MANIPAL INSTITUTE OF TECHNOLOGY

MADHAVA NAGAR MANIPAL UDUPI DISTRICT KARNATAKA
576104,MANIPAL,UDUPI,Karnatak a,576104 Institution Type Deemed to be
University(Pvt) Region South-West

Virtual Summer Internship Program 2024

A Virtual Summer Internship project report on cyber security submitted in partial fulfillment of the requirements for the AICTE-CISCO virtual Internship in cyber security Program 2024

Submitted By
Aditya Raj

AICTE Internship Student Registration ID) : STU66447a52bf2671715763794

Student ID (Enrolment number) : 210968136

Email : adityaraj006005@gmail.com

Contact Info : +917050804020

Cyber Shield: Defending the network
Problem Statement

PART 1:
Analyse your existing university/college campus network topology.
Map it out the using Cisco Packet Tracer and identify the security controls that are in place today.
Consider and note how network segmentation is done.
Observe what kind of intrusion detection systems, firewalls, authentication and authorization systems are in place.
Apply the knowledge gained from the NetAcad cyber security course to conduct an attack surface mapping.
Aim to identify potential entry points for cyber-attacks. Propose countermeasures to mitigate these risks.

Tasks:
1. Campus Network Analysis: conduct an analysis of your college campus network topology, including the layout, devices, and connections.
2. Network Mapping: Utilize Cisco Packet Tracer to map the network infrastructure, representing the placement and interconnectivity of routers, switches, firewalls, and other relevant network components.
3. Attack Surface Mapping: Conduct an attack surface mapping exercise to identify potential vulnerabilities and weaknesses within the network architecture and design. Consider factors such as unauthorized access, data breaches, and network availability.

Deliverables:
1. Network topology diagram depicting the existing infrastructure and attack surface findings.
2. Security assessment report highlighting identified security risks, proposed solutions and countermeasures to mitigate attack surface risks.

1. Campus Network Analysis:

Network Layout:

The existing network layout consists of a structured arrangement of connectivity between multiple network devices, including routers, switches, access points, firewalls, computers, and servers across different campus buildings.
Devices Configured:

Routers: strategically placed to manage traffic between networks.
Switches: facilitating data exchange within network segments.
Access Points: providing wireless connectivity across the campus.
Firewalls: guarding the network perimeters.
Computers: divided between faculty and students .
Servers: handling Web, Email, DNS, Database, Backup services.
Connections:High-speed Ethernet cables and wireless protocols interconnect these devices, ensuring robust campus-wide network accessibility.

2. Network Mapping Using Cisco Packet Tracer:

Attached Aditya_Raj_CyberSecurity.pkt file Where I have made the Network Mapping of my University MIT manipal Using Cisco Packet Tracer

3. Attack Surface Mapping:

Identification of Vulnerabilities:

Open Ports: Identify and assess the necessity of open ports on routers and switches, recommending closures or security enhancements where needed.
Weak Passwords: Audit all devices for weak or default passwords and enforce a strict password policy.
Encryption Gaps: Evaluate the encryption methods used for data in transit and at rest, proposing upgrades to more secure protocols where necessary.
Outdated Firmware: Check for outdated firmware versions that may expose the network to security risks and plan for regular updates.
Potential Entry Points for Cyber-Attacks:

Wireless Access Points: Ensure all wireless connections are secured with WPA2 or WPA3 encryption to prevent unauthorized access.
Web Servers: Update and secure all public-facing web servers to mitigate the risk of cyber-attacks.
Shared Passwords: Implement policies to prohibit password sharing and encourage the use of personal credentials.
Physical Security: Enhance physical security measures to prevent unauthorized physical access to critical network infrastructure.

Proposed Solutions and Countermeasures:

To robustly secure our university's network and address the identified vulnerabilities, we recommend the following specific technological and procedural countermeasures:

Technological Upgrades:

Update and Patch Management:
Implement a centralized patch management system to ensure all network devices, including routers, switches, and servers, are always updated with the latest security patches.

Strengthen Password Security:
Enforce a strict password policy that requires complex passwords combining letters, numbers, and special characters.
Implement multi-factor authentication (MFA) across all systems, especially for administrative access and remote connections.

Enhance Network Encryption:
Deploy end-to-end encryption for data in transit using protocols such as TLS and SSL.
Ensure that sensitive data stored on servers is encrypted at rest using robust encryption standards.

Secure Wireless Networks:
Upgrade all wireless networks to use WPA3 encryption.
Regularly audit and restrict the use of legacy wireless equipment or protocols that do not support the latest security standards.

Advanced Intrusion Detection and Prevention Systems (IDPS):
Deploy sophisticated IDS/IPS solutions that can detect and respond to both known and emerging threats.
Regularly update IDS/IPS signatures and monitor network traffic for anomalies.

Firewall Optimization:
Review and reconfigure firewall rules to minimize unnecessary open ports and to segment the network effectively, restricting traffic between critical network segments.
Procedural Enhancements:

Regular Security Audits and Penetration Testing:
Schedule annual third-party security audits and regular penetration testing to identify and remediate vulnerabilities before they can be exploited.

Security Training and Awareness Programs:
Conduct ongoing security training sessions for all university staff and students, focusing on the importance of security best practices, recognizing phishing attempts, and secure handling of sensitive information.

Incident Response Planning:
Develop and regularly update an incident response plan that includes clear procedures and roles for responding to cybersecurity incidents.
Conduct simulated cyberattack exercises to ensure all team members understand their responsibilities during an incident.

Physical Security Measures:
Improve physical security controls to protect network infrastructure from unauthorized physical access, including surveillance systems, access controls, and secure locking mechanisms for server rooms and data centers.

Conclusion:
The implementation of these proposed solutions and countermeasures is crucial for safeguarding our university's network against potential cyber threats. As digital threats continue to evolve in complexity and severity, the proactive enhancement of our network's security infrastructure and policies is not merely beneficial but essential. These measures will not only protect sensitive academic data but also safeguard the personal information of our students and staff, thereby maintaining the trust and

integrity of our institution. Adopting these recommendations will fortify our defenses and ensure that our network remains resilient against cyber threats, supporting our ongoing commitment to providing a secure and reliable digital environment for all educational activities.

PART 2:
Your college has hired you to design and architect a hybrid working environment for its faculty and students.
Faculty members will be provided with laptops by the college to connect to the college network and access faculty specific services & resources.
These should be accessible from home as well as on campus.
Students are allowed to connect using their personal devices to access student specific services & resources from home as well as on campus.
Campus network services should not be exposed to public internet and accessible only via restricted networks.

Tasks & Deliverables:
1. Explore options for how to achieve this and what kind of network security product can provide this capability
2. Update the campus network topology with the new components
3. Explain the reasoning behind your choices detailing the risks & advantages of your proposed solution

Solution:

1. Explore Options for Network Security Products:

Products and Technologies:

1. Virtual Private Network (VPN):
   - Product Example: Cisco AnyConnect Secure Mobility Client
   - Use: Securely connects faculty and students to the college network from remote locations by encrypting traffic and using strong authentication methods.

2. Network Access Control (NAC):
   - Product Example: Cisco Identity Services Engine (ISE)
   - Use: Manages and enforces security compliance on all devices that access the network, ensuring that only authorized devices can access specific resources.
3. Multi-Factor Authentication (MFA):
   - Product Example: Duo Security
   - Use: Adds an additional layer of security by requiring two or more verification methods to gain access to the network, reducing the risk of unauthorized access.

4. Cloud Access Security Broker (CASB):
    - Product Example: Cisco Cloudlock
    - Use: Protects data in cloud services and ensures that only authorized users can access sensitive information remotely.

Updating the Campus Network Topology:

New Components:

1. VPN Gateways:
    - Placement: Deployed at the network perimeter to handle incoming VPN connections securely.
2. NAC Solutions:
    - Placement: Integrated with the network infrastructure to monitor and control access at various network access points.
3. MFA Systems:
    - Integration: Across all user access points to the network, including initial login portals and cloud-based services access.

