# ASSIGNMENT BRIEF

| | |
|---|---|
| **HTU Course No:**<br>30201210 | **HTU Course Name:**<br>Network Security |
| **BTEC Unit Code:**<br>M/618/7443 | **BTEC UNIT Name:**<br>Network Security |

| | |
|---|---|
| **Student Name/ID Number/Section** | |
| **HTU Course Number and Title** | 30201210 Network Security |
| **BTEC Unit Code and Title** | M/618/7443 Network Security |
| **Academic Year** | 2024-2025 1 |
| **Assignment Author** | Elham Derbas |
| **Course Tutor** | Elham Derbas |
| **Assignment Title** | AI security company |
| **Assignment Ref No** | 1 |
| **Issue Date** | 15/11/2024 |
| **Formative Assessment dates** | From 20/11/2024 to 09/01/2025 |
| **Submission Date** | 02/02/2025 |
| **IV Name & Date** | Eyad Taqieddin 14/11/2024 |

**Submission Format**

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

1. **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.
2. **Evidence** of the implemented network (soft copy of the .pkt file). Students should use the Cisco Packet Tracer simulator version 8.2 or greater.
3. Discussion about the report and the implemented work. Instructions, dates, and times 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 the 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 penalized for exceeding the total word limit. The report must be supported with research and referenced using the Harvard referencing system.
**Note:**
Soft copy 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 AI security Inc., a prominent technological company that specializes in artificial intelligence technologies. AI security Inc. is headquartered in Amman, Jordan, and is extending its activities by establishing additional offices in Oman, Kuwait, Saudi arabia, and Qatar. You play a critical role in maintaining the network security and effectiveness of the business, particularly in light of the growing threat of cyberattacks.

AI security Inc. needs a secure and reliable network architecture to interconnect its GULF offices, Amman office and Amman data center. 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 Pentesting security check of the network, you discovered that not all the necessary network security best practices were being applied.

AI security's main data center is located in the same building as the headquarters office 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 AI security offices must utilize the Employee Information System, a secure website located at (https://eis.ai_security.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: 2 administrators.
- Resources: 2 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 AI security remote office including Amman Office:**

- Resources: one PC per subnet used to access the e-services required using a 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

| VLAN # | VLAN name | VLAN subnet IP | Device IP |
|---|---|---|---|
| 13 | Data centre (DC) | 13.0.0.0/8 | server 13.0.0.50<br>PC1 13.0.0.10<br>GW 13.0.0.1 |
| 21 | HQ employee (EMP) | 21.0.0.0/8 | PC1 21.0.0.10<br>GW 21.0.0.1 |
| 31 | HQ Sales | 31.0.0.0/8 | PC1 31.0.0.10<br>GW 31.0.0.1 |

| | | | |
|---|---|---|---|
| 41 | HQ guests (GN) | 41.0.0.1/8 | PC1 41.0.0.10<br>GW 41.0.0.1 |

| LAN # | NAME | LAN subnet IP | Device |
|---|---|---|---|
| 1 | Qatar VLAN 33 | 33.0.0.0/8 | PC1 33.0.0.10<br>GW 33.0.0.1 |
| 2 | Qatar VLAN 35 DC | 35.0.0.0/8 | Redundant Http server 35.0.0.2<br>PC1 35.0.0.10<br>GW 35.0.0.1 |
| 3 | OMAN | 45.0.0.0/8 | PC1 45.0.0.10<br>GW 45.0.0.1 |
| 4 | KUWAIT | 40.0.0.0/8 | PC1 40.0.0.10<br>GW 40.0.0.1 |
| 5 | Saudi Arabia | 50.0.0.0/8 | PC1 50.0.0.10<br>GW 50.0.0.1 |
| 6 | WAN HQ-QATAR | 155.0.0.0/8 | HQ-INT 155.0.0.1<br>QA-INT 155.0.0.2 |
| 7 | WAN HQ-Kuwait | 140.0.0.0/8 | HQ-INT 140.0.0.1<br>KU-INT 140.0.0.2 |
| 8 | WAN HQ-OMAN | 145.0.0.0/8 | HQ-INT 145.0.0.1/8<br>OM-INT 145.0.0.2 |
| 9 | WAN HQ-Saudi arabia | 150.0.0.0/8 | HQ-INT 150.0.0.1<br>SA-INT 150.0.0.2 |

**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 **except** QATAR 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 a 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 13 is 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 QATAR 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 Saudi arabia router with username
  (ADMIN) and password (Cl@ssP@$$w0rd&).
- The QATAR office is set to function as a disaster recovery site, featuring two separate VLANs. The first
  VLAN will serve the QATAR 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 QATAR ASA firewall is accessible only by HQ Datacenter PC1 (13.0.0.10).
  Configure the DMZ for VLANS ( VLAN 33 Private inside ,VLAN 35 DMZ , QATAR WAN as Public Outside)

**Part 1: In-class exam is scheduled for Sunday, December 29, 2024, covering the following criteria: P1, P2, and M1.**

**Part 2: Design and configure a secure network for AI security 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. Design and implement a secure network prototype according to the given scenario using Packet Tracer simulator.
4. 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.
5. Evaluate the importance of network security to an organization.

**Part 3: 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.

| **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.<br>**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. | **D1** Evaluate the importance of network security to an organisation. |
| **LO2** Design a secure network for a corporate environment. | **P3** Investigate the purpose and requirements of a secure network according to a given scenario.<br>**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. | |