OPTIMIZING CYBER DEFENSE EVALUATION THROUGH THREAT-BASED ADVERSARY EMULATION TECHNIQUES

[1]S. Vijay Kumar, [2]M. Anjali
[1]Assistant Professor, [2]MCA Student
Department Of MCA Student
Sree Chaitanya College of Engineering, Karimnagar

ABSTRACT

Attackers, including Advanced Persistent Threat (APT) attackers, use ever-more-sophisticated methods to breach organisations. Such attacks often aim to get vital data by taking advantage of endpoints. Organisations may use offensive security activities for defence evaluation and security controls. Penetration testing and red teaming are the most crucial, but they often need a lot of resources and take longer to complete. Furthermore, stealthy attacks have not been successfully mitigated by conventional Venerability Assessment and Penetration Testing (VAPT), despite its effectiveness in mitigating known assaults. Although VAPT views the whole offsec as an acting problem, an attacker must really deal with uncertainty when launching attacks in the real world. In this study, we describe an adversary emulation strategy that takes into account planning as a significant component of each assault phase, based on the MITRE ATT&CK opponent emulation plan. For defence evaluation, the method imitates the adversary using covert attack vectors and pathways. We selected over 40 strategies from ATT&CK, implemented their mitigation on target computers, and then launched attacks against each technique in order to evaluate the effectiveness of the defence. We demonstrate that attack routes and payloads created with our method are powerful enough to circumvent endpoint security measures. In order to assess organisational security readiness, this method offers a unique setting for cyber defenders to think like adversaries and develop novel attack pathways and vectors. With the least amount of resources available to the company, this procedure creates a unique atmosphere to broaden the assault landscape perspective and defence evaluation.

1. INTRODUCTION

Threat of cyber attacks continues to increase as cybercriminals become more sophisticated and organizations rely more heavily on technology. Recent stats show a drastic increase in cyber-attacks targeting endpoints. Such as servers, cell phones, and workstations. Endpoints are considered as the most valuable and vulnerable devices. One example is the use of ‘‘business email compromise’’ (BEC) [1] attacks, in which attackers impersonate executives or vendors to trick employees into providing sensitive information. Another example is the use of ransom ware, in which attackers encrypt a company’s data and demand a ransom payment to restore access. The threat of cyber attacks continues to increase as cybercriminals become more sophisticated and organizations rely more heavily on technology. Advancement of technology has

posed increased threats as the number of endpoint nodes are increasing so endpoints security must be prioritized. Thus endpoint security is considered as the future of cyber security [2].

Many organizations conduct penetration testing periodically to determine the presence of potential vulnerabilities [3]. Such testing aims to evaluate the security controls adopted by the organization. Sample penetration tools and methods are discussed in [4]. Usually, organizations have adversary simulation teams on board to run these offensive activities as a ‘‘cat and mouse’’ game. One team is responsible for launching attacks and the other team is responsible for detecting them, that’s how they evaluate security. This proved to be an effective approach, with one drawback: the red team’s operations are resource exhaustive. In a changing threat landscape, where attackers are employing increasingly sophisticated attacks, organizations are more prone to cyber attacks. Modern solutions, such as models for vulnerability scanning, vulnerability management, vulnerability mitigation and Vulnerability Assessment and Penetration Testing (VAPT), rely on ‘‘known threats’’, while we often see attackers exploiting unknown and zero-day vulnerabilities. Recent solutions tried to alleviate this situation by exploring control based evaluation [5], but this approach is still prone to zero days attacks.

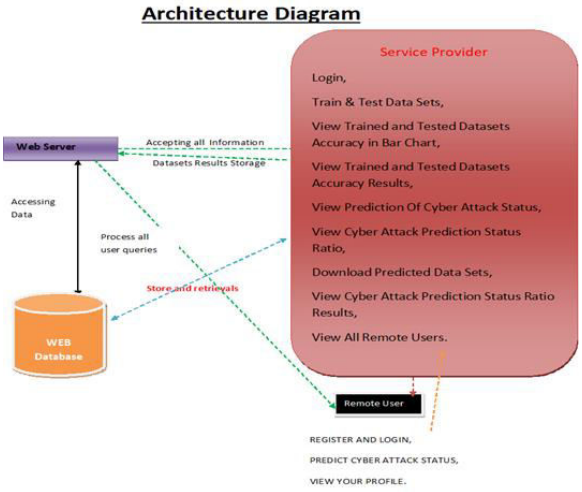
Adversary emulation in cyber security is a technique used to simulate real-world cyber attacks in order to test an organization’s security defenses. The process typically involves simulating the tactics, techniques, and procedures (TTPs) of known or hypothetical attackers in order to identify vulnerabilities and measure the effectiveness of security controls. This can include simulating phishing campaigns, malware attacks, and other types of cyber threats. The goal of adversary emulation is to improve an organization’s security posture by identifying and mitigating potential vulnerabilities before they can be exploited by real attackers. It is also known as ‘‘red teaming’’ or ‘‘threat emulation’’. It can be done internally by the organization’s security team or by hiring an external company to conduct the testing. In this paper, we show that employing threat-based emulation is an effective solution for evaluating security from an adversarial perspective, rather than performing full-scale red team operations.

In this research article, we introduce a threat-based adversary emulation approach that addresses the limitations of traditional penetration testing and red teaming techniques and provides a more effective and realistic simulation of real world attacks. Our approach utilizes Mitre ATT&CK to learn TTPs to continuously adapt the attack simulation to the organization’s evolving security posture. One of the key advantages of our approach is the ability to provide a more realistic simulation of real-world attacks, as it allows the red team to mimic the behavior of advanced persistent threats (APTs)and other sophisticated attackers. Additionally, by continuously adapting the attack simulation, our approach allows organizations to stay

ahead of evolving threats and improve their overall security posture. For an operator who is conducting threat-based adversary emulation, it's necessary to know about malware classes. Malware classifications are given in Table 1. Most common among them are droppers which assist adversaries to download any type of malware. Furthermore, we propose a threat-based adversary emulation approach with payload generation algorithms, which consists of unique agnostic methods, with similar capabilities which are carried by real-world attack vectors. Moreover, it can be used to generate new attack paths. We provide four algorithms for generating stealthy attack vectors and use them to emulate adversarial TTPs. During experimentations, we generated different payloads and tested them against endpoint security solutions for the prevention and detection of threats such as EDR/AV (endpoint detection and response/ antivirus). That's how we evaluated the effectiveness of stealthy payloads. We evaluated our approach and mapped test case payloads according to ATT&CK framework, which is a worldwide free-to-use database of adversarial knowledge based on TTP. Moreover, this approach has the ability to recreate new methods for similar techniques on ATT&CK. We evaluated our approach and algorithms against endpoint security and concluded that this approach is effective for launching dynamic threats as well as for ''emerging threats'' assessment.

For this research paper, we have considered Windows system and Linux (privilege escalation only), in table 2attack vector details are provided in form of payloads that are used in this research. More specifically we have used portable executable files, Open XML files and malicious scripts (CMD/PS1/Bat) for the experiment. Open XML files are zip archive files containing different XML files such asstyling and structure files. The customized raw malicious payload in .bin file is used to embed with macros. Mentioned attack vectors in table 2, can be generated by algorithms in section IV.

2. SYSTEM ARCHITECTURE



3. EXISTING SYSTEM

The contribution of this paper is the introduction of an effective process for threat-based adversary emulation that provides output as quantifying the overall integrity, coverage, and rigor of security controls. Additionally, our approach allows for more efficient use of resources and focusing on manual efforts in areas that are most likely to be targeted by attackers. In this section, we review existing literature on VAPT and Mitre ATT&CK and controls-based security.

When organizations started realizing that attackers tend to exploit vulnerabilities present in our network, they came up with different methods for countering them. One of them was keeping systems patched. Adversaries were still unbeatable. ‘‘Best Offense is the Best Defense’’, Organizations started thinking from the perspective of attackers and started exploiting vulnerabilities before attackers do so and fix vulnerabilities. This approach is called ‘‘Pen-testing’’. Pen-testing has evolved over time and is now usually referred to as ‘‘VAPT’’. This approach is adequate for small and mediumsize organizations for countering beginner and intermediate level attackers. Network attacks are elaborated here [6], [7]. VAPT helps organizations to assess how effective their security solutions are. In [8], the authors provide an overview of various techniques used in vulnerability assessment and penetration testing. Past researches [9], [10] considered vulnerability management and continuous installing of patches as a solution for securing organization. Recent research, such as the penetration testing approach for exploiting mobile devices [11], considered testing of common security controls.

Almost all these solutions are prone to different types of attacks such as zero days and social engineering. Many organizations conduct Red Team exercises to evaluate their security. Such penetration testing and red team operations are thoroughly discussed in [12] and [13]. Detailed Discussion on APT is explained in [14]. Recent research has also considered re-developing existing popular pen-testing suites [15]. Such types of implant redevelopment techniques are widely used by ethical hackers to conduct testing of security mechanisms. We have extended this approach and integrated it into adversary emulation. A comparison of pentesting and adversary emulation is given in table 3.

Such real-world attack emulation (adversary emulation) provides*live fire* training opportunities for analysts. Threat hunting vendor FireEye [16] has explained well how to extract techniques from IOCs and logs.We used this approach in adversary emulation and extended it with mappings on MITRE ATT&CK. Figure 1 explains, how techniques look like. We integrated this into our approach during the threat intelligence phase with the aid of open-source projects which make work easy by quickly analyzing threat reports. Automated penetration testing based on a threat model [17] is a recent work on penetration testing based on threats specific to an organization. However, this has limited scope and makes it prone to zero days and APT threats. Penetration testing with Metasploit is widely used by different organizations and is well explained in [18]. Moreover, it discusses different methods for evading security controls to make penetrating close to real-world attacks [19].

Adversary emulation assessments offer defenders the ability to view their networks from the point of view of an adversary. In [19] and [20], the authors have discussed the formal use of open-source tools such as ‘‘Atomic Red Team’’ to conduct adversary

emulation and build test cases against TTPs from MITRE. We derived our planning approach from this paper. This research article [19], [21] is not agile in working with a lot of attack techniques and has a limited scope to emulate adversaries. For example, if we want to launch APT41 attack cases. Some questions arise, such as how to order the sequence of attack cases. How to build attack chains and use all collected information after emulation for security awareness of the organization. The proposed approach is a continuation of our previous research
work [22], [23], [24], [25].

MITRE has provided some sample attack plans which depict the practical use of knowledge base [26]. We have used a modified form of these plans to incorporate the latest methods and techniques, in the ‘‘organizing and analysis’’ phase of our approach. ATT&CK knowledge base has diverse applications. One of them is the use of knowledge bases as threat intelligence. During this phase, noticeable action of the adversary can be mapped on different tactics on ATT&CK. There are many platforms, most of them are open source and support ATT&CK mappings. Such as MISP [27] and OpenCTI [28].We have leveraged this and used it in a hybrid mode to learn more about specific threats and adversarial techniques (from organizations sharing threat Intelligence).

Disadvantages

• The complexity of data: Most of the existing machine learning models must be able to accurately interpret large and complex datasets to detect Cyber Threat.

• Data availability: Most machine learning models require large amounts of data to create accurate predictions. If data is unavailable in sufficient quantities, then model accuracy may suffer.

• Incorrect labeling: The existing machine learning models are only as accurate as the data trained using the input dataset. If the data has been incorrectly labeled, the model cannot make accurate predictions.

4. PROPOSED SYSTEM

In this research article, we introduce a threat-based adversary emulation approach that addresses the limitations of traditional penetration testing and red teaming techniques and provides a more effective and realistic simulation of real world
attacks. Our approach utilizes Mitre ATT&CK to learn TTPs to continuously adapt the attack simulation to the organization’s evolving security posture. One of the key advantages of our approach is the ability to provide a more realistic simulation of real-world attacks, as it allows the red team to mimic the behavior of advanced persistent threats (APTs) and other sophisticated attackers. Additionally, by continuously adapting the attack simulation, our approach allows organizations to stay ahead of evolving threats and improve their overall security posture. For an operator who is conducting threat-based adversary emulation, it’s necessary to know about malware classes. Most common among them are droppers which assist adversaries to download any type of malware.

Furthermore, we propose a threat-based adversary emulation approach with payload

generation algorithms, which consists of unique agnostic methods, with similar capabilities which are carried by real-world attack vectors. Moreover, it can be used to generate new attack paths.We provide four algorithms for generating stealthy attack vectors and use them to emulate adversarial TTPs. During experimentations, we generated different payloads and tested them against endpoint security solutions for the prevention and detection of threats such as EDR/AV (endpoint detection and response/ antivirus). That's how we evaluated the effectiveness of stealthy payloads. We evaluated our approach and mapped test case payloads according to ATT&CK framework, which is a worldwide free-to-use database of adversarial knowledge based on TTP. Moreover, this approach has the ability to recreate new methods for similar techniques on ATT&CK. We evaluated our approach and algorithms against endpoint security and concluded that this approach is effective for launching dynamic threats as well as for ''emerging threats'' assessment.

Advantages

1. The system proposes the agnostic threat-based adversary emulation approach Which involves simulating a wide range of potential attacks, including both known and unknown threats.
2. The goal of the proposed approach is to identify vulnerabilities and measure the effectiveness of security controls in a more realistic and comprehensive way. It allows organizations to test their defenses against a wide range of potential threats and better understand their overall security posture. It also allows organizations to stay ahead of evolving threats by continuously testing and updating their defenses.

5. IMPLEMENTATION

Modules Description

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Train & Test Data Sets, View Trained and Tested Datasets Accuracy in Bar Chart, View Trained and Tested Datasets Accuracy Results, View Prediction Of Cyber Attack Status, View Cyber Attack Prediction Status Ratio, Download Predicted Data Sets, View Cyber Attack Prediction Status Ratio Results, View All Remote Users..

View and Authorize Users

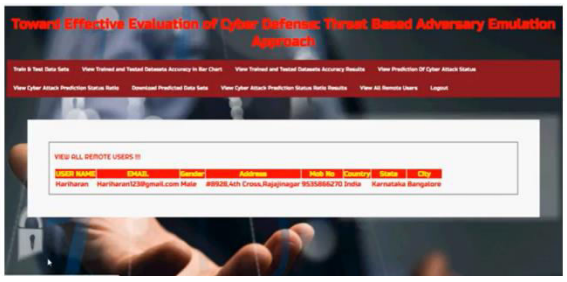
In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

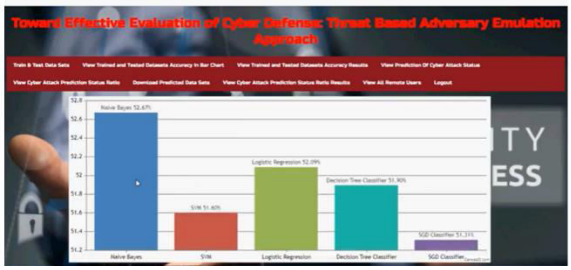
Remote User

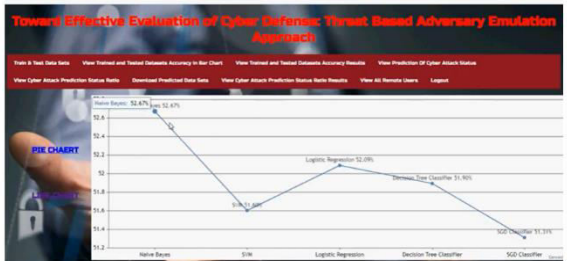
In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers,

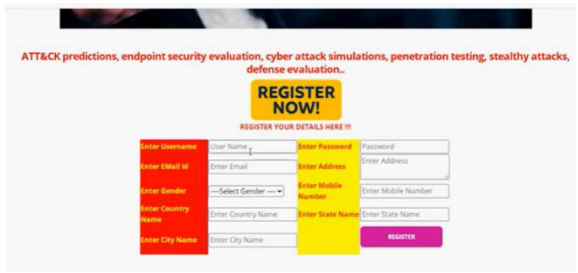
their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT CYBER ATTACK STATUS, VIEW YOUR PROFILE.

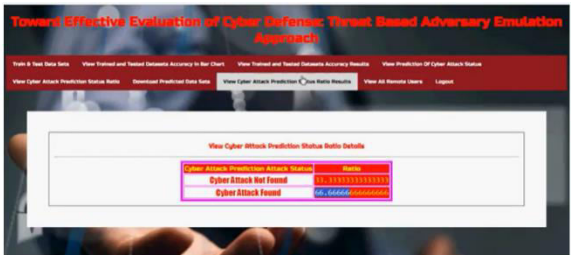
6. RESULTS



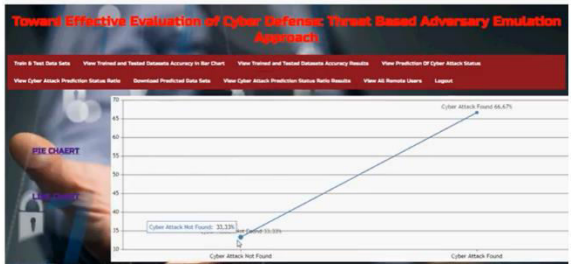


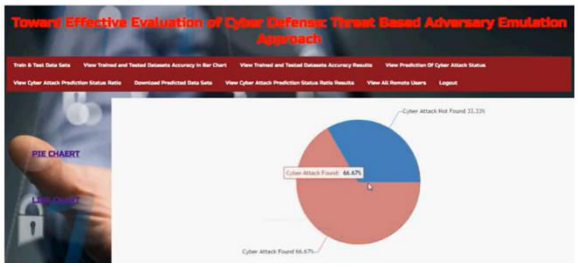






\





7. CONCLUSION

We require the same kinds of techniques and tactics that an adversary in the actual world would employ to assess security controls, with a greater focus on unidentified threats, in order to evaluate security architecture and controls. In order to construct an opponent emulation plan, collect intelligence, conduct pre-adversary emulation activities, evaluate tactics, and carry out plans, we provide a novel set of activities in this work. Our suggested method is centred on mimicking actual attacks while being constrained by a particular threat or enemy. By regularly testing and upgrading their defences, organisations may stay ahead of developing threats and obtain a better understanding of their overall security posture. It also enables them to test their defences against a wide range of potential threats. The MITRE APT strategy prompted us to take certain activities. We provide three methods for creating payloads that can get past security measures that are often put in place by businesses. We demonstrated the effectiveness of our method in assessing one's security against real APT attacks through a full-scale experiment. We hope to develop a modular automated system in the

future that can quickly transition between attack and defence evasion components.

REFERENCES

[1] S. Herbert-Lowe, ‘‘8 reasons why business email compromise is a risk for trustees,’’ *Australas. Law Manag. J.*, pp. 1–3, Mar. 2022. [Online]. Available: https://search.informit.org/doi/10.3316/informit.20220602067914

[2] B. Canner. (2020). *Here is Why Endpoint Security is Important to Your Enterprise*. [Online]. Available: https://solutionsreview.com/endpointsecurityhereiswhyendpointsecurityisimportantforyourenterprise

[3] M. Denis, C. Zena, and T. Hayajneh, ‘‘Penetration testing: Concepts, attack methods, and defense strategies,’’ in *Proc. IEEE Long Island Syst., Appl. Technol. Conf. (LISAT)*, Apr. 2016, pp. 1–6.

[4] H. M. Z. A. Shebli and B. D. Beheshti, ‘‘A study on penetration testing process and tools,’’ in *Proc. IEEE Long Island Syst., Appl. Technol. Conf. (LISAT)*, May 2018, pp. 1–7.

[5] D. Olifer, N. Goranin, A. Kaceniauskas, and A. Cenys, ‘‘Controls-based approach for evaluation of information security standards implementation costs,’’ *Technol. Econ. Develop. Economy*, vol. 23, no. 1, pp. 196–219, 2017.

[6] X. Cai, K. Shi, K. She, S. Zhong, Y. C. Soh, and Y. Yu, ‘‘Performance error estimation and elastic integral event triggering mechanism design for T–S fuzzy networked control system under DoS attacks,’’ *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 4, pp. 1327–1339, Apr. 2023.

[7] X. Cai, K. Shi, K. She, S. Zhong, and Y. Tang, ‘‘Quantized sampled-data control tactic for T–S fuzzy NCS under stochastic cyber-attacks and its application to truck-trailer system,’’ *IEEE Trans. Veh. Technol.*, vol. 71,no. 7, pp. 7023–7032, Jul. 2022.

[8] P. S. Shinde and S. B. Ardhapurkar, ‘‘Cyber security analysis using vulnerability assessment and penetration testing,’’ in *Proc.World Conf. Futuristic Trends Res. Innov. Social Welfare (Startup Conclave)*, Feb. 2016, pp. 1–5.

[9] S. Shah and B. M. Mehtre, ‘‘A modern approach to cyber security analysis using vulnerability assessment and penetration testing,’’ *Int. J. Electron. Commun. Comput. Eng.*, vol. 4, no. 6, pp. 47–52, 2013.

[10] S. Shah and B. M. Mehtre, ‘‘A reliable strategy for proactive self-defence in cyber space using VAPT tools and techniques,’’ in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res.*, Dec. 2013, pp. 1–6.

[11] I. L. Aller, J. M. R. Lopez, and L. A. V. Martinez, ‘‘Towards lightweight mobile pentesting tools to quickly assess machine security levels,’’ *IEEE Latin Amer. Trans.*, vol. 17, no. 7, pp. 1116–1123, Jul. 2019.

[12] G. Weidman, *Penetration Testing: A Hands-On Introduction to Hacking*. San Francisco, CA, USA: No Starch Press, 2014.

[13] B. Clark, *RTFM: Red Team Field Manual*, J. Vest, Ed. Createspace Independent Publishing Platform, Feb. 2014.

[14] T. Wrightson, *Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization*. New York, NY, USA: McGraw-Hill, 2014.

[15] N. T. Pages, ‘‘Module development in metasploit for pentesting,’’ M.S. thesis,

Universitat Politècnica de Catalunya, Barcelona, Spain, 2019.