**Layer 3 and Layer 4 Security**

**CYBR3010**

**Cybersecurity Foundations**

Arr Domingo

Student ID: 200458099

Instructor: Sam El-Awour

Table of Contents

[**1.** **Introduction** 1](#_Toc212396635)

[**2.** **IP Address Configuration** 1](#_Toc212396636)

[**2.1 Configure static IP address of Kali Linux** 1](#_Toc212396637)

[**2.2 Configure static IP address of Client 20 and Client 30 VM (both Windows 11)** 1](#_Toc212396638)

[**2.3 Configure the Firewall with static IP address** 1](#_Toc212396639)

[**2.4 Configure the Firewall to be a DHCP Server** 1](#_Toc212396640)

[**3.** **Network Diagram** 3](#_Toc212396641)

[NAT Configuration 3](#_Toc212396642)

[Subtopic 2.1 3](#_Toc212396643)

[**4.** **Vulnerabilities and potential impact** 4](#_Toc212396644)

[4.1 Network reconnaissance using Zenmap 4](#_Toc212396645)

[4.2 Research another vuln 4](#_Toc212396646)

[**5.** **Test Results (before and after scenarios)** 4](#_Toc212396647)

[5.1a. Before the actual cyber-attack, perform network reconnaissance using Zenmap 4](#_Toc212396648)

[5.1b. After the successful network reconnaissance using Zenmap 4](#_Toc212396649)

[5.2a. Before scenario –research 4](#_Toc212396650)

[5.2b. After scenario --research 4](#_Toc212396651)

[**6.** **Prevention and Mitigation** 4](#_Toc212396652)

[6.1 Implementation of VLAN as protection to network reconnaissance using Zenmap 4](#_Toc212396653)

[6.1.1. VLAN configuration in switch 4](#_Toc212396654)

[6.1.2. VLAN configuration in firewall 4](#_Toc212396655)

[6.2. Implementation of …. --research 4](#_Toc212396656)

[Questions and Answers 5](#_Toc212396657)

[Subtopic 3.1 5](#_Toc212396658)

[References 1](#_Toc212396659)

# **Introduction**

This document is about Layer 3 and Layer 4 of the OSI Layer, which is the Network Layer and Transport Layer. It is in Layer 3 where routing, packet forwarding, and logical addressing happens with the use of an IP address; hence this document will cover on how to configure IP addresses statically and dynamically through enabling Dynamic Host Control Protocol (DHCP) on a firewall. For Layer 4, Transport layer ensures the reliable and efficient data delivery through segmentation; hence this document will cover the configuration of VLAN on the switch (to segment the network for better traffic control and security) and on the firewall. Moreover, this document will go through the configuration of NAT internet access.

Finally, network layer and transport layer are prone to cyberattacks. Therefore, this document will tackle the vulnerabilities and potential impact associated with this layer, compare results before and after the attack, and apply security measures to mitigate these vulnerabilities effectively.

# **IP Address Configuration**

An IP (Internet Protocol) Address is a unique numerical label assigned to each device connected to a computer network which serves two main purposes: to identify a device on a network, and to locate the device that enables communication with other devices over a network like the Internet. There are two ways to configure an IP address: static and dynamic. Static IP addresses are manually assigned and remain the same unless changed by an administrator, while dynamic IP addresses allow a device to automatically obtain network configuration information, including an IP address, from a DHCP server on the network.

## **2.1 Configure static IP address of Kali Linux**

* Right-click “Network Connections” and click “Edit Connections”

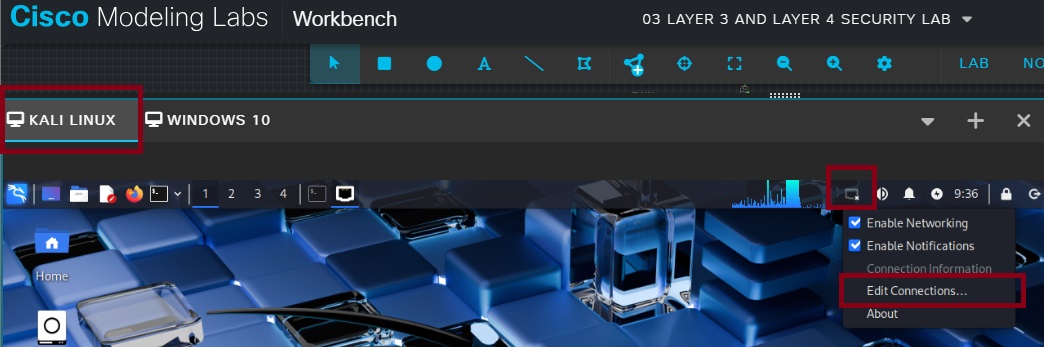


Figure 1. Starting point to configure static IP address of Kali Linux.

* Choose “Wired connection 1” and click the gear icon.

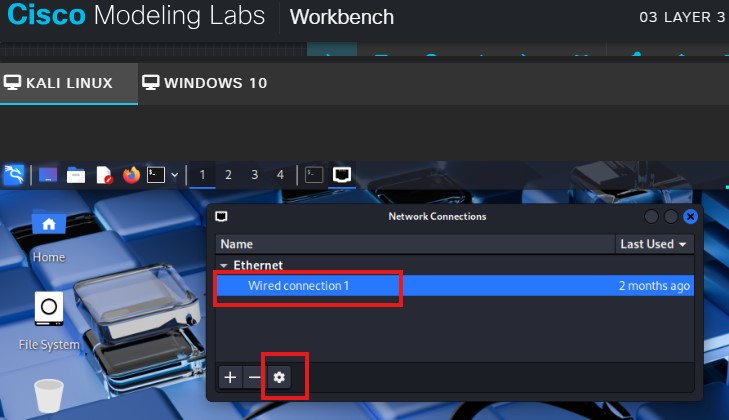


Figure 2. Choosing the connection.

* On “Editing Wired connection 1” window, go to “IPv4 Settings” tab. Method is “Manual”. Click “Add” button and put the following details:
* Address: 192.168.0.11
* Netmask: 255.255.255.0 (this is full format, can also be 24 format)
* Gateway: 192.168.0.1
* DNS servers: 8.8.8.8

Click “Save”.

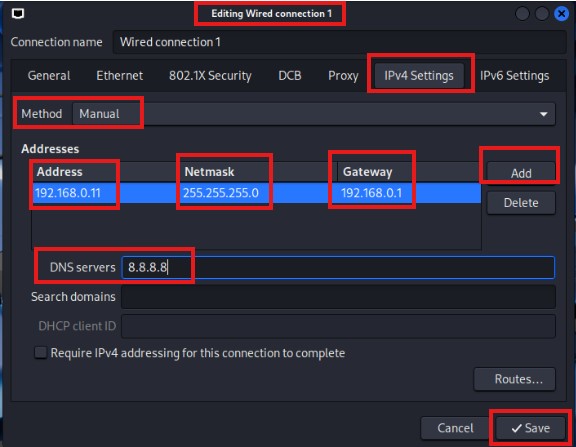


Figure 3. Step to edit the connection and enter necessary details.

* At this point, IP address of Kali Linux is configured. To verify the IP address of Kali Linux, open terminal and type “ifconfig”.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4. Static IP address of Kali Linux is 192.168.0.11.

* Considering other client VMs are properly configured, to verify the connection, ping the device using its own IP address and IP address of other devices.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 5. Successful ping for both self and other devices.

## **2.2 Configure static IP address of Client 20 and Client 30 VM (both Windows 11)**

* Right-click the network icon then click “Network and Internet settings”.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 6. Starting point to configure static IP address of Windows 11.

* Click “Ethernet”.

A black screen with a black background

AI-generated content may be incorrect.

Figure 7. Ethernet connection.

* Go to “Unidentified network”. On Ip assignment, click “Edit”.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 8 Continuation of Ethernet connection.

* Choose “Manual” on Edit IP settings. Turn on “IPv4”. Enter following details:
* Ip address: 192.168.0.12 (for Client 20) / 192.168.0.13 (for Client 30)
* Subnet mask: 255.255.255.0
* Gateway: 192.168.0.1
* Preferred DNS: 8.8.8.8

Click “Save”.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 9. Step to edit connection and enter necessary details.

* Windows 11 doesn’t automatically allow ping. So in order to ping Windows 11 device, need some configuration on Windows Defender Firewall with Advanced Security.
* Click Windows icon, type "Windows Defender Firewall with Advanced Security", and press enter.
* On left pane, click "Inbound Rules".
* Right-click all "File and Printer Sharing (Echo Request - ICMPv4-In)" and click "Enable Rule".

A screenshot of a computer

AI-generated content may be incorrect.

Figure 10. Configuration of firewall inbound rules.

* Also, create a “New Rule”. On the right pane, click "New Rule".
* Choose "Custom" and click "Next".
* Choose "All programs" and click "Next".
* On Protocol type, choose "ICMPv4" and click "Next".
* Keep default and click Next.
* Check "Allow the connection" and click Next.
* All options must be checked and click Next.
* Put name (Allow ICMP) and click "Finish".

A screenshot of a computer

AI-generated content may be incorrect.

Figure 11. Firewall configuration to Allow ICMP.

* To verify the IP address, open CMD and type “ipconfig /all”.

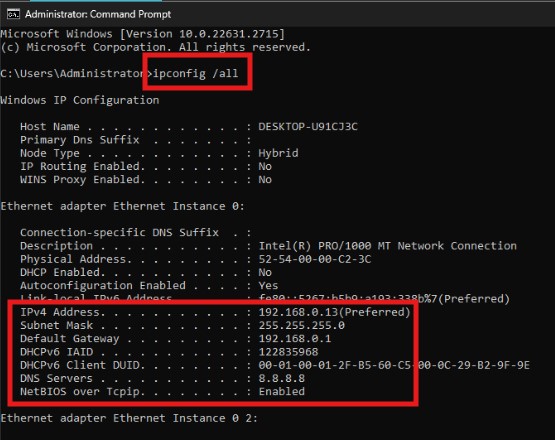


Figure 12.IP address of Client 20 is 192.168.0.12. IP address of Client 30 is 192.168.0.13. Static IP settings are configured manually.

* Considering other client VMs are properly configured, to verify the connection, ping the device using its own IP address and IP address of another device.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 13. This is the result of ping from Client20 VM. Note that this ping result is similar for Client30 VM.

## **2.3 Configure the Firewall with static IP address**

* Start the firewall (FW01) as well as all the devices.
* Right click the firewall (FW01) and choose “Console”. You know firewall is done booting when you are able to see the serial number and the firewall login.
* Type “**cisco**” in the “Firewall login” and “Password”.
* Wait until you see “Welcome”.

A screenshot of a computer

AI-generated content may be incorrect.

Initial step to open firewall in CML.

* Type “get system interface physical port1” to get information about port 1 that is connected to the internet. Open the IP address in another browser.

A screenshot of a computer

AI-generated content may be incorrect.

Information of Port 1.

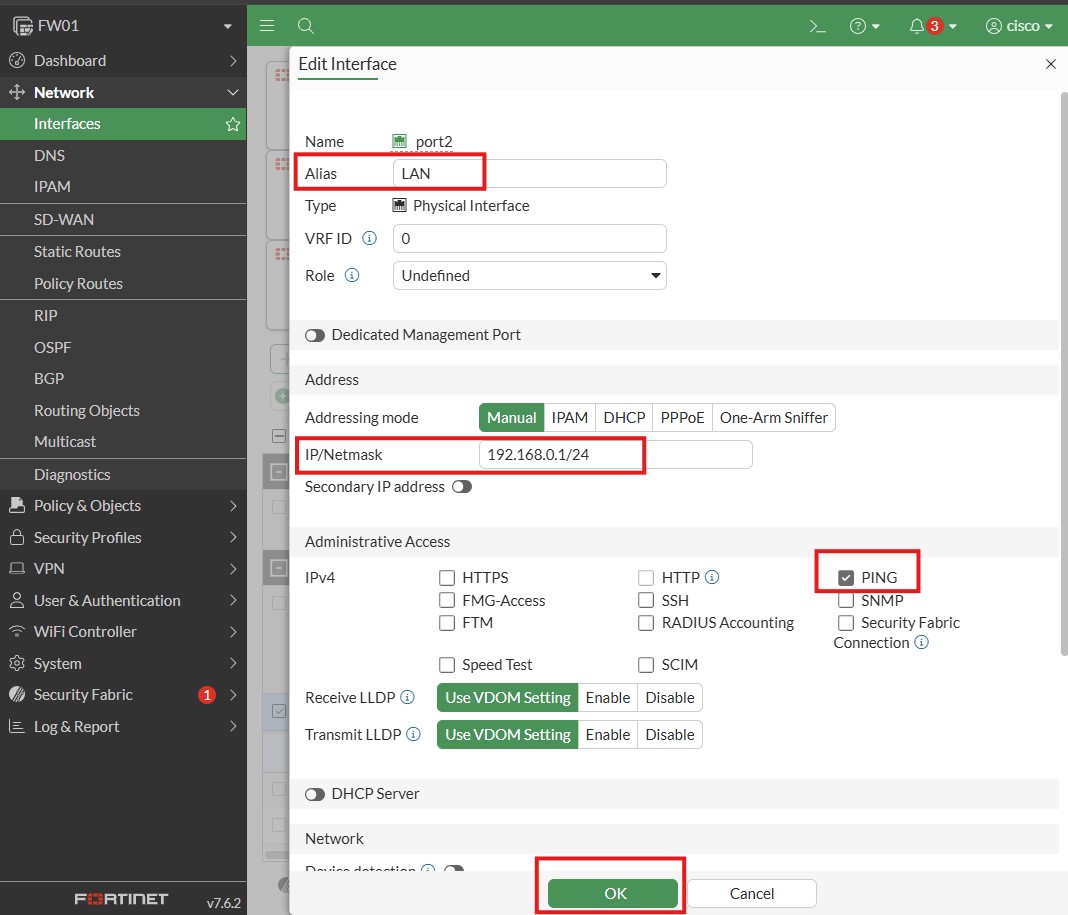
* On the browser, click “Advanced”.
* Click “Proceed to 192.168.202.146(unsafe)”.
* Type “**cisco**” as the Username and Password, then click “Login”.
* Click "Login Read-Write".
* Click "Yes".
* Click "Begin".
* In the Dashboard Setup, choose the default which is "Optimal" and press "OK".
* Firewall (FW01) dashboard will open up.

