S7/L2

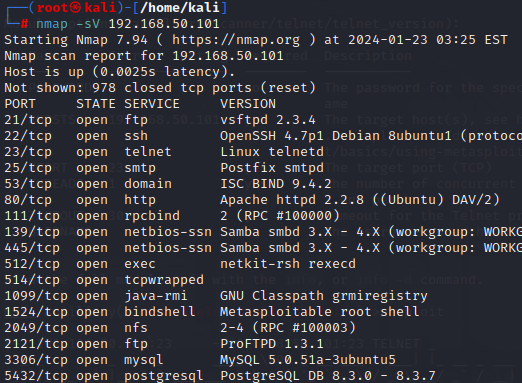
Traccia: Sulla base dell’esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet\_version sulla macchina Metasploitable.

Ci troviamo nella fase 3 di un penetration testing, ovvero nella fase dell’exploit, ovvero il momento in cui si cerca di sfruttare le vulnerabilità identificate nel sistema target. L'obiettivo è utilizzare gli exploit appropriati per ottenere accesso non autorizzato al sistema o per eseguire codice malevolo. L’exploit a differenza del malware, è un codice malevolo che va a sfruttare una vulnerabilità già presente nel software. Di solito questo problema si risolve correggendo il codice del programma attraverso degli upgrade/aggiornamenti. La soluzione migliore rimane quella di testare prima il nuovo aggiornamento su un dispositivo clone (sia a livello software, sia hardware).

Un tool utilissimo per questo tipo di attività è Metasploit, ovvero un tool open-source usato per lo sviluppo di exploit. Possiamo attivare l’interfaccia di Metasploit attraverso il comando MSFCONSOLE.

Per prima cosa attiviamo un NMAP -sV seguito dall’IP della nostra macchina vittima (metasploitable2), questo ci darà una scansione dei servizi per rilevare le versioni dei servizi aperti.

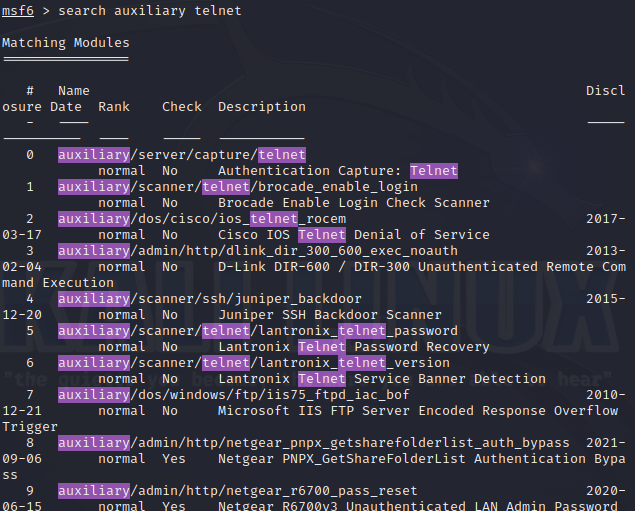
L’esercizio richiede di sfruttare la vulnerabilità relativa al telnet (porta 23).





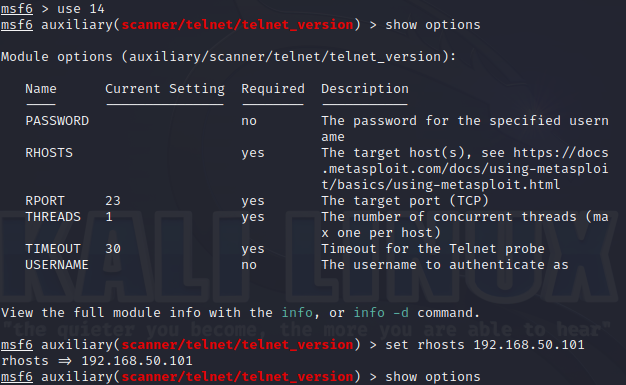
Dopo di che, sempre su terminale kali andiamo ad inserire la keywords “search auxiliary telnet” da qui otteniamo un elenco di moduli e exploit che sono correlati al servizio telnet.

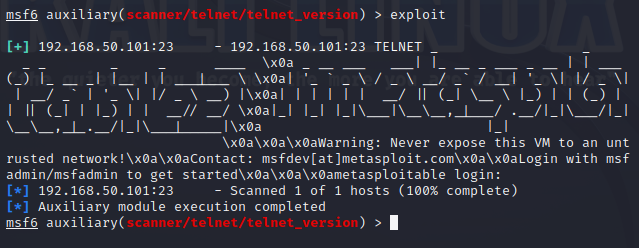
I moduli ausiliari in Metasploit sono progettati per svolgere funzioni di supporto durante i test sulla sicurezza, forniscono dunque informazioni utili per ottenere un quadro completo della sicurezza della rete o del sistema. A differenza dei moduli normali (utilizzati per lo più per attacchi diretti alle vulnerabilità) non utilizzano i payload.



Per prassi dovremmo testare tutti gli exploit ed una volta individuato quello più idoneo lo utilizziamo con il comando “use” + il suo relativo path; in questo caso usiamo il numero 14: (scanner/telnet/telnet\_version).

Vediamo quali parametri sono richiesti per lanciare l’attacco, attraverso il comando “show options”:



Andiamo a settare l’input richiesto (required) RHOSTS con l’IP della nostra macchina vittima, e attiviamo l’exploit con il suo relativo comando:

Importante ricordare che il protocollo telnet viene utilizzato per l’accesso remoto a dispositivi, tuttavia si tratta di un protocollo non sicuro in quanto trasmette dati in maniera non crittografato. L’uso di un exploit telnet su Metasploit può sfruttare questa falla di sicurezza per l’invio dei pacchetti malevoli e ottenere accesso non autorizzato al sistema. In questo caso come possiamo vedere dall’immagine ci vengono dati in chiaro le credenziali di login.

A verifica di ciò per vedere se effettivamente siamo ora in grado di accedere alla macchina vittima, da riga di comando su Kali, possiamo inserire il comando “telnet + l’IP di metasploitable” e come possiamo vedere dopo ver inserito le credenziali richieste siamo dentro.

