NFSU

National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance (Ministry of Home Affairs, Government of India)

PROJECT REPORT

ON

"WindSec – Windows OS Hardening Tool"

Submitted To

School of Cyber Security & Digital Forensics,

National Forensic Sciences University

For partial fulfilment for the award of degree

MASTER OF SCIENCES

In

CYBER SECURITY

Submitted By

Hardik Purohit

(101CTMSCS2122046)

Under the Supervision of

Asst. Professor Nilesh Panchal (SCSFD)

National Forensic Sciences University,

Gandhinagar Campus, Gandhinagar – 382009, Gujarat, India.

August, 2022

DECLARATION

I certify that

a. The work contained in the dissertation is original and has been done by myself under the supervision of my supervisor.

b. The work has not been submitted to any other Institute for any degree or diploma.

c. I have conformed to the norms and guidelines given in the Ethical Code of Conduct of the Institute.

d. Whenever I have used materials (data, theoretical analysis, and text) from other sources, I have given due credit to them by citing them in the text of the dissertation and giving their details in the references.

e. Whenever I have quoted written materials from other sources and due credit is given to the sources by citing them.

f. From the plagiarism test, it is found that the similarity index of whole dissertation within 25% and single paper is less than 10 % as per the university guidelines.

Date:
Place:

Hardik Purohit
Enrol No.: 101CTMSCS2122046

CERTIFICATE

This is to certify that the work contained in the dissertation entitled **"WindSec – Windows OS Hardening tool"**, submitted by **Hardik Purohit (Enroll. No.: 101CTMSCS21220146)** for the award of the degree of **Master of Sciences in Cyber Security** to the **National Forensic Sciences University**, **Gandhinagar Campus**, is a record of bonafide research works carried out by him under my direct supervision and guidance.

Date:
Place:

Mr. Nilesh Panchal
Assistant Professor,
School of Cyber Security & Digital Forensics,
National Forensic Sciences University,
Gandhinagar Campus, Gandhinagar, Gujarat, India.

ACKNOWLEDGEMENTS

Write an acknowledgement for maximum of one page. The candidate should convey his appreciation to all whom have played a role for completion of his dissertation work. The supervisor, supervisor, head of the department, faculty members, lab mates etc may be acknowledged. Any controversial statement or non-academic/abused sentiments are not allowed to write in this page.

With Sincere Regards,

Hardik Purohit

MSc. Cyber Security

ABSTRACT

Cybercrime is on the rise right now. Systems are prone to attack because of security setup errors. The majority of systems have client-side or endpoint vulnerabilities. Violations of operating system vulnerabilities may be used to gain access to the system. The security configurations and functions exclusive to the Windows operating system. Most users don't set up security configuration correctly, leaving computers open to attackers. Today's highly sophisticated assaults, such as malware, ransomware, remote administration tools, etc., can be used to compromise a system's security.

The only defence against such major threats is hardening the Windows operating system. Users can use WindSec – OS Hardening tool for the Hardening of the system. Due to security misconfiguration, ransomware like Wanncry and Petya infected almost every Windows system. In order to maintain the required security level, this project is focused on creating a tool for security configuration in Windows operating systems according to versions and vulnerabilities associated with those OS versions. As a result, an automated system security framework will be created to keep Windows-based operating systems at a high level of security.

Keywords: *OS Hardening; WindSec; Vulnerability; Security Audit; Threats;*

LIST OF FIGURES

Fig No	Figure Description	Page No
Figure 1	Operating System Market share	10
Figure 2	Sequence Diagram	16
Figure 3	Activity Diagram	17
Figure 4	Functional & Behavioural Diagram	18
Figure 5	User Account Access	23
Figure 6	VMware Configurations	30

LIST OF SCREENSHOTS

Screenshot No	Screenshot Description	Page No
Screenshot 1	Program Run	20
Screenshot 2	Mode Selection	20
Screenshot 3	Feature Implementations	21

TABLE OF CONTENTS

Acknowledgement			IV
Abstract			V
List of Figures			VI
List of Screenshots			VII
Table of Contents			VIII
Chapter 1.	**Introduction**		**1-4**
	1.1	Introduction	1
	1.2	Problem Summary	1
	1.3	Aim and Objectives of the Project	1
	1.4	Scope of the Project	2
Chapter 2.	**Literature Survey**		**5-7**
	2.1	Current/Existing System	5
		2.1.1 Study of Current System	5
		2.1.2 Problem & Weakness of Current System	6
	2.2	Requirements of New System	6
	2.3	Feasibility Study	7
Chapter 3.	**Design: Analysis, Design Methodology and Implementation Strategy**		**8-10**
	3.1	Sequence Diagram	8
	3.2	Activity Diagram	9
	3.3	Functional & Behavioural Modelling	10
Chapter 4.	**Implementation**		**11-23**
	4.1	Implementation Environment	11
	4.2	Security Techniques	14
	4.3	Privacy Techniques	19
	4.4	Laboratory Setup	21
	4.5	Tools and Technology Used	22
Chapter 5.	**Summary of Results and Future Scope**		**24-27**
	5.1	Advantages/Unique Features	24
	5.2	Future Scope of Work	27
Chapter 6.	**Conclusion**		**28**
References			**29-30**

1. INTRODUCTION

1.1 Introduction to OS Hardening

Operating System (OS) hardening is the cyclic process of configuring an Operating System as per security requirements. OS hardening includes installing regular updates from OS developers and also patches the vulnerabilities with automated tools or manual efforts. In OS Hardening user can create rules and defined policies to keep the system secure against cyber threats. OS Hardening should be performed periodically to minimizing the possible risks possessed by OS, to the system or network. Operating System Security Audit is a powerful method to harden the security of any operating system. Security audit of an Operating System can be used for user malicious activity identification, system forensic investigation and security compliance. Security audit is helpful to any of the security auditor to ensure the security levels of the information is maintained as per compliance and standards predefined by the users.

1.2 Problem Statement

Most operating systems are not very secure out of the box and favour convenience and ease of use over security. IT Security professionals may not agree with a vendor's user-friendly approach to their OS, but that does not mean they have to accept it. There are steps that can be taken to harden a system and eliminate as many security risks as possible.

It's very difficult to properly harden/configure a system so that it keeps running effectively. Documentation is scarce, and permissions are required to make it effective--and in the Windows world, permissions remain one of those mystic arts. Finally, even a hardened Windows server will probably have far too many resident files and registry entries to effectively monitor and maintain.

1.3Aim and Objectives of the Project

The objective of developing this project that is a Windows OS hardening tool is to make the whole OS Hardening process very smooth and most importantly efficient with the help of an interactive console that guides us to one of the best operating system configurations.

The tool can perform the hardening in both the ways that is manual as well as automatic. The automatic approach will consist all the required security measures implemented but they can vary from policy to policy. Hence, the feature of manual configuration will also be available within the tool. This feature will enable the System administrators to manually implement all the security configurations like they want to setup with the help of WindSec tool's command-line console.

WindSec will also implement many of the privacy features which is a plus point with an OS Hardening tool. The privacy features are like disabling all the data collection features available on the operating system itself. Apart from OS data collection features WindSec also disables other 3rd party software to access system data using many security measures.

