

Esercizio 07/11/2023

Nell'esercizio odierno ci viene richiesto di utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary sulla macchina Metasploitable.

L'Exploit è la fase 3 del Pentesting ed è la fase più delicata di tutto il processo.

L'Exploit non è una sola azione ma la prima fase di una **serie di azioni** che va a testare, ad identificare le vulnerabilità di un sistema, è una sorta di metodo di sfondamento, va a creare cioè un varco (N.B. ciò significa che c'è una **vulnerabilità già esistente**). Alla fine di queste fasi, essendo comunque entrati e avendo, quindi, scoperto la vulnerabilità, il lavoro dell'Ethical Hacker (almeno per questo programma) finisce qui e si può passare direttamente alla fase 7, il report. Stesso discorso se la shell non viene creata dopo l'exploit perché vuol dire che se non entro io non entra neanche il BH.

La seconda fase è andare a trovare un **payload** (un file nocivo che mi permette di creare una shell) che ci permetterà di passare alla terza fase, la **shell**, che crea una connessione tra due dispositivi. Quest'ultima può essere di tipo **reverse o bind**, la differenza è che, una volta creato il payload ed è andato a buon fine, la prima creerà una connessione dal computer vittima al computer attaccante (quindi dall'interno verso l'esterno), mentre nella bind accade il contrario. Poiché è molto probabile che ci siano sistemi di sicurezza (firewall, IDS, IPS), è meglio utilizzare la reverse, la bind viene usata quando siamo già all'interno della rete, e non è detto che funzioni perché il dispositivo in questione potrebbe comunque essere coperto da un dispositivo di sicurezza come un firewall e quindi non funzionare ugualmente.

L'Exploit, a differenza del **Malware**, sfrutta la vulnerabilità del sistema e non richiede alcun tipo di permesso. Quello che utilizzeremo deve essere specifico per la versione di quel determinato programma, se devo ad esempio testare una vulnerabilità su Office devo ricercare la versione dell'Office in questione altrimenti non è detto che funzionerà. Non è detto perché se vado ad immettere una versione più datata è possibile che la vulnerabilità in questione sia già stata corretta dall'aggiornamento del programma.

Per sapere se l'Exploit funziona avrò due strade, la prima a livello manuale (sconsigliata per via del tempo che impiegheremmo), la seconda a livello automatico e per fare questo si utilizzano programmi specifici come **Metasploit** che prova tutte le combinazioni in maniera automatica

