Enhancing Security: A Guide to Limiting Vulnerabilities in Windows Server

Sahmer Ismael

Old Dominion University

CYSE 280

Malik A Gladden

7/22/24

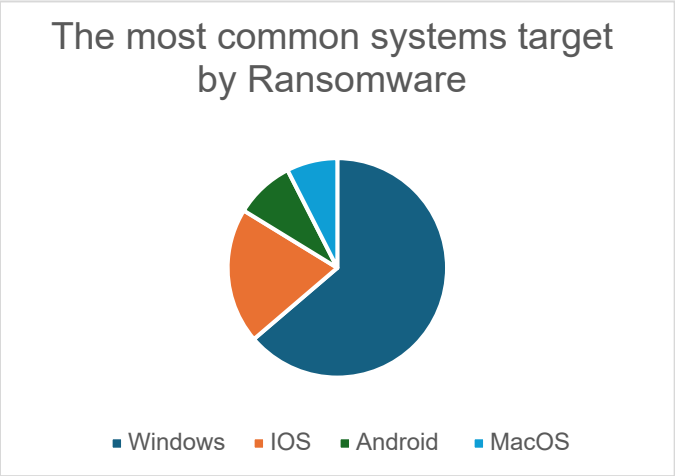
Windows server introduction

Windows servers are one of the most important aspects of organizations, IT Infrastructure, due to their wide variety of features, and services which they provide. These Microsoft operating systems are used daily in organizations and corporations, to handle unique task such as, advance networking, security, information processing, and application support. Without windows servers many organizations would fail to solve complex matters and would have look other ways for solutions. What are window servers, you may ask? Windows servers are a line of Microsoft operating systems, that handle the administrative group activities on a network, and are typically utilized within an organization setting (what is windows server, N.D.). Furthermore, a new version of windows server is created every 2-3 years, that brings upon new innovations, and solutions to security concerns. However, with every new distribution of windows server, also comes new vulnerabilities and security risk for organizations to take into consideration.

On average, there are over 513 vulnerabilities that can be found in a single version of windows sever, but not all of them are critical to security. This is why it is important to have a multi layered strategy featuring, best practices, security measures, and frequent updates to securing windows server. This paper aims to provide a guide on limiting vulnerabilities within a windows server environment, using a various number of techniques such as, network security, intrusion detection systems, backing up data, and security training awareness. However, first one must understand the top 2 cyber-attacks against windows servers and how they occur? And what are some ways in which they could have been mitigated or even avoided?

Ransomware attacks against Windows servers

Ransomware is a type of cyber-attack that concludes, malicious software that is used, to block access to a device, until a sum of money, also known as ransom, is paid (Bansal,2021). Ransomware can either be human or cooperate threats, and can be spread through, social engineering, vulnerable systems, and malicious ads. Ransomware viruses first developed around the year of 1989, but started to gain popularity around the 2000s, in causing cyber breaches for organizations (Bansal,2021). In 2019, ransomware had its biggest impact ever around the globe, in which it effected around 50% of organizations in countries such as the UK, Turkey, United states, Saudi Arabia, and China (Bansal,2021). However, the operating system that took the most damage from ransomware attacks was windows server operating system, as shown on the chart below.



The reason behind this, is that since windows server are widely spread throughout the world, and are critical for the network environments, they are more prone to being targeted for ransomware attacks. An example of this was the WannaCry ransomware attack that occurred on May 12th, 2017, that exploited vulnerabilities in a SMB protocol, in windows known as Eternal blue (Hsiao, et al.,2018). Furthermore, after the device was infected, it would encrypt the files on that

individual's device, until a ransom in bitcoin was to be paid (Hsiao, et al.,2018). This attack was very devastating due to the fact, that it reached over 150 countries worldwide, and affected over 200,000 devices, which caused over $4billion dollars in damages (5 years after,2022). Microsoft had released patches for the Eterna blue vulnerability months in advance, however many servers, did not complete the update, which made them prone to WannaCry. This is not the only brutal ransomware attack that occurred, against windows server, months later NotPetya came along and was adequate in damaging, such as WannaCry. This is why it is important to constantly install updates on windows servers and apply security patches, so you can better safeguard your environment.

Phishing Attacks Against Windows Servers

Phishing is a type of attack, that hackers use, with the aim to steal sensitive information of an individual, or even an organization such as their login credentials, and financial data by acting as a trustworthy source in online communications (Huseynov, et al., 2020). This type of cyber-attack is used preventively on targeting windows servers, in organizations, and is deemed very successful. The reason behind this attack being so successful, is that attackers tend to use the HTML full page phishing technique against windows servers which is very effective(Huseynov, et al., 2020). Unlike other phishing attacks, that can only mimic a single page or login form, HTML works to copy the whole operating system, plus the operating systems lock and unlock interface(Huseynov, et al., 2020). Which it makes it extremely difficult for users and organizations, to be able to detect the fake phishing page, which increases the likelihood of a successful phishing attack (Huseynov, et al., 2020). This HTML phishing attack evolves from the browser in the middle attack, by developing a fake display window, replicating the windows login page instead of a different browser window, using HTML and CSS techniques.

Furthermore, the HTML page is then portrayed in full screen mode using a JavaScript code, to copy the lockscreen and to create no distractions as the user logs into the operating system of windows with their credentials(Huseynov, et al., 2020). Once the user logs into the operating system, the credentials captured, are then sent to the malicious user to continue stealing sensitive information, of the individual or organization (Huseynov, et al., 2020). This unauthorized access from the malicious user, can lead to crimes such as, credential theft, Identity theft, spear phishing, and password reuse of other accounts. This is why it is extremely important to practice mitigation techniques and have good cyber hygiene to help defend against these crucial attacks on windows servers.

The Importance of Network Security and IDS

Network security corresponds to the practices, and mitigation tactics implemented to safeguard computer networks from, unauthorized access, misuse, and other security vulnerabilities (What is server security, N.D). Furthermore, it is crucial for windows servers to have a good network security tactic that includes, various technologies, polices, and strict procedures, to help protect the confidentiality, integrity, and availability of users, and organizations (What is server security, N.D). While IDS (Intrusion detection system), are both hardware and software components, that use gathering of analytical techniques to detect attacks, identify their sources, alert network administrators, and possibly mitigate against the cyber-attacks (Marian,et al., 2011). The incorporation of Network security and IDS are very important in a organization, of windows servers, because it protects the server against critical attacks, such as ransomware, and phishing attacks.

The Intrusion detection systems and network security frameworks in my opinion, that should be adopted by windows servers, that could help limit the attacks that are most critical such as ransomware and phishing should be the combination of, signature detection, anomaly detection, and Nist (Marian,et al., 2011). Signature detection is a IDS system, that works to scan packets and audit logs, to look for specific signatures that were previously demonstrated to indicate the presence of a specific attack (Marian,et al., 2011). The way in which this IDS system, scans packets and audit logs, is by using a pattern matching approach, which comes from, recognized attack vectors, features of the malware, and existing exploits (Marian,et al., 2011). Furthermore, this IDS system contains a very signature database, that helps users and organizations, stay up to date on the newest cyber-attacks and threats to security while keeping updates on new software components (Marian,et al., 2011). This would aid and defend Windows server in organizations, against attacks such as WannaCry, which expanded across the globe from user and organizations, not downloading the newest update Windows displayed for patching the ransomware.

Anomaly is a IDS, that uses its detection, and its behavior patterns to indicate malicious activity, and also looks at past activity to determine if the behavior is normal or not (Marian,et al., 2011). This monitoring of past activity, of a user on windows can help to create a baseline when it comes to monitoring traffic within the network or throughout the systems activity. Which can aid the system, being able to detect, a attack such as a phishing HTML attack, that creates a lock screen, so the user logs in, the system will be able to detect the unusual activity and report it. The security framework that can work perfectly, with both IDS systems to safeguard windows servers, is the NIST framework. The NIST framework is a cybersecurity framework that helps to provides rules and security guidelines for organizations, both in the private sector and public

sector to follow, to help prevent future attacks, monitor attacks, and prevent them (Lei & Lawyer, 2014). The main goal of the framework is to not set requirements or take the place of an organization's present cybersecurity procedures, but rather provides a baseline for organizations to measure their cyber programs (Lei & Lawyer, 2014). The combination of both the NIST framework and the IDS systems, would help to better safeguard windows servers from prevalent cyber-attacks, and would create a safer environment for individual and organizations.

Importance of data backup

Data backups are crucial when it comes to the security of windows servers and helping maintain availability and reliability, during a cyber-attack (Zhang, et al., 2017). Furthermore, consideration of a backup in windows servers with encryption offline, can help to ensure if a ransomware attack were to occur, availability of data and recovery options (Zhang, et al., 2017). Furthermore, backing up data can also help to ensure data recovery, if a natural disaster were to occur and still ensure confidentiality of data as well. Backing up data also allows for system updates while backing up process is occurring, to ensure the latest security features (Zhang, et al., 2017).

Importance of security awareness

Educating users on security is critical for a organization and individuals, no matter how many IDS systems are implemented, or even how many security frameworks are acquired, the organization and individual's data, will never be secure if security awareness is not implemented (McCoy & fowler, 2004). This is why it is important for windows to have a security awareness program set in place, to protect organizations and users. Furthermore, the implementation of a security awareness program, would help to limit phishing attacks, that occur on windows users,

for example such as clicking a phishing email. Furthermore, windows adhering to a security awareness program, will limit the results of human error, and promote safe browsing practices for windows users, and protect windows servers.

Conclusion

In conclusion, when looking at the number of vulnerabilities that windows server concludes, there are too many to take into consideration. However, when the focus is on the most damaging attacks that conclude a loss of data and a sense of security, for organizations and users, such as ransomware, and phishing, there are many security procedures, that can be set in place to help safeguard a individual's data. Furthermore, security frameworks such as the NIST framework incorporated with Intrusion detection systems such as the signature IDS, and anomaly, one can better safeguard windows servers, against present and future cyber-attacks, while protecting the confidentiality, integrity, and availability of data at the same time. Additionally, creating encrypted backups that are online, and are updated with the most recent security patches, can also help protect organizations and individuals, when it comes to issues, such as ransomware or even data corruption against windows servers. This also helps windows users, have availability to their data for attacks, that are not man made, such as natural disasters. However, The most important aspect to safeguard, windows servers, is to have security awareness. Security awareness helps to limit out human error issues, and to create a better environment for users and organizations to scroll on the web cautiously, and with alert.

Reference page

A Review on Ransomware Attack. (2021, May 21). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9478148

5 years after the first WannaCry attack - CyberTalk. (2022, May 20). CyberTalk. https://www.cybertalk.org/5-years-after-the-first-wannacry-attack/

Microsoft Vulnerabilities Hit a Record-High: Here's Why. (2023, June 23). BeyondTrust. https://www.beyondtrust.com/blog/entry/microsoft-vulnerabilities-report#:~:text=There%20were%20513%20Windows%20vulnerabilities,slightly%20to%20552%20in%202022.

What Is Windows Server?—IT Glossary | SolarWinds. (n.d.). https://www.solarwinds.com/resources/it-glossary/windows-server

The static analysis of WannaCry ransomware. (2018, February 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8323680?casa_token=GRClSLCS0OEAAAA:vYkGATAMiReCKImkkKSzPc_bljpaeDjb9I-TDboWa-YEl3w04jFR3C4wpP_OogGSc7xXEUvQ

McDonald, G., Papadopoulos, P., Pitropakis, N., Ahmad, J., & Buchanan, W. J. (2022). Ransomware: Analysing the Impact on Windows Active Directory Domain Services. *Sensors*, *22*(3), 953. https://doi.org/10.3390/s22030953

Phishing Windows Login Credentials Using HTML Full-page Technique. (2023, December 30). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/10442374

Network security basics. (2005, December 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/1556540

THE NIST CYBERSECURITY FRAMEWORK: OVERVIEW AND - ProQuest. (n.d.). https://www.proquest.com/docview/1681907475?pq-origsite=gscholar&fromopenview=true&sourcetype=Scholarly%20Journals

Research and Implementation of a Data Backup and Recovery System for Important Business Areas. (2017a, August 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8048193?casa_token=yf8FzfC5OHsAAAAA:2MVWmNZfswIsDCYowmiBYEqRNRQ3eJJw2dzs7Jb967OlmPdgd9iQLRQWlwCL2vQ_ikGyYnk8

Research and Implementation of a Data Backup and Recovery System for Important Business Areas. (2017b, August 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8048193?casa_token=yf8FzfC5OHsAAAAA:2MVWmNZfswIsDCYowmiBYEqRNRQ3eJJw2dzs7Jb967OlmPdgd9iQLRQWlwCL2vQ_ikGyYnk8

McCoy, C., & Fowler, R. T. (2004). *"You are the key to security."* https://doi.org/10.1145/1027802.1027882