Appendix 4A

UNIVERSITI TEKNOLOGI MALAYSIA

FACULTY OF COMPUTING

INDUSTRIAL TRAINING REPORT

VULNERABILITY ASSESSMENT AND DNS
APPLICATION SYSTEM

BY

NOR FARAHZIBA BINTI HAMADUN

2022

COMPUTER SCIENCE (COMPUTER NETWORKS & SECURITY)

TRAINING PLACE :	PUSAT KOMPUTERAN DAN INFORMATIK, UNIVERSITI MALAYSIA KELANTAN, 16300 BACHOK KELANTAN
TRAINING PERIOD :	5 MONTHS
SUPERVISORS :	EN MOHD FADLI BIN MOHD ZAIN
REPORT DATE :	FEBRUARY 2023

ABSTRACT

Industrial training is a vital component of the Bachelor of Computer Science (Computer Networks & Security) program because it prepares interns for the industrial environment before they graduate. Adaptation is essential since academic knowledge alone cannot completely prepare the student to enter the cybersecurity industry. This report will cover the details of the 20-week industrial training at the Centre for Computing & Informatics (CCI), Universiti Malaysia Kelantan (UMK). The organization supervisor of this industrial training is Mr. Mohd Fadli Bin Mohd Zain, the head of the Data Center and ICT Security section of the Centre for Computing & Informatics (CCI), Universiti Malaysia Kelantan (UMK). Meantime, Dr. Noorfa Haszlinna Binti Mustaffa, a lecturer in the School of Computing, Universiti Teknologi Malaysia, is the faculty supervisor. Numerous tasks relating to cybersecurity were given throughout the industrial training. The main goal of this internship program is to create an effective network security solution that helps organizations in lowering the risk of data theft and sabotage through staff education and testing of two different security tools: Network Detection and Response (NDR) and Vulnerability Assessment (VA). The next goal is to develop a DNS application system that allows staff to fill out a form to request a new Domain Name System (DNS). The system was built using ColdFusion Markup Language (CFML). This report will explain the process and the technologies and tools that were used to complete the assigned tasks. Besides, this report will also outline the skills developed during this industrial training. Finally, this report will sum up the overall achievements and opinions of this industrial training.

ABSTRAK

Latihan industri adalah komponen penting dalam program Sarjana Muda Sains Komputer (Rangkaian Komputer & Keselamatan) kerana ia melatih pelajar untuk menyesuaikan diri di persekitaran industri sebelum mereka menamatkan pengajian. Penyesuaian adalah penting kerana pengetahuan akademik sahaja tidak dapat menyediakan pelajar sepenuhnya untuk memasuki industri keselamatan siber. Laporan ini akan merangkumi butiran latihan industri selama 20 minggu di Pusat Komputeran & Informatik (CCI), Universiti Malaysia Kelantan (UMK). Penyelia organisasi latihan industri ini ialah En Mohd Fadli Bin Mohd Zain, ketua bahagian Pusat Data dan Keselamatan ICT di Pusat Komputeran & Informatik (CCI), Universiti Malaysia Kelantan (UMK). Sementara itu, Dr Noorfa Haszlinna Binti Mustaffa, pensyarah di Pusat Pengajian Pengkomputeran, Universiti Teknologi Malaysia, merupakan penyelia fakulti. Banyak tugas yang berkaitan dengan keselamatan siber telah diberikan sepanjang latihan industri. Matlamat utama program latihan ini adalah untuk mencipta penyelesaian keselamatan rangkaian yang berkesan yang dapat membantu organisasi dalam mengurangkan risiko kecurian data dan sabotaj melalui pendidikan kakitangan dan ujian dua alat keselamatan yang berbeza: Pengesanan dan Respons Rangkaian (NDR) dan penilaian kelemahan. Matlamat seterusnya adalah untuk membangunkan sistem aplikasi DNS yang membolehkan kakitangan mengisi borang untuk meminta Sistem Nama Domain (DNS) baharu. Sistem ini dibina menggunakan ColdFusion Markup Language (CFML). Laporan ini akan menerangkan proses dan teknologi serta alatan yang digunakan untuk menyelesaikan tugasan yang diberikan. Selain itu, laporan ini juga akan menggariskan kemahiran yang dibangunkan semasa latihan industri ini. Akhir sekali, laporan ini akan merumuskan keseluruhan pencapaian dan pendapat mengenai latihan industri ini.

ACKNOWLEDGEMENT

First of all, I would like to sincerely thank my faculty supervisor, Dr. Noorfa Haszlinna Binti Mustaffa, for helping me during this industrial training period, which starts from 2 October 2022 until 16 February 2023. Without her supervision and advice, the uncertainties and issues concerning industrial training would remain unresolved.

Next, I also would like to express my gratitude to Mr. Mohd Fadli Bin Mohd Zain, the head of the Data Center and ICT Security section of the Centre for Computing & Informatics (CCI), Universiti Malaysia Kelantan (UMK), for accepting me as an intern under him. He is very generous in sharing his knowledge of technology, network security, and company operation. After that, I also like to use this chance to thank the other staff and interns who taught me about technology and other aspects of life.

Finally, I want to thank my parents and family members for their spiritual and financial support throughout my internship. They constantly encourage me when I run into difficulties and motivate me to keep going till I complete my internship.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

VA	-	Vulnerability Assessment
SCC	-	Sangfor's Cyber Command
NDR	-	Network Detection and response
DNS	-	Domain Name System
UMK	-	Universiti Malaysia Kelantan
CCI	-	Center For Computing & Informatic
ICT	-	Information and Communication Technology
CFML	-	ColdFusion Markup Language
VPR	-	Vulnerability Priority Rating
MD5	-	Message Digest Method 5
SIEM	-	Security Information And Event Management

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Company Background

The Centre for Computing & Informatics (CCI) or also known as “Pusat Komputeran Dan Informatik” was established in early 2007 and was formerly known as the Department of Infra & ICT. It is a center in charge of not only ICT but also development, maintenance, and electrical, mechanical, and public services (Universiti Malaysia Kelantan, 2022).

The Department of Infrastructure and Information Technology (Infra & ICT) split into the Department of Information & Communication Technology (JTMK) and the Department of Development, Infrastructure, and Services (JPIP) in 2009. Infra & ICT focuses on ICT, while JPIP handles the development, maintenance, and engineering services for electrical, mechanical, civil, architectural, and material surveying.

In the final year of 2011, the design process proceeded with the restructure that transformed the Department of Information & Communication Technology (JTMK) into the Information Technology Centre (PTM). Finally, in 2016, renewal was implemented by making the Information Technology Center (PTM) become the Centre for Computing and Informatics (CCI).

1.1.1 Number of staff

CCI employs approximately 50 employees in total, including normal staffs and two web administrators.

1.1.2 Vision

To grow into an institution that develops specialties, curricula, research, and quality ICT infrastructure and service providers as a Teaching Knowledge Factory to face the rapidly changing and challenging environment in the industry market and to assist the national policy in order to grow workforces' knowledge on entrepreneurial education through the use of the technology-based learning concept (Universiti Malaysia Kelantan, 2022).

1.1.3 Mission

The CCI had four missions, which are listed below:

- To offer services and build out ICT infrastructure in pace with the advancement of ICT worldwide.
- Provide academic and professional ICT programs focused on entrepreneurship that appeals to the industry market.
- To provide academic and professional ICT expert services that are beneficial at every level, faculty, and university.
- To lead strategic plan and ICT innovation research towards the university's strategic growth.

1.1.4 Objective

The CCI organization's objectives are described below:

i. Curriculum development management for ICT – ICT knowledge discovery, development, learning, and teaching through study, experimentation, and consultation. Develop programs and prepare course modules of study

ii. ICT-based management of research and innovation – Manage postgraduate research, studies, administrative tasks, consultations, etc. Manage the governance of research activities while implementing continuous education and enhanced innovation and commercialization efforts.

iii. Policy management – ICT audit and security management, project management, and administration.

iv. Operational management – Network and communication, IICT infrastructure and technician services. Manage the main application system of the university.

1.1.5 Services

The following summarizes the CCI organization's services:

i. Communication Network

a. WIFI UMK – One of the ICT services offered for UMK students and staff to help with internet access is UMK WiFi.

b. VPN IP – The CCI has set up Internet Protocol Virtual Private Network (IPVPN) capabilities to link information technology services between UMK campuses for a completely secure network.

c. Internet Access – CCI uses Dedicated Internet Access (DIA). This service has enhanced security and doesn't interrupt access. Additionally, it enables high-speed simultaneous download and uploads traffic without reducing the performance of the internet network.

d. Network MYREN – MYREN is a network that links all public universities and polytechnics and provides high-speed connections for academics, researchers, and scientists throughout the nation. Also, MYREN links up with Malaysia Internet Exchange (MyIX) and TEIN3.

e. Teleconference – CCI provides tele video conferencing (VC) facilities to help lecturers, researchers, and administrative staff communicates and collaborate audio/visually in real-time.

f. Telephone Facilities – CCI provides and manages Telephone infrastructure facilities and ensures that it is secure, reliable, and robust for UMK residents.

ii. Website Development

a. Website Hosting – Users can utilize CCI's web hosting services for conferences, clubs, or other activities. To enable users to fully customize and configure servers and applications, CCI now offers dedicated servers. To make the task of informing the public easier, it is strongly advised that each department at Universiti Malaysia Kelantan (UMK) establish a department or faculty portal.

b. Website development – Website services offered by CCI Computer & Informatics Center include domain name or URL registration, consulting and advisory services on architecture, content organization, and website setting.

iii. Application Development – The CCI is also engaged in developing systems like the E-Community Portal, Student Financial System, Human Resource Management System (HRIS), and Student Information System (SIS) to further enhance governance operations at UMK. To guarantee that they always operate at their best, these designed systems are also managed and closely watched. Besides, system adjustments are constantly performed in response to demand.

iv. ICT Security – To protect the interests of the University, CCI takes this issue seriously and always makes sure that strict ICT security requirements are followed. To maintain the highest and most updated level of UMK security, CCI always employs high-quality tools and technology.

1.2 Organization Structure

The CCI's current organizational structure is displayed in Figure 1.1 below. It is divided into three departments: the Department of Information Infostructure, the Department of Administration and Finance, and the Department of Infrastructure (Universiti Malaysia Kelantan, 2022). I had been assigned to the Department of Infrastructure in the Data Center and ICT Security Section.

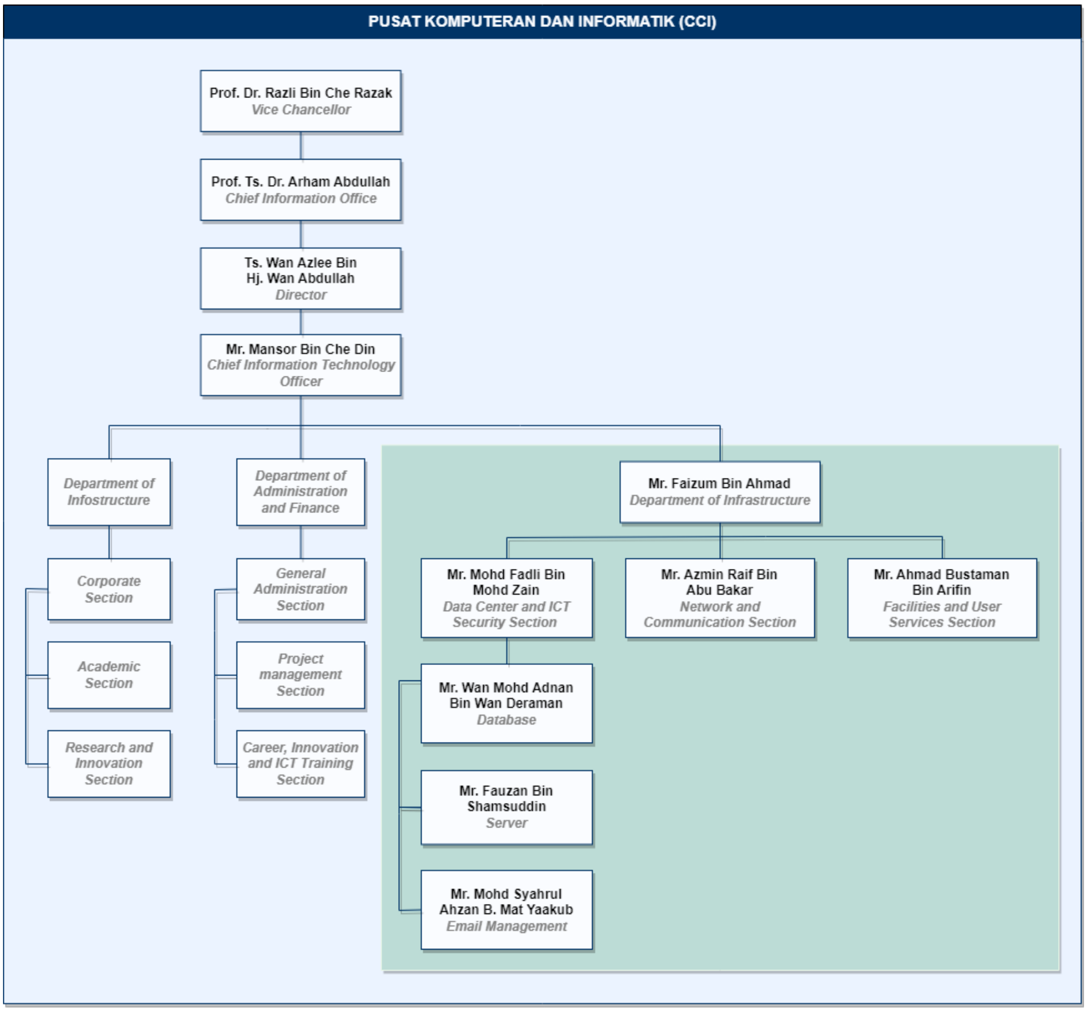

PUSAT KOMPUTERAN DAN INFORMATIK (CCI)
Prof. Dr. Razli Bin Che Razak
Vice Chancellor
Prof. Ts. Dr. Arham Abdullah
Chief Information Office
Ts. Wan Azlee Bin Hj. Wan Abdullah
Director
Mr. Mansor Bin Che Din
Chief Information Technology Officer
Department of Infostructure
Department of Administration and Finance
Mr. Faizum Bin Ahmad
Department of Infrastructure
Corporate Section
Academic Section
Research and Innovation Section
General Administration Section
Project management Section
Career, Innovation and ICT Training Section
Mr. Mohd Fadli Bin Mohd Zain
Data Center and ICT Security Section
Mr. Azmin Raif Bin Abu Bakar
Network and Communication Section
Mr. Ahmad Bustaman Bin Arifin
Facilities and User Services Section
Mr. Wan Mohd Adnan Bin Wan Deraman
Database
Mr. Fauzan Bin Shamsuddin
Server
Mr. Mohd Syahrul Ahzan B. Mat Yaakub
Email Management

Figure 1.1 CCI's organizational structure

1.2.1 Data Center and ICT Security Section

There are three parts within the Data Center and ICT Security section. Management of databases, servers, and emails. The UMK databases would need to be created and maintained by the database manager. He would design data storage and retrieval systems, address database problems, and put safety measures and recovery mechanisms in place.

The server manager are also responsible for a variety of technical jobs on the computer network systems at UMK. The UMK's servers and networks are set up and maintained by him. He connects workstations to the UMK network and checks it for potential problems. He also monitors server activities and audits the security of the server. Last but not least, the one in charge of managing all emails in UMK. He can create, delete, recover, and limit the amount of files that can be stored in Google Drive. He uses Google Admin to generate staff and student email. Users who never logged into their accounts for more than three years will be terminated because Google has a storage limit. By freeing up Google Drive space, UMK can ensure that every new student has an account.

Anyway, my supervisor Mohd Fadli Bin Mohd Zain was the head of the Data Center and ICT Security section. Following are the details of the supervisor.

- Name: Mr. Mohd Fadli Bin Mohd Zain
- Position: Senior Information Technology Officer
- Tel/Ext No: 09-7717170
- Email: fadli@umk.edu.my

1.3 Training Program

On the first day, report duty was performed, as well as a conversation with the supervisor about the scope project and tasks allocated for the five-month industrial training. The following day's job is to collect data on Network Detection and Response

(NDR) and Security Information and Event Management (SIEM). It had taken two days to complete. The supervisor then introduces Cyber Command Sangfor on 5th October 2022, and requests an investigation about its capabilities. Linux training must be attended for two days during the second week of October. The next assignment is to handle the UMK account between October 11th and 13th October 2022. Then, during the third week of October, Lucee would be installed and configured. A basic webpage must be developed using the Lucee and CFM languages. The timeframe is ten days.

There will be a Tenable.io training on 30th October 2022, and it has to be evaluated the following day. A FlowMon training would be held during the second week of November. It must then be examined the next day. The remaining days of November would be spent doing research on XDR. Following then, penetration testing would be done for about a month. On 25 December 2022, cybersecurity information must be gathered to create 25 cybersecurity guidelines that must be completed by 1st January 2023. Following that, 25 posters must be designed in accordance with the guidelines. The industrial training presentation must be prepared starting on 30th January 2023. For a detailed look at the industrial training program, please view Appendix A.

1.4 Conclusion

This chapter gave an overview of the history, purpose, vision, and services of CCI. The chapter also includes information about CCI's organizational structure and the section where the training was performed. In addition, a Gantt chart was provided to show the entire training schedule for the five months of industrial training.

CHAPTER 2

SPECIFIC DETAILS ON PROJECTS/TRAINING

2.1 Introduction

This chapter will provide additional detail on the tasks and training given during industrial training. The main tasks includes Vulnerability Assessment (VA), DNS application system, cybersecurity guidelines, Network Detection and Response (NDR). A Vulnerability Assessment is one approach to evaluating the overall security of an organization's systems since it identifies where technological weaknesses exist and how to resolve them (imperva, 2019). Meanwhile, NDR is a type of network security tool that uses purposely built sensors to monitor and analyze all network traffic, including east-west and north-south traffic. NDR automatically responds to threats or warns security operators for additional investigation when abnormal traffic patterns are found (Technologies, 2022). Next, a few posters describing cybersecurity best practices need to be prepared.

2.2 Objectives of the Project

The main objectives of this project are:

i. To find vulnerabilities in the systems.
ii. To develop a custom cybersecurity defence plan.
iii. To education staffs the importance of cybersecurity awareness.
iv. To develop a secure DNS application system.
v. To simplify the process of requesting new DNS.

2.3 Main Task Assigned

Network security is currently lacking at UMK Bachok. When the organization connects to the internet, it may get a large amount of traffic. This massive traffic can disrupt system stability and expose its vulnerabilities. However, network security can increase network stability by preventing lagging and downtimes by continuously monitoring any suspicious transactions that might undermine the system. Furthermore, a good network security solution helps organizations reduce the risk of data theft and sabotage. As a solution, the Data Center and ICT Security Section decided to experiment with two types of security tools: Network Detection and Respond (NDR) and Vulnerability Assessment (VA), to improve network security at UMK Bachok. Next, an education on cybersecurity is also necessary to safeguard users from cyberattacks. In addition, the process for requesting a new DNS also needs to be improved to make it easier for staff to apply.

2.3.1 VA- Tenable.io

Tenable.io is used by the organization to conduct vulnerability assessments. Tenable.io is an essential part of the Tenable Cyber Exposure Platform. It gives organizations useful insight into the security risks associated with their entire infrastructure, enabling them to quickly and precisely detect, examine, and prioritize vulnerabilities and misconfigurations in the modern IT environment (Tenable®, 2017).

2.3.1.1 Tenable.io Overview

Tenable.io allows users to check their organization's environment for vulnerabilities. Because tenable.io is hosted in the cloud, users can scan remotely using their Nessus scanners and Nessus Agent. Furthermore, the user can use the Tenable.io scanner to scan assets from an external network. Besides that, Tenable.io offers a variety of Nessus Scanner and Nessus Agent scan templates to meet a variety of business requirements. Traditional active scan is performed using the Nessus scanner. To conduct a scan, it need to reach out to the target hosts. Meanwhile, Nessus agent scans run on hosts independent of network location or connection, and the results are sent back to the manager when network connectivity is restored. The organization may not need to apply the agents if the Nessus scanner is suitable for the organizational environment and requirements. However, Tenable.io suggests a combination of agents and traditional scanning for most organizations to ensure comprehensive visibility across the entire network.

Vulnerability Scans, Configuration Scans, Tactical Scans, and Inventory collections are the four categories of the scan template. It is advised to apply a vulnerability scan template for the organization's regular, daily scanning needs. There are four main vulnerability scan templates. The first template is called Advanced Network/Agent Scan. It is the most configurable scan type provided by Tenable.io. This scan template is adaptable to any policy. The following is a Basic Network/Agent Scan. With all of Tenable.io's active plugins turned on, it is used to scan assets. This scan offers a quick and simple method for scanning all assets for vulnerabilities. The third template is Credentialed Patch Audit (Nessus Scanner only). It is used to grant the scanner direct access to the host, scan the target hosts, and identify missing patch updates. The fourth option is Host Discovery (Nessus Scanner only). This scan is launched to see what hosts are present on the network, and relevant information such as IP address, operating systems, and open ports, if available. Once a list of hosts is obtained, any host could be selected to be the target of a particular vulnerability scan.

Next, the configuration scan is used to check if host settings match different industry standards. Configuration scans are also known as compliance scans. Tactical scans, on the other hand, are lightweight, timely scan templates that can be used to scan assets for a specific vulnerability. Tenable regularly adds templates that identify the most recent vulnerabilities of public interest to the Tenable.io Tactical Scans library. Last but not least, the Collect Inventory template uses Tenable's Frictionless Assessment technology, which speeds up scan results and minimizes the scan's system footprint, in contrast to standard Nessus Agent vulnerability scans.

2.3.1.2 Objective of the VA project

The process of defining, identifying, categorizing, and prioritizing vulnerabilities in computer systems, applications, and network infrastructures is known as a vulnerability assessment (Rosencrance, 2021). It involves using automated testing tools, including network security scanners, the outcomes of that are listed in a vulnerability assessment report. Furthermore, it gives an organization the information, awareness, and risk background needed to recognize and respond to threats. Since, security vulnerabilities can allow hackers to access IT apps and systems, organizations must find and fix the flaw before hackers can exploit them. Considering the potential of the VA, CCI decided to participate in the VA training and experiment with Tenable.io to improve UMK security. The objective of the VA project is outlined below.

i. To check the reliability of tracking vulnerabilities based on assets.
ii. To see how fast vulnerabilities were found throughout the scanning process.
iii. To prioritize vulnerabilities and risks
iv. To apply the necessary security updates
v. To avoid vulnerabilities from being exploited before a fix has been made.
vi. To take action to mitigate, prevent, transfer, or accept the risk
vii. To verify whether the suggested solution for the vulnerability works.
viii. To automate manual processes and provides continuous monitoring, alerting, and remediation solutions

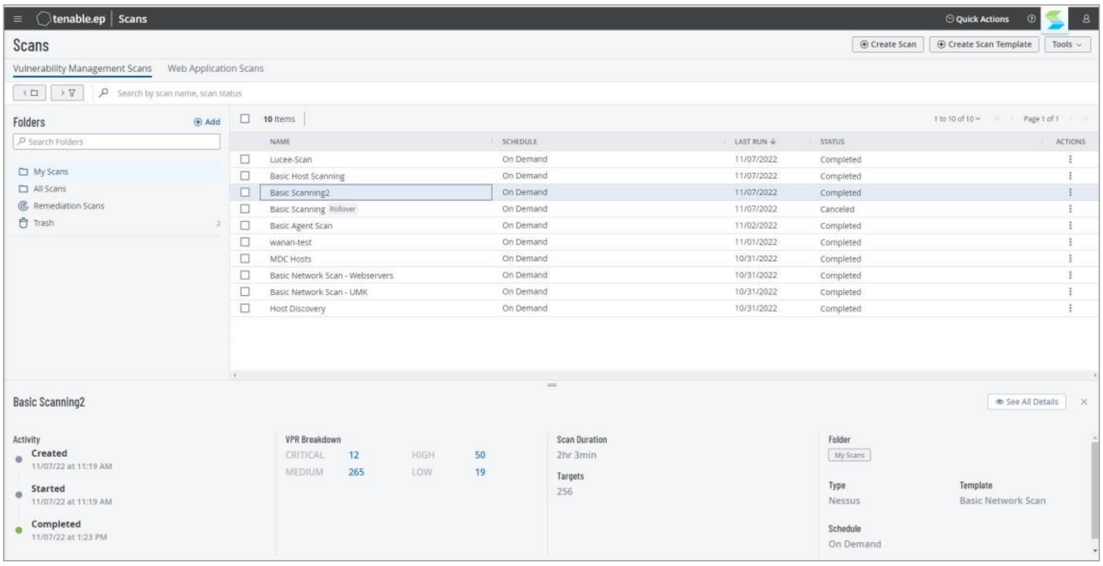
2.3.1.3 Type of Work Done

Vulnerability assessment is achieved through four security scanning processes: vulnerability identification, vulnerability analysis, risk assessment, and remediation.

2.3.1.3.1 Vulnerability Identification

Vulnerability identification is the process of identifying and compiling a detailed list of vulnerabilities in the IT infrastructure. Often, this is accomplished through vulnerability scanning (imperva, 2019).

The vulnerability scanning begins by running a basic network scan on the UMK server to identify the server's risk on the vulnerability priority rating (VPR) breakdown tab as shown in Figure 2.1. The scanning was then scheduled at midnight to compare the VPR breakdown during the regular hour and midnight. However, the VPR breakdown shows the same result for both scans. Figure 2.2 show the scheduled basic network scanning.



	NAME	SCHEDULE	LAST RUN	STATUS	ACTIONS
□	Lucee-Scan	On Demand	11/07/2022	Completed	⋮
□	Basic Host Scanning	On Demand	11/07/2022	Completed	⋮
□	Basic Scanning2	On Demand	11/07/2022	Completed	⋮
□	Basic Scanning Rollover	On Demand	11/07/2022	Canceled	⋮
□	Basic Agent Scan	On Demand	11/02/2022	Completed	⋮
□	wanan-test	On Demand	11/01/2022	Completed	⋮
□	MDC Hosts	On Demand	10/31/2022	Completed	⋮
□	Basic Network Scan - Webservers	On Demand	10/31/2022	Completed	⋮
□	Basic Network Scan - UMK	On Demand	10/31/2022	Completed	⋮
□	Host Discovery	On Demand	10/31/2022	Completed	⋮

Basic Scanning2

Activity

Created 11/07/22 at 11:19 AM

Started 11/07/22 at 11:19 AM

Completed 11/07/22 at 1:23 PM

VPR Breakdown

CRITICAL	12	HIGH	50
MEDIUM	265	LOW	19

Scan Duration: 2hr 3min

Targets: 256

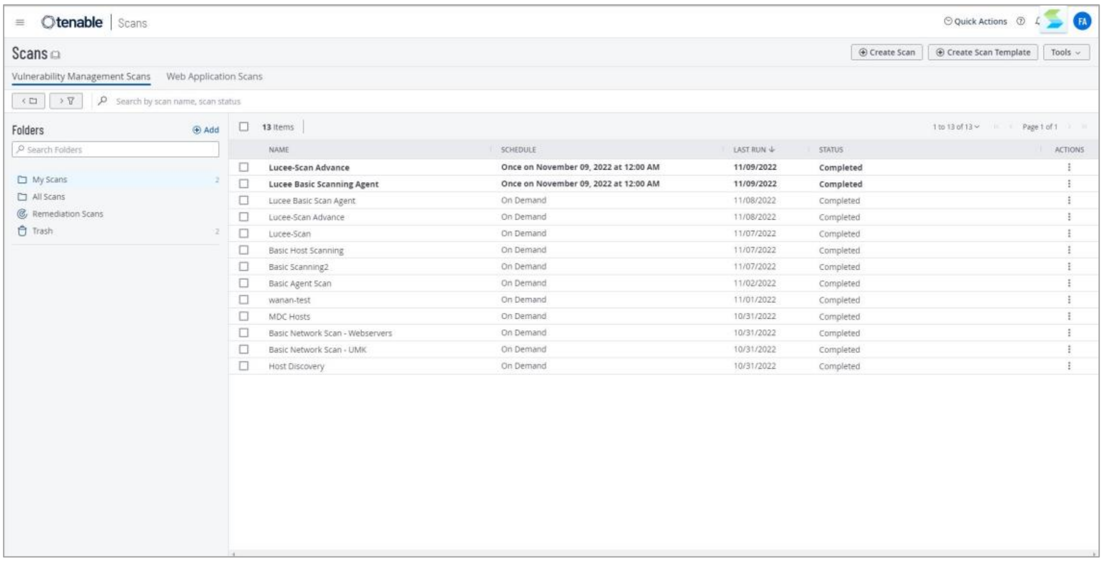
Folder: My Scans

Type: Nessus

Template: Basic Network Scan

Schedule: On Demand

Figure 2.1 The basic network scan on the UMK server



NAME	SCHEDULE	LAST RUN	STATUS	ACTIONS
Lucee-Scan Advance	**Once on November 09, 2022 at 12:00 AM**	**11/09/2022**	**Completed**	⋮
Lucee Basic Scanning Agent	**Once on November 09, 2022 at 12:00 AM**	**11/09/2022**	**Completed**	⋮
Lucee Basic Scan Agent	On Demand	11/08/2022	Completed	⋮
Lucee-Scan Advance	On Demand	11/08/2022	Completed	⋮
Lucee-Scan	On Demand	11/07/2022	Completed	⋮
Basic Host Scanning	On Demand	11/07/2022	Completed	⋮
Basic Scanning2	On Demand	11/07/2022	Completed	⋮
Basic Agent Scan	On Demand	11/02/2022	Completed	⋮
wanan-test	On Demand	11/01/2022	Completed	⋮
MDC Hosts	On Demand	10/31/2022	Completed	⋮
Basic Network Scan - Webservers	On Demand	10/31/2022	Completed	⋮
Basic Network Scan - UMK	On Demand	10/31/2022	Completed	⋮
Host Discovery	On Demand	10/31/2022	Completed	⋮

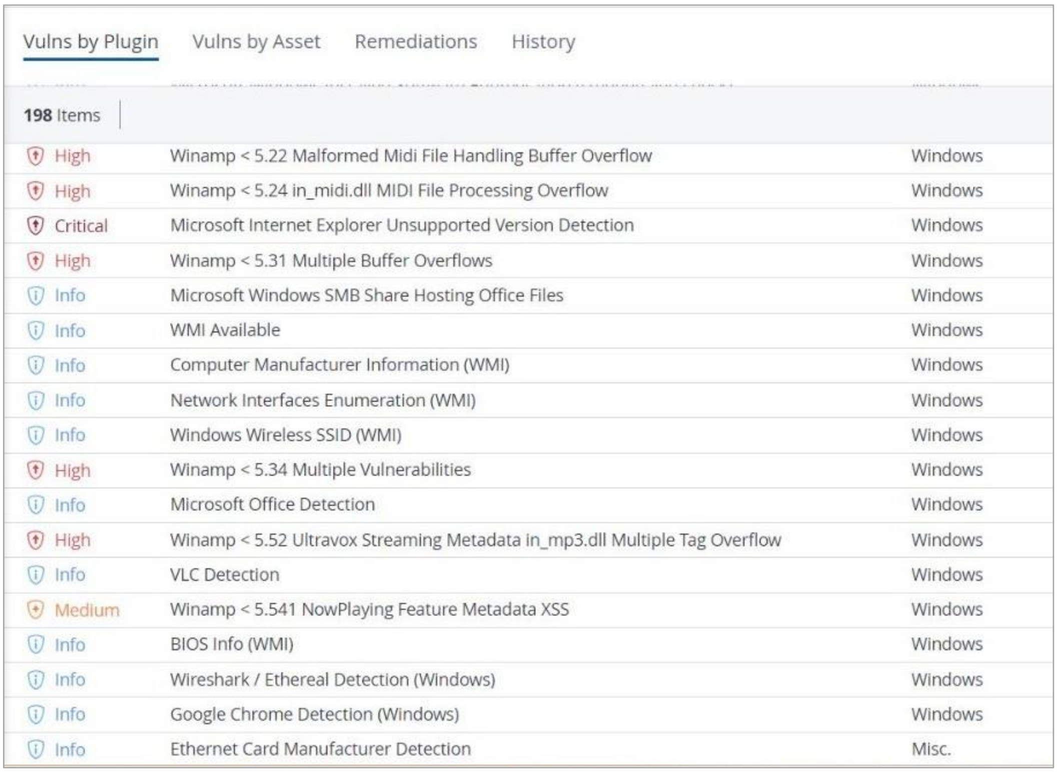
Figure 2.2 The scheduled basic network scanning

After that, a basic agent scanning on my computer was performed to view the computer VPR breakdown. The agent scanning required me to install Nessus Agent on my computer and link it to Tenable.io. The installation process starts with downloading the package for the user's operating system from the Nessus Agents Download Page. When the download is finished, complete the setup process. Then, in the configuration window, enter the key value and server value for the agent that was retrieved from Tenable.io.

Navigate to Settings in Tenable.io to verify that the agent has been successfully linked to the computer. Choose the sensor tile, then Nessus Agents. The Nessus Agent page loads, and the Linked Agent tab is active. The agent linking is successful if the new agent (computer name) is listed in the linked agent table. Before performing the basic agent scan, the "Agent Group" must be added. Enter the new agent group's name in the agent group setting and set the user permissions. By selecting Save, the new agent group appears in the table. The agent group is necessary for the agent scan configuration. The basic agent scan is used to identify endpoint (the computer) vulnerabilities.

2.3.1.3.2 Vulnerability Analysis

After vulnerabilities are identified, a vulnerability analysis was carried out. Finding the root of each vulnerability is the goal of the analysis process. To figure out the root cause, the infrastructure components responsible for each vulnerability must be validated and investigated further. This process of analysis also looks for improperly updated or installed systems. Fortunately, Tenable.io can aid with this process by identifying potential system flaws, risky hardware, and risky software. By clicking "See All Details" on the scanning result of the Tenable.io page, users can view the list of vulnerabilities. It also reveals the true cause of each vulnerability. Besides, due to the widespread reporting of vulnerabilities, vulnerability identification, and root cause analysis are extremely quick. Figure 2.3 displays the vulnerability analysis and risk assessment done by Tenable.io.



High	Winamp < 5.22 Malformed Midi File Handling Buffer Overflow	Windows
High	Winamp < 5.24 in_midi.dll MIDI File Processing Overflow	Windows
Critical	Microsoft Internet Explorer Unsupported Version Detection	Windows
High	Winamp < 5.31 Multiple Buffer Overflows	Windows
Info	Microsoft Windows SMB Share Hosting Office Files	Windows
Info	WMI Available	Windows
Info	Computer Manufacturer Information (WMI)	Windows
Info	Network Interfaces Enumeration (WMI)	Windows
Info	Windows Wireless SSID (WMI)	Windows
High	Winamp < 5.34 Multiple Vulnerabilities	Windows
Info	Microsoft Office Detection	Windows
High	Winamp < 5.52 Ultravox Streaming Metadata in_mp3.dll Multiple Tag Overflow	Windows
Info	VLC Detection	Windows
Medium	Winamp < 5.541 NowPlaying Feature Metadata XSS	Windows
Info	BIOS Info (WMI)	Windows
Info	Wireshark / Ethereal Detection (Windows)	Windows
Info	Google Chrome Detection (Windows)	Windows
Info	Ethernet Card Manufacturer Detection	Misc.

Figure 2.3 Vulnerability analysis and risk assessment by Tenable.io

2.3.1.3.3 Risk Assessment

After the organization's vulnerability have identified and analyzed, it’s time to conduct a risk assessment and determine prioritization. During a risk assessment, security analysts assign each vulnerability a severity score, and higher numbers indicate weaknesses that should be addressed as soon as possible. Vulnerabilities are ranked based on a variety of factors, including:

i. Which systems are affected?
ii. What data is at risk?
iii. Which business functions are at risk?
iv. Ease of attack or compromise.
v. The severity of an attack.
vi. Potential damage as a result of the vulnerability.

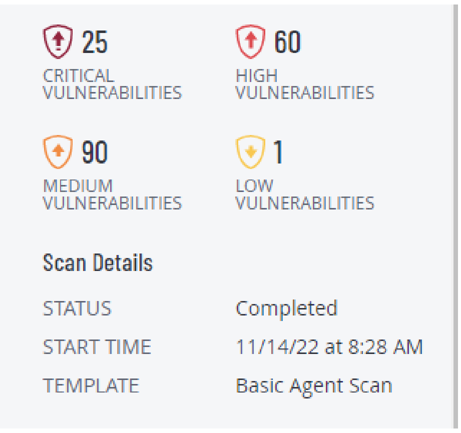
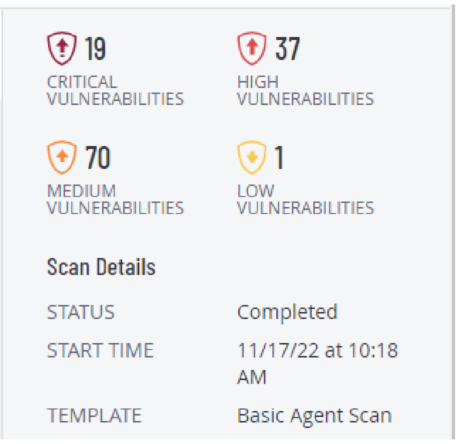
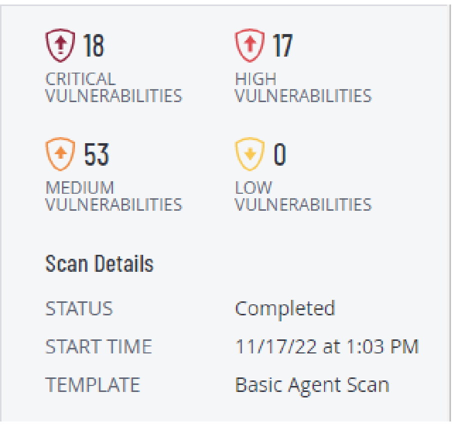
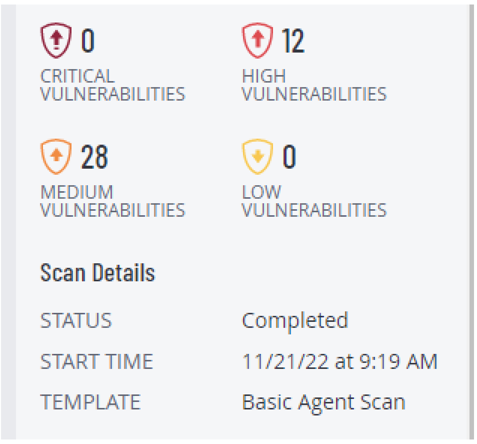
However, Tenable.io automate this manual process. Thus, the risk assessment has already been completed by Tenable.io. Each vulnerability was ranked by Tenable.io as info, low, medium, high, or critical. The purpose of this process is to prioritize vulnerabilities. Can refer to Figure 2.3 to view the risk assessment done by the Tenable.io.

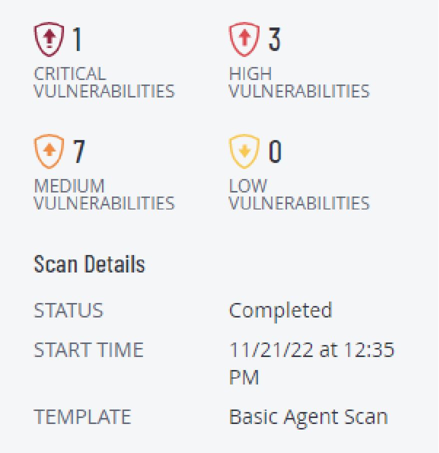
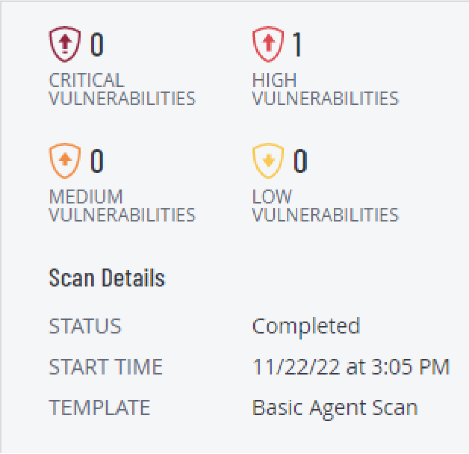
2.3.1.3.4 Remediation

Remediation and mitigation are the last processes in the vulnerability assessment process. Remediating vulnerabilities involves fixing any security vulnerabilities found during the risk assessment process. This stage, which is often carried out by security experts and operations teams, is focused on identifying weaknesses and implementing strategies to lessen the chances of reappearing vulnerabilities. Here again, Tenable.io assists with the process by making suggestions and a solution for every vulnerability.

Before the remediation, the computer had 25 critical vulnerabilities, 60 high vulnerabilities, 90 medium vulnerabilities, and 1 low vulnerability. This shows that the computer is unsafe to use and can be easily exploited by cybercriminals. Therefore, it is necessary to focus on the critical vulnerability before fixing the high, medium, and low vulnerabilities. The supervisor assigned me to remediate the computer by following the recommendation stated in Tenable.io. After testing with the solution, the basic agent scan must be done once more to check the current vulnerability. Scanning is necessary each time to determine the current vulnerability. The remediation must be carried out to the highest possible extent. Finally, the remediation was performed until just one high vulnerability remained. Check out Table 2.1 to view how the vulnerabilities were reduced during the remediation process.

Table 2.1 Remediation process

First Scan	Second Scan
 25 CRITICAL VULNERABILITIES 60 HIGH VULNERABILITIES 90 MEDIUM VULNERABILITIES 1 LOW VULNERABILITIES Scan Details STATUS Completed START TIME 11/14/22 at 8:28 AM TEMPLATE Basic Agent Scan	 19 CRITICAL VULNERABILITIES 37 HIGH VULNERABILITIES 70 MEDIUM VULNERABILITIES 1 LOW VULNERABILITIES Scan Details STATUS Completed START TIME 11/17/22 at 10:18 AM TEMPLATE Basic Agent Scan
Third Scan	Forth Scan
 18 CRITICAL VULNERABILITIES 17 HIGH VULNERABILITIES 53 MEDIUM VULNERABILITIES 0 LOW VULNERABILITIES Scan Details STATUS Completed START TIME 11/17/22 at 1:03 PM TEMPLATE Basic Agent Scan	 0 CRITICAL VULNERABILITIES 12 HIGH VULNERABILITIES 28 MEDIUM VULNERABILITIES 0 LOW VULNERABILITIES Scan Details STATUS Completed START TIME 11/21/22 at 9:19 AM TEMPLATE Basic Agent Scan

Fifth Scan	Final Scan
 1 CRITICAL VULNERABILITIES 3 HIGH VULNERABILITIES 7 MEDIUM VULNERABILITIES 0 LOW VULNERABILITIES Scan Details STATUS Completed START TIME 11/21/22 at 12:35 PM TEMPLATE Basic Agent Scan	 0 CRITICAL VULNERABILITIES 1 HIGH VULNERABILITIES 0 MEDIUM VULNERABILITIES 0 LOW VULNERABILITIES Scan Details STATUS Completed START TIME 11/22/22 at 3:05 PM TEMPLATE Basic Agent Scan

2.3.2 DNS Application System

During the internship, other tasks were assigned which is to assist the staff in developing a website called DNS Application System.

2.3.2.1 DNS Application System Overview

A domain name system (DNS) is a directory of all internet-connected resources. Humans use domain names such as cci.umk.edu.my to access online information. But actually, it is the IP addresses that enable communication between web browsers. Hence, for browsers to load Internet resources, DNS converts domain names to IP addresses. The website cannot be accessed if the DNS is unable to convert the domain name to the right IP address. In other words, almost all of the internet will stop working if DNS isn't present.

Organizations without domain names or websites are gradually falling behind because modern culture is so dependent on the internet. But, a registered domain name is just rented for a specific period rather than being owned. A domain name can be rented by another organization if it is not renewed. Besides, a DNS won't be able to connect to an IP address and won't provide any results if someone searches for an expired domain name. Fortunately, a domain name that has expired is still usable. A domain name that has expired can be "reused" to point to a different IP address and launch a new website.

Therefore, DNS management is necessary for UMK to have an online presence. Staff and students can visit any website hosted by UMK thanks to having an online presence. On the UMK campus, the majority of computers, even those that use DHCP, are automatically set up to use the campus DNS and are given names. In addition, the university handles the registration, setup, and renewal processes for domains (with umk.edu.my ending).

However, submitting an application for a new DNS is still done manually using paper and a pen. Moreover, it is easily damaged and misplaced. However, the process can be automated by developing the DNS application system. Staff can apply for a new DNS directly from the system by providing simply the DNS information. The information about the application is already in the database.

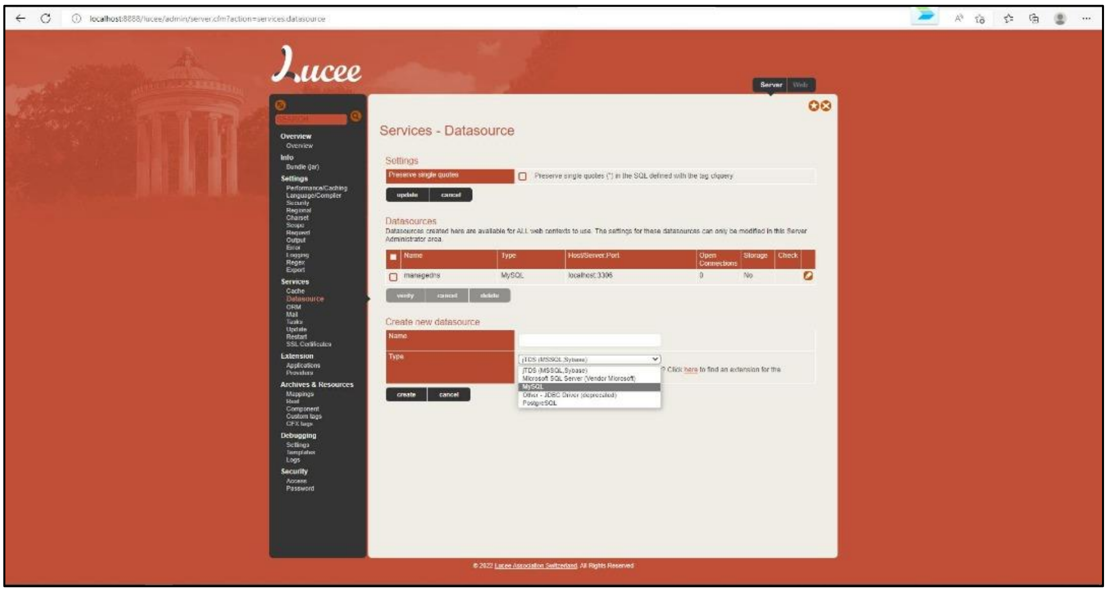
2.3.2.2 Objective of the System Development

The following is the objective of the DNS application system development:

i. To automate the process of applying new DNS.
ii. To validate the identity of the applicant.
iii. To simplify the process of filling out the application form.
iv. To provide clear and readable writing in the application form.
v. To avoid misplacing and damage on the application form.

2.3.2.3 Work Done During System Development

A member of the staff introduce a scripting language named ColdFusion Markup Language (CFML) and a server called Lucee. Furthermore, Lucee, the top open-source CFML application server, was also introduced by the staff. Creating a username and password is required during Lucee's installation. Only the user with the generated username and password is allowed access to the Lucee website. The Lucee website's datasource must then be configured in order to establish a connection with MySQL. Figure 2.4 displays the configuration of Lucee to connect to MySQL.



Services - Datasource

Settings

Preserve single quotes □ Preserve single quotes (') in the SQL defined with the tag cfquery

Datasources

Datasources created here are available for ALL web contexts to use. The settings for these datasources can only be modified in this Server Administrator area.

□	Name	Type	Host/Server:Port	Open Connections	Storage	Check
□	managedns	MySQL	localhost:3306	0	No	

Create new datasource

Name

Type: jTDS (MSSQL,Sybase)

jTDS (MSSQL,Sybase)
Microsoft SQL Server (Vendor Microsoft)
MySQL
Other - JDBC Driver (deprecated)
PostgreSQL

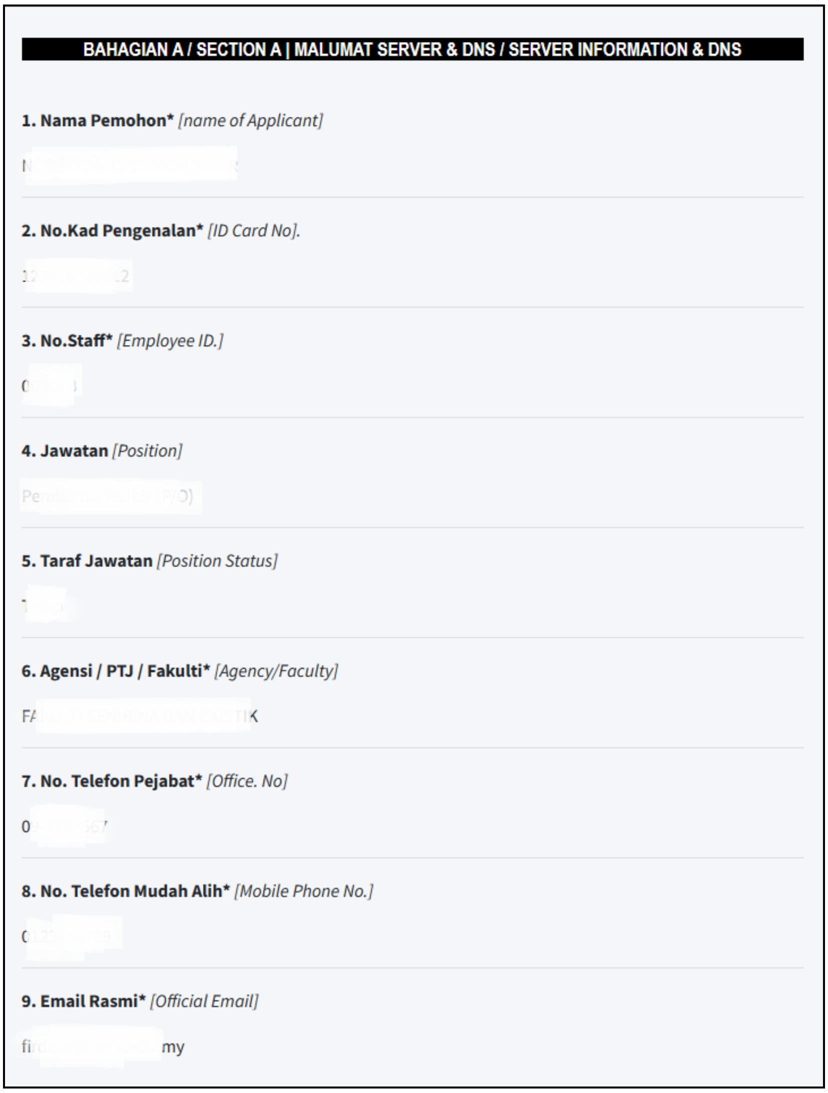
? Click here to find an extension for the

Figure 2.4 The setup of Lucee to connect to MySQL

During system development, five work is performed: applicant information, server information and DNS, the applicant's signature, form output, and the login verification process.

2.3.2.3.1 Section A – Applicant Information

The applicant information is necessary to identify the individual submitting the new DNS application. Plus, not every staff is eligible to apply for the new DNS. Thus, the position and the agency are both important. DNS setting needs the skill of a network and communication professional. Next, it's crucial to verify the staff members' identities using their employment IDs. Additionally, the applicant's telephone number is necessary to inform them of any DNS issues. However, the database already has the applicant's information. In this way, the system already confirms the applicant's identity and gathers information about them when they log in. As a result, the applicants do not need to enter their information because it is prefilled for them when the form is accessed. This can make it easier for the applicants to complete the form. The interface of Section A is shown in Figure 2.5 meanwhile the coding is shown in Figure 2.6.



BAHAGIAN A / SECTION A | MALUMAT SERVER & DNS / SERVER INFORMATION & DNS

1. **Nama Pemohon*** *[name of Applicant]*

[redacted]

2. **No.Kad Pengenalan*** *[ID Card No].*

[redacted]

3. **No.Staff*** *[Employee ID.]*

[redacted]

4. **Jawatan** *[Position]*

[redacted]

5. **Taraf Jawatan** *[Position Status]*

[redacted]

6. **Agensi / PTJ / Fakulti*** *[Agency/Faculty]*

[redacted]

7. **No. Telefon Pejabat*** *[Office. No]*

[redacted]

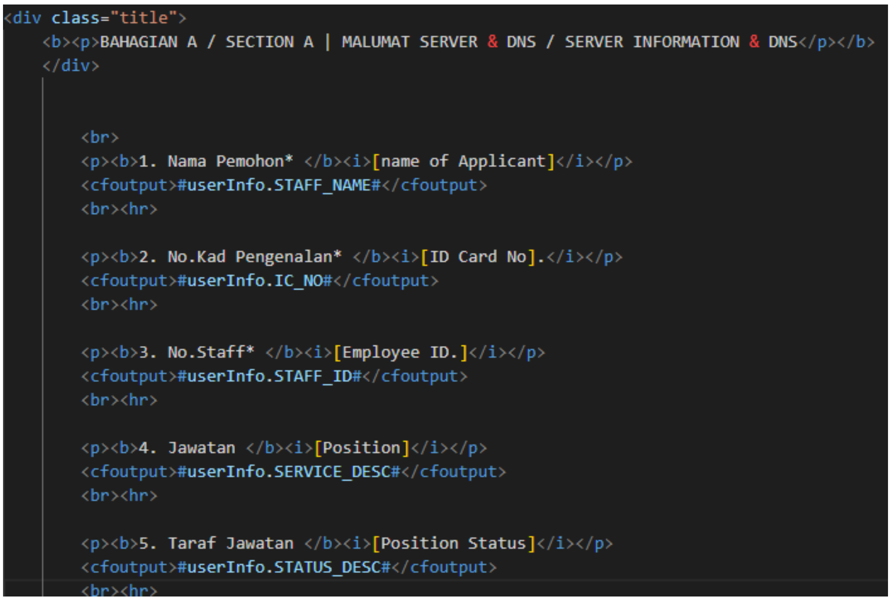
8. **No. Telefon Mudah Alih*** *[Mobile Phone No.]*

[redacted]

9. **Email Rasmi*** *[Official Email]*

[redacted]

Figure 2.5 The interface for Section A

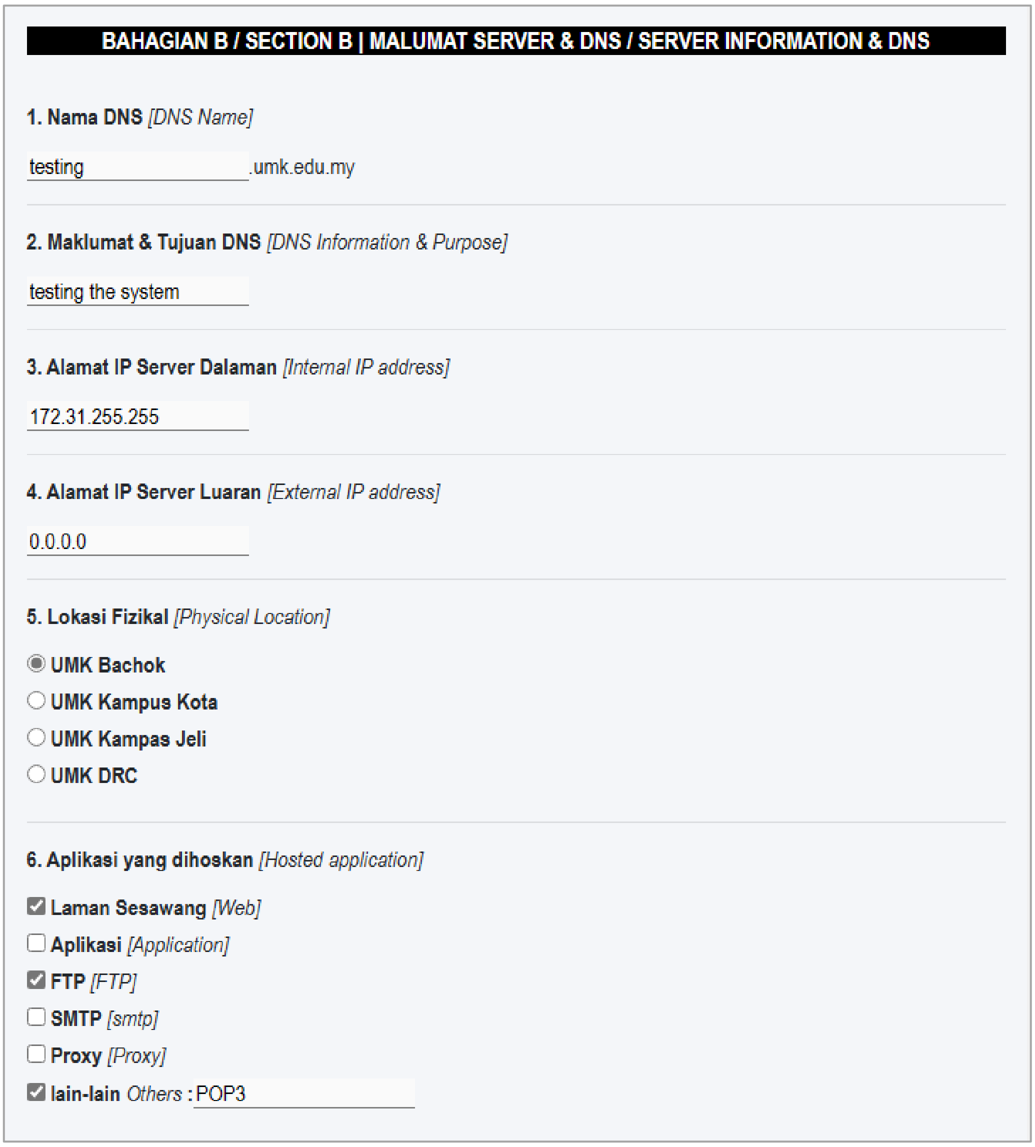


```
<div class="title">
    <b><p>BAHAGIAN A / SECTION A | MALUMAT SERVER & DNS / SERVER INFORMATION & DNS</p></b>
    </div>


        <br>
        <p><b>1. Nama Pemohon* </b><i>[name of Applicant]</i></p>
        <cfoutput>#userInfo.STAFF_NAME#</cfoutput>
        <br><hr>

        <p><b>2. No.Kad Pengenalan* </b><i>[ID Card No].</i></p>
        <cfoutput>#userInfo.IC_NO#</cfoutput>
        <br><hr>

        <p><b>3. No.Staff* </b><i>[Employee ID.]</i></p>
        <cfoutput>#userInfo.STAFF_ID#</cfoutput>
        <br><hr>

        <p><b>4. Jawatan </b><i>[Position]</i></p>
        <cfoutput>#userInfo.SERVICE_DESC#</cfoutput>
        <br><hr>

        <p><b>5. Taraf Jawatan </b><i>[Position Status]</i></p>
        <cfoutput>#userInfo.STATUS_DESC#</cfoutput>
        <br><hr>
```

Figure 2.6 The coding for Section A

2.3.2.3.2 Section B – Server Information and DNS

To begin with, the DNS name is necessary to determine the identity of the new DNS. The application then has to specify the DNS's purpose. The internal IP address and external IP address are also required since DNS transforms domain names into IP addresses. It is also crucial to learn where the DNS is located and what application is hosted on the DNS. Figure 2.7 show the interface for Section B of the application. Figure 2.8 show the coding to create the Section B. In Section B, input value checking also important to obtain the option chosen by the applicant, so the coding as displayed in Figure 2.9 is required.



BAHAGIAN B / SECTION B | MALUMAT SERVER & DNS / SERVER INFORMATION & DNS

1. Nama DNS *[DNS Name]*

testing .umk.edu.my

2. Maklumat & Tujuan DNS *[DNS Information & Purpose]*

testing the system

3. Alamat IP Server Dalaman *[Internal IP address]*

172.31.255.255

4. Alamat IP Server Luaran *[External IP address]*

0.0.0.0

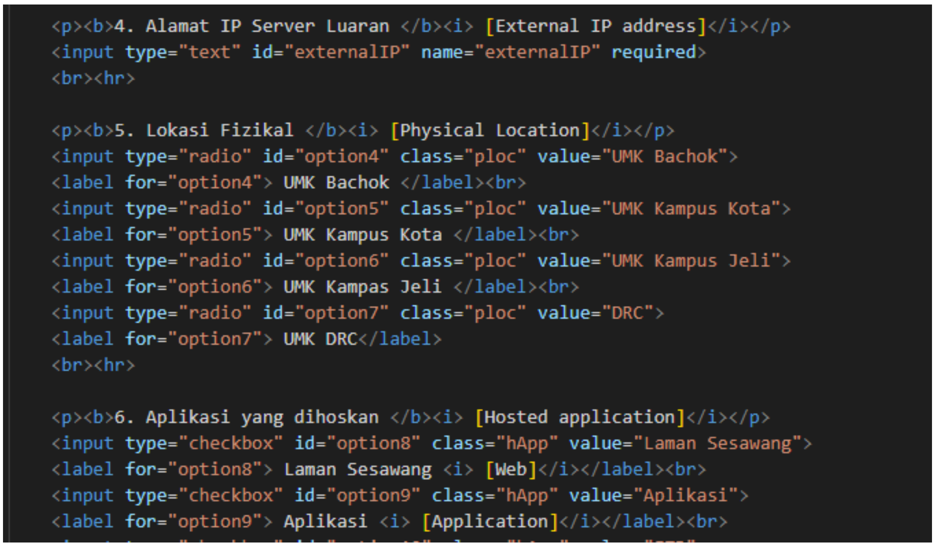
5. Lokasi Fizikal *[Physical Location]*

● **UMK Bachok**
○ **UMK Kampus Kota**
○ **UMK Kampas Jeli**
○ **UMK DRC**

6. Aplikasi yang dihoskan *[Hosted application]*

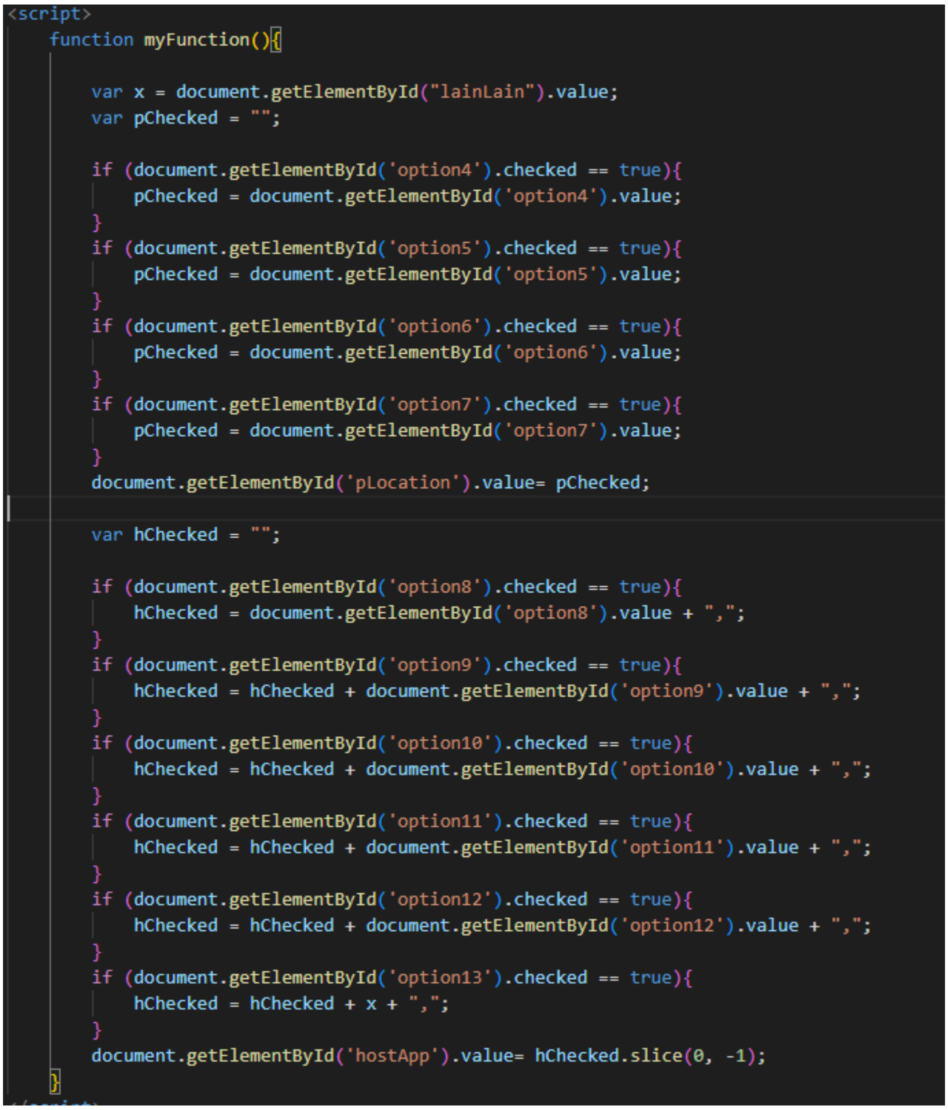
☑ **Laman Sesawang** *[Web]*
□ **Aplikasi** *[Application]*
☑ **FTP** *[FTP]*
□ **SMTP** *[smtp]*
□ **Proxy** *[Proxy]*
☑ **lain-lain** *Others* : POP3

Figure 2.7 The interface for Section B



```
<p><b>4. Alamat IP Server Luaran </b><i> [External IP address]</i></p>
<input type="text" id="externalIP" name="externalIP" required>
<br><hr>

<p><b>5. Lokasi Fizikal </b><i> [Physical Location]</i></p>
<input type="radio" id="option4" class="ploc" value="UMK Bachok">
<label for="option4"> UMK Bachok </label><br>
<input type="radio" id="option5" class="ploc" value="UMK Kampus Kota">
<label for="option5"> UMK Kampus Kota </label><br>
<input type="radio" id="option6" class="ploc" value="UMK Kampus Jeli">
<label for="option6"> UMK Kampas Jeli </label><br>
<input type="radio" id="option7" class="ploc" value="DRC">
<label for="option7"> UMK DRC</label>
<br><hr>

<p><b>6. Aplikasi yang dihoskan </b><i> [Hosted application]</i></p>
<input type="checkbox" id="option8" class="hApp" value="Laman Sesawang">
<label for="option8"> Laman Sesawang <i> [Web]</i></label><br>
<input type="checkbox" id="option9" class="hApp" value="Aplikasi">
<label for="option9"> Aplikasi <i> [Application]</i></label><br>
```

Figure 2.8 The coding for section B

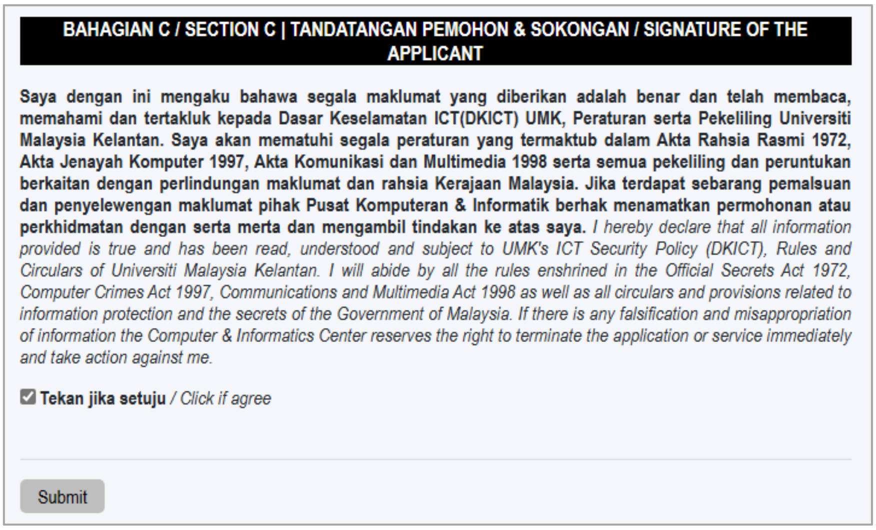


```
<script>
    function myFunction(){

        var x = document.getElementById("lainLain").value;
        var pChecked = "";

        if (document.getElementById('option4').checked == true){
            pChecked = document.getElementById('option4').value;
        }
        if (document.getElementById('option5').checked == true){
            pChecked = document.getElementById('option5').value;
        }
        if (document.getElementById('option6').checked == true){
            pChecked = document.getElementById('option6').value;
        }
        if (document.getElementById('option7').checked == true){
            pChecked = document.getElementById('option7').value;
        }
        document.getElementById('pLocation').value= pChecked;

        var hChecked = "";

        if (document.getElementById('option8').checked == true){
            hChecked = document.getElementById('option8').value + ",";
        }
        if (document.getElementById('option9').checked == true){
            hChecked = hChecked + document.getElementById('option9').value + ",";
        }
        if (document.getElementById('option10').checked == true){
            hChecked = hChecked + document.getElementById('option10').value + ",";
        }
        if (document.getElementById('option11').checked == true){
            hChecked = hChecked + document.getElementById('option11').value + ",";
        }
        if (document.getElementById('option12').checked == true){
            hChecked = hChecked + document.getElementById('option12').value + ",";
        }
        if (document.getElementById('option13').checked == true){
            hChecked = hChecked + x + ",";
        }
        document.getElementById('hostApp').value= hChecked.slice(0, -1);
    }
```

Figure 2.9 The input value checking for section B

2.3.2.3.3 Section C – Signature of the Applicant

Finally, the applicant must sign the form agreement by marking the checkbox. The applicant must verify that all the information submitted is accurate. If any of the information is false, the organization has the right to reject the application. Because of this, before signing the agreement, the applicant must double-checks the information that was given. Only after the applicant signs the agreement can the submission be completed. Figure 2.10 and 2.11 displays the interface and coding for Section C of the application form.

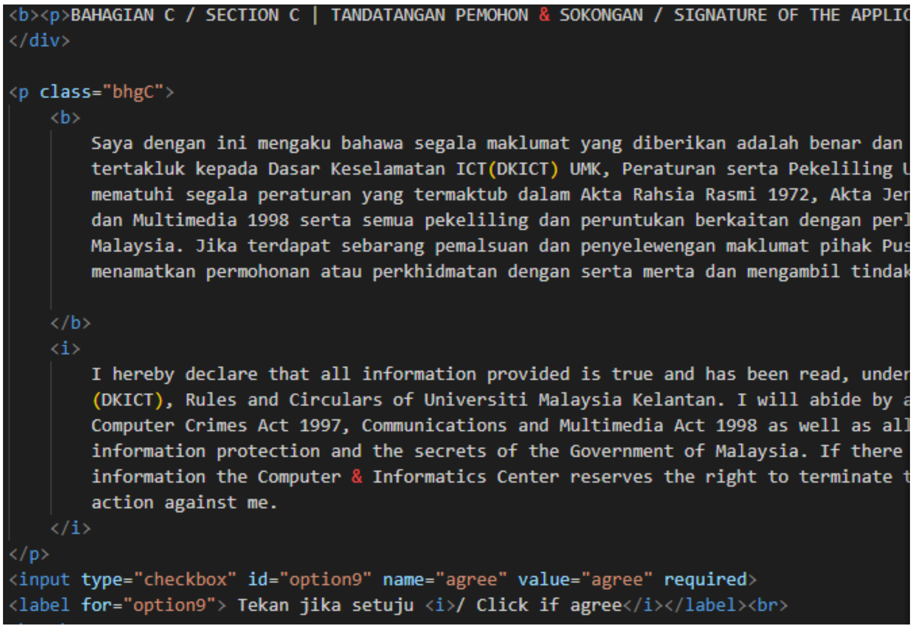


BAHAGIAN C / SECTION C | TANDATANGAN PEMOHON & SOKONGAN / SIGNATURE OF THE APPLICANT

Saya dengan ini mengaku bahawa segala maklumat yang diberikan adalah benar dan telah membaca, memahami dan tertakluk kepada Dasar Keselamatan ICT(DKICT) UMK, Peraturan serta Pekeliling Universiti Malaysia Kelantan. Saya akan mematuhi segala peraturan yang termaktub dalam Akta Rahsia Rasmi 1972, Akta Jenayah Komputer 1997, Akta Komunikasi dan Multimedia 1998 serta semua pekeliling dan peruntukan berkaitan dengan perlindungan maklumat dan rahsia Kerajaan Malaysia. Jika terdapat sebarang pemalsuan dan penyelewengan maklumat pihak Pusat Komputeran & Informatik berhak menamatkan permohonan atau perkhidmatan dengan serta merta dan mengambil tindakan ke atas saya. *I hereby declare that all information provided is true and has been read, understood and subject to UMK's ICT Security Policy (DKICT), Rules and Circulars of Universiti Malaysia Kelantan. I will abide by all the rules enshrined in the Official Secrets Act 1972, Computer Crimes Act 1997, Communications and Multimedia Act 1998 as well as all circulars and provisions related to information protection and the secrets of the Government of Malaysia. If there is any falsification and misappropriation of information the Computer & Informatics Center reserves the right to terminate the application or service immediately and take action against me.*

