## HETASPLOT HACKING:

## **#KALI LINUX** #SERVIZIO VSFTPD SU METASPLOITABLE

NELLA LEZIONE PRATICA DI OGGI VEDREMO COME EFFETTUARE UNA SESSIONE DI HACKING CON METASPLOIT SULLA MACCHINA METASPLOITABLE.

## TRACCIA:

PARTENDO DALL'ESERCIZIO GUIDATO VISTO NELLA LEZIONE TEORICA, 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 MACCHI-NA 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 DIREC-TORY DI ROOT (/). CHIAMATE LA CARTELLA TEST\_METASPLOIT.

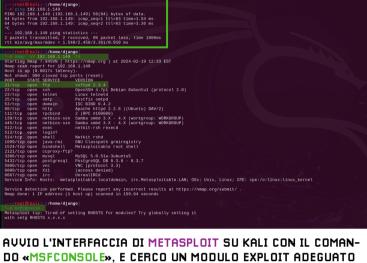
AL FINE DELL'ESERCIZIO LE DUE MACCHINE (KALI E METASPLOI-

TABLE) STARANNO SU RETI DIVERSE, CAMBIO QUINDI L'IP STATICO DI METASPLOITABLE IN 192.168.1.149 COME DA TRACCIA, MENTRE QUELLO DI KALI LINUX RESTERÀ 192.168.50.100. LI METTO IN CONNESSIONE TRAMITE PFSENSE DI CUI REIMPOSTO LA LAN2 (QUELLA PREDEFINITA PER META-SPLOITABLE) SU 192.168.1.1/24 E FACCIO UN PING DI PROVA DA KALI.

ARP Table

#TABELLA ARP DI PFSENSE:

Interface	IP Address	MAC Address	Hostname	Status	Link Type	Actions
WAN	10.0.2.15	08:00:27:0b:52:a1		Permanent	ethernet	■心面
WAN	10.0.2.2	52:54:00:12:35:02		Expires in 40 seconds	ethernet	■心面
WAN	10.0.2.3	52:54:00:12:35:03		Expires in 70 seconds	ethernet	□∪亩
LAN	192.168.50.100	08:00:27:ea:09:65		Expires in 1154 seconds	ethernet	□∪亩
LAN2	192.168.1.1	08:00:27:e7:49:df		Permanent	ethernet	□∪亩
LAN2	192.168.1.149	08:00:27:dc:03:d4		Expires in 842 seconds	ethernet	□○亩
LAN	192.168.50.1	08:00:27:c5:d4:fd	pfSense.home.arpa	Permanent	ethernet	■心面
Map v 10/.109.1.149 Starting Mnap 7.9459N ( https://map.org ) at 2024-02-19 12:33 EST						
(root@kall) (home/django)						



AL SERVIZIO VULNERABILE CITATO NELLA TRACCIA CON

«SEARCH VSFTPD». INDIVIDUATO L'EXPLOIT LO APRO CON IL COMANDO «USE» SEGUITO DAL PATH DELL'EXPLOIT STESSO E CONTROLLO I PARAMETRI NECESSARI PER LANCIARLO CON IL COMANDO «SHOW OPTIONS». NOTO LA VOCE «YES» DI FIANCO ALLA COLONNA DEI PARAMETRI REQUIRED RHOSTS, DEVO DUNQUE INSERIRE L'INDIRIZZO IP DELLA MACCHINA VITTIMA CON «SET RHOSTS 192.168.1.149». LA PORTA È GIÀ SETTATA DI DEFAULT SU 21 (TCP), CHE È QUELLA DEL SERVIZIO VSFTPD INDIVIDUATA ANCHE CON UNA VELOCE SCANSIONE CON NMAP. CONTROLLO I PAYLOAD ED UNA VOLTA APPURATO CHE NON CE NE SONO DA SELEZIONARE IN QUETSO CASO, POSSO DUNQUE LANCIARE L'ATTACCO CON IL COMANDO «EXPLOIT». ED ECCO CHE TRAMITE UNA REVERSE SHELL POSSO INTERAGIRE DIRET-TAMENTE CON LA MACCHINA VITTIMA METASPLOITABLE, ED ESEGUIRE UNA SERIE DI COMANDI TRA CUI LA CREAZIONE DI UNA CARTELLA DENOMINATA "TEST\_METASPLOT" NELLA DIRECTORY DI ROOT COME RICHIESTO DALLA TRACCIA.

