Appendix 4A

UNIVERSITI TEKNOLOGI MALAYSIA

FACULTY OF COMPUTING

INDUSTRIAL TRAINING REPORT

<VULNERABILITY ASSESSMENT AND ICT ACCESS CONTROL REGISTRATION SYSTEM>

BY

FATEEN NASHUHA BINTI YUSOF

4 SECR

COMPUTER SCIENCE (COMPUTER NETWORKS & SECURITY)

TRAINING PLACE :	CENTER FOR COMPUTING AND INFORMATIC, UNIVERSITY MALAYSIA KELANTAN, 16300 BACHOK KELANTAN
TRAINING PERIOD :	2nd October 2022 – 16th February 2023
SUPERVISOR :	MR MOHD FADLI BIN MOHD ZAIN
REPORT DATE :	9 FEBRUARY 2023

ABSTRACT

Industrial training have become an essential way for candidates to build a successful career with expert guidance. Internships teach students soft skills such as communication, critical thinking, teamwork, and problem-solving, as well as technical skills that may be useful in their future careers. This report details the 20 weeks of internship experience from 2nd October 2022 until 16th February 2023 at the Center for Computing and Informatics at the University Malaysia Kelantan (UMK) in Bachok, Kelantan. Mr Mohd Fadli bin Mohd Zain is the company supervisor, and Dr Noorfa as my faculty supervisor was assigned me as an internship trainee at the information and communication technology (ICT) security and data centre team. During the industrial training period, there are various of IT-related job tasks were assigned, including vulnerability assessment, monitoring cyber threat in local network, design cybersecurity awareness posters and the development of an ICT access control registration system particularly for UMK used. This report includes contains an explanation of the organization's background, information on the main and additional tasks during the industrial practical, and the conclusion on the industrial training journey. Besides, this report also includes the problems that have been encountered as well as the recommendations that can be used as a reference for the industrial training process in the future. By completing the assigned tasks, the valuable experiences and new knowledges were gained that would not have obtained in class for sure. Each task was completed and exposed to the real work environment.

ABSTRAK

Latihan amali telah menjadi cara penting untuk calon membina kerjaya yang berjaya dengan bimbingan pakar. Latihan amali mengajar pelajar kemahiran insaniah seperti komunikasi, pemikiran kritis, kerja berpasukan, dan penyelesaian masalah, serta kemahiran teknikal yang mungkin berguna dalam kerjaya masa depan mereka. Laporan ini memperincikan pengalaman latihan selama 20 minggu dari 2 Oktober 2022 hingga 16 Februari 2023 di Pusat Pengkomputeran dan Informatik di Universiti Malaysia Kelantan (UMK) di Bachok, Kelantan. En Mohd Fadli bin Mohd Zain ialah penyelia syarikat telah menugaskan saya sebagai pelatih amali di pasukan keselamatan dan pusat data teknologi maklumat dan komunikasi, dan Dr Noorfa sebagai penyelia fakulti. Terdapat pelbagai tugas pekerjaan berkaitan IT telah diberikan, termasuk menilai kelemahan dalam rangkaian computer, pemantauan ancaman siber dalam rangkaian tempatan, reka bentuk poster kesedaran keselamatan siber dan pembangunan sistem pendaftaran kawalan akses ICT khususnya untuk digunakan oleh UMK. Laporan ini mengandungi penjelasan tentang latar belakang organisasi, maklumat mengenai tugas utama dan tambahan semasa amali industri, dan kesimpulan tentang perjalanan latihan industri. Selain itu, laporan ini juga merangkumi masalah-masalah yang telah dihadapi serta cadangan-cadangan yang boleh dijadikan rujukan untuk proses latihan industri pada masa hadapan. Melalui tugasan yang diberikan, pengalaman berharga dan pengetahuan baru yang diperolehi sepanjang Latihan idustri pastinya tidak akan diperolehi di dalam kelas. Setiap tugasan telah disiapkan dan didedahkan kepada persekitaran kerja sebenar.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Company Background

University Malaysia Kelantan or known as UMK is the only autonomous public institution of higher learning was established in the state of Kelantan. It is one of the components in 9th Malaysia Plan to support the development of quality human capital in the country's higher education sector. On June 14, 2006, the Cabinet Meeting approved the establishment of the university. Professor Dato' Ir Dr Zainai bin Mohamed was appointed as the first Vice Chancellor of UMK on 1st October 2006. Currently, UMK operates in three campuses from its main campus located in Bachok, second campus in Jeli and the last one is a temporary campus in Pengkalan Chepa.

The cabinet has mandated that the curriculum philosophy at UMK be based on entrepreneurship and enterprise education in all study programmes. After the consideration, the UMK philosophy was improved by focusing on six components includes entrepreneurial education, foreign language, ICT as an enabler, lifelong learning, quality human capital, and uniqueness and relevance. The goal is to develop high-quality human capital with a first-class mentality and exemplary entrepreneurship characteristics. It is hoped that this will contribute to global prosperity by improving the capability and capacity of Small and Medium Enterprises (SME), as well as the development of a commercial society that is highly entrepreneurial.

However, the university is rapidly expanding its globalisation efforts in the field of entrepreneurship to become number one (1) entrepreneurial university in Malaysia. Therefore, the university's taglines, "Entrepreneurship is Our Thrust" and "Entrepreneurial University," are widely used to promote the university's philosophy. As an entrepreneurial university, UMK has fostered an entrepreneurial skills and

environment among students and faculty through its teaching and learning activities, so that they will be able to develop and apply those skills in the real world. Presently, UMK consists of 9 faculties with variety of main courses. The main objectives of UMK's establishment includes:

1) To gain a better understanding of the earth's natural resources, environmental change, and sustainable science through integrated and scientific research.
2) To create a conducive, fair, and productive working environment, as well as great teamwork, which will greatly support basic research.
3) To integrate earth science and other disciplines in academic and intellectual problem solving for the community.
4) To strengthen the relationship between university faculties through university alumni and cooperative networks.
5) Increase external grants and support for research, education, and expectation.

1.2 Details of Organization Supervisor

Table 1.1 shows the details of my organization's supervisor:

Name	Mr. Mohd Fadli bin Mohd Zain
Position	Head of Data Center and ICT Security unit
Telephone Number	+6 019-955 7173
Email	fadli@umk.edu.my
Office	Center for Computing and Informatic (CCI), UMK

Table 1.1 Organization's Supervisor Details

1.3 Organization Structure of CCI

The Figure 1.1 below shows the organization structure for (CCI) department in UMK.

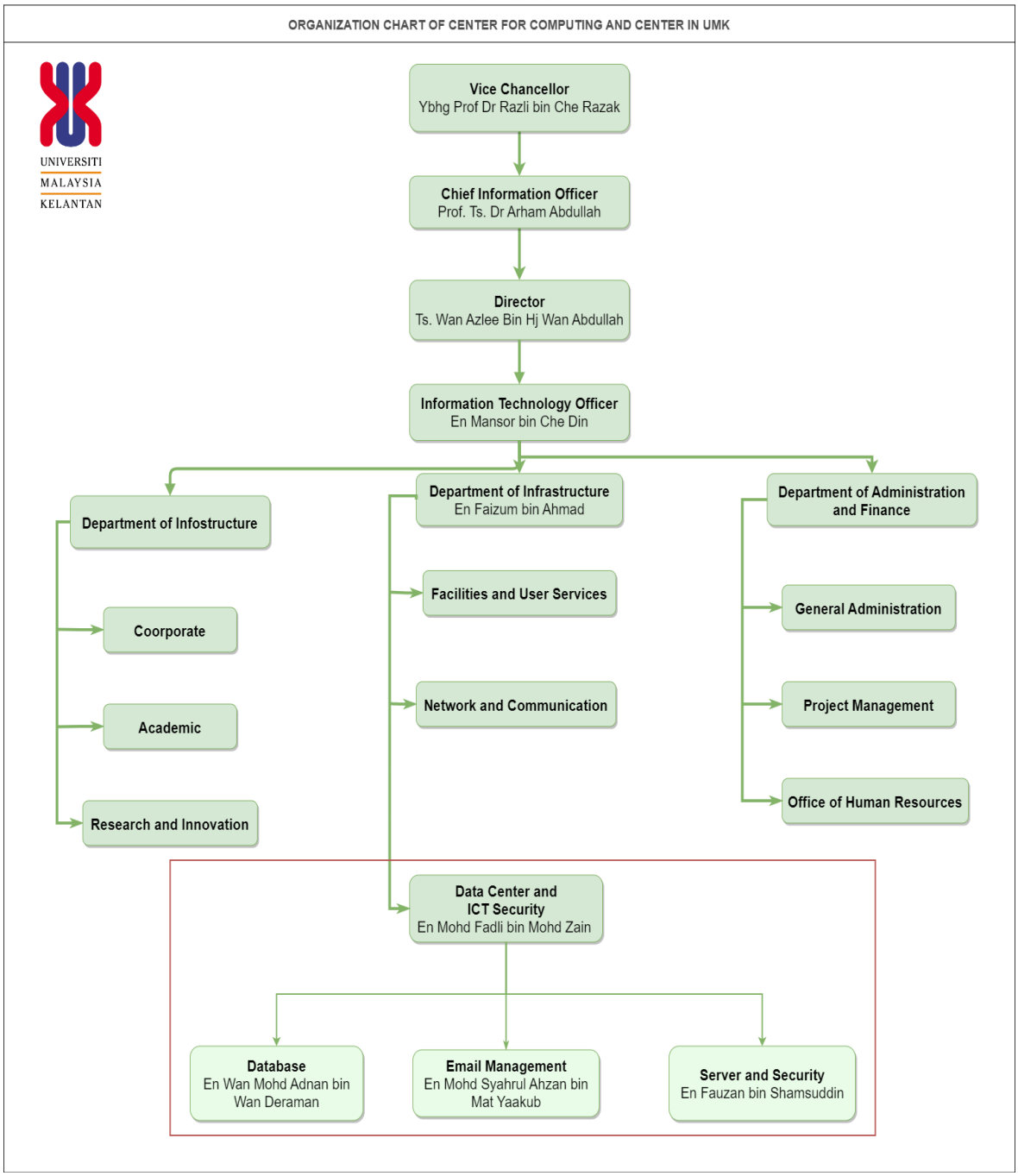


Figure 1.1 Organization Chart in CCI

1.4 Data Center and ICT Security unit, Infrastructure department

The Computer & Informatics Centre (CCI), formerly known as the Infra & ICT Department was established in early 2007. This CCI serves as a catalyst and enabler in UMK's vision and mission of producing quality human capital later. Here, they consist of more than 50 staffs which includes director, information technology officer, admins, full-time staffs, part-time staffs, and internship students. In UMK, CCI was divided into three (3) departments that are Administration and Finance, Infostructure, and Infrastructure.

