Riccardo Agostino Monti

S7 L2
HACKING CON METASPLOIT

Scopo del test

Nell’esercizio di oggi ci viene chiesto di collegarci alla macchina Metasploitable utilizzando telnet dal framework di metasploit.

Passo 1

Setup dell’exploit di scanning del telnet.

```
msf6 > search telnet_version

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

   #  Name                                                Disclosure Date  Rank    Check  Description
   -  ----                                                ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version                    normal  No     Lantronix Telnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version                              normal  No     Telnet Service Banner Detection


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version

msf6 > use auxiliary/scanner/telnet/telnet_version
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/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

Description:
  Detect telnet services


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

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.50.101
rhosts => 192.168.50.101
```

Passo 2

Collegamento tramite telnet a metasploitable2.

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.50.101:23     - 192.168.50.101:23 TELNET
[*] 192.168.50.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.50.101
[*] exec: telnet 192.168.50.101

Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^]'.
                                                  _
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```

Exploit

Un exploit informatico è un programma, un software o una sequenza di comandi che sfrutta un errore o una vulnerabilità in un software, hardware o qualsiasi dispositivo elettronico. Questo può provocare un comportamento non previsto o imprevisto.
Gli exploit sono spesso utilizzati per scopi malevoli.
Gli exploit informatici funzionano identificando una vulnerabilità o un difetto nel software o nell'hardware. Una volta identificata questa vulnerabilità, un hacker può scrivere un exploit con il preciso scopo di sfruttarla. Molti hacker utilizzano gli exploit per diffondere malware.

Protocollo TELNET

Il protocollo Telnet è un protocollo client-server che si basa sullo scambio di dati tramite connessioni TCP, permettendo la trasmissione di segnali. Consente il controllo remoto dei computer tramite input e output testuali. Viene stabilita una connessione client-server per impostazione predefinita tramite il protocollo di trasmissione TCP e la porta TCP 23.