S7/L2

Noemi de Martino

Traccia

Sulla base dell’esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Svolgimento

01 Avvio di Metasploit Framework:

Si è avviato **msfconsole**, l'interfaccia a riga di comando del Metasploit Framework.

Svolgimento

02 Selezione del modulo Telnet:

Si è eseguito il comando

auxiliary/scanner/telnet/telnet_version

per selezionare e utilizzare il modulo Telnet di Metasploit.

```
msf6 > scanner/telnet/telnet_version
[-] Unknown command: scanner/telnet/telnet_version
This is a module we can load. Do you want to use scanner/telnet/telnet_version? [y/N]   y
msf6 auxiliary(scanner/telnet/telnet_version) > info
```

03 Verifica dei parametri del modulo

Si è eseguito il comando “**info**” per visualizzare i parametri configurabili del modulo Telnet selezionato.

```
This is a module we can load. Do you want to use scanner/telnet/telnet_version? [y/N]   y
msf6 auxiliary(scanner/telnet/telnet_version) > info

       Name: Telnet Service Banner Detection
     Module: auxiliary/scanner/telnet/telnet_version
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <x@hdm.io>

Check supported:
  No

Basic options:
  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/b
                                       asics/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

Description:
  Detect telnet services

View the full module info with the info -d command.
```

04 Impostazione dell'host target ed esecuzione:

- Si è impostato l'indirizzo IP del target (Metasploitable) utilizzando il comando

set RHOSTS 192.168.1.149

- Si è lanciato l'esecuzione del modulo con il comando **exploit**
- Dall'output generato, si è ottenuto le credenziali di accesso **msfadmin/msfadmin.**

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.149:23      - 192.168.1.149:23 TELNET _                  _     _ _     _     _     ____  \x0a _
__ ___   ___| |_ __ _ ___ _ __ | |  ___ (_) |_ __ _| |__ | |  ___|____ \ \x0a| '_ ` _ \ / _ \__/ _` / __| '_ \| |/ _ \
| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_|
|_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|______|\x0a                              |_|
                              \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msf
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
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Svolgimento

05 Accesso al sistema target via Telnet:

- Si è eseguito il comando **telnet 192.168.1.149** per connettersi all'indirizzo di Metasploitable

- Si è utilizzato le credenziali **msfadmin/msfadmin** per effettuare l'accesso con successo.