

Metasploit-Telnet

Introduzione:

L'obiettivo del compito è quello di **exploitare** metasploitable attraverso alcune **vulnerabilità del protocollo telnet**. Attraverso sempre **Metasploit** installato sulla macchina Kali Linux.

Preparazione:

Vediamo subito se la porta del **servizio telnet 23** è aperta:

```
File Actions Edit View Help

zsh: corrupt history file /home/kali/.zsh_history

(kali® kali)-[~]

$ nmap -p 23 192.168.0.102

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 06:52 EST

Nmap scan report for 192.168.0.102

Host is up (0.00s latency).

PORT STATE SERVICE is grid
23/tcp open telnet

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds

(kali® kali)-[~]

$ [ kali® kali - [~]
```

Dopo aver avuto conferma, avviamo Metasploit digitando **msfconsole** sul prompt di Kali:

```
kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
__(kali⊗kali)-[~]

$ msfconsole
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>
  Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
access: PERMISSION DENIED....and...
      =[ metasploit v6.4.18-dev
--=[ 2437 exploits - 1255 auxiliary - 429 post
--=[ 1471 payloads - 47 encoders - 11 nops
     --=[ 1471 paylo
--=[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
<u>msf6</u> >
```

Ed andiamo ad utilizzare un exploit ausiliare:

use auxiliary/scanner/telnet/telnet_version

E tramite *show options* vediamo che manca il RHOSTS, ovvero l'IP della macchina vittima.

Tramite il comando **set** vado ad impostare l'IP di metasploitable:

```
set rhosts 192.168.0.102
<u>msf6</u> auxiliary(<mark>scanner/t</mark>
rhosts ⇒ 192.168.0.102
<u>msf6</u> auxiliary(scanner/t
Module options (auxiliary/scanner/telnet/telnet_version):
                Current Setting Required Description
   PASSWORD
                                                   The password for the specified username
                                                   The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html The target port (TCP)
   RHOSTS
               192.168.0.102
                                      ves
   THREADS
                                                   The number of concurrent threads (max one per host)
   TIMEOUT
                                                   Timeout for the Telnet probe
The username to authenticate as
   USERNAME
View the full module info with the info, or info -d command.
<u>msf6</u> auxiliary(<mark>s</mark>
```

Pratica:

Dopo aver digitando *exploit* e premuto invio, vengono raccolte informazioni sul servizio Telnet, come la versione e il banner. I **modelli ausiliari** come questo aiutano a identificare e raccogliere informazioni su potenziali vulnerabilità senza eseguire attacchi diretti.

Notiamo che questo exploit ci ha permesso di vedere informazioni che viaggiano in chiaro, come **username** e **password**, per accedere a metasploitable (evidenziate in giallo)

Ed ora avendo avuto accesso a quelle informazioni, posso accedere tranquillamente alla macchina, grazie alle credenziali viste:

```
[*] Auxiliary module execution completed
msf6 auxiliary(:
                                           on) > telnet 192.168.0.102
[*] exec: telnet 192.168.0.102
Trying 192.168.0.102...
Connected to 192.168.0.102.
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: Tue Nov 12 06:50:14 EST 2024 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:~$ ifconfig
         Link encap:Ethernet HWaddr 08:00:27:e1:ed:f1
eth0
          inet addr:192.168.0.102 Bcast:192.168.0.255 Mask:255.255.255.0
         inet6 addr: fdd7:21:9d01:8782:a00:27ff:fee1:edf1/64 Scope:Global
         inet6 addr: 2a0e:419:3357:0:a00:27ff:fee1:edf1/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fee1:edf1/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
         RX packets:1353 errors:0 dropped:0 overruns:0 frame:0
         TX packets:1327 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
         RX bytes:105384 (102.9 KB) TX bytes:93400 (91.2 KB)
```

Conclusione:

Esporre Telnet, soprattutto con credenziali di default, è un rischio grave in un contesto reale. Gli amministratori dovrebbero:

- Disabilitare Telnet se non necessario.
- Usare SSH al posto di Telnet per una connessione sicura.
- Cambiare le credenziali di default e adottare password forti.