International Journal of Computer Applications Technology and Research
Volume 7–Issue 02, 58-62, 2018, ISSN:-2319–8656

Endpoint Protection through Windows Operating System Hardening

Shruchi Mistry
M.E Student, GTU PG School,
Gandhinagar 382007, Gujarat,
India

Punit Lalwani
Project Scientist,
Bhaskaracharya Institute for Space Applications and Geo-Informatics,
Gandhinagar 382007, India

M. B. Potdar
Project Director,
Bhaskaracharya Institute for Space Applications and Geo-Informatics,
Gandhinagar 382007, India

Abstract: Nowadays Cybercrimes are rapidly increasing. Systems are always vulnerable to attack due to Security misconfiguration. Most of the systems are vulnerable at client side or endpoint. The intrusion into the system can be done via violating operating systems vulnerabilities. Windows operating system has its own security functionalities and configurations. Most users not setup the security configuration properly and because of that systems are vulnerable to attacks. Today very sophisticated attacks like Ransomware, malware, Remote Admin tools etc. can be exploit throughout the system, which is securely misconfigured.
Windows operating system hardening is the only solution against such threats to the system. System hardening is the technique through which users can generate a checklist according to the requirements. A ransomware like Wanncry and Petya infected almost windows system due to security misconfiguration. This project is focused on preparing the checklist for security configuration in Windows operating system as per versions and vulnerabilities related with those OS versions; also Securely Audit those systems periodical basis to maintain required security level. As result automated system audit report framework will be developed to maintain the security level of Windows based operating system.

Keywords: OS Hardening; Security Checklist; Vulnerability; Security Audit; Threats; Ransomware

1. INTRODUCTION

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.[1] 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.

2. BACKGROUND SURVEY

Today insider threats are at rise. Corporate, Governments sectors, Multinational firms data at risk not due to external attack but internal leakage.[2] Our approach is to identify maximum risk factors affect the overall security of information or assets of any corporate, public sector, MNC's or individuals. The main factor in the insider threat is the host or endpoint. Though almost all endpoints and hosts are secured by antivirus, anti-malware, data leakage prevention, anti-ransomware etc. and also the compliance followed to safeguard the endpoints. But in recent researches that is found that the endpoint operating systems and their different versions are vulnerable to attacks. As an example, recently the malware called Ransomware infected the windows based operating systems using operating systems vulnerable service. The vulnerability exploited in Wannacry, Bad Rabbit, petyaransomware was unknown by most of the antivirus, anti ransomware or anti malware systems. These Vulnerabilities are present in the versions of windows operating system since long but not consider into security and compliance.

Users always keep the desktop busy with various tasks. Users perform activities like installs, uninstalls, starting and stopping services, disable and unable configurations etc. into the system regularly and periodically. Some activities perform by the users and some activities performed by operating system vice a versa. Such activities by default performed by the system. Many modifications keep the system vulnerable to exploits and attacks. But if periodically and prioritize the risk of the operating system user can assure the better level of security to the overall system. To secure the system through periodical audit, and reducing risks as per priority called as system hardening.[3]

The security audit in windows operating system is essential, especially when the system is part of a corporate network. The main objective for Windows Operating System security audit is to assure protection of information assets and to dispense information to authorized parties. If the endpoints are periodically audited then the information can be protected from various latest cyber threats. Security audit of operating system procedures required creating checklist, logging and reporting of security incidents.

2.1 VTAE in Operating system context

VTAE stands for combination of Vulnerability of the Operating System, which can eventually become threat to system, which can be attacked by any of the attacker with exploits.

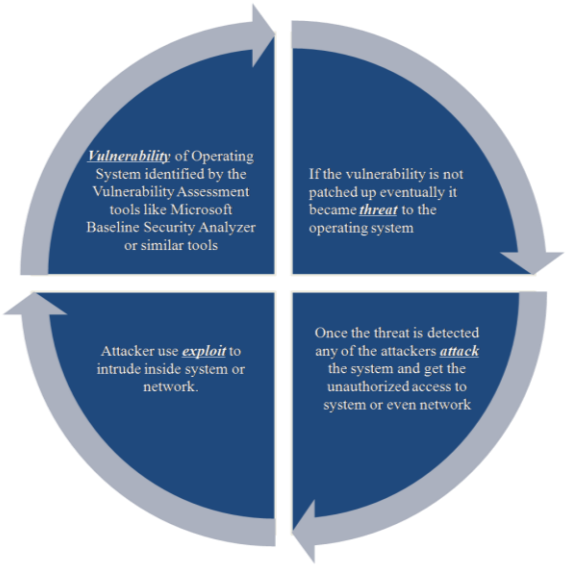

Figure. 1 VATE Model

Vulnerability: A weakness or loophole in any system or application or utility which gives an opportunity to the attacker to cause damage, unwanted performance issues or unauthorized access to the system or information. Eg. Buffer Overflow

Threat: A potential breach of security using known and unknown vulnerabilities of the system or applications is known as threat. It refers as anything that has the potential to cause serious harm to a computer system. Eg. Malicious Wares

Attack: A malicious activity through which security violation of the system can be done to gain unauthorized access or stealing the assets. Eg. Password Cracking

Exploit: A well defined script or automated one by one commands execution to gain advantage of a known or unknown vulnerability of the system or application. Eg. Eternal Blue

2.2 Assessment of Vulnerable System

Vulnerability Analysis is a periodical system audit process to identify potential loopholes.[4] With periodically system vulnerability audit overall security posture of the IT Infrastructure or network infrastructure can be enhanced. Systematic and periodic vulnerability assessment provides overall flaws exists into the system. It also gives holistic view of impact of each flaws exists into the system. To avoid false positives in vulnerability assessment manual assessment techniques can also be used.[5] After periodical analysis of vulnerability, patch management can be applied. And after the patch management and proper risk assessment system can be hardened against potential attacks.

2.3 Hardening Windows Operating System

As per figure 2, 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

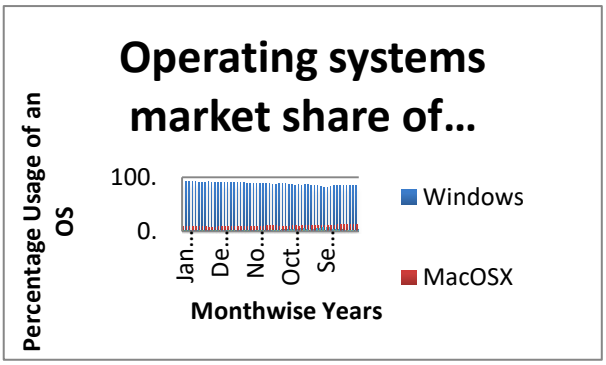

Figure. 2 Operating System Market share of desktop PCs from year 2013-2017

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.[6] 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 depends upon it's IT infrastructure and Network Infrastructure security. Firewall, Intrusion Detection Prevention System and Unified Threat Management solution can only provides perimeter security or network related operation level security. IT Infrastructure security is only depends upon security auditing of the endpoints and harden that endpoints with proper patches to reduce risks associated with known and unknown vulnerability exploits.[7]

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.

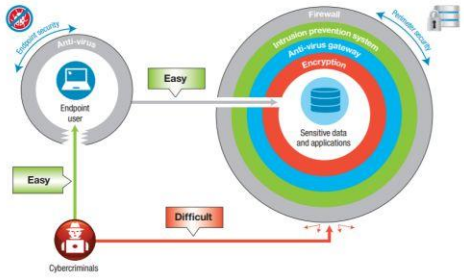

Figure. 3 Attack Scenario for Insider Threats

2.4 Benefits of OS Hardening

Cost reduction

By use of hardening, requirement of hardware and software running on the computer decreases. This would be resulted into cost reduction. Because of this, overhead of malware removal is also decreased.

Eliminates entry points

It also helps to lessen the number of probable and vulnerable entry points to the system on which attack can be possible. This is done by removing unused files and software and also stops unwanted services.[8]

Performance improvement

System hardening enhances overall performance of the system. It frees up disk space and memory, which were utilized by unwanted software and utilities. The system starts working very efficiently.[21]

Reduces security risks

More security benefits are added when the system hardening is performed. System hardening also eliminates the disabled files and programs which are no longer in used and omitted by users and are potential points of target by the attackers.

2.5 Techniques used for OS Hardening

Following techniques can be applied to harden the Windows operating 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.

3. PRIORITY WISE SECURITY TESTING PARAMETERS

In windows operating systems there are plenty of facilities provides as a part of user friendlyness of the operating system, but while talking about security User needs to prioritize the security testing of all the functionalities.[12] The priority could be divided into following three types,

3.1 High Priority: The security controls having excellent effectiveness against the exploits and vulnerabilities should be treated as high priorities for hardening Operating System. High priority risks if exploited will result in high cost of loss of assets, significantly harm organization operations or can even cause human death or serious injuries. E.g. Automation & SCADA Systems vulnerabilities, Stuxnet

3.2 Medium Priority: The security controls having very good effectiveness against adversary's attempt to exploit vulnerabilities, which result into loss of assets, impede organization's operation or can cause injury.[13]

3.3 Low Priority: The security control addresses risks that may result in loss of few assets or may affect organization's

operation but will not totally render the system ineffective. Operations may continue but are not at their optimum.

Table 1: Risk Priorities

Sr. No.	High Priority	Medium Priority	Low Priority
1	Application Versions & Patching	Account lockout policy	Displaying File Extensions
2	Application White listing	Audit Event Management	File & Folder Security Properties
3	Credentials Caching	Autoplay&Autorun	Location Awareness
4	Data Execution Prevention	BIOS & UEFI Passwords / Trusted Protection Module	Error Reporting
5	Elevating Privileges	Boot Device Encryption	Data Uploading &Downloading Policies
6	Local Administrator Accounts	USB & CD Drive Access	User Quotas (Disk Space)
7	Multi Factor Authentication	Executing privilege commands	Browser Helper Objects
8	Operating System Updates and Hotfix	Direct Memory Access / System Driver Installation	Task Manger Access
9	Service Pack fixes	File & Print Sharing	Flash Player
10	Password Policies	Host based intrusion prevention	Popup Blocker
11	Temporary / Guest Accounts	Registry editing tools	Hosts File
12	Overwrite Protection	Remote Assistant & Desktop Services	Debugger
13	Active Directory & Domain Control	Antivirus & Firewalls	Executing Portable programs
14	Network Port Scanning	System Backup & Restore	Date & Time Settings
15	Remote Management & Remote Shell Access	Group Policy Editor	Access to event manager

4. METHODOLOGY FOR CONDUCTING SECURITY HARDENING OF OS

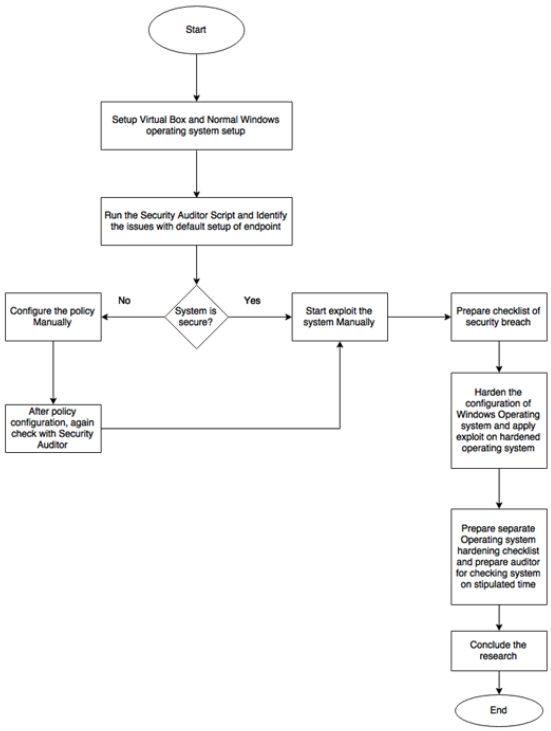

Figure. 4 Flowchart for conducting OS hardening

4.1 Techniques:

To enhance the security and compliance of Operating system manual and semi-automated audit and security configuration techniques can be used.[14,15]

4.1.1 Manual Technique:

Manual Technique is to audit manual security setting and prioritize to reduce risks. [16,17]

- Prepare the checklist of security parameters
- Review the security configuration parameters
- Setting the security configuration manually
- Exploit the operating systems as per configuration parameters

4.1.2 Semi Automated Technique:

- Semi-Automated Technique is to audit with using various script and utility [18]
- Prepare the checklist of security parameters
- Review the security configuration parameters with Auditor Utility and Semi automated scripts like .bat script and .ps script
- Prepare the script and setting up the security configuration [19]

Exploit the operating system with scripted payloads with exploit frameworks.

5. CONCLUSION

Till the time, this research is very important to the public and private sector to safeguard their information and data from being compromised because of Operating Systems Security misconfiguration. In this, the key vulnerabilities and exploits will be applied to learn the default security and patch management of the windows operating system. Accordingly the security will be enhanced up to the extent and again check in Security Audit Framework, and compare the results. After then the security checklist will be defined and maintained. Though there are very few literature and quality research paper is available in this domain, we can take it as opportunity to research and develop a better security enhanced harden Operating System.

Most of the security settings are changed with installed applications and software version up gradations. Windows updates can harden the OS at some extent. Very important aspect of OS security hardening is to prioritize risk and effectiveness of that risks to business or critical IT and Network Infrastructure. Periodical security audit can be reviewed and can be useful to patch up the vulnerabilities. Fuzzing can also be useful identifying unknown security misconfigurations and if patched at early stages security may enhance up to some extent. As an example, if early stage detection of security misconfiguration detected in periodical audit, user can safeguard IT or Network Infrastructure against sophisticated attacks like Ransomware attacks, unauthorized access, data theft, data modification or identity theft etc.

6. ACKNOWLEDGMENTS

We are thankful to Shri T. P. Singh, Director, BISAG for providing infrastructure and encouragement, and Special thanks to Abdul Zummarwala, Research Scholar, BISAG for permitting to carry out this project at BISAG.

REFERENCES

[1] Yile, Fan. "Research on the Security Problem in Windows 7 Operating System." Measuring Technology and Mechatronics Automation (ICMTMA), 2016 Eighth International Conference on. IEEE, 2016.

[2] Berghel, Hal. "A Quick Take on Windows Security Evolution." *Computer* 50.5 (2017): 120-124.

[3] Lin, Ma, Chen Houwu, and Liu Fuqiang. "The monitoring and auditing method of Windows File manipulations." Information Management, Innovation Management and Industrial Engineering (ICIII), 2012 International Conference on. Vol. 3. IEEE, 2012.

[4] Berlin, Konstantin, David Slater, and Joshua Saxe. "Malicious behavior detection using windows audit logs." Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security. ACM, 2015.

[5] Guo, Hui, et al. "Research on Detecting Windows Vulnerabilities Based on Security Patch Comparison." Instrumentation & Measurement, Computer, Communication and Control (IMCCC), 2016 Sixth International Conference on. IEEE, 2016.

[6] Shukla, Himanshu, et al. "Enhance OS security by restricting privileges of vulnerable application." Consumer Electronics (GCCE), 2013 IEEE 2nd Global Conference on. IEEE, 2013.

[7] Jing, Luo, Jiang Chunhua, and Yang Xia. "Design and implementation of security os based on trust zone." Electronic Measurement & Instruments (ICEMI), 2013 IEEE 11th International Conference on. Vol. 2. IEEE, 2013.

[8] Lin, Ma, Chen Houwu, and Liu Fuqiang. "The monitoring and auditing method of Windows File manipulations." Information Management, Innovation Management and Industrial Engineering (ICIII), 2012 International Conference on. Vol. 3. IEEE, 2012.

[9] Feifei, Liu. "The principle and prevention of windows buffer overflow." Computer Science & Education (ICCSE), 2012 7th International Conference on. IEEE, 2012.

[10] Berlin, Konstantin, David Slater, and Joshua Saxe. "Malicious behavior detection using windows audit logs." Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security. ACM, 2015.

[11] China National Vulnerability Database. Vulnerability trend graph .http://www.cnvd.org.cn/ flaw/ statistic, April 2016.

[12] SecurityTechCenter, Microsoft Security Bulletin MS15-034.https://technet.microsoft.com/ library/security/ms15-034, 2015.

[13] File detection test of malicious software.http://www.av-comparatives.org/wp-content/uploads/2015/04/avc_fdt_201503_en.pdf, August 2017.

[14] B. Anderson, D. Quist, J. Neil, C. Storlie, and T. Lane.Graph-based malware detection using dynamic analysis.Journal in Computer Virology, 7(4):247-258, 2011.

[15] K. D. Bowers, C. Hart, A. Juels, and N. Triandopoulos. Pillarbox: Combating next-generation malware with fast forward-secure logging. In Research in Attacks, Intrusions and Defenses, pages 46-67. Springer, 2014.

[16] M.Chandramohan, H. B. K. Tan, and L. K. Shar. Scalable malware clustering through coarse-grained behavior modeling. In Proceedings of the ACM SIGSOFT 20thInternational Symposium on the Foundations of Software Engineering, pages 27:1{27:4. ACM, 2012.

[17] J. Dai, R. Guha, and J. Lee. E_cient virus detection using dynamic instruction sequences. Journal of Computers, 4(5):405-414, 2009.

[18] M.Egele, T. Scholte, E. Kirda, and C. Kruegel. A survey on automated dynamic malware-analysis techniques and tools. ACM Computing Surveys, 44(2):6, 2012.

[19] W.Enck, P. Gilbert, S. Han, V. Tendulkar, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth. Taintdroid: An information tracking system for real time privacy monitoring on smartphones. ACM Transactions on Computer Systems, 32(2):5:1-5:29, June2014.

[20] T.-F. Yen, A. Oprea, K. Onarlioglu, T. Leetham, W. Robertson, A. Juels, and E. Kirda. Beehive: Large-scale log analysis for detecting suspicious activity in enterprise networks. In Proceedings of the 29th Annual Computer Security Applications Conference, pages 199-208. ACM, 2013.

[21] http://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference/, accessed on October 10, 2017.

[22] https://www.pcmag.com/encyclopedia/term/58124/os-hardening, Accessed on August 11, 2017.