

ESERCIZIO W16D1 PRATICA 1

Attività: Scansione della versione del servizio Telnet su Metasploitable utilizzando Kali Linux e Metasploit Framework.

Passaggi eseguiti:

1. Configurazione degli indirizzi IP: L'indirizzo IP della macchina Kali è stato impostato su 192.168.1.25 e l'indirizzo IP della macchina Metasploitable è stato impostato su 192.168.1.40.

```
(kali@kali)~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:9d:d6:98:f5 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe21:b1d0 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
    RX packets 52 bytes 3172 (3.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 2430 (2.3 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)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
in@metasploitable:~$ ifconfig
Link encap:Ethernet HWaddr 08:00:27:c6:f6:ed
    inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
    inet6 addr: fe80::a00:27ff:fec6:f6ed/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:300 errors:0 dropped:0 overruns:0 frame:0
    TX packets:43 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:19428 (18.9 KB) TX bytes:5144 (5.0 KB)
    Base address:0xd020 Memory:f0200000-f0220000

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:113 errors:0 dropped:0 overruns:0 frame:0
    TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:29705 (29.0 KB) TX bytes:29705 (29.0 KB)
```

2. Avvio di Metasploit Framework: Metasploit Framework è stato avviato nel terminale della macchina Kali Linux utilizzando il comando **msfconsole**.
3. Caricamento del modulo: Il modulo auxiliary telnet_version è stato caricato utilizzando il comando **use auxiliary/scanner/telnet/telnet_version**.

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/telnet/telnet_version
```

4. Impostazione delle opzioni del modulo: L'indirizzo IP di destinazione per la scansione Telnet è stato impostato su 192.168.1.40 utilizzando il comando **set RHOSTS 192.168.1.40**.

5. Esecuzione del modulo: La scansione della versione del servizio Telnet su Metasploitable è stata avviata utilizzando il comando **run**.

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > run
```

Risultati ottenuti:

- La scansione ha rivelato che il servizio Telnet è in esecuzione sulla porta 23 della macchina Metasploitable.
- Il banner del servizio Telnet mostra un messaggio di avviso e fornisce le credenziali predefinite ("msfadmin/msfadmin") per accedere alla macchina Metasploitable.

[illegible]

Conclusioni: L'esercizio è stato completato con successo, ottenendo informazioni sulla versione del servizio Telnet e le credenziali di accesso per la macchina Metasploitable. Questo dimostra l'efficacia di Metasploit Framework nell'identificare vulnerabilità e nel fornire informazioni utili per scopi di test di penetrazione e sicurezza informatica.