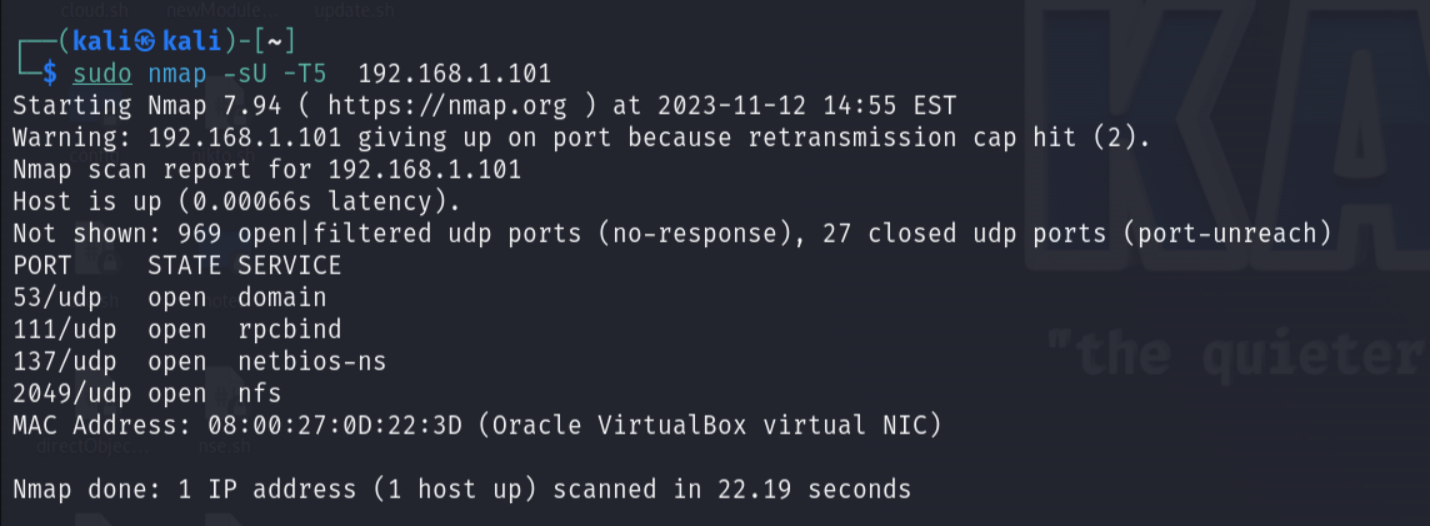
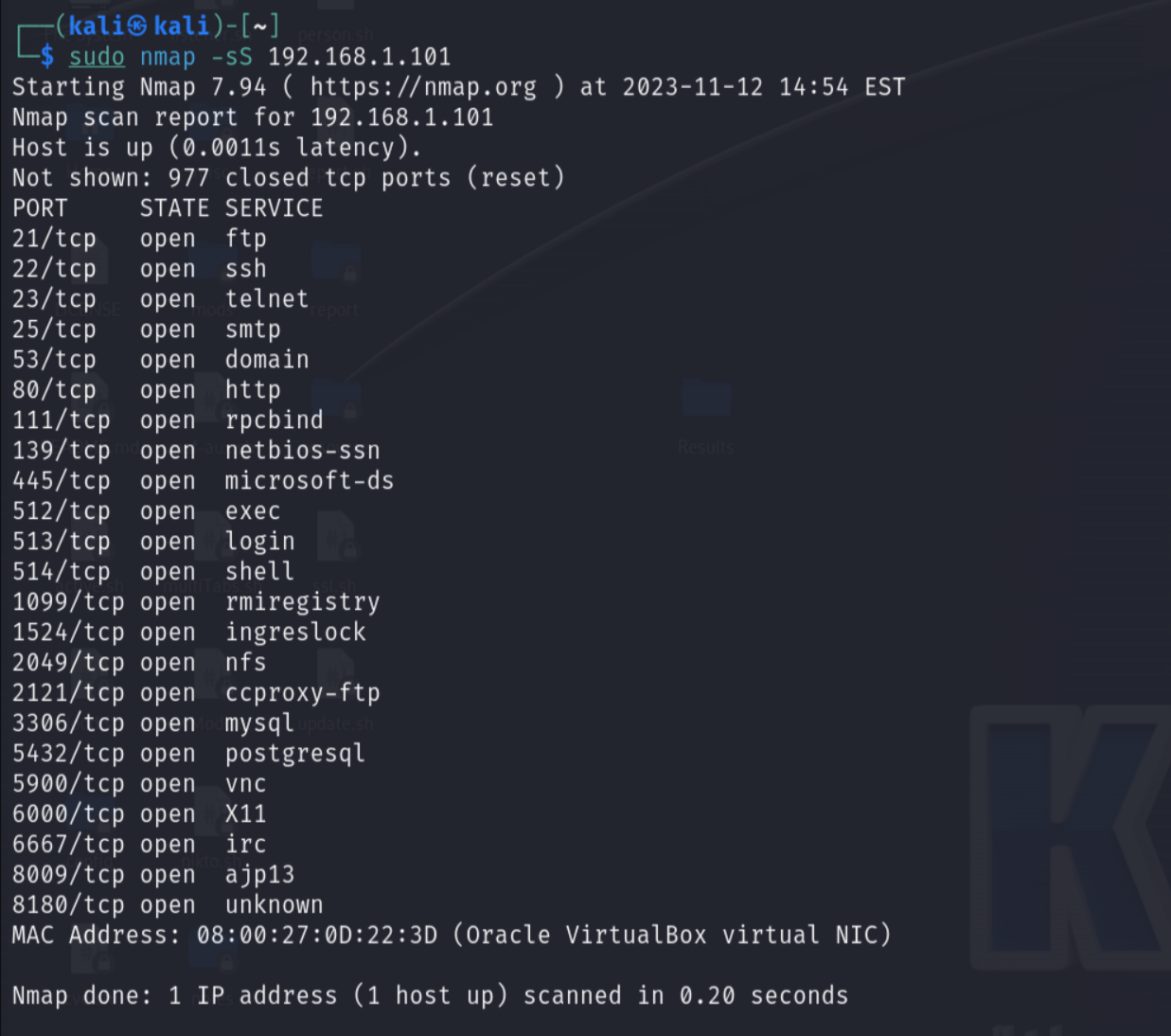
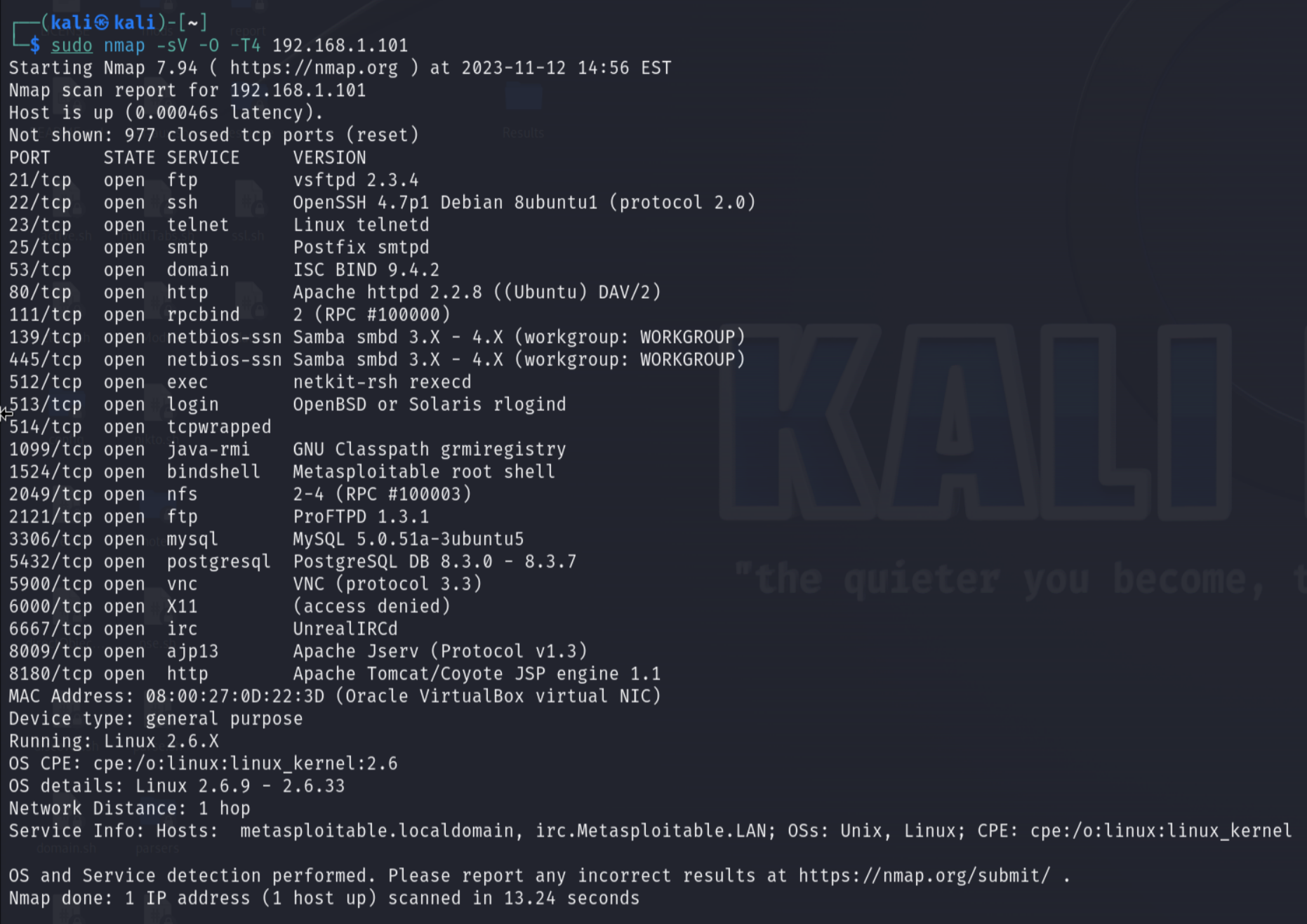
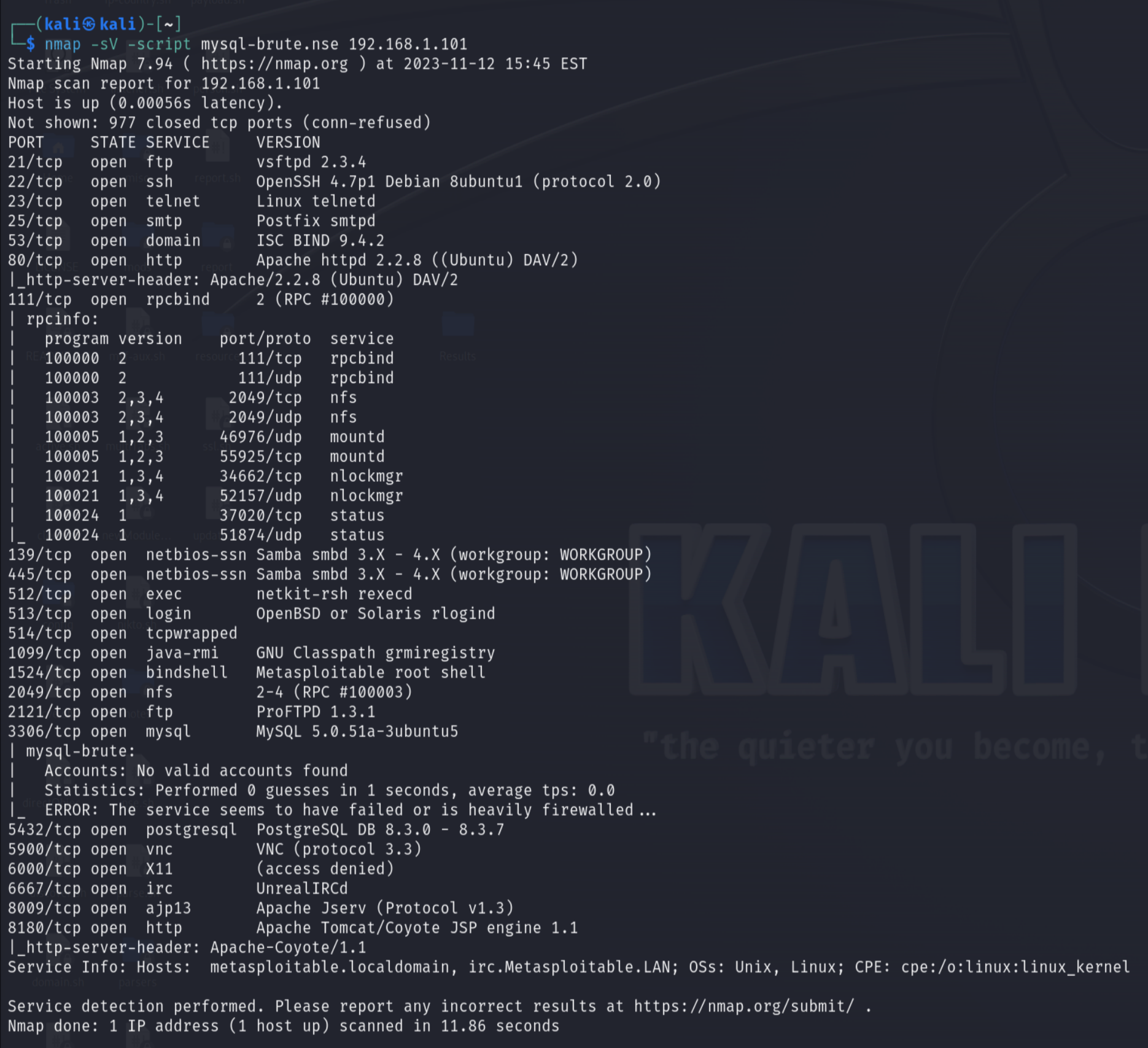
**1. Three basic Nmap commands (w/out Scripting Engine):**





**2. Nmap commands with the Scripting Engine:**

See list of scripts: dir /usr/share/nmap/scripts



**3A. How many open ports are there? 23 ports**

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)

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 rexecd

513/tcp open login OpenBSD or Solaris rlogind

514/tcp open tcpwrapped

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 ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

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

**3B. What ports, if any, ought to be closed?**

**Port #: Service - why it should be closed**

Port 21 & 2121: FTP - plaintext data

Port 23: Telnet - plaintext data

Port 80 & 8180: HTTP - HTTPS would be better

Ports 139 & 445: Netbios - vulnerable names, session info, & user IDs

Port 512: RSH - No need to remote into a shell (hopefully)

Port 513: rlogin - sends passwords in cleartext

Port 1524: Bindshell - connectable to anyone

Port 6667: IRC - not commonly used anymore and might be good to close

Port 8009: AJP13 - connectable with Telnet

**3C. What operating system & version, is running? Linux 2.6.9 - 2.6.33**

**Output:**

MAC Address: 08:00:27:0D:22:3D (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel