Efficient Machine Learning Techniques for Detection of Cyber Attacks

[1] G.AppaRao, [2]M.Rithvik
[12]SRK Institute of Technology,Enikapadu,Vijayawada

Abstract : Technology is changing its trends rapidly and in this regard it is highly essential to build a system that detects and manipulates the cyber attacks because now a days there are various frauds that are occurring due to the cyber attacks and this is the time to build a protective measure over the cyber attacks. Cyber security being one of the major wings in any technological support it is essential to build a cyber path over the several domains that are going to take place now a days but this is the time to build a cyber path over the cyber attacks. Security onion is one of the tools that is joined to build cyber path over these attacks. This path illustrates a pathway towards the utilization of security onion. Which has certain features of machine learning that are inbuilt in it?

Keywords **- Machine Learning, Cyber Security, Security Attacks, social networks, security tools.**

I. INTRODUCTION

In chess, a team of amateurs operating even standard desktop PCs dramatically outperforms both the strongest human players and the most powerful supercomputers in isolation. There is a small quote in English "Technology makes us faster and farther than thinking of human mind". In this scenario of utilization of technology with this technology cyber crime is also increasing and changing its path from day by day. In this scenario it is essential for a layman to identify and organize all the things that are pertaining towards the technology and protect from the cyber crimes. In order to analyze the unwanted malware that is coming over a period of time from various internet sources is being a tough task to analyze the unwanted malware coming from the internet and using it without proper understanding on that malware. In the olden days a serious problem called Y2K problem takes place and it crashes several systems and several companies went into the losses. There should be a problem channel to identify these kind of problems and make primitive measures not to repeat these problems for further growth rate of technology.

II. STATE OF THE ART

Machine Learning in Cyber Security Domain; In recent years, attackers have been developing more sophisticated ways to attack systems. Thus, recognizing these attacks is getting more complicated in time. Most of the time, network administrators were not capable to recognize these attacks effectively or response quickly. For this purpose there are a lot of algorithms have been developed until today. These algorithms are used for many research area such as; image processing, speech recognition, biomedical area, and of course cyber security domain. One of the biggest barriers to human intelligence is language. With modern natural language processing, machines can process text irrespective of language, including slang and industry jargon. The battle in threat intelligence is balancing time and context. Analysts need intelligence promptly, but they also need enough information to make a decision on how to act. This is only possible using modern AI and machine-learning processes

III. CURRENT WORK AND PRELIMINARY RESULTS

Security Onion is configured to run on version 12.04 of any Ubuntu-based Linux server or desktop distribution, such as Ubuntu, Lubuntu, Xubuntu, and Kubuntu.

Security Onion

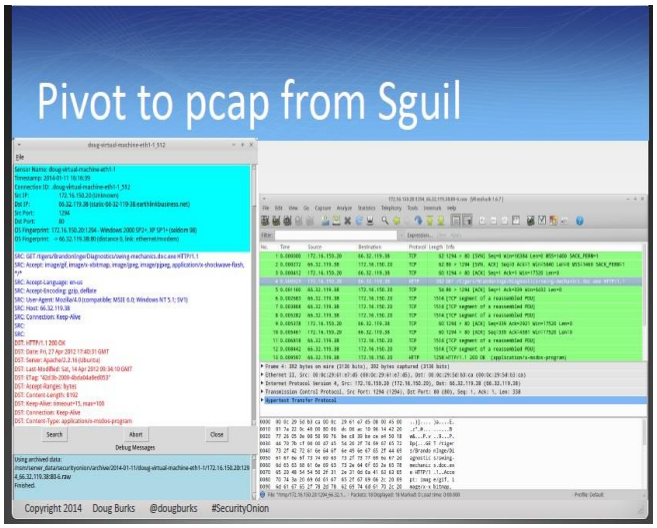
The aim of Security Onion is to provide a good security aspect with the integration of several tools together as a single base platform to utilize enhance and make a change over few or more data.

The job of security onion is to predict the malware automatically and display the contents of that particular malware.

This makes a sense of identifying only a single malware and analyzing the sub contents of that particular malware with the help of various tools.

The tools that are available in the security onion are as follows:

1. Wireshark
2. Bro
3. Network Minor



The above is the data that is generated by using the security onion tool with the help of network minor tool.

1. Wireshark: It is the tool that act as a base to analyze the malware and displays the individual contents in a raw data form..

2. BRO: It is the tool that enhances all the contents of a malware file by addressing the coding defects.

3. NETWORK MINOR: The most widely used tool in the intrusion detection system is the network minor where a data can be processed in a structured order manner and displays each and every content of the malware file with the defects in a structured manner. By using or predicting this tool a user can easily identify few of the defects that are coming over from the system and can easily predict that issues that are abandon.

MACHINE LEARNING AND CYBER SECURITY
ZERO TRUST FRAMEWORKS

Pertaining to the industry it is essential for an industry to develop a zero trust framework where a user can get the system with all the security features embedded in it and it plays a major role for a company to test all the developing framework automatically with the comparison of position of test cases along with the data present in the system. Now a days it is essential to develop an application with the security service embedded in it and this serves the zero trust model.

RED HAT TEAM

Every industry have some threat with the hackers and in identifying them and developing them is the greatest job for all the employees residing in the company and red hat team is the team which thinks and works like hackers in that particular company and make protective measures before the attack is going to take place.

IV. FUTURE WORK

As businesses and consumers accelerate the adoption of internet-connected devices, Internet of Things space is forcing companies to think holistically about the security behind their devices.

The major security problems that are seen with IoT devices:

- Cloud Attacks
- Botnet Problems
- Transport Encryption
- Insecure Cloud and Web Interface
- Insecure Software and Firmware
-

Need to take necessary actions to secure them now before the problem becomes unmanageable. Over the next 10 years the Internet of Things (IoT) will start to develop distinct segments, each of which will end up with its own security solutions, device security will mature and stabilize significantly.

IV. CONCLUSION

Machine learning approaches are increasingly employed for multiple applications and are being adopted also for cyber security; hence it is important to develop algorithms that can achieve adequate results. We are trying applying these techniques for different cyber security problems. We initially propose an original taxonomy of the most popular categories of ML algorithms and show which of them are currently applied to which problem. Then we explore several issues that influence the application of ML to cyber security. Our results provide evidence that present machine learning techniques are still affected by several shortcomings that reduce their effectiveness for cyber security. All approaches are vulnerable to adversarial attacks and require continuous re-training and careful parameter tuning that cannot be automatized. Moreover, especially when the same classifier is applied to identify different threats, the detection performance is unacceptably low; a possible mitigation can be achieved by using different ML classifiers for detecting specific threats. Significant improvements may be expected, especially considering the recent and promising development

of adversarial learning. Our conclusion based on our study is that machine learning techniques can support the security operator activities and automate some tasks. In our further work it will be presented.

REFERENCES

[1] S. Habibi Lashkari A., Draper Gil G., Mamun M. and Ghorbani A., "Characterization of Tor Traffic using Time based Features," Proceedings of the 3rd International Conference on Information Systems Security and Privacy – Volume 1, pages 253-262, 2017
[2] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," Science, 2015.
[3] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, 2015.
[4] A. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, 2015.
[5] E. Blanzieri and A. Bryl, "A survey of learning-based techniques of email spam filtering," Artificial Intelligence Review, 2008.