VALLURUPALLI NAGESWARA RAO VIGNANA JYOTHI INSTITUTE OF ENGINEERING & TECHNOLOGY

UGC Autonomous Institution, Govt. of India
(Affiliated to JNTUH, Approved by AICTE, NBA &NAAC with 'A++' Grade)
Vignana Jyothi Nagar – 500090, Telangana , India
www.vnrvjiet.ac.in

Virtual Summer Internship Program 2023

A Virtual Summer Internship project report on cyber security submitted in partial fulfillment of the requirements for the AICTE-CISCO virtual Internship Program 2023

by

SPURTHIK GURRAM **21071A6657**

Computer Science & Engineering - AIML

CISCO CYBER SECURITY

Report

22-JULY-2023

Project By:

Spurthik Gurram 21071A6657

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.

Tasks:

1. Campus Network Analysis: Choose a university or college campus and conduct an analysis of its existing 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,

considering factors such as unauthorized access, data breaches, and network availability.

4. Secure Access Controls: Incorporate appropriate security controls (e.g., VLANs, IDP/IPS, VPN, Firewalls, password management, vulnerability management etc.) in your design to enhance security posture.

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

Security Assessment Report for University/College Campus Network

1. Campus Network Analysis

The campus network of university was analyzed to understand its existing topology. The network encompasses various departments, administrative offices, student dormitories, and faculty areas. The network topology is primarily based on a centralized design, with core switches connecting to distribution switches, which, in turn, connect to access switches deployed across the campus. The following devices were identified in the network:

Device Name	Device Model
ADMIN	2960-24TT
HR	2960-24TT
FINANCE	2960-24TT
BUSINESS	2960-24TT
E&C	2960-24TT
A&D	2960-24TT
STUDENT LAB	2960-24TT
IT-DEPT	2960-24TT
CLOUD ROUTER	2911
PC0	PC-PT
Printer0	Printer-PT
PC1	PC-PT
PC2	PC-PT
PC3	PC-PT
PC4	PC-PT
PC5	PC-PT
PC6	PC-PT
PC7	PC-PT
Printer1	Printer-PT
Printer2	Printer-PT
Printer3	Printer-PT
Printer4	Printer-PT
Printer5	Printer-PT
Printer6	Printer-PT
WEB SERVER	Server-PT
FTP SERVER	Server-PT
EMAIL SERVER	Server-PT
BRANCH CAMPUS ROUTER	2911
BRANCH CAMPUS SWITCH	3650-24PS
Switch8	2960-24TT
Switch9	2960-24TT
PC8	PC-PT
Printer8	Printer-PT
PC9	PC-PT
Printer9	Printer-PT
MAIN CAMPUS ROUTER	2911
MAIN CAMPUS SWITCH	3650-24PS

2. Network Mapping

Using Cisco Packet Tracer, the campus network infrastructure was mapped to visualize the placement and interconnectivity of network components. The network topology diagram represents the logical and physical connections, including VLANs, subnets, and network segments. It is attached as " Network Topology Diagram."

3. Attack Surface Mapping

An attack surface mapping exercise was conducted to identify potential vulnerabilities and weaknesses within the network architecture. The following security risks were identified:

a. Unauthorized Access

Weak authentication mechanisms in some critical services.

Lack of multi-factor authentication (MFA) for privileged access to network devices.

Unsecured remote access to network devices.

b. Data Breaches

Insufficient encryption of sensitive data in transit.

Limited data segmentation, increasing the risk of lateral movement in case of a breach.

c. Network Availability

Single points of failure in the network design.

Limited redundancy and failover mechanisms.

4. Secure Access Controls

To enhance the security posture of the campus network, the following countermeasures and security controls are proposed:

a. Authentication and Authorization

Implement strong password policies with regular password updates.

Enforce multi-factor authentication (MFA) for all administrative and privileged access to network devices.

Deploy Cisco Identity Services Engine (ISE) for centralized authentication, authorization, and accounting (AAA) services.

b. Data Protection

Ensure end-to-end encryption of sensitive data using protocols like HTTPS and VPNs.

Segment data traffic using Virtual LANs (VLANs) and Access Control Lists (ACLs) to limit lateral movement in case of a breach.

c. Network Availability

Implement redundant links and utilize technologies like Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) to prevent network disruptions due to link failures.

Deploy hot standby or failover systems for critical network components to ensure high availability.

d. Intrusion Detection and Firewalls

Continuously monitor the network using Cisco Firepower 9300 IDS to detect and respond to potential threats in real-time.

Configure firewalls (Cisco ASA 5500-X Series) to control traffic flow and block unauthorized access to critical resources.

e. Vulnerability Management

Establish a routine vulnerability scanning process to identify and address potential weaknesses in network devices and software.

Regularly apply security patches and firmware updates to mitigate known vulnerabilities.

Conclusion:

In conclusion, the security assessment of XYZ University's campus network identified potential security risks and vulnerabilities. By implementing the proposed security controls and countermeasures, the university can significantly enhance its security posture and protect against potential cyber-attacks.

Network topology diagram: