MIS 690 System Hardening Worksheet

Section 1.0 - Student Info

Student Name:	Moses Kanagaraj

Section 1.1 - *Provide the device being tested, as well as software being tested. [Text] is provided as sample content only, replace with system-specific content. You must test at least TWO (2) things: your OS and a Software (Chrome, Adobe, Office, etc)*

Hardware and Software List

Device/Host Name/Software	Version	Manufacturer	Model Number	Firmware / OS	Purpose
Moses' Desktop	[N/A]	HP	Envy 360	Windows 10	General Use Workstation
Google Chrome	131.0.6778.86	Google	[N/A]	[N/A]	[Report viewing, and web browsing]
MS Edge	131.0.2903.63	Microsoft	[N/A]	[N/A]	[Report viewing, and web browsing]
ADD ROWS AS NEEDED					

Section 2.0 Vulnerabilities

From your scans, select FIFTEEN (15) Vulnerabilities that you are investigating. I advise starting with CAT-I (High/Criticals) if you'd interested in securing your system. And fill in the fields for Vulnerability Investigation.

Total Number of Vulnerabilities in your SCC/SCAP scan of your OS: 21 Vulnerabilities

Vulnerability Investigation

Testing Source (which STIG)	Vulnerability ID (This should be V-#### from STIG Viewer)	RESULT (Open/Not a Finding/ Not Applicable)	CIA Triad Impact	NIST 800-53 Security Control Affected (short description. If Vuln has multiple, pick one). Refer to https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf for reference, after looking at the security control info in Stig Viewer.
Windows 10 STIG	V-242002	Open	This is related to Unsolicited inbound connections which would allow attackers unauthorized access, impacting Confidentiatlity and Integrity	NIST SP 800-53 CM-7 requires organizations to manage the use of administrative privileges on information systems. This control mandates the implementation of appropriate measures to monitor, restrict, and control the use of these privileges to prevent unauthorized access and mitigate security risks.
Windows 10 STIG	V-241997	Open	This is related to Unsolicited inbound connections which would allow attackers unauthorized access, impacting Confidentiatlity and Integrity	NIST SP 800-53 Revision 4, CM-7 (b) requires organizations to implement additional measures to control the use of system configuration settings. Specifically, it mandates that organizations must take actions to prevent unauthorized changes to system configurations that could compromise the security of the system
Windows 10 STIG	V-241992	Open	This is related to Unsolicited inbound connections which would allow attackers unauthorized access, impacting Confidentiatlity and Integrity	NIST SP 800-53 Revision 4, CM-7 (b) requires organizations to implement additional measures to control the use of system configuration settings. Specifically, it mandates that organizations must take actions to prevent unauthorized changes to system configurations that could compromise the security of the system
Microsoft Edge	V-235759	Open	* Older versions of TLS (1.0 and 1.1) provide weaker encryption and are vulnerable to attacks such as Man-in-the-Middle compromising confidentiality, Integrity, Availability.	NIST SP 800-53 AC-17 (2) focuses on managing the use of remote access to organizational systems. It mandates that remote access to systems must be controlled through a session timeout or other appropriate mechanisms to terminate inactive sessions, ensuring that unauthorized access or use is prevented after a period of
Microsoft Edge	V-235758	Not Reviewed	* Outdated versions of Edge may have unpatched vulnerabilities that allow attackers to intercept sensitive data affecting confidentiality * Using unsupported versions of Edge can compromise the integrity of data	NIST SP 800-53 Revision 4 SI-2 (c) requires that organizations ensure the integration of security event monitoring tools to detect, log, and respond to security incidents across their information systems.
Microsoft Edge	V-260467	Open	* Persistent cookies can compromise confidentiality by allowing unauthorized users to access private data associated with a session * Allowing session-only cookies can help prevent attackers from tampering with cookies or using them to alter the integrity of the session.	NIST SP 800-53 AU-10 requires organizations to implement the capability to automatically generate audit records for specific system activities, such as security events or access control actions, and ensure that audit information is protected from unauthorized access or modification.
Microsoft Edge	V-260466	Open	* Persistent cookies can compromise confidentiality by allowing unauthorized users to access private data associated with a session * Allowing session-only cookies can help prevent attackers from tampering with cookies or using them to alter the integrity of the session.	NIST SP 800-53 CM-7 requires organizations to manage the use of administrative privileges on information systems. This control mandates the implementation of appropriate measures to monitor, restrict, and control the use of these privileges to prevent unauthorized access and mitigate security risks.
Microsoft Edge	V-260465	Open	* Disabling Visual Search helps protect the Confidentiality of sensitive images by ensuring they are not shared with external services for processing.	NIST SP 800-53 CM-7 requires organizations to manage the use of administrative privileges on information systems. This control mandates the implementation of appropriate measures to monitor, restrict, and control the use of these privileges to prevent unauthorized access and mitigate security risks.
Google Chrome	V-245538	Open	* QUIC could undermine the integrity of the communication channel by preventing the detection of alterations or attacks * Data exchanges that are potentially malicious or otherwise undesirable cannot be inspected, threatening the confidentiality	NIST SP 800-53 Revision 4 CM-7 (1) (b) specifies that information systems must enforce the use of strong authentication methods to secure administrative access to the system. It requires the implementation of multi-factor authentication (MFA) for administrators to reduce the risk of unauthorized access and enhance the security of administrative functions.
Google Chrome	V-241787	Open	* Attackers could disable or interfere with Bluetooth devices, preventing them from functioning correctly threatening availability * Misconfigured Web Bluetooth API , could potentially gain access to sensitive data from Bluetooth devices without user knowledge. This breach	NIST SP 800-53 CM-7 requires organizations to manage the use of administrative privileges on information systems. This control mandates the implementation of appropriate measures to monitor, restrict, and control the use of these privileges to prevent unauthorized access and mitigate security risks.
Google Chrome	V-226404	Open	* The main concern with importing AutoFill data is that sensitive user information may be imported from a compromised environment * Importing potentially compromised or outdated AutoFill data could affect the integrity of the information being used within the browser	NIST SP 800-53 SC-18 (1) requires organizations to implement measures to protect the confidentiality and integrity of communications across a system. This control specifically mandates the use of cryptographic mechanisms to protect the information during transmission, ensuring that unauthorized parties cannot access or alter it.
Windows 10 STIG	V-242009	Not Reviewed	* Inbound exceptions are not strictly limited to authorized systems, unauthorized access leading to a breach of confidentiality and Integrity	NIST SP 800-53 AC-17 (1) requires organizations to implement remote access policies and controls to restrict and monitor remote access to their systems. This control mandates the use of secure communication channels and appropriate access controls for remote users, ensuring that remote sessions are authorized and protected against
Windows 10 STIG	V-242005	Not A Finding	* The firewall's integrity could be compromised if the rules are incorrectly merged, allowing unauthorized modifications	NIST SP 800-53 SC-24 requires organizations to implement measures to protect against unauthorized data transfers across network boundaries. This control mandates the use of security mechanisms, such as encryption and traffic filtering, to prevent the leakage or interception of sensitive information during communication between systems
Windows 10 STIG	V-242003	Open	* The availability of system resources and services could be impacted if outbound connections are improperly blocked * Integrity could be impacted if the firewall is configured in such a way that legitimate outbound communication is blocked	NIST SP 800-53 SC-5 (1) requires organizations to control the use of communications protocols that may pose security risks. This control specifically focuses on disabling unnecessary or insecure protocols, such as Telnet or FTP, to prevent unauthorized access or data leakage
Windows 10 STIG	V-241991	Not A Finding	* Availability could be impacted if the system becomes compromised or subject to denial-of-service (DoS) attacks * Malicious actors could use the unprotected system to alter or corrupt data affecting Integrity	NIST SP 800-53 AC-4 requires organizations to manage and control the use of remote access to their systems. This includes enforcing policies to ensure that remote access is authorized, properly authenticated, and monitored to prevent unauthorized access or malicious activity.