

RESEARCH ARTICLE

Cyber Kill Chain Framework Approach to Map Potential Attack Vectors on Windows-based OS

Amanda Fairuz Syifa* and Muhammad Salman

Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, Indonesia

*Corresponding author. Email: amanda.fairuz42@ui.ac.id

Abstract

The widespread adoption of Windows 11 necessitates a comprehensive evaluation of its security vulnerabilities, particularly in light of increasingly sophisticated cyberattacks. This study exclusively focuses on Windows 11 Home and Enterprise editions, applying the Cyber Kill Chain framework to map potential attack vectors. The analysis reveals significant weaknesses in SMB and RDP protocols, with Windows 11 Enterprise proving more vulnerable to specific threats such as SMB Relay Attacks. Adversary emulation using the Caldera platform successfully simulated real-world cyber threats, highlighting critical security issues, including the extraction of sensitive information and privilege escalation risks through PowerShell. The emulation demonstrated that commands could identify user accounts and shared directories, exposing potential avenues for unauthorized access. Recommended countermeasures include enabling SMB signing, enforcing strong password policies, disabling unused RDP services, and deploying active antivirus solutions. This research provides key insights into enhancing the security posture of Windows 11 against modern cyber threats, emphasizing the importance of proactive security measures and continuous vulnerability assessments.

Keywords: Windows 11 Security Evaluation, Adversary Emulation, SMB, and RDP Vulnerabilities, Privilege Escalation Risks, and Windows Cybersecurity Mitigation Strategies

1. Introduction

In today's interconnected world, securing operating systems is critical as both individuals and organizations rely heavily on technology. Released in October 2021, Windows 11 has quickly gained widespread adoption, drawing increased attention from malicious actors seeking to exploit its vulnerabilities. This paper explores the security challenges and vulnerabilities of Windows 11, analyzing potential risks through ad-

vanced security evaluation frameworks. It also offers mitigation strategies to strengthen the system's defenses against modern cyber threats.

2. Security Features in Windows 11

Windows 11, launched on October 5, 2021, is Microsoft's latest operating system, requiring specific hardware, including a 64-bit architecture, a 1 GHz processor with two or more cores, 4 GB of RAM, DirectX 12-compatible graphics, and 20 GB of HDD space [1]. Certain features also require a secure boot and an internet connection with a Microsoft account. Windows 11 prioritizes foreground applications, improves performance on lower-end devices, and offers a modern interface to enhance productivity.

For security, Windows 11 includes Virtualization-Based Security (VBS), secure boot, and BitLocker encryption[2], [3], [4]. VBS isolates memory for critical services, while secure boot ensures only trusted software loads during startup. BitLocker encrypts data to prevent unauthorized access. Windows 11 also mandates TPM 2.0 for hardware-based security, supports newer processors, and employs Hypervisor-Protected Code Integrity (HVCI) to ensure kernel security. The system integrates application isolation, a zero-trust security model, and ongoing updates to address emerging threats.

3. Related Works

The field of information security is continuously evolving, presenting new challenges as technology advances. Threat actors exploit malicious techniques to compromise critical data and systems within networks[5]. IBM's research indicates a significant rise in cyberattacks between 2020 and 2021, largely driven by vulnerability exploitation[6]. Since its release in October 2021, Windows 11 has seen rapid adoption, with over 400 million active users in its first year and projected to reach half a billion by early 2024[7]. Despite enhanced security measures, the Windows family—from versions 7 to 10—has a history of vulnerabilities frequently targeted by attackers[8], [9], [10], [11].

Previous research into Windows systems revealed ongoing security challenges. A study of Windows 10 editions, using tools like Nmap, Nessus, and Metasploit, found various vulnerabilities, including critical SMB signing issues and batch file and PowerShell exploits. However, it lacked a detailed analysis of attack impacts and specific mitigation strategies for Windows 10 [12]. As Windows 11 gains attention, addressing its vulnerabilities remains crucial to counter rising threats. The frequency of sophisticated attacks, such as ransomware campaigns like WannaCry and Petya, underscores the need for comprehensive security assessments and tailored mitigation strategies for Windows 11[13]. Research in this area deepens understanding of risks and informs proactive measures to strengthen the resilience of Windows 11, protecting user data in today's complex threat landscape.

4. Experimental Setup and Analysis

This chapter details the experimental setup and analysis used to assess Windows 11's security against various attack scenarios. Using the Cyber Kill Chain Framework as the primary methodology, we identified and evaluated vulnerabilities, simulating real-world attacks to gain insights into the system's defense mechanisms and the effectiveness of its security measures.

4.1 Proposed Method

This study uses a black-box testing approach, simulating an external attacker's perspective without prior knowledge of the system's internal architecture. This method effectively replicates real-world attack scenarios, helping identify vulnerabilities that may not be revealed through other strategies. The Cyber Kill Chain framework, developed by Lockheed Martin, is applied to structure the testing process.

The Cyber Kill Chain is a widely recognized cybersecurity framework that outlines the seven stages of a cyberattack, from reconnaissance to actions on objectives [14], [15]. It enables security teams to understand and disrupt attack vectors at various stages, particularly against Advanced Persistent Threats (APTs). By analyzing each phase, defenders can intervene early, reducing the risk of a full-scale compromise[15]. This approach provides insights into attackers' tactics, techniques, and procedures (TTPs), improving incident response and enhancing overall system security. The process of attack will be shown in Figure 1.

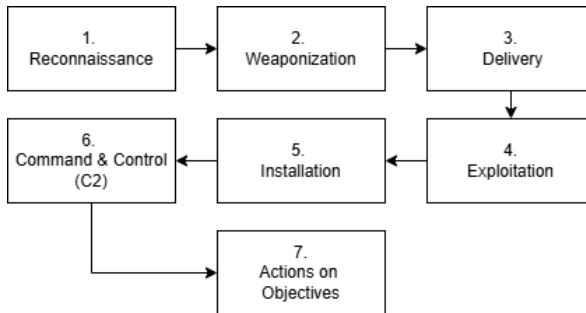


Figure 1. Cyber Kill Chain Steps

The Cyber Kill Chain consists of the following phases:

1. Reconnaissance: Identifying and gathering information about the target
2. Weaponization: Developing or customizing malicious payloads
3. Delivery: Transmitting the payload to the target system
4. Exploitation: Taking advantage of vulnerabilities to compromise the target
5. Installation: Deploying malware to maintain persistence
6. Command and Control (C2): Establishing communication for remote control
7. Actions on Objectives: Completing the attacker's goal, such as data exfiltration or system disruption.

To simulate adversary actions, we used MITRE CALDERA, an automated adversary emulation platform. CALDERA integrates with the MITRE ATT&CK framework, allowing for structured simulations that reflect real-world techniques used by threat actors. The adversary emulation was conducted on a Windows 11 environment, simulating multiple phases of the kill chain.

4.2 Lab Setup and Analysis

The research was conducted on an Infinix Inbook X2 laptop running Windows 11 Home Single Language. The specific hardware details are outlined in Table 1.

Table 1. Specifics of the workstation

Component	Specifications
CPU	Intel® Core™ i7-1065G7 CPU @1.30GHz 1.50 GHz
RAM	8,00 GB
Storage Memory	SSD 512GB M.2 NVMe PCIe
System Type	64-bit operating system, x64-based processor

The research used VirtualBox 7.0 to create a virtual environment with controlled testing conditions and isolated network configurations. To maintain consistency, no third-party software, updates, or patches were installed during the setup. The attacker system, VM 1, ran Kali Linux 2023.4 for penetration testing. VM 2 used Nessus Essentials 10.6.3 to detect vulnerabilities. VMs 3 through 5, running Windows 11 Home and Enterprise versions 23H2, were designated as targets for security evaluation across different OS editions. VM 6 acted as the domain controller, managing network resources and enforcing security policies. The network configuration used a NAT network, enabling communication between all VMs while isolating them from the host system and external networks. This setup provided a secure environment for detailed security analysis. The Windows 11 Home network topology is shown in Figure 2, illustrating connections and communication flow during testing. The Windows 11 Enterprise topology is in Figure 3, highlighting the setup for evaluating security features. Both topologies maintain isolation while enabling comprehensive testing.

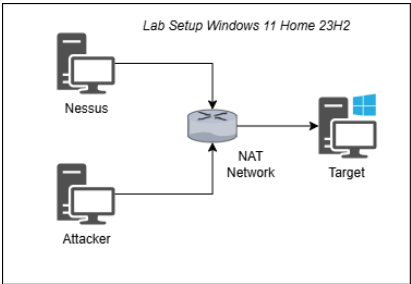


Figure 2. Network Topology for Windows 11 Home

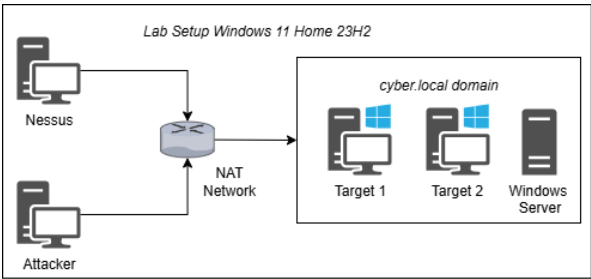


Figure 3. Network Topology for Windows 11 Enterprise

4.3 Tools

The tools and their functions are detailed in Table 2.

Table 2. Tools used in this research

No	Steps	Tools	Functions
1	Reconnaissance	Google Dorks	Passive data gathering, which collects publicly available information about the target.
		Nmap	Scan for host, service, and open port within the network.
2	Weaponization	Nmap	Scan for vulnerabilities based on their extensive vulnerability databases
		Nessus Essentials	Assesses SMB security, identifying weak configurations and credentials vulnerable to SMB relay attacks.
		Crackmapexec	Scores vulnerabilities by severity, aiding in prioritizing security threats.
		CVSS V3.0	
3	Delivery & Exploitation	Impacket	Employs for SMB relay attacks
		Responder	Capture NTLM Credentials for further attacks
4	Installation & Command and Control	John the Ripper	Password cracking
		Remmina	RDP Access
		Netcat	Create SMB Interactive Shell
		Metasploit	Install backdoors
5	Actions on Objectives	Metasploit	Erase Windows event logs and masking the attacker's activities effectively and compromising data on the victim.

4.4 Reconnaissance

In the Reconnaissance phase, Google Dorks revealed critical vulnerabilities in Windows 11, including an information disclosure flaw in the Windows kernel and multiple privilege escalation risks (e.g., kernel-level elevation, backup service, and improper permission assignments). These could allow attackers to gain elevated access to the system. Additionally, a DLL hijacking vulnerability in 'apsds.dll' was found, allowing attackers to execute malicious code. Remote code execution vulnerabilities, stemming from CWE-434 and point-to-point protocol issues, were also identified, enabling remote arbitrary code execution.

Further authentication issues, such as missing authentication for critical functions and hard-coded credentials, were uncovered, posing risks of unauthorized access. These findings highlight key security risks in Windows 11 that must be addressed. During network mapping with Nmap, the study identified key systems: IP address 192.168.100.9 (Windows Enterprise, User 1), IP 192.168.100.13 (Windows Enterprise, User 2), and IP 192.168.100.15 (Windows Home). This provided insights into network layout and vulnerabilities, informing further security evaluation.

4.5 Weaponization

During the Weaponization phase, various tools were used to assess the network's security:

4.5.1 Nessus

Detected a medium-severity vulnerability, "SMB Signing Not Required," and provided 37 informational findings related to system configurations and security hardening (Figure 4).

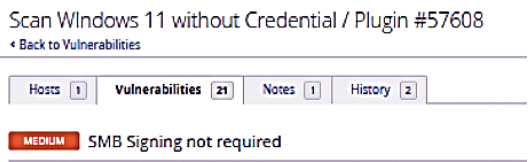


Figure 4. Nessus Result

4.5.2 Nmap

Identified an open port (445/tcp) running Microsoft-DS, suggesting potential risks related to file-sharing services on Windows systems (Figure 5).

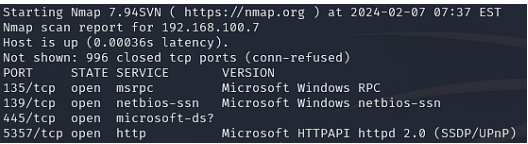


Figure 5. Nmap Result


```

(kali@kali)-[~]
$ impacket-ntlmrelayx -tf targets.txt -smb2support -i
Impacket v0.12.0.dev1+20240308.164415.4a62f391 - Copyright 2023 Fortra

[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

```

Figure 8. Impacket Simulation

4.7 Installation and Command & Control

During the Installation phase, the attacker cracked the previously captured password hashes using a tool called John the Ripper, which uses a dictionary of common passwords to guess the correct one. This demonstrates how weak or reused passwords can be a major security risk. Once the passwords were cracked, the attacker gained unauthorized access to the system. This shows how one small weakness—like a poorly chosen password—can lead to a full system compromise. (Figure 9).

```

Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, al
P@$$w0rd (USER-2)
1g 0:00:00:00 DONE (2024-05-19 01

```

Figure 9. John the Ripper Crack the Password

In the Command and Control (C2) phase, the attacker established remote access using two tools:

4.7.1 Remmina

A remote desktop application, was used to connect to the victim's machine using the cracked credentials. It successfully connected to the Windows 11 Enterprise system, but failed on the Home edition, which had stronger default protections (Figure 10).

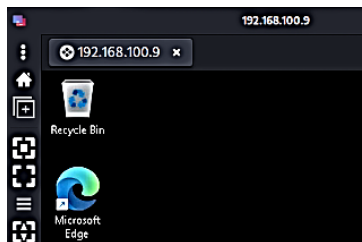
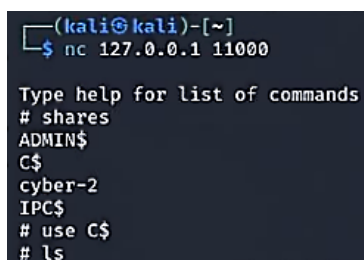


Figure 10. Successful Access the Target via Remmina

4.7.2 Netcat

A network utility that can create command-line shells, was used to simulate an interactive session between the attacker and the victim's system. While the Home version blocked this attempt, the Enterprise system allowed it, exposing a major vulnerability. These tools allowed the attacker to take control of the machine and continue further actions without detection. The result of the netcat is shown in Figure 11.



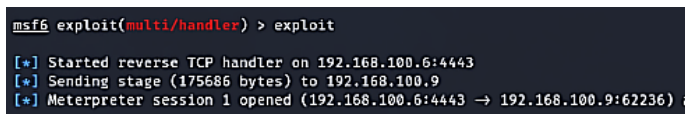
```
(kali㉿kali)-[~]
$ nc 127.0.0.1 11000
Type help for list of commands
# shares
ADMIN$
C$
cyber-2
IPC$
# use C$
# ls
```

Figure 11. Netcat Build the SMB Interactive Shell

The key takeaway is strong password policies and endpoint security configurations are critical to prevent unauthorized remote access. Security teams should disable remote desktop access for unnecessary users, implement multi-factor authentication (MFA), and continuously monitor for suspicious login attempts and shell activities.

4.7.3 Metasploit

A payload was deployed using Metasploit, creating persistent remote access on Windows 11 Enterprise systems via a Meterpreter session, ensuring ongoing control (Figure 12).



```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.100.6:4443
[*] Sending stage (175686 bytes) to 192.168.100.9
[*] Meterpreter session 1 opened (192.168.100.6:4443 -> 192.168.100.9:62236) a
```

Figure 12. Backdoor Successful Installed

4.8 Actions on Objectives

In this phase, the attacker used their access to manipulate system data and erase traces of the attack. Once inside the system, unauthorized changes were made, and Windows event logs were cleared using Metasploit's 'clearev' command. This removed evidence of the attacker's activity and helped maintain long-term stealth (Figure 13). Such actions simulate real-world scenarios where attackers clean up logs to avoid detection by security teams and forensic investigators.

```
meterpreter > clearev
[*] Wiping 2146 records from Application ...
[*] Wiping 7068 records from System ...
[*] Wiping 27323 records from Security ...
meterpreter > 
```

Figure 13. Clear Logs using Metasploit

Key takeaway is organizations must implement centralized logging and use log forwarding to external SIEM (Security Information and Event Management) systems to preserve audit trails. Security teams should deploy tools that detect log tampering, monitor endpoint behavior for anomalies, and ensure critical events are stored in write-once, read-many (WORM) formats.

5. Research Results and Discussion

This chapter presents the results of a penetration test on Windows 11 systems using the Cyber Kill Chain framework, aimed at evaluating their security. The test involved disabling the firewall and antivirus to expose vulnerabilities and followed a structured process, which included reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. The study focused on Windows 11 Enterprise and Home editions to assess their resilience against different attack techniques.

5.1 Results of Penetration Testing using Cyber Kill Chain

The security evaluation of Windows 11 Home and Enterprise systems revealed significant vulnerabilities, particularly in SMB and RDP protocols, which were systematically exploited following the Cyber Kill Chain framework. In the Reconnaissance phase, Google Dorks exposed critical flaws, including kernel-level privilege escalation and DLL hijacking vulnerabilities, alongside remote code execution risks. Nmap scans further identified key systems, laying the groundwork for potential attacks. The Weaponization phase uncovered SMB Signing vulnerabilities through Nessus and Nmap, while Crackmapexec confirmed SMB Signing was disabled, presenting risks for file-sharing communications.

In the Delivery and Exploitation phases, LLMNR Poisoning and SMB Relay Attacks were executed successfully on Windows 11 Enterprise systems, while the Home edition proved more resistant. The attacker established remote access to Enterprise systems using John the Ripper and Remmina, exploiting cracked credentials, while Netcat enabled an interactive shell and Metasploit installed a backdoor for persistent control. Actions on Objectives involved manipulating data and erasing logs, demonstrating attackers' ability to maintain stealthy control over compromised Enterprise systems. These findings underscore serious vulnerabilities in Windows 11, particularly in the Enterprise edition. A detailed summary of the result is provided in Table 3.

Table 3. Result of the Experiment

No	Attack Scenario	Target	Result
1	LLMNR Poisoning with SMB	Windows 11 Home	Success (Hash successfully obtained and cracked)
2	LLMNR Poisoning with SMB	Windows 11 Enterprise	Success (Hash successfully obtained and cracked)
3	LLMNR Poisoning with WPAD	Windows 11 Home	Success (Hash successfully obtained and cracked)
4	LLMNR Poisoning with WPAD	Windows 11 Enterprise	Success (Hash successfully obtained and cracked)
5	SMB Relay Attack	Windows 11 Home	Failed to establish SMB Interactive Shell
6	SMB Relay Attack	Windows 11 Enterprise	Successfully established SMB Interactive Shell

5.2 Result of Remediation and Verification of Remediation

The remediation phase focused on addressing the vulnerabilities identified during the penetration testing of Windows 11. After executing various attack techniques, the vulnerabilities were documented and prioritized by severity and impact. This phase implemented security patches and protective measures to strengthen the system against future exploits and unauthorized access. The goal was to improve the security of the Windows 11 environment and ensure resilience against advanced cyber threats while protecting sensitive data and critical systems. A detailed summary of the remediation steps is provided in Table 4.

Verifying remediation ensures the applied security measures effectively address the vulnerabilities. This involves retesting each step against prior attack scenarios to confirm successful risk mitigation. A detailed overview is in Table 5.

5.3 Adversary Emulation Findings : Extracting Insights from Simulated Threats

Another study revealed that the use of Caldera, an open-source adversary emulation platform developed by MITRE, can effectively simulate real-world cyber threats and assess organizational defenses[16]. Caldera integrates the MITRE ATT&CK framework to replicate adversary tactics, techniques, and procedures (TTPs), providing a structured approach to identifying vulnerabilities, enhancing detection systems, and refining incident response strategies. The implementation involves a Windows 11 machine as the compromised system, a Windows Server 2022 domain controller, and an Ubuntu-based command and control (C2) server, creating a realistic testbed for adversary emulation.

Table 4. Suggestion of Remediations

No	Attack Scenario	Target	Remediation Steps
1	LLMNR Poisoning with SMB	Windows 11 Home	Change Password Complex
2	LLMNR Poisoning with SMB	Windows 11 Enterprise	Disable RDP and Change Complex Password
3	LLMNR Poisoning with WPAD	Windows 11 Home	Change Password Complex
4	LLMNR Poisoning with WPAD	Windows 11 Enterprise	Disable RDP and Change Complex Password
5	SMB Relay Attack	Windows 11 Home	N/A
6	SMB Relay Attack	Windows 11 Enterprise	Enable SMB Signing and Remove Local Administrator
7	Installing Backdoor	Windows 11	Enable antivirus

