Using AI/Machine Learning for Reconnaissance Activities During Network Penetration Testing

George Stone, Douglas Talbert and William Eberle
Tennessee Tech University, Cookeville, USA
gstone42@tntech.edu
DTalbert@tntech.edu
WEberle@tntech.edu
DOI: 10.34190/IWS.21.029

Abstract: Penetration testing is an important tool used by a variety of organizations to ensure a proper, working cybersecurity infrastructure. However, these tools come with limited automation abilities that require manual intervention or interpretation. Ideally, pentesters should have access to equally sophisticated tools, as do the intruders that are exposing daily vulnerabilities. A significant portion of pentesting is focused on reconnaissance and enumeration. In other words, the better the pentester can map out the security landscape of the target network, the better and more specific any attacks can be designed. Since the early stages of penetration testing are arguably the most important, where vulnerabilities can be exploited through social engineering, recon and enumeration demand a significant amount of creativity. Machine learning is proving to be an essential tool to carry out sophisticated functions and learns from previous data or experiences. Research using machine learning could be beneficial to cybersecurity professionals tasked with testing and securing precious assets. However, there seems to be a relative scarcity of research that combines machine learning and pentesting. In this context, one of the most comprehensive pentesting tool suites, Metasploit, provides the user with the ability to integrate additional modules. Therefore, it is conceivable that machine learning algorithms could be integrated into the Metasploit framework, allowing for an improved pentesting approach. The research presented in this work assesses and compares existing tools for manual penetration testing, focusing on efficiency, precision, accuracy, and scope. Ultimately, by implementing an automated machine learning cyber penetration system, manually intensive and expensive cyber penetration testing can be simplified by reducing the amount of time and resources needed for current tests.

Keywords: cybersecurity, machine learning, pentesting, python, reconnaissance

1. Introduction

Cybersecurity plays an ever-increasing role as society becomes more and more reliant on computer and network technology in almost all areas of everyday life. As hackers and malicious actors are using more sophisticated methods to target these systems, there is a growing demand to test network security mechanisms. Unfortunately, many testing methods are still based on manual threat management. The integration of artificial intelligence and machine learning (AI/ML) allows for the automation of network security testing and threat assignment, and it is able to spot more complex threats that are difficult to detect with traditional methods. Consequently, the research introduced in this study seeks to establish ways to implement machine learning - using Python as a programming language - within the Metasploit framework for penetration testing. In general, as society becomes more and more connected via the internet, social media, and the internet of things (IoT), ML algorithms in cybersecurity are taking on an increasingly important function in everyday life (Roopak et al, 2019).

Several different machine learning approaches have been used in the implementation of cybersecurity algorithms. Early protocols were built on supervised machine learning. Here, the programmers feed the models with known examples of malware and corrupted data, training the software to recognize similar threats. In addition, programmers use ensemble learning - the application of several algorithms together to extend the software's functionality. Examples for supervised and ensemble learning are the Deep Forest or AdaBoost algorithms (Sornsuwit and Jaiyen, 2019; Utkin et al, 2019). Unsupervised learning algorithms are trained without any information about the outcome to which the existing data should be mapped. Examples for this kind of ML approach can be found in neural networks or principal component analysis (Tuor et al, 2017). Third, reinforcement learning (RL) uses the principle that the program learns in each step from previous attempts. RL uses rewards (both positive and negative) to learn a strategy to advance the system toward a goal. In cybersecurity applications, deep reinforcement learning is an example of an unsupervised reinforcement learning algorithm (Nguyen and Reddi, 2019).

