

CONSEGNA 5 MARZO S7L2

L'obiettivo odierno consiste nell'utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet utilizzando il modulo `auxiliary/telnet/version` sulla macchina Metasploitable. Mediante questo exploit, è stato possibile recuperare le credenziali d'accesso al servizio sopra menzionato, il quale è in ascolto sulla porta 23.

Inizialmente, è stato avviato msfconsole e successivamente è stato caricato il modulo ausiliario auxiliary/scanner/telnet/telnet_version. In seguito, è stato configurato l'indirizzo IP dell'host e infine è stato lanciato l'exploit. Come evidenziato nella Figura 1, è stato possibile ottenere le credenziali d'accesso al servizio Telnet (msfadmin, msadmin).

È da notare che il modulo ausiliario è stato progettato per svolgere funzioni di supporto durante il test di sicurezza. Tali moduli non eseguono necessariamente attacchi diretti, ma forniscono informazioni e supporto aggiuntivi che possono risultare utili per ottenere un quadro completo della sicurezza.

```
[*] Invalid parameter "option", use "show -h" for more information
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 RHOST 192.168.1.40
RHOST => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Fig.1