4.0 Operations and Incident Response

4.1 Given a scenario, use the appropriate tool to assess organizational security.

- **Network reconnaissance and discovery**
  - tracert/traceroute
  - nslookup/dig
  - ipconfig/ifconfig
  - nmap
  - ping/pathping
  - hping
  - netstat
  - netcat
  - IP scanners
  - arp
  - route
  - curl
  - theHarvester
  - sn1per
  - scanless
  - dnsenum
  - Nessus
  - Cuckoo
- **File manipulation**
  - head
  - tail
  - cat
  - grep
  - chmod
  - logger
- **Shell and script environments**
  - SSH
  - PowerShell
  - Python
  - OpenSSL
- **Packet capture and replay**
  - Tcpreplay
  - Tcpdump
  - Wireshark
- **Forensics**
  - dd
  - Memdump
  - WinHex
  - FTK imager
  - Autopsy
- **Exploitation frameworks**
- **Password crackers**
- **Data sanitization**

4.2 Summarize the importance of policies, processes, and procedures for incident response.

- **Incident response plans**
- **Incident response process**
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons learned
- **Exercises**
  - Tabletop
  - Walkthroughs
  - Simulations
- **Attack frameworks**
  - MITRE ATT&CK
  - The Diamond Model of Intrusion Analysis
  - Cyber Kill Chain
- **Stakeholder management**
- **Communication plan**
- **Disaster recovery plan**
- **Business continuity plan**
- **Continuity of operations planning (COOP)**
- **Incident response team**
- **Retention policies**

4.3 Given an incident, utilize appropriate data sources to support an investigation.

- **Vulnerability scan output**
- **SIEM dashboards**
  - Sensor
  - Sensitivity
  - Trends
  - Alerts
  - Correlation
- **Log files**
  - Network
  - System
  - Application
  - Security
  - Web
  - DNS
  - Authentication
  - Dump files
  - VoIP and call managers
  - Session Initiation Protocol (SIP) traffic
- **syslog/rsyslog/syslog-ng**
- **journalctl**
- **NXLog**
- **Bandwidth monitors**
- **Metadata**
  - Email
  - Mobile
  - Web
  - File
- **Netflow/sFlow**
  - Netflow
  - sFlow
  - IPFIX
- **Protocol analyzer output**

4.4 Given an incident, apply mitigation techniques or controls to secure an environment.

- **Reconfigure endpoint security solutions**
  - Application approved list
  - Application blocklist/deny list
  - Quarantine
- **Configuration changes**
  - Firewall rules
  - MDM
  - DLP
  - Content filter/URL filter
  - Update or revoke certificates
- **Isolation**
- **Containment**
- **Segmentation**
- **SOAR**
  - Runbooks
  - Playbooks

4.5 Explain the key aspects of digital forensics.

- **Documentation/evidence**
  - Legal hold
  - Video
  - Admissibility
  - Chain of custody
  - Timelines of sequence of events
    - Time stamps
    - Time offset
  - Tags
  - Reports
  - Event logs
  - Interviews
- **Acquisition**
  - Order of volatility
  - Disk
  - Random-access memory (RAM)
  - Swap/pagefile
  - OS
  - Device
  - Firmware
  - Snapshot
  - Cache
  - Network
  - Artifacts
- **On-premises vs. cloud**
  - Right-to-audit clauses
  - Regulatory/jurisdiction
  - Data breach notification laws
- **Integrity**
  - Hashing
  - Checksums
  - Provenance
- **Preservation**
- **E-discovery**
- **Data recovery**
- **Non-repudiation**
- **Strategic intelligence/ counterintelligence**