IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURITY OF WINDOWS OPERATING SYSTEM- A REVIEW

[1,*]Aachal A. Godse, [2]Sakshi D. Sonone ,[3]Supriya S.Kesgire,[4]Mayuri M. Bapat
[1]Student, [2]Student, [3]Student, [4]Ass. Professor
[1]Department of Computer Science,
[1]MIT ACSC, Pune, India.

Abstract: With the increasing reliance on digital technologies, ensuring robust security measures for operating systems like Windows is paramount. This review paper explores practical ways to enhance security on Windows systems using simple language and accessible methods. By identifying common security risks and proposing straightforward solutions, users can better protect their digital assets. The study provides an overview of Windows security, outlines easy-to-implement security measures, and discusses their effectiveness in mitigating threats. By examining various aspects including user authentication, data encryption, network security, and malware protection, this paper aims to provide insights.

Index Terms **-Rootkit, privilege escalation, cryptojacking.**

I. INTRODUCTION

An operating system is an important component of the software system which handles the computer hardware and software resources and provides common functionality for computer programs.[1] The Windows operating system is a user-friendly interface, extensive software compatibility, enterprise integration capabilities, security features, customization options, hardware support, and developer-friendly platform.

Windows serves as a foundational element of modern computing environments, enabling individuals and organizations to access a vast array of applications, manage large-scale networks effectively, ensure data security and privacy, enhance productivity, and foster innovation.[1] Windows security is crucial for protecting personal and business data, maintaining operational continuity, preventing malware infections and cyber-attacks, ensuring compliance with regulations, maintaining trust and confidence among users, preventing data loss, and protecting intellectual property. Investing in robust Windows security measures is essential for safeguarding the integrity, confidentiality, and availability of computer systems and data.

II. VULNERABILITIES IN WINDOWS:

Common vulnerabilities in Windows OS can vary depending on factors such as the specific version of Windows, the configuration of the system, and the software installed. However, some vulnerabilities tend to be more prevalent across different versions. Here are some common vulnerabilities in Windows OS:

2.1 Remote Code Execution:

Vulnerabilities that allow remote code execution (RCE) enable attackers to execute arbitrary code on a Windows system remotely. These vulnerabilities can be exploited through malicious emails, websites, or network attacks, potentially leading to system compromise and data theft.[3]

2.2 Malware and Viruses:

Windows systems are often targeted by malware and viruses due to their widespread use. These can be delivered through email attachments, malicious websites, or compromised software. Securing Windows systems presents several challenges due to the complexity of the operating system, its widespread use, and the evolving nature of cyber threats. Here are some of the key challenges:

2.3 Privilege Escalation:

Securing Windows systems presents several challenges due to the complexity of the operating system, its widespread use, and the evolving nature of cyber threats. Here are some of the key challenges:

2.4 Misconfigured Security Settings:

Securing Windows systems presents several challenges due to the complexity of the operating system, its widespread use, and the evolving nature of cyber threats

2.5 Social Engineering Attacks:

Securing Windows systems presents several challenges due to the complexity of the operating system, its widespread use, and the evolving nature of cyber threats.

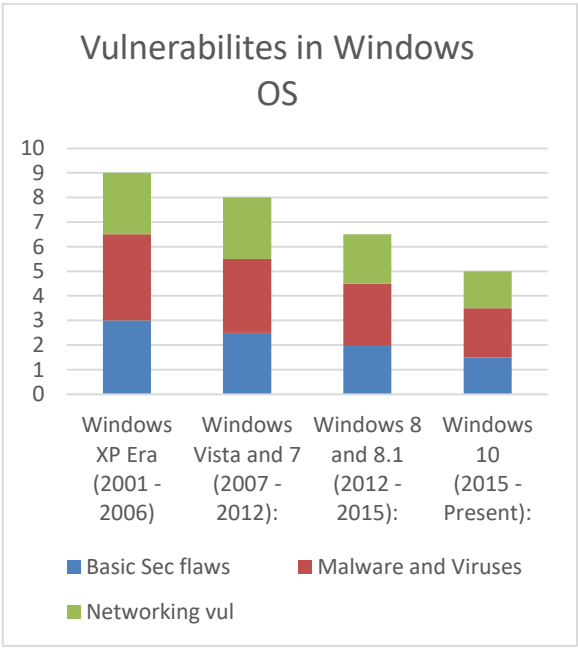

fig. vulnerabilities in os by years

III. CHALLENGES:

Securing Windows systems presents several challenges due to the complexity of the operating system, its widespread use, and the evolving nature of cyber threats. Here are some of the key challenges:

3.1 Malware and Ransomware:

This includes viruses, worms, Trojans, ransomware, and spyware designed to compromise the system, steal data, or disrupt operations. Malicious software that encrypts files on the system and demands payment for decryption, often causing significant disruption to businesses and individuals.

3.2 Phishing:

Cybercriminals use deceptive emails or websites to trick users into revealing sensitive information like login credentials or credit card details.[2]

3.3 Remote Access Trojans (RATs):

These allow attackers to remotely control the infected system, enabling theft of data, installation of additional malware, or surveillance.

3.4 Brute Force Attacks:

Attackers attempt to gain access to a system by guessing usernames and passwords repeatedly until they succeed.

3.5 Man-in-the-Middle (MitM) Attacks:

Intercepting communication between two parties to steal or alter data.

3.6 Cryptojacking:

Illegally using a victim's computing resources to mine cryptocurrencies without their knowledge.

3.7 Kernel Rootkits:

To take total control of a computer, an attacker must get access to the kernel of the operating system. A section of the kernel is replaced by these rootkits, allowing them to run as soon as the system starts up.[3]

3.8 Bootkits:

These are rootkits that have the basic capabilities of a rootkit as well as the power to attack the Master Boot Record. Individuals create bootkits so they can run from the system's master boot record and stay active during its use. [3]

To mitigate these threats, users should keep their Windows systems and software up to date with the latest security patches, use robust antivirus and antimalware solutions, employ strong and unique passwords, and practice safe browsing habits. Additionally, regular backups of important data are crucial to mitigate the impact of ransomware attacks.

IV. METHODS:

A number of security measures to protect Windows OS are covered in the literature which we cover in this section.

4.1 Authentication and user identification:

Users need to be confirmed and recognized. The system needs to know a user's identity in order to identify them. Authentication is the process of connecting a user's identity to the user.

4.2 Access Control:

Access control is the most crucial tool for computer system security. There are three steps to it. The first step is authorization, then access permission, and lastly imposing access permission.[4]

4.3 Least Privilege:

Grant users the minimal amount of access required to complete the position

4.4 Trusted Channel:

On the majority of computers, an unsecured middle application layer serves as the interface between the user and the operating system. The operating system must therefore make sure that a Trojan horse cannot steal data while it is being transmitted.

4.5 Virus protection:

It can be difficult to safeguard our computer system against viruses in the actual world. Generally, specific functions will be secured using a virus prevention technique.

4.6 Malware scanners:

Malware scanners are software tools that detect and remove malicious software from computers and networks. They come in various types, including antivirus, anti-spyware, anti-rootkit, behavioral analysis tools, online scanners, network intrusion detection systems, and endpoint detection and response solutions.

4.7 Firewalls:

A firewall is a security barrier that monitors and controls network traffic based on predefined rules. It prevents unauthorized access while allowing legitimate data to pass through, helping protect networks from cyber threats.

4.8 Anti-virus software:

Antivirus software is a type of security program designed to detect, prevent, and remove malware from computers and networks. It scans files and incoming/outgoing data for known malware signatures and suspicious behavior, helping to safeguard against viruses, trojans, worms, ransomware, and other malicious software threats.

V. WINDOWS SECURITY ARCHITECTURE:

The basic fundamental security blocks in the Windows operating system include[8]:

1.Security Reference Monitor (SRM)
2.Local Security Authority (LSA)
3.Security Account Manager (SAM)
4.Active Directory (AD)
5.WinLogon (local) and NetLogon (net)

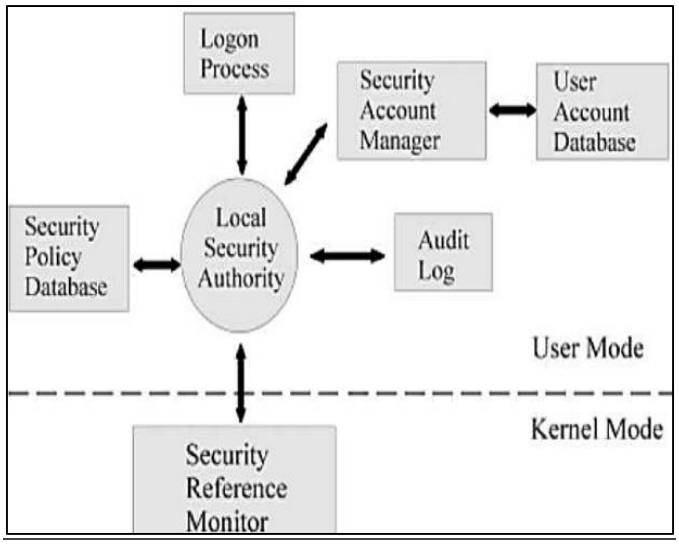

fig .windows sec architecture[7]

5.1 Security Reference Monitor (SRM):

It is a kernel-mode component that performs access checks. It generates audit log entries. Manipulates user privileges. Ultimately, every permission check is performed by the SRM.[6]

5.2 Local Security Authority (LSA):

Resides in a user-mode process named lsass.exe. It is responsible for enforcing local security policy in Windows. Security policy includes password policy, auditing policy, and privilege settings.[6]

5.3 Security Account Manager (SAM):

It is a database that stores user accounts and relevant security information about local users and local groups. When a user logs on locally, the SAM process verifies credentials against this database. Note that the SAM does not perform the logon, that is the job of the LSA. The SAM file is binary rather than text, and passwords are stored using the MD4 hash algorithm.[6]

5.4 Active Directory (AD):

It is Microsoft's LDAP directory service included in Windows Server, used for centralized management of user accounts, groups, and security policies. It facilitates authentication for domain-based logons across a network.[6]

5.5 WinLogon (local) and NetLogon (net):

WinLogon handles local logons at the keyboard. NetLogon handles logons across the network. Both authenticate users against their respective databases (SAM for local, AD for domain) and grant access upon successful verification.[6]

VI. CONCLUSION:

In conclusion, this comprehensive review of Windows security challenges highlights the importance of implementing robust security measures to protect personal and business data. The review identifies common vulnerabilities in Windows OS, such as remote code execution and malware, and discusses the challenges of securing Windows systems. It also provides insights into various security methods, including authentication, access control, virus protection, and firewalls. Additionally, the review explains the fundamental security blocks in the Windows operating system, such as the Security Reference Monitor and the Local Security Authority. Overall, this review emphasizes the need for users to stay updated with security patches, use strong passwords, and practice safe browsing habits to mitigate threats and enhance Windows security.

VII. ACKNOWLWGMENT:

The authors of the review paper titled " Security of Windows Operating System " are Aachal Godse, Supriya Kesgire, Sakshi Sonone and Ass. Prof Mayuri M Bapat from the Department of Computer Science, MIT Arts, Commerce and Science College , Pune, India.

REFERENCES

[1] Rijah, Muhammed & Rajapaksha, Samantha. (2023). Security Issues and Challenges in Windows OS Level. 07. 19-25.

[2] F. Yile, 2016 "Research on the Security Problem in Windows 7 Operating System," Eighth International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), Macau China, 2016, pp. 568-571, doi: 10.1109/ICMTMA.2016.139.

[3] Ramasamy, Kiran & Thakur, Shubham & Baskaran, Vinoth Kumar. (2019). Security in Windows 10. 10.13140/RG.2.2.18410.75208

[4] Radu, Constantinescu & Zota, Razvan Daniel. (2007). Issues of Operating Systems Security

[5] 2014 IJIRT | Volume 1 Issue 5 | ISSN : 2349-6002 IJIRT 100350, INTERNATONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY 1167 ,“Operating Systems Security – A Review”.

[6] https://slideplayer.com/slide/10952922/

[7] https://shounaksaheb.files.wordpress.com/2013/01/1.png

[8] Bassil, Youssef. (2012). Windows And Linux Operating Systems From A Security Perspective. Journal of Global Research in Computer Science. 3.