Kod Project :	**BITU 3923**

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

WORKSHOP 2 BITZ

PROPOSAL FORM

GROUP NAME: CYBER GUARD

TITLE OF PROJECT: NETWORK INFRASTRUCTURE PROJECT XYZ

GROUP MEMBERS:

No.	Student Name	Matric Number	Email
1	Ooi Chiou Xiang	B032010388	B032010388@student.utem.edu.my
2	Izzatul Hanani binti Kamarul Nizar	B031910032	B031910032@student.utem.edu.my
3	Siti Aishah binti Mustafa	B031910420	B031910420@student.utem.edu.my
4	Muhammad Izham bin Norhamadi	B032020039	B032020039@student.utem.edu.my

TABLE OF CONTENT

(1.0) INTRODUCTION

Workshop 2 (BITU 3923) is a subject taken by a third-year student from the BITZ course. Workshop 2 is a project that gives practice and experience for students to apply their knowledge from the previous subject taken, especially in security and network. This workshop will develop students' understanding of the methods to solve the problems and tackle the issues and requirements needed in the project. Due to the online learning during pandemic Covid-19, the students need to use the VNC connection to implement this project in a group.

Next, each group is assigned to make a video, poster, and presentation regarding the service given to us. Cyber Guard needs to present about Network Address Translation (NAT). Every group needs to implement 12 services in the project. The services are active directory with minimum 2 UAC/GPO, IDS with port mirroring and management console (SIEM), IPsec VPN server for remote employees, Samba & Samba security services, DNS (IPv4), DHCP (IPv4), ACL router, Router authentication & authorization, user authentication by integrating AD with Linux, VLAN and port security, Windows server hardening vulnerability report, and Linux server hardening vulnerability report.

As the business grows, more devices will be connected to the business's network, and a proper networking plan is needed to ensure all business operations can run smoothly and securely. When a company plans to branch to a new department, it is good to rethink how the networking works within the new department. Network Infrastructure Project XYZ is executed to design a secure network infrastructure for Company XYZ. This project aims to keep the confidentiality, integrity, and availability of its resources so that all employees can access them. To successfully secure the network infrastructure, all of the traffic that comes from outside of the network will be blocked to ensure that only authorized users can access the system or information in the company. The port security will be implemented on each of the switches to ensure safety. Lastly, the access-control list (ACL) will also be implemented in the network.

(2.0) PROBLEM STATEMENT

- **Installation Operating System**

  We need to install three Operating System such as Windows Server, Linux Server, and Ubuntu Server. We need to make sure these three servers are connected and can communicate with each other.

- **Design and implement a secure network infrastructure**

  We need to setup the functions of network for internal and external communications IT.

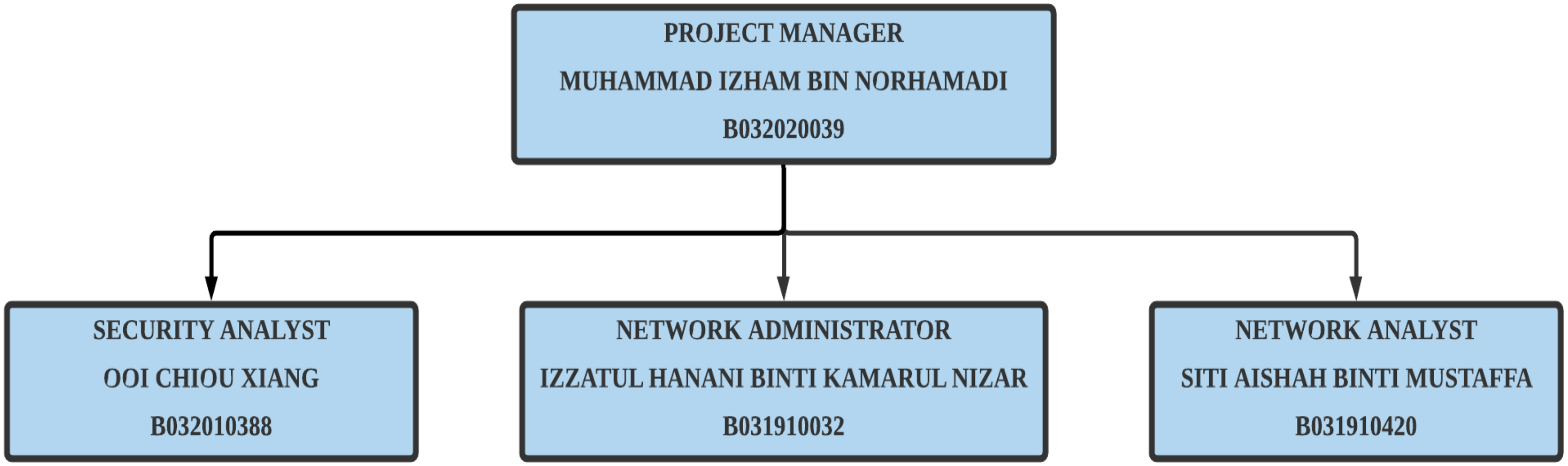
- **The company setup the new IT department with approximately 100 workers**

  There are two sites of the company which are HQ and Branch where the main server is in HQ site. We need to connect both HQ and Branch with simple point-to-point connection.

