Karunya INSTITUTE OF TECHNOLOGY AND SCIENCES
(Declared as Deemed to be University under Sec.3 of the UGC Act, 1956)
MoE, UGC & AICTE Approved; NAAC Accredited A++
Karunya Nagar, Coimbatore - 641 114, Tamil Nadu, India.

(SIP 2911)
An Internship report submitted by

GODFRAY BUEX- URK22AI1025

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY
in
DATA SCIENCE & CYBER SECURITY
under the supervision of

Mrs. A Bertia
Assistant Professor

DIVISION OF DATA SCIENCE AND CYBER SECURITY
SCHOOL OF COMPUTER SCIENCE AND TECHNOLOGY

July 2024

Karunya INSTITUTE OF TECHNOLOGY AND SCIENCES
(Declared as Deemed to be University under Sec.3 of the UGC Act, 1956)
MoE, UGC & AICTE Approved; NAAC Accredited A++
Karunya Nagar, Coimbatore - 641 114, Tamil Nadu, India.

DIVISION OF DATA SCIENCE AND CYBER SECURITY

BONAFIDE CERTIFICATE

This is to certify that the report entitled, "CISCO VIRTUAL INTERNSHIP " is a bonafide record of Internship (SIP2911) work done at Cybersecurity during the academic year 2023-2024 by

GODFRAY BUEX (URK22AI1025)

in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in **Data Science And Cyber Security** of Karunya Institute of Technology and Sciences.

Guide Signature

A Bertia
Assistant Professor

ACKNOWLEDGEMENT

First and foremost, I praise and thank ALMIGTHY GOD whose blessings have bestowed in me the will power and confidence to carry out my Internship.

I am grateful to our beloved founders **Late. Dr. D.G.S. Dhinakaran, C.A.I.I.B, Ph.D** and **Dr. Paul Dhinakaran, M.B.A, Ph.D**, for their love and always remembering us in their prayers.

We extend Our thanks to **Dr. Dr. Prince Arulraj, Ph.D.,** our honorable Vice Chancellor, **Dr. E. J. James, Ph.D.,** and **Dr. Ridling Margaret Waller, Ph.D.,** our honorable Pro-Vice Chancellor(s) and **Dr. R. Elijah Blessing, Ph.D.,** our respected Registrar for giving me this opportunity to do the internship.

I would like to thank **Dr. Ciza Thomas, Ph.D.,** Dean, School of Engineering and Technology for her direction and invaluable support to complete the same.

I would like to place my heart-felt thanks and gratitude to **Dr. E. Grace Mary Kanaga M.Tech., Ph.D.,** Head of the Division, Data science and cyber security for her encouragement and guidance.

I feel it a pleasure to be indebted to, Ms A Bertia for the invaluable support, advice and encouragement.

I also thank all the staff members of the Division for extending their helping hands to make this in Internship a successful one.

I would also like to thank all my friends and my parents who have prayed and helped me during the Internship.

INTERNSHIP CERTIFICATE

CONTENTS

1.Overview

The Cisco Networking Academy Cybersecurity Internship was an intensive program aimed at providing practical experience in network security and cybersecurity concepts. Over the course of the internship, I applied theoretical knowledge gained from the NetAcad courses to real-world network scenarios using Cisco Packet Tracer. The internship involved analyzing the existing network infrastructure of my college campus, identifying potential vulnerabilities, and designing security improvements.

I worked on tasks that involved network mapping, security risk assessment, and proposing countermeasures to mitigate threats. I gained hands-on experience with tools such as firewalls, VLANs, and web content filtering solutions, which allowed me to implement effective security measures. Additionally, I designed solutions for hybrid work environments, focusing on secure access for faculty and students, both on-campus and remotely.

This internship enhanced my understanding of network architecture, security protocols, and the challenges involved in protecting complex networks from cyber threats. Through the use of Cisco Packet Tracer, I was able to simulate and test various security solutions in a controlled environment, preparing me for future roles in network security and IT management.

