INFORMATION SECURITY

CONTENT

1.0 Network Concepts and Security

- OSI Reference model
- Network Design elements and components
- Implement common protocols and services
- Implement security configuration parameters on network devices and other technologies.
- Given a scenario, use secure network administration principles.

2.0 Compliance and Operational Security

- Explain the importance of risk related concepts.
- Given a scenario, implement basic forensic procedures.
- Summarize common incident response procedures.
- Explain the importance of security related awareness and training.

3.0 Threats and Vulnerabilities

- Explain types of malware.
- Summarize various types of attacks.
- Summarize social engineering attacks and the associated effectiveness with each attack.
- Wireless attacks.
- Application attacks.
- Analyze a scenario and select the appropriate type of mitigation and deterrent techniques.

4.0 Cryptography

- Given a scenario, utilize general cryptography concepts.
- Given a scenario, use appropriate cryptographic methods.
- Given a scenario, use appropriate PKI, certificate management and associated components.

5.0 Penetration Testing

- Perform penetration testing using kaliLinux tools.