Name :- Ch.V.S.Dhiraj Reg No :- 21BCE5717

Task – 6

CIS Controls Assessment Specification

Basic Controls

CIS Control 1: Inventory and Control of Hardware Assets

Control 1 helps the CIS to actively manage (inventory, track, and correct) all hardware devices on the network. This ensures only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

A hardware asset is any device that operates at the Datalink layer (Layer 2) or the Network layer (Layer 3).

The CIS Control 1 Dashboard provides information to assist in identifying assets collected during a vulnerability scan.

CIS Control 2: Inventory and Control of Software Assets

The focus of this control is to acΘvely manage (inventory, track, and correct) soŌware installed on systems within the organizaΘon. A fundamental aspect of risk management is discovering risk by tracking soŌware present on informaΘon systems. Ensuring only authorized soŌware is used by the organizaΘon will increase the effecΘveness of risk management efforts. Being able to quickly idenΘfy unauthorized and unmanaged soŌware can prevent security breaches and increase the producΘvity of users.

The CIS Control 2 Dashboard provides informaΘon to assist in idenΘfying unwanted or potenΘally dangerous applicaΘons, therefore enabling an efficient vulnerability management program.

CIS Control 3: Continuous Vulnerability Management

The focus of this control is to have an established vulnerability management program that is configured to conduct regular, comprehensive, credentialed scans across the organization. The most effective vulnerability scanning programs not only identify vulnerabilities, but also evaluate and report on a number of other critical concerns such as:

- Security configurations of systems
- Misconfigurations
- Unauthorized changes
- Patch levels of systems

such as the CIS Control 3/18 ConΘnuous Vulnerability Management and ApplicaΘon Security Dashboard.

CIS Control 4: Controlled Use of

Administrative Privileges

The focus of this control is to ensure that all users with administraϴve level access use a dedicated or secondary account for any elevated acϴvity. This administrator account should not be used for any other purpose, and should not be used for email, web-browsing, or similar acϴvity.

The misuse of administraϴve privileges is a primary method for aΣackers to spread inside a target enterprise. Two very common aΣacker techniques take advantage of uncontrolled administraϴve privileges.

he CIS Control 4/5 Secure ConfiguraϴOns and Group Memberships Dashboard provides useful informaϴon to assist organizaϴons with this control.

CIS Control 5: Secure Configuration for Hardware and Software on MobileDevices, Laptops, Workstations and Servers

The focus of this control is to maintain documented security configuration standards for all authorized operating systems and software. Organizations must establish a baseline security configuration, implement a configuration management and change control process, and actively be able to report on the security configuration of all endpoint devices such as:

- Mobile devices
- Laptops
- Servers
- Workstations

The CIS Control 4/5 Secure ConfiguraΘons and Group Memberships Dashboard provides useful informaΘon to assist organizaΘons with this control.

CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs

Deficiencies in security logging and analysis allow aΣackers to hide their locaΘon, malicious soŌware, and acΘviΘes on vicΘm machines. Even if the vicΘms know that their systems have been compromised, without protected and complete logging records they are blind to the details of the aΣack and to subsequent acΘons taken by the aΣackers.

FoundaΘonal Controls

CIS Control 7: Email and Web Browser Protections

The journey of implementing the CIS Controls with CIS Control 7 moves from Basic to Foundational controls, and begins with Email and Web Browser Protections. Organizations are directed to ensure that only fully supported web browsers and email clients are used. Ideally, only the latest version of these fully supported web browsers and email clients should be used. Organizations are also directed to use Domain Name System (DNS) filtering services to assist in the identification and blocking of malicious domains. The specific sub controls that are part of Implementation Group 1 (IG1) are:

- 7.1 Ensure Use of Only Fully Supported Browsers and Email Clients

Software - 7.7: Use of DNS Filtering Services

CIS Control 7: Email and Web Browser Protections

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups 1	2	3
7.1	Applications	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	●	●	●
7.2	Applications	Protect	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.		●	●
7.3	Applications	Protect	Limit Use of Scripting Languages in Web Browsers and Email Clients	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.		●	●
7.4	Network	Protect	Maintain and Enforce Network-Based URL Filters	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.		●	●
7.5	Network	Protect	Subscribe to URL-Categorization Service	Subscribe to URL-categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.		●	●
7.6	Network	Detect	Log All URL Requests	Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.		●	●
7.7	Network	Protect	Use of DNS Filtering Services	Use Domain Name System (DNS) filtering services to help block access to known malicious domains.	●	●	●
7.8	Network	Protect	Implement DMARC and Enable Receiver Side Verification	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.		●	●
7.9	Network	Protect	Block Unnecessary File Types	Block all email attachments entering the organization's email gateway if the file types are unnecessary for the organization's business.		●	●
7.10	Network	Protect	Sandbox All Email Attachments	Use sandboxing to analyze and block inbound email attachments with malicious behavior.			●

CIS Control 8: Malware Defenses

The journey of implementing the Foundational CIS Controls continues with CIS Control 8 Malware Defenses. Organizations are directed to ensure that the scanning engine and signature database are updated on a regular basis for all anti-malware software. Ideally, only the latest version should be used. Organizations are also directed to configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected. Finally, as part of the IG1 set of controls, organizations are advised to configure devices to not auto-run content from removable media. The specific sub-controls that are part of Implementation Group 1 (IG1) are:

- 8.2 Ensure Anti-Malware Software and Signatures are Updated
- 8.4 Configure Anti-Malware Scanning of Removable Media
- 8.5 Configure Devices to Not Auto-Run Content

CIS Control 8: Malware Defenses

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups 1	2	3
8.1	Devices	Protect	Utilize Centrally Managed Anti-Malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●
8.2	Devices	Protect	Ensure Anti-Malware Software and Signatures Are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	●	●	●
8.3	Devices	Detect	Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●
8.4	Devices	Detect	Configure Anti-Malware Scanning of Removable Media	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	●	●	●
8.5	Devices	Protect	Configure Devices to Not Auto-Run Content	Configure devices to not auto-run content from removable media.	●	●	●
8.6	Devices	Detect	Centralize Anti-Malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.		●	●
8.7	Network	Detect	Enable DNS Query Logging	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.		●	●
8.8	Devices	Detect	Enable Command-Line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.		●	●

CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services

The journey of implementing the Foundational CIS Controls continues with CIS Control 9 Limitation and Control of Network Ports, Protocols, and Services. The full CIS 9 Control evolves around organizations ensuring that only those ports, protocols, and services with a validated business requirement are open/running on each system. Organizations are also directed to perform automated scans on a regular basis against all systems to ensure that unauthorized ports/services are detected. The specific sub-controls that are part of Implementation Group 1 (IG1) are:

- 9.4 Apply Host-Based Firewalls or Port-Filtering

CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups 1	2	3
9.1	Devices	Identify	Associate Active Ports, Services, and Protocols to Asset Inventory	Associate active ports, services, and protocols to the hardware assets in the asset inventory.		●	●
9.2	Devices	Protect	Ensure Only Approved Ports, Protocols, and Services Are Running	Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.		●	●
9.3	Devices	Detect	Perform Regular Automated Port Scans	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.		●	●
9.4	Devices	Protect	Apply Host-Based Firewalls or Port-Filtering	Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
9.5	Devices	Protect	Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.			●

CIS Control 10: Data Recovery Capabilities

The journey of implementing the CIS Controls continues with data recovery capabilities. This control addresses the importance of backing-up and protecting an organization's system data. Organizations which implement sound data backup strategies ensure their ability to recover lost data or data that has been tampered-with quickly and efficiently.

- 10.1: Ensure Regular Automated Backups
- 10.2: Perform Complete System Backups
- 10.4: Protect Backups
- 10.5: Ensure All Backups Have at Least One Offline Backup Destination

CIS Control 10: Data Recovery Capabilities

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups 1	2	3
10.1	Data	Protect	Ensure Regular Automated Backups	Ensure that all system data is automatically backed up on a regular basis.	●	●	●
10.2	Data	Protect	Perform Complete System Backups	Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.	●	●	●
10.3	Data	Protect	Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.		●	●
10.4	Data	Protect	Protect Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	●	●	●
10.5	Data	Protect	Ensure All Backups Have at Least One Offline Backup Destination	Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.	●	●	●

CIS Control 11: Secure Configuration for Network Devices, such as Firewalls,

Routers, and Switches

The journey of implementing the CIS Controls, continues with CIS Control 11: Secure Configuration for network devices, such as Firewalls, Routers, and Switches. Organizations are directed to review the configuration of all network devices against approved configurations. Organizations should record and mitigate any deviation. Organizations are also directed to establish a rigorous configuration management program and change control process in order to prevent attackers from exploiting network device vulnerabilities.

The specific sub-controls that are part of Implementation Group 1 (IG1) are:

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

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups 1	2	3
11.1	Network	Identify	Maintain Standard Security Configurations for Network Devices	Maintain documented security configuration standards for all authorized network devices.		●	●
11.2	Network	Identify	Document Traffic Configuration Rules	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●
11.3	Network	Detect	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	Compare all network device configurations against approved security configurations defined for each network device in use, and alert when any deviations are discovered.		●	●
11.4	Network	Protect	Install the Latest Stable Version of Any Security-Related Updates on All Network Devices	Install the latest stable version of any security-related updates on all network devices.	●	●	●
11.5	Network	Protect	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	Manage all network devices using multi-factor authentication and encrypted sessions.		●	●
11.6	Network	Protect	Use Dedicated Workstations for All Network Administrative Tasks	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.		●	●
11.7	Network	Protect	Manage Network Infrastructure Through a Dedicated Network	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.		●	●

CIS Control 12: Boundary Defense

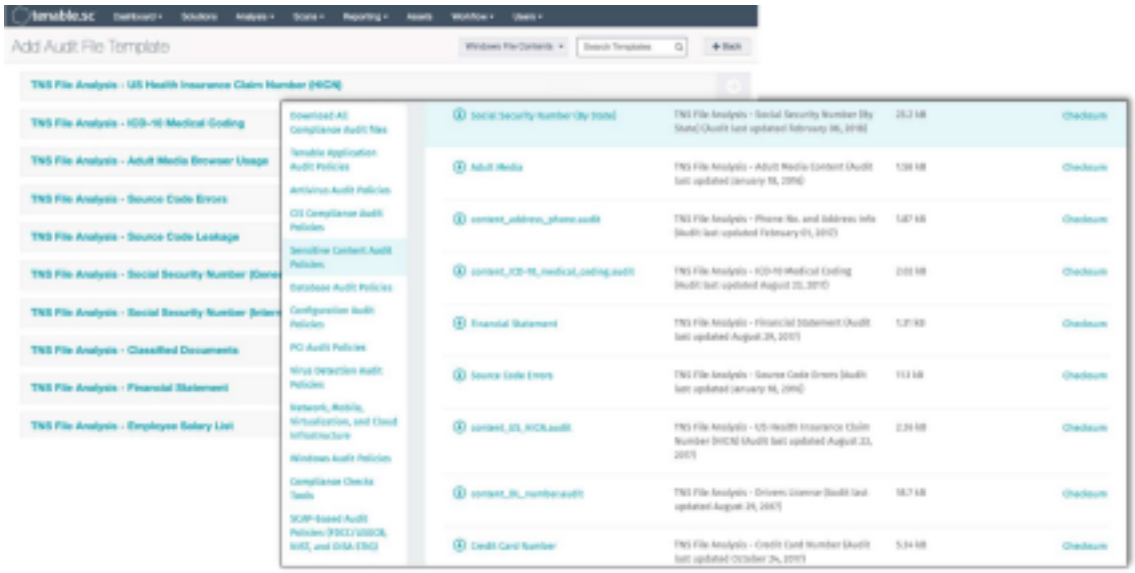
The journey of implementing the CIS Controls continues with understanding the boundaries of a the network and defining how access should be controlled. Organizations are directed to deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed. The two specific sub-controls that are part of Implementation Group 1 (IG1) are:

- 12.1: Maintain an Inventory of Network Boundaries
- 12.4: Deny Communication Over Unauthorized Ports

CIS Control 13: Data Protection

The journey of implemenΘng the CIS Controls conΘnues with the prevenΘon of data exfiltraΘon, miΘgaΘng the effects of exfiltrated data, and ensuring the privacy and integrity of sensiΘve informaΘon. As with many of the CIS controls, the first step is establishing an asset inventory. With data files, this can feel like an insurmountable task. This is where knowing what is stored on the network, and where, is extremely important.

- 13.1: Maintain an Inventory of Sensitive Information
- 13.2: Remove Sensitive Data or Systems Not Regularly Accessed by Organization
- 13.6: Encrypt Mobile Device Data



CIS Control 14: Controlled Access Based on the Need to Know

The journey of implementing the CIS Controls continues with controlling access using Access Control Lists (ACL). Organizations are directed to protect all information stored on systems using native ACL methods. These methods include network layer access controls, file level permissions, and other application centric controls. The specific sub-controls that are part of Implementation Group 1 (IG1) are:

- 14.6: Protect InformaΘon Through Access Control Lists

CIS Control 15: Wireless Access Control

The journey of implementing the CIS Controls continues with controlled use of wireless networking. Organizations are directed to verify that Advanced Encryption Standard (AES) is configured for all wireless technology. The sub-control that is part of Implementation Group 1 (IG1) is:

- 15.7: Leverage the Advanced Encryption Standard (AES) to Encrypt

CIS Control 15: Wireless Access Control

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups 1	2	3
15.1	Network	Identify	Maintain an Inventory of Authorized Wireless Access Points	Maintain an inventory of authorized wireless access points connected to the wired network.		●	●
15.2	Network	Detect	Detect Wireless Access Points Connected to the Wired Network	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.		●	●
15.3	Network	Detect	Use a Wireless Intrusion Detection System	Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.		●	●
15.4	Devices	Protect	Disable Wireless Access on Devices if Not Required	Disable wireless access on devices that do not have a business purpose for wireless access.			●
15.5	Devices	Protect	Limit Wireless Access on Client Devices	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.			●
15.6	Devices	Protect	Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients	Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.		●	●
15.7	Network	Protect	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.	●	●	●
15.8	Network	Protect	Use Wireless Authentication Protocols That Require Mutual, Multi-Factor Authentication	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), that requires mutual, multi-factor authentication.			●
15.9	Devices	Protect	Disable Wireless Peripheral Access to Devices	Disable wireless peripheral access of devices (such as Bluetooth and Near Field Communication (NFC)), unless such access is required for a business purpose.		●	●
15.10	Network	Protect	Create Separate Wireless Network for Personal and Untrusted Devices	Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.	●	●	●

Wireless Data

CIS Control 16: Account Monitoring and Control

Many systems (operaΘng systems and applicaΘon systems) may have the ability to set controls and policies on user accounts. The centralized management of these

types of accounts can oÕen be neglected or fall out of scope of normal business processes. OrganizaΘons are directed to disable any unassociated or dormant accounts. These accounts are oÕen overlooked or set up with a default password, both of which are undesirable for more than a short period of Θme.

The three specific sub-controls that are part of Implementation Group 1

(IG1) are: - [16.8: Disable Any Unassociated Accounts]

- [16.9: Disable Dormant Accounts]
- [16.11: Lock WorkstaΘon Sessions AÕer InacΘvity]

Organizational Controls

CIS Control 17: Implement a Security Awareness and Training Program

Tenable Security Center provides reports and other data display tools to help the security awareness team understand how risk miΘgaΘon efforts are progressing. As shown in the image below, we have created accounts for the execuΘve team who organizaΘonally, is responsible for assets. This visualizaΘon can be used to help provide awareness of the current state of the vulnerability management program. Other filters and queries can also be used to help illustrate risk management funcΘons.

CIS Control 18: Application Software Security

AΣacks oŌen take advantage of vulnerabiliΘes found in web-based and other applicaΘon soŌware. VulnerabiliΘes can be present for many reasons, including coding mistakes, logic errors, incomplete requirements, and failure to test for unusual or unexpected condiΘons.

CIS Control 19: Incident Response and Management

This passive sensor monitors network flows and looks for vulnerability based on clear text informaΘon or other traffic paΣerns. This detecΘon method may assist organizaΘons during incident response (IR), as the passive data collected is another source of informaΘon. Tenable Security Center and this collected data is valuable to ensuring the IR
team has the informaΘon they need, and a history of system vulnerabiliΘes and configuraΘons, especially when conducΘng post incident review and process improvements.

CIS Control 20: Penetration Tests and Red Team Exercises

As a final testament to a good security program, the CIS Control 20 recommends the organizaΘon test all the security controls. These exercises are very beneficial to training and security awareness. Many Θmes well intended measures can be exploited. For example, a really strict password policy can result in users taping

passwords to their keyboard. A great technical control, thwarted by a forgeɳul user and an observant adversary. Many Ɵmes developers find protocols they find useful, and never realize there is an inherent security flaw

Reference link :- hΣps://docs.tenable.com/security-center/CIS CAS/Content/Controls/FoundaƟonal/FoundaƟonalControls.htm