2.Objective of the Project

The primary objective of this project was to assess and enhance the security of my college campus network through:

1. Analyzing the current network topology.
2. Identifying security controls in place, including firewalls, VLAN segmentation.
3. Mapping the attack surface and proposing solutions to mitigate potential entry points for cyber-attacks.
4. Implementing a secure hybrid working environment for faculty and students with controlled access to campus resources.

Additionally, the project focused on restricting web access for students to ensure that only relevant educational content was accessible.

2.1 Purpose

- Strengthen cybersecurity awareness.
- Provide solutions for enhancing network security.
- Implement network management best practices using Cisco Packet Tracer.

2.2 Technical Exposure Gained

- Network mapping using Cisco Packet Tracer.
- Experience with VLANs, firewalls, and access control systems.
- Implementation of web content filtering policies.

3.System Design

1.Network Architecture

- Follows a hierarchical design model with three main layers:
  - Core Layer: Provides high-performance routing and resilient connectivity between sites.
  - Distribution Layer: Implements policy-based connectivity and boundary control.
  - Access Layer: Provides user/workgroup access to the network.
- Utilizes a modular design approach for scalability and easier management.
- Supports both three-tier (Core, Distribution, Access) and two-tier (Combined Core/Distribution, Access) models based on the network size.

2.Security and Firewall Configuration

- Cisco ASA 5505 firewalls are deployed at both the main and branch campuses.
- Firewalls are configured to segment the network into Inside, Outside, and DMZ zones.
- Site-to-site IPsec VPN is set up between the main and branch campus firewalls.
- Wireless security is implemented using WPA2-Enterprise with RADIUS authentication.

3.Server and Service Configuration

- Two physical servers host virtualized Active Directory and DHCP services, placed in the DMZ for security.

4.Network Services and Features

- VLANs are configured for management, LAN, WLAN, and unused ports (blackhole).
- Inter-VLAN routing is implemented using SVI or Router-on-a-Stick.
- QoS policies are configured to manage and prioritize network traffic.

5.Modularity and Scalability

- Modular design approach is used to create scalable and manageable network blocks.
- Redundant links, hot standby protocols, and robust routing configurations ensure high availability and resiliency.

6.Documentation and Testing

- Comprehensive network documentation is created, including diagrams and IP/VLAN details.
- Thorough testing is conducted to verify connectivity, VPN functionality, and security measures.

4. Implementation of the Project

1. Set up the Main Campus Network:
   - Configured the Airtel ISP Router.
   - Installed and set up the Cisco ASA 5505 firewall.
   - Deployed two Catalyst 3850 core switches and configured VLANs.
   - Installed multiple Catalyst 2960 distribution switches for different faculties.
   - Set up two physical servers for virtualization in the DMZ.
   - Configured virtual machines for Active Directory and DHCP.
   - Installed the Cisco Wireless LAN Controller and Lightweight Access Points.

2. Replicated the Setup for the Branch Campus:
   - Repeated the same steps as the main campus for the branch network.

3. Configured the Site-to-Site VPN:
   - Set up IPsec VPN between the main and branch campus ASA firewalls.

4. Implemented Security Configurations:
   - Configured firewall rules on the ASA firewalls.
   - Implemented WPA2-Enterprise on the wireless network.
   - Ensured proper VLAN segregation and access controls.

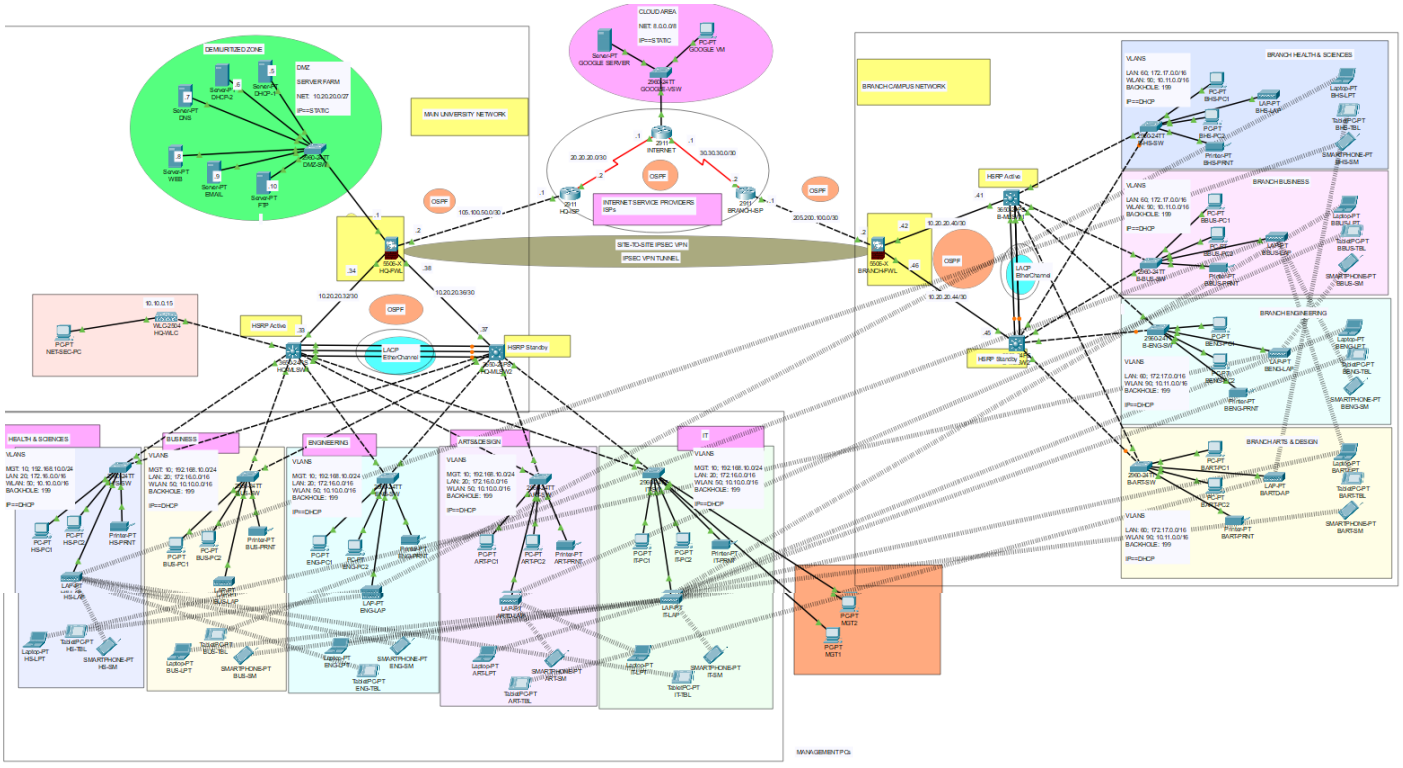
5. Configured Core Services:
   - Set up Active Directory on one of the virtual servers.
   - Configured DHCP service on another virtual server.

6. Conducted Testing and Verification:
   - Verified connectivity between network segments.
   - Tested the site-to-site VPN.
   - Performed security tests on firewall rules and wireless security.

7. Documented the Network:
   - Created a detailed network diagram.
   - Documented IP addresses, VLAN assignments, and security policies.

SCREENSHOTS OF THE IMPLEMENTATIONS

OUTPUT SCREENSHOTS:



5.Key Learning Experiences

Collaboration and Communication

This virtual internship allowed me to collaborate with peers and mentors fromacross different geographic locations, enhancing my ability to communicate technical concepts effectively.

Time Management

Managing my time effectively was crucial in meeting project deadlines while balancing learning and implementation tasks. The structured approach of the internship helped me improve my project planning skills.

Application of Cybersecurity Knowledge

The internship enabled me to put the cybersecurity theories I had learned into practice, particularly in the areas of network defense mechanisms, intrusion prevention systems, and secure remote access solutions.

6..Summary

The Cisco Networking Academy Cybersecurity Internship provided me with a valuable opportunity to work with real-world network architectures and hone myskills in cybersecurity. I gained hands-on experience with network simulation tools, learned to identify and mitigate security risks, and designed solutions to meet the needs of both campus and hybrid working environments. This experience has significantly contributed to my understanding of how to secure modern networks from cyber threats.