EXPLOIT TELNET CON METASPLOIT

1)PUNTI CHIAVE

- Analisi servizio telnet
- Accesso Metasploitable
- Gestione Accessi
- Upgrade sessione a Meterpreter

2)INTRODUZIONE

L'attività si è concentrata sull'analisi e lo sfruttamento del servizio **Telnet** attraverso l'uso di **Metasploit.**

È stato eseguito un attacco a dizionario per ottenere l'accesso, seguito dalla gestione e upgrade della sessione da **shell** a **Meterpreter.**

3)OBIETTIVO

Gli obiettivi sono:

- Analizzare il servizio telnet
- Ottenere accesso alla Metasploitable con attacco a dizionario
- Gestire le sessioni
- Upgrade sessione a Meterpreter

4)STRUMENTI

- **Metasploitable ----->** macchina target
- **Metasploit ----->** piattaforma di attacco

5)SVOLGIMENTO

5.1) ANALISI SERVIZIO TELNET

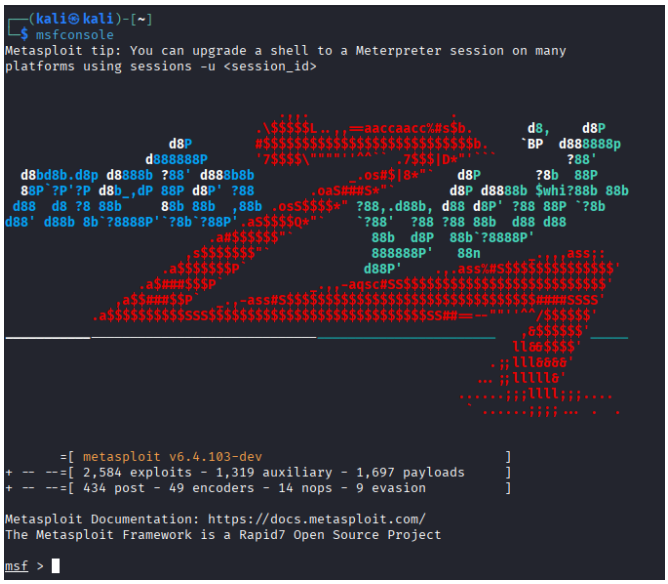

Fig.1 Accesso Metasploit

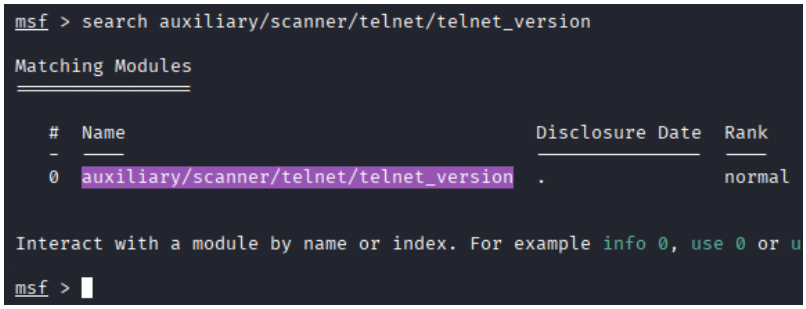

Fig.2 Ricerca modulo

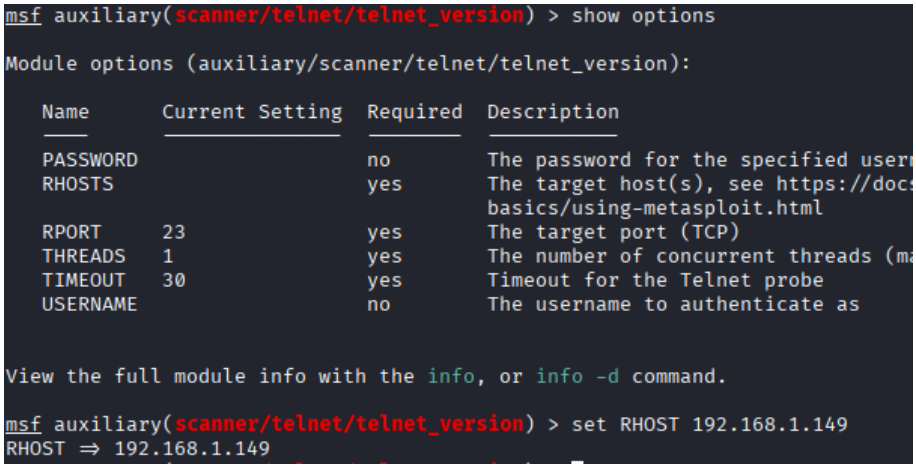

Fig.3 Configurazione modulo

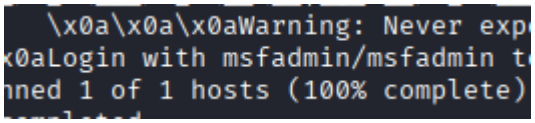

*Fig.4 Risultato exploit

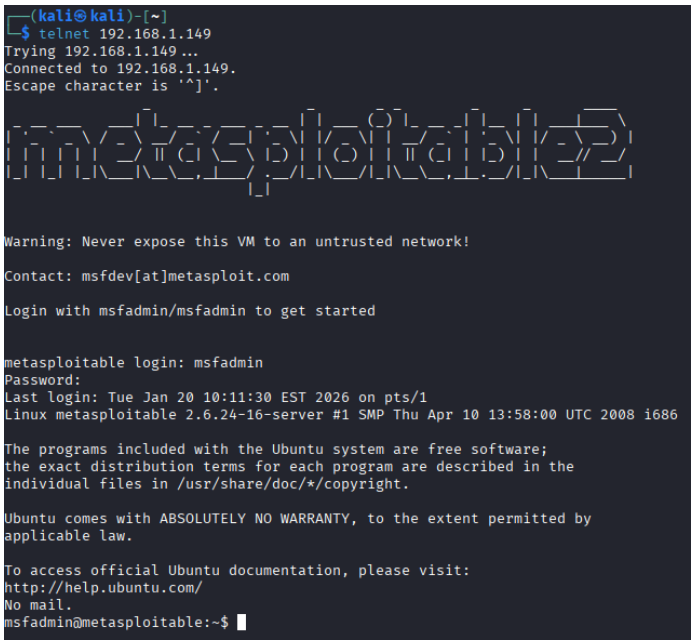

*Fig.5 Verifica accesso Metasploitable

Per fare un'analisi del servizio telnet, viene usato il modulo ***auxiliary/scanner/telnet/telnet_version*** che permette di **identificare e analizzare i servizi Telnet attivi** su uno o più target.

Nella configurazione del modulo vengono inserite:

- **RHOST ----->** IP Metasploitable (192.168.1.149)

Lanciando l'attacco, è stato possibile recuperare le credenziali di accesso al servizio **telnet** e sono state verificate attraverso il comando ***telnet 192.168.1.149***

