

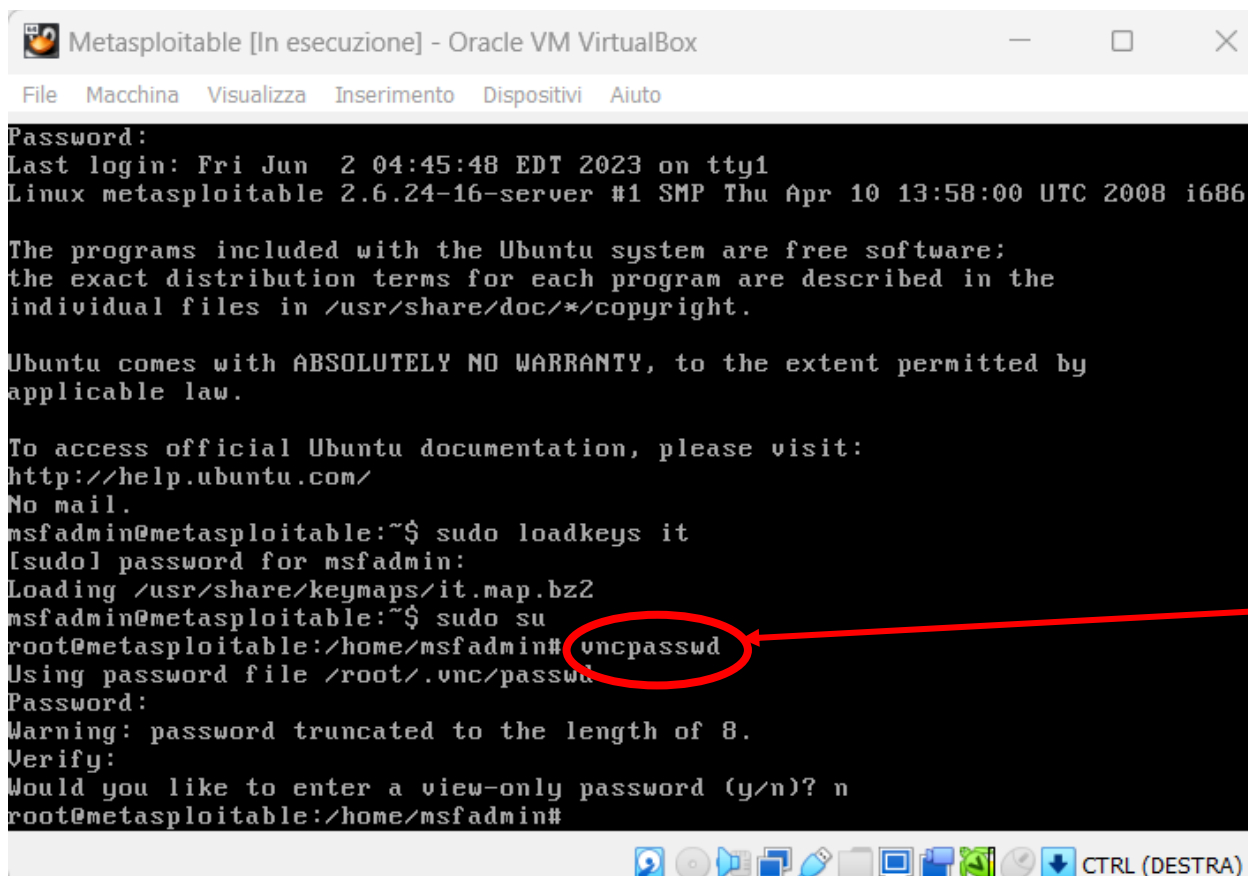
## REMEDIATION ACTION METASPLOITABLE 2

Vulnerabilità risolte:

- 1) VNC server 'password' password
- 2) NFS exported Share Information Disclosure
- 3) Bind Shell Backdoor Detection (porta 1524, service: ingreslock)
- 4) Rexecd Service Detention (porta 512, service exec)
- 5) Vulnerabilità extra: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (porta 22 service ssh)

- 1) **VNC server 'password' password:** VNC (Virtual Network Computing) è un protocollo che ha come scopo controllare un computer da remoto e visualizzare il suo desktop. Nessus ha rilevato tale vulnerabilità poiché tale servizio aveva una common password, per l'appunto 'password'.

Come ben noto, è doveroso utilizzare una password corposa e robusta, di almeno 12 caratteri, composta da lettere, numeri e caratteri. Per far ciò, previo comando "sudo su", tramite il comando "vncpasswd" ho avuto modo di cambiare la password in **"Meta-1996!!!"**



The screenshot shows a terminal window titled "Metasploitable [In esecuzione] - Oracle VM VirtualBox". The terminal output includes the following text:

```
Password:
Last login: Fri Jun  2 04:45:48 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

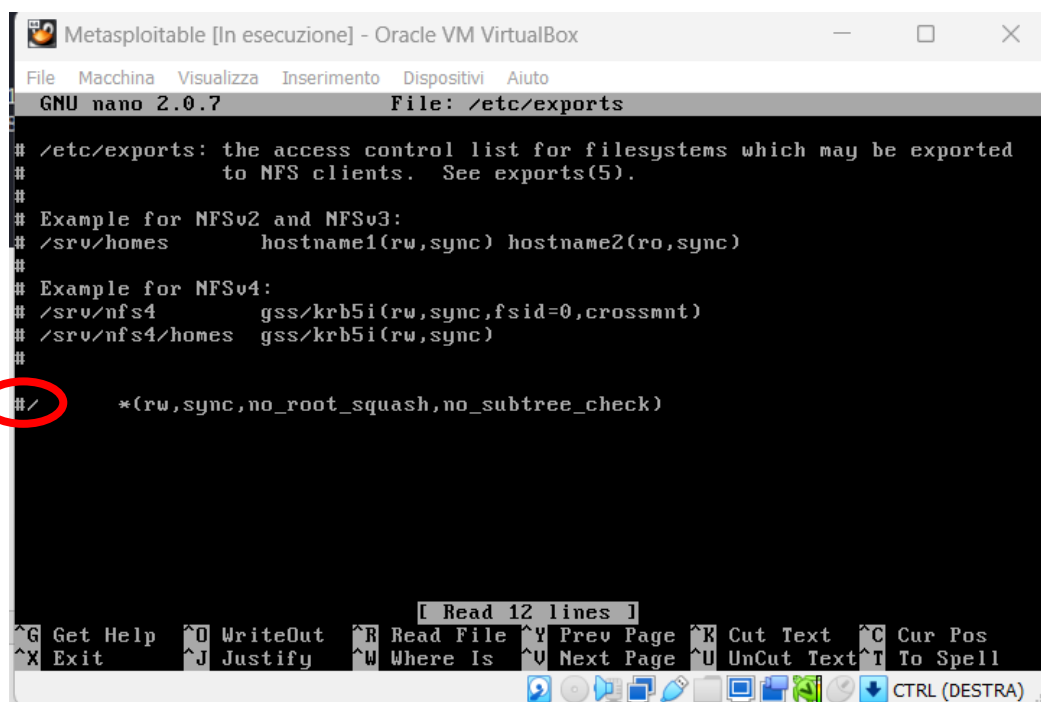
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo loadkeys it
[sudo] password for msfadmin:
Loading /usr/share/keymaps/it.map.bz2
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin#
```

A red circle highlights the `vncpasswd` command, and a red arrow points to it from the right side of the image.

**2) NFS exported Share Information Disclosure:** NFS è un protocollo di rete per consentire ai client di accedere e condividere file su una rete. Un server NFS esporta directory o file specifici che possono essere montati e accessibili dai client NFS. Tuttavia, se le informazioni sulle condivisioni NFS esportate sono accessibili senza le adeguate misure di sicurezza, potenziali attaccanti potrebbe avere accesso ad informazioni sensibili, come nomi dei file, dati aziendali ecc., in modo non autorizzato! Detto ciò, un potenziale attaccante potrebbe essere in grado di sfruttare ciò per leggere (e potenzialmente scrivere) file sull'host remoto.

Ho risolto tale vulnerabilità accedendo tramite permessi di root al file `/etc/exports`, e commentando l'ultima riga.



```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/exports

# /etc/exports: the access control list for filesystems which may be exported
#                 to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
# /              *(rw,sync,no_root_squash,no_subtree_check)
```

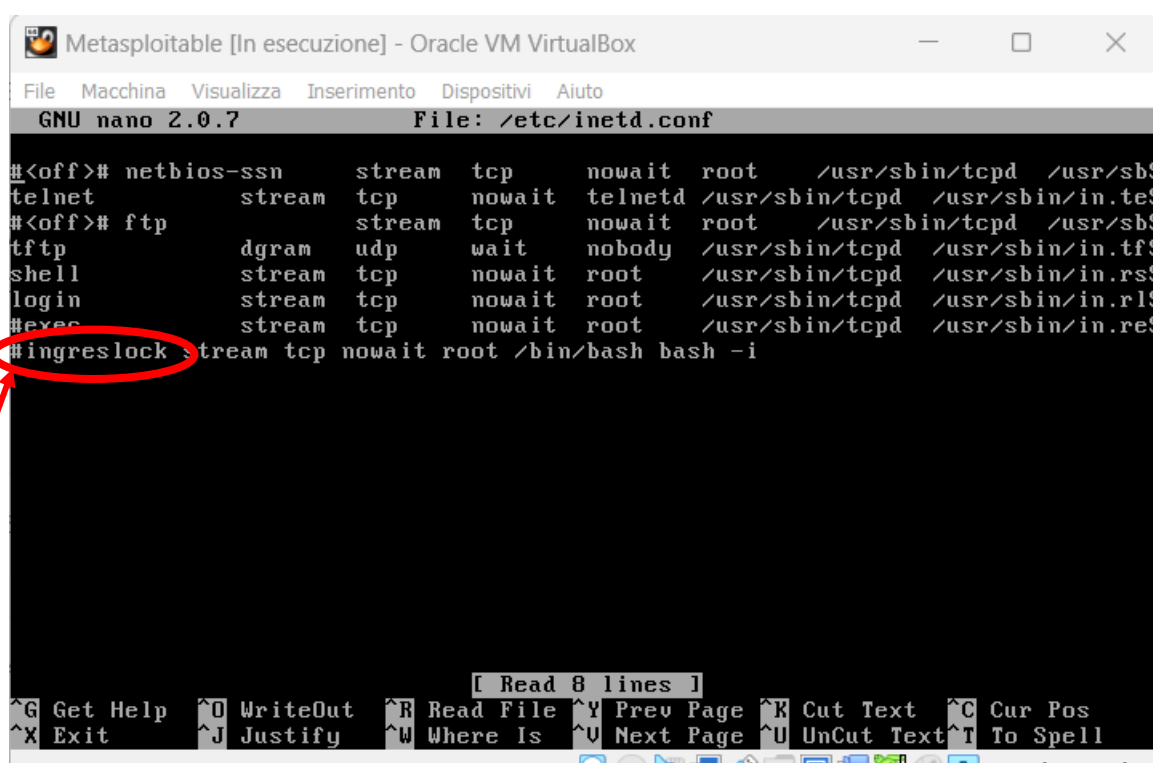
Nelle seguente immagine, tramite comando `sudo showmount -e 192.168.50.101`, prima della modifica al file `/etc/exports`, tramite Kali riuscivo ad importare del testo da Metasploitable (1). Dopo le modifiche invece nulla era possibile (2).

```
(kali㉿kali)-[~]  
$ sudo showmount -e 192.168.50.101  
Export list for 192.168.50.101:  
/ *  
  
(kali㉿kali)-[~]  
$ sudo showmount -e 192.168.50.101  
Export list for 192.168.50.101:  
  
(kali㉿kali)-[~]  
$
```

**3) Bind Shell Backdoor Detection (porta 1524, service: ingreslock):** si riferisce alla rilevazione di backdoor del tipo "bind shell" su un sistema informatico. Una backdoor è un tipo di accesso non autorizzato o una vulnerabilità introdotta in un sistema al fine di consentire a un attaccante di ottenere un accesso remoto nascosto e non rilevato.

In questo modo, il potenziale attaccante può collegarsi a questa porta di ascolto per stabilire una connessione di rete bidirezionale con il sistema compromesso, grazie alla quale può eseguire comandi o intraprendere azioni non autorizzate.

La soluzione di questa vulnerabilità è di commentare con # la riga "ingreslock" del file /etc/inetd.conf



```
Metasploitable [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
GNU nano 2.0.7 File: /etc/inetd.conf  
#<off># netbios-ssn stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.tftpd  
telnet stream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd  
#<off># ftp stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.ftpd  
tftp dgram udp wait nobody /usr/sbin/tcpd /usr/sbin/in.tftpd  
shell stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rsh  
login stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rlogin  
#exec stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rexecd  
#ingreslock stream tcp nowait root /bin/bash bash -i  
  
[ Read 8 lines ]  
^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
```

Dopo la remediation action, come da immagine sottostante, con il comando "nc" (netcat) non è più possibile accedere da Kali a Metasploitable tramite backdoor sita sulla porta 1524

```
(root@kali)-[/home/kali]
# sudo nc 192.168.50.101 1524
(UNKNOWN) [192.168.50.101] 1524 (ingreslock) : Connection refused
(root@kali)-[/home/kali]
#
```

**4) Rexecd Service Detention (porta 512, service exec):** rexec è un servizio di rete che consente l'esecuzione di comandi su un host remoto attraverso una connessione di rete (per l'appunto è detto Remote Execution). Malgrado ciò, tale servizio è spesso considerato un potenziale rischio per la sicurezza, poiché rexec non fornisce un buon mezzo di autenticazione, motivo per cui potrebbe essere usato da un attaccante per scansionare un host di terze parti.

Per risolvere questa vulnerabilità ho commentato la riga "exec" con # all'interno del file /etc/inetd.conf.

```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/inetd.conf
#<off># netbios-ssn      stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/$
telnet                  stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp              stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/$
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
```

Dopo la remediation action non è stato più possibile accedere a Metasploitable tramite comando "rlogin -l root 192.168.50.101"

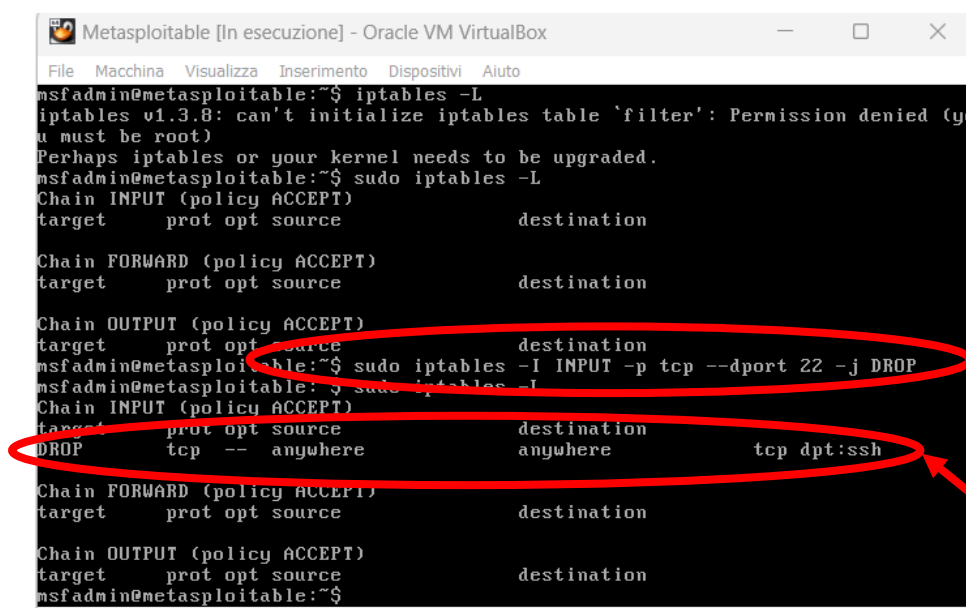
```
(root@kali)-[/home/kali]
# ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.030 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.163 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.048 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.061 ms
^C
— 192.168.50.101 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3066ms
rtt min/avg/max/mdev = 0.030/0.075/0.163/0.051 ms

(root@kali)-[/home/kali]
# rlogin -l root 198.162.50.101
198.162.50.101: Network is unreachable
```

## 5) Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

**(porta 22):** sui sistemi Debian e Ubuntu è stata scoperta una vulnerabilità nel generatore di numeri casuali utilizzato da OpenSSL, motivo per cui alcune chiavi di crittografia risultano molto più comuni di quanto dovrebbero, tanto che un potenziale attaccante potrebbe facilmente la chiave attraverso un attacco brute force. Questa vulnerabilità riguarda solo i sistemi operativi basati su Debian, ma non è detto che anche altri sistemi possano essere indirettamente interessati se vengono importate chiavi deboli in essi.

Ho risolto la vulnerabilità attraverso regola di firewall iptables (programma di firewall a livello di kernel per sistemi Linux), il quale permette di gestire il flusso del traffico di rete in entrata, in uscita e di transito attraverso il sistema. Con il comando “**sudo iptables -I INPUT -p tcp --dport 22 -j DROP**” ho rigettato il traffico in entrata sulla porta 22, dove è stata rilevata la vulnerabilità.



```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
msfadmin@metasploitable:~$ iptables -L
iptables v1.3.8: can't initialize iptables table 'filter': Permission denied (you
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
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 22 -j DROP
Chain INPUT (policy ACCEPT)
target prot opt source destination
DROP tcp -- anywhere anywhere tcp dpt:ssh
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
msfadmin@metasploitable:~$
```

Dopo aver eseguito il comando “**sudo iptables -L**” grazie al quale ho appurato che la regola di firewall era stata correttamente inserita, da Kali ho effettuato un port scanner sul nostro target tramite **nmap -sS**

192.168.50.101. Come si nota dall'immagine sottostante, dopo aver inserito la regola di firewall, la porta 22 risulta "filtered".

```
(kali@kali)-[~]
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 12:51 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0037s latency).
Not shown: 979 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    filtered ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
5900/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:E2:A5:69 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 15.20 seconds
```

## DIFFERENZE PRE E POST REMEDIATION ACTION

Sia prima che dopo l'applicazione delle "remediation action", ho effettuato uno scan con nmap sul mio target 192.168.50.101.

- Nello screen di sinistra, effettuato precedentemente alle remediation action, le porte 22 (ssh), 512 (exec) e 1524 (shell) risultano attive, motivo per cui Nessus ha rilevato le relative vulnerabilità.
- Nello screen di destra, effettuato dopo le remediation action, le porte 512 (exec) e 1524 (shell) risultano chiuse, mentre la porta 22 (ssh), alla quale ho applicato la regola di firewall tramite iptables, risulta filtrata.

Figura 1 Scan effettuato prima delle remediation action

Figura 2 Scan effettuato dopo le remediation action

```

(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-27 14:00:27
Nmap scan report for 192.168.50.101
Host is up (0.0089s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:66:40:1E (Oracle VM VirtualBox)
Nmap done: 1 IP address (1 host up) scanned

(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-27 14:00:28
Nmap scan report for 192.168.50.101
Host is up (0.0037s latency).
Not shown: 979 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    filtered ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:E2:A5:69 (Oracle VM VirtualBox)
Nmap done: 1 IP address (1 host up) scanned

```