2020 International Conference on Software Security and Assurance (ICSSA) | 978-1-6654-3246-7/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICSSA51305.2020.00018

Anomaly Detection to Protect Networks from Advanced Persistent Threats Using Adaptive Resonance AI Concepts

Syed Rizvi, Tanner Flock, Travis Flock, Iyonna Williams
Department of Information Sciences and Technology, Pennsylvania State University, Altoona, PA
srizvi@psu.edu; txf5163@psu.edu; tqf5159@psu.edu; iaw5056@psu.edu

***Abstract*—In this paper, we will improve the Advanced Persistent Threats (APT) attack detection rate accuracy by using an artificial intelligence based anomalous intrusion detection that will be based on unsupervised learning techniques. This system will be mainly network-based with a thin layer running on the host device. We plan to mainly use an unsupervised artificial intelligence technique that utilizes Adaptive Resonance theory that will be paired with a signature-based system that will filter anomalous data and significantly improve detection rates and decrease false positive rates compared to typical anomalous intrusion detection system (IDS). If proven here, this system could be applied to future IDS and can significantly increase overall network security for an organization.**

Keywords*—*Intrusion detection and prevention; artificial intelligence; network security; advanced persistent threats

I. Introduction

Network security has been a concern of many corporations for as long as the dawn of the Internet. The challenge to sustain goals like confidentiality, integrity, and availability has proven to be an extremely difficult task. As IT professionals spend time solidifying networks from known attacks, attackers are staying one step ahead making for unsecured networks. Even today, defending against attacks like ransomware and credit card theft remains the top priority of many companies. When it comes to network security, an IDS offers a large amount of its security by monitoring the network traffic in various ways. Building an effective IDS is difficult and requires precise algorithms to eliminate false alarms. Some systems can have thousands of false alerts reducing the security of the network. A perfect IDS is the mix of a high detection rate with a near zero false positive rate [5].

Used in conjunction with user authentication, encryption, and firewalls, a proper intrusion detection system (IDS) will defend against certain exploits and vulnerabilities within a network. Unlike firewalls, IDS's can react to more situational attacks such as APT's, DoS, and U2R attacks [1]. IDS's are used to determine normal acts from abnormal and alert an administrator in real time. In this paper, we specifically focus on reducing false positives and increasing detection rates in regard to an APT. This paper analyzes the reasons for the low detection rate of APTs in anomaly systems and solutions for improvement.

Intrusion detection is typically based off two techniques: signature-based detection and anomaly-based detection. Signature-based detection involves monitoring network packets using various rule sets that identify malicious activities based on those predetermined sets. This detection system can allow for quick identification of malicious activity as long as the proper rule sets are used for specific scenarios. This system fails to detect novel attacks, as their signatures are not within the database and suffer when it is faced with anomalous or undefined data that is not a part of the rule set [2]. This allows for the threat to pass without detection. In a situation as such, where the threat cannot be identified by strictly a rule set, anomalous-based detection can be implemented. This detection system establishes a baseline or a model of normal network activity. This baseline is then used alongside a rule set in order to raise an alarm whenever activity falls within the rules or is anomalous compared to the baseline [2]. Using an unsupervised learning artificial intelligence technique based on Rossberg's Adaptive Resonance Theory (ART), a system framework can be constructed that logically allows for the sorting and identification of anomalous malicious data.

There are many different existing techniques and models that adequately handle Intrusion Detection, but the major challenges these models face are security and accuracy issues pertaining to the detection rate, as well as the false positive rate [4]. Specifically, APTs in anomalous-based Intrusion Detection shows significantly lower detection rates as well as increased false positive rates versus its denial of service and remote to user counterparts that typical IDS defend against [1]. This can be attributed to the nature of an APT and how it relates to the typical parameters used by IDS such as bandwidth usage, out-of-protocol events, and payload limitations [2]. This paper will improve on the typical Signature-Based IDS using an anomaly-based AI system that will consist of an unsupervised learning component known as Adaptive Resonance Theory (ART).

II. Related Work

The C4.5 data mining algorithm was created by J. Ross Quinlan and is known as a supervised technique for training artificial intelligence. It receives its name from a precursor algorithm, ID3. C4.5 is multiple algorithms, C4.5, C4.5-no-pruning, and C4.5-rules, but they are combined into one name. It is a very complex algorithm because it learns to map from the values of the attributes, then applies that to new, unseen

978-1-6654-3246-7/20/$31.00 ©2020 IEEE
DOI 10.1109/ICSSA51305.2020.00018

instances C4.5 uses decision trees to split the data into smaller pieces, then tests for a specific attribute to help narrow down a prediction of the class variable. The process will continue to split and test until the subsets become "pure", at this time the decision tree will stop growing. The main attribute that C4.5 looks for when making a decision tree is called a gain ratio. Gain is described as "reduction in entropy of the class distribution due to applying a test." C4.5 can also apply new rules to a decision tree, and it will adapt to those new sets of guidelines [4].

The C4.5 algorithm is known for its pruning ability that is based on rules given from a specific decision tree. A decision tree is viewed as a combination of rules where every rule follows a path from the roots of the tree, up to individual leaves. The predecessors in each rule are the decision conditions through the path, and the result is the class label. At the beginning of the process, the algorithm will view an individual class from the dataset and create rules originating from the unpruned decision tree. For each established rule, the algorithm will perform a "hill-climbing" search through the tree if any predecessors can be deleted. The deletion of predecessors is similar to "knocking out" nodes in an "induced" decision tree. Due to this, the algorithm's negative pruning approach is used here. The number of rules that are remaining after this process is almost guaranteed to be drastically smaller than the amount of leaves, or paths, in the initial decision tree. The main disadvantage of rulesets in the C4.5 Algorithm is that as the size of the dataset increases, there are accelerated increases in learning time [10]. A common problem that can occur is that the decision trees have unneeded complexity, this can bring inaccuracy as well. To combat this, tree pruning was developed to slimline the process and improve accuracy. The majority of the time, tree pruning is executed after the tree is "fully grown". When it is executed, it will run from the bottom to the top of the tree. Various innovations in C4.5 such as reduced error pruning and pessimistic pruning have helped to improve tree pruning and C4.5 overall. Reduced error pruning uses a different test dataset, but it is different from tree pruning because it uses the fully induced tree to classify the instances. Pessimistic pruning does not need a different test set because it only estimates the error percentage that could happen due to the number of misclassifications in the training set [4].

There are many proposed improvements to the C4.5 algorithm. One is an improvement that three scholars had come up with to further the decision-making skills of the C4.5 algorithm. It is a two-level model selection method based on a top model construction process, as well as an underlying model selection process. The top model construction process is based on assertive reasoning and an underlying model selection process is based on the C4.5 decision tree. This proposed method reduces the requirements for emergency domain knowledge and improves the accuracy and speed that the algorithm can process and detect threats. This improved model was created for the Tianjin explosions in 2015 that took the lives of 173 people. They hope to further the algorithm and expand upon the decision trees to save lives and prevent this from ever happening again [3]. Another skill that the C4.5 algorithm possesses is called windowing. Windowing is the technique used to create decision trees for subgroups of larger training sets. Sometimes, the decision tree will be too large and not accurate enough for the data in the window. To fix this, the algorithm creates a larger window repeatedly until the final tree is created. Often, the process will create many smaller trees and select from the trees created for the best one. The repeated process is called the "trials" technique. When the windowing and trials technique are combined, it creates a very efficient and accurate decision tree [9]. Typically, an IDS is solely signature-based or anomaly-based, minimizing system complexity and resource usage while achieving reasonable results with respect to detection rate and the false alert rate. The hybrid system proposed by Ali Aydin [11] is one that consists of both anomaly and signature-based systems, running identical layers as the AEGIS system (both host and network). This system was developed under the premise that signature-based systems have a natural disadvantage of only being able to detect known signatures and that typical anomaly systems have rather high false alert rates.

