Report Tecnico: Analisi, Exploit e Post-Exploitation del Servizio Telnet

1. Introduzione

Il presente documento descrive le attività di penetration testing condotte contro l'host target **Metasploitable 2** (`192.168.1.149`). L'obiettivo dell'esercitazione è analizzare le vulnerabilità del protocollo Telnet, ottenere l'accesso tramite credenziali note e procedere all'upgrade della sessione per massimizzare il controllo sul sistema.

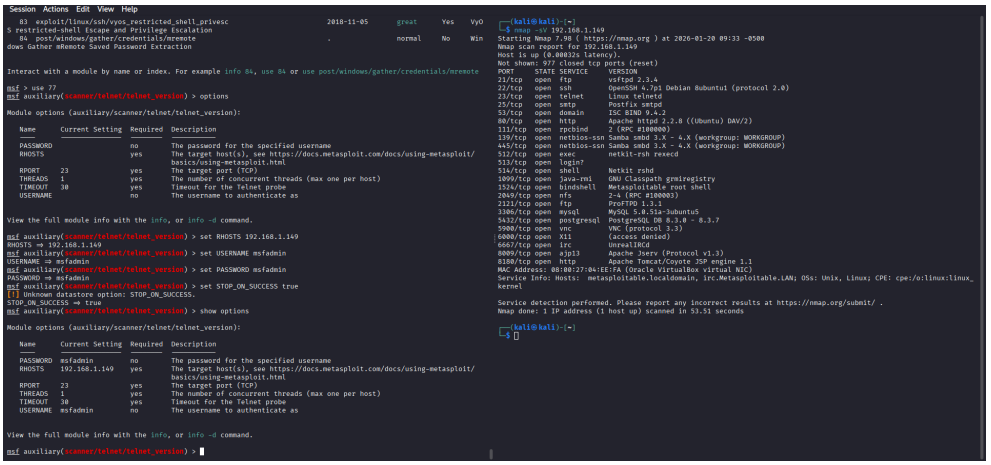
Come preparazione per l'esercizio, apriamo **Metasploit** eseguendo il comando `msfconsole`

2. Fase 1: Scansione e Fingerprinting

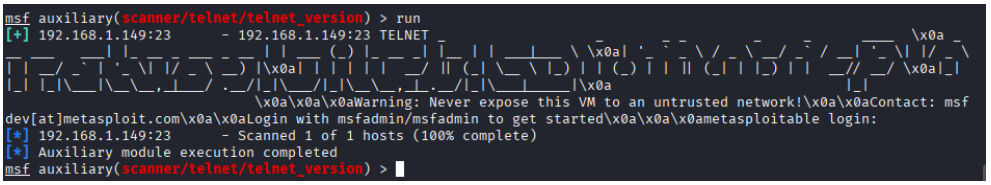
La fase di ricognizione è fondamentale per identificare la superficie di attacco e i servizi attivi sul target.

- **Scansione di Rete**: Utilizzando lo strumento `nmap -sV`, è stata identificata la porta **23/tcp** come aperta, confermando la presenza del servizio `Linux telnetd`.

- **Identificazione della Versione**: Per approfondire l'analisi, è stato caricato il modulo Metasploit `auxiliary/scanner/telnet/telnet_version`.



- **Analisi dell'Output**: L'esecuzione del comando `run` ha permesso di catturare il banner del servizio.

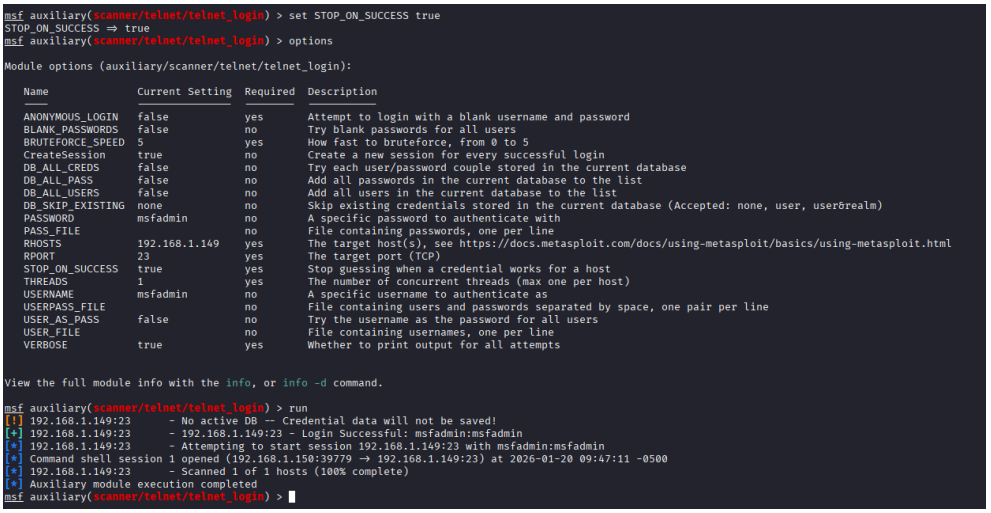


---

3. Fase 2: Autenticazione e Creazione della Sessione

Una volta confermata l'accessibilità del servizio, si è proceduto al tentativo di login sfruttando le credenziali di sistema predefinite.

