Journal of Engineering and Applied Sciences 12 (12): 3108-3112, 2017
ISSN: 1816-949X

A Semi Supervised Hybrid Protection for Network and Host Based Attacks

Jaspreet Kaur
Department of Information Technology,
India Ghandi Dehli Technological University for Women, Delhi, India

Abstract: In the era of internet there are various cyber-attacks which are easily performed by the intruder to gain unauthorized access of our confidential resources. Mainly cyber-attacks are categorized into 2 types as: network based and host based attacks. These both type of attacks are very dangerous because these steal or monitor our private data. So, we need to detect and prevent these types of attacks with very high accuracy rate. There are various techniques for detection of these attacks such as signature or pattern based attack detection (static analysis), anomaly based attack detection (static analysis), sandboxing based attack detection (dynamic analysis). These all techniques are better for detection of one kind (either network or host based) of attack and good for another one. But these are not the best for detection of both types of attacks. So, we introduce a new semi supervised hybrid protection for all of the attacks which gives us a very high accuracy and feasibility rate from earlier protection mechanism.

Key words: Static analysis, dynamic analysis, smart sandboxing, network based attacks, host based attacks, network intrusion detection/prevention system, host intrusion detection/prevention system

INTRODUCTION

There are mainly two types of attacks: network based and host based. Any intruder firstly perform the network based attack as SSL attack, browser attack, manin the middle attack, denial of service attack, deauthentication attack, disassociation attack, access point spoofing attack, arp spoofing attack, etc. Network based attacks are the first step for performing the host based attack because any intruder firstly take the information about their target during the network attacks. Then attacker performs the end point attacks such as: privilege escalation, stack overflow, heap overflow, system crash, malware installation etc for gaining the total control of the system or some other financial benefits.

There are various techniques available for detecting and preventing these attacks. Mainly static analysis (pattern based or anomaly based) is used for detecting the network based attacks. For host based attacks, dynamic analysis (sandboxing) is used for the checking the execution of the files. When any file is executed it's become a process. Then it creates a log or registry which is checked by the signature database of sandboxing for proving that it is a attack or not. We cannot detect both of the attacks using static analysis because static analysis needs the space requirement and dynamic analysis needs the space and time requirement both. Pattern based analysis cannot detect the zero day attack and anomaly based detect these attacks with very high false positive rate. Sandboxing technique also has the limitations as if malware check it is executing on the virtual or emulating environment or what if when malware is on the sleep mode, etc. So, we introduce a new semi supervised hybrid protection for both types of attacks which gives us a satisfactory results than the previous learning mechanisms.

Literature review: There are various study's which discuss the mechanisms from protection of these attacks as: in this study, researcher used IDS/IPS approach for the detection of wlan network attacks such as deauthentication attack, disassociation attack, access point spoofing attack. Their tool firstly Sniff Wi-Fi data, then performed static analysis on it. Based on the throughput of the network and deauthentication frame or disassociation frame in the network or at the particular client side they decide denial of service attack has to be performed or not in the network (Agarwal *et al*., 2013). In this study, we studied out various types of layer 2 network attacks detection and their countermeasures. They mainly focused on the ARP spoofing and tell that dynamic ARP inspection prevents current ARP attacks (Yusuf, 2005).

In next study, they perform the ICMP flood attack and uses an IDPS technique for detection and prevention of these attacks in which Snort uses as IDS and for the prevention technique uses aireplaying tool as sending the deauthentication packets to the attacker

(Korcak *et al*., 2014). In this study, they use the machine learning tool called as WEKA which includes the variety of supervised algorithms for the anomaly based detection of attacks. But they mainly used the J48 tree and Naive Bayes algorithm for detection of ping sweeps and port sweeps network attacks (Nevlud *et al*., 2013).

In this study, researcher suggest an artificial intelligence technique for detecting the various network based cyber-attacks. They actually used a semi supervised method along with manual tagging of the attacks for detecting the cyber-attacks with very high accuracy rate (Veeramachaneni *et al*., 2016). In the next study, they discussed the dynamic analysis technique called as the sandboxing for the execution of untrusted code in the virtual or emulator environment (Peterson *et al*., 2002). In this study, researcher discussed the various evasion technique taking by the intruder for avoiding the detection in the sandboxing. They also give a solution by which no one intruder can escape from it technique called as the smart sandboxing.

In the one study they discussed the host based attack such as the privilege escalation attack on the android operating systems. They also discussed the process to perform these types of attacks as taking the heap overflow vulnerability using return oriented programming (Davi *et al*., 2010). In the next study, they discussed the malware attacks on the host. They also tell the static analysis detection of the previous attack and how we need the dynamic analysis for the detection of new advanced persistent attacks (Gandotra *et al*., 2014).

In the next study, they discussed the all type of detection mechanism such as pattern based, anomaly based, static analysis, dynamic analysis, hybrid analysis for the malware attacks. They also did the comparative analysis among them and also tell the malware evasion and protection techniques from intruders (Teller, 2013). In the next study, SANS also tell the detecting malware and sandbox evasion techniques in the well appropriate manner (Keragala, 2016). In the next study, they describe Snort (a free open source network based intrusion detection system), their installation, rules and advantages (Roesch, 1999). We also study the host based intrusion detection tool called as OSSEC and their installation, procedures, protection such as file integrity, log analysis, etc. For wireless LAN network security we study the Kismet intrusion detection documentation and their procedures (Potter, 2004).

MATERIALS AND METHODS

In our proposed approach, we firstly used the semi supervised technique for checking the header abnormalities in the network packets. In this, we take packet dump captured by the wireshark. Then, we selected particular attributes for each attack for making a attribute selected file. These attributes are taken so precisely by which our technique gives high detection rate such as: for wireless LAN (deauthentication, disassociation, AP spoofing) attacks parameters considered as: source MAC address, destination MAC address, sequence number of each packet, location (latitude, longitude) of the access point, frame length of a packet, secure means which authentication protocol is used, signal strength of the access point, channel number at which access point is working, reason code for sending deauth/disas packets, Frame control flags indicating malicious packets other information such as frame type, frame subtype, etc.

For ping flood parameters taken as: source IP address, destination IP address, frame length of a packet, ID (identification number) of an ICMP packet, TTL (Time to Live) information, other information such as ping request, ping reply.

For Nmap scan (portsweep) parameters considered as: source IP address, sestination IP address, frame length of a packet, other information such as source port number, destination port number, etc.

For ARP spoofing parameters considered as: source IP address, destination IP address, MAC address of the source, MAC address of the destination, protocol is to be used, other information such as redirect (ICMP error), etc. We have given some network based attacks selected attributes but there are many more network based attacks such as denial of service, browser attacks which are detected by us using their header formats whose parameters are taken same as above for better detection rate.

After making this attribute file, this file is given to the input of the supervised and unsupervised learning methods. The output of the unsupervised learning method then becomes the input of manual tagging at which packets are tagged either a normal or abnormal one based on their ranking and selection. Then this file is given to the input of supervised learning as the feedback for the better detection rate. So that at the next time when the same attack is happen again then supervised learning can detect that very efficiently. If any abnormality is found in the header part of the packet then discard that packet otherwise go to the next level for checking the abnormalities in the content part of that packet. At this level we use network intrusion detection/prevention tool for counting the threshold values of the packet and for checking the content abnormalities. If it found any

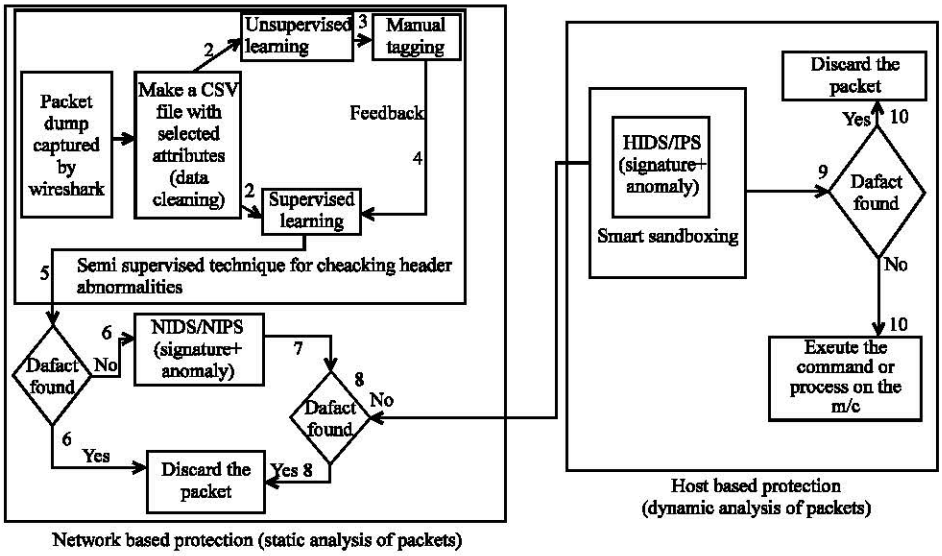

Fig. 1: A semi supervised hybrid protection for network and host based attacks

abnormality in the packet then discard the packet otherwise go the next level of protection. These header and content checking have to be done at network based protection and we apply only static based analysis for detecting these kinds of attacks.

If any packet passes the above level then it go to the next level for host based protection. At the next level, we use dynamic analysis as smart sandboxing at which every file or process is to be executed at the virtual or emulator environment for checking the abruption in the packets. Every smart sandboxing also includes the functions of host based intrusion detection/prevention. It finds the privilege escalation attack, memory overflow attack, file integrity attack and many more host based attacks. It also creates the signature of new attack and update the corresponding host based intrusion detection database for the next time early detection of the same attack. The diagram of our proposed approach is shown in Fig. 1.

RESULTS AND DISCUSSION

Firstly, we compare the network based protection using different learning techniques in the static analysis. In this, we take the signature based technique, supervised technique, unsupervised technique and our proposed technique (semi supervised along with manual tagging for the header part and signature or anomaly based protection for the content part). As, we can see in the below graph, our technique give us very high accuracy rate comparatively to another techniques. The graph is shown in Fig. 2.

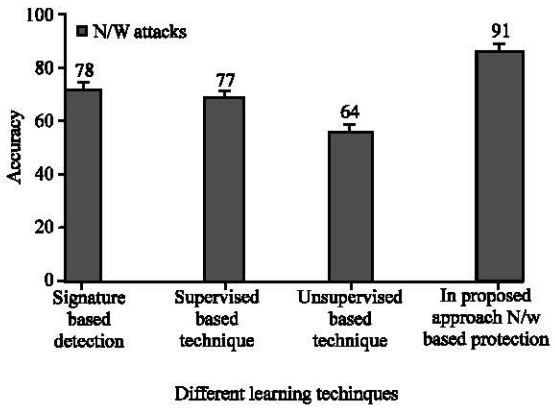

Fig. 2: Network based attacks analysis using different learning techniques

In the above graph, we compare the host based protection using different learning techniques in the dynamic analysis. We take the signature based technique, anomaly based techniques and sandboxing based technique and our proposed technique (smart sandboxing along with HIDS/HIPS (pattern or anomaly based). As, we can see in the above graph, our technique give us very high accuracy rate comparatively to another techniques. The graph is shown in Fig. 3.

Finally, we take both network based and host based protection, compare to both types of attacks using different learning techniques as static analysis, dynamic

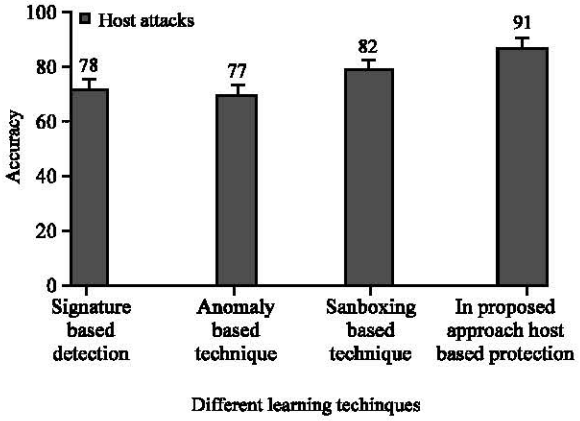

Fig. 3: Host based attacks analysis using different learning techniques

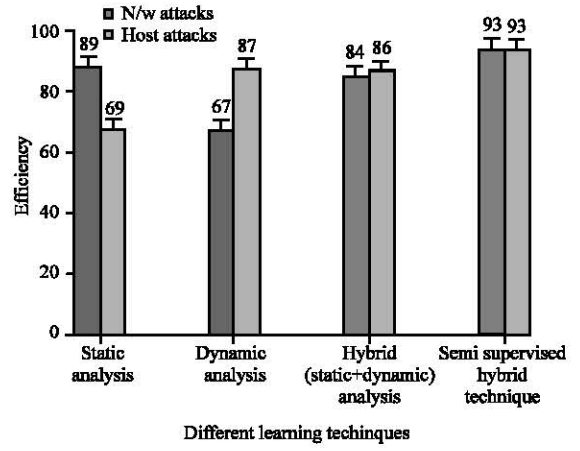

Fig. 4: Network and host based attacks analysis using different learning techniques

analysis, hybrid analysis and our proposed approach. Static analysis is useful for network attacks, dynamic analysis is useful for the host attacks, hybrid analysis give both of the attacks a satisfactory result and our proposed approach give us very high efficiency comparatively to another techniques. The graph is shown in Fig. 4.

CONCLUSION

As, we can see that there are various network and host based protection techniques are available now a days. But some techniques are better for the protection of few attacks and another for the rest of the attacks. There are various hybrid techniques are also available which gives us a satisfactory results. But we need a combined or hybrid (new) technique which gives us a very high accuracy results. So as you can see that we compare the alone network and host based attacks through various learning algorithms at which our method gives us high accuracy. When we combined the both types of the attacks detection our overall complete method also maintain the same accuracy ratio.

RECOMMENDATIONS

For the future work, attackers are always keen to evade from these protection. They always find the way for breaking the security. So, we have to maintain our mechanism as secure as possible and improve our technique accuracy rate as high as possible.

REFERENCES

Agarwal, M., S. Biswas and S. Nandi, 2013. Detection of de-authentication denial of service attack in 802.11 networks. Proceedings of the 2013 Annual IEEE Conference on India (INDICON), December 13-15, 2013, IEEE, Guwahati, India, ISBN: 978-1-4799-2276-5, pp: 1-6.

Davi, L., A. Dmitrienko, A.R. Sadeghi and M. Winandy, 2010. Privilege escalation attacks on android. Proceedings of the 13th International Conference on Information Security 2010, October 25-28, 2010, Springer, Boca Raton, Florida, pp: 346-360.

Gandotra, E., D. Bansal and S. Sofat, 2014. Malware analysis and classification: A survey. J. Inf. Sec., 2014: 1-9.

Keragala, D., 2016. Detecting malware and sandbox evasion techniques. SANS Institute, USA.

Korcak, M., L. Jaroslav and J. Frantisek, 2014. Intrusion prevention /intrusion detection system (IPS/IDS) for wifi networks. Intl. J. Comput. Netw. Commun., 6: 77-89.

Nevlud, P., M. Bures, L. Kapicak and J. Zdralek, 2013. Anomaly-based network intrusion detection methods. Adv. Electr. Electron. Eng., 11: 468-474.

Peterson, D.S., M. Bishop and R. Pandey, 2002. A flexible containment mechanism for executing untrusted code. Proceedings of the Usenix Symposium on Security, August 7, 2002, Usenix, Santa Clara, California, pp: 207-225.

Potter, B., 2004. Wireless intrusion detection. Netw. Secur., 2004: 4-5.

Roesch, M., 1999. Snort: Lightweight Intrusion Detection for Networks. Proceedings of the 13th USENIX conference on System Administration, November 7-12, 1999, Seattle, Washington, USA., pp: 229-238.

Teller, T., 2013. Detecting the one percent: Advanced targeted malware detection. Proceedings of the RSA Conference on Antivirus Vol. 8, February 25-March 1, 2013, Moscone Center, San Francisco, USA., pp: 1-38.

Veeramachaneni, K., I. Arnaldo, V. Korrapati, C. Bassias and K. Li, 2016. AI2: Training a big data machine to defend. Proceedings of the 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity) and IEEE International Conference on High Performance and Smart Computing (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), April 9-10, 2016, IEEE, Cambridge, Massachusetts, ISBN:978-1-5090-2403-2, pp: 49-54.

Yusuf, B., 2005. Layer 2 attacks and mitigation techniques. Cisco Systems, San Jose, California. http://www.sanog.org/resources/sanog7/yusuf-L2-attack-mitigation.pdf