ASSIGNEMNT BRIEF

HTU Course No: 10203210 BTEC UNIT No: M/618/7443	HTU Course Name: Network Security BTEC UNIT Name: Network Security

Assignment Brief Number: 1

Version 1

Assignment Brief

Student Name/ID Number/Section	
HTU Course Number and Title	10203210 Network Security
BTEC Unit Number and Title	M/618/7443 Network Security
Academic Year	2022/2023 (Spring Semester)
Assignment Author	Eng. Sami Al-Mashaqbeh
Course Tutor	Dr. Eyad Taqieddin , Eng. Sami Al-Mashaqbeh. Eng. Mohammad Erdisat
Assignment Title	JNR Network Security
Assignment Ref No	Assignment 1
Issue Date	19-04-2023
Formative Assessment dates	26-04-2023 & 26-05-2023
Submission Date	19-06-2023
IV Name & Date	Dr. Safaa Hreiz

Submission Format

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

a) **An individual written report** covering the required details in the (Assignment Brief and Guidance) section.

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.

d) **An in-class written exam.** Instructions, date, and time for the exam will be provided later.

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 joined Jordan National Railway (JNR) as a Senior Network Security Engineer. JNR is a railway company in Jordan that operates a reliable freight railway network connecting key cities including the capital Amman, the major industrial city of Irbid, and the country's gateway port in Aqaba. The company's top management has decided to establish new offices in Saudi Arabia and Turkey to connect with the railways. As part of the project team responsible for connecting these new offices with the headquarters in Amman, your role includes ensuring the confidentiality, integrity, and availability (CIA) of data and related services. During your security check of the network, you discovered that not all the necessary network security best practices were being applied.

JNR's primary data center is situated in the same building as the headquarters in Amman, but it has been set up as a distinct virtual subnet within the HQ networks. In order to access and share project data and facilitate collaboration among employees, the remote offices need to be connected to the data center network as well as to each other. The business requirements specify that employees at JNR offices need to access the company's internal system for sharing project tasks and data via a secure website at ***(https://eis.jnr.com.jo)***, which is the Employee Information System. Access to the system should be done using the Fully Qualified Domain Name (FQDN). Additionally, employees need to access the Mail and FTP servers.

Your team leader noticed your strong understanding of network Security principles during the team discussion and has tasked you with proposing a design (based on the specifications provided below) and simulating it using the Packet Tracer network simulator to assess its feasibility before actual implementation. The specifications are as follows:

HQ datacenter:

People: 3 administrators.

Resources: 3 PCs, one server with (HTTP, HTTPS, FTP, DHCP, and DNS) services.

- Each device in each subnet must have a dynamic IP address except for (the servers and the gateways must be static).

Each JNR 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
10	Data Center (DC)	10.0.0.0/8	Server 10.0.0.100 PC1 10.0.0.10 PC2 10.0.0.20 PC3 10.0.0.30 GW 10.0.0.1
20	HQ Employees (EMP)	20.0.0.0/8	PC1 20.0.0.10 GW 20.0.0.1
30	HQ Human Resources (HR)	30.0.0.0/8	PC1 30.0.0.10 GW 30.0.0.1
40	HQ Guests (GN)	40.0.0.0/8	PC1 40.0.0.10 GW 40.0.0.1

LAN #	Name / Place	LAN Subnet IP	Device IP
1	AQABA VLAN 50	50.0.0.0/8	PC1 50.0.0.10 GW 50.0.0.1
2	AQABA VLAN 60 DC	60.0.0.0/8	PC1 60.0.0.10 GW 60.0.0.1
3	SAUDI ARABIA	70.0.0.0/8	PC1 70.0.0.10 GW 70.0.0.1
4	TURKEY	80.0.0.0/8	PC1 80.0.0.10 GW 80.0.0.1
5	IRBID	90.0.0.0/8	PC1 90.0.0.10 GW 90.0.0.1
6	WAN HQ-AQABA	100.0.0.0/8	HQ-INT 100.0.0.1 AQ-INT 100.0.0.2
7	WAN HQ-IRBID	110.0.0.0/8	HQ-INT 110.0.0.1 IR-INT 110.0.0.2
8	WAN HQ-SAUDI	120.0.0.0/8	HQ-INT 120.0.0.1 SA-INT 120.0.0.2
9	WAN HQ-TURKEY	130.0.0.0/8	HQ-INT 130.0.0.1 TU-INT 130.0.0.2

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 10 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 IRBID router with username (ADMIN) and password (HTUNETSEC2023).

- 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 router is accessible only by HQ Datacenter PC1 (10.0.0.10).
  - Configure the DMZ for VLANS (VLAN 50 private and VLAN 60 public)

Part 1 :Design and configure a secure network for JNR 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. Design and implement a secure network prototype according to the given scenario using Packet Tracer simulator.
5. 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.

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.

Part 3 : The in-class written exam will cover all the material taught during the course, with particular emphasis on the following topics:

1. Examine the various categories of devices employed for ensuring network security.
2. Analyze the network security protocols and the application of distinct cryptographic methodologies within the domain of network security.
3. Draw comparisons and contrasts between significant network security protocols.
4. Evaluate the importance of network security to an organization.
5. Determine which network hardware and software to use in the network. Justify your choices.

Learning Outcomes and Assessment Criteria		
Pass	**Merit**	**Distinction**
LO1 Examine network security principles, protocols and standards		**LO1 & 2** **D1** Evaluate the importance of network security to an organisation.
P1 Discuss the different types of network security devices. **P2** Examine network security protocols and the use of different cryptographic types in network security.	**M1** Compare and contrast at least two major network security protocols.	
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 a secure 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 a network.	**M3** Justify the choices made in the implemented network security configuration.	**D2** Critically evaluate the design, planning, configuration and testing of the network.
LO4 Undertake the testing of a network using a Test Plan		
P6 Comprehensively test the network using a devised Test Plan.	**M4** Analyse the results of testing to recommend improvements to the 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: **Student ID:** **Is the student repeating this unit? YES NO**		**Assessor name:**
Issue date: 19-04-2023	**Submission date:** 19-06-2024	**Submitted on:**
Programme: Computing		
HTU Course Name: Network Security **HTU Course Code:** 10203210	**BTEC Course name:** Network Security **BTEC Course Code:** M/618/7443	
Assignment number and title: Assignment 1 [JNR Network Security]		

Plagiarism

Student declaration

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 **Date**

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalized. 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.