PART ONE:
Explain the output for each nmap command below.
From cscd-linux01:

•nmap 10.101.130.*
The output from this command is the open ports of every machine with the network address 10.101.130 because of the wildcard, it will return every possible value after the last dot. It shows the scan report for each IP address that is connected to the network, the IP, whether or not the host is up and its latency, how many ports are closed, and then lists every open port and the service it provides.

•nmap 10.101.130.100-120
The output from this is similar to the previous, except it only shows the hosts connected to the range of 10.101.130.100 - 10.101.130.120. In this case, there were 21 addresses but 0 hosts connected.

•nmap 10.101.130.0/24
This command is essentially the same as 10.101.130, because it will scan every host address after the /24 mask. The difference with this one is that it can be used for every mask and be more precise than the wildcard.

•Complete a ping scan on 10.101.130.0/24 What address ranges are active?
There are 8 addresses active. 10.101.130.1 , 10.101.130.20 , 10.101.130.51 , 10.101.130.55 , 10.101.130.57 , 10.101.130.61 , 10.101.130.77 , 10.101.130.81

•Scan all TCP ports. What ports are open on my windows server? What commands did you use? What is the IP address?
The command I used is nmap -sT 10.101.130.0/24 and ports 53, 80, 135, 139, 445, 2179, and 3389 are all open. The IP address is 10.101.130.81

•Nearly every address in the 10.101.130.1-255 range is assigned to some device. Explain why you see so few.
I believe that I don't see every host on the network because either, I don't have root privileges, the firewall is blocking my scans, the device isn't connected to the internet, or it's switched off.

•Complete a ping scan on 10.102.134.235-255. How many hosts did the ping scan discover? Were there gaps in the host numbers? Why? What are these machines?
The ping scan discovered 8 hosts up. There were gaps in the host numbers, most likely because they are shut off. These machines are Eastern servers.

•Complete a version scan on 10.102.134.235. What command did you use? What are the results? Be specific as possible.
I used the command nmap -sV 10.102.134.235. The results are a typical scan of the address 10.102.134.235 along with the current version of the services running on the port (when it can discover it). The scan returned:

```
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1309/tcp open  tcpwrapped
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Port 1309 returned service tcpwrapped because it is protected by tcpwrapper. The TCP handshake happened, but no data was received. This is to protect the service on the port, not the actual port, and signifies that I am not on the list of hosts allowed to talk to it.
Port 135, 139, and 3389 returned the version the service is using, which is all Microsoft. The last two ports, 445 and 2179, both have a question mark after the service which means that nmap was not able to identify a known service.

PART TWO:
What's the difference between these two commands?
•nmap 10.101.130.1
•sudo nmap -O 10.101.130.1
•Answering "The second command uses sudo and -O" is not good enough. Why!?
The difference is, just using nmap yields the open ports of the IP 10.101.130.1. But using the -O option (which requires root privilege because it is sending and receiving raw packets) returns the open ports, as well as the operating system of the target.

Part 3: Look for machines
Look for a computer in the 10.101.130.0 – 10.101.130.255 range that has port 902 open.
•What command did you use?
I used the command nmap -p 902 10.101.130.0-255 (There was only one computer that wasn't closed, but its state was filtered.)

•What are the computer's IP address(es)?
10.101.130.81

•What are the name(s)?
csc-win-server.eastern.ewu.edu

•My school desktop is one of the machines. What is its name and IP address? What other ports are open?
The only machine that has a name within that range that is available to scan is the csc-win-server.eastern.ewu.edu machine with IP address 10.101.130.81. The open ports are 53 domain, 80 http, 135 msrpc, 139 netbios-ssn, 445 microsoft-ds, 2179 vmrdp, 3389 ms-wbt-server.

Look for a computer in the entire 23-bit subnet that has the "domain" port open.

•What command did you use?
I used nmap -p 53 10.101.130.0/23

•Did you find one? What are the computer's IP address(es)? What is its name?
Again, the only computer with the domain port open was csc-win-server.eastern.ewu.edu with IP 10.101.130.81

```
[ahall38@cscd-linux01:~$ nmap -p 53 10.101.130.0/23

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-15 02:14 PDT
Nmap scan report for 10.101.130.1
Host is up (0.0019s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Nmap scan report for 10.101.130.20
Host is up (0.0019s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Nmap scan report for 10.101.130.51
Host is up (0.00082s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Nmap scan report for 10.101.130.53
Host is up (0.0012s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Nmap scan report for 10.101.130.55
Host is up (0.0021s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Nmap scan report for 10.101.130.57
Host is up (0.0020s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Nmap scan report for 10.101.130.61
Host is up (0.00040s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Nmap scan report for 10.101.130.77
Host is up (0.0012s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Nmap scan report for csc-win-server.eastern.ewu.edu (10.101.130.81)
Host is up (0.00065s latency).

PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 512 IP addresses (9 hosts up) scanned in 3.42 seconds
ahall38@cscd-linux01:~$
```

Look for the computers in CEB 207/CEB 208.
•What command did you use?
I used the command nmap -sn 10.102.134.0/23. The -sn so that it would be easier to look for hostnames and 10.102.134.0/23 because I knew from a previous question the CEB computers were in the 10.102.134.0 range and applied a /23 mask to check the 10.101.135.0 range as well.
•What are the computer's IP address(es) and names (list 3 or 4)?
```
cscd-ceb208w14.eastern.ewu.edu (10.102.135.76)
cscd-ceb208w09.eastern.ewu.edu (10.102.135.90)
cscd-ceb207w27.eastern.ewu.edu (10.102.134.131)
cscd-ceb207w21.eastern.ewu.edu (10.102.134.106)
```

Part 4: Analysis
Using all the completed scans answer the following.
•Which TCP port appeared the most?
The TCP port 80: HTTP appeared the most

•Which UDP port appeared the most?
This requires root privilege to see

•Are there any security vulnerabilities associated with any of the open ports Where did you look? Google or some other search engine is not acceptable.
There are security vulnerabilities associated with some of the common ports I found. Port 80, 443, 135, and 139 are all known as vulnerable. I looked on researchgate.net and tenable.com.

•How might a system administrator discover someone running nmap or a similar program to probe their network? How can someone scanning a network with a tool similar to nmap avoid detection? (I am expecting at least a couple of sentences in response to this, think about it)
A system administrator might discover them by noticing a large amount of pings across a large number of ports, especially if the pings go across the network or ports sequencially. Patterns in network logs are an indication of a network being probed. Another indicator is when a single IP makes some kind of contact with the network in a suspicious way, such as lots of contact in a short amount of time. Someone can avoid detection by doing the opposite of what raises an alarm; scan ports out of order, at different times, but sending packets too small to be detected, and avoid patterns