File   Macchina   Visualizza   Inserimento   Dispositivi   Aiuto

kali@Host-004: ~

File   Actions   Edit   View   Help

```
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: 08:00:27:38:94:A1 (Oracle VirtualBox virtual NIC)
Device type: general purpose|WAP|proxy server|specialized
Running (JUST GUESSING): Linux 2.6.X|2.4.X|3.X (97%), Linksys embedded (94%), AVM embedded (94%
), WebSense embedded (94%), Citrix XenServer 5.X (94%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:2.4.32 cpe:/h:linksys:wrv54g cp
e:/h:avm:fritz%21box_fon_wlan_7240 cpe:/o:linux:linux_kernel:3.0 cpe:/o:citrix:xenserver:5.5 cp
e:/o:linux:linux_kernel:2.4.18 cpe:/o:linux:linux_kernel:2.4.20
Aggressive OS guesses: Linux 2.6.9 - 2.6.24 (97%), Linux 2.6.9 - 2.6.30 (97%), Linux 2.6.9 - 2.
6.33 (97%), Linux 2.6.13 - 2.6.32 (97%), Linux 2.6.9 (97%), Linux 2.6.24 - 2.6.28 (96%), Linux
2.6.18 - 2.6.32 (96%), Linux 2.6.21 (96%), Linux 2.6.22 - 2.6.23 (96%), Linux 2.6.23 (96%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.07 seconds
```

```
┌──(kali㉿Host-004)-[~]
└─$
```

12:54

CTRL (DESTRA)

Trash   Home

File System

root@Host-004: /home/kali

File   Actions   Edit   View   Help

```
└$ nmap -sS 192.168.80.101
You requested a scan type which requires root privileges.
QUITTING!

┌──(kali㉿Host-004)-[~]
└$ sudo su
┌──(root㉿Host-004)-[/home/kali]
└# nmap -sS 192.168.80.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 12:56 CET
Nmap scan report for 192.168.80.101
Host is up (0.0094s 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: 08:00:27:38:94:A1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds

┌──(root㉿Host-004)-[/home/kali]
└#
```

"the   ome, the more you are able to hear"

12:56

Trash

Home

File System

root@Host-004: /home/kali

File   Actions   Edit   View   Help

```
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:38:94:A1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds

┌──(root㉿Host-004)-[/home/kali]
└─# nmap -sT 192.168.80.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 12:57 CET
Nmap scan report for 192.168.80.101
Host is up (0.0092s latency).
Not shown: 977 closed tcp ports (conn-refused)
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: 08:00:27:38:94:A1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds

┌──(root㉿Host-004)-[/home/kali]
└─#
```

12:58

CTRL (DESTRA)

kali [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Trash
Home
File System

root@Host-004: /home/kali

File Actions Edit View Help

```
└─# nmap -sV 192.168.80.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 12:58 CET


┌──(root㉿Host-004)-[/home/kali]
└─# nmap -sV 192.168.80.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 13:00 CET
Nmap scan report for 192.168.80.101
Host is up (0.0026s 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?
25/tcp   open  smtp?
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?
513/tcp  open  login?
514/tcp  open  shell?
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  ccproxy-ftp?
3306/tcp open  mysql?
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
MAC Address: 08:00:27:38:94:A1 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: 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 193.67 seconds


┌──(root㉿Host-004)-[/home/kali]
└─#
```

13:06

CTRL (DESTRA)