International Journal of Multidisciplinary Innovation and Research Methodology (IJMIRM)
ISSN: 2960-2068, Volume 2, Issue 3, July-September, 2023, Available online at: https://ijmirm.com

Linux OS Versus Windows OS Security

Abdullah Suliman Alassaf

Cybersecurity and Networks Trainer, at HAFR Albatin Technical College, TVTC, Saudi Arabia

ABSTRACT

Security in computer systems is one of the essential factors that is considered by different users. Data and information security is critical to the users of computer systems because they need to maintain privacy and confidentiality. There are different researchers who have come up with evidence about the way these operating systems respond to various threats regarding how they protect the computer system. Some use ransomware, and other malware that is meant to give them access to systems so that they can get the information they need to launch attacks. Many companies have suffered the attacks and high levels of damage experienced. This essay will analyze the security features of the Windows OS and Linux OS' security, and develop insights on which operating system has the best security features. The study concludes that privacy is an essential factor that should be considered by the organizations. Attackers tend to search for information that they can use for their malicious purposes and that makes it necessary for the system security to be taken with a lot of seriousness.

Keywords: Security, data, information, confidentiality, ransomware, attacks, malware, privacy, attackers, malicious, operating system, Linux OS, Windows OS, Virtualization, defender, Bitlocker, Encryption, digital, Discretionary Access Control, Unix.

INTRODUCTION

Security in computer systems is one of the essential factors that is considered by different users. Data and information security is critical to the users of computer systems because they need to maintain privacy and confidentiality. There are debates about the importance of utilizing a highly secure operating system, a factor that has led to discussions about the operating system that offers the best security features. Linux, windows and Mac OS are the common operating systems that have been in operation over a long period. Arguments about the best in terms of security have been raised and there has been adequate information that has been developed through empirical research. There are different researchers who have come up with evidence about the way these operating systems respond to various threats regarding how they protect the computer system.

All of the operating systems have been developed with security features that protect users from any form of breaches or threats that may affect the way they operate. Enterprises spend a lot of resources to ensure their systems are secure and cannot be penetrated through attacks that may come from different malicious people. Computer systems are highly vulnerable because they are always targeted by attackers who have different intentions. Some of their actions are meant to benefit them financially and that affects the way they attack systems. Some use ransomware, and other malware that is meant to give them access to systems so that they can get the information they need to launch attacks. Many companies have suffered the attacks and high levels of damage experienced. Much as it is difficult to completely eliminate all forms of threats, having adequate measures in place is necessary in ensuring the systems are protected from attacks.

Security is a key factor in computer systems since most organizations have digitalized their data and they can easily be crippled by attacks that may arise. This essay will analyze the security features of the Windows OS and Linux OS' security, and develop insights on which operating system has the best security features.

Background

System threats that enterprises face keeps on changing over time as new technologies are developed. It is important for the organization to analyze different types of defenses that are supposed to be employed for the systems to be secured. Once an organization has taken a step to utilize a given operating system, it becomes difficult for it to shift to another one whenever there are challenges regarding the security features of such an operating system. For instance, an organization can be worked using Windows OS and a discovery is made that there are weaknesses that are exhibited by the OS. Changing to another OS may become challenging for such an organization for people and other systems are developed for the OS (Philip

& Raju, 2019). Whenever procurement and implementation of a given operating system is done, a lot of analysis needs to be done to ensure there are adequate security features that can satisfy the needs of an organization.

There are questions about the effect of the type of operating system that is utilized by an organization in their systems. The type of operating system that is deployed for the users can make a difference in the nature of security that such a system is likely to have in place. Attacks are most likely to arise from the users of a given system. Attackers today do not launch attacks directly on the systems because there are many security features that have been implemented in such systems (Vernotte et al., 2017). Enterprises should focus more on how they can implement highly secure operating systems because this is the point at which defense can be achieved in the system.

Windows and Linux operating systems have been developed to give users a satisfying experience where the security features of these systems have to be taken into account to ensure there is effectiveness in the manner in which data is secured. The companies have developed various operating systems that are meant for servers and this is one of the ways through which the strength of their security features can be tested. Deploying a secure operating system is necessary.

However, there is a need to have user education, strong firewalls, and consistent vigilance to ensure the systems are secured effectively. Even the most secure systems can be invaded and that can affect the nature of security that is needed for the systems to be free of threats. Organizations apply multiple strategies to ensure there is effectiveness in the way they secure their systems (Philip & Raju, 2019). Applying software updates regularly is an essential factor for the systems' security because threats keep on changing with advancements in technology.

Technical Specifications

With the rise in cybersecurity threats, there are different issues that need to be analyzed critically in order to come up with the most effective operating system for an organization. Understanding the type of operating system that is used is necessary because there are security features that need to be utilized for a given system to be highly effective. Without an analysis of such features, it may be difficult for a decision to be made on which operating system to be used.

WINDOWS OS SECURITY FEATURES

Vulnerabilities of the Windows OS

Windows have been developing different versions of operating systems. Security has been one of the major factors considered in each version with Windows 10 being considered to be having high security features that the other versions. Some of the features that have been developed in the operating system are essential in ensuring there is adequate security of the users' data. For instance, there is the windows defender smart screen. This is a feature that protects the users against websites that have been reported to contain phishing and malware. It helps in stopping the downloading of malicious files. This is an essential security feature that is developed in the windows operating system. Most attackers tend to use malware through sharing, links that will ensure they access the system easily if the users click on the links. The feature is one of the multiple layers of defense that the operating system provides. There is anti-phishing and malware protection for the users.

Windows Defender

The windows defender application guard is the other security feature in this operating system. Microsoft's Hyper-V virtualization technology is applied in protecting against advanced targeted threats which can affect the way the computer

systems work. Untrusted applications cannot be accessed by the computer and this is one of the ways through which the operating system protects the computer systems. It has been known to provide protection against the dangers that are posed by attacks that can access the system through applications (Sundar & Kumar, 2016). This is an important development in the computer systems that can be used to ensure there is effectiveness in the way security is implemented. It is one of the strengths that the OS has in place to ensure effectiveness is achieved in securing the systems.

Account Control

Windows OS also has the user account control (UAC) which is responsible for protecting the machine from damage that can be caused by malware. When this feature is enabled on a system, applications run in the security context where the users have to authorize different actions in the computer. The administrator is the only one who can conduct different activities on the computer to ensure there is high security in the manner in which activities are carried out in the system.

User control is essential in managing the type of activities that are conducted on the system. This makes it easy for the users to work effectively towards ensuring their systems are secure. The OS has this feature in place to create an enabling environment for the administrators to have control over the traffic of data in the systems.

The defender device guard is the other important feature in the Windows OS. It is a measure that involves the drivers and application whitelisting. The feature has a mode whereby the applications that are authorized by the enterprise are the ones that are run on the systems. Trusted applications are the ones that are used in delivering the best outcomes in the way they handle different issues within their networks. There is a total lockdown of the applications that cannot be trusted because this is where attackers can gain access to the systems. Integrity is key in computer security and this feature enables the machine to manage different applications. Whenever an app is not trusted, it cannot run on the system.

Windows Defender Exploit Guard

Windows defender exploits guard is another security feature that is developed for the Windows operating system. This is an important feature that was developed to ensure there is control of how folders are accessed. It protects the computer from any threats within the network. The security feature allows for auditing of the system to ensure there are adequate measures in place for the management of various issues that may arise in the network. Network security is essential in managing different attacks that may come through the network since they are the ones that can affect the way different issues are handled within the computer system.

Microsoft Bitlocker

Microsoft Bitlocker is a full drive encryption feature in Windows 10 which helps in enhancing file and system protection. It is an essential feature that aids the protection of data. Computer systems can be highly vulnerable at times whenever there are attackers who target critical information that is found in the computer systems. Encryption is one of the best means through which data can be protected from unauthorized parties who may want to access it. Windows Bitlocker is an important feature in the system that manages the way data is transferred (Meijer & Gastel, 2019). If the computer system is stolen or destroyed, data cannot be accessed unless it is decrypted. The key is available for the administrators and they are the ones who can decrypt such data. Through this file encryption, high levels of file security are achieved in the computer system.

Windows Defender Credential Guard

The windows defender credential guard is another important security feature in the windows operating system. It utilizes virtualization-based security to isolate secrets. This feature is meant to allow specific and authorized applications to access various files in the system. It is an important security feature because any suspect applications are not allowed to access the secret files in the system. Microsoft came up with various security features because there was a need to have a highly effective means through which the files in a system can be managed without facing various threats which can affect the way a computer system operates. With such security features in place, it is easy for the administrators to regulate the type of engagements of computer systems.

There are different researchers who have come up with evidence about the way these operating systems respond to various threats regarding how they protect the computer system. All of the operating systems have been developed with security features that protect users from any form of breaches or threats that may affect the way they operate. Enterprises spend a lot

of resources to ensure their systems are secure and cannot be penetrated through attacks that may come from different malicious people. Computer systems are highly vulnerable because they are always targeted by attackers who have different intentions. Some of their actions are meant to benefit them financially and that affects the way they attack systems. Some use ransomware, and other malware that is meant to give them access to systems so that they can get the information they need to launch attacks. Many companies have suffered the attacks and high levels of damage experienced. Much as it is difficult to completely eliminate all forms of threats, having adequate measures in place is necessary in ensuring the systems are protected from attacks. Security is a key factor in computer systems since most organizations have digitalized their data and they can easily be crippled by attacks that may arise.

Linux OS Security Features

Linux security features are built on the foundations of the Discretionary Access Control model (DAC), a model used by the Unix operating system. It's thereby safe to say that Linux was initially built as the clone of Unix. However, over time it has undergone upgrades and changes to meet the modern requirements. DAC gives the user or owner of an object like a file to set security policies of that file; this means he/she/it has root privileges to that object. Most hackers tend to try and gain root privileges of an object and given that Linux has given control this to the owner it becomes difficult for the hacker to breach or do so unnoticed and this is the basis of Linux security.

As highlighted above Linux found its basis in Unix. It's therefore important to look at Linux security as an extension of the Unix system. Being an open source software various parties have improved the Unix properties over time. Security-Enhanced Linux (Flask) by the United States National Security Agency (NSA) is an example; it supports the definition of a security policy in a specialized language and enforces that policy. There are a lot more: the Medusa DS9, LIDS (Linux intrusion detection system), subterfuge and others (Catuogno & Galdi, 2016).

Extended DAC

Another Linux security development worth to expound on is the extended DAC. In Linux it's defined as the Trusted Computer Systems Evaluation Criteria (TCSEC). It defines the relationship between the object, the user and the owner.

Access Control Lists (ACLs) are widely used to implement this. DAC restricts that object must have an owner having control over the object's permissions, making unauthorized access almost impossible (Gul et al., 2019). The portable operating systems interface (POSIX) is another important feature to consider. Linux uses POSIX to make applications securely portable over various operating environments. Access control lists for Linux are based on this too. POSIX capabilities also help in keeping in check the capabilities of the super user. This is important because if a super user is compromised serious damage can be done.

Namespaces

Namespaces is a feature of Linux whose architecture allows unprivileged user to create its user namespace, giving its process full privilege but staying unprivileged in its previous user namespace. This allows running untrusted code as root without putting in jeopardy the host.

Linux also has network security features. Network features of Linux are very robust. It can be used as an end point node or as a router in a network; this therefore calls for specialized security features. Being an open source it has to support a number of protocols among other numerous features. Linux can deny connections by first checking the host, one very effective way of throwing away attacks. Spoofing can however get around this and allow in threats and hence that's why SSH used (Timmers & Mune, 2017). SSH implies means secure shell which is an open source system well developed that provides encryption as well as authentication of connections. Systems can become less accessible if you make them more secure. Linux has a set of programs set a good balance between access and security.

Linux Cryptography Features

Like many Unix based Oss Linux uses a one-way encryption algorithm and its referred to as the Data Encryption Standard (DES). There is a framework in Linux called the Linux Security Modules (LSMs). It allows its kernel to support several computer security models, avoiding biases towards any one security implementation. The Linux capability system will be a substitute if there is no LSM built into the kernel (Luo et al., 2016). LSM can be implemented in several ways, adding to it mandatory access control (MAC). There is a provision of one inventing a unique security model and implement it as a

module in the frameworks. LSM provides a mechanism to control access to the kernel; a check function provided by LSM is called before the kernel addresses an internal object.

Security enhanced Linux is a feature of Linux security abbreviated as SELinux which gives administrators more power on who accesses the system. It defines controls for processes, applications and files for a system. It has a set of rules used to tell it what can and what can't be accessed. There is an access vector cache (AVC) that it checks with before it allows an application or process, making a request to access an object to do so. If it is unable to make a decision on access based on the cached permissions it will then send a request to the security server (Zhanget al., 2016).

Smack for Linux

Smack for Linux is the simplified mandatory access control (MAC). It is a kernel based implementation of MAC making its primary design goal to be simplicity. However, it isn't the only MAC implementation scheme available for Linux.

Linux features a comprehensive audit system that collects specific system activity to facilitate incident investigation. Through this one can understand certain system behavior and detect attempts at any unauthorized intrusion of the system. It is capable of system calls, file access and to select pre-configured auditable events within the kernel. It is important to note that i9t doesn't protection, but very useful for post-hoc investigation.

Linux has an integrity management subsystem with integrity measurement architecture (IMA). IMA maintains a runtime measurement list and is anchored to the Trusted Platform Module (TPM) to ensure an aggregate integrity value over the list. The benefit of this is that the list cannot be compromised by any software attack without being detected. It can therefore be used to test the system's runtime integrity.

Linux Uses Hardening and Platform Security

Hardening is a collection of techniques, tools and best practices to reduce vulnerabilities of a system. It is a methodical approach needed throughout the lifecycle of a system. It is always tuned up and customized based on a certain need. Linux already a built in model in place and it is up to the person to customize it according to the need.

System calls by processes can also be restricted by the secure computer mode feature (secomp). It prevents applications entering system calls they don't need thereby reducing attacks on the kernel. Bugs in system calls are potential avenues for attack if you take to account the privileged nature of the kernel. With integration with audit login secomp can allow for arbitrary specifications of which system calls are permitted for a process. It should be noted that secomp doesn't virtualize the system's resources, but isolates the processes from them completely.

It is clear, therefore Linux has quite robust security features. It can even be safe to say that in its architecture as an operating system security is the best feature and it forms a fundamental basis of its development

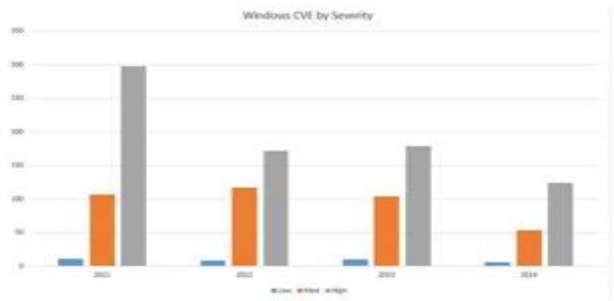
Comparison of the Operating Systems' Security Features

Linux OS and Windows OS have some differences in their security features. There are different ways through which the operating systems deliver security for the computer systems. Linux is considered more secure than Windows. This is because of various features that make it strong in protecting the computer systems from any form of attacks. Attacks are mainly launched through social engineering.

Users of different computer systems end up exposing the systems to various threats through spreading them from one computer to another. For instance, a virus or malware can be spread through clicking on links that contain the viruses and malware software. The operating systems are designed in a way to help in minimizing the chances of having computers exposed to such viruses. Linux does not have root access and it is not easy for users to be exposed to any tricks that may lead them into downloading malware and exposing the systems to security threats. There are many procedures that are followed before the users can authorize the opening of a link in their systems.

This is unlike in windows where a user can click on a link without having any warnings about engaging in such an activity.

Malicious websites can be detected easily to ensure the users are not exposed to such links which, in extension threaten computer security.



Linux is an open source and has transparency. This is one of the features that is exhibited by Linux and instead of being a major security threat, it is in fact, one of the factors that make it highly secure. There is room for improvement in open source development. When a vulnerability is identified, the developers can easily come up with a solution to such an issue because of the availability of different brains that can deliver the operating system from such vulnerabilities. It is important to have a highly effective means through which the operating system can be secured. While the open source exists for some of the programs in Windows, the operating system as a whole is closed. This makes it difficult to bring about ideas that can be used to secure the system whenever there are vulnerabilities.

Linux employs security through variety. This is not a security feature as such for the system, but it plays a vital role in eliminating some of the vulnerabilities to which a given computer system may be exposed. The varieties available for Linux users make it harder for malware to target the majority of the users. Windows on the other hand has only five varieties for their users, which exposes them to various malware which can be developed for such versions. Using different tools and applications is necessary in ensuring there is sufficient security in the system and avoiding some of the issues that may arise as a result of having a less effective operating system in terms of the level of security that is offered by such an OS. There are many cases where the Windows systems have been penetrated by attackers due to lack of a range of products that can lead to difficulty in delivering high levels of security.

Linux assigns privileges to various users like the administrators. Windows on the other hand, generally gives administrators access to the users. The limited nature of assigning privileges to users is necessary in coming up with a highly effective security feature in the systems. Whenever there is a threat, Windows may not be in a position to protect the computer system from such vulnerability. Linux on the other hand can limit the nature of access privileges that users have and that can save the situation for the computer system. This is an important security factor that is supposed to be considered by all the operating systems to minimize the nature of attacks that they can face. Attacks can be detrimental to the delivery of services because such systems can easily be manipulated and controlled by unauthorized parties. This poses a high risk level to the organization and individuals who use such computer systems.

Some of the features that have been developed in the operating system are essential in ensuring there is adequate security of the users' data. For instance, there is the windows defender smart screen. This is a feature that protects the users against websites that have been reported to contain phishing and malware. It helps in stopping the downloading of malicious files. This is an essential security feature that is developed in the windows operating system. Most attackers tend to use malware through sharing, links that will ensure they access the system easily if the users click on the links. The feature is one of the multiple layers of defense that the operating system provides.

Linux OS security Features Versus Windows OS Security Features

Linux OS security features	Windows OS security features
Extended DAC	Windows Defender
Namespaces	Account Control
Linux Cryptography Features	Windows Defender Exploit Guard
Security enhanced Linux is a feature of Linux security abbreviated as SELinux which gives administrators more power on who accesses the system.	Microsoft Bitlocker
Smack for Linux	Windows Defender Credential Guard
Linux has an integrity management subsystem with integrity measurement architecture (IMA).	

SUMMARY

Different operating systems have different security features that enable them to manage applications and minimize any form of security threats to the systems. This research has analyzes the features of Windows and Linux operating systems. It is evident that Linux offers better security compared to Windows. This is because of the nature of abilities that have been exhibited by the operating system. Windows is popular because it has many users and so are the number of attackers who are aware of the weaknesses of the operating system. They understand the nature of activities that are carried out by different users and the security strategies that are applied are similar. Attackers tend to use the weaknesses that are exhibited by different operating systems and that is why it is important to choose the most effective one in terms of security. Security in computer systems is one of the essential factors that is considered by different users. Data and information security is critical to the users of computer systems because they need to maintain privacy and confidentiality.

CONCLUSION

Empirical studies have shown that Linux is not as popular as Windows OS, but it offers better security than the latter. Security is of paramount importance in computer systems. It is through such security features that different computer systems can be used to enhance the performance of different functions. Privacy is an essential factor that should be considered by the organizations. Attackers tend to search for information that they can use for their malicious purposes and that makes it necessary for the system security to be taken with a lot of seriousness. Much as there are differences in the levels of security features in the operating systems, administrators should be keen to implement different security strategies that should be used to ensure there are measures to minimize attacks to the systems.

REFERENCES

[1]. Catuogno, L., & Galdi, C. (2016). On the Evaluation of Security Properties of Containerized Systems. *2016 15th International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security (IUCC-CSS)*. doi: 10.1109/iucc-css.2016.018

[2]. Gul, M. J., Rabia, R., Jararweh, Y., Rathore, M. M., & Paul, A. (2019). Security Flaws of Operating System Against Live Device Attacks: A case study on live Linux distribution device. *2019 Sixth International Conference on Software Defined Systems (SDS)*. doi: 10.1109/sds.2019.8768590

[3]. Luo, Y., Luo, W., Puyang, T., Shen, Q., Ruan, A., & Wu, Z. (2016). OpenStack Security Modules: A Least-Invasive Access Control Framework for the Cloud. *2016 IEEE 9th International Conference on Cloud Computing (CLOUD)*. doi: 10.1109/cloud.2016.0017

[4]. Meijer, C. & Gastel, B. (2019). "Self-Encrypting Deception: Weaknesses in the Encryption of Solid State Drives,"*IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2019, pp. 72-87.

[5]. Philip, J., & Raju, M. (2019). An Overview About the Security Architecture of the Mobile Operating System iOS. *Indian Journal of Computer Science*, *4*(1), 13. doi: 10.17010/ijcs/2019/v4/i1/142412

[6]. Sundar, K., & Kumar, S. (2016). Blue Screen of Death Observed for Microsoft Windows Server 2012 R2 under DDoS Security Attack. *Journal of Information Security*, *07*(04), 225–231. doi: 10.4236/jis.2016.74018

[7]. Timmers, N., & Mune, C. (2017). Escalating Privileges in Linux Using Voltage Fault Injection. *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. doi: 10.1109/fdtc.2017.16

[8]. Vernotte, A., Johnson, P., Ekstedt, M., & Lagerstrom, R. (2017). In-Depth Modeling of the UNIX Operating System for Architectural Cyber Security Analysis. *2017 IEEE 21st International Enterprise Distributed Object Computing Workshop (EDOCW)*. doi: 10.1109/edocw.2017.26

[9]. Zhang, R., Liu, G., Yuan, X., Ji, S., & Zhang, G. (2016). A New Intrusion Detection Mechanism in SELinux. *2016 International Symposium on System and Software Reliability (ISSSR)*. doi: 10.1109/isssr.2016.018