COMP 189: Homework #4

Assigned Feb 4, 2022
Due Feb 11, 2022

55 points total

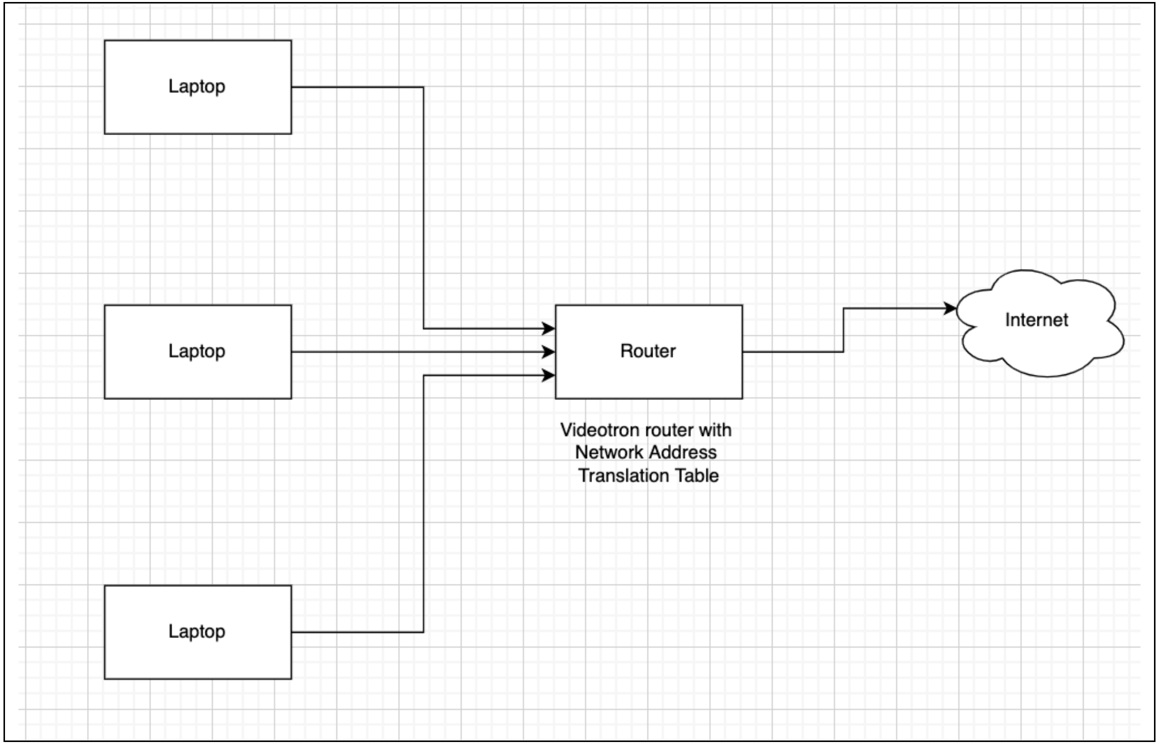
Instructions: *For each problem, show all your work (required for credit). For answers requiring written answers, while no more than five or six sentences are expected, sufficient justification must be given for any position, opinion, or perspective taken.*

Submission Instructions: *submit your solutions in PDF format through MyCourses Assignments.*

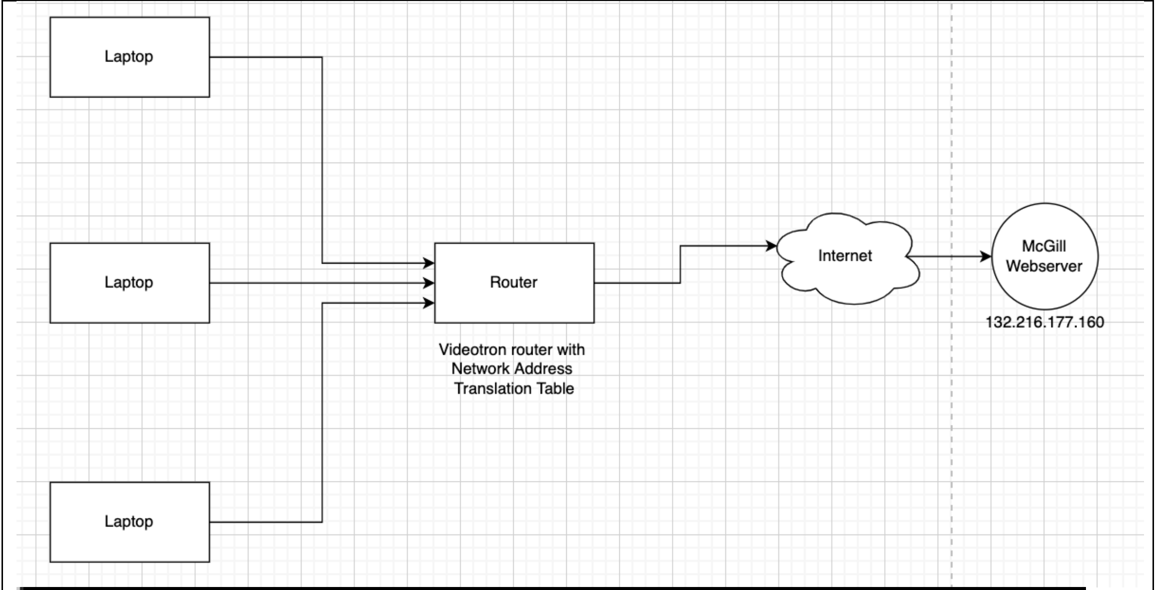
Technical Exercises

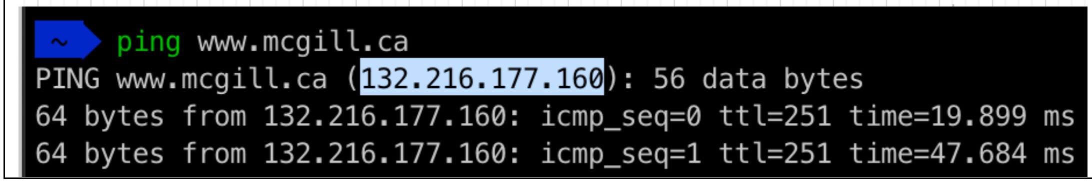
1. Basic NAT (8 pts)

1. Diagram (as done in class) a situation in which there is one local area network (LAN), A. LAN A should contain exactly one router (which has the public IP address) and 3 laptops. Depict connections to the public internet using lines connecting to a cloud.



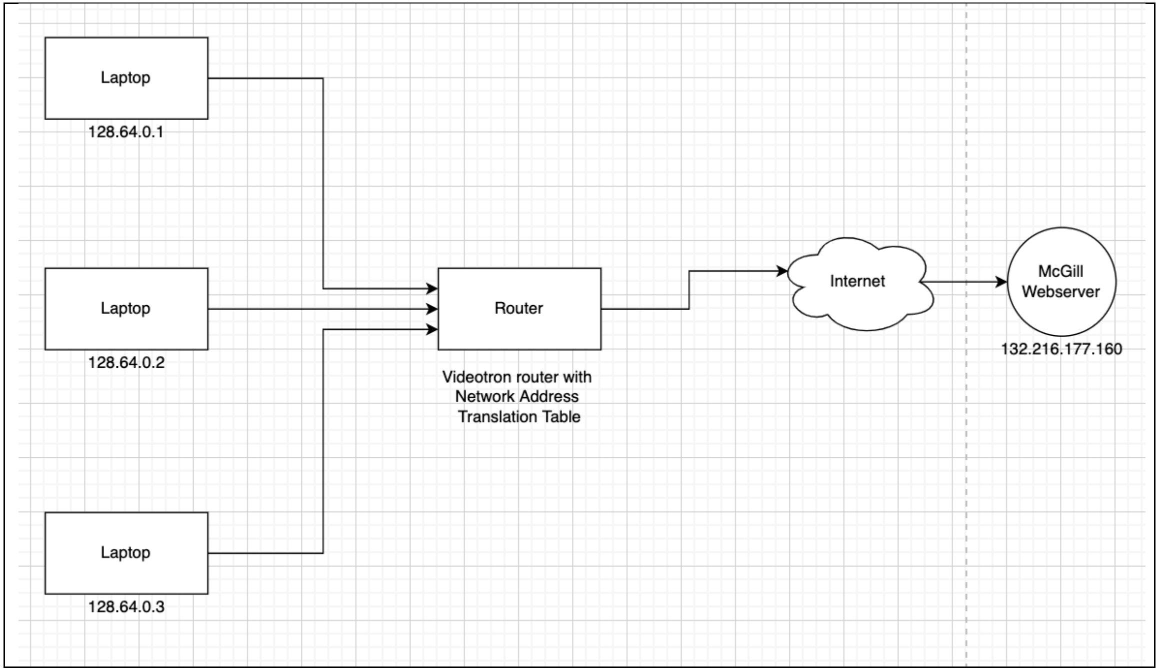
2. Add McGill's webserver to your diagram. Use ping to determine the IP address it actually has in real life. (show evidence of this in your answer)



