Progetto Modulo 4

HACKING SERVIZIO JAVA RMI SU METASPLOITABLE 2

La Traccia

Traccia:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, 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 3) altro...

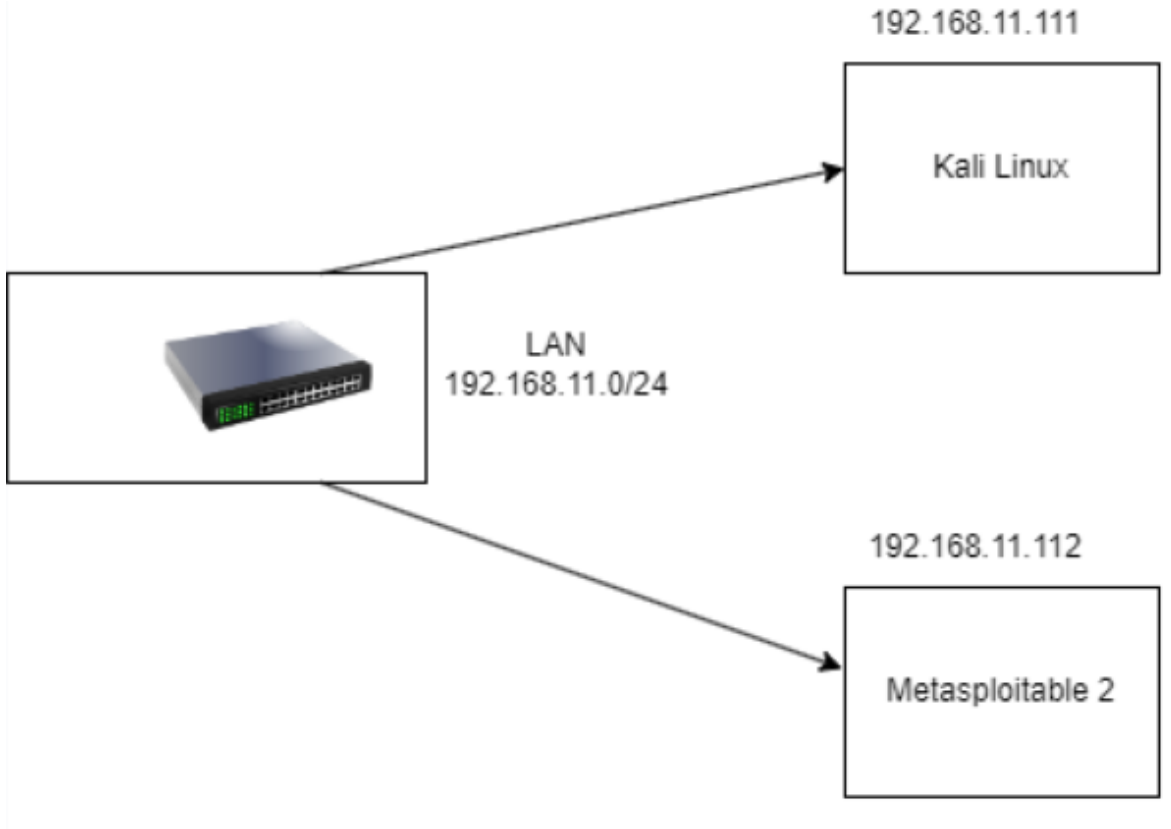
Introduzione e premesse.

Per «Kali» si intenderà la macchina Kali Linux utilizzata hackerare il servizio citato in precedenza, per «Meta» si intenderà la macchina Metasploitable 2 ovvero la macchina da hackerare.

