TASK-6

K. Naveen Abhiram

21BCE7357

Understanding CIS Critical Security Controls

- **Control-1: Inventory and Control of Hardware Assets**

  Control every piece of gear connected to the network. Take steps to detect and restrict unauthorized or unmanaged devices, and make sure that only authorized devices have access.

- **Control-2: Inventory and Control of Software Assets**

  Control all of the network's software. Make certain that only approved software is being used. Prevent unmanaged applications from being installed or running.

- **Control-3: Continuous Vulnerability Management**

  Keep an eye out for any system vulnerabilities on a regular basis. If a vulnerability is discovered, take the required steps to repair it to reduce the amount of time that attackers have to exploit it.

- **Control-4: Controlled Use of Administrative Privileges**

  Utilize appropriate administrative privileges and rules for computers, networks, and software.

- **Control-5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers**

  Implement robust security settings for workstations, servers, laptops, and mobile devices. Use a robust configuration management procedure to stop attackers from taking advantage of services and establishing vulnerabilities.

- **Control-6: Maintenance, Monitoring and Analysis of Audit Logs**

  Audit logs of occurrences should be gathered, managed, and analysed to get insight into possible threats. These logs may be used to find, comprehend, and fix security flaws.

- **Control-7: Email and Web Browser Protections**

  Limit the ability of attackers to influence user behaviour through email and online browsers. Reduce the possibility of an assault on these vital communication instruments.

- **Control-8: Malware Defences**

  Establish safeguards to prevent the installation, execution, and dissemination of malicious software in your environment. Utilize automation to maintain the effectiveness of your defences.

- **Control-9: Limitation and Control of Network Ports, Protocols, and Services**

  To reduce potential attack vectors, close unused network ports and protocols. This control entails evaluating network communication and limiting it to only the most necessary services.

- **Control-10: Data Recovery Capabilities**

  Create and keep up strong data recovery capabilities. In order to apply this control, methods, practices, and technologies must be used that allow for quick data recovery in the case of data loss, data corruption, or other types of data breach. In the event of unforeseen catastrophes or cyberattacks, you may reduce downtime and data loss by making sure that data can be reliably and rapidly recovered.

- **Control-11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches**

  One may preserve the integrity and security of the network infrastructure by applying strong security configurations and settings to network devices like switches, routers, and firewalls.

- **Control-12: Boundary Defence**

  Defend the perimeter of the workplace against outside dangers. To monitor and manage incoming and outgoing network traffic, this entails putting firewalls, intrusion detection systems, and other security measures into place.

- **Control-13: Data Protection**

  Keeping in place safeguards against internal and external risks. To lessen the danger of attacks, this control also comprises access restrictions, data loss protection techniques, and user monitoring.

- ## Control-14: Controlled Access Based on the Need to Know

  Implement access restrictions so that users can only access the data and resources they need to do their jobs. This idea—often referred to as "need-to-know"—ensures that people may only access information and resources that are pertinent to their jobs and duties.

- ## Control-15: Wireless Access Control

  In order to prevent unwanted access, secure the wireless networks. To safeguard wireless infrastructure, proper configuration, authentication, and encryption are essential.

- ## Control-16: Account Monitoring and Control

  Check user rights and accounts for any indications of unusual behaviour. Review and audit user accounts often to stop privilege escalation and unlawful access.

- ## Control-17: Implement a Security Awareness and Training Program

  Inform everyone in the office on security dangers and recommended practices. A well-informed workplace is better able to identify and address security problems.

- ## Control-18: Application Software Security

  Throughout each stage of the software application's existence, ensure its security. This entails incorporating security procedures into the design, coding, testing, and deployment phases of the application development process. Sensitive data may be protected by lowering the risk of security breaches through early identification and mitigation of vulnerabilities and shortcomings.

- ## Control-19: Incident Response and Management

  To identify security issues, respond to them, and recover from them, create a strong incident response strategy. To lessen the effects of security breaches, quick and efficient incident response is crucial.

- ## Control-20: Penetration Tests and Red Team Exercises

  Perform regular penetration tests and red team drills to test your security procedures. These actions assist in locating flaws and vulnerabilities that potential attackers might use against you.