1.4 Scope of the Project

Since, most of the end users are using Windows Operating System in the personal or office desktop PCs. The by default security of Windows Operating System is not adequate to provide security against latest threats to the users. Here in this research, Windows internals will be studied, identification of known and unknown vulnerability of various Windows versions like Windows 7, 8, 8.1 and 10. Windows OS hardening contains following techniques or tactics:

- Windows Vulnerability Assessment
- Security Audit
- Security Log Analysis

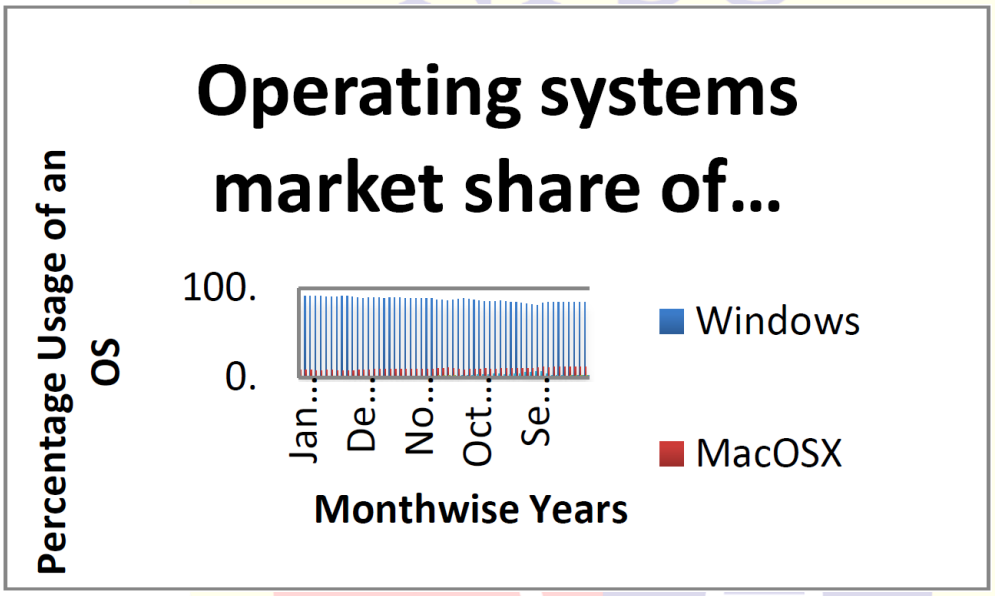


Fig 1: Operating System Market share of desktop PCs from year 2013-2017

Today sophisticated attack can grab malicious content via malvertising, advertising banners, fake or bogus links, emails with malicious office file-based macro code attachments and storage media. Here, important part of reducing such risk is to audit the system against such threats periodically and steps should be taken to patch the high impact vulnerability. That's how the system can hardened against sophisticated and malicious cyber-attacks. Most desktops with Microsoft windows operating systems have by default firewall for network security, but few computers start and configure the services provided by default in the windows operating system. Utilities such as spyware blockers, ad blockers, and antimalware solutions may useful to prevent execution of malicious software on the system at some extent. Though the antimalware or antivirus solution installed on the system, it is still vulnerable to malicious attacks like ransomwares etc. Any public or private sector asset security is depending upon its IT infrastructure and Network Infrastructure security. Firewall, Intrusion Detection Prevention System and Unified Threat Management solution can only provide perimeter security or network related operation level security. IT Infrastructure security is only depending upon security auditing of the endpoints and harden those endpoints with proper patches to reduce risks associated with known and unknown vulnerability exploits.

Windows Operating System hardening helps users in minimizing the risk associated with security vulnerabilities. The prime purpose of system hardening is to disclose the vulnerability remains into the system, identifying the risk associated with that vulnerability and patch that vulnerability to avoid security risks. Some security risks can be reduced by removing unnecessary utilities, software programs and utilities from the system.

Windows operating systems are designed for a great number of purposes. For this reason,

they include a lot of possible hardening objects. While developing an all new hardening configuration was not done in this thesis, a lot of examination of possible Windows hardening parameters was done. Some security testing and AppLocker auditing was also done

to review the current level of hardening. This section presents some of those parameters

which includes a few settings and removable features that should be considered to be

removed when hardening Windows operating systems. Operating systems in focus are

Windows 10 and Windows Server 2012 R2 that were used for the script implementation

in this thesis. The following hardening objects do not give a fully comprehensive hardening configuration. The section only gives some ideas of what to look for when hardening

Windows operating systems, and how hardening could be improved. Unlike in a traditional ICT environment, restrictions in an ICS environment can prevent classic ways to

implement the hardening configuration. Remote connections can be very limited and internet connection is not available. For these reasons, the configuration is usually implemented locally. Configuring manually all required parameters is time consuming and so

the hardening is done automatically with scripts.

Windows 10 is quite aggressive in collecting telemetry information and error reporting.

Having these features in system that does not have an internet connection is quite pointless. Disabling all settings, services and scheduled tasks related to these, can be recommended for all Windows devices in ICSs. Even if this would not increase the security

very much, it can decrease unnecessary network traffic. Other Windows features that require an internet connection can also be removed in most cases. These include the Windows Store, social features, such as Messaging or Skype, OneDrive, an e-mail program,

the Weather application and other features depending on the Windows version. In addition to these there are games and gaming related services and tasks running in Windows

10, some of which are found even in server versions of Windows. These include Microsoft Solitaire Collection, Xbox live services and tasks, which should be removed, and

disabling the Windows 10 gaming mode. After that, there are still media content and other

programs that should be removed. The server versions are a little better in this way, because server computers rarely need those features, and so Microsoft does not include

them. However, this has changed a little bit with the latest Server 2016 which seems to

include two Xbox live related services if the desktop experience is installed. These are recommended to be disabled even by Microsoft Security Guidance blog [32]. Additionally, the local group policy should be configured in a secure way. The Windows secure baseline configuration can be most helpful in this part of hardening. It has a list of policy objects with descriptions, suggested values of these objects, and registry keys. [51] The baseline includes settings for user accounts, audit and logging, security options, firewall and a lot of other settings.

2. Literature Review

2.1 Current/Existing System

2.1.1 Study of Current System

Programs clean-up

Program clean up includes remove unwanted programs. Most of the free tools and demo tools came with their own vulnerabilities, which may infect the overall security of the system. Most of programs may convert as backdoor for an attacker.[9] Cyber attacker looks for zero-days, backdoors and program vulnerabilities to exploit the system. To minimize the risk of exploitation of the system, junk programs or unused programs cab be cleaned up from the system. For that user may have to regularly scan for the residues of the unused programs like dynamic link libraries, dependency files, or any other files created by that program on windows operating system.[22]

Use of service packs

Always look for the new updates came from Microsoft. Windows update feature in windows operating system automatically check for the new updates and keep system up to-date and remind user to install the latest available versions. Complete security never possible on any system, but if user up-to-date with the system up-gradation, user can safeguard the system against zero-day attacks or overall system vulnerabilities identified till that upgrade.

Patches and patch management

User has to follow PDCA (Plan, Do, Check and Act) cycle periodically as a part of regular audit. User can make manual, semi-automated or fully automated tools or scripts to conduct PDCA for identifying new patches and apply those patches to ensure the overall security of an operating system.

Group policies

Windows operating system is having one of the best features i.e. Group Policies. It is used to create different users or user groups with distinct functionality or access assigned to that particular user or user group. In most of the cases, errors done by users leads to cyber-attack or devices got compromised. If single user is there, then also group policy can be defined. Configure, implement and update group user policies to ensure users security and reduce the risk of cyber-attack due to user error.[10] For example, every user must have to comply with clean desktop policy.

Security templates

Security templates can be used in corporate, where the users size is huge and distribution of the work is scattered. In such cases maintaining security is challenging task.[20] To automate and simplifying the security compliance to each use or user group, security templates can be used. In which, policies defined for users or groups

can be loaded into procedure or function. Such templates can be enforced to each users or user group to comply.