(3.0) OBJECTIVE

- To ensure the security of the infrastructure that covers all the networking functions for internal and external that comprises several services have been setup
- To ensure that the network services infrastructure remains secure
- To ensure each staff has sufficient privileges to perform operations and avoid unauthorized use of data

(4.0) ORGANIZATION CHART



(5.0) REQUIREMENT ANALYSIS

(5.1) PLATFORM AND EQUIPMENT ANALYSIS

a. Windows Server 2012

Windows Server is a server operating system by Microsoft specifically creates to run servers that provide resources for other computers. In order to develop our secured network infrastructure, our team has decided on using Windows Server 2012 as our network server for features such as:

(i) Server Manager

Server Manager is a management console in Windows Server that helps IT professionals' provision and manage both local and remote Windows-based servers without the need to enable Remote Desktop protocol (RDP) connections to each server.

(ii) Active Directory Domain Services

Active Directory Domain Services (AD DS) stores information about users, computers, and devices on the network and help administrators securely manage resources and information.

(iii) Not Oriented Toward Single Server

It features an advanced server manager which is not oriented toward single server management. Cloud concept has been incorporated while designing this server, which allows it to manage multiple servers simultaneously. Also, its dashboard lets you drill down into local servers.

(iv) Shared nothing live migration

New features of Hyper-V 3.0 shared nothing live migration, which allows us to move VMs from one machine to another without the requirement of having shared storage before making the transfer. It makes it easy to move VMs around without expensive share storage. It helps organization become even more agile and responsive to business and customer needs.

System Requirement	
Processor	3.6 GHz dual core processor
Memory	4 GB
Disk	60GB

b. **Ubuntu Server**

Ubuntu Server is a server operating system, that works with nearly any hardware or virtualization platform. It can serve up websites, file shares, and containers, as well as expand your company offerings with an incredible cloud presence. Ubuntu is a server platform that anyone can use for the following and much more:

- Websites
- FTP
- Email server
- File and print server
- Development platform
- Container deployment
- Cloud services
- Database server

One benefit that makes Ubuntu Server so appealing is it's cost effective. Anyone can download a copy of the latest version of Ubuntu Server and deploy it on as many machines as necessary at zero cost minus hardware and time. Just because Ubuntu Server is an open source free to download, businesses need not worry about a lack of support. If support is needed just purchase the “Enterprise-grade support” for the platform. Another advantage Ubuntu Server has over many platforms in its class is the new snap package feature. Snap packages are universal packages that contain all necessary dependencies and can be installed with a simple command such as “sudo snap install nextcloud”. Snaps can also be easily updated with a single command “sudo snap refresh”, so there are fewer administrative tasks.

System Requirement	
Processor	3.6 GHz dual core processor
Memory	4 GB
Disk	40GB

c. **Ubuntu Desktop**

Ubuntu Linux is the most popular open-source operating system. Apart from being free and open source, it’s highly customizable and has a Software Centre full of apps. Other than that, here are few main reasons why we choose Ubuntu Desktop:

(i) Ubuntu is user-friendly

Many computer users consider Linux-based systems hard to use and made for developers. It’s a huge misconception and Ubuntu Linux acts as a perfect myth-buster. Just like Windows, installing Ubuntu Linux is very easy and any person with basic knowledge of computers can setup his/her system.

(ii) Ubuntu is free

Downloading, installing, and using Ubuntu Linux doesn’t cost a penny. Download it from t from Canonicals’ website or visit favourite torrent website, create a bootable ISO, or burn it on a USB drive. It’s also being adopted at various educational and government organizations across the world to reduce costs. Moreover, most of the software is also free.

(iii) Ubuntu is secure

In comparison to Windows, which needs use of antivirus, the malware risks associated with Ubuntu Linux are negligible. It also saves the antivirus cost because don't need any. Its built-in Firewall and virus protection method makes sure that you're protected.

(iv) Low system requirement

While two specific flavors–Lubuntu and Xubuntu–are developed to cater the needs of lower-end systems, the default Ubuntu Unity doesn't need high-end system requirements. The recommended hardware requirements are 700 MHz processor, 512MB RAM, and 5GB hard disk.

System Requirement	
Processor	3.6 GHz dual core processor
Memory	2 GB
Disk	30GB

(5.2) APPLICATION AND SERVICES ANALYSIS

(i) Active Directory

Active Directory (AD) is Microsoft's proprietary directory service. It runs on Windows Server and enables administrators to manage permissions and access to network resources. It can store the data as the object which object is a single element such as user and device like printer. Active Directory categorize the directory object by name and attributes.

