Exploit Telnet con Metasploit S7-L2

ESERCIZIO

Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet\_version sulla macchina Metasploitable.

TELNET

Il protocollo Telnet è uno standard di rete usato per accedere a un dispositivo remoto attraverso una connessione di tipo terminale. Utilizza la porta TCP 23 per stabilire una comunicazione e permette agli utenti di eseguire comandi su un server come se fossero fisicamente presenti sulla macchina remota. Telnet è stato uno dei primi protocolli di rete sviluppati per la gestione remota, ma, essendo non crittografato, espone i dati in chiaro, rendendolo vulnerabile a intercettazioni e attacchi di tipo "man-in-the-middle". Per motivi di sicurezza, è stato ampiamente sostituito da protocolli più sicuri come SSH (Secure Shell), che cifra le comunicazioni. Telnet è comunque utilizzato per scopi di debugging o su reti locali non esposte a internet.

SVOLGIMENTO

La macchina Metasploitable presenta un servizio Telnet in ascolto sulla porta 23, che trasferisce il traffico su canale non cifrato. Questo significa che un potenziale attaccante potrebbe intercettare la comunicazione e rubare informazioni sensibili come username, password e i comandi scambiati tra client e server.

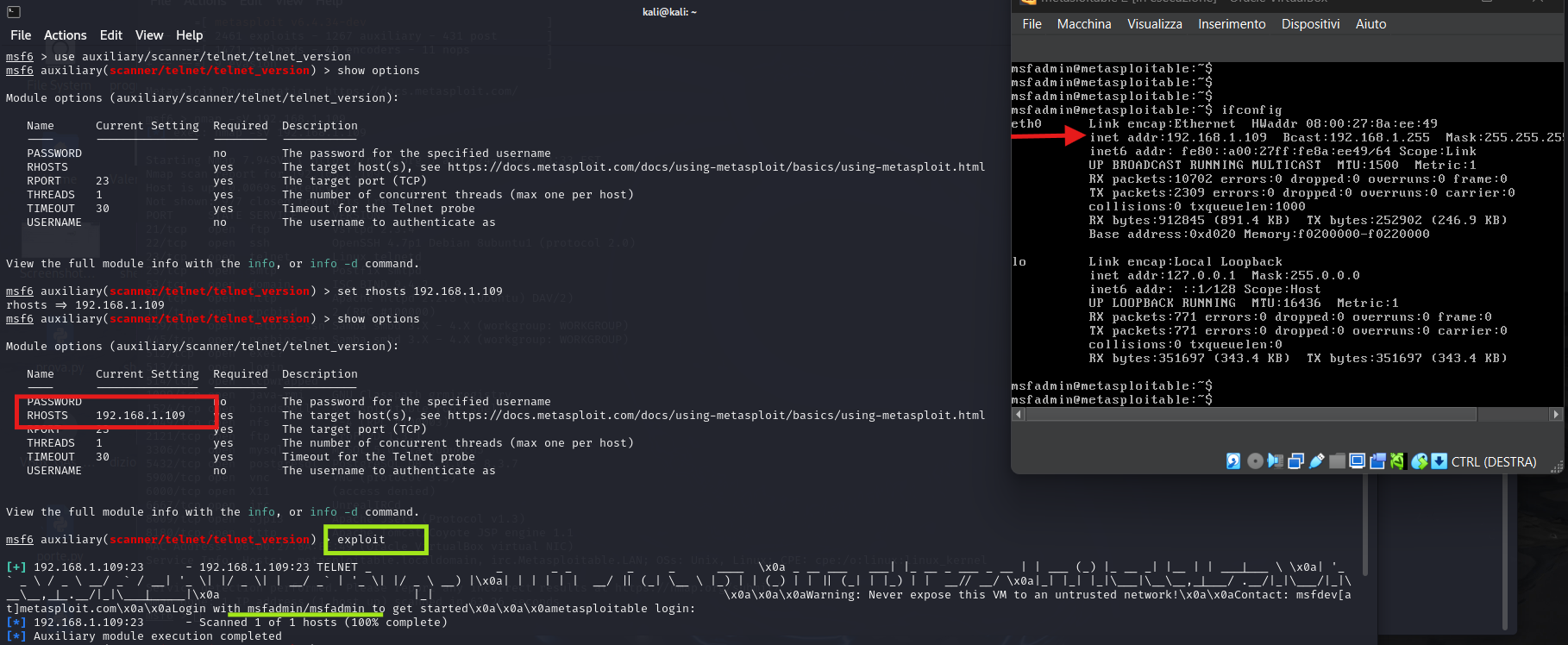
Per sfruttare questa particolare vulnerabilità del servizio Telnet, utilizziamo un modulo ausiliario :

path auxiliary/scanner/telnet/telnet\_version

Per utilizzare un modulo, dovremmo anteporre al path del modulo la keyword «use».

Controlliamo le opzioni necessarie per lanciare lʼattacco, eseguendo il comando «show options», come in figura sotto. Vedremo che tra i parametri da inserire abbiamo RHOSTS, ovvero lʼindirizzo target dove è in esecuzione il servizio telnet. Tutti gli altri parametri necessari sono già configurati di default.

Configuriamo il parametro RHOSTS utilizzando il comando «set» seguito dal parametro e dal valore del parametro.



Per il modulo scelto non cʼè bisogno di specificare un payload, infatti non è specificata nessuna opzione per il payload. Possiamo quindi eseguire lʼattacco con il comando: «exploit»

Il modulo ha recuperato i dati di login del servizio, come si vede nella linea gialla in figura. Ci sta dicendo che le credenziali da utilizzare sono username: «msfadmin», password «msfadmin».

Per verificare la correttezza delle informazioni, facciamo un test. Eseguiamo da Metasploit il comando «telnet» seguito dallʼip della macchina Metasploitable. Nel nostro lab la Metasploitable ha IP 192.168.1.109, quindi eseguiremo il comando

telnet 192.168.1.109

