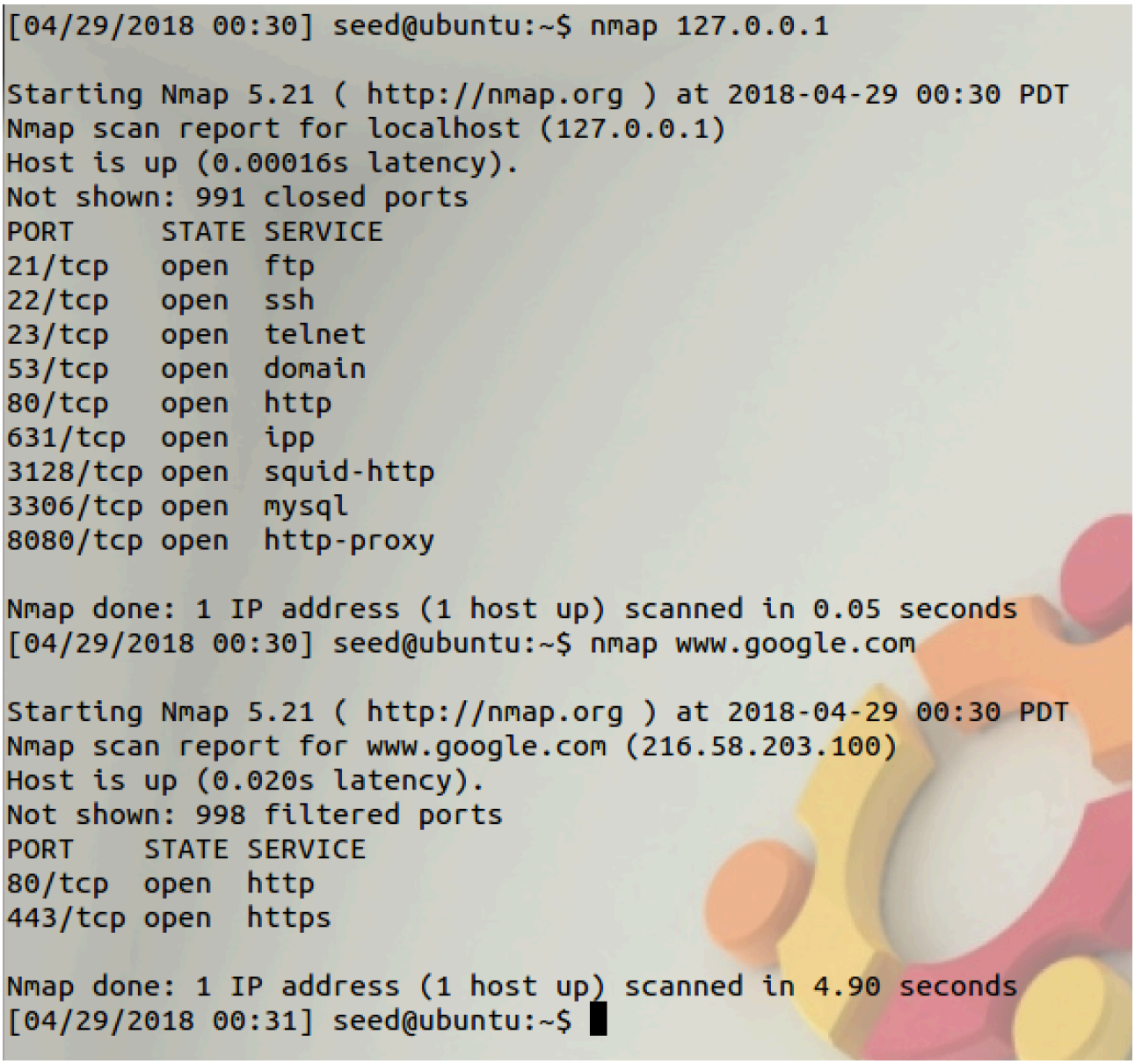
FIT3173 Week 8 Tutorial

Task 1



Based on the output, we can see that the ports open when scanning 127.0.0.1 and then again the ports that are open when scanning **www.google.com**.

