**Task -6 Wednesday-30-08-23 by Sameer Chauhan**

**Top -20 Critical Security Controls**

**Formerly the SANS Critical Security Controls (SANS Top 20) these are now officially called the CIS Critical Security Controls (CIS Controls).**

**1*-Inventory and Control of Hardware Assets: Maintain an up-to-date inventory of all hardware devices within your organization's network. This includes servers, workstations, mobile devices, and any other connected devices.***

***2****-* **Inventory and Control of Software Assets: Keep track of all software applications installed on your systems. This helps in identifying and addressing vulnerabilities, ensuring software compliance, and reducing the risk of unauthorized or outdated software being used.**

**3**- **Continuous Vulnerability Management**: **Regularly scan your systems for known vulnerabilities and weaknesses. Apply patches and updates promptly to address these vulnerabilities, reducing the potential for exploitation by attackers.**

**4- Controlled Use of Administrative Privileges: Limit the number of users who have administrative privileges on systems and devices. Admin privileges provide significant control, and limiting their use helps prevent unauthorized changes and potential misuse.**

**5 -Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers: Implement secure configurations for all devices, including mobile devices, laptops, workstations, and servers. Secure configurations reduce the attack surface by disabling unnecessary services and applying security settings.**

6- **Maintenance, Monitoring, and Analysis of Audit Logs: Regularly review and analyze system logs and audit trails. This helps detect and respond to suspicious activities, breaches, and security incidents in a timely manner.**

7- **Email and Web Browser Protections**: **Implement security measures in email systems and web browsers to protect against phishing attacks, malicious downloads, and other**

8-**Malware Defences**: **Employ strong anti-malware solutions to detect and prevent the execution of malicious software on systems. Regularly update malware definitions to stay protected against new threats.**

9- **Limitation and Control of Network Ports, Protocols, and Services: Disable unnecessary network ports, protocols, and services on systems to reduce the potential attack surface and limit avenues for attackers to exploit.**

10-**Data Recovery Capabilities**: **Establish and maintain reliable data backup and recovery processes. Regularly test backup restoration to ensure data can be recovered in the event of data loss or a cyberattack.**

11-**Secure Configuration for Network Devices: Apply secure configurations to network devices such as firewalls, routers, and switches. These configurations enhance network security and prevent unauthorized access.**

12- **Boundary Defences**: **Implement measures to protect your network perimeter and external-facing systems from unauthorized access and attacks. Firewalls, intrusion detection/prevention systems, and network segmentation are examples of boundary defences measures.**

13- **Data Protection**: **Encrypt sensitive data both in transit and at rest. Encryption helps safeguard data from being accessed by unauthorized parties even if they gain access to the data storage.**

14-**Controlled Access Based on the Need to Know**: **Limit access to data and systems based on job roles and responsibilities. Users should only have access to the resources necessary for their tasks.**

15-**Wireless Access Control: Implement secure configurations and access controls for wireless networks to prevent unauthorized access and attacks.**

16- **Account Monitoring and Control: Continuously monitor user accounts for suspicious activities. Implement strong authentication mechanisms and promptly deactivate accounts that are no longer needed.**

17- **Implement a Security Awareness and Training Program**: **Train employees on security best practices, social engineering threats, and how to recognize and respond to potential security incidents.**

18- **Application Software Security**: **Ensure that software applications are developed, configured, and maintained securely to prevent vulnerabilities that could be exploited by attackers.**

19-**Incident Response and Management: Establish an incident response plan to effectively respond to security incidents. This includes procedures for detection, containment, eradication, and recovery.**

20-P**enetration Tests and Red Team Exercises: Regularly conduct penetration tests and red team exercises to identify vulnerabilities and weaknesses in your organization's defences. These exercises simulate real-world attacks to improve your overall security posture.**