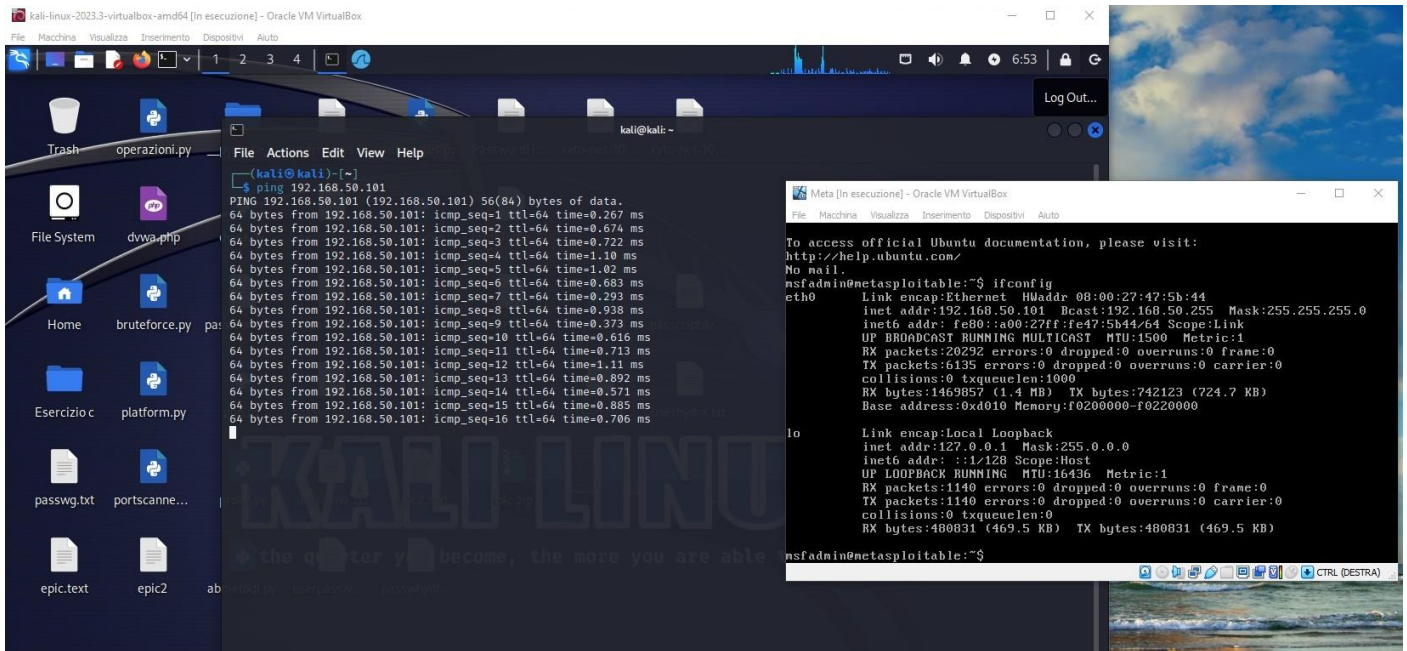
Per arrivare a tutto questo si avvia Metasploit e si utilizzano una serie di comandi che ci porteranno all'ultima fase. E' molto importante sapere che perché l'exploit abbia effetto il programma che andiamo ad "exploitare" deve essere attivo, startato.

I moduli auxiliary, a differenza dei normali che eseguono attacchi diretti e utilizzano un payload, sono moduli di supporto, forniscono cioè funzionalità ausiliarie che possono essere utilizzate in diverse fasi di pentesting. La differenza sostanziale sta proprio nel fatto che non usano (quasi mai) il payload

