**Relazione sull’accesso a Metasploitable tramite Telnet utilizzando Metasploit**

**Introduzione**

In questo esercizio, l’obiettivo è stato quello di accedere a un sistema Metasploitable sfruttando il protocollo Telnet, utilizzando l’ambiente di pentesting Metasploit. Il protocollo Telnet, che permette l’accesso remoto tramite linea di comando, non è sicuro e può esporre le credenziali in chiaro, rendendo possibile l’accesso non autorizzato.

**Obiettivo**

Accedere al sistema Metasploitable ottenendo credenziali valide (username e password) attraverso Metasploit e poi utilizzarle per entrare nel sistema remoto.

**Procedura**

1. **Avvio di Metasploit e ricerca di exploit**

• Dopo aver aperto Metasploit con il comando msfconsole, abbiamo cercato moduli relativi a Telnet digitando il comando:

search telnet

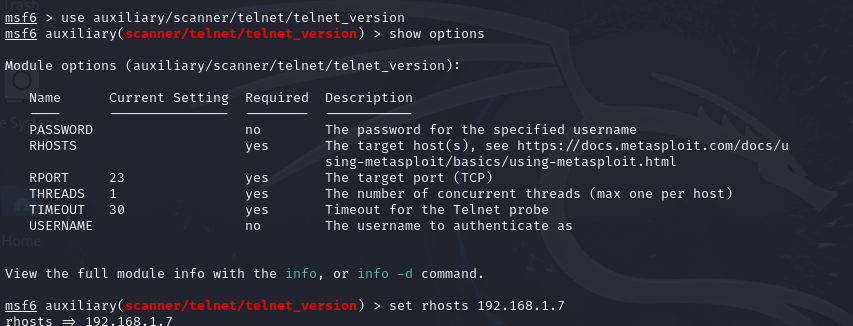
• Questa ricerca ha restituito una lista di moduli relativi a Telnet, tra cui scanner, exploit e auxiliary che potevano essere utilizzati per identificare vulnerabilità o ottenere informazioni sul protocollo Telnet del target.

2. **Scelta dell’exploit e configurazione del modulo**

• Tra i vari moduli, è stato scelto il modulo auxiliary/scanner/telnet/telnet\_version, utilizzato per ottenere informazioni sulla versione del servizio Telnet attivo sul sistema target.

• Abbiamo selezionato questo modulo con il comando:

use auxiliary/scanner/telnet/telnet\_version



3. **Configurazione dell’indirizzo IP del target**

• Dopo aver selezionato il modulo, è stato necessario configurare l’indirizzo IP del target, ovvero la macchina Metasploitable con IP 192.168.1.7. Questo è stato impostato con il comando:

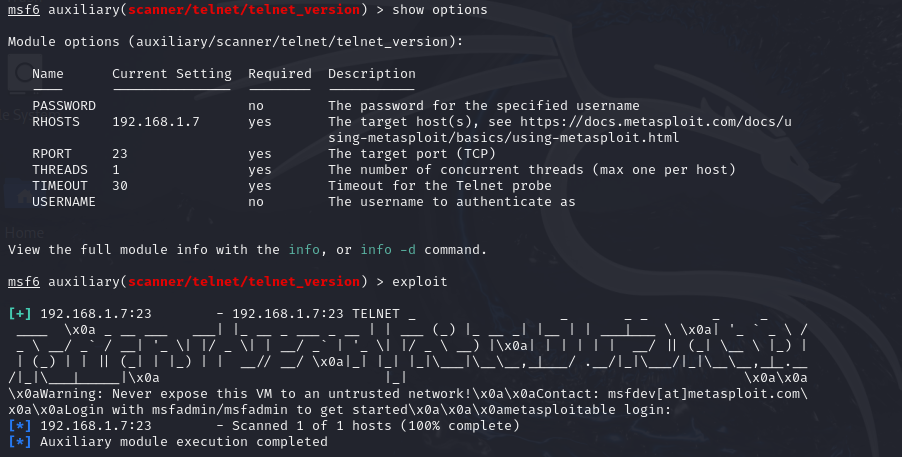
set RHOSTS 192.168.1.7

4. **Esecuzione dello scanner**

• Con il modulo configurato e l’indirizzo IP impostato, abbiamo avviato la scansione con il comando:

exploit

• Questo ha permesso di ricavare informazioni sul servizio Telnet e di individuare alcune credenziali di accesso valide, ovvero username e password per il sistema target.

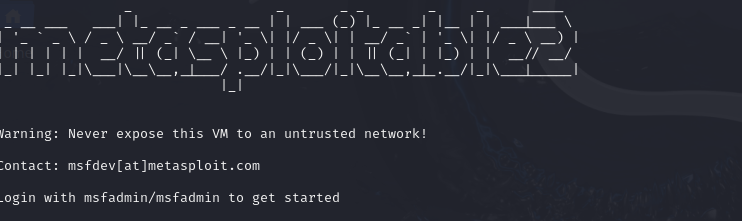


5. **Accesso al sistema tramite Telnet**

• Dopo aver ottenuto le credenziali, è stato possibile accedere al sistema Metasploitable utilizzando il comando Telnet da Metasploit:

telnet 192.168.1.7

• Abbiamo inserito username e password quando richiesto, ottenendo accesso alla shell del sistema target.



**Risultato**

L’operazione ha avuto successo, e siamo riusciti ad accedere al sistema Metasploitable tramite Telnet, utilizzando le credenziali acquisite. Questo accesso ha dimostrato come un servizio non sicuro come Telnet possa essere sfruttato in un contesto di test di penetrazione per ottenere accesso non autorizzato a un sistema vulnerabile.

**Conclusioni**

Questo esercizio evidenzia i rischi di utilizzare protocolli di comunicazione insicuri come Telnet, soprattutto su macchine esposte a reti non sicure. Sfruttando Metasploit, è possibile dimostrare come un attaccante possa individuare ed esplorare vulnerabilità legate a servizi obsoleti o non sicuri. In un contesto reale, sarebbe fortemente consigliato disabilitare Telnet e utilizzare protocolli sicuri come SSH per proteggere l’accesso remoto ai sistemi.