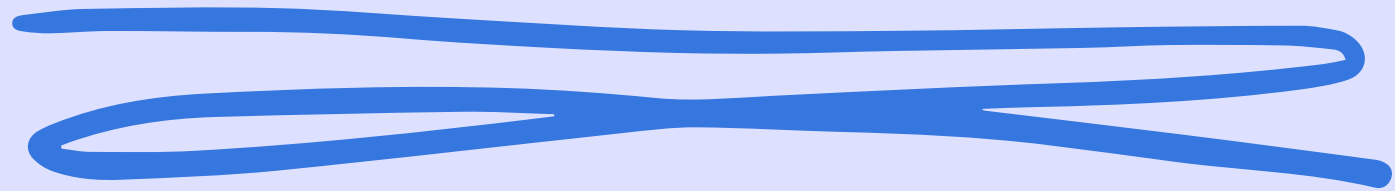


S7 L2

EXPLOIT TELNET META



Daniele Zizzi

EXPLOIT

Un exploit è un programma informatico, un software o una sequenza di comandi che sfrutta un errore o una vulnerabilità per provocare un certo comportamento nel software, nell'hardware o in qualsiasi dispositivo elettronico. Questi comportamenti possono includere l'assunzione del controllo di un sistema, la concessione di privilegi di amministratore a un intruso o l'avvio di attacchi di negazione del servizio (DoS o DDoS)



Ho effettuato una scansione con nmap con lo switch -sV, che mi permette di visualizzare la versione del servizio scansionato, in questo caso il telnet su porta 23.

```
(daniele@kali)-[~]  
$ nmap -sV 192.168.1.149 -p 23  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 13:18 CET  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try  
using --system-dns or specify valid servers with --dns-servers  
Nmap scan report for 192.168.1.149  
Host is up (0.00038s latency).  
  
PORT      STATE SERVICE VERSION  
23/tcp    open  telnet  Linux telnetd  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/  
submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

Metasploit [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:86:bd:ae  
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
```

Avvio metasploit da kali, attraverso il comando
msfconsole.

Cerco l'exploit di cui ho bisogno attraverso il comando "search telnet_version". Telnet è un protocollo per la connessione remota verso un host con l'utilizzo di una shell di comando.

Possiamo notare due exploit possibili, ma andremo ad utilizzare il secondo, come da traccia.

```
msf6 > search telnet_version
```

Matching Modules

```
# Name
ck Description
```

```
0 auxiliary/scanner/telnet/lantronix_telnet_version
  Lantronix Telnet Service Banner Detection
1 auxiliary/scanner/telnet/telnet_version
  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`

[illegible]

Diciamo al tool di utilizzare l'exploit desiderato attraverso il comando "use 1". Impostiamo l'ip della macchina vittima e poi visualizziamo le opzioni dell'exploit scelto, in modo da vedere se è configurato correttamente. L'exploit è configurato correttamente, quando i campi "required" sono tutti compilati.

Lanciamo l'attacco attraverso il comando "exploit".

L'exploit v   a buon fine e ci restituisce user e password per collegarci all'interfaccia telnet.

[illegible]