Updated Network Topology Diagram:

- The diagram will include the newly added VPN gateways, NAC appliances, and points of MFA integration, demonstrating the comprehensive approach to securing remote access.

Risks & Advantages:

- VPN:
    - Risks: Potential for decreased network performance due to encryption overhead.
    - Advantages: Provides secure remote access, encrypts data in transit, and effectively extends the network perimeter in a controlled manner.
- NAC:
    - Risks: Complex configuration and maintenance.
    - Advantages: Ensures that only compliant and authorized devices can connect to the network, significantly reducing the risk of infected devices compromising the network.
- MFA:
    - Risks: User resistance due to added complexity in the login process.
    - Advantages: Greatly enhances security by mitigating the risk of compromised passwords leading to unauthorized access.
- CASB:
    - Risks: Can be resource-intensive in terms of monitoring and managing cloud access.
    - Advantages: Provides visibility and control over data in the cloud, ensuring compliance and data security across remote access scenarios.

Conclusion:

Implementing these technologies will create a robust hybrid working environment that supports the dynamic needs of faculty and students. It ensures secure and controlled access to network resources from both on-campus and remote locations, while maintaining compliance with security policies and protecting against potential cyber threats. This design not only meets the current needs but is scalable for future expansion and integration with emerging technologies.

This comprehensive plan provides the necessary details to implement a secure and efficient hybrid working environment tailored to the unique requirements of the academic setting, ensuring security, flexibility, and compliance

PART 3:
The college has discovered that students are misusing campus resources and accessing irrelevant sites. They want a solution which will restrict access to only allowed categories of web content.
Tasks & Deliverables:
1. Explore how this can be achieved and what kind of network security product can provide this capability.
2. Update the campus network topology with new component(s)
3. Explain the reasoning behind your choice, detailing the risks & advantages of your proposed solution
4. Write the policies you would apply (can use simple English language commands)

Solution:

Explore Options for Network Security Products

Products and Technologies:

1. Web Content Filtering Solutions:
   - Product Example: Cisco Umbrella
   - Use: Provides DNS-based security by blocking access to websites based on categories, security risks, or specific URLs, ensuring that only approved content is accessible.
2. Firewall with Integrated Security Services:
   - Product Example: Cisco Firepower
   - Use: Offers capabilities such as URL filtering, malware detection, and intrusion prevention, which can be configured to enforce web access policies.

Updating campus network topology

New Components

1. Cisco Umbrella:
   - Placement: Integrated at the DNS layer to filter internet traffic and prevent access to non-approved websites before a connection is even established.

2. Cisco Firepower:
    - Placement: Deployed alongside existing firewalls to enhance security with deep packet inspection and real-time threat intelligence.

Updated Network Topology Diagram:

- The diagram will now include Cisco Umbrella for DNS filtering and Cisco Firepower for enhanced firewall protection, showing their integration points within the existing network infrastructure.

Risks & Advantages:

- Cisco Umbrella:
    - Risks: Overblocking can occur, where legitimate educational sites might be inadvertently blocked if not properly categorized.
    - Advantages: Provides a first line of defense at the DNS layer, which is effective in preventing access to unwanted sites quickly and efficiently.
- Cisco Firepower:
    - Risks: May require significant resources to manage and maintain, especially with frequent updates and policy changes.
    - Advantages: Offers comprehensive network protection that extends beyond URL filtering to include threat detection and response capabilities.

Sample Policies for Web Content Filtering:

1. **Block Access to Non-Educational Entertainment Sites:**
    - `deny access to categories "Entertainment, Gaming, Social Media" during school hours`
2. **Allow Educational and Research-Related Websites:**
    - `allow access to categories "Education, Research" at all times`
3. **Restrict Certain High-Bandwidth Activities:**
    - `deny access to categories "Streaming Media, File Sharing" except during non-school hours`
4. **Custom Rules for Specific Needs:**
    - `allow access to "youtube.com/edu" for educational videos; deny "youtube.com/watch"`
    - `block websites categorized under "Adult Content, Gambling" at all times`

Conclusions :

The deployment of Cisco Umbrella alongside Cisco Firepower will enable the college to effectively manage and monitor web traffic, ensuring that only content relevant to educational and research activities is accessible. This solution not only maximizes network resource utilization but also fosters a safer and more productive educational environment. By implementing these comprehensive content filtering measures, the college can maintain control over its network usage and prevent misuse, aligning technology use with educational goals and policies.

Cloud Security
Problem Statement:
You have been hired as a cloud architect by a start-up. The start-up is an ecommerce retailer which has popular sale days on regional festivals or holidays.
Last year during 15Aug sale, the start-up faced two challenges - the service was unable to handle the huge influx of web requests and the company faced flak and complaints on social media. They also experienced a DDOS attack during this time, which made the situation worse.
You have been asked to propose a revised design to address this problem in preparation for the upcoming sale.
Refer the existing simplified architecture diagram
1. The existing architecture is very basic, aim to improve availability of the system
2. The existing data base is a bottle neck and is prone to corruption, aim to have backup service available within few seconds
3. During flash sale, the service should be able to handle burst traffic, but the large resources will not be needed on regular days. Your design should incorporate this requirement.
4. To mitigate any DDOS attack, aim to add a perimeter layer controlling access to the service to mitigate the attack.

Proposed Revise Design

1. Improve System Availability:

- **Load Balancing:** Implement an elastic load balancer to distribute incoming web traffic evenly across multiple instances. This ensures no single server bears too much load and helps in maintaining high availability and fault tolerance.
- **Auto-Scaling:** Utilize auto-scaling to automatically adjust the number of instances up or down according to the demand. This will be especially useful during flash sales when traffic spikes.

2. Database Scalability and Reliability:

- **Database Clustering:** Use a clustered database environment with a primary and replica setup to ensure high availability. The replica can serve read requests and act as a failover solution.
- **Backup and Recovery:** Implement real-time data replication to a secondary database and regular snapshots to ensure that backups are available and can be restored within a few seconds in case of corruption.

3.Handle Burst Traffic Efficiently:

- **Content Delivery Network (CDN):** Deploy a CDN to cache static content at edge locations closer to the user, significantly reducing load times and server load during high traffic periods.
- **Caching Strategies:** Implement caching mechanisms like Redis or Memcached to serve frequently accessed data quickly without hitting the database repeatedly.

4. DDOS Attack Mitigation:

- **Perimeter Layer:** Introduce a Web Application Firewall (WAF) that can inspect incoming traffic and filter out malicious requests like those commonly found in DDOS attacks.
- **Rate Limiting:** Apply rate limiting to prevent any single source from sending too many requests, which is a common tactic in DDOS attacks.
- **Third-Party DDOS Protection Services:** Consider services like Cloudflare or AWS Shield that provide advanced DDOS mitigation techniques.

Updating Cloud Architecture Diagram :

The new architecture diagram would incorporate the following components:

- **Load Balancer** at the front, distributing incoming traffic across multiple web servers.
- **Auto-Scaling Group** for web servers to scale resources based on traffic load.
- **WAF and DDOS Protection** as the first line of defense against potential threats.
- **Database Cluster** with a primary and replica configuration for high availability.
- **CDN and Caching Layers** to reduce latency and improve the response time during peak traffic.

Explanation and Benefits:

- **Load Balancers and Auto-Scaling:** These ensure that the service can handle variable loads efficiently without downtime or performance bottlenecks.
- **Database Clustering and Backups:** Provide redundancy and quick recovery options, safeguarding data integrity and availability.
- **WAF and DDOS Protection:** Protect against common web threats and help to mitigate the risk of service disruption during DDOS attacks.
- **CDN and Caching:** Reduce the load on the servers and help to manage sudden spikes in traffic more smoothly.

By implementing these strategies, the startup can expect improved resilience, scalability, and security of its e-commerce platform, ensuring a smooth user experience even during high-demand periods. This redesign will address the current challenges and prepare the infrastructure for future growth and potential threats.