Table 5. Verification of Suggestion Remediations

No	Attack Scenario	Target	Verification of Remediation
1	LLMNR Poisoning with SMB	Windows 11 Home	Successful (Unable to retrieve original password from hash)
2	LLMNR Poisoning with SMB	Windows 11 Enterprise	Successful (Unable to retrieve original password from hash and RDP access to the machine blocked)
3	LLMNR Poisoning with WPAD	Windows 11 Home	Successful (Unable to retrieve original password from hash)
4	LLMNR Poisoning with WPAD	Windows 11 Enterprise	Successful (Unable to retrieve original password from hash and RDP access to the machine blocked)
5	SMB Relay Attack	Windows 11 Home	N/A
6	SMB Relay Attack	Windows 11 Enterprise	Successful (Failed to establish SMB Interactive Shell).
7	Installing Backdoor	Windows 11	Successful (Backdoor cannot be run on Windows)

The technical findings of this study highlight several key aspects of adversary emulation. The emulation succeeded in extracting sensitive information from the Windows 11 system. Commands such as `$env:username` and `Get-WmiObject -Class Win32_UserAccount` identified user accounts, including administrative and guest accounts, revealing details such as account types, domains, and security identifiers (SIDs) [16]. PowerShell scripts further identified processes running under administrative privileges, such as `cmd` and `powershell`, which could be leveraged for privilege escalation. The study also retrieved details of shared directories using `Get-SmbShare`, uncovering administrative shares like `ADMIN$` and `C$` and their configurations [16]. Additionally, the emulation analyzed the antivirus setup via the `wmic` command, extracting details about Windows Defender, including its GUID and executable paths. Domain controller information was also uncovered through `nltest /dsgetdc:$env:USERDOMAIN`, revealing the domain name, site name, and IP address, which is critical for understanding potential lateral movement opportunities.

5.4 Operational Insights and Industry-Relevant Implications

The significance of this study lies in its ability to replicate real-world cyberattack scenarios in a controlled environment, particularly through the emulation of advanced persistent threats (APTs) using the Caldera platform and MITRE ATT&CK framework. By simulating common attack vectors such as SMB relay and credential harvesting, organizations can critically assess how their systems respond under adversarial conditions. This adversary emulation approach offers not only theoretical insight but also actionable intelligence to improve operational resilience. It enables organizations to identify security gaps, validate detection mechanisms, and develop more effective response strategies against sophisticated threats [16].

From a practical standpoint, security teams can use the findings to evaluate whether SMB signing is enforced, monitor and limit RDP exposure via secure channels like VPNs or bastion hosts, and map internal defenses against the MITRE ATT&CK matrix to uncover coverage blind spots. These recommendations align with the best practices already adopted by industry leaders such as Microsoft and Google, including multi-factor authentication (MFA), network segmentation, and Endpoint Detection and Response (EDR) systems. By incorporating these measures, organizations can transition from a reactive to a proactive security posture, significantly reducing exposure to lateral movement and unauthorized access while reinforcing their overall cybersecurity readiness.

5.5 Long-Term Impact on Performance and Usability

While the countermeasures outlined above introduce additional layers of protection, they may also have minor implications for system performance and user experience. For example, enabling SMB signing can slightly delay file transfers due to the added verification process. Similarly, routing RDP traffic through a gateway may result in increased latency, especially in high-load environments. Nonetheless, these trade-offs are generally minimal and are outweighed by the substantial security benefits. Improved threat detection, stronger authentication, and reduced exposure to lateral

movement collectively enhance the resilience of the system, justifying any minor inconvenience introduced by the countermeasures.

6. Conclusion

This research evaluated the security of Windows 11 Home and Enterprise using the Cyber Kill Chain framework. Key vulnerabilities, such as SMB Signing Not Required, exposed both versions to attacks like LLMNR Poisoning, SMB Relay, and Backdoor Installation. These weaknesses allowed attackers to capture credentials, gain unauthorized system access, and install malware remotely. Windows 11 Enterprise showed greater susceptibility to SMB Relay Attacks and remote access via RDP compared to Home, due to differences in domain management. Effective mitigation measures included enabling SMB Signing, removing local Administrator accounts, disabling RDP, and activating antivirus software. These steps help strengthen the defenses of Windows 11 systems against various threats.

Adversary emulation with Caldera highlighted key security issues, such as extracting sensitive information from user accounts and identifying privilege escalation risks through PowerShell. It also exposed shared directories and antivirus configurations, underscoring the importance of emulation in detecting vulnerabilities and improving security.

References

- [1] Panos Panay. *Windows 11: A new era for the PC begins today*. [Accessed 1 March 2025]. 2021. URL: <https://blogs.windows.com/windowsexperience/2021/10/04/windows-11-a-new-era-for-the-pc-begins-today/>.
- [2] Surur Davids. *Microsoft explains the security benefits of Windows 11*. [Accessed 1 March 2025]. 2021. URL: <https://mspoweruser.com/microsoft-explains-the-security-benefits-of-windows-11/>.
- [3] Kyle Alspach. *Windows 11 Security: 10 Key Updates From Microsoft*. [Accessed 1 March 2025]. 2021. URL: <https://www.crn.com/slide-shows/applications-os/windows-11-security-10-key-updates-from-microsoft?page=11%5C&itc=refresh>.
- [4] David Weston. *New security features for Windows 11 will help protect hybrid work*. [Accessed 1 March 2025]. 2022. URL: <https://www.microsoft.com/en-us/security/blog/2022/04/05/new-security-features-for-windows-11-will-help-protect-hybrid-work/>.
- [5] P. Arora and A. Dhar. "CYBER ATTACKS: OPERATION AND PREVENTION". In: *International Journal of Engineering Applied Sciences and Technology* 1.12 (2016), pp. 93–96.
- [6] IBM. *X-Force Threat Intelligence Index 2022 Full Report*. [Accessed 1 March 2025]. 2022. URL: <https://www.securityhq.com/reports/ibm-x-force-threat-intelligence-index-2022/>.
- [7] Zac Bowden. *Exclusive: Windows 11 is active on almost half a billion devices, ahead of Microsoft's expectations*. [Accessed 1 March 2025]. 2025. URL: <https://www.windowscentral.com/software-apps/windows-11/exclusive-windows-11-is-active-on-almost-half-a-billion-devices-ahead-of-microsofts-expectations>.
- [8] Ö. Aslan and R. Samet. "Mitigating Cyber Security Attacks by being Aware of Vulnerabilities and Bugs". In: *International Conference on Cyberworlds*. 2017.
- [9] K. Dashora, D. S. Tomar, and J. Rana. "A Practical Approach for Evidence Gathering in Windows". In: *International Journal of Computer Applications* 5 (2010).
- [10] Windows Central. *Vulnerability Statistics*. [Accessed 1 March 2025]. 2025. URL: <https://www.windowscentral.com/software-apps/windows-11/exclusivewindows-11-is-active-on-almost-half-a-billion-devices-ahead-of-microsofts-expectations>.

- [11] CVE Details. *Vulnerability Statistics*. [Accessed 1 March 2025]. 2025. URL: https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-22318/Microsoft-Windows-8.html?page=1&order=1&trc=254&sha=6f5a3638e845b84d5353922e56e4723cb60ed07f.
- [12] J. Softic and Z. Vejzovic. "Windows 10 Operating System: Vulnerability Assessment and Exploitation". In: *2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH 2022) - Proceedings*. Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/INFOTEH53737.2022.9751274.
- [13] J. S. Aidan, H. K. Verma, and L. K. Awasthi. "Comprehensive Survey on Petya Ransomware Attack". In: *International Conference on Next Generation Computing and Information Systems (ICNGCIS)*. 2017.
- [14] Lockheed Martin. *Cyber Kill Chain*®. [Accessed 1 March 2025]. 2025. URL: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>.
- [15] S. J. Kim, S. K. Lee, and S. H. Lee. "Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures". In: *Journal of Information and Communication Convergence Engineering* 17.4 (Dec. 2019). [Accessed 1 March 2025], pp. 239–246. URL: <https://koreascience.kr/article/JAKO201925462478086.page>.
- [16] M. Gierblinski. *Introduction to Adversary Emulation with Caldera*. [Accessed 7 January 2025]. 2024. URL: <https://blog.curios-it.eu/2024/12/17/introduction-to-adversary-emulation-with-caldera/>.