III. Proposed Advanced Entropy Guided Intrusion Detection System (AEGIS)

Our proposed solution consists of a hybrid system that will use both signature and anomaly-based IDS methodologies along with host and network configurations. We call it AEGIS (Advanced Entropy Guided Intrusion Detection System). The problem faced with most IDS's is that they have a very low detection rate for U2R attacks making for a weak point in any network. To combat this, AEGIS will run both on Host and Network systems allowing for both layers to be monitored, giving a network the maximum amount of protection. Typically, IDS's will run solely on the network, meaning privilege escalation could happen without detection. With the use of a host-based system, the IDS is better able to identify threats. AEGIS will also be able to take declared "clean" data that made is successfully through the signature-based system, run it through the anomaly-based system, confirming its cleanliness or disproving it. If disproved, the data will be able to feedback into our signature-based system, improving the ruleset, leading to progressively less contaminated data. The combination of these systems into AEGIS will allow for greater overall network security [3]. A basic system architecture can be seen in Fig. 1.

A. Defining Normal Baseline Behavior (Profile Generation)

For the anomaly system to detect anomalies, it must have a predefined list of raw data that is inputted into the system in order to create and identify a statistical norm. This statistical norm is then turned into a normal behavior baseline; a crucial component in all anomaly-based IDS and essentially is the foundation for the system to learn. Once a normal behavior baseline is established, it can be compared with live data from an organization. If the data varies greatly and patterns or activities do not match to a certain degree in regards to the normal baseline, the AI system will be able to flag that data as anomalous, allowing for further inspection of the data to take place and eventually leading to the data being filed as malicious or clean [6]. As stated above, defining this normal behavior baseline accurately is crucial to the system's ability to

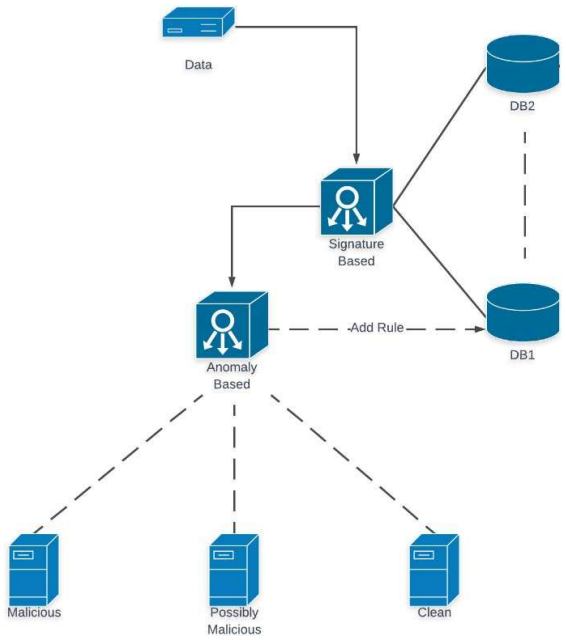

Figure 1: AEGIS System Architecture

learn. If the normal behavior baseline is created carelessly or is missing important criteria, the effectiveness of the system will be significantly impacted. This poor defining of the behavior will expose a vulnerability in the organization's network that would allow for detrimental events to take place. Many techniques can be applied to generate this normal baseline behavior. Most if not all modern anomaly systems incorporate multiple information gathering techniques so that anomalies can be better defined and detected. The techniques used in this system are discussed below:

Audit Trails: Audit trails is a common technique used in early IDS's and remain a necessary component in any anomalous IDS. This information gathering technique is generated through individual host data on the network, collecting information such as a chronological order of system activities that allows for the clear identification of the systems state at a given time. This information is somewhat valuable by itself, but when paired with other techniques, audit trails can reveal a vast amount of information regarding host activities when examined in a strong anomalous system. An audit trail technique has a great benefit over other techniques in the sense that it collects a massive amount of user/host data, but this massive collection of data can impact overall network/device performance negatively and bog resources.

Network Monitors: Network monitors have been referred to by many as "the solution" to intrusion detection. Network monitors provide extremely valuable information based upon network traffic and helps to create profiles of a user's network activity. Network monitors can allow for the anomaly system to detect more intricate attacks that would otherwise breach a standalone audit trail system. This network activity could potentially be paired with audit trails to recognize even more complex attacks. Network Monitors would cause little to no impact on an organization's resources, as it is placed at a single control point where it can receive all host network data as well as general network data.

Tripwires: A simple yet effective technique for information gathering would be a tripwire technique. "Tripwires" are specifically and strategically placed to monitor certain files or system characteristics. These tripwires are especially important in securing an organization's network against attackers who attempt to create a back-door entry point (a crucial part in the APT strategy). Tripwires can be customized to specific locations in an organization's network, and generally monitor important activities such as file additions, modifications, and deletions [15].

Configuration Checking Tools: Typically, configuration checking tools are used in a standalone fashion apart from an IDS, but when it comes to anomaly detection, this information gathering technique can be very valuable. This tool can be used to detect insecure operating systems, file systems, and network configurations. This data is useful in regard to revealing system misconfigurations that may have malicious intent [15].

Operating System Commands: Operating system commands are used commonly by system administrators to manually monitor and detect security breaches. These commands can give insight into an attacker's intent or method of attack. These commands can also help the anomalous system look for hidden processes as well as malicious tampering of log files [15].

B. Artificial Intelligence using Adaptive Resonance Theory

The anomaly-based system uses statistical techniques to decide about a given piece of data or packets, defining it as malicious, non-malicious, or clean. This decision can be based off many different techniques such as clustering, Bayesian networks, data mining, neural networks, and more. Using one or a mix of these techniques allows for the anomaly system to collect data, therefore enabling it to create a statistical model that would better understand threats that a static signature-based system could not [13]. The utilization of Artificial Intelligence (AI) component within the system would leave the system better equipped than a standard anomaly system when it comes to identifying and understanding threats from a statistical standpoint. The use of unsupervised learning through AI has proven to show large increases regarding detection rates and lowering of false positive rates [12]. An AI utilizing an unsupervised learning model has the unique capability of training itself with no supervisor and unlabeled data; meaning that the model must create meaning from the data with no previous inferences or knowledge. This unsupervised learning capability is a strong technique for the anomaly-system, as it adds a more versatile system for examining odd or unknown data. This AI component would allow for a more efficient and better performing IDS that would be well suited for creating statistical models and pulling meaning out of those models.

The AI component of the Anomalous system will be based around a powerful unsupervised learning technique known as Adaptive Resonance Theory (ART). Stephen Grossbergs ART is a unique process of labeling and predicting information,

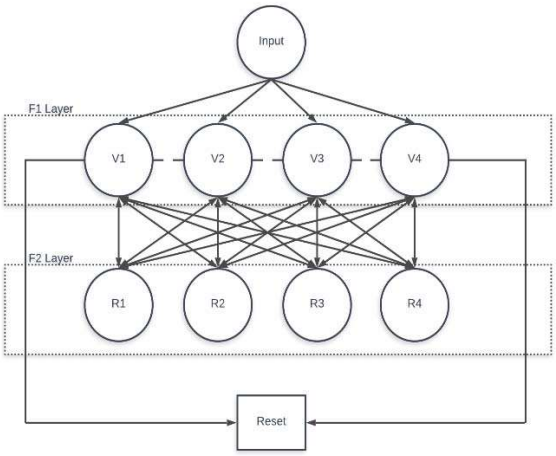

Figure 2: Adaptive Resonance Theory

similar in a way to how the human brain can understand the information given and adapt and change in real time to come up with a reasonable solution. ART is widely used in all fields for its ability to quickly categorize and predict data in a changing environment all while incrementally improving itself (and the AEGIS system) as a whole. This unique capability makes ART the perfect candidate for unsupervised learning in the Anomalous system. The ART AI technique, shown in Fig. 2, uses what Rossberg calls "top-down" expectations matched with "bottom-up" expectations of the data to understand crucial patterns that in the case of an IDS, could significantly improve detection rates and lower false positive rates [13]. A good enough match between the two expectations can lead to resonance and quick learning of the data by the system. A large enough mismatch would lead to hypothesis testing or memory search to learn and predict more.

An example of this would be if ART was hypothetically asked to locate an object such as a red hat. ART would input the expectation of red hat in to its top-down expectations, eventually leading to an excitatory match between the bottom-up expectations which will generate the resonant brain states. When the matching of these expectations in strong enough, positive feedback modules within ART increase which increases mutual activation of the data sets, eventually creating more resonant brain states. These resonant states provide a global expectation of incoming data which then teaches the ART system what data is worthy to learn. If specific resonant states exist for long enough and at a high enough level during computation, the system will understand more about the data that is creating resonant states [14].

The architecture shown in Fig. 1 is that of a typical ART unsupervised learning setup. The ART architecture can be broken down into 2 layers: F1 and F2 which are the grounds for the system to learn. The F1 layer can be treated as short-term memory while the F2 layer is viewed by the system as long-term memory. A vigilance parameter or degree of similarity is assigned to each layer allowing the system to create more general memories when the vigilance parameter is smaller and more detailed memories when the vigilance parameter is larger [12]. Using these memory layers as well as a reasonable vigilance parameter gives rise to the systems unique capability of learning without having to be trained, also known as unsupervised learning. This learning is then done through 3 distinct phases: Recognition, Comparison, and Search. In the recognition phase, the data is inputted into the system and originally classified using data from better trained and classified nodes, or mature nodes, that have satisfied the vigilance parameter requirement. If the classifications applied to the input data are comparable to the classification of a mature node, a gain value is given to the node eventually allowing the node to create a stronger resonant state leading to a smarter overall system. In the comparison phase, the reset mechanic is introduced into the system. This mechanic allows the nodes with low information gain to be reset, reclassified, and ran through the system again in an attempt to have a higher degree of similarity to a mature node than its previous state. In the search phase, the system will search for possible resets that have not been performed in the above phases. If no reset is needed, the classification is over. If a reset is needed, the process will be repeated until the node is no longer reset [12].

C. *Host/Network Implementation*

IDS can be classified as Host-based or Network-based. A Host-based system runs locally on the computer, analyzing local system functions such as logs or system calls [7]. These systems tend to be resource intensive and not used as often. A network-based system runs over the whole network analyzing things such as packets and traffic. In this case, the system draws from the existing infrastructure. AEGIS uses both Host-based and Network-based systems to defend against attacks on either front. The network-based would be the main system with our Host-based being a light "piggyback" in order to keep computations to a minimum. Typically, User-to-Root attacks cannot be detected by Network-based systems since privilege escalation happens locally. This is where the Host-based system fits perfectly into AEGIS. A Host-Based system can read logs and instantly determine if there is a privilege escalation. Since this would be considered a critical piece of information and could cause the most network damage, the host-based system would immediately send a quarantine signal to the network side, disconnecting the computer from the network. If the escalation was legitimate, the administrator could link the computer from the network side. This allows the systems to work together to prevent a zero-day exploit that would give an attacker full administrator privilege. The Network-Based system will be the main, using C4.5 trees and signature-based trees with rulesets, it will handle most of the computations needed for AEGIS on delegated infrastructure that would not clutter current infrastructure. This is the most efficient way to analyze the large amounts of network data in a fashion that will yield results [8].

D. *Systems Working in Conjunction*

These intrusion detection methods will be almost entirely located on the network side, yet a thin layer will be running on the host location that can input back into our network system where the data can then be analyzed. This would theoretically provide superb protection against a U2R attack as most IDS's are based in one location or the other, forcing a system of

compromises that are more effective against one attack versus the other. The AEGIS system should face no such compromise as it is built with both locations in mind allowing data to be taken from both locations but primarily processed within the network location. One could suspect that the system would be computationally expensive, and that would be a proper claim, yet the systems products are theorized to be more than the inputs. Meaning despite the computational power it would take to run the systems in conjunction, the product of running these systems in conjunction would always yield higher output. This can be due to the way the anomaly-based system "teaches" the signature-based system by actively checking the signature systems work to see if it can identify a threat the signature system cannot. If it does identify a threat the signature system cannot, new rulesets can now be made to improve the signature system progressively further with each new ruleset. Also, the system runs only a thin layer to the host location in order to save computational power that traditional host-based systems tend to use up. This creates a synergetic relationship between the AEGIS system parts, therefore creating a superior IDS that is more capable of detecting U2R attacks. The entire AEGIS system is based on 2 intrusion detection methods; signature-based and anomaly-based working in conjunction with one another, as shown in Fig. 3.

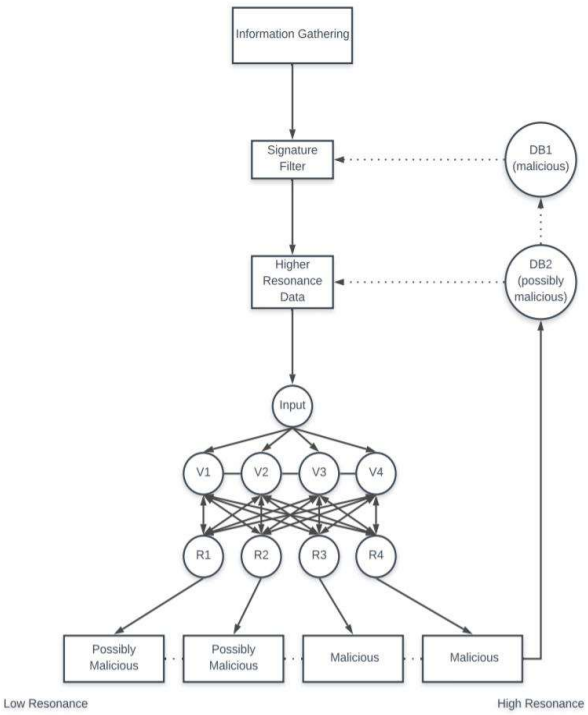

Figure 3: System Architecture

IV. Analyzing the Effectiveness of AEGIS Using Case Studies

The AEGIS systems usability can be seen in the way it handles data as well as how it stacks up against some of the most difficult to defend attacks. Using three different case studies, we demonstrate the effectiveness of the system when it is faced with attacks such as: User 2 Root (U2R), Denial of Service (DOS), and Advanced Persistent Threats (ATP's).

A. Defending Against User 2 Root (U2R) Attacks

William is an active IT employee of a large defense contracting firm where he performs basic level tasks for his company. William has recently become upset, as his co-worker who has been at the company significantly shorter, has already received a promotion that he was destined to receive. In a fit of rage and anger, William decides that he is going initiate a U2R attack to escalate his privileges to gain root access to the system, as he knows that typical IDS are network based, and therefore blind to U2R attacks that are host-based. Little did William know that the company he was working for had recently upgraded to a Hybrid IDS known as AEGIS. The AEGIS system is largely network-based, with a very small layer running on the host devices that allow for communication to the bulk of the system. This small host layer is capable of monitoring escalations through a predefined rule set. If the escalation is not within the predefined ruleset, it will still be sent off to the anomaly-based system, where the data can be further examined and flagged through the C4.5 decision tree. The system would then flag the action as malicious, immediately quarantining the host device where the escalation originated and alerting the network administrators as well as the IT security team. In this case, Root access would have been avoided due to the quarantining of the device along with the quick identification of the attack. This system is invaluable to a company such as the one William works for, as they deal with highly classified and sensitive information, and cannot afford a security breach, especially one as aggressive as a U2R attack.

B. Defending Against Denial of Service (DoS) Attacks

Timmy is an average teenage boy who loves to play video games. One day when Timmy was playing his favorite game, he got angry at the other team and typed some explicit messages. Any type of profanity is strictly prohibited by the terms of the game and administrators ban Timmy for 3 days as a punishment for his actions. Timmy disagrees that he should be banned and sets up a DoS attack as revenge. He rents multiple servers from different companies that all have unique IP addresses. Timmy then begins to spam thousands of messages to the server that read "Unban my account!". A signature-based system has a hard time defending against attacks like these, but AEGIS can make rules regarding similarities in messages. For example, a signature-based system could only block out one IP address at a time, but AEGIS takes in many factors. Message size, content, source, destination, and more. The system then takes similar attributes and ranks them to determine if the packet is malicious or not. In this case, the messages had similar content allowing for the system to create a rule to not allow packets with that specific content in, along with blocking the source IP for any future attacks.

C. Defending Against an Advanced Persistent Threats (APT)

An APT is an attacker that utilizes uncommon exploits and techniques for long term data collection and manipulation.

APT's will try to blend in as much as possible doing things like mimicking network traffic. In this case, a malicious and capable hacker is seeking credit card numbers through a massive online vendor, where he will then sell this information to anonymous buyers on the dark web. This hacker executes a social engineering attack to an IT employee and succeeds, this hacker also has gained access through a software exploit, giving him access to the system at 2 different points on the network. At this point, the network would be compromised (with no knowledge of the administrator), but not yet breached, as no information has been taken at this point. AEGIS's anomaly-based system would be analyzing this network data since the breach, which would be able to be compared to typical network data. AEGIS filters data into 3 categories; clean, malicious, and possibly malicious to keep the false positive rate low as well as to make sure all possible threats are examined. This hacker is no amateur and therefore is initially filtered into the possibly malicious category, as his behaviors are slightly different from that of typical network behavior. The attacker then attempts to export smaller amounts of credit card data to his personal holding server. The AEGIS system would instantly recognize the malicious exporting of network data into an unknown server, sending the quarantine packet to stop the threat in its tracks, and removing it from the network. AEGIS would stop the breaching of the system, as it is a very identifiable behavior for the decision trees/anomaly-based system to catch. IT should be noted that the network would remain compromised until the system had time to identify all the behaviors of the threat. This is one of the biggest concerns with an APT, yet the AEGIS system is self-learning, therefore it can correlate behaviors of the APT, eventually leading to its eradication. This is vastly superior to static IDS that would have no hope in eliminating such an attack, putting them at the mercy of the hacker.

V. Conclusion

The AEGIS IDS is a hybrid system that is implemented on both the network and host locations, running a signature-based (using rulesets) and anomaly-based (using ART) systems that work in conjunction with one another. This proposed system benefits greatly from its hybrid scheme, as the signature-based system is typically computationally inexpensive, and rulesets are available in an open-source like fashion making them easily improvable and updatable. The anomaly-based system uses Adaptive Resonance Theory to identify anomalous data that could not otherwise be identified through rulesets and the signature-based system, thus increasing the detection rate of any malicious activity or attack compared to non-hybrid system. The rulesets of the signature-based system can then be improved through the detection of the anomaly-based system. The anomaly-based system filters network data into 3 different categories, these categories being clean, malicious, and possibly malicious. This categorizing of data allows for all threats to be examined by the system. This is much different from how a non-hybrid signature-based system would label the data due to the nature of the rulesets because if malicious activity is not defined within the ruleset, it will pass through the system without being detected. A major flaw in the non-hybrid system signature-based system. Overall, the potential impact of a hybrid system such as AEGIS in network security would be large. The ability to close security loopholes that typical IDSs have is invaluable when it comes to securing high-level sensitive data.

References

[1] M. Kumar, M. Hanumanthapa and S. Kumar, "Intrusion Detection System using decision tree algorithm - IEEE Conference Publication", Ieeexplore.ieee.org, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/6511281

[2] S. Bahl and S. Sharma, "Detection rate analysis for user to root attack class using correlation feature selection - IEEE Conference Publication", Ieeexplore.ieee.org, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/7148345.

[3] "NSL-KDD | Datasets | Research | Canadian Institute for Cybersecurity | UNB", Unb.ca, 2019. [Online]. Available: https://www.unb.ca/cic/datasets/nsl.html.

[4] S. Omar, A. Ngadi and H. H. Jebur, "Machine Learning Techniques for Anomaly Detection: An Overview", International Journal of Computer Applications, vol. 79, no. 2, pp. 33-41, 2013. Available: 10.5120/13715-1478.

[5] V. Jyothsna and V. Prasad, "A Review of Anomaly based Intrusion Detection Systems", International Journal of Computer Applications, vol. 28, no. 7, 2019. Available: https://pdfs.semanticscholar.org/9c21/441e384c32bea9680648417e91884b7aaff4.pdf.

[6] Nevlud, Pavel, et al. "Anomaly-Based Network Intrusion Detection Methods." Advances in Electrical and Electronic Engineering, vol. 11, no. 6, 2013, doi:10.15598/aeee.v11i6.877.

[7] M. H. Kamarudin, C. Maple, T. Watson and H. Sofian, "Packet Header Intrusion Detection with Binary Logistic Regression Approach in Detecting R2L and U2R Attacks," 2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), Jakarta, 2015, pp. 101-106. doi: 10.1109/CyberSec.2015.28

[8] A. H. Almutairi and N. T. Abdelmajeed, "Innovative signature based intrusion detection system: Parallel processing and minimized database," 2017 International Conference on the Frontiers and Advances in Data Science (FADS), Xi'an, 2017, pp. 114-119. doi: 10.1109/FADS.2017.8253208

[9] S. Ruggieri, "Efficient C4.5 [classification algorithm]," in IEEE Transactions on Knowledge and Data Engineering, vol. 14, no. 2, pp. 438-444, March-April 2002. doi: 10.1109/69.991727

[10] Kumar, Vipin. The Top Ten Algorithms in Data Mining, edited by Xindong Wu, and Vipin Kumar, CRC Press LLC, 2009. ProQuest Ebook Central

[11] Aydın, M. Ali, et al. "A Hybrid Intrusion Detection System Design for Computer Network Security." Computers & Electrical Engineering, vol. 35, no. 3, May 2009, doi:10.1016/j.compeleceng.2008.12.005.

[12] Jahan, A., & M, A. A. (2017). Intrusion detection systems based on artificial intelligence. International Journal of Advanced Research in Computer Science, 8(5) Retrieved from http://ezaccess.libraries.psu.edu/login?url=https://search-proquestcom.ezaccess.libraries.psu.edu/docview/1912629399?accountid=13158

[13] Bukhanov, D G, and V M Polyakov. "Detection of Network Attacks Based on Adaptive Resonance Theory." Journal of Physics: Conference Series, vol. 1015, 2018, p. 042007., doi:10.1088/1742-6596/1015/4/042007.

[14] Carpenter, Gali A, and Stephen Grossberg. "Adaptive Resonance Theory." Boston University Libraries, May 2009, open.bu.edu/handle/2144/1972

[15] Goan, Terrance. "A Cop on the Beat: Collecting and Appraising Intrusion." Communications of the ACM, vol. 42, no. 7, July 1999.