WORKSHOP II IMPLEMENTATION FOR BITZ 2021

1.1 Learning Outcomes

a) Student should be able to design the secure network infrastructure by using the available tools.
b) Student should be able to implement designated network and security services.
c) Student should be able to install and secure integrate network services infrastructure to suit the network environment.
d) Student should be able to maintain and control the secure network services infrastructure.

1.2 Other Related Subjects

The scope of the project for BITZ program is related to the following subjects:

- ✓ BITS 1123 – Computer Organization and Architecture
- ✓ BITS 1213 – Operating System
- ✓ BITS 1323 – Data Communication & Networking
- ✓ BITS 2343 – Computer Network
- ✓ BITS 2413 – Network Security Infrastructure & Design
- ✓ BITS 2513 – Internet Technology
- ✓ BITS 3363 – Network Security Project Management

1.3 Project Scenario Description

Company XYZ is expanding with approximately 100 employees and is in the process of setting up a new IT department. The company is divided into two sites. The HQ site, where the main server is homed, and the clients connect to and the remote site (Branch). The sites relate to a simple point-to-point internetworking that can be used to carry packets between the sites. As the company has multiple sites, you have to use dynamic routing connections.

You work as an IT infrastructure manager for the company. Fortunately, your team have a lot of IT experience and agree to configure the IT environment for the company. Your job is to setup the secure infrastructure for company XYZ that covers all networking functions for internal and external IT communications that comprises several services as in Table 1 and Table 2 or Table 3.

1.4 Project Implementation

a) Each group consists of **3 or 4** BITZ students.
b) Each group of **BITZ** students must implement **ALL** network and security services which have been determined as a **Group Work** and **Individual Core and Group Core**. *(Refer to Table 1, Table 2 or Table 3)*
c) Each group is required to fairly distribute tasks to each member of the group.

    i. **ALL** members of the group must be responsible for the proposal, Inter VLAN and VLSM addressing and security policy.
    ii. Each student must be responsible for **ONE (1)** service from **individual core.**
    iii. Each group must be responsible for **ALL** service in **group Core**.
    iv. Each student must also be responsible for **ALL** services performed by the group members.

d) Each group needs to ensure that **remote access** to the server at the laboratory is **tested first before end of week 1**. The VNC application for remote desktop applications has been installed in prior at the pre-determined workstation. **Consultation** with supervisor is necessary to setup this remote connection.
e) Each group needs to install and use **THREE VMs** as servers at HQ Site (**VM1** with **Windows** platform, **VM2** with **Linux** platform and **VM3** with **Windows/Linux** platform). Furthermore, the Remote Site (Branch) must comprise **TWO VMs** to act as a client and attacker. Use **GNS3** to simulate the network topology and connect **ALL** Virtual Machine. Below is an example of services that can be considered for each VMs servers. You may need to use BGP or OSPF or other tools for point-to-point connection between Branch and HQ routers.

    HQ Site (Servers)
    VM1 (Linux): Samba, DHCP and User Authentication
    VM2 (Windows): DNS, AD, IPsec, and FTP
    VM3 (Linux or Windows): IDS and Radius Server

    Remote Site (Branch)
    VM1: Client 1 -> To test IPsec
    VM2: Client 2 -> Act as an attacker

1.5 Project Scope

a) Each group is required to **design a secure network infrastructure** by using the available or selected tools.
b) Each group is free to develop their own network design.
c) Each group **MUST** install the following services/applications in their network environments.

Table 1: Services/Configuration for ALL Students (Groupwork)

Inter VLAN routing and Network Address Translation (NAT)
VLSM addressing (provide addressing table in the proposal)
Security Policy (all rules and procedures must be implemented)

Table 2: Services/Configuration for BITZ (applicable for 4 students only)

Individual Core (1 Service/Student)	Group Core (ALL)
1. **Active directory (minimum 2 UAC/GPO)** 2. **IDS with port mirroring and management console such as SIEM (QRadar).** 3. **IPsec VPN server for remote employees.** 4. **Samba & Samba security services (minimum 3 security services)**	1. DNS (IPv4) 2. DHCP (IPv4) 3. ACL Router 4. Router Authentication & Authorization (Radius) 5. User authentication by integrating AD with Linux 6. VLAN and Port Security 7. Windows Server Hardening Vulnerability Report 8. Linux Server Hardening Vulnerability Report

Table 3: Services / Configuration for BITZ (applicable for 3 students only)

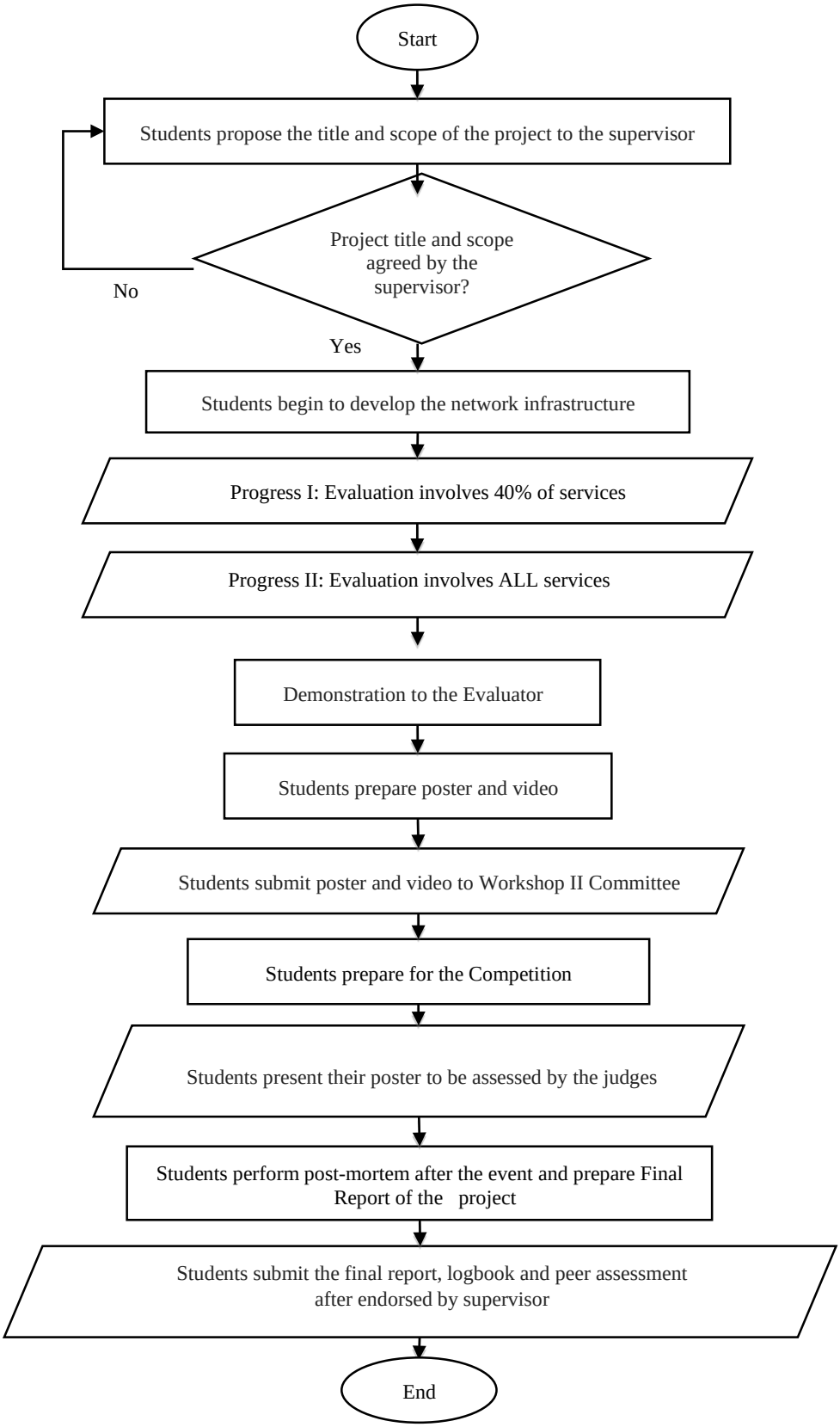
Individual Core (1 Service/Student)	Group Core (ALL)
1. **Active directory (minimum 2 UAC/GPO)** 2. **IDS with port mirroring and management console such as SIEM (QRadar).** 3. **IPsec VPN server for remote employees.** 4. **Samba & Samba security services (minimum 2 security services)**	1. DNS (IPv4) 2. DHCP (IPv4) 3. ACL Router 4. Router Authentication & Authorization (Radius) 5. User authentication by integrating AD with Linux 6. VLAN and Port Security 7. Windows Server Hardening Vulnerability Report

Each group MUST **propose and implement** its own network services (including the above-mentioned services) until adequate to **ALL services / configurations**.

d) Each group will need to **install and integrate network services infrastructure** to suit the network environment and security policies that have been set.

e) Each group must use **different operating systems** such as Windows Server and Linux.

1.6 Implementation Process Flowchart



1.7 Project Requirements

a) Each group is provided with the following software:

1) Host preinstalled with Windows 10
2) Installer:
    - iso Ubuntu 16
    - iso Windows 2012
    - VMware
    - SIEM (QRadar)
    - Remote Desktop Connection (VNC)
    - GNS3

b) By using the software provided, each group is required to design, install, maintain, and secure the simulated network environment with stated basic client applications and services.

1.8 Project Deliverables

1.8.1 Project Proposal

Each group must submit their plan and project proposal and at the beginning of the semester. Project proposal must include the following items:

1) Executive Summary
2) Network Design (Logical)
3) Network Design (Physical)
4) Project Plan based on Gantt Chart
5) Task distribution

Proposal Content

1.0 Introduction
2.0 Problem Statement – problem that needs to be solved in this project
3.0 Objective – objectives that need to be achieved in this project
4.0 Organization chart
5.0 Requirements Analysis
4.1 Platform and equipment analysis – justification
4.2 Application and services analysis – justification
6.0 Network Design
7.0 Draft Security Policy
8.0 Project Planning based on Gantt Chart
9.0 Individual tasks
10.0 Conclusion
11.0 References
12.0 Appendices – Gantt Chart (required), etc…

1.8.2 Logbook

a) Each member of the group is required to submit their logbook to the supervisor.
b) Marks are based on individual logbook which the student must report to supervisor on the progress for each task. Supervisor will monitor the project and signing the logbook as a confirmation.
c) The content of the logbook for each week should include:

- Summary of the task.
- Problems encountered during the Workshop 2.
- Supervisor comment and result of the discussion with the supervisor.

1.8.3 Progress I

Progress I cover the development of the project where each group is required to complete **ALL Group Work** and **individual core services**.

1.8.4 Progress II

a) Progress III covers the development of the project where each group is required to complete **ALL** configuration, services, and network environment.

b) Each group is required to hold a demonstration to supervisor for evaluation purpose. Each member of the group is required to present **ALL** services that has been setup.

1.8.5 Demo/Final Presentation

a) Each group is required to hold a demonstration with evaluator. Each member of the group is required to present **ALL** services that has been setup.

1.8.6 Poster and Video

a) Each group is required to prepare a poster and video that explain **ONE** service that has been set.

b) The content of the poster and video should include the following items:

- A brief introduction about the collection and segregation of duties.
- The introduction of such services includes the usability, advantages, and disadvantages.
- Background theory of the services and method for configuring the service.

- Method to test the service.
- The total duration of the video **should not exceed 10 minutes** and the Video content from outside source **should not exceed 20%**.

c) Video and poster (softcopy) should be presented to supervisor for the purpose of updates or revision. The actual assessment will be conducted during the exhibition day.

1.8.7 Competition

a) During the competition, **ONE (1)** pre-determined service will be evaluated by judges.

b) Each student must be prepared to answered questions from the judges which is not just about the service under evaluation, but also for **ALL** the services carried out during the Workshop 2.

1.8.8 Final Report

Each group should provide **TWO (2)** copies of the final report for submission to the supervisor and evaluator.

Example: Content of Final Report

4.0 Chapter 4: SERVICES

- 4.1 Introduction
- 4.2 List of services
- 4.3 Brief overview for services
  - 4.3.1 DNS 4.3.2 DHCP
  - 4.3.3 ...
- 4.4 Conclusion

5.0 Chapter 5: INSTALLATION AND CONFIGURATION

- 5.1 Introduction
- 5.2 Services testing and individual who responsible for the testing
  - 5.2.1 DNS Testing
  - 5.2.2 SMTP Testing
  - 5.2.3 …
- 5.3 Conclusion

6.0 Chapter 6: TESTING

- 6.1 Introduction
- 6.2 Services testing
  - 6.2.1 DNS Testing
  - 6.2.2 SMTP Testing
  - 6.2.3 …….
- 6.3 Conclusion

7.0 Chapter 7: CONCLUSION

- 7.1 Introduction
- 7.2 Project advantages
- 7.3 Project disadvantages
- 7.4 Project limitation
- 7.5 Conclusion

BIBLIOGRAPHY
APPENDIX

1.9 Project Activities (Milestone)

WEEKS (DATE)	ITEM	ACTION
W1-W2 (04/10/2021-17/10/2021)	**Project Proposal** Includes: Executive Summary Organization Chart Network Design (Logical and Physical) VLSM Addressing Gantt charts and Project Distribution. **Device Setup** The student must ensure that the provided PCs at the Lab can be accessed from home using remote desktop connection via **VNC Viewer**.	**Proposal Submission (ULearn)** **Logbook Review 1** **Test Remote Connection Access**
W3-W6 (18/10/2021-14/11/2021)	**Progress I** Presentation of project progress: setup minimum **40%** services.	**Present Progress I** **Logbook Review 2**
W7-W11 (15/11/2021-19/12/2021)	**Progress II** Presentation of project progress: completed all services **100%**. The student is required to **demonstrate their individual and group progress respectively to the supervisor.**	**Present Progress II Logbook Review 3**
W12 (20/12/2021-26/12/2021)	**Video & Poster** Video and poster preparation involves **ONE (1) service** that has been set by the coordinator. **Video and poster** (softcopy) should be presented to supervisor earlier for the purpose of re-evaluation before submitting at week 12.	**Video & Poster Submission (ULearn)** **Logbook Review 4**
W13 (27/12/2021-02/01/2022)	**Demonstration** The student is required to **demonstrate their individual and group task respectively to the evaluator**.	**Final Presentation (Online)**
W14 (03/01/2022-09/01/2022)	**Workshop II Competition** Video is pre-evaluated by the juries. Only **poster** is evaluated in an online session by the juries on the competition day.	**Workshop II Competition (Online)**

Study Week W15 (10/01/2022-16/01/2022)	**Final Report, Peer Assessment Report, and Logbook** The student is required to **submit all the documents** after getting endorsement from the supervisor.	**Final Report, Peer Assessment Report, and Logbook Review 5 & Submission to SV**

1.10 Evaluation

Students will be evaluated based on the results of work in terms of commitment, reports, and presentations of development of network infrastructure and security services implemented. Distribution of marks is shown below:

No.	Outcome	Marks	
		Individual	Group
1	Proposal	5%	-
2	Progress I	15%	
3	Progress II		15%
4	Demonstration (Evaluator)	10%	
5	Showcase, poster, and video		25%
6	Final Report	-	20%
7	Logbook	5%	-
8	Peer Evaluation	5%	-