Relazione Tecnica: Exploitation del Servizio Telnet su Metasploitable 2

Studente: Mirko Imbrogno

Corso: Cyber Security & Ethical Hacking - EPICODE

Oggetto: Analisi vulnerabilità, accesso e upgrade di sessione tramite servizio Telnet.

Introduzione e Obiettivi

L'attività svolta ha avuto come obiettivo l'analisi del servizio Telnet esposto sulla macchina target *Metasploitable 2*. Seguendo la metodologia del Penetration Testing, l'esercizio si è articolato in quattro fasi principali:

1. **Ricognizione:** Identificazione della versione del servizio Telnet.
2. **Accesso Iniziale:** Ottenimento di una shell di comando tramite credenziali note.
3. **Gestione Sessioni:** Interazione con la shell ottenuta.
4. **Post-Exploitation:** Upgrade della sessione da shell semplice a Meterpreter.

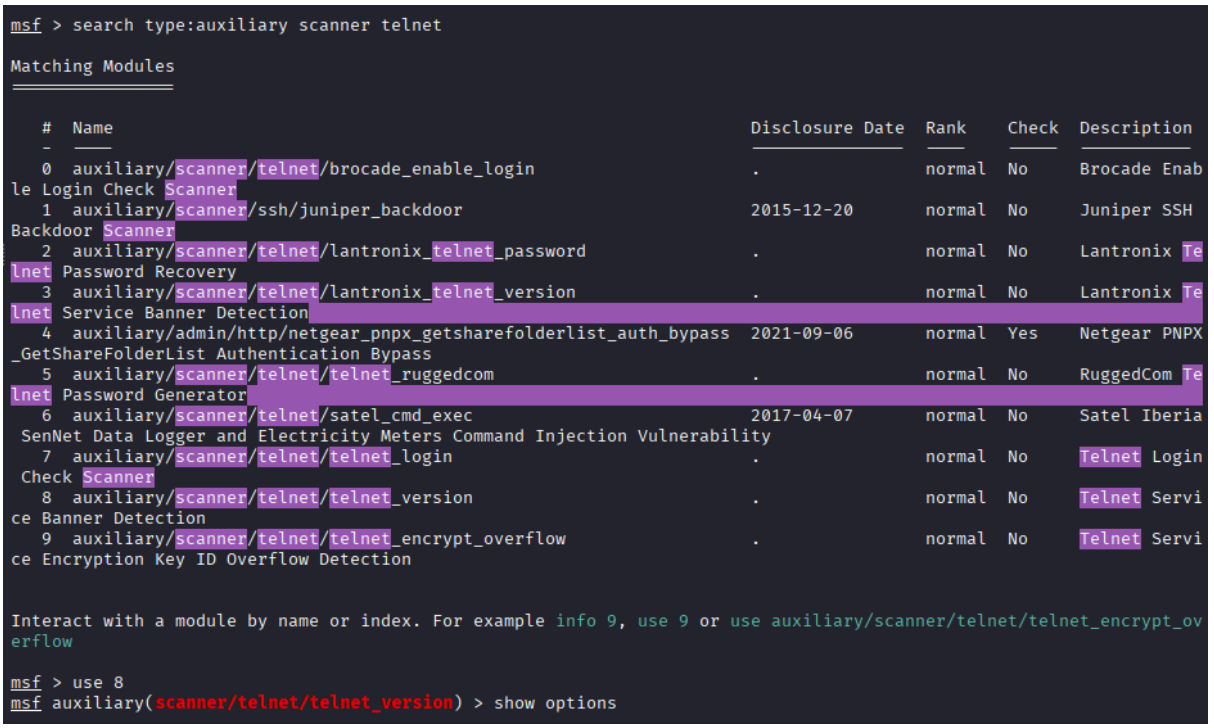
Fase di Preparazione

È stata avviata la console di Metasploit Framework (`msfconsole`) sulla macchina attaccante (Kali Linux) per preparare l'ambiente di test.

Avvio di Metasploit Framework.

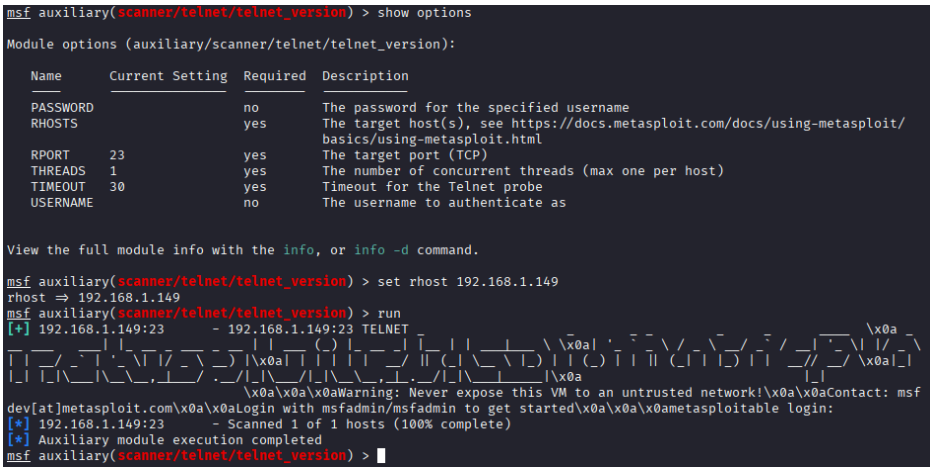
Fase 1: Scansione del Servizio (Information Gathering)

Per identificare le specifiche del servizio Telnet attivo sul target, è stato ricercato il modulo scanner appropriato nel database di Metasploit. È stato selezionato il modulo `auxiliary/scanner/telnet/telnet_version`.



Ricerca e selezione del modulo telnet_version.

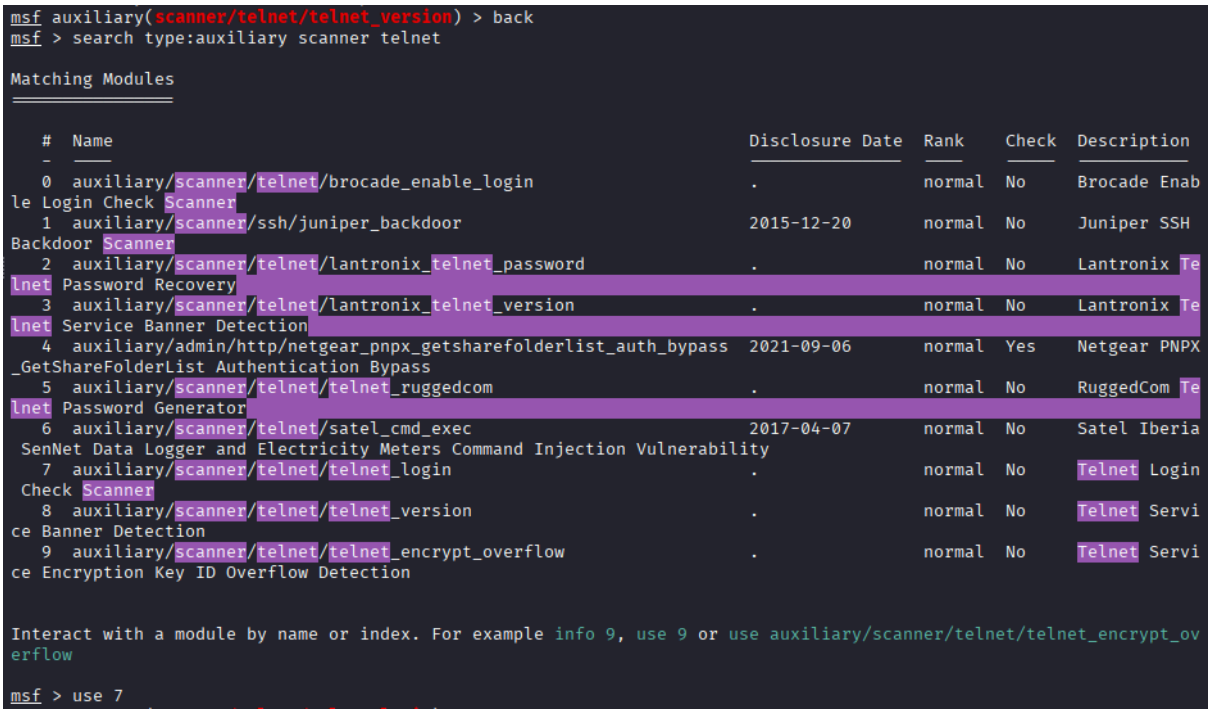
Successivamente, il modulo è stato configurato impostando l'indirizzo IP della macchina target (`RHOSTS 192.168.1.149`). L'esecuzione dello scanner ha confermato che la porta 23 è aperta e ha restituito il banner del servizio, identificando il sistema operativo come "Metasploitable" (Ubuntu).



Configurazione ed esito della scansione Telnet.

Fase 2: Autenticazione e Creazione della Sessione

Una volta confermata la presenza del servizio, si è proceduto al tentativo di accesso utilizzando credenziali note (`msfadmin:msfadmin`). È stato ricercato e selezionato il modulo `auxiliary/scanner/telnet/telnet_login`.



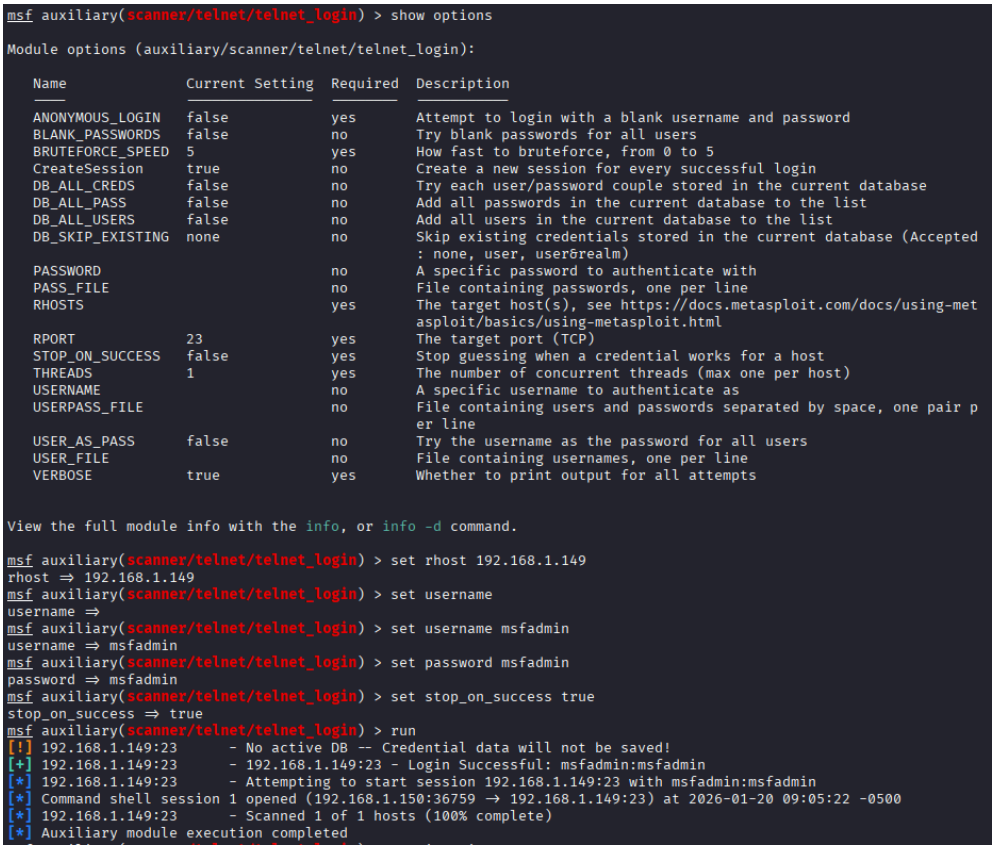
```
msf auxiliary(scanner/telnet/telnet_version) > back
msf > search type:auxiliary scanner telnet

Matching Modules
================

   #  Name                                                     Disclosure Date  Rank    Check  Description
   -  ----                                                     ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/brocade_enable_login                            .  normal  No     Brocade Enable Login Check Scanner
   1  auxiliary/scanner/ssh/juniper_backdoor                   2015-12-20       normal  No     Juniper SSH Backdoor Scanner
   2  auxiliary/scanner/telnet/lantronix_telnet_password                       .  normal  No     Lantronix Telnet Password Recovery
   3  auxiliary/scanner/telnet/lantronix_telnet_version                        .  normal  No     Lantronix Telnet Service Banner Detection
   4  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06       normal  Yes    Netgear PNPX_GetShareFolderList Authentication Bypass
   5  auxiliary/scanner/telnet/telnet_ruggedcom                        .  normal  No     RuggedCom Telnet Password Generator
   6  auxiliary/scanner/telnet/satel_cmd_exec                  2017-04-07       normal  No     Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
   7  auxiliary/scanner/telnet/telnet_login                    .  normal  No     Telnet Login Check Scanner
   8  auxiliary/scanner/telnet/telnet_version                  .  normal  No     Telnet Service Banner Detection
   9  auxiliary/scanner/telnet/telnet_encrypt_overflow         .  normal  No     Telnet Service Encryption Key ID Overflow Detection


Interact with a module by name or index. For example info 9, use 9 or use auxiliary/scanner/telnet/telnet_encrypt_overflow

msf > use 7
```

Selezione del modulo telnet_login.

Il modulo è stato configurato con i seguenti parametri:

- **RHOSTS:** `192.168.1.149` (Target)
- **USERNAME:** `msfadmin`
- **PASSWORD:** `msfadmin`
- **STOP_ON_SUCCESS:** `true` (per fermare il modulo al primo login valido).

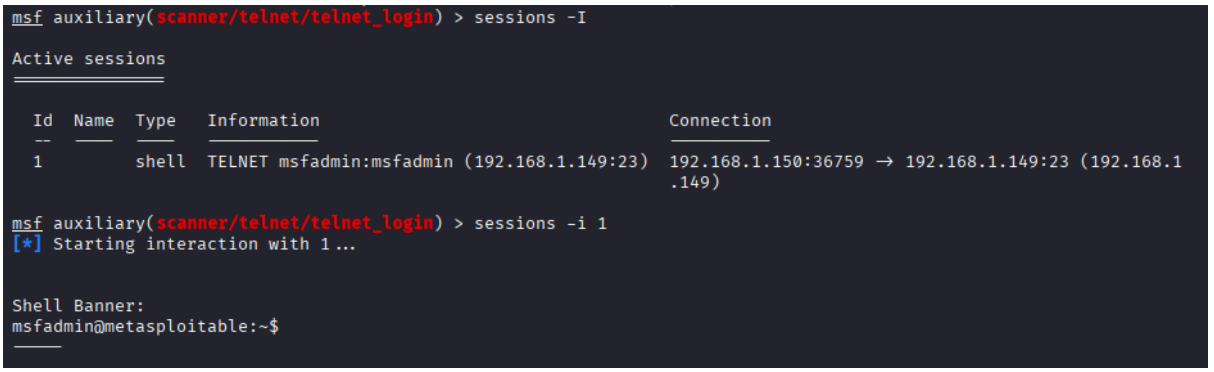
L'esecuzione ha avuto successo, portando all'apertura della **Sessione 1**.



Esecuzione del login e apertura della sessione shell.

Fase 3: Verifica e Gestione delle Sessioni

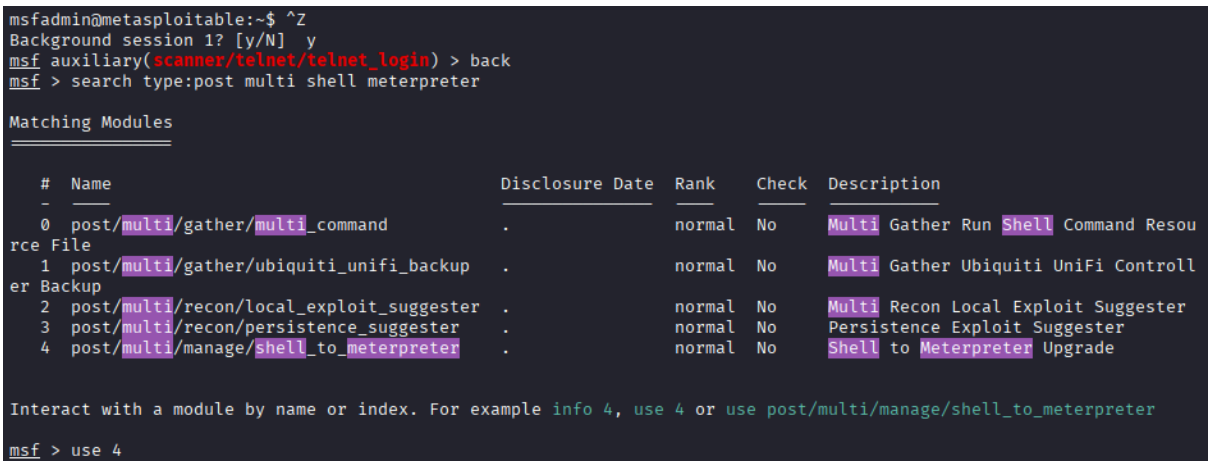
Per confermare la stabilità della connessione, sono state elencate le sessioni attive con il comando `sessions -I`. Successivamente, si è interagito con la sessione appena creata utilizzando il comando `sessions -i 1`. L'output ha confermato l'accesso alla shell del sistema target (`msfadmin@metasploitable:~$`).



Interazione con la sessione Telnet attiva.

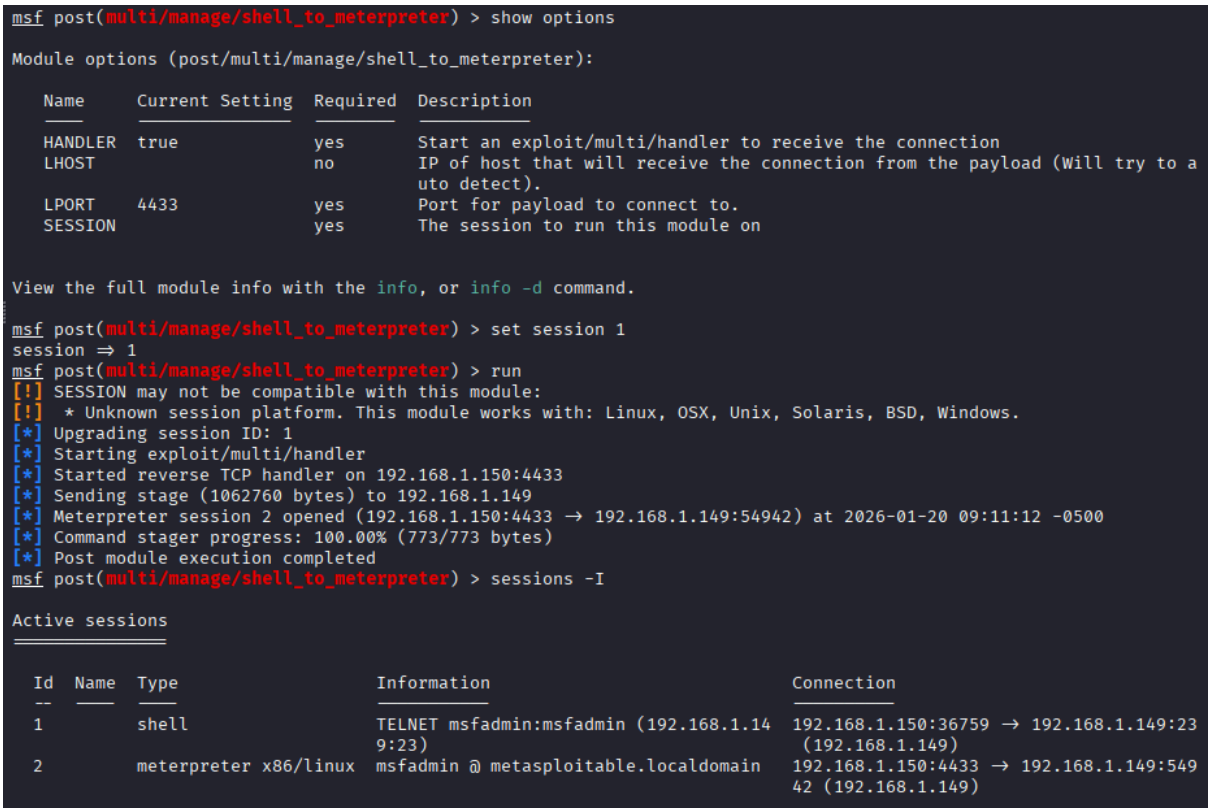
Fase 4: Upgrade della Sessione a Meterpreter

L'ultima fase ha riguardato l'elevazione della qualità della connessione, trasformando la shell di base in una sessione **Meterpreter**, che offre funzionalità avanzate di post-exploitation. La sessione 1 è stata messa in background (Backgrounding). È stato quindi ricercato il modulo di post-exploitation `post/multi/manage/shell_to_meterpreter`.



Background della sessione e ricerca del modulo di upgrade.

Il modulo è stato configurato impostando il parametro `SESSION` su `1` (l'ID della shell Telnet precedentemente ottenuta). L'esecuzione del modulo ha avviato un handler locale sulla porta 4433 e ha inviato lo stage al target. L'operazione si è conclusa con successo aprendo la **Sessione 2 (Meterpreter)**. La verifica finale con `sessions -I` mostra ora due sessioni attive: la shell originale e la nuova sessione Meterpreter.



Esecuzione dell'upgrade e conferma della sessione Meterpreter.

Conclusioni

L'esercitazione ha dimostrato come un servizio Telnet configurato con credenziali deboli o di default possa essere facilmente sfruttato per ottenere l'accesso iniziale a un sistema. Inoltre, è stato verificato come sia possibile scalare da una shell limitata a uno strumento potente come Meterpreter utilizzando i moduli di post-exploitation di Metasploit, evidenziando l'importanza di disabilitare servizi non sicuri come Telnet in favore di protocolli cifrati come SSH.