Configuration baselines

Baseline configuration is the concept in which user can start measuring changes in file system, operating system, application, hardware, network infrastructure, etc. In Operating system hardening, baseline can be crucial aspect.[11] To create a baseline for OS Hardening, user can select and measure OS level updates, processes, applications, and patch management etc. for a period of time.

2.1.2 Problem & Weakness of Current System

A lot have been said about server security baselines, but still a great amount of heavily regulated organizations are struggling to show compliance with hardening baseline requirements.

Server security baseline deployments processes are rife with challenges. Whether organizations use scripts to manually brute-force their system-level compliance baseline, or perhaps leverage the common "Gold Disk" approach or GPO's, achieving and maintaining security baseline compliance deployment remains largely an unsolved and constant challenge even for the most mature of IT organizations.

Applying a baseline to a newly deployed server or application is one thing, but validating compliance throughout the server and application lifecycle typically requires a separate set of tools and processes. As the main challenge deploying a baseline is to avoid affecting the server availability and causing downtime while ensuring the baseline is constantly enforced.

To add to the challenge, organizations have issues frequently arise around how to identify new systems that require baselining as they come online, and then immediately recognize what needs to be done on those systems in order to verify their compliance.

2.2 Requirement of New System

Protecting endpoints is a fundamental task in securing your organization from cyber-attacks. Endpoints are a popular attack vector used by malicious actors. Estimates suggest that 70% of all breaches originate in endpoints. With today's advanced attack mechanisms, trusting only firewalls and antivirus software for security won't cut it anymore. Endpoint hardening is a must for achieving full cybersecurity protection.

Endpoint hardening refers to control over configuration changes in the endpoint's operating system, with the intention of minimizing the attack surface. The configuration changes are usually made on unsecure and unnecessary protocols and services that are enabled by default in the operating system. These protocols and services are usually enabled to provide the

endpoint with maximal functionality. Unfortunately, they often expose the network to vulnerabilities.

Changing the default configuration of the endpoint in accordance with best-practice recommendations may sound simple, but it poses great risks to your endpoint's functionality. Each change requires a long and complex process of testing before implementation – to make sure nothing will break as a result of the change. This labour and time-consuming process often leads organizations to neglect this task, increasing endpoint vulnerability. Furthermore, since vulnerabilities are constantly discovered and endpoint requirements are constantly changing, the hardening process is not a one-time operation – it requires protocols for routine, periodic maintenance.

2.3 Feasibility Study

Although the principles of system hardening are universal, specific tools and techniques do vary depending on the type of hardening you are carrying out. System hardening is needed throughout the lifecycle of technology, from initial installation, through configuration, maintenance, and support, to end-of-life decommissioning. Systems hardening is also a requirement of mandates such as PCI DSS and HIPAA.

Hence, there is a need already there in the market for an OS Hardening Tools which works effectively as well as the tool should also be easy to configure. Some of more features which WINDSEC have within it.

If we concern about operational feasibility then the WINDSEC is performing very well with the Windows Environment. It will also be operational in future also as there will be continuous development that will be performed to keep the Tool operational and also feasible.

