

## Introduzione:

L'obiettivo del compito è quello di **exploitare** metasploitable attraverso alcune **vulnerabilità del protocollo telnet**. Attraverso sempre **Metasploit** installato sulla macchina Kali Linux.

## Preparazione:

Vediamo subito se la porta del **servizio telnet 23** è aperta:

```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ nmap -p 23 192.168.0.102  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 06:52 EST  
Nmap scan report for 192.168.0.102  
Host is up (0.00s latency).  
tcp_23: RST: 0x00000000: 0x00000000 (192.168.0.102) [RST] Seq=123456789 Win=0 Len=0  
PORT      STATE SERVICE  
23/tcp    open  telnet  
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds  
(kali@kali)-[~]  
$
```

Dopo aver avuto conferma, avviamo Metasploit digitando **msfconsole** sul prompt di Kali:

```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ msfconsole 192.168.0.101  
Metasploit tip: You can upgrade a shell to a Meterpreter session on many  
platforms using sessions -u <session_id>  
Host is up (0.00s latency).  
  
Metasploit Park, System Security Interface  
Version 4.0.5, Alpha E  
Ready ...  
> access security  
access: PERMISSION DENIED.  
> access security grid  
access: PERMISSION DENIED.  
> access main security grid  
access: PERMISSION DENIED....and ...  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
  
+ -- ==[ 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 > 
```

Ed andiamo ad utilizzare un **exploit ausiliare**:

*use auxiliary/scanner/telnet/telnet\_version*

E tramite *show options* vediamo che manca il RHOSTS, ovvero l'IP della macchina vittima.

```
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    
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) > 
```

Tramite il comando **set** vado ad impostare l'IP di metasploitable:

```
msf6 auxiliary(scanner/telnet/telnet_version) >
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.0.102
rhosts => 192.168.0.102
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   | 192.168.0.102   | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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) > |
```

## Pratica:

Dopo aver digitando **exploit** e premuto invio, vengono raccolte informazioni sul servizio Telnet, come la versione e il banner. I **modelli ausiliari** come questo aiutano a identificare e raccogliere informazioni su potenziali vulnerabilità senza eseguire attacchi diretti.

Notiamo che questo exploit ci ha permesso di vedere informazioni che viaggiano in chiaro, come **username** e **password**, per accedere a metasploitable (evidenziate in giallo)

[illegible]

Ed ora avendo avuto accesso a quelle informazioni, posso accedere tranquillamente alla macchina, grazie alle credenziali viste:

[illegible]

## Conclusione:

Esporre Telnet, soprattutto con credenziali di default, è un rischio grave in un contesto reale. Gli amministratori dovrebbero:

- **Disabilitare** Telnet se non necessario.
- **Usare SSH** al posto di Telnet per una connessione sicura.
- Cambiare le credenziali di default e adottare **password forti**.