**S7 L2**

**AMATO SARA**

**HACKING CON METASPLOIT**

L’obiettivo dell’esercizio è stato l’utilizzo di Metasploit per condurre un attacco di autenticazione su Telnet contro una macchina virtuale Metasploitable. L’attacco mirava a sfruttare una vulnerabilità del servizio Telnet attivo su Metasploitable, cercando di ottenere l’accesso tramite il modulo telnet\_version di Metasploit.

Avvio di Metasploit Console

Abbiamo iniziato aprendo Metasploit con il comando:

msfconsole

Questo comando avvia la console di Metasploit, da cui è possibile gestire vari moduli e attacchi.

Ricerca del Modulo Telnet

Una volta all'interno di Metasploit, abbiamo cercato il modulo appropriato per analizzare e attaccare il servizio Telnet:

search telnet\_version

Il comando di ricerca ha mostrato diversi moduli, e abbiamo selezionato il modulo auxiliary/scanner/telnet/telnet\_version, utile per verificare la versione del servizio Telnet e per testare possibili credenziali di accesso.

Selezione del Modulo e Configurazione dell’Indirizzo IP

Per caricare il modulo, abbiamo usato il comando:

use 1

Abbiamo poi impostato l'indirizzo IP target della macchina Metasploitable:

set rhosts 192.168.1.149

Con il comando:

show options

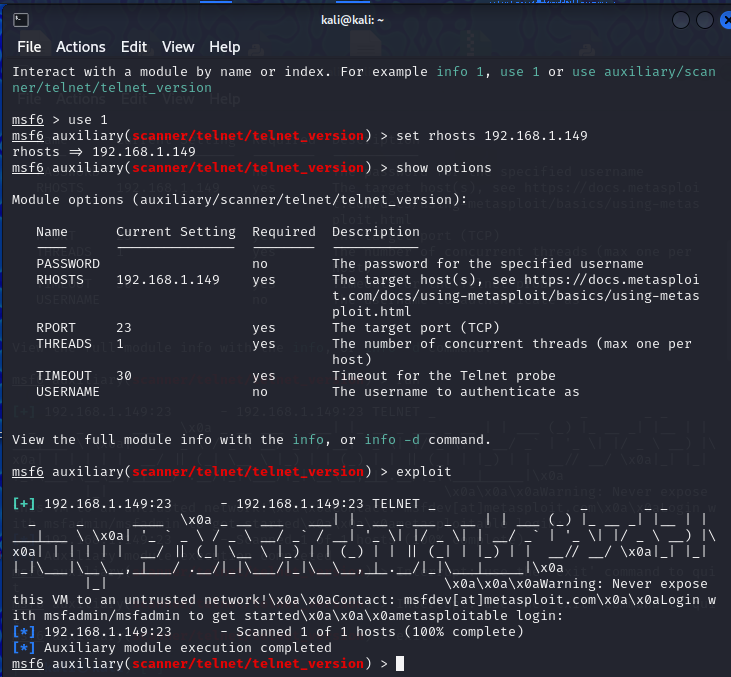
abbiamo verificato le impostazioni del modulo per assicurarci che l’indirizzo IP e le altre opzioni necessarie fossero correttamente configurate.

Esecuzione dell’Exploit

Una volta completata la configurazione, abbiamo eseguito il modulo con:

exploit

Al termine dell’esecuzione, il modulo ha restituito con successo una schermata di autenticazione della macchina Metasploitable. In questa schermata erano visibili il prompt di accesso e le credenziali ottenute (username e password), permettendo un accesso al sistema Telnet.



L’esercizio ha permesso di familiarizzare con l’uso di Metasploit e con i moduli di attacco su servizi specifici, come Telnet. Utilizzando telnet\_version, siamo riusciti a identificare e sfruttare la vulnerabilità presente nel servizio Telnet della macchina target, ottenendo le credenziali di accesso. Questa metodologia evidenzia l'importanza di configurazioni di sicurezza adeguate e dimostra la potenza degli strumenti di penetration testing per testare e rafforzare le difese di rete.