Another important aspect of computer networks is that their complexity allows potential attackers to explore a multitude of different entry vectors that could be exploited to gain access. Such reconnaissance activities can

either be passive - for example, the hacker may attempt to eavesdrop on a Wi-Fi network and extract information about network traffic using a program like Wireshark - or they can be active, where the attacker engages with the system to find any vulnerabilities. One way of doing this is by using Nmap to scan the target system and gathering information about it that could suggest possible angles of attack. One of the central duties of a cybersecurity professional is the adherence to and preservation of the triad of confidentiality, integrity and accessibility (CIA); in other words, the privacy of the network stakeholders must be guaranteed (confidentiality); the data must be kept intact, and the coherence of the filesystem must be maintained (integrity); and the system must remain accessible to its users (accessibility). Cyberattacks can compromise any three branches of the CIA triad (Kachhwaha and Purohit, 2019).

Recently, there has been growing research into using ML for cyber defensive/reactive purposes. Such research has created innovation to defend computer systems for world governments, enterprises, and individuals. Since there is limited research into ML's use for proactive cyber use, such as ethical pentesting, an opportunity exists for scientific research. Thus, this work aims to design an ML-based algorithm that can be used to automate reconnaissance activities for network security. More specifically, the algorithm will be used in conjunction with penetration testing, or pentesting. In this study, we will first review the concepts of penetration testing. Second, we will present the related work in this area. Third, we will enumerate current research opportunities and conclude with our next steps.

2. Penetration testing (Pentesting)

Pentesting is a procedure by which a team of ethical hackers attempts to breach cybersecurity to enter a specific computer system or network. This procedure, in turn, will show the vulnerabilities of the system so that the administrators can enhance security measures in a specific manner. Pentests are essential components in organizational risk assessment, and in particular industries - such as medical devices, public health management, credit and debit card processing, technology services, and financial organizations - they are legally required (Ankele et al, 2019; Alpine Security, 2020; U.S. General Services Administration, 2020). Penetration testing is usually done on five different levels, networks, web applications, client-side applications, wireless carriers, and social engineering, as illustrated in Figure 1 (Schaab et al, 2016; Nagpure and Kurkure, 2017; Singh and Singh, 2017; Zabicki and Ellis, 2017; Singh et al, 2018; Firch 2019).

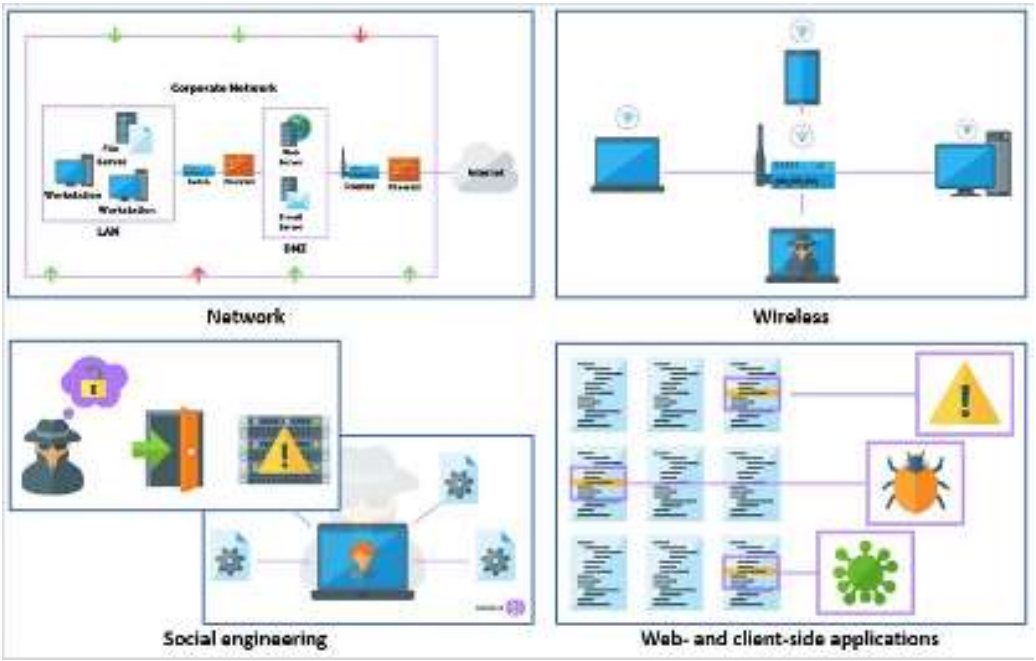

Figure 1: Different levels of penetration testing (Firch, 2019)

