iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** III **Month of publication:** March 2020

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue III Mar 2020- Available at www.ijraset.com

Automation in Cyber-Deception Evaluation with Deep Learning

Alex Mathew
Department of Cybersecurity, Bethany College, USA

Abstract: ***Cyber-deceptive evaluation is important in the current world of cyberspace defense which is vulnerable to various attacks. To protect an organization or national infrastructure from any form of cyber threat, cyber-deceptive defenses have taken their place in protecting these systems. For this reason, this paper proposes a deep learning methodology that can be implemented to conduct automated cyber-deceptive defenses. This methodology requires minimal human involvement and can prevent any impediments related to human deceptive research. Additionally, it can reduce the efficacy involved in the automation process before human subjects are taken for research. This paper leverages the current advancements in machine learning and uses a realistic and interactive approach for use by large web services which might be targeted. Also, an evaluation of intrusive detection systems has been integrated specifically for systems whose deceptive responses are equipped with the application layer. The results obtained from this paper suggest that developing adaptive web traffic equipped with evasive attacks are challenging and aggressive to cyber-deceptive defenses.***

Keywords: automative, cyber-deceptive, defenses, evaluation approach, framework, intrusion detection system (IDS).

I. INTRODUCTION

With the current growth in technology, cyber-deceptive defenses are increasingly being applied for securing government critical infrastructure and organizational systems from external cyber threats. According to [1], cyber-deceptive products will increase in the industry with numbers of up to 2 billion dollars by 2022. The new advances in cyber defense have integrated new layers which can improve the conventional defense. This is done by moving the traditionally-burdened asymmetries back to the hackers. For instance, the current cyber-deceptive defense introduces a challenge where attackers are left wondering which the actual vulnerability is, among a pool of vulnerabilities. Contrary to this, convention cyber defenses allow attackers to detect the vulnerability, thus, permitting them to successfully penetrate the network [2]. The increase in complexity among the newer technologies in software and networks has led to an increase in hacker-defender asymmetries. Cyber-deceptive strategies utilize this situation by leveling these asymmetries which, in turn, become essential for large-scale defenses. It is important to set up robust strategies of evaluation in the development of effective cyber-deceptive systems. However, the methodologies used in the cyber evaluation are frequently challenged by the difficulty in carrying out experiments using the relevant human subjects. Rare humans with exceptional expertise and cyber skills are required to capture the ingenuity, diversity, and resourcefulness of a system. However, there is a new deep learning approach that evaluates cyber-deceptive systems without the need for human subjects. To advance the current cyber-deceptive defenses, efficient methods of carrying out significant evaluations without human intervention are needed.

II. METHODOLOGY

It is extremely difficult to eliminate human subjects and depend entirely on machine learning approaches in the evaluation of cyber-deceptive systems. A common challenge in this new approach is the ability to emulate human-like decision-making capabilities which can automatically synthesize attacks. However, the new approach to be introduced relies solely on automated tools that can be used for offense. For instance, the human bots rely mostly on reports delivered by automatic bots which are, then, used to assess the attack status and send commands to the botnet [3] These are simple commands which can conduct kill chains that are automated and are recognized as malicious software. This is a human mastery which automates the machine section of the deception evaluation and is feasible and very useful [1]. The methodology of evaluation applies targets intrusion detection system (IDS) defenses which are enhanced with deceptive cyber-attack responses using means such as monitoring response. Figure 1 below shows the block diagram of and IDS monitoring system.

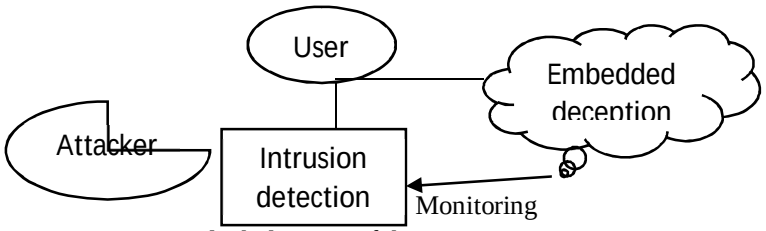


Figure 1: Block diagram of the monitoring system

Contrary to the conventional approach, IDS enhanced with deceptive responses continuously builds a certain model which contains a malicious and legitimate behaviour. This behaviour is based on the attack traces and audit streams that have already been collected from successfully conducted deceptions.

These deceptions can leverage the interactions occurring on the network and can solicit additional communication with attackers, thus, wasting their resources, misdirecting them, and gathering intelligence [4]. Also, a quantitative assessment of the resiliency of deceptive and adaptive web services can be conducted against adaptive attacks. This method is different from the techniques that conduct measurements on IDS accuracy.

Firstly, we present our method for generating traffic on the web to replay malicious user-behaviours which can be harnessed to generate tests and training datasets automatically for an attack. The testing harness is, then, discussed and analysed to investigate the impacts of different classes of attacks and attack instances on the accuracy and predictability of the intrusion detection [5]. This evaluation method can create attack kill chains and end-to-end workloads that are realistic and can test the cyber-deceptive defenses integrated into server applications in addition to decoy telemetry in processes for the extraction of features and IDS model evaluation [6].

Figure 2 below shows a flowchart used for an overview of the framework for generating traffic. This framework streams legitimate and malicious workloads that are encrypted and directs them to end-points which are enhanced with deceptions, thus, resulting in attack traces and audit streams that are labeled. Also, a support vector machine (SVM) can be leveraged to classify various features within the model.

SVM utilizes a complex technique that maps separated non-linear data to linearly distinguishing void in a higher dimension [7]. The confidence of the classification can be obtained using Platt scaling which using a formula (see appendix 1) where y is the label given, x is the vector used to test, f(x) is the output SVM, and A and B are scalar parameters [1]. Also, the success of the IDS can be estimated using Bayes theorem (see appendix 2) where the base detection rate is used. Additionally, A and D are random variables representing the attacker targeted and the detection classifier respectively [1].

III. RESULTS

The methodology applied enables concept learning of different IDS systems that can incrementally develop supervised models capable of capturing malicious and legitimate behaviour. The labeled data streams which are pre-processed can be used in feature extraction which is very efficient and can also be used to perform automatic extraction. These processes are periodically repeated according to the issued administrator-specific policy. The evaluation methodology also transmits packets which when received, form the basic information flow unit.

Encrypted opacity in the network during the process can lead to the extraction of features from TCP packet headers [8]. The transmission time and length of the packet data can be extracted from the network sessions where the histograms, time intervals, and directions can be obtained. Also, the cyber-deceptive evaluation framework can be used for monitoring threats and collecting complex data.

The methodology applied tracks two different events in the lifecycle associated with the monitoring decoys. The framework records a timestamp showing the start of an attacking session upon each decoy hit. This happens when a certain security condition is met and the session disconnects upon the arrival of the abort event.

Using this monitoring session, the session trace can be extracted, labeled, and stored outside the used decoy for any feature extractions that follow subsequently. The embedded deceptions are also allowed to host the attack sessions and can collect and label the traces effortlessly using our methodology.

Using our approach, it becomes easy to distinguish between separate input data namely audit stream which is collected at the targeted server, attack traces which are obtained at the decoys, and the monitoring stream which is the actual stream test obtained for the regular servers [9].

Each of these streams possesses network packets and operating system events that are captured in each of the servers. Also, our methodology minimizes the impact of performance by applying two efficient and powerful software monitoring systems. The two monitors are ‘sysdig’ which tracks system modifications and calls and ‘tcpdump’ which monitors network packets’ egress and ingress [1].

The framework avoids tampering of collected data by storing monitored data outside of the decoy environment. Our solution to monitoring network systems and collecting data has been designed to cover for large scale, distributed, and cloud deployment systems.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue III Mar 2020- Available at www.ijraset.com

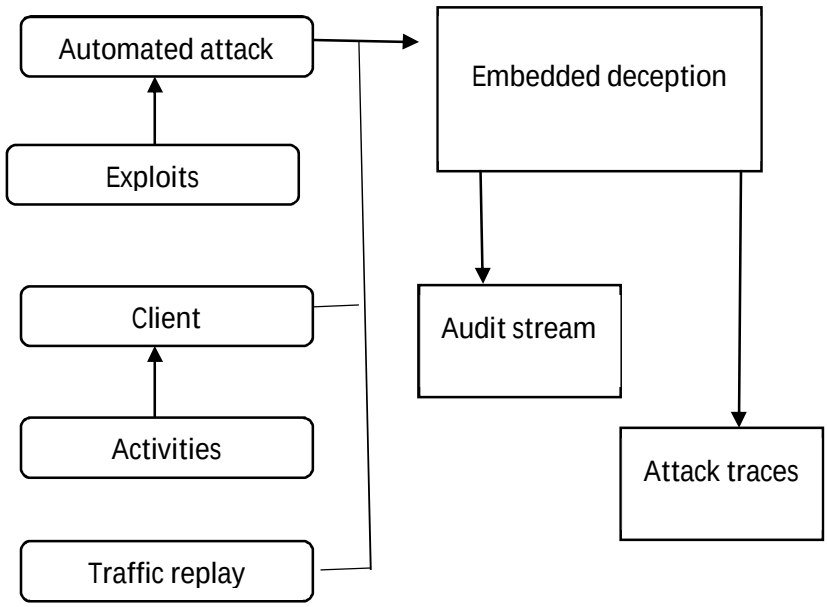


Figure 2: Flowchart for an overview of the framework.

IV. DISCUSSION

The cyber-deception evaluation approach improves the already existing thread detection model due to the IDS platform which deceptively offers cybersecurity solutions to web servers. The deceptively enhanced IDS platform can automatically feed attack traces that use a classifier to trigger honey-patch traps.

This is a core feature in the model that makes it advanced and more intelligent than conventional cyber defenses since it can easily be evaluated by the use of static datasets.

The traffic generator in the automatic cyber-deceptive evaluation model can be deployed on different hosts to prevent interference with the test server [10]. Also, the evaluation framework can account for differences in operation and the environment by developing different workload profiles.

This is mostly done according to the time of the day against different targeted configurations such as server workloads and background processes.

Additional targeted configurations are the network settings which include the congestion controls of the TCP. An important aspect of the evaluation framework is feature extraction which contains up to 1800 normal instances of training data and 1600 instances of attacks [11]. Additionally, the testing data for monitoring consist of 3400 normal instances and attack instances which are gathered at the unpatched web servers.

V. CONCLUSION AND FUTURE SCOPE

The deep learning automated cyber-deceptive evaluation technique is an advanced and efficient method that can protect complex cyber systems. The design of the framework is used for replay and generation of numerous web traffic that, in turn, develops and directs scripted attacks into output streams.

These attacks are conducted more effectively than any previous model and can train, test, and assess deceptive IDS systems which are known to be concept-learning. The main challenge for the automated cyber-deceptive evaluation framework is the inadequacy of datasets used in static attacks in the IDS which, due to this, cannot react to various deceptive interactions [12]. Using these datasets to test the deceptive defenses renders the applied deceptions useless. To improve on this, future models should apply a dynamic synthesis method of attack. This is a suitable technique for future cyber systems since it can learn the different ways in which the attacking agents can react based on the feedback they obtain from similar interactions during real-world interactions obtained from real attack data.

REFERENCES

[1] G. Ayoade et al., "Automating Cyberdeception Evaluation with Deep Learning", 2020.
[2] C. Du and L. Huang, "Sentiment Analysis Method based on Piecewise Convolutional Neural Network and Generative Adversarial Network", International Journal of Computers Communications & Control, vol. 14, no. 1, pp. 7-20, 2019. Available: 10.15837/ijccc.2019.1.3374.
[3] U. Noor, Z. Anwar, T. Amjad and K. Choo, "A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise", Future Generation Computer Systems, vol. 96, pp. 227-242, 2019. Available: 10.1016/j.future.2019.02.013.
[4] V. Urias, W. Stout, J. Luc-Watson, C. Grim, L. Liebrock and M. Merza, "Technologies to enable cyber deception", 2017 International Carnahan Conference on Security Technology (ICCST), 2017. Available: 10.1109/ccst.2017.8167793 [Accessed 12 March 2020].
[5] A. Gupta, A. Anpalagan, G. Carvalho, A. Khwaja, L. Guan and I. Woungang, "RETRACTED: Prevailing and emerging cyber threats and security practices in IoT-Enabled smart grids: A survey", Journal of Network and Computer Applications, vol. 132, pp. 118-148, 2019. Available: 10.1016/j.jnca.2019.01.012.
[6] S. Mansfield-Devine, "DevOps: finding room for security", Network Security, vol. 2018, no. 7, pp. 15-20, 2018. Available: 10.1016/s1353-4858(18)30070-9.
[7] Y. Qin and C. Huang, "Identifying underground voids using a GPR circular-end bow-tie antenna system based on a support vector machine", International Journal of Remote Sensing, vol. 37, no. 4, pp. 876-888, 2016. Available: 10.1080/01431161.2015.1137990.
[8] F. Araujo, G. Ayoade, K. Al-Naami, Y. Gao, K. Hamlen and L. Khan, "Improving intrusion detectors by crook-sourcing", Proceedings of the 35th Annual Computer Security Applications Conference on - ACSAC '19, 2019. Available: 10.1145/3359789.3359822 [Accessed 12 March 2020].
[9] L. Liu, O. De Vel, Q. Han, J. Zhang and Y. Xiang, "Detecting and Preventing Cyber Insider Threats: A Survey", IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp. 1397-1417, 2018. Available: 10.1109/comst.2018.2800740.
[10] M. Stoecklin, J. Zhang, F. Araujo and T. Taylor, "Dressed up", Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization - SDN-NFV Sec'18, 2018. Available: 10.1145/3180465.3180466 [Accessed 12 March 2020].
[11] M. Ozdag, "Adversarial Attacks and Defenses Against Deep Neural Networks: A Survey", Procedia Computer Science, vol. 140, pp. 152-161, 2018. Available: 10.1016/j.procs.2018.10.315.
[12] T. Shimanaka, R. Masuoka and B. Hay, "Cyber Deception Architecture: Covert Attack Reconnaissance Using a Safe SDN Approach", Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019. Available: 10.24251/hicss.2019.876 [Accessed 12 March 2020].

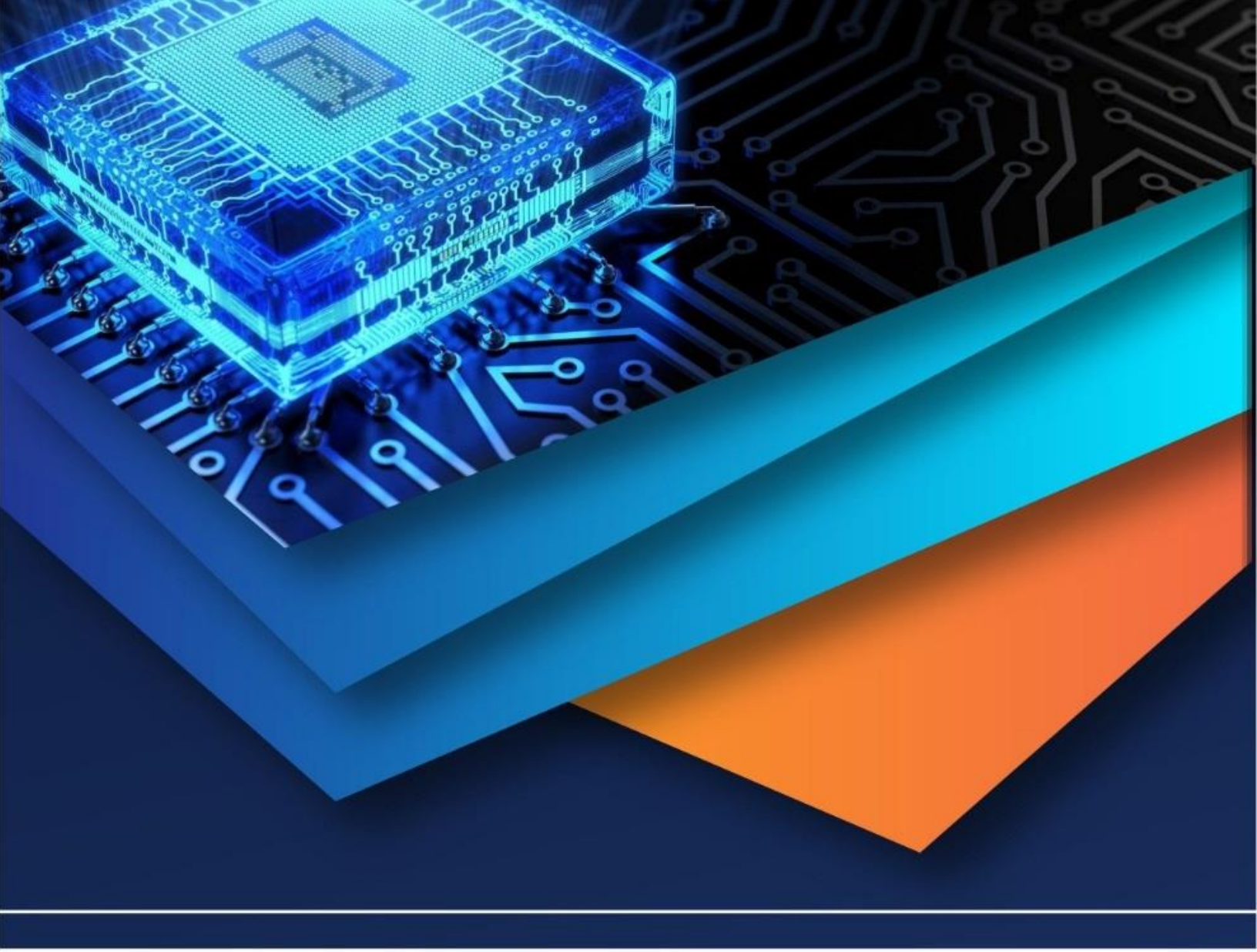
APPENDIX

Eq. (A.1)

$$P(y = 1|x) = \frac{1}{1+\exp(Af(x)+B}$$

Eq. (A.2)

$$P(A|D) = \frac{P(A)P(D|A)}{P(A)P(D|A)+P(\neg A)\,P(D|\neg A)}$$



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY