Relazione dell’Esercizio: Sfruttamento della Vulnerabilità Telnet con Metasploit

Obiettivo: Utilizzare Metasploit per rilevare la versione del servizio Telnet sulla macchina Metasploitable, sfruttando una vulnerabilità conosciuta tramite il modulo **telnet_version**.

Telnet_version è un modulo di tipo **ausiliario** e ha dunque l’obiettivo di **ottenere delle informazioni** dalla macchina vittima.

In questo esercizio andremo a rubare username e password di metasploitable. Le credenziali saranno in chiaro per via del protocollo non crittografato.

Richiamo dell’exploit

1. Aprire il terminale su **Kali Linux** e lanciare `msfconsole` per accedere all'interfaccia di Metasploit.
2. Caricare il modulo di scansione Telnet con il comando:
   `use auxiliary/scanner/telnet/telnet_version`

Importante: selezionare il modulo che ha come descrizione “Telnet Service Banner Detection”.

Telnet invia un messaggio di benvenuto di default quando riceve delle richieste. Questo messaggio si chiama **banner**.

Configurazione del Target

Impostiamo l’indirizzo IP di Metasploitable come dispositivo vittima:
`set rhosts 192.168.1.149`

Esecuzione del Modulo

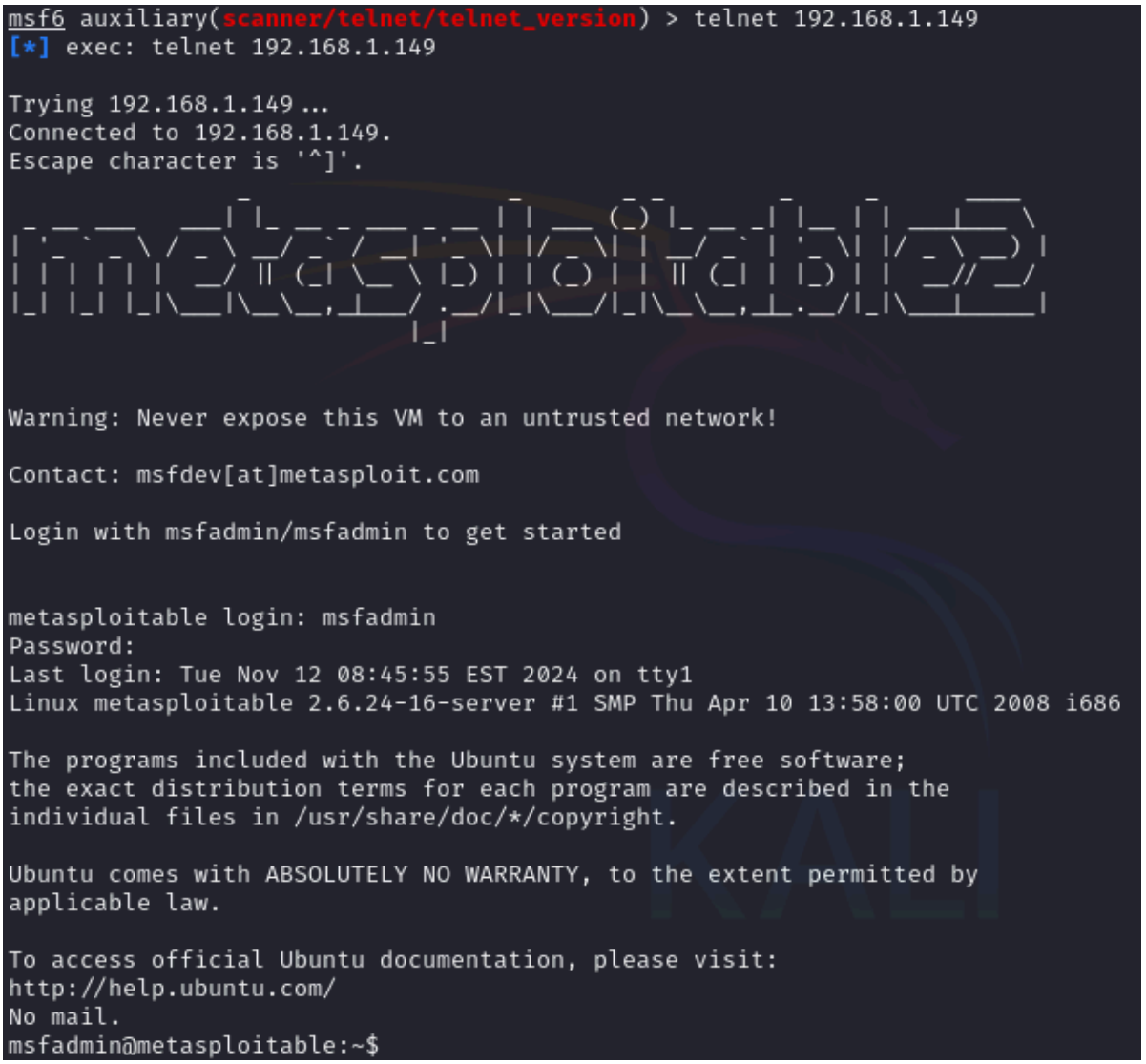
Eseguiamo l’exploit con il comando:
`exploit`

Risultato

Dopo l'esecuzione, se l'exploit ha avuto successo, ci restituirà le credenziali del servizio Telnet attivo su Metasploitable.

Questo ci permetterà poi di accedere da remoto alla macchina vittima, semplicemente utilizzando da terminale il comando `telnet 192.168.1.149`.

Una volta digitato il comando inseriamo le credenziali rubate per autenticarci e avremo accesso alla macchina vittima.



Considerazioni Finali

Tramite i moduli ausiliari, anche se non eseguono attacchi in modo diretto, possiamo ottenere delle informazioni molto preziose.

In questo caso, riusciamo addirittura a ottenenere le credenziali del servizio telnet del dispositivo vittima in pochi istanti e ad accedervi successivamente, senza che la vittima si accorga di tutto questo.

Questi moduli sono dunque molto utili nella fase di ricerca delle informazioni e ci permettono di comprendere quanto un dispositivo possa essere vulnerabile e accessibile da terzi senza autorizzazione.

I danni possono essere serissimi in base alle azioni effettuate dall'attaccante, dato che avrà l'accesso completo al dispositivo vittima.