iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.53795

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

Eternal Blue Vulnerability

Manoj R. Gupta[1], Yash P. Koli[2], Vedant A. Patiyane[3], Kedar P. Wagh[4]
[1, 2, 3, 4]*Student Cyber Security Engineering, Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India*

Abstract: ***Many organizations have experienced the damage caused by cyberattacks exploiting Windows vulnerabilities. For operational reasons, the parameters of Windows are still used, especially in the enterprise management system (ICS). In this case, attackers can torture them to spread the disease. Specifically, the vulnerability in MS17-010 was used in attacks to spread malware such as WannaCry ransomware and other malware. Many systems for example, electronic newspapers, payment centres and car manufacturers are used around the world and there is a security vulnerability in Windows that causes serious problems. Since tools like Eternal Blue or Eternal Romance are published on the internet, attackers can easily exploit these vulnerabilities. This tool attacks legitimate processes running on Windows systems. It can be difficult for employees to see the signs of a struggle. Attacks can be mitigated using security updates; however, security updates are sometimes difficult to implement due to their long lifetime and stringent requirements. There are many ways to identify attacks that cause vulnerabilities, such as intrusion detection systems (IDS), but they are sometimes difficult to use because they require prior service. In this research, we propose a method to identify the attack that exploited the vulnerability in MS17-010 by analysing Windows built-in event Logs. This method can detect attacks against almost all supported versions of Windows. It can also be easily integrated into the production environment as it only uses the standard Windows operating system.***
Keywords: Eternal Blue, Vulnerability, Ransomware, attacks, malware.

I. INTRODUCTION

The cybersecurity world was flooded with reports about the infamous and widespread WannaCry ransomware attack. The plot begins shortly after with some of the National Security Agency's revelations that (NSA) was used by the Shadow Brokers hacking group. WannaCry attack, which uses a globally immutable system, uses a vulnerability named "Eternal Blue" and is distributed in 150 countries. The notorious Shadow Brokers hacker group has been operating since 2016 and is responsible for various NSA leaks, zero-day attacks and hacking tools of vulnerabilities. According to Wikipedia, the Shadow Brokers group has reported five violations to date. Leak, which surfaced on April 14, 2017, was the most devastating. The same day, Microsoft published a blog post announcing the patch for, which fixes Shadow Brokers' vulnerability. A month before the leak (March 14, 2017), Microsoft released Security Bulletin MS17-010, which fixes some of the vulnerabilities, including the one used by the "Eternal Blue" exploit. However, many users did not use the patch and on May 12, 2017, suffered the WannaCry attack, the largest ransomware attack in history.

A. Overview

WannaCry gained worldwide attention after affecting more than 230,000 computers in over 150,444 countries. Famous organizations such as hospitals and telecommunications, gas, electricity and other service providers were the first victims of this attack [3]. Shortly after WannaCry took place, other serious attacks were also seen using Eternal Blue and other exploits and hacks from the same NSA leak. This contains the Eternal Rocks worm Petya Ak. Not Petya ransomware and BadRabbit ransomware. The cryptocurrency mining campaign has also spread to other machines, apparently using exploits leaked by Shadow Brokers. These include Adaluz, Zealot, and Wanni Mine. Fifth Shadow Brokers NSA leak contains 30 vulnerabilities and a total of 7 hacking tools/devices are integrated into a framework called "Fuzz bunch".

B. Problem Statement

External Blue vulnerability is a vulnerability that affects many aspects of the Windows operating system. It was discovered in 2017 and is believed to have been used for surveillance by the US National Security Agency (NSA) before being leaked to the public. This vulnerability is called Outer Blue because it affects the use of the Windows Server Message Block (SMB) protocol, which is used to share files and printers on the network. An attacker can use Outside Blue to gain unauthorized access to a system by sending code or special packets that can execute commands to a vulnerable computer. One of the most important features of the Outdoor Blue is that it does not require user intervention or authentication to use it. This means that attackers can easily target systems without requiring a username or password.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

In addition, the remote attack becomes a threat to organizations with multiple computer networks. Outside Blue was responsible for the May 2017 WannaCry ransomware attack that hit thousands of generations worldwide. The attack affects computers running older versions of Windows that have not been updated with security patches released by Microsoft two months ago. The ransomware encrypts the data on the infected system and demands a ransom in exchange for the decryption key.

II. REVIEW OF LITERATURE

A. Reference Paper

The literature review for this project weighed 20 literature Projects based on the Eternal Blue Vulnerability. Most of the papers were based on the concept of ease of use This Vulnerability. The document explains the use of chaining vulnerabilities and highlights the importance of patching systems to prevent attacks. The Eternal Blue vulnerability is a major security issue in the Microsoft Windows operating system that was discovered in 2017. It allows hackers to remotely execute code and gain control of the computer without compromising the user. The WannaCry ransomware attack exploits this vulnerability, infecting more than 200,000 computers in 150 countries. Since this Vulnerability was discovered, a lot of research has been done to understand the Nature of the vulnerability, the risk it poses, and ways to mitigate its effects. Here are some Key findings from the data:

1) *WannaCry Impact:* A 2018 study by the National Bureau of Economic Research analysed the economic impact of the WannaCry ransomware attack. The study estimates the global Cost of the attack to be around $8 billion.
2) *Risk Assessment:* A 2019 research paper by the Centre for Strategic and International Studies assesses the risk of cyberattacks against critical infrastructure. The data identifies Eternal Blue as one of the top threats to critical systems and recommends steps to mitigate the risk.
3) *Mitigation Strategies:* A 2019 report from the National Institute of Standards and Technology provides guidance for mitigating the effects of Eternal Blue. The report recommends several measures, including patching systems, disablingSMBv1, and applying network partitioning.
4) *Use by other Malware:* A 2020 Kaspersky report examined the use of Eternal Blue by various malware families, including Trick Bot and Emoted. The report highlights the need for additional safeguards and security measures.

Fig. 1 Research Work

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

III. DESIGN DETAIL

The Eternal Blue payload represents a significant and infamous cybersecurity exploit those targeted vulnerabilities in Microsoft Windows systems. While it is important to note that discussing specific details of exploits or vulnerabilities can potentially be used for malicious purposes, we can explore the design principles and strategies employed to understand its impact and implications in the context of cybersecurity. The design of the Eternal Blue payload showcases a meticulous fusion of technical ingenuity and strategic planning. At its core, the payload aimed to exploit a weakness in the Windows Server Message Block (SMB) protocol, specifically targeting the vulnerability known as "Eternal Blue." This vulnerability allowed for the execution of arbitrary code, enabling unauthorized access to systems and potentially leading to the deployment of additional malware. One key design detail of the Eternal Blue payload lies in its ability to remain undetected and propagate seamlessly across interconnected networks. By leveraging the SMB vulnerability, the payload could exploit systems with outdated or unpatched software, emphasizing the critical importance of regular software updates and security patches. This design detail demonstrated the significance of proactive cybersecurity measures and the need for constant vigilance in the face of evolving threats. Additionally, the payload exhibited advanced evasion techniques to bypass security measures, enabling it to spread rapidly and efficiently. Design details included obfuscation methods, where the payload disguised its code to appear benign or indistinguishable from legitimate system processes. This intricate design approach enabled the payload to evade detection by traditional antivirus solutions and further highlighted the necessity for multi-layered security strategies. Furthermore, the Eternal Blue payload demonstrated the potential impact of combining multiple vulnerabilities to maximize its effectiveness. The design incorporated various exploits, leveraging weaknesses beyond the initial SMB vulnerability. This layered approach showcased the importance of holistic security practices, emphasizing the need for comprehensive vulnerability management and robust defines-in-depth strategies. It is important to note that discussing specific design details of the Eternal Blue payload should be done responsibly and with a focus on promoting awareness and education in the field of cybersecurity. Understanding the intricacies of such exploits can help reinforce the urgency of maintaining strong cybersecurity practices, fostering a proactive approach to protecting systems and networks. The design detail of the Eternal Blue payload exemplifies the ingenuity and sophistication employed in cyberattacks. By exploiting vulnerabilities, evading detection, and leveraging multiple exploits, the payload showcased the need for continuous improvement in cybersecurity defences. Understanding the design principles behind such exploits can help organizations and individuals enhance their security measures, fostering a safer digital landscape.

A. Windows Operating System

Eternal Blue targets Windows operating systems, specifically Windows XP through to Windows Server 2008 R2. This means that any system running a Windows operating system in this range is potentially vulnerable to this exploit. However, Microsoft has released patches to address this vulnerability for all affected versions of Windows. *Title and Author Details*

B. SMBv1

The vulnerability exists within the Server Message Block (SMB) protocol version 1 implementation in Windows. SMB is a network protocol that allows for file and printer sharing across networks. SMBv1 is the first version of the protocol and is still supported in some Windows systems, but it is considered to be outdated and insecure. Eternal Blue exploits a flaw in SMBv1 to execute remote code on the targeted system.

C. Unpatched system

The vulnerability was patched by Microsoft in March 2017, but systems that have not been updated with the patch are still vulnerable. This means that any system that has not applied the necessary security update is still at risk of being exploited. Microsoft has since released several updates to address this vulnerability, and it is crucial to ensure that these updates have been installed on all affected systems to prevent attacks

D. Kali Linux

Kali Linux is a popular Linux-based operating system designed for advanced penetration testing, ethical hacking, and security auditing. It is a powerful tool used by security professionals and hackers alike to test and improve the security of computer systems, networks, and applications. Kali Linux is based on Debian and is preloaded with a wide range of security tools, including vulnerability scanners, network analysers, password crackers, wireless tools, exploitation tools, and forensic tools.

Some of the popular tools available in Kali Linux include Nmap, Metasploit Framework, Wireshark, John the Ripper, Air crack-ng, and many others. Kali Linux is designed to be used by security professionals who have advanced knowledge of computer networks, operating systems, and programming languages. It provides a robust command-line interface (CLI) that allows users to run various security tools and scripts, automate tasks, and perform complex operations.

E. Metasploit

Metasploit is widely used by security researchers, penetration testers, and hackers to identify and exploit vulnerabilities in a target. It includes several modules for different types of applications, including remote launch, privilege escalation, and brute force attacks. One of the key features of Metasploit is its modular design, which allows users to create their own custom exploits and payloads. This flexibility makes it a popular tool for both offensive and defensive security.

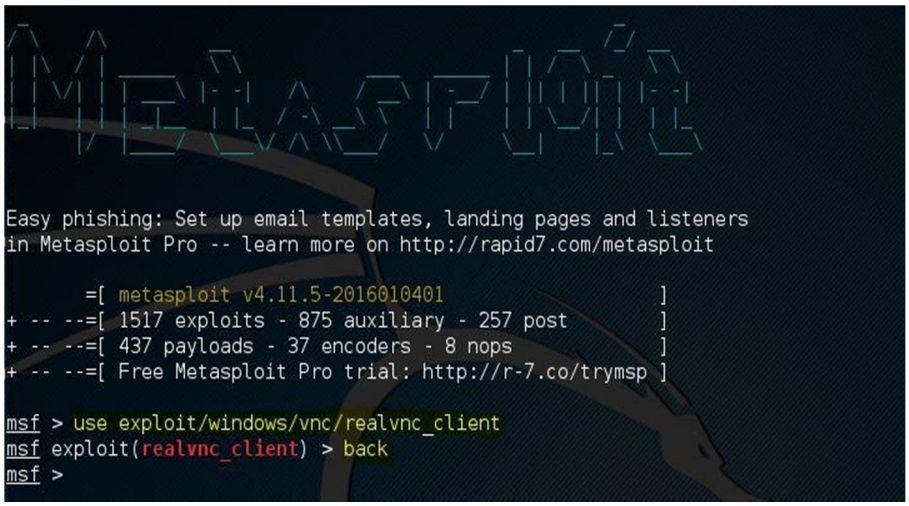


Fig. 2 Metasploit

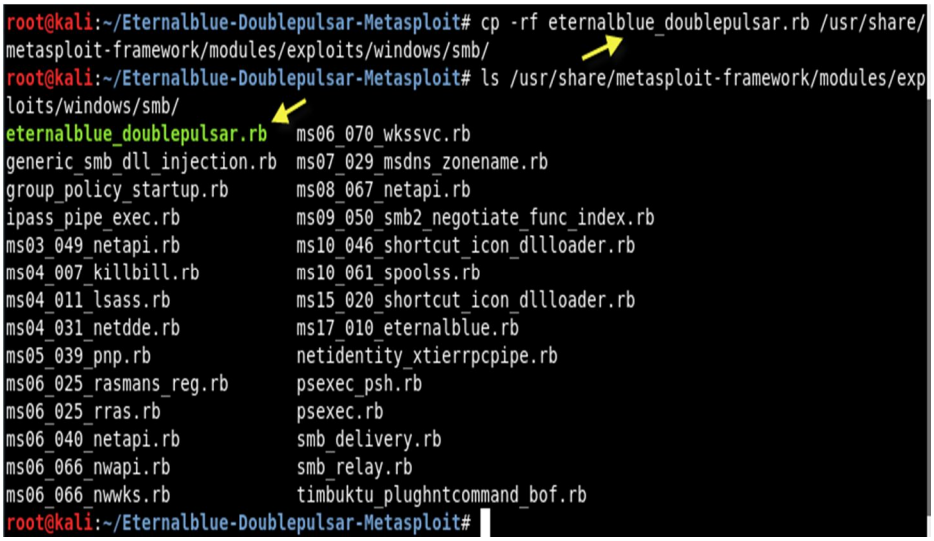


Fig. 3 Metasploit info

F. Nmap

Nmap (short for Network Mapper) is a free and open-source network discovery and security monitoring tool. It is widely used by network administrators, security professionals, and penetration testers to find hosts and services on the network and identify potential vulnerabilities. Nmap uses various techniques such as port scanning, version control, and operating system fingerprinting to gather information about hosts and services on the network. It can also be used to perform various other tasks such as ping scans, traceroutes, and script-related targeting.

