Structured Approaches in Penetration Testing: Navigating the Landscape of Cybersecurity Automation and AI Advancements

Kiera Conway
Dakota State University
Seattle, USA
Kiera.Conway@trojans.dsu.edu

Abstract— **The increasing threat of cyberattacks has made Penetration Testing (PT) a crucial strategy for protecting digital assets in today's growing digital landscape. This literature review explores the imperative shift toward structured methodologies in the PT process, ensuring comprehensive assessments, operational efficiency, vulnerability prioritization, and adherence to ethical practices. These complex and resource-intensive conditions demand a high level of expertise from penetration testers (pentesters). Therefore, to keep pace with the field's evolving demands, pentesters often dedicate substantial time to continuous training and skill development. This intricate workload has resulted in a shortage of skilled pentesters, spurring the rise of automation through Artificial Intelligence (AI), Machine Learning (ML), and Reinforcement Learning (RL). While this automation significantly reduces the time and resources required for security testing, the limited research in this area hinders its adaptability and scalability. As innovative approaches emerge, studies explore leveraging neural networks to enhance AI's aptitude for comprehending the intricacies of modern security landscapes. These advancements represent a pivotal transformation in the field of PT, paving the way for more efficient and effective security assessments.**

Keywords— Artificial Intelligence, Penetration Testing, Machine Learning, Reinforcement Learning, Deep Learning, Cybersecurity, Ethical Hacking, Vulnerability Assessment, Phases

INTRODUCTION

In an age defined by the relentless increase of technology, the growing digital landscape has become both a playground for innovation and a battleground for cyber threats. As organizations increasingly rely on technology to operate, communicate, and store critical data, safeguarding these assets against potential adversaries becomes paramount. This realization has given rise to Penetration Testing (PT) as a vital and proactive strategy that allows organizations to simulate cyberattacks on their systems to discover and eliminate dangerous vulnerabilities.

This offensive approach to PT emphasizes the importance of following a structured process to systematically evaluate a system's security. While the specific phases of PT may exhibit variations in terminology depending on the source, their fundamental organization remains the same: preparation, implementation, and analysis [1]. However, as the complexity and scale of networks continue to expand, traditional manual methods need help to cope with the substantial workload inherent to this process. Penetration testers (pentesters) involved in this field must maintain a continuous regimen of training and practical skill development to remain at the forefront. Unfortunately, this excessive pressure, combined with the recent shortage of pentesters, has left many in the field feeling overburdened and overtired. [2]

This situation has prompted a growing trend toward integrating automation technologies, including Artificial Intelligence (AI), Machine Learning (ML), and Reinforcement Learning (RL) into PT. Automated PT can significantly reduce the time and resources required for testing, making it a crucFial development in the field. While extensive research has already begun to explore this integration [2] [3], many of these approaches still require manual human intervention for vulnerability identification. However, recent innovative methods have emerged that leverage neural networks to gain a deeper understanding of the intricate and dynamic security environments within modern networks, ultimately enhancing the role of AI in PT. This evolution is a pivotal moment for cybersecurity and AI as they converge to tackle digital threats.

LITERATURE REVIEW

Review 1: Introduction to PT Methodology

Introduction

The “Penetration Testing: Practical Introduction & Tutorials" blog published by Splunk, a leading authority in cybersecurity, serves as a critical resource for understanding the intricate methodologies of digital defense. Splunk provides valuable insights and resources across various domains, including cybersecurity, compliance, data management, IT monitoring, and overall management of IT and business operations [4]. This report introduces PT as an offensive strategy to identify system vulnerabilities by simulating cyberattacks. Watts [5] emphasizes the primary goal of this process is to uncover weak points, understand potential attack scenarios, and analyze the severity of vulnerabilities. By emulating the actions of a genuine attacker and reporting discovered vulnerabilities, this approach allows target systems to prioritize critical security enhancements before real threats materialize.

In addition to introducing PT as an offensive strategy, the blog delves into the intricacies of the PT process. It not only discusses how PT enhances security but also details the specific and complex steps and procedures involved in the PT process. These steps systematically assess and analyze system security through information gathering, scanning, exploitation, connection maintenance, eliminating intrusion evidence, and reporting. It then bridges the gap between theoretical knowledge and practical application by providing tangible examples of PT tasks and outlining the basic functionality of various essential PT tools. Overall, this article delivers a comprehensive perspective on the importance of PT in cybersecurity and its practical relevance to safeguarding businesses when digital threats are both inevitable and evolving.

Summary

This article offers an in-depth exploration of the structured stages involved in PT, ensuring a methodical, ethical, and comprehensive evaluation of a system's security. These stages contribute to the overall effectiveness of PT by simulating real-world attack scenarios, identifying vulnerabilities, assessing their severity, and guiding the enhancement of cybersecurity measures. While other sources may present slightly different PT stage breakdowns, this blog distinguishes itself by not only submitting a comprehensive analysis of these stages but also by providing concrete examples, precise definitions, and practical insights into their importance. The stages outlined in this Splunk article include 'Information Gathering,' 'Scanning,' 'Exploiting,' 'Maintaining Access,' 'Covering Tracks,' and 'Reporting' [5]. This structured approach enables security professionals to systematically assess vulnerabilities and prioritize security improvements.

Due to the growing complexity of modern networks, Watts highlights skills critically necessary for pentesters and underscores the importance of continuous training and practice to excel in the field of PT. These skills encompass a wide range of technical and practical competencies, ranging from "knowledge of operating systems and networking," an understanding of "authentication and authorization mechanisms," to a strong foundation in programming [5]. Whether it is achieved through self-directed efforts, such as reading and exploring online resources, or through formal education, continuous skill development is crucial. Hands-on practice is emphasized as one of the most essential components, as it allows individuals to apply their knowledge and techniques in a controlled environment, ensuring proficiency maintenance and adaptability.

The author reinforces this principle through a series of practical demonstrations. The first demonstration establishes a controlled test environment through VMWare, including an attacker and victim machine. This approach showcases the use of different PT tools in various phases, starting with gathering important network-related information: First by gathering domain-specific intelligence with Whois, then identifying vulnerable devices exposed on the internet through Shodan, and finally conducting a comprehensive network topology scan with Nmap. The examples in this foundational phase can be used to assist security professionals, obtain a detailed understanding of network infrastructure, and identify potential security vulnerabilities.

Once a thorough network visualization has been established, the author demonstrates a series of exploitation tools, such as password cracking with John the Ripper and web traffic interception and manipulation with Burp Suite. Watts [5] then proceeds to highlight the use of Metasploit exploits to establish a "backdoor shell that [will enable him] to run commands on the victim system."

Methodologies

This article thoroughly explores the fundamental techniques and processes behind PT and provides a structured approach for identifying and resolving security vulnerabilities. These methodologies are categorized into several stages, each playing a crucial role in the PT process. From information gathering and scanning to exploiting vulnerabilities and maintaining access, each step simulates real-world attack scenarios, helping organizations comprehend their system's weak points. By conducting PT, businesses can effectively prioritize security measures, subsequently enhancing the overall security of their digital assets.

The first stage, as defined by this article, is 'Information Gathering.' This initial phase is equivalent to conducting reconnaissance, during which a pentester collects essential data about the target system or organization. The primary goal is to gather relevant data to understand the available testing surface and potentially detect security vulnerabilities. Some common categories of information pentesters aim to collect in this stage include IP addresses, server details, subdomain identification, and specific software applications, platforms, operating systems (OS) or frameworks [5]. This phase is about building a comprehensive profile of the target to serve as the foundation for subsequent stages of the testing process.

After identifying potential entry points and vulnerabilities in the target system during the previous phase, the pentester begins to assess these points for possible weaknesses during the 'Scanning' phase. Exploration of the target system must be conducted systematically rather than haphazardly testing each potential vulnerability. Not only is a blind approach more time-consuming, but it is also significantly less effective. Therefore, to increase the chances of successful vulnerability detection, pentesters identify known vulnerabilities in their target's framework and assess how the system responds to intrusion attempts [5]. This stage significantly improves the efficiency of the testing process as it refines the list of potential vulnerabilities, allowing testers to concentrate on only the most relevant.