1.4.1 Objectives of CCI

CCI has a vision to become an institute for the development of expertise, curriculum, research, and innovation, as well as a provider of quality ICT infrastructure and services in line with the development of global advanced ICT as a Teaching Knowledge Factory to face a dynamic and challenging industrial market environment, in addition to supporting the national policy to develop human capital based on entrepreneurship education through the application of the concept of Technology-Based Learning. Thus, UMK's CCI is designed to enhance the ICT operation with few objectives includes:

1) **CCI was established as ICT Expert Service Centre**
    a. To make research, ICT development and innovation
    b. ICT and operational expertise services
    c. To develop professional team of ICT

2) **ICT strategic planning and development**
    a. Sharing areas of expertise from industry and academic
    b. Regulate and manage the committee under ICT

3) **ICT revenue generation mechanism**

   a. Offering ICT training, consulting services to meet human capital needs and competency enhancement

4) **Collaboration of academic and professional expertise in the field of ICT**

   a. Involve academic and industry expertise and experience in the development and improvement of the University's ICT services

5) **Improve the quality of ICT services**

   a. The use of the latest technology in supporting the University's business

1.5 Infrastructure department, Data Center and ICT Security unit

The infrastructure department has been divided into three units, which are Data Center and ICT security, Facilities and User Services, and Network and Communication. As a student who has network and security computer background, I was assigned to Data Center and ICT security unit that was led by Mr. Mohd Fadli, and become the industrial training supervisor. There are another three (3) staffs who works together under this unit with slightly different job scopes which are Mr. Wan Mohd Adnan, Mr. Fauzan and Mr. Mohd Syahrul Ahzan.

1.5.1 Services by Infrastructure department

The infrastructure department is responsible for proactive administration and management of technology tools. This includes the ability to monitor for errors and issues, track fixes, and trace all errors back to their origins. The goal of IT infrastructure is to provide information technology teams with the structure they need to efficiently manage all company's technology and tools. It is done with the goal to minimize product and system downtime while also providing security and scalability.

This department most needed to support and improve the various aspect in computing. Infrastructure department in UMK are provided few services included:

1) operation and maintenance of data centers
2) management of ICT services
3) email management
4) network management
5) maintenance for physical security equipment

1.6 Gantt Chart of Training Program

On 2nd October 2022, I was registered myself at CCI, UMK and have been introduced to the whole staff in Infrastructure department. At the beginning of internship, student was asked to study about the Cyber Command that used Network Detection and Response or called as NDR solutions. On the next day, the team offer for getting familiar with new programming language which is ColdFusion Markup Language (CFML) and Lucee is a server application for CFML. Then, I have tried exploring and creating a simple system for UMK which is ICT access control registration form using those CFML.

After that, the supervisor invited to join a customer training for Tenable.io with the representative from the company during week 5. Tenable.io use a scanner to scan and identify if any vulnerabilities occur in a network using Nessus sensor likes Nessus Agent. The next activity is participating in a marketing meeting for a network monitoring system from Flowmon company. The participants involved in this meeting are staff from infrastructure department and representative form Flowmon. It was a great experience to see how professional teams discusses the project ideas, best recommendations, and the outcomes. In addition, Mr Fadli also planned for internship students to explore about another security technology known as Extended Detection Response (XDR).

Aside from that, the supervisor also asked to provide some material such as poster or guideline regarding ICT security awareness based on the current issues. The goal of this task is to raise the awareness among the internet users, so that they can be more alert and careful when using internet or any technology since there are so many cyber malwares on nowadays such as ransomwares. Finally, Mr Fadli also scheduled to participate in a penetration testing activity with the team later during week 12. All these planning was depicted in a Gantt chart in Figure A.1 of Appendix A.

1.7 Conclusion

In conclusion, the first chapter has discussed the organization’s background and history that also includes the company's department where my training will take place for 20 weeks. In addition, the planned purposed by my supervisor for the practical training program was briefly discussed in the provided Gantt Chart.

CHAPTER 2

PRACTICAL TRAINING PROJECT

2.1 Introduction

This chapter discussed the main projects that were completed within the internship period that is 20 weeks. It will include a brief explanation of the steps involved in completing the projects. The main projects that I worked on during industrial training are vulnerability assessment or called as VA project and developing on front-end system development for ICT Access Control registration form that will used by UMK. However, there are another task that have been done which includes designed 25 cybersecurity awareness posters, wrote an article with the topic “Future Technology” prediction in healthcare, explored Network Detection and Response (NDR) solution, as well as other additional tasks given throughout the industrial training journey at UMK.

2.2 Vulnerability Assessment (VA)

VA also known as vulnerability scans is the process of identifying and evaluating the vulnerabilities in website, application, network, or devices. These scans are typically automated and give an initial look at what could possibly be exploited by consulting a vulnerability database. VA is focused on identifying and classifying system vulnerabilities. It is essentially impossible to achieve zero false positives with an automated vulnerability assessment and it is also often fails to acknowledge complex and critical vulnerabilities.

In order to provide an unbiased view of the network environment and prevent conflicts of interest, it is preferable for external vendors to perform penetration tests

rather than internal staff. Vulnerability assessment is an essential component of penetration testing. Since the risk environment changes over time nowadays, the regular vulnerability assessments, scanning, and pen test should be routine components of a company's security assessment plan. Once user have verified the discovered vulnerabilities and identified the false positives, they must determine whether these flaws will ultimately harm the organization or not. The remediation efforts should be including an execution plan and timeline for completion.

2.2.1 Project Overview using Nessus

The main project that was assigned during the industrial training period are Vulnerabilities Assessment (VA) assisted by Data Centre and Security Computer teams and supervisor, Mr Fadli. When unauthorised changes are made to the environment, vulnerability scanners such as Nessus, Rapid7, Retina, and Qualys can notify the network defenders. In this project, Nessus scanners engine from Tenable company are used. Nessus is a remote security scanning tool that scans the organization’s infrastructure sold by Tenable Security. Nessus is referred as a "remote scanner" because it does not require installation on a computer in order to test that computer. Instead, customer can install it on just one computer and test it on as many as you want. Then, it will generate an alert if it finds any vulnerabilities that malicious hackers could exploit to gain access to any computer connected to a network.

Nessus comes with four (4) types of basic scans and allows the user to create their own custom scans for giving the user control. Nessus sensors can scan individual computers, IP address ranges, or entire subnets. Nessus have over 1200 vulnerability plug-ins that allow user to test for a single vulnerability or a set of vulnerabilities. There are few things that will be detected when running Nessus scan includes missing patches and outdated protocols, certificates, and illegal activities. Each computer has thousands of ports, some of which may or may not be used by services. Nessus works by scanning each port on a computer, determining what service is running, and then testing the service to ensure there are no vulnerabilities that could be exploited by a hacker to launch a malicious attack.

Nessus agent scanner provide a flexible method of scanning hosts in your environment without requiring hosts to provide credentials. The agent scanner able to be performed even when the hosts are not available. Consider environments where traditional malware protection, such as antivirus solutions, is not available. In this case, agent consume minimal system resources on the hosts in which it was installed while still providing adequate malware protection. VA allows the organization to remediate infrastructure and application weaknesses before threats actor can exploit it. Anyway, all team members include the internee had to install these two (2) scanners into own devices either laptop or desktop computer before start running this project as. Nessus and Nessus Agent, as shown in Figures 2.1 and 2.2, are two scanners that must be downloaded and installed from https://www.tenable.com/downloads.

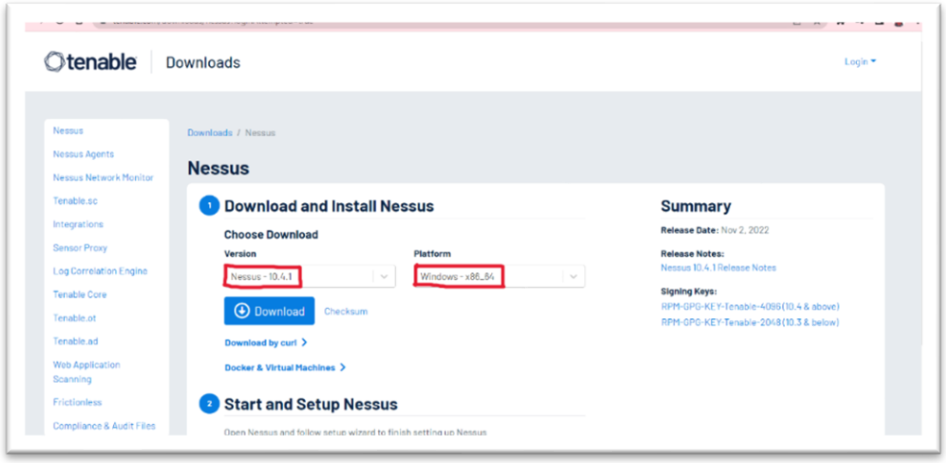


Figure 2.1 Installation of Nessus Scanner

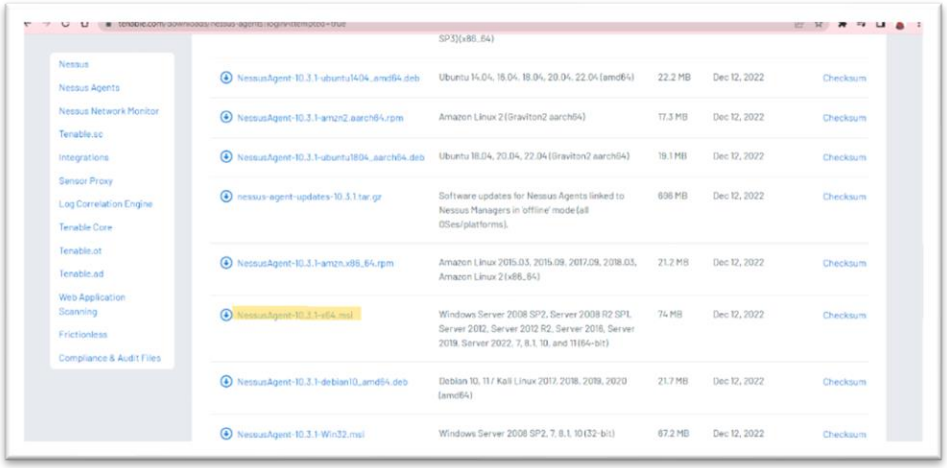


Figure 2.2 Installation of Nessus Agent Scanner

Meanwhile, Tenable sells the Nessus product line, as well as several other products that are built on Nessus and help aggregate the Nessus output in ways that are more useful to businesses. However, Tenable.io is a paid subscription service which enables the teams in an organization to share scanners, schedules, scanning policies, and scan results. Tenable.io also allows for workflow customization to give an effective vulnerability management to the customer. At Tenable, results from the Nessus scans can be integrated with penetration testing tools which makes it even easier to start penetration testing from a solid foundation. Correspondingly, the security team in an organization should perform vulnerability scans as frequently as operationally possible because the list of known vulnerabilities changes daily.

2.2.2 Objective of VA Project

Before conducting this VA project, Data Centre and Security team members include the internship students were participating in a customer training with a representative from Tenable company. The goal of this customer training is to provide an overview of the tool and to teach users how to use all the features provided by Tenable.io. After that, the supervisor, Mr Fadli was asked the internship students to perform the VA on the endpoint network only which refers to personal devices. Thus, the main objectives for this project are to be achieved are as follows:

a) To apply the theoretical knowledge VA into user's actual environment.

b) To conduct the endpoint vulnerability assessment on user device.

c) To recognize the security threats and vulnerabilities by interpreting the result of VA scanning.

d) To identify the percentage of devices in own environment either in Low, Moderate. High, or Critical health through the risk score report.

e) To resolve the vulnerabilities found based on the recommendations.

f) To get the minimum number of vulnerabilities in the personal environment.

2.2.3 Type of Work Done for VA

VA is a wireless network scans of an organization's Wi-Fi networks and one of the effective techniques to identify the security flaws in the wireless network infrastructure. There are 4 steps as presented in Figure 2.3 for conducting a proper cycle of vulnerability assessment ("What is Vulnerability Assessment", 2022) that will be detailed discussed in the following section below.

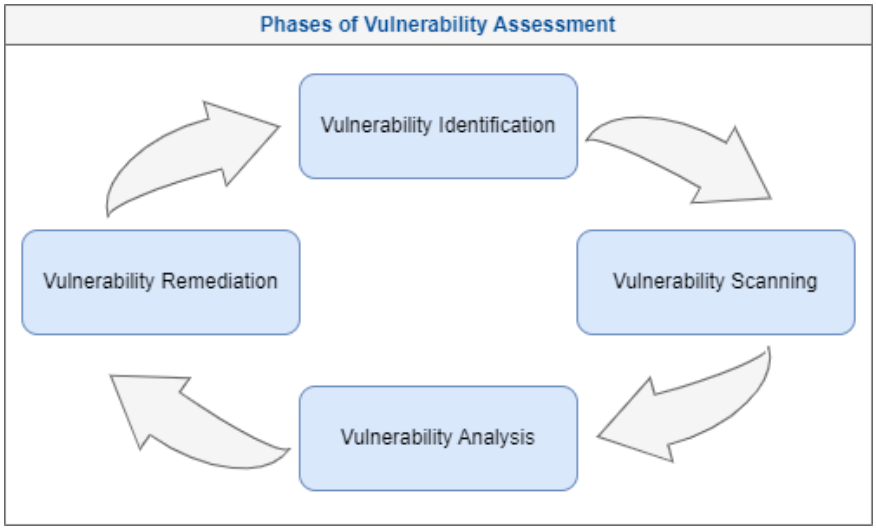


Figure 2.3 Standard VA process

2.2.3.1 Phase 1: Vulnerability Identification

The risk identification process begins with identifying all assets in a company's information system. Following that, conducting the analysis will determine the actual risk that each asset faces. Vulnerability scanners identify various assets within the network, including servers, laptops, firewalls, printers, containers, firewalls, and constantly collect the operational details. As far as concerned by the supervisor, he requested the internship students to do endpoint vulnerability scanning towards personal device through wireless network of this organization's which refers to UMK Wi-Fi. VA on endpoint provides a centralized view of device patching in user's environment and then display the risk posture of each endpoint. Figure 2.4 shown the IP address of 192.168.56 that was get from command "ipconfig" in command prompt.

```
Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a90a:dc24:a9cf:1c0%2
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

Figure 2.4 Get the IP Address of UMK Wi-Fi

2.2.3.2 Phase 2: Vulnerability Scanning

Conducting a network vulnerability scanning allows organizations to detect flaws in their systems before attackers do. The goal of this step is to rank each vulnerabilities severity score by security analysts. Before that, an agent group with named as "Intern" was created. The IP address of 192.168.56.0/24 is used for this Nessus agent group. The detail of scanning result can be seen in Figure 2.5 below. All 256 hosts addresses including the network address and broadcast address in the network that will use to send requests data over the internet will be scanned by the Nessus agent scanner. Even though each vulnerability scanning tool automatically prioritizes vulnerabilities, certain types of vulnerabilities should be prioritized. Moreover, a network basic scan template was chosen when to launch this scanning. During the back-and-forth problem-solving between teams, numerous follow-up scans are usually performed until all vulnerabilities that need to be mitigated no longer appear in the reports.

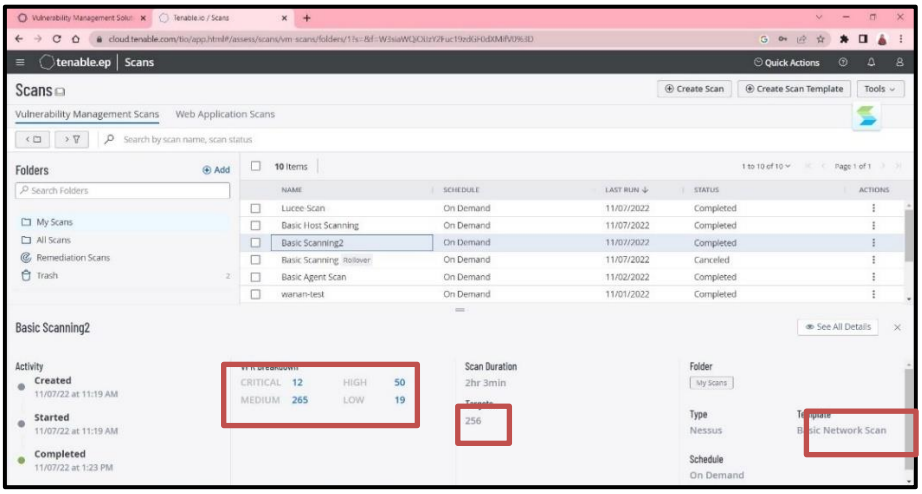


Figure 2.5 Result of Vulnerability Scanning

2.2.3.3 Phase 3: Vulnerability Analysis

The goal of this step is to determine the source and root cause of the vulnerabilities discovered in step one. The scanning tool, Tenable.io will generate a detailed report with various risk ratings and vulnerability scores. Most tools assign a numerical score using a Common Vulnerability Scoring System (CVSS). A careful examination of these scores will reveal which vulnerabilities must be addressed first and it will categorize intro critical, high, medium, and low level. In Tenable, each potential vulnerability is sequentially identified, tested, evaluated, and given a priority score based on following factors:

- How the component is effect?
- Is it the data is compromised?
- The likelihood and ease of a hack?
- How severe the attack can be?
- What the potential loss that could arise from the vulnerability?

For example, if a public exploit for a vulnerability found in a system, giving priority to that vulnerability should take precedence over other vulnerabilities discovered that are exploitable but require far more effort. It identifies and quantifies the security weaknesses including the application software, hardware, and network. As highlighted in Figure 2.6 below, there is an example of critical level vulnerabilities at endpoint and it was listed based on the score in Vulnerability Priority Rating (VPR).

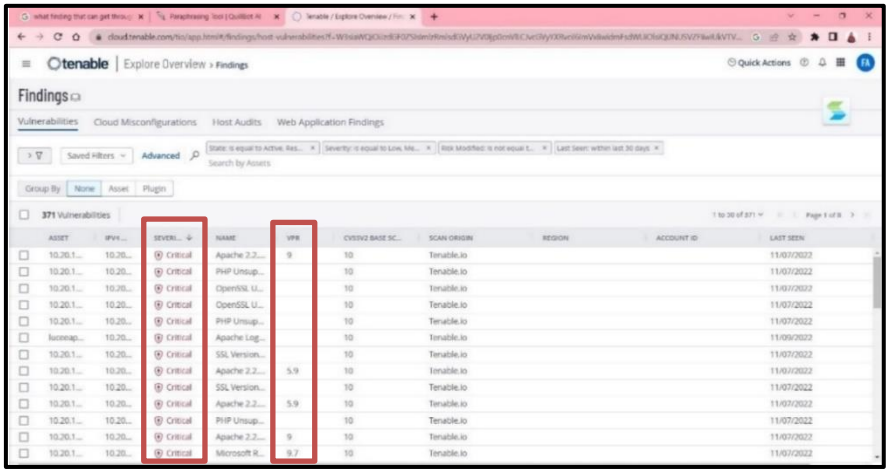


Figure 2.6 Lists of Vulnerabilities in Critical level

2.2.3.4 Phase 4: Vulnerability Remediation

After interpreting the results, information security personnel should prioritize the mitigation of each detected vulnerability and collaborate with IT personnel to communicate mitigation actions. The detailed instructions on how to solve those vulnerabilities as soon as possible also were provided. Several remediation things were done during this phase to reduce the number of vulnerabilities, particularly those with critical and high severity. Remediating process includes updating some application to the latest version supported by the laptop and operating system, configuring some files, and implementation of vulnerability patch. The differences in number of vulnerabilities before and after remediation can be observed in Figures 2.7 and 2.8.

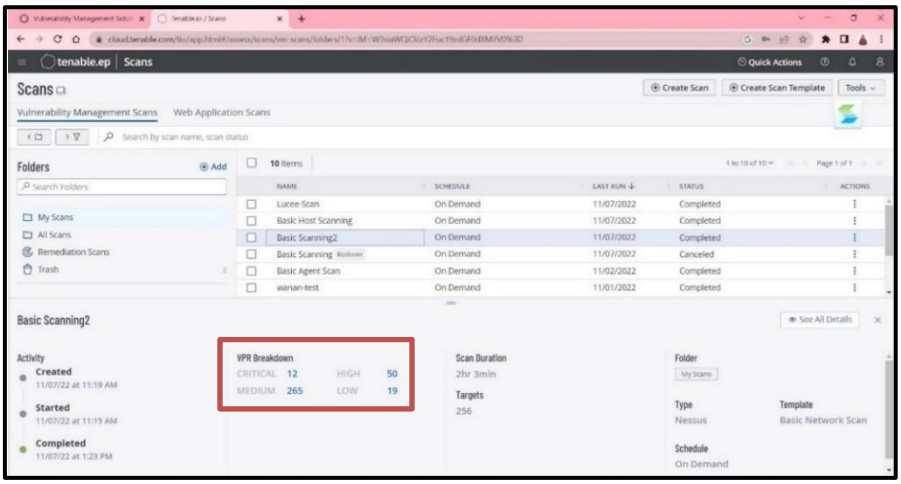


Figure 2.7 Vulnerabilities Before Remediation Process

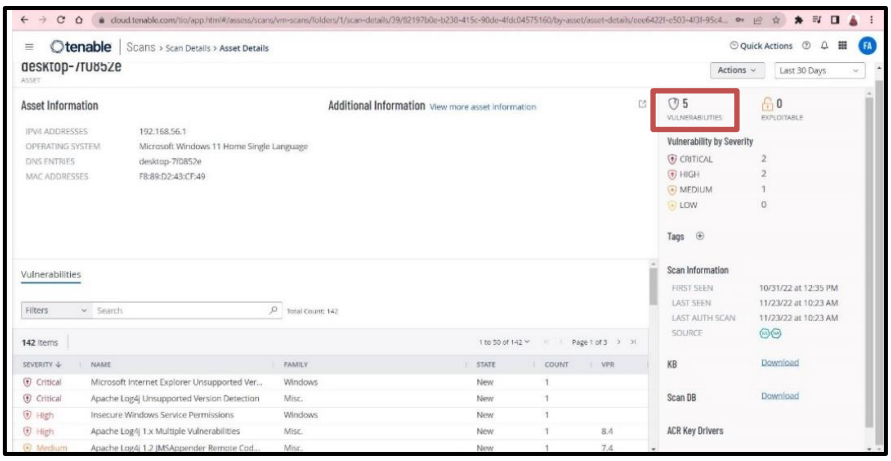


Figure 2.8 Vulnerabilities After Remediation Process

2.3 Front-End Development for ICT Access Control Registration System

Front-end and back-end development are required for all websites. Front-end development is the visual aspects of a website that users see and interact with while back-end development includes the structure, system, data, and logic of a website.

2.3.1 System Development Overview

In overview, this project is a group project with three (3) other team members in Data Center and Security unit. They request the internship students to develop for front-end part of the system. Commonly, the developer use Hypertext Markup Language (HTML) and Cascading Style Sheet (CSS). However, ICT access control registration system was developed using Cold Fusion Markup Language (CFML) which is a new programming language to learn together with Lucee, as the leading open-source for CFML application server.

2.3.2 Objective of Front-End System Development

Currently, staff in UMK only used traditional method where they need to fill-in ICT access control products in paper form and then submit to the responsible staff. Moreover, another problem occurred is difficult to transfer form information into the computer. Thus, one of the ways to address this issue is developing a simple online system to be used by UMK staffs for ICT access control registration instead of using traditional method previously. The objectives of this front-end system development task are to be achieved as follows:

a) To improve the management of user data electronically and effectively.

b) To improve the new programming skills in using CFML.

c) To provide a user-friendly of graphic user interface (GUI) between all visual elements in the system.

2.3.3 ICT Access Control Registration Form

There are four (4) main sections for this online form system which includes the applicant information, the server information, the database access information, and the applicant verification. A table form was designed because it is an online form interface.

2.3.3.1 Section A: Applicant Information

Section A is where applicants must enter their information to be saved for use by the appropriate office as can be seen in Figure 2.9 and Figure 2.10. All information like name, ID card number, employee ID, position, status, agency, office number, mobile phone number, branch, and email are all required.

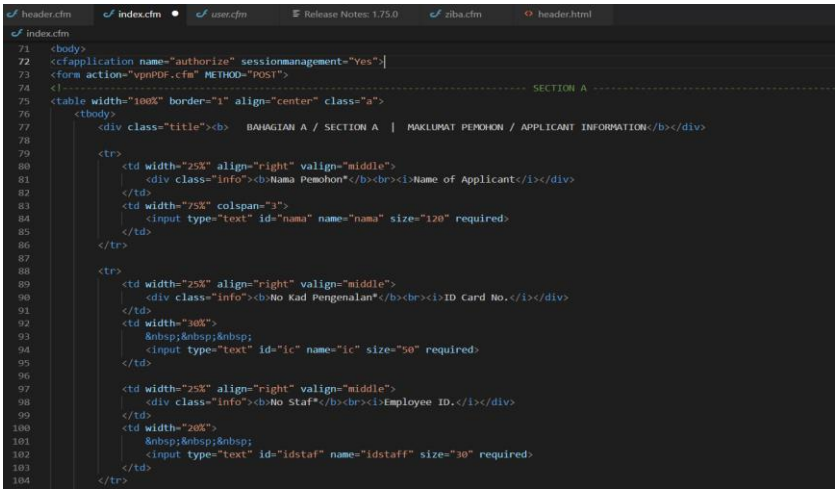


Figure 2.9 Source code for front-end of section A

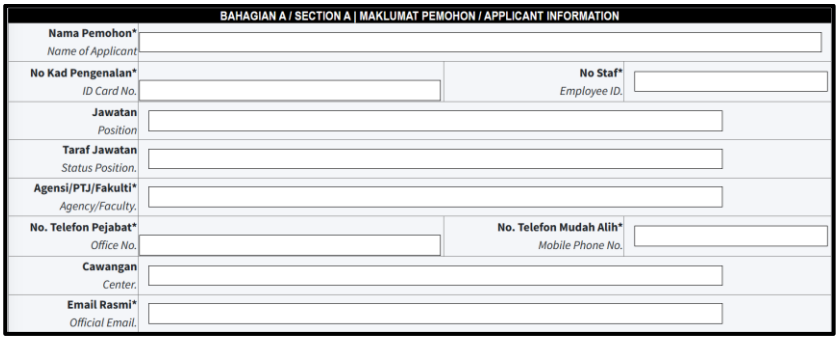


Figure 2.10 User interface for section A

2.3.3.2 Section B: Server Information

Section B is where applicants must enter the server information for which they wish to register. The information, which includes the reason for accessing the server, the server destination, and the server location, is required to facilitate the server's implementation. Figures 2.11 and 2.12 in the below section show the details of the source code and user interface that was developed.

