METASPLOIT HACKING:

#KALI LINUX
#SERVIZIO TELNET SU METASPLOITABLE

TRACCIA:

SULLA BASE DELL'ESERCIZIO VISTO IN LEZIONE TEORICA, UTILIZZARE KALI PER SFRUTTARE LA VULNERABILITÀ RELATIVA A TELNET CON IL MODULO **AUXILIARY TELNET_VERSION** SULLA MACCHINA METASPLOITABLE.

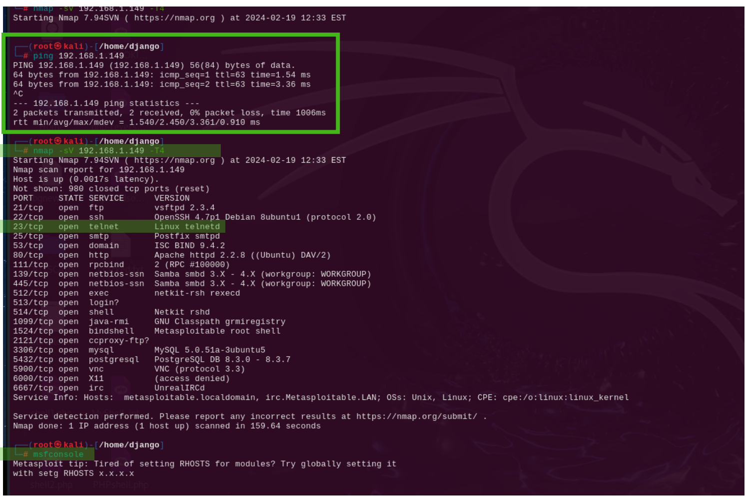
REQUISITO: SEGUIRE GLI STEP VISTI IN LEZIONE TEORICA. PRIMA, CONFIGURATE L'IP DELLA VOSTRA KALI CON 192.168.1.25 E L'IP DELLA VOSTRA METASPLOITABLE CON 192.168.1.40

L'ESERCIZIO RICHIEDE CHE LE DUE MACCHINE KALI E METASPLOITABLE SIANO SULLA STESSA RETE CON DUE IP STATICI DIFFERENTI IN NOTAZIONE CIDR /24.
PER VELOCIZZARE IL PROCEDIMENTO LASCIO INVECE CHE STIANO SU RETI DIVERSE COME DA ESERCIZIO PRECEDENTE. QUINDI L'IP STATICO DI METASPLOITABLE RESTA 192.168.1.149, MENTRE QUELLO DI KALI LINUX SARÀ 192.168.50.100. LI METTO IN CONNESSIONE TRAMITE PFSENSE DI CUI REIMPOSTO LA LAN2 (QUELLA PREDEFINITA PER METASPLOITABLE) SUL GATEWAY 192.168.1.1/24 E FACCIO UN PING DI PROVA DA KALI.

#TABELLA ARP DI PFSENSE:

ARP Table

Interface	IP Address	MAC Address	Hostname	Status	Link Type	Actions
WAN	10.0.2.15	08:00:27:0b:52:a1		Permanent	ethernet	
WAN	10.0.2.2	52:54:00:12:35:02		Expires in 40 seconds	ethernet	
WAN	10.0.2.3	52:54:00:12:35:03		Expires in 70 seconds	ethernet	
LAN	192.168.50.100	08:00:27:ea:09:65		Expires in 1154 seconds	ethernet	
LAN2	192.168.1.1	08:00:27:e7:49:df		Permanent	ethernet	
LAN2	192.168.1.149	08:00:27:dc:03:d4		Expires in 842 seconds	ethernet	
LAN	192.168.50.1	08:00:27:c5:d4:fd	pfSense.home.arpa	Permanent	ethernet	



AVVIO L'INTERFACCIA DI METASPLOIT SU KALI CON IL COMANDO «MSFCONSOLE», E CARICO IL MODULO EXPLOIT ADEGUATO AL SERVIZIO VULNERABILE CITATO NELLA TRACCIA CON «USE AUXILIARY/SCANNER/TELNET/TELNET_VERSION». 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 23 (TCP), CHE È QUELLA DEL SERVIZIO TELNET 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». L'ATTACCO VA A BUON FINE E MI RESTITUISCE LE CREDENZIALI DI LOGIN SULLA MACCHINA VITTIMA "MSFADMIN/MSFADMIN", CHE UTILIZZO AL VOLO CONNETTENDOMI AL SERVIZIO CON IL COMANDO TELNET SEGUITO DALL'IP DI METASPLOITABLE. ED ECCO CHE POSSO INTERAGIRE DIRETTAMENTE CON LA MACCHINA VITTIMA ESEGUENDO UNA SERIE DI COMANDI TRA CUI "WHOAMI" E "PS AUX > FILE.TXT | MORE FILE.TXT", CHE MI CREERÀ UN FILE DIRETTAMENTE CONSULTABILE SUL QUALE TRASFERIRE L'ELENCO DI TUTTI I PROCESSI IN FUNZIONE SULLA MACCHINA VITTIMA.