Le macchine sono sulla stessa LAN, per convezione gli ip delle macchine saranno:

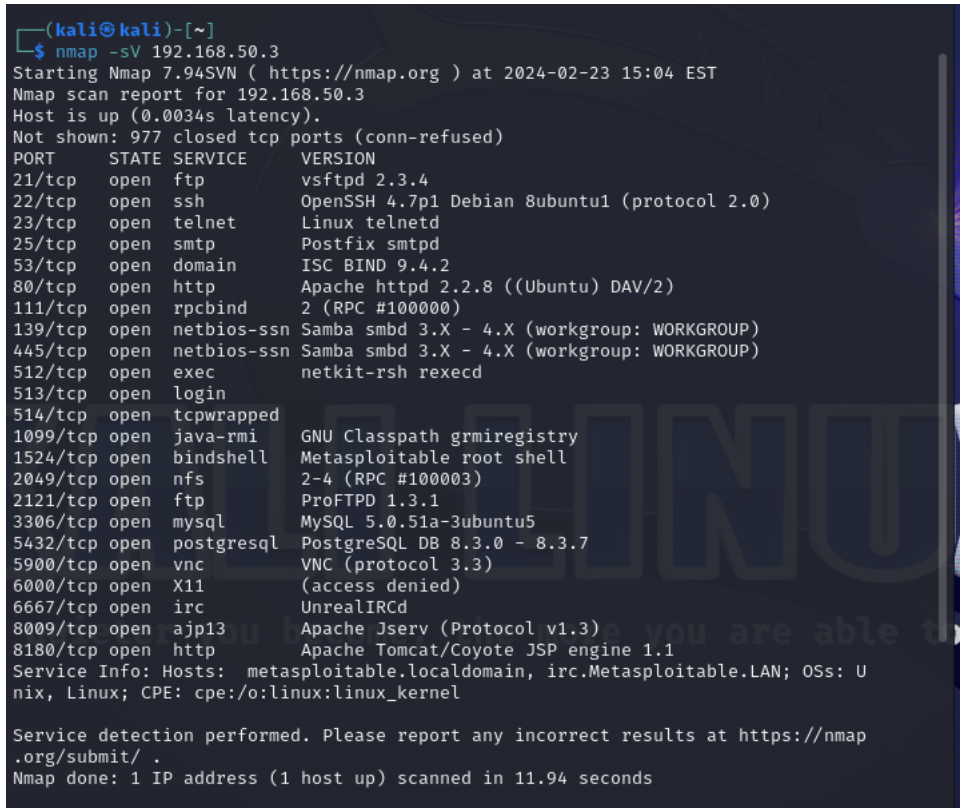
-Kali: 192.168.50.2

-Meta: 192.168.50.3



Attacco servizio Java Rmi

Per prima cosa avvio Nmap con lo switch –sV per visualizzare i servizi attivi sulla macchina attaccata Meta, tra cui quello che ci siamo prefissati di attaccare cioè Java Rmi sulla porta 1099.



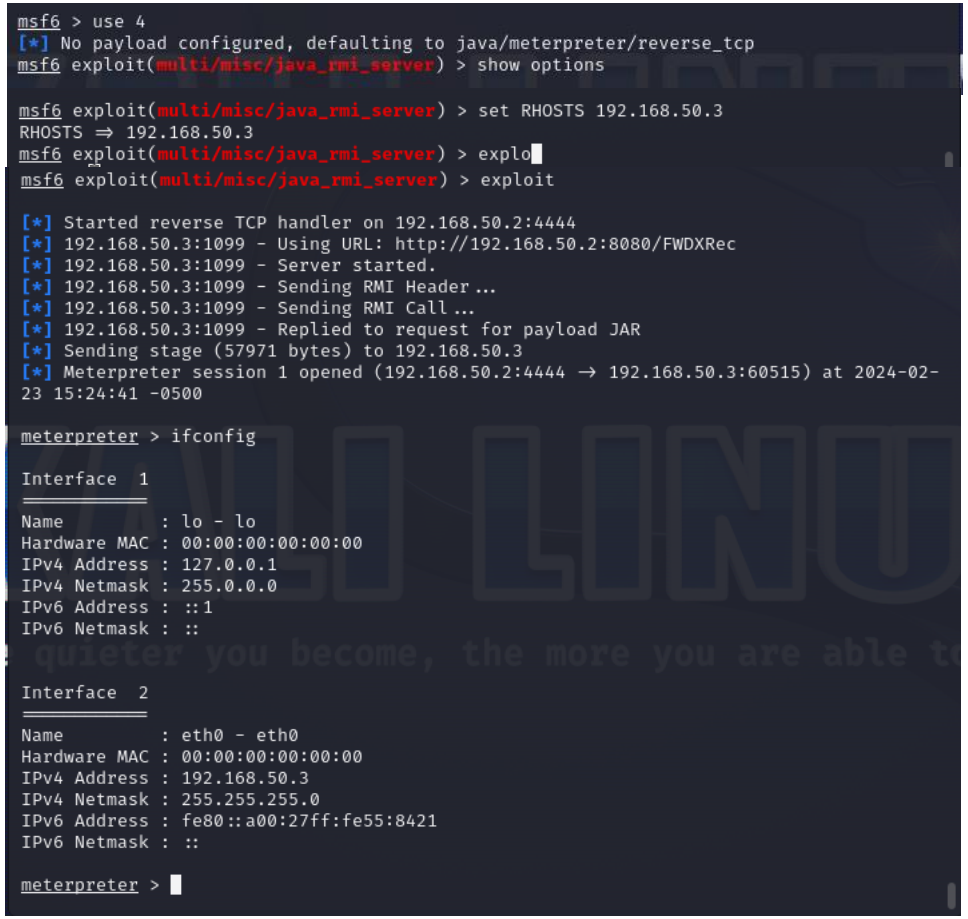
Attacco servizio Java Rmi

Avvio la Msfconsole ed uso il comando search per trovare i moduli per attaccare il servizio Java Rmi.

```
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


Interact with a module by name or index. For example info 15, use 15 or use exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc
```

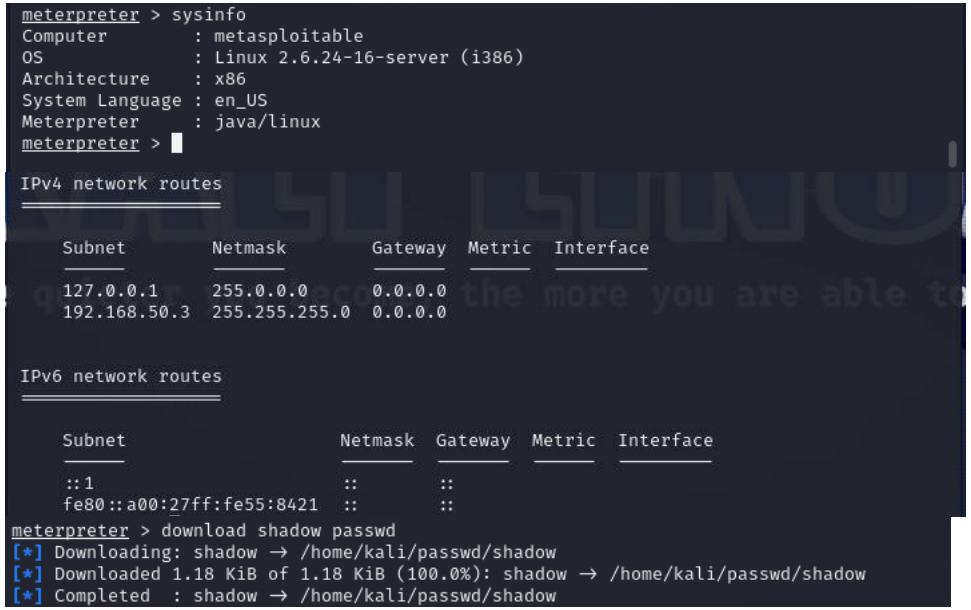
Attacco servizio Java Rmi

Utilizzo il modulo 'java_rmi_server', setto l'ip della macchina Meta da attaccare e lancio l'attacco con il comando 'exploit'.
Andato a buon fine inserisco comandi per raccogliere informazioni, il primo è 'ifconfig' per vedere la configurazione di rete.



Attacco servizio Java Rmi

Con ‘sysinfo’ ottengo le informazioni di sistema e con ‘route’ le informazioni di routing.
Scarico i file passwd e shadow in modo da poterli utilizzare con programmi come ‘John The Ripper’ per craccare le password dei vari utenti.



Attacco di altri servizi di Metasploitable 2

Con il modulo postgres_hashdump ottengo l'hash del DB postgres che posso craccare in un secondo momento