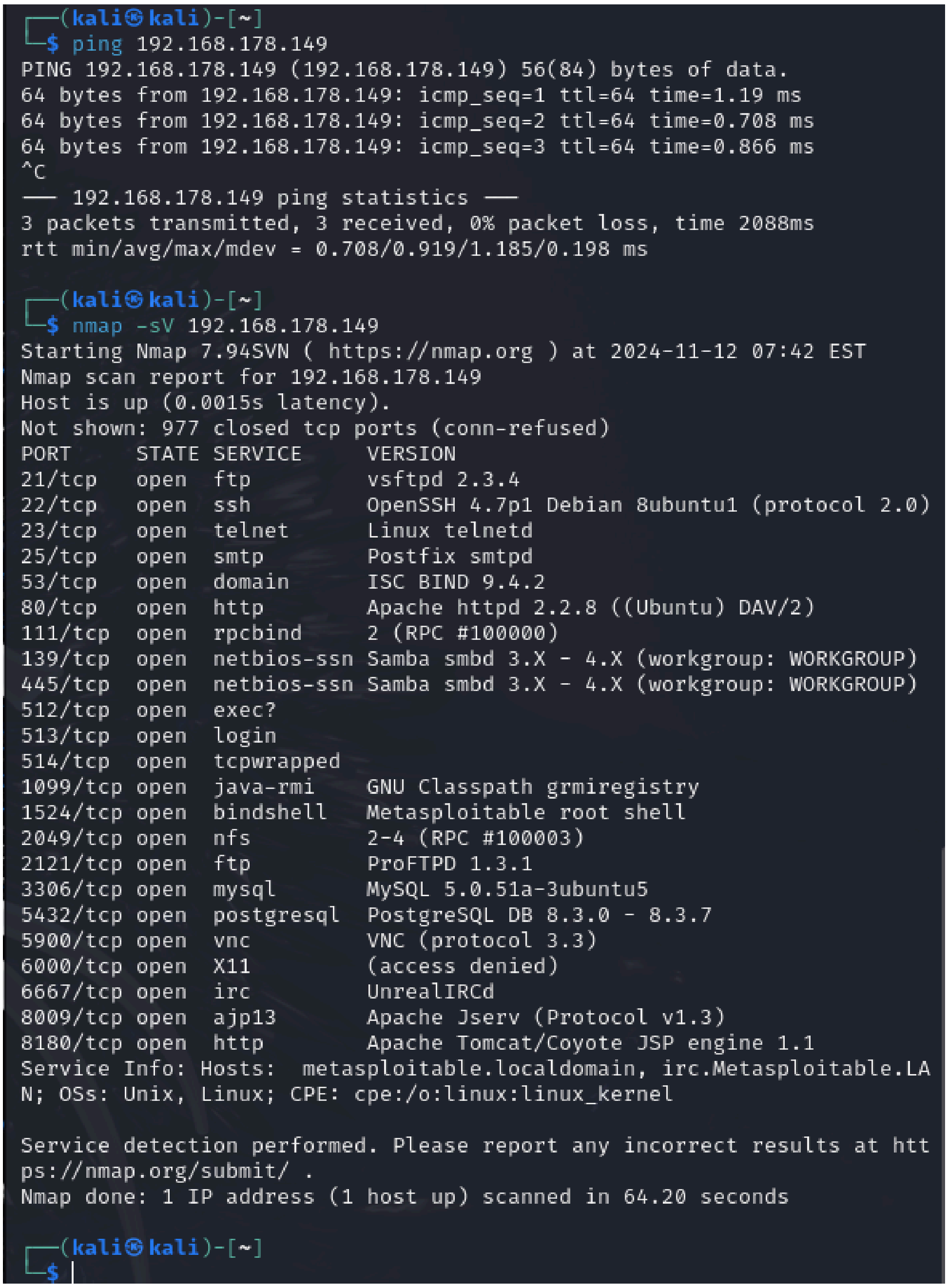
12.11.2024

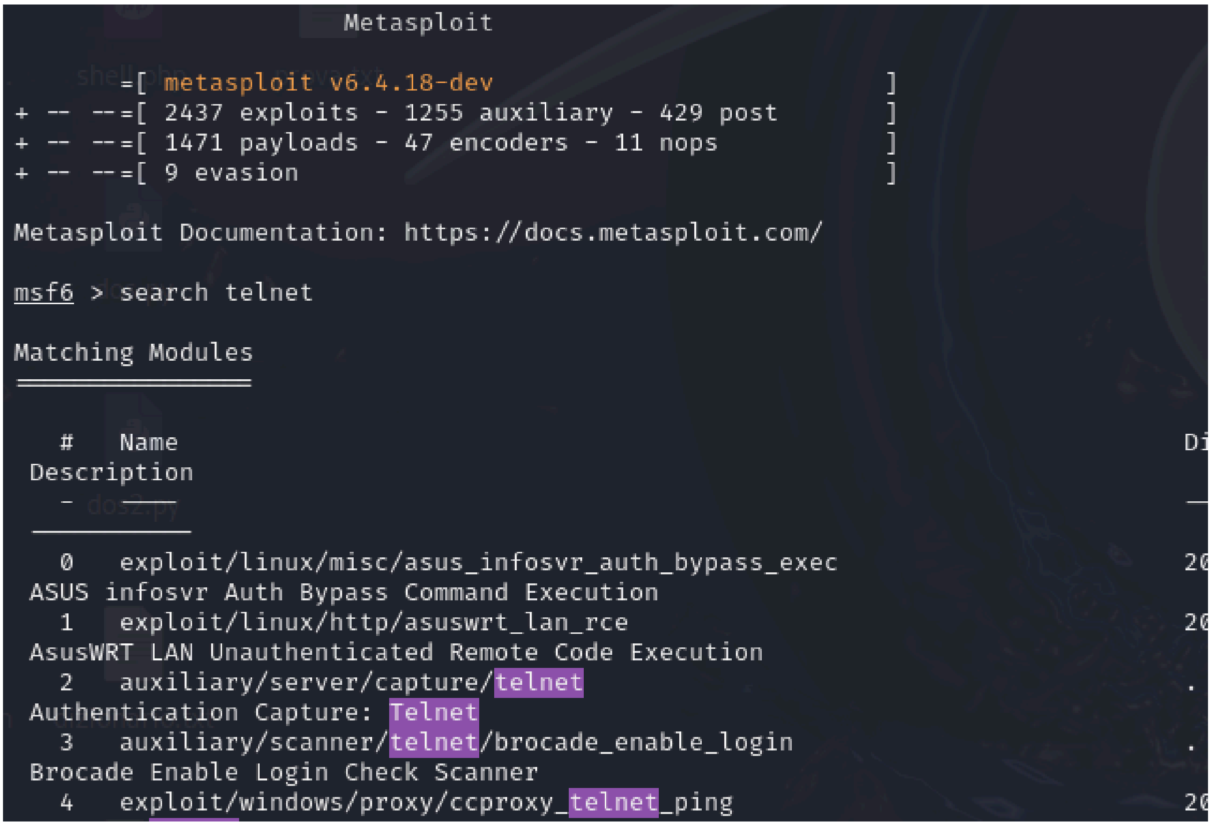
Traccia:
Sulla base dell’esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

come da traccia andiamo ad hackerare la Metaspoitable.
Ci assicuriamo prima che i due dispositivi pinghino e facciamo uno scan con nmap
i pinghino e facciamo uno scan con nmap