```
<!-------------------------------------------------------------------------- SECTION B ----------------------------------------------------------------------->
<table width="100%" border="1" align="center" class="b">
    <tbody>
        <div class="title">
            <b>   BAHAGIAN B / SECTION B  |  MAKLUMAT SERVER / SERVER INFORMATION</b>
        </div>

        <tr>
            <td width="25%" colspan="1" align="right" valign="middle">
                <div class="info">
                    <b>Tujuan Akses*</b><br><i>Purpose of Access</i>
                </div>
            </td>
            <td width="75%" colspan="3">
                   
                <input type="text" id="tujuan" name="aim" size="100" required>
            </td>
        </tr>

        <tr>
            <td width="25%" align="right">
                <div class="info">
                    <b>Destinasi Server*</b><br><i>Server Destination</i>
                    <br><font size="2">*Jika lebih dari senarai, sila lampirkan senarai server/If more than in list,
                    please attach a list of servers</font>
                </div>
            </td>
            <td width="30%">
                   
                <input type="text" id="destinasi" name="destination" size="30" required>
            </td>ß
            <td width="10%" align="right">
                <div class="info">
                    <b>Lokasi Server*</b><br><i>Server Location</i>
                </div>
            </td>
            <td width="35%" align="left">
                      
                <input type="radio" id="loc1" name="location" value="Pusat Data Utama">
                <label for="loc1"><font size="3">Pusat Data Utama/Main Data Center</font></label><br>

                     
                <input type="radio" id="loc2" name="location" value="Pusat Pemulihan Bencana">
                <label for="loc2"><font size="3">Pusat Pemilihan Bencana/Disaster Recovery Center</font></label>
            </td>
        </tr>
    </tbody>
</table>
```

Figure 2.11 Source code for front-end of section B

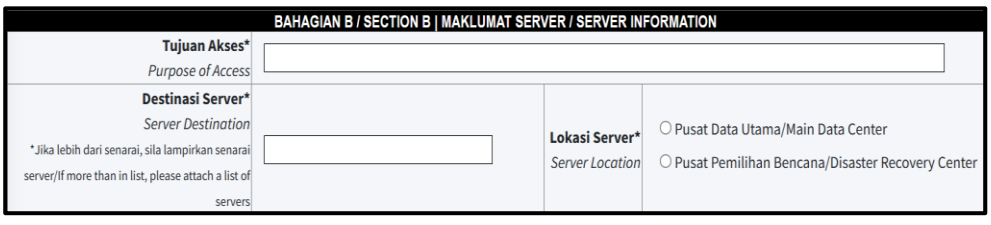


Figure 2.12 User interface for section B

2.3.3.3 Section C: Database Access Information

Section C requires applicants to input the detail of database access information. The information, includes type of database, table information, and database access time period were created as shown in Figures 2.13 and 2.14 in the following section.

```
<!-------------------------------------------------------------------------------- SECTION C ----------------------------------------
<div class="title">
    <b>   BAHAGIAN C / SECTION C  |  MAKLUMAT AKSES PENGKALAN DATA / DATABASE ACCESS INFORMATION</b>
</div>

<table width="100%" border="1" align="center" class="c">
    <tbody>
        <tr>
            <td width="25%" align="right">
                <div class="info">
                    <b>Jenis Pengkalan Data</b><br><i> Database Type</i>
                </div>
            </td>

            <td width="30%" align="left">
                     
                <input type="radio" id="type1" name="typee" value="Mysql/MariaDB">
                <label for="type1">Mysql/MariaDB</label><br>

                     
                <input type="radio" id="type2" name="typee" value="Postgres">
                <label for="type2">Postgres</label><br>

                     
                <input type="radio" id="type3" name="typee" value="Oracle">
                <label for="type3">Oracle</label><br>

                     
                <input type="radio" id="type4" name="typee" value="Informix">
                <label for="type4">Informix</label><br>

                     
                <input type="radio" id="type5" name="typee">
                <label for="type5">Others:</label>  <input type="text" id="elseElse" name="typee">
            </td>

```

Figure 2.13 Source code for front-end of section C

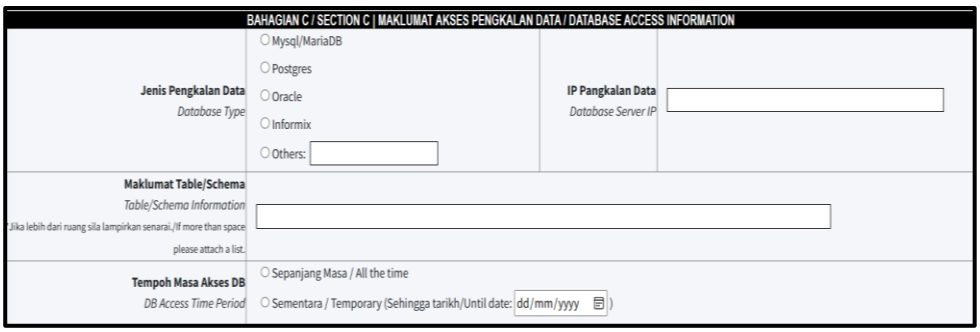


Figure 2.14 User interface for section C

2.3.3.4 Section D: Applicant Verification

Section D is where the applicant must sign, refers to confirmation of the contents of a document before they submit it. Figures 2.11 and 2.12 in the following section show the source code and user interface that were formed.

