SSRG International Journal of Computer Science and Engineering
ISSN: 2348 – 8387 / https://doi.org/10.14445/23488387/IJCSE-V9I3P101

Volume 9 Issue 3, 1-4, March 2022

Original Article

VAPT & Exploits, along with Classification of Exploits

Sheetakshi Shukla[1], Tasneem Bano Rehman[2]

[1,2]*School of Advanced Computing, Sage University Bhopal, M.P, India*.

Received: 06 February 2022 Revised: 19 March 2022 Accepted: 26 March 2022 Published: 31 March 2022

Abstract *- Vulnerability assessment and penetration testing is a process done at every level in cyber security due to regular attacks and the problems created by the attackers, either for personal or professional reasons. On the other hand, Exploits are the main asset of Vulnerabilities. This paper aims to classify the exploits based on their existence. Also, this paper tries to give a fair judgment to review Vulnerability Assessment and Penetration Testing with Exploits. Along with some awareness and prevention techniques. A study on preventive and defensive measures could be taken from the view of any Penetration Tester. Detailed Classification of Exploits and their existence is the main aspect of this paper*.

Keywords *- Classification of exploits, Exploits, Penetration testing, Vulnerability assessment, Zero-Day Attacks, Zero-Day Exploits.*

1. Introduction

Any flaw, loophole, or misconfiguration during the software's update or installation or any faulty coding patch usually leads to the production of any Vulnerability. Detecting such Vulnerability is known as Vulnerability Assessment. On detection of such Vulnerability, a probable solution is deployed, and the problem is being fixed; such a process is known as Penetration Testing [11]. As far as the Exploits are concerned, they can be introduced as a mere coding malfunction that may lead to serious situations detected by any attacker [1]. All such kinds of vulnerability detection are now usually done with advanced technology with the help of Machine Learning and Artificial Intelligence [4, 5, 6].

In this paper, the discussion is about VAPT and Exploits & there is detail about the Penetration Testing process and Remote attack process. Further classification of Exploits based on various aspects is a little contribution proposed, ending with the Research work and Conclusion.
Vulnerability assessments and penetration tests are the main ways to discover and mitigate vulnerabilities in a system. Vulnerability assessments are typically conducted regularly, either independently or as part of a penetration test to complement the assessment's results. Vulnerability assessments can be performed manually or automatically. Manual assessments are generally performed by an individual who would use an automated tool to collect information that can later be manually analyzed. However, manual assessments may become more time-consuming as the number of assessment systems increases. Automatic assessments rely on tools to automatically scan and test the system for any vulnerability. These tools analyze the information they collect to generate results and reports. It can be accomplished through a number of different methods, including multiple static analysis techniques, such as source code analysis and syntax-based fuzzing, dynamic analysis techniques, such as binary instrumentation, and real-time tests. Defensive techniques include writing secure code, Performing Bound Checks, Runtime Instrumentation, and static and dynamic code analysis.

2. Literature Reviews

Vikash Kumar is a "robust intelligent zero-day cyber-attack detection technique" by Vikash Kumar and Ditipriya Sinha. The authors have enlightened the entire working, detection, and prevention of Zero Attacks. They define some algorithms to satisfy the agenda of detecting the Zero-Day Exploits with the help of fingerprints and signatures of the earlier known and identified exploits. They propped a robust system to detect the Zero Attack Exploits with the help of the highly updated network traffic of the earlier discovered Exploits. Also, for this approach, they preferred a stream of raw bytes capable enough to capture real-time traffic. The model is neither dependent on network nor source and destination-specific information. This model is the solution for earlier research that was limited and less reliable for detecting Zero-Day attacks. The case studies included in the proposal give a better vision of different variants of zero-day attacks like HVA(High Volume Attacks) and LVA(Low Volume Attacks). Apart from this, the proposal and the Case Studies discuss various vulnerabilities based on DoS or Buffer Overflow.