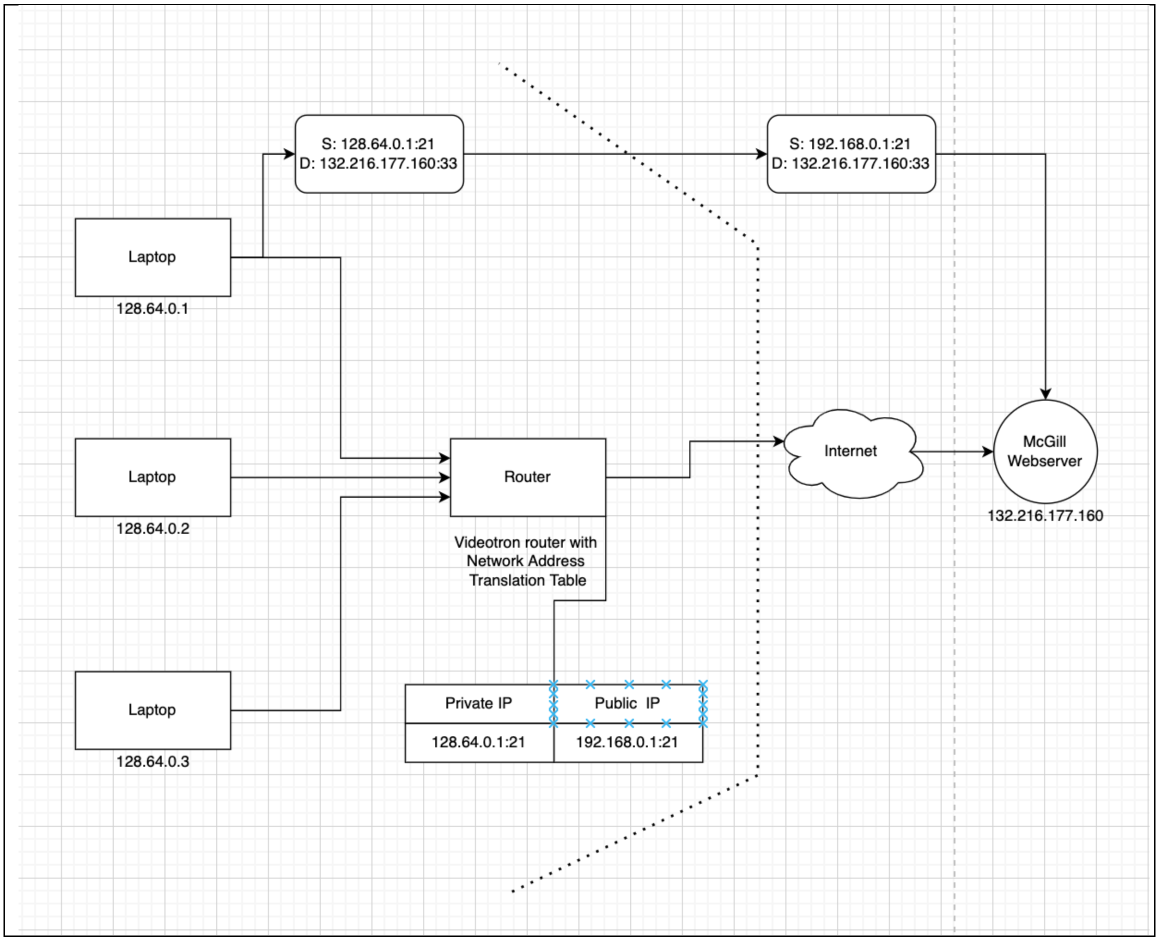


```
~  ping www.mcgill.ca
PING www.mcgill.ca (132.216.177.160): 56 data bytes
64 bytes from 132.216.177.160: icmp_seq=0 ttl=251 time=19.899 ms
64 bytes from 132.216.177.160: icmp_seq=1 ttl=251 time=47.684 ms
```

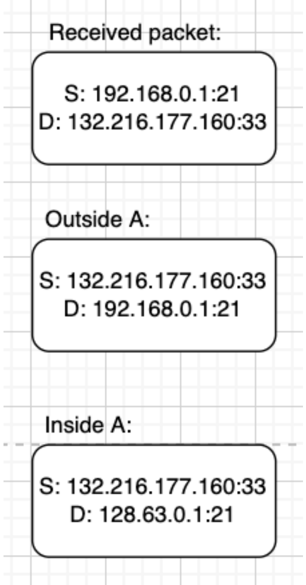
3. Assign valid IP addresses to each machine in your diagram. LAN A uses 128.64.0.X IP addresses internally.



4. A laptop in LAN A is contacting McGill's website. Diagram the process by which a packet is moved from the laptop to McGill's server (including any changes to network address translation tables will be updated).



5. McGill's server receives the packet and responds. Show the response packet header as it looks outside A and inside A.


Received packet:

S: 192.168.0.1:21
D: 132.216.177.160:33

Outside A:

S: 132.216.177.160:33
D: 192.168.0.1:21

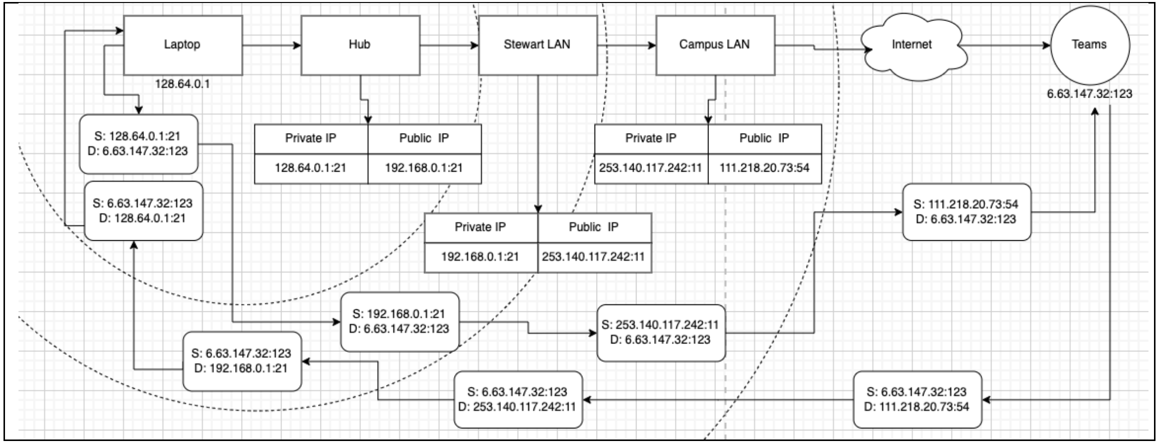
Inside A:

S: 132.216.177.160:33
D: 128.63.0.1:21

2. Triple NAT (10 pts)

Your laptop is connected by wifi to a hub inside a classroom in Stewart Bio. That hub performs NATing on your packets. The hub is a member of Stewart Bio-wide LAN in which the gateway *also* performs NATing on packets it carries. Finally, that building-wide LAN is situated inside a LAN that *also* performs NATing on packets that leave it. Your laptop sends a packet to the Microsoft Teams server (which is outside of McGill).

- Diagram this setup.
- As we did in class, diagram the journey one packet takes from your computer to the Teams server.
- Diagram the journey that one response packet makes back to your computer.



Private IP	Public IP
128.64.0.1:21	192.168.0.1:21

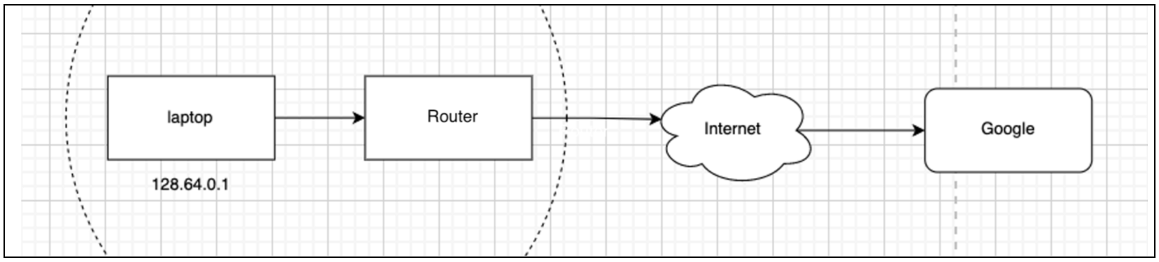
Private IP	Public IP
192.168.0.1:21	253.140.117.242:11

Private IP	Public IP
253.140.117.242:11	111.218.20.73:54

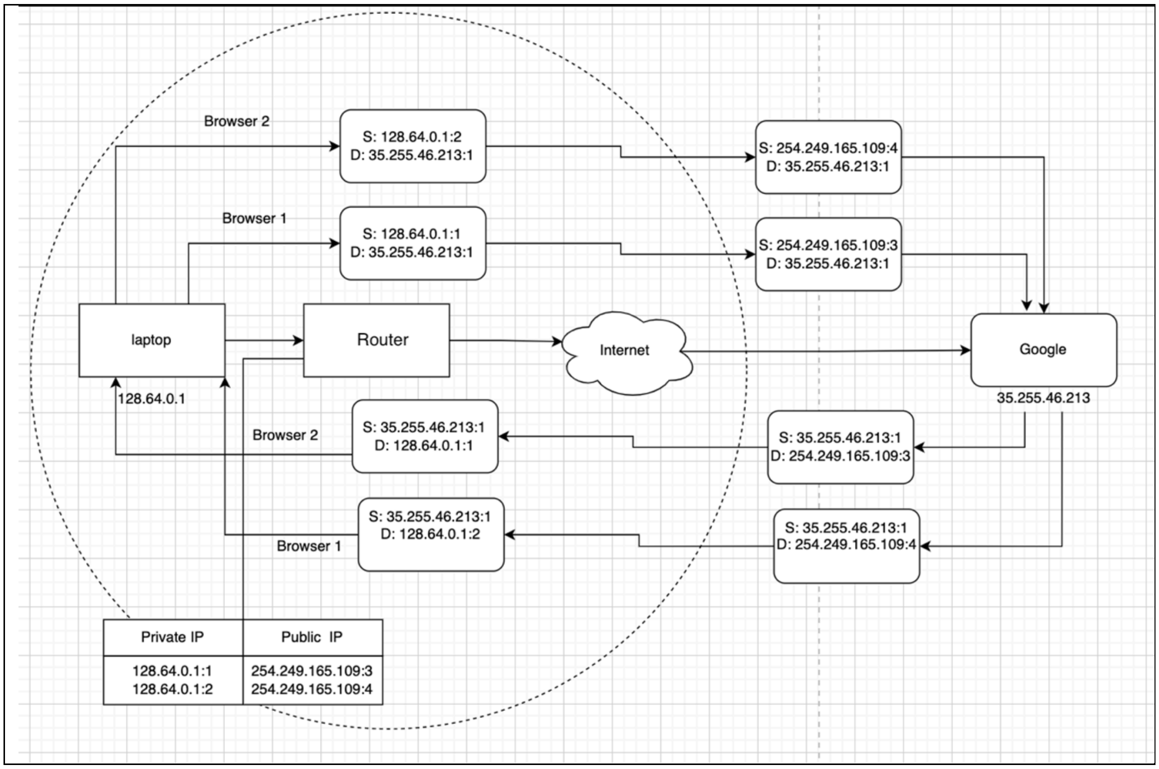
3. Dueling Google searches (10 pts)

On your laptop, which is behind a NAT, you open two tabs in your web browser and load the Google webpage in BOTH tabs.

1. Diagram the setup as done in class, showing your laptop, the NAT, and Google.



2. Diagram the movement of one packet from each of your browser tabs to Google (as well as the response from Google).



Private IP	Public IP
128.64.0.1:1 128.64.0.1:2	254.249.165.109:3 254.249.165.109:4

3. How does the right response from Google get passed to the correct tab?

The right response from Google gets passed to the correct tab based on the host of where the tab was sent from. In other words, the tab sending a packet attaches a port number to the IP address and while communicating with the server (in this case Google) it will keep using the same port number. Every time another tab is opened, that tab will add its own the port number to the IP address. That's how the response can distinguish between different tabs using the same IP address.

4. VPN server (12 pts)

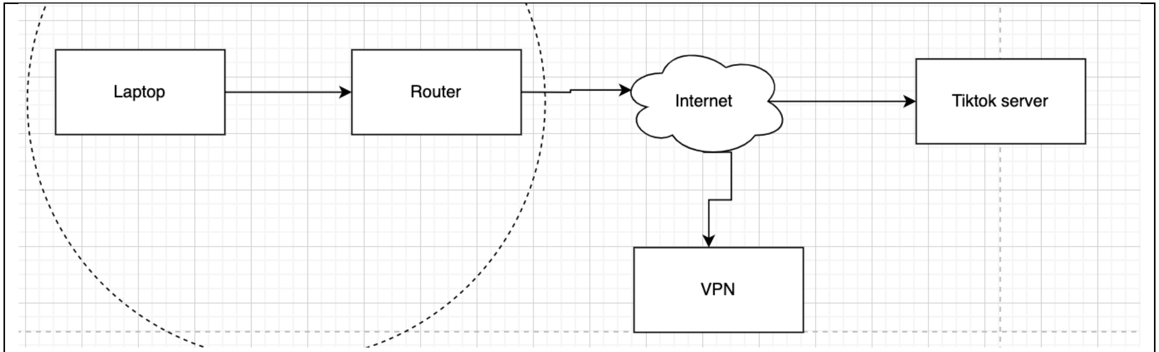
You are trying to access TikTok from your local library's wifi… except that they seem to have blocked access to it.

1. What does it mean that access is blocked? Explain what is happening on the packet level – specifically, why isn't communication possible and where is it breaking down?

Having the access blocked means that my requests are not being registered. Meaning somewhere between sending packets to make a request to a server, and that server responding to that request, the packets get shutdown, and my device is not being allowed to access the resources.

Now to get into more details about what is happening on the packet level; The reason why the packets are being broken down is because when opening an app, the device sends packets to a server to make a request and it goes through the library's router. The router has a list of IP addresses which are blacklisted, meaning it will not allow any requests to be made to those servers and will instead drop the packets. The router then interprets the destination IP address and can either send the packets to the server or deny them. In this case, TikTok has a unique IP address which the router has blocked off sending any requests to it. Thus using the port number attached to the IP address, the router will let my device know that I will not get any response from the intended server.

2. Knowing the ways of VPN, you activate a VPN client to circumvent the block. Your packets are now flowing. As we did in class, diagram this setup (but you don't have to show packets moving). What machines are involved in this VPN solution? What is each of their roles?



1. The device (laptop) sends packets to TikTok to request access to the apps services and content.
2. The libraries router on the schools LAN acts as a firewall. Meaning it manages all packets being sent and received from devices and servers. Like mentioned in part 1 of this question, it accepts or denies sending the packets by looking at the IP address and returns the appropriate response to the port number attached to that IP address.
3. The VPN client which serves as a proxy for the libraries router and circumvent firewalls. Once the client is on, the device sends packets to the VPN client since the router has not blacklisted the VPN client destination. Once the packets are sent to the VPN client, the new packets content get encrypted and it's destinations is routed to the TikTok server which can then return the appropriate response and like so, we have found a way around the firewall.
4. The TikTok server which is simply hosting all of TikTok's content and is the end destination for the packets. It handles all requests from different devices and returns the appropriate response.

Discussion

1. Virus protection? (5 pts)

A computer can "catch a virus" when it receives information containing malicious software. Your lab partner uses a VPN to access some pretty shady sites on the internet. This person claims that the VPN will protect their computer from getting viruses. Why is this incorrect?

Yes, it's possible. VPNs encrypt and secure your internet traffic and personal data and only protects part of the path from your laptop to the server. The VPN does not have any effect on the behavior of the server and what the server will respond to the request. Meaning they also have no effect on what the server returns to your laptop. Thus, the server can return any packet or software that your device can download.

2. Anonymization, take 2 (5 pts)

Your friend from a previous assignment (who said that they were anonymous on the internet) has now installed a VPN and uses that for their internet activities. He now assures you that he is anonymous on the internet. Why is this still not quite right?

VPN offers better privacy, but privacy is not interchangeable with anonymity. A VPN only encrypts all the data being sent from your laptop to the VPN server, including your IP address which gets changed, but does not encrypt anything from the VPN server to the destination website/server. So, whoever is on the receiving end of your traffic isn't prevented from tracing that traffic back to you IP address (the VPN server's given IP address). But that VPN provider will be able to trace that IP address back to the laptops address. For example, law enforcement can always request the logs of a VPN. Or like mentioned above, they can install a software/virus and trace you like so. The point is the VPN encryption definitely makes it difficult but not impossible to trace your laptop.

Note that there's also many other ways that a website can take away your anonymity. Things like, cookies, if you're logged into the website or their service, your metadata, etc.

3. Tor requirements (5 pts)

Your friend is smitten with a painfully boastful hacker. Over a rather awkward dinner to which this person has been invited, they're boasting about how they've been able to hack the Tor network and can now see anyone who is using it. Effectively, the hacker is claiming that they can single-handedly remove anonymity from Tor. Appealing to the design principles of Tor we discussed in class, why is this unlikely?

This is unlikely because TOR offers privacy and security but does not provide anonymity. The user is still able to reveal themselves in other ways like proven in other questions above (name, email, metadata, etc.).

Also, note that anonymity is technically impossible on the internet, but we can make it very difficult to identify a device. There are a large number of nodes in the TOR network, and the random configuration of nodes makes it so that the anonymity is even stronger. The route a source packet makes to reach a server is completely random within these nodes, so if someone found and IP address tracing back to the source, it's most likely the TOR's original location and not the actual that sent the original packet. Because of the way TOR allows packets to be sent, the packet could have gone through a lot of different TOR machines before reaching its destination. Meaning the hacker is going to have to correctly identify the sequence and nodal configurations of the path the packet took, which is highly unlikely.