(ii) IDS

Intrusion Detection System (IDS) can be used either as software application or device that monitors the network from malicious activities. Any malicious activities will be reported to centrally using security information and event management system. IDS with port mirroring means that the network switch ability to send a copy of network data packets that being transmitted over a switch port to network monitoring or inspection device.

(iii) IPsec VPN

IPsec is a group of protocol that being used together to setup the encrypted connections between devices, IPsec often used to setup the VPN and it will encrypt the IP packet along with authenticating the source where the packets come from. VPN use IPsec protocol to establish and run these encrypted connections.

(iv) Samba & Samba security services

Samba is a free software that re-implementation of the SMB networking protocol. It provides file and print services for various Microsoft Windows clients and can integrate with Microsoft Windows Server domain. There are only two types of security modes for Samba which are share-level, and user-level which are known as security levels. Share-level can only be implemented in one way, whereas user-level can be implemented in one of four different ways.

(v) DNS (IPv4)

The purpose of DNS is to translate domain name into appropriate IP address. An IP addresses are given to each device in the network and that address are necessary to find the appropriate Internet device When user wants to load a webpage, translation must occur between what user types into their web browser. Also, the machine friendly address necessary to locate the webpage.

(vi) DHCP (IPv4)

Dynamic Host Configuration Protocol is a network management protocol used to automate the process of configuring devices on IP network and allowing them to use network services such as DNS, NTP, and communication protocol UDP and TCP. DHCP will dynamically assigns an IP address and other network configuration parameters to each device on network so that they can communicate with other IP network.

(vii) ACL Router

Access Control List (ACL) act as the gatekeeper of the network by regulating all incoming and outgoing data packets. The ACL works according to sets of rules and check all incoming and outgoing data to determine whether it complies with the rules. ACL has two types which are Extended ACL and Standard ACL. Standard ACL is the basic ACL that just look at the source address and determine whether to let data go through. Whereas the Extended ACL is more advanced where it can block entire network and traffic based on their protocol information.

(viii) Router Authentication and Authorization (Radius)

Radius or Remote Authentication Dial-In User Service is a client-server networking protocol that runs in the application layer. It consists of Radius Client and Radius Server. Radius Client is a networking device that is used to authenticate user. While Radius Server is a background process that runs on UNIX or Windows Server. It lets you maintain user profiles in central database.

(ix) User authentication by integrating AD with Linux

Microsoft's Active Directory is used by institutions and individuals the world over to centrally control access to resources belonging to the organization. It gives you the ability to manage users, passwords, resources such as computers, and dictate who has access to what.

(x) VLAN and Port Security

Port security enables us to restrict the number of MAC addresses on a port, allowing us to prevent access by unauthorized MAC address. If a secure MAC address is secured on a port, that MAC address is not allowed to enter on any other port of VLAN.

(xi) Windows Server hardening vulnerability report

Windows Server hardening involves identifying and remediating security vulnerabilities. It is used to reduce the risk of attackers compromising the critical data and systems.

(xii) **Linux Server hardening vulnerability report**

Many of Linux server security issues we may experience occur because we do not arrive hardened out of box. Further complicating matters, many of today's top security initiatives focus on the front office rather on the server rack. This provides more chances for malicious parties to acquire sensitive data, and the result can be devastating. A strategic protocol focused on risk prevention and early mitigation can make all the difference.

(6.0) NETWORK DESIGN

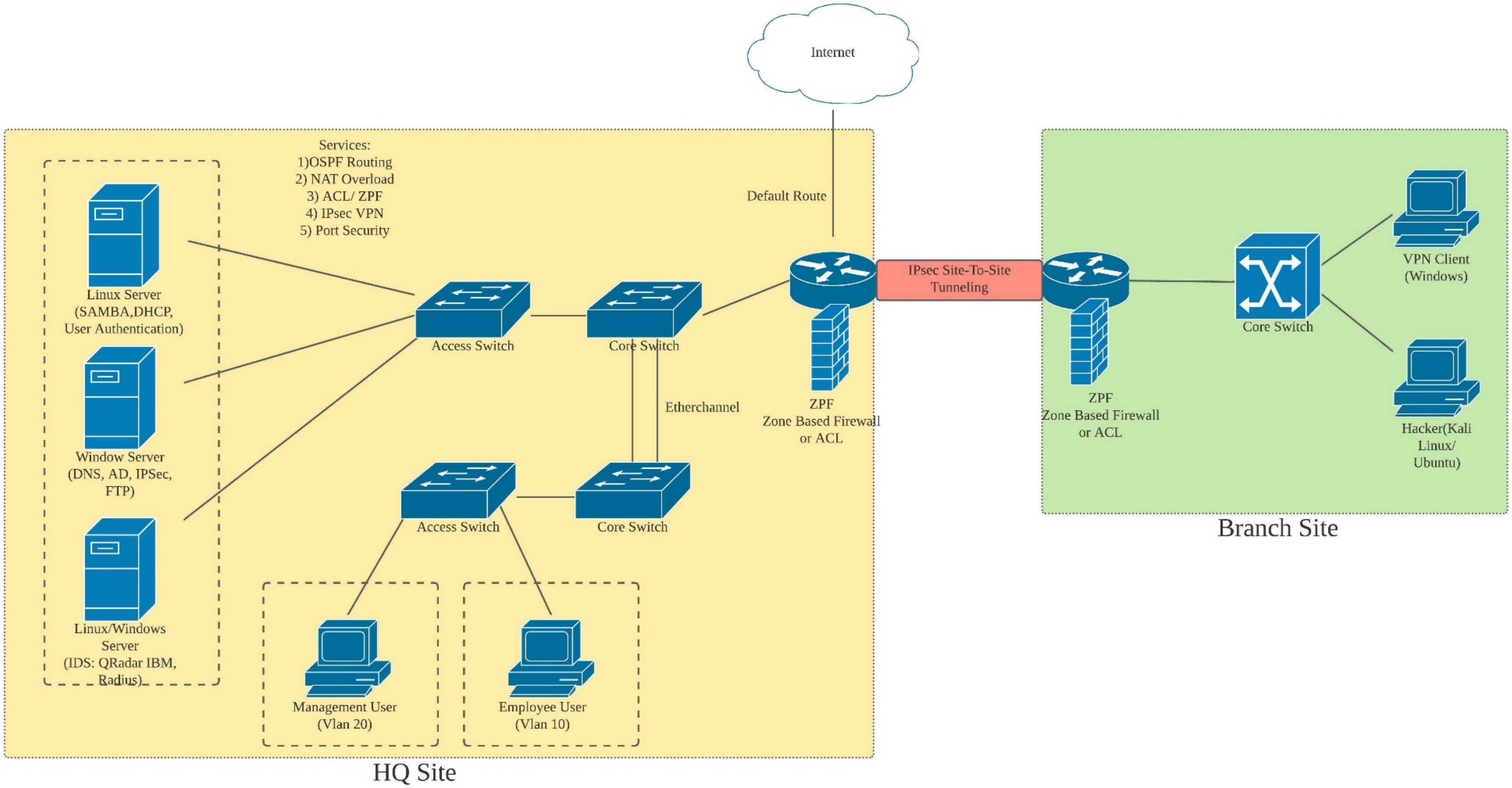


Diagram 1: The Logical Network Diagram

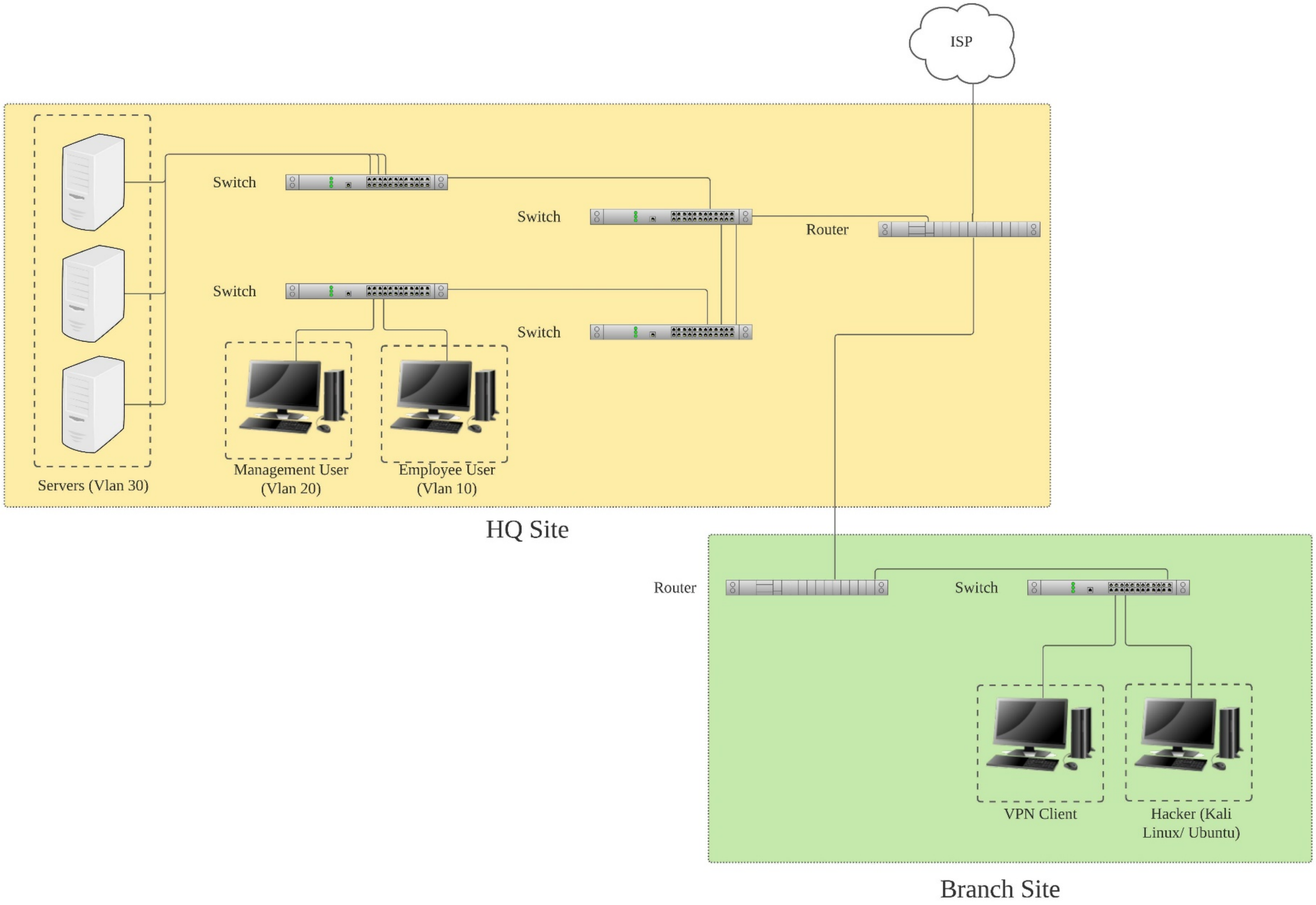


Diagram 2: The Physical Network Diagram

VLAN	VLAN Name	Network ID	Broadcast ID	Available IP
10	Employee	10.10.0.0/16	10.10.255.255/16	10.10.0.1 – 10.10.255.254 (65534 Hosts)
20	Management	10.20.0.0/18	10.20.63.255/18	10.20.0.1 – 10.20.63.254 (16382 Hosts)
30	Server	10.30.0.0/24	10.30.0.255/24	10.30.0.1 - 10.30.0.254 (254 Hosts)
40	Wireless	10.40.0.0/23	10.40.1.255/23	10.40.0.1 - 10.40.1.254 (510 Hosts)

Table 1: VLSM Addressing Table

(7.0) SECURITY POLICY

Security policy is a written document in an organization outlining how to protect the organization from threats, including computer security threats, ad how to handle the situations when they occur. The security policy was published to protect the computer network against any harmful actions or malicious activity by giving the guidelines to enforce, monitor, and maintain the computer network security. The secure network infrastructure is designed to ensure the CIA, which is confidentiality, integrity, and availability of the company's information are being protected. In addition, it is essential to protect the system and data from unauthorized access, unauthorized manipulation or modification, and protection against any cyber-attack in the company system.

- **Software Installation Policy**

  Most software nowadays is not freeware. Therefore, the cost of software is a consideration for their deployment. It is the responsibility of the organization to ensure the license are accurate and up to date. IT department is responsible for purchasing a software license for the following software categories:

  - Operating System Software.
  - Internet Software.
  - Productivity tools package.

  The other software categories are the responsibility of the Head of Department in which they serve. The software installation policy is used to protect the organization from unauthorized software that sometimes has several viruses that can infect each computer and network.

- **Server Security Policy**

  Every Server Administrator at the organization must take reasonable security measures to secure their hosts as outlined in the policy. Servers should be placed in physically attached areas accessible only to authorized personnel. It is the responsibility of the administrator to:

- Regularly scan all the servers using updated virus detection software.
- The accounts must be periodically reviewed for inactivity and any dormant accounts disabled.
- Ensure that logs of user activity must be retained for some time. Keep the records for at least six months.

- **Remote Access Policy**

  It is the responsibility of the organization requesters and approvers with remote access privileges to the corporate network to ensure that their access privileges are more minor or minimal to carry out the functions. The requirements for this policy are:

  - All the remote access should be strictly controlled.
  - Users with remote access privileges must ensure that their computer firewall settings shall be turned on and constantly running when connecting to the organization group.
  - No dial-in access shall be permitted to bypass the organization firewall.
  - No time should any user share their login or password to anyone else, including family members and close friends.
  - Password Protection Policy

Passwords are an essential aspect of computer security. A poorly chosen password may result in unauthorized access and exploitation. This policy aims to establish the standard for creating a strong password and the protection for those passwords.

- ➢ Password creation is vital to protect from unauthorized access. To create a good password, you need to follow this guideline:

  (i) The password cannot contain all or part of the user account name or ID.

(ii) The password must be at least eight characters in length.

(iii) The password must contain uppercase, lowercase, number, AND symbol.

- We need to protect the password because all passwords must be treated as sensitive and confidential data. To preserve the password, we must:

  (i) Do not share the password with anyone, including family members.