```
311  <!-------------------------------------------------------------------------- SECTION D ---------------------------------------------------------------------->
312  <div class="title">
313      <b>   BAHAGIAN D / SECTION D  |  TANDATANGAN PEMOHON / SIGNATURE OF THE APPLICANT</b>
314  </div>
315
316  <table width="100%" border="1" align="center" class="d">
317      <tbody>
318          <tr>
319              <td width="100%" align="justify">
320                  <div class="info">
321                      <b>Saya dengan ini mengaku bahawa segala maklumat yang diberikan adalah benar dan telah membaca, memahami dan
322                      tertakluk kepada Dasar Keselamatan ICT(DKICT) UMK, Peraturan serta Pekeliling Universiti Malaysia Kelantan. Saya akan
323                      mematuhi segala peraturan yang termaktub dalam Akta Rahsia Rasmi 1972, Akta Jenayah Komputer 1997, Akta Komunikasi
324                      dan Multimedia 1998 serta semua pekeliling dan peruntukan berkaitan dengan perlindungan maklumat dan rahsia Kerajaan
325                      Malaysia. Jika terdapat sebarang pemalsuan dan penyelewengan maklumat pihak Pusat Komputeran & Informatik berhak
326                      menamatkan permohonan atau perkhidmatan dengan serta merta dan mengambil tindakan ke atas saya.</b>
327                      <br><br>
328                      <i>I hereby declare that all information provided is true and has been read, understood and subject to UMK's ICT Security Policy
329                      (DKICT), Rules and Circulars of Universiti Malaysia Kelantan. I will abide by all the rules enshrined in the Official Secrets Act 1972,
330                      Computer Crimes Act 1997, Communications and Multimedia Act 1998 as well as all circulars and provisions related to
331                      information protection and the secrets of the Government of Malaysia. If there is any falsification and misappropriation of
332                      information the Computer & Informatics Center reserves the right to terminate the application or service immediately and take
333                      action against me.</i>
334                  </div>
335                  <br>
336                        
337                      <input type="checkbox" id="agree" name="agree" value="Agree" required>
338                      <label for="type1">Tekan jika setuju / Click to agree</label><br>
339              </td>
340          </tr>
341      </tbody>
342  </table>
343
344  <!-------------------------------------------------------------------------- SUBMIT FORM ---------------------------------------------------------------------->
345      <br>
346      <input type="hidden" id="lokasi" name="lokasi">
347      <input type="hidden" id="type" name="type">
348      <input type="hidden" id="masa" name="tarikh">
349
350      <input onclick="myFunction()" type="Submit">
351
352  </form>
```

Figure 2.15 Source code of section D and submit button

BAHAGIAN D / SECTION D | TANDATANGAN PEMOHON / 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 to agree

Submit

Figure 2.16 User interface for section D and submission

2.4 Design Cybersecurity Awareness Posters

Posters are commonly used to share the awareness messages. The reason of poster is most popular method among the netizen because it is one of the simplest mechanisms, and most people loves to read the content on poster because the content is not overload of texts but have attractive design with graphic. The industrial training supervisor was asked to do this task because he wishes to distribute those posters on social media within the UMK organization. The purpose of this task is to raise awareness about cybersecurity among the audience, so that they will be more cautious and alert to the current cyber issues.

In order to design 25 cybersecurity awareness posters, lots of research have been done through reading the cyber news, and study many resources such as article, and journal on the internet. The benefit of completing this task is that student gained new knowledge about current cyber issues together with learned on how to prevent and overcome them. The topic for each poster was decided by take into the type of audience the poster is supposed to target which are staff and student in UMK, and the purpose of the poster that is to give more awareness about current cybersecurity issues. The topics that were chosen to design the posters are listed down below:

- ✓ Careful when Scanning QR Code
- ✓ Tips for Avoiding Dark Web Danger
- ✓ Get Multi-Factor Authentication (MFA) Now
- ✓ Think Twice before Post Photo
- ✓ Bring Your Own Device (BYOD) Security Policies
- ✓ Tips to Safe when Online Chatting
- ✓ Tips to Use Public Wi-Fi
- ✓ Beware of Cracked Software
- ✓ Watch Out for Malicious Advertising
- ✓ How to Take a Social Media Break
- ✓ Tips to Prevent Cloud Security Threat
- ✓ How to Overcome Log4J Vulnerability
- ✓ SMS-Phishing Protections

- ✓ Challenge Social Media Detox
- ✓ Online Safety Tips
- ✓ Watering Hole Attack
- ✓ Tips to Prevent SQL Injection Attack
- ✓ Pretexting Attack
- ✓ Risks of Using Outdated Hardware
- ✓ Anatomy of Distributed Denial-of-Service (DDoS) Attack
- ✓ What are the Best Practices to Consider when Defending Against Botnet Attacks
- ✓ Five (5) Essential Phases for Optimal Security
- ✓ Social Engineering
- ✓ Risks to User of DNS Spoofing
- ✓ Scareware Removal Tips

Figure 2.17 is shown the overview of cybersecurity awareness posters that were created using online graphic tool that is Canva and can be achieved from https://www.canva.com/design/DAFTSvsxuy0/a9lqUTfMlfL0seoDXuBTuQ/edit?utm_content=DAFTSvsxuy0&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton.

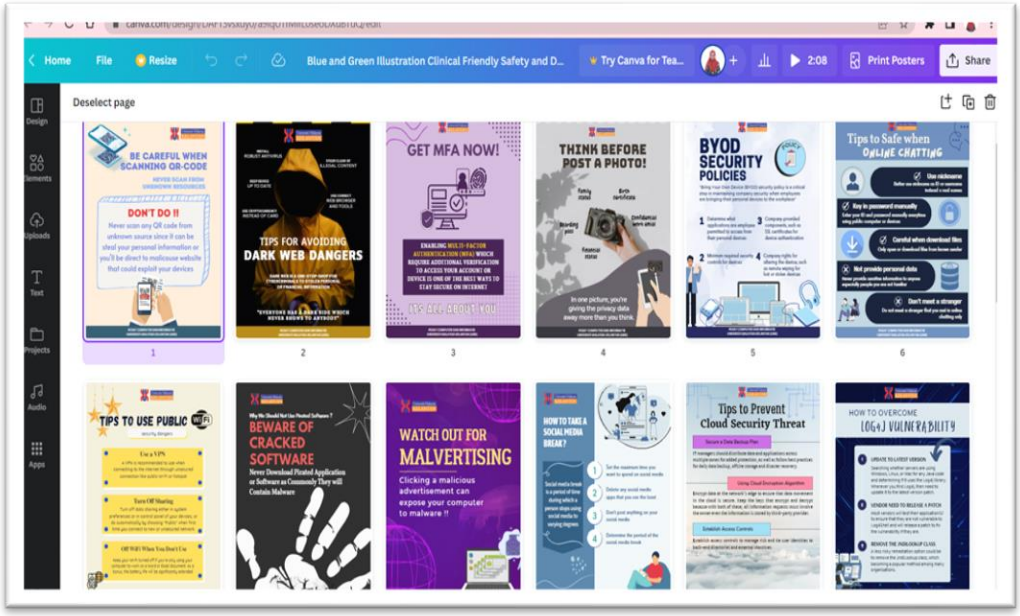


Figure 2.17 Cybersecurity Awareness Posters

2.5 Writing an article with the tittle “Future Technology”

Writing an article allows a person to help simplify a difficult topic or share a solution to a difficult problem. The purpose of this task basically for academic analysis only. The topic of future technology prediction was given by supervisor. Nowadays, every industry is becoming increasingly dependent on technology and it is critical to be alert and adapt to these new technologies in future (“Importance of emerging technologies,” 2021). However, technology in healthcare has piqued my interest after study the narrow of this topic.

This task was begun with reading few existing articles on Google Scholars and news about future technology. Then, preliminary research about the main points of article was conducted. After that, find the article's key points of technology growing in healthcare which includes the wearable technology, how 3D bioprinting applied in medical application, and how future industry 4.0 will impact in pharmaceutical packaging. By writing the article, it takes on board new knowledge about future technology prediction in this global world. Figure 2.18 is a diagram that shown the final result once the article was completed.

Figure 2.18 Writing an Article of Future Technology

2.6 Network Detection Response (NDR) Solution

Threat monitoring is essential in an organization because it provides technology professionals with visibility into the network and allows them to take actions on behalf of the users who access it, enabling stronger data protection and preventing damage caused by breaches. Meanwhile, NDR solutions are designed to detect cyber threats on organization networks using artificial intelligence (AI), machine learning (ML), and data analytics. Then, Cyber Command will raise alert to security professional if there is any abnormal traffic.

1) Monitoring Cyber Threat with Sangfor's Cyber Command

Monitoring cyber threat only covered superior threat detection capabilities on internal network either on East-West and North-South traffic for UMK Wi-Fi network. After that, there are few securities incident that can be identified from Figure 2.19 below which are crypto mining, backdoor, and coin miner while the top incident happened to the most host network is crypto mining. The term "mining" refers to the process of validating transactions that are waiting to be added to the blockchain database.