☑ **Tekan jika setuju** / *Click if agree*

Figure 2.10 The interface for Section C

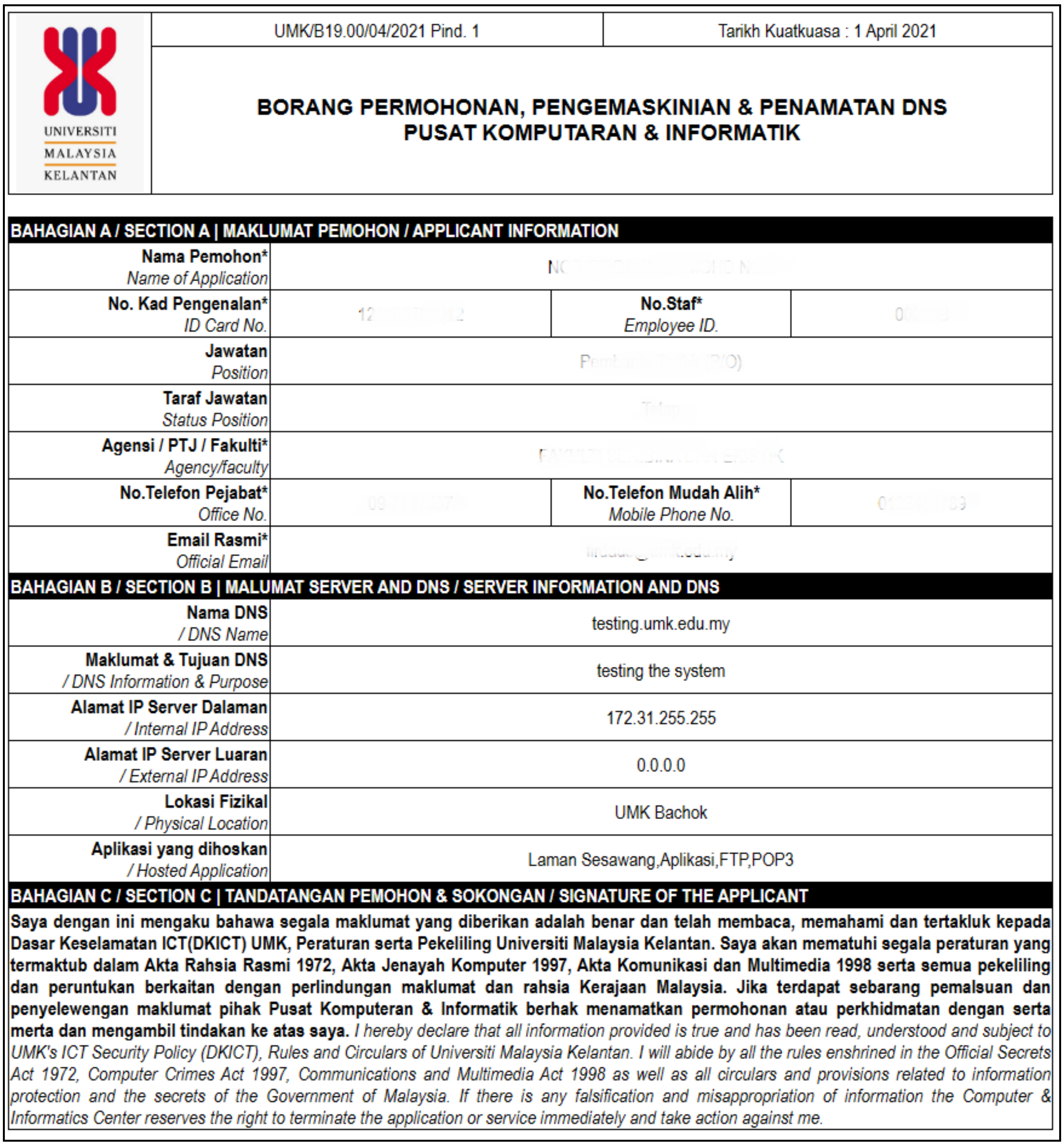


```
<b><p>BAHAGIAN C / SECTION C | TANDATANGAN PEMOHON & SOKONGAN / SIGNATURE OF THE APPLIC
</div>

<p class="bhgC">
    <b>
        Saya dengan ini mengaku bahawa segala maklumat yang diberikan adalah benar dan
        tertakluk kepada Dasar Keselamatan ICT(DKICT) UMK, Peraturan serta Pekeliling U
        mematuhi segala peraturan yang termaktub dalam Akta Rahsia Rasmi 1972, Akta Jer
        dan Multimedia 1998 serta semua pekeliling dan peruntukan berkaitan dengan perl
        Malaysia. Jika terdapat sebarang pemalsuan dan penyelewengan maklumat pihak Pus
        menamatkan permohonan atau perkhidmatan dengan serta merta dan mengambil tindak

    </b>
    <i>
        I hereby declare that all information provided is true and has been read, under
        (DKICT), Rules and Circulars of Universiti Malaysia Kelantan. I will abide by a
        Computer Crimes Act 1997, Communications and Multimedia Act 1998 as well as all
        information protection and the secrets of the Government of Malaysia. If there
        information the Computer & Informatics Center reserves the right to terminate t
        action against me.
    </i>
</p>
<input type="checkbox" id="option9" name="agree" value="agree" required>
<label for="option9"> Tekan jika setuju <i>/ Click if agree</i></label><br>
```

Figure 2.11 The coding for Section C

2.3.2.3.4 Forms Output

The page will load once the applicant has filled in all the required fields and signed the agreement. The page shows all the data that was previously entered for the DNS application along with the agreement as displayed in Figure 2.12. The form is now prepared for printing.



UNIVERSITI MALAYSIA KELANTAN

UMK/B19.00/04/2021 Pind. 1 | Tarikh Kuatkuasa : 1 April 2021

BORANG PERMOHONAN, PENGEMASKINIAN & PENAMATAN DNS
PUSAT KOMPUTARAN & INFORMATIK

BAHAGIAN A / SECTION A | MAKLUMAT PEMOHON / APPLICANT INFORMATION			
Nama Pemohon* *Name of Application*	[redacted]		
No. Kad Pengenalan* *ID Card No.*	[redacted]	**No.Staf*** *Employee ID.*	[redacted]
Jawatan *Position*	[redacted]		
Taraf Jawatan *Status Position*	[redacted]		
Agensi / PTJ / Fakulti* *Agency/faculty*	[redacted]		
No.Telefon Pejabat* *Office No.*	[redacted]	**No.Telefon Mudah Alih*** *Mobile Phone No.*	[redacted]
Email Rasmi* *Official Email*	[redacted]		
BAHAGIAN B / SECTION B | MALUMAT SERVER AND DNS / SERVER INFORMATION AND DNS			
Nama DNS */ DNS Name*	testing.umk.edu.my		
Maklumat & Tujuan DNS */ DNS Information & Purpose*	testing the system		
Alamat IP Server Dalaman */ Internal IP Address*	172.31.255.255		
Alamat IP Server Luaran */ External IP Address*	0.0.0.0		
Lokasi Fizikal */ Physical Location*	UMK Bachok		
Aplikasi yang dihoskan */ Hosted Application*	Laman Sesawang,Aplikasi,FTP,POP3		
BAHAGIAN C / SECTION C | TANDATANGAN PEMOHON & SOKONGAN / SIGNATURE OF THE APPLICANT			

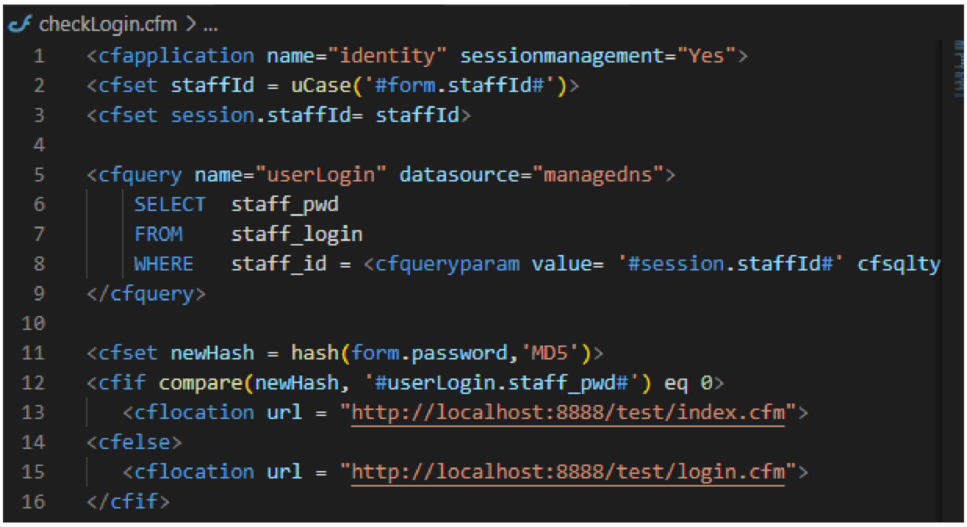
Saya dengan ini mengaku bahawa segala maklumat yang diberikan adalah benar dan telah membaca, memahami dan tertakluk kepada Dasar Keselamatan ICT(DKICT) UMK, Peraturan serta Pekeliling Universiti Malaysia Kelantan. Saya akan mematuhi segala peraturan yang termaktub dalam Akta Rahsia Rasmi 1972, Akta Jenayah Komputer 1997, Akta Komunikasi dan Multimedia 1998 serta semua pekeliling dan peruntukan berkaitan dengan perlindungan maklumat dan rahsia Kerajaan Malaysia. Jika terdapat sebarang pemalsuan dan penyelewengan maklumat pihak Pusat Komputeran & Informatik berhak menamatkan permohonan atau perkhidmatan dengan serta merta dan mengambil tindakan ke atas saya. *I hereby declare that all information provided is true and has been read, understood and subject to UMK's ICT Security Policy (DKICT), Rules and Circulars of Universiti Malaysia Kelantan. I will abide by all the rules enshrined in the Official Secrets Act 1972, Computer Crimes Act 1997, Communications and Multimedia Act 1998 as well as all circulars and provisions related to information protection and the secrets of the Government of Malaysia. If there is any falsification and misappropriation of information the Computer & Informatics Center reserves the right to terminate the application or service immediately and take action against me.*

Figure 2.12 The output of the application form

2.3.2.3.5 Login Verification Process

The staff has already built the login page, but not the verification process. Every user that registered with the system had their passwords kept in a database after being hashed to MD5. Hashing is used to make the password unreadable to the hacker. Using an encryption algorithm, hashing transforms the password into a short string of characters and digits. If a website is hacked, malicious hackers do not get direct exposure to the real (plaintext) password. Instead, they just get hashed password, which is unreadable.

Then, whenever a user inputs their password on the login page, the system compares it to the stored password in the database. To match the password (hashed) in the database, the password entered on the login page would first be transformed to MD5. Only if the passwords and username match will the system user be able to access the system. The coding used to perform the user authentication is shown in Figure 2.13.



```
<cfapplication name="identity" sessionmanagement="Yes">
<cfset staffId = uCase('#form.staffId#')>
<cfset session.staffId= staffId>

<cfquery name="userLogin" datasource="managedns">
    SELECT  staff_pwd
    FROM    staff_login
    WHERE   staff_id = <cfqueryparam value= '#session.staffId#' cfsqlty
</cfquery>

<cfset newHash = hash(form.password,'MD5')>
<cfif compare(newHash, '#userLogin.staff_pwd#') eq 0>
   <cflocation url = "http://localhost:8888/test/index.cfm">
<cfelse>
   <cflocation url = "http://localhost:8888/test/login.cfm">
</cfif>
```

Figure 2.13 The coding to verify the system user

2.3.3 Cybersecurity Guidelines

The next task is to publish 25 cybersecurity guidelines. Information regarding cybersecurity risk and ways to prevent it was gathered through research. Since the guidelines must be presented in the form of a poster, Canva (https://www.canva.com) is the most suitable software for this purpose. It is easier to design a poster here because it provides a variety of templates. However, the template must be customized to fit the guidelines' theme. The following is a list of 25 guidelines topics for the poster.

1. The basics of safe online shopping
2. Should you plug that in?
3. Who sent you the friend request?
4. Common Password Mistakes

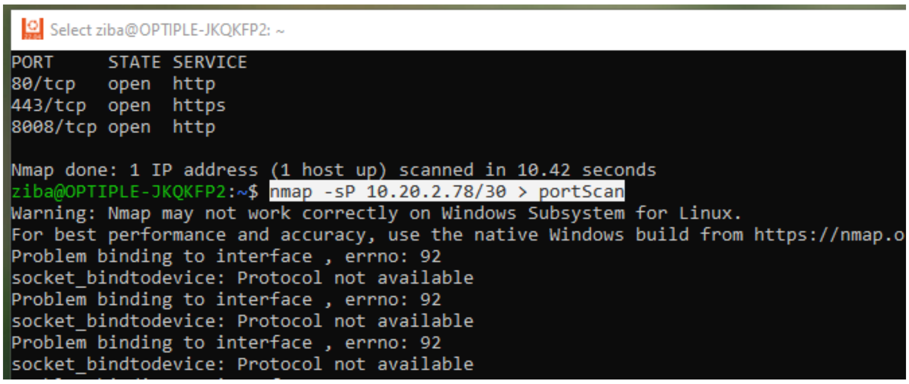
5. Smartphone Security FTW
6. You still need antivirus
7. Get your 2-FA on
8. Keep it in check
9. Lock it up
10. How to protect what matters
11. Have you ever heard of keyloggers?
12. Track your digital footprint
13. Watch out for bogus antivirus
14. Shadowy purposes
15. Clean up your mobile applications
16. Check your email’s activity log
17. Ransomware 101
18. Too good to be hacked
19. Gone phishing
20. Are you HTTPS?
21. No PUPs allowed
22. Less spam, less problems
23. Your phone is smart, but is it secure?
24. No bad, bad ads
25. Check it before you click it

Security is a broad topic. These posters aims to raise staff awareness of the threat of a cyberattack. Please visit the link to view each designed posters: https://www.canva.com/design/DAFTSQf_rps/hwv14kejgx0-ShDA7gkGfA/view?utm_content=DAFTSQf_rps&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink

2.3.4 NDR - Sangfor's Cyber Command (SCC)

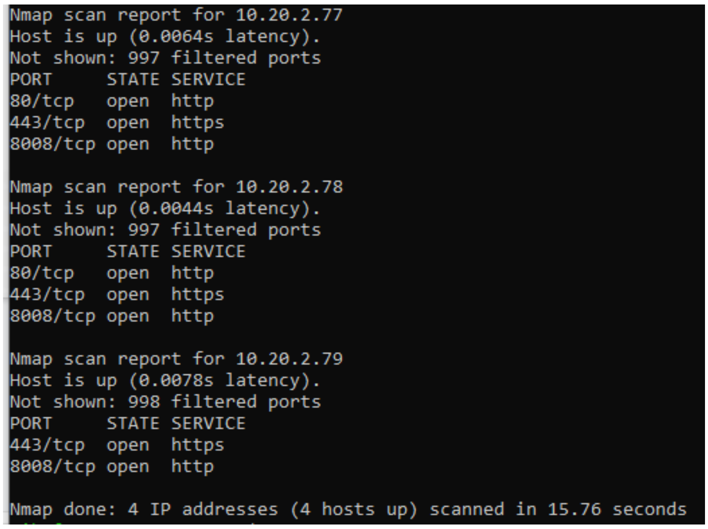
The purpose of the task is to investigate the SCC's features. The supervisor provided me with a unique URL to the SCC website as well as the account username and password to access the SCC system. The SCC is an advanced threat detection and response system (NDR). Network detection and response (NDR) detect abnormal network activity by combining non-signature-based advanced analytical approaches such as machine learning (Technologies, 2022). SCC can detect an unknown attack that poses a possible danger to the organization, provides better visibility of infrastructure security posture, detects any compromised areas, and helps in mitigation prioritization. It is also less expensive than security information and event management (SIEM). Please refer to Appendix B to view some of the SCC interfaces.

Throughout the investigation, an attack had been carried out to evaluate the SCC's features and abilities. The "nmap" command line and Ubuntu were used to conduct the attack. Ubuntu is a full-featured desktop Linux operating system that is free of charge (DistroWatch, 2019). The command line and the IP address of the UMK server were used in the attack as displayed in Figure 2.14. The nmap scan provides a report on the server that was attacked as shown in Figure 2.15.



```
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8008/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 10.42 seconds
ziba@OPTIPLE-JKQKFP2:~$ nmap -sP 10.20.2.78/30 > portScan
Warning: Nmap may not work correctly on Windows Subsystem for Linux.
For best performance and accuracy, use the native Windows build from https://nmap.o
Problem binding to interface , errno: 92
socket_bindtodevice: Protocol not available
Problem binding to interface , errno: 92
socket_bindtodevice: Protocol not available
Problem binding to interface , errno: 92
socket_bindtodevice: Protocol not available
```

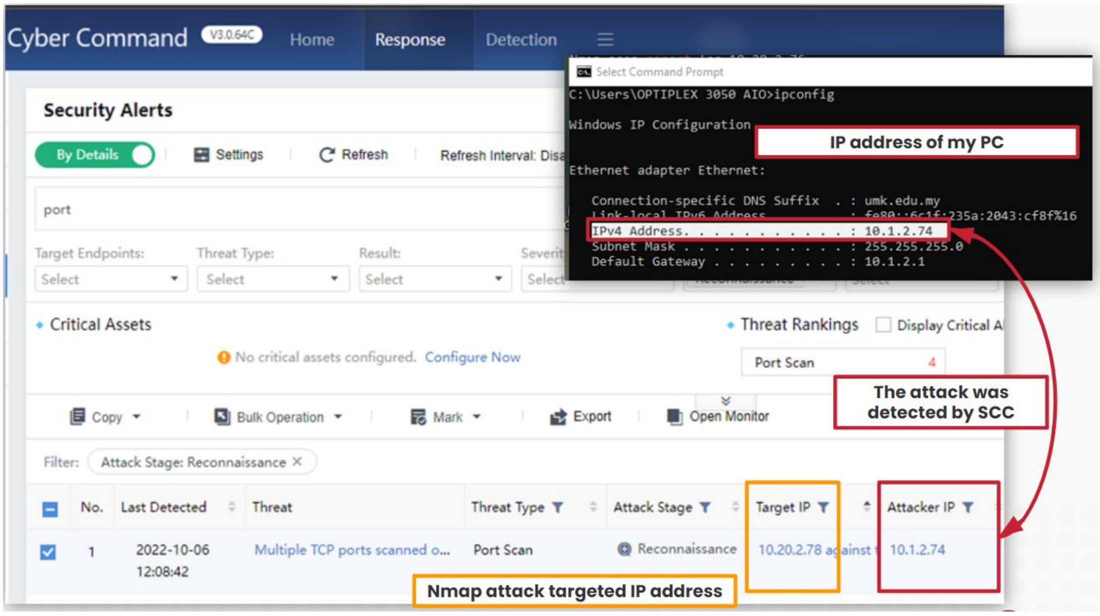
Figure 2.14 The "nmap" command line to launch attack



```
Nmap scan report for 10.20.2.77
Host is up (0.0064s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8008/tcp open  http

Nmap scan report for 10.20.2.78
Host is up (0.0044s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8008/tcp open  http

Nmap scan report for 10.20.2.79
Host is up (0.0078s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
443/tcp  open  https
8008/tcp open  http

Nmap done: 4 IP addresses (4 hosts up) scanned in 15.76 seconds
```

Figure 2.15 Nmap scan report about the targeted server

As intended, the SCC responds to the attack and includes it in the security alert section. Furthermore, the SCC classifies the attack as a "Port Scan" threat and displays the attacker's IP (my IP) along with the target's IP. Figure 2.16 displays the SCC response to the attack.



port

Target Endpoints: Select
Threat Type: Select
Result: Select
Severit Select

Critical Assets
No critical assets configured. Configure Now

Threat Rankings □ Display Critical A
Port Scan 4

Filter: Attack Stage: Reconnaissance ×

☐	No.	Last Detected	Threat	Threat Type	Attack Stage	Target IP	Attacker IP
☑	1	2022-10-06 12:08:42	Multiple TCP ports scanned o...	Port Scan	Reconnaissance	10.20.2.78 against t	10.1.2.74

Select Command Prompt

```
C:\Users\OPTIPLEX 3050 AIO>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : umk.edu.my
   Link-local IPv6 Address . . . . . : fe80::6c1f:235a:2043:cf8f%16
   IPv4 Address. . . . . . . . . . . : 10.1.2.74
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.2.1
```

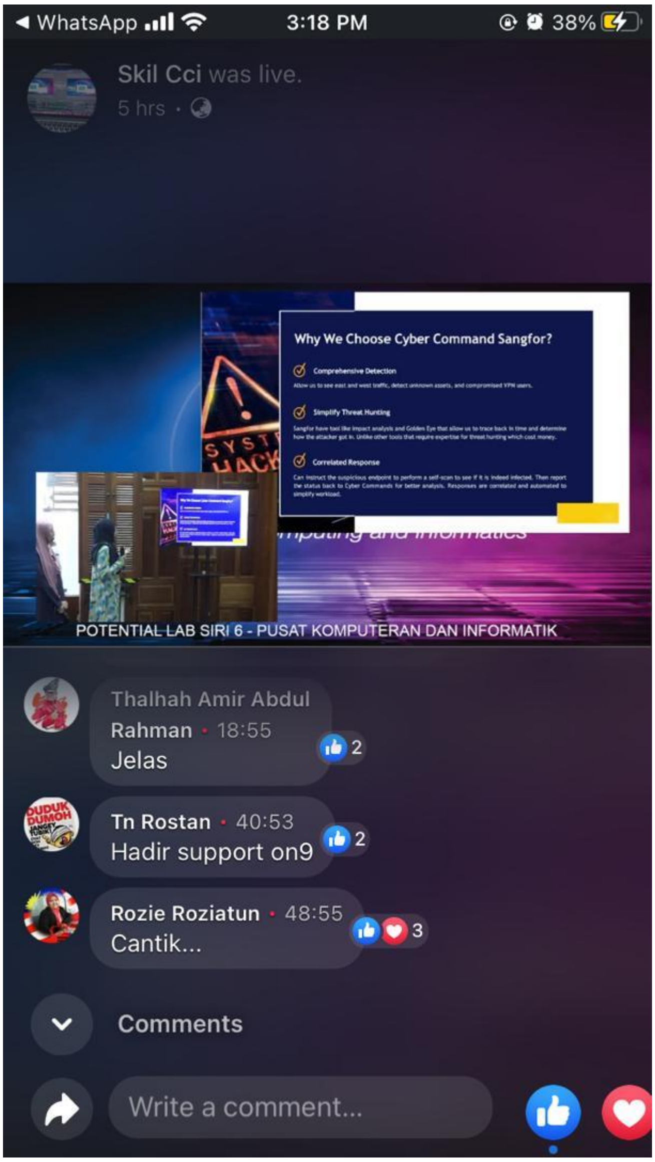
IP address of my PC

The attack was detected by SCC

Nmap attack targeted IP address

Figure 2.16 SCC response to the attack

Following several weeks of research on SCC, all the information was gathered. On 3rd November 2022, a presentation was performed introducing the security-enhancing solution (the SCC) for UMK Bachok and attempts to raise awareness of the cybersecurity dangers in UMK Bachok among CCI staff. The slide was prepared one week before the presentation. The presentation covers what NDR is, why it's necessary, how its features compare to SIEM, why SCC was selected, and the findings. The presentation was done physically and live-streamed on Facebook as shown in Figures 2.17.



Skil Cci was live.
5 hrs ·

Why We Choose Cyber Command Sangfor?

Comprehensive Detection

Allow us to see east and west traffic, detect unknown assets, and compromised VPN users.

Simplify Threat Hunting

Sangfor have tool like impact analysis and Golden Eye that allow us to trace back in time and determine how the attacker got in. Unlike other tools that require expertise for threat hunting which cost money.

Correlated Response

Can instruct the suspicious endpoint to perform a self-scan to see if it is indeed infected. Then report the status back to Cyber Commands for better analysis. Responses are correlated and automated to simplify workload.

POTENTIAL LAB SIRI 6 - PUSAT KOMPUTERAN DAN INFORMATIK

Thalhah Amir Abdul Rahman · 18:55
Jelas
👍 2

Tn Rostan · 40:53
Hadir support on9
👍 2

Rozie Roziatun · 48:55
Cantik...
👍❤️ 3

Figure 2.17 The SCC presentation

Click on the link listed below for further details:

i. Slide presentation (Cyber Command): https://www.canva.com/design/DAFN8Y6CAlI/tmS-3qxUZS8tZLPNzwfPgQ/view?utm_content=DAFN8Y6CAlI&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

ii. FB live: https://m.facebook.com/story.php?story_fbid=522151619457408&id=100077172315204

2.4 Additional Task Assigned

The additional task includes port labeling, cybersecurity trend article, UMK convocation registration, and penetration testing.

2.4.1 Port Labeling

The port labeling was handled inside the server room with the help of one of the staff from the Network and Communication section. The unlabeled port must be labeled, and the old label should be replaced because it cannot be read. A label printer is used to generate the label sticker to make the labeling neater and easier to read. By following the staff instruction, each port must be labeled with the correct name and port number using the label sticker. It is crucial to label the port correctly to avoid people unplugging the wrong cable at the wrong moment. Figure 2.18 and 2.19 displays the process of generating label sticker and process of port labeling.

Figure 2.18 Generating label sticker

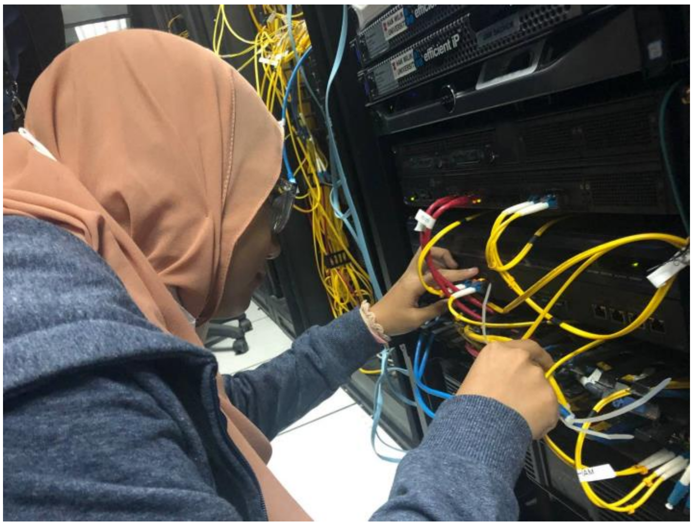


Figure 2.19 Port labeling process

2.4.2 Cybersecurity Trend Article

Top 5 Cybersecurity Trends in 2022 is the title of the article. Due to rising internet usage and worldwide digitization, cybersecurity is more important than ever. Continual cyberattacks are a problem for organizations since technology is advancing. As hackers and cybersecurity professionals compete to surpass one another, the area of cybersecurity develops quickly. New threats and creative countermeasures against cyberattacks develop daily. To prevent these cyberattacks, it is important for cybersecurity professionals to keep up with the latest trends in the field. Hence, the article covers the recent top five trends in cyber security. Starting with the potential of artificial intelligence (AI), then moving on to the Internet of Things (IoT) threats, the growing threat of ransomware, attacks on cloud services, and finally, mobile is the new target. Figure 2.20 displays the first page of the article.

November 17, 2022

Top 5 Cybersecurity Trends in 2022

By Farahziba

Abstract

Cybersecurity is more crucial than ever due to global digitalization and increased internet use. Organizations have to deal with ongoing cyberattacks due to technological advancement. The field of cyber security moves quickly as both hackers and cybersecurity experts compete to surpass one another. Every day, new dangers and innovative defences against them develop. Hence, it is essential for cybersecurity experts to stay on top of the latest cybersecurity trends to avoid these cyberattacks. This article will cover the recent top five trends in cyber security. Starting with the potential of artificial intelligence (AI), then moving on to the Internet of Things (IoT) threats, the growing threat of ransomware, attacks on cloud services, and finally, mobile is the new target.

Keywords: *Cybersecurity, Cyberattack, Hacker, Technology, Internet, Network, Vulnerable, Artificial Intelligence (AI), Internet of Things (IoT), Ransomware, Cloud services, Mobile*

Introduction

Cybersecurity is defined as the activity of securing a

Although most hackers' goal is to steal, manipulate, and harm data, some hackers, known as white hat hackers or

Figure 2.20 The cybersecurity trend article

To view the full article, please visit the link provided below: https://drive.google.com/file/d/1GE-cDt3uwYBb8TJaQmUTkfL5lTcoNN9L/view?usp=sharing

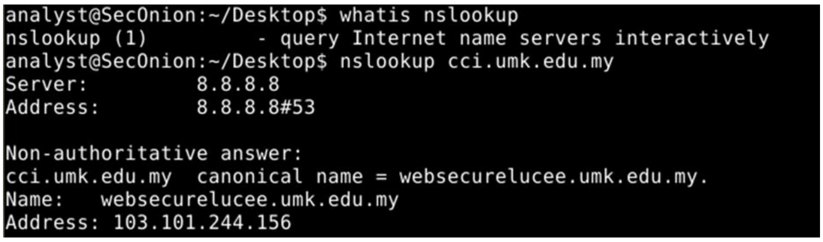
2.4.3 UMK Convocation Registration

The convocation ceremony took place from November 23rd to November 25th, 2023. Due to the lack of staff, the organizer relies on all interns to help manage the convocation event. For three days, interns from the infrastructure department were assigned to assist with convocation registration. The registration process begins by identifying the graduates' names and obtaining their queue numbers. The queue number, which consists of a bar code, would then be scanned to add the student to the system attendance list. Figure 2.21 show the convocation registration day.

Figure 2.21 The convocation registration day

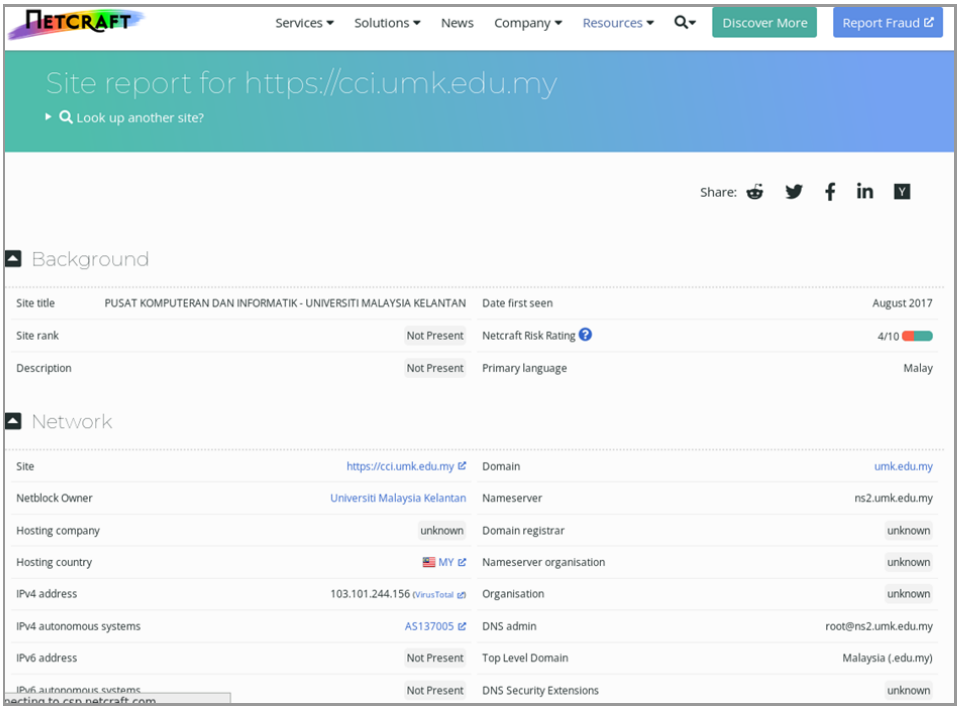
2.4.4 Penetration Testing

A penetration test is necessary to find any flaws in a system's security that an attacker may exploit (Cloudflare, 2022). Penetration testing consists of five stages planning and reconnaissance, scanning, gaining access, maintaining access, and analysis. However, only the initial step has been carried out. The process of reconnaissance involves gathering data such as the domain name, IP address, server name, email server, and more. During the reconnaissance, the target website's IP address and canonical name were obtained using the 'host' and 'nslookup' commands on Linux. The ‘nslookup’ command is executed as in Figure 2.22. The 'dig' program was then used to discover the server name and another related domain name. Last but not least, DNS admin was acquired by using the Netcraft website as in Figure 2.23.



```
analyst@SecOnion:~/Desktop$ whatis nslookup
nslookup (1)         - query Internet name servers interactively
analyst@SecOnion:~/Desktop$ nslookup cci.umk.edu.my
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
cci.umk.edu.my  canonical name = websecurelucee.umk.edu.my.
Name:   websecurelucee.umk.edu.my
Address: 103.101.244.156
```

Figure 2.22 Perform reconnaissance using nslookup



Site report for https://cci.umk.edu.my

Look up another site?

Background

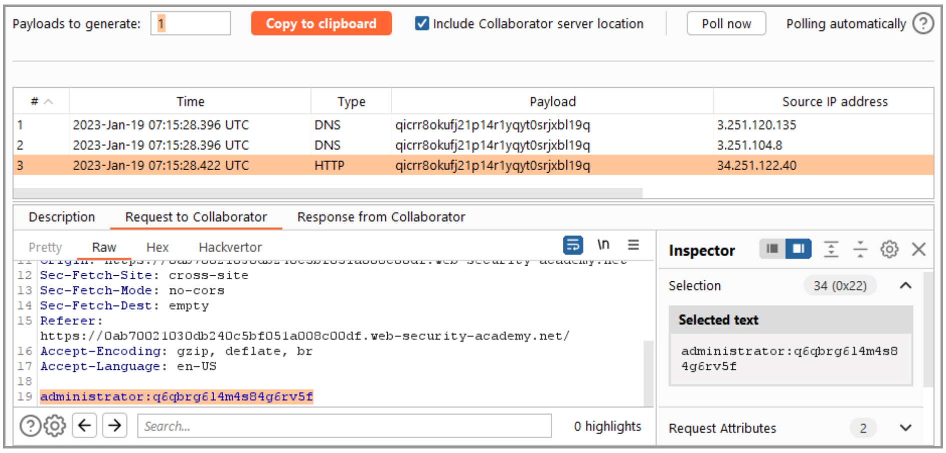
Site title	PUSAT KOMPUTERAN DAN INFORMATIK - UNIVERSITI MALAYSIA KELANTAN	Date first seen	August 2017
Site rank	Not Present	Netcraft Risk Rating	4/10
Description	Not Present	Primary language	Malay

Network

Site	https://cci.umk.edu.my	Domain	umk.edu.my
Netblock Owner	Universiti Malaysia Kelantan	Nameserver	ns2.umk.edu.my
Hosting company	unknown	Domain registrar	unknown
Hosting country	MY	Nameserver organisation	unknown
IPv4 address	103.101.244.156 (VirusTotal)	Organisation	unknown
IPv4 autonomous systems	AS137005	DNS admin	root@ns2.umk.edu.my
IPv6 address	Not Present	Top Level Domain	Malaysia (.edu.my)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown

Figure 2.23 Perform reconnaissance using Netcraft

Before the real implementation of penetration testing, a lot of self-learning was made. In addition, vulnerability websites such as PortSwigger and Hacker101 are used for self-practice hacking. The PortSwigger labs educate how to perform SQL injection and Cross-Site Scripting (XSS) to steal a username and password. Figure 2.24 displays the exploitation by capturing password using Burp Suite. The Hacker101 website then educates how to carry out SQL injection, cross-site scripting (XSS), URL poisoning, and cookie poisoning. Hacker101 also teach the use of SqlMap to take over database as in Figure 2.25. But all self-practice is considered exploitation, which is classified as stage three of penetration testing (Gaining Access).



Payloads to generate: 1

☑ Include Collaborator server location

#	Time	Type	Payload	Source IP address
1	2023-Jan-19 07:15:28.396 UTC	DNS	qicrr8okufj21p14r1yqyt0srjxbl19q	3.251.120.135
2	2023-Jan-19 07:15:28.396 UTC	DNS	qicrr8okufj21p14r1yqyt0srjxbl19q	3.251.104.8
3	2023-Jan-19 07:15:28.422 UTC	HTTP	qicrr8okufj21p14r1yqyt0srjxbl19q	34.251.122.40

```
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
Referer:
https://0ab70021030db240c5bf051a008c00df.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US

administrator:q6qbrg614m4s84g6rv5f
```

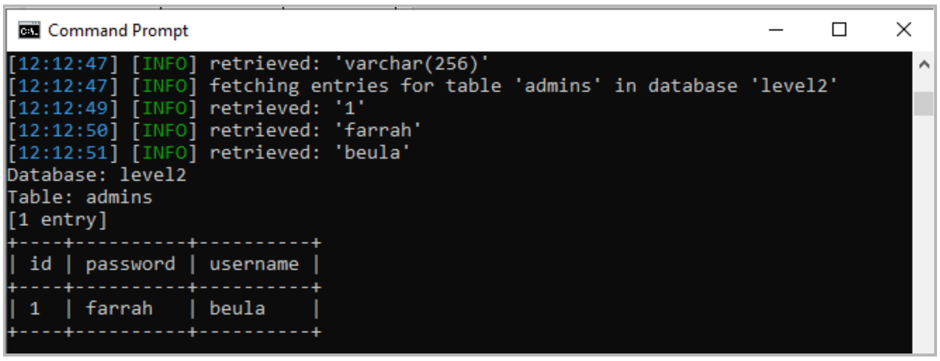
Selection 34 (0x22)

Selected text

```
administrator:q6qbrg614m4s8
4g6rv5f
```

Request Attributes 2

Figure 2.24 Capturing password using Burp Suite



```
[12:12:47] [INFO] retrieved: 'varchar(256)'
[12:12:47] [INFO] fetching entries for table 'admins' in database 'level2'
[12:12:49] [INFO] retrieved: '1'
[12:12:50] [INFO] retrieved: 'farrah'
[12:12:51] [INFO] retrieved: 'beula'
Database: level2
Table: admins
[1 entry]
+----+----------+----------+
| id | password | username |
+----+----------+----------+
| 1  | farrah   | beula    |
+----+----------+----------+
```

Figure 2.25 Takeover database using SqlMap

2.5 Hardware and Software Used

List of hardware and software that are used to execute all the works are as stated in Table 2.2 and Table 2.3.

Table 2.2 Hardware used to execute the tasks

Hardware	Specification
Processor	Intel Core i5-10500T CPU @ 2.30GHz
RAM	8.00 GB
Graphic Card	Intel UHD Graphics 630
Input Device	Mouse, Keyboard
Output Device	Computer Screen Monitor

Table 2.3 Software used to execute the task

Hardware	Specification
Operating System	Windows 10 Pro for Workstations 64-bit
Tools	Sangfor's Cyber Command, Tenable.io, Canva

2.6 Period to Complete Task

The actual internship timeline was quite different from what had been planned in Figure A.1 from Appendix A. The investigation of Sangfor's Cyber Command begins in the first week and finishes in the third week of the internship. However, the presentation about the SCC took place on November 3, 2022, during Week 5. As a result, Week 5 was used to complete the presentation preparation. Meanwhile, development of DNS Application System was spend in Week 2 until Week 3. Then, the vulnerability assessment evaluation using Tenable.io starts on Week 5 and continues until Week 9. Weeks 10 to 13 were spent creating the cybersecurity guidelines poster. To view the main task Gantt chart, please refer to Figure A.2 in Appendix A.

2.7 Theoretical and Practical Knowledge Used

To finish the project, three different pieces of knowledge are required. Knowledge of operating system and command-line come first, then network security control and threat awareness.

2.7.1 Knowledge of Operating Systems and Command-line

Strong familiarity with operating systems like Windows, Linux, and Mac OS is important for a cybersecurity specialist. During the investigation of SCC, Ubuntu was used to launch an attack on the UMK server network. The attack was carried out to monitor the SCC's response to the attack. The "nmap" command line and the IP address of the UMK server were used in the attack. Nmap is a network scanner that sends packets and analyses responses to discover hosts and services on a computer network (Ferranti, 2018). As a result, it was classified as "Port Scan" on SCC.

2.7.2 Network Security Control

The term "network security control" describes a variety of techniques used to improve network security (Panhalkar, 2019). The project requires an understanding of how the UMK network, NDR, and vulnerability assessment work. Since SCC is considered an NDR, understanding the basics of NDR is important when investigating the SCC. Moreover, recognizing security policy violations, the type of attack, and network anomalies are necessary for the SCC investigation. It is also important to be familiar with the use of firewalls, NDR, and virtual private networks (VPNs). Following that, Tenable.io is a vulnerability assessment tool that necessitates network knowledge. The ability to configure network and agent scans is required. Along with it, Tenable.io's mediation process aids in reducing the computer's vulnerability.

2.7.3 Threat knowledge

To protect against any cybersecurity attack, it is crucial to know the enemy. Being knowledgeable about the threat landscape is helpful for cybersecurity defense strategy. Therefore, obtaining cybersecurity information to create guidelines helps in keeping on top of the latest cyberattack. Thus, a strategy for defense can be developed to mitigate risks. That's how the poster was made. The poster warns users to be cautious and explains how to defend themselves from any attack.

2.8 Problems Faced

This part will describe the issues encountered when executing the task, applying general skills, and managing its implementation.

2.8.1 Task execution

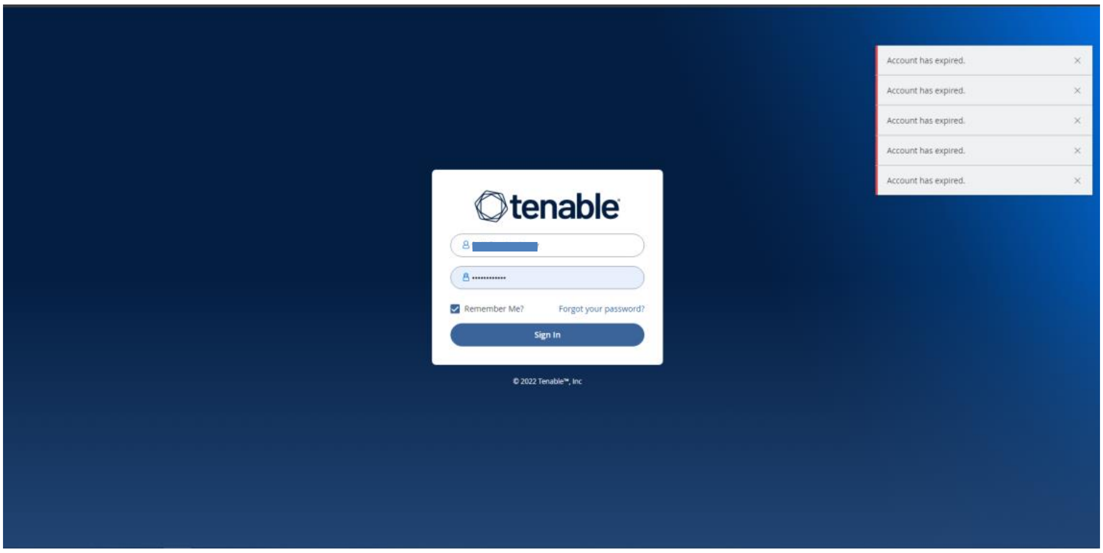
NDR and vulnerability assessments are being used for the first time in my life to monitor the network. To begin with, a lack of NDR and vulnerability assessment understanding leads to confusion. Before proceeding with the investigation, a revision must be made. During the investigation on SCC, numerous information was provided on the SCC page. So, it is clueless about where to begin or what to observe. Additionally, not much can be studied because some of the SCC's functionality cannot be accessed or changed. Following that, when scanning on Tenable.io, a configuration is required. The initial scan requires assistance from nearby staff to teach it. Moreover, it also requires a specific IP address known only to the staff. Finally, during the Tenable.io mediation, some of the suggested solutions were unable to resolve the vulnerability. Furthermore, certain instructions are difficult to understand. As a result, one vulnerability in the computer has not been fixed. Next, the DNS application system develops using the CFM language and the Lucee server, which were not taught in the classroom. As a result, extensive research has been performed to complete the development of the DNS application system.

2.8.2 General Skills

An attack was launched using Linux to test the SCC response to an attack. The UMK server is attacked using the "nmap" command, also known as port scanning (reconnaissance). However, it is tough to perform the attack because Nmap knowledge was forgotten. To save the results of the attack, basic command line knowledge is also necessary. Therefore, to execute and save the attack result, a revision is required. Also, many commands are used to obtain information about the targeted website during the first step of penetration testing. Besides that, programming knowledge is necessary for the DNS application form implementation to ensure that the code is executed properly. However, because this is the first time using the CFM language, the system constantly displays an error message, especially when attempting to retrieve information from the database. As a result, fixing the issue is a lengthy process.

2.8.3 Implementation Management

When attempting to log into the Tenable.io website, it sometimes displays that the account password has expired as shown in Figure 2.26. It must be renewed, and getting the account takes time. As a result, the vulnerability assessment must be delayed until it can be accessible. Furthermore, there are times when the scanning process fails. Although it displays that the scanning is complete, the warning states that it has not been scanned. A single scan can take up to three hours. Thus, time is wasted on unsuccessful scanning.



Account has expired.

Account has expired.

Account has expired.

Account has expired.

Account has expired.

Figure 2.26 The account expiration alert

Furthermore, since the DNS application system applies the CFM language, which is rarely used by any organization, resources are limited. There isn't much information available, not even while browsing material using Google. The only way to fix the coding error is to try an error.

2.9 Conclusion

This chapter discusses the precise details of the main tasks carried out during the internship, including the investigation of NDR, vulnerability assessment, and preparation of cybersecurity guidelines. The chapter also discusses the issues that arise when carrying out the task, applying general abilities, and managing its implementation. Although the internship environment is difficult to adjust to, it provides the first true taste of the working world.

CHAPTER 3

OVERALL INFORMATION OF THE INDUSTRIAL TRAINING

3.1 Introduction

This chapter will provide detail about the skills that have improved as a result of the industrial training at CCI UMK. This chapter also includes the reference resources used when carrying out a task and constructive feedback on overall task completion.

3.2 Knowledge Gained and Skill Improvement

Participating in an internship will give an individual real-world experience and broaden knowledge. A lot of information was gained throughout the internship from the supervisor, staff, and reference materials. Network security control, programming, command-line, and communication skills were also strengthened during industrial training.

3.2.1 Network Security Control Skill

The research on SCC and Tenable.io increased the Network Security Control skill. Throughout the research, knowledge about how to monitor traffic in NDR had been obtained. The vulnerability assessment task also aids in learning how to set up the network scan and agent scan. Besides, the root cause of the vulnerability and ways to mitigate it was learned through the mediation process in Tenable.io. Thus, each security tool contributes in learning how to reducing the risk of cyber-attacks.

3.2.2 Programming Skill

The language and server used during the development of the DNS application system are new. Usually, while developing a web application, only PHP, JavaScript, and phpMyAdmin are used. However, CFML and Lucee are used this time. This is regarded as new information in creating a web application that could advance programming skills. Despite the restricted CFML resources available, the web application was still managed to finish due to improved programming skills. If other organization employs the same scripting language, it might be beneficial for a future career. By then, the problems in understanding the language would have lessened.

3.2.3 Command-line Skill

This skill was taught by the supervisor. To test SCC's response to an attack, the use of Linux known as Ubuntu is necessary. The supervisor explains the basic command line to conduct the Nmap attack. Nmap was used to discover the open port in the UMK server, and the results were saved. Numerous cases have proven that open ports are highly vulnerable to attack when the services that are listening to them are not patched or set incorrectly, which can result in compromised systems and networks. The command line skill then keeps getting better through self-study on penetration testing. A lot of information must be gathered during the reconnaissance stage using various command lines. Each command line has its own set of features and ways of gathering data. Therefore, doing reconnaissance during penetration testing contributed to improving this skill.

3.2.4 Communication Skill

Being in an industrial environment has improved the communication skills and confidence. Especially during the SCC presentation. Giving a speech about the SCC investigation in front of an audience requires a lot of courage. During the presentation, all of the information and findings were shared. Opinions on how to strengthen the security system at UMK Bachok were also confidently presented. On top of that, presentation and communication skills are interrelated. Presentation skills are crucial for effective communication. When presenting ideas, projects, and strategies to an audience, presentation skills enable speakers to communicate with the audience more effectively and professionally.

3.2.5 Reference Material

Most of the information used to complete the project was obtained through research using online materials, and tutorials. The internet is an excellent learning resource for students. Much information, including those related to CFML, Lucee, NDR, and vulnerability assessment, can be discovered by using the Google search engine. Google was also used for most of the investigation on SCC and Tenable.io. In addition, YouTube and Udemy both have tutorials on how to use the Nmap attack and perform a basic scan using Tenable.io.

3.3 Comments on Task Performance

Altogether, I'd like to express my gratitude to the CCI staff for their willingness to welcome me as one of them. When faced with difficulties while carrying out a task, they always offer guidance without making a fuss. They enjoy sharing their work experience and acting as a mentor. They have provided me with a wealth of knowledge and skills that will be useful in my future career. Additionally, each task's result was satisfying in many ways. All of the tasks assigned by the company supervisor were completed on time, along with a side task.

3.4 Conclusion

This chapter covered overall information about industrial training including the skills that have improved as a result of the internship, reference resources used when carrying out a task, and constructive feedback on overall task completion.

CHAPTER 4

CONCLUSION

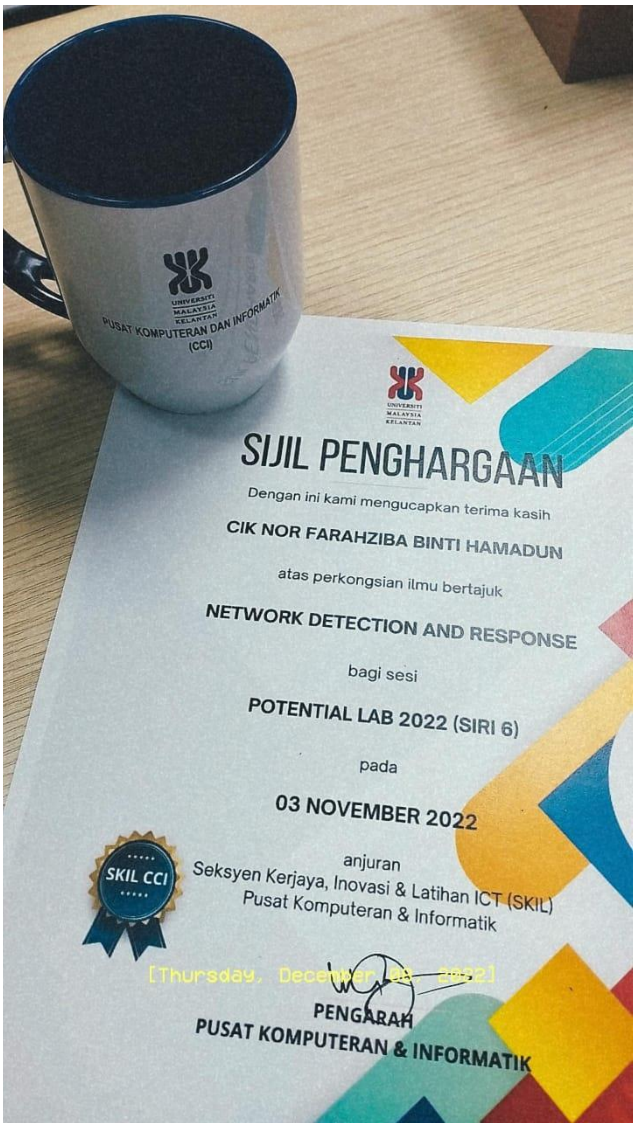
4.1 Introduction

This chapter describes the overall achievements performed and earned during the period of the 20-week industrial training. Following that are the problems and suggestions related to industrial training.

4.2 Achievements

The 20 weeks of industrial training gave me the chance to work in a real industry. It is considered the practice to apply what was learned in class to a real-world situation. From the internship, a lot of information and skill were obtained throughout the execution of the project job.

The presentation of SCC was the first success. There had been extensive research and investigation done before the SCC was introduced to the staff. Knowledge of SCC and NDR is required to produce the finest performance and deliver the presentation's message to the audience. The presentation aims to raise awareness of the value of cybersecurity and offer suggestions for strengthening UMK Bachok's cyberattack defense. It is a success because the audience is satisfied with the presentation. As a token of appreciation, the organizer gave me a certificate and one UMK cup as displayed in Figure 4.1.



UNIVERSITI MALAYSIA KELANTAN
PUSAT KOMPUTERAN DAN INFORMATIK (CCI)
SKIL CCI

UNIVERSITI MALAYSIA KELANTAN

SIJIL PENGHARGAAN

Dengan ini kami mengucapkan terima kasih

CIK NOR FARAHZIBA BINTI HAMADUN

atas perkongsian ilmu bertajuk

NETWORK DETECTION AND RESPONSE

bagi sesi

POTENTIAL LAB 2022 (SIRI 6)

pada

03 NOVEMBER 2022

anjuran
Seksyen Kerjaya, Inovasi & Latihan ICT (SKIL)
Pusat Komputeran & Informatik

[Thursday, December 08, 2022]

PENGARAH
PUSAT KOMPUTERAN & INFORMATIK

Figure 4.1 Appreciation token by the organizer

The following achievement relates to skill development. Numerous jobs have been carried out during the project and finished on time. Many skills, including command-line and network security management, programming, and communication, are all improving at the same time. The presentation and interactions with the supervisor, staff, and other trainees help to strengthen communication skills. After that, SCC traffic monitoring and Tenable.io network and agent scanning were given the chance to improve the network security control skill. In the meantime, developing DNS application system using CFML and Lucee enhanced the programming skills. Although unfamiliar with the language and server to develop the web application, the coding issue still can be fixed. The command-line skill is then attained when performing attack to UMK server to test capabilities of NDR. The skill then gets better when performing reconnaissance of the targeted website during penetration testing.

Last but not least, using Tenable.io to mediate the computer until there was just one vulnerability left is a success. Although a suggested solution has been provided, remediation is not easy since the instructions are sometimes unclear and unable to fix the issue. Thus, other resources must be used to solve the issue.

4.3 Issues and Challenges

From my point of view, there is no issue concerning the working environment except for their culture. I'm not familiar with the Kelantan dialect that is used by the majority of the people here. Aside from that, the organization provides the workspace, computer, internet, and software. The staffs and trainees here seem to be friendly and willing to assist.

However, several issues arise when the task is being carried out. First of all, it takes some time to identify what to investigate with the SCC since using NDR to monitor traffic is a new experience. Furthermore, not much can be tested out or observed because some permissions are restricted to be viewed and altered. Following that, the Tenable.io login screen always demands that the account password need to be renewed to have access to it. Obtaining a new password from the provider takes time as well. Furthermore, certain solution suggestions provided during the mediation in Tenable.io could not solve the vulnerability, and the instructions were imprecise. Furthermore, there are not enough resources available since the DNS application system uses the CFM language, which is not often used by any organization. Even when searching for information on Google, there is not much to be found. Try an error is the only way to correct the code problem. Despite this, the web application was completed thanks to improved programming skills.

Consequently, to perform all of the tasks assigned, much investigation and study are necessary. However, thanks to the assistance of the supervisor, the staff, and the internet material, all the tasks were completed successfully.

4.4 Opinions and Suggestions

From my viewpoint, if the student wants a basic understanding of cybersecurity and how to execute it, CCI UMK is a good option. Additionally, the task is not overly challenging and is pretty relaxing. However, the language used here is not the normal Malay we speak in everyday life. The majority of the staff and trainees spoke in the Kelantan dialect, which I was unfamiliar with because I am not from Kelantan. Simply put, UMK CCI is the recommended organization if the student is searching for a change in culture and leisurely work. But, if the student is seeking a more challenging job and experience, they should pick a different organization.

4.5 Conclusion

Although classroom learning is crucial, internships allow students to apply what they have learned in class in real-world practice. Through an internship, skills and knowledge are continued to grow outside of the classroom. It is possible to learn new skills and get a lot of feedback from experienced professionals. Furthermore, the knowledge gained during an internship can be applied to future careers. Therefore, gaining work experience through an internship is important to starting a job as a fresh graduate.

REFERENCES

Cloudflare. (2022). What Is Penetration Testing? What Is Pen Testing? | Cloudflare. *Cloudflare*. https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/

DistroWatch. (2019). *DistroWatch.com: Ubuntu*. Distrowatch.com. https://distrowatch.com/table.php?distribution=ubuntu

Ferranti, M. (2018, August 17). *What is Nmap? Why you need this network mapper*. Network World. https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html

imperva. (2019). *Vulnerability Assessment*. Imperva. https://www.imperva.com/learn/application-security/vulnerability-assessment/

Panhalkar, T. (2019, November 18). *Network Security Controls*. Infosavvy Security and IT Management Training. https://info-savvy.com/network-security-controls/

Rosencrance, L. (2021). *What is a vulnerability assessment (vulnerability analysis)? Definition from SearchSecurity*. SearchSecurity. https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis

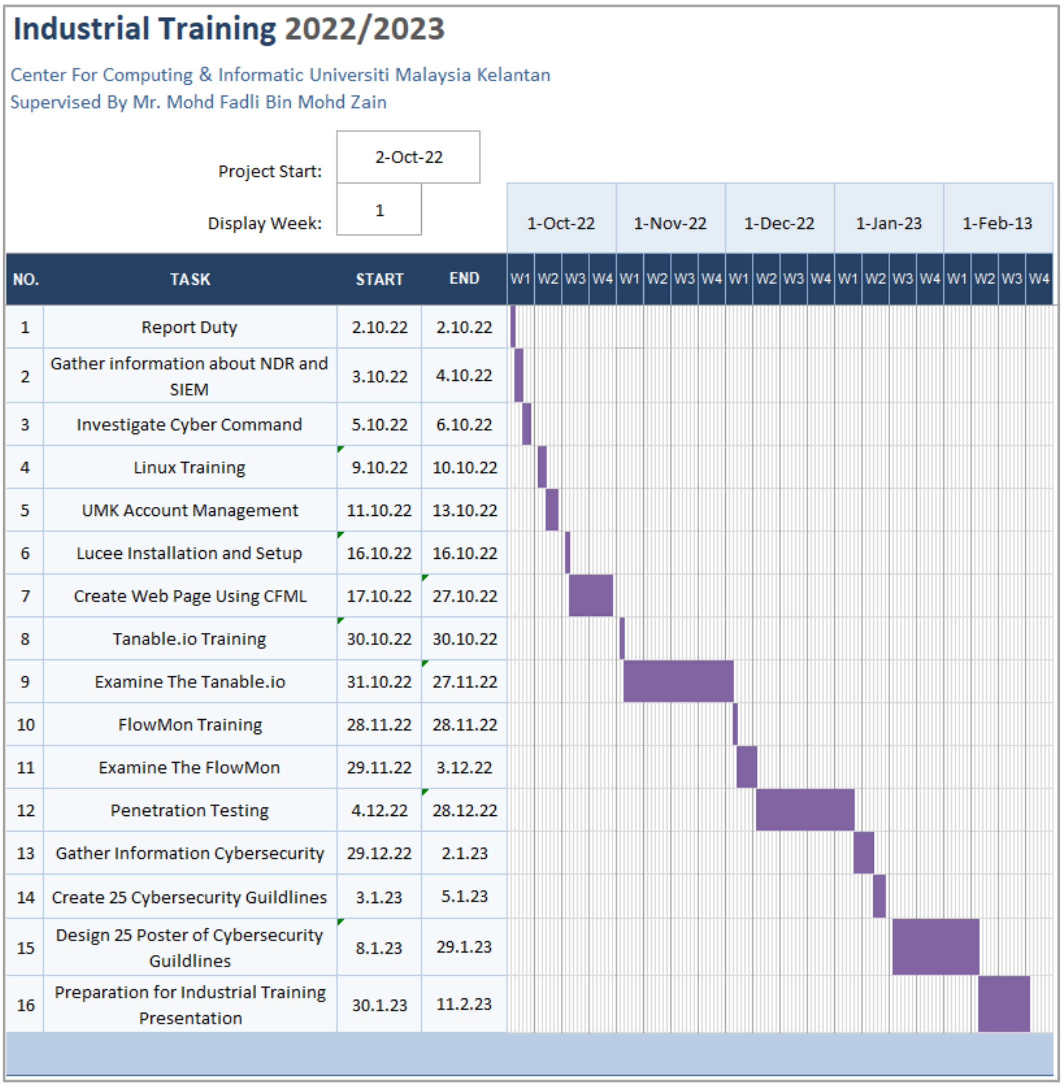
Technologies, S. (2022, November 15). *What is Network Detection and Response (NDR)?* SANGFOR. https://www.sangfor.com/blog/cybersecurity/what-is-network-detection-and-response-ndr

Tenable®. (2017, January 26). *Tenable.io FAQ*. Tenable®. https://www.tenable.com/products/tenable-io/faq

Universiti Malaysia Kelantan. (2022, December 15). *PUSAT KOMPUTERAN DAN INFORMATIK - UNIVERSITI MALAYSIA KELANTAN*. Cci.umk.edu.my. https://cci.umk.edu.my/

APPENDICES

Appendix A Industrial Training's Gantt Chart



Industrial Training 2022/2023

Center For Computing & Informatic Universiti Malaysia Kelantan
Supervised By Mr. Mohd Fadli Bin Mohd Zain

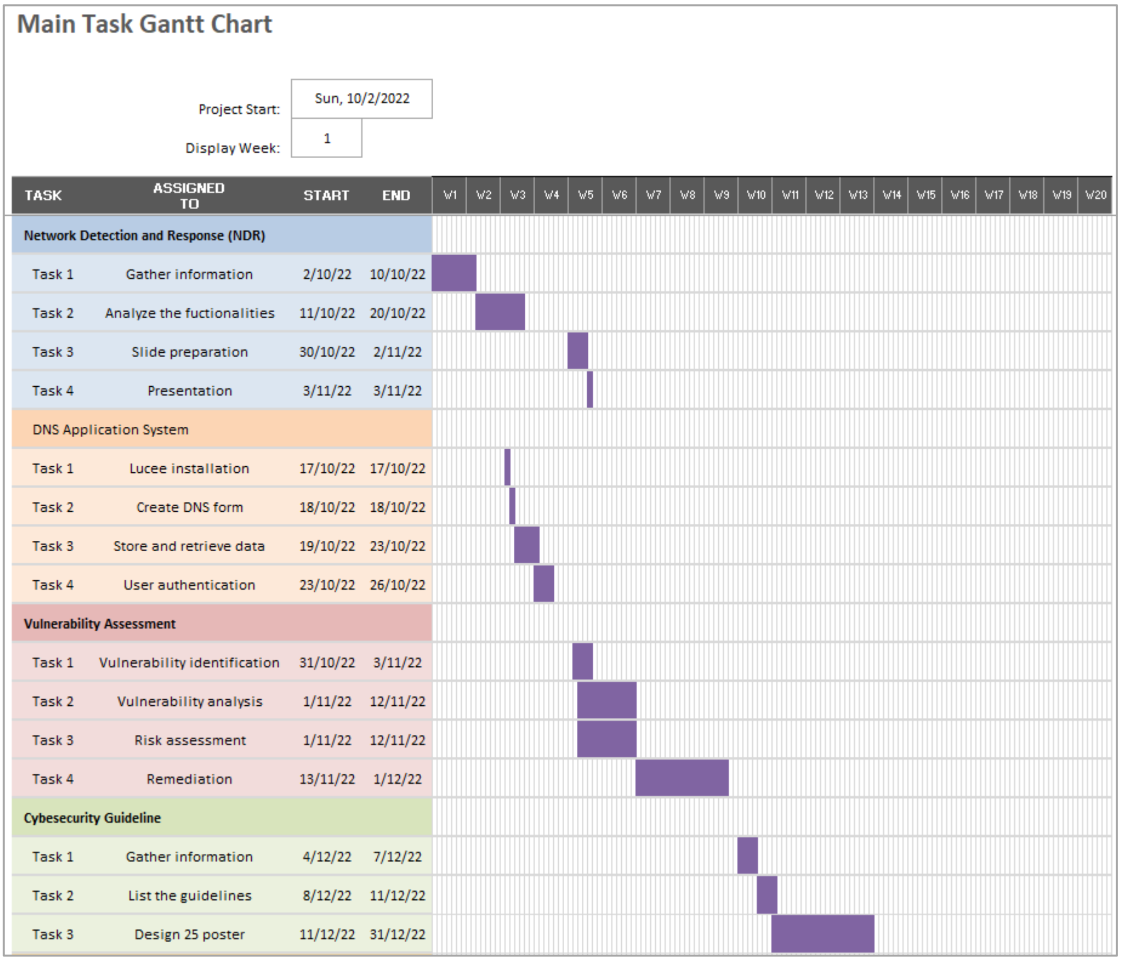
Project Start: 2-Oct-22

Display Week: 1

1-Oct-22 | 1-Nov-22 | 1-Dec-22 | 1-Jan-23 | 1-Feb-13

NO.	TASK	START	END
1	Report Duty	2.10.22	2.10.22
2	Gather information about NDR and SIEM	3.10.22	4.10.22
3	Investigate Cyber Command	5.10.22	6.10.22
4	Linux Training	9.10.22	10.10.22
5	UMK Account Management	11.10.22	13.10.22
6	Lucee Installation and Setup	16.10.22	16.10.22
7	Create Web Page Using CFML	17.10.22	27.10.22
8	Tanable.io Training	30.10.22	30.10.22
9	Examine The Tanable.io	31.10.22	27.11.22
10	FlowMon Training	28.11.22	28.11.22
11	Examine The FlowMon	29.11.22	3.12.22
12	Penetration Testing	4.12.22	28.12.22
13	Gather Information Cybersecurity	29.12.22	2.1.23
14	Create 25 Cybersecurity Guildlines	3.1.23	5.1.23
15	Design 25 Poster of Cybersecurity Guildlines	8.1.23	29.1.23
16	Preparation for Industrial Training Presentation	30.1.23	11.2.23

Figure A.1 The overall task Gantt chart for internship



Main Task Gantt Chart

Project Start:	Sun, 10/2/2022
Display Week:	1

TASK	ASSIGNED TO	START	END
Network Detection and Response (NDR)			
Task 1	Gather information	2/10/22	10/10/22
Task 2	Analyze the fuctionalities	11/10/22	20/10/22
Task 3	Slide preparation	30/10/22	2/11/22
Task 4	Presentation	3/11/22	3/11/22
DNS Application System			
Task 1	Lucee installation	17/10/22	17/10/22
Task 2	Create DNS form	18/10/22	18/10/22
Task 3	Store and retrieve data	19/10/22	23/10/22
Task 4	User authentication	23/10/22	26/10/22
Vulnerability Assessment			
Task 1	Vulnerability identification	31/10/22	3/11/22
Task 2	Vulnerability analysis	1/11/22	12/11/22
Task 3	Risk assessment	1/11/22	12/11/22
Task 4	Remediation	13/11/22	1/12/22
Cybesecurity Guideline			
Task 1	Gather information	4/12/22	7/12/22
Task 2	List the guidelines	8/12/22	11/12/22
Task 3	Design 25 poster	11/12/22	31/12/22

Figure A.2 The main task Gantt chart for internship

Appendix B Sangfor's Cyber Command (SCC)

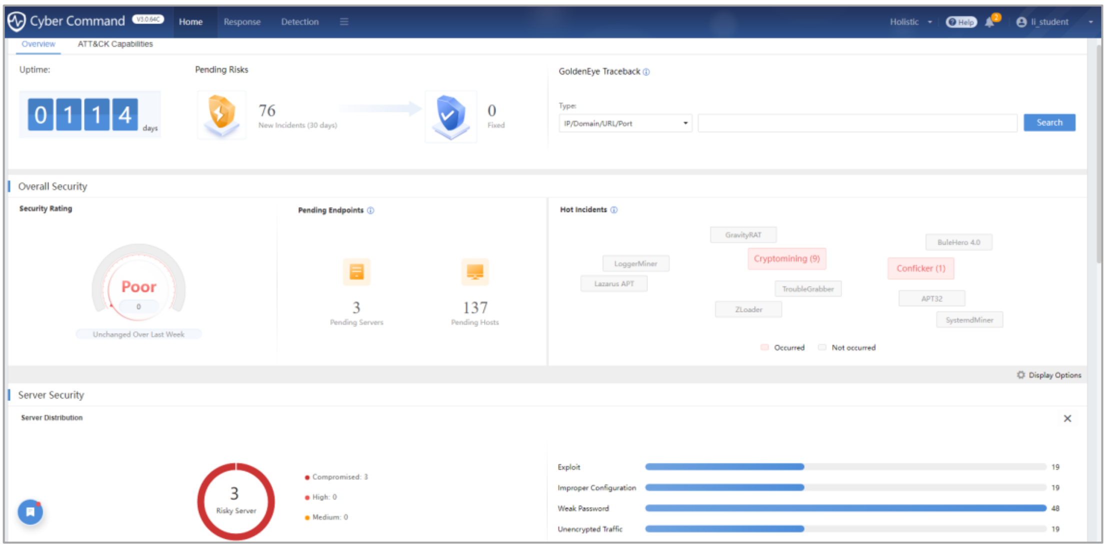


Figure B.1 SCC's overview page

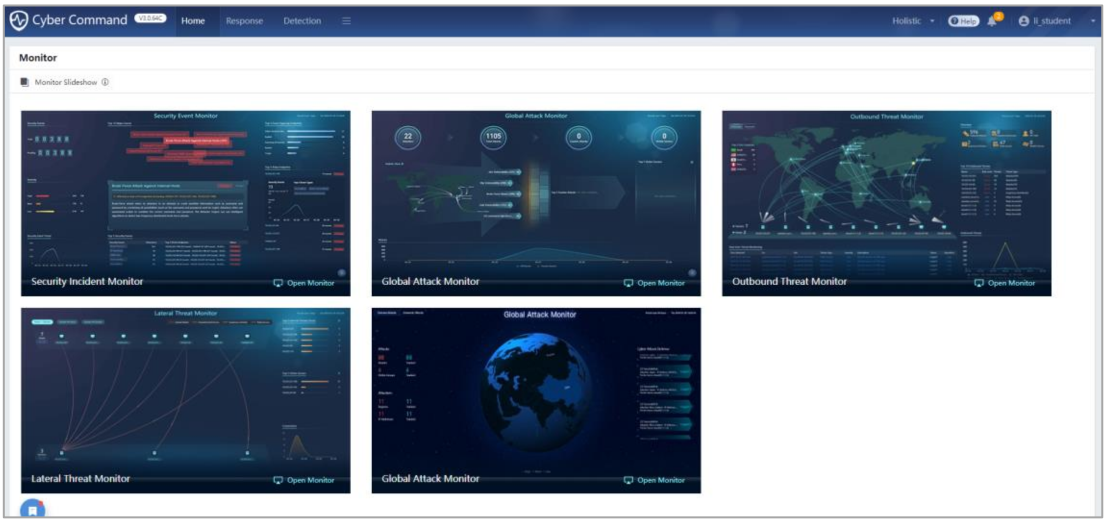
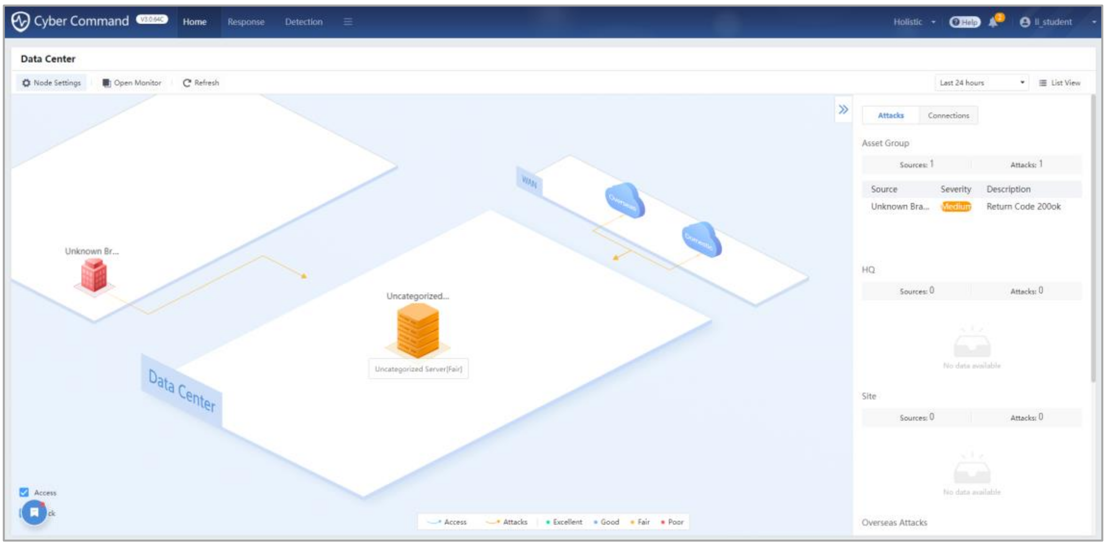


Figure B.2 SCC's monitor page



Data Center

Asset Group

Sources: 1 Attacks: 1

Source	Severity	Description
Unknown Bra...	Medium	Return Code 200ok

HQ

Sources: 0 Attacks: 0

No data available

Site

Sources: 0 Attacks: 0

No data available

Overseas Attacks

Figure B.3 SCC's data center page

INDUSTRIAL TRAINING ACHIEVEMENTS AND CHECKLISTS

Sekretariat Latihan Industri
Sekolah Komputeran,
Universiti Teknologi Malaysia,81310 SKUDAI, JOHOR
Fax: 07-5565044 Tel: 07-5532008

INDUSTRIAL TRAINING ACHIEVEMENTS

(This form must be filled by student and must be attached in the Industrial Training report)

Student's Name : Nor Farahziba Binti Hamadun
Organisation : Centre for Computing & Informatics (CCI)

No.	**Task**	**Month of Task Achieved**				
	(List all tasks have been completed)	**Month 1**	**Month 2**	**Month 3**	**Month 4**	**Month 5**
1	Investigation on Network Detection and Response (NDR) and Sangfor's Cyber Command (SCC)	√				
2	DNS Application System using CFML and Lucee	√				
3	Do a presentation about Sangfor's Cyber Command (SCC)		√			
4	Perform vulnerability assessment in Tenable.io (network scanning, agent scanning, and remediation)		√			
5	Create 25 cybersecurity guidelines in the form of a poster			√		
6	Self-learning in penetration testing using PortSwigger and Hacker101 website				√	
7	Perform reconnaissance (stage 1 in penetration testing)					√

Deliverable/Training reflection

(Outcomes that have been achieved)

- Monitor the network in SCC and share findings regarding the SCC to the staff
- Develop DNS Application System using CFML and Lucee
- Perform vulnerability assessment using Tenable.io (scanning and remediation)
- Create 25 posters of cybersecurity guidelines

Student Signature: ______________________ Date: 8/2/2023

Approval

Organisation’s Supervisor:	Faculty Supervisor:
………………………………	………………………………
(Signature)	(Signature)
Name: Mr Mohd Fadli Bin Mohd Zain	Name:
Date: 9/2/2023	Date:

INDUSTRIAL TRAINING CHECKLISTS (PLACEMENT)

No.	**Activities/Tasks**	**Tick (√)**	**Endorse by and date**
1.	Report Duty To The Organization Approved by faculty	√	2/10/2022
2.	E-mail Report Duty Verification (BLI-1D) to faculty supervisor.	√	6/10/2022
3.	Upload Report Duty Verification (BLI-1D) in e-learning for course code SCS*4114.	√	3/11/2022
4.	Contact faculty supervisor to inform the job scope and organization information	√	18/10/2022
5.	Fill in organization supervisor information survey in ITS	√	26/10/2022
6.	*Update of Industrial Training site (address). Inform faculty supervisor and JKL, if any changes.*		
7.	Updating Industrial Training Logbook online – daily basis	√	
8.	Ensure that organization supervisor able to login to ITS successfully (Organization supervisor get ITS userid and password).		
9.	Faculty Supervisor Visit. Date: 5 February 2023	√	5/2/2023
10.	Industrial Training Presentation.	√	5/2/2023
11.	Performance evaluation by organisation supervisor. Online or *submission BLI-2B during supervisor visit.*	√	12/2/2023
12.	Submission of Industrial Training Logbook.	√	12/2/2023
13.	Submission of Industrial Training Report with checklist and achievement form as Appendix.	√	12/2/2023
14.	Fill in Industrial Training Performance Evaluation by student (BLI-1E) in ITS.		
15.	End Industrial Training	√	16/2/2023

Note:

1. *Italic activities are optional depending on student situation.*

IIMPORTANT: This checklist must be put as attachment in the industrial training report.