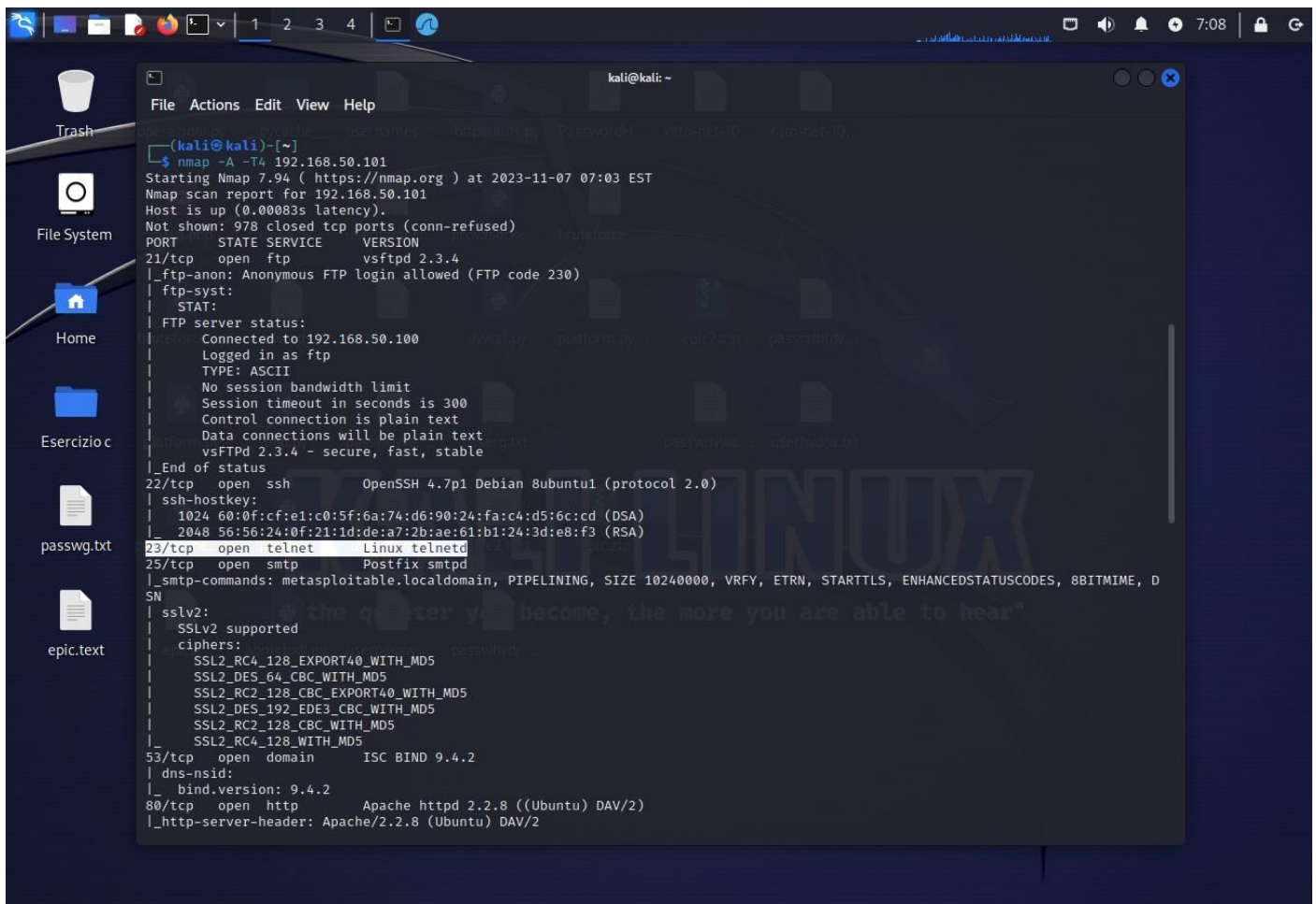
Telnet è un protocollo che consente di stabilire una connessione da remoto (porta 23 di default).

Di seguito la serie di comandi utilizzati per arrivare all'obiettivo:

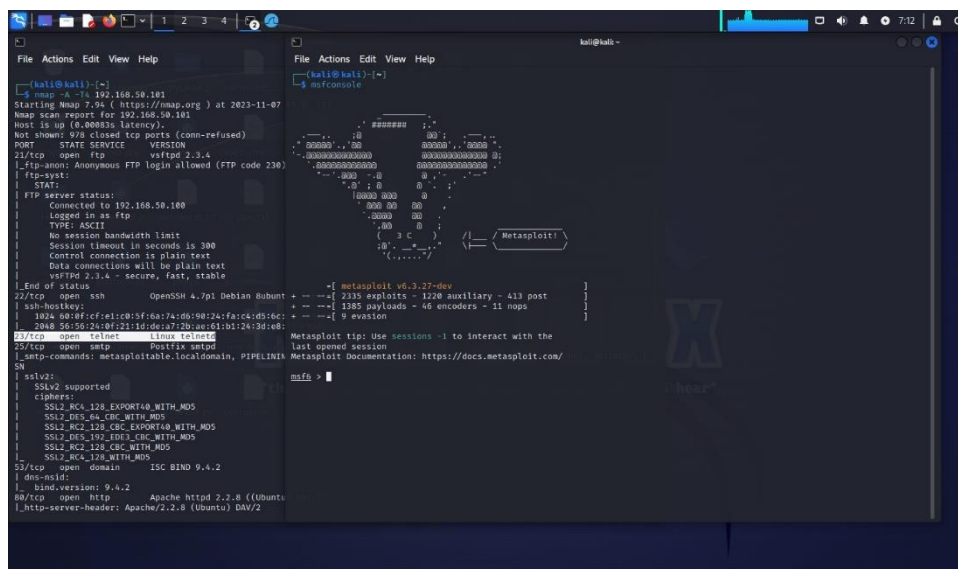
Prima di tutto controllo che le macchine riescano a pingare



A questo punto, verificata la comunicazione tra le macchine, faccio una ricerca approfondita (scansione) delle porte con nmap e vado a cercare la porta che ci serve, la 23 telnet

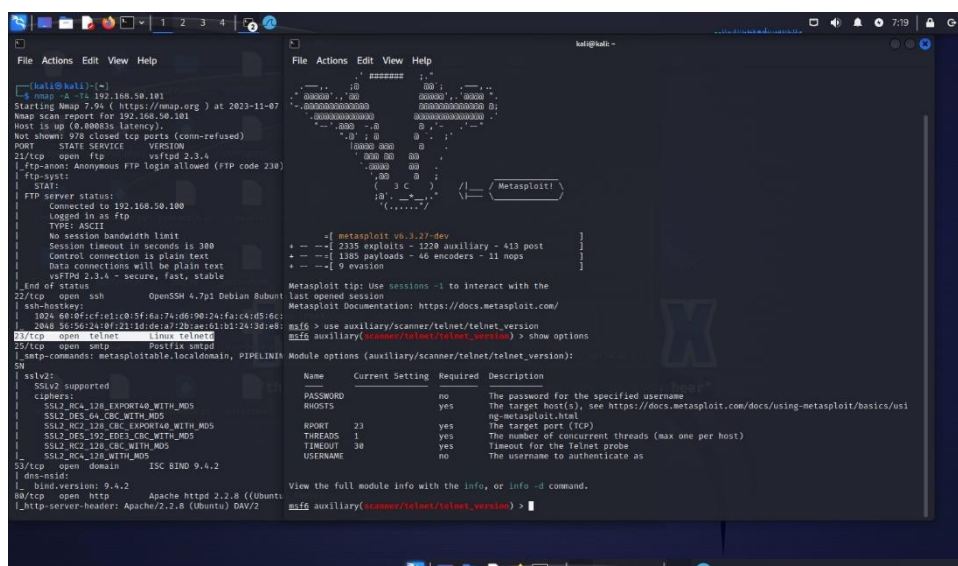


Fatto questo avvio Metasploit sulla macchina Kali



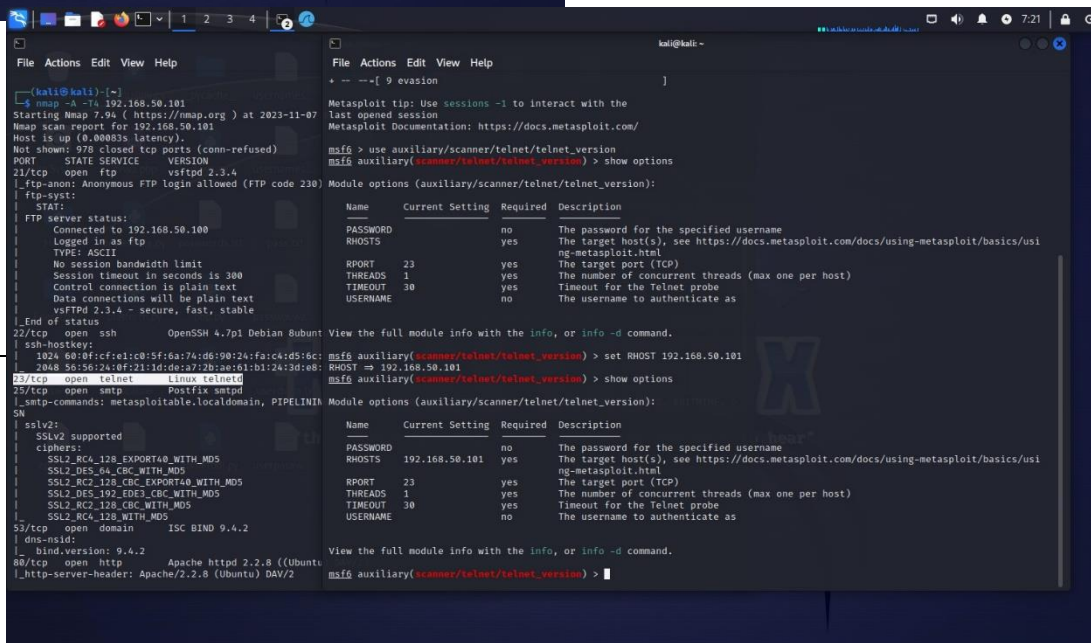
Avvio Metasploit

Quindi eseguo tutti i comandi per arrivare all'exploit:



Use e options

Set RHOST e verifica



Infine lancio l'Exploit che mi restituirà le credenziali e verifico di poter effettivamente entrare nella macchina vittima

```
(kali@kali)-[~]
$ nmap -A -T4 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07
Nmap scan report for 192.168.50.101
Host is up (0.000835 latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp             vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 192.168.50.100
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_  vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh             OpenSSH 4.7p1 Debian 8ubuntu
|_ssh-hostkey:
|_  1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:
23/tcp    open  telnet          Linux telnetd
23/tcp    open  smtp            Postfix smtpd
|_smtp-command: set metasploit.localdomain, PIPELINING
SN
|_sslv2:
|_SSLv2 supported
|_ciphers:
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
|_  SSL2_DES_64_CBC_WITH_MD5
|_  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_  SSL2_DES_192_EDE3_CBC_WITH_MD5
|_  SSL2_RC2_128_CBC_WITH_MD5
|_  SSL2_RC4_128_WITH_MD5
53/tcp    open  domain         ISC BIND 9.4.2
|_dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http            Apache httpd 2.2.8 ((Ubuntu
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

```
kali@kali: ~
File Actions Edit View Help

Name      Current Setting  Required  Description
PASSWORD  RHOSTS           no        The password for the specified username
RHOSTS    yes             The target host(s), see https://docs.metasploit.com/docs/using-metasploit/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 RHOST 192.168.50.101
RHOST => 192.168.50.101
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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

Name      Current Setting  Required  Description
PASSWORD  RHOSTS           no        The password for the specified username
RHOSTS    192.168.50.101  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/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) > exploit

[*] 192.168.50.101:23 - 192.168.50.101:23 TELNET
[*] 192.168.50.101:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > |
```

```

kali@kali: ~
File Actions Edit View H File Actions Edit View Help
$ nmap -A -T4 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org )
Nmap scan report for 192.168.50.101
Host is up (0.00083s latency)
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
ftp-anon: Anonymous FTP (vsFTPD 2.3.4 - secure)
ftp-syst:
  STAT:
FTP server status:
  Connected to 192.168.50.101
  Logged in as ftp
  TYPE: ASCII
  No session bandwidth
  Session timeout in 300 seconds
  Control connection is open
  Data connections will be established
vsFTPD 2.3.4 - secure
End of status
22/tcp    open  ssh
ssh-hostkey:
  1024 60:0f:cf:e1:c0:5f:2a:4d:4a:8b:1a:1a:1a:1a:1a:1a
  2048 56:56:24:0f:21:1c:2a:4d:4a:8b:1a:1a:1a:1a:1a:1a
23/tcp    open  telnet
25/tcp    open  smtp
smtp-commands: metasploit
SN
sslv2:
  SSLv2 supported
ciphers:
  SSL2_RC4_128_EXPORT40
  SSL2_DES_64_CBC_WITH_MD5
  SSL2_RC2_128_CBC_EXP
  SSL2_DES_192_EDE3_CBC
  SSL2_RC2_128_CBC_WITH_MD5
  SSL2_RC4_128_WITH_MD5
53/tcp    open  domain
dns-nsid:
  bind.version: 9.4.2
80/tcp    open  http
http-server-header: Apache/2.4.18 (Ubuntu)

```

N.B. Nel comando show options è importante che tutti i “Required” contrassegnati con “yes” siano inseriti, quelli invece contrassegnati con “no” sono facoltativi.