**Course 2**

**Cybersecurity Roles, Processes & Operating System Security**

**Cybersecurity Roles:**

1. Security Analyst:

- Monitors and analyzes security alerts.

- Investigates incidents and implements security measures.

- Conducts risk assessments.

2. Security Engineer:

- Designs and implements security systems.

- Configures and manages security infrastructure.

- Collaborates with other IT professionals to integrate security measures.

3. Incident Responder:

- Responds to security incidents in real-time.

- Analyzes and mitigates the impact of security breaches.

- Develops incident response plans.

4. Penetration Tester (Ethical Hacker):

- Identifies vulnerabilities in systems and networks.

- Conducts simulated attacks to assess security measures.

- Recommends improvements based on findings.

5. Security Consultant:

- Provides advice on security best practices.

- Assesses organizational security needs.

- Designs and implements security solutions.

**Cybersecurity Processes:**

1. Risk Management:

- Identifies and assesses potential risks.

- Develops strategies to mitigate and manage risks.

- Regularly reviews and updates risk assessments.

2. Incident Response:

- Establishes procedures for responding to security incidents.

- Defines roles and responsibilities during incidents.

- Conducts post-incident analysis for continuous improvement.

3. Access Control:

- Manages user access to systems and data.

- Implements authentication and authorization mechanisms.

- Regularly reviews and updates access permissions.

4. Security Auditing:

- Regularly audits security controls and configurations.

- Identifies and addresses vulnerabilities.

- Ensures compliance with security policies and standards.

**Operating System Security:**

1. User Account Management:

- Enforces strong password policies.

- Regularly reviews and updates user accounts.

- Implements the principle of least privilege.

2. Patch Management:

- Regularly updates and patches operating systems.

- Addresses known vulnerabilities promptly.

- Maintains an inventory of software and versions.

3. Antivirus and Anti-malware:

- Installs and updates antivirus software.

- Conducts regular scans for malware.

- Implements email and web filtering for malicious content.

4. Firewall Configuration:

- Configures firewalls to control incoming and outgoing traffic.

- Monitors firewall logs for suspicious activity.

- Regularly reviews and updates firewall rules.