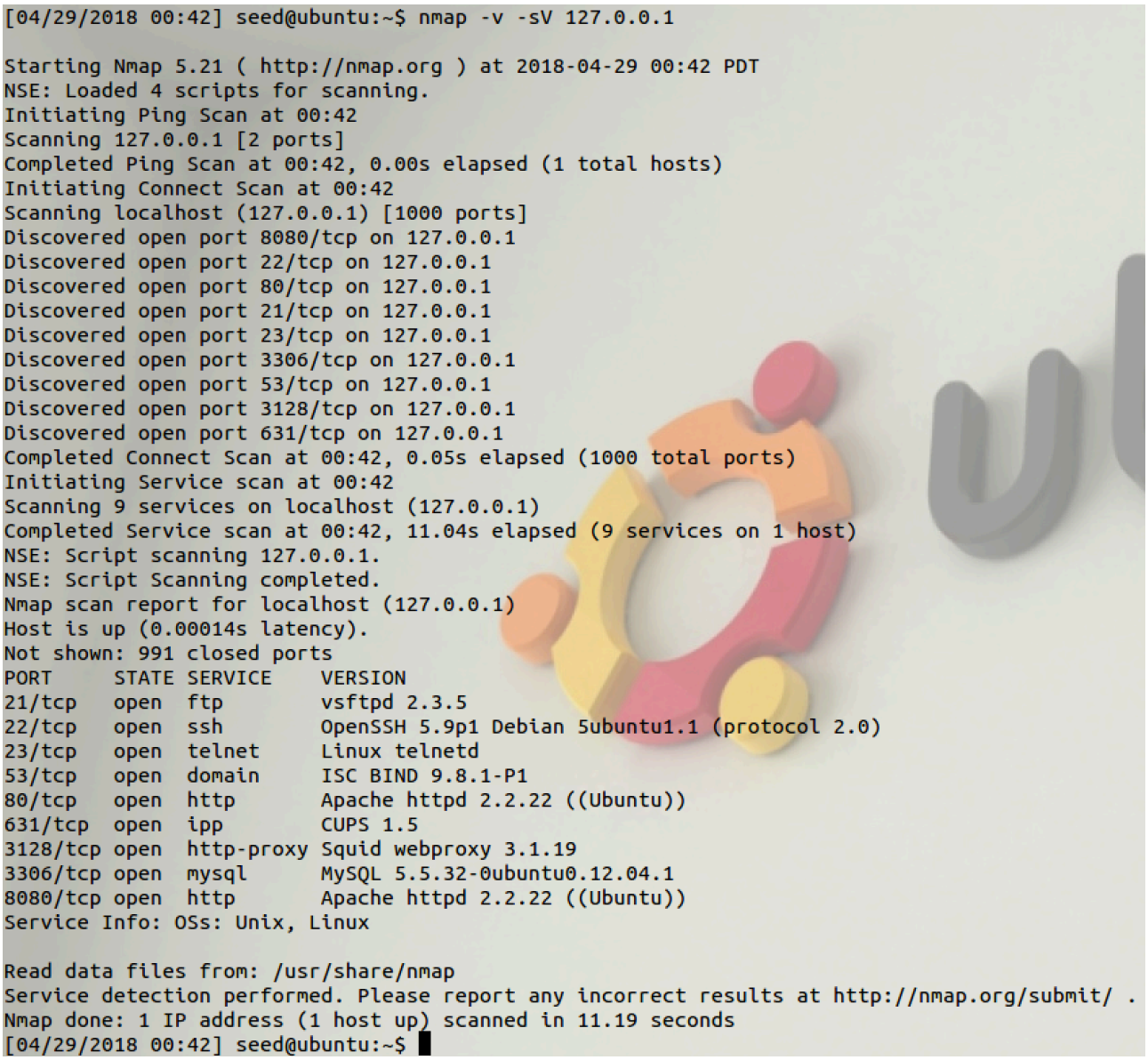
Task 2

```
[04/29/2018 00:38] seed@ubuntu:~$ sudo nmap -O 127.0.0.1
[sudo] password for seed:

Starting Nmap 5.21 ( http://nmap.org ) at 2018-04-29 00:38 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000038s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
631/tcp  open  ipp
3128/tcp open  squid-http
3306/tcp open  mysql
8080/tcp open  http-proxy
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.21%D=4/29%OT=21%CT=1%CU=43407%PV=N%DS=0%DC=L%G=Y%TM=5AE5767D%P=
OS:i686-pc-linux-gnu)SEQ(SP=109%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=8)OPS(O1=M4
OS:00CST11NW7%O2=M400CST11NW7%O3=M400CNNT11NW7%O4=M400CST11NW7%O5=M400CST11
OS:NW7%O6=M400CST11)WIN(W1=8000%W2=8000%W3=8000%W4=8000%W5=8000%W6=8000)ECN
OS:(R=Y%DF=Y%T=40%W=8018%O=M400CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(
OS:R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%
OS:F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N
OS:%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%C
OS:D=S)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.55 seconds
[04/29/2018 00:38] seed@ubuntu:~$
```

```
[04/29/2018 00:39] seed@ubuntu:~$ sudo nmap -O www.google.com

Starting Nmap 5.21 ( http://nmap.org ) at 2018-04-29 00:39 PDT
Nmap scan report for www.google.com (216.58.203.100)
Host is up (0.010s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 3Com SuperStack 3 Switch 4300, Dell PowerEdge 2650 remote access controller, Samsung ML-2571N or 6555N printe
r, or Xerox Phaser 3125N printer (88%), Dell 1815dn printer (88%), Slingmedia Slingbox AV TV over IP gateway (87%), Bay Networks Bay
Stack 450 switch (software version 3.1.0.22) (87%), Bay Networks BayStack 450 switch (software version 4.2.0.16) (87%), Cabletron EL
S100-24TXM Switch or Icom IC-7800 radio transceiver (86%), Cisco Catalyst 1900 switch or RAD IPMUX-1 TDM-over-IP multiplexer (86%),
Samsung CLX-3160FN printer (86%), Sanyo PLC-XU88 digital video projector (86%), Dell 1600n printer (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.94 seconds
[04/29/2018 00:39] seed@ubuntu:~$
```

```
[04/29/2018 00:39] seed@ubuntu:~$ sudo nmap -O www.monash.edu

Starting Nmap 5.21 ( http://nmap.org ) at 2018-04-29 00:40 PDT
Nmap scan report for www.monash.edu (202.9.95.188)
Host is up (0.012s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 3Com SuperStack 3 Switch 4300, Dell PowerEdge 2650 remote access controller, Samsung ML-2571N or 6555N printe
r, or Xerox Phaser 3125N printer (88%), Dell 1815dn printer (88%), Slingmedia Slingbox AV TV over IP gateway (87%), Bay Networks Bay
Stack 450 switch (software version 3.1.0.22) (87%), Bay Networks BayStack 450 switch (software version 4.2.0.16) (87%), Cabletron EL
S100-24TXM Switch or Icom IC-7800 radio transceiver (86%), Cisco Catalyst 1900 switch or RAD IPMUX-1 TDM-over-IP multiplexer (86%),
Samsung CLX-3160FN printer (86%), Sanyo PLC-XU88 digital video projector (86%), Dell 1600n printer (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.13 seconds
[04/29/2018 00:40] seed@ubuntu:~$
```

Task 3



```
[04/29/2018 00:42] seed@ubuntu:~$ nmap -v -sV 127.0.0.1

Starting Nmap 5.21 ( http://nmap.org ) at 2018-04-29 00:42 PDT
NSE: Loaded 4 scripts for scanning.
Initiating Ping Scan at 00:42
Scanning 127.0.0.1 [2 ports]
Completed Ping Scan at 00:42, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 00:42
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 8080/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 21/tcp on 127.0.0.1
Discovered open port 23/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 53/tcp on 127.0.0.1
Discovered open port 3128/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Completed Connect Scan at 00:42, 0.05s elapsed (1000 total ports)
Initiating Service scan at 00:42
Scanning 9 services on localhost (127.0.0.1)
Completed Service scan at 00:42, 11.04s elapsed (9 services on 1 host)
NSE: Script scanning 127.0.0.1.
NSE: Script Scanning completed.
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 2.3.5
22/tcp   open  ssh        OpenSSH 5.9p1 Debian 5ubuntu1.1 (protocol 2.0)
23/tcp   open  telnet     Linux telnetd
53/tcp   open  domain     ISC BIND 9.8.1-P1
80/tcp   open  http       Apache httpd 2.2.22 ((Ubuntu))
631/tcp  open  ipp        CUPS 1.5
3128/tcp open  http-proxy Squid webproxy 3.1.19
3306/tcp open  mysql      MySQL 5.5.32-0ubuntu0.12.04.1
8080/tcp open  http       Apache httpd 2.2.22 ((Ubuntu))
Service Info: OSs: Unix, Linux

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.19 seconds
[04/29/2018 00:42] seed@ubuntu:~$
```

Task 4

```
[04/29/2018 00:50] seed@ubuntu:~$ nmap -p ssh 127.0.0.1

Starting Nmap 5.21 ( http://nmap.org ) at 2018-04-29 00:50 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00062s latency).
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
[04/29/2018 00:50] seed@ubuntu:~$
```

Task 5

```
[04/29/2018 00:50] seed@ubuntu:~$ nmap -sn 127.0.0.1

Starting Nmap 5.21 ( http://nmap.org ) at 2018-04-29 00:51 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000040s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
[04/29/2018 00:51] seed@ubuntu:~$
```

Task 6

```
[04/29/2018 00:52] seed@ubuntu:~$ ifconfig
eth10     Link encap:Ethernet  HWaddr 08:00:27:c9:43:2d
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec9:432d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:219 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6318 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20045 (20.0 KB)  TX bytes:420238 (420.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:6452 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6452 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:320309 (320.3 KB)  TX bytes:320309 (320.3 KB)
```

```
Nmap scan report for h*1** (10.0.2.2)
Host is up (0.00045s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
88/tcp  open  kerberos-sec
445/tcp open  microsoft-ds
548/tcp open  afp
631/tcp open  ipp

Nmap scan report for h*1** (10.0.2.3)
Host is up (0.00064s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
88/tcp  open  kerberos-sec
445/tcp open  microsoft-ds
548/tcp open  afp
631/tcp open  ipp

Nmap scan report for h*1** (10.0.2.4)
Host is up (0.00066s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
88/tcp  open  kerberos-sec
445/tcp open  microsoft-ds
548/tcp open  afp
631/tcp open  ipp

Nmap scan report for h*1** (10.0.2.15)
Host is up (0.00043s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
3128/tcp open  squid-http
8080/tcp open  http-proxy

Nmap done: 256 IP addresses (4 hosts up) scanned in 39.94 seconds
[04/29/2018 00:54] seed@ubuntu:~$
```