S7/L1

Traccia: Partendo dall’esercizio visto nella lezione di oggi, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd».

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test\_metasploit.

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. Tuttavia in una situazione ideale, la soluzione migliore è quella 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.

Gli step da seguire per sfruttare una vulnerabilità sono:

1. Identificare un servizio vulnerabile.

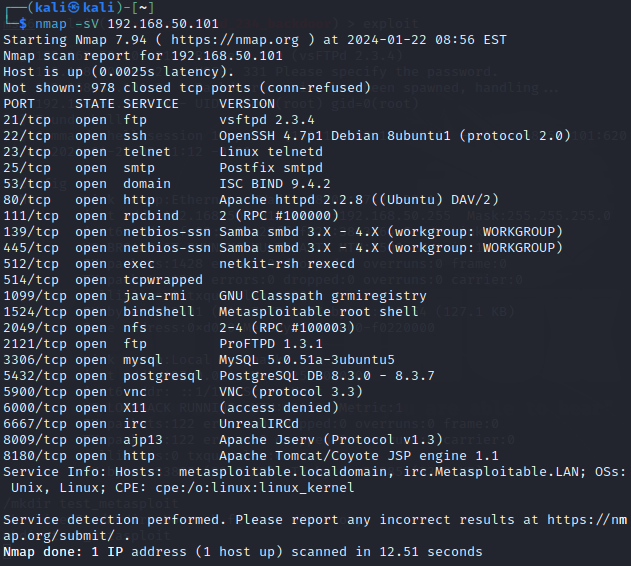
2. Cercare l’exploit più adatto

3. Caricare e configurare sia l’exploit che il payload da utilizzare.

5. Avviare l’exploit per ottenere accesso alla macchina vulnerabile/vittima.

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.

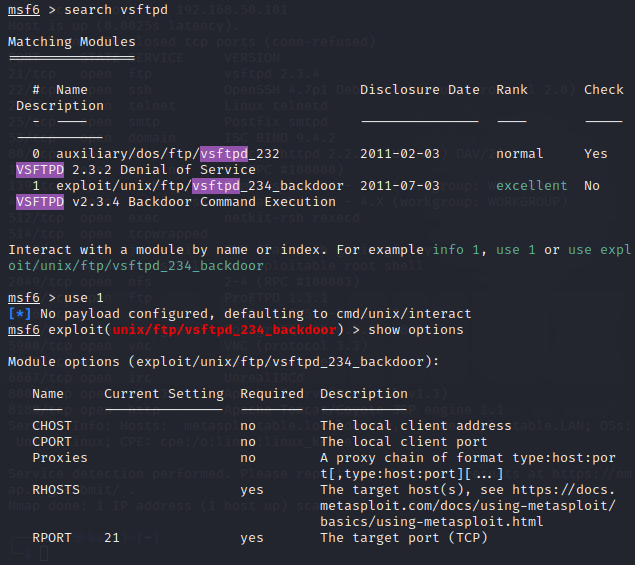
L’esercizio richiede di verificare la versione vsftpd del servizio FTP sulla porta 21.





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

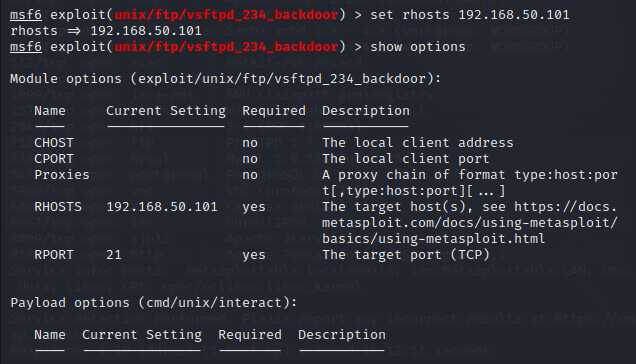
Dopo aver scelto l’exploit da utilizzare, lo si abilita con il comando «use» seguito dal percorso dell’exploit, in questo caso selezioniamo “use 1”.



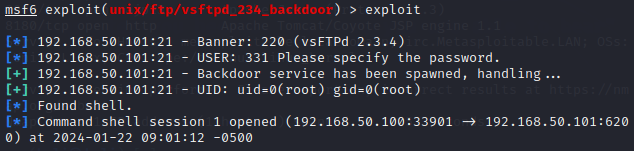
Alcune configurazioni sono «required», ovvero è obbligatorio inserirle per utilizzare l’exploit.

Ad esempio, qui abbiamo bisogno di due parametri: RHOSTS: ovvero l’indirizzo IP della macchina target; e RPORT: ovvero la porta sulla macchina target dove il servizio è in ascolto (21 già inserita).

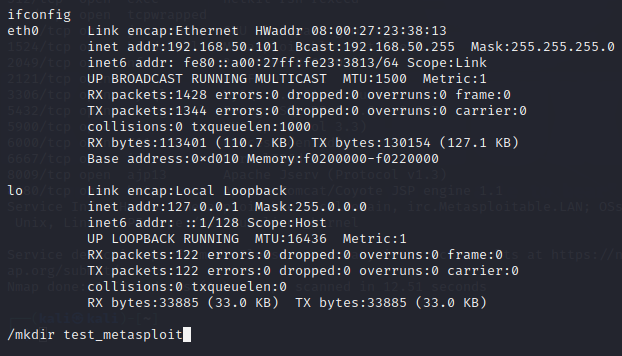
Per cui settiamo l’IP tramite il comando “set rhosts + IP meta” e per controllare se lo ha salvato rimandiamo un altro “show options”:



Adesso attiviamo l’exploit; se ha successo otteniamo l’accesso al target/macchina vittima:



Come controverifica per vedere se effettivamente abbiamo ottenuto l’accesso, possiamo provare con “ifconfig” per verificare se l’IP che ci viene mostrato è quello della nostra “macchina vittima”:



Ora che siamo dentro, l’esercizio ci chiede di creare una cartella, con il comando “mkdir test\_metasploit”, per verificare se effettivamente è stata creata, possiamo vederla su metasploitable con il comando “ls”:

