WORKSHOP 2 BRIEFING BITZ

SEM 1 SESI 2021/2022

29 SEPT 2021

Agenda

01 Learning Outcome

02 Project Scenario Description

03 Project Implementation

04 Service Configuration

05 Project Requirements

06 Video & Poster

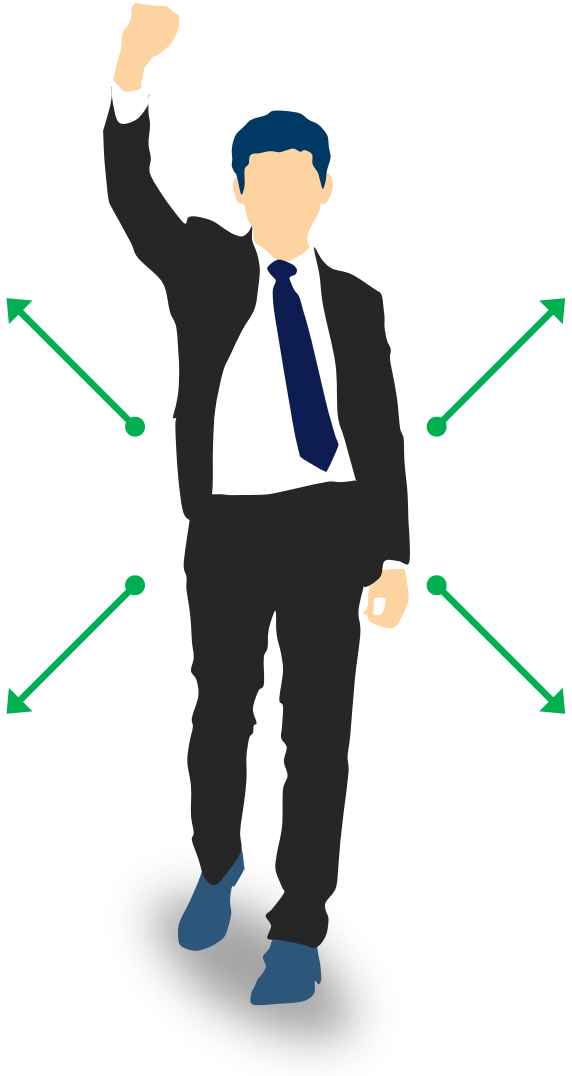
07 Project Milestone

08 Project Evaluation

01 LEARNING OUTCOME

1
Student should be able to ***design the secure network infrastructure*** by using the available tools.

4
Student should be able to ***maintain and control the secure network services infrastructure***.



2
Student should be able to ***implement designated network and security services***.

3
Student should be able to ***install and secure integrate network services infrastructure*** to suit the network environment.

02 PROJECT SCENARIO DISCRIPTION

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. Because in the real scenario the company has multiple sites, you decided 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.

03 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.

03 PROJECT IMPLEMENTATION

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.

03 PROJECT IMPLEMENTATION

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

04 SERVICE CONFIGURATION (GROUP TASK-ALL STUDENTS)

Design

Each group is required to **design a secure network infrastructure** by using the available tools

Develop

Each group is free to **develop** its own network design

Installation

Each group **MUST** install the stated services/applications in their network environments

Propose & Implementation

Each group MUST **propose and implement** its own network services (including the above-mentioned services) until adequate to **12 services / configurations**.

Integration

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

Operating Systems

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

Services

ALL server must have **TWELVE (12) services** from the services mentioned above.

Configuration

Configuration and test must be carried out using remote desktop application.

04 SERVICE CONFIGURATION (GROUP TASK-ALL STUDENTS)

Service 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)

Jabatan Sistem dan Komunikasi Komputer, Fakulti Teknologi Maklumat dan Komunikasi UTeM

04 SERVICE CONFIGURATION (BITZ STUDENTS)

Individual Core (Main)	Group Core
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

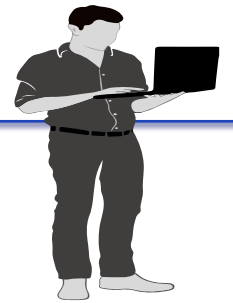
Individual Core (Main)	Group Core
1. Active directory (minimum 2 UAC/GPO) 2. IDS with port mirroring and management console such as SIEM (QRadar). 3. IPsec VPN server for remote employees. 4. Samba & Samba security services (minimum 2 security services)	1. DNS (IPv4) 2. DHCP (IPv4) 3. ACL Router 4. Router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

05 PROJECT REQUIREMENTS

a) Each group is provided with the following software:
b) Host preinstalled with Windows 10
c) Installer:

- ✓ iso Ubuntu 16
- ✓ iso Windows 2012
- ✓ VMware
- ✓ SIEM (QRadar)
- ✓ Remote Desktop Connection (VNC)
- ✓ GNS3

d) 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.



06 POSTER & 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 include the usability, advantages and disadvantages.
- Background theory of the services
- The method for configuring the service and to test the service.
- The total duration of the video **should not exceed 10 minutes**.
- 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.

07 PROJECT MILESTONE

SEM1 2021/2022

ITEM	WEEKS	ACTION
Project Proposal	Weeks 1-2	Proposal Submission, Log Book Review 1 & Test Connection (VNC)
Progress 1 (40%)	Weeks 3-6	Progress 1 Presentation & Logbook Review 2 (minimum 40% services)
Progress 2 (ALL)	Weeks 7-11	Progress 2 Presentation & Logbook Review 3 (ALL services)
Demo (Evaluator)	Weeks 13	Progress Report 3 Presentation & Logbook Review (completed all services 100%)
Video & Poster (1 Service)	Weeks 12-13	Evaluation, Improvement, Submission & Logbook Review 4
Poster Competition (Juries)	Week 14/15	Online
Document Submission	Study Week	Submission of Final Report , Logbook & Peer Assessment Logbook Review 5

08 PROJECT EVALUATION

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

No.	Outcome	Marks	
		Individual	Group
1	Proposal	5%	-
2	Progress I (40%)	15%	
3	Progress II (ALL)		15%
4	Demo (Evaluator)	10%	
5	Showcase, poster and video		25%
6	Final Report	-	20%
7	Logbook	5%	-
8	Peer Evaluation	5%	-
Total Marks		40%	60 %

Fakulti Teknologi Maklumat dan Komunikasi

Jabatan Sistem dan Komunikasi Komputer, Fakulti Teknologi Maklumat dan Komunikasi UTeM

TERIMA KASIH

s.m.warusia@utem.edu.my (Dr Warusia)