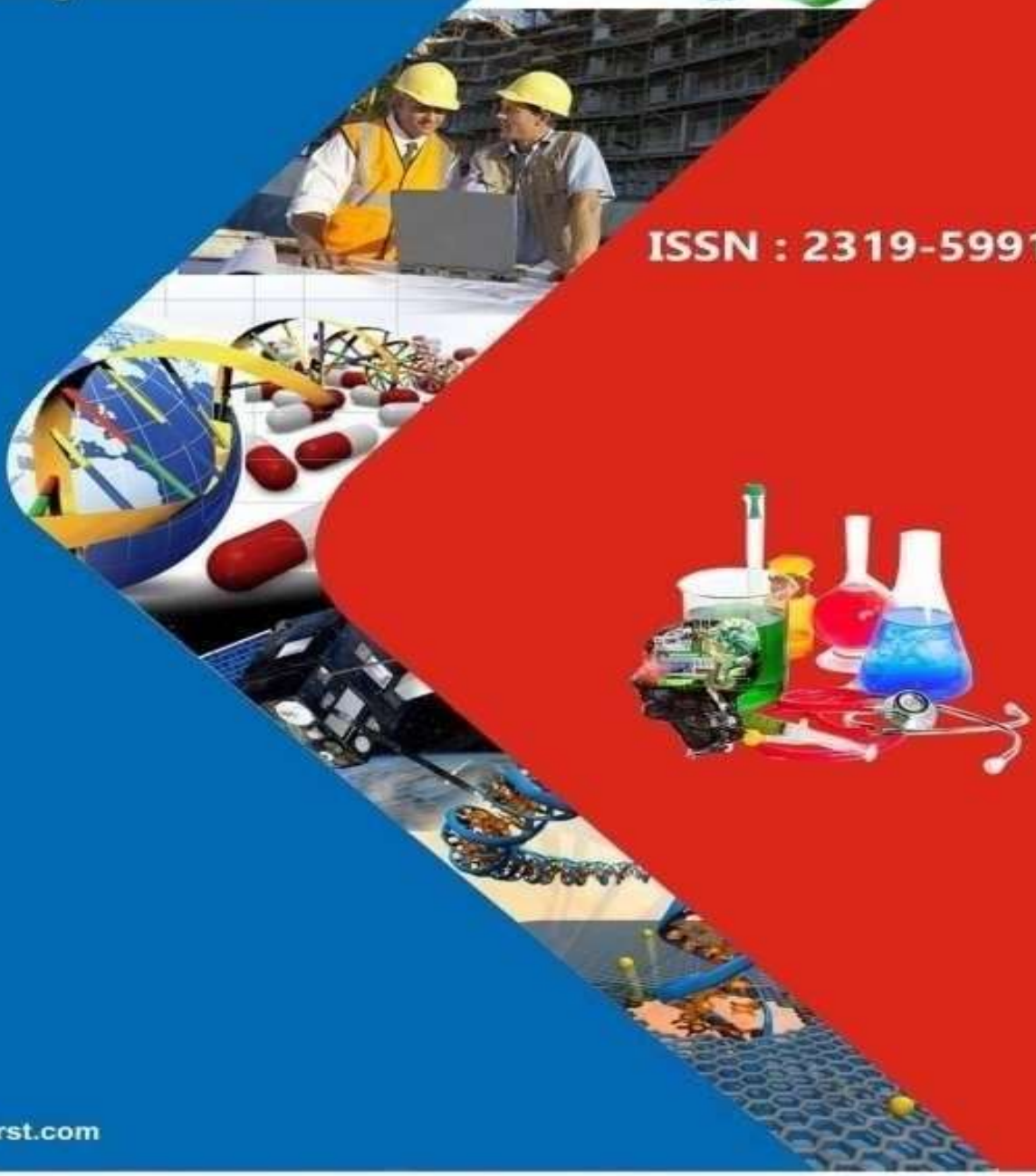
International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991



www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp599-609

Vol. 21, Issue 2, 2025

ENHANCING CYBER DEFENSE EVALUATION THROUGH THREAT-BASED ADVERSARY EMULATION

[1] *Shaik Farooq Basha, MCA Student, Department Of MCA*

[2]*K Muddu Swamy, M.Tech, Assistant Professor ,Department Of MCA*

[12]*Dr KV Subba Reddy Institute of Technology, Dupadu, Kurnool*

ABSTRACT

Attackers compromise organizations with increasingly sophisticated ways, such as Advanced Persistent Threat (APT) attackers. Usually, such attacks have the intention to exploit endpoints to gain access to critical data. For security controls and defense evaluation, organizations may employ offensive security activities. The most important one is penetration testing and red teaming, but such operations are usually resource exhaustive and extend over a longer period of time. Furthermore, traditional Venerability Assessment and Penetration Testing (VAPT) works effectively in the mitigation of known attacks but did not prove to be effective against stealthy attacks. VAPT considers the whole offsec as an acting problem but in reality, an attacker has to deal with uncertainty while conducting real-world attacks. In this paper, we are presenting an adversary emulation approach based on MITRE ATT&CK adversary emulation plan with consideration of planning as a major part of each attack phase. The approach utilizes stealthy attack vectors and paths to emulate adversary for defense evaluation. For effective defense evaluation, we picked more than 40 techniques from ATT&CK, deployed their mitigation on target machines, and then launched attacks against all those techniques. We show that attack paths and payloads generated using our approach are strong enough to evade security controls at endpoints. This approach provides a special environment for cyber defenders to think like adversary, and create new attack vectors and paths to evaluate organizational security preparedness. This process constructs a special environment to expand the attack landscape view and defense evaluation with minimal resources for the organization

.

1. INTRODUCTION

As organisations depend more on technology and thieves grow more skilled, the threat of cyberattacks keeps growing. Cyberattacks targeting endpoints have dramatically increased, according to recent statistics. like desktops, servers, and cell phones. Endpoints are thought to be the most important and susceptible devices. The use of "business email compromise" (BEC) [1] attacks is one instance, wherein hackers pose as executives or suppliers to fool staff members into divulging private information. The use of ransomware, where hackers encrypt a company's data and demand a ransom to unlock it, is another example. As organisations depend more on technology and thieves grow more skilled, the threat of cyberattacks keeps growing. Since there are more endpoint nodes due to technological advancements, endpoint security needs to be given top priority. Endpoint security is

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp599-609
Vol. 21, Issue 2, 2025

therefore regarded as the cyber security of the future [2].

To find out if there are any possible vulnerabilities, many organisations periodically perform penetration testing [3]. The purpose of this examination is to assess the security measures that the company has implemented. In [4], sample penetration techniques and tools are covered. In order to conduct these offensive activities as a "cat and mouse" game, organisations typically have adversary simulation teams on board. To assess security, one team is in charge of initiating assaults, while the other team is in charge of identifying them. This strategy worked well, but there is a catch: the red team's operations require a lot of resources. Organisations are more vulnerable to cyberattacks in a dynamic threat environment where attackers are using more complex tactics. While attackers frequently take advantage of undiscovered and zero-day vulnerabilities, modern solutions like models for vulnerability scanning, vulnerability management, vulnerability mitigation, and Vulnerability Assessment and Penetration Testing (VAPT) rely on "known threats." By investigating control-based evaluation, recent solutions attempted to mitigate this issue [5], although this strategy is still vulnerable to zero-day attacks.

In cyber security, adversary emulation is a method for testing an organization's security defences by simulating actual cyberattacks. To find vulnerabilities and gauge how well security controls are working, the approach usually entails mimicking the tactics, techniques, and procedures (TTPs) of actual or potential attackers. This can involve mimicking virus attacks, phishing attempts, and other online dangers. By spotting and fixing such weaknesses before actual attackers can take advantage of them, adversary emulation aims to strengthen an organization's security posture. It is also referred to as "threat emulation" or "red teaming." The organization's security team may choose to carry out the testing internally or by contracting with a third party. In contrast to conducting full-scale red team operations, we demonstrate in this work that using threat-based emulation is a viable method for assessing security from an adversarial viewpoint.

In this study, we present a threat-based adversary emulation method that overcomes the drawbacks of conventional red teaming and penetration testing strategies and offers a more accurate and realistic representation of actual attacks. Our method continuously adjusts the attack simulation to the organization's changing security posture by using Mitre ATT&CK to learn TTPs. Our method's ability to simulate real-world attacks more realistically is one of its main advantages; it enables the red team to imitate the actions of sophisticated attackers and advanced persistent threats (APTs). Furthermore, our method enables organisations to enhance their overall security posture and stay ahead of changing threats by continuously modifying the attack simulation. Understanding malware classifications is essential for an operator performing threat-based adversary simulation. Malware classifications are given in Table 1. The most prevalent of these are droppers, which help adversaries download

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp599-609
Vol. 21, Issue 2, 2025

malware of any kind. Additionally, we provide a threat-based adversary emulation strategy using payload generation algorithms. This strategy comprises of distinct agnostic techniques that possess comparable capabilities to those of actual attack vectors. It can also be utilised to create new avenues of assault. In order to simulate adversarial TTPs, we offer four strategies for creating covert attack paths. We created many payloads during the experiments and evaluated them against endpoint security programs like EDR/AV (endpoint detection and response/antivirus) to prevent and identify attacks. We assessed the efficacy of covert payloads in this manner. The ATT&CK framework, a global free-to-use database of adversarial knowledge based on TTP, was used to assess our methodology and map test case payloads. Furthermore, this method can be used to replicate novel approaches for comparable procedures on ATT&CK. After comparing our methodology and algorithms to endpoint security, we came to the conclusion that this strategy works well for both launching dynamic threats and assessing "emerging threats."

Linux (privilege escalation only) and Windows systems were taken into consideration for this research article. Table 2 provides information on the attack vector in the form of payloads employed in this study. More precisely, for the experiment, we used malicious scripts (CMD/PS1/Bat), portable executable files, and Open XML files. Zip archive files that contain various XML files, including style and structural files, are known as open XML files. Macros are used to incorporate the customised raw malicious payload in a.bin file. Algorithms in section IV can produce the attack vectors mentioned in table 2.

This is how the remainder of the paper is structured: In section II, the immediate section presents relevant work on adversary emulation and various penetration testing and vulnerability assessment methodologies. A formal model for threat-based adversary emulation is presented in section III. A prototype of our paradigm is implemented algorithmically in section IV. We provide the findings of the assessment of our methodology in sections V and VII. In section VIII, we wrap up this article with some closing thoughts and suggestions for future developments.

2. LITERATURE SURVEY

‘‘Penetration testing: Concepts, attack methods, and defense strategies,’’

M. Denis, C. Zena, and T. Hayajneh,

Penetration testing identifies security flaws and aids in network security. Examine various facets of penetration testing in this paper, such as tools, attack techniques, and defence tactics. More precisely, we used devices, virtualised systems, private networks, and tools to conduct various penetration tests. We mostly used the Kali Linux suite of tools. We conducted the following attacks: traffic sniffing, WPA Protected WiFi hacking, smartphone penetration testing, hacking phones' Bluetooth, Man-in-the-Middle attack, spying (gaining access to a PC microphone), hacking remote PCs via IP and open ports using an advanced port scanner, and hacking smartphones. After that, a summary and

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp599-609
Vol. 21, Issue 2, 2025

discussion of the findings follow. Additionally, the paper described the specific procedures and techniques used to carry out these attacks.

.

‘‘A study on penetration testing process and tools,’’

H. M. Z. A. Shebli and B. D. Beheshti,

Information is more susceptible than ever, and new security threats are brought about by every technological advancement, necessitating the development of new security solutions. By carefully exposing an IT infrastructure's flaws, penetration testing is done to assess its security. It also aids in evaluating the effectiveness of the defence mechanisms, methods, and policies that are currently in place. To detect threats and control them in order to meet increased security requirements, penetration testing is carried out on a regular basis. This paper addresses the significance of penetration testing, the elements and factors taken into account when performing a penetration test, a survey of the tools and processes used, the role of penetration testing in implementing IT governance in an organisation, and, lastly, the professional ethics that the penetration test team should possess.

‘‘Controls-based approach for evaluation of information security standards implementation costs,’’

D. Olifer, N. Goranin, A. Kaceniauskas, and A. Cenys,

The average cost of a single information security and data protection breach has doubled in 2015, according to a PricewaterhouseCoopers report (Pricewaterhouse Coopers 2015). According to PricewaterhouseCoopers (2016), the number of organisations reporting major breaches has also increased, rising from 9% in 2015 to 17% in 2016. Criminals employ a variety of tactics to accomplish their objectives, beginning with social engineering (phishing, whaling), and concluding with the installation of malware (like ransomware) on target computers. Attacks like the one on the Central Bank of Bangladesh, the one on the CEO of Mattel, and the one on the state-run Government bank ATM in Thailand demonstrate how well-prepared and well-organised criminals are, and how much time and money they invest in planning their attacks. Organisations must adopt sophisticated security solutions that can guarantee the necessary level of information security at reasonable prices and adhere to security in depth principles in order to defend themselves. However, the lack of defined cost-benefit approaches and the difficulty of comparing IT security solutions in light of current uncertainty make evaluating the costs and benefits of information security difficult. Current approaches are focused on certain standard implementations, environment lifecycles, or procedures. Because of this, reusing existing approaches is a challenging undertaking and does not cover all necessary security areas. In an attempt to address this problem, we have put forth a novel approach to evaluating the implementation costs of information standards that is based on information security rules.

3. SYSTEM ANALYSIS AND DESIGN

EXISTING SYSTEM

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp599-609
Vol. 21, Issue 2, 2025

This paper's contribution is the creation of a successful threat-based adversary emulation procedure that yields results that quantify the overall rigour, coverage, and integrity of security mechanisms. Furthermore, our method makes it possible to deploy resources more effectively and concentrate manual labour in places where attackers are most likely to target. This section examines the body of research on controls-based security, VAPT, and Mitre ATT&CK.

Organisations developed several strategies to combat network vulnerabilities after they began to realise that attackers frequently take advantage of them. Maintaining patched systems was one of them. The opposition remained invincible. Because of the adage "Best Offence is the Best Defence," organisations began to consider themselves as attackers, exploiting weaknesses before they were discovered and fixing them. This method is known as "pen-testing." Over time, pen-testing has changed and is now often known as "VAPT." Small and medium-sized businesses can effectively combat novice and intermediate attackers with this strategy. This article elaborates on network assaults [6], [7]. VAPT assists businesses in evaluating the efficacy of their security measures. The authors of [8] give a summary of the several methods used in penetration testing and vulnerability assessment. Vulnerability monitoring and patching continuously were examined in earlier studies [9], [10] as ways to secure an organisation. Testing of common security controls was taken into consideration in recent research, such as the penetration testing technique for mobile device exploitation [11].

Nearly all of these systems are vulnerable to various forms of assaults, including social engineering and zero days. Red Team exercises are a common way for organisations to assess their security. In [12] and [13], such penetration testing and red team operations are covered in detail. [14] provides a detailed discussion of APT. Recent studies have also looked on revamping well-known pen-testing programs [15]. Ethical hackers frequently utilise these kinds of implant redevelopment techniques to test security features. We have taken this strategy a step further and incorporated it into adversary emulation. Table 3 presents a comparison between adversary emulation and pentesting.

For analysts, such opponent simulation, or real-world attack emulation, offers opportunity for live fire training. FireEye [16], a threat hunting company, has provided clear instructions on how to extract methods from IOCs and logs. We enhanced this strategy using mappings on MITRE ATT&CK and utilised it in adversarial emulation. Figure 1 illustrates the appearance of techniques. With the help of open-source initiatives that facilitate work by rapidly analysing threat data, we incorporated this into our strategy during the threat intelligence phase. One new development in penetration testing based on organization-specific risks is automated penetration testing based on a threat model [17]. This has a narrow reach, though, and is vulnerable to APT and zero-day threats. Many organisations utilise Metasploit penetration testing, which is thoroughly described in [18]. Additionally, it

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp599-609
Vol. 21, Issue 2, 2025

explores various ways to circumvent security measures to make penetrations more akin to actual attacks [19].

Defensors can see their networks from the perspective of an attacker by using adversary emulation assessments. The formal use of open-source tools like "Atomic Red Team" to carry out adversary emulation and create test cases against MITRE TTPs was covered by the authors in [19] and [20]. This report served as the basis for our planning strategy. This study article [19], [21] has a limited scope to mimic opponents and is not agile when working with several attack strategies. For instance, say we wish to initiate APT41 assault scenarios. Some queries come up, such how to arrange the assault case sequence. How to construct attack chains and apply all gathered data for the organization's security awareness following emulation. The suggested methodology is an extension of our earlier studies [22], [23], [24], and [25].

A few sample attack plans that illustrate the useful application of knowledge bases have been made available by MITRE [26]. In the "organising and analysis" stage of our strategy, we have adapted these plans to include the most recent strategies and tactics. Applications for the ATT&CK knowledge base are numerous. Using knowledge bases to gather threat intelligence is one of them. The adversary's observable actions during this phase can be translated onto various ATT&CK techniques. There are numerous platforms that enable ATT&CK mappings, the majority of them are open source. like OpenCTI [28] and MISP [27]. To learn more about particular risks and adversary tactics, we have taken advantage of this and utilised it in a hybrid fashion (from organisations sharing threat Intelligence).

.

Disadvantages

• Data complexity: To identify cyber threats, the majority of machine learning models now in use need to be able to correctly analyse sizable and intricate datasets.

• Data availability: In order to produce precise predictions, the majority of machine learning models need a lot of data. The accuracy of the model may degrade if data is not accessible in large enough amounts.

• Inaccurate labelling: The accuracy of the machine learning models that are now in use depends on how well the input dataset was used for training. Inaccurate labelling of the data prevents the model from producing reliable predictions.

PROPOSED SYSTEM

In this study, we present a threat-based adversary emulation method that overcomes the drawbacks of conventional red teaming and penetration testing strategies and offers a more accurate and realistic representation of actual attacks. Our method continuously adjusts the attack simulation to the organization's changing security posture by using Mitre ATT&CK to learn TTPs. Our method's ability to simulate real-world attacks more realistically is one of its main benefits, as it enables the red team to imitate the actions of sophisticated attackers and advanced persistent threats (APTs). Furthermore, our method enables organisations to enhance their overall security posture and stay ahead of changing threats by continuously modifying the attack

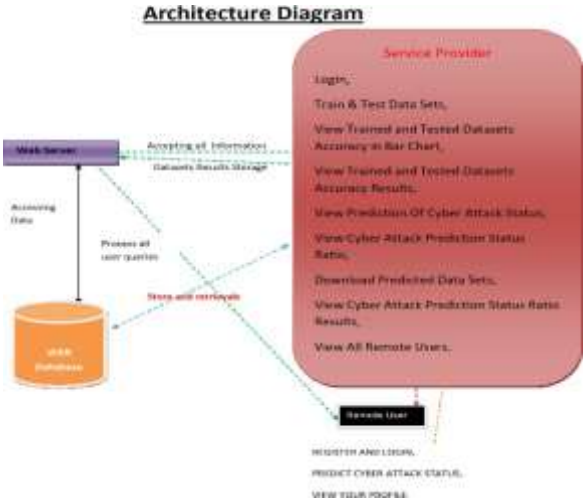
International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp599-609
Vol. 21, Issue 2, 2025

simulation. Understanding malware classes is essential for an operator performing threat-based adversary emulation. The most prevalent of these are droppers, which help adversaries download malware of any kind. Additionally, we provide a threat-based adversary emulation strategy using payload generation algorithms. This strategy comprises of distinct agnostic techniques that possess comparable capabilities to those of actual attack vectors. It can also be utilised to create new avenues of assault. In order to simulate adversarial TTPs, we offer four strategies for creating covert attack paths. We created many payloads during the experiments and evaluated them against endpoint security programs like EDR/AV (endpoint detection and response/antivirus) to prevent and identify attacks. We assessed the efficacy of covert payloads in this manner. The ATT&CK framework, a global free-to-use database of adversarial knowledge based on TTP, was used to assess our methodology and map test case payloads. Furthermore, this method can be used to replicate novel approaches for comparable procedures on ATT&CK. After comparing our methodology and algorithms to endpoint security, we came to the conclusion that this strategy works well for both launching dynamic threats and assessing "emerging threats.".

Advantages

1) The system suggests the adversary emulation technique based on agnostic threats, which entails modelling a variety of possible attacks, including known and undiscovered threats.
2) The purpose of the suggested technique is to detect vulnerabilities and measure the effectiveness of security controls in a more realistic and complete way. It helps businesses to test their defenses against a wide range of potential attacks and better understand their overall security posture. It also allows enterprises to keep ahead of evolving threats by regularly testing and updating their defenses.

4. SYSTEM ARCHITECTURE



IMPLEMENTATION

Modules

Service Provider

In this module, the Service Provider has to login by using legitimate user name and password. After login successful he can do several actions 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

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp599-609
Vol. 21, Issue 2, 2025

Cyber Attack Prediction Status Ratio, Download Predicted Data Sets, View Cyber Attack Prediction Status Ratio Results, View All Remote Users.

View and Authorize Users

The administrator can access the list of all registered users in this module, as well as the user's information, including name, email address, and permissions.

Remote User

Additionally, there are n users in this module. The user must first register before proceeding. The user's information will be entered into the database after they register. Once his registration is complete, he must use his password and authorised user name to log in. The user will perform several tasks after successfully logging in, including registering and logging in, predicting the status of cyberattacks, and seeing their profile.

ALGORITHMS

Logistic regression Classifiers

The relationship between a set of independent (explanatory) variables and a categorical dependent variable is examined using logistic regression analysis. When the dependent variable simply has two values, like 0 and 1 or Yes and No, the term logistic regression is applied. When the dependent variable has three or more distinct values, such as married, single, divorced, or widowed, the technique is sometimes referred to as multinomial logistic regression. While the dependent variable's data type differs from multiple regression's, the procedure's practical application is comparable.

When it comes to categorical-response variable analysis, logistic regression and discriminant analysis are competitors. Compared to discriminant analysis, many statisticians believe that logistic regression is more flexible and appropriate for modelling the majority of scenarios. This is due to the fact that, unlike discriminant analysis, logistic regression does not presume that the independent variables are regularly distributed.

Both binary and multinomial logistic regression are calculated by this program for both category and numerical independent variables. Along with the regression equation, it provides information on likelihood, deviance, odds ratios, confidence limits, and goodness of fit. It does a thorough residual analysis that includes diagnostic residual plots and reports. In order to find the optimal regression model with the fewest independent variables, it might conduct an independent variable subset selection search. It offers ROC curves and confidence intervals on expected values to assist in identifying the optimal classification cutoff point. By automatically identifying rows that are not used throughout the study, it enables you to validate your findings.

.

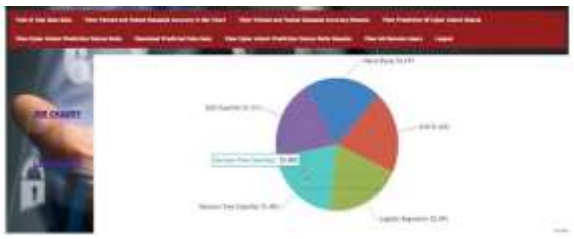
5. **SCREEN SHOTS**

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp599-609

Vol. 21, Issue 2, 2025



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 adversary 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 updating their defences, organisations may stay ahead of evolving 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 plan prompted us to take certain activities. We offer three

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp599-609
Vol. 21, Issue 2, 2025

algorithms 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 threats 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.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp599-609
Vol. 21, Issue 2, 2025

[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.[Online]. Available: https://upcommons.upc.edu/bitstream/handle/2117/
171278/Module%20development%20in%20 Metasploit%20for%20 pentesting.pdf
[16] N. Moran. (Nov. 2014). *Operation Double Tap.* [Online]. Available:https://www.fireeye.com/blog/threatresearch/2014/11/operation_ doubletap.html
[17] N. A. Almubairik and G. Wills, ‘‘Automated penetration testing based on a threat model,’’ in *Proc. 11th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2016, pp. 413–414.
[18] A. Singh, N. Jaswal, M. Agarwal, and D. Teixeira, *Metasploit Penetration Testing Cookbook: Evade Antiviruses, Bypass Firewalls, and Exploit Complex Environments With the Most Widely Used Penetration Testing Framework.* Birmingham, U.K.: Packt, 2018.
[19] D. Miller, R. Alford, A. Applebaum, H. Foster, C. Little, and B. Strom, ‘‘Automated adversary emulation: A case for planning and acting with unknowns,’’ MITRE, McLean, VA, USA, Tech. Rep. 18-0944-1, 2018. [Online]. Available: https://www.mitre.org/sites/default/files/2021-11/prs-18-0944-1-automated-adversary-emulation-planning-acting.pdf
[20] A. Belfadel, M. Boyer, J. Letailleur, Y. Petiot, and R. Yaich, ‘‘Towards a security impact analysis framework: A risk-based and MITRE attack approach,’’ in *Computer Security. ESORICS 2022 International Workshops:CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers*. Copenhagen, Denmark: Springer, 2023, pp. 212–227. [Online]. Available: https://www.springerprofessional.de/en/towards-a-security-impactanalysis-framework-a-risk-based-and-mi/24040982