In general, pentests follow a simple principle. The testers will search for specific network security weaknesses through passive and active means, design an attack that exploits those weaknesses, test the attack, and implement it. The pentester will attempt to remain undetected for as long as possible, to access and download as many files as possible. Often, the attack itself will also include the delivery of a specific payload. In some cases, the pentest's goal may be to take control of the targeted company and its operations. These examples illustrate

the importance of performing regular pentests (Denis et al, 2016; Shinde and Adharpurkar, 2016; Shah et al, 2019).

Unfortunately, pentesting approaches are mostly manual, which places them at an increasing disadvantage when facing more and more complex network security protocols. However, recent ML algorithms have started to make penetration testing more manageable and efficient. Since many network security algorithms and intrusion detection systems also use technologies based on AI/ML, the introduction of ML to pentesting serves as a welcome counterbalance.

3. Related work

There are several different ways in which machine learning has been used for penetration testing. For example, common patterns in a network's cybersecurity code can point at security flaws, and ML algorithms can detect such patterns. In the work of Harer et al. (2018), they construct control flow graphs (CFGs) from existing code in order to provide a topological overview of the security code. They then use ML algorithms to extract vulnerabilities.

ML algorithms based on deep learning can extract security weaknesses from PHP and other code. In this case, the key is to transform the entire code into tokens that can be more easily understood by the ML algorithm. As a result, vectors are constructed that point at security flaws (Fang et al, 2019).

Another way in which ML algorithms can be deployed for cybersecurity purposes is in the form of expert systems, which contain a specific database with knowledge provided by 'experts'. Such programs will consult the database to execute its functions, and over time, add more of its own 'experiences' to the knowledge base (Sun et al, 2019). The expert system captures information about the target, verifies any attack, and creates a report. Its inference engine then accesses a database consisting of both domain-expert and self-learned knowledge about sensitivities and vulnerabilities within the system. The domain expert knowledge includes libraries with known exploits and fingerprint information, while self-learned knowledge gets added in the course of the program application. This can be, for example, a library about attack events and a functioning defense strategy against them.

Other authors point to common security flaws in modern computer networks. These flaws can then be targeted in ML-based pentesting protocols and range from attacks on the network level, including the attempted exploitation of TCP/IP and DNS, entry by utilizing software and hardware vulnerabilities, social engineering attacks based on Spam, Phishing and drive-by downloads (Jang-Jaccard and Nepal, 2014). Therefore, complete pentesting approaches will often involve a test of human interactions to see how easy it is to enter the company's premises via impersonation or 'tailgating' (Archibald and Renaud, 2019).

4. Research opportunities

Given the state of pentesting and the use of machine learning towards efficiently automating this cyber-security function, we propose to focus on four key research questions. First, we need to assess and compare existing manual penetration testing approaches. For our eventual ML approaches to be effective, we will focus on four aspects: efficiency, accuracy, scope, and the CIA triad.

Second, we will examine existing ML approaches (some of which are noted in the previous section) and some tangential approaches in other research spaces to describe the role of machine learning in penetration testing and enumerate existing algorithms' strengths and weaknesses. Examples of such tools are ML approaches that incorporate model-based planning, or, more recently, reinforcement learning that is free of any assumptions for a specific model (Schwartz and Kurniawati, 2019). In general, we are reviewing ML frameworks for pentesting from supervised learning, unsupervised learning, and reinforcement learning, as well as any potential hybrid between these approaches. The algorithms that seem most feasible to implement are then further used for addressing our primary goal.

Third, we will assess the types of vulnerabilities detected by ML approaches, and subsequently design novel algorithms that address the weaknesses in existing approaches. In this respect, it is interesting to see whether our algorithms would be able to even detect new and unexpected anomalies that might be exploitable for entities seeking to intrude into a network.

Fourth, a question that is of immense practical importance, but not always mentioned in conjunction with the use of ML algorithms for pentesting, is how well the system can scale up to accommodate larger organizational structures.

Thus, the study's central hypothesis is that it is possible to create a machine learning algorithm for active reconnaissance that can be scaled up 10 - 100 fold to accommodate small and large organizations.

5. Future work

To establish the use of ML in reconnaissance activities during pentesting, our research will utilize three main technologies. First, we will program the machine learning algorithms using Python. We hope to benefit from the extensive knowledge about this language, the large community of programmers, and the plethora of resources, such as several libraries designed to integrate machine learning (Raschka and Mirjalili, 2017).

Second, we will use the Metasploit framework, which is utilized in numerous pentesting procedures. We made this decision because (1) the framework works well with Python as a programming language; (2) Metasploit is open source; and (3) it can be used in numerous ways during pentesting, from manually inserting fragments of code into the target network protocols to the programming of more complex code (Singh et al, 2018).

The third technology this project will use are the Open Source Intelligence (OSINT) tools, such as Censys and Shodan. We believe this will allow us to find a wealth of relevant metadata from websites, online applications, and access portals (Lee et al, 2017; Miller, 2018).

To ensure that the quality of our designed algorithms remains high, we will use several different parameters to measure efficiency: precision, which refers to how faithful the applied ML algorithm enumerates the vulnerabilities of the target network; accuracy, which is similar, yet refers to how well the ML algorithm is able to classify the vulnerabilities it finds; and speed, which will allow us to evaluate the scalability of our approach. We will test scalability by simulating a small target network and then by orders of magnitude, increasing the network's size. We will compare our ML approaches to the manual use of reconnaissance tools as well as to the use of already published ML algorithms.

In the end, the goal of our research is to find suitable ML algorithms that work with OSINT, Metasploit, and Python to create a sufficient pentesting method that can be implemented in practical approaches and applications, and that can be scaled up from small to medium and large networks. As we focus mainly on the reconnaissance phase of pentesting, we will investigate the ability to expand the activities to handle payload delivery and stay undetected after entering the network. Thus, whenever possible, the reconnaissance algorithms will be tested on their initial capability to deliver payloads into the system via the identified vulnerabilities.

References

Archibald, J.M. and Renaud, K., 2019. Refining the PoinTER "human firewall" pentesting framework, *Information and Computer Security,* Vol 27, No. 4, pp. 575-600.

Alpine Security (2020). *Penetration testing for compliance: The top 5 laws and regulations that require testing*, [online], https://alpinesecurity.com/blog/penetration-testing-for-compliance-the-top-5-laws-and-regulations-that-require-testing/.

Ankele, R., Marksteiner, S., Nahrgang, K., Vallant, H., 2019. Requirements and recommendations for IoT/IIoT models to automate security assurance through threat modelling, security analysis and penetration testing. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (pp. 1-8).

Fang, Y., Han, S., Huang, C., Wu, R., 2019. TAP: A static analysis model for PHP vulnerabilities based on token and deep learning technology. *PloS One, 14*(11), e0225196.

Firch, J., 2019. What are the different types of penetration testing? [online], https://purplesec.us/types-penetration-testing/

Harer, J. A., Kim, L. Y., Russell, R. L., Ozdemir, O., Kosta, L. R., Rangamani, A., ... & Antelman, E., 2018. Automated software vulnerability detection with machine learning. *arXiv preprint arXiv:1803.04497*.

Jang-Jaccard, J.Nepal, S., 2014. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences,* Vol 80, No. 5, pp. 973-993.

Kachhwaha, R. and Purohit, R., 2019. Relating vulnerability and security service points for web applications through penetration testing. In *Progress in Advanced Computing and Intelligent Engineering* (pp. 41-51). Springer.

Lee, S., Shin, S. H., Roh, B. H., 2017. Abnormal behavior-based detection of Shodan and Censys-like scanning. In *2017 Ninth International Conference on Ubiquitous and Future Networks* (ICUFN) (pp. 1048-1052). IEEE.

Miller, B. H., 2018. Open source intelligence (OSINT): An oxymoron? *International Journal of Intelligence and Counterintelligence,*Vol 31, No. 4, pp. 702-719.

Nagpure, S. and Kurkure, S., 2017. Vulnerability assessment and penetration testing of web applications. In *2017 International Conference on Computing, Communication, Control and Automation* (ICCUBEA) (pp. 1-6). IEEE.

Nguyen, T.T. and Reddi, V.J., 2019. Deep reinforcement learning for cyber security. *arXiv preprint arXiv:1906.05799*.

Raschka, S. and Mirjalili, V., 2017. *Python machine learning*. Packt Publishing Ltd.

Roopak, M., Tian, G. Y., Chambers, J., 2019. Deep learning models for cyber security in IoT networks. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference* (CCWC) (pp. 0452-0457). IEEE.

Schaab, P., Beckers, K., Pape, S., 2016. A systematic gap analysis of social engineering defence mechanisms considering social psychology. In *HAISA* (pp. 241-251).

Schwartz, J., & Kurniawati, H., 2019. Autonomous penetration testing using reinforcement learning. *arXiv preprint arXiv:1905.05965*.

Shinde, P.S. and Ardhapurkar, S.B., 2016. Cyber security analysis using vulnerability assessment and penetration testing. In *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare* (Startup Conclave) (pp. 1-5). IEEE.

Singh, H., & Singh, J., 2017. Penetration testing in wireless networks. *International Journal of Advanced Research in Computer Science*, Vol. 8, No. 5.

Singh, A., Jaswal, N., Agarwal, M., Teixeira, D., 2018. *Metasploit penetration testing cookbook: Evade antiviruses, bypass firewalls, and exploit complex environments with the most widely used penetration testing framework*. Packt Publishing Ltd.

Sornsuwit, P. and Jaiyen, S., 2019. A new hybrid machine learning for cybersecurity threat detection based on adaptive boosting. *Applied Artificial Intelligence,* Vol 33, No. 5, pp.462-482.

Sun, X. D., Ren, Z., Yang, P. W., Li, J., Chen, H. Y., & Liu, T. Q., 2019. Artificial intelligence design research on the cyber security penetration testing of power grid enterprises. In *IOP Conference Series: Earth and Environmental Science* (Vol. 354, No. 1, p. 012104). IOP Publishing.

Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N. and Robinson, S., 2017. Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. *arXiv preprint arXiv*:1710.00811.

U.S. General Services Administration, 2020. *Highly adaptive cybersecurity services (HACS)*, viewed on September 20, 202 , [online], https://www.gsa.gov/technology/technology-products-services/it-security/highly-adaptive-cybersecurity-services-hacs

Utkin, L.V., Meldo, A.A. and Konstantinov, A.V., 2019. Deep Forest as a framework for a new class of machine-learning models. *National Science Review,* Vol 6, No. 2, pp.186-187.

Zabicki, R., Ellis, S. R., 2017. Penetration testing. In *Computer and Information Security Handbook* (pp. 1031-1038). Morgan Kaufmann.

Jeffrey A. Nichols, Ph.D., is a Cybersecurity Research Scientist at Oak Ridge National Laboratory in Oak Ridge, TN, USA. He has been trying to figure out how computers work since he disassembled (and reassembled) his parents' newly purchased $8000 IBM PC. He has worked previously on bioenergy and climate supercomputer models written in FORTRAN.

