## EXPLOIT TELNET

WITH METASPLOIT

Metasploit Framework è uno strumento potente per il penetration testing. Questo report descrive l'utilizzo del **modulo auxiliary/scanner/telnet/telnet\_version** per sfruttare e identificare vulnerabilità relative al servizio Telnet sulla macchina Metasploitable.

## Ambiente di Test

- Target: Macchina virtuale Metasploitable 2
- IP del Target: 192.168.1.40
- Attacker: Kali Linux con Metasploit Framework installato

Metasploit Documentation: https://docs.metasploit.com/

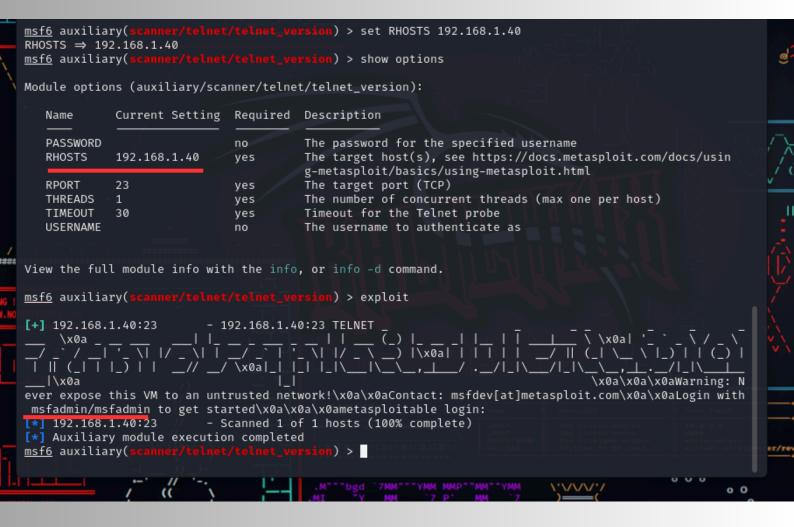
Modulo Usato: auxiliary/scanner/telnet/telnet\_version

## Objettivo

L'obiettivo è eseguire una scansione per identificare la versione del servizio Telnet in esecuzione sulla macchina target, che può rivelare informazioni utili per ulteriori exploit.

```
<u>ms+6</u> > use auxiliary/scanner/telnet/telnet version
msf6 auxiliary(
                                              ) > show options
Module options (auxiliary/scanner/telnet/telnet_version):
             Current Setting
                               Required Description
   Name
   PASSWORD
                                         The password for the specified username
                               no
                                         The target host(s), see https://docs.metasploit.com/docs/usin
   RHOSTS
                               yes
                                         g-metasploit/basics/using-metasploit.html
   RPORT
                                         The target port (TCP)
                                         The number of concurrent threads (max one per host)
   THREADS
                               yes
                                         Timeout for the Telnet probe
   TIMEOUT
   USERNAME
                                         The username to authenticate as
```

Il comando **show options** all'interno di Metasploit, visualizzi un elenco delle opzioni configurabili per il modulo attualmente selezionato. Queste opzioni includono variabili che devono essere impostate per eseguire correttamente il modulo, come l'indirizzo IP del target, la porta di destinazione, e altre configurazioni specifiche del modulo.



Configurare RHOSTS è un passaggio cruciale nell'uso di Metasploit perché definisce chiaramente quale o quali sistemi verranno presi di mira per la scansione o l'attacco. Senza questa configurazione, il modulo non avrebbe un target specifico su cui operare.

Il comando **exploit** è il passo finale per eseguire un attacco con Metasploit, sfruttando le vulnerabilità del sistema target per ottenere accesso e controllo.

Come vediamo abbiamo ottenuto i dati di login. (nell'img. sono sottolineati in rosso)