  (ii) Do not hint at the format of the password, such as "my family name."

  (iii) Please do not write the passwords down and store them anywhere in the office.

  (iv) Encrypt the password when we store it in a file in a computer system or mobile device.

  (v) Do not use "Remember Password."

(8.0) GANTT CHART

In Section (12.0) Appendices.

(9.0) TASKS DISTRIBUTION

In Section (12.0) Appendices

(10.0) CONCLUSION

Workshop 2 has given the best platform for us to experience the real environment of working. Other than that, we have learned the skills that we are unable to learn during class in previous semester. It allows us to discuss and interact about a given topic which may be the useful skills for us to handle the real working environment. In Workshop 2, we are learning about how to design a secure network infrastructure using any tools and software that available and suitable for our network infrastructure as well as how to implement the network that has been designed by our group with the services given to us.

Besides that, we need to install some of applications and software. From that, we are learning how to use it, how to configure, how to control the secure network services using the knowledge that we have but of course we are in the learning phase so might be we never learn that before, but we are putting effort on how to find the solution by searching the answer on Google.

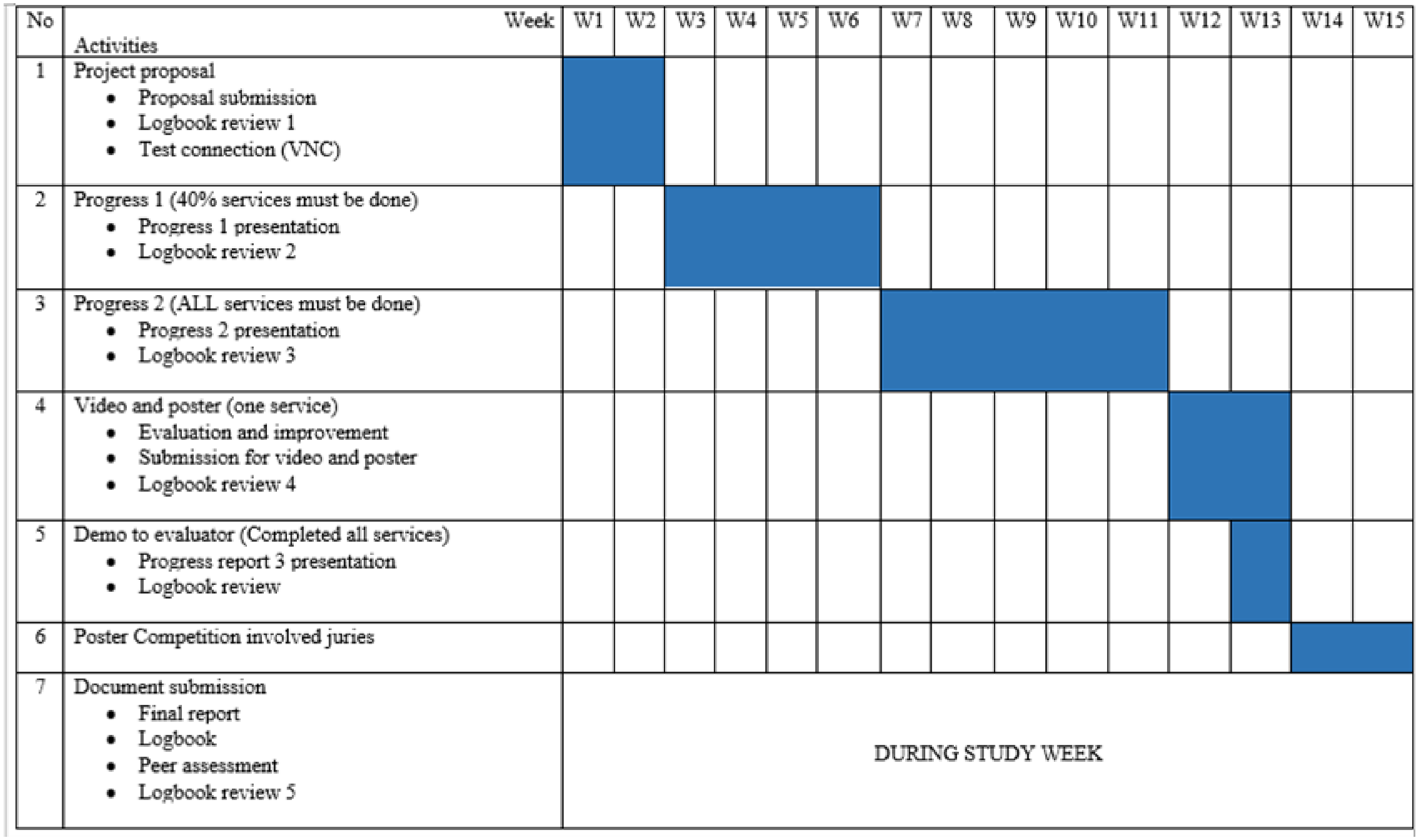
In conclusion, we will do this project in group with the guidance from our supervisor. In a group, cooperation from each of the group members are necessary to achieve the objectives of this project. In addition, good planning of this project also will be the main reason for our group to succeed. Lastly, we will gain more knowledge and skills in this project so that we will prepare ourselves for the working environment soon.

(11.0) REFERENCES

1. Wesley Chai, Alexander S.Gillis. June 2021. *What is Active Directory and how does it work?* *https://searchwindowsserver.techtarget.com/definition/Active-Directory*
2. Barracuda. *What is an Intrusion Detection System?* *https://www.barracuda.com/glossary/intrusion-detection-system#:~:text=An%20intrusion%20detection%20system%20(IDS,information%20and%20event%20management%20system*.
3. Yigal Amram. November 2018. *To SPAN the virtual network.* *https://blog.niagaranetworks.com/blog/to-span-the-virtual-network*
4. Cloudflare. *What is IPsec? | How IPsec VPN work.* *https://www.cloudflare.com/learning/network-layer/what-is-ipsec/*
5. The Official Samba Tree. *Samba-3 server types and security modes.* *https://www.informit.com/articles/article.aspx?p=169560&seqNum=3*
6. Cloudflare. *What is DNS? | How DNS works.* *https://www.cloudflare.com/learning/dns/what-is-dns/*
7. Infoblox. *What is Domain Name System (DNS)?* *https://www.infoblox.com/glossary/domain-name-system-dns/*
8. Efficient iP. *What is DHCP?* *https://www.efficientip.com/what-is-dhcp-and-why-is-it-important/*
9. Zenlayer. *What is an Access Control List (ACL)?* *https://www.zenlayer.com/blog/what-is-access-control-list/*
10. Foxpass. *RADIUS Server (RADIUS Authentication) and how it works.* *https://www.foxpass.com/blog/radius-server-and-how-it-works*
11. Edem Afenyo. October 2020. *How to join a Linux system to an Active Directory domain.* *https://www.redhat.com/sysadmin/linux-active-directory*
12. Cisco. *Configuring port security*. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/44sg/configuration/guide/Wrapper-44SG/port_sec.pdf
13. Netwrix. *Windows Server security best practices.* *https://www.netwrix.com/windows_server_hardening_checklist.html*

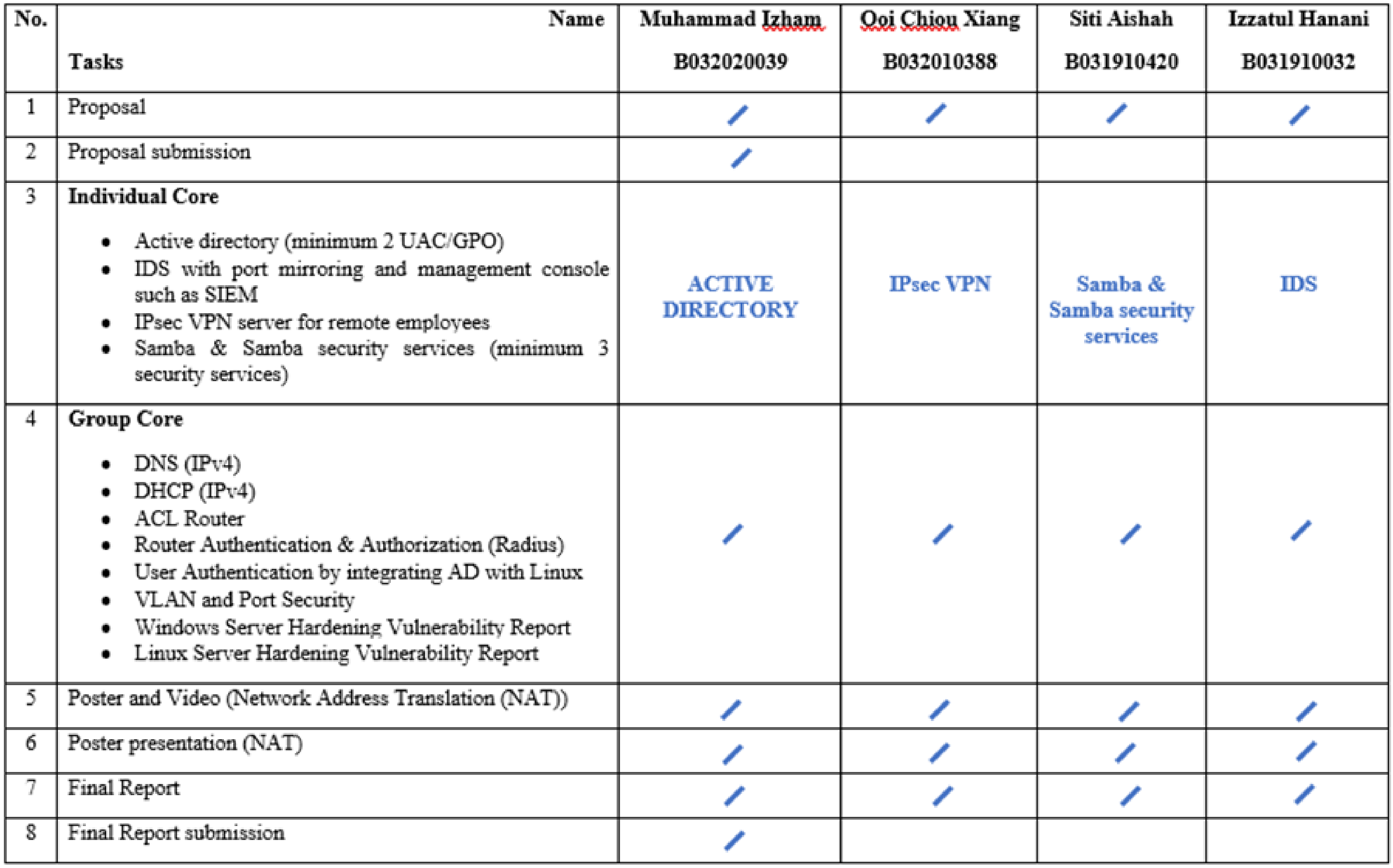
14. Yevgeniya Davydov. August 2020. *Linux Server Security: 10 Linux hardening & and security best practices.* https://securityboulevard.com/2020/08/linux-server-security-10-linux-hardening-security-best-practices/
15. Techopedia. January 2017. *Security policy.* https://www.techopedia.com/definition/4099/security-policy
16. Preteshbiswas. February 2020. *Example of software installation policy.* https://isoconsultantkuwait.com/2020/02/02/example-of-software-installation-policy/
17. Baylor University. April 2020. *Server security policy.* https://www.baylor.edu/risk/doc.php/341714.pdf
18. Project Practical. *Sample remote access policy.* https://www.projectpractical.com/sample-remote-access-policy-free-download/
19. Connecticut College. *Password protection policy.* https://www.conncoll.edu/information-services/policies/password-protection-policy/