Analysis and Impact of Vulnerability Assessment and Penetration Testing, by Yugansh Khera, Deepansh Kumar, Sujay, Nidhi. in this research, the authors depicted dangers to the trustworthiness and privacy of data and assets expanded. To remain secure, associations perform VAPT to check the security stance of the framework. As we have gone through the writing study about VAPT techniques, it is observed that there are different devices accessible for

the recently developed weaknesses. This issue can be tended to by making instruments so adaptable that new assault marks can be added for weaknesses. To make VAPT results significant, it should focus on and clarify weaknesses with CVE numbers which can be purchased from industry-standard references like public weakness information base (NVD), normal weakness scoring framework (CVSS), open-source weakness information base (OSVDB), and so on, performing VAPT. Assailants are tracking down better approaches to sidestep security instruments, so new weaknesses are developing which should be tended to. Subsequently, existing apparatuses should be added with instruments to distinguish and evaluate.

3. Proposed Work

3.1. Remote Attacks

How can remote attacks happen? Remote attacks are possible for several reasons. For example, a hacker could use a trojan horse or virus to infiltrate your computer from an external.

Following is the block representation of steps included in any remote attack.

Fig. 1 Process of Remote Attack

In Fig. 1, it is to be explained that once the process of Reconnaissance is done, the major work to be done is all on exploits; first of all, the configuration is done, then the attack process is done, where the attacker finds a medium whether remote or physical for the attack to be successful. It exploits itself and holds on to the Trojan too. It may be hidden inside an image file or anything that lures the attention of the target and forces the target to access them.
Preventive measures that can be taken include:

- To be proactive. That means installing a good antivirus and firewall.
- Monitoring your computer and checking that all the programs on your computer are up-to-date with the latest security patches.
- One should also use strong passwords and change them often. It's also helpful to create different user accounts for each program, so you don't have to share passwords for everything.

3.2. Penetration Testing

Penetration testing is a control system assessment that mirrors an attack by a malicious individual. The test aims to identify how vulnerable your systems are to potential security breaches. Information gathered from this type of assessment can be used to make necessary adjustments to increase your company's overall security.

Penetration tests come in two different varieties: external and internal. External tests involve hackers or malicious individuals attempting to access sensitive information outside the company's firewall (i.e., customer data and credit card numbers). Internal tests involve staff members attempting to break through security measures within the company's network (i.e., phishing scams). Both types of tests provide feedback on how secure a system is but each has its advantages and disadvantages in terms of effectiveness and cost-effectiveness. An external penetration test might be cheaper but less effective than an internal one because it doesn't assess as much of the organization's network infrastructure as an internal test. Penetration testing is typically done by a third-party entity that will be permitted to test the system's security.

The primary goal of penetration testing is to identify any potential vulnerability on your website or network. The information gathered from the test can be used to make adjustments to increase your company's overall security. Continual assessment can help you protect your business more effectively and efficiently than if you were relying solely on one-time assessments. Pen tests are also cost-effective because they're generally much less expensive than hiring a cybersecurity firm for continual security checks. If one finds that a Vulnerability has been identified during penetration testing, you have the opportunity to take steps to fix the problem before malicious actors exploit it. It enhances your company's security and demonstrates that you care about safeguarding customer data and information.

Following is the explanation of the process included in any Penetration Testing done.

Fig. 2 Process of Penetration Testing

In the previous section, it was the discussion from the point of view of an attacker, but herein, the above figure is discussed how Penetration Testing is done. So, exploits have a defensive approach too, when it comes to terms of Penetration testing. Testers need to find the vulnerabilities and launch the exploits when any vulnerability is found in any atmosphere. So that the security program is processed and the exploitation is diagnosed with a suitable Security program. Post security, a report is being generated to update for future reference.

3.3. Classification of Exploits

Following is the classification of Exploits on Different measures.

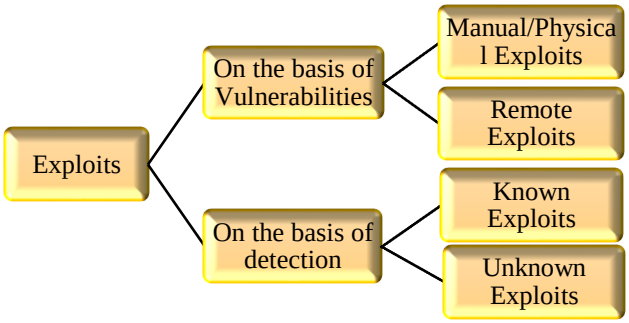

Fig. 3 Classification of exploits

The above tree representation is of the Classification of the Exploits.

Based on Vulnerabilities, Exploits can be divided into two parts

3.3.1. Manual Exploits

Also called Physical Exploits, the attack is done by physical means like being loaded in a pen drive, any image or CD, or any video sent to the target.

3.3.2. Remote Exploits

These exploits must go through a long process, like gaining the target's IP address, Port Forwarding, launching the Exploit, and then poisoning it on the Web.

Based on Detection, Exploits can be divided into two parts:

3.3.3. Known Exploits

The Exploit that has been already discovered by the Penetration Tester and the solution to those Exploit have also been found previously are known as Known Exploits. If an attack has been done on a global or personal level, the mode of attack and Vulnerability is detected. Hence it's easier for the tester to resolve the problems caused by the attack.

3.3.4. Zero-Day Exploits

The Exploits developed on the same day when any new software or any OS or update is launched known as Zero-Day Exploits. These exploits are considered dangerous as it might take longer to detect the Shell-Coding of the Exploit that has been used for the attack, resulting in more time to find a probable solution to tackle any such attack.

Difference between Zero-Day Attacks & Exploits

Zero-Day Attack	Zero-Day Exploit
Hackers could also discover software vulnerabilities, security firms or researchers, by the computer code vendors themselves or users. If discovered by hackers, Any exploit will be an unbroken secret for as long as attainable and can flow solely through the ranks of hackers till computer code or security firms become alert to it or of the attacks targeting it. Some outline these sorts of attacks as 'less than zero-day' attacks.	A zero-day exploit is once hackers profit from a computer code security flaw to perform a cyber attack, which security flaw is just illustrious to hackers, which means computer code developers don't have any clue to its existence and don't have any patch to mend it.

3.4. Top Examples of Zero-Day Attacks

- LinkedIn (June 2021)
- Alibaba(November 2019)
- Facebook(April 2019)
- MarriottInternational(September 2018)
- Yahoo(August 2013)

As per the analysis, every minute, a new bug, Vulnerability or loophole is detected by various hackers or the penetration tester, so the possibility of a new exploit taking birth is directly proportional to the detection of Vulnerability. Below is a graphical representation of zero-day attacks that happened over a decade

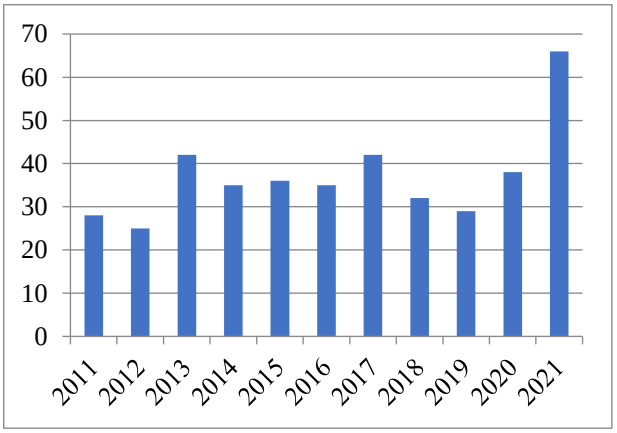

Fig. 4 Graphical representation of zero-day attacks in the past decade

4. Conclusion and Future Work

The overall study was about Vulnerability Assessment and Penetration Testing and their direct and indirect relations with Exploits. With the rising number of attacks, either remote or manual, attackers are capable enough to find new approaches for infection on various platforms. It is up to the Penetration Testers, the skills they also possess the awareness they spread among the users to make a safer browsing and Vulnerability-free environment in this world.

Being a current issue in Cybercrime and Cyberspace, this research area has a wide ground related to newer approaches to detecting Vulnerabilities and Exploits with the help of Artificial Intelligence and Machine Learning. As far as the Zero Day Exploits are concerned, one can have a deeper study and development of any such algorithm, which can give justice and help Testers instantly detect the mechanism and architecture of such attacks.

References

[1] Vikash Kumar, and Ditipriya Sinha, "A Robust Intelligent Zero Day Cyber Attack Detection Technique," *Complex & Intelligent Systems*, vol. 7, no. 5, pp. 2211-2234, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Andrew Johnson, and Rami J.Haddad, "Evading Signature Based Antivirus Software using Reverse Exploit Shell-Code," *In IEEE Southeastcon*, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Ajjarapu Kusuma Priyanka, and Siddemsetty Sai Smruthi, "Web Applicationvulnerabilities: Exploitation and Prevention," *Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 729-734, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Olufogorehan Tunde-Onadele et al., "A Study on Container Vulnerability Exploit Detection," *In IEEE International Conference of Cloud Engineering*, pp. 121-127, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[5] Xin Zhou, and Jianmin Pang, "Expdf Exploit Detection System Based on Machine Learning," *International Journal of Computational Intelligence Systems*, vol. 12, no. 2, pp. 1019 – 1028, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] Yugansh Khera et al., "Analysis and Impact of Vulnerability Assessment and Penetration Testing," *International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, pp. 525-530, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[7] Jukka Ruohonen, "Classifying Web Exploits with Topic Modelling," *In International Workshop on Database and Expert Systems Applications, IEEE*, pp. 93-97, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[8] Tiffany Bao et al., "Your Exploit is Mine-Automatic Shellcode Transplant for Remote Exploits," *In IEEE Symposium on Security and Privacy*, pp. 824-839, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[9] Richard Ciancioso, Danvers Budhwa, and Thaierhayajneh, "A Framework for Zero-Day Exploit Detection and Containment," *IEEE 3rd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress*, pp. 663-668, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[10] Prashant S. Shinde, and Prof. Shrikant B. Ardhapurkar, "Cyber Security Analysis Using Vulnerability Assessment and Penetration Testing," *In IEEE Sponsored World Conference on Futuristic Trends in Research and Innovation for Social Welfare*, pp. 1-5, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[11] Ivan Nikolaev, Martin Grill, and Veronica Valeros, "Exploit Kit Website Detection Using HTTP Proxy Logs," *In IEEE ACM International Conference Proceeding Series*, pp. 120-125, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[12] Phongphun kijsanayothin, and Rattikorn Hewett, "Exploit Based Analysis Attack Models," *IEEE 12th International Symposium on Network Computing and Applications*, pp. 1-4, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[13] Deshen Fu, and Feiyue Shi, "Buffer Overflow Exploit and Defensive Techniques," *In IEEE 4th International Conference on Multimedia and Security*, pp. 87-90. 2012. [CrossRef] [Google Scholar] [Publisher Link]

[14] EC-COUNCIL, *CEH-Ethical Hacking and Countermeasures*, vol. 1.

[15] David Kennedy et al., *Metasploit- A Complete Penetration Testing Guide*, pp. 1-332, 2011. [Publisher Link]

[16] The Offensive Security, 2020. [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/completing-exploit/

[17] Improving Vulnerability Remediation Through Better Exploit Prediction, 2020. [Online]. Available: https://academic.oup.com/cybersecurity/article/6/1/tyaa015/5905457

[18] 2020. [Online]. Available: https://www.avast.com/c-exploits#gref

[19] Graphology of Exploits, 2020. [Online]. Available: https://research.checkpoint.com/2020/graphology-of-an-exploit-volodya/