- **Configurazione Modulo**: È stato selezionato il modulo `auxiliary/scanner/telnet/telnet_login`. Tramite il comando `show options`, sono stati impostati i parametri necessari:
    - `RHOSTS`: Indirizzo IP del target (`192.168.1.149`).
    - `USERNAME` e `PASSWORD`: Inserite le credenziali note `msfadmin`.
    - `STOP_ON_SUCCESS`: Impostato su `true` per arrestare il modulo una volta stabilita la connessione.



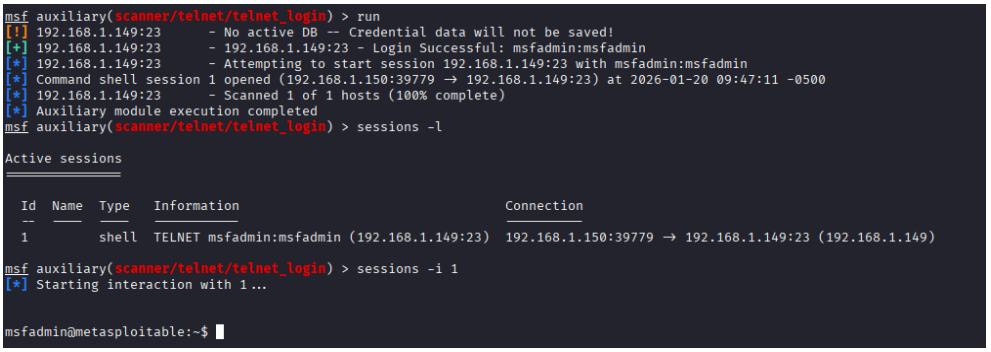
- **Ottenimento della Shell**: Il modulo ha verificato correttamente le credenziali, avviando una sessione di comando interattiva (Command Shell session 1).

---

4. Fase 3: Gestione delle Sessioni

In questa fase è stata verificata la stabilità della connessione e l'identità dell'utente sul sistema remoto.

- **Elenco Sessioni**: Utilizzando il comando `sessions -l`, è stata confermata l'apertura di una shell di tipo `telnet`.
- **Interazione**: Tramite `sessions -i 1`, è stata avviata l'interazione con il target. Il comando `uname -a` ha confermato i dettagli del sistema operativo Linux Metasploitable.

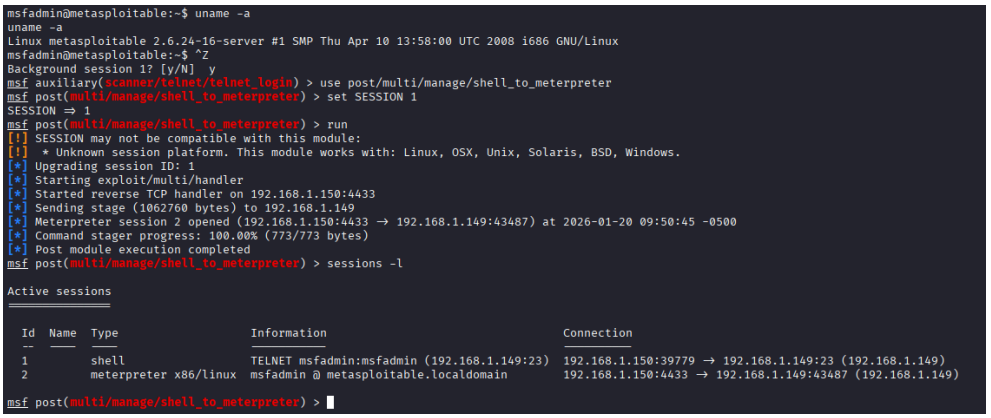


---

5. Fase 4: Upgrade a Meterpreter

Per ottenere funzionalità di post-exploitation avanzate, la shell standard è stata convertita in una sessione Meterpreter.

- **Backgrounding**: La sessione attiva è stata messa in pausa con `Ctrl+Z` per tornare al prompt di Metasploit.
- **Upgrade del Payload**: È stato utilizzato il modulo `post/multi/manage/shell_to_meterpreter`.
- **Esecuzione**: Dopo aver impostato l'ID della sessione (`set SESSION 1`), il modulo ha inviato lo stage Meterpreter al target.
- **Verifica Finale**: Un controllo finale con `sessions -l` ha mostrato la nuova sessione `meterpreter x86/linux` attiva e pronta all'uso.



Da qui sarà possibile ottenere i permessi di **root** attraverso vari **exploit**, ma lo vedremo nella prossima puntata.

---

6. Conclusioni

L'esercitazione ha dimostrato come l'uso di protocolli non cifrati e l'omissione del cambio delle credenziali di default espongano il sistema a rischi critici. Il successo dell'upgrade a Meterpreter evidenzia come un attaccante possa rapidamente passare da un accesso limitato a una compromissione totale della macchina.