Dr. Oakley is a foremost expert on offensive cybersecurity for space systems. He is an author and professional with 15 years of experience specialized in offensive cybersecurity to include red teaming and penetration testing within DoD and commercial environments. His books Professional Red Teaming, Waging Cyber War and Cybersecurity for Space are published by Apress.

Augustine Orgah is a Computer Science PhD student from New Orleans, Louisiana attending Louisiana State University. His advisor is Prof. Golden Richard III. His main research area is Information Assurance/Cybersecurity, specifically malware analysis.

Dave Ormrod is a cyber security and information operations professional with over 24 years of military, government and industry experience. Has a PhD in computer science in addition to various certifications, including Australian Information Security Registered Assessors Program (IRAP), Certified Information Systems Security Professional (CISSP) and Certified Information Security Auditor (CISA). Dave enjoys collecting Scotch Whisky and books between adventures.

Mr Vicente Pastor is one of the founder members of NATO's Cyberspace Operations Centre as Head of the Situational Awareness Support Section. He received his MSc in Computer Science in 2007 and a Diploma of Advanced Studies in 2009 from UNED (Spain). His main research interests are related to cyberspace situational awareness and decision making.

Alexander Pfeiffer is recipient of a Max Kade Fellowship awarded by the Austrian Academy of Science to work at the Massachusetts Institute of Technology (MIT), Department for Comparative Media Studies / Writing and former head of the center for applied game studies at Donau-Universität Krems. | https://www.alexpfeiffer.at

Dr Heloise Pieterse is currently employed as a senior researcher within the Cyber Warfare research group at the Council of Scientific and Industrial Research. She completed her PhD Computer Science degree in 2019, with a focus on identifying the authenticity of smartphone data. Her interests include digital forensics, mobile device security and cyber security.

Dr. Dorothy Potter has over 20 years' experience in Federal Financial Management. She is currently a Professor of Practice and Joint Professional Military Education Course Director, National Defense University, focused on Financial Management and Leadership, She is a Certified Defense Financial Manager and former Senior Audit Remediation and Risk Manager for Headquarters Marine Corps.

Lucas Potter is a Biomedical Engineering PhD Student and member of the SAMPE (Systems Analysis of Metabolic Physiology) Lab at Old Dominion University. His doctoral research is focused on cellular metabolism. Past research endeavors include human factors research (including human factors analysis of performance in virtual reality), modeling of physiology, and materials engineering.

Dr. Jouni Pöyhönen, Col (ret.) is a project researcher of cyber security programs in University of Jyväskylä. He received his PhD in information technology from University of Jyväskylä in 2020. He has over 30 years' experience of C4ISR systems in Finnish Air Forces. He has twenty research reports and articles on areas of cyber security.

Dr Keith Scott is a Senior Lecturer in English Language at De Montfort University UK, where he a member of the Cyber Security Centre. His research interests lie in the fields of the cultural and social implications of new technologies, online influence, and simulations/game-based learning.

Tiia Sõmer is researcher at Tallinn University of Technology, Estonia. Her research concentrates on modelling cyber crime, and other research interests include cyber warfare, cyber security workforce challenges, cybersecurity education and training. Before an academic career she served over 20 years in Estonian Army, in different posts including international assignments at NATO and the EU.

Kevin Spakes: Junior Cyber Security Engineer. I am a father of two wonderful kids. At Oak Ridge National Laboratory, I am an engineer, and have been part of the team that built and maintains the Cybersecurity Operations Research Range (CORR) for the Cybersecurity Research Group. My hobbies include backpacking, camping, and precision shooting.

George Stone was born in Clark AFB, Philippines and graduated with a BSc and MSc in Cybersecurity and Information Assurance from Western Governors University in 2011. He worked for Scripps Networks Interactive for over a decade as a Network Security Architect and currently works at the DOE/Oak Ridge National Laboratory as a Cyber Technical Expert.