International Journal of Scientific and Technical Advancements
IJSTA
ISSN: 2454-1532

A Survey on Defensive Framework Against Various Network Attacks and Zero Day Attacks

Mehak Mengi[1], Mehndi Samra[2], Sparsh Sharma[3], Naveen Kumar Gondh[4]
[1, 2, 3, 4]School of Computer Science Engineering, Shri Mata Vaishno University, Katra, India-180001
Email address: [1]mengimehak14@gmail.com, [2]mehndi.samra16@gmail.com, [3]sparsh_23june@yahoo.co.in, [4]naveen.gondhi@smvdu.ac.in

***Abstract*—**with the increasing amount of network throughput and security threat, Intrusion detection system has gained a lot of attention in computer science field. Current conventional security techniques cannot be able to deal with the security threats. So, Intrusion detection systems have the potential to prevent such attacks. There are many existing literature reviews to survey IDS. In this paper, we have discussed the various detection methodologies, detection approaches, technology types that are used to provide better defense against intrusion. A survey of automatic detection of zero-day attacks along with network attacks is also introduced in this paper.

***Keywords*—**IDS; IPS; snort; network attacks; zero-day attacks.

I. INTRODUCTION

Internetization of the world is happening at a rapid speed. Due to the explosive use of networks, Internet has raised various numbers of security issues. According to statistics reports, the amount of intrusions has greatly increased every year. When network and system activities are carried out frequently with malicious intentions or others violate the computer security policies this type of activity or attempt is called intrusion and its creator is referred to as intruder**.** An intrusion or attack may be fast or slow. When an attack uses large size packets or extremely high volume traffic within a very short time it is referred to as fast attack. The attack that completes its process in minutes or hours is referred to as slow attack. So, to prevent from malicious attacks or intrusions a defensive framework need to be established against various attacks. This defensive framework is known as Intrusion detection and prevention system. Firstly, we need to make a clear distinction between Intrusion detection system and Intrusion prevention system. An intrusion detection system (Ertoz et al., 2004) is designed to monitor network activity and identify suspicious activity .The function of intrusion detection system includes logging all the suspicious events and give alert to administrator. It is a passive security solution on the other hand, Intrusion prevention system (Desai, 2009) is an active security solution. Intrusion prevention system has all the capabilities of Intrusion detection system, but it allows the administrator to provide the immediate action upon being alerted. This paper is organized as follows: Section I is the introductory part, related works regarding IDS is presented in Section II, Section III describes the detection methods. Section IV introduces the various intrusion detection approaches; Section V presents the different classes of IDS technologies. Software oriented solution (snort) is studied in Section VI. In Section VII, we discussed the approach used for the automatic detection of zero-day attacks. Section VIII draws the conclusion. Section IX describes the future challenges.

II. RELATED WORKS

Several surveys on approaches to intrusion detection and prevention are published such as Patel et al. (2010) [1], Bhuyan et al. (2014b) [2], Hoque et al. (2013) [3], Kumar (2007) [4], Richhariya and Srivastava (2013) [5], and Patel et al. (2013) [6] Bai and Kobayashi (2003) [7] describe detailed designs of both signature and anomaly-based NIDS (Network-based Intrusion Detection System). Murali (2005) surveys recent IDPSs and alarm management techniques by providing a comprehensive taxonomy and investigating possible solutions to detect and prevent intrusions in cloud computing systems [8].

Comparison with existing surveys

References	IDS	IPS	Different approaches	Detection of Zero Day Attacks
Bai and Kobayashi (2003)	Yes	No	Yes	No
Murali (2005)	Yes	No	Yes	No
Kabiri and Ghorbani (2005)	Yes	No	Yes	No
Kumar (2007)	Yes	No	Yes	No
Patel et al. (2010)	Yes	Yes	No	No
Sandhu et al. (2011)	Yes	Yes	No	No
Rathore (2012)	Yes	Yes	Yes	No
Patel et al. (2013)	Yes	Yes	Yes	NO
Richhariya and Srivastava (2013)	Yes	No	Yes	No
Bhuyan et al. (2014b)	Yes	No	Yes	NO
This paper	Yes	Yes	Yes	Yes

Patel et al. (2010) review current trends in intrusion detection along with a study of implemented technologies. Sandhu et al. (2011) reviews methods for building intrusion detection and prevention systems (IDPSs) and uses a cost effective intrusion detection and prevention method that is

Mehak Mengi, Mehndi Samra, Sparsh Sharma and Naveen Kumar Gondhi, "A survey on defensive framework against various network attacks and zero day attacks", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 189-193, 2015.

based on the concept of intelligent mobile agents to design an effective agent based intrusion prevention system (AIPS) [9]. Richhariya and Srivastava (2013) address issues of information security and describe the security needs of an organization so as to protect its critical information from attacks [10].

III. Detection Methods

Intrusion detection methods are classified into three major classes:

1. Signature based detection
2. Anomaly based detection.
3. Stateful protocol analysis.

Signature Based Detection

In signature based detection (Kruegel and Toth, 2003) [11] there is a repository that stores all the sequence of patterns and signatures of various known attacks. When the attacker attempts to attack , the IDS matches the captured events with the predefined signatures to detect if it is an attack or not ,if there is a match then the system generates an alert to administrator. Attack signatures are built in such a way that they can be easily searched using information that is placed in audit logs that are provided by computer systems. Each time, when a new attack is discovered, attack signature repository must be updated to keep the signatures up to date. Different numbers of signature matching algorithms are used. This type of detection is also known as Knowledge-based Detection as it uses the knowledge provided by specific attacks.

Anomaly Based Detection

An anomaly is defined as a deviation to a normal behaviour, expected behaviour .These behaviours are derived from monitoring activities on a regular basis. Then, Anomaly based detection compares captured events to regular activities to detect significant attacks. This type of detection is also known as Behaviour-Based Detection. Examples of AD are: Denial of service (DOS), Trojan horse.

Table 1. Pros And Cons Of Various Detection Methods.

Signature based(knowledge based)	**Anomaly based (behavior based)**	**Stateful Protocol Analysis(Specification Based)**
PROS: Simplest and effective method to detect known attacks. Detail Contextual Analysis CONS: Ineffective to detect unknown attacks . Hard to keep signatures up to date.	Effective to detect unknown attacks. Less dependent on OS. Weak profiles accuracy due to observed events. Difficult to trigger alerts in right time.	Know and trace the protocol states. Distinguish unexpected sequence of commands. Resource Consuming to protocol state tracing and examination.

Stateful Protocol Analysis

In Stateful protocol analysis, the IDS could trace the protocol states .SPA process is same as that of ADs but with a slight difference. SPA is totally dependent on vendor developed generic profiles.SPA is also known as Specification Based Detection. Table 1 shows pros and cons of three detection methodologies.

IV. Detection Approach

Intrusion detection approaches can be studied from two major views, anomaly detection and misuse detection. Stavroulakis and Stamp (2010) [12] proposed a classification to subdivide the approaches into three categories that is based on computational-depended approach, artificial intelligence and biological concepts. Table 2 gives a deep perceptive of five detection approaches that includes which detection methodology to be used in specific detection approach ,whether the mentioned approach contains time series behavior or not, what type of attacks can be detected by the mentioned approach, type of sources and other characteristics of various approaches.

Table 2. Classifications and comparisons of various intrusion detection approaches.

Detection approach		Detection methodology			Time series	Technology type	Detection of attacks	sources
		AD	SD	SP				
Statistics based	Statistics	✔	✔	-	°	H/N	B	Audit data, user profiles
	Distance-based	✔	-	-	°	N	U	Audit data, network packets
	Game theory	✔	✔	-	°	H/N	U	System events or incident Log events
Pattern based	Pattern matching	-	✔	-	✖	N	K	signatures of known attacks
	Perti net	-	✔	-	°	H	K	Audit records,
	File system checking	✔	✔	-	✖	H	B	System/ /configuration/ User files,
Rule Based	Rule-based	✔	✔	-	✖	H/N	B	Audit records,
	Data mining	✔	✔	-	✖	N	B	Audit data,
	Model/profile-based	✔	-	-	✖	H/N	U	User profiles,
State based	State-transition analysis	-	✔	-	°	H/N	K	Audit records,
	User intention identification	✔	-	-	°	H	U	Audit records,
Heuristic Based	Neural networks	✔	✔	-	°	N	B	Predict events
	Immune system	✔	✔	-	°	H	B	Audit data, sequence of system calls
Hybrd approach	Honeypot	-	✔	-	✖	H/N	Z	Computer and security vulnerabilities

V. Technology Types

Many technologies are used to identify intrusions or suspicious events. These technologies are classified into four

Mehak Mengi, Mehndi Samra, Sparsh Sharma and Naveen Kumar Gondhi, "A survey on defensive framework against various network attacks and zero day attacks", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 189-193, 2015.

categories, on the basis of events that they detect. We describe these four classes as under:Host based (HIDS), Network based (NIDS) ,Wireless based IDS (WIDS), Network Behaviour Analysis(NBA), Mixed IDS(MIDS).

A. *Host Based IDS (HIDS)*

In Host based Intrusion detection system (HIDS), analysis of data is carried out by the host. In Host Based IDS, software agent resides on each of the hosts in the system so, it is agent based. Host based intrusion detection system monitors and processes the data that are present in computer themselves example: kernel logs.
Components: Agent, Management server, Database server, Single Host
Architecture: Managed network or standard Network
Strengths: Only HIDS can be able to analyze encrypted communication.
Detection methods used: Signature based Detection and Anomaly Based Detection (combined)
Limitations: causing delays in generation of alerts, Due to the lack of context knowledge it is more challenging in detection accuracy.

B. *Network Based IDS (NIDS)*

A network based intrusion detection system (NIDS) analyses data that are exchanged among computers in the network. At specific network segments, the Network based intrusion detection system captures network traffic by the use of sensors to identify the suspicious activities. If any suspicious behavior occurs, it generates alarm to administrator.
Components: Sensor, Management server, Database server, Network subnet, Host
Architecture: Managed Network
Strengths: broadcast scope of AP protocols can be best analyzed by this technique.
Detection methods used: Signature based detection (major), Anomaly based detection and Stateful protocol analysis.
Limitations: cannot be able to analyze wireless protocols, High false positives and false negatives rates.

C. *Wireless based IDS (WIDS)*

Wireless based IDS is similar to NIDS, but it captures wireless network traffic to identify the suspicious events or activities. Example: adhoc network, wireless mesh network.
Components: Sensor (passive), Management server
Architecture: WLAN, WLAN client
Strengths: WIDS is more accurate as it can only analyze the wireless protocols.
Detection methods used: Anomaly based detection (major), Signature based detection and Stateful protocol analysis.
Limitations: cannot be capable to monitor application layer, transport layer, Network layer protocol activities.

D. *Network Behaviour Analysis (NBA)*

An NBA system captures network traffic to identify attacks that flows in an unexpected manner.
Components: Sensor (most passive), Management server, Database server
Architecture: Managed Network or Standard Network
Strengths: At reconnaissance scanning, it has superior detection powers.
Detection methods used: Anomaly based detection (major), Stateful protocol analysis
Limitations: Transferring flow data to NBA in batches causes delays in detection attacks.

E. *Mixed IDS*

In MIDS, multiple technologies are adopted to fulfil the goal for more complete and accurate detection.
Additional information regarding technology types: The components in IDS contain sensor and agent, sensor is used for NIDS, WIDS, and NBA whereas agent is used for HIDS. The data delivered by sensor and agent is stored in Management Server and Database server. Management server processes the captured events where as Database server is simply a repository in which all the captured events are stored. Two kinds of network architectures are: Managed Network and Standard Network.

For security software management, an isolated network is deployed that is known as Managed Network (MS). In general terms, Standard network (SN) is a public network without any protection.

VI. Open Source Tool for IDS/IPS

High-speed networks and fast propagating threats are proven to be a great challenge to current IDSs. Most modern IDSs possess their own rules where every byte of packet is analyzed in detail. So, we introduce a popular open source tool that is Snort. In the field of open source software, Snort is a famous intrusion detection system and can be used in various environments. This tool is implemented by adopting rule based approach. In general, rule consists of following elements:
Filter Specification: For which particular threat the rule works.
String: basically a signature of suspicious events.
Position: is for the occurrence of that string.

As per Amdal's Law, String matching is proved to be the best consideration to improve performance as it accounts for 76% CPU load of IDSs(Cabera et al, 2004) [13] .For improving processing throughput, many works pays attention to the parallel techniques with special type of hardware technologies but hardware approaches are costly. So, we prefer to choose a software oriented solution that is Snort. Snort is basically a platform for the automatic detection of various network attacks (ARP Spoofing, DDOS attack, DHCP starvation) and zero day attacks like (cross site scripting, SQL injection, and directory traversal attack). Snort has little more than 4000 rules. It examines multi -criteria in a rule so, snort's detection could be time consuming. For exact-match signature detection, snort explores Aho-Cora algorithm (Aho and Corasick, 1975) [14].

Mehak Mengi, Mehndi Samra, Sparsh Sharma and Naveen Kumar Gondhi, "A survey on defensive framework against various network attacks and zero day attacks", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 189-193, 2015.

VII. Automatic Detection of Zero-Day Attacks

Zero Day Exploits: Zero-day exploits are those that takes full Advantage of computer and security vulnerabilities .There are Zero-days between the vulnerability is discovered and the first Attack. Basically, these attacks are mostly on the educational institutes .Various measures can be taken to prevent the educational institutes from suspicious traffic but as we know the port numbers 80 and 443 remain open for web related activities. This thing makes the educational institutes a target for hacking attempts. So, a framework must be required that includes all the measures that are taken in advance to prevent from various zero-day http attacks. Broadly, there are two detection approaches: Anomaly based detection and Signature based Detection as we discussed earlier. Both of these approaches require high human involvement. The speed of introducing intrusions is faster than the speed of updating. To prevent from such attacks, automated signature generation systems must be introduced. No single technique can help to prevent from zero-day attacks.

Related Work

The detection and prevention of network attacks is of great concern for researchers. For automatic detection and signature generation, many researchers have proposed various proactive and reactive methods: Honeycomb is the first approach for the automated generation of attack signatures. This approach has been proposed by Kreibich and Crowcroft (2003) [15]. Karp (2004) proposed a system known as Autograph that creates worm signatures by dividing each network flow into blocks [16]. Argos (Portokalidis et al, 2006) is an emulator that fingerprints zero-day attacks [17]. For automatic generation of intrusion signatures from honey pot packet traces, a system known as Neman is introduced by Yegneswaran (2005) [18].

Cui et al. (2007) proposed ShieldGen, which takes full advantage of the knowledge regarding data format of malicious attacks to generate potential attacks [19]. Eudaemon (Portokalidis and Bos, 2008) is a technique whose motive is to blur the borders between protected and unprotected applications [20]. Hancock is a system that is proposed by Griffin et al (2009) for the automatic generation of String Signatures [21]. F-Sign proposed by Shabtai et al (2011), a function based signature generation for malware files [22]. Honeyfarm proposed by Jain and Sardana (2012) is a combination of anomaly, signature based techniques and honeypots used for defending against Internet worms [23]

Various Zero-Day HTTP Attacks

In web communication, Http is the primary protocol. Due to the increased shift towards web applications, various zero-day http attack vectors are introduced i.e. Cross-site Scripting, Directory traversal Attack, SQL Injection attack and Command Injection attack.

Cross site Scripting attack: In this attack, the script tags are embedded in http requests and inviting the users to click on them. So, that the malicious script gets executed on the victim's machine .This attack can be explained with the help of an example.

Example: a facebook post on your wall contains a malicious script which if not filtered by facebook server, will be injected into your wall and executed on the browser of every person who visits your facebook profile.

Directory traversal attack: Directory traversal is also referred to as path traversal.

It aims to access files and directories that are stored outside the web root folder. It is basically a http exploit in which a hacker uses the software on a web server to access data in a directory other than the server's root directory .If the attempt is successful, the hacker can see the restricted files.

SQL Injection: In this attack, the malicious SQL queries are injected into the user input forms. These malicious queries can directly make a change in database.

Command Injection Attack: The goal of this attack is to inject and execute the commands in vulnerable applications. These commands are specified by the attacker.

For the automatic detection of zero-day attacks, a hybrid approach is introduced (Sanmeet kour and Manminder singh, Thapar University, Patiala, India) that involves signature based detection in conjunction with honeypots.

Motivation Behind the Automatic Detection of Zero-Day HTTP Attacks: To secure the sesnsitive information of educational institutions from hackers.

VIII. Conclusion

In this paper, recent surveys related to Intrusion detection and prevention systems are presented.These recent surveys are presented by different researchers. Previously,the existing surveys were based only on the detection of network attacks but in this paper,we have discussed an approach for the automatic detection of zero-day attacks along with network attacks.

IX. Future Challenges

In this paper,we present a comprehensive survey to current IDSs but there are still many open issues and challenges: Security issues of wireless IDSs, Divison of jobs of intrusion detection in parallelism, Mangement and coordination of multiple nodes, urgent topic for services on cloud computing is the slight performance degradation of IDS to VMs.

References

[1] A. Patel, Q. Qassim, and C. Wills, "A survey of intrusion detection and prevention systems," *Inf. Manag. Comput. Secur.*, vol. 18, issue. 4, pp. 277–90, 2010.

[2] M. H. Bhuyan, H. J. Kashyap, D. K. Bhattacharya, and J. K. Kalita, "Detecting distributed denial of services attacks: methods, tools and future directions," *Comput. J.*, vol. 57, issue 4, pp. 537–56, 2014.

[3] N. Hoque, M. H. Bhuyan, R. Baishya, D. K. Bhattacharya, and J. K Kalita, "Network attacks: taxonomy, tools and systems," *J. Netw. Comput. Appl.*, vol. 40, issue. 1, pp. 307–24, 2013.

[4] S. Kumar, "Survey of current network intrusion detection techniques," pp.1–18, 2007.

[5] V. Richhariya and R. Srivastava, "Survey of current network intrusion detection techniques," *J. Inf. Eng. Appl.*; vol. 3, issue 6, pp. 27–33, 2013.

Mehak Mengi, Mehndi Samra, Sparsh Sharma and Naveen Kumar Gondhi, "A survey on defensive framework against various network attacks and zero day attacks", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 189-193, 2015.

[6] A. Patel, M. Taghavi, K. Bakhtiyari, J. C. Junior, "An intrusion detection and prevention system in cloud computing: a systematic review," *J. Netw. Comput. Appl*., vol. 36, pp.25–41, 2013.
[7] Y. Bai, H. Kobayashi, "Intrusion detection systems: technology and development," *International Conference on Advanced Information Networking and Applications*, pp. 710–15, 2003.
[8] A. Murali, "A survey on intrusion detection approaches," *In 1st International Conference on Information and Communication Technologies (ICICT)*, pp. 233–40, 2005.
[9] U. A. Sandhu, S. Haider, S. Naseer, and O. U. Ateeb, "Survey of intrusion detection and prevention techniques," *In International Conference on Information Communication and Management*, Islamabad, pp. 16, 2011.
[10] V. Richhariya and R. Srivastava, "Survey of current network intrusion detection techniques, *J. Inf. Eng. Appl*., vol. 3, issue 6, pp. 27–33, 2013.
[11] C. Kruegel and T. Toth, "Using decision tree to improve signature based intrusion detection," *In 6th Symposium on Recent Advances in Intrusion Detection*, pp.173–91, 2003.
[12] P. Stavroulakis and M. Stamp, *Handbook of information and communication security*, New York: Springer-Verlag, 2010.
[13] J. B. D. Cabrera, J. Gosar, W. Lee, and R. K. Mehra, "On the statistical distribution of processing times in network intrusion detection," *In 43rd IEEE Conference On Decision and Control*, Paradise Island, Bahamas, pp. 75–80, 2004.
[14] A. V. Aho and M. J. Corasick, "Efficient string matching: an aid to bibliographic search," *Communications of the ACM*, 18:333–40, 1975.
[15] C. Kreibich and J. Crowcroft, "Honeycomb: Creating intrusion detection signatures using honeypots," *ACM SIGCOMM Computer Communication Review*, vol. 34, issue 1, pp.51–56, 2004.
[16] H. A. Kim and B. Karp, "Autograph: Toward automated, distributed worm signature detection," *Thirteenth Usenix Security Symposium (Security)*, San Diego, CA, pp. 271–286, 2004.
[17] G. Portokalidis, A. Slowinska, and H. Bos, "Argos: An emulator for fingerprinting zero-day attacks," *International Conference of ACM SIGOPS EUROSYS*, Leuven, Belgium, pp. 15–28, 2006.
[18] V. Yegneswaran, J. T. Giffin, P. Barford, and S. Jha, "An architecture for generating semantics-aware signatures," *Fourteenth USENIX Security Symposium, USENIX Association*, Baltimore, MD, US, pp. 97–112, 2005.
[19] W. Cui, M. Peinado, H. J. Wang, and M. Locasto, "Shield Gen: Automated Data Patch Generation for Unknown Vulnerabilities with Informed Probing," *IEEE Symposium on Security and Privacy*, Berkley, CA, pp. 252–266, 2007.
[20] G. Portokalidis and H. Bos, "Eudaemon: Involuntary and On- Demand Emulation against Zero-Day Exploit," *Third International Conference on ACM SIGOPS/ EuroSys European Conference on Computer Systems*, New York, US, pp. 287–299, 2008.
[21] K. Griffin, S. Schneider, X. Hu, and T. Chiueh, "Automatic generation of string signatures for malware detection," *Twelfth International Symposium on Recent Advances in Intrusion Detection*, Berlin, Heidelberg. Springer Press, Springer-Verlag, pp. 101–120, 2009.
[22] A. Shabtai, E. Menahem, and Y. Elovici, "F-Sign: Automatic, Function-Based Signature Generation for Malware," *IEEE Transaction on Systems, Man, and Cybernetics*, Part C, vol. 41, issue 4, pp. 494–508, 2011.
[23] P. Jain and A. Sardana, "Defending against internet worms using honeyfarm," *International Information Technology Conference (CUBE)*, Pune, India, pp. 795–800, 2012.

Mehak Mengi, Mehndi Samra, Sparsh Sharma and Naveen Kumar Gondhi, "A survey on defensive framework against various network attacks and zero day attacks", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 189-193, 2015.

ISSN: 2454-1532

Mehak Mengi, Mehndi Samra, Sparsh Sharma and Naveen Kumar Gondhi, "A survey on defensive framework against various network attacks and zero day attacks", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 189-193, 2015.