los hackers de sombrero blanco, porque sus acciones son maliciosas. Esta es la definición tradicional de un hacker y lo que la mayoría de la gente considera que es un hacker.

### 2.7.3 GRAY HATS

Gray Hats o Hackers de Sombreros grises son aquellos que pueden trabajar ofensiva o defensivamente, dependiendo de la situación. Es referente a un hacker talentoso quien a veces actúa ilegalmente, pero con buenas voluntades. Por ejemplo, si una debilidad se descubre en un servicio ofrecido por un banco de inversión, el hacker está haciendo un favor al banco, dando al banco la posibilidad de corregir la vulnerabilidad. Son un híbrido entre los hackers de sombrero blanco y de sombrero negro. Usualmente no atacan por intereses personales o con malas intenciones, pero están preparados para cometer crímenes durante el curso de sus hazañas tecnológicas con el fin de lograr una mayor seguridad

## 2.8 PENTEST

Test de Penetracion o Pruebas de penetración, a veces abreviado como PenTest, es un proceso que se sigue para realizar una evaluación de la seguridad o hardcore de auditoría.

Una metodología define un conjunto de reglas, prácticas, procedimientos y métodos que son perseguidos y ejecutados durante el curso de las auditorías de cualquier programa de seguridad de la información. Por lo tanto, la metodología de pruebas de penetración se define un plan de trabajo con ideas prácticas y

prácticas probadas que debe ser manejado con mucho cuidado a fin de evaluar el sistema de seguridad correctamente.

Las pruebas de penetración pueden ser realizadas de manera independiente o como parte de un proceso de gestión de la Tecnologías de la Información o TI security risk que pueden ser incorporados en un normal desarrollo del ciclo de vida. Aquí subyace una división del profesional de seguridad, el profesional de seguridad independiente, aquel que realiza de manera independiente el test de penetración, informa y muestra las deficiencias en seguridad, y el profesional de seguridad que forma parte de un equipo de consultoría de seguridad, el que realiza el test de penetración como parte de un proceso mayor dentro de la organización de seguridad a la que brinda sus servicios de esta manera ejecutando el test de penetración y encargado de dar a conocer las deficiencias de seguridad, para posteriormente en conjunto mejorar los niveles de seguridad.

Es de vital importancia darse cuenta de que la seguridad de un producto no sólo depende de los factores relacionados con el entorno de TI. También se basa en productos específicos de seguridad que brinde mejores prácticas. Esto implica la aplicación de los requisitos de seguridad adecuados, la realización de análisis de riesgos, modelado de amenazas, revisiones de código, la seguridad y la medición operativa. Se considera pentesting o test de penetración a la evaluación de seguridad en forma sistemática y agresiva manejados por profesionales calificados con o sin conocimiento previo de un sistema en estudio. Puede ser utilizado para evaluar los componentes de la infraestructura de las Tecnologías de

la Información, incluyendo todas las aplicaciones, los dispositivos de red, sistemas operativos, medios de comunicación, seguridad física y la psicología humana. El resultado de las pruebas de penetración Por lo general, contiene un informe que se divide en varias secciones frente a las debilidades encontradas en el estado actual del sistema y las contramedidas para siguiendo sus recomendaciones.

## TIPOS DE PRUEBAS DE PENETRACIÓN

Existen diferentes tipos de pruebas de penetración, los dos enfoques que son más ampliamente aceptados en general por la industria son Black-Box(pruebas de caja negra) y White-Box(pruebas de caja blanca).

## BLACK-BOX O PRUEBAS DE CAJA NEGRA

El enfoque de Caja Negra también se conoce como pruebas externas. Si bien la aplicación de este enfoque, el Auditor de Seguridad evaluará la infraestructura de red desde una ubicación remota y no estará al tanto de las tecnologías internas desplegadas por la organización. Mediante el empleo de técnicas de hacking se puede revelar un conjunto conocido o desconocido de vulnerabilidades que puedan existir en la red. Un auditor Black-Box o de Caja Negra también se conoce

como Black-Hat o Hacker de sombrero negro. Es importante para un auditor entender y clasificar estas vulnerabilidades según su nivel de riesgo (bajo, medio o alto). El riesgo en general puede ser medido de acuerdo con la amenaza impuesta por la vulnerabilidad ya sea financiera u otras y que pérdida podría ocurrir

Una vez que el proceso de prueba se ha completado, se genera un informe con toda la información necesaria sobre la evaluación de seguridad de destino, además se realiza una clasificación de los riesgos identificados para el contexto empresarial.

Por lo tanto, el uso de un proceso metodológico proporciona grandes beneficios al entender y analizar críticamente la integridad de las defensas actuales durante cada etapa del proceso de pruebas.

**WHITE-BOX O PRUEBAS DE CAJA BLANCA**

El enfoque de caja blanca también se conoce como las pruebas internas. Un auditor que participa en este tipo de proceso de pruebas de penetración debe estar consciente de todas las tecnologías internas y los soportes utilizados por el entorno de destino. Por lo tanto, se abre una puerta ancha de un auditor para ver y

evaluar críticamente las vulnerabilidades de seguridad con un mínimo esfuerzo posible. Un auditor comprometido con las pruebas de caja blanca es también conocido como Hacker de sombrero blanco. Hace aportar más valor a la organización en comparación con el enfoque de caja negra en el sentido de que se eliminarán todos los asuntos de seguridad interna que yace en el entorno de destino de infraestructura, tanto, por lo que es más apreciado por el adversario malicioso para infiltrarse desde el exterior. El número de pasos involucrados en pruebas de caja blanca es más similar a la de caja negra, excepto por el uso de la meta de alcance, la recopilación de información, fases de identificación pueden ser excluidos. Además, el enfoque de caja blanca se puede levantar fácilmente integrado un ciclo de desarrollo lo más regular posible para erradicar cualquier problema de seguridad en su etapa temprana, antes de ser explotados por los intrusos maliciosos. El tiempo y costo requerido para encontrar y resolver las vulnerabilidades de seguridad es comparativamente menor que el enfoque de Pruebas de caja negra.

La combinación de ambos tipos de pruebas de penetración proporciona una visión de gran alcance para los puntos de vista de seguridad interna y externa. Esta combinación se conoce como pruebas de caja gris, auditores comprometidos con las pruebas de caja gris es también conocida como Hackers de Sombrero gris. Los principales beneficios en la elaboración y práctica de la caja gris enfoque es un conjunto de ventajas planteados por los dos enfoques antes mencionados. Sin

embargo, esto requiere que un auditor con conocimientos limitados de un sistema interno para elegir la mejor manera de evaluar su seguridad en general. En el otro lado, los casos de prueba externa orientada por el enfoque de la caja gris son similares a las del enfoque de Caja negra, sobre todo esto puede ayudar a tomar mejores decisiones al tener un enfoque global de las vulnerabilidades tanto internas como externas de la organización.

# CAPÍTULO III

# EVALUACION DE LA SEGURIDAD

El método empleado para este análisis de seguridad, es el de un profesional de seguridad o hacker ético mencionado en el Capítulo II, por lo cual se pretende explicar detalladamente a continuación.

## 3.1 FOOTPRINTING

El primer paso del proceso de intrusión es la recopilación de información sobre un objetivo. La recopilación de información, también conocida como FootPrinting o huella, es el proceso de recopilación de toda la información disponible acerca de

una organización. En la actualidad la información está disponible en partes y piezas de muy diversas fuentes dentro de la Internet.

La ventaja de utilizar herramientas de footprinting es que utiliza Google u otros navegadores para obtener información. De esta forma el atacante determina la mejor manera de acceder a los objetivos. Antes de un ataque o la utilización de algún exploit que pueda ser puesto en marcha, el atacante comprueba el sistema operativo y versión, así como los tipos de aplicaciones que se ejecutan para que el ataque resulte más eficaz y puedan ser lanzados contra el objetivo.

Entre lo que el atacante en el proceso de footprinting puede encontrar mostramos las siguientes:

- Nombre de dominio
- Bloques de red
- Servicios de red y aplicaciones
- Arquitectura del sistema
- Sistema de detección de intrusos
- Mecanismos de autenticación
- Direcciones IP específicas

- Acceso a los mecanismos de control
- Direcciones de contacto
- Los números de teléfono

El propósito de esta fase preparatoria por parte del atacante es aprender lo más que pueda acerca de un sistema, sus capacidades de acceso remoto, sus puertos y servicios, y algunos aspectos específicos de su seguridad.

Footprinting puede hacer uso de varias herramientas de hacking, aplicaciones o sitios web, que permiten a los hackers para localizar información de forma pasiva.

Mediante el uso de herramientas de footprinting, un posible atacante puede ganar un poco de información básica sobre el objetivo. Un hacker puede eliminar instrumentos que no son efectivos contra los sistemas de destino o de la red. Footprinting no sólo acelera el proceso de intrusión mediante la eliminación de ciertos conjuntos de herramientas sino que también reduce la probabilidad de detección, menos pérdida de tiempo al hacer uso de la herramienta adecuada para el trabajo.

A continuación se muestra herramientas de footprinting que vienen embebidas en BackTrack.

Metagoofil es una herramienta que utiliza el motor de búsqueda de Google para obtener los metadatos de los documentos disponibles en el dominio de destino.

Un metadato es información relativa a un documento o dicha de otra manera metadato es la información insertada en los archivos por el software de edición o creación de los mismos, estos metadatos contienen información acerca de la creación del archivo como: nombre de autor, autores anteriores, nombre de compañía, cantidad de veces que el documento fue modificado, fecha de creación y más. Los metadatos, si bien son útiles para la elaboración y edición de documentos, pueden terminar convirtiéndose en una fuente de información de riesgo que un atacante puede utilizar.

Actualmente Metagoofil soporta los siguientes tipos de documentos:

- Documentos de Word (doc, odt)
- Hojas de cálculo del documento (XLS, ODS)
- Presentaciones de archivos (ppt, odp)
- Archivos PDF

Metagoofil trabaja de la siguiente manera:

- Busca todos los tipos de archivos por encima del dominio de destino utilizando Google

- Descarga todos los documentos encontrados y los guarda en el disco local
- Realiza la extracción de los metadatos de los documentos descargados
- Guarda el resultado en un archivo HTML

Los metadatos que se pueden encontrar son los nombres de usuario, la ruta o path, y la dirección MAC.

En la consola de BackTrack mediante los siguientes comandos ingresamos a Metagoofil.

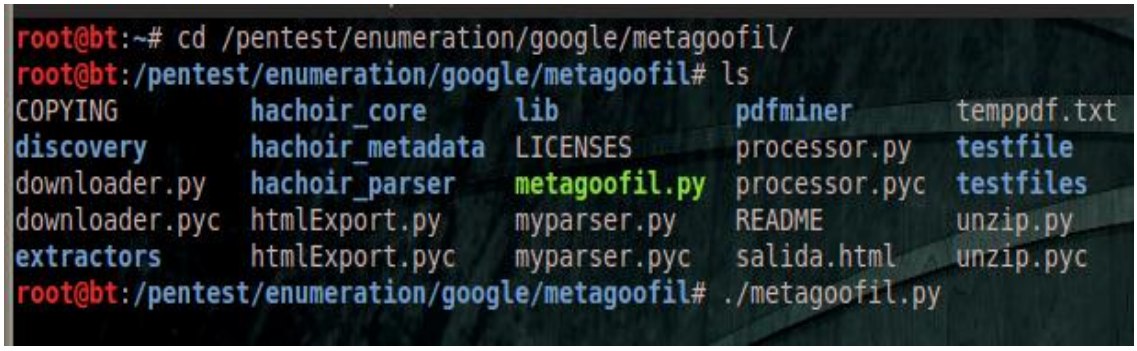



**FIGURA III.I Ingreso a Metagoofil**

Para el uso de metagoofil, se procede a recoger todos los documentos de un dominio de destino en este caso es *espoch.edu.ec* y guardarlos en la siguiente ruta llamado */root/Jorge/Analisis_sistemas/metagoofil.html* limitamos la descarga en este caso de archivos .doc en 25 archivos. El informe generado se guardará en metagoofil.html previamente creado en la ruta especificada anteriormente. El siguiente es la orden que se ejecuta en un terminal, lo cual se muestra en la Figura III.2 a continuación.

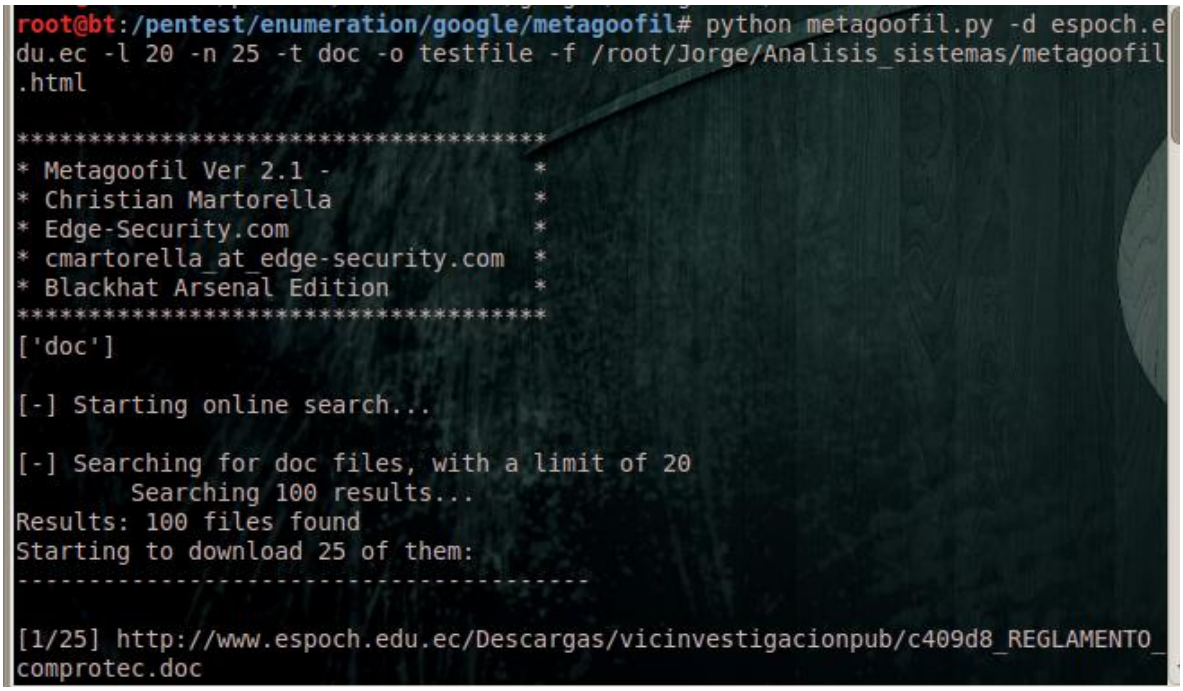



**FIGURA III.II Metagoofil en ejecución**

Metagoofil inicia la descarga de los archivos .doc lo cual se muestra en la Figura III.3

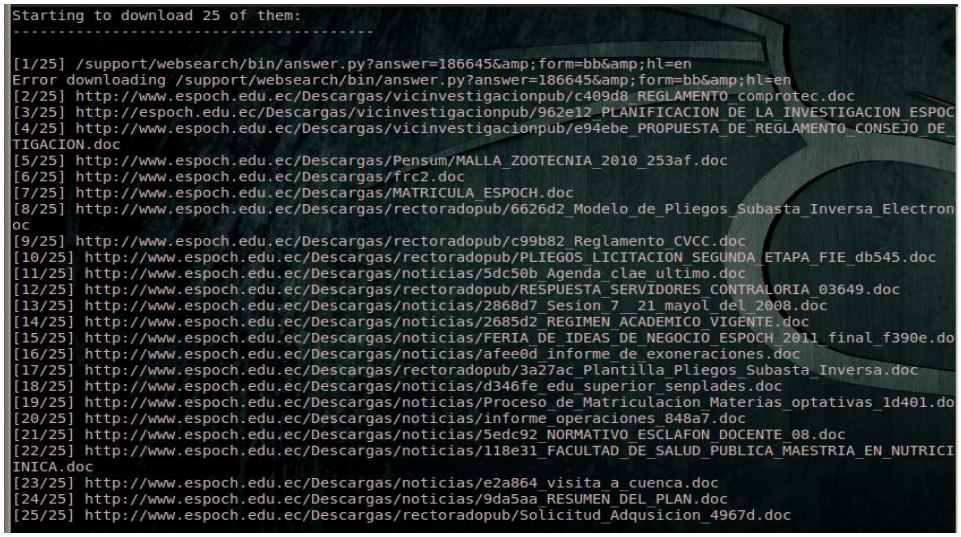



**FIGURA III.III Documentos descargados por Metagoofil**

Metagoofil automáticamente extrae la metadata de los archivos descargados y en primera instancia muestra una lista de usuarios encontrados, esto se muestra en la Figura lll.4

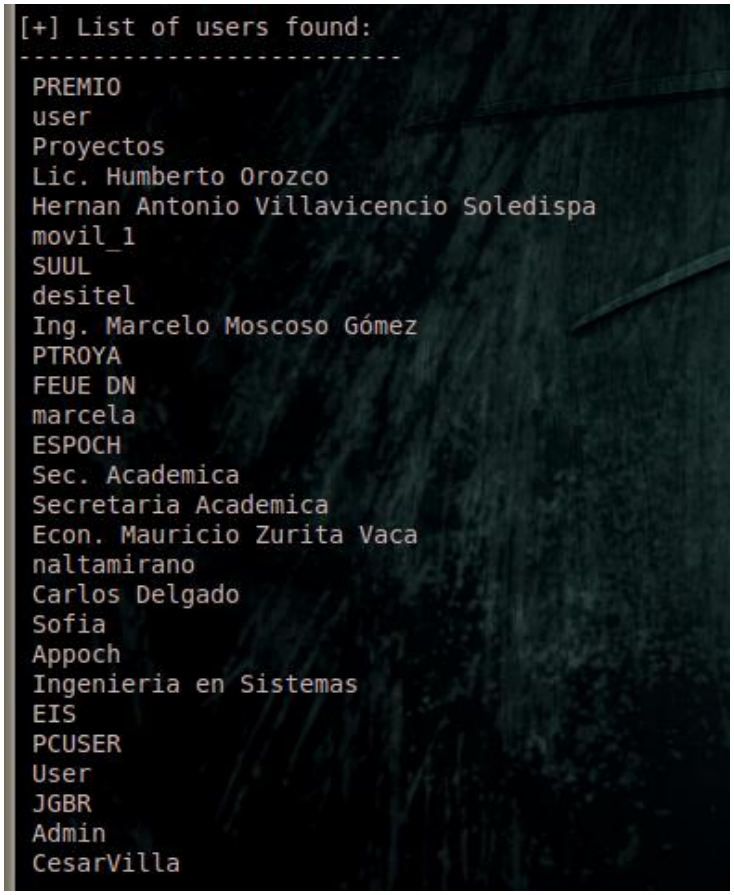



**FIGURA lll.IV Lista de Usuarios Encontrados.**

Además se encuentra el software utilizado para la edición de los documentos descargados, se muestra en la Figura lll.

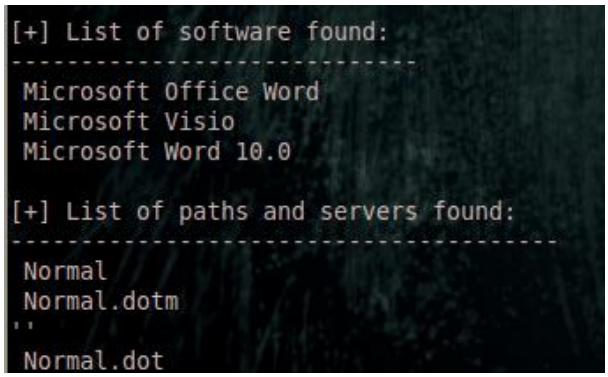



**FIGURA III.V Lista de Software Encontrado**

Una de las ventajas adicionales de metagoofil es que puede representar de forma gráfica los resultados, al ser almacenados la información obtenida por la extensión .html, se visualiza el resultado en el navegador del cual se desprende una gran cantidad de información de los documentos que se ha recogido, como nombres de usuario y la información de la ruta. Se puede utilizar los nombres de usuario para realizar diccionarios y de esta manera realizar ataques de fuerza bruta por contraseña, mientras que la información de la ruta se puede utilizar para adivinar el sistema operativo utilizado por el objetivo. Se obtuvo toda esta información sin tener que ir a la página web de dominio del objetivo.

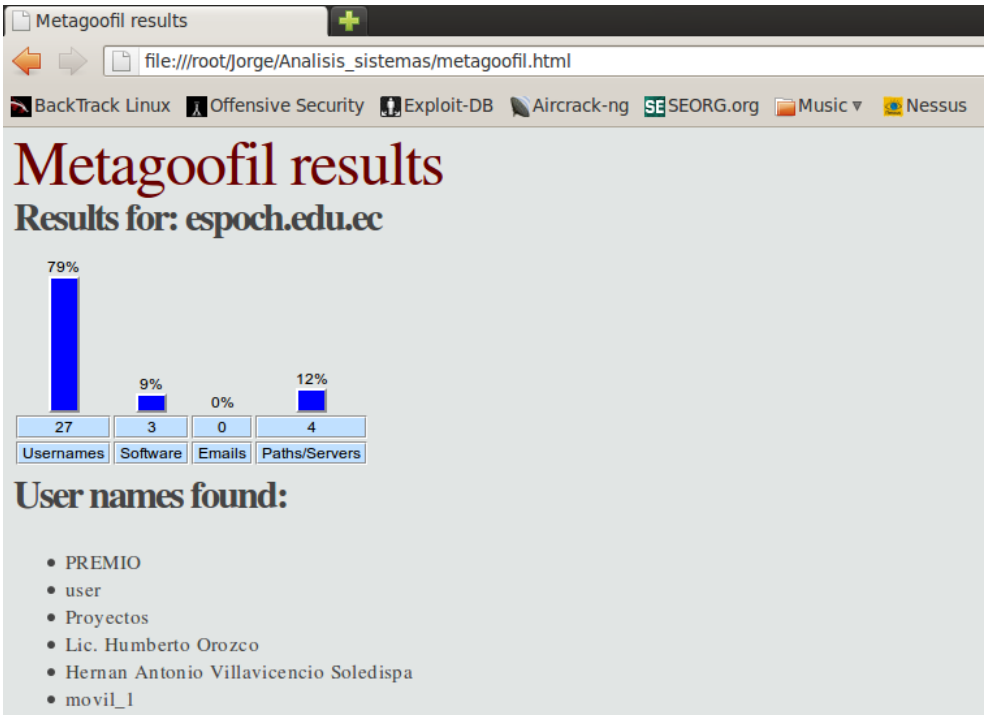



**FIGURA III.VI Resultado Grafico de Metagoofil**

Además de obtener la misma información que la que se tuvo en la consola mostrada en las figuras anteriores, Metagoofil muestra la metadata encontrada y al documento del que se sustrajo dicha información.


**FIGURA III.VII Archivos y metadatos encontrados.**

## Enumeración DNS

*Enumeración DNS* es el proceso de localizar todos los servidores DNS y los registros correspondientes para una organización. Una empresa puede tener los servidores DNS internos y externos que pueden contener información como nombres de usuario, nombres de equipos y direcciones IP de los sistemas de destino potencial. El atacante puede utilizar el Domain Name System (DNS) para comprobar la configuración de los servidores DNS.

La siguiente lista describe los tipos de registro DNS comunes y su uso:

- A MAP (Addres) un nombre de host a una dirección IP
- SOA (Start of Authority) Identifica el servidor DNS responsable de la información de dominio

- CNAME (nombre canónico) Proporciona otros nombres o alias para el registro de dirección
- MX (Mail Exchange) Identifica el servidor de correo para el dominio
- SRV (Service) identifica los servicios tales como servicios de directorio
- PTR (Pointer) asigna direcciones IP a nombres de host
- NS (Name Server) Identifica otros servidores de nombres para el dominio.

Una herramienta de gran alcance es NSlookup, esta herramienta realiza consultas a servidores DNS para registrar la información.

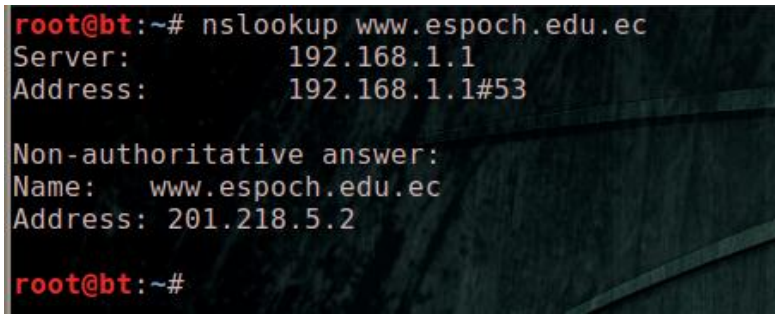



**FIGURA III.VIII Nslookup al sitio de la ESPOCH.**

Traceroute es una herramienta de rastreo de paquetes que está disponible para la mayoría de sistemas operativos. Opera enviando un Internet Control Message Protocol (ICMP) echo a cada salto (router o gateway) a lo largo del camino, hasta

que la dirección de destino sea alcanzado. Cuando los mensajes ICMP se envían desde el router, el tiempo de vida (TTL) se reduce en uno por cada router a lo largo del camino. Esto permite que un atacante determine el número de saltos que un router es del remitente.

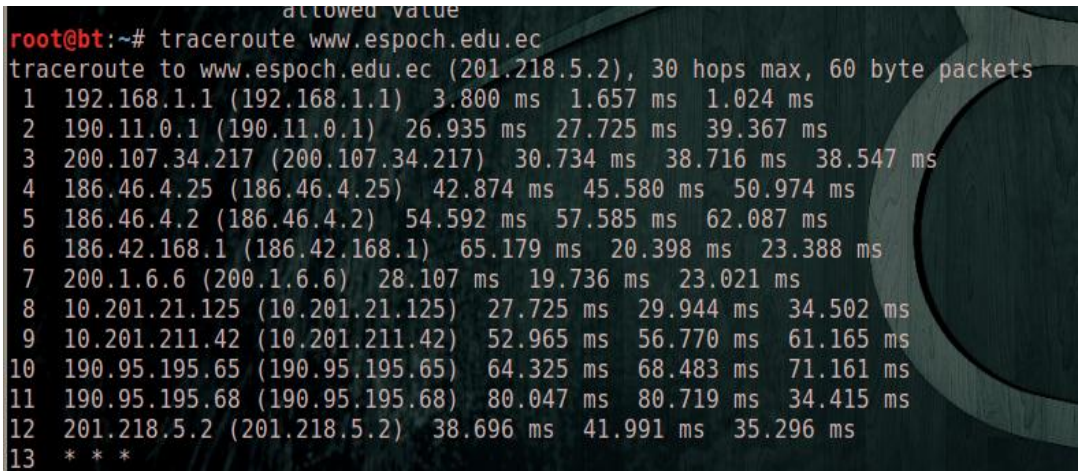



**FIGURA III.IX Traceroute al sitio de la ESPOCH.**

Theharvester, el objetivo de esta herramienta es recolectar cuentas de correo y nombres de usuarios pertenecientes a un dominio o una empresa en particular. La idea es poder utilizarlos en posteriores ataques, como pueden ser de fuerza bruta, ingeniería social.

Las fuentes públicas soportadas son:

- Google
- Bing

- PGP
- Linkedin

Mediante los siguientes comandos se hace uso de esta herramienta.

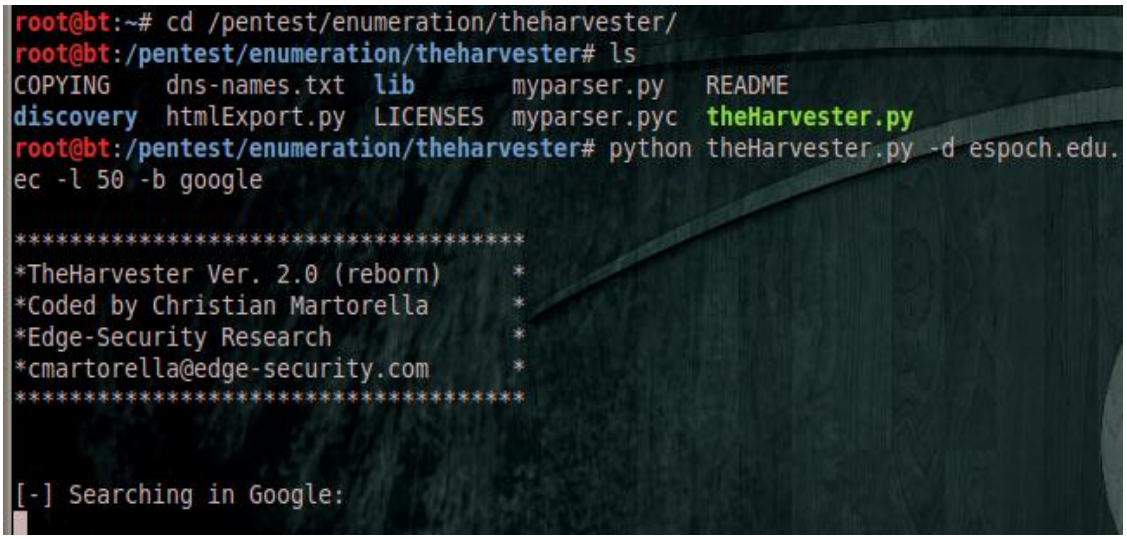



**FIGURA III.X Thehavester al sitio de la ESPOCH.**

La información brindada por thehavester es muy útil para el atacante, ya que se obtiene mails con sus respectivos usuarios y además muestra los dominios internos dentro de la institución.

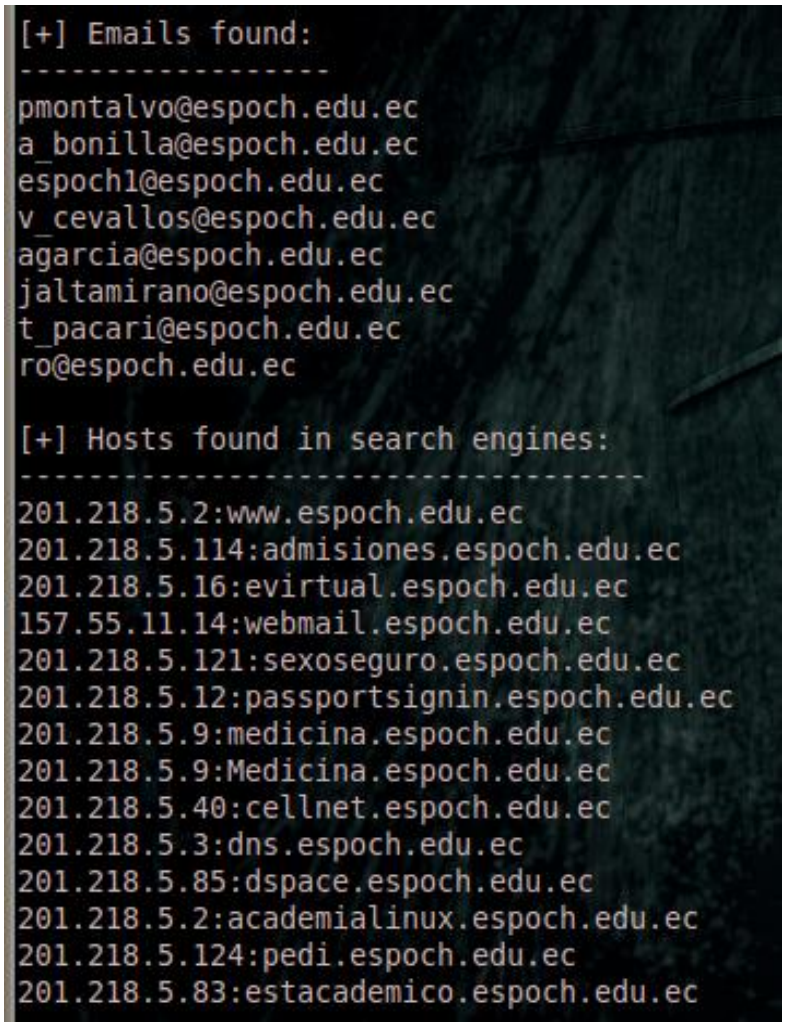



**FIGURA III.XI Subdominios de la ESPOCH.**

De este modo el atacante sin recurrir hasta el momento al sitio oficial de la ESPOCH, cuenta con información de cuentas de usuarios del correo interno de la institución, posibles subdominios, software utilizado y usuarios, lo cual puede brindar un panorama poco alentador para la institución en cuestión, a continuación se muestra una herramienta que recopila la mayor parte de las herramientas utilizadas hasta el momento.

Maltego es una aplicación inteligente de código abierto, permite reunir información, y representar la información de una manera significativa. La palabra "código abierto" en Maltego significa que recopila información de los recursos de código abierto, no quiere decir que Maltego es un software de código abierto.

Maltego permite enumerar la información de infraestructura de Internet, tales como:

- Los nombres de dominio
- nombres DNS
- Información Whois
- Los bloques de red
- Las direcciones IP

Para ingresar en maltego en BackTrack

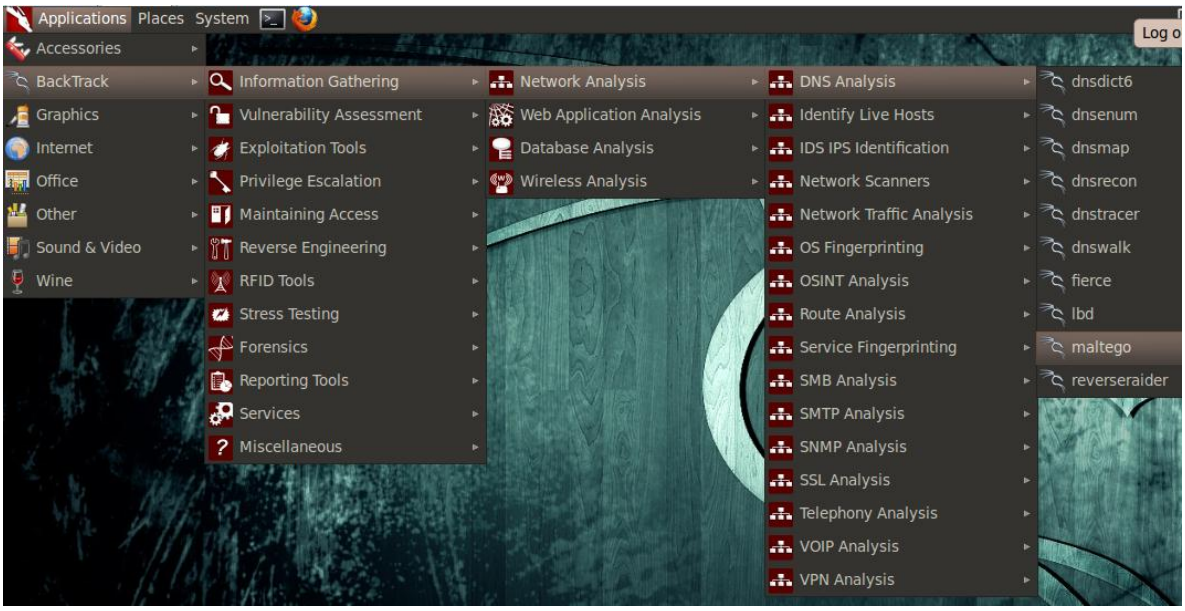



**FIGURA III.XII Localización de Maltego en BackTrack.**

También se puede utilizar para recopilar información sobre las personas, tales como:

- Las empresas y organizaciones relacionadas con la persona
- Dirección de correo electrónico relacionados con la persona
- Sitios web relacionados con la persona
- Las redes sociales en relación con la persona
- Los números de teléfono con la persona

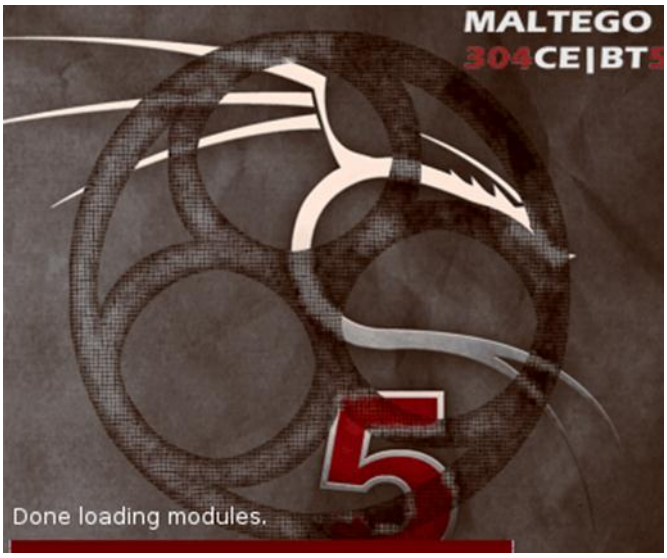



**FIGURA III.XIII Inicialización de Maltego en BackTrack.**

**Limitaciones de Maltego.**

- Se mostrará una pantalla de aviso de 13 segundos antes de poder empezar a utilizar Maltego
- No guardar y exportar las capacidades
- Los niveles de zoom son limitadas
- Sólo se puede ejecutar transforma en una sola entidad en un momento
- No se puede copiar y pegar texto desde el punto de vista detallada
- Transforma limitada a 75 veces por día
- La conexión limitada al Servidor de Aplicaciones de Transformación (SAT)

Hay más de 70 se transformaciones en Maltego disponibles. La palabra "transformación" se refiere a la fase de recopilación de información realizado por Maltego. Una transformación significa que Maltego sólo lo hará una fase de recopilación de información.

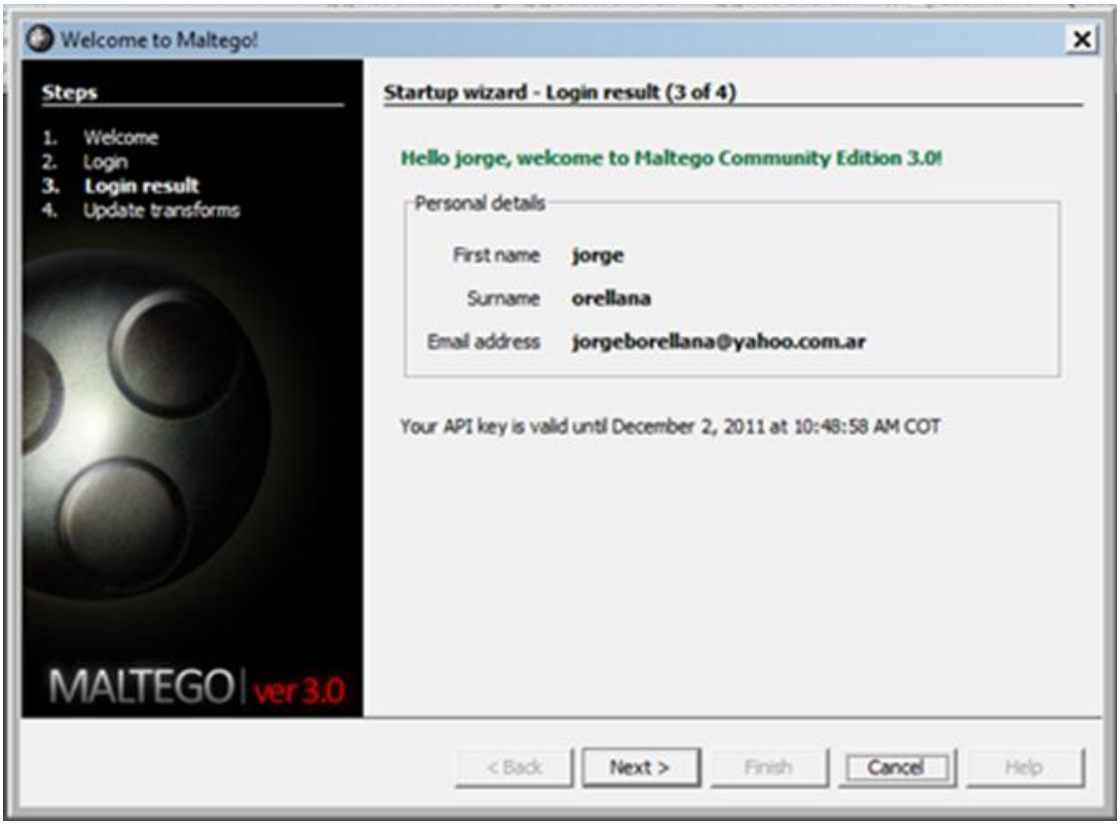



**FIGURA III.XIV Ingreso a Maltego en BackTrack.**

Previamente al ingreso Maltego necesita registrar al usuario para poder utilizar dicha herramienta.

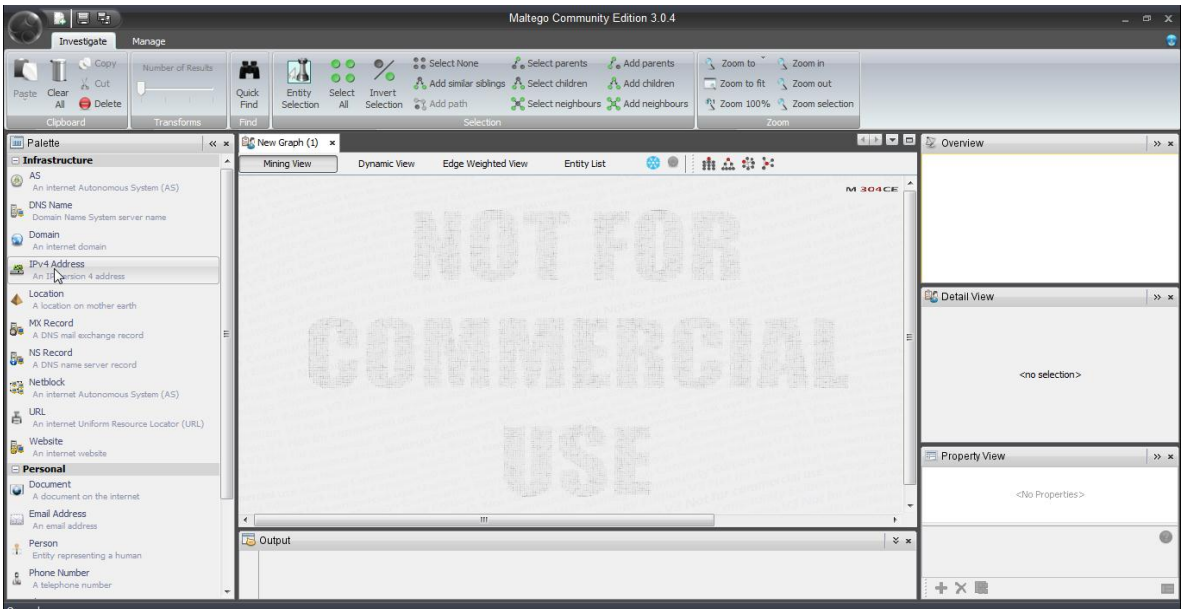



**FIGURA III.XV Interfaz de Trabajo en Maltego.**

En la parte superior izquierda, se puede observar la ventana de palette o paleta en español. En la paleta, podemos elegir la entidad en la que queremos recoger la información de las entidades. Maltego divide en cuatro grupos en su versión pagada y en la versión free solo se tienen dos.

Entre las opciones que vienen por defecto en maltego de prueba se tiene:

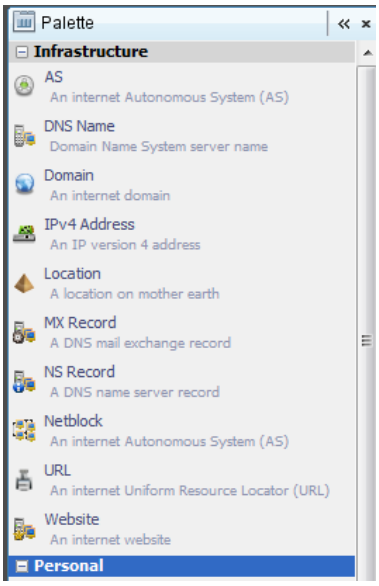



**FIGURA III.XVI Infraestructura.**

Infraestructure contiene As, DNS name, Domain, IP addres, Netblock y WEB Site, importantes para la localización de alguna organización o institución.

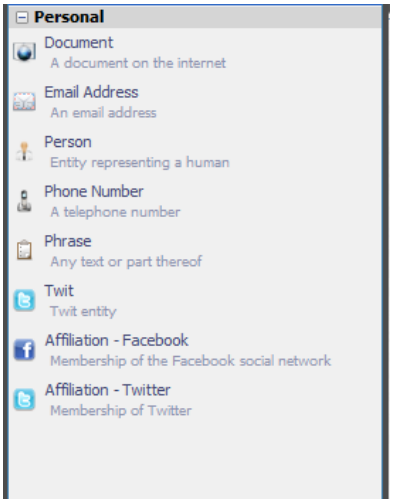



**FIGURA III.XVII Personal.**

Personal, enfocado más hacia la búsqueda de información de alguna persona, ideal para ingeniería social.

Estas dos últimas vienen incluidas en la versión pagada.

• Pentesting contiene Banner, Puerto, Servicio, Vuln, Webdir y Webtitle

• Wireless contiene OPEN-AP, AP-Desconocido, WEP AP, AP-WPA, WPA2 y AP-

Esto indica el potencial de esta herramienta, que no solo recaba información sino además encuentra vulnerabilidades y facilita el trabajo del atacante.

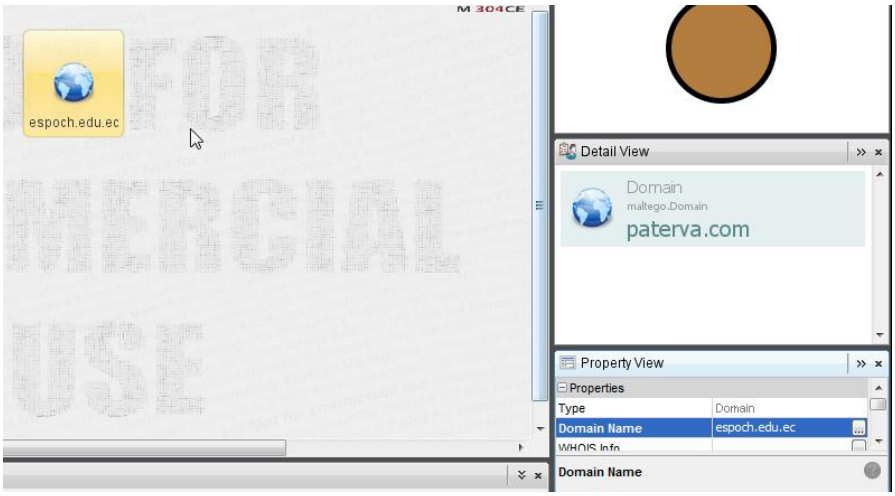



**FIGURA III.XVIII Ingreso del Dominio a examinar en Maltego.**

Hay más de 70 transformaciones en disponibles Maltego. La palabra "transformación" se refiere a la fase de recopilación de información realizado por

Maltego. Una transformación significa que Maltego sólo lo hará una fase de recopilación de información. Como se muestra en la Figura.

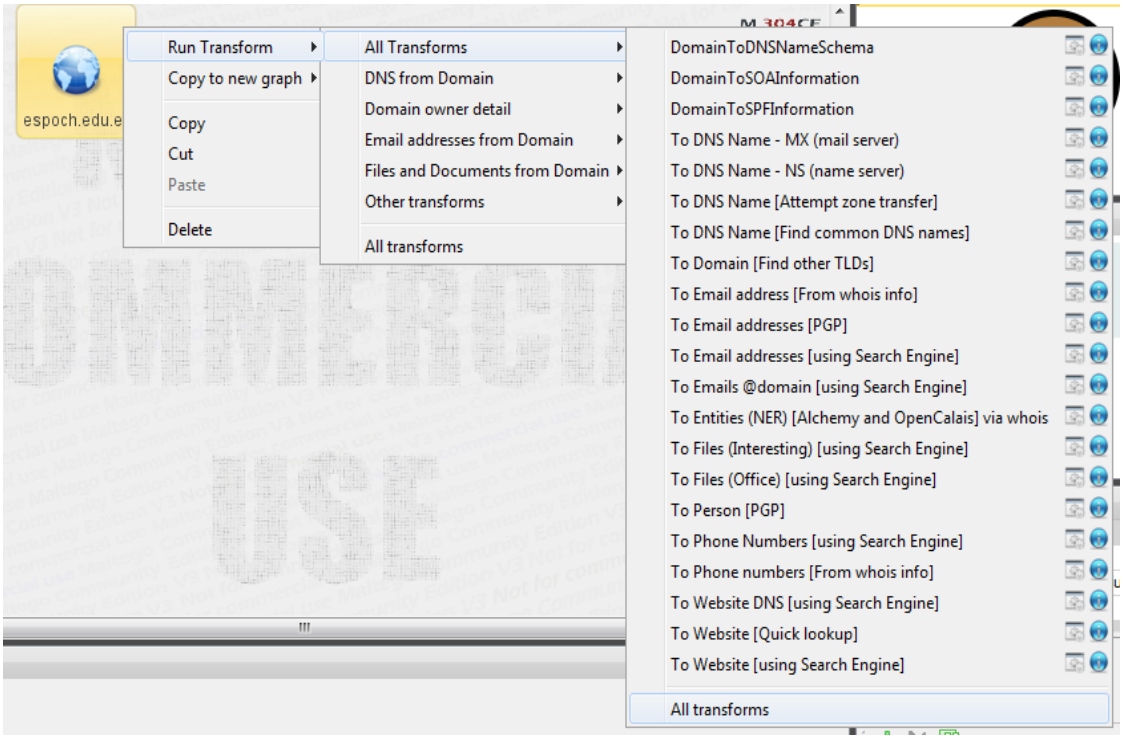



**FIGURA III.XIX Transformadas que utiliza Maltego.**

Para un análisis más exhaustivo se escoge All transforms. o todas las transformaciones como se muestra en la figura.

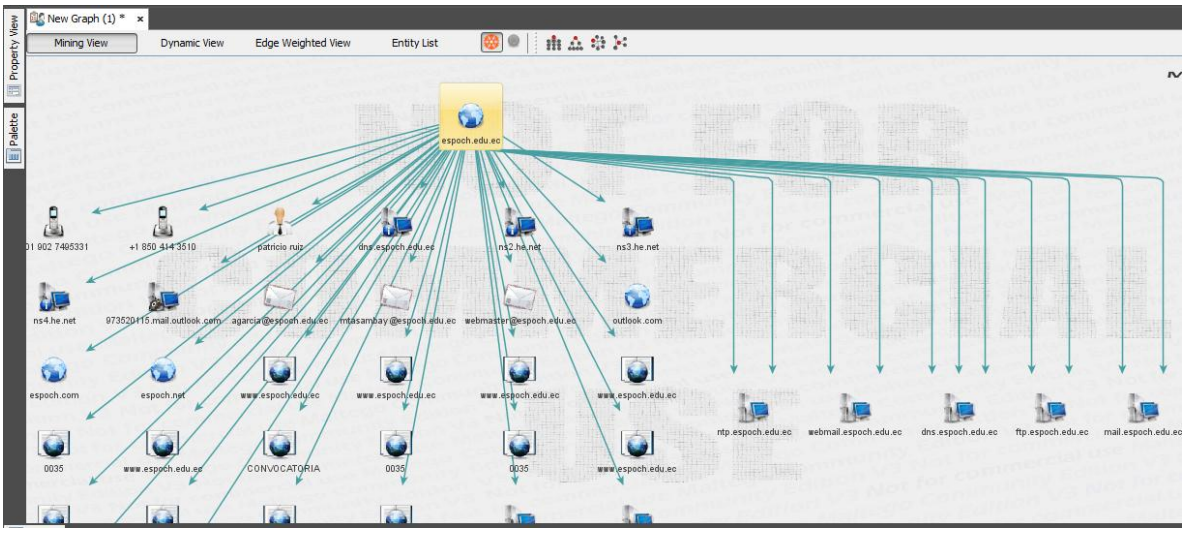



**FIGURA III.XXResultado de Maltego con Mining View.**

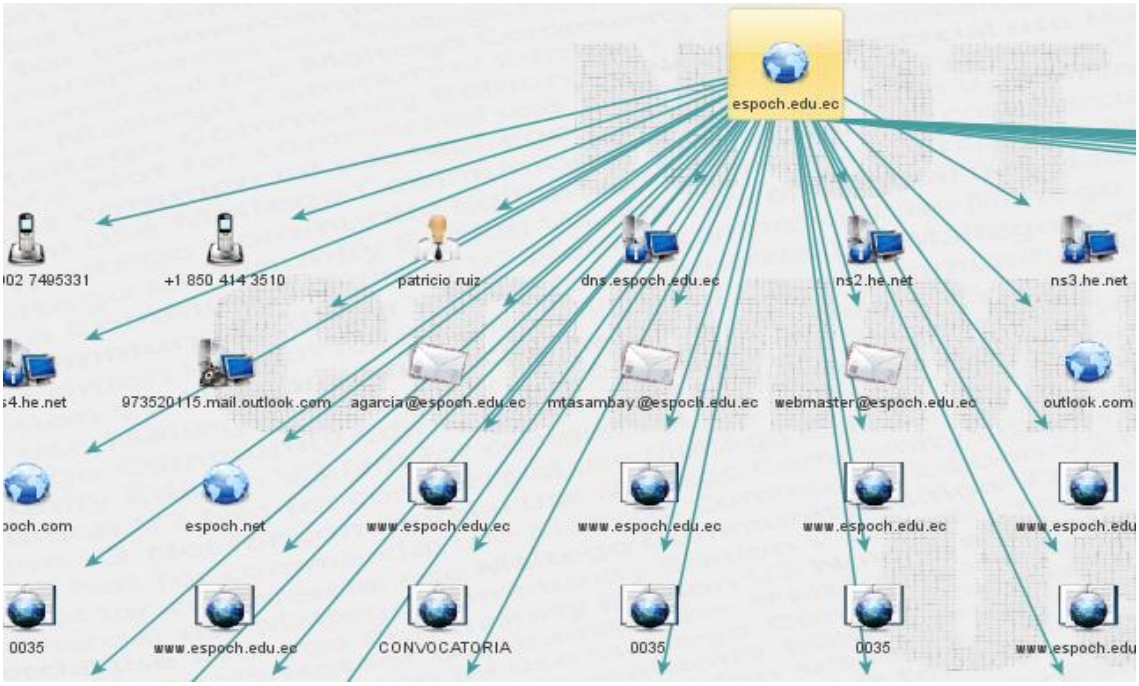



**FIGURA III.XXI Información encontrada con Maltego.**

De manera gráfica Maltego proporciona información de posibles usuarios, documentos, números telefónicos, y varios subdomios notablemente visibles en la figura. Y figura ..

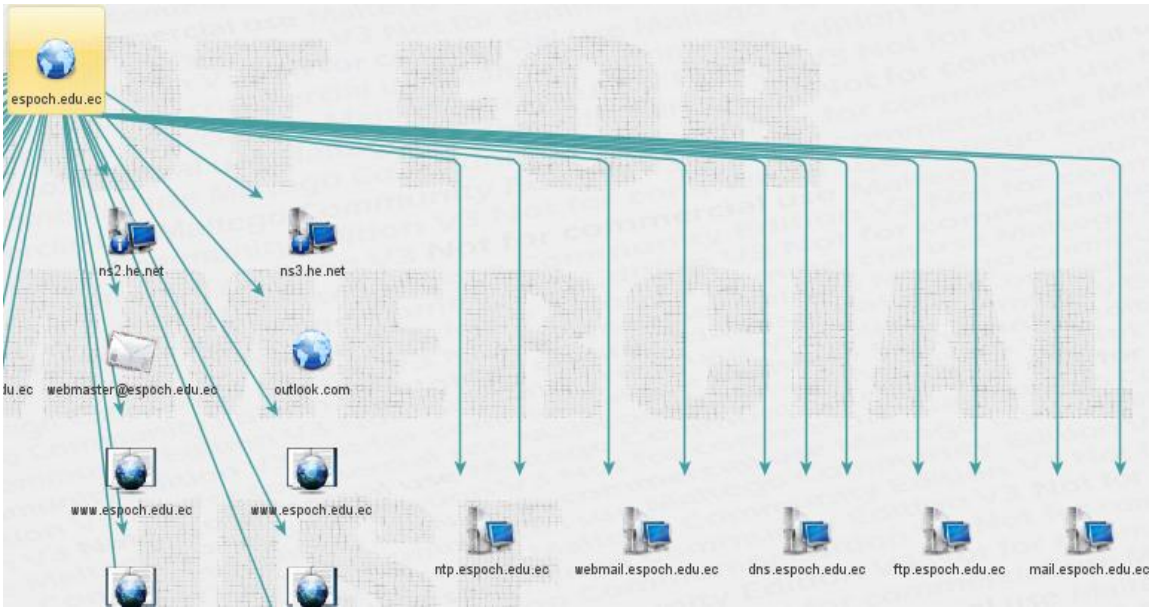



**FIGURA III.XXII Resultado de Maltego con Mining View.**

Maltego utiliza forma de vistas o Views para mostrar la información entre ellas destacamos las siguientes:

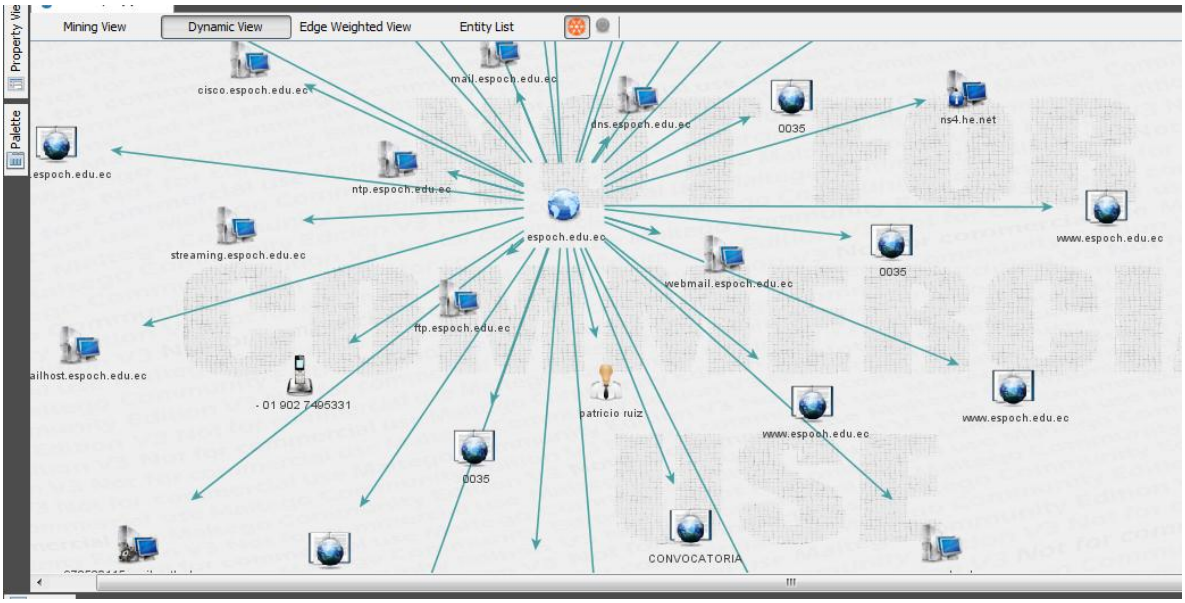



**FIGURA III.XXIIIResultado de Maltego con Dynamic View.**

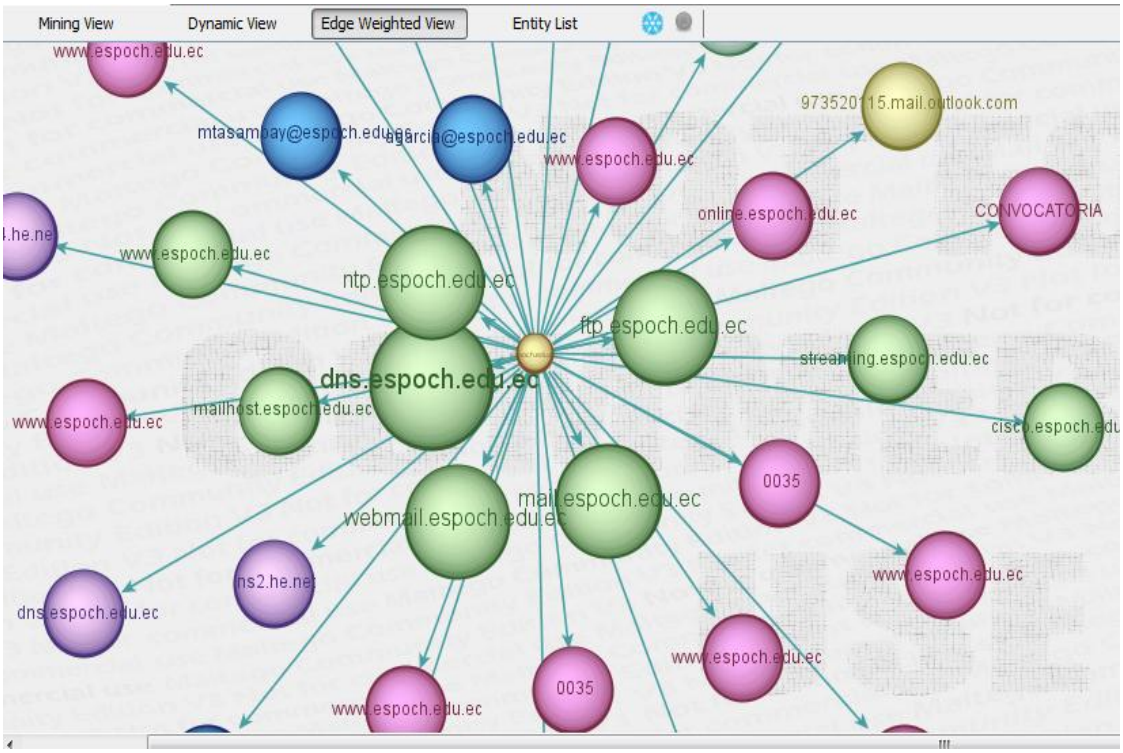



**FIGURA III.XXIV Resultado de Maltego con Edge Weighted View.**

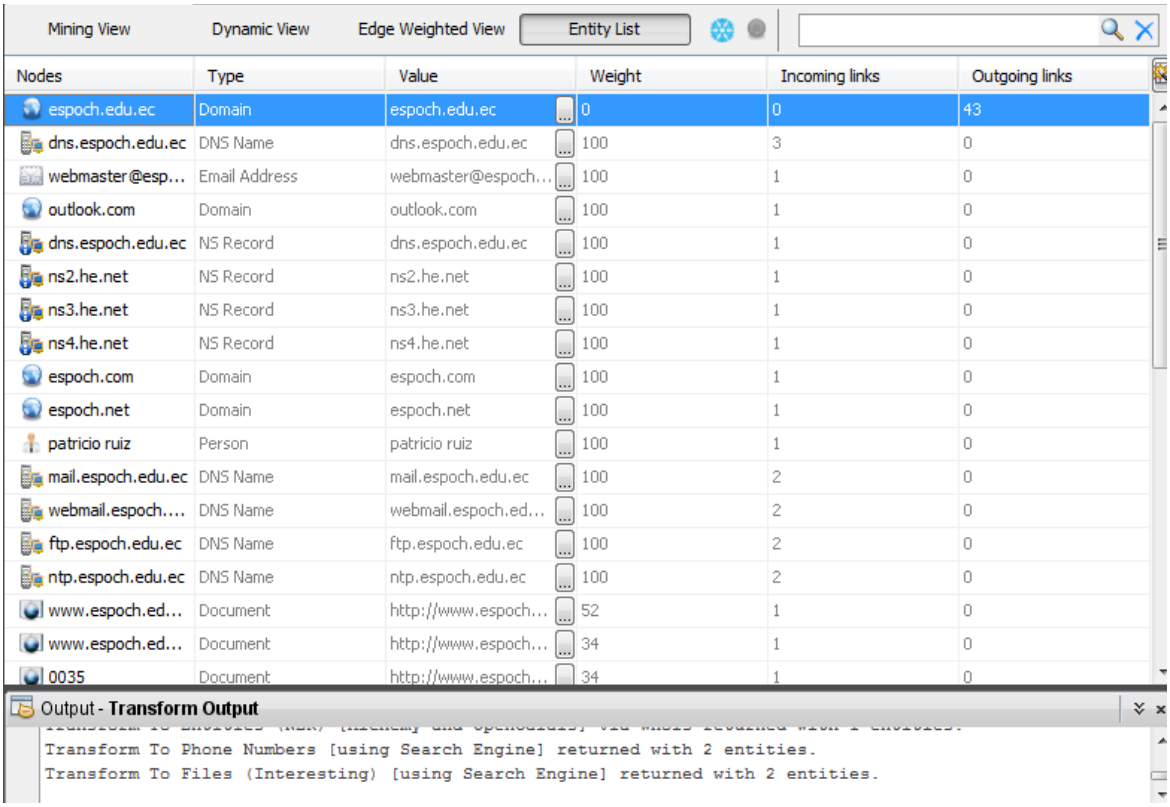



**FIGURA III.XXV Resultado de Maltego con Entry list.**

De esta manera el atacante tiene un panorama más claro del objetivo. Mediante estas herramientas se ha obtenido información que circula por internet y que compromete de cierta manera la integridad de la institución y a los empleados que laboran en dicha institución.

## 3.2 ESCANEO

Después de recolectar información acerca de la red de destino a partir de fuentes de terceros, tales como los motores de búsqueda, se tendrá que descubrir equipos del objetivo. El propósito de este proceso de descubrimiento es la siguiente:

- Para conocer el sistema operativo que es utilizado la máquina objetivo.
- Para saber qué máquina de la red del objetivo está disponible para investigar.

*Escanear* es el proceso de localización de los sistemas que están funcionando y respondiendo en la red. Los Hackers éticos utilizan la exploración para identificar las direcciones IP de los objetivos. El análisis también se utilizan para determinar si un sistema está en la red y disponible. Herramientas de detección se utilizan para recopilar información sobre un sistema, como direcciones IP, el sistema operativo y los servicios que se ejecutan en el equipo de destino.

El siguiente esquema mostrado en la figura, ilustra la manera en la que un profesional de seguridad scanning o escaneo.

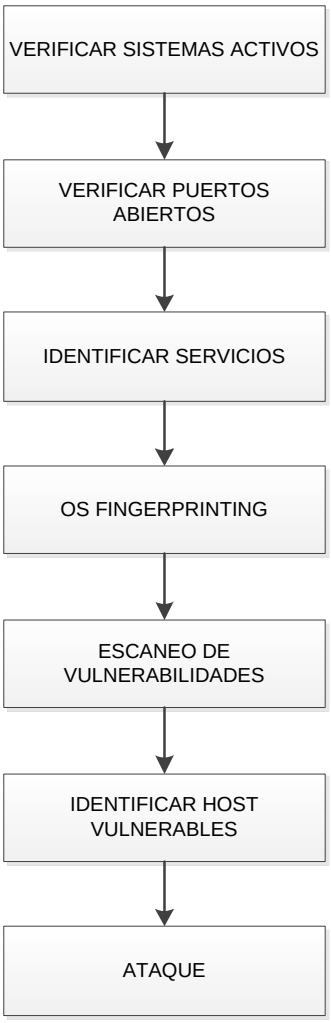



**FIGURA III.XXVI Método de scanning de un Hacker Ético.**

Ping es la herramienta más famosa para comprobar si un host en particular está disponible. La herramienta de ping consiste en enviar una solicitud ICMP (Internet Control Message Protocol) de eco al host de destino. Si el host de destino está disponible y si no el bloqueo de una solicitud de ping responderá con el paquete ICMP ECHO REPLY.

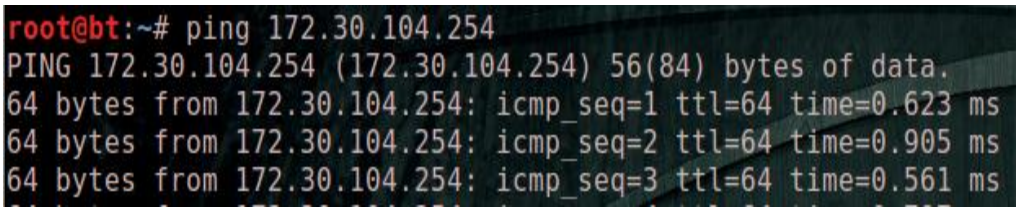



**FIGURA III.XXVII Resultado de Ping al Proxy de la Escuela de Sistemas.**

Exploración ICMP, o un barrido ping, es el proceso de envío de una solicitud ICMP o ping a todos los hosts de la red para determinar cuáles son y responder a los pings. ICMP comenzó como un protocolo utilizado para enviar mensajes de prueba y error entre los hosts de Internet.

Se ha desarrollado como un protocolo utilizado por cada sistema operativo, router, switch o Protocolo de Internet (IP) basado en el dispositivo. La capacidad de usar la solicitud de eco ICMP Echo y la respuesta como una prueba de conectividad entre los hosts está integrado en todos los dispositivos habilitados para IP mediante el comando ping. Es una prueba rápida y sucia para ver si dos equipos tienen conectividad y se utiliza ampliamente para la solución de problemas.

Casi cualquier sistema de prevención de IDS o de intrusiones (IPS) sistema para detecta y alerta al administrador de seguridad que un barrido ping ocurre en la red. La mayoría de cortafuegos y servidores proxy bloquean las respuestas de ping por lo que un hacker no puede determinar con precisión si los sistemas están

disponibles mediante solo un barrido de ping. El escaneo de puertos más intenso se debe utilizar si los sistemas no responden a un barrido ping. El hecho de que un barrido de ping no devuelve todos los hosts activos en la red no significa que no están disponibles, se tiene que probar un método alternativo de identificación.

La herramienta arping se utiliza para hacer ping a un host de destino en la red de área local o LAN mediante una solicitud ARP (Address Resolution Protocol). Arping es útil para probar si una determinada dirección IP está en uso en la red.

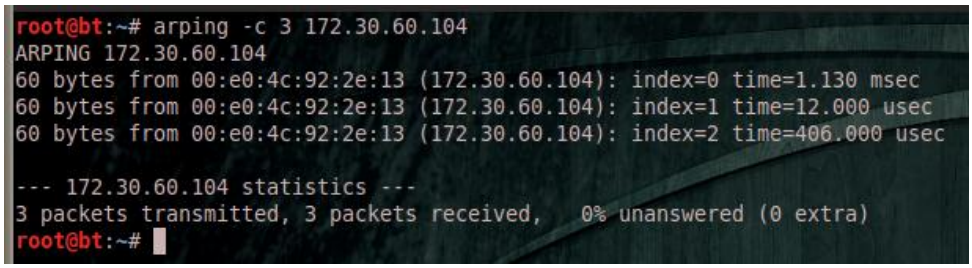



**FIGURA III.XXVIII Resultado de Arping al Proxy de la Escuela de Sistemas.**

En este momento a más de comprobar la disponibilidad del servidor proxy, al herramienta arping nos proporciona su dirección MAC.

La herramienta arping funciona en la capa 2 del modelo OSI (Open System Interconnection) y además sólo se puede utilizar en la red local. Y ARP no se puede enrutar a través de routers o gateways.

Netifera es una herramienta de seguridad de la red y también una plataforma modular para el desarrollo de herramientas de seguridad de red.

Como una plataforma modular, ofrece la interfaz de programación de aplicaciones (API) para tareas tales como:

- Alto rendimiento en conexión de socket asíncrona y comunicación
- Vincular nivel de captura de paquetes e inyección de conector directo
- Protocolo de red de la construcción de cabecera y el análisis (Ethernet, IP, TCP, y así sucesivamente)
- Aplicación de capa de protocolo de las bibliotecas (HTTP, DNS, FTP, etc)
- Si bien como una herramienta de seguridad de red, que tiene las siguientes capacidades:
- El escaneado en red y la detección de servicio en TCP y UDP
- Identificación de sistema operativo
- Apoyando plenamente IPv4 e IPv6
- Brute-forcing DNS name
- Llevar a cabo la transferencia de zonas DNS

- Descubrir las aplicaciones web, recoger direcciones de correo electrónico y la adición de la estructura del sitio web al modelo de datos

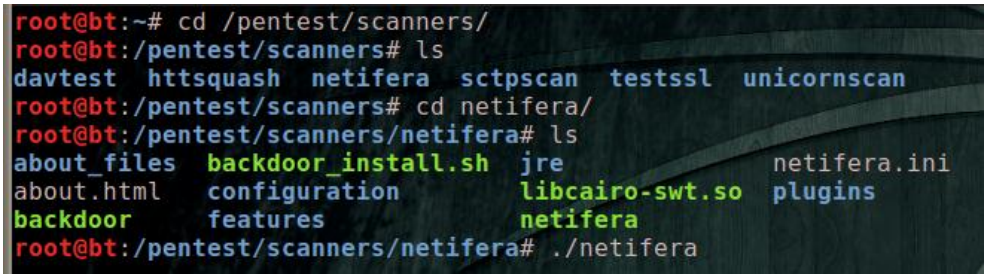



**FIGURA III.XXIX Ingreso a Netifera.**

Se ubica el bloque de red de 172.30.104.0/24 para ser analizado en barra de entrada.

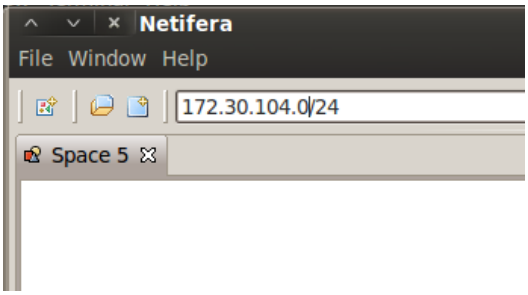



**FIGURA III.XXX Ingreso del bloque de red a analizar por netifera.**

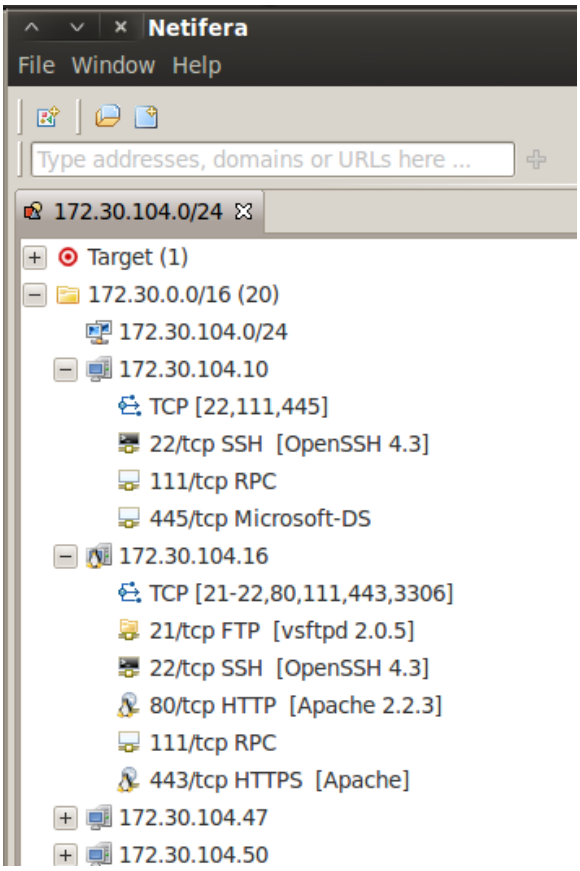



**FIGURA III.XXXI Resultado de netifera analizado el bloque de red de la Escuela de Sistemas.**

En la figura Netifera no solo muestra que equipos están trabajando con su respectiva dirección IP, también adiciona los servicios activos que el equipo está ejecutando y los puertos correspondientes a dichos servicios. Cabe recalcar que también indica el tipo de Sistema operativo de cada equipo.

Escaneo de puertos es el proceso de identificación abierta y disponible puertos TCP / IP en un sistema, herramientas de escaneo de puertos permiten a un hacker aprender sobre los servicios disponibles en un sistema dado. Cada servicio o

aplicación en una máquina se asocia con un número de puerto conocido. Los números de puerto se dividen en tres categorías:

- Puertos bien conocidos: 0-1023
- Puertos registrados: 1024-49151
- Los puertos dinámicos: 49152-65535

Además el atacante apunta a ciertos puertos que comúnmente son los mas utilizados.

- FTP, 21
- Telnet, 23
- HTTP, 80
- SMTP, 25
- POP3, 110
- HTTPS, 443
- SMB, 445

Nmap es una herramienta gratuita, de código abierto que lleva a cabo con rapidez y eficacia barridos ping, escaneo de puertos, servicios de identificación, detección de direcciones IP, y la detección del sistema operativo.

Nmap tiene la ventaja de escanear un gran número de máquinas en una sola sesión.

El estado del puerto según lo determinado por un análisis con Nmap puede ser abierto, filtrada o sin filtrar. Abierto significa que el equipo de destino acepta la petición de entrada en ese puerto. Filtrado significa un filtro de firewall o una red de detección es el puerto y la prevención de nmap de descubrir si está abierto. Filtrar significa que el puerto se determina que es cerrado, y que el cortafuegos o firewall está interfiriendo con las solicitudes de nmap.

| | |
|---|---|
| Conexión TCP o TCP connect | El atacante tiene una conexión TCP completa al sistema de destino. El análisis más fiable, sino también el tipo más detectable. Puertos abiertos responder con un paquete SYN / ACK, mientras que los puertos cerrados responder con un RST / ACK. |
| XMAS tree | El atacante busca los servicios de TCP mediante el envío de XMAS tree scan de paquetes, que son nombrados como |

| | |
|---|---|
| scan | tales porque todas las "luces" se encuentra, es decir, la FIN, URG y PSH son las banderas (el significado de las banderas será discutido más adelante en este capítulo). Los puertos cerrados responder con un RST. |
| SYN stealth scan | Esto se conoce también como *medio de exploración abierta.* El hacker envía un paquete SYN y recibe un SYN-ACK del servidor. Es cauteloso, porque una conexión TCP completa no se abre. Puertos abiertos responder con un paquete SYN / ACK, mientras que los puertos cerrados responder con un RST / ACK. |
| Null scan | Se trata de una exploración avanzada que puede ser capaz de pasar a través de firewalls sin ser detectados o modificado. Null scan tiene todas las banderas de establecer o no. Sólo funciona en sistemas Unix. Los puertos cerrados devolverá un RST. |
| Windows scan | Este tipo de exploración es similar a la exploración de ACK y también puede detectar los puertos abiertos. |
| ACK scan | Este tipo de análisis se utiliza para mapear reglas de cortafuegos. Sondeo ACK sólo funciona en Unix. El puerto es considerado filtrada por las reglas del firewall si un |

| | |
|---|---|
| | mensaje de destino inalcanzable ICMP se recibe como resultado de la exploración de ACK. |

**TABLA III.I Tipos de escaners de Nmap**

El comando nmap tiene numerosos interruptores para realizar diferentes tipos de exploraciones. Los interruptores de comando comunes se listan:

| | |
|---|---|
| -ST | TCP connect scan |
| -SS | SYN |
| -SF | FIN scan |
| -SX | XMAS tree scan |
| -SN | Null scan |
| -SP | Ping exploración |
| -SU | El sondeo UDP |

**TABLA III.II Interruptores de Nmap**

| nmap<br>comando<br>switch | Análisis realizado |
|---|---|
| -SO | El sondeo de protocolos |
| -SA | ACK scan |
| -SW | Windows scan |
| -RS | El sondeo RPC |
| -SL | Lista / DNS exploración |
| -Si | Inactivo exploración |
| -Po | No de ping |
| -PT | Mesa de ping TCP |
| -PS | Mesa de ping SYN |
| -PI | De ping ICMP |
| -PB | TCP y ICMP ping |
| -PB | Timestamp ICMP |

| | |
|---|---|
| -PM | Máscara de red ICMP |
| -ON | Producción normal |
| -OX | XML de salida |
| -OG | Salida Greppable |
| -OA | Todas las salidas |
| Paranoid-T | Serie de análisis; 300 segundos entre exploraciones |
| Sneaky-T | Serie de análisis; 15 segundos entre exploraciones |
| Cortés-T | Serie de análisis; 0,4 segundos entre exploraciones |
| Normal-T | Paralelo exploración |
| Agresivo-T | Paralelo exploración, tiempo de espera de 300 segundos, |

| | |
|---|---|
| | y 1,25 seg / sonda |
| T-Insane | Paralelo exploración, tiempo de espera de 75 segundos, y 0.3 seg / sonda |

**TABLA III.III Análisis realizado por los interruptores de Nmap**

Tipos de análisis de TCP se basan en el protocolo TCP de tres vías o TCP three-way handshake. Las conexiones TCP requieren un apretón de manos a tres sentidos antes de que pueda realizar la conexión y transferencia de datos entre el emisor y el receptor. Figura a continuación detalla los pasos de los TCP de tres vías.

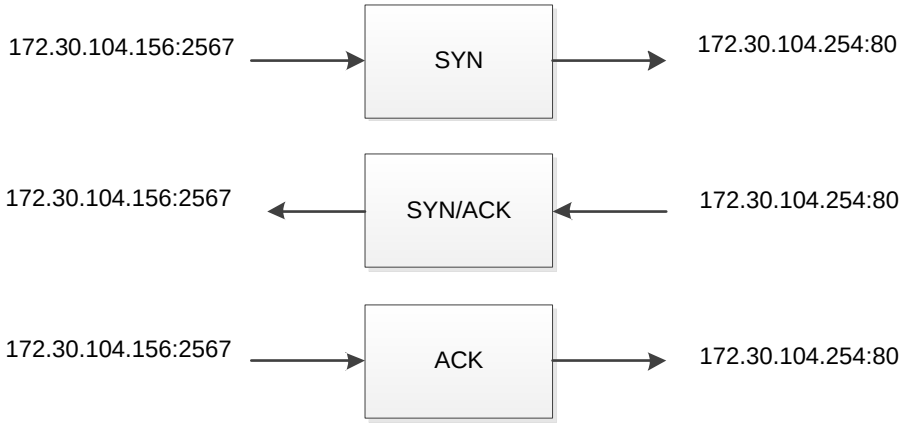



**FIGURA III.XXXII TCP three-way handshake.**

Para completar el enlace de tres vías y efectuar la conexión entre dos máquinas, el emisor debe enviar un paquete TCP con el bit de sincronización (SYN). Entonces, el sistema receptor responde con un paquete TCP con la sincronización (SYN) y RECONOCE bits (ACK) para indicar el ordenador está listo para recibir datos. El sistema de origen envía un paquete final con el conjunto de bit ACK para indicar que la conexión es completa y los datos están listos para ser enviados.

Debido a que TCP es un protocolo orientado a conexión, un proceso para establecer una conexión de tres fases, el reinicio de un error de conexión, y el acabado de una conexión es parte del protocolo. Estas notificaciones se llaman protocolo de las banderas o flags. TCP contiene ACK, RST, SYN, URG, PSH, y banderas de FIN. La siguiente lista identifica la función de los indicadores TCP:

- SYN Sincronizar. Inicia una conexión entre los hosts.
- ACK Reconocimiento. Conexión establecida entre los hosts.
- PSH Push. Sistema es el reenvío de datos en el búfer.
- URG urgente. Paquetes de datos deben ser procesados rápidamente.
- FIN Finalizar. Las transmisiones más.
- RST Reset. Restablece la conexión.

Un hacker puede intentar eludir la detección mediante el uso de banderas en lugar de completar una conexión TCP normal.

Zenmap es la interfaz gráfica de Nmap. Las ventajas de Zenmap en comparación con Nmap son:

- Es interactivo. Zenmap organizar los resultados del análisis de una forma sencilla. Incluso puede dibujar un mapa topológico de la red descubierta.
- Zenmap puede hacer una comparación entre dos escaneos.
- Zenmap realiza un seguimiento de los resultados del análisis.
- Para ejecutar la configuración de escaneo más de una vez, la prueba de intrusión puede utilizar el perfil de Zenmap.
- Zenmap siempre mostrará el comando para ejecutar lo que la prueba de intrusión puede verificar que el comando.

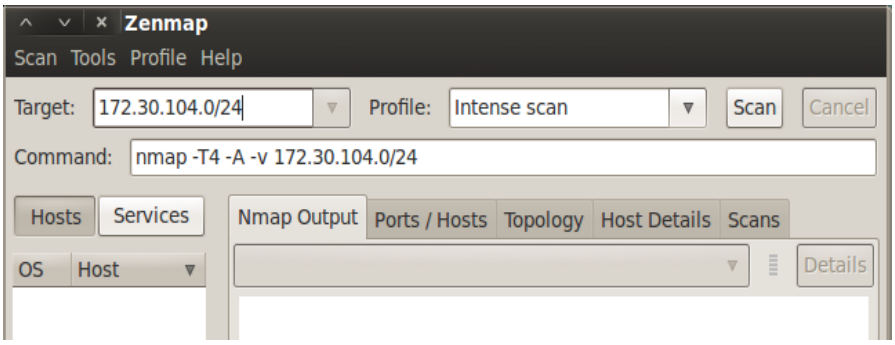



**FIGURA III.XXXIII Bloque de direcciones a calcular con Zenmap.**

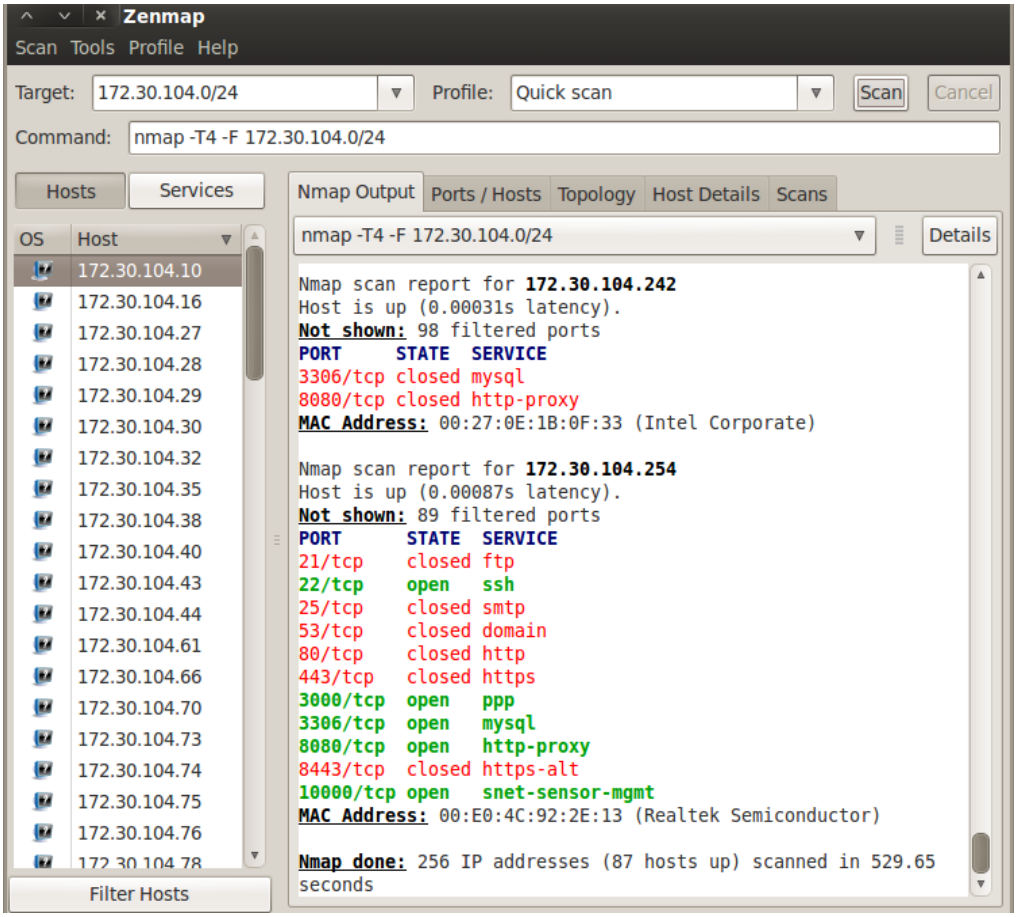



**FIGURA III.XXXIV Resultado mostrado en la interfaz de Zenmap.**

Además de un análisis global de las direcciones IP activas, zenmap permite elegir una dirección en especial y poder examinar más detalladamente el análisis previo, en el siguiente grafico se muestra la dirección 172.30.104.176 y muestra la cantidad de puertos abiertos y zenmap lo posiciona con un color rosa indicando mayor probabilidad de ser vulnerable.

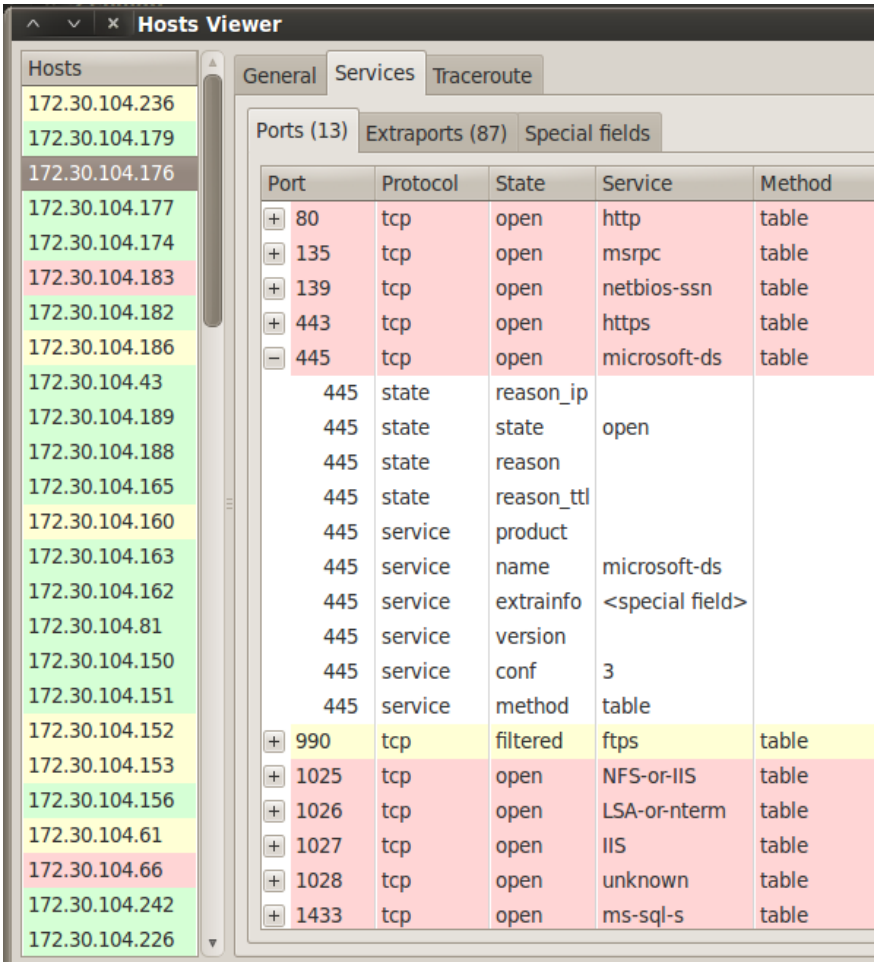



**FIGURA III.XXXVResultado mostrado en la interfaz de Zenmap.**

## 3.3 ENUMERACIÓN

La *enumeración* tiene lugar después de la digitalización y el proceso de recopilación y compilación de nombres de usuario, nombres de equipos, recursos de la red, acciones y servicios. También se refiere a la consulta activa o la conexión a un sistema de destino para obtener esta información.

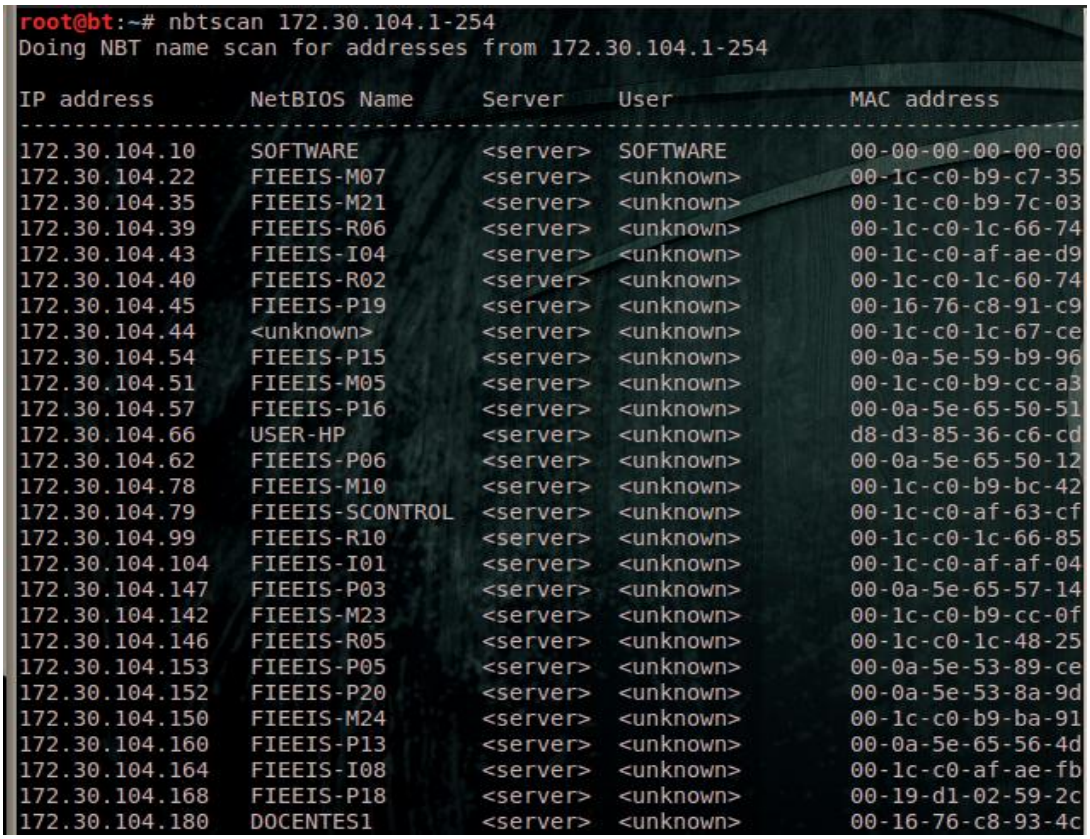
Un analista de seguridad debe ser metódico en su acercamiento al objetivo. Los siguientes pasos son un ejemplo de los que un profesional de seguridad podría realizar en la preparación para hackear un sistema de destino:

- Extracción de nombres de usuario con la enumeración.
- Reunir información sobre el uso de acogida sesiones nulas.
- Realizar la enumeración de Windows.
- Adquirir las cuentas de usuario.
- Realizar el escaneo de puertos SNMP.

El objeto de la enumeración es la identificación de una cuenta de usuario o la cuenta del sistema para su uso potencial en la penetración del sistema de destino. No es necesario encontrar una cuenta de administrador del sistema, porque la

mayoría de los privilegios de la cuenta se puede escalar para permitir el acceso de la cuenta más de lo concedido anteriormente.

La herramienta nbtscan puede ser utilizado para escanear direcciones IP para obtener información del nombre NetBIOS. Elaborará un informe que contiene la dirección IP, nombre de equipos NetBIOS, servicios disponibles, registrados en el nombre de usuario y la dirección MAC de las máquinas correspondientes. Esta información será útil en los pasos de PenTest. La diferencia entre nbtstat de Windows y nbtscan es que nbtscan puede operar en un rango de direcciones IP. Se debe tener en cuenta que el uso de esta herramienta generara una gran cantidad de tráfico y puede ser registrado por los equipos de destino.



```
root@bt:~# nbtscan 172.30.104.1-254
Doing NBT name scan for addresses from 172.30.104.1-254

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
172.30.104.10    SOFTWARE         <server>  SOFTWARE         00-00-00-00-00-00
172.30.104.22    FIEEIS-M07       <server>  <unknown>        00-1c-c0-b9-c7-35
172.30.104.35    FIEEIS-M21       <server>  <unknown>        00-1c-c0-b9-7c-03
172.30.104.39    FIEEIS-R06       <server>  <unknown>        00-1c-c0-1c-66-74
172.30.104.43    FIEEIS-I04       <server>  <unknown>        00-1c-c0-af-ae-d9
172.30.104.40    FIEEIS-R02       <server>  <unknown>        00-1c-c0-1c-60-74
172.30.104.45    FIEEIS-P19       <server>  <unknown>        00-16-76-c8-91-c9
172.30.104.44    <unknown>        <server>  <unknown>        00-1c-c0-1c-67-ce
172.30.104.54    FIEEIS-P15       <server>  <unknown>        00-0a-5e-59-b9-96
172.30.104.51    FIEEIS-M05       <server>  <unknown>        00-1c-c0-b9-cc-a3
172.30.104.57    FIEEIS-P16       <server>  <unknown>        00-0a-5e-65-50-51
172.30.104.66    USER-HP          <server>  <unknown>        d8-d3-85-36-c6-cd
172.30.104.62    FIEEIS-P06       <server>  <unknown>        00-0a-5e-65-50-12
172.30.104.78    FIEEIS-M10       <server>  <unknown>        00-1c-c0-b9-bc-42
172.30.104.79    FIEEIS-SCONTROL  <server>  <unknown>        00-1c-c0-af-63-cf
172.30.104.99    FIEEIS-R10       <server>  <unknown>        00-1c-c0-1c-66-85
172.30.104.104   FIEEIS-I01       <server>  <unknown>        00-1c-c0-af-af-04
172.30.104.147   FIEEIS-P03       <server>  <unknown>        00-0a-5e-65-57-14
172.30.104.142   FIEEIS-M23       <server>  <unknown>        00-1c-c0-b9-cc-0f
172.30.104.146   FIEEIS-R05       <server>  <unknown>        00-1c-c0-1c-48-25
172.30.104.153   FIEEIS-P05       <server>  <unknown>        00-0a-5e-53-89-ce
172.30.104.152   FIEEIS-P20       <server>  <unknown>        00-0a-5e-53-8a-9d
172.30.104.150   FIEEIS-M24       <server>  <unknown>        00-1c-c0-b9-ba-91
172.30.104.160   FIEEIS-P13       <server>  <unknown>        00-0a-5e-65-56-4d
172.30.104.164   FIEEIS-I08       <server>  <unknown>        00-1c-c0-af-ae-fb
172.30.104.168   FIEEIS-P18       <server>  <unknown>        00-19-d1-02-59-2c
172.30.104.180   DOCENTES1        <server>  <unknown>        00-16-76-c8-93-4c
```

**FIGURA III.XXXVI Nbtscan.**

A partir del resultado de la figura anterior, se podrá encontrar el servicio NetBIOS además de la IP a la que está relacionado y su respectiva dirección MAC, resultado que también se puede analizar con otras herramientas como nmap, zenmap o netifera, la ventaja de utilizar esta herramienta es que proporciona información valiosa sobre grupos de trabajos a los que pertenece la máquina, haciendo un análisis más exhaustivo.

NetBIOS, "Network Basic Input/Output System", es un protocolo de resolución de nombres que puede ser encapsulado sobre TCP/IP. NetBIOS funciona a nivel de

la capa de aplicación, dando una apariencia uniforme a todas las redes Windows independientemente de los protocolos que se hayan utilizado para las capas de red y transporte. Permite compartir archivos e impresoras así como ver los recursos disponibles en Entorno de red. NetBIOS utiliza los puertos 137, 138 y 139. Es un protocolo exclusivo de máquinas Windows.

```
root@bt:~# nbtscan -hv 172.30.104.1-254
```

**FIGURA III.XXXVII Comando nbtscan y un rango de direcciones.**

```
NetBIOS Name Table for Host 172.30.104.196:

Incomplete packet, 155 bytes long.
Name             Service          Type
----------------------------------------
TOLEDO-PC      <00> Workstation Service
WORKGROUP      <00> Domain Name
TOLEDO-PC      <20> File Server Service

Adapter address: 00-26-9e-8c-78-c2
----------------------------------------

NetBIOS Name Table for Host 172.30.104.201:

Incomplete packet, 173 bytes long.
Name             Service          Type
----------------------------------------
FIEEIS-M20     <00> Workstation Service
WORKGROUP      <00> Domain Name
FIEEIS-M20     <20> File Server Service
WORKGROUP      <1e> Browser Service Elections

Adapter address: 00-1c-c0-b9-9c-0e
----------------------------------------
```

**FIGURA III.XXXVIII Resultado parcial de Nbtscan.**

En equipos que manejan Windows en especial distribuciones en XP y que tengan activado el servicio de NetBios, existen varias maneras de explotarlas con exploits que utilizan vulnerabilidades de ese servicio.

Enumeración SNMP es el proceso de utilizar SNMP para enumerar cuentas de usuario en un sistema destino. SNMP utiliza dos tipos principales de componentes de software para la comunicación: el agente SNMP, que se encuentra en el dispositivo de red, y la estación de administración SNMP, que comunica con el agente.

Casi todos los dispositivos de infraestructura de red, como routers y switches que incluyan sistemas de Windows, contienen un agente SNMP para gestionar el sistema o dispositivo. La estación de administración SNMP envía las solicitudes a los agentes y los agentes de enviar respuestas. Las solicitudes y respuestas se refieren a las variables de configuración accesible por software del agente. Gestión de las estaciones también pueden enviar solicitudes para establecer los valores de ciertas variables. Las trampas que la estación de administración que algo importante ha sucedido en el software del agente, como un reinicio o un error de interfaz. Management Information Base (MIB) es la base de datos de variables de configuración que se encuentra en el dispositivo de red.

SNMP tiene dos contraseñas que puede utilizar para acceder y configurar el agente SNMP de la estación de gestión. El primero se llama una *read community string* o cadena de comunidad de lectura. Esta contraseña le permite ver la configuración del dispositivo o sistema. El segundo se llama *read/write community string* la comunidad de lectura / escritura, es para cambiar o modificar la configuración en el dispositivo. En general, el valor predeterminado leer cadena de comunidad es pública y el valor por defecto de lectura / escritura cadena de comunidad es privada. Un agujero de seguridad común se produce cuando las cadenas de comunidad están a la izquierda en la configuración por defecto: un hacker puede utilizar contraseñas por defecto para ver o cambiar la configuración del dispositivo.

Onesixtyone puede ser utilizado como un escáner de SNMP o Simple Network Monitoring Protocol, para averiguar si existe la cadena de SNMP en un dispositivo. La diferencia con otros escáneres de SNMP es que se envía todas las solicitudes SNMP tan rápido como pueda (10 milésimas de segundo de diferencia). Luego se espera la respuesta y los registra. Si el dispositivo está disponible, entonces se envían respuestas que contiene la cadena SNMP.

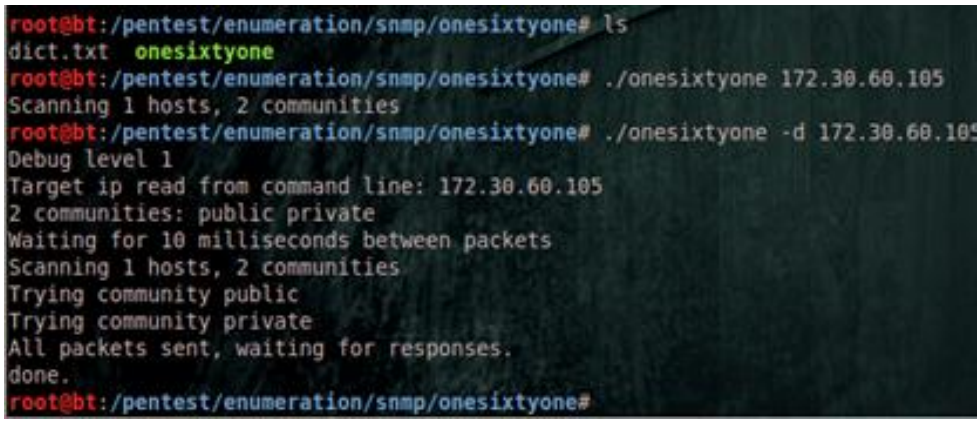



**FIGURA III.XXXIXOnesixtyone.**

IKE

Ike-Scan es una herramienta de seguridad que se pueden utilizar para descubrir, huella digital, y prueba de sistemas de IPSec VPN. Funciona mediante el envío de IKE de fase 1 los paquetes a los servidores VPN y la visualización de las respuestas que recibió. Internet Key Exchange (IKE) es el mecanismo de intercambio de claves y autenticación que utiliza IPsec.

Aquí hay varias características de Ike-scan:

- Es capaz de enviar paquetes IKE a cualquier número de servidores de destino
- Capaz de construir el paquete IKE saliente de una manera flexible
- Es capaz de decodificar y mostrar todos los paquetes de respuesta
- Capaz de romper agresivo modo de claves pre-compartidas con la ayuda de la

- herramienta pskcrack

En resumen, la herramienta de Ike-scan es capaz de dos cosas:

- Discovery o Descubrimiento: Descubrir hosts que ejecutan IKE mostrando máquinas que responden a la solicitud de IKE.
- Fingerpringting: Identificar la implementación de IKE que utiliza el servidor VPN IPSec.

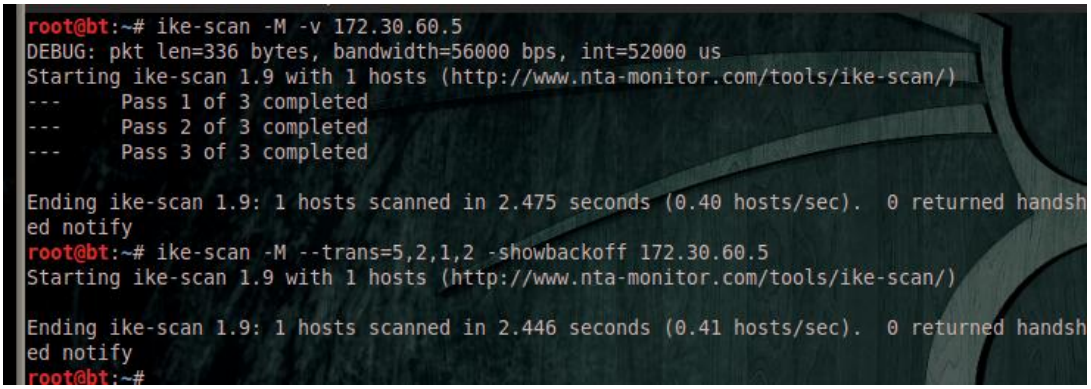



**FIGURA III.XL IKE SCAN**

Como se muestra en la figura no existe conexión vpn

Por lo general, esta información contiene el proveedor de VPN y el modelo del servidor VPN. Esto es útil para su uso posterior en el proceso de análisis de vulnerabilidad.

## 3.4 ANALISIS DE VULNERABILIDADES

Análisis de Vulnerabilidades es el proceso de identificación proactiva de las vulnerabilidades de los sistemas informáticos en una red. Por lo general, un escáner de vulnerabilidades primero identifica el sistema operativo y el número de versión, incluyendo paquetes de servicio que puedan estar instalados. A continuación, el escáner identifica las debilidades o vulnerabilidades en el sistema operativo. Durante la fase de ataque más tarde, el pirata informático puede explotar esas debilidades con el fin de obtener acceso al sistema.

Mapeo de Vulnerabilidades es un proceso de identificación y análisis de las fallas críticas de seguridad en el entorno de destino. Esta terminología es conocida también como evaluación de vulnerabilidades. Es una de las áreas claves del programa de gestión de vulnerabilidades a través del cual los controles de seguridad de una infraestructura de TI se pueden analizar detenidamente. Una vez que las operaciones de recolección de información, el descubrimiento, y la enumeración se han terminado, es hora de investigar las vulnerabilidades que puedan existir en la infraestructura del objetivo y que podría conducir a

comprometer el sistema y la violación de la confidencialidad, integridad y disponibilidad de un negocio del sistema.

Hay tres clases principales de vulnerabilidad que puede ser la distinción de los tipos de fallas local y remota. Estas clases se dividen generalmente en la categoría de *diseño*, *implementación* y *funcionamiento.*

Vulnerabilidades de diseño son las que se descubren debido a las debilidades encontradas en las especificaciones del software, las vulnerabilidades de aplicación son los fallos de seguridad técnicas que se encuentran en el código de un sistema, y las vulnerabilidades operacionales son los que pueden surgir debido a una configuración inadecuada y el despliegue de un sistema en un determinado el medio ambiente.

VULNERABILIDAD LOCAL

Un sistema en el que el atacante requiere acceso local a fin de activar la vulnerabilidad mediante la ejecución de un fragmento de código que se conoce como "vulnerabilidad local". Al tomar ventaja de este tipo de vulnerabilidad, un atacante puede aumentar los privilegios de acceso para tener acceso sin restricciones al sistema informático.

VULNERABILIDAD REMOTA

Un sistema en el que el atacante no tiene acceso previo, sino la vulnerabilidad de la que todavía puede ser explotada mediante la activación de la pieza de código malicioso en la red se conoce como "vulnerabilidad remota". Este tipo de vulnerabilidad permite a un atacante obtener acceso remoto al ordenador sin hacer frente a cualquier barrera física o local. Por ejemplo, el Atacante y la Victima están conectados a la Internet de forma individual. Ambos tienen direcciones IP diferentes y están dispersos geográficamente en dos regiones diferentes.

Nessus es una aplicación de escaneo de vulnerabilidades que opera en diversos sistemas operativos. Consiste en nessusd, el daemon Nessus, que realiza el escaneo en el sistema objetivo, y nessus, el cliente este último basado en consola o gráfico, que muestra el avance y reporte de los escaneos. Desde consola nessus puede ser programado para hacer escaneos de redes.

Nessus comienza escaneando puertos con su propio escaneador de puertos para buscar puertos abiertos y después probar varios exploits para un posible ataque y mostrarlo en la interfaz del cliente nessus. Las pruebas de vulnerabilidad disponibles en nessus son contenidas en una larga lista de plugins, además estos

son escritos en NASL Nessus Attack Scripting Language, o Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés, un lenguaje scripting optimizado para interacciones personalizadas en redes.

Nessus muestra los resultados del escaneo que pueden ser exportados en reportes en varios formatos, como texto plano, XML, HTML, y LaTeX. Los resultados también pueden ser guardados en una base de datos para referencia en futuros escaneos de vulnerabilidades.

Nessus por defecto no viene incorporado en la estantería de BackTrack, por lo cual se necesita instalarlo desde la fuente oficial. La razón por la que BackTrack no incluye la última versión Nessus es por el tema de las licencias. Desde Versión 3, Nessus no es software de código abierto. Una distribución de Linux no puede distribuirlo ya que sin licencia de la Seguridad sostenible de la empresa que desarrolla Nessus.

Se Puede descargar el último paquete Nessus genera para Linux Ubuntu 8.10 la distribución del sitio web de Nessus (http://www.nessus.org). Para instalar el paquete que ejecute el comando:

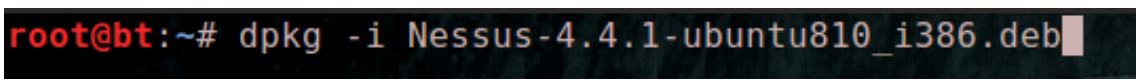



**FIGURA III.XLI Comando para descargar Nessus.**

A continuación se procede a dar ciertas instrucciones para poder ingresar a nessus, en primera instancia necesitamos registrar un usuario con su respectiva contraseña.

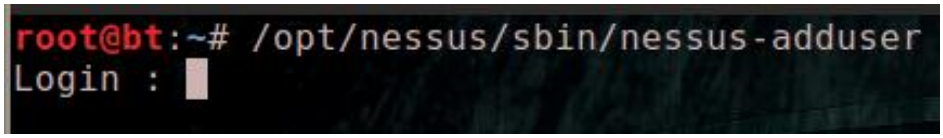



**FIGURA III.XLII Agregando un usuario a Nessus.**

Previamente instalado la activación mediante una cuenta de correo usando internet, en dicha cuenta consta un código de registro que se activara en BackTrack de la siguiente manera.


**FIGURA III.XLIII Ingresando código de registro de Nessus.**

Una vez activado el producto se procede a dar inicio al servicio Nessus.


**FIGURA III.XLIV Iniciando el servidor de Nessus.**

Se procede a continuación abrir el navegador y conectar al sitio https://localhost:8334

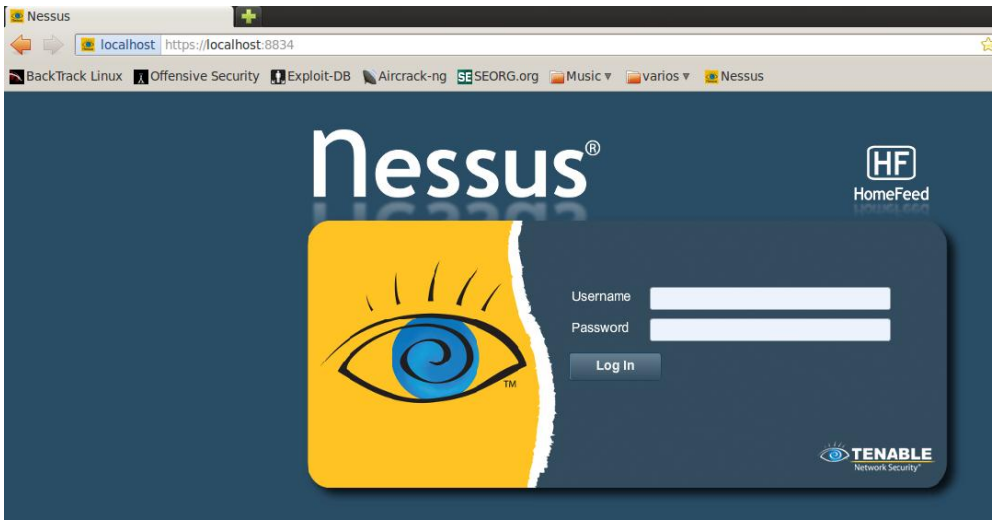



**FIGURA III.XLVIngreso a Nessus.**

Una vez que se haya conectado con la UI de un servidor Nessus, se puede crear una directiva personalizada haciendo clic en la opción “Policies” de la barra situada en la parte superior, y luego en el botón “+ Add” de la derecha. Aparecerá la pantalla “Add Policy”, como se muestra a continuación:

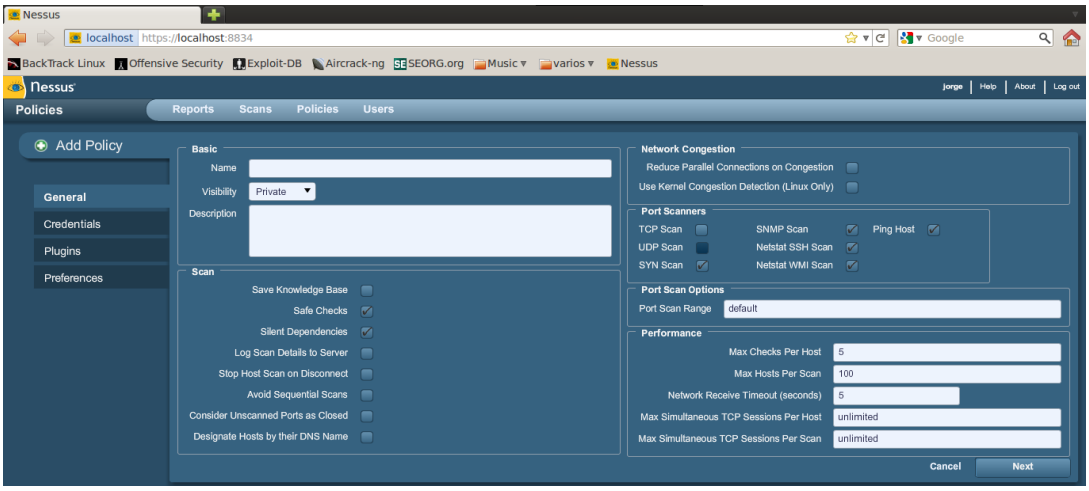



**FIGURA III.XLVI Agregando una Política de Escaneo.**

Se muestra que hay cuatro fichas de configuración: General, Credentials, Plugins y Preferences. En la mayoría de los entornos no es necesario modificar la configuración predeterminada, pero estas proporcionan un control más pormenorizado de la operación del analizador Nessus. El objetivo de modificar ciertos parámetros de las fichas antes mencionas se debe al ejecutor de esta aplicación, para el caso en estudio es preferible adecuar ciertos parámetros para personalizar el análisis de vulnerabilidades, para lo cual se ha hecho una política basada en requisitos para la LAN, ya que el trabajo de pentest se está realizando dentro de la LAN de la Escuela de Sistemas.

Después de crear una directiva se puede crear un nuevo análisis; para ello se realiza un clic en la opción “Scans” de la barra de menús situada en la parte

superior y luego se hace clic en el botón “+ Add” de la derecha. Aparecerá la pantalla “Add Scan”.

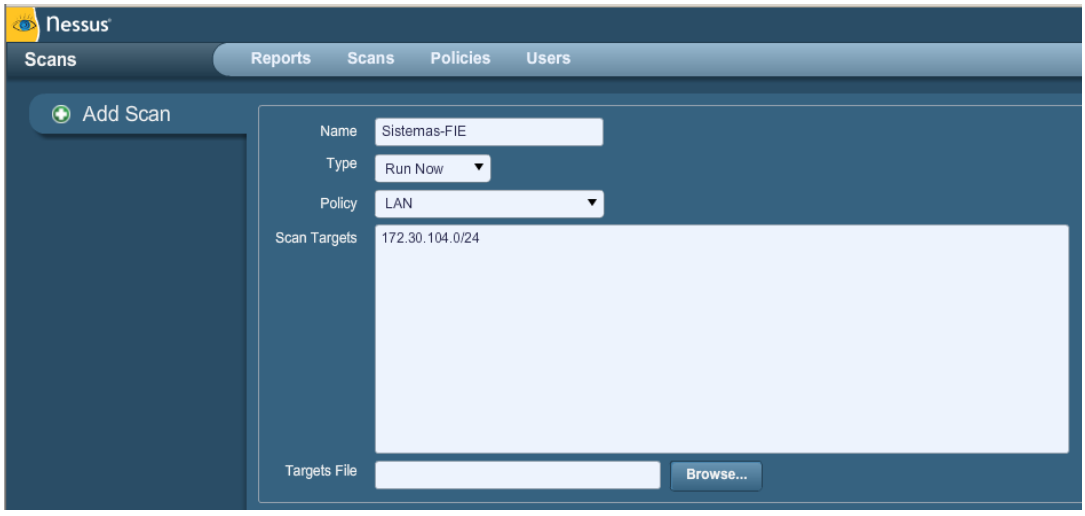



**FIGURA III.XLVII Configuración antes del Escaneo.**

En Name se establece el nombre que aparecerá en la UI de Nessus para identificar el análisis. Conjuntamente se selecciona “Run Now” en Type para ejecutar el análisis inmediatamente después de ejecutar el comando “Submit”. Posteriormente se selecciona en Policy una directiva creada anteriormente que para este caso es LAN, que usará el análisis para establecer los parámetros que controlan el comportamiento de análisis del servidor Nessus. Finalmente se establece el objetivo en Targets File, para este caso el bloque de red de la Escuela de Sistemas. Verificando que todos los parámetros estén correctamente ingresados se procede a ejecutar el análisis.

Se hace clic en la ficha **"**Reports**"**, en la barra de menús situada en la parte superior de la interfaz, aparecerá la lista de análisis en ejecución y terminados.

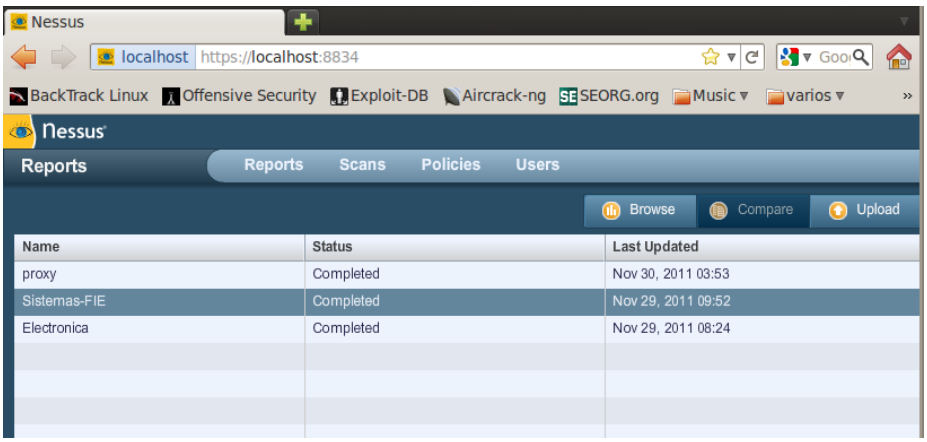



**FIGURA III.XLVIII Lista de Reportes.**

La pantalla "Reports" se desempeña como punto central para ver, comparar, cargar y descargar resultados de análisis.

Para explorar los resultados de un análisis, se selecciona un nombre de la lista "Reports" para el caso en cuestión seleccionamos Sistemas-FIE y se hace clic en "Browse". Esto permite ver resultados al navegar por hosts, puertos y vulnerabilidades específicas. La primera pantalla de resumen muestra cada host analizado, junto con un detalle de las vulnerabilidades y los puertos abiertos.

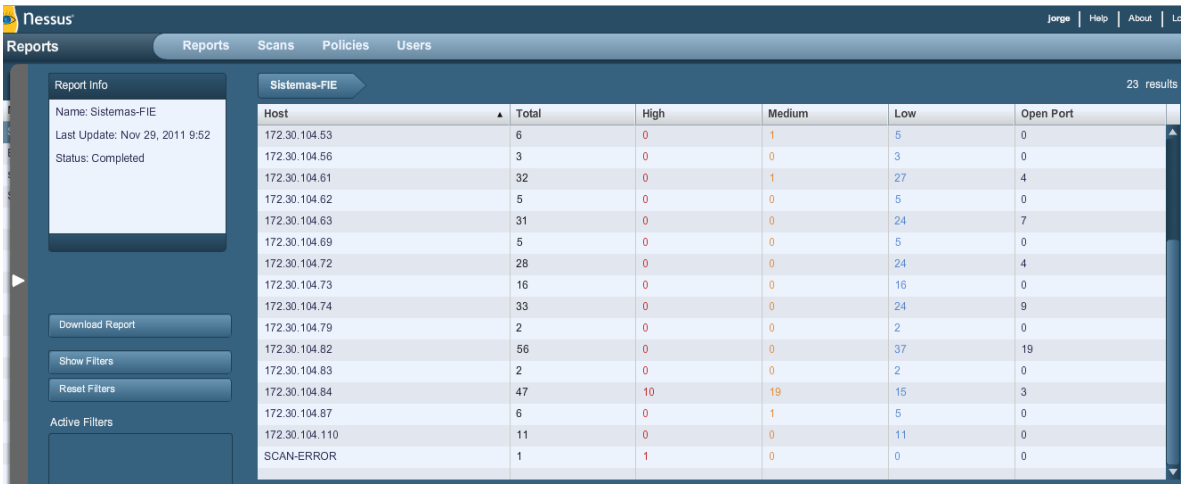



**FIGURA III.XLIX Reporte del Escaneo.**

Se escoge un host dentro del análisis realizado, el informe se dividirá por números de puerto y aparecerá información relacionada, tal como el protocolo y el nombre del servicio, así como también un resumen de las vulnerabilidades clasificadas por gravedad del riesgo. A medida que se navega por los resultados del análisis, la interfaz de usuario mantendrá la lista de hosts y una serie de flechas interactivas de ayuda para navegar rápidamente hasta un componente específico del informe.

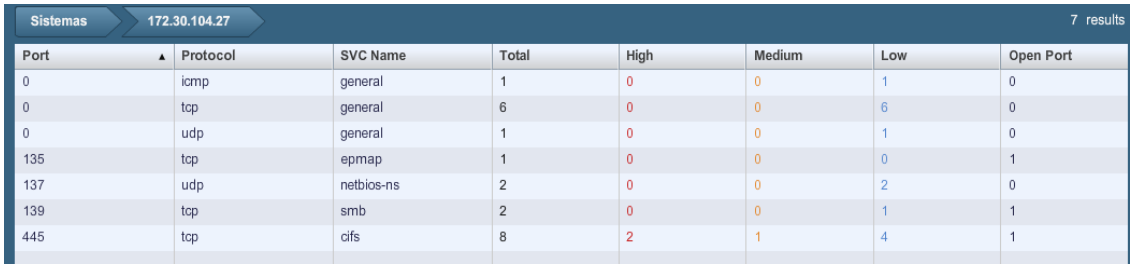
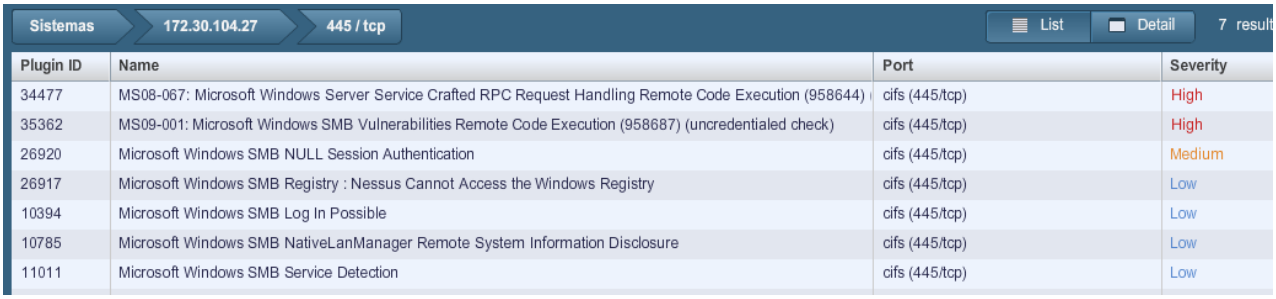



**FIGURA III.L Análisis de un Host.**

Si se selecciona un puerto, aparecerán todos los resultados de las vulnerabilidades que se relacionan con el puerto y el servicio.




| Plugin ID | Name | Port | Severity |
|---|---|---|---|
| 34477 | MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) | cifs (445/tcp) | High |
| 35362 | MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check) | cifs (445/tcp) | High |
| 26920 | Microsoft Windows SMB NULL Session Authentication | cifs (445/tcp) | Medium |
| 26917 | Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry | cifs (445/tcp) | Low |
| 10394 | Microsoft Windows SMB Log In Possible | cifs (445/tcp) | Low |
| 10785 | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure | cifs (445/tcp) | Low |
| 11011 | Microsoft Windows SMB Service Detection | cifs (445/tcp) | Low |

**FIGURA III.LI Análisis del puerto 445.**

En el resultado mostrado en la figura anterior se observa que el host 172.30.304.84 tiene 24 vulnerabilidades relacionadas con el puerto TCP 445.

El protocolo SMB (Server Message Block), también conocido como CIFS (Common Internet File System), permite habilitar la compartición de recursos a través de la red. Muchos usuarios permiten el acceso a sus discos con la intención de facilitar el trabajo en grupo con sus colaboradores. Sin saberlo, están abriendo sus sistemas a cualquier atacante al permitir el acceso, tanto de lectura como de escritura, a otros usuarios de la red. Habilitar la propiedad de compartir archivos en máquinas Windows las hace vulnerables tanto al robo de información como a ciertos tipos de virus que se propagan con rapidez.

Los mecanismos SMB que permiten el compartir archivos en Windows pueden ser también utilizados por posibles atacantes para obtener información sensible acerca de dichos sistemas. A través de conexiones de tipo "sesión nula" ("null session") con el servicio de sesión de NetBIOS es posible obtener información sobre usuarios y grupos, nombres de usuario, fecha de la última sesión, política de contraseñas, información de acceso remoto RAS, sobre el sistema, y ciertas claves del registro. Toda esta información es útil para los intrusos porque les ayuda a preparar un ataque contra el sistema consistente en la predicción de posibles contraseñas o simplemente la averiguación de las mismas por la fuerza bruta.

Si se selecciona una vulnerabilidad de la lista aparecerán detalles completos de los resultados, incluidos una sinopsis, una descripción técnica, la solución, el factor de riesgo, el puntaje CVSS, salidas relevantes que prueben los resultados, referencias externas, la fecha de publicación de la vulnerabilidad, la fecha de publicación o modificación de los plugins y la disponibilidad de las vulnerabilidades de seguridad.

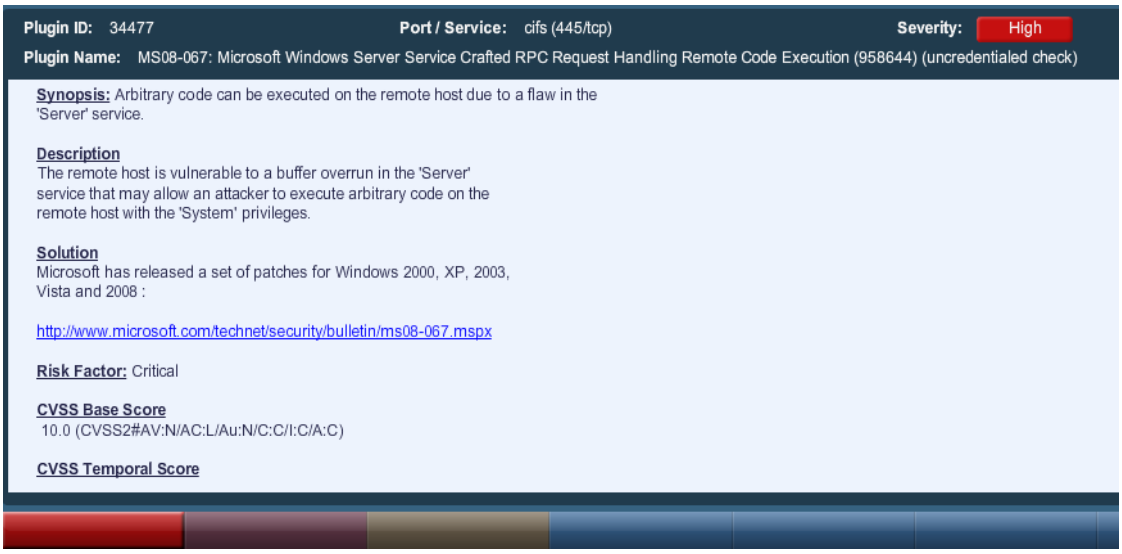



**FIGURA III.LII Análisis del puerto 445.**


**FIGURA III.LIII Análisis del puerto 443.**

En la disponibilidad de las vulnerabilidades de seguridad se mostrarán las vulnerabilidades de seguridad conocidas y públicas, incluidas las encontradas en marcos de trabajo de vulnerabilidades públicos o comerciales, tales como CANVAS, CORE o Metasploit.

## 3.5 EXPLOTACIÓN

Después de un cuidadoso examen de las vulnerabilidades descubiertas, el siguiente paso es penetrar en el sistema de destino basada en los tipos de exploits disponibles. Con el análisis de vulnerabilidades identificamos el objetivo y se procede a investigar ahora como penetrar el sistema, puede ser alguna aplicación que presente algún tipo de vulnerabilidad, algún host donde no esté bien configurado su firewall o algún dispositivo que no esté bien configurado.

A veces puede requerir investigación adicional o modificaciones a la explotación existente con el fin de que funcione correctamente. Por lo tanto, esta fase se centra principalmente en el proceso de adquisición de objetivos.

Se intenta describir brevemente los pasos para explotar un objetivo utilizando el módulo de Metasploit.

Metasploit es una plataforma de software libre que contiene varias herramientas necesarias para realizar pruebas de penetración, con las que se puede explotar vulnerabilidades dentro de la red.

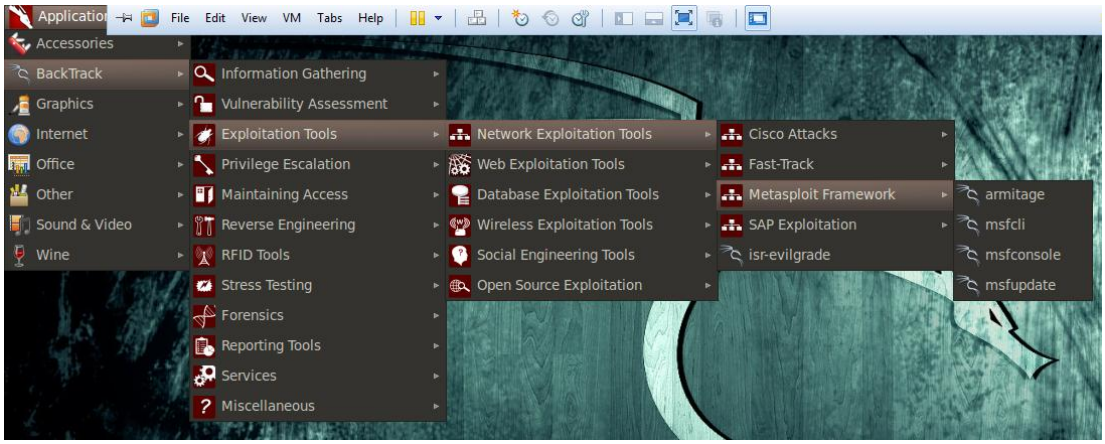



**FIGURA III.LIV Localización de Metasploit.**

También se puede ingresar a Metasploit utilizando su ruta desde la consola


**FIGURA III.LV Ruta de Metasploit.**

Metasploit ofrece más de una interfaz a su funcionalidad, incluyendo la consola, la línea de comandos e interfaces gráficas.

Msfconsole ofrece una práctica interfaz todo en uno para casi todos los parámetros y opciones disponibles, es como una ventanilla única para todos los requerimientos de la explotación. En el presente proyecto de tesis se utiliza msfconsole para el lanzamiento de un exploit además esta herramienta dispone

para realizar , la carga de módulos auxiliares, carga de payloads para correr explotación de las masas dentro de toda la red..

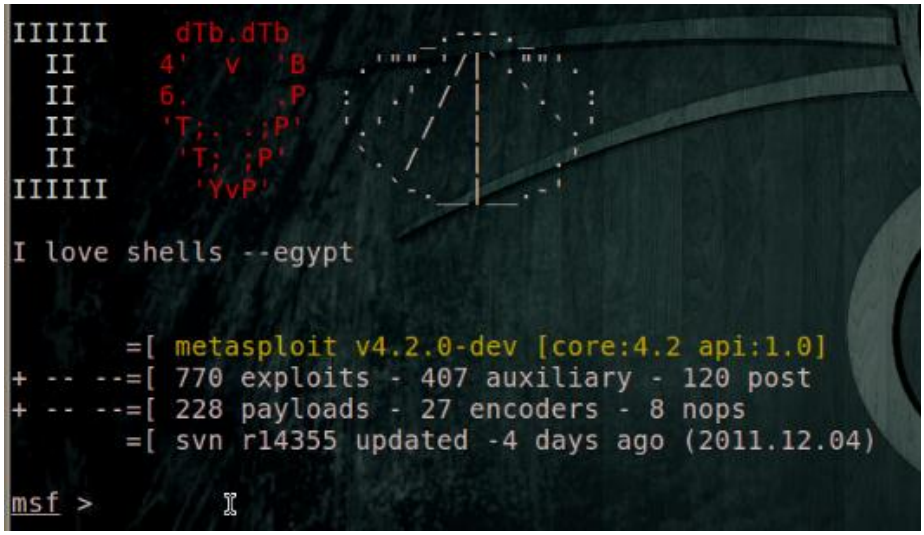



**FIGURA III.LVI Mfconsole de Metasploit.**

A continuación se muestra la explotación de un objetivo que se obtuvo sus respectivas vulnerabilidades anteriormente en la Figura… de análisis del puerto 445.

En primer lugar se procede a buscar el exploit que indica nessus en su análisis, utilizando de esta manera la consola de metasploit. Para poder visualizar una lista de todos los exploits disponibles, se escribe show exploit.

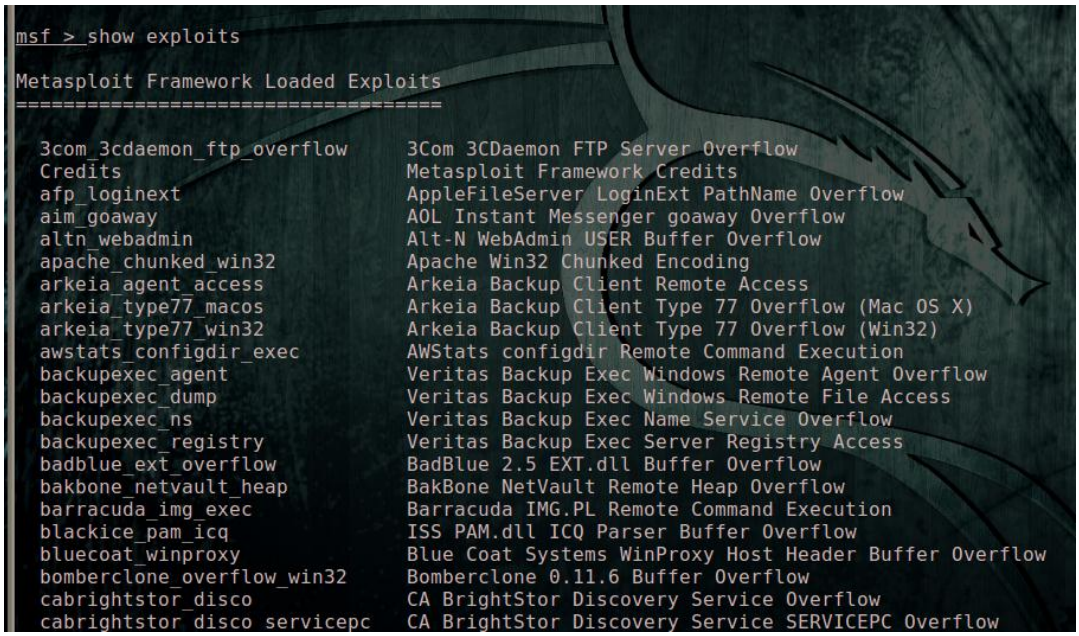



**FIGURA III.LVII Exploits disponibles de Metasploit.**

Nuevos exploits Siempre se están desarrollando, y la lista seguirá creciendo. El comando que se visualiza en al figura LVII mostrará todos los explotan actualmente disponibles dentro del framework.

Para obtener más información acerca de un determinado exploit, se escribe "info nombre_del_modulo". La interfaz de consola fue diseñada para ser rápida y flexible. Si se introduce un comando que no es reconocido por la consola, se buscará la ruta del sistema de determinar si es un símbolo del sistema. Esto le permite utilizar su conjunto de herramientas estándar, sin tener que salir de la consola. La interfaz de consola es compatible con la implementación del autocompletador de comandos conocidos.

Para encontrar el exploit MS08-067 en concreto (un exploit relacionado con el famoso gusano Conficker que explota una debilidad en el control remoto que llama al procedimiento [RPC] de servicios), se deberá introducir el siguiente comando:

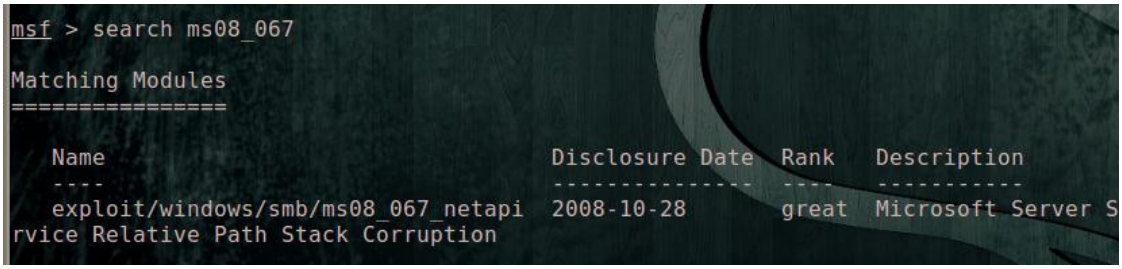



**FIGURA III.LVIII Busqueda del Exploit ms08_067.**

Una vez encontrado el exploit (windows/smb/ms08_067_netapi), se procede a cargar el modulo encontrado con el siguiente comando:

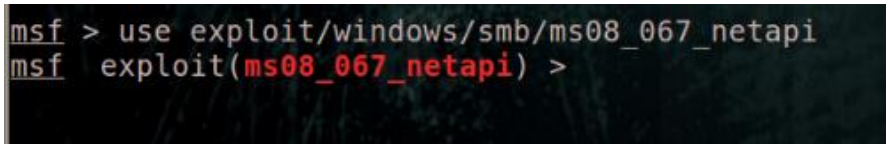



**FIGURA III.LIX Carga del Exploit ms08_067.**

Esto indica que hemos seleccionado el módulo ms08_067_netapi y que las órdenes emitidas en este indicador se realizarán bajo dicho exploit.

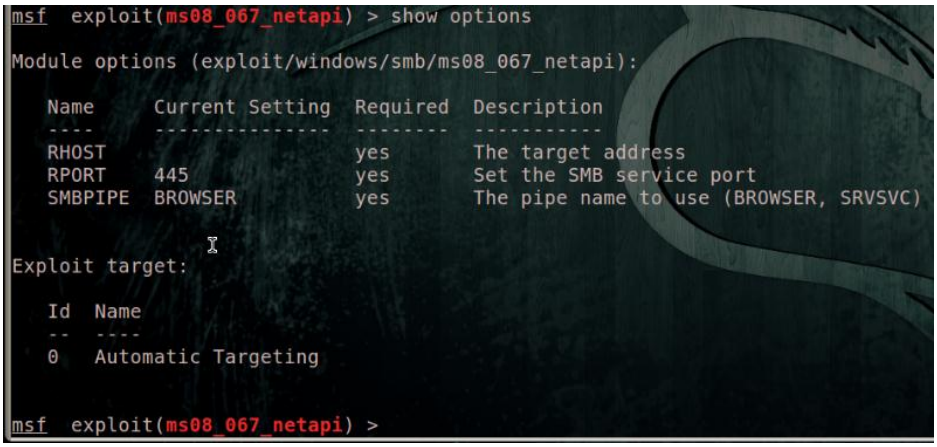



**FIGURA III.LX Muestra de Opciones del Exploit ms08_067.**

Este enfoque contextual de opciones de acceso mantiene la interfaz más sencilla y permite centrarse sólo en las opciones que importa en este momento.

Hasta el momento tenemos cargado en la consola el exploit que va a explotar la vulnerabilidad encontrada, pero aun no le indicamos que hacer luego de la explotación, en este punto se buscaría el payload más apropiado.

Payload o carga útil es el código que queremos que el sistema ejecute y que se va a seleccionar y entregar por el framework. Para el caso de estudio se procede a ejecutar un reverse meterpreter, lo que hará una conexión reversa desde la máquina del objetivo hasta el atacante y proporcionara un intérprete de comandos en la máquina del atacante.

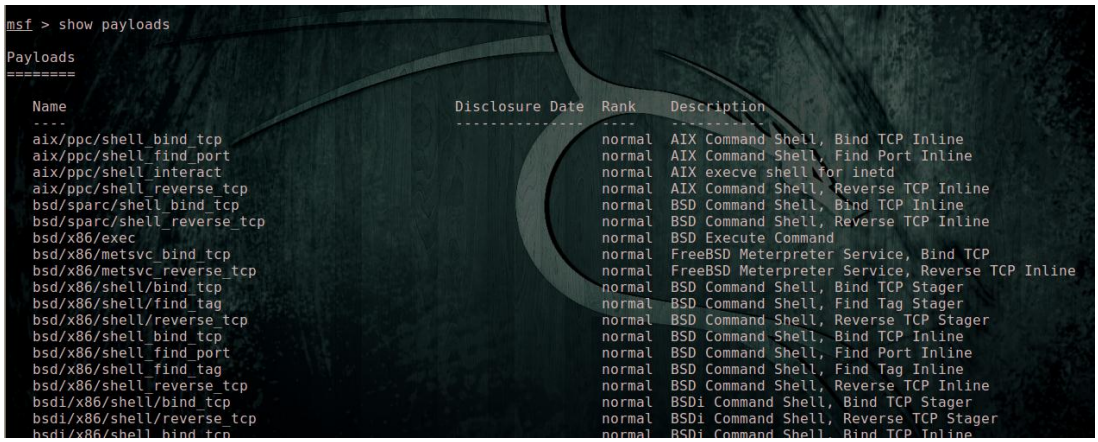



**FIGURA III.LXI Payloads disponibles de Metasploit.**

A continuación se ingresa set payload windows/meterpreter/reverse_tcp para seleccionar el reverse payload.

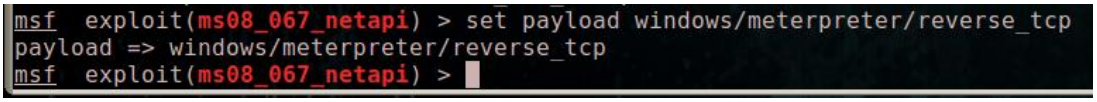



**FIGURA III.LXII Carga del Payload.**

Hasta el momento se tiene ingresado el exploit y payload respectivamente, con el análisis de vulnerabilidades se determinó que host son propensos a este ataque, y se procede a ingresar en RHOST el host del objetivo y LHOST la ip del atacante, cabe recalcar como es una prueba de pentest autorizada no se a cambiado MACs ni direcciones IPs.

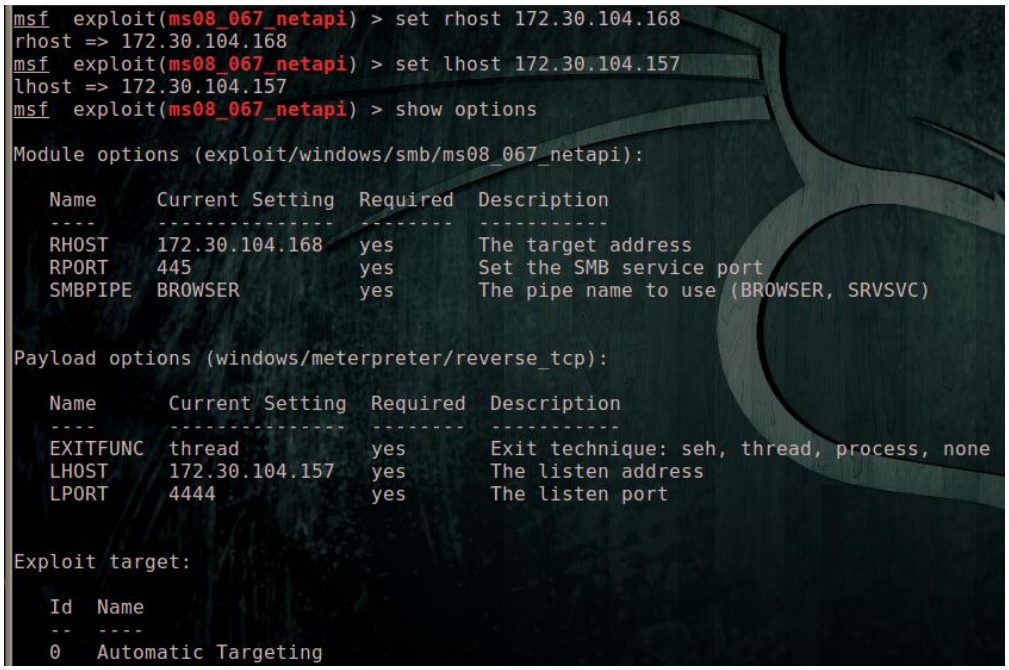



**FIGURA III.LXIII Ingreso de direcciones IP.**

En la figura se muestra el ingreso de las direcciones tanto del objetivo como del atacante, se visualiza con el comando show options y se muestra cargado exitosamente el exploit a ejecutar y el respectivo payload.

En lo que respecta al objetivo o Target framework selecciona automáticamente el target más apropiado para la explotación.

Teniendo todos los parámetros necesarios listos, para ejecutar la explotación se digita el comando exploit e inmediatamente realiza su trabajo.

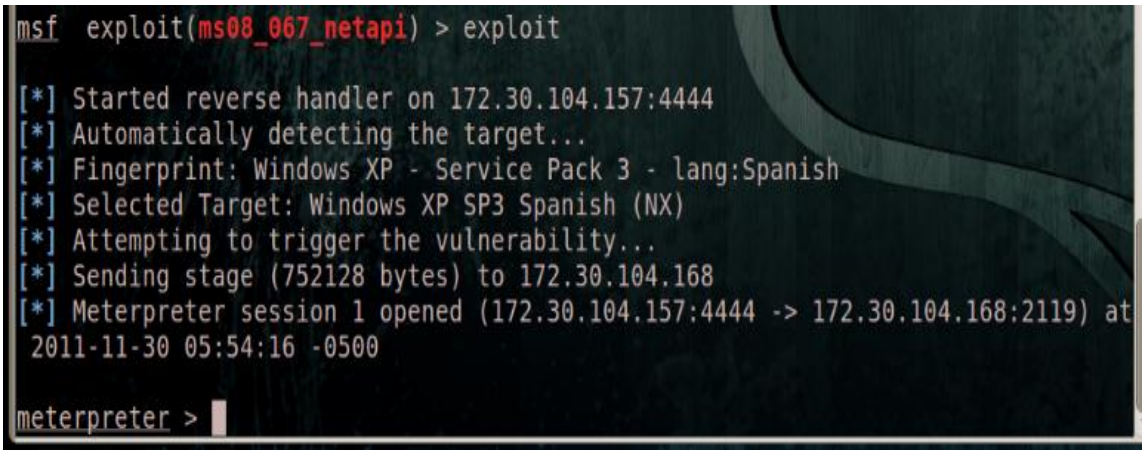



**FIGURA III.LXIV Explotación del objetivo.**

Al final muestra una Shell de meterpreter indicando que se ha realizado exitosamente la explotación.

Para verificar que efectivamente esta hecha la explotación se digita uno de los comandos que tiene meterpreter que es screenshot

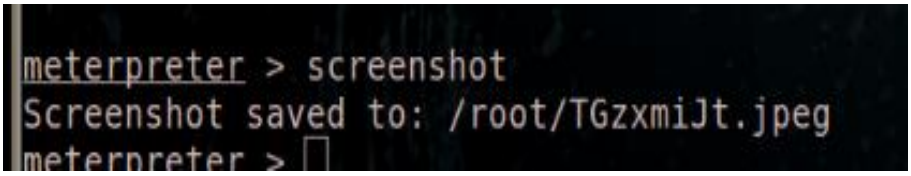



**FIGURA III.LXV Screenshot del objetivo.**

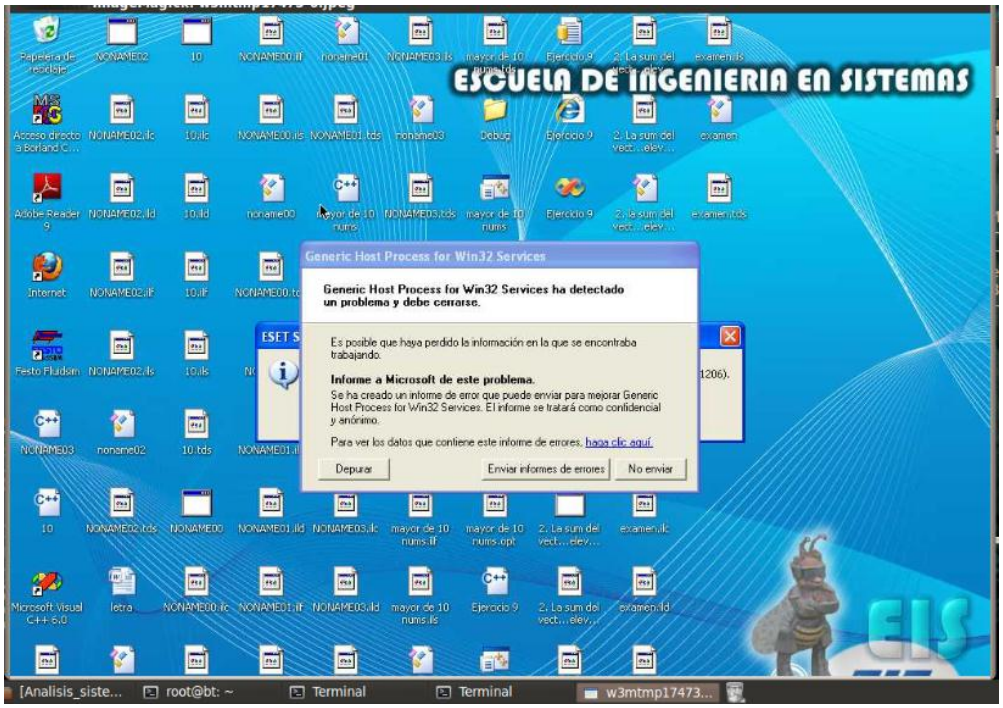



**FIGURA III.LXVI Explotación del objetivo.**

Las fases de Manteniendo Acceso y Borrado de huellas no son necesarias puesto que se cuenta con la autorización de las autoridades de la Escuela de Ingeniería en Sistemas de la Escuela Superior Politécnica de Chimborazo.

## 3.6 REPORTE DEL TEST DE PENETRACIÓN DE LA RED.

### INFORMACIÓN GENERAL

El presente trabajo investigativo se origina por la necesidad de mostrar las diferentes vulnerabilidades que posee la red a tratar. Estas vulnerabilidades pueden ser explotadas desde adentro de la intranet para este caso de estudio.

## RESUMEN EJECUTIVO

Antecedentes.

La mayoría de las estadísticas de seguridad en cómputo indican que cerca del 80% de los fraudes relacionados con las computadoras provienen de los usuarios internos o un uso inapropiado de las LAN, por esto las intranets son las más vulnerables a ataques de ésta índole.

Para determinar las fallas de seguridad de la red, se toma a consideración la metodología Hacker, más conocido en el ámbito de seguridad Informática como pentest de la red o prueba de penetración, que consiste en realizar en primer plano un análisis de vulnerabilidades y continuando con ataques controlados a los equipos y dispositivos de la red, determinando así las deficiencias de seguridad para poder tomar las correcciones necesarias de esta manera disminuir las incidencias negativas en la red y minorar las probabilidades de sufrir ataques.

- Objetivo del proyecto

El principal objetivo de la culminación del ejercicio de pentest es la contribución al fortalecimiento de seguridad en Redes de Área Local, por medio de la utilización

de la distribución de Linux Backtrack, a la vez demostrar las diversas vulnerabilidades que posea la red de la Escuela de Ingeniería en Sistemas.

**INFORME TECNICO**

Para la presente investigación se realiza un informe de evaluación técnica. Este tipo de informe general, se desarrolla para los técnicos que deberían comprender las características básicas de seguridad manejados por el sistema y responder a la vez cuestiones que se debería tomar en cuenta al momento de diseñar e implementar la red, ¿qué características son vulnerables, como pueden ser explotados, que impacto en el servicio podría traer? y cómo dar soluciones de resistencia para contrarrestar las amenazas visibles.

- Objetivos de la prueba

  Utilizando el método de hacking ético realizar un análisis de vulnerabilidades intensivo.

- Alcance del Test

  Descubrir la mayor parte de las vulnerabilidades e identificar su peligrosidad y riesgos de ser explotadas.

- Fuerza del Test

Explotar vulnerabilidades críticas en ambientes controlados

- Enfoque

  Demostrar la importancia de un análisis de pentest y su beneficio para la Institución.

Recopilación de información:

Recopilación de información y evaluación de la información son la base de una buena prueba de penetración.

Inteligencia pasiva:

Para la recopilación de información se utilizo herramientas de footprinting como metagofil, thehavester y maltego, de lo cual se pudo extraer información a partir de terceros mostrados en las figuras de footprinting.

Se logro obtener información del objetivo a través de este método y lo que se vislumbra una lista de lo extraído de la metadata en Internet.

- Nombre de dominios y sus respectiva IPs
- Nombre de subdominios y sus respectiva IPs

- Nombres de Usuarios
- Software encontrado en lo que respecta Sistemas Operativos en uso
- Bloques de red
- Servicios de red y aplicaciones
- Arquitectura del sistema
- Sistema de detección de intrusos
- Mecanismos de autenticación
- Direcciones IP específicas y sus respectivos
- Acceso a los mecanismos de control
- Direcciones de contacto
- Los números de teléfono

Cabe mencionar que el análisis pasivo, no corresponde a la ejecución de pentest dentro de la LAN, pero se ha optado por tomar en consideración ya que brinda valiosa información al momento de realizar el análisis de vulnerabilidades con BackTrack.

Inteligencia activa:

En esta sección se muestran los métodos y resultados de las tareas tales como el mapeo de infraestructura, escaneo de puertos, y la evaluación de la arquitectura. Se muestra inteligencia activa en las figuras, haciendo uso de las herramientas como Nmap, netifera, ntbscan y Zenmap, de lo cual se desprende la siguiente información:

- Puertos Abiertos, protocolo que utiliza, estado y el servicio que ejecuta.
- Direcciones IPs y servicios activos (netbios,etc).
- Sistema Operativo en servicio.
- Dirección Mac.
- Topología grafica de la Red.
- Comunidades SNMP.
- VPNs Activas.

Evaluación de la vulnerabilidad:

Evaluación de la vulnerabilidad es el acto de la identificación de las posibles vulnerabilidades que existen en una prueba y la clasificación de amenaza de cada amenaza.

- Clasificación de los niveles de vulnerabilidad

High Severity, corresponde al nivel critico de vulnerabilidad, según la clasificacion de la aplicación Nessus. Se identifica con el color rojo.

Medium Severity su nivel de peligrosidad medio de vulnerabilidad, indica que tiene un nivel de riesgo medio.

Low Severity o nivel bajo de riesgo, indica un nivel bajo de insidencia con esta vulnerabilidad en particular.

- Mapa de Vulnerabilidades

La figura muestra un resumen de las vulnerabilidades y el nivel de riesgo que poseen, así como las direcciones IP que las contienen. Para el análisis de vulnerabilidades se utilizo la Aplicación Nessus en su versión Home.

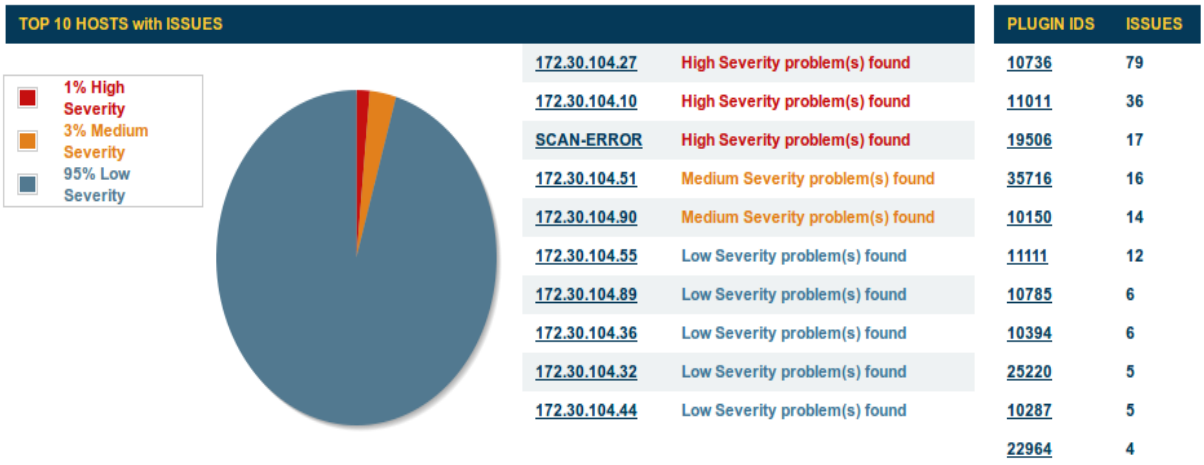



**FIGURA III.LXVII Resumen ejecutivo en HTML del reporte de Sistemas-FIE en Nessus.**

Para evitar falsos negativos y positivos cabe recalcar que el análisis de vulnerabilidades se llevo a cabo en toda la infraestructura de red al menos tres veces, coincidiendo los resultados obtenidos en las evaluaciones previas.

## Vulnerabilidad y niveles de Riesgo

| PLUGIN IDS | SEVERITY | # OF ISSUES | SYNOPSIS |
|---|---|---|---|
| 34477 | High | 1 | MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)<br>Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service. |
| 35362 | High | 1 | MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)<br>It is possible to crash the remote host due to a flaw in SMB. |
| 42411 | High | 1 | Microsoft Windows SMB Shares Unprivileged Access<br>It is possible to access a network share. |
| 12218 | Medium | 2 | mDNS Detection<br>It is possible to obtain information about the remote host. |
| 26919 | Medium | 2 | Microsoft Windows SMB Guest Account Local User Access<br>It is possible to log into the remote host. |
| | | | NFS Exported Share Information Disclosure |

| | |
|---|---|
| 10395 | 2 |
| 10859 | 2 |
| 10397 | 2 |
| 53513 | 2 |
| 10860 | 2 |
| 17651 | 1 |
| 11356 | 1 |
| 53335 | 1 |
| 34477 | 1 |
| 26920 | 1 |

**FIGURA III.LXVIII Información de las vulnerabilidades técnicas y su descripción del Resumen Ejecutivo.**

Además se puede extraer del resumen de ejecutivo de nessus las características de cada vulnerabilidad y su respectivo nivel de riesgo.

**Explotación**

Confirmación de la explotación o vulnerabilidad es el acto de la activación de las vulnerabilidades identificadas en las secciones anteriores para obtener un nivel específico de acceso a los activos de destino.

A Continuación se muestra una breve reseña de ataques exitosos comprobado y verificado contra el objetivo.

| ATAQUES | HERRAMIENTAS | VECES |
|---|---|---|
| Port Scanning | Nmap | 15 |
| Sniffing | Wireshark | 12 |
| ARP Spoofing | Ettercap | 11 |
| DNS Spoofing | Ettercap | 8 |
| Social Ingeenery (Ingenieria Social) | SET (Social Engineering Toolkit) | 8 |
| Man in the midle(hombre en el Medio) | Arp spoof y DNS-spoof | 7 |
| Denegacion de Servicio | Ettercap | 5 |
| Password Cracking | Hydra-Gtk | 5 |

| | | |
|---|---|---|
| Desbordamiento de buffer | Metaesploit Framework | 9 |

**TABLA III.IVResumen de ataques realizados con éxito.**

En primera instancia en ciertos países como el vecino País de Colombia Port Scanning o Escaneo de Puertos es considerado como delito, en el caso en cuestión al haber obtenido permiso de las autoridades pertinentes se procedió a ejecutar un escaneo como se muestra en la figura III.15 con zenmap.

Al finalizar el Escaneo de puertos y conjuntamente con un Ping Sweep o barrido de puertos se obtiene un Network Mapping mas especifico.

Seguidamente se realizo un ataque 'Man in the middle', o como se conoce en español 'El hombre en el medio', con ARP-Spoof.


**FIGURA III.LXIX Interacción normal de la Solicitud ARP.**

La figura anterior muestra la normal interacción del usuario o varios usuarios con el equipo de capa de enlace que es el encargado de encontrar la dirección hardware o la Ethernet MAC que corresponde a una determinada dirección IP. El protocolo ARP se encarga de traducir las direcciones IP a direcciones MAC que

son las direcciones físicas antes mencionadas. Para realizar esta conversión, el nivel de enlace utiliza las tablas ARP y cada interfaz tiene tanto una dirección IP como una dirección física MAC. A continuación se muestra el normal funcionamiento de la tabla arp dentro de la LAN.

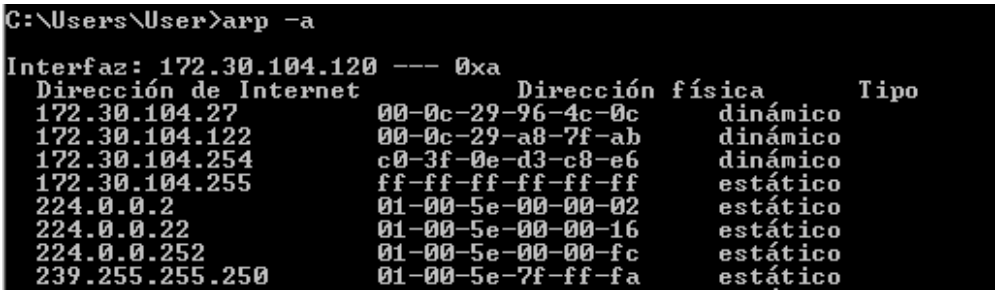



**FIGURA III.LXX Visualización de la Tabla ARP desde el Host del Atacante.**

En la figura se visualiza la utilización del protocolo de resolución de direcciones o ARP la cual indica la dirección física de cada maquina asociada a una dirección IP del equipo correspondiente. Con el comando arp –a si existe mas de una interfaz de red que utilice ARP se visualizara en la tabla ARP como muestra la figura.

Lo que se intenta hacer con el ataque de Hombre en el medio es interponerse entre las comunicaciones y hacerse pasar tanto por el Usuario y el Gateway al mismo tiempo. Para ello se utiliza ARP-Spoofing.

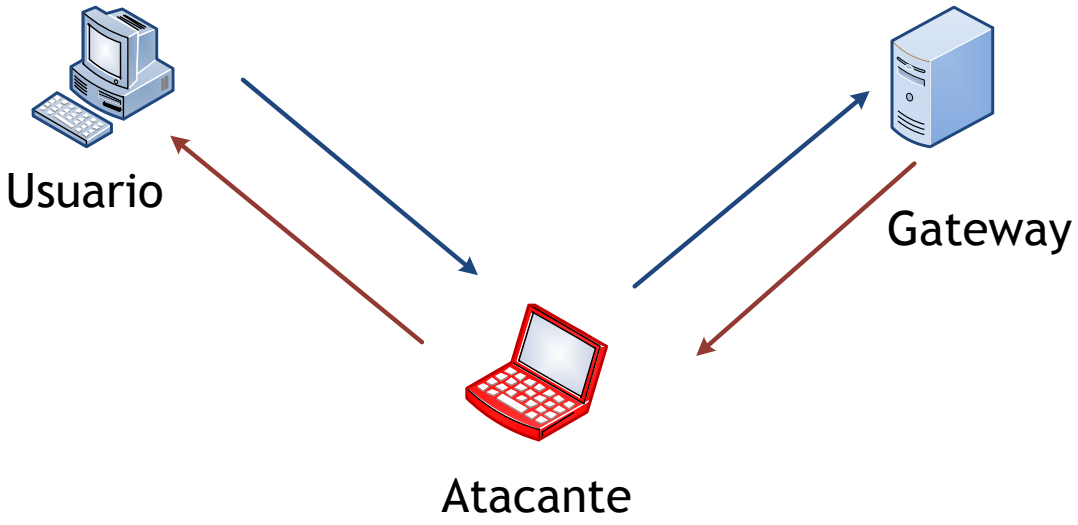



**FIGURA III.LXXI Diagrama de Ataque de hombre en el medio.**

ARP Spoofing, también conocido como ARP Poisoning o ARP Poison Routing, La técnica, consiste en envenenar la cache ARP de un cliente de una red LAN para hacerle creer que la MAC de la puerta de enlace es la dirección MAC del equipo atacante, pudiendo de este modo situar la máquina del atacante en medio de las comunicaciones efectuadas entre el equipo víctima y la puerta de enlace.

Una herramienta bien conocida para hacer ARP-Spoof es Ettercap, la cual permite utilizar tanto en modo texto como en modo grafico. Para ingresar en modo grafico dentro de una consola de BackTrack digitamos el siguiente comando.


**FIGURA III.LXXII Sintaxis de Ettercap Grafico.**

A continuación se nos despliega un frame con las siguientes opciones


**FIGURA III.LXXIII Inicio de Ettercap.**

Seguidamente acudimos a una de las tantas utilidades de ettercap que es Sniff y se procede a escoger Unified sniffing, e inmediatamente se visualiza un cuadro en el cual nos indica desde que interfaz se procederá a Sniffear, para el caso en cuestión eth0.

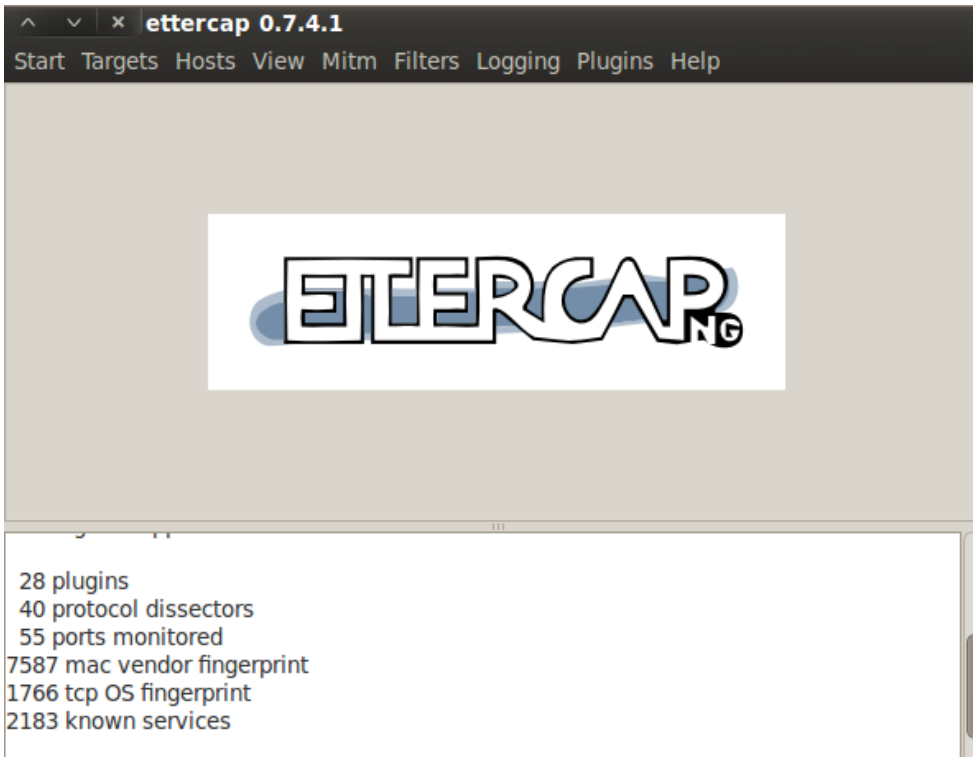



**FIGURA III.LXXIV Menu de opciones dentro de Ettercap.**

Posteriormente se procede a buscar a los Host dentro de la LAN mediante el menú mostrado en la barra de menus de Ettercap y ubicándonos en Host y Scan for host.


**FIGURA III.LXXV Busqueda de Host con Ettercap.**

Ya encontrado los host se procedió a visualizarlos con Host list.

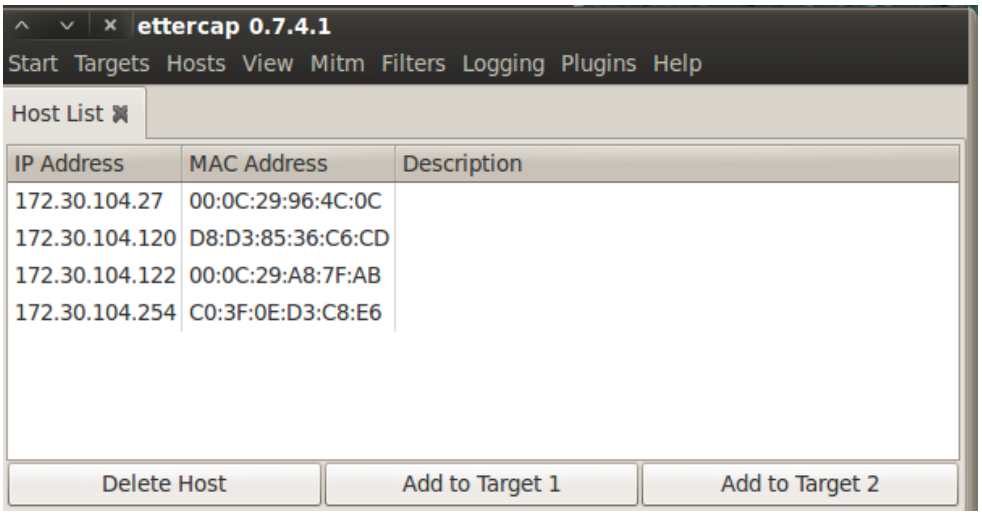



**FIGURA III.LXXVI Visualización de host encontrados.**

A continuación procedemos a identificar los objetivos en Targets.

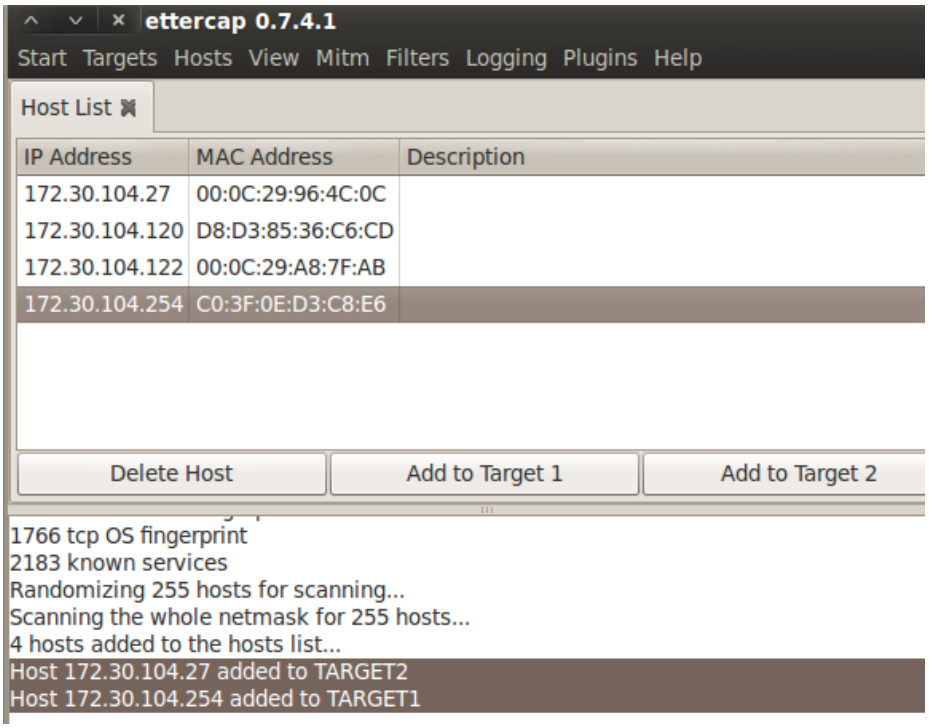



**FIGURA III.LXXVII Objetivos agregados dentro de Ettercap.**

Se ha añadido en TARGET1 la dirección del Gateway, en el caso en cuestión es la dirección del Servidor Proxy y en TARGET2 la dirección de una pc dentro de la LAN.

Para empezar a realizar el ataque se procede a ubicar en Mitm y seguidamente en Arp poisoning.

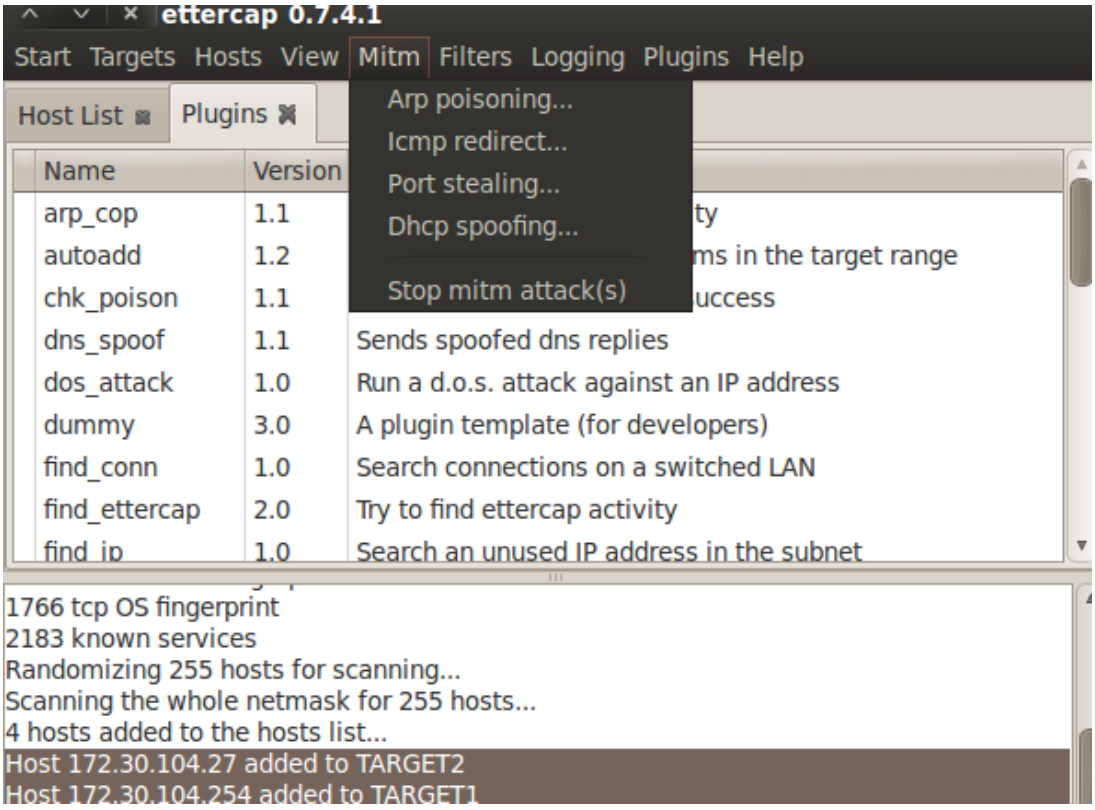



**FIGURA III.LXXVIII Ingreso a ARP poisoning.**

Seguido aparecerá un recuadro indicando parámetros opcionales, para lo cual se escoge Sniff remote connections, lo cual permitirá envenenar varias conexiones remotas.

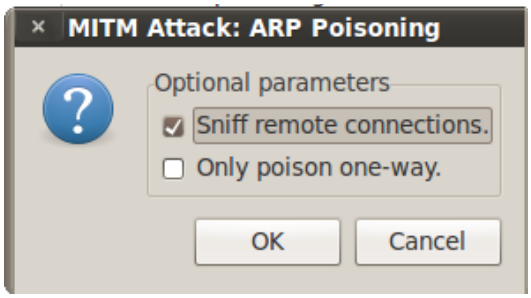


**FIGURA III.LXXIX Cuadro para Empezar ARP poisoning.**

El principio del ARP Spooffing es enviar mensajes ARP falsos dentro de la Ethernet. Normalmente la finalidad es asociar la dirección MAC del atacante con la dirección IP de otro nodo atacado, en el caso en cuestión a la puerta de enlace predeterminada que es el servidor proxy. Cualquier tráfico dirigido a la dirección IP del proxy, será erróneamente enviado al atacante, en lugar de a su destino real y de la misma manera será enviado el tráfico de la dirección IP del host Atacado.

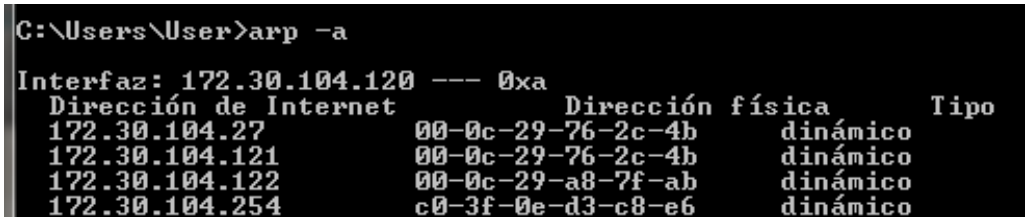



**FIGURA III.LXXX Direcciones MAC duplicadas.**

Se muestra en la figura que existe MAC duplicadas con direcciones IP diferentes lo cual indica que el ataque se ha realizado con éxito.

El atacante puede incluso lanzar un ataque de tipo DoS (Denegación de Servicio) contra una víctima, asociando una dirección MAC inexistente con la dirección IP de la puerta de enlace predeterminada de la víctima. Además se realizo DNS-Spooff siguiendo principios similares para la ejecución de un ataque de ingeniería social conocido como Client-Site.

Cabe recalcar que le presente trabajo de investigación no brinda una guía de ataque, al contrario esto es una muestra de vulnerabilidades halladas y explotadas para un mejor manejo de la seguridad, por eso todos los ataques realizados no se muestran.

## 3.7 COMPROBACIÓN DE LA HIPOTESIS

Para la comprobación de la hipótesis se muestra la siguiente tabla con las vulnerabilidades encontradas y el grado de severidad de las vulnerabilidades de seguridad encontradas en las instalaciones de la FIE de la Escuela Superior Politécnica de Chimborazo.

| PLUGIN ID# | # | PLUGIN NAME | SEVERITY |
|---|---|---|---|
| 55925 | 2 | PHP 5.3 < 5.3.7 Multiple Vulnerabilities | High Severity problem(s) found |
| 52717 | 2 | PHP 5.3 < 5.3.6 Multiple Vulnerabilities | High Severity problem(s) found |
| 51140 | 2 | PHP 5.3 < 5.3.4 Multiple Vulnerabilities | High Severity problem(s) found |
| 48245 | 2 | PHP 5.3 < 5.3.3 Multiple Vulnerabilities | High Severity problem(s) found |
| 45004 | 2 | Apache 2.2 < 2.2.15 Multiple Vulnerabilities | High Severity problem(s) found |
| 42411 | 1 | Microsoft Windows SMB Shares Unprivileged Access | High Severity problem(s) found |
| 19506 | 1 | Scan Error | High Severity problem(s) found |
| 26919 | 3 | Microsoft Windows SMB Guest Account Local User Access | Medium Severity problem(s) found |

| | | | |
|---|---|---|---|
| 12218 | 3 | mDNS Detection | Medium Severity problem(s) found |
| 56216 | 2 | Apache 2.2 < 2.2.21 mod_proxy_ajp DoS | Medium Severity problem(s) found |
| 53896 | 2 | Apache 2.2 < 2.2.18 APR apr_fnmatch DoS | Medium Severity problem(s) found |
| 51439 | 2 | PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS | Medium Severity problem(s) found |
| 50070 | 2 | Apache 2.2 < 2.2.17 Multiple Vulnerabilities | Medium Severity problem(s) found |
| 48205 | 2 | Apache 2.2 < 2.2.16 Multiple Vulnerabilities | Medium Severity problem(s) found |
| 44921 | 2 | PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities | Medium Severity problem(s) found |
| 11213 | 2 | HTTP TRACE / TRACK Methods Allowed | Medium Severity problem(s) found |
| 10678 | 2 | Apache mod_info /server-info Information Disclosure | Medium Severity problem(s) found |
| 10677 | 2 | Apache mod_status /server-status Information Disclosure | Medium Severity problem(s) found |
| 56211 | 1 | SMB Use Host SID to Enumerate Local Users Without Credentials | Medium Severity problem(s) found |
| 56210 | 1 | Microsoft Windows SMB LsaQueryInformationPolicy Function | Medium Severity problem(s) |

| | | | |
|---|---|---|---|
| | | SID Enumeration Without Credentials | found |
| 51192 | 1 | SSL Certificate signed with an unknown Certificate Authority | Medium Severity problem(s) found |
| 26920 | 1 | Microsoft Windows SMB NULL Session Authentication | Medium Severity problem(s) found |
| 11356 | 1 | NFS Exported Share Information Disclosure | Medium Severity problem(s) found |
| 10736 | 69 | DCE Services Enumeration | Low Severity problem(s) found |
| 11011 | 28 | Microsoft Windows SMB Service Detection | Low Severity problem(s) found |
| 35716 | 19 | Ethernet Card Manufacturer Detection | Low Severity problem(s) found |
| 19506 | 16 | Nessus Scan Information | Low Severity problem(s) found |
| 22964 | 15 | Service Detection | Low Severity problem(s) found |
| 10150 | 13 | Windows NetBIOS / SMB Remote Host Information Disclosure | Low Severity problem(s) found |
| 11111 | 12 | RPC Services Enumeration | Low Severity problem(s) found |
| 10287 | 11 | Traceroute Information | Low Severity problem(s) found |
| 25220 | 10 | TCP/IP Timestamps Supported | Low Severity problem(s) found |
| 11936 | 8 | OS Identification | Low Severity problem(s) found |
| 10785 | 7 | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure | Low Severity problem(s) found |

| | | | |
|---|---|---|---|
| 10394 | 7 | Microsoft Windows SMB Log In Possible | Low Severity problem(s) found |
| 10114 | 7 | ICMP Timestamp Request Remote Date Disclosure | Low Severity problem(s) found |
| 54615 | 6 | Device Type | Low Severity problem(s) found |
| 45590 | 6 | Common Platform Enumeration (CPE) | Low Severity problem(s) found |
| 10107 | 6 | HTTP Server Type and Version | Low Severity problem(s) found |
| 53513 | 5 | Link-Local Multicast Name Resolution (LLMNR) Detection | Low Severity problem(s) found |
| 26917 | 5 | Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry | Low Severity problem(s) found |
| 24260 | 5 | HyperText Transfer Protocol (HTTP) Information | Low Severity problem(s) found |
| 20301 | 5 | VMware ESX/GSX Server detection | Low Severity problem(s) found |
| 43815 | 4 | NetBIOS Multiple IP Address Enumeration | Low Severity problem(s) found |
| 10397 | 4 | Microsoft Windows SMB LanMan Pipe Server Listing Disclosure | Low Severity problem(s) found |
| 24786 | 3 | Nessus Windows Scan Not Performed with Admin Privileges | Low Severity problem(s) found |
| 11153 | 3 | Service Detection (HELP Request) | Low Severity problem(s) found |

| | | | |
|---|---|---|---|
| **10860** | **3** | **SMB Use Host SID to Enumerate Local Users** | **Low Severity problem(s) found** |
| **10859** | **3** | **Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration** | **Low Severity problem(s) found** |
| **10395** | **3** | **Microsoft Windows SMB Shares Enumeration** | **Low Severity problem(s) found** |
| **39520** | **2** | **Backported Security Patch Detection (SSH)** | **Low Severity problem(s) found** |
| **11424** | **2** | **WebDAV Detection** | **Low Severity problem(s) found** |
| **10881** | **2** | **SSH Protocol Versions Supported** | **Low Severity problem(s) found** |
| **10267** | **2** | **SSH Server Type and Version Information** | **Low Severity problem(s) found** |
| **53335** | **1** | **RPC portmapper (TCP)** | **Low Severity problem(s) found** |
| **51891** | **1** | **SSL Session Resume Supported** | **Low Severity problem(s) found** |
| **50845** | **1** | **OpenSSL Detection** | **Low Severity problem(s) found** |
| **43111** | **1** | **HTTP Methods Allowed (per directory)** | **Low Severity problem(s) found** |
| **42263** | **1** | **Unencrypted Telnet Server** | **Low Severity problem(s) found** |
| **25240** | **1** | **Samba Server Detection** | **Low Severity problem(s) found** |
| **22319** | **1** | **MSRPC Service Detection** | **Low Severity problem(s) found** |
| **21745** | **1** | **Authentication Failure - Local Checks Not Run** | **Low Severity problem(s) found** |

| | | | |
|---|---|---|---|
| **21643** | **1** | **SSL Cipher Suites Supported** | **Low Severity problem(s) found** |
| **20094** | **1** | **VMware Virtual Machine Detection** | **Low Severity problem(s) found** |
| **17651** | **1** | **Microsoft Windows SMB : Obtains the Password Policy** | **Low Severity problem(s) found** |
| **13855** | **1** | **Microsoft Windows Installed Hotfixes** | **Low Severity problem(s) found** |
| **11422** | **1** | **Web Server Unconfigured - Default Install Page Present** | **Low Severity problem(s) found** |
| **10863** | **1** | **SSL Certificate Information** | **Low Severity problem(s) found** |
| **10757** | **1** | **Webmin Detection** | **Low Severity problem(s) found** |
| **10674** | **1** | **Microsoft SQL Server UDP Query Remote Version Disclosure** | **Low Severity problem(s) found** |
| **10437** | **1** | **NFS Share Export List** | **Low Severity problem(s) found** |
| **10428** | **1** | **Microsoft Windows SMB Fully Accessible Registry Detection** | **Low Severity problem(s) found** |
| **10400** | **1** | **Microsoft Windows SMB Registry Remotely Accessible** | **Low Severity problem(s) found** |
| **10281** | **1** | **Telnet Server Detection** | **Low Severity problem(s) found** |
| **10223** | **1** | **RPC portmapper Service Detection** | **Low Severity problem(s) found** |

**TABLA III.V VULNERABILIDADES ENCONTRADAS**

En la siguiente grafica se muestra el porcentaje de las vulnerabilidades de seguridad encontradas.

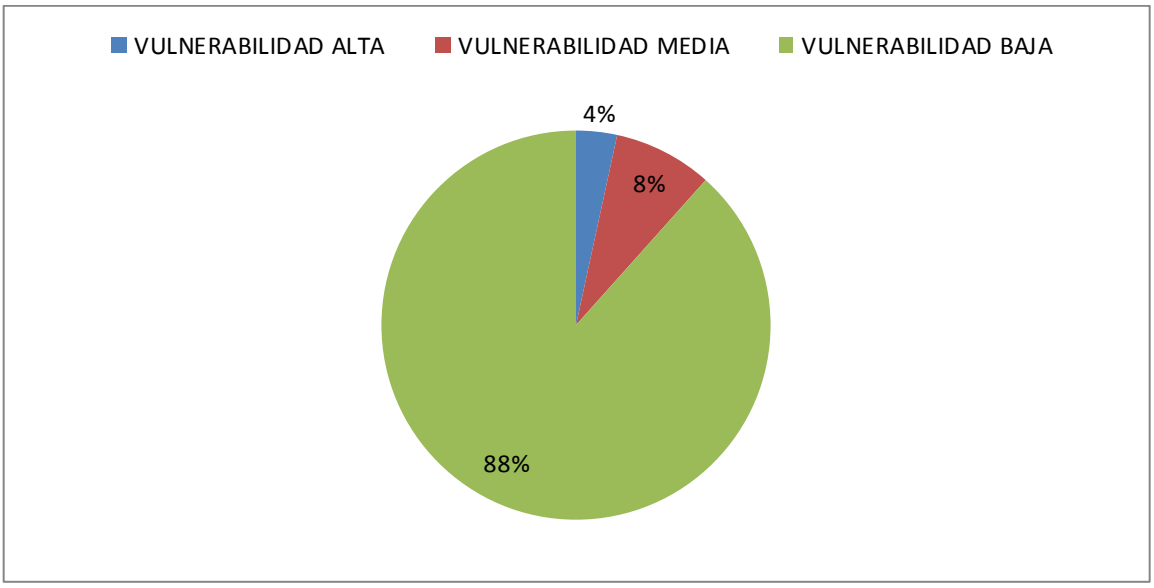



**FIGURA III.LXXXI RESUMEN VULNERABILIADES ENCONTRADAS**

# CAPÍTULO IV

# MEJORES PRÁCTICAS

## 4.1 ANÁLISIS DE LA INFRAESTRUCTURA

La red de datos de la Escuela de Sistemas de la Escuela Superior Politécnica de Chimborazo presenta un diseño Jerárquico.

A continuación se inicia indicando las VLANS que están configurados dentro de la Red.

| ***LABORATORIO*** | ***PUERTO*** | ***VLAN*** | ***DESCRIPCION*** |
|---|---|---|---|
| | | VLAN SERVIDORES | |
| Sala de Servidores | P21 | Proxy | 172.30.60.104/24 |
| | P23 | Server Software | 172.30.104.31/24 |
| | P22 | Servidor Web | 172.30.60.39/24 |

| | | | |
|---|---|---|---|
| VLAN AUTORIDADES | | | |
| Dirección | P6 | Dirección EIS | 172.30.10.X/24 |
| VLAN ADMINISTRADORES | | | |
| Secretaria | P2,P4 | Secretaria EIS | 172.30.20.X/24 |
| VLAN ACADEMICA | | | |
| Multimedia | P3 | EIS_LAB_MULTIMEDIA | 172.30.40.0/27 |
| Redes | P5 | EIS_LAB_REDES | 172.30.40.32/27 |
| Investigación | P7 | EIS_LAB_INVESTIGACION | 172.30.40.67/27 |
| Desarrollo | P9 | EIS_LAB_Desarrollo | 172.30.40.96/27 |
| Programación | P17 | EIS_LAB_PROGRAMACION | 172.30.104.0/24 |
| Automatización | P11 | EIS_LAB_AUTOMATIZACION | 172.30.40.128/27 |
| Sala de Profesores | P13 | EIS_PROFESORES | 172.30.40.160/27 |
| Aso. Escuela | P15 | EIS_ASO_ESCUELA | 172.30.104.192/27 |

**TABLA IV.I Descripción de las VLANs y puertos asociados al Switch Cisco.**

Tercer Piso

| *LABORATORIO* | *N° DE PCs* | *DESCRIPCION* | *N° DE PUERTO* | *DIRECCIONAMIENTO* |
|---|---|---|---|---|
| Sala de Servidores | 1 | Proxy | P21 | 172.30.60.104/24 |
| | 1 | Server Software | P23 | 172.30.104.31/24 |
| | 1 | Servidor Web | P22 | 172.30.60.39/24 |
| Investigación | 13 | EIS_LAB_INVESTIGACION | P7 | 172.30.40.67/27 |
| Redes | 21 | EIS_LAB_REDES | P5 | 172.30.40.32/27 |
| Multimedia | 25 | EIS_LAB_MULTIMEDIA | P3 | 172.30.40.0/27 |
| Programación | 28 | EIS_LAB_PROGRAMACION | P17 | 172.30.104.0/24 |

**TABLA IV.II Descripción de la infraestructura del Tercer Piso y su direccionamiento.**

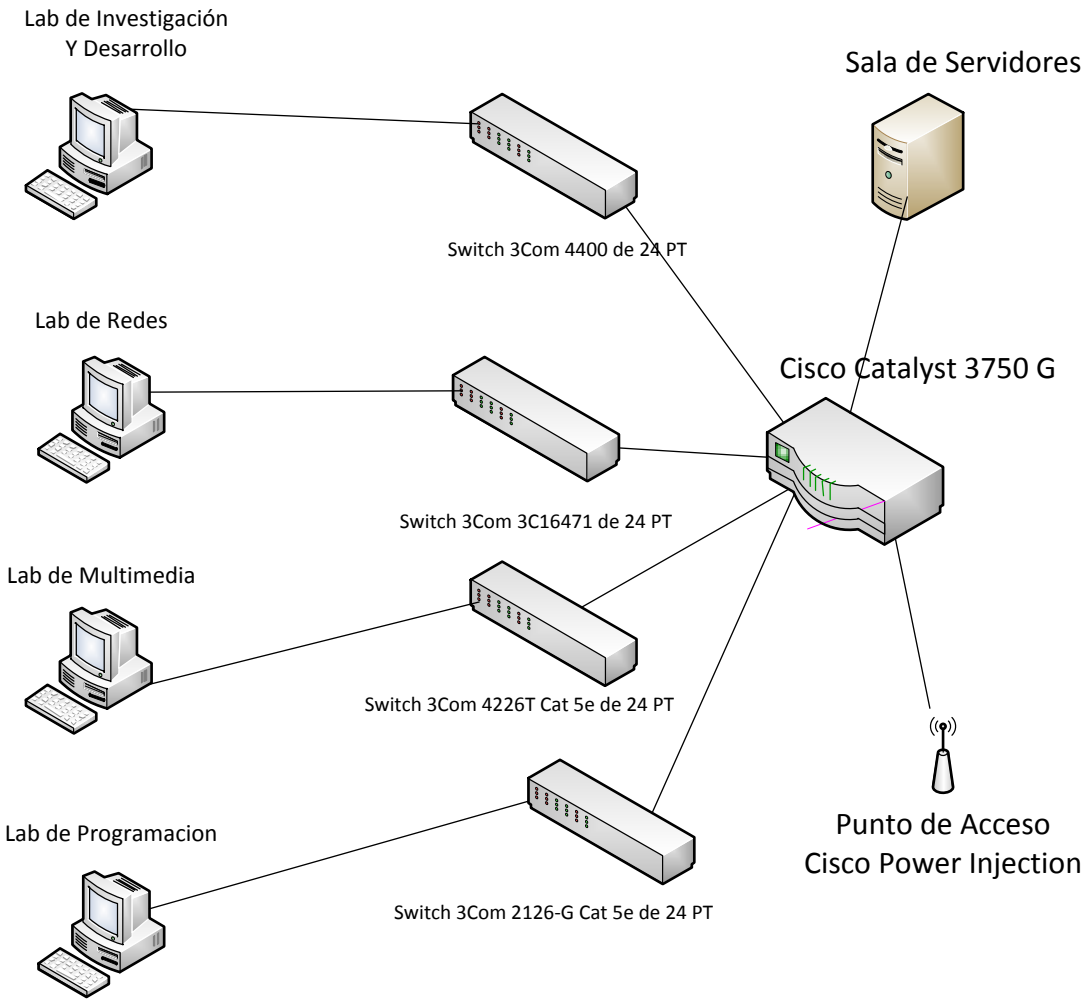



**FIGURA IV.I Diseño Lógico de la Red del Tercer Piso.**

Segundo Piso

| *LABORATORIO* | *N° DE PCs* | *DESCRIPCION* | *N° DE PUERTO* | *DIRECCIONAMIENTO* |
|---|---|---|---|---|
| Desarrollo | 21 | EIS_LAB_DESARROLLO | P9 | 172.30.40.96/27 |

| | | | | |
|---|---|---|---|---|
| Automatización | 11 | EIS_LAB_AUTOMATIZACION | P11 | 172.30.40.128/27 |
| Sala de Profesores | 2 | EIS_PROFESORES | P13 | 172.30.40.160/27 |
| Secretaria | 2 | Secretaria EIS | P2,P4 | 172.30.20.X/24 |
| Dirección | 1 | Dirección EIS | P15 | 172.30.10.X/24 |

**TABLA IV.III Descripción de la infraestructura del Segundo Piso y su direccionamiento.**

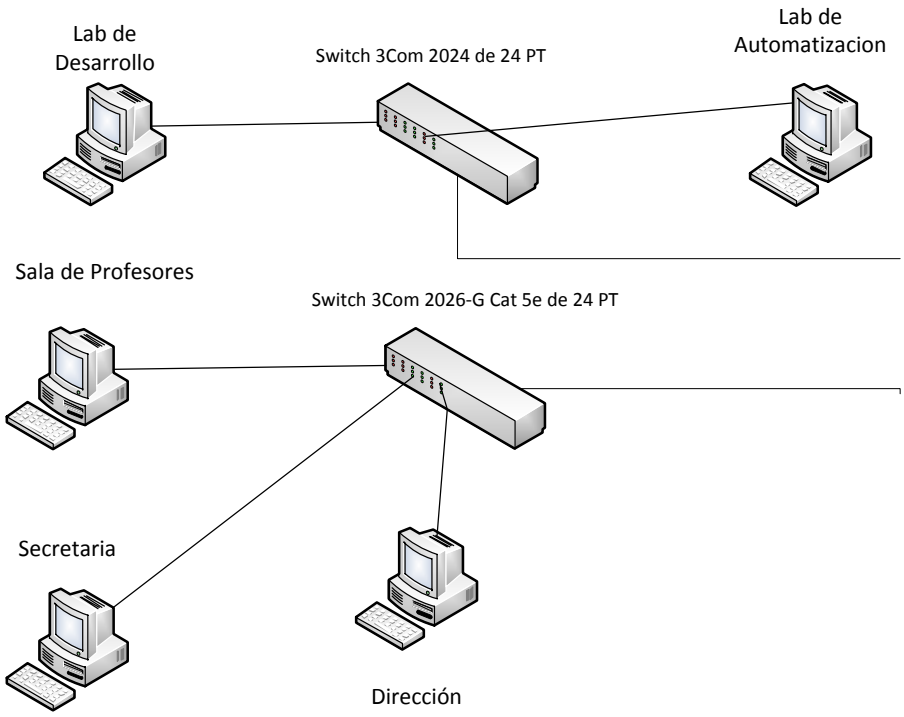



**FIGURA IV.II Diseño Lógico de la Red del Segundo Piso.**

Las conexiones salientes de los Switchs 3Com del segundo piso se dirigen hacia el Switch Cisco en el Tercer Piso.

| *LABORATORIO* | *N° DE PCs* | *DESCRIPCION* | *N° DE PUERTO* | *DIRECCIONAMIENTO* |
|---|---|---|---|---|
| Aso. Escuela | 3 | EIS_ASO_ESCUELA | P17 | 172.30.104.192/27 |

**TABLA IV.IV Descripción de la infraestructura del Primer Piso y su direccionamiento.**

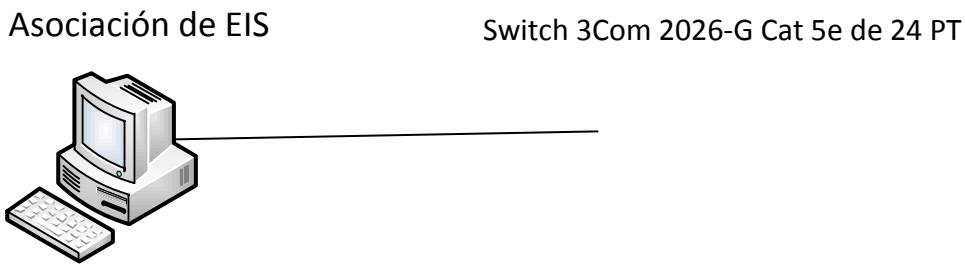



**FIGURA IV.III Diseño Lógico de la Red del Primer Piso.**

Las conexiones salientes de la Asociación de la Escuela de Sistemas se dirigen hacia el segundo piso donde se encuentra el Switch 3Com 2026 como se muestra en la figura.

## 4.2 ANÁLISIS DE RIESGOS

**Identificación del peligro:**

Para la identificación inicial del riesgo, se requiere identificar ciertos parámetros como

- Existencia de una fuente de daño.

Estadísticas informan que el 70% de los ataques sufridos en las instituciones son efectuados desde el interior de las propias empresas.

Adicionalmente, la falta de capacitación a los Administradores de Sistemas, en temas técnicos como la administración de redes y sobre todo en seguridad interna que es un tema casi inexistente dentro de las instalaciones de la Escuela Superior Politécnica de Chimborazo, a crecenta la probabilidad de vulnerabilidades y por consecuencia riesgos relacionados con delitos informáticos. También se suma la falta de alguna concesión de software antimalware o antivirus para la protección de los PCs.

- Por consecuencia puede ser dañado.

La institución y sus usuarios tanto internos como externos pueden sufrir algún tipo de ataque.

- Como puede ocurrir el daño

Por la posible existencia de vulnerabilidades en el diseño de red, en el sistema operativo y en sus aplicaciones. El daño puede ocurrir por medio de denegación de servicios, pérdida de información confidencial, suplantación de identidad, debido a una complicidad implícita o explícita de los administradores actuales de red.

- Estimación del Riesgo

En la estimación del riesgo valoramos la probabilidad y las consecuencias en caso de que se materialice el peligro.

A este riesgo le asignaremos un valor matemático, luego de investigar y tabular casos similares aplicaremos la fórmula:

Número de veces que sucede un riesgo/ Número de casos investigados = Valor matemático

Se ha investiga en 10 instituciones Universitarias, de las cuales 4 han sufrido varios ataques por motivo de vulnerabilidades existentes, provocando daños a la institución y a sus clientes al registrarse al recibir algún tipo de contagio por malware o sufrido de phishing

Se determina que la probabilidad de ocurrencia es aproximadamente del 40%.

En vista de que la probabilidad de ocurrencia es media, las consecuencias podrían ser dañinas, como: perdida de información confidencial, pérdida de prestigio y confianza por parte de los usuarios, contagio de malware.

Dentro del análisis de riesgo se debe además llevar a cabo una inspección física para determinar si la red de la Escuela de Sistemas cuenta con todas las seguridades físicas y tecnológicas para mitigar el riesgo, así como manuales de operación para empleados dependiendo de su nivel de responsabilidad y de

funciones, además de encuestas, entrevistas, cuestionarios, supervisiones para determinar el tipo de riesgo, frecuencia e impacto.

**Valoración del Riesgo:**

Luego de analizado el riesgo procedemos con la valoración del mismo, comparándolo con el riesgo tolerable

**Evaluación del Riesgo**

Frecuencia y Severidad

La frecuencia del riesgo tiene una probabilidad alta, mientras que la severidad del daño puede resultar extremadamente dañina porque los costos podrían ser relativamente bajos ya que se afecta directamente al prestigio de la institución.

Toma de acciones alternativas

Eliminar el riesgo es imposible porque la institución para ello debería dejar de operar, debería existir un análisis constante de lo que sucede dentro de la infraestructura de red, una constante capacitación y actualización por parte de los Administradores, se pueden probar software o aplicaciones libres que vendrían a reducir significativamente el nivel de riesgo existente.

A partir de esta evaluación iniciamos con la acción preventiva para llevar a cabo las acciones correspondientes.

**El control de alternativas**

El control de las dos decisiones tomadas anteriormente debe ser evaluado periódicamente, mediante inspecciones estadísticas que permitan mediar la eficiencia y eficacia de las técnicas aplicadas para minimizar el riesgo y el constante estudio para ir ajustándolo de acuerdo a las necesidades de la Institución, las cuales pueden ser cambiantes conforme el paso del tiempo.

METODOLOGIA DE LA AMINISTRACION DE RIESGOS

La metodología que nos permite mejorar la gestión de la Administración de Riesgos está compuesta por 4 fases:

Identificación de los Riesgos

Estimación de los Riesgos

Valoración de los Riesgos

Control de Riesgos

A continuación la aplicación de cada fase con respecto al riesgo que estamos analizando:

**FASE I**

Identificación de los Riesgos

Riesgo: El riesgo identificado es:

“Riesgo de existencia de vulnerabilidades en sistemas informáticos dentro de infraestructura de red de la Escuela de Sistemas de la Escuela Superior Politécnica de Chimborazo”.

Descripción:

Según Matias Katz, experto en seguridad informática: “Todo software (el 100% rotundamente), posee errores de diseño y/o desarrollo que representen una vulnerabilidad de seguridad en nuestra infraestructura”.

Esto reafirma la posible existencia de vulnerabilidades en sistemas informáticos ya que todo sistema necesita software para su funcionamiento, así mismo se encuentran vulnerabilidades en la infraestructura de redes, aplicaciones y protocolos utilizados de todas las instituciones, por lo tanto la existencia del riesgo tiene una alta probabilidad especialmente en instituciones donde la seguridad para los usuarios no es prioridad, en donde el contagio de malware es mas notorio.

El daño que la materialización de este peligro puede generar es la pérdida de prestigio de la institución y la afección directa sus usuarios, además los atacantes pueden ejecutar mediante ataques de ingeniería social informático que emula la

identidad de las víctimas contagio de malware especializado, fuga de información por medio de empleados de la institución.

Posibles consecuencias

Estos delitos mueven más dinero que el narcotráfico a nivel mundial, y las consecuencias para los usuarios dentro de la institución pueden llegar a ser incluso económicas además también psicológicas y morales, siendo la única manera de evitarlos a través de la prevención y ejecución de planes concisos de seguridad, por consecuencia existe una notable desconfianza al hacer uso de las instalaciones de la red evaluada, por lo cual una perdida de prestigio de la institución.

**FASE II**

| FACTOR DE RIESGO | TIPO | | RIESGO | DESCRIPCIÓN | POSIBLES CONSECUENCIAS |
|---|---|---|---|---|---|
| | INTERNO | EXTERNO | | | |
| Sistemas informáticos (hardware, software y aplicaciones | X | | Desactualización | Costos elevados de licencias del software utilizado tanto en los equipos de red y servicios , negligencia y descuido de los encargados del manejo de los Sistemas Informaticos. | La Institución es propensa a ser atacada por vulnerabilidades encontradas en las versiones caducas del software desde los dispositivosde red, sistemas operativos y aplicaciones en las que basan su funcionamiento. |
| Sistemas de información (politicas de seguridad) | X | | Perdida de información | Ddivulgacion de información sensible implícita o explicitamente por parte del personal a terceros, contaminación de los sistemas con malware y virus especializados por medio del incumplimiento o desconocimiento del tratamiento a la información. | Perdida de datos confidenciales y Acceso del intruso a los sistemas de la institución. |
| Infraestructura de Red | X | | Snniffers e Intrusión | Comunicaciones sin encriptación, Descuido en el diseño de red al no contar con la detección y contramedidas contra Snniffers y ataques de envenamiento ARP. | Exposición de información, denegación de servicios. |
| Desastres Naturales | | X | Perdida de activos e información | Perdida de información a causa de backups desactualizados. | Inaccesibilidad a los últimos respaldos lo cual origina perdida de recusos y tiempo. |

**TABLA IV.V FACTORES DE RIESGO**

## Estimación del Riesgo

En esta fase realizamos la matriz de priorización en donde medimos el riesgo de acuerdo el impacto y la probabilidad, antes de ello debemos considerar que el

impacto es la forma que el riesgo podría afectar los resultados del proceso, y la probabilidad es la frecuencia con que podría presentarse el riesgo.

| | | CONSECUENCIAS | | |
|---|---|---|---|---|
| | | Ligeramente dañino | Dañina | Extremadamente Dañino |
| PROBABILIDAD | Baja | | | Perdida de Activos e Información |
| | Media | | | Snniffers e Intrusión |
| | Alta | | Desactualización | Fuga de Información |

**TABLA IV.VI ESTIMACIÓN DE RIESGOS**

- Desactualización: La Desactualización de Sistemas Informáticos (hardware, software y aplicaciones) corresponde un riesgo importante porque la frecuencia de ocurrencia es alta y las consecuencias son dañinas, por lo tanto es recomendable no iniciar el trabajo hasta que se haya reducido el riesgo, se precisaran recursos económicos considerables, en la adquisición de licencias actualizadas ya que estas vienen con mejoras al rendimiento y parches o bugs en versiones anteriores en lo que corresponde a hardware de la infraestructura de red, adicionalmente si se usa sistemas privativos se necesita ejecutar todas las actualizaciones o cambiar de versiones superiores.

- Fuga de Información: La fuga de información confidencial por medio de la divulgación de información sensible, implícita o explícitamente por parte del

personal a terceros, contaminación de los sistemas con key logers, malware y virus especializados por medio del incumplimiento o desconocimiento del tratamiento a la información, es un riesgo intolerable debido a que su frecuencia de ocurrencia es alta y puede resultar extremadamente dañino, debido a que la información sustraída puede comprometer las operaciones de la Institucion y generar perdidas económicas a la institución financiera y a sus clientes, del mismo modo se recomienda no iniciar el trabajo hasta haber tomado las medidas correspondientes, entre ellas tenemos la creación de un manual de políticas de seguridad basado en la Norma ISO/IEC 27001 (*Information technology - Security techniques - Information security management systems - Requirements*) que permita establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información, el cual involucra a todo el personal según su grado de responsabilidad y funciones, debe existir un compromiso entre directivos y empleados para cumplir con todas las disposiciones, y adicional a esto, en la institución financiera debe existir al menos un responsable de la seguridad informática, con los conocimientos necesarios para salvaguardar la información y prevenir ataques a la institución.

- Snnifers e Intrusión: La falta de encriptación en las comunicaciones, por lo tanto su riesgo es Moderado y se debe determinar las inversiones y medidas para reducir el riesgo, se recomienda no iniciar el proceso mientras no se generen controlen efectivos, en este caso se recomienda que los encargados

de la administración de sistemas monitoreen constantemente la infraestructura de red y dispositivos conectados, se recomienda adquirir Sistemas Inteligentes de Detección de Intrusos o IDS como pueden ser utilizado la tecnología de Honeynets y herramientas que permitan detectar ataques a la tabla ARP de los equipos, para reducir ataques de hombre en el medio por este mecanismo.

- Pérdida de Activos e Información: Puede ser provocada por la pérdida de información a causa de backups desactualizados, su frecuencia de ocurrencia es baja con consecuencias extremadamente dañinas por lo tanto su Riesgo es Moderado, y se debe establecer acciones para establecer con más precisión la probabilidad del daño para generar medidas de control efectivas.

**FASE III**

Valoración de Riesgos:

En esta fase priorizamos los riesgos identificando controles asociados y analizando si estos son efectivos para determinar el nivel de riesgo:

| CONSECUENCIA | ANALISIS DE CONTROLES | | | | |
|---|---|---|---|---|---|
| Daño | No existe | Descripcion del Control | Existe y No es Efectivo | Existe y no esta documentado | Existe esta documentado y es efectivo |
| La Escuela de Sistemas es propensa a ser atacada por vulnerabilidades encontradas en las versiones caducas del software de los dispositivosde red. | X | Versiones actualizadas de dispositivos cisco en el caso del Switch Catalyst 3750 G, ya que debe incorporar recursos para seguridad. | | | |
| La Escuela de Sistemas es propensa a ser atacada por vulnerabilidades encontradas en las versiones caducas del software respecto al Sistema Operativo que se utiliza | X | Actualizar los PCs Windows 7 y utilizar la herramienta por defecto dels SO para deteccion de malware, en el caso que no se posea recursos para antivirus comerciales. | | | |
| La Escuela de Sistemas es propensa a ser atacada por vulnerabilidades encontradas en las versiones caducas del software respecto a las aplicaciones que hace uso. | X | Actualizar constantemente o de forma automatica todas las aplicaciones existentes que esten involucradas en el desembolvimiento de los usuarios incluyendo los navegadores y pluggins de los mismos. | | | |
| Perdida de datos confidenciales y Acceso del intruso a los sistemas de la institucion. | X | Agregar herramientas libres que permitan la deteccion de ataques de hombre en el medio. | | | |
| Exposicion de informacion de transacciones, denegacion de servicios. | | Antivirus con limitaciones | X | | |
| Inaccesibilidad a los ultimos registros transaccionales lo cual origina perdida de dinero y de prestigio. | | Backup generado una vez al mes | X | | |

**TABLA IV.VII ANÁLISIS DE CONTROLES**

- Desactualización: Es un riesgo importante, con priorización alta y media, controles no efectivos, requieren acciones preventivas.
- Fuga de Información: Es un riesgo importante, con priorización media y alta, controles no efectivos, requieren acciones preventivas.
- Snnifers e Intrusión: Es un riesgo moderado, con priorización alta y baja, con controles efectivos pero no documentados, requieren acciones preventivas.

- Pérdida de Activos e Información: Es un riesgo tolerable con priorización baja y media, con controles efectivos pero no documentados, requieren acciones preventivas.

**FASE IV**

En esta fase controlamos los riesgos analizados tomando acciones que los minimicen, analizando el desempeño de los procesos, evidenciando posibles desviaciones frente al resultado esperado para la adopción de acciones preventivas, el control se lo realiza mediante un tratamiento a los riesgos, las acciones alternativas constan de cuatro fases:

La Eliminación del riesgo es una difícil decisión y para poder eliminarlo tendría que dejar de poseer el bien.

Reducir el riesgo se realiza o se logra a través de medidas de prevención que disminuyen el impacto de este peligro, juega un papel muy importante la seguridad industrial por ejemplo en el caso de enfermedades, las personas para prevenirlas, se deben hacer chequeos médicos periódicos.

| RIESGO | TRATAMIENTO | ACCIONES | RESPONSABLE (S) EN EL PROCESO | CRONOGRAMA | | INDICADORES |
|---|---|---|---|---|---|---|
| | | | | FECHA INICIO | FECHA FINAL | |
| Desactualización software dispositivos de red | Reducción | Comprar versiones actualizadas de los dispositivos de red | Administrador de Sistemas y Encargado de la Seguridad de la Información | 01/04/2012 | 15/04/2012 | Monitoreo constante de red y rendimiento |
| Desactualización Sistemas Operativos | Reducción | Comprar versiones actualizadas de Sistemas Operativos en caso de ser privativos. Actualizar a versiones mas recientes de sistemas operativos libres. | Administrador de Sistemas y Encargado de la Seguridad de la Información | 01/04/2012 | 15/04/2012 | Monitoreo constante de red y rendimiento |
| Desactualización aplicaciones, buscadores y sus plggins | Reducción | Actualizacion constante de aplicaciones y navegadores con sus respectivos pluggins | Administrador de Sistemas y Encargado de la Seguridad de la Información | 01/05/2012 | 15/05/2012 | Monitoreo constante de red y rendimiento |
| Perdida de Información | Reducción | Capacitacion al personal que maneja la infraestrucatura de red y sus recursos sobre el seguimiento de mejores practicas para el desarrollo de | Administrador de Sistemas y Encargado de la Seguridad de la Información | 01/05/2012 | 15/05/2012 | Monitoreo constante de red y rendimiento |
| Snniffers e Intrusión | Reducción | Adquisición de sistemas de detección y protección contra intrusos, mediante software libre como Honeynets, prevencion contra ataques de hombre en le medio como | Administrador de Sistemas y Encargado de la Seguridad de la Información | 01/05/2012 | 15/05/2012 | Monitoreo constante de red y rendimiento |
| Perdida de Activos e Informacion | Reducción | Generación de BackUps en sitios remotos o de existeir los recursos en la nube, a l realizar el cierre diario de actividades | Administrador de Sistemas y Encargado de la Seguridad de la Información | 01/05/2012 | 15/05/2012 | Monitoreo constante de red y rendimiento |

**TABLA IV.VIII ACCIONES Y TRATAMIENTO**

## 4.3 POLITICAS DE SEGURIDAD

### 4.3.1 ALCANCE DE LAS POLITICAS DE SEGURIDAD

Este documento de políticas de seguridad se ha realizado en base a un análisis de riesgos y vulnerabilidades en las instalaciones de la Escuela de Ingeniería Informática de la ESPOCH, por consiguiente las políticas se encuentran sujetas a estas instalaciones

### 4.3.2 RESPONSABILIDADES

Un comité de gerencia de seguridad informática integrado por los responsables de la administración de la red y las autoridades, revisará periódicamente, en reuniones trimestrales y ad hoc, el estado de la seguridad de las redes y los computadores de la red, estudiará y evaluará el trabajo de recuperación relacionado con incidentes de seguridad de las redes y los computadores, autorizará y posteriormente emitirá juicio sobre los resultados de los proyectos importantes relacionados con la seguridad de las redes y los computadores, aprobará políticas, normas, lineamientos y procedimientos nuevos o modificados en materia de seguridad informática y realizará otras actividades en esta materia.

Los administradores del sistema tienen la responsabilidad de actuar como coordinadores locales de la seguridad de los sistemas informáticos. Estas personas son responsables de establecer privilegios de usuario adecuados, de evaluar los registros de control de acceso y de llevar a cabo acciones de seguridad similares para los sistemas que ellos administran.

Es responsabilidad del encargado de red someter a revisión y divulgar a las diferentes personas que utilizan la red las políticas que van a ser implementadas para así lograr una mayor eficiencia de la red.

Los usuarios tienen la responsabilidad de acatar ésta y otras políticas que definan las medidas de seguridad de las redes y los computadores y de reportar todas las vulnerabilidades y las violaciones a la seguridad informática que ellos identifiquen, al encargado de la red.

### 4.3.3 CONTROL DE ACCESO AL SISTEMA

Contraseñas de los usuarios finales

Los usuarios deben seleccionar contraseñas fijas que sean difíciles de adivinar, lo cual significa que las mismas no deben estar relacionadas con la vida personal o el trabajo del usuario, como por ejemplo, el número de placa de un automóvil, el nombre del cónyuge o fragmentos de una dirección, ni palabras incluidas en diccionarios o alguna parte gramatical tales como nombres propios, lugares, términos técnicos y jerga. Los usuarios deben abstenerse de elegir contraseñas que se pueden adivinar con facilidad en los lugares en donde este tipo de software de sistemas está disponible.

Los usuarios pueden seleccionar contraseñas fáciles de recordar, pero que sean difíciles de adivinar por terceros no autorizados, si:

- Enlazan varias palabras en una sola frase conocida sólo por ellos.

- Mueven una palabra una fila hacia arriba, hacia abajo, hacia la izquierda o hacia la derecha en el teclado.
- Mueven caracteres en una palabra varias letras en forma ascendente o descendente del alfabeto.
- Transforman una palabra normal siguiendo un método específico, como por ejemplo cambiando cada letra de por medio por un número que indique su posición en la palabra.
- Combinan signos de puntuación o números con una palabra normal.
- Crean siglas de palabras tomadas de una canción, un poema u otra secuencia conocida de palabras.
- Deletrean mal una palabra deliberadamente.
- Combinan un número de datos personales como fechas de cumpleaños y colores favoritos.

Los usuarios no deben construir contraseñas que sean idénticas o similares a las empleadas con anterioridad. Los usuarios deben abstenerse de volver a usar contraseñas anteriores en los lugares en donde las facilidades de software de sistemas están disponibles.

Los usuarios no deben construir contraseñas usando una secuencia básica de caracteres que se modifica parcialmente basándose en la fecha o en algún otro factor predecible. Por ejemplo, los usuarios no deben emplear contraseñas tales como "X34ENE" en enero y "X34FEB" en febrero.

Las contraseñas no deben guardarse en forma legible en archivos por lotes, en resumen de comandos de inicio de sesión automático, en macros de software, en teclas de función, en software de comunicaciones de datos, en exploradores de la web, en unidades de disco duro o en otras ubicaciones donde personas no autorizadas puedan descubrirlas.

Las contraseñas no deben anotarse y dejarse en lugares donde personas no autorizadas puedan descubrirlas. Aparte de la asignación de la contraseña inicial y de las situaciones de reinicialización de la contraseña, si existiese alguna razón para creer que una contraseña ha sido revelada a alguna persona distinta al usuario autorizado, se debe cambiar inmediatamente.

Las contraseñas no deben compartirse o revelarse a ninguna otra persona aparte del usuario autorizado, así que, si los usuarios necesitan compartir datos que se encuentran en el computador, entonces deben usar el correo electrónico, los directorios públicos en los servidores de red de área local y otros mecanismos. Esta política no impide el uso de contraseñas predeterminadas, generalmente

usados para la asignación de identificación de usuario nuevo o situaciones de reinicialización de la contraseña, las cuales se cambian de inmediato cuando el usuario vuelve a conectarse al sistema mencionado. Se deben cambiar todas las contraseñas cuando se sospeche que han sido reveladas o se tiene el conocimiento de que han sido reveladas a alguna persona distinta al usuario autorizado.

### 4.3.4 PROCESO DE INICIO Y CIERRE DE SESIÓN

Todos los usuarios deben identificarse positivamente antes de poder usar algún computador multiusuario y otros recursos del sistema de comunicaciones. La identificación positiva para las redes internas incluye un identificador de usuario y una contraseña fija, siendo ambos únicos para cada usuario individual o, en su defecto, un sistema extendido de autentificación de usuario.

La combinación de un identificador de usuario y una contraseña fija no brinda suficiente seguridad para las conexiones discadas o de Internet a los sistemas y las redes. Queda prohibido el uso de módems agregados a las estaciones de trabajo conectadas a la red ubicada en los laboratorios, a menos que tengan un sistema extendido de autentificación de usuario autorizado por el encargado de red. Los módems conectados a computadores independientes tales como

computadores portátiles y de uso doméstico son permitidos siempre y cuando se instale un cortafuego autorizado de computadores personales y el software de comunicaciones correspondiente no esté habilitado para recibir llamadas entrantes.

Cuando el software del sistema lo permita, cada mensaje de bienvenida mostrado en los computadores multiusuario debe incluir un aviso especial, el cual debe señalar que el sistema es para el uso exclusivo de usuarios autorizados y que de continuar usando el sistema, el usuario se presenta como un usuario autorizado, tiene conocimiento de que todo el uso del sistema se registra y entiende que las violaciones de las políticas de seguridad informática y otros requerimientos pueden ocasionar acciones disciplinarias y acciones legales.

El proceso de conexión para los sistemas de computación conectados a la red debe simplemente pedirle al usuario que se conecte, suministrando mensajes según sea necesario. No debe suministrarse información específica que el computador contenga sobre la organización, el sistema operativo, la configuración de la red y otros asuntos internos, hasta que el usuario haya proporcionado con éxito una identificación de usuario y una contraseña válidas.

Si no ha habido actividad en un terminal, una estación de trabajo o un computador personal por cierto periodo de tiempo (el periodo de tiempo recomendado es de 15 minutos), el sistema debe obscurecer la pantalla en forma automática y suspender la sesión cuyo restablecimiento debe producirse solamente después de que el usuario haya suministrado una contraseña válida. De acuerdo con esta política, se podrá hacer excepciones en aquellos casos en donde el área inmediata que rodea a un sistema está físicamente asegurada con puertas cerradas, con lectores de distintivos o tecnologías similares.

### 4.3.5 PRIVILEGIOS Y LIMITACIONES DE ACCESO AL SISTEMA

Los privilegios del sistema de comunicaciones y computación de todos los usuarios, sistemas y programas que operan independientemente, deben restringirse a la necesidad de conocer, lo cual significa que los privilegios no deben ser extendidos a menos que exista una necesidad legítima.

Los permisos predeterminados para ingresar a un archivo no deben permitir que ningún usuario del sistema lea, escriba, ejecute o elimine un archivo. Los permisos se otorgan a un grupo limitado de personas que tengan una verdadera necesidad de acceso. Queda prohibido que los usuarios reinicialicen los permisos archivo por archivo aunque puedan hacerlo

Los computadores y los sistemas de comunicación deben restringir el acceso a los computadores que puedan alcanzar los usuarios a través de las redes. Estas restricciones pueden implementarse a través de enrutadores, puertas de enlace, cortafuegos y otros componentes de la red y deben usarse, por ejemplo, para controlar la habilidad del usuario de iniciar sesión en un computador específico y, después, moverse desde ese computador a otro.

### 4.3.6 ESTABLECIMIENTO DE VÍAS DE ACCESO

Las modificaciones a las redes internas incluyen instalar un software nuevo, cambiar las direcciones de la red, reconfigurar enrutadores y agregar líneas de discado. Exceptuando las situaciones de emergencia, todos estos cambios deben documentarse en una solicitud y estar previamente autorizados. Los cambios de emergencia a las redes deben ser realizados por personas autorizadas por este departamento. Este proceso evita problemas inesperados que abarcan desde la negación del servicio hasta la divulgación de la información. El proceso se aplica no sólo a los usuarios sino también al personal del proveedor.

Los usuarios no deben instalar sistemas de foros y boletines electrónicos, redes de área local, servidores de protocolo de transferencia de archivos (FTP), servidores web, conexiones modem a redes de área local existentes o algún otro

sistema multiusuario para comunicar información ni establecer nuevos tipos de conexión en tiempo real entre dos o más sistemas internos de computación sin la autorización.

Todos los computadores que se conectan a una red interna o externa deben emplear controles de acceso basados en contraseña o un sistema extendido de autentificación de usuario.

Los puertos de mantenimiento remoto para los computadores y los sistemas de comunicación deben inhabilitarse hasta que el proveedor los necesite y desactivarse de inmediato después de usarse.

### 4.3.7 VIRUS, GUSANOS Y CABALLOS DE TROYA

Los usuarios deben mantener activado en sus computadores el software antivirus actual autorizado, el cual puede utilizarse para rastrear todo el software proveniente de terceros antes de ejecutar el nuevo software y no deben omitir los procesos de rastreo que pudiesen detener la transmisión de virus.

Los usuarios tienen la responsabilidad de erradicar los virus de todos los sistemas de computadores personales bajo su control cada vez que se detecten, empleando el software instalado por el personal. En cuanto el usuario detecte el virus, debe llamar al encargado para asegurarse de que no se produzcan nuevas infecciones y de que los expertos que se necesiten para erradicar el virus se dediquen a la tarea con prontitud.

Todo el software de los computadores personales debe copiarse antes de su uso inicial y almacenarse en un lugar seguro. Estas copias maestras no deben emplearse para las actividades normales sino más bien reservarse para la recuperación de infecciones por virus del computador, colapsos del disco duro y otros problemas e igualmente deben almacenarse en un sitio seguro.

No debe usarse el software descargado de foros o boletines electrónicos, de software compartido, de software de dominio público y otro software de fuentes no confiables, a menos que se halla sometido a pruebas rigurosas autorizadas.

### 4.3.8 RESPALDO DE PROGRAMAS Y DATOS

Los usuarios son responsables de efectuar el respaldo periódico de la información contenida en los computadores que se encuentren utilizando.

Debe respaldarse periódicamente toda la información Secreta o Confidencial, valiosa o crítica contenida en los sistemas de computación y las redes. Los encargados de la red deben definir cuál información y cuáles máquinas deben respaldarse, así como la frecuencia y el método de respaldo que se empleará, en concordancia en los siguientes lineamientos:

- Si el sistema soporta más de un usuario y contiene datos críticos para las operaciones diarias, se hacen respaldos diarios.
- Si el sistema se emplea para soportar funciones relacionadas con el trabajo y contiene datos críticos esenciales para las operaciones diarias de ese trabajo, se hacen respaldos semanales.
- Si el sistema se emplea principalmente como una herramienta personal y no contiene datos clasificados como de trabajo o del departamento, se hacen respaldos a discreción del usuario.

Los lapsos de tiempo mencionados anteriormente para realizar el respaldo periódico no impiden la realización de respaldos más frecuentes, según se requiera ocasionalmente por razones operativas o de negocios.

El almacenamiento de los medios de respaldo es responsabilidad del usuario del computador personal o del administrador del sistema multiusuario que participan en el proceso de respaldo.

La información debe retenerse únicamente por el tiempo que sea necesario. Cualquier otra información debe destruirse cuando ya no se necesite, generalmente después de dos años.

Los encargados de la red definen el cronograma de respaldo también tienen la responsabilidad de preparar y actualizar regularmente los planes de contingencia de los departamentos usuarios para restaurar el servicio a todas las aplicaciones, a pesar de que se requieran o no los servicios internos de red para el soporte de estas aplicaciones.

Toda la información Secreta o Confidencial almacenada en los medios de respaldo debe cifrarse empleando métodos autorizados.

### 4.3.9 CIFRADO

Cuando la información Secreta o Confidencial se transmite a través de cualquier red de comunicación, debe enviarse en forma cifrada. Cada vez que el código

fuente. Las definiciones de las palabras "Confidencial" y "Secreta" se pueden encontrar en la Política de Clasificación de Datos.

Cuando la información Confidencial o Secreta no se está usando, debe almacenarse en forma cifrada, lo cual significa que cuando se almacena o se transporta en medios de almacenamiento legibles, debe cifrarse.

El cifrado de información almacenada o en tránsito debe completarse mediante el uso de productos disponibles comercialmente y autorizados.

Cada vez que se emplee el cifrado, los usuarios no deben eliminar la única versión legible de la información a menos que hayan demostrado que el proceso de descifrado es capaz de restablecer una versión legible de la información.

Las claves de cifrado usados para la información siempre se clasifican como información Confidencial o Secreta. El acceso a dichas claves debe limitarse a aquellas personas con necesidad de conocer. A menos que se obtenga la autorización, las claves de cifrado no deben revelarse y deben estar siempre cifradas cuando se envían a través de una red.

### 4.3.10 COMPUTADORES PORTÁTILES

Los usuarios que posean computadores portátiles o de mano que contengan información Confidencial no deben descuidar sus equipos en ningún momento a menos que su información esté cifrada.

Cada vez que información Confidencial o Secreta se guarde en disco flexible, cinta magnética, tarjeta inteligente u otro medio de almacenamiento, el medio debe estar identificado apropiadamente con la clasificación de confidencialidad más alta correspondiente.

### 4.3.11 IMPRESIÓN REMOTA

Las impresoras no deben desatenderse cuando se está imprimiendo o se va a imprimir información y las personas a cargo de ellas deben estar autorizadas para tales efectos. Está permitido que la impresión se haga sin supervisión cuando el área alrededor de la impresora está físicamente protegida de forma que personas no autorizadas para ver el material no tengan acceso a la misma.

### 4.3.12 PRIVACIDAD

Cuando proporciona servicios de red, no suministra servicios de protección de mensajes de manera predeterminada, como por ejemplo el cifrado; no se asume ninguna responsabilidad por la divulgación de la información enviada a través de las redes ni garantiza la privacidad de la información manejada por las redes internas. En los casos en que se requiera el cifrado de la sesión u otros controles especiales, el usuario es responsable de garantizar que se tomen medidas de seguridad adecuadas.

### 4.3.13 REGISTROS Y OTRAS HERRAMIENTAS DE SEGURIDAD EN SISTEMAS

Todo sistema de comunicaciones o de computación multiusuario debe incluir suficientes herramientas automatizadas para ayudar al administrador del sistema a verificar el estado de la seguridad del mismo, como por ejemplo mecanismos para el registro, detección y corrección de problemas de seguridad comúnmente encontrados.

Cuando los costos sean justificables, estas herramientas automatizadas deben usarse en las redes y los computadores. Por ejemplo, debe usarse con regularidad

un software que verifique en forma automática las licencias del software de los computadores personales a través de una red de área local.

Hasta donde el software lo permita, los sistemas de comunicaciones y de computación que manejan información confidencial, valiosa o crítica deben registrar correctamente todos los eventos significativos en materia de seguridad, como por ejemplo los cambios de identificador de usuario durante una sesión en línea, los intentos por descifrar contraseñas, los intentos de usar privilegios no autorizados, las modificaciones a las aplicaciones de producción, las modificaciones del software del sistema, los cambios en los privilegios del usuario y en las configuraciones del sistema de registro.

Los registros que contienen sucesos de seguridad significativos en los computadores o sistema de comunicaciones deben retenerse por un periodo mínimo de tres meses durante el cual los registros deben guardarse de manera tal que no puedan modificarse y únicamente las personas autorizadas puedan leerlos.

Cuando se sospeche que se ha cometido un delito o un abuso relacionado con algún computador o la red, la información pertinente debe capturarse y almacenarse adecuadamente fuera de línea hasta que se determine que no

tomará acciones legales o usará la información de alguna otra manera. La información que debe recogerse de inmediato incluye los registros del sistema, pistas para la auditoría de las aplicaciones, otros indicios de los estados actuales del sistema y copias de todos los archivos relacionados.

El personal de operaciones de computación, de seguridad informática o de administración de sistemas, debe revisar periódica y oportunamente todos los registros que reflejen sucesos significativos en materia de seguridad.

Los usuarios deben ser informados de los actos específicos que constituyen violaciones en la seguridad de los computadores y las redes y de que dichas violaciones serán registradas.

Aunque no es necesario que los administradores del sistema carguen con prontitud la versión más reciente de los sistemas operativos, sí tienen que aplicar todos los parches de seguridad a los sistemas operativos que han sido dados a conocer por grupos de usuarios expertos y confiables, autoridades conocidas en seguridad de los sistemas o el proveedor del sistema operativo.

Los metadatos en los documentos ofimáticos pueden ser especialmente sensibles y revelar información no deseada. Conocer qué información se almacena en un

documento que va a ser publicado o enviado a otra persona es de vital importancia. Antes de entregar un archivo es recomendable asegurarse de qué información se está entregando. Para ello se hace uso de una de las herramientas desarrolladas por Informática 64, como es el caso de MetaShield para IIS 7 capas de eliminar metadatos de los documentos Ofimáticos. De este modo con solo instalar este módulo todos los documentos accesibles públicamente a través de un portal no contendrán metadatos. Al hablar de portal se le podría instalar a la salida del Servidor Proxy de la Escuela de Sistemas.

MetaShield protector puede limpiar los siguientes tipos de documentos:

- Microsoft Office de la versión 97 a la 2007
- OpenOffice
- Portable Document Format (pdf), wpd y jpg

Otra aplicación que brinda limpieza de documentos Ofimáticos OOMetaExtractor, esta herramienta permite la eliminación de metadatos en documentos Open Ofice

Los ataques Man In The Middle utilizando la técnica de ARP Spoofing son unos de los métodos más utilizados por usuarios malintencionados para robo de todo tipo

de datos en una red. Para la mitigación de este tipo de ataque se utiliza una herramienta ***Marmita*** que mediante el análisis de paquetes y el estudio de las direcciones ARP que se asocian a un ordenador es capaz de identificar si un usuario está siendo atacado.

Marmita funciona a la escucha de los paquetes de la interfaz de red seleccionada y analizando aquellos paquetes bien sean ARP o DHCP en busca de posibles ataques MITM. Cuando detecta un ataque muestra una alerta y la información del atacante que haya podido obtener.

La herramienta permite varias configuraciones, pudiendo elegir los tipos de ataques que se desean detectar, si se desea que se mitiguen los ataques ARP Poisoning, así cómo la posibilidad de iniciar Marmita con Windows lo que implica la factibilidad del uso de esta herramienta ya que la mayor parte de los PC's están bajo la plataforma de Microsoft.

### 4.3.14 MANEJO DE LA INFORMACIÓN DE SEGURIDAD DE LA RED

Cada cierto tiempo, se designará a personas para auditar el cumplimiento de ésta y las otras políticas relacionadas con la seguridad de la red y de los

computadores. Igualmente, todo usuario debe reportar con prontitud cualquier sospecha de problemas en la seguridad de la red, incluyendo intromisiones y situaciones de incumplimiento.

Siempre y cuando no hubiere habido intención de dañar los sistemas, no se tomarán acciones disciplinarias si los usuarios reportan una infección por virus de un computador inmediatamente después de haberlo notado, aun cuando haya habido negligencia de su parte.

Todas las fallas en el funcionamiento del software de sistemas o de la red deben reportarse inmediatamente al encargado de la red.

La información sobre las medidas de seguridad para los sistemas de comunicación y los computadores es confidencial y no debe ser revelada a personas que no sean usuarios autorizados de los sistemas mencionados, a menos que se haya obtenido el permiso.

### 4.3.15 SEGURIDAD FÍSICA DE LOS EQUIPOS DE COMPUTACIÓN Y DE COMUNICACIONES

Todo equipo de red debe asegurarse físicamente con dispositivos antirrobo. Además deben usarse controles adicionales de acceso físico, por ejemplo, los servidores de red de área local deben colocarse en gabinetes, armarios o salas de computación cerrados.

El acceso a las oficinas del personal de desarrollo de sistemas, a los armarios con cableado de teléfono, a las salas de computadores, a las salas de comunicaciones y otras áreas de trabajo en donde se maneje información Confidencial o Secreta debe restringirse físicamente.

### 4.3.16 EXCEPCIONES

El encargado de red reconoce que en circunstancias poco usuales, algunos usuarios necesitarán emplear sistemas que no estén conformes con estas políticas. Todos esos casos deben ser autorizados por escrito y con antelación.

### 4.3.17 VIOLACIONES

Todo trabajador que por voluntad propia y deliberada viole esta política, estará sujeto a acciones disciplinarias.

### 4.3.18 GLOSARIO

Administrador del sistema: Persona designada que tiene privilegios especiales sobre sistemas de computadores multiusuario y que vela por la seguridad del mismo y otros asuntos administrativos.

Cifrado: Proceso que incluye la codificación de datos, con el objeto de lograr confidencialidad, anonimato, marca de hora y fecha (time stamping) y demás objetivos de seguridad.

Clave de cifrado: Clave secreta o cadena de bits que se utiliza para controlar el algoritmo que rige un proceso de cifrado.

Computador independiente: Computador que no se encuentra conectado a una red o a cualquier otro computador, por ejemplo, un computador personal independiente.

Contraseña: Cualquier sucesión secreta de caracteres que se utilizan para identificar de manera positiva al usuario o proceso computarizado.

Contraseña compartida: Contraseña conocida o utilizada por más de una persona.

Control de Acceso: Sistema utilizado para restringir las actividades de los usuarios y los procesos de acuerdo con la necesidad de conocer.

Control de acceso basado en contraseñas: Software que depende de las contraseñas como mecanismo primario para controlar los privilegios en el sistema.

Copias maestras del software: Copias del software que se encuentran retenidas en un archivo y que no son utilizadas para las actividades normales.

Cortafuego: Barrera lógica que evita que los usuarios de computadores o procesos computarizados vayan más allá de un punto determinado de la red, salvo que estos usuarios o procesos hayan pasado por cierta verificación de seguridad, tal como suministrar una contraseña.

Cronograma de retención informática: Listado formal de los tipos de información que se deben retener con fines de archivo y los periodos de tiempo que deben guardarse.

Enrutador: Dispositivo que interconecta las redes utilizando distintos estratos del Modelo de Referencia de Interconexión de Sistemas Abiertos (Open Systems Interconnection (OSI)).

Identificador de usuario: Se conoce también como cuentas; son sucesiones de caracteres que asignan una identificación particular a los usuarios de computadores o procesos computarizados.

Identificador de usuario privilegiado: Identificador de aquel usuario a quien le ha sido otorgada la facultad de realizar actividades especiales, tal como apagar un sistema multiusuario.

Información secreta: Información particularmente sensible cuya divulgación significa un grave problema de seguridad.

Información crítica: Cualquier información esencial para las actividades cuya destrucción, modificación y falta de disponibilidad ocasionarían una grave interrupción de las mismas.

Mensaje de bienvenida: Mensaje inicial que se le presenta a un usuario cuando se conecta con un computador.

Parche de Seguridad: Software que se utiliza para resolver problemas de seguridad, o de otro tipo, que se aplica comúnmente a los sistemas operativos, sistemas de administración de bases de datos y otros.

Privilegio: Facultad concedida para realizar ciertas acciones en un computador, tal como leer un archivo específico del computador.

Protector de pantalla: Programa de computador que blanquea automáticamente la pantalla del monitor de un computador, luego de un determinado periodo de inactividad.

Proceso de Inicio (y sus derivados): Proceso de inicialización de un sistema de computadores, desde el momento en que éste se encuentra apagado o desconectado.

Puerta de enlace: Sistema computarizado utilizado para conectar redes y que puede restringir el flujo de información y emplea algunos métodos de control de acceso.

Privilegio especial en el sistema: Privilegios de acceso al sistema que permiten al usuario o proceso involucrado realizar actividades que normalmente no son otorgados a otros usuarios.

Reinicialización de contraseña: Asignación de una contraseña temporal a aquel usuario que olvida o extravía su contraseña.

Sistema de computadores multiusuario: Cualquier computador que pueda soportar a más de un usuario simultáneamente.

Software antivirus: Software disponible a nivel comercial que busca ciertos patrones de bits u otras evidencias de infección de virus en un computador.

Usuario final: Usuario que emplea los computadores y que actúa como fuente o destino de la información que fluye a través de un sistema de computadores.

Verificación de condición de seguridad: Proceso mediante el cual se garantiza que los controles están instalados y funcionan correctamente.

## CONCLUSIONES

- Por medio del análisis de vulnerabilidades, del cual se desprende que dentro de la infraestructura de red de la Escuela de Ingeniería en Sistemas de la ESPOCH existen efectivamente vulnerabilidades tales como desbordamiento de buffer en el servicio de netbios, envenamiento ARP, dns spoof entre las principales, las cuales siguiendo la metodología de un profesional de seguridad (hacker ético) se ha llegado a explotar un numero limitado de dichas deficiencias de seguridad; para prevenir futuros ataques se ha llevado a cabo una propuesta de best practice para la mitigación de las deficiencias de seguridad.

- Se utilizó la metodología de hacker ético con lo que se ha logrado un análisis exhaustivo de la infraestructura de red, protocolos involucrados y aplicaciones en uso por los sistemas informáticos de la Escuela de Sistemas de la Escuela Superior Politécnica de Chimborazo, con lo información obtenida se ha realizado una propuesta de mejoras basada en el Estándar Internacional ISO/IEC 17799 que sirva como guía para reducir las deficiencias de seguridad dentro de la infraestructura de red.

- De acuerdo al análisis de vulnerabilidades se determino que existe un 4% de los equipos analizados con alto riesgo de ser victima de un ataque relacionado a sus vulnerabilidades, entre la vulnerabilidades más criticas se encontró el desbordamiento de buffer en el servicio smb del puerto 445 MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote(respuesta a manejo remoto), también vulnerabilidades para diversos pluggins de los navegadores, por lo que es necesario la actualización inmediata del sistema operativo y de sus navegadores con sus pluggins respectivos.

- BackTrack en su distribución 5 ofrece una gran cantidad de herramientas de una forma organizada e intuitiva, muy practica en el momento de realizar el análisis de vulnerabilidades y posteriormente las pruebas de intrusión. Se utilizo herramientas como zenmap que permitió un escaneo de puertos y dio una visión de la infraestructura de red, metaesploit para la explotación de vulnerabilidades halladas con Nessus. Para evitar falsos positivos y lograr una mayor fiabilidad con los resultados obtenidos se realizaron varias pruebas del mismo tipo, además los exploits utilizados en su totalidad son libres.

- Se desarrollo una propuesta de best practice o mejores prácticas para el tratamiento de la información y de los recursos involucrados en la infraestructura de red de Escuela de Ingeniería en Sistemas de la ESPOCH, que permitirá ayudar al fortalecimiento de la seguridad de la información y de la infraestructura de red.

## RECOMENDACIONES

- Se recomienda realizar el mismo estudio de vulnerabilidades en todas las Facultades y Escuelas de Escuela Superior Politécnica de Chimborazo para reducir de forma sustancial el riesgo de sufrir algún tipo de ataque.

- Es importante mencionar además del encargado de la Administración de la Infraestructura de Red debe existir un Profesional calificado en materia de seguridad tanto de la información, el cual contemple los conocimientos necesarios y siempre se mantenga actualizándose, ya que se encuentran cada vez un mayor numero de vulnerabilidades que pueden ser explotadas.

- Debe existir un compromiso tanto por las autoridades y los encargados de Sistemas Informáticos en cumplir y hacer cumplir las políticas de seguridad planteadas para lograr una mayor eficiencia en la mitigación de riesgos dentro de la infraestructura de red.

- Se recomienda la implementación de sistemas de detección de intrusos para prevenir diferentes ataques como denegación de servicio o desbordamiento de buffer. Además de agregar herramientas como marmita para la mitigación de ataques de hombre en le medio.

- Se recomienda la migración del servicio Telnet hacia uno encriptado como es SSH, ya que Telnet envía su información en texto plano y se podría interceptar la información y acceder a ella.

## RESUMEN

Investigación para realizar un análisis de vulnerabilidades y proponer una guía de mejores prácticas de los laboratorios en la Escuela de Ingeniería en Sistemas, ESPOCH.

Se utilizó la distribución de software libre Backtrack 5, conjunto de herramientas para comprobar seguridad informática o vulnerabilidades en la infraestructura de red o sistemas de información, mediante aplicación de metodología de profesional de seguridad o hacker ético que se basa en un análisis inductivo deductivo.

El análisis de vulnerabilidades determino que existe un 4% de equipos se hallan en alto riesgo de sufrir un algún tipo de ataque, el 8% están en riesgo medio y los restantes en bajo riesgo, para lograr una mayor confiabilidad de estos resultados se procedió a efectuar al menos dos veces cada tipo de ataque informático utilizando metaexploit, para luego proponer una metodología de mejores practicas para la seguridad de la información siguiendo los lineamientos del Estándar Internacional ISO/IEC 17799, lo que permitirá mitigar las deficiencias de seguridad.

El haber aplicado metodología de hacker ético propuesta se logró realizar análisis minucioso de la infraestructura de red, de los protocolos involucrados y aplicaciones en uso de los sistemas informáticos de la Escuela de Sistemas.

Se recomienda a los administradores de red implementar las políticas propuestas de mejores prácticas de seguridad de la información aquí planteadas.

## SUMMARY

This research was done for making a vulnerability analysis and a proposal guide to develop better practices in laboratories of the Systems Engineering School of the ESPOCH.

Free software Backtrack 5 was used, as a set of tools for checking vulnerabilities in computer security or network infrastructure or information systems, by applying a professional safety methodology, ethical hacker, based on a deductive-inductive analysis.

The vulnerability analysis determined that there is a 4% of equipment's which are in high risk of attack; 8% are in medium risk and the remaining ones are in low risk. To achieve greater reliability from these results, at least two times of each type of computer attacks was done, using metaesploit to propose a methodology with better practices for information security; following the guidelines of International Standards ISO/IEC 17799, which will help to mitigate safety deficiencies.

By applying the methodology proposed as an ethical hacker, a thorough analysis of network infrastructure was achieved; protocols and applications that are in use in the computer systems in the Systems School.

It is recommended to the network administrators, to apply these proposed policies which set the best practices in information security.

## BLIOGRAFÍA


1 **THOMAS WILHELM.** Professional Penetration Testing. USA, Elsevier, 2010, P gs.197-214.

2 **COORDINACIÓN DE EMERGENCIA EN REDES TELEINFORMÁTICAS DE LA ADMINISTRACIÓN PÚBLICA ARGENTINA**. Manual de Seguridad en Redes. Argentina-Buenos Aires, ArCERT, 2002, Pgs. 2.1 – 3.10.

3 **SHAKEEL ALI &TEDI HERIYANTO**, BackTrack 4: Assuring Security by Penetration Testing, BIRMINGHAM – MUMBAI, 2011, Pgs. 9-345.

4 **CHARLES CRESSON WOOD**, Políticas de Seguridad Informática - Mejores Prácticas Internacionales, Estados Unidos de America, 2002, Pgs. 555–567

## BIBLOGRAFÍA DE INTERNET


5 . **HERRAMIENTAS DE HACKING**

http://www.informatica64.com/herramientas.aspx

2011-10-12

http://es.scribd.com/doc/73364142/19/DNS-spoofing-con-Ettercap-y-Metasploit

2011-10-15

http://foros.hackerss.com/index.php?showtopic=2788

2011-10-17

6 **INTRUSIÓN DE SISTEMAS INFORMÁTICOS**

http://www.offensive-security.com/metasploit-unleashed/Main_Page

2011-11-1

http://www.metasploit-es.com.ar/wiki/index.php/Mass-Client_Attack

2011-11-18

http://www.danscourses.com/Network-Penetration-Testing/client-side-exploits-using-metasploit.html

2011-11-24

# 7 REPORTE DE PENTEST

http://www.pentest-standard.org/index.php/Reporting

2012-01-15

http://www.segu-info.com.ar/politicas/seguridad

2012-01-18