**Part 1: University Campus Network Analysis and Security Assessment**

**Task 1: Campus Network Analysis**

**1. Existing Network Topology:**

* **Main Router:** Placed at the centre of the university layout, serving as the primary routing device.
* **Server Switch:** Connected to the main router via a gigabit ethernet port with a copper straight-through cable. It connects to the EMAIL, DNS, and WEB servers.
* **Campus Router:** Connected to the main router using the serial port with a serial DCE cable. The campus router links to the campus switch.
* **Campus Switch:** Connected to wireless access points in academic blocks (AB5, AB2, AB1), administration, library, and Server Centre.
* **Hostel Router:** Connected to the main router using the serial port with a serial DCE cable. The hostel router links to the hostel switch.
* **Hostel Switch:** Connected to wireless access points in boys and girls hostel blocks.
* **Wireless Access Points:** Each area has a dedicated access point with WPE encryption and password protection, connected to computing devices (PCs, laptops, and smartphones).

**2. Network Segmentation:**

* The network is segmented into three main areas:
  + **Server Area:** Includes EMAIL, DNS, and WEB servers connected to the server switch.
  + **Campus Area:** Includes academic blocks, administration, library, and Server Centre connected to the campus switch.
  + **Hostel Area:** Includes boys and girls hostel blocks connected to the hostel switch.

**3. Security Controls in Place:**

* **Wireless Encryption:** WPE encryption is used for wireless access points, though this is outdated and less secure.
* **Password Protection:** Wireless access points require a password for connectivity.

**4. Missing Security Controls:**

* **Access Control:** Implemented but not up to the mark.
* **Virtual Private Networks (VPN):** Not mentioned in the existing setup.
* **Port-Security:** No mention of port-security, it could result into unauthorized devices connecting to the network making it vulnerable to potential breaches.

**Task 2: Network Mapping**

Using Cisco Packet Tracer, the university campus network was mapped as follows:

* **Main Router:** Central point of the network, connected to the server switch, campus router, and hostel router.
* **Server Switch:** Connected to EMAIL, DNS, and WEB servers.
* **Campus Router:** Connected to the campus switch, which is further connected to wireless access points in academic blocks, administration, library, and Server Centre.
* **Hostel Router:** Connected to the hostel switch, which is further connected to wireless access points in boys and girls hostel blocks.
* **Wireless Access Points:** Strategically placed in each area, connecting to various computing devices.

**Task 3: Attack Surface Mapping**

**1. Identified Vulnerabilities and Weaknesses:**

* **Weak Wireless Encryption:** The use of WPE encryption is highly vulnerable to attacks.
* **Lack of VPN and Port-Security:** No port-security systems or VPNs in place to prevent unauthorized access and protect the network.
* **Basic Access Control:** Only password protection for wireless access points, no robust authentication and authorization systems.

**2. Potential Entry Points for Cyber-Attacks:**

* **Wireless Networks:** Weak encryption (WPE) makes wireless access points easy targets for unauthorized access.
* **Unmonitored Network Segments:** Lack of VPNs and port-security leaves network segments exposed to potential threats.
* **Unauthorized Access:** Insufficient access control mechanisms could allow unauthorized users to connect to the network.

**Deliverables**

**1. Network Topology Diagram:**

(Visual representation of the existing infrastructure in Cisco Packet Tracer, depicting the placement of routers, switches, wireless access points, and connected devices.)

**2. Security Assessment Report:**

**Security Risks:**

* **Weak Wireless Encryption:** WPE is highly vulnerable to attacks.
* **Lack of IDS and Firewalls:** No mechanisms in place to monitor and protect the network.
* **Basic Access Control:** Only password protection for wireless access points.

**Proposed Solutions and Countermeasures:**

* **Upgrade Wireless Security:** Implement WPA3 encryption for all wireless access points to enhance security.
* **Deploy ACLs, VPN and Port-Security:** Implement Access Control Lists, Port-Security and set-up VPN to protect the network from potential threats.
* **Regular Security Audits:** Conduct periodic security audits and vulnerability assessments to identify and address potential weaknesses in the network.