International Journal of Future Generation Communication and Networking
Vol. 9, No. 6 (2016), pp. 339-350
http://dx.doi.org/10.14257/ijfgcn.2016.9.6.32

Rule-Based Network Intrusion Detection System for Port Scanning with Efficient Port Scan Detection Rules Using Snort

Satyendra Kumar Patel[1], Abhilash Sonker[2]

[1]*Master of Technology, Department of CSE & IT*
Madhav Institute of Technology & Science
Gwalior-474005, India
[2]*Assistant Professor, Department of CSE & IT*
Madhav Institute of Technology & Science
Gwalior-474005, India
[1]*satyendra.pfg2013@gmail.com*, [2]*abhilashsonkerit@gmail.com*

Abstract

In the field of network security, researchers have implemented different models to secure the network. Intrusion Detection System is also one of them and Snort is an open source tool for Intrusion Detection and Prevention System. Today intrusion Detection System is a growing technology in network security and mostly researchers have focused in this field, some of them used signature or rule-based technique and some are anomaly based techniques to improve security of network. In this paper we propose a rule-base Intrusion Detection System with our self generated new Efficient Port Scan Detection Rules (EPSDR). These rules will be used to detect naive port scan attacks in real time network using Snort and Basic Analysis Security Engine (BASE). BASE is used to view the snort results in font-end web page because Snort has no graphic user interface. In This rule-based Intrusion Detection System we will match the signature with our Efficient Port Scan Detection Rules (EPSDR) from captured packet. As a definition of signature based IDS this new EPSDR based IDS will be useful to reduce the false positive alarm.

Keywords*: Network security, Intrusion Detection System (IDS), Network Intrusion Detection System (NIDS), Snort, Port Scan, Efficient Port Scan Detection Rules (EPSDR), Basic Analysis Security Engine (BASE).*

1. Introduction

This era is completely depends on computer and network in any form (like social media, E-marketing, E-banking etc.), and today's in the field of network security, Intrusion Detection System (IDS) playing an important role to secure network infrastructure. Whenever we are talking about security, network security is the big challenge among the researchers and most researchers are working in the field of network security (as an Intrusion Detection System) from 1987 when Dorothy Denning published an intrusion detection model [1].

The purpose of network security is to protect the network from unauthorized access and disclosure, but till now we did not get the perfect solution for network security. In network security area there are different tools (as a software and hardware) are available such as antivirus, firewall etc. but they are not able to cover all security risk in this field. The main work of intrusion detection system is to collect the packet from network, process it and if attack identifying then It will generate an alert for possible attack. Network security, intrusion detection system has two flavors for both Network and Host based categories and that's flavors known as signature or rule bases intrusion detection and anomaly based intrusion detection. Signature based intrusion detection system also

ISSN: 2233-7857 IJFGCN

known as misuse detection, and the essence of misuse detection centers around using an expert system to identify intrusions based on a predetermined knowledge base [2].

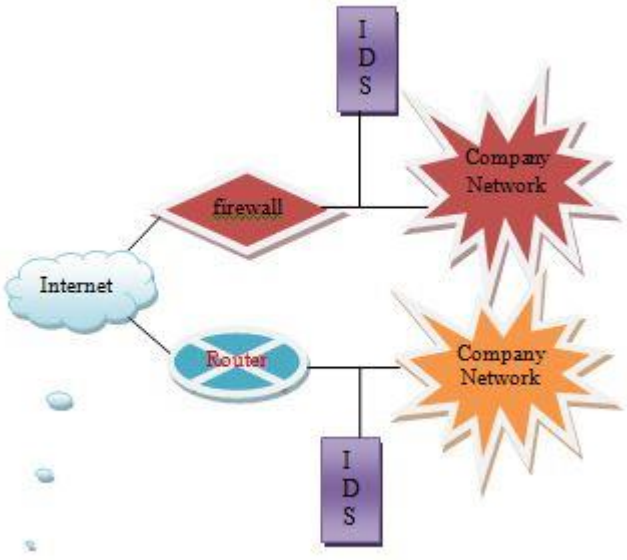

Figure 1. Typical Location for an Intrusion Detection System

Anomaly detection is concerned with identifying events that appear to be anomalous with respect to normal system behavior. A wide variety of techniques including statistical modeling, neural networks, and hidden Markov models have been explored as different ways to approach the anomaly detection problem.

2. Port Scan Attack

Port scanning is performed by sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can be probed for further security weaknesses [5]. It is a technique which is used to launches port scan when attacker or penetration tester want to see what port are open in your machine. Using this technique an attacker can identify the vulnerability and weakness on your machine ports. In term of network security, port scanning is not an offence until the intension of port scan is not intrusive, because this technique is also used by security expert when they perform the penetration testing on a machine [8]. By port scanning, the attacker can find the following information about the targeted systems: what users own those services, what services are running, whether anonymous logins are supported, and whether certain network services require authentication. Here port scanning categorized in two types.

2.1 Non stealth port scanning

Non stealth scanning is a process to identify open ports in a host. These types of scanning mostly performed by administrator using the TCP connect () method of connecting to the destination host and it's easily detected by routers and firewalls [15].

2.1.1 Full open: This types of scan uses connect () method, it's a system call provided by the operating system to open a connection to a remote host. The TCP connect() uses the 3-way handshake and will succeed if the port being scanned is listening, otherwise it will fail. Following figure show the 3-way handshake procedure of TCP connect () method.

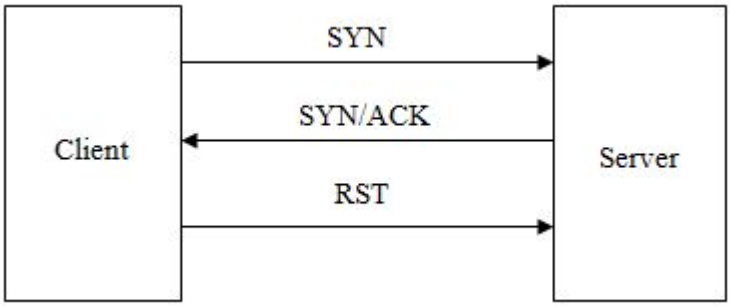

Figure 2. Three-Way Handshake Connection between Client and Server

In a TCP connect method, When a client wants to connect with a server, it first sends a TCP packet with the SYN (Synchronize Sequence Number) flag set. The server then sends back a TCP packet with the SYN and ACK (Acknowledge) flags set if the port is open on the server. A RST (Reset) packet is sent to the client if the port is closed. If the port is open and the server sends back the SYN|ACK packet, the client computer then sends an ACK back to the server.

2.1.2 Half open scanning: This is occurring when port scanning terminates before completing the three-way handshake process, as such, these scan method often go to unlogged by the destination application. Since this technique uses known TCP flag, it can be easily detected by an edge firewall and router.

2.2 Stealth scanning

Any scan that bypassing filter, firewall, router and behaving as casual network traffic are considered as stealth port scanning. Mostly used stealth scan techniques are discussed here.

2.2.1 FIN Scan: In the FIN scan, a packet is sent with just the FIN flag set. If the port is closed, the host sends back a RST flag, whereas an open port simply ignores the packet and nothing is returned to the client. Following figure show the process of FIN (stealth) scan.

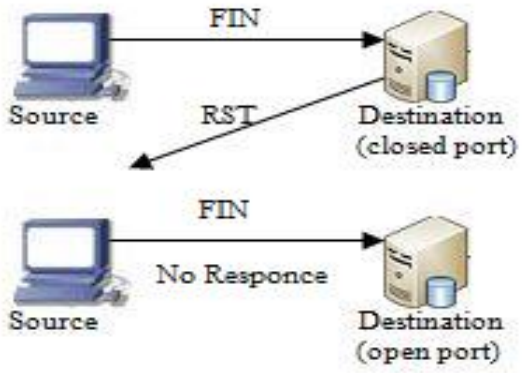

Figure 3. FIN Scan Packet Exchange

2.2.2 SYN/ACK Scan: It is relatively fast scan method that avoids the use of three way handshake. In this scan type source sends a SYN with ACK flag to the target. For a closed port, the target will replay with a RST packet (A TCP packet with reset flag set) while a request to an open port will not generate a response. This scan technique generate

notable amount of false positives due to the filtering devices, heavy traffic, slow link, and timeouts etc [18].

2.2.3 Xmas Tree Scan: In Xmas tree scan source send 3 packet header flags together, which are the FIN, URG (Urgent), and PSH (Push) to destination. In Xmas tree scan a closed port will return a RST packet, whereas an open port will ignore the packet. This type of scan is very similar to the FIN scan.

2.2.4 Null Scan: The Null scan produces a reaction similar to the FIN and Xmas tree scans, but differs in packet header flags. It just sends a packet with no flag set. This again causes a RST packet to be sent to the client if a port is closed, but is ignored if the port is open.

3. Literature Review

Recently, researchers have proposed various techniques to detect port scans. In [3] and [4], researcher implements the signature based intrusion detection system using snort and Basic Analysis Security Engine (BASE) to understand the concept of snort and BASE by novel users and this system also helpful to detect the attacks on TCP protocols. The authors in [6] outline several approaches to detect intrusions and malicious activity, including port scanning. More specifically, the authors proposed techniques that correspond to both the anomaly detection and misuse detection. In [7], the researchers used the number of the different TCP control packets and SYN as input for Back Propagation algorithm in order to detect port scans.

Cynthia Bailey Lee, Chris Roedel and Elena Silenok in [8], the goal of the author is to analyze sample network traces to identify and classify properties of port scans. The majority of this scans were carried over TCP, with TCP SYNs dominating the traffic. UDP was another protocol that they saw, although it was not very prevalent. In this paper most of the scans were horizontal scans or simple vertical, with vertical scans prevailing by a factor of nearly two.

Jaekwang Kim and Jee-Hyong Lee in [9], suggested an abnormal traffic control framework to detect slow port scan attacks using fuzzy rules. In this paper, researchers presented a new detecting and managing mechanism for slow port scan attacks and framework control abnormal traffic, effectively prevented slow port scan attacks using fuzzy rules and a stepwise policy. This approach has an effect on slow port scan attacks as well normal port scan attacks.

Jaeyeon Jung, Vern Paxson, Arthur W. Berger, and Hari Balakrishnan in [10], use this insight approach to develop TRW (Threshold Random Walk), an online detection algorithm that identifies malicious remote hosts. Using an analysis of traces from two qualitatively different sites, there theory show that TRW requires a much smaller number of connection attempts to detect malicious activity compared to previous schemes, while also providing theoretical bounds on the low (and configurable) probabilities of missed detection and false alarms.

Wassim El-Hajj, Fadi Aloul and Zouheir Trabelsi in [11], used fuzzy-based snort to detect port scan attacks. They using customized fuzzy logic controller to enhance the capability of snort to detect port scan attacks. This technique also helps in reducing palse negative and positive alarm. But this research does not solve the problem of finding all network based atracks.

Z. Jammes and M. Papadaki in [12], research examines the evasion technique provided by Nmap, a Metasploit and port scanner Framework, an exploit launcher against famous IDS named Snort. The result tends to prove that Snort has the ability to detect port scan and exploit on condition to have a good configuration of Snort and signature for the exploit.

Chunmei YIN, Mingchu LI, Jianh MA and Jizhou SUN in [13], in this paper researcher uses a security scanner tool Nmap [16], to scan there system in a typical network and comparing its result with the one of a normal network, then find no difference between them. This system reporting 17 kinds of scans they defined including the slow scan and distributed scan.

Mehiar Dabbag, Ali J. Ghandour, Kassem Fawa, Wassim El Hajj, Hazem Hajj in [14], approach for detecting slow port scanning. In this method processes the captured traffic in a small time window and therefore overcomes the disadvantages of the previous approaches that work on a large time window, thus requiring a lot of processing which causes degradation in the Quality of Service and might become a target for a DoS attack. This approach divides the IPs into three categories: scanner IPs, suspicious IPs and legitimate user which is different than the traditional IDS that classify the IPs into either scanners or legitimate users. These traditional IDS can't detect slow port scanning.

Rajni Ranjan Singh and Deepak Singh Tomar In [15], researcher proposed a system to detect stealth port scanning attack which is carried out on the basis of forensic principles. This work presented a storage efficient capturing system that captures relevant packets and an analysis system that perform precise classification of suspicious packets. Snort rules are developed for the capturing and analysis of network traffic.

4. Tools Used In Rule-Based NIDS

To implement network intrusion detection system based on rules or signature; we need to install some tools, such as Snort, libpcap, BASE etc. In fig. 2, snort is installed in the computer within the network. Once it's installed completely it will automatically capture the network packet which are passed over the network. Identification of attack in snort based on protocols and that protocols categorized into four groups (TCP, UDP, IP and ICMP protocol).

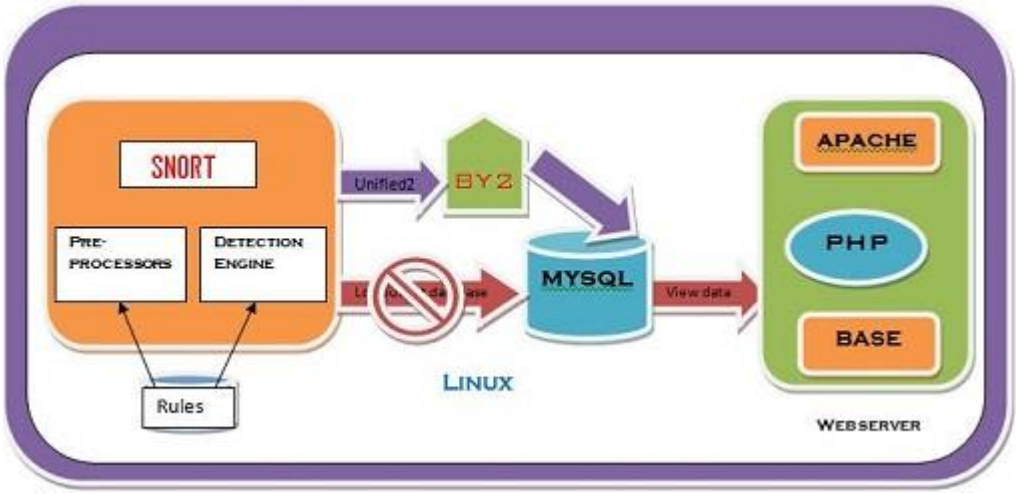

Figure 4. Snort-Based NIDS Architecture

4.1 SNORT

Snort is an open source network intrusion detection and prevention system [4] (available at http:// www.snort.org/snort-downloads?). It can analyze real-time traffic analysis and data flow in network. It is able to check protocol analysis and can detect different type of attack. Snort rules can be written in any language, its structure is also good and it can be easily read and rules can be modify also. Whenever any packet comes into network then snort checks the behaviour of network if performance degrades of

network then snort stop the processing of packet, discards the packet and stores its detail in the signature database.

4.2 BASE

BASE is the Basic Analysis and Security Engine, its searches and processes databases containing security events logged by heterogeneous network monitoring tools such as IDS and firewalls programs [17]. It is based on the code from the Analysis Console for Intrusion Databases (ACID) project. This application provides a web-based GUI to query and analyze the alerts coming from SNORT Intrusion Detection System. BASE is written in the PHP language and displays information from database in a user friendly web page.

5. Proposed Methodology

We proposed a rule-based Network IDS which will examines ongoing traffic, transactions, activity, or behavior for matches with known patterns of events specific to known attacks. Rule- based detection system (also called misuse based), very effective against known attack, it implies that misuse detection requires specific knowledge of given intrusive behavior [3]. An example of rule-based Intrusion Detection System tool is SNORT. The advantages of rule-based network Intrusion detection system is, it produces low false positives, and it is easy to use. The structure of Snort rules looks like as follows.

alert ip any any → any any (msg:“snort bad rule”;)

rule header rule option

5.1 Structure of Snort Rule Header

Action	Protocol	Src. Address.	Src. Port	Direction	Dest. Address.	Dest. Port

Figure 5. Structure of Snort Rule Header

New action is defined in the following general structure:
ruletype action_name
{
action definition
}
The ruletype keyword is followed by the action name. Two braces enclose the actual definition of the action, just like a function in C programming.

Here we present an intrusion detection system to improve the detection of port scanning on different port using snort. In [3], [4] and [8], researchers implements rule based IDS and apply some own rules to detect attacks on TCP and UDP specific protocols to detect port scanning. Rule looks like as follows.

alert tcp any any → any any (msg: “tcp packet detected”;)
alert udp any any → any any (msg: “udp packet detected”;)

So the problem with this types of rules are they will apply for all types of TCP and UDP packets but port scan need to apply some flag based rules to detect them.

In [6],[7],[10],[11] and [13], researchers used some algorithms to detect port scanning attack in network, where some them used data mining technique and others used fuzzy based algorithm. But the problem with existing techniques are, they consider all the scan as a attack while in any network most of scanning are used by system connect () method to establish the communication between client and server.

In [14] and [15], researchers categorized port scan attack in two parts, one is normal scan (Non-stealth) and another is stealth scan attack using flag based specific rules. But rules used by the researcher are not efficient to detect stealth scan and they also used same SID for rule 2, 3, 4 and 5, which is not a right way to write the rules. In snort rules, the SID keyword used to uniquely identify snort rule and it must be unique for each rule otherwise it will be conflict [4].

alert tcp any any → any any (flags:*FPU; sid: 7987660;)
alert tcp any any → any any (msg: " FIN Scan Detected";flags:*FPU; sid: 7987660;)

In [17], above to rules are used to detect FIN scan attack But that is not right and correct rule writhen in our Efficient Port Scan Detection Rules. In our proposed IDS we are applying some Efficient Port Scan Detection Rules (EPSDR) to detect port scan attacks on real time network as well as pre-defined dataset which are something different from other normal rules, and our rules are look like as follows.

5.2 Efficient Port Scan Detection Rules (EPSDR)

Rule 1
alert tcp any any → any any (msg:"FIN Scan"; flags: F; sid: 1000001;)
Rule 2
alert tcp any any → any any (msg:"NULL Scan"; flags: 0;sid : 1000002;)
Rule 3
alert tcp any any → any any (msg:"SYN attack"; flags:S,12;sid : 1000003;)
Rule 4
alert tcp any any → any any (msg:"XMUS attack"; flags:FPU; sid 1000004;)

Process of our Efficient Port Scan Detection Rules (EPSDR) based IDS describe in following diagram.

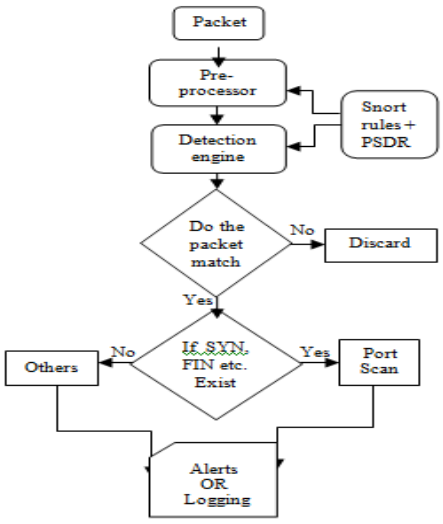

Figure 6. Process Diagram of Proposed EPSDR Based IDS

In this first rule flags: F will identify the FIN keyword in network if it matches then it will generate the alert for port scan attack. This process will be continue for all types of rule option field like seq., flags, flow, class-types, ACK, RST etc. and we can also apply content keyword in rule option area to match some content related to port scan.

Advantages of this methodology is, useful to detect port scan attacks however some other techniques are not able to identify the different between ping and port scan. It is also unique from others because its used the specific flags for particular port scan attacks.

6. Results

First we evaluate the snort Network Intrusion Detection System on real time network without configuring port scanning and Efficient Port Scan Detection Rules (EPSDR).we have review the paper [3], but we are not able to see any port scan attack because they not configured port scan preprocessor, even in that paper they are also not able to detect other than TCP protocol attack. We can see in following figure only TCP protocol attacks are identified by snort. After evaluation of some SNORT rules for UDP and ICMP, here we are able to detect UDP and ICMP protocol attacks in SNORT.

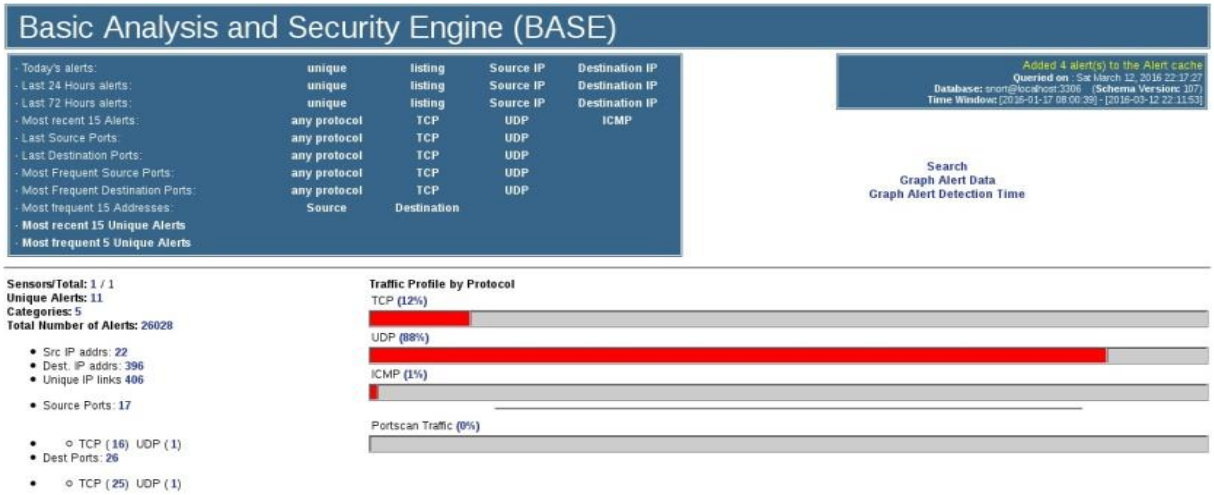

Figure 7. Results Generated by Snort for TCP, UDP and ICMP Protocols on BASE

Now we have detected all protocol attack but still we can't detect port scan attacks. After configuring port scan preprocessor and using Network Forensics Stealth Port Scan Attack (NFSPSA) rules [15], it is able to detect port scan attack for NULL and XMUS attack but fail to detect FIN attack due to bad rule for FIN attack and BASE show 1% result in port scan field and total 18 attack detected. In our proposed models of snort with Efficient Port Scan Detection Rules (EPSDR) will detect the port scan attacks for NULL, XMUS as well as FIN scan attack after using modified and efficient rules and it detect total 27 attack for same log file.

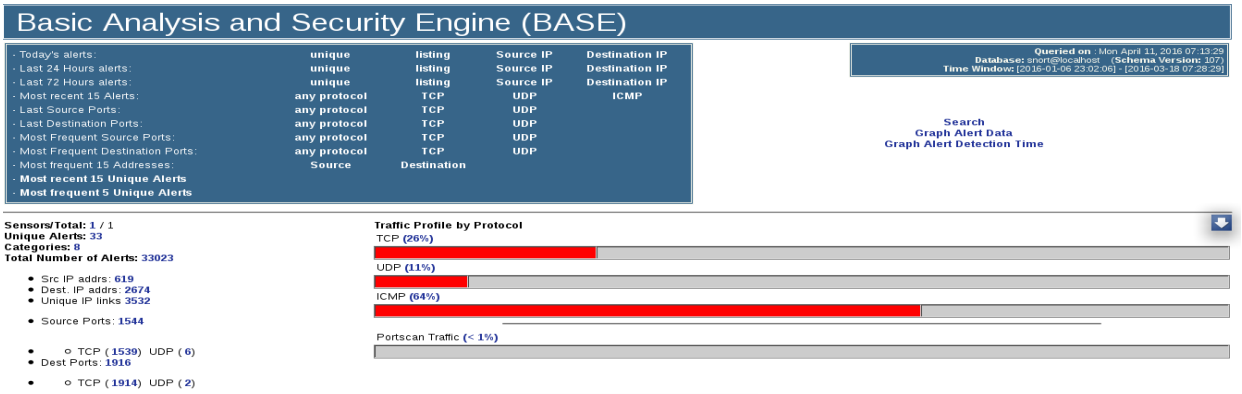

Figure 8. Results Generated by Snort for TCP, UDP, ICMP and Port Scans (1%) Protocols

In above result finally we detect the port scan, but the numbers of attacks of these categories are very less in our network. So its show the < 1% attack in port scans section. In following figure we can see all port scan attack with its signature and other details for both NFSPSA and EPSDR models.

Figure 8. Results Generated by Snort on BASE for NFSPSA and EPSDR Model

In the following table, comparison given on the bases of total number of attacks detected, detected attacks percentage and number of unique source and destination IP addresses.

Table 1. Comparison between NFSPSA and EPSDR Based on Source IP, Destination IP and Total Number of Attacks

S. No.	Total Packet (Analyzed)	Port Scanning Method	Total Port Scan Attack Detected	No. Of Source IP Address	No. Of Destination IP Address	% Of Total Detected Attack
1.	90	Using NFSPSA Method	18	1	13	20
2.	90	Using EPSDR Method	27	2	16	30

In above table and following graph, clearly shows that our EPSDR model detecting 10% more attacks compare to previous NFSPSA model for same log file.

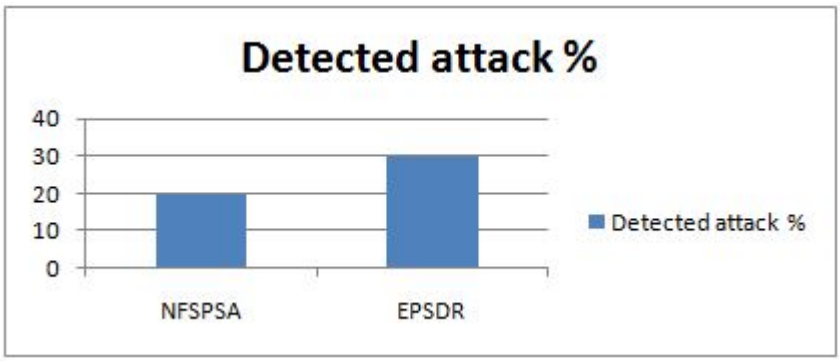

Figure 9. Bar graph Comparison for NFSPSA and EPSDR for Detected Attacks Percentage

7. Conclusion

In this work we improve the detection rate of stealth port scan attack using our new modified and efficient rules. After using SNORT tool as an intrusion detection system, we have seen it has the full ability to detect port scan attack but the fact is, snort detection is depends on signature match, so it will detect all attacks which have predefined rule for signature match. Today's hackers are very clever and they generate the new signature for different attacks, so they may be success full some time but not always, because we have a weapon like rules and plugging in snort. Our purpose for implement this paper is, detecting stealthy port scan attack using new Efficient Port Scan Detection Rules (EPSDR) in snort. In result part we have seen that snort with EPSDR are able to detect port scan attacks with better detection rate.

Here we apply port scanning rules to detect attack on TCP protocol only but in future, this work can be extended for UDP and ICMP protocol to detect stealth port scan.

References

[1] D. E. Dorothy, "An Intrusion-Detection Mode,l" IEEE Transactions on Software Engineering, Vol. Se-13, No. 2, February 1987, 222-232.

[2] D. J. Brown, B. Suckow and T. Wang, "A Survey of Intrusion Detection Systems," Department of Computer Science, University of California, San Diego (2002).

[3] V. kumar and O. P. Sangwan, "Signature Based Intrusion Detection System Using SNORT," International Journal of Computer Applications & Information Technology Vol. I, Issue III, November 2012 (ISSN: 2278-7720).

[4] R. U. Rafeeq, Intrusion detection systems with Snort: advanced IDS techniques using Snort, Apache, MySQL, PHP, and ACID. Prentice Hall Professional, 2003.

[5] R. Christopher, "Port Scanning Techniques and the Defense Against Them," SANS Institute InfoSec Reading Room October 5, 2001.

[6] P. Dokas, L. Ertoz, V. Kumar, A. Lazarevic, J. Srivastava and P.Tan, "Data Mining for Network Intrusion Detection," In Proc. 2002 NSF Wrokshop on Data Mining, p. 21-30.

[7] B. Soniya and M. Wiscy, "Detection of TCP SYN Scanning Using Packet Counts and Neural Network," Signal Image Technology and Internet Based Systems, 2008. SITIS '08. IEEE International Conference, pp.646-649, Nov. 30 2008-Dec. 3 2008 doi: 10.1109/SITIS.2008.33.

[8] C. B. Lee, C. Roedel and E. Silenok, "Detection and Characterization of Port Scan Attacks," Univeristy of California, Department of Computer Science and Engineering (2003).

[9] J. Kim and J. H. Lee, "A Slow Port Scan Attack Detection Mechanism Based on Fuzzy Logic and a Stepwise P1olicy," Intelligent Environments, 2008 IET 4th International Conference on. IET, 2008.

[10] J. Jung, V. Paxson, A.W. Berger and H. Balakrishan, "Fast Portscan Detection Using Sequential Hypothesis Testing," In Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on, pp. 211-225. IEEE, 2004.

[11] W. El-Haji, F. Aloul, Z. Trabelsi and N. Zaki, "On Detecting Port Scanning Using Fuzzy Based Intrusion Detection System," In Wireless Communications and Mobile Computing Conference, 2008. IWCMC'08. International, pp. 105-110. IEEE, 2008.

[12] Z. Jammes and M. Papadaki, "Snort IDS Ability to Detect Nmap and Metasploit Framework Evasion Techniques," Advances in Communications, Computing, Networks and Security 2010.

[13] C. Yin, M. Li, J. Ma, J. Sun, "Honeypot and Scan Detection in Intrusion Detection System," Electrical and Computer Engineering, 2004. Canadian Conference on. Vol. 2. IEEE, 2004.

[14] M. Dabbagh, A. J. Ghandour, K. Fawaz, W. E. Hajj, and H. Hajj, "Slow Port Scanning Detection," In Information Assurance and Security (IAS), 2011 7th International Conference on, pp. 228-233. IEEE, 2011.

[15] Rajni Ranjan Singh and Deepak Singh Tomar "Network Forensics: Detection and Analysis of Stealth Port Scanning Attack" International Journal of Computer Networks and Communications Security VOL. 3, NO. 2, FEBRUARY 2015, 33–42.

[16] Z. Durumeric, E. Wustrow and J.A. Halderman, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure, 2009.

[17] http://base.professionallyevil.com/.

[18] Brenden Claypool "Stealth Port Scanning Methods" Global Information Assurance Certification Paper – 2002.

[19] Roger Christopher "Port Scanning Techniques and the Defense Against Them" SANS Institute InfoSec Reading Room - 2001.

