1. Wireless Network Security Configuration (WPA2 Enterprise)

Objective:

To secure the wireless network by implementing robust encryption and authentication mechanisms, ensuring that only authorized users can connect to the network.

Wireless Network Configuration:

- **Location:** Building #2
- **Authentication Type:** WPA2 Enterprise with RADIUS server
- **Purpose:** Ensure secure authentication for employees through WPA2 Enterprise, which requires credentials to be verified by the RADIUS server.

WPA2 Enterprise Configuration Details:

- **Encryption:** WPA2 with AES encryption, which provides strong data protection by encrypting communication over the wireless network.
- **Authentication Method:** 802.1X authentication with a **RADIUS server**.
- **RADIUS Server Setup:**
    - The RADIUS server is configured to authenticate employees using their corporate credentials (username and password), ensuring that only authorized individuals can access the corporate wireless network.

RADIUS Configuration Example (simplified):

bash

Copy

```
radius-server host 192.168.1.10 key secret123
dot1x authentication-method radius
```

- **Effect:** Only authorized employees can authenticate to the network, and all communications are encrypted with AES encryption, ensuring confidentiality and data integrity.

Example Detected Event:

- **Event:** An unauthorized user attempts to authenticate using incorrect credentials.
- **Detection:** The RADIUS server rejects the authentication request.
- **Response:** The device is unable to access the network, and the authentication failure is logged.

2. Wireless Network Configuration for Guest Access (WPA2 Personal)

Objective:

To provide a secure, segregated wireless network for guest access, ensuring that guests can access the internet without compromising the security of the internal corporate network.

Guest Network Configuration:

- **Network Type:** WPA2 Personal

- **Purpose:** Provide internet access to guests while keeping them isolated from the internal corporate network.
- **VLAN Segmentation:** Guest wireless access is placed in a separate **VLAN**, ensuring that guest devices cannot access sensitive internal resources.
- **Encryption:** WPA2 Personal (Pre-Shared Key) is used for simplicity, with a strong, unique passphrase.

Guest Network Configuration Details:

- **SSID (Service Set Identifier):** Guest_Network
- **Encryption:** WPA2 Personal with AES
- **VLAN Assignment:** All guest devices are placed on VLAN 20 to isolate them from corporate resources.

Example Guest Network Configuration:

bash

Copy

```
ssid Guest_Network
encryption aes-ccm
wpa2 personal key "strongguestpassword"
vlan 20
```

- **Effect:** Guest devices can connect to the internet but cannot access the internal corporate network. The use of WPA2 Personal ensures a secure connection for the guest network.

Example Detected Event:

- **Event:** A guest device connects to the guest network using the correct passphrase.
- **Detection:** The device is placed on VLAN 20, which has no access to internal corporate resources.
- **Response:** The device is granted internet access but is isolated from internal servers and data.

3. Access Point Security

Objective:

To secure the physical access points in the network by using strong passwords, MAC filtering, and ensuring that the firmware is up-to-date.

Access Point Security Configuration:

- **Strong Passwords:** All access points (APs) have strong, unique administrator passwords to prevent unauthorized configuration access.
- **MAC Filtering:** Only approved MAC addresses of employee devices are allowed to connect to the corporate network (WPA2 Enterprise).
- **Firmware Updates:** All access points are configured to automatically check for and apply firmware updates to ensure that security vulnerabilities are patched promptly.

Access Point Configuration Example (simplified):

bash

Copy

```
ssid Corporate_Network
authentication wpa2 enterprise
mac-filtering enable
mac-address 00:11:22:33:44:55
mac-address 00:11:22:33:44:56
firmware auto-update enabled
```

- **Effect:**
  - Only approved devices (based on MAC addresses) can connect to the corporate wireless network.
  - All access points are kept secure by ensuring they have the latest firmware, reducing the risk of vulnerabilities being exploited.

Example Detected Event:

- **Event:** An attempt to connect to the network from a device with an unapproved MAC address.
- **Detection:** The access point denies the connection attempt and logs the event.
- **Response:** The device is not allowed to access the network, and the administrator is notified of the unauthorized attempt.

4. Wireless Intrusion Prevention System (WIPS) Implementation

Objective:

To monitor and prevent unauthorized access points (rogue APs) from connecting to the network, ensuring the integrity of the wireless infrastructure.

WIPS Configuration:

- **WIPS Deployment:** A Wireless Intrusion Prevention System (WIPS) is deployed across the network to detect and mitigate threats such as rogue access points and unauthorized devices attempting to connect.
- **Monitoring:** The WIPS continuously scans the airwaves for rogue APs that may attempt to join the corporate network or interfere with legitimate wireless communication.
- **Alert Configuration:** Alerts are configured to notify administrators whenever an unauthorized access point or device is detected.

WIPS Configuration Details:

- **Rogue AP Detection:** The WIPS scans for APs that have not been authorized to join the network. It compares the MAC addresses of detected APs against a whitelist of known, legitimate devices.
- **Alert Configuration:** The WIPS is set to send email alerts to the network administrators whenever a rogue AP is detected.

Example WIPS Configuration:

bash

Copy

```
wips enable
wips rogue-detection enable
wips alert-email admin@company.com
wips scan-interval 10m
```

- **Effect:** The WIPS ensures that only authorized access points are allowed to connect to the network. Rogue APs are detected and flagged in real-time, and alerts are sent to the network administrators to take action.

Example Detected Event:

- **Event:** A rogue access point is detected by the WIPS.
- **Detection:** The WIPS identifies the rogue AP’s MAC address and compares it to the allowed list.
- **Response:** The WIPS sends an alert to the administrator, and the rogue AP is blocked or isolated from the network.