ESERCITAZIONE WEEK 16 DAY 2

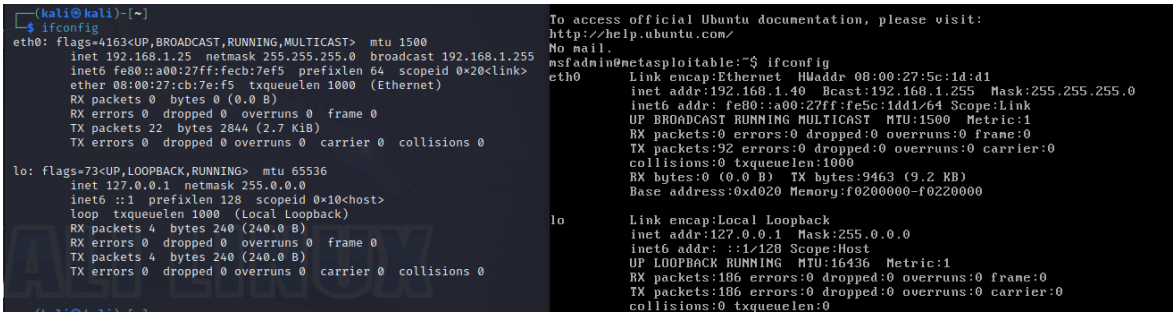
EPICODE | W16D1 - Pratica (1) PDF | Esercizio Traccia

Traccia:

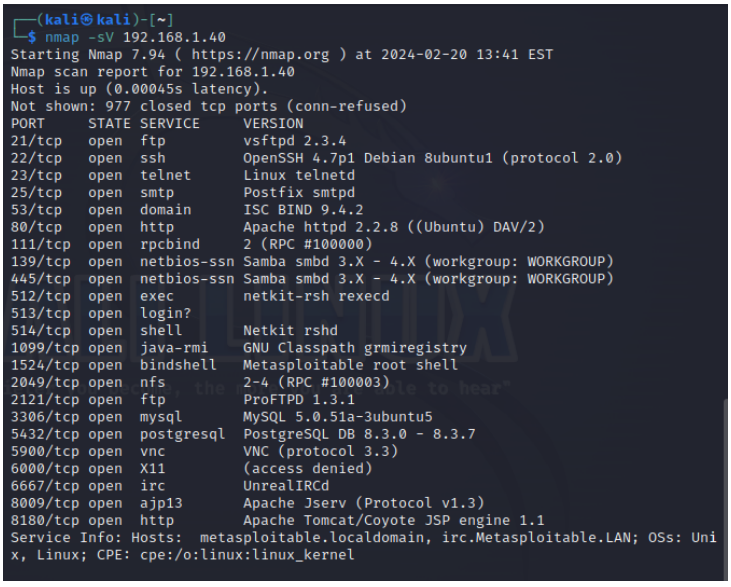
Sulla base dell'esercizio visto in lezione teorica, utilizzare Kali per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Requisito: Seguire gli step visti in lezione teorica. Prima, configurate l'IP della vostra Kali con 192.168.1.25 e l'IP della vostra Metasploitable con 192.168.1.40

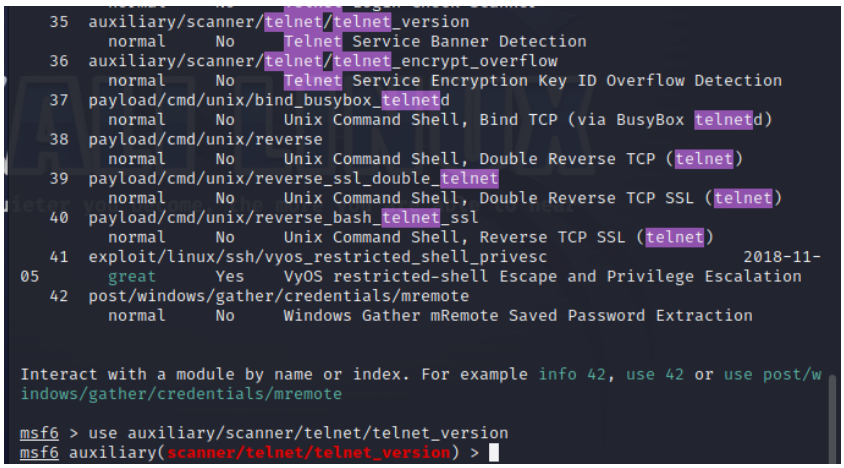
Configurazione macchine:



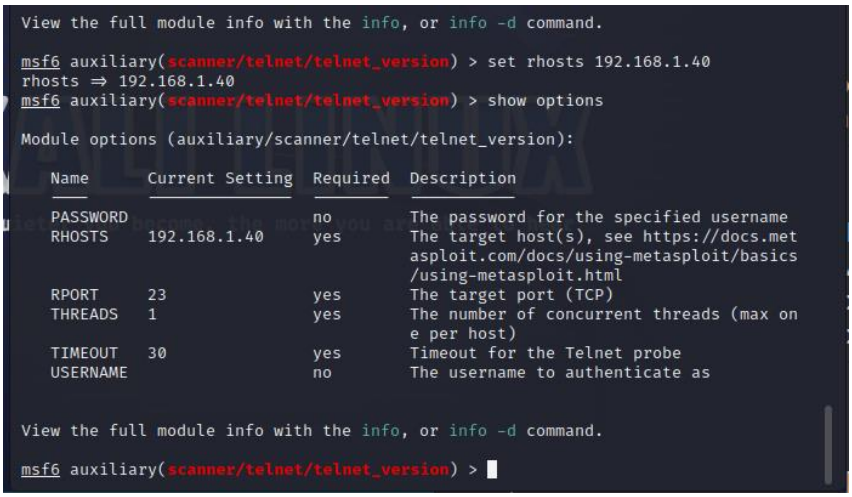
Scansione nmap su target Metasploitable: è presente il servizio telnet in ascolto su porta 23 che trasmette su canale non cifrato. Ciò significa che un potenziale attaccante potrebbe sniffare la comunicazione e rubare informazioni sensibili come username, password ed i comandi scambiati tra client e server:



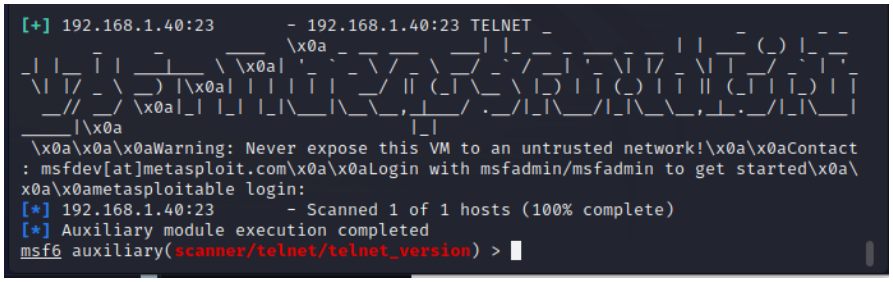
Per sfruttare questa particolare vulnerabilità del servizio Telnet, si usa il modulo ausiliario **auxiliary/scanner/telnet/telnet_version**:



Configurazione delle opzioni necessarie:

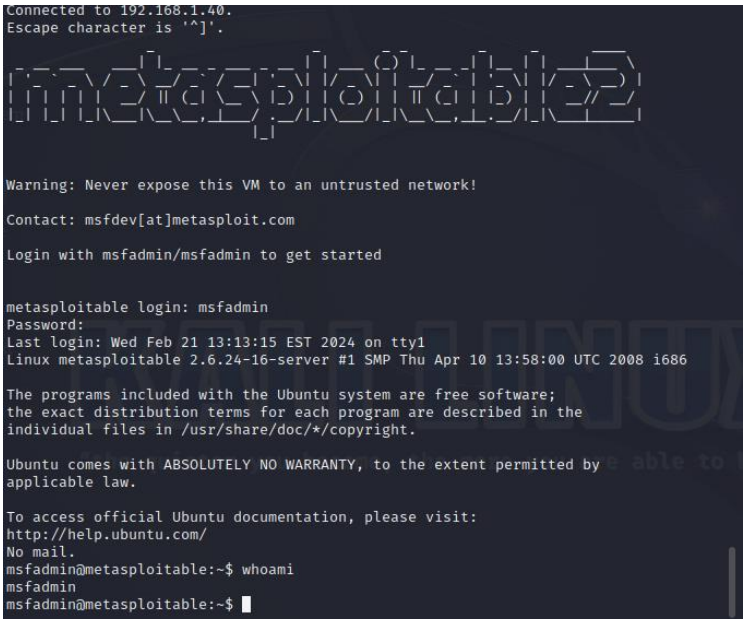


Non serve in questo caso specificare alcun payload, quindi si procede con il comando exploit:



Sono così recuperati i dati di login.

Per verificare lo sfruttamento di questa vulnerabilità, possiamo accedere da kali al servizio Telnet:



Proviamo con le informazioni che ci ha restituito Metasploit, quindi username «msfadmin», password «msfadmin» per confermare che l'attacco ha avuto effettivamente successo e la vulnerabilità del servizio Telnet è stata sfruttata correttamente, in quanto abbiamo ottenuto accesso non autorizzato alla macchina.