3. Design: Analysis, Design Methodology and Implementation Strategy

3.1 Sequence Diagram

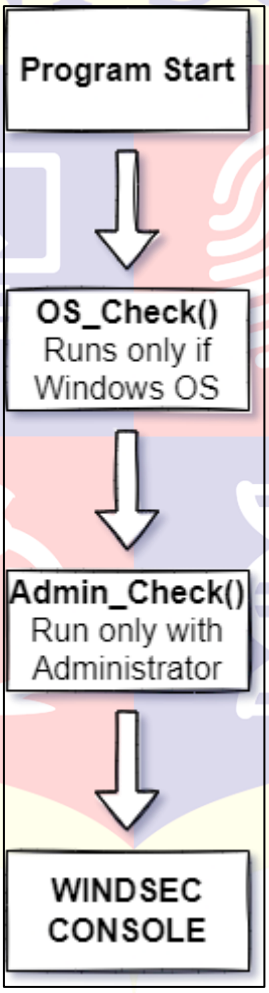


Fig 2: Sequence Diagram

3.2 Activity Diagram

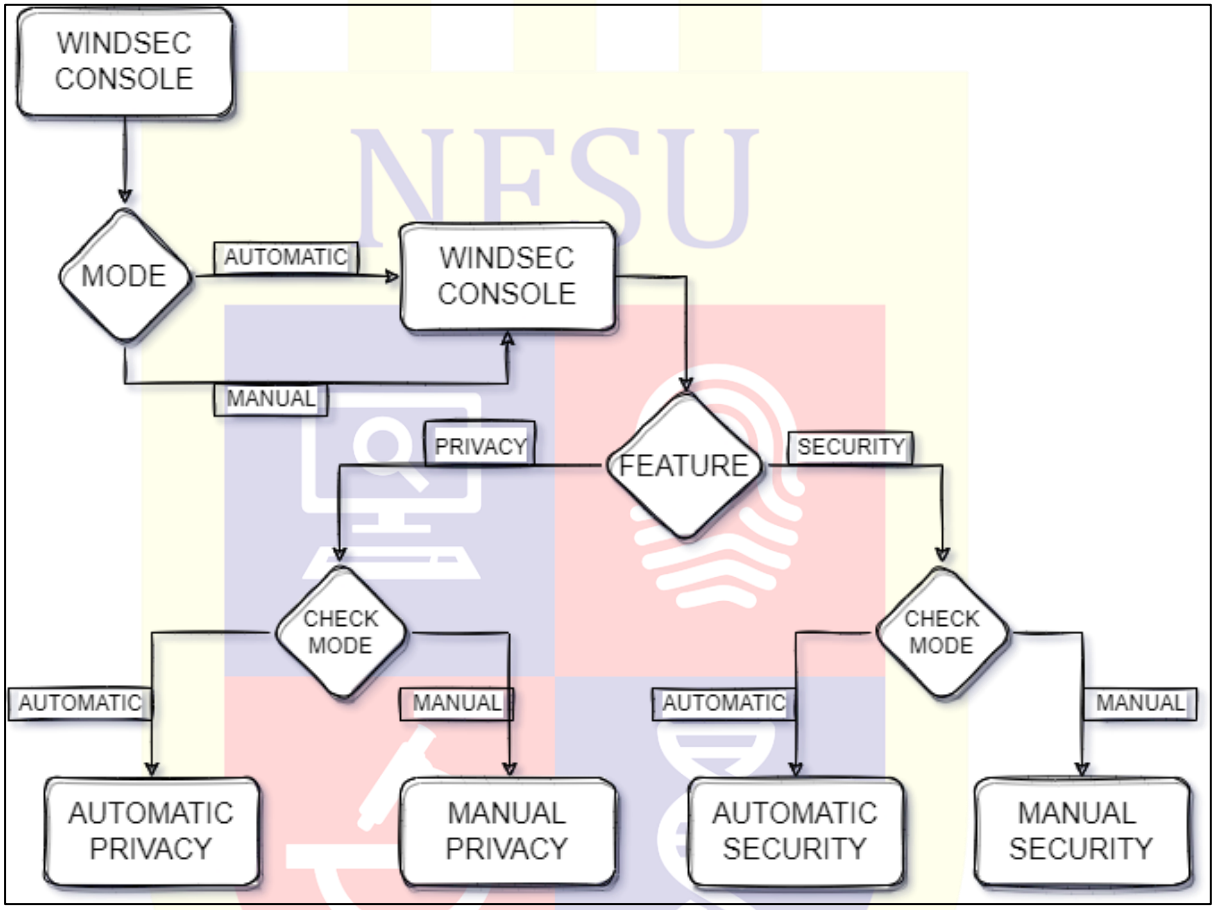


Fig 3: Activity Diagram

3.3 Functional & Behavioural Modelling

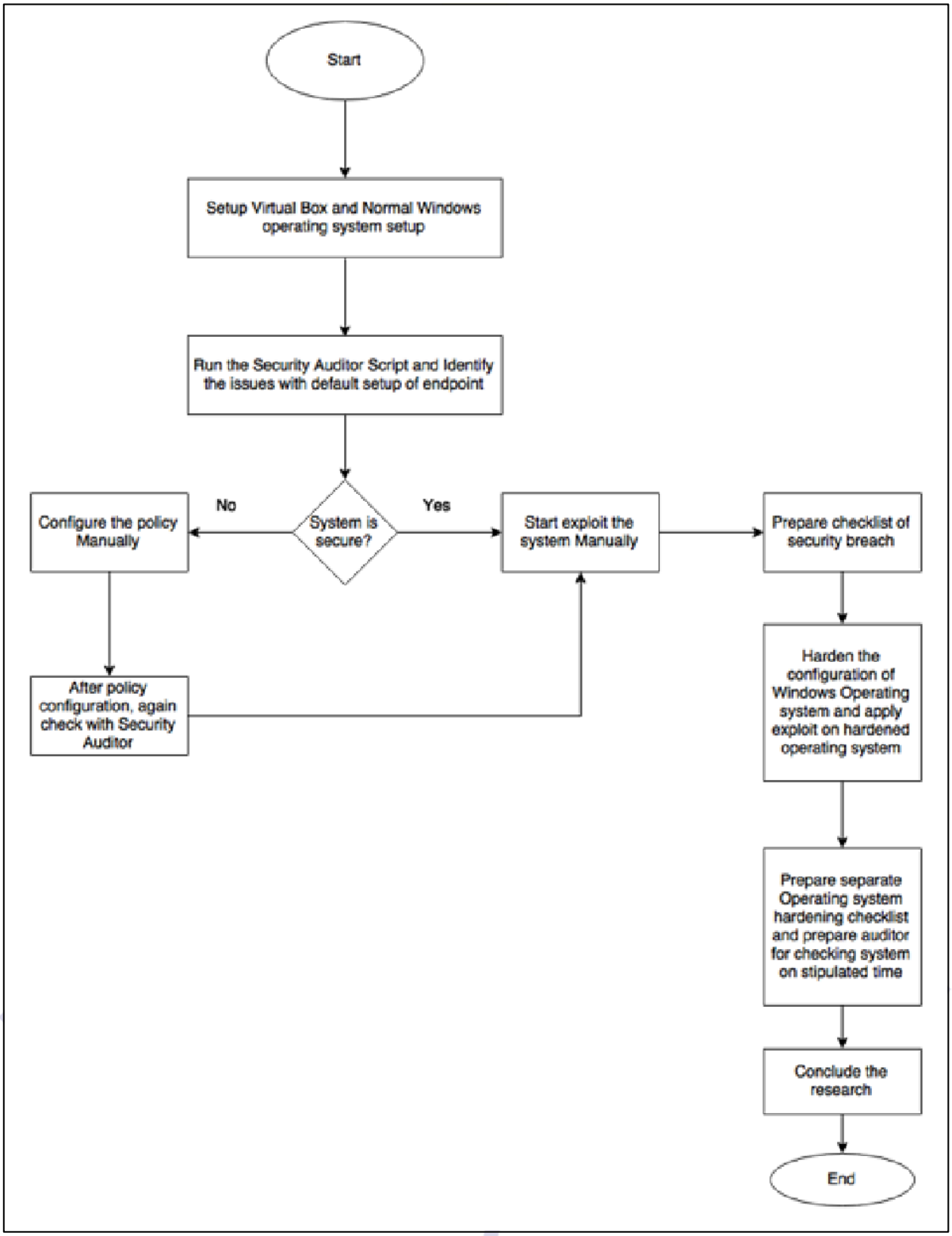


Fig 4: Functional Modelling of OS Hardening

4.0 Implementation

4.1 Implementation Environment

To implement the WindSec OS Hardening configurations, we have to take a freshly installed Windows Machine on which the security configurations have to be implemented.

Now let's look at steps to implement Windows Operating System Hardening using our WINDSEC tool.

Step 1: Setup a new Windows Machine.

Step 2: Download WINDSEC from its GitHub Repository.

https://github.com/hardhax10/WindSec

You can find a file named **WINDSEC.EXE**

Step 3: Run the executable file using Administrative Privileges.

Right Click on File > Run as Administrator

Step 4: The WINDSEC Console Window will be visible in front of the screen.

Now, the tool can be used efficiently by first of all selecting the Flow of the application using commands like "use auto pilot" OR "use manual".

All these instructions will also be available within the WindSec Console.

Step 5: Since, you have selected the flow mode. Hence, you have to select the Functioning which you want to implement.

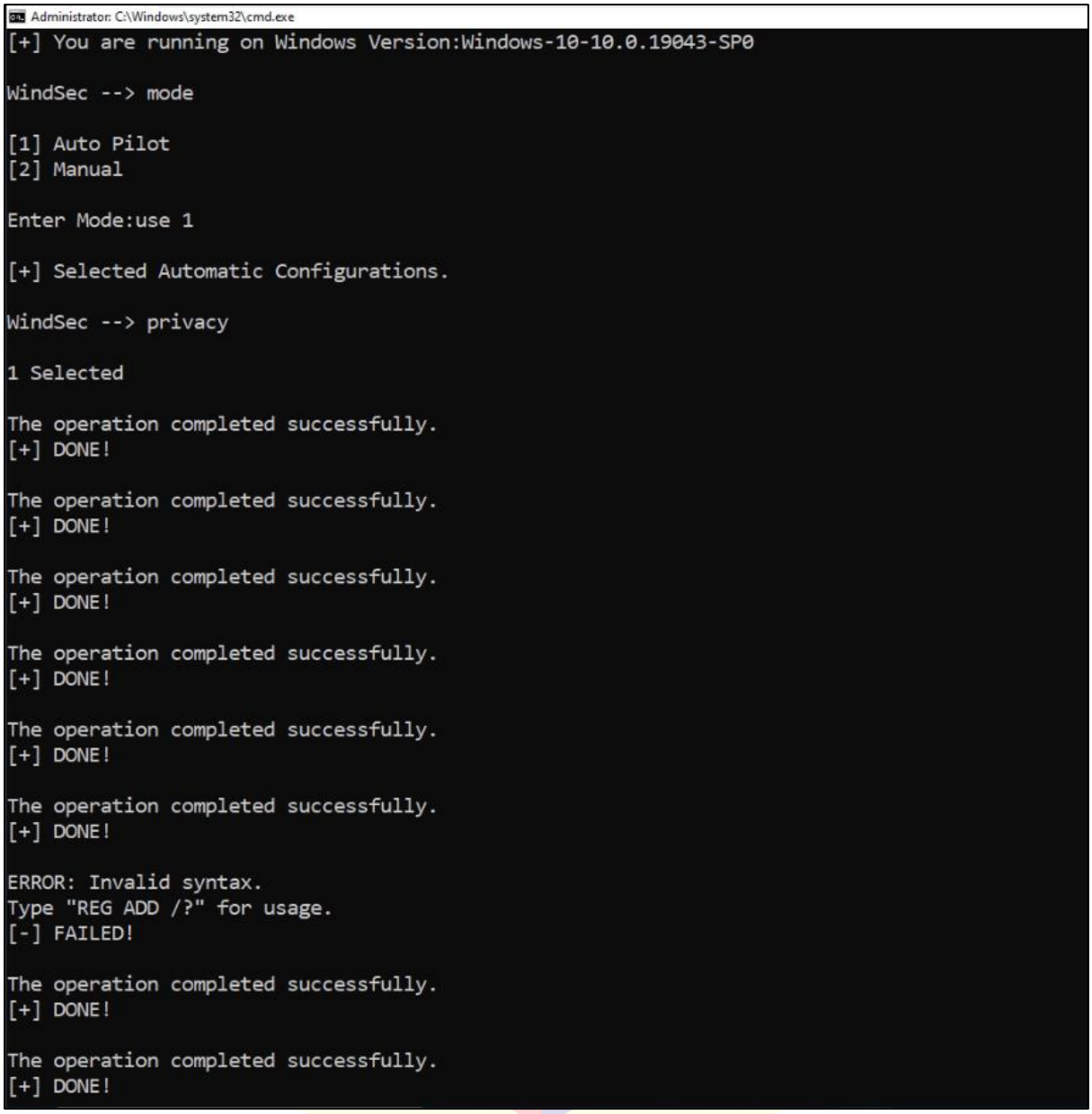
```
[+] You are running on Windows Version:Windows-10-10.0.22000-SP0

WindSec --> mode

[1] Auto Pilot
[2] Manual

Enter Mode:use 1

[+] Selected Automatic Configurations.

WindSec --> use 2
Entered input is not a valid command in WindSec

WindSec -->
```

Screenshot 1: Flow Mode

```
Administrator: C:\Windows\system32\cmd.exe
[+] You are running on Windows Version:Windows-10-10.0.19043-SP0

WindSec --> mode

[1] Auto Pilot
[2] Manual

Enter Mode:use 1

[+] Selected Automatic Configurations.

WindSec --> security

1 Selected

The operation completed successfully.
[+] DONE!

The operation completed successfully.
[+] DONE!

The operation completed successfully.
[+] DONE!

The operation completed successfully.
[+] DONE!

The operation completed successfully.
[+] DONE!

The operation completed successfully.
[+] DONE!

ERROR: Invalid syntax.
Type "REG ADD /?" for usage.
[-] FAILED!

The operation completed successfully.
[+] DONE!

The operation completed successfully.
[+] DONE!
```

Screenshot 2: Security Implementation

For Privacy:



Screenshot 3: Privacy Implementation

4.2 Security Techniques

- **MICROSOFT DEFENDER FIREWALL**

  Windows Defender Firewall with Advanced Security is an important part of a layered security model. By providing host-based, two-way network traffic filtering for a device, Windows Defender Firewall blocks unauthorized network traffic flowing into or out of the local device. Windows Defender Firewall also works with Network Awareness so that it can apply security settings appropriate to the types of networks to which the device is connected. Windows Defender Firewall and Internet Protocol Security (IPsec) configuration settings are integrated into a single Microsoft Management Console (MMC) named Windows Defender Firewall, so Windows Defender Firewall is also an important part of your network's isolation strategy.

  Features:

  - **Reduces the risk of network security threats.** Windows Defender Firewall reduces the attack surface of a device, providing an extra layer to the defense-in-depth model. Reducing the attack surface of a device increases manageability and decreases the likelihood of a successful attack.
  - **Safeguards sensitive data and intellectual property.** With its integration with IPsec, Windows Defender Firewall provides a simple way to enforce authenticated, end-to-end network communications. It provides scalable, tiered access to trusted network resources, helping to enforce integrity of the data, and optionally helping to protect the confidentiality of the data.
  - **Extends the value of existing investments.** Because Windows Defender Firewall is a host-based firewall that is included with the operating system, there's no other hardware or software required. Windows Defender Firewall is also designed to complement existing non-Microsoft network security solutions through a documented application programming interface (API).

- **SERVICES**

  Windows 10 systems contain many services that organizations don't want or need running. The system should be checked for both rogue services and those that came pre-installed.

  - Disable any unnecessary services on the system
  - Disable Remote Registry
  - Disable SMB shares

- **USER ACCOUNTS**
  Apply the principle of least privilege

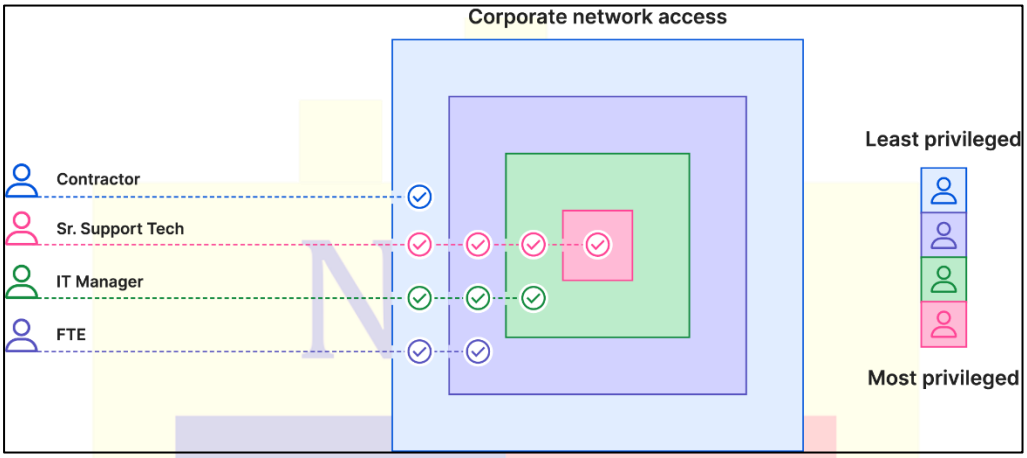


Fig 5: User Account Access

Disable Accounts
- Default accounts
- Unused accounts

- **STARTUP**

  Disable or remove any unnecessary executables or services that run on startup / logon

  This can be implemented using 2 techniques:

  - SysInternals Autorun.exe
  - Windows Registry
  - Startup Settings on Windows

- **WINDOWS FEATURES**

  Windows 10 comes with a number of "optional" features that you can turn on or off through the Windows Features dialog. Many of these features are intended for business networks and servers, while some are useful to everyone. Here's an explanation of what each feature is for, and how to turn them on or off.

  All these Windows 10 features take up space on your hard drive whether you have them enabled or not. But you shouldn't just enable every feature–that could result in security problems and slower system performance. Only enable the features you need and will actually use.

  Disable unused features (e.g., Telnet / TFTP clients, WSL)

- **WINDOWS UPDATES**

  Windows Update is used to keep Microsoft Windows and several other Microsoft programs updated.

  Updates often include feature enhancements and security updates to protect Windows from malware and malicious attacks.

  You can also use Windows Update to access the update history that shows all the updates that have been installed to the computer through the Windows Update service.

  How you access Windows Update depends on which Windows operating system you're using:

  - Windows 11 and Windows 10: Windows Update is built-in and a part of Settings, available from the Start menu.
  - Windows 8, Windows 7, and Windows Vista: Windows Update is integrated as a Control Panel applet and is accessible from within Control Panel.
  - Windows XP, 2000, ME, 98: In older Windows versions, Windows Update is accessible using the Windows Update website through Internet Explorer.

- **WINDOWS DEFENDER ANTIVIRUS**

  Microsoft Defender Antivirus is available in Windows 10 and Windows 11, and in versions of Windows Server.

  Microsoft Defender Antivirus is a major component of your next-generation protection in Microsoft Defender for Endpoint. This protection brings together machine learning, big-data analysis, in-depth threat resistance research, and the Microsoft cloud infrastructure to protect devices (or endpoints) in your organization. Microsoft Defender Antivirus is built into Windows, and it works with Microsoft Defender for Endpoint to provide protection on your device and in the cloud.

- **GROUP POLICY OBJECT (GPO)**

  Password policy
  - Minimum password length: 8 characters
  - Maximum password length: 64 characters
  - Minimum password age: 1 day
  - Maximum password age: 90 days
  - Complexity requirements: Enabled
  - Store passwords using reversible encryption: Disabled

  Lockout policy
  - Account lockout duration: 15 minutes
  - Account lockout threshold: 10 failed authentication attempts

- Reset counter after: 15 minutes

User Account Control

- Admin Approval Mode for the built-in Administrator account: Enabled
- Run all administrators in Admin Approval Mode: Enabled

Interactive logon

- Machine inactivity limit: 900 seconds
- Prompt user to change password before expiration: 14 days
- Do not require CTRL+ALT+DEL: Disabled

Network Access

- Do not allow anonymous enumeration of SAM accounts: Enabled
- Do not allow anonymous enumeration of SAM accounts and shares: Enabled

Network Security

- LAN Manager authentication level: 5 (Send NTLMv2 response only. Refuse LM & NTLM)

Windows Defender Antivirus

- Turn off Windows Defender Antivirus: Disabled

Windows Update

- Configure Automatic Updates: 3 (automatically download and notify for install)
- Remove access to use all Windows Update features: Disabled

Additional notes

- Applocker: restrict executables for certain users
- Bitlocker: encrypt drives through File Explorer or GPO
- Password: protect the screensaver

- **REGISTRY**

The registry is a hierarchical database used to store configuration information for users, applications, and hardware devices. Group policy is used to push values into the registry for settings. There are registry keys associated with these policies. If you want to use Command Prompt, you can edit the registry directly with the reg command. If you edit the registry directly, we recommend that you back it up beforehand in case anything goes wrong.

- **REGISTRY COMMANDS**

Enable User Account Control (UAC):

reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t Reg DWORD /d 1 /f

Enable Windows Defender Antivirus:

reg delete "HKLM\Software\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /f

Enable Automatic Updates

reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\AU" /v NoAutoUpdate /t Reg_DWORD /d 0 /f

Automatically download and notify of install for updates

reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\AU" /v AUOptions /t Reg_DWORD /d 3 /f

Restrict anonymous access:

reg add HKLM\System\CurrentControlSet\Control\Lsa\ /v restrictanonymous /t Reg_DWORD /d 1 /f

Block anonymous enumeration of SAM accounts and shares:

reg add HKLM\System\CurrentControlSet\Control\Lsa\ /v restrictanonymoussam /t Reg_DWORD /d 1 /f

Send NTLMv2 response only; refuse LM & NTLM:

reg add HKLM\System\CurrentControlSet\Control\Lsa\ /v lmcompatibilitylevel /t Reg_DWORD /d 5 /f

Disable admin autologon:

reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t Reg_DWORD /d 0 /f

Prevent the inclusion of the Everyone security group SID in the anonymous user's access token:

reg add HKLM\System\CurrentControlSet\Control\Lsa\ /v everyoneincludesanonymous /t Reg_DWORD /d 0 /f

Disable EnablePlainTextPassword:

reg add HKLM\System\CurrentControlSet\services\LanmanWorkstation\Parameters /v EnablePlainTextPassword /t Reg_DWORD /d 0 /f

Disable IPv6:

reg add HKLM\System\CurrentControlSet\services\TCPIP6\Parameters /v DisabledComponents /t Reg DWORD /d 255 /f

Disable Remote Desktop Protocol (RDP):

reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /f /v fDenyTSConnections /t Reg DWORD /d 1

4.3 Privacy Techniques

- **Turn Off Tailored Adverts**
  Firstly you will want to deal with the tailored adverts system, you do this in Windows 10 security settings.
  To disable it go to Settings > Privacy > General and slide the option that says 'Let apps use my advertising ID for experience across apps (turning this off will reset your ID)' to the Off position.
  Now turn off any ad blockers in your browser (as they interfere) and head over to choice.microsoft.com/en-us/opt-out. Once there, choose Off for 'Personalized ads wherever I use my Microsoft account' and 'Personalized ads in this browser.'

- **Disable Cortana**
  Open Cortana in your taskbar, and hit the notebook icon on the left-hand side of the pop-up.
  Click on Settings, and slide to Off the option that says 'Cortana can give you suggestions, ideas, reminders, alerts, and more'.
  With Cortana gone, you also have the option to disable Bing results. If Bing is not your cup of tea, then disable 'Search online and include web results.

- **Stop Getting to Know Me!**
  Now go back into Settings and go to Privacy > Speech, inking, and typing.
  Here you must click 'stop getting to know me. That will disable the infamous keystroke and recorder that has been causing so much debate.

- **Erase Cortana's memory**
  At this point click on 'Go to Bing and manage personal info for all your devices.' Where you can delete everything that Cortana has up to that point managed to figure out about you by clicking on Clear at the bottom.

- **Choose Your Hotspots**
  Fifth on your to-do list: go to Settings > Network & Internet > Wi-Fi > Manage Wi-Fi Settings.
  Here is where you turn off Wi-Fi Sense. Do that by sliding 'Connect to suggested open hotspots' and 'Connect to open networks shared by my contacts' to the Off position.

- **Stop Sharing System Files**
  Stop Windows 10 sharing system files and updates to your PC (and from your PC to other users) by default.

Go to Settings > Update & Security > Windows Update > Advanced Options > Choose how updates are delivered.
Here you will need to make the choice to either completely disable ‘Updates from more than one place' or deciding to opt for sharing info just with ‘PCs on your local network’. Up to you.

- **Turn Off One Drive**
  At this stage, you will want to stop Windows 10 from storing info on Microsoft’s servers. This is called OneDrive.

- **Stop Sending Info to Microsoft**
  Now return to Settings > Privacy and select General, where you will want to turn off 'Send Microsoft info about how I write to help us improve typing and writing in the future,' and 'Let websites provide locally relevant content by accessing my language list.'

- **Disable Windows 10 Location Service**
  If you want to, you can also disable the Windows 10 Location service that is found directly under General. Here you can either get rid of it completely in Change or set it to Off only for that particular user.

- **App permissions**
  Continue down the list of apps under General and Location: disabling any of the features you do not want.
  Do consider carefully, however, as some options (like the Mail app looking in your contacts) may be beneficial.

- **Microsoft Edge**
  Microsoft Edge is the new Internet browser in Windows 10. It is set to communicate with Microsoft by default.
  To stop it, open Edge, click the menu (three horizontal dots) select Settings > View Advanced Settings.
  Here switch off everything that you do not want in the 'Privacy and services’ section (‘show search suggestions’ and 'Help protect me from malicious sites and downloads with SmartScreen filter' may well be worth leaving on as they both serve legitimate functions.)

- **Settings Sync**
  If you do not want your Windows 10 settings to be available on your request to other PC’s, then you should go to Settings > Accounts > Sync your settings and slide it to Off.

- **SmartScreen**
  SmartScreen is a feature that helps protect you from unwanted and malicious desktop programs. You should only disable this if you are certain about what you are doing. Otherwise, leave it on.
  To disable it go to Start menu > Control Panel. Select System and Security > Security and Maintenance, and choose ‘Change Windows SmartScreen settings’ from on the left.
  Now click the radio button next to 'Don’t do anything (turn off Windows SmartScreen)’.

- **SmartScreen + Apps**
  Finally, disable the other SmartScreen filter in Settings > Privacy > General and slide the option that says 'Turn on SmartScreen Filter to check web content (URLs) that Windows Store apps use' also to Off.

4.4 Laboratory Setup

The laboratory to showcase the Hardened Windows OS will be implemented using following techniques:

- Virtual Machine
- Windows 10 Professional/Enterprise ISO image.
- WINDSEC – OS Hardening tool.

Now let us look at the steps to setup the laboratory for using the WINDSEC tool:

Step 1: Download VMware and install it on your host machine.

https://www.vmware.com/go/getworkstation-win

Step 2: Download Windows 10 ISO image from official Microsoft website.

Step 3: Now, we need to import the ISO in the VMware to install Windows 10 Professional.

Recommended settings are mentioned in the below screenshots.

Fig 6: VMware Configurations

Step 4: After all this the WINDSEC should be downloaded onto the Windows 10 VM from the GitHub Repository: https://github.com/hardhax10/WindSec

You can find a file named WINDSEC.EXE

Step 5: Now, the Windows OS Hardening can be done using the tool.

4.5 Tools & Technology Used

WINDSEC is developed using Python 3.10 Programming Language.

Python

Python is an interpreted, object-oriented, high-level programming language with dynamic semantics. Its high-level built-in data structures, combined with dynamic typing and dynamic binding, make it very attractive for Rapid Application Development, as well as for use as a scripting or glue language to connect existing components together. Python's simple, easy to learn syntax emphasizes readability and therefore reduces the cost of program maintenance. Python supports modules and packages, which encourages program modularity and code reuse.

The Python interpreter and the extensive standard library are available in source or binary form without charge for all major platforms, and can be freely distributed.

Platform Module

The Platform module is used to retrieve as much possible information about the platform on which the program is being currently executed. Now by platform info, it means information about the device, it's OS, node, OS version, Python version, etc. This module plays a crucial role when you want to check whether your program is compatible with the python version installed on a particular system or whether the hardware specifications meet the requirements of your program.

OS Module

The OS module in Python provides functions for interacting with the operating system. OS comes under Python's standard utility modules. This module provides a portable way of using operating system-dependent functionality. The *os* and *os.path* modules include many functions to interact with the file system.

String Module

Python string module contains a single utility function - capwords(s, sep=None). This function split the specified string into words using str.split(). Then it capitalizes each word using str.capitalize() function. Finally, it joins the capitalized words using str.join(). If the optional argument sep is not provided or None, then leading and trailing whitespaces are removed and words are separated with single whitespace. If it's provided then the separator is used to split and join the words.

5.0 Summary of Results and Future Scope

5.1 Advantages/Unique Features

Let's discuss some of the advantages of this particular tool's implementation which is OS Security Hardening:

Improved System Security

When you do the System Hardening process on your IT infrastructure, you are minimizing the scope of data breaches, unauthorized access, malware attack, etc.

Improved System Efficiency

The system updates, security patches, and disabling of the unwanted processes are a part of system hardening and it helps in improving the efficiency of Information Technology.

Regulatory Compliance

Most of the industries and governments across the globe understand the disastrous consequences of the cyberattack. Hence, organizations now need to comply with the rules and regulations. The rules and regulations are based on the information security and data protection best practices.

Cost Savings in the Long Run

By improving the security of your infrastructure, you are reducing the events that can jeopardize your organization's security. This in terms, will help you save money that either would have been spent on disaster recovery in case of a security breach.

How Can I Harden My System?

As we said before, system hardening differs based on the needs of an organization. Hardening your system usually depends on the configuration of your server, its operating system, software applications, server hardware, etc.

We are done with advantages of hardening, now let's discuss advantages of Privacy:

“The idea of privacy is not to keep everything private, but to set boundaries defining those with whom we want to share and those we don’t,” says K. Sudhir, professor of marketing at Yale SOM. “Every day we evaluate what we might say to friends, co-workers, and so on, depending on how much trust they’ve earned.”

With this notion in mind, Sudhir and T. Tony Ke, at the Chinese University of Hong Kong, analysed the European Union’s General Data Protection Regulation (GDPR), widely considered the regulatory gold standard of personal data protection. The GDPR is centred on three basic principles. Namely, consumer have,

- The right to explicit consent by opting into data collection;
- The right to be forgotten: data should be erased upon consumer request, and;
- The right to data portability: data should be transferred to competitors upon request.

GDPR also sets guidelines around how companies must store and protect consumer data.

Since the GDPR went into effect in May of 2022, much ink has been spilled decrying its harmful effects on the data economy. Sudhir and Ke, wading into the issue, modeled the interactions between firms and consumers to capture a clearer picture of what, in fact, the implications are. Does the GDPR throttle data sharing and, in that way, diminish value for both firms and consumers? Do only consumers gain from data protections, or might firms also derive benefits?

The model looks, broadly, at the ways in which firms are incentivized to earn trust: if they invest in better data security measures and are transparent about the ways in which they use data, for instance, then consumers will more likely trust them and be willing to share data. Consumers, on the other hand, when deciding whether to share personal data, must balance the value of customized services against the potential costs of privacy breaches and price discrimination.

Consumers may worry about how technologies will evolve, how partnerships will evolve, and because of that may be concerned about sharing data in certain sectors.”

Sudhir and Ke find that, for the most part, the GDPR benefits both consumers and firms. Though opt-in alone can detract from the quantity of data shared, when this is bundled with stronger security measures people seem to be more willing to share their data. “Consumers may worry about how technologies will evolve, how partnerships will evolve, and because of that may be concerned about sharing data in certain sectors,” Sudhir says. “But because the GDPR provides this right to withdraw, protecting personal data forever into the future, and because it encourages greater data security within firms, consumers are more confident and more likely to give their data today. That allows the data economy to grow.”

There are exceptions to this finding, of course, which this work reveals by modelling variations in the cost of data breaches. People, for example, may not be terribly concerned if data about their news reading habits were stolen; they would be more concerned if shopping habits and credit card information were stolen; they might be deeply concerned if their biometric data were stolen.

In these cases of extremely sensitive data—fingerprints, healthcare, and so on—the cost of a privacy breach may be so high that consumers are unwilling to share data no matter what. Here, too, the GDPR proves valuable: rather than forego a transaction entirely because of concerns about data breaches, consumers can unbundle their data from the exchange; the goods economy can keep going in sensitive sectors even when no data is shared.

“The challenge with a law like this—and it’s big—is that one needs to think about a way to make it somehow generally applicable and yet flexible enough for consumers and firms to both get value out of it,” Sudhir says. The GDPR seems to do this well. “The regulations set in place are able to offer protections not only for today, but for the future, which allows society, firms, and consumers to take advantage of the full benefits of the data-driven economy while keeping the core principles of privacy alive.”

5.2 Future Scope of Work

In future, there are many needs of upgradation to the Security features. Every day there is a new threat evolving around the security of an endpoint. These endpoints have to be secured at any cost, to make it happen it is important to keep upgrading our security measures.

Hence, the WINDSEC tool will also evolve with a newer features and securities to implement in the windows OS.

Apart from these upgrades and the feature upgrades, there will be another aspect in which the WINDSEC will be updating itself that is providing all these functionalities for other major OS’s available in the market. That includes Linux OS Hardening as well as the IOS/MAC OS Hardening.

Even though the scripts meet their purpose for the most part, they do not include all functionality that was planned. Also, a lot more exception and error handling should be included, as well as more testing of the different configuration templates. Planned features

that were not yet included are an automatic checking option for installed automation features, ability to include multiple different roles in a host computer, and creating a user

specified feature list. Also, functions for the registry type parameters did not get finished

in time, even though some registry hardening settings were included in the security template. These functions can be created with Set-ItemProperty and Get-ItemProperty commands, which are found in the Microsoft.PowerShell.Management PowerShell module.

With the included functions for registry parameters, it should be figured out what security

policy settings in the hardening template could be replaced with registry settings. This

way the need for Secedit could be decreased or removed altogether. Including the Windows Settings menu items in the hardening configuration could also be very useful, because currently these settings must be configured and audited manually, and the Windows updates sometimes change these settings. Additionally, more settings from the Windows security baselines should be added into the hardening configuration baseline. However, including new parameters into

hardening needs comprehensive testing before they can be applied into the production environment. The method used in the scripts to allow setting exceptions for each feature, could be used for configuring application whitelisting or firewall exceptions. This would allow automated configuration of application whitelist or firewall exceptions for installed applications. Tools like Windows AppLocker and Firewall are included in Windows operating systems, and already include management commands in PowerShell. Remote hardening features can be quite easily added to the PowerShell scripts. For example, the way that the script uses a list of IP addresses of available host devices in an accessed network segment to harden or audit all of those. This needs Windows Remote Management to be turned on, and might cause misconfigurations that are hard to notice. If this kind of a function is needed, the PowerShell DSC should be reviewed first, because it functions very similarly. Two methods for securing the scripts against unwanted changes were considered in this thesis. The scripts could be digitally signed. This means that if the scripts are changed and the PowerShell script execution policy set as AllSigned, PowerShell should not allow execution of the scripts. However, this seemed to be very easily bypassed. Another idea was to convert the scripts to executives, though hardening and auditing could also be made, for example in C#, with the use of the PowerShell class, if PowerShell tools are required.

6.0 Conclusions

In this thesis, the goal was to study how hardening should be managed over the ICS lifecycle, and how to deal with the problems met in maintaining the OS hardening configuration, especially in the Windows environment. To make the hardening management possible, automated hardening and auditing scripts were implemented with Windows PowerShell. Additionally, some hardening configuration improvements were researched to better meet the demands of newer Windows operating systems. The review showed that hardening is underrated in many security guides. This might be because it does not add fancy new security software or features, but vice versa. Although hardening is usually used as a security feature in ICSs, a more systematic hardening approach can improve security, reduce unnecessary network traffic, and free computer resources. The need for hardening management also increases with the use of more modern operating systems. To make hardening management possible in build and operation phases, two new scripts are developed in this thesis. One for hardening the system and other for auditing it. The scripts are implemented with Windows PowerShell to review its capabilities for hardening and auditing of the Windows environment. Windows PowerShell is feasible for local hardening and auditing script implementation, but with some difficulties. While PowerShell operates well, it seems a bit unfinished when considering the tools available. Tools, such as local user and group management commands, appeared only in PowerShell 5.1 during this thesis, and were not used in the scripts. Managing of network and service settings needed multiple different methods, and some settings needed to be configured with old command line tools. In addition, there were tools that executed unwanted configuration restoring when used. However, if Microsoft keeps pushing PowerShell in the right way, it can be a very powerful tool to implement hardening and auditing to ICS devices. Even if PowerShell is not directly used, it can be implemented, for example, into C# program with PowerShell class. Additionally, remote functions for hardening and auditing scripts can be easily added with PowerShell to harden or audit multiple devices at once. Though, if remoting is needed, PowerShell DSC should be reviewed. When considering the use of Windows operating systems in ICSs, it was clear that new Windows versions have more features and automatic functions that can be harmful in ICS. This leads to the conclusion that hardening is even more important in new Windows systems. However, using a modified Windows 10 IOT Enterprise version can make it a little easier. When it comes to Windows updates, the long-term servicing channel should be used in Windows 10 to reduce feature updates. Overall Windows 10 caused a lot of problems in the target environment. Its automated functions and updates restored security features that conflicted with the control system. Disabling those was difficult, because the features enabled themselves sometime after disabling. This kind of functioning can be justified to keep an unskilled user from harming their security, but is not acceptable in an ICS. This means that when using later Windows operating systems in an ICS, the need for hardening increases. Also, the need of management features, such as well-designed configuration audition is necessary. When considering both operating systems used in this thesis, the Windows Server 2012 R2 is better suited for ICS use. This might be because it is a server version or because problematic features are included in Windows 10, which can raise some concern about Windows Server 2016.

References

[1.] CERN, Computer Management Framework, version 2022. Available from https://cmf.web.cern.ch/cmf/Help/?kbid=001001 [accessed 2022-02-14]

[2.] Microsoft, System Center Configuration Manager, version 2012 R2 SP1, 2012.Available from https://www.microsoft.com/en-us/cloud-platform/system-center-configuration-manager [accessed 2022-03-01]

[3.] Microsoft, Security features comparison: Windows 7 vs Windows 10, 2022. Available from http://download.microsoft.com/documents/uk/enterprise/windows10/win10-win7-security-comparison.pdf [accessed 2022-03-05]

[4] Microsoft, Windows 10 security features, 2017. Available from https://docs.microsoft.com/en-us/windows/security/threat-protection/overview-of-threat-mitigations-in-windows-10 [accessed 2022-03-15]

[5.] Microsoft, AppLocker, version Windows 10, 2017. Available from https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview [accessed 2022-03-18]

[6.] SANS ISC, Blocking PowerShell connections via Windows Firewall, 2016. Available from https://isc.sans.edu/forums/diary/Blocking+Powershell+Connection+via+Windows+Firewall/21829 [accessed 2022-04-06]

[7.] Microsoft, BitLocker, version Windows 10, 2017. Available from https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview [accessed 2022-04-12]

[8.]Tracker Software X-CHANGE Editor, 2017. https://www.tracker-software.com/product/pdf-xchange-editor [accessed 2022-04-29]

[9.] CVE Details X-Change vulnerability statistics https://www.cvedetails.com/product/23116/Tracker-software-Pdf-xchange.html?vendor_id=12248 [accessed 2022-05-07]

[10.] CVE Details,Adobe Reader vulnerability statistics https://www.cvedetails.com/product/497/Adobe-Acrobat-Reader.html?vendor_id=53 [accessed 2022-05-24]

[11.] Adobe Communications, Flash Update, 2017. https://theblog.adobe.com/adobe-flash-update/ [accessed 2022-06-20]

[12.] Eyeo GmbH, Adblock Plus, 2022. Available from https://github.com/adblockplus [accessed 2022-06-24]

[13.] MalwareBytes, Malwarebytes Endpoint Security, 2022. Available from https://www.malwarebytes.com/business/endpointsecurity/ [accessed 2022-07-12]

[14.] Microsoft, Local Administration Password Solution, version 6.2, 2022. Available from https://technet.microsoft.com/en-us/mt227395.aspx [accessed 2022-06-18]

[15.] BloodHound AD, BloodHound , version 2.0.4, 2022 Available from https://github.com/BloodHoundAD/BloodHound [accessed 2022-03-04]

[16] Microsoft, PowerShell Constrained Language, 2022. Available from https://blogs.msdn.microsoft.com/powershell/2017/11/02/powershell-constrained-language-mode/ [accessed 2022-02-26]

[17.] GRR, GRR Rapid Response, 2022. Available from https://github.com/google/grr [accessed 2022-07-21]

[18.] Microsoft, Windows Defender Application Guard, 2022. Available from https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/wd-app-guard-overview [accessed 2022-08-01]