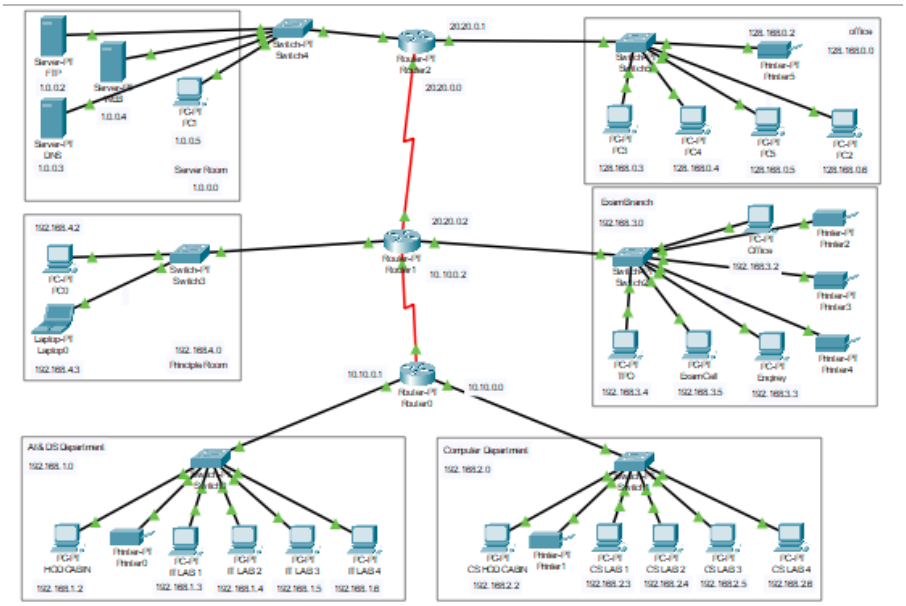
Cisco Cyber Security VIP 2023

Problem Statement: Choose a university/college campus and analyze its network topology. Map the network using Cisco Packet Tracer and identify the security controls that are in place, such as network segmentation, intrusion detection systems, firewalls, and authentication and authorization systems. Apply the knowledge gained from the NetAcad cyber security course to conduct an attack surface mapping, aiming to identify potential entry points for cyber-attacks. Propose countermeasures to mitigate these risks.

Network topology without security



A network consisting of servers, routers, switches, and end devices is a common architecture used in organizations to enable communication, data transfer, and resource sharing.
Let's understand the role of each component in this network:

1. **Servers:** Servers are powerful computers that provide various services and resources to other devices in the network. They can include file servers, web servers, database servers, email servers, and more. Servers store and manage data, host applications and websites, and offer centralized services for client devices.

2. **Routers:** Routers are devices responsible for directing network traffic between different networks or subnets. They connect multiple networks together, enabling data packets to be routed efficiently from one network to another. Routers analyze

IP addresses to determine the best path for data transmission and ensure that information reaches its intended destination.

3. **Switches:** Switches are devices that connect multiple devices within a network. They create a network segment or a local area network (LAN). Switches enable devices to communicate with each other by forwarding data packets to the appropriate destination based on the Media Access Control (MAC) addresses of the devices. Switches are typically used for local traffic within a network.

4. **End devices:** End devices, also known as client devices or hosts, are the devices used by end users to access the network and its resources. They can include desktop computers, laptops, smartphones, tablets, IoT devices, and more. End devices initiate communication by sending requests to servers or other devices and receive responses in return. End devices can also act as clients or servers, depending on the network architecture and their roles.

In this network architecture, end devices connect to switches, which provide local connectivity within a LAN. The switches are then connected to routers, which enable communication between different networks or subnets. Routers direct traffic between these networks and ensure efficient data transfer. Servers are connected to the switches or routers, providing services and resources to the client devices.

Overall, this network architecture allows for efficient data routing, centralized services, and connectivity among different devices within an organization's network infrastructure. It facilitates communication, resource sharing, and the seamless exchange of information across the network.

Vulnerabilities associated with this network topology

Networks can have various vulnerabilities that can potentially compromise their security and expose sensitive information to unauthorized access or malicious activities. Here are some common vulnerabilities to be aware of:

1. **Weak Authentication and Passwords:** Weak or easily guessable passwords, default credentials, or shared accounts make it easier for attackers to gain unauthorized access to network devices, servers, or user accounts. It is crucial to enforce strong password policies, implement multi-factor authentication (MFA), and regularly update passwords.

2. **Lack of Patch Management:** Failure to regularly apply security patches and updates to network devices, servers, and applications leaves them vulnerable to known exploits and vulnerabilities. Regular patch management helps address security weaknesses and protects the network from potential attacks.

3. **Misconfigured Network Devices:** Incorrectly configured routers, switches, and firewalls can create security holes, allowing unauthorized access or network disruptions. Configuration errors may include open ports, weak firewall rules, or improperly implemented access control lists (ACLs). Regular security audits and best practices should be followed when configuring network devices.

4. **Insufficient Network Segmentation:** Lack of proper network segmentation can increase the attack surface. Without segmenting the network into isolated zones, an attack on one device or system can potentially compromise the entire network. Implementing network segmentation using VLANs, firewalls, and access control mechanisms can help contain attacks and limit their impact.

5. **Malware and Phishing Attacks:** Malicious software (malware) and phishing attacks pose significant threats to networks. Malware, such as viruses, worms, ransomware, or spyware, can spread across the network, compromising data and disrupting operations. Phishing attacks target users through deceptive emails or websites to obtain sensitive information like login credentials. Robust antivirus software, email filtering, and user awareness training are essential to mitigate these risks.

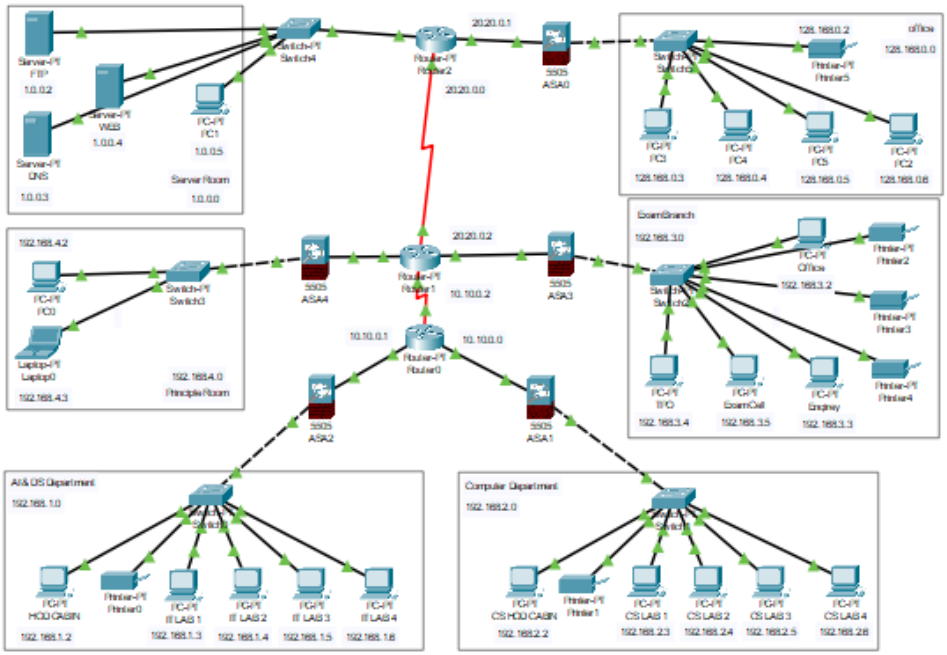
6. **Insider Threats:** Insider threats, whether intentional or accidental, can be a significant vulnerability. Employees or individuals with privileged access may misuse their permissions or inadvertently introduce security risks. Implementing

access controls, monitoring user activities, and conducting periodic security awareness training can help mitigate the insider threat.

7. **Lack of Network Monitoring and Logging:** Inadequate network monitoring and logging make it difficult to detect and respond to security incidents promptly. Having a robust logging and monitoring system allows for the identification of suspicious activities, network anomalies, or signs of compromise, enabling timely incident response.

It's important to note that network vulnerabilities can vary based on the specific network setup, infrastructure, and technologies used. Regular security assessments, vulnerability scans, and penetration testing can help identify and address vulnerabilities specific to your network environment.

Network topology with security



Adding Cisco-ASA (Adaptive Security Appliance) devices to a network can significantly enhance its security posture. Cisco ASA is a next-generation firewall and security appliance that provides a wide range of security features and capabilities. Here's how incorporating Cisco ASA devices can increase network security:

1. **Robust Firewall Protection:** Cisco ASA devices act as firewalls that can enforce security policies at the network perimeter. They inspect incoming and outgoing traffic, blocking unauthorized access attempts and potentially malicious data packets. With Cisco ASA, you can define and enforce granular access control rules based on IP addresses, ports, protocols, and application-layer information.

2. **VPN (Virtual Private Network) Support:** Cisco ASA devices offer VPN functionality, allowing secure remote access for authorized users. Through VPNs, remote users can connect to the network over encrypted tunnels, ensuring confidentiality and integrity of data transmitted over public networks like the internet.

3. **Intrusion Prevention System (IPS):** Cisco ASA can function as an IPS, providing real-time threat detection and blocking capabilities. It analyzes network traffic patterns, signatures, and anomalies to identify potential security threats and take appropriate action to prevent attacks.

4. **Web Application Firewall (WAF):** Cisco ASA includes WAF features that protect web applications from common web-based attacks, such as SQL injection, cross-site scripting (XSS), and application-layer DoS attacks. This helps secure web servers and applications against known vulnerabilities and exploits.

5. **Advanced Threat Protection:** Cisco ASA integrates with Cisco's security ecosystem, allowing it to access threat intelligence and provide protection against emerging threats and zero-day attacks. By leveraging Cisco's threat intelligence feeds, the ASA can identify and block malicious traffic more effectively.

6. **Security Management and Visibility:** Cisco ASA devices come with comprehensive management interfaces and reporting tools that provide visibility into network activity, security events, and potential threats. Network administrators can monitor and analyze security incidents, enabling them to respond quickly to potential security breaches.

7. **Identity-Based Access Control:** Cisco ASA supports identity-based access control, allowing you to define security policies based on user identities and groups. This ensures that only authorized users have access to specific resources and services.

8. **High Availability and Redundancy:** Cisco ASA supports clustering and failover capabilities, ensuring high availability and redundancy. If one device fails, another ASA can seamlessly take over, reducing the risk of network downtime.

9. **SSL/TLS Inspection:** Cisco ASA can perform SSL/TLS decryption and inspection, allowing it to detect and block threats hidden within encrypted traffic.

By deploying Cisco ASA devices in the network, organizations can bolster their security infrastructure, protect critical assets, and mitigate a wide range of cyber threats effectively. However, it is essential to ensure proper configuration, maintenance, and updates of these devices to maintain their effectiveness in the evolving threat landscape.