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.



Successivamente ho poi selezionato il modulo ausiliare da eseguire scegliendo come parametro il "telnet_version" e selezionando l'opzione 1. In questo caso ci ha tirato fuori due payload legati al servizio "telnet", in casi analoghi o laddove ci siano più risultati simili dobbiamo vedere la descrizione per scremare i risultati, basandoci su ciò che stiamo cercando, o testare più payload per trovare la vulnerabilità.

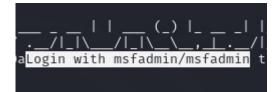
Dopo aver selezionato il payload lo andiamo a configurare, in questo caso ho impostato l'indirizzo IP della macchina target:

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts ⇒ 192.168.1.40
```

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.

Si può vedere che l'accatto ha avuto successo ed è riuscito a fornirmi le credenziali di accesso alla



macchina target. In questo caso la macchina Metaspoitable2 ha come credenziali:

ID: msfadmin

Password: msfadmin

Essendo questo l'obiettivo del modulo ausiliare, cioè la raccolta di dati/informazioni, l'attacco si può ritenere concluso.