5.2) ACCESSO A METASPLOITABLE CON ATTACCO A DIZIONARIO

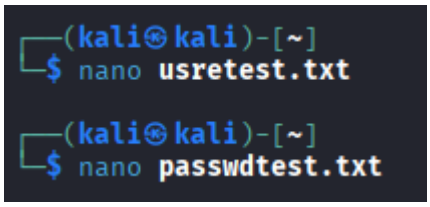

*Fig.6 Creazione liste password

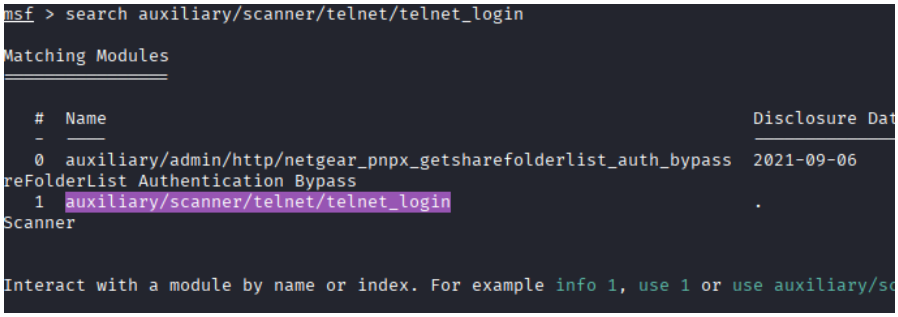

Fig.7 Ricerca modulo

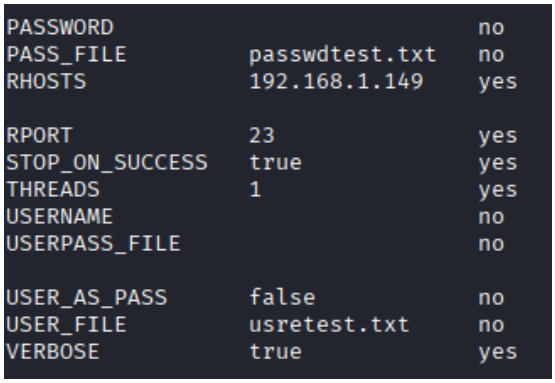

Fig.8 Configurazione modulo

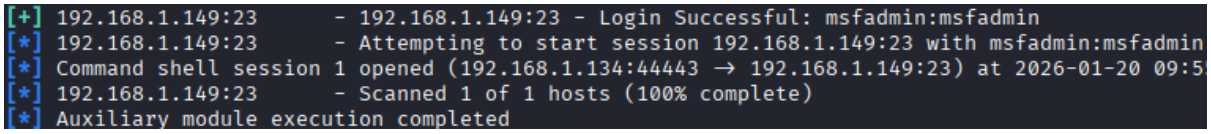

Fig.9 Lancio exploit

Prima di passare al login del servizio attraverso un attacco a dizionario, sono state simulate delle liste di usernames e passwords che verranno usate da Metasploit per il cracking.

Viene usato il modulo ***auxiliary/scanner/telnet/telnet_login*** che prenderà in questo caso un elenco di password e username in un determinato range di indirizzi IP per accedere a qualsiasi servizio telnet attivo.

Nella configurazione vengono inseriti:

- **RHOST: 192.168.1.149 ----->** IP macchina target
- **USER_FILE: usretest.txt ----->** Lista usernames
- **PASS_FILE: passwdtest.txt ----->** Lista passwords
- **STOP_ON_SUCCESS ----->** permette di fermare l'operazione al primo login riuscito

Al momento del lancio,Metasploit cercherà le diverse combinazioni fra le due liste fino a trovare un nome utente e password corrispondenti.

Una volta trovate le credenziali e aver effettuato l'accesso al servizio telnet,si passa alla gestione delle sessioni.

5.3) GESTIONE ACCESSI

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

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

  Id  Name  Type   Information                              Connection
  --  ----  ----   -----------                              ----------
  1         shell  TELNET msfadmin:msfadmin (192.168.1.149:23)  192.168.1.134:37679 → 192.168.1.149:23 (192.168.1.149)
```

Fig.10 Lista sessioni attive

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


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

Fig.11 Background sessione

Per gestire le sessioni vengono utilizzati diversi comandi:

- **sessions –l ----->** permette di vedere la lista di sessione attive
- **sessions –i {ID sessione} ---->** permette di interagire con una delle sessioni attive
- **Ctrl + z ---->** consente di mettere in background una sessione

5.4) UPGRADE SESSIONE A METERPRETER

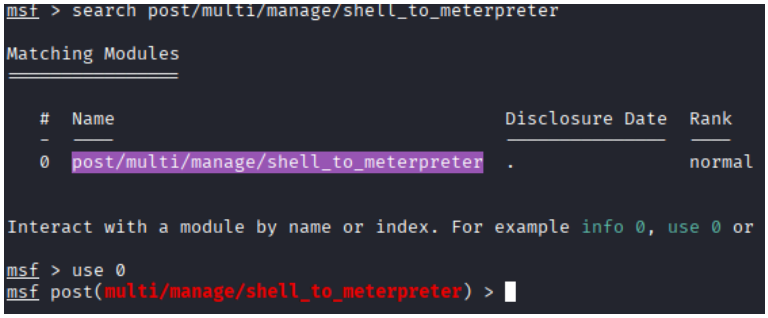

*Fig.12 Ricerca modulo meterpreter

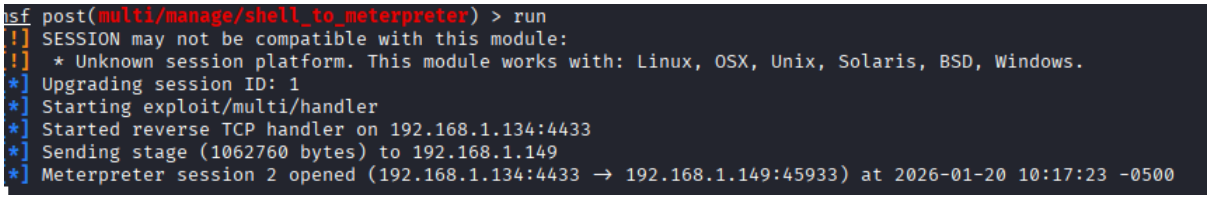

*Fig.13 Lancio exploit

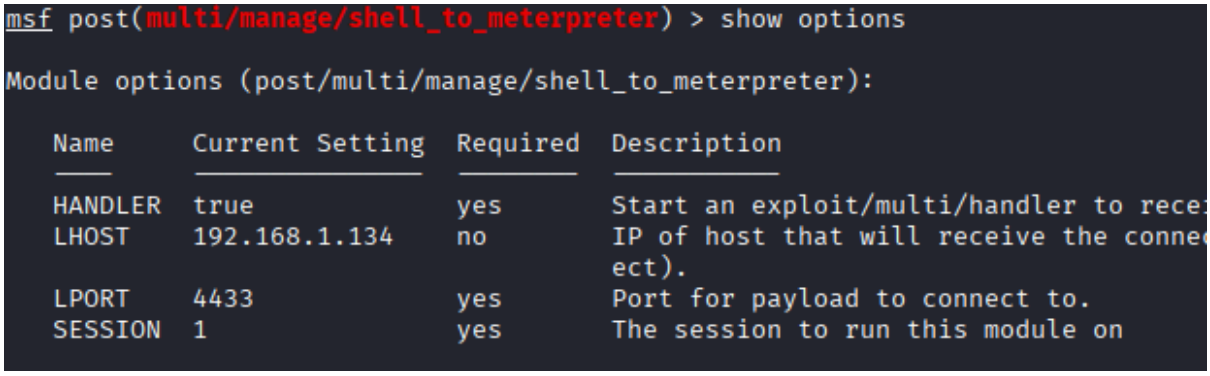

*Fig.14 Configurazione modulo

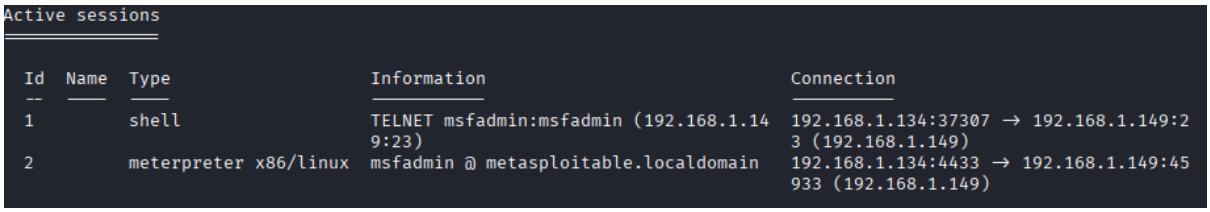

*Fig.15 Verifica upgrade

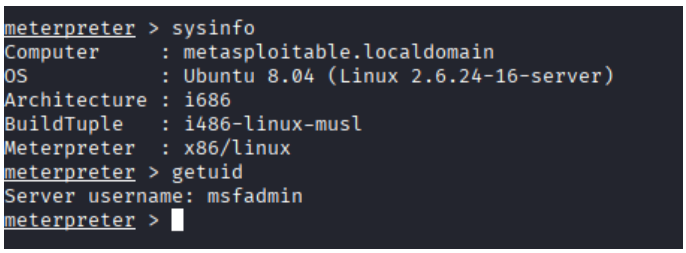

*Fig.16 Verifica meterpreter

Per effettuare un upgrade di una sessione da shell a **meterpreter**, viene caricato il modulo ***post/multi/manage/shell_to_meterpreter*** ,

Vengono configurati:

- **LHOST: 192.168.1.134 ---->** IP della macchina a cui il target dovrà connettersi
- **SESSION: 1 ----->** ID della sessione

Viene successivamente verificata l'operazione di migrazione attraverso il comando ***session –l*** e come mostrato in ***Fig.13,*** la nuova sessione **meterpreter** è stata creata.

Come ulteriore verifica, è stato confermato l'accesso al sistema tramite la sessione **meterpreter**, utilizzando i comandi **sysinfo** e **getuid** per raccogliere informazioni sul target.

---

6)CONCLUSIONE

Il report conferma la vulnerabilità di servizi legacy non solo attraverso attacchi a dizionario che hanno permesso di ottenere rapidamente l'accesso grazie all'uso di credenziali deboli ma anche dall'upgrade da shell a **meterpreter** che ha dimostrato la facilità con cui un attaccante può assumere controllo avanzato sulla macchina target.

Una soluzione è di disabilitare Telnet sostituendolo con protocolli come SSH e di adottare policy per le passwords.