4.0 Network Security

4.1 Explain the importance of basic network security concepts.

- **Logical security**
  - Encryption
    - Data in transit
    - Data at rest
  - Certificates
    - Public key infrastructure (PKI)
    - Self-signed
  - Identity and access management (IAM)
    - Authentication
      - Multifactor authentication (MFA)
      - Single sign-on (SSO)
      - Remote Authentication Dial-in User Service (RADIUS)
      - LDAP
      - Security Assertion Markup Language (SAML)
      - Terminal Access Controller Access Control System Plus (TACACS+)
      - Time-based authentication
    - Authorization
      - Least privilege
      - Role-based access control
  - Geofencing
- **Physical security**
  - Camera
  - Locks
- **Deception technologies**
  - Honeypot
  - Honeynet
- **Common security terminology**
  - Risk
  - Vulnerability
  - Exploit
  - Threat
  - Confidentiality, Integrity, and Availability (CIA) triad
- **Audits and regulatory compliance**
  - Data locality
  - Payment Card Industry Data Security Standards (PCI DSS)
  - General Data Protection Regulation (GDPR)
- **Network segmentation enforcement**
  - Internet of Things (IoT) and Industrial Internet of Things (IIoT)
  - Supervisory control and data acquisition (SCADA), industrial control System (ICS), operational technology (OT)
  - Guest
  - Bring your own device (BYOD)

4.2 Summarize various types of attacks and their impact to the network.

- **Denial-of-service (DoS)/ distributed denial-of-service (DDoS)**
- **VLAN hopping**
- **Media Access Control (MAC) flooding**
- **Address Resolution Protocol (ARP) poisoning**
- **ARP spoofing**
- **DNS poisoning**
- **DNS spoofing**
- **Rogue devices and services**
  - DHCP
  - AP
- **Evil twin**
- **On-path attack**
- **Social engineering**
  - Phishing
  - Dumpster diving
  - Shoulder surfing
  - Tailgating
- **Malware**

4.3 Given a scenario, apply network security features, defense techniques, and solutions.

- **Device hardening**
  - Disable unused ports and services
  - Change default passwords
- **Network access control (NAC)**
  - Port security
  - 802.1X
  - MAC filtering
- **Key management**
- **Security rules**
  - Access control list (ACL)
  - Uniform Resource Locator (URL) filtering
  - Content filtering
- **Zones**
  - Trusted vs. untrusted
  - Screened subnet