

2. Pasos de un Ataque a la Ciberseguridad

4. Hacking del Sistema

4.1 Introducción

El Hacking del sistema es un gran paso en el sentido en que ya no es el simple escaneo y la enumeración. En este punto, estamos tratando de obtener acceso. Las cosas empiezan a cambiar, porque esta etapa se trata de romper y entrar en el sistema de destino. Los pasos previos, como footprinting, escaneo y la enumeración, son considerados etapas previas al ataque.

El objetivo principal de la fase de hacking del sistema es autenticarse en el host remoto con el más alto nivel de acceso. Este tema cubre algunos ataques de contraseña no técnicos y técnicos comunes contra sistemas de autenticación.

4.2 Ataques no Técnicos a Contraseñas

Los atacantes siempre están buscando formas fáciles de ganar acceso a los sistemas. Hackear los sistemas de autenticación actuales es más difícil porque la mayoría de las organizaciones han mejorado mucho, se utiliza autenticación fuerte y controles de auditoría. Esa es una razón por la que los ataques no técnicos siguen siendo tan populares.

Las técnicas básicas incluyen las siguientes:

- Dumpster Diving: es el acto de mirar en la basura de una empresa para encontrar información que pueda ayudar en un ataque. Se pueden encontrar códigos de acceso, notas, contraseñas, e incluso información de cuentas.
- Ingeniería Social: Veremos más adelante técnicas de Ingeniería Social, pero por ahora basta saber que la ingeniería social es la manipulación de la gente para realizar acciones o para divulgar información confidencial.
- Shoulder Surfing: El acto de mirar por encima del hombro de alguien para obtener información como contraseñas, nombres de usuarios y datos de cuentas.

4.3 Ataques Técnicos a Contraseñas

Estos ataques se basan en la información que hemos obtenido en los pasos anteriores. Las herramientas utilizadas durante la enumeración pueden haber devuelto algunas pistas valiosas sobre cuentas específicas. A estas alturas, podríamos incluso tener los nombres de cuenta, saber quién es el administrador, saber si hay una directiva de bloqueo, e incluso conocer los nombres de los recursos compartidos abiertos.

Las técnicas de ataque de contraseña técnicas discutidos aquí son los siguientes:

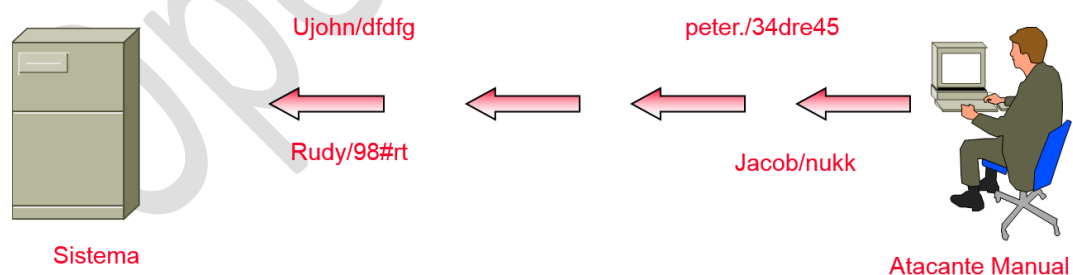
- Password guessing
- Automated password guessing
- Password sniffing
- Keyloggers

4.3.1 Password Guessing

Para adivinar nombres de usuario y contraseñas es necesario que revisemos las conclusiones de los pasos anteriores. Una buena documentación es siempre necesaria durante una prueba de penetración, así que debemos asegurarnos de que hemos documentado todas nuestras actividades anteriores. Cuando adivinamos la contraseña correcta, por lo general es porque la gente prefiere usar palabras y frases fáciles de recordar. Un atacante buscará pistas sutiles a lo largo del proceso de enumeración. ¿Qué sabemos acerca de este individuo?, ¿cuáles son sus aficiones?

Básicamente, el método a seguir es:

1. Encontrar un usuario válido
2. Crear una lista de posibles contraseñas
3. Ordenar las contraseñas por orden de probabilidad
4. Introducir cada contraseña
5. Si el sistema permite la entrada – Éxito, de lo contrario intentamos de nuevo



4.3.2 Automated Password Guessing

Adivinar la contraseña de forma automática puede ser tan simple como crear bucle usando comandos de shell de NT/2000 basado en la sintaxis del comando NET USE.

1. Crear un archivo de nombres de usuario y contraseñas.
2. Introducirlo en un comando FOR

```
C:\> FOR /F "token=1, 2*" %i in (credentials.txt)
```

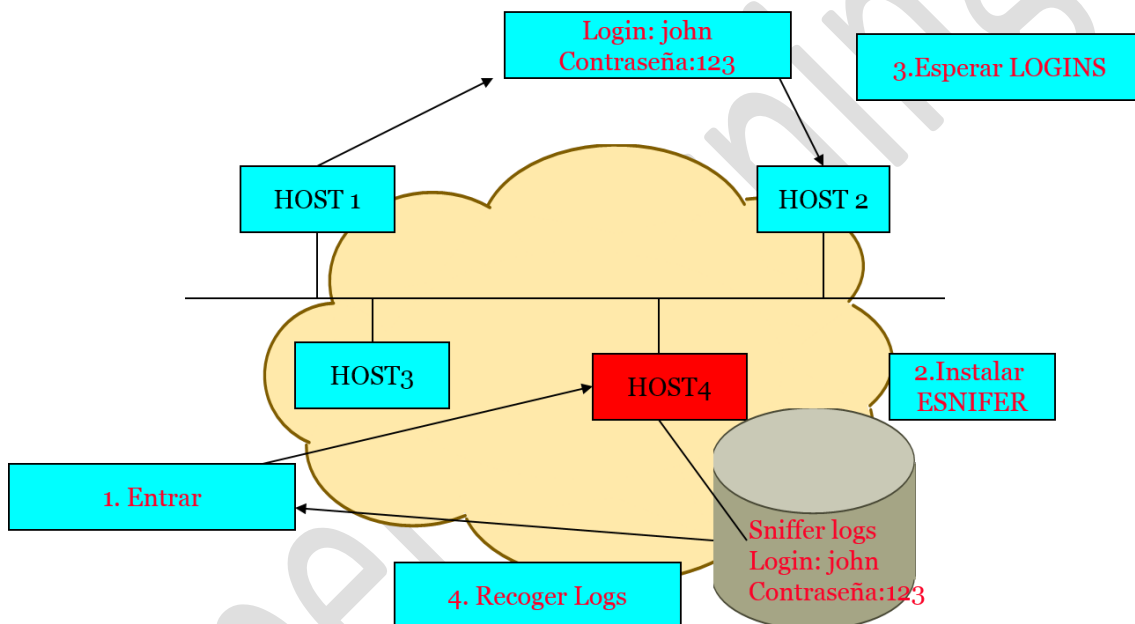
Type net use \\target\IPC\$ %i /u: %j

O bien usar herramientas específicas diseñadas para ello como:

- John The Ripper
- Hydra
- Brutus

4.3.3 Password Sniffing

Si nuestros intentos para adivinar las contraseñas no han tenido éxito, esnifar la red o usar keyloggers podrían ser otra opción. La mayoría de las redes manejan una gran cantidad de tráfico, y una gran parte de él incluso viaja sin ser encriptado. El sniffing de contraseñas requiere que tengamos acceso físico o lógico al dispositivo. Si esto se puede lograr, sólo tiene que esnifar las credenciales en el cable cuando los usuarios inicien sesión.



4.3.4 Keyloggers

Los registradores de pulsaciones de teclas pueden ser software o dispositivos de hardware que se utilizan para supervisar esta actividad. Aunque una persona ajena a la empresa podría tener algunos problemas para instalar uno de estos dispositivos, alguien de dentro se encuentra en una posición privilegiada.

Los keyloggers hardware generalmente se instalan mientras los usuarios están fuera de sus escritorios y son completamente indetectables, a excepción de su presencia física. ¿Cuándo fue la última vez que miramos en la parte posterior de nuestro ordenador?



Incluso entonces, pueden pasarse por alto porque se asemejan a un cable alargador para el teclado o un adaptador; www.keyghost.com tiene una gran colección. Algunos keyloggers de hardware utilizan Wi-Fi, lo que significa que una vez que se implemente el atacante no tiene que recuperar el dispositivo y puede comunicarse con él de forma remota a través de conexión inalámbrica o Bluetooth.

Los keyloggers software se instalan entre el sistema operativo y el teclado. La mayor parte de estos programas de software son simples, pero algunos son más complejos y puede incluso enviar las pulsaciones registradas a una dirección preconfigurada. Lo que todos tienen en común es que funcionan en modo oculto y pueden capturar todo el texto que un usuario introduce. La tabla muestra algunos keyloggers comunes.

Product	URL
ISpyNow	www.ispynow.net
PC Activity Monitor	PCActivityMonitor.org
RemoteSpy	www.remotespy.com
Spector	www.spectorsoft.com
KeyStrokeSpy	www.keylogger-software.com

4.4 Escalado de Privilegios y Explotación de Vulnerabilidades

Si el atacante puede obtener acceso a un sistema como un usuario estándar, el siguiente paso es una escalada de privilegios. Este paso es necesario porque las cuentas de usuario estándar están limitadas, para estar en pleno control, se necesita acceso de administrador. Esto podría no ser siempre una tarea fácil porque las herramientas de escalado de privilegios deben ejecutarse en el sistema de la víctima. ¿Cómo se llega a la víctima para ayudar a explotar una vulnerabilidad? Las técnicas más comunes incluyen los siguientes:

- La explotación de una aplicación
- Engañar al usuario para que ejecute el programa
- Copiar la herramienta de escalada de privilegios en el sistema de destino y programar el exploit para ejecutarse en un momento predeterminado, como el comando AT
- El acceso interactivo al sistema, tales como Terminal Server, pcAnywhere, y otros

4.5 Metasploit

Tal como se menciona en su sitio en Internet, Metasploit Framework, es una avanzada plataforma “Open Source”, diseñada específicamente con el objetivo de potenciar y agilizar, el desarrollo, testeo y utilización de exploits.

El proyecto relacionado con este framework, que según sus progenitores naciera como un juego, ha mostrado un crecimiento espectacular, aspecto que le ha permitido ganarse un lugar privilegiado, dentro del kit de herramientas de todo aquel profesional relacionado de uno u otro modo con las tecnologías de seguridad de la información.

Desde la consolidación de Metasploit Framework, la comparación con productos comerciales de similares características es inevitable. Proyectos tales como CANVAS de Immunity Sec o CORE IMPACT de Core Security Technology, cuentan con una gran clientela que va desde grandes clientes corporativos, quienes hacen uso de estos productos a la hora de realizar sus propios test de penetración, hasta cientos de consultoras de seguridad independiente que lo utilizan como herramienta al momento de vender este servicio a terceros.

Sin dudas, la principal diferencia entre Metasploit Framework y este tipo de productos es el “foco”. Mientras que los productos comerciales necesitan proveer constantemente a sus clientes los últimos exploits acompañados de interfaces gráficas cuidadas e intuitivas, el Framework de Metasploit se encuentra orientado a facilitar la investigación y experimentación con las nuevas tecnologías.

Metasploit Framework, incluye como parte de su distribución, una serie de exploits listos para utilizar. A pesar de ello, existe una comunidad sumamente activa en torno a este producto, que periódicamente libera nuevos exploits, algunos de los cuales pueden ser adicionados fácilmente a nuestro Framework, por medio de una utilidad denominada “msfupdate”, que a partir de la versión 2.2 es incluida como parte de la instalación estándar de Metasploit.

A fin de actualizar en forma on-line nuestro framework, ejecutaremos desde nuestra consola, la mencionada utilidad:

```
root # msfupdate -u
```

Luego de ejecutada, “msfupdate” nos mostrará información acerca de las últimas novedades y pedirá nuestra confirmación a fin de hacer efectivo el update. Terminado el proceso, nuestro framework contará con los últimos exploits disponibles públicamente para Metasploit.

Antes de comenzar, es preciso que conozcamos que Metasploit Framework nos brinda básicamente tres interfaces distintas al momento de interactuar con el mismo:

- Interfaz de Línea de Comando: Es la forma correcta de interactuar con el framework, cuando de automatizar secuencias de pruebas de exploits se trata, o sencillamente en aquellos casos que no se requiera una interfaz interactiva. La utilidad se ejecuta por medio del comando “msfcli”.
- Interfaz de Consola: Probablemente sea esta la interfaz comúnmente utilizada, debido a lo intuitivo de su uso interactivo, la rapidez de su operación y su flexibilidad. Su principal característica es la de brindarnos un prompt de Metasploit, a partir del cual podremos interactuar con cada uno de los aspectos del Framework. En caso de querer hacer uso de este modo, deberemos ejecutar el comando “msfconsole”.
- Interfaz Web: Aunque posee muchos detractores, la interfaz web de metasploit puede ser de suma utilidad en ciertas circunstancias especiales, tal como presentaciones

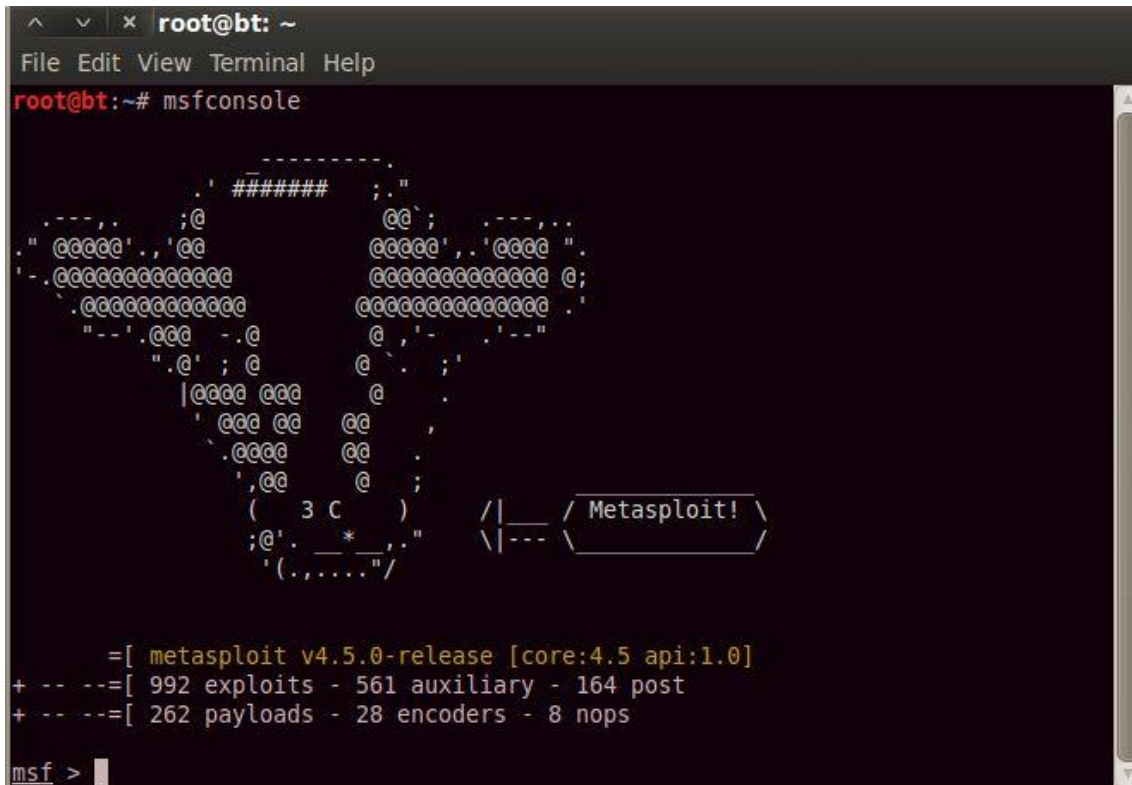
públicas o trabajo en equipo. A tal efecto, esta versión “web” de metasploit, incluye su propio servidor http, a fin de brindarnos la posibilidad de acceder vía navegador a prácticamente las mismas características que en su versión de consola.

Veamos cómo usar de forma básica la consola de Metasploit.

Para acceder a la consola de Metasploit, deberemos ejecutar:

```
root # msfconsole
```

Luego de dar entrada a este comando, nuestra consola mostrara la pantalla de inicio de Metasploit ilustrada en la figura,



```
root@bt:~# msfconsole

-----
  .#####. ;.
  '#####' ;@
  " @@@@' . '@@ @@@@' . '@@@@' .
  '- @@@@@@@@@@@@@ @@@@@@@@@@@@@ @;
  .@@@@@@@@@@@@ @@@@@@@@@@@@@ .
  "'-' .@@@ -' @ @ ' -' .'"
  ".@' ; @ @ @ ' ;'
  |@@@ @@@ @
  ' @ @ @ @
  .@@@ @ @
  ',@ @
  ( 3 C ) /|___ \ Metasploit! \
  ;@' ._*' " \|--- \|
  '(,....."

  =[ metasploit v4.5.0-release [core:4.5 api:1.0]
+ -- --=[ 992 exploits - 561 auxiliary - 164 post
+ -- --=[ 262 payloads - 28 encoders - 8 nops

msf >
```

en la cual se podrá leer a su vez, información tal como la versión instalada, cantidad de Exploits y Payloads disponibles, y un prompt identificatorio (msf >) a partir del cual estaremos en condiciones de dar las indicaciones correspondientes.

El set de comandos disponibles en Metasploit dependerá del contexto, o dicho de otro modo, el listado de los mismos puede variar respecto de la sección del framework en la que nos encontremos. Por tal motivo, el primer comando que ejecutaremos una vez dentro del framework, será sin dudas el comando “help”, el cual nos brindará una breve descripción de cada uno de los comandos y su efecto en el contexto actual (En nuestro caso y por llamarle de algún modo, el directorio raíz).

```
msf > help
```

Lo primero que haremos, será echar un vistazo al listado de exploits disponibles. Para ello deberemos escribir:

```
msf > show exploits
```

Como podremos observar, el listado de exploits es importante.

A continuación seleccionaremos alguno que cumpla con las características necesarias para ser lanzado sobre nuestro equipo de pruebas.

La forma de llevar a cabo dicha tarea es sencilla, tan solo deberemos hacer uso del comando “use” seguido del módulo de exploit a utilizar:

```
msf > use lsass_ms04_011
```

Una instrucción de suma utilidad dentro de la consola de Metasploit, es aquella denominada “info”. Aplicando este comando sobre alguno de los módulos del Framework, a menudo obtendremos información adicional acerca del mismo. En nuestro caso, en respuesta al comando:

```
msf lsass_ms04_011 > info lsass_ms04_011
```

Obtendremos datos tales como el de las versiones de Windows afectadas por la vulnerabilidad de la que se aprovecha este exploit, así como también una descripción general de su utilización, referencias a los boletines de seguridad publicados, nombre de el/los coder's, etc.

Bien, ya hemos hecho nuestra elección respecto de un exploit apto para ser utilizado contra nuestra plataforma de pruebas, ahora deberemos decidir la “Shellcode” o “Payload” que metasploit ejecutará en caso de que la explotación pueda ser llevada a cabo. Otra vez, Metasploit nos brinda muchas posibilidades al respecto. Echemos un vistazo a los “Payloads” disponibles para el exploit seleccionado:

```
msf lsass_ms04_011 > show payloads
```

Siempre podremos utilizar el comando “info” para obtener información adicional del Payload que creamos más conveniente en cada caso.

Probaremos suerte seleccionando “win32_bind”. Si todo sale bien, y de acuerdo a las características de esta shellcode, una vez lanzado el exploit deberíamos poder acceder a una shell sobre el sistema remoto. ¿Cómo hacemos para seleccionarlo? Sencillo, deberemos asignar a la variable PAYLOAD, el valor adecuado mediante el comando “set”:

```
msf lsass_ms04_011 > set PAYLOAD win32_bind
```

Llegado este punto, hemos revisado la lista de exploits y payloads disponibles, obtenido más información acerca de ellos y configurado nuestras preferencias (Exploit: lsass_ms04_01, Payload: win32_bind), ahora veamos las opciones que nos quedan por completar. Para dicha tarea tan solo tendremos que solicitar al Framework que nos muestre las opciones disponibles para el entorno seleccionado:

```
msf lsass_ms04_011 (win32_bind) > show options
```

Si prestamos un poco de atención, veremos que la información brindada por este comando, nos permite conocer las variables/opciones disponibles a la hora de configurar la dupla exploit/payload que estamos a punto de ejecutar. En muchos casos, alguna de las opciones requeridas se completara con valores por defecto en forma automática, aunque siempre habrá que configurar por ejemplo, aspectos tales como la dirección IP de nuestro TARGET (RHOST). Del mismo modo podríamos si quisiéramos cambiar el puerto de escucha propuesto por defecto por el framework (LPORT).

<http://www.openlearning.es>

Set es nuevamente el comando a utilizar. Si en nuestro entorno de pruebas, el target se encuentra tras la IP 172.16.1.96, debemos dar entrada al siguiente conjunto de comandos:

```
msf lsass_ms04_011 (win32_bind) > set RHOST 172.16.1.96
```

```
msf lsass_ms04_011 (win32_bind) > show options
```

Con el primero hemos definido el host destino, y con el segundo verificaremos que no nos estamos olvidando de suministrar ningún parámetro antes de lanzar mi exploit.

Ahora solo deberemos ejecutar el exploit con el comando “exploit” y esperar a que todo haya salido como lo planeamos:

```
msf lsass_ms04_011 (win32_bind) > exploit
```

Esto es solo una pequeña muestra de lo que se puede hacer con Metasploit. Tenemos mucha más información y más detallada en:

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

4.6 Mantener el Acceso

Una vez el atacante gana acceso al sistema objetivo su prioridad es mantener el acceso que ha obtenido en el sistema. En esta fase el atacante usa sus recursos y recursos del sistema y usa el sistema objetivo como plataforma de lanzamiento de ataques para escanear y explotar a otros sistemas que quiere atacar, también usa programas como sniffers para capturar todo el tráfico de la red, incluyendo sesiones de telnet y FTP (File Transfer Protocol).

En esta fase el atacante puede tener la habilidad de subir, bajar y alterar programas y datos.

El atacante querrá permanecer indetectable y para eso puede hacer uso de Backdoors (puertas traseras) y Troyanos para ganar acceso en otra ocasión y tratar de tener acceso a cuentas de altos privilegios como cuentas de Administrador. También usan los caballos de Troya (Trojans) para transferir nombres de usuarios, passwords e incluso información de tarjetas de crédito almacenada en el sistema.

Tenemos un vídeo muy interesante al respecto en:

<http://www.youtube.com/watch?v=RLFQQJvyGh8>

Una de las herramientas más utilizadas para mantener el acceso son los Rootkits.

Los Rootkits son programas de nivel kernel que tienen la habilidad de ocultarse a sí mismos y eliminar cualquier rastro de sus actividades. Pueden reemplazar ciertas llamadas y utilidades del sistema operativo con sus propias versiones modificadas. De esta forma, el atacante consigue mantener el acceso al sistema pasando desapercibido:

<http://es.wikipedia.org/wiki/Rootkit>

4.7 Eliminación de Registros

Los atacantes eliminarán cualquier rastro de su actividad para:

- Atacar de nuevo en otra ocasión.
- Evitar ser detectados.

Para esto pueden llevar a cabo varias tareas:

- Limpiar las listas MRU (Most Recently Used)
- Eliminar registros de eventos.
- Deshabilitar auditoria

Puede ejecutar estas tareas de forma manual, como vemos en la demostración que acompaña a este tema, o utilizando herramientas diseñadas para ello:





OpenLearning