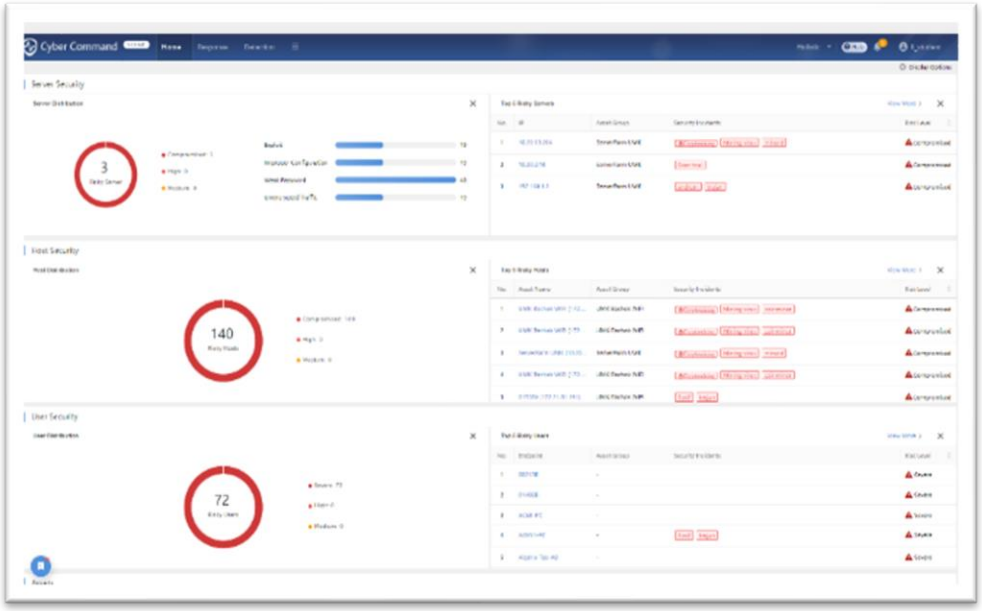


Figure 2.19 Result of Security Incident in UMK

2) NDR Presentation during potential lab

On the first day entering the industrial training, my internee-mate and I were asked to do a presentation with a topic of NDR from Sangfor Cyber Command. Figure 2.20 shows the presentation that was held during Potential Lab which is one of the weekly activities in CCI, UMK. Cyber Command is a new security platform that used NDR solutions for monitoring internal networks, correlating existing security events, and using AI to analyze behaviors was investigated before the presentation. The content of this sharing session is including the introduction to NDR solutions that used by Cyber Command, the reason of why an organization need this tool, the findings after monitored the network of UMK Wi-Fi, and what the differences between NDR solution and Security Information and Event Management (SIEM).

Figure 2.20 NDR Presentation during Potential Lab

2.7 Additional Tasks

During 20 weeks of industrial training at UMK, internship trainees are given the opportunity to participate in lots of other department and company activities. There are many experiences that made students feel excited and would be meaningful.

1) Switch Labelling in UMK's Data Center

Figure 2.21 and Figure 2.22 are the prove when the internship students got the opportunity to assist one of the network departments staff, Mr Zariman in labelling the existing cables that connected to switches and servers using the labels printer. Futhermore, Mr Zariman also shows the students on how he was configuring the switches to find the port cables using Cisco Packet Tracer in the data center room. This goal for this step is to label the ports correctly before they replace all the switches. This would be very memorable experience for me because it was the only chances to see the processes that they must do when switching to new switches.

Figure 2.21 Cable Labelling on Switch

Figure 2.22 Internship Students with the Network Staff

2) Marketing Meeting with Flowmon

Figure 2.23 shows when joining the marketing meeting with the representative from Flowmon company thorugh Microsoft Teams. It was valuable experience since able to see on how Flowmon professionals met with few IT experts from CCI, UMK to discuss the marketing strategies. Flowmon Network is a private technology company that creates network performance monitoring and network security products based on traffic flow data.

Figure 2.23 Marketing Meeting with Flowmon

3) Customer Training with Tenable

Figure 2.24 illustrated during customer service training with a Tenable representative through Zoom. The aim of this training is to expose the staffs including the interns about the features in Tenable.io, Nessus sensors, how to use their product, and the competencies needed to increase customer satisfaction. It is essential since we will use their product to launch VA.

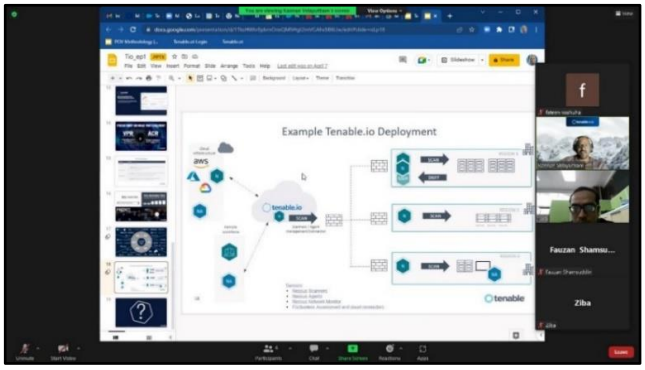


Figure 2.24 Tenable Training

4) Self-learning on Burp Suite

Burp Suite is an application security and testing solution for performing web application security testing. It is developed by a company named PortSwigger. Burp Suite are available in three editions includes free community edition, professional edition, and enterprise edition. In this self-learning, Burp Suite community edition was used because it is free open-source, despite some feature limitations. As a beginner, a few labs exercise were completed by following the tutorial from YouTube. Example of tutorial that have been completed are two factor authentication (2FA) broken logic as shown in Figure 2.25, try reset password poisoning, and populate a sitemap like in Figure 2.26.

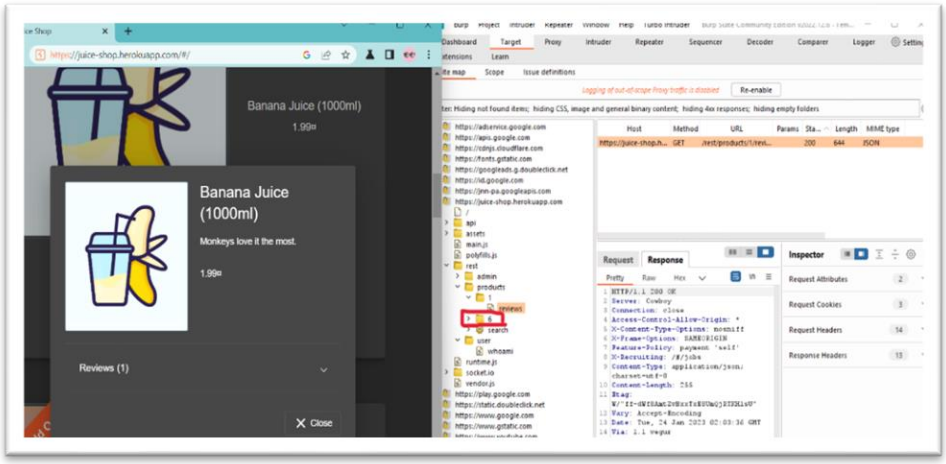


Figure 2.25 New Sitemap Created in Host Entry

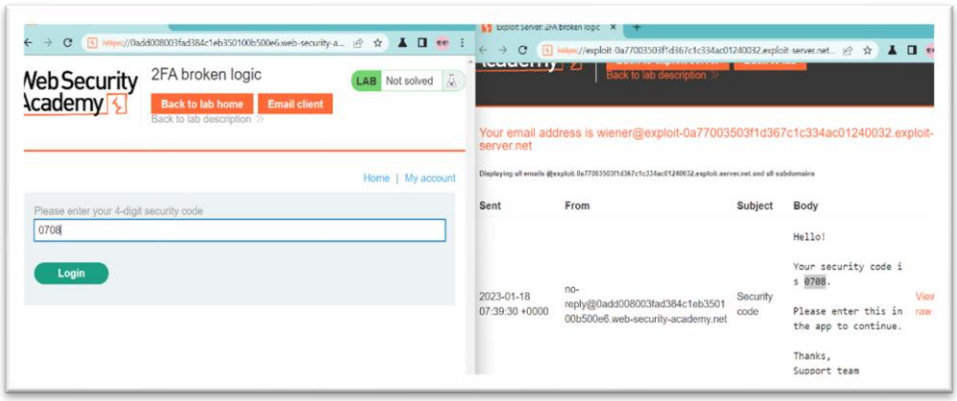


Figure 2.26 Get 4-digit Security Code for 2FA Broken Logic

2.8 Hardware and Software Used

Table 2.1 is the listing of hardware tools and software tools that were used with its specifications during the VA and front-end development projects execution and the extra tasks too.

Tools	Specification
Hardware	
Laptop	Dell Inspiron 15
Random Access Memory (RAM)	16 GB
Processor	11th Gen Intel(R) Core (TM) i5-1135G7
Software	
Operating System (OS)	Window 11
Browser	Google Chrome, Microsoft Edge, Firefox
Open Source	Nessus (x64) Web Client, Lucee
Cloud Tool	Cyber Command, Canva, PortSwigger

Table 2.1 List of hardware and software used

2.9 Period to Complete Main Projects (provide Gantt Chart if possible)

Undergraduate students were required to undergo industrial training for duration of 20 weeks. However, the projects and the extra tasks did not take time for the whole weeks to be accomplished. Therefore, there are few weeks that can spend on self-learn and try out the existing cybersecurity tools in order to improve the skills.

The time period to complete the VA project is within four (4) weeks only which from week 4 to week 8. The first three phases did not require a lot of time and it was able to finish within a week only, but the remediation process needed more time and took around four (4) weeks to achieve the goal, as each scanning procedure did. The

next main project is developing front-end interface for ICT access control system only takes one (1) week. Most of the time was spent learning the language and concepts because Lucee and CFML were new to the students. The Gantt chart for these two projects can be achieved at Figure B.1 in Appendix B.

2.10 Theoretical and Practical Knowledge used

The implementation of VA required the computer security knowledges in order to identify the potential security vulnerabilities in the network infrastructure before launch the assessment. Throughout the learning journey in Computer Network and Security degree, the capability to integrate computer science knowledge and skills on a continuous basis to the real world during the implementation of these two main projects. Moreover, the exposition to the process of exploiting the vulnerabilities using Burp Suite also learnt in Secure Programming course previously. Even though this project has not yet covered the exploitation part, but some of the knowledge are very useful in understanding the results of vulnerability scanning.

Every student who taking computer security course is essential to have the basic of programming knowledge. In system coding to develop the front-end of ICT Access Control system, the programming skill and knowledge of HTML and CSS languages helps a lot to easily create a nice UI/UX for the system. This is because CFML commands are similar to HTML commands. Furthermore, the Visual Studio Code features and work environment is already familiar since few coding was developed in few courses previously such as Programming Technique, Web Programming, and Application Development. Only a few ColdFusion extensions are required to be installed in order to run the cfml files.

However, the other courses that were studied previously are useful and applicable to the other tasks too include the side tasks. For example, the exposure to network lab in Computer Network course support me to recognize, understand the functionalities and how to connect cables on fiber tray.

2.11 Problem Faced

Several problems that encountered throughout the VA process of my internal network that will be listed as followed. The first three (3) phases do not face with the serious issues since it was guided by the team members in Data Centre and Security unit. Moreover, those three phases are only simple steps need to be carried out and able to do successfully. The issue occurred for this project VA was happened during vulnerability remediation phase. Remediating vulnerabilities often comes in the form of patching or updating software and bug fixes.

For example, the problem come up when disabled Microsoft Edge software as recommended by Tenable, but then the vulnerability remains even after rescan it. Moreover, there are some vulnerabilities for some remediation instructions were unable to be done because the items required are not present on the laptop. Furthermore, the scanning process is time-consuming, causing the process of diminish the vulnerabilities to take longer than expected.

For front-end development project, the problem only arises when to setup the Lucee sever on laptop because being unable to access the Lucee server admin because the directory is incorrect. But, the solution to the problem was discovered on the internet. Since Lucee and CFML were new to the students, the majority of the time was spent learning the language and concepts. However, the project's implementation is quite simple because it is nearly identical to HTML language.

2.12 General Skills

Even security analysts spend majority of their time on their laptops, but to fill cybersecurity positions, either soft or hard skills are needed. As same to the case when conducting both VA and system development projects. Literally, in terms of hard skills, VA is never been conducted before, but my soft skills allowed me to participate in this project successfully as well. From my point of view, there are three (3) important skills needed to do these projects which are communication, teamwork and

problem-solving. Verbal communication skill is needed since always need to present and update the technical security information to variety of stakeholders including the team members and the internship supervisor.

Teamwork skill is essential since solving security issues does not take place in a vacuum, nor do have all the answers. For instance, the team members frequently work as a team, collaborating with the intern-mate and enlisting the help from others security expert when run into problems. Last but least, problem-solving also a very crucial soft skill in cybersecurity field because security expert constantly facing scenarios where they need to troubleshoot. Example scenario is programmers must identify and resolve any issues that may arise after creating program. This is not always an easy task because even minor errors can wreak havoc on a program. Even though problem solving is the most difficult skill to master, but never give up polish this skill.

2.13 Implementation Management of Task

An implementation plan is a project management tool that aids in the execution of a company's or project's strategic plan by breaking it down into smaller steps and defining the timeline, teams, and resources required. The aspects of task management are critical to the success of task implementation in any given task or project. These areas include: task specification, task planning, leadership, and management, monitoring and coaching, and, most importantly, communication.

2.14 Conclusion

Finally, the main project completed by the student can be invaluable training that can be applied in a real-world situation. The given tasks that are significant in developing student knowledge, skills, and experiences will be very beneficial to the students in their future careers, particularly in the field of computer security. Thus, the following chapter will discuss some of the tasks that were also completed during the 20 weeks of internship period at UMK.

CHAPTER 3

OVERALL INFORMATION OF INDUSTRIAL TRAINING

3.1 Introduction

This chapter will be explained regarding the reference materials that were used and some the comment from overall tasks that have been done throughout 5 months of doing industrial training at CCI, UMK.

3.2 Reference Materials

When conducting the project, mostly all the information and guidance were found through Google search, Yotube and online material from the "udemy" website. The account for udemy was provided by supervisor as references to run the VA project and to run the Burp Suite lab exercies. Figures C.1 and C.2 in Appendix C show examples of content from the udemy website. The website is excellent because it teaches in depth and assists learners in exploring their interests, learning new skills, and advancing their careers. The pictures of the edemy online courses are provided in the section below. If the required information cannot be found on the internet, staffs and company's supervisor always willing to help whenever internee asked them.

3.3 Comments from Overall Tasks

Overall, it was a great experience to intern at CCI because the UMK staffs are very welcoming and it was a blessed because of their willingness to accept and guide the internship students along the internship journey at there. They were kind to the

trainee and always made the environment fun. The staffs always provide a lot of guidance and share knowledge when faced with a problem during task execution. For instance, I have zero knowledge about to execute the VA, then the staff asked me to join the customer training and willing to answer any questions that curious. Finally, all the tasks assigned by the company's supervisor were able to complete on time, and allowing me to handle the other tasks on time.

3.4 Conclusion

As the conclusion, subsidiary projects provided by the Data Center and ICT Security unit help to broaden students' knowledge and experiences while keeping them on track with their courses. It also provides students with an opportunity to improve their technical, social, and writing skills. Each task was completed with the assistance of Data Center and ICT Security staffs and supervisor. With their assistance, the mistakes are appropriately improved.

CHAPTER 4

CONCLUSION

4.1 Introduction

This chapter will conclude about the overall achievements, issues and challenges that were facing during project and tasks given together with the suggestion to overcome the challenges.

4.2 Overall Achievements

It is normal for those who receive industrial training to gain precious memorable experiences and valuable knowledge because students gain experienced on how real-world experience working environment that they cannot be found in a syllabus. UMK is the best choice for industrial training at CCI because internship students given the opportunity to involve in variety of tasks that are quite difficult and challenging. The tasks assigned not only improve an individual's technical skills, but also student's critical thinking and problem-solving abilities.

The staff in the team, Mr Fauzan was introduced the internee to Lucee and CFML programming language at the beginning of industrial training, as well as basic training to develop a system for ICT access control registration form. Another remarkable achievement since got the chance to be one of the presenters during potential labs held by Skills CCI, UMK. The internship student under Data Center and Security unit who were only given the opportunity to present on this sharing session. Potential lab is a weekly presentation activity, and all CCI employees are required to present at least once a year. Another achievement is that have learned more about cybersecurity, and especially detailed about the VA process.

Besides, social interaction is one of the skills that need to be applied in work environment and it was improved slowly because always interact and communicate with the upper management and other trainees. Additionally, teamwork is also important because it must be applied during any project accomplishment to ensure the project can be completed smoothly and well. Those are the skills that have been improvised during the industrial training.

4.3 Issues and Challenges

Overall, there is no serious issues or difficulties with the working environment, working space, communication tools, hardware used, or software required because it was provided by the company. The staff at UMK have been extremely friendly to me and have taught me a great deal. They are always willing to answer any question that been asked if they knew. However, there were some difficulties or challenges that can be encountered during the internship period.

One of the problems is takes time to understand some of the job tasks such as when getting familiar with NDR solution. NDR used to detect suspicious network activity, NDR solutions employ a combination of non-signature-based advanced analytical techniques such as machine learning. It was quite hard to understand the result from monitoring threat in Cyber Commend and to understand how NDR solution works such as the process of analytical technique.

Another issue that occurred is during getting familiar with VA process. As stated, it is difficult to remediate each of the vulnerabilities since did not have prior experience with VA tasks previously. Even the Tenable.io tool already provide the recommendations to eliminate each vulnerability, but there is one vulnerability which is Apache Log4j vulnerability that unable to resolve it despite following the steps. After speaking with the supervisor, he stated that this is a common occurrence because maybe the personal laptop may not support what was suggested.

The next difficulty is when updating the log book into the Industrial Training System (ITS). After trying to save what have been written and the network connection was unstable, then the data was lost. Thus, the content of the logbook had to rewrite again. On the next time, student need to use different text editor as a backup file to save the data. Moreover, the database of the system was crash for several weeks too. It became a problem for to write down the daily activities in spreadsheet, and then had to save and share in Google Drive with company supervisor and university supervisor.

4.4 Opinion and Suggestion

The suggestion that will be discussed in this section are based on my opinion and experiences. First and foremost, I would like to suggest to Faculty of Computing, UTM to change the semester of industrial training to the last semester which refers to 8^{th} semester. Currently, this internship program is done during seven semester and student need to enter the class again for the last semester. This might be a problem for student who got the offered to become the permanently staff at their internship company and if the company asked to join as soon as possible. Another consideration is related to final year project (FYP). In my view, students should complete their FYP 1 and FYP 2 in two semesters sequentially before moving on to industrial training. This is because students may be more focus on finishing their FYP and still remember on what they have put in documentation.

Next, students should carefully consider what the job scope they are truly interested to learn during industrial training. Please conduct extensive research on the organization before start to apply the internship placement. It is such an important step to ensure that student can learn lots of beneficial things and got into more technical experiences. Completing the internship program at the appropriate organization can help the students to enjoy themselves while learning without stress. Finally, students should not be afraid to do work outside of their job scope as long as students get the permission from their supervisor. Doing a variety of tasks allows to gain more experiences in the real world of future career. Students can also learn how to multitask, which is an important skill that most organizations value.

4.5 Conclusion

Industrial training is the best path for students to gain knowledge and experience because it exposes them to a real-world work environment. Students will be able to sharpen their social skills and expand their networking through industrial training. Not only that, but industrial training allows students to put the theories they learned in class into practice. This is because in a real-world work environment, each task has a broad intersection, even if it is related to a subject studied at university. Maximizing the skills and knowledge gained will assist the student in obtaining a position at their desired company after graduation.

REFERENCES

Sharma, S. (2022, July 13). Penetration testing report or VAPT report by Astra Security Astra. Retrieved December 11 2022, from https://www.getastra.com/blog/security-audit/penetration-testing-report/

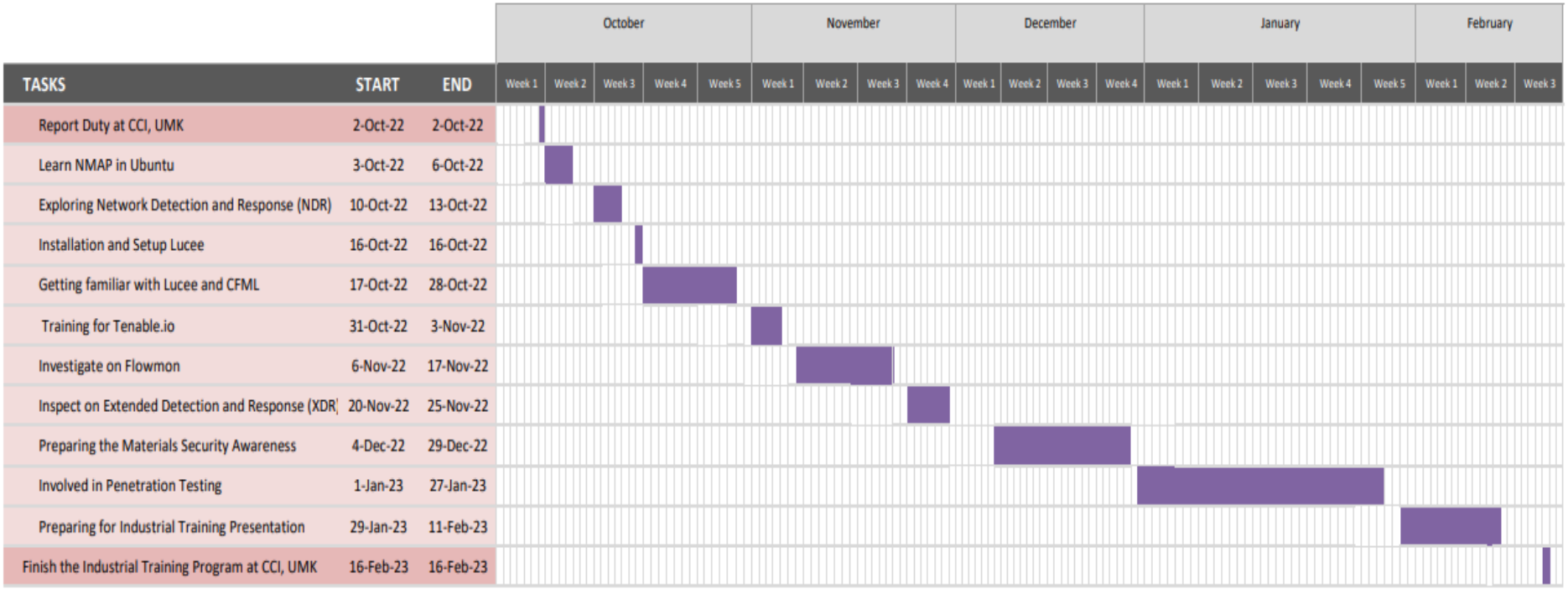
What is Vulnerability Assessment: VA Tools and Best Practices: Imperva. Learning Center. (2022, August 10). Retrieved December 12 2022, from https://www.imperva.com/learn/application-security/vulnerability-assessment

Importance of emerging technologies. IIMT Group of Colleges. (2021, October 13). Retrieved December 14 2022, from https://www.iimtindia.net/Blog/importance-of-emerging-technologies/

Appendix A Gantt Chart of Industrial Training Program

Universiti Malaysia Kelantan

Gantt Chart for Industrial Training Program
Supervised by Encik Mohd Fadli



TASKS	START	END
Report Duty at CCI, UMK	2-Oct-22	2-Oct-22
Learn NMAP in Ubuntu	3-Oct-22	6-Oct-22
Exploring Network Detection and Response (NDR)	10-Oct-22	13-Oct-22
Installation and Setup Lucee	16-Oct-22	16-Oct-22
Getting familiar with Lucee and CFML	17-Oct-22	28-Oct-22
Training for Tenable.io	31-Oct-22	3-Nov-22
Investigate on Flowmon	6-Nov-22	17-Nov-22
Inspect on Extended Detection and Response (XDR	20-Nov-22	25-Nov-22
Preparing the Materials Security Awareness	4-Dec-22	29-Dec-22
Involved in Penetration Testing	1-Jan-23	27-Jan-23
Preparing for Industrial Training Presentation	29-Jan-23	11-Feb-23
Finish the Industrial Training Program at CCI, UMK	16-Feb-23	16-Feb-23

Figure A.1 Gantt chart of Industrial Training

Appendix B Gantt Chart for Main Projects

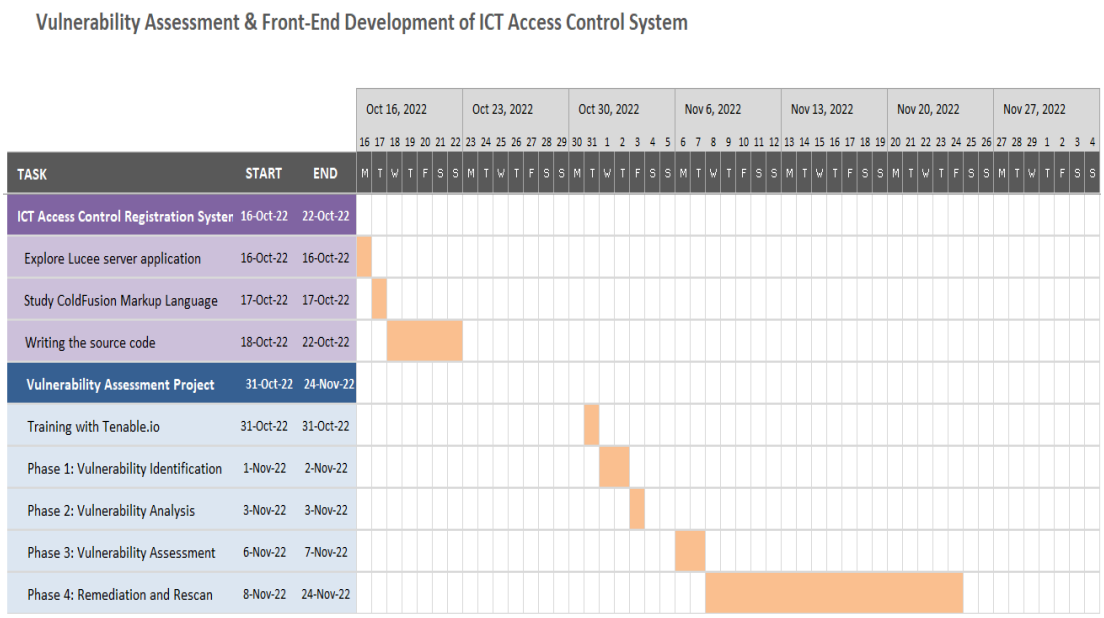


Figure B.1 Gantt chart for main projects

Appendix C Reference Material

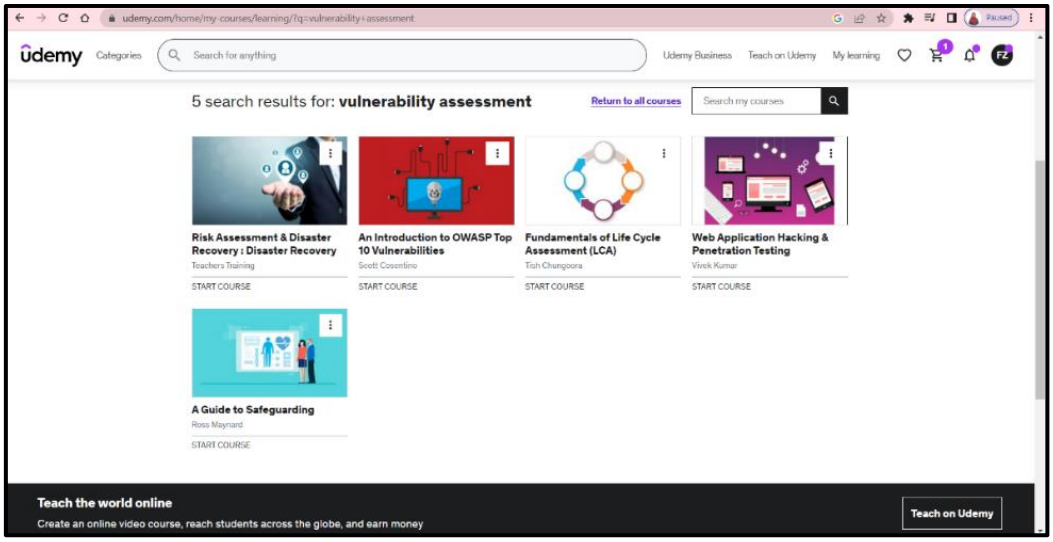


Figure C.1 Lecture of VA on “udemy”

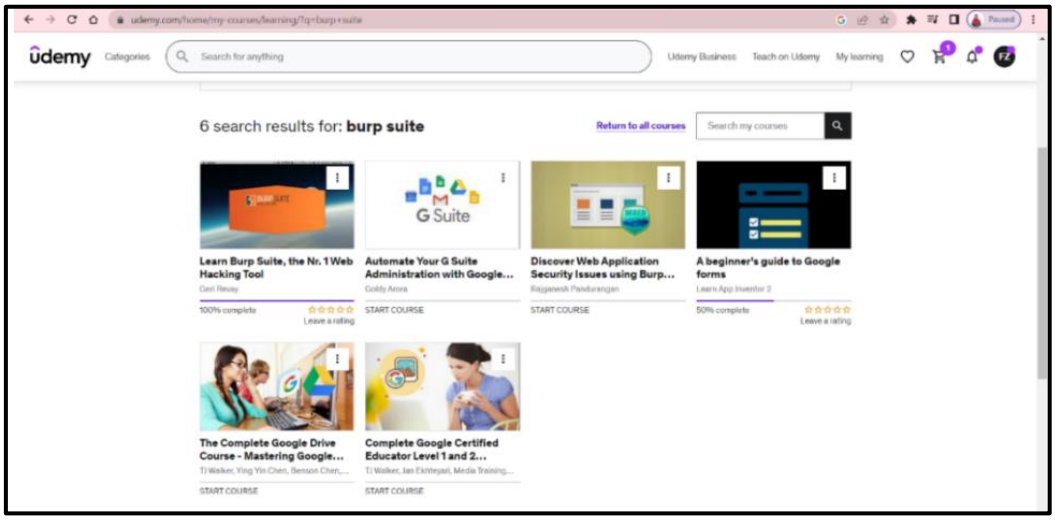


Figure C.2 Lecture of Burp Suite on “udemy”

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

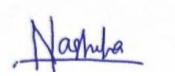
INDUSTRIAL TRAINING ACHIEVEMENTS

Student's Name : Fateen Nashuha Binti Yusof

Organization : University Malaysia Kelantan (UMK)

No.	Task (List all tasks have been completed)	Month of Task Achieved				
		Month 1	Month 2	Month 3	Month 4	Month 5
1.	Monitoring Cyber Threat with Cyber Command	✓				
2.	Writing an Article about Future Technology		✓			
3.	System Development for ICT Access Control Registration Form	✓				
4.	Switch Labelling in UMK's Data Center Room	✓				
5.	NDR Solution Presentation	✓				
6.	Vulnerability Assessment (VA) using Nessus		✓			
7.	Design Cybersecurity Awareness Poster			✓		
8.	Self-learning on Burp Suite				✓	
9.	Expose to Fiber Optic Cables Installation Process					✓

Deliverable/Training reflection (Outcomes that have been achieved)
The tasks assigned not only improved an individual's technical skills, but also offered me with memorable experiences and valuable knowledge because I was gained on real-world experience working environment. The most biggest achievement are explore the process of conducting vulnerability assessment, improve new programming language skill, and learnt the process of cable installation and improve my social interaction is one of the skills that need to be applied in work environment.

Student Signature:  Date: 8/2/2023

Approval

Organisation's Supervisor:

.....
(Signature)

Name: Mohd Fadli Bin Mohd Zain
Date: 9/2/203

Faculty Supervisor :

.....
(Signature)

Name:
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	✓	16/10/2022
5.	Fill in organization supervisor information survey in ITS	✓	27/10/2022
6.	Update of Industrial Training site (address). Inform faculty supervisor and JKL, if any changes.		
7.	Updating Industrial Training Logbook online – daily basis	✓	Daily
8.	Ensure that organization supervisor able to login to ITS successfully (Organization supervisor get ITS user id and password).		
9.	Faculty Supervisor Visit. Date:	✓	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.	✓	9/2/2023
13.	Submission of Industrial Training Report with checklist and achievement form as Appendix.	✓	9/2/2023
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.