PHLAK COMO HERRAMIENTA DE SEGURIDAD

Ing. Johana Katerine Guzmán. Autor 1, Ing.Luis Miguel Rodríguez. Autor 2, Ing. Milton Quiroga. Asesor
Enero de 2006, joh-guzman@uniandes.edu.co, luis-ro1@uniandes.edu.co,
mquiroga@uniandes.edu.co

Resumen – **En este documento se analiza la importancia y utilidad del paquete Phlak como herramienta de seguridad, mediante el estudio de las herramientas que los autores consideran más importantes: metasploit, nessus, netcat, hydra, nmap y ethercap. Se hace un estudio de su manejo y su aplicación practica, con base en lo cual se demuestra la gran utilidad de estas herramientas para detectar vulnerabilidades en redes de computadores.**

Palabras clave – redes, seguridad

I. INTRODUCCION

Uno los riegos mas grandes a los que están sometidas las redes de computadores existentes es la de ser atacados por individuos denominados hackers, con algunos objetivos como son adquirir información ajena y afectar el correcto funcionamiento de la maquina atacada.

Para enfrentar este tipo de problemas los administradores de redes han recurrido a diferentes tipos de tecnologías como son firewalls, software antivirus, uso de certificados de acceso, etc. Estas son algunas medidas defensivas con las cuales el administrador espera estar debidamente protegido.

Ahora surge un nuevo tipo de medida de seguridad más ofensivo que consiste en el uso por parte de los administradores de red de herramientas que les permiten auto-atacarse y determinar las vulnerabilidades existentes en su propia red antes de ser atacado por un agente externo, esta es la verdadera fortaleza de conocer estas herramientas.

Este tipo de herramientas generalmente son de carácter comercial y el usuario tiene que pagar por su adquisición y actualización. Recientemente han surgido un tipo de herramientas que son de código abierto, es decir son de carácter público y gratuito que pueden ser descargadas para su instalación, Actualización y posterior estudio por parte de los usuarios desde Internet. Este es el caso del paquete phlak, un software de seguridad que trabaja en ambiente linux. Consta de diferentes módulos para la detección de vulnerabilidades ya conocidas, puertos abiertos para la penetración de agentes externos, etc.

Este documento busca hacer un estudio de la sencillez y utilidad del software Phlak para efectos didácticos en lo que se refiere al tema de seguridad de redes de computadores. Para esto se han escogido las cinco herramientas diversas que se consideraron las más importantes: metasploit, nessus, netcat, hydra, nmap y ethercap.

Para cada herramienta se describe sus características mas importantes y su utilidad, con base en lo cual se dan unas conclusiones y recomendaciones.

Metasploit: Herramienta que permite ejecutar ataques a sistemas remotos por medio del uso de scripts o códigos diseñados en lenguajes de programación como c++, assembler o perl, éstos con llamadas exploits y payloads.

Nessus: Herramienta que permite detectar vulnerabilidades en sistemas remotos mediante el uso de plugins.

Netcat: Esta herramienta llamada la navaja suiza de los administradores, su mayor atractivo es la capacidad de leer y escribir datos a través del protocolo TCP y UDP. Netcat tiene muchas aplicaciones para los administradores de redes, entre las más destacadas están: scaner y redireccionar de puertos, escuchar puertos, etc.

Nmap: Herramienta sencilla que permite el scaneo de computadores a nivel de dirección IP y de puerto.
Hydra: Su mayor atractivo es proporcionar buenas herramientas para "adivinar login y password validos para un servidor objetivo. Hydra ayuda a encontrar passwords vulnerables en la red.

Ethercap: Nace como sniffer, pero rápidamente se ha convertido en una poderosa herramienta para ataques "man in te middle".

II. HERRAMIENTAS

Phlak (Professional Hacker's Linux Assault) es una reciente distribución Linux que tiene un entorno amigable, el cual ofrece diversas posibilidades de exploración. Esta herramienta se ofrece de manera gratuita en la web y tiene la posibilidad de ser utilizada desde un medio de almacenamiento externo, booteando desde un CD, detectando el hardware del PC cada vez que se arranca, usando la memoria RAM para leer y guardar datos.

Phlak se especializa en realizar diagnósticos, auditorias de seguridad y análisis forense. Este completo paquete de seguridad contiene sniffers, herramientas para el análisis de protocolos, cifrado de ficheros, etc.

a) METASPLOIT

Metasploit es actualmente una de las herramientas más utilizadas en seguridad informática, contenidas en phlak, para el desarrollo de exploits, payload e investigación de vulnerabilidades.

En Metasploit existen varias consolas de trabajo: **MSFUpdate, MSFConsole, MSFWeb** y **Cygshell. MSweb** esta en desarrollo y implementación resulta interesante ya que la selección de exploits y payload resulta más eficiente. Metasploit también se puede ejecutar desde windows La ventana principal de comandos es MSFConsole:

Para entrar a msfconsole, basta con ingresar a la ventana de comandos de phlak, y ejecutar msfconsole.

Con el propósito de visualizar todos los exploits disponibles, se ejecuta en la ventana de comandos: show exploits.

Para seleccionar uno de la lista, se ejecuta: use exploit seleccionado, en este caso se ha seleccionado msrpc_dcom_ms03_026. Después de realizar la selección del exploit el prompt se modifica.

El exploit seleccionado realiza un ataque al subproceso de Windows llamado RPC, es el exploit llamado msrpc_dcom_ms03_026. El tipo de vulnerabilidad que se va a explorar consiste en aprovechar errores en el filtrado de las entradas del usuario en las aplicaciones. Para esto se emplean técnicas para inyectar código ejecutable en el cliente o código ejecutable en el servidor.

El nombre genérico de este subsistena es DCE RPC, el cual ha tomado el nombre de MSRPC para Windows. DCE RPC se ocupa de implementar la comunicación entre cliente y servidor de una aplicación a través de RPC. RPC proporciona a los usuarios la posibilidad de iniciar una interacción entre cliente y servidor, al igual que un proceso de llamada. Este es un protocolo utilizado para permitir que un programa que se ejecuta en un equipo, pueda acceder a los servicios de otro equipo conectado a la red. El puerto 135 correspondiente al Proceso RPC Llamada a Procedimiento Remoto, o Remote Procedure Call. En realidad este proceso existe en otros sistemas operativos, y su función siempre suele ser la misma: habilitar conexiones entre Programas y Conexiones remotas sin tener que entender un protocolo de comunicación entre redes. Windows XP no ofrece posibilidad de cerrar este puerto, por su arquitectura, a menos de que se utilice un firewal.

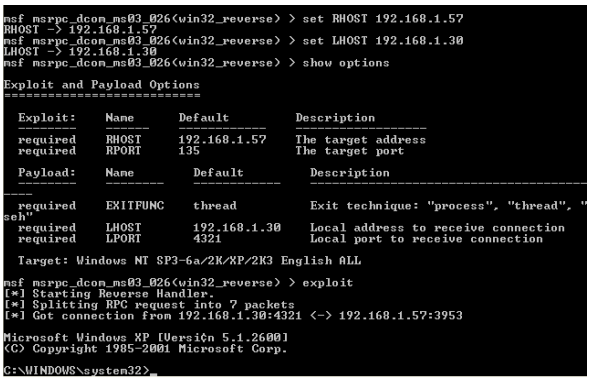
Después de seleccionar el payload, el código que se ejecutará en el PC remoto. En este caso se ha seleccionado "win32_reverse". Para realizar la configuración del ataque es necesario configurar los parámetros necesarios solicitados por el

payload: para este caso los parámetros se configuración son:
RHOST, RPORT, EXITFUNC, LHOST, LPORT.

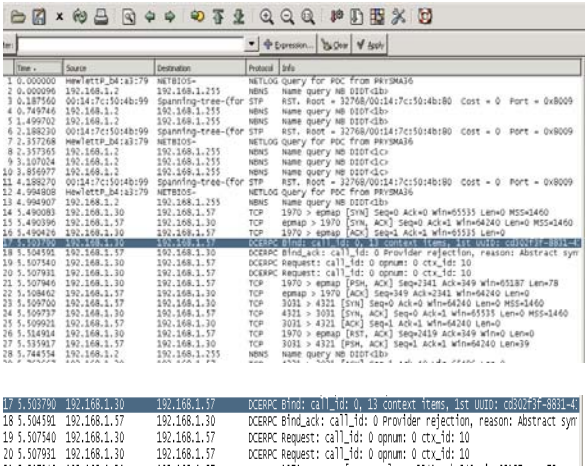
RPORT y LPORT, se pueden dejar con el valor por defecto. El parámetro target también es modificable y esta relacionado con el sistema operativo a quien va dirigido el ataque.

Para configurar los datos del ataque se emplea el comando set. Para este caso es importante diferenciar las mayúsculas de las minúsculas.

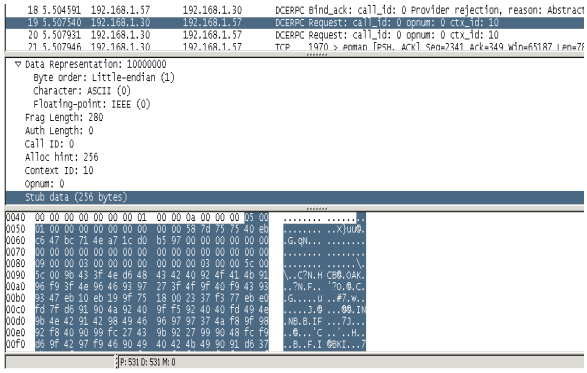
Y finalmente se ejecuta el comando EXPLOIT que hará que se ejecute el código del payload en el Pc remoto. En este momento se ha entrado al Pc remoto. Ya estamos en el sistema operativo.



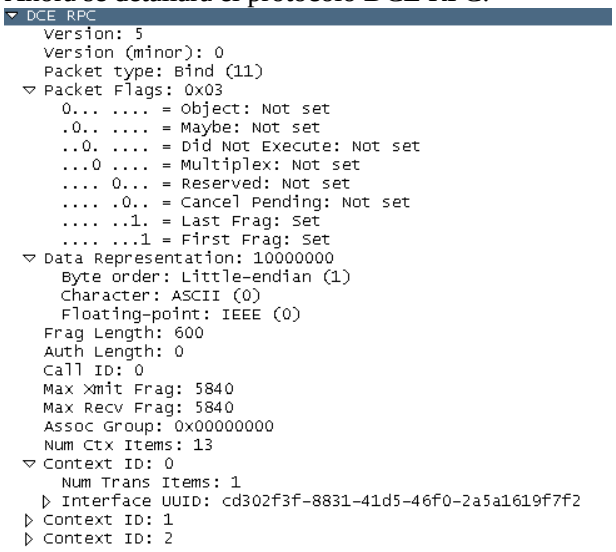
Ahora se puede entrar a analizar lo que ha pasado con el ataque, la siguiente es una captura de ethereal.



En los bytes correspondientes al protocolo RPC se observa la ráfaga de caracteres que hacen el overflow, que aparecen señalados en el código del exploit:



Ahora se detallará el protocolo DCE RPC:



A continuación, se detallan algunos de los campos más importantes:
Versión: Es la versión del protocolo RPC, es no-negativo y entero.
Packet Type: Esta encriptado en los últimos bits significativos.
Flags: Cada bandera tiene 8 Bit, y son usados para el control del protocolo.
Data Representation: Son 4 bytes, aunque solo se usan tres, es el formato que debe ser validado por el recetor
Context ID: Es un identificador de objeto, contiene un UUID que únicamente identifica el objeto con el cual el procedimiento de llamada remota esta

operando. Si la llamada no es operada por el objeto, es te tiene un campo nulo en el UUID.
Interface Identifier: Es un UUID, que identifica la interface que esta siendo llamada.
Interface Version: Es un campo de 32 Bits, esta relacionado con el numero de la versión de la interface que esta siendo llamada.

b) NETCAT

Netcat, es una de las herramientas más populares de Phlak, llamada la navaja suiza de los administradores, tiene como su mayor atractivo la capacidad de leer y escribir datos a través del protocolo TCP y UDP. Netcat tiene muchas aplicaciones para los administradores de redes, entre las más destacadas están: escaner y redireccionar de puertos, escuchar puertos, etc. En muchas de estas aplicaciones, Netcat no es la mejor herramienta, pero lo más interesante es que se puede emplear para muchos de éstos propósitos. Esta herramienta viene en Phlak, también se consigue de manera gratuita en Internet para Windows. Esta aplicación se puede trabajar desde MS-DOS en Windows o desde la ventana de comandos en Linux.

El principal comando en Netcat es nc. El formato es el siguiente:

nc [-opciones] hostname [puertos] [puertos] ...

NETCAT Como Port Scanner

Netcat con sus múltiples opciones, permite realizar un gran número de combinaciones, como escaneo aleatorio, ascendente, descendente, con intervalos de tiempo y a través de gateways.

```
C:\>nc -v -v -z 192.168.1.67 1-100
COMUNICACIONES [192.168.1.67] 100 (?): connection refused
COMUNICACIONES [192.168.1.67] 99 (?): connection refused
COMUNICACIONES [192.168.1.67] 98 (?): connection refused
COMUNICACIONES [192.168.1.67] 97 (?): connection refused
COMUNICACIONES [192.168.1.67] 96 (?): connection refused
COMUNICACIONES [192.168.1.67] 95 (?): connection refused
```

Se puede observar en una captura de tráfico que el equipo origen envío datagramas a el rango de puertos, de manera descendente.

Netcat Como Sniffer

Esta es otra aplicación de Netcat, se pueden escuchar conexiones en cualquier puerto, adicionalmente es posible redireccionar todo el tráfico hacia un archivo a la pantalla:

```
C:\>nc -v -v -L 192.168.1.40  -p 80
listening on [any] 80 ...
```

En este caso hemos direccionado la captura del tráfico al archivo login.txt. Y Netcat informa de las novedades ocurridas en el puerto 23.

Otras Aplicaciones Con Netcat

Si bien es cierto, que existen otras aplicaciones que son más eficientes en scaneo como Nmap o en examinar las vulnerabilidades como Nessus, la gran ventaja de Netcat es que tiene diversas aplicaciones, incluso esta incluido en el código de muchos exploits. Los usos de Netcat dependen de las necesidades del administrador y de la imaginación. Ahora se verá una pequeña pero interesante aplicación de Netcat, como un primitivo Chat.

Esta aplicación se inicia programando a netcap para escuchar por el puerto 4000. Así que todo lo que entre a este puerto se puede estar visualizando, así mismo recibimos una conexión de 192.168.1.67.

Situados en 192.168.1.67, estamos realizando una conexión al puerto 4000 de 192.168.1.65, desde un puerto no especificado.

```
C:\Documents and Settings>cd..

C:\>cd netcat

C:\Netcat>nc 192.168.1.65 4000
hhhhlll
jjfg
hola
kjhkhklk
uihhlk
jkjkhk
jhhhj
```

Por medio de Ethereal se puede ver que, los datagramas enviados desde este.

Desde la estación origen, salen por el puerto 4000 hacia el puerto 2037 de la estación destino. Es así como se establece una conexión peer to peer a través del 4000 entre los dos PC's

c) HYDRA

THC – Hydra, fue creado por The Hackers Choice (THC), es soportada por Unix, Windows y Palm. Hydra es un crakeador remoto, que también funciona en windows. La única diferencia es que desde Windows no se maneja entono gráfico. En general lo que hace Hydra es realizar combinaciones de login y passwords hasta acertar. Esta operación lógicamente requiere tiempo y recursos de máquina. Las principales características de este crakeador, considerados por muchos como una de los mejores, son las siguientes:

- Soporta múltiples protocolos, como Telnet, HTTP, FTP, SSH, POP3, ICQ, LDAP, etc.
- Es muy rápido

Cuando no estoy en phlak, sino desde otro sistema donde no se tiene instado esta herramienta, descargamos desde la página de THC – Hydra el archivo comprimido y seguimos las instrucciones del archivo README.

En Phlak se debe mover el archivo libssh.so a las librerias locales (lib), para que esta herramienta se pueda ejecutar con éxito.

En hydra se debe colocar la dirección del pc donde se ejecutará el ataque. También se especifica el protocolo y el puerto por donde se entrará. En la segunda pestaña PASSWORDS, se entran los posibles password. La mayor efectividad en esto se tiene cuando se ejecuta desde archivos de usuarios y passwords. En TURNING se especifica la velocidad del procesamiento y el tiempo máximo de espera de respuesta. Finalmente START me permite realizar el ataque.

Este ataque fue realizado al puerto 23 (telnet), de una máquina Windows XP. Inicialmente fue necesario configurar todos los servicios de locales de Windows, para que el acceso telnet se realizara desde otro PC. Adicionalmente es necesario deshabilitar el firewalls, pues éste cierra el puerto 23. Cuando se emplean los archivos de usuarios y passwords, hydra realiza todas las combinaciones posibles. Finalmente se obtiene el resultado el ataque:

d) NESSUS

Nessus es una herramienta de seguridad que permite detectar vulnerabilidades ya conocidas en sistemas remotos. Las detección se realiza mediante la ejecución de plugins escritos en lenguaje nasl.

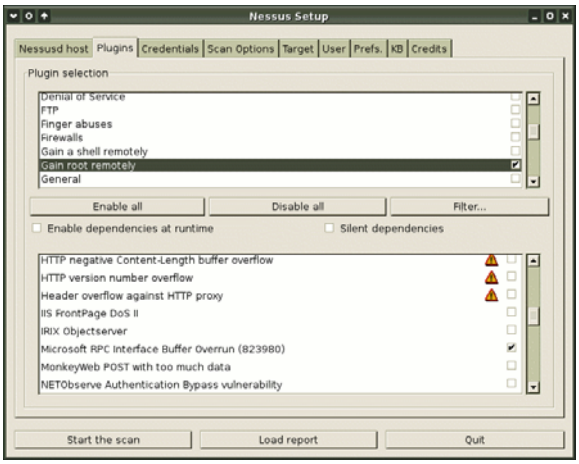
El paquete tiene una arquitectura Cliente-servidor donde el cliente puede estar o no en la maquina donde está instalado el servidor. El servidor corre en ambiente Linux y el cliente puede correr incluso en Windows.

El paquete puede ser descargado incluso de la red libremente para su instalación. EN la pagina WEB acreditada es posible encontrar plugins actualizados con las ultimas vulnerabilidades descubiertas. Esto permite que la herramienta tenga diferentes tipos de usuarios: desde el administrador de redes que quiere auto evaluar la seguridad de sus red, hasta el estudiante que quiere analizar en detalle como se realiza un ataque mediante el uso de las vulnerabilidades.

Los archivos de las vulnerabilidades están escritos en lenguaje NASL que es un lenguaje exclusivo para la creación de ataques con el fin de detección de vulnerabilidades. Su set de instrucciones es muy sencillo, y además de las instrucciones básicas de programación (logicas, aritmeticas, de entrada, de salida, de formato) tambien tiene ordenes realcionadas con el intercambio de paquetes en TCP/IP.

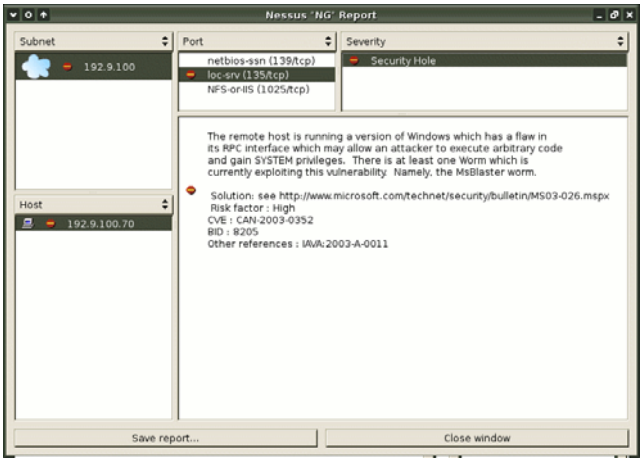
La aplicación permite escoger entre diferentes familias de plugins, y a su vez permite escoger un tipo específico de plugin dentro de cada familia.

Cada plugin tiene un determinado sistema operativo y versión y puertos que son victimas de los ataques. En la siguiente gráfica se muestra la ventana donde se puede escoger el plugin y la familia.



El programa permite la ejecución de más de un plugin al mismo tiempo.

Como practica con esta herramienta se implementó una red local de dos computadoras uno de los cuales tenia Nessus (Phlak) y el otro Windows 2000. Se realizó la detección de la vulnerabilidad "RPC Buffer Overflow".
Efectivamente Nessus detecto dicha vulnerabilidad en el puerto 135, tal como aparece en la siguiente figura:



Durante todo el escaneo de nessus sobre la computadora remota, los autores utilizaron Ethreal para capturar los paquetes intercambiados entre las dos máquinas, y mediante su estudio poder determinar el proceso de deteccion de la vulnerabilidad. Se identificaron tres estapas:

1- Escaneo para saber que puertos están abiertos
2- Revisa la vulnerabilidad en los puertos descubiertos como abiertos.

Por lo tanto se comprobó que Nessus es una herramienta que permite saber que tan segura es una red con respecto a las vulnerabilidades de los sistemas operativos, y a la vez posee una interface de usuario de sencillo manejo que permite en combinación con sniffers hacer estudios profundos de cómo se realizan ciertos ataques.

e) NMAP

Esta es una sencilla herramienta para el scaneo de puertos de un host remoto. Para ejecutar un scaneo se utilizan comandos los cuales permiten utilizar diferentes funcionalidades de la herramienta, como son:

- Escogencia los objetivos del scaneo: desde una lista, excluir elementos, escoger al azar.
- Prueba de los hosts remotos: sacar una lista de los objetivos, hacerles ping solamente, no hacer este paso, hacer o no resolución de nombres por DNS.
- Técnicas de scaneo
- Puertos a escanear y en que orden
- Detección de servicios
- Detección del sistema operativo del host remoto
- Evasion de firewalls and spoofing
- Presentación de salida

La combinación de estas opciones permite al usuario ejecutar scaneos sin ser detectado. Por ejemplo para el tipo de scaneo se tienen diferentes formas de hacerlo de acuerdo al tipo de paquete que se envía al host remoto.

La practica realizada consistió en la conexión directa de un computador con Phlak instalado y en el otro computador se tenía el sistema operativo Windows 98SE. Se ejecutó nmap con la única opción de detectar el sistema operativo y detectar que puertos están abiertos.

Se ejecutó la orden:

Nmap –O 192.9.100.30

donde –O es la opción de detectar sistema operativo y 192.9.100.30 es la dirección IP del host donde estaba instalada la plataforma Windows.

El resultado es la visualización en la linea de comandos de los puertos que estaban abiertos. En este caso nmap detectó que los puertos abiertos eran el 139 con TCP y el servicio netbios—ssn y el 3531 con TCP y peerenabler. Además entregó una indicación de que tipo de sistema posee el host remoto; en este caso el sistema operativo puede ser Microsoft Windows 95/98/ME/NT.

Por medio del análisis de los paquetes intercambiados por ambos computadores se pudo deducir como se produce el scaneo de los puertos por parte de nmap. Primero una barrido de todos los 1665 puertos que escanea el por defecto (pude ser modificado) y después realiza la evaluación del sistema operativo (si esto es necesitado).

f) ETTERCAP

Ettercap es un sniffer/interceptor/logger para redes LAN con switchs, que soporta la disección activa y pasiva de muchos protocolos (incluso cifrados) e incluye muchas características para el análisis de la red y del host (anfitrión)".
Entre sus funciones, las más destacadas son las siguientes:

- Injection de caracteres en una conexión establecida emulando comandos o respuestas mientras la conexión está activa.

- Compatibilidad con SSH1: Puede interceptar users y passwords incluso en conexiones "seguras" con SSH.

- Compatibilidad con HTTPS: Intercepta conexiones mediante http SSL (supuestamente seguras) incluso si se establecen a través de un proxy.

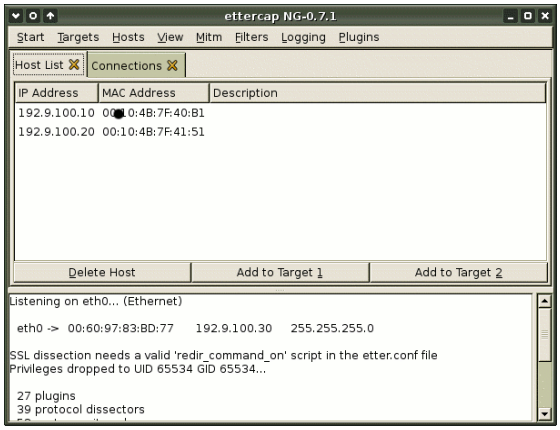
- Intercepta tráfico remoto mediante un tunel GRE: Si la conexión se establece mediante un tunel GRE con un router Cisco, puede interceptarla y crear un ataque "Man in the Middle".

- "Man in the Middle" contra tuneles PPTP (Point-to-Point Tunneling Protocol).

- Soporte DE Plug-ins.

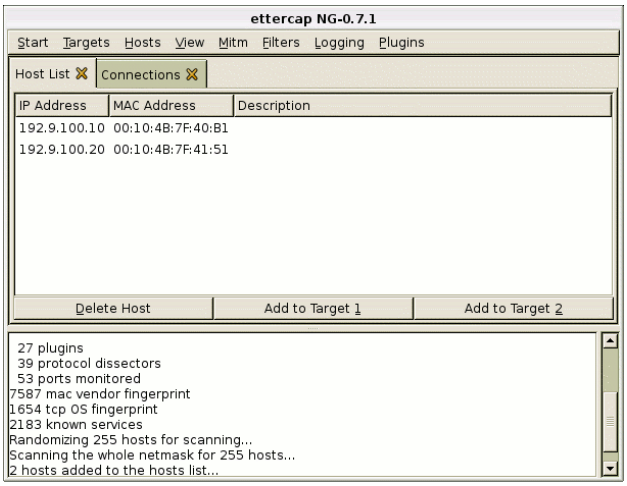
Al igual que nessus y de metasploit sus funciones son cargadas por medio de archivos desarrollados (similares a scripts).

Después de iniciar la aplicación de ettercap en el menú sniff con la opción unified sniffing, aparece otra ventana que es la que se muestra en la siguiente figura:



En esta se puede explicar el manejo básico de ettercap, por medio de los siguientes menús:

Start: Para comenzar o para un sniffing
Targets: Para seleccionar y visualizar los hosts que van a ser objetivos de los ataques.
Hosts: Para buscar, listar o cargar una lista de hosts
View: Para visualizar conexiones en la red, perfiles y estadísticas
Mitm (Man In The Middle): Para seleccionar el tipo de sniffing entre ARP poisoning, ICMP redirect, Port stealing, Dhcp spoofing.
Filters: Para efectuar algún tipo de filtrado sobre los paquetes
Logging: Para la creación de logs de los paquetes o de los mensajes de los usuarios
Plugins: Para cargar y correr algún tipo especifico de plugin



Conclusiones

La exploración por cada una de estas herramientas evidencia la virtud de cada una:

Metaexploit: Permite diseñar y ejecutar exploit de manera singular, permitiendo la ejecución de procesos mediante programación en perh, aseembler o c++.

Netcat: El poder de esta herramienta esta es sus multiples facetas. Además de esto, es especial para profundizar en conocimientos de puertos virtuales.

Hydra: Es uno de los craceadores más versátiles del momento.

Nessus: Detector de vulnerabilidades de sistemas remotos.

Nmap: Escaneador de puertos y detector de sistemas operativos del host remoto.

Este Paper, es una corta exploración con las herramientas más destacadas de Phlak. Se busca evidenciar de los vulnerables que resultan los sistema cuando, se tiene un poco de creatividad e ingenio.

Durante el recorrido por este documento se ha enfatizado en la programación de auditorias que evidencien el estado de vulnerabilidad de la red, pero otro aspecto igualmente importante dentro de los aspectos de seguridad es la capacidad de los administradores de seguridad para reaccionar rápidamente a eventuales ataques.

Se evidencia también que las recomendaciones de los administradores de redes al emplear políticas que contemplan emplear password seguros, cerrar los servicios y conexiones que no se necesiten, no están de más, pues existen diversas herramientas como hydra que encuentran con facilidad password “comunes” en la red.

Conocer que estas herramientas existen y como funcionan es una buena base para sostener una red segura y alejada de los ataques.

REFERENCIAS

www.phalak.org
www.elhacker.net
www.thc-hydra.com
www.microsoft.com

Autor 1. Johana Katerine Guzman, es Ingeniera de Centros de Gestión de LAN SOLUTION Colombia. Es ingeniera electrónica egresada de la universidad Bolivariana (Colombia) con especialización en Finanzas y Proyectos de la Universidad de Antioquia Medellín y especialización en telemática de la Universidad de Los Andes de Bogota (Colombia).

Autor 2. Luis Miguel Rodríguez, es Ingeniero Especialista en Gestión de Sistemas de Transmisión de NERA AMERICA LATINA. Es ingeniero electrónico egresado de la Universidad Distrital Francisco Jose de Caldas de Bogota (Colombia), con especialización en Telemática en la Universidad de los Andes de Bogota (Colombia).