192.168.1.90

23	7	18	7	72
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 127

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.2	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	9.0	9.2	156164	Apache Log4Shell CVE-2021-45046 Bypass Remote Code Execution
CRITICAL	10.0	10.0	156016	Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)
CRITICAL	10.0	10.0	156056	Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)
CRITICAL	10.0	10.0	156257	Apache Log4Shell RCE detection via callback correlation (Direct Check DNS)
CRITICAL	10.0	10.0	156115	Apache Log4Shell RCE detection via callback correlation (Direct Check FTP)
CRITICAL	10.0	10.0	156014	Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP)
CRITICAL	10.0	10.0	156669	Apache Log4Shell RCE detection via callback correlation (Direct Check MSRPC)
CRITICAL	10.0	10.0	156197	Apache Log4Shell RCE detection via callback correlation (Direct Check NetBIOS)
CRITICAL	10.0	10.0	156559	Apache Log4Shell RCE detection via callback correlation (Direct

CRITICAL	10.0	10.0	156197	Apache Log4Shell RCE detection via callback correlation (Direct Check NetBIOS)
CRITICAL	10.0	10.0	156559	Apache Log4Shell RCE detection via callback correlation (Direct Check RPCBIND)
CRITICAL	10.0	10.0	156232	Apache Log4Shell RCE detection via callback correlation (Direct Check SMB)

192.168.1.90 11

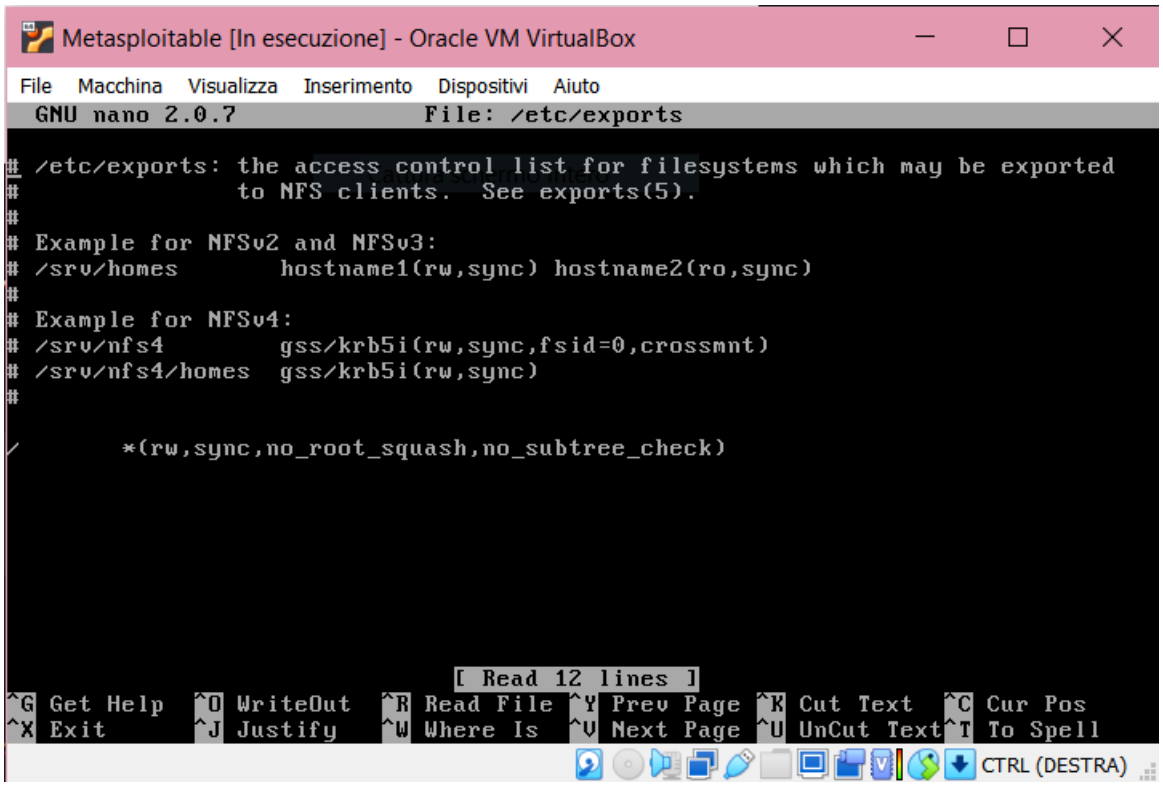
CRITICAL	10.0	10.0	156132	Apache Log4Shell RCE detection via callback correlation (Direct Check SMTP)
CRITICAL	10.0	10.0	156166	Apache Log4Shell RCE detection via callback correlation (Direct Check SSH)
CRITICAL	10.0	10.0	156162	Apache Log4Shell RCE detection via callback correlation (Direct Check Telnet)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.8	7.4	164017	NodeJS System Information Library Command Injection (CVE-2021-21315)
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable

Vulnerabilità scelte:

1) NFS EXPORTED SHARE INFORMATION DISCLOSURE

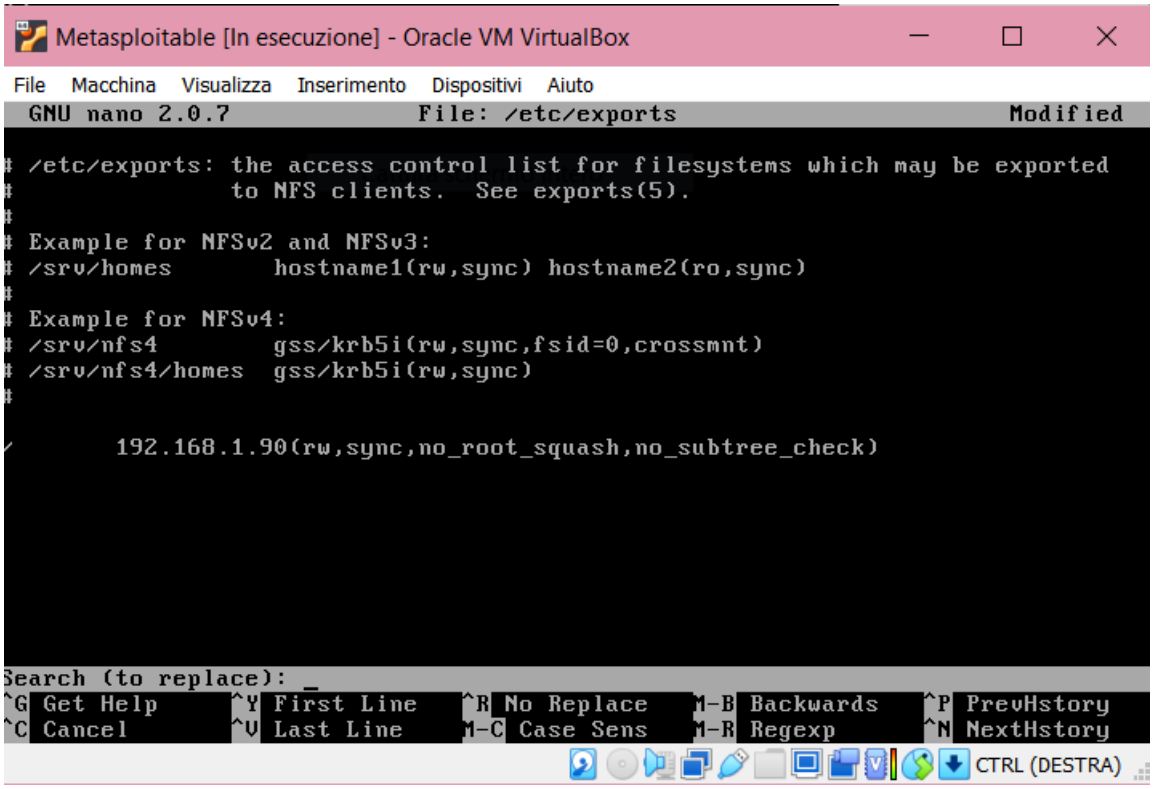
NFS (Network File System) è un protocollo di rete utilizzato in ambiente Unix per la condivisione di file.

Per risolvere la vulnerabilità bisogna modificare i permessi.