(12.0) APPENDICES



No	Week Activities	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15
1	Project proposal • Proposal submission • Logbook review 1 • Test connection (VNC)	■	■													
2	Progress 1 (40% services must be done) • Progress 1 presentation • Logbook review 2			■	■	■	■									
3	Progress 2 (ALL services must be done) • Progress 2 presentation • Logbook review 3							■	■	■	■	■				
4	Video and poster (one service) • Evaluation and improvement • Submission for video and poster • Logbook review 4												■	■		
5	Demo to evaluator (Completed all services) • Progress report 3 presentation • Logbook review													■		
6	Poster Competition involved juries														■	■
7	Document submission • Final report • Logbook • Peer assessment • Logbook review 5	DURING STUDY WEEK														

Table 1: Gantt Chart of the activities.



No.	Name Tasks	Muhammad Izham B032020039	Ooi Chiou Xiang B032010388	Siti Aishah B031910420	Izzatul Hanani B031910032
1	Proposal	✓	✓	✓	✓
2	Proposal submission	✓			
3	**Individual Core** • Active directory (minimum 2 UAC/GPO) • IDS with port mirroring and management console such as SIEM • IPsec VPN server for remote employees • Samba & Samba security services (minimum 3 security services)	ACTIVE DIRECTORY	IPsec VPN	Samba & Samba security services	IDS
4	**Group Core** • DNS (IPv4) • DHCP (IPv4) • ACL Router • Router Authentication & Authorization (Radius) • User Authentication by integrating AD with Linux • VLAN and Port Security • Windows Server Hardening Vulnerability Report • Linux Server Hardening Vulnerability Report	✓	✓	✓	✓
5	Poster and Video (Network Address Translation (NAT))	✓	✓	✓	✓
6	Poster presentation (NAT)	✓	✓	✓	✓
7	Final Report	✓	✓	✓	✓
8	Final Report submission	✓			

Table 2: Task distribution

GROUP MEMBERS SIGNATURE

NAME AND SIGNATURE	DATE
Ooi Chiou Xiang	15/10/2021
Izzatul Hanani binti Kamarul Nizar	15/10/2021
Siti Aishah binti Mustafa	15/10/2021
Muhammad Izham bin Norhamadi	15/10/2021

SUPERVISOR SIGNATURE **DATE: 21 October 2021**

Khadijah

KHADIJAH BINTI WAN MOHD GHAZALI
LECTURER
FACULTY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

COMMENT: Thank you for re-making this proposal in response to my comments for the 1st draft. This final proposal contains a lot of comments too. However, please don't remake the proposal as you need to move to the next milestone. Instead, reflect your improved reporting based on this comment in the writing of your final report.