MANIPAL INSTITUTE OF TECHNOLOGY

MADHAVA NAGAR MANIPAL UDUPI DISTRICT KARNATAKA
576104, MANIPAL, UDUPI, Karnataka, 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
Siddhant
Saini

AICTE Internship Student Registration ID): STU64dcf3470d20f1692201799

Student ID (Enrolment number): 210962160

Email: siddhantsaini3536@gmail.com, siddhant.saini@learner.manipal.edu

Contact Info: +919559900558

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:

The current network configuration features a systematic setup that includes routers, switches, access points, firewalls, computers, and servers spread throughout various buildings on campus.
Devices Configured:

- **Routers**: Positioned to efficiently manage traffic across networks.
- **Switches**: Enable data flow within network segments.
- **Access Points**: Offer campus-wide wireless connectivity.
- **Firewalls**: Protect the network's boundaries.
- **Computers**: Allocated among faculty and students.
- **Servers**: Support Web, Email, DNS, Database, and Backup services.
- **Connections**: Utilize high-speed Ethernet and wireless protocols to link these devices, ensuring comprehensive network access across campus.

2. Network Mapping Using Cisco Packet Tracer:

I've attached the " Siddhant_Saini_CISCOCyberSecurity" file, showcasing the network mapping of MIT Manipal University using Cisco Packet Tracer.

3. Attack Surface Mapping:

Identification of Vulnerabilities:

- **Open Ports**: Review and evaluate the need for open ports on routers and switches, with

recommendations for closures or enhancements for security.
- **Weak Passwords**: Conduct audits on all devices for weak or default passwords, enforcing a strict password regime.
- **Encryption Gaps**: Assess encryption practices for data both in transit and at rest, suggesting upgrades to more secure protocols as needed.
- **Outdated Firmware**: Inspect for old firmware that could open up security risks and arrange regular updates.

Potential Entry Points for Cyber-Attacks:
- **Wireless Access Points**: Secure all wireless connections with WPA2 or WPA3 encryption to block unauthorized access.
- **Web Servers**: Strengthen and update all servers accessible to the public to reduce the risk of cyber-attacks.
- **Shared Passwords**: Establish policies against sharing passwords and promote the use of individual credentials.
- **Physical Security**: Boost measures to prevent unauthorized physical access to crucial network components.

Proposed Solutions and Countermeasures:
Technological Upgrades:
- **Update and Patch Management**: Set up a centralized system for managing patches to keep all network devices updated with the latest security fixes.
- **Strengthen Password Security**: Implement a stringent password policy requiring complex passwords that include a mix of letters, numbers, and special characters. Add multi-factor authentication (MFA) for all systems, particularly for administrative and remote access.
- **Enhance Network Encryption**: Implement end-to-end encryption using protocols like TLS and SSL for data in transit. Ensure data at rest on servers is encrypted with strong standards.
- **Secure Wireless Networks**: Upgrade all wireless networks to use WPA3 encryption and routinely check and limit the use of outdated wireless equipment.
- **Advanced Intrusion Detection and Prevention Systems (IDPS)**: Introduce sophisticated IDS/IPS that can identify and address both known and new threats. Keep the IDS/IPS updated and monitor network traffic for any unusual activity.
- **Firewall Optimization**: Reassess and reconfigure firewall rules to minimize open ports and effectively segment the network, limiting traffic between essential network parts.

Procedural Enhancements:
- **Regular Security Audits and Penetration Testing**: Plan for annual external security checks and frequent penetration tests to find and fix vulnerabilities early.
- **Security Training and Awareness Programs**: Offer continuous security training for all university personnel and students, emphasizing secure practices, phishing recognition, and secure data handling.
- **Incident Response Planning**: Develop and regularly refine an incident response strategy detailing clear procedures and roles for managing cybersecurity incidents. Run mock cyber-attack drills to ensure team readiness.
- **Physical Security Measures**: Enhance physical security to safeguard network infrastructure from unauthorized access, including advanced surveillance, access control systems, and secured locks for server and data rooms.

Conclusion: Implementing these solutions and countermeasures is vital for protecting our university's network against emerging cyber threats. With digital risks evolving in complexity, proactive security enhancements are crucial. These steps will not only defend academic and personal data but also uphold our institution's integrity and trust.

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:

Assessing Options for Network Security Enhancements:
Products and Technologies:

1. Virtual Private Network (VPN):
    - **Product Example**: Cisco AnyConnect Secure Mobility Client
    - **Purpose**: Facilitates encrypted connections for faculty and students to access the university network remotely, ensuring security through rigorous authentication.
2. Network Access Control (NAC):
    - **Product Example**: Cisco Identity Services Engine (ISE)
    - **Purpose**: Regulates and applies security protocols on all devices trying to connect to the network, permitting only verified devices access to network resources.
3. Multi-Factor Authentication (MFA):
    - **Product Example**: Duo Security
    - **Purpose**: Strengthens security by requiring several verification methods before network access is granted, effectively reducing unauthorized entry risks.
4. Cloud Access Security Broker (CASB):
    - **Product Example**: Cisco Cloudlock
    - **Purpose**: Safeguards data in cloud applications and manages access rights to ensure that only qualified users can access sensitive data.

Upgrades to the Campus Network Architecture:
New Integrations:

1. VPN Gateways:
    - **Location**: Positioned at the network perimeter to securely manage incoming VPN traffic.
2. NAC Implementations:
    - **Location**: Embedded within the network infrastructure to oversee and regulate access at key points.
3. MFA Implementations:
    - **Application**: Deployed across various network access points, encompassing initial login portals and access to cloud-based applications.

Revised Network Topology Diagram:

- The updated diagram will showcase the additions of VPN gateways, NAC systems, and MFA touchpoints, depicting a comprehensive strategy for securing remote access.

Risks and Advantages:

- **VPN**:
  - **Risks**: Potential for reduced network efficiency due to encryption processes.
  - **Advantages**: Offers secure remote connectivity, encrypts data during transmission, and extends the network boundary in a secure manner.
- **NAC**:
  - **Risks**: Requires intricate configuration and continuous upkeep.
  - **Advantages**: Ensures only compliant and authenticated devices access the network, significantly lowering the risk of security breaches.
- **MFA**:
  - **Risks**: May lead to user dissatisfaction due to the complexity of logging in.
  - **Advantages**: Dramatically increases security by lessening the impact of compromised credentials.
- **CASB**:
  - **Risks**: Involves intensive resource allocation for monitoring and managing cloud accesses.
  - **Advantages**: Offers control and visibility over cloud data, ensuring regulatory compliance and security across remote usage scenarios.

Conclusion:
Implementing these sophisticated technologies will cultivate a strong hybrid working environment tailored to meet the dynamic needs of faculty and students. It assures secure and compliant access to network resources, whether on-campus or remotely, upholding security protocols and guarding against potential cyber threats. This strategy not only satisfies current demands but is also scalable for future enhancements and compatibility with emerging technologies.
This detailed plan outlines steps to create a secure and efficient hybrid working model suitable for the academic environment, emphasizing security, flexibility, and regulatory 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:

Exploring Network Security Products and Technologies:

1. **Web Content Filtering Solutions**:
   - **Product Example**: Cisco Umbrella

    - **Functionality**: Utilizes DNS-based security to block access to websites by categories, security risks, or specific URLs, ensuring accessibility to only approved content.
2. **Integrated Security Firewalls**:
    - **Product Example**: Cisco Firepower
    - **Functionality**: Provides features like URL filtering, malware detection, and intrusion prevention, tailored to enforce specific web access policies.

Updating the Campus Network Infrastructure with New Components:

1. **Cisco Umbrella**:
    - **Location**: Implemented at the DNS level to preemptively filter internet traffic, blocking access to unauthorized websites before a connection is established.
2. **Cisco Firepower**:
    - **Location**: Positioned alongside current firewalls, augmenting security with advanced packet inspection and real-time threat intelligence.

Revised Network Topology Diagram:

- The updated diagram will illustrate the integration of Cisco Umbrella for DNS-level filtering and Cisco Firepower for advanced firewall security within the existing network framework.

Risks and Benefits:

- **Cisco Umbrella**:
    - **Risks**: Potential overblocking may lead to unintended restriction of legitimate educational websites if they are misclassified.
    - **Benefits**: Acts as an initial security barrier at the DNS level, effectively and efficiently preventing access to undesirable websites.
- **Cisco Firepower**:
    - **Risks**: Requires substantial resources for management and ongoing updates.
    - **Benefits**: Delivers extensive network protection that goes beyond simple URL filtering to encompass active threat detection and mitigation capabilities.

Guidelines for Web Content Filtering:

1. **Limit Non-Educational Entertainment Sites**:
    - Block access to "Entertainment, Gaming, Social Media" categories during academic hours.
2. **Permit Access to Educational and Research Sites**:
    - Always allow access to "Education, Research" categories.
3. **Control High-Bandwidth Activities**:
    - Restrict access to "Streaming Media, File Sharing" categories to non-academic hours.
4. **Establish Specific Access Rules**:
    - Enable access to educational segments like "youtube.com/edu" while restricting general access like "youtube.com/watch".
    - Continuously block sites under "Adult Content, Gambling" categories.

Conclusion:
Integrating Cisco Umbrella with Cisco Firepower empowers the institution to effectively oversee and regulate web traffic, ensuring only content pertinent to educational and research purposes is accessed. This strategy enhances network resource management, promotes a secure and conducive learning environment, and ensures that network activities align with institutional educational objectives. By applying these sophisticated content filtering strategies, the college can effectively govern its network and prevent misuse, aligning technological practices with educational standards.

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.

1. **Enhancing System Availability:**
    - **Load Balancing:** Introduce an elastic load balancer to distribute web traffic uniformly across various servers, preventing overload on any single server and promoting both high availability and fault tolerance.
    - **Auto-Scaling:** Implement auto-scaling features to dynamically adjust server capacity based on real-time traffic needs, which is critical during peak periods like flash sales.
2. **Database Scalability and Reliability:**
    - **Database Clustering:** Establish a clustered database system with a primary server and replicas to support high availability. The replicas will manage read operations and serve as a backup in case the primary fails.
    - **Backup and Recovery:** Set up continuous data replication to a secondary database and frequent snapshots to guarantee quick restoration and backup availability in the event of data loss.
3. **Efficient Management of Burst Traffic:**
    - **Content Delivery Network (CDN):** Implement a CDN to store static content at edge servers, thereby reducing server load and improving load times during traffic surges.
    - **Caching Strategies:** Utilize caching tools such as Redis or Memcached to quickly deliver frequently requested data, minimizing database queries.
4. **DDOS Attack Mitigation:**
    - **Perimeter Layer Security:** Deploy a Web Application Firewall (WAF) to scrutinize incoming traffic and block malicious requests typical of DDOS attacks.
    - **Rate Limiting:** Enforce rate limiting to restrict excessive requests from a single source, a common method used in DDOS attacks.

    - **Third-Party DDOS Protection Services:** Consider adopting robust DDOS protection services like Cloudflare or AWS Shield that offer advanced mitigation capabilities.

Updating Cloud Architecture Diagram:

The revised architecture diagram will feature:

- **Front-End Load Balancer:** Positioned to evenly distribute traffic across multiple servers.
- **Web Server Auto-Scaling Group:** Configured to automatically adjust based on traffic volume.
- **WAF and DDOS Protection:** Serving as primary security defenses.
- **Database Clustering:** With primary and replica setups for enhanced availability.
- **CDN and Caching Layers:** Optimized to reduce latency and manage load during peak periods.

Explanation and Advantages:

- **Load Balancers and Auto-Scaling:** These components guarantee that traffic fluctuations are managed effectively without service interruptions.
- **Database Clustering and Backups:** They ensure data redundancy and quick recovery, maintaining data security and uptime.
- **WAF and DDOS Protection:** These provide robust security against prevalent online threats and mitigate risks associated with service disruptions during attacks.
- **CDN and Caching:** They lighten server demands and facilitate smoother handling of sudden traffic increases.

By adopting these enhancements, the startup will significantly boost the resilience, scalability, and security of its e-commerce platform, ensuring consistent performance even under high demand. This strategic update is designed to tackle present challenges and equip the infrastructure for anticipated growth and emerging threats.