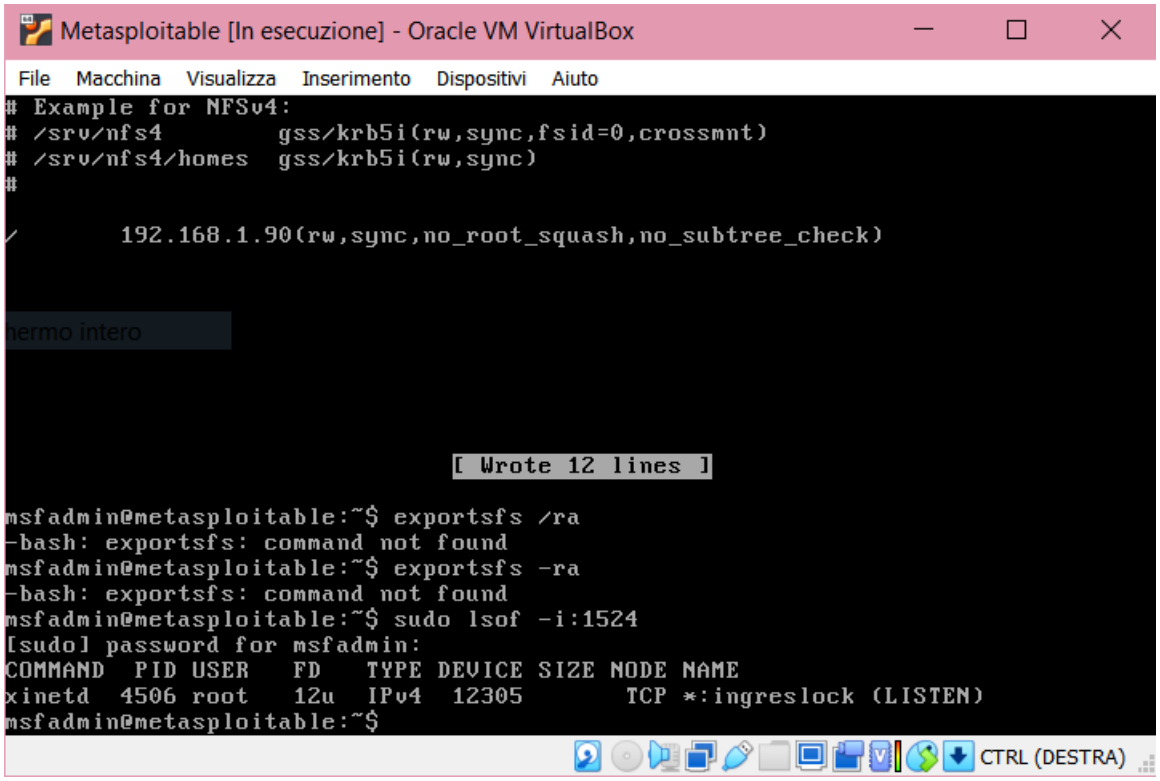
L'ultima riga non commentata fa vedere come tutti i client presenti in rete (*) possano accedervi.

Modifichiamo * con l'indirizzo IP della nostra macchina:



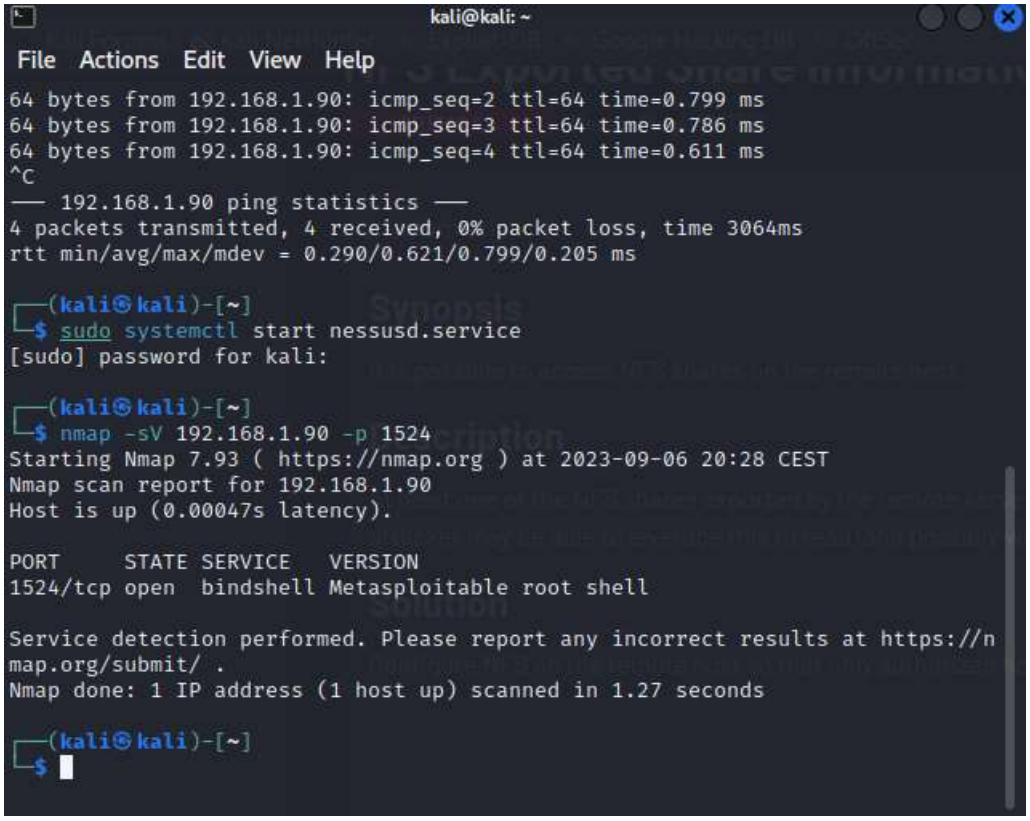
2) BIND SHELL BACKDOOR DETECTION

È una shell in ascolto su una porta senza che sia richiesta una autorizzazione.



In figura notiamo come sia presente servizio in ascolto sulla porta.

Verifichiamo anche su Kali con Nmap :



Kali conferma. Utilizzando Iptables ho creato una regola che rigetta tutto il traffico in entrata nella porta e poi verificato nuovamente che fosse chiusa.

Metasploitable [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
msfadmin@metasploitable:~$ iptables -I INPUT -p tcp -s 192.168.1.90 --dport 1524
 -j ACCEPT
iptables v1.3.8: can't initialize iptables table `filter': Permission denied (yo
u must be root)
Perhaps iptables or your kernel needs to be upgraded.
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp -s 192.168.1.90 --dport
 1524 -j ACCEPT
msfadmin@metasploitable:~$ iptables -L
iptables v1.3.8: can't initialize iptables table `filter': Permission denied (yo
u must be root)
Perhaps iptables or your kernel needs to be upgraded.
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.1.90         anywhere            tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp --dport 1524 -j DROP
msfadmin@metasploitable:~$
```

CTRL (DESTRA)

kali@kali: ~

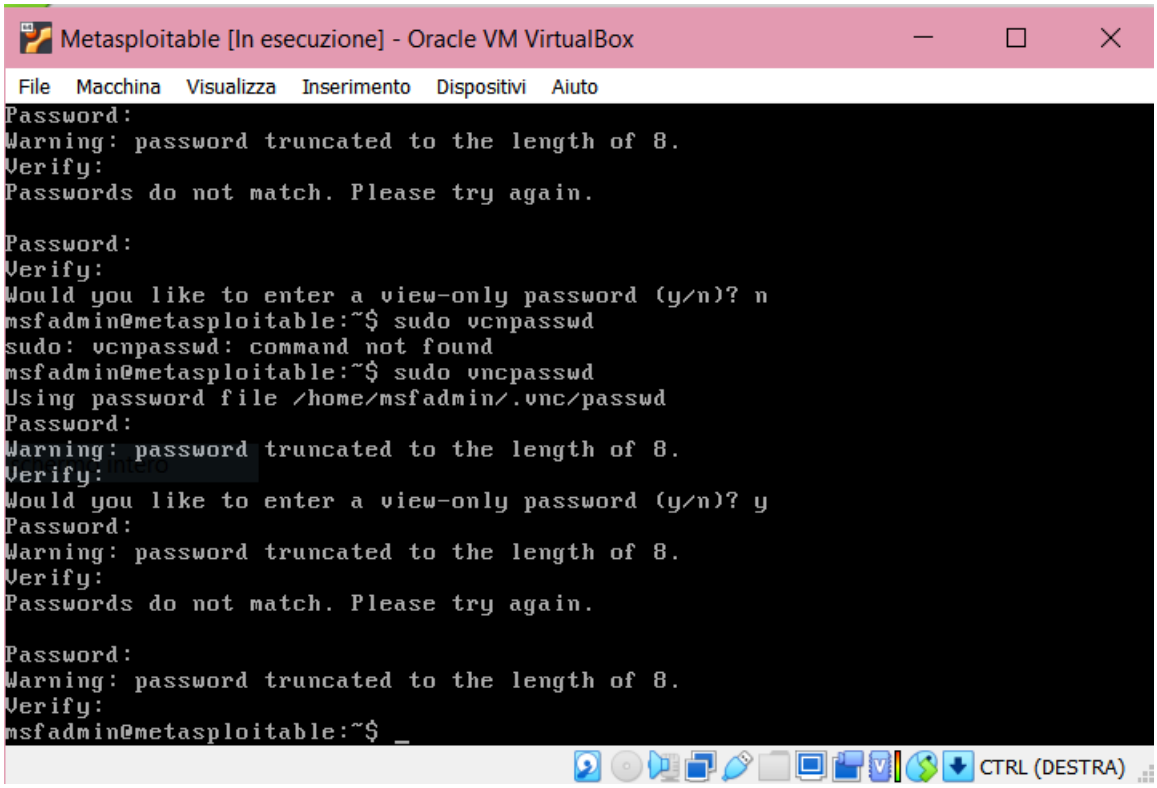
File Actions Edit View Help

```
└─$ nmap -sV 192.168.1.90 -p 1524
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 20:38 CEST
Nmap scan report for 192.168.1.90
Host is up (0.00065s latency).

PORT     STATE SERVICE   VERSION
1524/tcp open  bindshell Metasploitable root shell

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.90 -p 1524
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 20:39 CEST
Nmap scan report for 192.168.1.90
Host is up (0.00067s latency).

PORT     STATE    SERVICE    VERSION
1524/tcp filtered ingreslock

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.90 seconds

┌──(kali㉿kali)-[~]
└─$
```

3)VNC SERVER ‘PASSWORD’ PASSWORD

Un virtual network computing (VNC) è un'applicazione grafica di condivisione desktop che utilizza il protocollo di buffer frame remoto per controllare in remoto un altro computer.

La PASSWORD è troppo easy perciò:



Cambiata (2 volte perché la prima non mi piaceva).

4) APACHE TOMCAT AJP CONNECTORE REQUEST INJECTION (GHOSTCAT)

È presente un connettore JP in ascolto sull'host. Si può procedere bloccando il traffico sulla porta. Verifichiamo su kali con nmap lo stato della porta:

```
kali@kali: ~
File  Actions  Edit  View  Help
└─$ nmap -sV 192.168.1.90 -p 1524
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 20:39 CEST
Nmap scan report for 192.168.1.90
Host is up (0.00067s latency).

PORT     STATE    SERVICE    VERSION
1524/tcp filtered ingreslock

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.90 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.90 -p 8009
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-07 17:13 CEST
Nmap scan report for 192.168.1.90
Host is up (0.0011s latency).

PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.00 seconds

┌──(kali㉿kali)-[~]
└─$
```

Blocchiamo il traffico:

```
[ New File ]

msfadmin@metasploitable:~$ sudo /etc/tomcat9/server.xml
sudo: /etc/tomcat9/server.xml: command not found
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p DROP --Dport 8009
iptables v1.3.8: unknown protocol `drop' specified
Try `iptables -h' or 'iptables --help' for more information.
msfadmin@metasploitable:~$ sudo iptables -A INPUT -j DROP --dport 8009
iptables v1.3.8: Unknown arg `--dport'
Try `iptables -h' or 'iptables --help' for more information.
msfadmin@metasploitable:~$ sudo iptables -A INPUT -j --dport 8009 DROP
Bad argument `8009'
Try `iptables -h' or 'iptables --help' for more information.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp --dport 8009 -j DROP
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
msfadmin@metasploitable:~$
```

Controlliamo:

```
kali@kali: ~
File  Actions  Edit  View  Help
└─$ nmap -sV 192.168.1.90 -p 8009
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-07 17:13 CEST
Nmap scan report for 192.168.1.90
Host is up (0.0011s latency).

PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.00 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.90 -p 8009
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-07 17:18 CEST
Nmap scan report for 192.168.1.90
Host is up (0.00065s latency).

PORT     STATE    SERVICE VERSION
8009/tcp filtered ajp13

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds

┌──(kali㉿kali)-[~]
└─$
```

5) RLOGIN SERVICE DETECTION

Il servizio rlogin è in esecuzione sull'host remoto. Questo servizio è vulnerabile poiché i dati vengono passati tra il client e il server rlogin in chiaro. Un utente malintenzionato man-in-the-middle può sfruttare questa situazione per sniffare login e password.

La soluzione è commentare la linea 'login':

```
  GNU nano 2.0.7            File: /etc/inetd.conf                      Modified

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
#login          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
exec            stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```