After vulnerabilities have been identified during the previous stages, pentesters actively exploit them during the 'Exploitation' phase. The goal is to simulate an actual intrusion by accessing data within the target system, intentionally triggering failures, or making unauthorized changes [5]. While this critical phase mimics the actions of a genuine attacker, the author emphasizes the importance of maintaining ethical and controlled PT practices by focusing on understanding vulnerabilities rather than causing actual damage.

After successful exploitation, the testing focus shifts from gaining initial access to the 'Post-Exploitation' phases: 'Maintaining Access,' 'Covering Tracks,' and 'Reporting.' These phases, encompassing Steps 4 to 6, align with this primary purpose of assessing and improving security measures rather than engaging in malicious actions. Unlike authentic attacks, these phases aim to evaluate and enhance security by examining the system's ability not only to detect unauthorized access but also to log and store data related to security incidents [5]. Then, by reporting their insights in detail, pentesters enable organizations to fortify their defenses against real-world cyber threats.

Main Findings

The main findings in the article revolve around the importance of PT in the context of cybersecurity. The report highlights that businesses undergoing significant growth are more likely to attract the attention of cybercriminals and emphasizes PT as an essential strategy for protecting their digital assets. The testing process is introduced as a proactive and offensive method for identifying system vulnerabilities by simulating cyberattacks to uncover weak points, anticipate potential attack scenarios, and assess the severity of vulnerabilities.

The article also emphasizes Splunk's multi-phase testing process, with each stage crucial in systematically replicating real-world attack scenarios. 'Information Gathering' provides critical insights into the target, while 'Scanning' refines the focus by identifying specific vulnerabilities, thus preventing inefficient testing of unrelated weaknesses. The 'Exploitation' phase, while simulating an actual attack, strictly adheres to ethical principles to avoid harming the target system. After successful exploitation, the post-exploitation phases, 'Maintaining Access' and 'Covering Tracks,' evaluate an attacker's ability to sustain a persistent presence and evade detection. The final 'Reporting' phase is crucial for outlining and prioritizing vulnerabilities to guide businesses to address easily exploitable weaknesses first.

Overall, this blog highlights that PT is a proactive, systematic, and highly effective approach for identifying and addressing security vulnerabilities within an organization's system. Simulating the actions of potential attackers enables organizations to fortify their security measures and safeguard their valuable assets from complex cyber threats. The article not only emphasizes the significance of PT but also provides a foundational framework for conducting the testing process through well-defined phases, all while upholding essential ethical considerations. This structured and ethical approach ensures that PT not only identifies and exploits vulnerabilities but utilizes this data to equip organizations with practical strategies to improve their overall security.

Relevance to Your Course Content

While the specific phases of PT may exhibit variations in terminology depending on the source, their fundamental organization and underlying concepts remain the same. Since my course is developed explicitly around these phases, it was essential to find a credible basis from which to structure the modules. As such, the decision to adopt Splunk's PT methodology into the curriculum is substantiated by their extensive expertise and experience in cybersecurity. Integrating these well-structured phases into the course will provide a solid and reliable foundation upon which to build.

Another reason this article is an invaluable resource for my course content is because it effectively bridges the gap between theoretical knowledge and practical implementation. It not only offers an in-depth exploration of PT stages, but it also provides additional context, insights into practical applications, guidance for setting up testing environments, and real-world examples of popular tools. These practical applications demonstrate the impact of PT tools in identifying vulnerabilities, creating custom exploits, and enhancing offensive strategies. By providing a blend of theoretical insights and hands-on experience, this article will further develop a solid PT foundation for my course, serving as the launchpad from which to delve into AI-enhanced cybersecurity strategies seamlessly.

Some tools discussed in this report, including Nmap, Metasploit, and Burp Suite, are commonly used in the field and are essential for carrying out PT and identifying vulnerabilities. Although these tools do not innately contain AI functionality, they can be integrated with AI and ML techniques to enhance their capabilities. For example, AI can automate the detection of vulnerabilities or streamline the exploitation of weaknesses using data analysis to identify patterns or trends in data [2] [3]. My course will explore the possibilities of this integration and demonstrate how AI can augment the functionalities of various tools. While I will provide some background on the discussed tools throughout the course, this article is a valuable resource to provide additional context on AI-driven PT tools that leverage ML for improved threat identification and exploitation.

Review 2: Deep RL in PT

Introduction

The article "Autonomous Security Analysis and Penetration Testing" from Arizona State University introduces an innovative framework designed to address the growing challenge of evaluating network security amidst the complexity of expanding networks and the shortage of cybersecurity professionals. By leveraging advanced RL techniques based on DeepQ Networks (DQN), this framework in this study integrates vulnerability information into the PT processes. It associates RL reward values with Common Vulnerability Scoring System (CVSS) scores, enabling prioritization of the most critical vulnerabilities. The result is a highly efficient, automated PT system that can significantly reduce assessment time and improve overall efficiency.

Summary

Previous research on using RL for automating PT has focused predominantly on smaller networks and often failed to harness vulnerability information effectively. These traditional AI models have struggled to grasp the intricacies of real-world networks, falling short in accounting for the specific network structure, distribution of vulnerabilities, or correlation between vulnerabilities and exploitation probabilities [6]. This limitation has led to difficulty in prioritizing vulnerabilities, resulting in less accurate and efficient security assessments. To obtain essential information about a target and its associated vulnerabilities, these methods often rely on known sources, scans, or manual analysis for identification. This overall failure of traditional AI models to comprehensively understand the nuances of the dynamic and complex security landscapes of modern networks has resulted in a desperate need for a more comprehensive approach to PT.

Recognizing these limitations, the authors introduced the Autonomous Security Analysis and Penetration Testing framework (ASAP) as an innovative approach to security analysis and PT. This autonomous system not only understands the interconnectedness of vulnerabilities and their relation to a network's structure, but it also leverages an RL reward system based on vulnerability severity and exploitability. The approach adopted by the authors emphasizes domain-specific modeling by integrating the CVSS to quantify known vulnerabilities. This system tracks the severity of vulnerabilities and the complexity of exploiting them, allowing for a more comprehensive understanding of the network's security landscape. This modeling approach harnesses state-transition diagrams to visualize the most optimal PT policy for the network. These diagrams represent different network states and the associated actions, including probability values derived from the vulnerability's Access Complexity (AC). By generating autonomous attack plans and validating them against real-world networks, ASAP creates a comprehensive map of security threats and potential attack paths. This approach ensures efficiency not only in smaller networks but also in large-scale environments, demonstrating its exceptional performance and scalability.

To enable autonomous PT, the authors adopt an RL-based AI algorithm to identify the optimal "attack path that maximizes the reward value for the pentester [6]." RL is a concept where an agent learns through the consequences of its interactions within an environment, focusing on long-term objectives; this can be compared to security professionals experimenting with attack strategies against vulnerabilities until successful exploitation. However, what sets their RL model apart from other traditional AI models in the PT domain is that the authors propose using a DQN-based RL model. Since DQ models learn directly from interactions with the environment by utilizing neural networks, it is more equipped to handle diverse network conditions, including those that may not have been encountered during training. As such, their RL approach involves dynamic interactions with the environment by considering the current user privilege level, actions linked to vulnerability exploitation, the difficulty and probability of a successful action, reward values, and the decision-making process. The outcome of this method is a carefully designed attack plan that "guides the security professional" through subsequent actions based on their user privilege and progression strategy [6].

Methodologies

The methodologies of ASAP involve a structured series of steps that enable efficient and effective PT. First, researchers employ popular scanners such as Nessus and OpenVAS to scan for vulnerabilities in the target network. The obtained scan information about the availability and accessibility of network services (e.g., open ports, protocols) and vulnerabilities within those services are then generated into an attack graph. This graph creates a visual representation of potential attack paths, relationships between different elements of a network, "and dependencies between the vulnerabilities [6]." Essential information from the attack graph is then converted into a structured format, known as a State Graph, and passed to the RL algorithm for further analysis.

The State Graph represents how privileges transition within the network and if a specific vulnerability leads to an exploit. When a vulnerability is discovered and linked to an exploit, certain attributes such as the CVSS and AC are extracted and saved for future reference. The reward value is determined by the vulnerability's CVSS score, where higher severity vulnerabilities, with a more critical potential impact if exploited, earn a higher reward. This information is vital for calculating exploit success probabilities as it is used to define and build the RL algorithm through parameters including the state of user privilege, actions, transition probability, reward values, and the agent's decision policy [6]. After confirming the success of their exploits through log analysis, the state graph and any relevant threat information are generated into an attack plan.

Finally, after the attack plan is generated, a Python wrapper for the Metasploit framework is used to validate its effectiveness. If vulnerabilities and weaknesses are found in the target organization's network or systems, the findings are used to recommend actions to improve the security of the organization. These actions may include applying patches or making changes to the network based on the vulnerabilities and weaknesses discovered during the test. Once these changes are implemented, the attack graph, which represents the network's vulnerabilities and potential attack paths, can be updated to reflect the new security measures. The system can then be retested to ensure that the implemented changes have effectively addressed the identified security issues and that the network's security posture has improved. This cyclical process of testing, improving, and retesting to enhance the organization's security is vital in cybersecurity, as it ensures that security measures remain robust, modern, and adaptive to evolving threats.

Main Findings

Overall, the main findings of the article emphasize that the ASAP framework, with its use of RL and attack graphs, offers a more efficient and effective approach to PT. It not only reduces the manual effort and time required, but it also reveals previously undiscovered attack paths that manual testing might miss, ultimately improving the overall security assessment process.

A case study involving the PT of an enterprise network with an industrial control system and IoT devices was conducted. The network consisted of 16 hosts distributed across three networks and offered a mix of Windows and Linux systems. The goal was to compromise email information by exploiting vulnerabilities on the SMTP service and infiltrating the IoT subsystem through a vulnerability in the gateway machine. The study investigated the effect of changes in the Discount Factor (DF) on determining the degree of significance assigned to future rewards in the decision-making process. Values closer to 0 prioritize immediate rewards, while values closer to 1 prioritize future rewards. The researchers also explored variations in batch size (BS) to explore the number of interactions the AI system uses to learn and improve its policy. These variations were analyzed to assess their influence on the RL agent's ability to make effective decisions.

The case study findings revealed that the DQN algorithm reached an effective solution quickly for different variations in DF, with the optimal value being around 0.8. Higher DF variations, 0.9 and 0.99, caused the agent to take more time to learn and make decisions as it required more time to explore each potential future outcome [6]. Similarly, reward value diminishes considerably the more the agent prioritizes long-term rewards, regardless of the number of interactions the system used to learn and improve. The agent's reward value was highest for the optimal DF around 0.8, especially with a BS of 16. The study showed that larger BS, such as 32 or 64, caused the AI's performance to decline [6]. However, researchers note that this observation might only hold true for a small network due to the increased complexity and scale of large networks, which can lead to different dynamics in the learning process for the AI system.

Researchers also conducted a scalability experiment on a simulated flat network comprising 300 hosts and three vulnerabilities. This experiment aimed to highlight the framework's scalability in situations where determining the balance between exploiting actions that appear promising based on its current knowledge and exploring new actions to discover potentially better strategies is challenging. Pentesters often experience this challenge in real-world situations, where they must decide how to allocate their resources, time, and efforts effectively.

In such situations, the experiment demonstrated the framework's ability to provide an attack plan within a short timeframe, about 70 seconds, when BS and DF parameters were set to their optimal values. This time frame is notably faster than research that utilized autonomous methods for PT, where a similar process took approximately 300 seconds (5 minutes) to perform on a network with only seven hosts. Even when the framework faced challenging scenarios with extreme BS and DF parameter values, it consistently generated effective attack plans within approximately 350 to 400 seconds [6]. These results indicate that the tested framework is highly efficient and capable of providing rapid and effective attack plans in various scenarios, significantly outperforming traditional PT methods.

What sets the ASAP framework apart from manual methods is its distinct strategy for PT. Unlike traditional manual testing, AI-based approaches, like ASAP, prioritize exploiting certain vulnerabilities before others, resulting in more efficient and effective PT. This data-driven approach involves adapting to the characteristics of vulnerabilities within unique network environments. Sometimes, starting with less challenging vulnerabilities can lead to a more efficient overall PT. The ASAP framework's adaptability and its consideration of vulnerability characteristics make it an asset in the field of cybersecurity and offers a significant reduction in the time and effort required over traditional manual approaches.

Relevance to Your Course Content

This article is highly relevant to my course as it aligns with the central theme of harnessing AI techniques for offensive strategies in PT. In the article, an ASAP framework provides a practical example of various aspects touched on in my course, including AI-driven PT tools, RL, DQ, and real-world applications of AI in security assessments. This in-depth exploration forms the foundational knowledge for the course's focus on AI-driven PT techniques and demonstrates the efficiency and effectiveness of AI in identifying security vulnerabilities.

Furthermore, the article's application of DQN as a deep RL technique serves as a practical example of how ML models can be used for identifying vulnerabilities and threats. This integration aligns with my course's content, which covers the training of various ML models. The ASAP framework showcased in the article also highlights the scalability of AI-driven techniques, making it suitable for large-scale networks. It demonstrates the transformative power of AI in PT by uncovering hidden attack paths, offering valuable insights about AI's practical applications in identifying vulnerabilities, and optimizing security assessments.

Conclusion

The articles reviewed in this report have provided valuable insights into PT, offering structured frameworks and innovative approaches to address the challenges faced by cybersecurity professionals. Splunk's "Penetration Testing: Practical Introduction & Tutorials" provides a foundational understanding of PT, emphasizing its importance in securing digital assets. The article also offers a structured breakdown of PT phases, highlighting the significance of training and continuous skill development, which aligns with the evolving demands of the field. Alternatively, "Autonomous Security Analysis and Penetration Testing" introduces the groundbreaking ASAP framework, demonstrating the potential of AI and deep RL techniques, such as DQN, to revolutionize PT. The framework efficiently identifies vulnerabilities, prioritizes them, and adapts to the unique network environment, thereby offering valuable insights into security assessments. By adopting AI-driven approaches like the ASAP framework, the industry can address the growing challenge of evaluating network security in the face of expanding networks and a shortage of cybersecurity professionals.

In conclusion, PT remains a vital proactive strategy in the dynamic digital landscape. The fusion of human expertise and AI capabilities promises to revolutionize security assessments, offering a more efficient and effective means of identifying and mitigating vulnerabilities. As the world of cybersecurity continues to evolve, AI-driven PT becomes an indispensable tool for identifying vulnerabilities, optimizing security assessments, and fortifying digital defenses. By embracing these innovations, organizations can stay ahead in the ongoing battle against digital threats, ultimately ensuring the security and integrity of their digital assets.

References

[1] H. M. Z. A. Shebli and B. D. Beheshti, "A study on penetration testing process and tools," in *Long Island Systems, Applications and Technology Conference (LISAT)*, Farmingdale, 2018.

[2] M. C. Ghanem and T. M. Chen, "Reinforcement Learning for Intelligent Penetration Testing," in *Second World Conference on Smart Trends in Systems, Security and Sustainability*, London, 2018.

[3] A. AlMajali, L. Al-Abed, R. Mutleq, Z. Samamah, A. A. Shhadeh, B. J. Mohd and K. M. Ahmad Yousef, "Vulnerability Exploitation Using Reinforcement Learning," in *Jordan International Joint Conference on Electrical Engineering and Information Technology*, Amman, 2023.

[4] C. Kidd, *What Is Splunk & What Does It Do? An Introduction To Splunk,* 2022.

[5] S. Watts , *Penetration Testing: Practical Introduction & Tutorials,* 2022.

[6] A. Chowdhary, D. Huang, J. S. Mahendran, D. Romo, Y. Deng and A. Sabur, "Autonomous Security Analysis and Penetration Testing," in *16th International Conference on Mobility, Sensing and Networking (MSN)*, Tokyo, 2020.