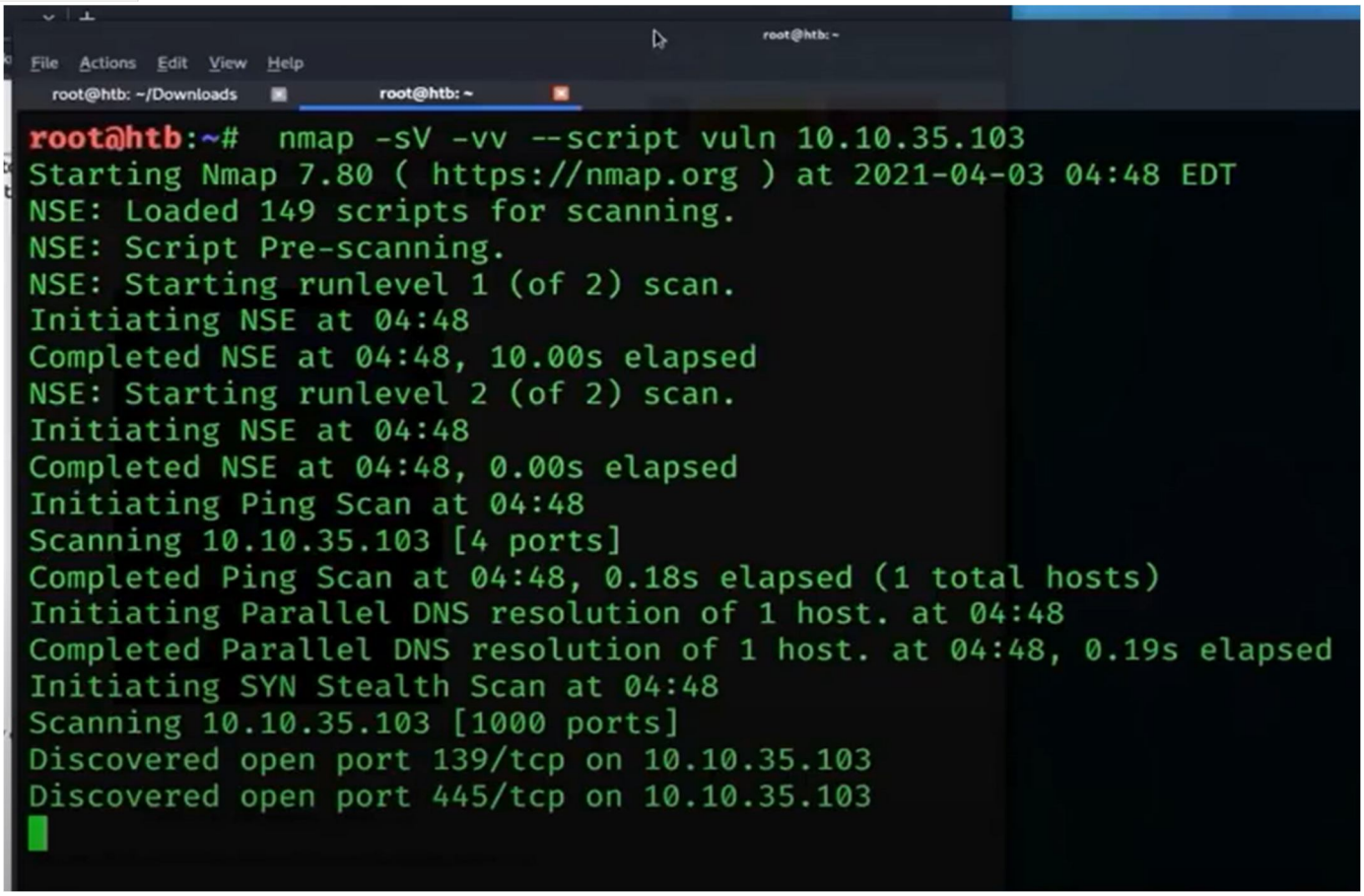


Fig. 4 Nmap

IV. RESULT

The Eternal Blue vulnerability is a vulnerability found in the Windows operating system, specifically the Server Message Block (SMB) protocol. This vulnerability was used in the WannaCry ransomware attack that affected thousands of computers worldwide in 2017. Since the discovery of the vulnerability, many researchers and security experts have been working to understand and mitigate the risks posed by the Eternal Blue vulnerability. Some of the affected projects in this area are

A. Security Patches

Microsoft has released several security updates and patches to address the Eternal Blue vulnerability in different versions of the Windows operating system. This patch aims to fix the SMB vulnerability and prevent attackers from exploiting this vulnerability.

B. Detection Tools

Many security companies have developed detection tools to detect and block attacks that lead to the Eternal Blue vulnerability. These tools often use a combination of network traffic analysis and behavioral analysis to detect and block malicious activity.

C. Exploit Kits

Cybercriminals have developed exploit kits to facilitate the Eternal Blue vulnerability exploitation process. These tools allow unskilled attackers to attack vulnerable systems.

D. Reverse Engineering

Researchers reverse engineer the Eternal Blue vulnerability to understand how it works and identify mitigation strategies. This approach helps security professionals improve detection and protection.

E. Vulnerability Analysis

Security researchers analyzed Eternal Blue's vulnerabilities to understand their root causes and identify potential areas for improvement in Windows operating system development. This review has led to the development of more secure systems and designs that are less susceptible to similar vulnerabilities.

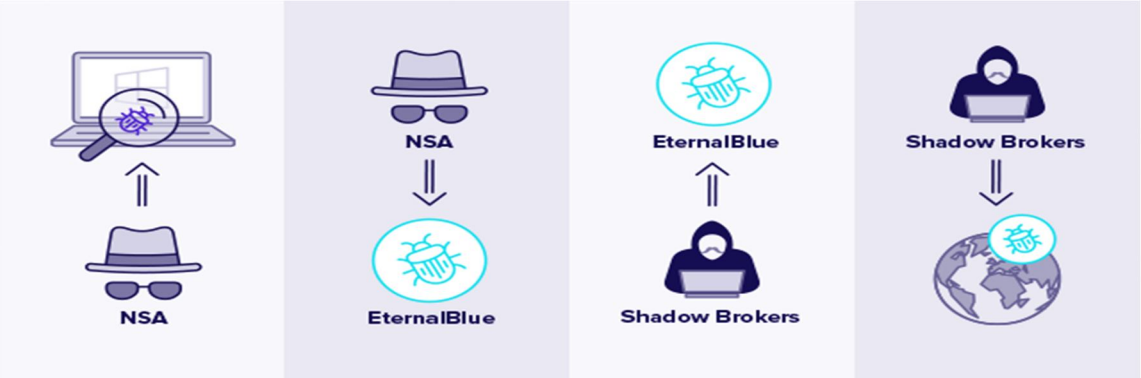


Fig. 5 Result

V. CONCLUSIONS

The Eternal Blue vulnerability is a critical vulnerability found in the Windows operating system, specifically the Server Message Block (SMB) protocol. It was previously known for the WannaCry ransomware attack that affected thousands of computers worldwide in 2017. [12] Since the discovery of the vulnerability, the cybersecurity industry has taken a number of steps to try the issue from the negative. Microsoft released a security patch to fix SMB vulnerabilities, security companies developed detection tools to detect and block attacks from the vulnerabilities, and researchers reverse engineered Eternal Blue's vulnerability to understand how it works and identify mitigation strategies.

The discovery and patching of Eternal Blue vulnerabilities highlights the importance of cybersecurity and the need to improve security and processes. Although this vulnerability has been fixed, new vulnerabilities will emerge in the future and attackers will continue to develop more and more attacks.

Therefore, organizations must remain vigilant and continually adapt to new threats to maintain the security of their systems and information [19].

The entire story of Eternal Blue from the beginning to the present (not yet "end") is a warning to those concerned about cybersecurity.[9] From the use of 0day tools to the trick of not applying security updates on time, to who knows what happens after WannaCry and Not Petya, many disasters can be avoided. In conclusion, Eternal Blue reminds us of the modern threat of cyber-attacks and the importance of taking preventative steps against them. By implementing cybersecurity measures and being alert to emerging threats, organizations can protect their data, finances and reputations from harm. To prevent the Eternal Blue exploit from being used against vulnerable systems, it's crucial to apply security patches and updates, use strong passwords and authentication methods, and implement proper security measures, such as firewalls and intrusion detection systems. Additionally, organizations should conduct regular security audits and vulnerability assessments to identify and address any security weaknesses in their systems.

Overall, the Eternal Blue exploit serves as a reminder of the importance of cybersecurity and the need for constant vigilance and proactive measures to protect computer systems and data from malicious attacks.

VI. ACKNOWLEDGMENT

We have great pleasure in presenting the project on "ETERNAL BLUE VULNERABILITY". We take this opportunity to express our sincere thanks to our Guide, Ms. Pranali Pawar, the faculty in the Department of Cyber Security in Shah and Anchor Kutchhi Engineering College for guiding us and suggesting regarding the line of work. We would like to express our gratitude towards their constant encouragement, support and guidance throughout the progress.

Also, we would like to thank our principal – Dr. Bhavesh Patel and Dr. Nilakshi Jain, Head of Cyber Security Department, for their help, support & guidance for this project. We are also thankful to all Faculty members of our department for their help and guidance during completion of our project

REFERENCES

[1] Dalvi, P. Kulkarni, A. Kore and S. G. Bharu, "Dark Web Crawling for Cybersecurity: Insights into Vulnerabilities and Ransomware Discussions," 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2023, pp. 1-6, doi: 10.1109/INOCON57975.2023.10101162. https://ieeexplore.ieee.org/document/10101162

[2] D. Liu et al., "From Release to Rebirth: Exploiting Thanes Objects in Linux Kernel," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 533-548, 2023, doi: 10.1109/TIFS.2022.3226906. https://ieeexplore.ieee.org/document/9970376

[3] B. Fiore, K. Ha, L. Huynh, J. Falcon, R. Mendiola and Y. Li, "Security Analysis of Ransomware: A Deep Dive into WannaCry and Locky," 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2023, pp. 285-294, doi: 10.1109/CCWC57344.2023.10099114. https://ieeexplore.ieee.org/document/10099114

[4] M. Alcaide et al., "NHS WannaCry Ransomware Attack: Technical Explanation of The Vulnerability, Exploitation, and Countermeasures," 2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICWAI), Zarqa, Jordan, 2022, pp. 1-6, doi: 10.1109/EICEEAI56378.2022.10050485. https://ieeexplore.ieee.org/document/10050485

[5] Z. Liu, Z. Wang, Y. Zhang, T. Liu, B. Fang and Z. Pang, "Automated Crash Analysis and Exploit Generation with Extendable Exploit Model," 2022 7th IEEE International Conference on Data Science in Cyberspace (DSC), Guilin, China, 2022, pp. 71-78, doi: 10.1109/DSC55868.2022.00017. https://ieeexplore.ieee.org/document/9900190

[6] Y. Mogahed, M. Cuvier and I. Gash, "Predicting the Discovery Pattern of Publicly Known Exploited Vulnerabilities," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 2, pp. 1181-1193, 1 March-April 2022, doi: 10.1109/TDSC.2020.3014872. https://ieeexplore.ieee.org/document/9161273

[7] Liu, Z., Chen, C., Zhang, L.Y., Gao, S. (2022). Working Mechanism of Eternal blue and Its Application in Ransom worm. In: Chen, X., Shen, J., Susilo, W. (eds) Cyberspace Safety and Security. CSS 2022. Lecture Notes in Computer Science, vol 13547. Springer, Cham. https://doi.org/10.1007/978- 3-031-18067-5_13 https://link.springer.com/chapter/10.1007/978-3-031-18067-5_13#cities

[8] Smith, Joshua. (2021). Ex150 - Eternal Blue Exploit. 10.13140/RG.2.2.26161.71525. https://www.researchgate.net/publication/351035706_Ex150_-_Eternal_Blue_Exploit

[9] H. Li, L. Zhou, M. Xing and H. b. Taha, "Vulnerability Detection Algorithm of Lightweight Linux Internet of Things Application with Symbolic Execution Method," 2021 International Symposium on Computer Technology and Information Science (ICSTIS), Guilin, China, 2021, pp. 24-27, doi: 10.1109/ISCTIS51085.2021.00013. https://ieeexplore.ieee.org/document/9603596

[10] A. Hildebrandt and A. Diehl, "Securing Machine Learning: A Red vs Blue Approach," NAECON 2021 - IEEE National Aerospace and Electronics Conference, Dayton, OH, USA, 2021, pp. 337-340, doi: 10.1109/NAECON49338.2021.9696441. https://ieeexplore.ieee.org/document/9696441

[11] E. Iannone, D. D. Nucci, A. Sabita and A. De Lucia, "Toward Automated Exploit Generation for Known Vulnerabilities in Open-Source Libraries," 2021 IEEE/ACM 29th International Conference on Program Comprehension (ICPC), Madrid, Spain, 2021, pp. 396-400, doi: 10.1109/ICPC52881.2021.00046. https://ieeexplore.ieee.org/document/9462983

[12] H. Eck, "Comparison of Active Vulnerability Scanning vs. Passive Vulnerability Detection," 2021 International Conference on Information Security and Cryptology (ISCTURKEY), Ankara, Turkey, 2021, pp. 87-92, doi: 10.1109/ISCTURKEY53027.2021.9654331. https://ieeexplore.ieee.org/document/9654331

[13] G. Usha, P. Madhavan, M. Vimal Cruz, N. A. S. Vinoth, Veena and M. Nancy, "Enhanced Ransomware Detection Techniques using Machine Learning Algorithms," 2021 4th International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 2021, pp. 52- 58, doi: 10.1109/ICCCT53315.2021.9711906. https://ieeexplore.ieee.org/document/9711906

[14] M. A. Mos and M. M. Chowdhury, "The Growing Influence of Ransomware," 2020 IEEE International Conference on Electro Information Technology (EIT), Chicago, IL, USA, 2020, pp.643- 647, doi:10.1109/EIT48999.2020.9208254. https://ieeexplore.ieee.org/document/9208254

[15] G. Lu, Y. Liu, Y. Chen, C. Zhang, Y. Gao and G. Zhong, "A Comprehensive Detection Approach of WannaCry: Principles, Rules and Experiments," 2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (Cybercop), Chongqing, China, 2020, pp. 41-49, doi: 10.1109/CyberC49757.2020.00017. https://ieeexplore.ieee.org/document/9329407

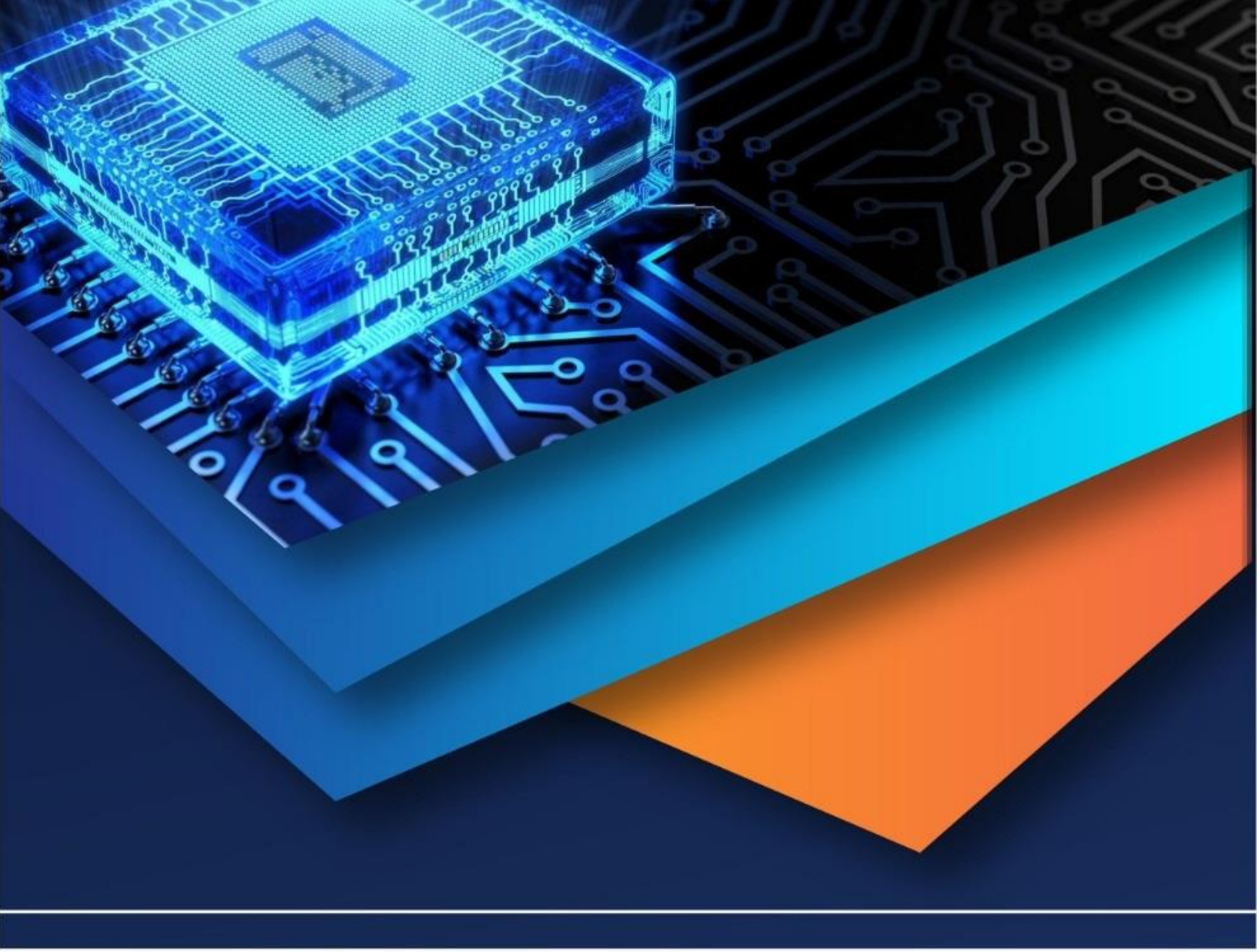
[16] M. Fujimoto, W. Matsuda and T. Matsunaga, "Detecting attacks leveraging vulnerabilities fixed in MS17-010 from Event Log," 2019 IEEE Conference on Application, Information and Network Security (AINS), Pulao Pinang, Malaysia, 2019, pp. 42-47, doi: 10.1109/AINS47559.2019.8968703. https://ieeexplore.ieee.org/document/8968703

[17] A. Chaquille, T. Guard and G. Nantahala Quian, "Ransomware - WannaCry Security is everyone's," 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), Coimbra, Portugal, 2019, pp. 1-4, doi: 10.23919/CISTI.2019.8760749. https://ieeexplore.ieee.org/document/8760749

[18] N. Naik, P. Jenkins, N. Savage and L. Yang, "Cyber Threat Hunting - Part 2: Tracking Ransomware Threat Actors using Fuzzy Hashing and Fuzzy C-Means Clustering," 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), New Orleans, LA, USA, 2019, pp. 1-6, doi: 10.1109/FUZZ-IEEE.2019.8858825. https://ieeexplore.ieee.org/document/8858825

[19] A. D. Widegap and Y. Dewi Ward Hana Aznar, "Integrated Exploit Kit for Web Application," 2019 International Conference on Electrical Engineering and Computer Science (ICECOS), Bantam, Indonesia, 2019, pp. 299-302, doi: 10.1109/ICECOS47637.2019.8984449. https://ieeexplore.ieee.org/document/8984449

[20] U. Javed Butt, M. Abbot, A. Lords, H. Jamatkhana, A. Jamal and A. Kumar, "Ransomware Threat and its Impact on SCADA," 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 2019, pp. 205-212, doi: 10.1109/ICGS3.2019.8688327. https://ieeexplore.ieee.org/document/8688327



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY