

```
lsarting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 09:18 EST
bin: scan report for 192.168.1.149
boot is up (0.0014s latency).
cdrom: 977 closed tcp ports (conn-refused)
dev:
etc:
tcp: open  ftp          vsftpd 2.3.4
home:
tcp: open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
initrd:
tcp: open  telnet       Linux telnetd
initrd.img:
tcp: open  smtp          Postfix smtpd
lib:
tcp: open  domain       ISC BIND 9.4.2
lost+found:
tcp: open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
media:
tcp: open  rpcbind       2 (RPC #100000)
mnt:
tcp: open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
nohup.out:
tcp: open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
opt:
tcp: open  exec          netkit-rsh rexecd
proc:
tcp: open  login?
root:
tcp: open  shell         Netkit rshd
sbin:
tcp: open  java-rmi       GNU Classpath grmiregistry
srv:
tcp: open  bindshell      Metasploitable root shell
sys9:
tcp: open  nfs           2-4 (RPC #100003)
tmp:
tcp: open  ftp           ProFTPD 1.3.1
usr6:
tcp: open  mysql         MySQL 5.0.51a-3ubuntu5
var:
tcp: open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
vmlinuz:
tcp: open  vnc           VNC (protocol 3.3)
cd root:
tcp: open  X11          (access denied)
ls57:
tcp: open  irc          UnrealIRCd
Desktop:
tcp: open  ajp13        Apache Jserv (Protocol v1.3)
reset_logs.sh:
tcp: open  http         Apache Tomcat/Coyote JSP engine 1.1
vnc.log: Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN;
mkdir test_metasploit
ls
Desktop detection performed. Please report any incorrect results at https://nmap.org
reset_logs.sh IP address (1 host up) scanned in 66.06 seconds
test_metasploit
vnc.log 2024-03-05 09:18:18 [~]
■ s ■
```