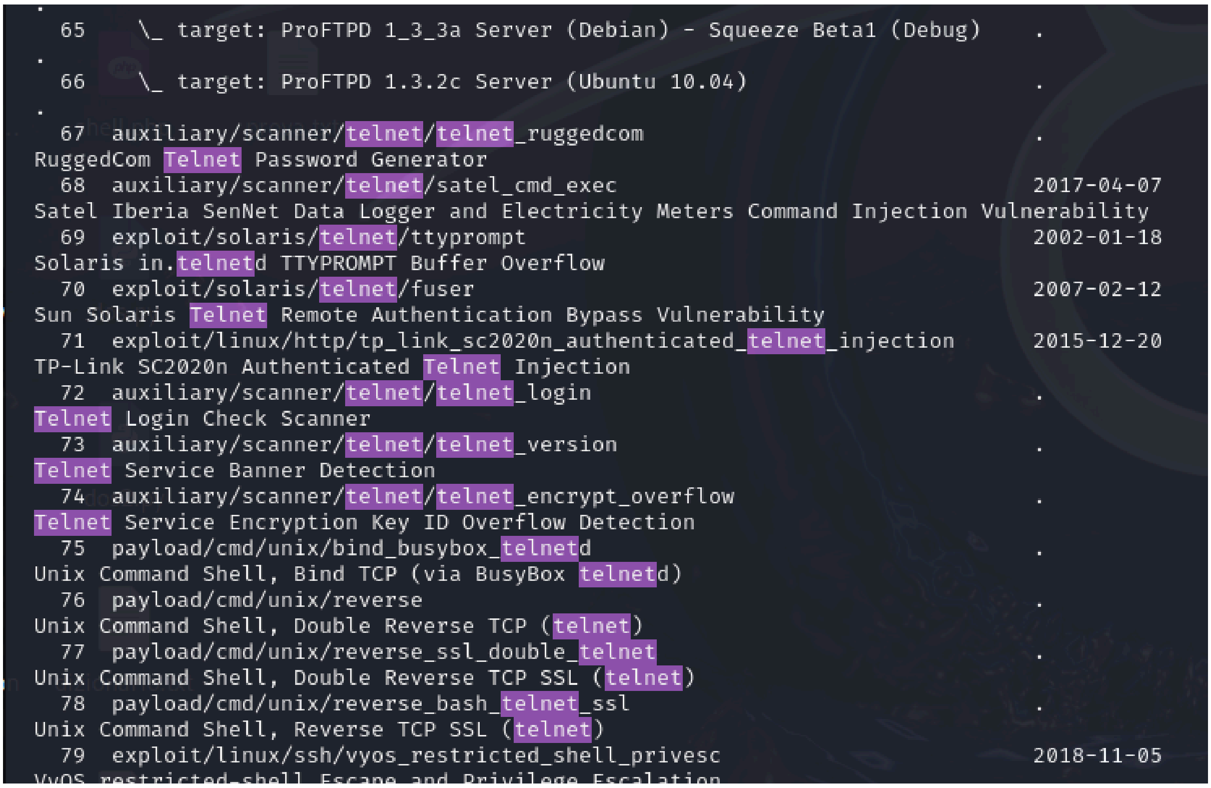


```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.178.149
PING 192.168.178.149 (192.168.178.149) 56(84) bytes of data.
64 bytes from 192.168.178.149: icmp_seq=1 ttl=64 time=1.19 ms
64 bytes from 192.168.178.149: icmp_seq=2 ttl=64 time=0.708 ms
64 bytes from 192.168.178.149: icmp_seq=3 ttl=64 time=0.866 ms
^C
─── 192.168.178.149 ping statistics ───
3 packets transmitted, 3 received, 0% packet loss, time 2088ms
rtt min/avg/max/mdev = 0.708/0.919/1.185/0.198 ms

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.178.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 07:42 EST
Nmap scan report for 192.168.178.149
Host is up (0.0015s 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  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?
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LA
N; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.20 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Avviamo msfconsole su Kali e cerchiamo l’exploit telnet e lo scegliamo tra la lista:

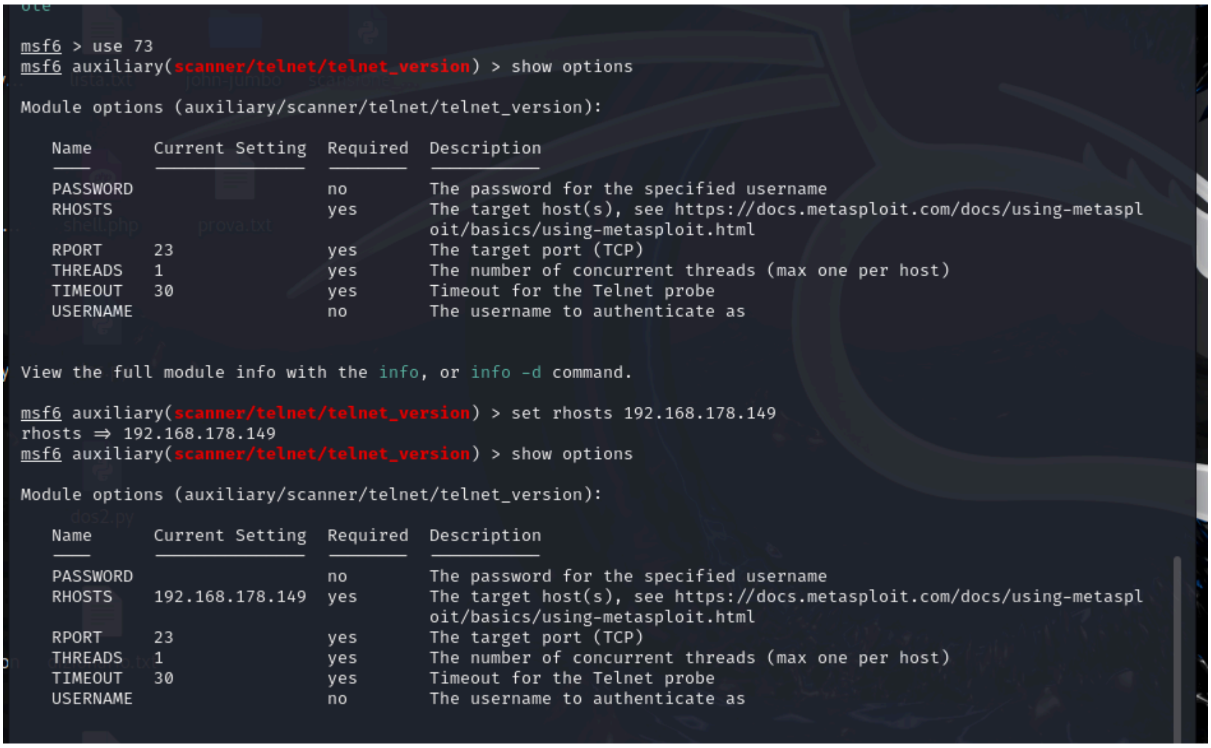


```
                        Metasploit

     =[ metasploit v6.4.18-dev                         ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search telnet

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

   #   Name                                                    Di
 Description
   -   ----                                                    --
 -----------

   0   exploit/linux/misc/asus_infosvr_auth_bypass_exec        20
 ASUS infosvr Auth Bypass Command Execution
   1   exploit/linux/http/asuswrt_lan_rce                      20
 AsusWRT LAN Unauthenticated Remote Code Execution
   2   auxiliary/server/capture/telnet                         .
 Authentication Capture: Telnet
   3   auxiliary/scanner/telnet/brocade_enable_login           .
 Brocade Enable Login Check Scanner
   4   exploit/windows/proxy/ccproxy_telnet_ping               20
```



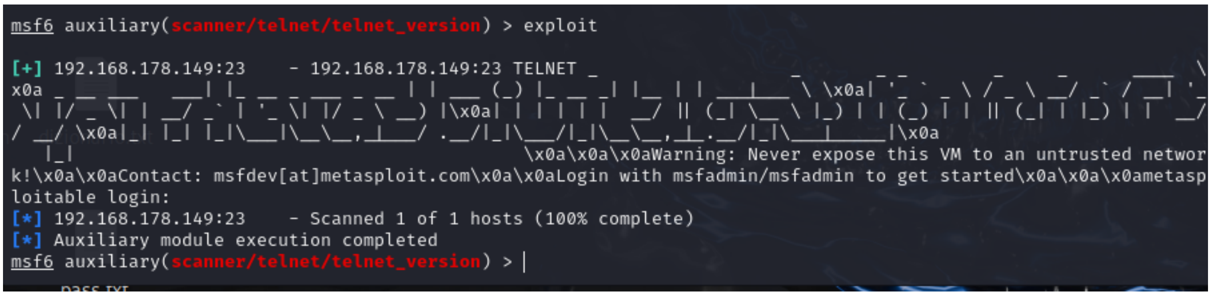
```
 .
   65    \_ target: ProFTPD 1_3_3a Server (Debian) - Squeeze Beta1 (Debug)    .
 .
   66    \_ target: ProFTPD 1.3.2c Server (Ubuntu 10.04)                      .
 .
   67  auxiliary/scanner/telnet/telnet_ruggedcom                              .
 RuggedCom Telnet Password Generator
   68  auxiliary/scanner/telnet/satel_cmd_exec                                2017-04-07
 Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
   69  exploit/solaris/telnet/ttyprompt                                       2002-01-18
 Solaris in.telnetd TTYPROMPT Buffer Overflow
   70  exploit/solaris/telnet/fuser                                           2007-02-12
 Sun Solaris Telnet Remote Authentication Bypass Vulnerability
   71  exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection      2015-12-20
 TP-Link SC2020n Authenticated Telnet Injection
   72  auxiliary/scanner/telnet/telnet_login                                  .
 Telnet Login Check Scanner
   73  auxiliary/scanner/telnet/telnet_version                                .
 Telnet Service Banner Detection
   74  auxiliary/scanner/telnet/telnet_encrypt_overflow                       .
 Telnet Service Encryption Key ID Overflow Detection
   75  payload/cmd/unix/bind_busybox_telnetd                                  .
 Unix Command Shell, Bind TCP (via BusyBox telnetd)
   76  payload/cmd/unix/reverse                                               .
 Unix Command Shell, Double Reverse TCP (telnet)
   77  payload/cmd/unix/reverse_ssl_double_telnet                             .
 Unix Command Shell, Double Reverse TCP SSL (telnet)
   78  payload/cmd/unix/reverse_bash_telnet_ssl                               .
 Unix Command Shell, Reverse TCP SSL (telnet)
   79  exploit/linux/ssh/vyos_restricted_shell_privesc                        2018-11-05
 VyOS restricted-shell Escape and Privilege Escalation
```

Come di consueto settiamo rhosts e lanciamo l’exploit:



```
msf6 > use 73
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metaspl
                                        oit/basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


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

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.178.149
rhosts => 192.168.178.149
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS    192.168.178.149  yes       The target host(s), see https://docs.metasploit.com/docs/using-metaspl
                                        oit/basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as
```

Lanciato l’exploit riusciremo a vedere user e password del servizio Telnet.



```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.178.149:23    - 192.168.178.149:23 TELNET _                  _     _ _        _     _         ____   \
x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_
 \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __/
/ __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a
   |_|                                    \x0a\x0a\x0aWarning: Never expose this VM to an untrusted networ
k!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasp
loitable login:
[*] 192.168.178.149:23    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > |
```