

Esercitazione S7/L2

In questa esercitazione ho svolto un attacco con il modulo ausiliario “telnet” per sfruttare la vulnerabilità del protocollo e ricavarne le credenziali di login.

Dispositivi/software utilizzati:

- Kali (attaccante)
- Metaspoitable (vittima)
- Metasploit (software)

Metasploit:

Metasploit è un software utilizzato per effettuare un attacco ad una macchina target, cercando di prenderne il controllo. L'obiettivo è creare una shell che permetta la comunicazione tra due macchine, per fare ciò ho bisogno di attaccare la macchina con il giusto payload.

Moduli ausiliari:

Lo scopo dei moduli ausiliari di Metasploit sono moduli che forniscono supporto durante il test della sicurezza. Infatti non sono mirati a prendere il controllo della macchina target ma per raccogliere dati e informazioni e, quindi, non utilizzano payload

Payload:

Il payload è un insieme di parti di codice che una volta ricomposto ci permetterà l'exploit e di conseguenza si stabilirà un collegamento alla macchina vittima, la shell.

Shell:

Con shell si intende il collegamento tra una macchina attaccante e una vittima, ne esistono due tipi:

- Bind: Collegamento diretto dalla macchina attaccante alla macchina vittima
 - Reverse: Collegamento inverso dalla macchina vittima alla macchina attaccante.
- Questa soluzione ci permetterà di bypassare un firewall perimetrale ad esempio.

Svolgimento:

Come prima fase ho configurato l'indirizzo IP della macchina Metaspoitable mettendo un ip statico modificando il file interfaces con il comando “sudo nano /etc/network/interfaces”. Ho verificato poi il collegamento tra Kali e Metaspoitable con un ping.

```
msf6 > search auxiliary telnet_version

Matching Modules
=====
#  Name                                                                 Disclosure Date  Rank  Check  Description
-  -                                                                 -
0  auxiliary/scanner/telnet/lantronix_telnet_version .             normal No     Lantronix Telnet Service Banner Detection
1  auxiliary/scanner/telnet/telnet_version .             normal No     Telnet Service Banner Detection

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version
msf6 > |
```

Dopo aver selezionato il payload lo andiamo a configurare, in questo caso ho impostato l'indirizzo IP della macchina target:

Ora posso procedere con l'exploit:

Come si può vedere dalla foto superiore c'è tutto l'output che mi ha dato l'attacco. Nel dettaglio (foto di destra) la parte focale dell'output.

```

_ _ _ _ _ | | _ _ _ ( ) | _ _ _ | |
_ _ _ / | _ _ _ / | _ _ _ \ _ _ _ , _ _ _ / |
a Login with msfadmin/msfadmin t

```