Name :Veekshitha
Reg no:21BCE8943

# Task - 5

**BASIC :**

1.Inventory and Control of Hardware Assets: Maintain a list of all hardware assets, track their usage, and ensure proper disposal when needed.

2.Inventory and Control of Software Assets: Keep track of software applications, licenses, and versions to ensure compliance and minimize security risks.

3.Continuous Vulnerability Management: Regularly scan and assess systems for vulnerabilities, apply patches, and prioritize security updates.

4.Controlled Use of Administrative Privileges: Limit access to administrative privileges to authorized personnel and monitor their usage to prevent misuse.

5.Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers: Configure devices and software securely to reduce potential attack surfaces.

6.Maintenance, Monitoring, and Analysis of Audit Logs: Keep logs of system activities, monitor them for suspicious behavior, and analyze them in case of security incidents.

**Foundational:**

7. Email and Web Browser Protections: Implement security measures to protect against phishing, malicious email attachments, and browser-based attacks.

8.Malware Defenses: Employ antivirus and anti-malware solutions to detect and prevent malicious software from compromising systems.

9.Limitation and Control of Network Ports, Protocols, and Services: Disable unnecessary network services, ports, and protocols to minimize potential avenues of attack.

10.Data Recovery Capabilities: Establish backup and recovery procedures to ensure data can be restored in case of data loss or cyber incidents.

11.Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches: Configure network devices securely to protect against unauthorized access and attacks.

12.Boundary Defense: Implement measures like firewalls and intrusion detection/prevention systems to monitor and control traffic entering and leaving the network.

13.Data Protection: Encrypt sensitive data both in transit and at rest to prevent unauthorized access.

14.Controlled Access Based on the Need to Know: Limit access to sensitive data and systems based on the principle of least privilege.

15.Wireless Access Control: Secure wireless networks through strong encryption, authentication mechanisms, and access controls.

16.Account Monitoring and Control: Monitor user accounts for suspicious activity and promptly disable or revoke access for terminated employees.

**Organizational:**

17. Implement a Security Awareness and Training Program: Educate employees about cybersecurity best practices to minimize human-related security risks.

18.Application Software Security: Develop and deploy applications securely to prevent vulnerabilities and code-based attacks.

19.Incident Response and Management: Establish procedures for detecting, reporting, and responding to security incidents effectively.

20.Penetration Tests and Red Team Exercises: Conduct controlled security assessments to identify vulnerabilities and assess the organization's readiness to defend against real-world attacks.

---