A screenshot of a computer

AI-generated content may be incorrect.

Firewall dashboard.

* In the firewall (FW01) dashboard, click “Network”.
* Click “Interfaces”.
* Double click “port2” as this is the port connecting firewall to the switch.
* On “Edit Interface” window, enter the following details:
* Alias: LAN
* IP/Netmask: 192.168.0.1/24
* On “IPv4”, check the “PING”
* Click OK.



Edit the interface of firewall.

* From the client VM, ping the firewall/gateway IP (192.168.0.1) to check the connection.

A screenshot of a computer

AI-generated content may be incorrect.

Successful ping of client machines to the firewall/gateway IP.

## **2.4 Configure the Firewall to be a DHCP Server**

* With the same static IP address setup on port2, click to enable “DHCP Server”.
* On the “Address range”, leave an IP address for other devices such as printer, fax machine, etc. Therefore, just put 192.168.0.50-192.168.0.200.
* Keep the “Default gateway” and “DNS server” as is.
* Click OK.

A screenshot of a computer

AI-generated content may be incorrect.

Firewall with DHCP Server enabled.

* On the client machines, type the command “ipconfig /renew” to request a new IP address from a DHCP server. This will take some time to process. Or do the other way which is faster. Go to >Control Panel >Network and Internet >Network and Sharing Center >Change Adapter Settings >Right click Ethernet to disable >Right click Ethernet to enable.
* At this moment, client VMs must be taking dynamic IP addresses. For Kali Linux, type “ifconfig” in the terminal. For Client20 and Client30, type “ipconfig” in the CMD.

A screenshot of a computer

AI-generated content may be incorrect.

Dynamic IP of Kali Linux is 192.168.0.52. Dynamic IP of Client20 is 192.168.0.51. Dynamic IP of Client30 is 192.168.0.50.

# **Network Diagram**

One of the crucial components of an organization’s security strategy is often referred to as Identity and Access Management (IAM). IAM ensures that the right people, machines, and software components access the right digital resources at the right time and for the right reasons.

# NAT Configuration

MODULE 2, LESSON 2a:

NETWORK LAYER SECURITY

## Subtopic 2.1

# **Vulnerabilities and potential impact**

## 4.1 Network reconnaissance using Zenmap

Zenmap is the graphical user interface (GUI) for Nmap that provides a user-friendly interface for tasks like discovering active devices/hosts, identifying open ports, and finding vulnerabilities without requiring extensive command-line knowledge. It is a powerful tool in the context of the network and transport layers, as they are reconnaissance techniques used as critical initial steps to a more malicious activity. It also helps in identifying the operating systems and application/service versions that can be exploited in the later stages of an attack.

As a result of the network scan with zenmap, the information gathered will be used to plan and execute more damaging actions like denial-of-service (DOS) attacks, data breaches, etc. For example, an attacker might discover an open port for a specific version of a service and then use a known exploit for that vulnerability.

## 4.2 ICMP Attack (Ping Flood)

ICMP ping flood attack is a form of Distributed Denial-of-Service (DDoS) attack in which an attacker floods the recipient device by overwhelming it with ICMP echo requests, also known as pings. Essentially, Internet Control Message Protocol (ICMP) ping requests are used to check for connectivity and the health of networking devices. In a legitimate ICMP ping, the recipient device replies to an ICMP echo request. The response indicates the health of the recipient.

The goal of ICMP ping flood attack is to consume the target’s network bandwidth and/or processing capacity so legitimate traffic or services are disrupted or slowed. These attacks can severely disrupt an organization’s online network operations, compromise the security of the cloud or local infrastructure, and making services unavailable to legitimate users. The resulting service disruptions and outages can significantly impact businesses, particularly those that rely heavily on online services.

Follow this: Deep Packet Analysis Ep4 - ICMP PING FLOOD + FortiGate Firewall Part 1

<https://www.youtube.com/watch?v=vegnSkRNMJs>

<https://www.youtube.com/watch?v=bYM3lWzqPwI&list=PL12zYfEw-h5q_yDEcQyzSa87pxwZq2rrw&index=12>

how to do ICMP ping flood in kali linux and firewall?

# **Test Results (before and after scenarios)**

## 5.1a. Before the actual cyber-attack, perform network reconnaissance using Zenmap

* Click Kali Linux icon and type “zenmap”.
* Type “cisco” as the password and click “Authenticate” to open up zenmap.

A screenshot of a computer

AI-generated content may be incorrect.

Zenmap is a tool use to do network reconnaissance.

* On a real cyber-attack scenario, once you are connected to a network, you will get an idea of what range of IP addresses to scan. For this purpose, put IP address network range which is “192.168.0.0-250” on “Target”.
* On “Profile”, choose “Quick Scan”.
* Click “Scan” to quickly see what is in the network, figure out more information of what hosts are active, and from there, it is possibly the launch of further attack.

A screenshot of a computer

AI-generated content may be incorrect.

Result of Zenmap scan where 3 active hosts were found.

## 5.1b. After the successful network reconnaissance using Zenmap

* From those active hosts, choose one IP address to scan in order to get more information. This time, choose “Intense Attack” on Profile and click Scan.

A screenshot of a computer

AI-generated content may be incorrect.

Result of Zenmap scan for specific host, which is a successful cyber-attack.

* At this point in time, the attacker achieves the ultimate objective of network reconnaissance which is to gather more information about a target’s network and plan an effective strategy for future cyber-attack.

## 5.2a. Before scenario –research

## 5.2b. After scenario --research

# **Prevention and Mitigation**

## 6.1 Implementation of VLAN as protection to network reconnaissance using Zenmap

VLAN blah blah…

To prevent and mitigate from getting information on the network via Zenmap, the solution is to configure VLAN so that every device cannot be on the same network.

### VLAN configuration in switch

* On the switch console, type “enable”.
* Type “config” to configure the switch.
* Press enter when ask “Configure from terminal?”.
* Inside the switch config, type “vlan 10” and press enter.
* Type “name HR” to put a name on vlan 10 and press enter.
* Add another vlan which is “vlan 20” and press enter.
* Type “name IT” and press enter.
* Another vlan which is “vlan 30” and press enter.
* Type “name Finance” and press enter.

A screenshot of a computer program

AI-generated content may be incorrect.

Vlan configuration in the switch.

* Type “exit” and press enter.
* Type “exit” and press enter.
* Type “show vlan” to show lists of existing vlan.

A screenshot of a computer

AI-generated content may be incorrect.

Trunk port is used to connect switches or routers, transmitting data from multiple VLANs simultaneously. Access port connects virtual machines to a switch or VLAN, transmitting data within a single VLAN.

* Trunk port configuration (e0/0)
* Type “configure terminal” and press enter.
* Type “int e0/0” and press enter.
* Type “switchport trunk encapsulation dot1q” and press enter.
* Type “switchport mode trunk” and press enter.

A screenshot of a computer program

AI-generated content may be incorrect.

Commands in switch console to configure trunk port.

* Access port configuration (e0/1, e0/2, e0/3)
* In the same switch configuration, type “int e0/1” and press enter.
* Type “switchport mode access” and press enter.
* Type “switchport access vlan 10” and press enter.

A computer screen shot of a computer

AI-generated content may be incorrect.

Commands in switch console to configure access port of e0/1.

* For e0/2, type “int e0/2” and press enter.
* Type “switchport mode access” and press enter.
* Type “switchport access vlan 20” and press enter.

A screenshot of a computer

AI-generated content may be incorrect.

Commands in switch console to configure access port of e0/2.

* For e0/3, type “int e0/3” and press enter.
* Type “switchport mode access” and press enter.
* Type “switchport access vlan 30” and press enter.

A computer screen shot of a computer

AI-generated content may be incorrect.

Commands in switch console to configure access port of e0/3.

* Type “exit” and press enter.
* Type “exit” and press enter.
* Type “show vlan” and press enter to show lists of vlan .

A screenshot of a computer

AI-generated content may be incorrect.

Show lists of vlan after the configuration.

* Finally, type “write” and press enter to save the configuration made.

>> Firewall configuration with VLAN in place in the switch,

### VLAN configuration in firewall

* Go back to the firewall (FW01) specifically on port 2. On “IP/Netmask”, remove the existing IP and replace it with “0.0.0.0/0”. Disable “DHCP Server” as well. Press OK. This is like going back to the basic LAN.
* Next step is to create 3 different virtual interfaces under port 2 that talk to each VLANs created in switch.
* ----
* On the left panel of firewall (FW01) UI, go to “Network” and click “Interfaces”.
* Click “Create New” and click on “Interface”.
* On “New Interface” window, put “VLAN10” under “Name” (others are VLAN20 and VLAN30).
* Alias is “HR” (IT for VLAN20; Finance for VLAN30).
* Type is VLAN.
* VLAN protocol is 802.1Q.
* In Interface, choose “LAN(port2)”.
* VLAN ID is “10” (“20” for VLAN20; "30” for VLAN30).
* Click “Manual” in the “Addressing mode”.
* IP/Netmask is “192.168.10.1/24” (192.168.20.1/24 for VLAN20; 192.168.30.1/24 for VLAN30).
* Check “PING” on IPv4.
* Enable “DHCP Server”.
* Put “192.168.10.50-192.168.10.200” in the “Address range” (192.168.20.50-192.168.20.200 for VLAN20; 192.168.30.50-192.168.30.200 for VLAN30).
* Click OK.
* Repeat the process for VLAN20 and VLAN30.

A screenshot of a computer

AI-generated content may be incorrect.

VLAN 10 (HR) configuration.

A screenshot of a computer

AI-generated content may be incorrect.

VLAN 20 (IT) configuration.

A screenshot of a computer

AI-generated content may be incorrect.

VLAN 30 (Finance) configuration.

A screenshot of a computer

AI-generated content may be incorrect.

These are the 3 VLANs created.

* Verify if machines have the VLAN configured.

Insert ss of folder 6 images 5-7 here!

* At this point, VLAN is now in-place. It means VLAN10, VLAN20, and VLAN30 cannot communicate with each other anymore.

Insert ss of folder 6 image 8 here!

## 6.2. Implementation of …. --research

# Questions and Answers

## 7.1. What is IP spoofing, and how is it commonly used in network attacks? Discuss multiple mitigations explaining their benefits and limitations in different network environments.

7.2. How do ACLs operate at Layer 3/4 to filter traffic based on IP addresses, protocols, and ports? Evaluate their strengths and weaknesses as security control in large, distributed networks, and suggest how they should be combined with other defenses for layered security.

7.3. What are SYN flood attacks, and how do they exploit the TCP three-way handshake? Compare multiple mitigation approaches such as SYN cookies, connection rate-limiting, and load balancer filtering, and discuss their operational trade-offs.

7.4. How does Deep Packet Inspection differ from traditional packet filtering at Layers 3 and 4? Analyze its advantages and privacy concerns and propose scenarios where DPI should or should not be implemented in enterprise environments.

# References

*Difference Between Trunk Port and Access Port*. (2025, July 23). Retrieved from Geeks for Geeks: https://www.geeksforgeeks.org/computer-networks/difference-between-trunk-port-and-access-port/

Hess, K. (n.d.). *Scanning with Zenmap*. Retrieved from Linux Magazine: https://www.linux-magazine.com/Online/Features/Scanning-with-Zenmap

*What Is A Ping (ICMP) Flood DDOS Attack?* (n.d.). Retrieved from radware: https://www.radware.com/security/ddos-knowledge-center/ddospedia/icmp-flood/#WhatIsAPingFloodAttack

*What is a Ping Flood Attack?* (n.d.). Retrieved from Akamai: https://www.akamai.com/glossary/what-is-a-ping-flood-attack

*What is an IP Address?* (2025, October 7). Retrieved from GeeksforGeeks: https://www.geeksforgeeks.org/computer-science-fundamentals/what-is-an-ip-address/