ASSIGNMENT BRIEF

HTU Course No: 10203210	**HTU Course Name:** Network Security
BTEC Unit No: L/615/1646	**BTEC UNIT Name:** Network Security

Version: 3

Student Name/ID Number/Section	
HTU Course Number and Title	10203210 Network Security
BTEC Unit Number and Title	L/615/1646 Network Security
Academic Year	2023-2024 Fall
Assignment Author	Fawaz Khasawneh
Course Tutor	
Assignment Title	TechGlobal
Assignment Ref No	1
Issue Date	25/11/2023
Formative Assessment dates	From 01/12/2023 to 11/01/2024
Submission Date	29/01/2024
IV Name & Date	Eyad Taqieddin 24/11/2023

Submission Format

Each student is expected to individually submit his/her work including:

a) **An individual written report** ***in Word format*** covering the required details in the (Assignment Brief and Guidance) section. ***Including signed student assessment submission and declaration form.***

b) **Evidence** of the implemented network (**soft copy of the .pkt** file). Students should use the **Cisco Packet Tracer** simulator **version 8.2 or greater.**

c) **Discussion about the report and the implemented work.** Instructions, date, and time for the discussion will be provided later. A witness statement or observation record is considered as evidence for this part.

PS: Files should be uploaded separately rather than in a zipped file.

Report guidelines:

The report should be written in a concise, formal business style using single spacing and font size 12 with use of headings, paragraphs and subsections as appropriate (Cover page, table of contents, and an introduction to provide an overview of your report.). The expected word limit is about 5000 words, *although you will not be penalised for exceeding the total word limit*. The report must be supported with research and referenced using the Harvard referencing system.

Note:

Soft copies submissions should be done through the university's eLearning system (https://elearning.htu.edu.jo) by the deadline assigned above.

Unit Learning Outcomes

LO1 Examine network security principles, protocols and standards

LO2 Design a secure network for a corporate environment

LO3 Configure network security measures for the corporate environment

LO4 Undertake the testing of a network using a Test Plan.

Assignment Brief and Guidance

You have recently become an employee of TechGlobal Inc., a prominent technological company that specializes in cloud computing and artificial intelligence technologies. TechGlobal Inc. is headquartered in Amman, Jordan, and is extending its activities by establishing additional offices in Turkey, Kuwait, Aqaba, and Tunisia. You play a critical role in maintaining the network security and effectiveness of the business, particularly in light of the growing threat of cyberattacks.

TechGlobal Inc. needs a secure and reliable network architecture to interconnect its worldwide offices and data centers. Your main responsibility is to design a network that guarantees the Confidentiality, Integrity and Availability (CIA) of the company's data and services. During your security check of the network, you discovered that not all the necessary network security best practices were being applied.

TechGlobal's main data center is located in the same building as the headquarters in Amman, although it has been established as a separate virtual subnet within the HQ networks. To enable access and sharing of project data and promote collaboration among employees, it is necessary to provide connectivity between the remote offices and the data center network, as well as between the remote offices themselves. As per the business needs, employees at TechGlobal offices must utilize the Employee Information System, a secure website located at (https://eis.techglobal.com.jo), to access and share project tasks and data internally. System access must be performed exclusively through the Fully Qualified Domain Name (FQDN). Furthermore, it is necessary for employees to have access to both the Mail and FTP servers.

Based on your demonstrated expertise in network security principles, your team leader has assigned you the responsibility of proposing a design, according to the specifications provided, and simulating it using the Packet Tracer network simulator to evaluate its feasibility prior to implementation. The specifications are as shown below:

HQ datacenter:

- People: 3 administrators.
- Resources: 3 PCs, one server with (HTTP, HTTPS, FTP, DHCP, and DNS) services.
- Each device in this subnet must have a dynamic IP address except for (the servers, PC1, and the gateways must be static)

Each TechGlobal remote office including Amman Office:

- Resources: one PC per subnet used to access the e-services required using wired connection
- Each station must use a different IP subnet than the other remote offices or HQ VLANS.
- Each device in each subnet must have a static IP address.

All needed IP subnets are below:

VLAN#	Site Name (VLAN Name)	VLAN Subnet IP	Device IP
15	Data Center (DC)	15.0.0.0/8	Server 15.0.0.100 PC1 15.0.0.10 GW 15.0.0.1
25	HQ Employees (EMP)	25.0.0.0/8	PC1 25.0.0.10 GW 25.0.0.1
35	HQ Human Resources (HR)	35.0.0.0/8	PC1 35.0.0.10 GW 35.0.0.1
45	HQ Guests (GN)	45.0.0.0/8	PC1 45.0.0.10 GW 45.0.0.1

LAN #	Name / Place	LAN Subnet IP	Device IP
1	AQABA VLAN 55	55.0.0.0/8	PC1 55.0.0.10 GW 55.0.0.1
2	AQABA VLAN 65 DC	65.0.0.0/8	PC1 65.0.0.10 GW 65.0.0.1
3	KUWAIT	75.0.0.0/8	PC1 75.0.0.10 GW 75.0.0.1
4	TURKEY	85.0.0.0/8	PC1 85.0.0.10 GW 85.0.0.1
5	TUNISIA	95.0.0.0/8	PC1 95.0.0.10 GW 95.0.0.1
6	WAN HQ-AQABA	105.0.0.0/8	HQ-INT 105.0.0.1 AQ-INT 105.0.0.2
7	WAN HQ-TUNISIA	115.0.0.0/8	HQ-INT 115.0.0.1 TU-INT 115.0.0.2
8	WAN HQ-KUWAIT	125.0.0.0/8	HQ-INT 125.0.0.1 KU-INT 125.0.0.2
9	WAN HQ-TURKEY	135.0.0.0/8	HQ-INT 135.0.0.1 TU-INT 135.0.0.2

After evaluating the client's requirements, it was determined that the following should be achieved in the secure network:

The networks situated outside of Jordan must be linked to the Amman data center via a VPN/IPsec site-to-site connection.

All switches and routers must be hardened to avoid any malicious activity. This involves the use of strong passwords, using SSH instead of telnet shutting down any unused ports, applying port security with maximum MAC address of two, and applying DHCP security (protect from spoofing and starvation with rate limit of 5)

Proper routing must be supported. DO NOT USE STATIC ROUTING.

The server in VLAN 15 are accessible by other VLANs according to the following rules:

HTTPs server is accessible by all VLANs and LANS.

Mail server is accessible by all VLANs and LANS.

DNS server is accessible by all VLANs and LANS.

FTP server is accessible by only the HQ EMP, and Aqaba office.

DHCP server is accessible by only HQ datacenter VLAN.

HTTP server is accessible only by HQ EMP LAN.

Configure Local AAA Authentication for VTY Lines for SSH protocol on TUNISIA router with username (ADMIN) and password (@SecureP@$$W0rd#).

The Aqaba office is set to function as a disaster recovery site, featuring two separate VLANs. The first VLAN will serve the Aqaba office, while the second VLAN will house a redundant HTTPS server. You should use ASA firewall instead of router and configure it according to the following rules:

- ○ SSH service on Aqaba ASA firewall is accessible only by HQ Datacenter PC1 (15.0.0.10).
- ○ Configure the DMZ for VLANS (VLAN 55 Private inside ,VLAN 65 DMZ , Aqaba WAN as Public Outside)

Part 1: Design and configure a secure network for TechGlobal headquarter and remote offices:

1. Design a secure networked system to meet the business requirements listed above. You should include in your report a written step-by-step plan on how you are going to design a secure networked system, a clear blueprint of your overall network including all devices in all locations (you can use a packet tracer snapshot).
2. Investigate the purpose and requirements of the secure network according to the given scenario.
3. Determine which network hardware and software to use in the network.
4. Examine the various categories of devices employed for ensuring network security.
5. Analyze the network security protocols and the application/discussion of distinct cryptographic methodologies/types within the domain of network security.
6. Design and implement a secure network prototype according to the given scenario using Packet Tracer simulator.

7. Configure Network Security measures for your network. Those measures include Firewalls, Routers, Switches, Gateways, passwords, SSH, SSL, IPSec, VPN, HTTPs, FTPs, DHCP and DNS. And provide a justification for the choices made in the network security configuration that was implemented along with the network security configuration scripts/files/screenshots with comments.
8. Draw comparisons and contrasts between at least two significant network security protocols.
9. Evaluate the importance of network security to an organization.

Part 2 : Evaluation and testing of network security through the implementation of a Test Plan.

1. Create a test plan for your network. Your test plan should consider different testing methods in terms of checks on network security, testing for network vulnerabilities etc.
2. Comprehensively test your network using the devised test plan. Tests should be carried out on all devices (Firewall, Servers, Routers, Switches, gateways, passwords). Record the test results and analyze these against expected results. You need to provide scripts/files/screenshots of the testing of your network.
3. Critically evaluate the design, planning, configuration and testing of your network security. Make some improvement recommendations.
4. Review what is meant by Quality of Service (QoS) in relation to Network Security configuration and how the security configuration can affect the Quality of Service.

Learning Outcomes and Assessment Criteria			
Learning Outcome	**Pass**	**Merit**	**Distinction**
LO1 Examine network security principles, protocols and standards	**P1** Discuss the different types of Network Security devices. **P2** Examine Network Security protocols.	**M1** Compare and contrast at least two major Network Security protocols.	**D1** Review the importance of network security to an organization.
LO2 Design a secure network for a corporate environment	**P3** Investigate the purpose and requirements of a secure network according to a given scenario. **P4** Determine which network hardware and software to use in this network.	**M2** Create a design of a secure network according to a given scenario.	
LO3 Configure network security measures for the corporate environment	**P5** Configure Network Security for your network. **P6** Discuss different cryptographic types of Network Security.	**M3** Provide Network Security configuration scripts/files/screenshots with comments.	**D2** Review what is meant by Quality of Service (QoS) in relation to Network Security configuration.
LO4 Undertake the testing of a network using a Test Plan.	**P7** Create a Test Plan for your network. **P8** Comprehensively test your network using the devised Test Plan.	**M4** Provide scripts/files/screenshots of the testing of your network. **M5** Make some improvement recommendations.	**D3** Critically evaluate the design, planning, configuration and testing of your network.

STUDENT ASSESSMENT SUBMISSION AND DECLARATION

When submitting evidence for assessment, each student must sign a declaration confirming that the work is their own

Student name:	**Assessor name:**	
Issue date: 25/11/2023	**Submission date:** 29/01/2024	**Submitted on:**

Programme: Computing

HTU Course Name: Network Security

HTU Course Code: 10203210

BTEC Course Title: Network Security

BTEC Course Code: L/615/1646

Assignment number and title: 1, TechGlobal

Plagiarism:

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalised. It is your responsibility to ensure that you understand **correct referencing practices.** As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.

Student Name:

Student Signature:

Date: