# Related Literature

## Cyberthreat Intelligence

In the last several years, a disturbing trend—attackers are innovating much faster than defenders are. Large botnets are available for rent, allowing attackers to send spam or launch DDoS attacks at will. Many attackers reuse malware and command and control protocols and methods, adapting their “products” over time to keep ahead of the antimalware industry and security professionals. The idea behind cyberthreat intelligence is to provide the ability to recognize and act upon indicators of attack and compromise scenarios in a timely manner. While bits of information about attacks abound, cyberthreat intelligence (CTI) recognizes indicators of attacks as they progress, in essence putting these pieces together with shared knowledge about attack methods and processes. Cyberthreat intelligence, when used correctly, can help defenders detect attacks during—and ideally before—these stages by providing indicators of actions taken during every stage of the attack. (Shackleford, 2015)

## Machine Learning

Traditionally, network intrusion detection systems (NIDS) are broadly classified based on the style of detection they are using: systems relying on misuse-detection monitor activity with precise descriptions of known malicious behavior, while anomaly-detection systems have a notion of normal activity and flag deviations from that profile.1 Both approaches have been extensively studied by the research community for many years. However, in terms of actual deployments, the team observed a striking imbalance: in operational settings, of these two main classes most people find almost exclusively only misuse detectors in use—most commonly in the form of signature systems that scan network traffic for characteristic byte sequences. It can be surprising at first to realize that despite extensive academic research efforts on anomaly detection, the success of such systems in operational environments has been very limited. In other domains, the very same machine learning tools that form the basis of anomaly detection systems have proven to work with great success, and are regularly used in commercial settings where large quantities of data render manual inspection infeasible. (Robin Sommer, 2010)

## Intrusion Detection System

Intrusion Detection System (IDS) is meant to be a software application which monitors the network or system activities and finds if any malicious operations occur. Tremendous growth and usage of internet raises concerns about how to protect and communicate the digital information in a safe manner. Nowadays, hackers use different types of attacks for getting the valuable information. Many intrusion detection techniques, methods and algorithms help to detect these attacks. These application areas made the network an attractive target for the abuse and a big vulnerability for the community. Malicious users or hackers use the organization’s internal systems to collect information and cause vulnerabilities like Software bugs, Lapse in administration, leaving systems to default configuration. As the internet emerge into the society, new stuff like viruses and worms are imported. (S.Vijayarani, 2015)

## Detection of Attacks

Intrusion detection systems (IDSs) are usually deployed along with other preventive security mechanisms, such as access control and authentication, as a second line of defense that protects information systems. There are several reasons that make intrusion detection a necessary part of the entire defense system.

Traditional systems and applications were developed without security in mind. In other cases, systems and applications were developed to work in a different environment and may become vulnerable when deployed intrusion detection complements these protective mechanisms to improve the system security. Moreover, even if the preventive security mechanisms can protect information systems successfully, it is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future attacks. The attack can be launched in term of fast attack or slow attack. Fast attack can be defined as an attack that uses a large amount of packet or connection within a few second. Meanwhile, slow attack can be defined as an attack that takes a few minutes or a few hours to complete. Currently IDS is used as one of the defensive tools in strengthens the network security especially in detecting the first two phases of an attack either in form slow or fast attack An intrusion detection system can be divided into two approaches which are behavior based anomaly and knowledge based. Hence, unknown attacks in network intrusion pattern and characteristic might not be capture using this technique. Anything that does not correspond to the system profile is flagged as intrusive. False alarms generated by both systems are major concern and it is identified as a key issue and the cause of delay to further implementation of reactive intrusion detection system. (Amrita Anand, 2012)

## Snort based Intrusion Detection System

Snort is the signature based anomaly detection method. It captures the incoming packets that are transmitted over the network (Roesch, 1999). It incorporates rules within it and thereby performs preprocessing by itself. It mainly reduces the burden of system administrator. New rules can be included within the rule set per the occurrence of new attacks. Snort is used with statistical methods to improve the detection strategy in real time. (G.V. Nadiamma, 2013)

## Automatic Snort IDS rule generator based on Honeypot log

Intrusion detection is an attempt to monitor and detect illegal data stream. This is one way that can be used to reduce the illegal actions enters the network. The data flow to be detected is divided into two categories, namely Signature Based intrusion and Anomaly Based intrusions. Snort rule generation based on honeypot log has been developed at various university and national labs research cyber security concerns. (Sagala, 2015)

## 0-Day Vulnerabilities

One such attack that this thesis will address is the zero-day, or commonly abbreviated 0-day, vulnerability which can cause damage as it is unknown what the target of the attack might be when it is first utilized or how to guard against it. 0-day vulnerabilities are those that have just been released and may or may not have a patch against them, some of which may not be known to the vendors for a patch to be created. Several applications exist to help security analysts find these vulnerabilities. One category of these tools is Intrusion Detection Systems, or IDS, which monitor network traffic for predefined patterns. An intrusion detection system, IDS, provides a stack of hardware and software components that listen to all traffic on a hardware network interface card or from a packet capture file and scans each packet looking for predefined patterns, such as a flood of packets, or invalid packet headers which may indicate a problem. It then responds to these patterns in a predetermined matter, from recording the attempt, to warning administrators through email or visual alerts. As hackers become more creative in their attacks and begin using exploits that may or may not be known to the environment, these systems will help in analyzing potential threats. (Truhan, 2011)

# Bibliography

Amrita Anand, B. P. (2012, August). *An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols*. Retrieved from International Journal of Advanced Research in Computer Science and Software Engineering: https://pdfs.semanticscholar.org/72e2/b7045910bda635d0864117438553d13c45b6.pdf

G.V. Nadiamma, M. H. (2013, January 11). *Handling Intrusion Detection System using Snort Based Statistical Algorithm and Semi-supervised Approach*. Retrieved from Pak Academic Search: http://pakacademicsearch.com/pdf-files/eng/392/2914-2922%202013(Vol.%206,%20Issue%2016).pdf

Robin Sommer, V. P. (2010, May 16). *Outside the Closed World:*. Retrieved from UTDALLAS: https://www.utdallas.edu/~muratk/courses/dmsec\_files/oakland10-ml.pdf

S.Vijayarani, M. S. (2015, February). *INTRUSION DETECTION SYSTEM – A STUDY*. Retrieved from AIRCC Publishing Corporation: http://airccse.org/journal/ijsptm/papers/4115ijsptm04.pdf

Sagala, A. (2015, October). *Automatic SNORT IDS Rule Generation Based on Honeypot Log*. Retrieved from Research Gate: https://www.researchgate.net/publication/301325633\_Automatic\_SNORT\_IDS\_rule\_generation\_based\_on\_honeypot\_log

Shackleford, D. (2015, February). *Who's Using Cyberthreat Intelligence and How?* Retrieved from Sans: https://www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767

Truhan, N. D. (2011, August). *INTRUSION DETECTION FOR 0-DAY VULNERABILITIES*. Retrieved from OhioLINK: https://etd.ohiolink.edu/rws\_etd/document/get/kent1310682482/inline