Ankita Tuteja, Ravi Shanker / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.1768-1774 Optimization of Snort for Extrusion and Intrusion Detection and Prevention

Ankita Tuteja* Ravi Shanker**

*(Department of Computer Science LPU, Phagwara, Punjab) ** (Department of Computer Science LPU, Phagwara, Punjab)

ABSTRACT

Intrusion is an attempt or threat resulting to attempt to access unauthorized information, manipulate information or render a system unreliable or unusable. Firewall can prevent unauthorized access but it cannot monitor the network attacks. In order to monitor network activities we need an Intrusion detection system which is the first line of defense against network activity. Over the last decades, malicious software or malware in the form of viruses, worms, Trojan horses, Botnets have risen to become a primary source of most of the threats used for scanning, distributed denial of service activities and direct attacks taking place across the internet. Most of the work has been done to monitor the inbound traffic i.e. Intrusion traffic but goal here is to monitor outbound traffic i.e. extrusion traffic as well. For the purpose of detection of Intrusion and Extrusion traffic Snort is optimized which is primarily made for Intrusion detection and prevention. It is famous Intrusion detection system in the field of open source software. Further the optimization of the Snort database is done to make it more network specific on the two designed parameters. The experimental results shows that working according to the designed system architecture a more secure network can be obtained through which specific network attacks can be easily targeted.

Keywords-Extrusion, Intrusion, Malware, Signature, Signature-Based, Snort

I. INTRODUCTION

Every network is potentially vulnerable to network intrusions despite of all security measures. It is practically impossible to build a completely secure network. Many business and government organizations use the internet as a means of providing public access to public records and information. Here arises the concept of Intruders which may be a hacker or a cracker. The three types of intruders are, Masquerader who is an unauthorized user who penetrates a computer system's access control and gains access to user accounts. Misfeasor, who is legitimate user who accesses resources he is not authorized to access or who is authorized such access but misuses his privileges. Clandestine user, a user who seizes the supervisory control of the system and uses it to evade auditing and access control.

Initially firewall was used but it could only prevent unauthorized access and cannot monitor network attacks. Intrusion Detection is the possibility of finding the incorrect or inappropriate action. It is considered as one of the consistent security measures against an incident. The incident may be a threat, attack or occurrence of damage to information. Security measures include detection, prevention, correction, reduction, reaction and evaluation.

Every system includes a software or hardware which is responsible for monitoring all the activities within the system or network in order to detect malicious activity and report to administrator. To protect a network from vast number of threats a Network based intrusion detection system is needed. The data of the single host might be insufficient to properly identify such malware. An ideal network-based intrusion detection system would correlate data from as many hosts as possible and could provide better detection. There are many problems of false alarms and false negatives as the amount of data to be analyzed is huge so in order to overcome the issues we need the analysis of the outbound traffic as well which we say as the extrusion traffic which would be more useful to the detect attacks because it is always assumed that a host always react to an infection of penetration in some way. So this can be acknowledged by monitoring both the outbound and intra network [11].

Another reason why extrusion is included with the intrusion is that intrusion is only the half solution to secure a network from different types of malware. There may be a possibility that an attack will make past the network boundary or even originate from the inside the network boundary so it is beneficial that the entire network is monitored.

The signature-based detection methodology is used as it is very effective at detecting known threats by comparing signature against observed events to identify possible attacks.

Snort is a lightweight network intrusion detection system capable of performing real time traffic analysis and packet logging on IP networks. Snort uses signature based detection. When we include extrusion with intrusion the problem of false negative decreases this is because

Ankita Tuteja, Ravi Shanker / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 <u>www.ijera.com</u> Vol. 2, Issue 3, May-Jun 2012, pp.1768-1774

extrusion confirms that an intrusion has taken place as the infected host always moves outward for attack propagation thus confirming the intrusion.

Our Contributions: Our primary contribution to this paper is (1) to analyze the entire traffic both inbound, outbound, intra network. (2) To work for the reduction of false alarms. (3) To analyze offline traffic as well. (4) To carry out network specific optimization using Snort. (5) To make network more secure.

II. RELATED WORK

The proposed work utilizes the concept from the paper [11] about the study of extrusion detection that how important extrusion detection is in combination with intrusion. The factors for the optimization of snort database are taken from C. Lussi paper [4] as the optimization is very important after the traffic is being analyzed on the basis of signature and frequency. Different factors from the different sources are studied and combined to build an efficient system that could be developed such that the attacks which are compromising our network security and too harmful for the network could be prevented and security could be enhanced.

III. SYSTEM DESIGN AND IMPLEMENTATION

Snort itself cannot do the entire work there are number of software's which need to compiled together to carry out the desired task.



Fig1: Software applications for Snort installation

Winpcap is a packet capture library, Wamp is Windows Apache MySql Php server and BASE which is Basic Analysis and Security Engine is used for traffic analysis.

We have two modes in which Snort works one is the Intrusion detection mode, Snort does not log each captured packet as it does in the network sniffer mode. Instead it applies rules on all catured packets. If a packet matches a rule only then it is logged or an alert is generated. If packet doensot match any rule, the packet is dropped silently and no log entry is created. We used Snort in intrusion detection mode where we provided a configuration file on the command line which further contains information about input and output plugins. The name of the snort configuration file is snort.conf.

Signatures and rules for signature-based detection are downloaded from the various sources as from the official site of snort itself and from www.emergingthreats.com

Fig2 shows the proposed NIEDPS to detect and prevent any extrusion and intrusion activity. Both online and offline traffic will be analyzed. The main aim is to provide a software solution such that false alarms could be reduced and more secure network could be made. The extrsuion has two parts (1) Detection of attacks within the network (2) Detecting the movement of data out from the network



Fig2: System Design

We ran snort in the Intrusion detection mode where it matches the packets of data and logs and generates alerts correspondingly. The analysis of traffic is done on the basis of IP addresses i.e. the source and destination IP addresses as well as source and destination Ports.

Afte the packet of data are matched alerts generated and stored in the database the next step would be to filter it on two designed factors:

- **Frequency**: Will check whether a particular signature exceeds a fixed limit.
- **Signature-correlation**: This will combine signature with that of frequency.

A table will be separately created inside Snort database which will have two entries for the frequency search; it will import two fields from already existing database:

- Signature-name
- Frequency

Ankita Tuteja, Ravi Shanker / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 <u>www.ijera.com</u> Vol. 2, Issue 3, May-Jun 2012, pp.1768-1774

	Field	Type	Collation	Attributes	Null Default	Extra			Act	ion		
3	signature_name	varchar(200)	latin1_swedish_ci		No		1	X	1	3	W.	(F)
)	frequency	int(11)			No		1	X	12	12	W	Ŧ

Fig3: Shows table for signature-name and frequency

We will decide a certain threshold value for frequency by making analysis from BASE, this decision of setting the threshold value for the frequency will highly depend upon how large the network is and how frequently a particluar signature is triggered in the network. In the results and discussion column of the paper we will be representing the signatures with their frequency when we implemented the proposed work on our test enviornment. Say we set our threshold value of frequency to 265. Now, we need to fire the query saying if the frequency is greater than 265 the database should show the remaining filtered signatures. Same is the case with if a particular signature is found in combination with a certain value of frequency a query will be fired and the filetered signatures will be left. The resulting traffic would thus be dropped thus preventing it.

Simple alerting is insufficient; we want to actively respond to an attempt that compromise security.

If we change rule type from alert to drop, Snort will start dropping whole of the traffic that matches with the rules in the database. So, in this way snort NIDS could be converted into a reactive NIDS.



Fig4: Block Diagram of NIEDS

Depending on the alerts generated, we analyze those alerts and observed which kind of attack is more harmful to the network under observation and need to be dropped. Also filtering is done on the basis of the two designed factors signature and frequency as discussed above. We convert those rules/ signatures from alert type to drop type.

The other way of creating reactive NIDS is:

- If you want to reset any illegitimate connection attempts, use the ttresp/tt keyword.
- If you want to use Snort to modify the rules of a firewall to block unwanted traffic, use SnortSAM.
- If you want to use Snort as a filter to remove unwanted traffic, you need to run Snort inline.

This removes the problem of attacker using an intrusion prevention system to create a denial of service. As it drops only packets that are suspect, it doesn't exclude an entire IP address.

We have used the first method that converts the types of rules from alert to drop. So we have made a Reactive and Preventive system for malware detection in a network.

Using snort the rules can be applied to following parts of packets:

- The IP header of the packet
- The transport layer header. This includes TCP, UDP and ICMP header.

Initially we had 5775 Snort rules/signatures. We ran the snort IDS for four weeks on a network, Analyze the traffic and make one table comprises of Signatures verses frequency with which they occur. From this, we got the top triggered signatures in a network under analysis. We repeat the exercise with Intrusion rules and extrusion rules separately and compare the two. There were number of malware types like botnets which can't be detected with Intrusion rules only. So it indicates that Extrusion traffic is equally important to analyze along with Intrusion traffic. After optimization only 1785 rules remains in Snort rules database.

BASE provides a web front-end to query and analyze the alerts coming from a SNORT IDS system. Multiply the values obtained from BASE by 1, 00 000 to show the escalation of results for at least 1 month as the results are for 1 hour of Network activity only. The optimization of rules is done in the following way:

- Unique alerts
- Categories of traffic in our network along with frequency of signatures triggered.
- Unique Source and Destination IP addresses observed
- Unique Source and Destination IP ports observed
- Top most frequent alerts in a network
- Show the traffic profile by protocol.

All these points are related to optimization of rules. As we have removed those rules from the rules database that never triggered during the course of analysis of network over a span of 4 weeks.

Snort will read all the contents from the specified tcpdump or log file and store the results in database which can be then analyzed using BASE. Our tool can read any log file which is in .pcap or .tcpdump format. The data of the file will be stored to MySQL database and output will be shown in BASE accordingly.

We had used our tool to read 2000 DARPA LLS_DDOS_1.0-inside.dump file. The majority of the traffic analyzed is ICMP-93%, TCP 6% and UDP-1%.

So, the tool is generalized one and can be used for both offline and online signature based detection of malware.

Ankita Tuteja, Ravi Shanker / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com

Vol. 2, Issue 3, May-Jun 2012, pp.1768-1774

IV. RESULTS AND DISCUSSION	C Basic Analysis and Security Engine (BASE) : Alert Listing - Windows Internet Explorer	.∂⊠
Below given are the screenshots from BASE after the test	🚱 🕤 💌 🔊 http://locahost/base_stat_alerts.php?sensor=2 🛛 💌 🗟 🐓 🗙 🦉 Live Search	P -
environment was analyzed.	File Edit View Favorites Tools Help	
🖉 Basic Analysis and Security Engine (BASE) : Sensor Listing - Windows Internet Explorer	🖕 Favorites 🛛 🙀 💽 Suggested Sites 🔹 🔊 Free Hotmail 🖉 Web Site Gallery 🔹	
S S 🔹 http://locahost/base_stat_sensor.php	🍘 🖉 🔊 🕐 🖉 🖉 🖉 🖉 🖉 🖉 🖉	@• [»]
File Edit View Favorites Tools Help		
👷 Favorites 🔹 📴 Suggested Sites 🕶 🖉 Free Hotmail 🖉 Web Site Gallery 🔹	Basic Analysis and Security Engine (BASE)	
Basic Analysis and Security Engine (BASE) : Sensor Lis	Home Search	
Basic Analysis and Security Engine (BASE)		Back]
Home Search	Queried on : Tue April 24, 2012 13:19:57	
[Back]	IP Criteria any Unique Alerts (classifications)	
Queried on : Tue April 24, 2012 13:17:43 Mata Criteria any	Payload Criteria any Unique Plinks	
IP Criteria any Layer 4 Criteria none	Source Fort, ICF UDP Operational Port, ICF UDP Time profile of alerts	
Payload Criteria any Displaying sierts 1-2 of 2 total	Displaying alerts 1-43 of 43 total	_
<sensor> <name> Cotal <unique Events> Events> <sec. addr.=""> <dest. addr.=""> <last></last></dest.></sec.></unique </name></sensor>		ast >
ANKITA-Devide-NPF [95401AD-ATEA-4536-874-50854900C05]/Devide-NPF_ 1915 34 262 38 2012-03-202012-03-21 [95401AD-ATEA-4536-874-50855490C055]/Devide-NPF_ 1915 34 262 [95401AD-ATEA-4536-874-50855490C055]/Devide-NPF_ 1915 34 262 [95401AD-ATEA-4536-874-50855490C055]/Devide-NPF_ 1915 34 262 [95401AD-ATEA-4536-874-50855490C055]/Devide-NPF_ 1915 34 262 [95401AD-ATEA-4536-874-50855490C055]/Devide-NPF_ 1915 34 265 [95401AD-ATEA-4536-874-50000]/Devide-NPF_ 1915 34 262 [95401AD-ATEA-4536-874-5085490C055]/Devide-NPF_ 1915 34 262 [95401AD-ATEA-4536-874-50000]/Devide-NPF_ 1915 34 202000]/Devide-NPF_ 1915 34 202000000000000000000000000000000000	Salod i Obligi Culte Destination Cinteschable (Differing Coder) miscretorivity 1622(40/a) 2 230 6 10500004 20124 1722002 10/3 1722002 10/3	18:42
2 AVVI IK 0 outside topoump outside topoump outside topoump 2143 16 32 39 1556-00-41 1556-00-40 1729 02 10.49 58 2 2010 0	Enorgi Lotter miteriocure Exceeded in Transit miteriocurvy to(c/a) 1 5 1 20/2021 20124 (Undefined Code) 10/28/04 10/31 (Undefined Code) 10/28/04 10/31 (Undefined Code) 10/28/04 10/31	13:24
(acton) Selected ALL on Screen	Story Four Interfoctive Exceeded in Transit Interfoctive View (1975) Society (19	13:24
Alert Group Maintenance Cache & Status Administration	European Control of the Control	28:09
BASE 1.4.5 (Ilitas) (by Kevin Johnson and the BASE Project Team	Langung pringer okneen even avon one policymaation ajong in in in 2012/oser 2012/ Italiae Pole Policie (2012)	>
∑ Done	🖉 🖌 🖓 🕶 🖏 759	% • ;;
🛃 start 🖉 🖉 🧭 Basic Analysis an 🗟 snap - Microsoft 🗟 Document2 - Micr 😰 👷 😓 🕉 🔺 1:18 PM	🛃 Start 🖉 🥙 🌈 Basic Analysis an 📓 snap - Microsoft 📓 Document 2 - Micr 👔 🕺 났 😓 🖉 🛋	1:20 PM
Fig5: Both offline and online analysis of traffic	Fig7: Alert Listing	
🖉 Basic Analysis and Security Engine (BASE) 1.4.5 (lilias) - Windows Internet Explorer	🖉 Basic Analysis and Security Engine (BASE) : Classification - Windows Internet Explorer	. 7 🗙
🚱 🗢 🖻 http://locahost.base_main.php	🚱 💿 🖻 http://localhost/base_stat_dass.php?sort_order=dass_a 🔽 🗟 🐓 🗙 🦉 Live Search	P -
File Edit View Favorites Tools Help	File Edit View Favorites Tools Help	
👷 Favorites 🛛 🙀 🔽 Suggested Sites 🔹 🖉 Free Hotmail 🖉 Web Site Gallery 🔹	🖕 Favorites 🛛 🙀 🔽 Suggested Sites 🔻 🖉 Free Hotmail 🖉 Web Sice Gallery 👻	
🖉 Basic Analysis and Security Engine (BASE) 1.4.5 (Ilias)	🖗 Rasic Analysis and Security Engine (BASE) : Classificat	(?) - »
		Back
Basic Analysis and Security Engine (BASE)	Queried on : Tue April 24, 2012 13:22:44	
	Meta Criteria any	
Today's alerts: unique listing Source IP Destination IP Dutatew. son@coatext.305 (Skewa Vesion: 107) Last 24 Hours alerts: unique listing Source IP Destination IP The Whole (1924) (1924) (1924) (1924) (1924)	IP Criteria any Laver 4 Criteria none	
- Last 72 Hours alerts: unique listing Source IP Destination IP	Payload Criteria any	
- Idea recent to Alerts. any protocol TCP UDP -Last Source Ports: any protocol TCP UDP	Displaying alerts 1-12 of 12 total	
- Last Destination Ports: any protocol TCP UDP Search - Most Frequent Source Ports: any protocol TCP UDP Graph Alert Data		:38:42
- Most Frequent Destination Ports: any protocol TCP UDP Graph Alert Detection Time	web-application-attack 15 (0%) 1 4 2 9 2012-03-20 18-48-23 2012-03-21 10: mittamproductions (2) (1%) 2 9 45 45 1020.05.01 (10.0000 0010.02.01 (10.0000 0000 0000 0000 0000 0000 00	:38:27
- Kost frequent to Addresses: Source Destination - Most recent 15 Unique Alerts	policy-violation 5 (%) 1 2 1 2 2012-03-21 10:20	:33:08
- Most frequent 5 Unique Alerts	trojan-activity 109 (3%) 2 3 5 28 1996-05-04 17:32:14 2012-03-21 10: unknown 57 (1%) 2 2 6 2 1998-05-04 19:16:53 2012-03-21 10:	:28:09 :38:27
Sensors/Total: 2 / 2 Traffic Profile by Protocol	web-application-activity 38 (1%) 1 1 1 1 10 2012-03-21 10:28-04 2012-03-21 10:	38:28
Unique Alerts: 43 TCP (%) Categories: 12	casummoun z3 (1%) z 4 6 4 1959-05-04 20:30:09 2012-03-21 10:30:24 sttempted-dos 6 (0%) 1 1 6 2012-03-21 10:30:24	:38:18 :33:29
Total Number of Alerts: AUSB UDP (< 1%)	system-call-detect 1 (0%) 1 1 1 1 1 2012/03/21 10: 2012/03/200/2012/03/200/2012/00/2012/00/200/200/200/200/200	:38:32
Sinc IP addrs: 283 Dest: IP addrs: 77 Instructional address and address a	attempte5-admin 1 (0%) 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	:49:58
Unique IP Infs 333 Source Forts: 241	ACTION	
• or TCP (237) UDP (4) Portscan Traffic (%)	(acton) ALL on Soreen	-
		_ , `
😧 Internet 🖓 🔹 🕺	ې المعاد الم	% • .:
🛃 Start 🛛 🖉 🦉 🧭 Basic Analysis an 🔛 snap - Microsoft 🔛 Document 2 - Micro 😰 🕺 👷 😓 🖗 1.1.9 PM	🕂 Start 🤌 🖗 🌈 Basic Analysis and Se 🖾 Document 2 - Microsof 🛛 🛛 🗮 🕄	1:22 PM
Figh Main comon of the traffic analyzed		

Fig6: Main screen of the traffic analyzed

Fig8: Categories of Alert Listing

Ankita Tuteja, Ravi Shanker / International Journal of Engineering Research and Applications (IJERA)

ISSN: 2248-9622 <u>www.ijera.com</u>

Vol. 2, Issue 3, May-Jun 2012, pp.1768-1774

	windows internet explorer		🖉 Basic Analysis and Security Engin	e (BASE) : IP Links - Wind	dows Internet Explorer		- 6 🛛
COO V Intp://localhost/base_stat_ports.php?por	vrt_type=18proto= 💌 🗟 🐓 🗙 🖡	🖌 Live Search	🚱 🗢 🙋 http://localhost/base_sta	at_iplink.php	💌 🗟 🐓 🗙 🧗 Live Search		• 9
File Edit View Favorites Tools Help			File Edit View Favorites Tools He	łp			
🚖 Favorites 🛛 🍰 Suggested Sites 🔹 🖉 Free Hotm	ail 🙋 Web Slice Gallery 🕶		😭 Favorites 🛛 🚔 🔁 Suggested Sites 🔻	🖉 Free Hotmail 🙋 Web Slic	e Gallery 🔹		
Basic Analysis and Security Engine (BASE) :	🔄 👌 · 🖻	🔹 📑 🔹 Page 🕶 Safety 🕶 Tools	Basic Analysis and Security Engine (BASE)) : IP Links	🏠 • 🗟 - 🖬 🖷 🌲 •	Page 🔹 Safety 🕶	Tools • 💽 • 👋
Queried on : Tue April 24, 2012 13:23:53 Meta: Criteria #ny IP: Criteria #ny Layer: 4 Criteria none Payload Criteria #ny	Displaying alerts 1-41 of 41 total		Queried on Tue April 24, 2012 13 28.48 Meta Criteria eny IP Criteria any Layer 4 Criteria none Payload Criteria eny	Displaying aler	ris 1-48 of 933 total		
< Port > < Sensor > < Occurre 20 [sans] [tantalo] [sstats] 1 2	ences > < Unique Alerts > < Src. Addr. > 1 1	<dest. addr.=""> < First > < La 1 1998-05-04 19:18:53 1998-05-04</dest.>	s Source FQDN < Source IP no DNS resolution attempted 192.168.1.1	Direction < Destination IP > > 192.168.1.2	Destination FQDN Protocol Unique Dst I ICMP 0	Ports Unique Events 2	Total Events 22
21 / tog (sans) [tunklo] (statis) 1 47 53 / tog (sans) [tunklo] (statis) 1 3 00 / dog (sans) [tunklo] (statis) 1 1 128 / tog (sans) [tunklo] (statis) 1 1 128 / tog (sans) [tunklo] (statis) 1 1 000 / tog (sans) [tunklo] (statis) 1 1 000 / tog (sans) [tunklo] (statis) 1 1 0169 / tog (sans) [tunklo] (statis) 1 1 0179 / tog (sans) [tunklo] (statis) 1 1 0100 / tog (sans) [tunklo] (statis) 1 1 01029 / tog (sans) [tunklo] (statis)	7 1 18 1 1 1 1 1 1 1 1 1 1 1 1 1 1	2 1988-054-115733 1980-054-0 1 2012-05421 102816 2012-0521 57 1988-0540 113211 2012-0521 1 1988-0540 113211 2012-0521 1 1988-0540 113241 21980-0540 1 2012-05421 102816 2012-0521 1 1988-0544 2010-02 1988-0544 1 998-0544 10022 1988-0544 1 2012-0541 1028 02 2012-0521 1 2012-0541 1028 02 2012-0521 1 2012-0541 1028 02 1988-0544 1 1988-0544 1800.24 1988-0544 1 998-0544 1800.24 1988-0544 1 998-0544 1800.24 1988-0544 1 998-0544 1800.24 1988-0544 1 2012-0541 1028 02 2012-05421 1 2012-0541 1028 02 2012-05421 1 2012-05421 1028 02 2012-05421 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	no DNS resolution attemptes 192.168.1.2 no DNS resolution attemptes 117.238.66 no DNS resolution attemptes 45.1324.152.0 no DNS resolution attemptes 45.1324.153.2 no DNS resolution attemptes 45.1324.153.2 no DNS resolution attemptes 27.124.1166 no DNS resolution attemptes 12.184.152.5 no DNS resolution attemptes 71.184.157 no DNS resolution attemptes 190.160.266 no DNS resolution attemptes 190.160.266 No NS resolution attemptes 190.160.266 <	→ 115.112.20 → 4.86256.125 3 → 117.228.666 → 74.125.256.103 9 → 117.228.666 1 → 117.228.565 5 → 117.228.565 → 117.228.	TCP 1 TCP 1 ICNP 0 TCP 1 ICNP 0 ICMP <		1 1 2 3 4 2 20 4 8 15 384 4 4 4 4 2 8 ₩ ¥ 15 384 4 4 2 8 ₩ ¥ 15 384 4 2 8 ₩ 15 384 4 2 8 ₩ 15 384 4 2 8 ₩ 15 384 4 2 8 ₩ 15 384 4 2 8 ₩ 16 16 16 16 16 16 16 16 16 16
Basic Analysis and Security Engine (BASE) : Alert Lis	ting Window Internet Synlarer		1	igii. Oilique	IF LINKS	4	
	ILINE - WINDOWS INTELLED UTEL		🖉 localhost / localhost / snort ph	pMvAdmin 2.6.4-pl3 - Wi	indows Internet Explorer		_ 3 X
A ttp://localhost/base_stat_alerts.php	🗸 🔊 🍕 🗙 🧗 Live Search		Cocalhost / localhost / snort ph	pMyAdmin 2.6.4-pl3 - Wi dmin/	indows Internet Explorer		¥5 - م
Image: Stat_alerts.php File Edit View Favorites Tools Heb	English and the search		localhost / localhost / snort ph	p MyAdmin 2.6.4-pl3 - Wi dmin/ eb	indows Internet Explorer		
Pavorites Pavorites	Web Size Gallery •		localhost / localhost / snort ph O	pMyAdmin 2.6.4-pl3 - Wi dmin/ elp Free Hotmail	indows Internet Explorer		
Image: State of the second state of	Web Sice Gallery •	P • Page + Safety + Tools + @ + **	C localhost / localhost / snort ph C localhost / localhost / snort ph Ple Edit View Favorites Tools H Favorites D upgested Sites * C localhost / localhost / snort phpMyAdmi	pMyAdmin 2.6.4-p13 - Wi dmin/ elp @ Free Hotmail @ Web Si n 2.6.4-p13	indows Internet Explorer Image: Second sec	▼ Page → Safety →	×
Image: State of the second state of	Web Sice Gallery • Web Si		C localhost / localhost / snort ph C localhost / localhost / snort ph C localhost / localhost / snort ph File Edit View Favorites Tools H Favorites C localhost / snort phpMyAdmin Distabase: snort (23)	htyAdmin 2.6.4-pt3 - Wi dmin/ ep Free Hotmal @ Web SI n2.6.4-pt3 nalert & Acc palert & Acc paler	indows Internet Explorer	Page - Safety - Collation Size swedish_d 320 swedish_d 480 swedish_d 320 swedish_d 320 swedish_d 160 swedish_d 160 swedish_d 1.61	Overhead KB KB
Classifica Sort Uncelnast Contact State Sort Uncelnast Contact State Sort Uncelnast Contact State Sort Uncelnast State	Web Sice Gallery Web Sice Gallery Web Sice Ga	Press Safety + Tools + Page + Safety + Tools + Page + Safety + Tools + Press + Page + Safety + Tools + Page + Safety + Tools + Page + Safety + Saf	localhost / localhost / snort ph ph phpMyAdmin Database: snort (23) snort s	pMyAdmin 2.6.4-p13 - Wi dmm/ eb E Free Hotmal @ Web St n2.6.4-p13 	indows Internet Explorer	Page - Safety - Collation Size swedish_d 320 swedish_d 480 swedish_d 301 swedish_d 320 swedish_d 180 swedish_d 160 swedish_d 160 swedish_d 160 swedish_d 160 swedish_d 160	
Constitution Constend on Constend Constit Constitution Constitutio	Summary Statistics Size Gallery • Size Gallery • Size Gallery • Size Gallery • Summary Statistics Search Size Gallery • Summary Statistics Search Unique Allert Classification Unique Allert Unique Allert Source Foil Unique Allert Unique Allert Classification Unique Allert Statistics Unique Allert Statistics Statistics Statistics Statistics Statistics Statistics Statistics Statistics		Iocalhost / localhost / snort ph Iocalhost / localhost / snort ph Image: State of the state of th	pMyAdmin 2.6.4-p13 - Wi dmin/ @ Free Hotmal @ Web SI n2.6.4-p13	indows Internet Explorer	Page - Safety - Ollation Size swedish_d 22.01 swedish_d 48.01 swedish_d 48.01 swedish_d 16.01 swedish_d 16.01 swedish_d 16.01 swedish_d 16.01 swedish_d 48.01 swedish_d 48.01 swedish_d 16.01 sw	
Image: Second State Secon	Numbers Numbers <t< td=""><td>Page - Safety + Tools - Page - Safety + Tools - Page - Safety + Tools - Page - Safety - Tools - Page - Page - Safety - Tools - Page - Page - Safety - Tool - Page - Safety - Tool - Page - Safety - Tool - Safety - Tool - Safety - Tool -</td><td>C localhost / localhost / snort ph Image: Signal Sign</td><td>hty Admin 2. 6. 4. pt 3 - Wi dmin/ elp Pree Hotmal () Web SI n 2.6.4-pt 3 p.alent 6 2 p.alent 7 2 p.al</td><td>indows Internet Explorer</td><td>Page - Safety - Dilation Size _swedish_d 22.0 _wedish_d 48.0 _wedish_d 48.0 _wedish_d 16.0 _wedish_d 16.0 _wedish_d 16.0 _wedish_d 16.0 _wedish_d 48.0 _wedish_d 48.0 _wedish_d 16.0 _wedi</td><td>Image: Construction of the second s</td></t<>	Page - Safety + Tools - Page - Safety + Tools - Page - Safety + Tools - Page - Safety - Tools - Page - Page - Safety - Tools - Page - Page - Safety - Tool - Page - Safety - Tool - Page - Safety - Tool - Safety - Tool - Safety - Tool -	C localhost / localhost / snort ph Image: Signal Sign	hty Admin 2. 6. 4. pt 3 - Wi dmin/ elp Pree Hotmal () Web SI n 2.6.4-pt 3 p.alent 6 2 p.alent 7 2 p.al	indows Internet Explorer	Page - Safety - Dilation Size _swedish_d 22.0 _wedish_d 48.0 _wedish_d 48.0 _wedish_d 16.0 _wedish_d 16.0 _wedish_d 16.0 _wedish_d 16.0 _wedish_d 48.0 _wedish_d 48.0 _wedish_d 16.0 _wedi	Image: Construction of the second s
Image: Start Sta	Number variations Sammary Statistics Web Size Gallery * Image Advances Web Size Gallery * Image Advances Image Advances Sammary Statistics Sammary Statistics Sensors Image Advances Sensors Image Advances Unique Advances Image Advances Sensors # Image Advances Source Address > Vity 13075) 1 Image Advances Source Address > Vity 13075) 1 Image Advances Source Address > Vity 1075) 1 Image Advances Source Address > Image Advances Source Address > Vity 1075) 1 Image Advances Source Address > Image Advances Source Advances Image Advances Source Advances Image	Page - Safety + Tools -	Collabost / localhost / snort ph Image: Start Image: Start	hty Admin 2.6.4.pt 3 - Wi dmin/ elp elp elp elp elp free Hotmal p free Hotmal elp trable	indows Internet Explorer	Page - Safety - Collation Size _swedish_d 32.0 _swedish_d 48.0 _swedish_d 16.0 _s	

Ankita Tuteja, Ravi Shanker / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com

Vol. 2, Issue 3, May-Jun 2012, pp.1768-1774

ICMP PING NMAP ICMP PING Sun Solaris

Incalhost / Incalhost	/ snort / signature	nhnWvAdmin 2.6	↓ 4-n13 - Windows Li	OI. Z, . nternet Explo	Issue 3, .	May-
No v 🖉 http://de	calhost/ohomvadmin/	, in party in the second second		Nuive Search		ا ع ا
e Edit View Favorit	es Tools Help					
Favorites 🛛 👍 🐻 Su	opested Sites 🔹 🖉 Fre	e Hotmail 🖉 Web Sice	Gallery 🕶			
elocahost / locahost / sn	ort / signature phpMvAd	min	- 	a - 🗆 🖨	▼ Page ▼ Safety ▼	Tools 🔹 🔞 🕶
~ /	R Server localhost	A Database: snort k l	Table: signature "Inc	oDR free: 10240	κR'	
	Browse Struct	ure SQL Dearch	insert Export	%Operations	Empty XDrop	
phpMyAdmin	Field T	ype Collation	Attributes Null Defau	lt Extra	Action	
A 🖬 🛛 🖉	sig id int(1	0)	UNSIGNED NO	auto_increment	🖊 🗙 🖫 📴 🗉 🗉	
TWAA	sig_name vard	ar(255) latin1_swedish_c	i No		🖊 🗙 🖫 📝 🗊 🗉	
tabase:	sig_class_id int(1))	UNSIGNED NO		🖊 🗙 🖫 📴 🗉 🗉	
ort (25)	sig_priority int(1)	J)	UNSIGNED Yes NULL		🖊 🗙 🖫 📴 🗉 🗉	
scid_event scid_jp_csche	sig_rev int(1)))	UNBIGNED Yes NULL		/ X 🛛 🖻 🔍 🗉	
base_roles	sig_sid int(1))	UNSIGNED Yes NULL			
data 🖉	sig_gid int(1)))	UNSIGNED Yes NULL		🗸 🔨 🕅 🕅 🗉	
Setail encoding	Check All / Un	pheok All With selected	/ 🖍 🖁 🖻 🔟			
event	Sela Print view	tion view 🛛 📠 Propose ta	ble structure@			
emprior phár	Add 1 field(s)	At End of Table OAt	Beginning of Table 🔘	After sig_id	Go Go	
opt mierence					-	
eference_system	Indexes: (7) Keyname Tyr	e Cardinality Action	Field Type	usage:	Row Statistics: Statements V	alue
chema ensor	PRIMARY PRIM	ARY 43 🖉 🗙 :	sig_id Data	16,384 Bytes	Format Compact	
sig_class in Iran	sign_idx INDEX	(43 🖉 🗙 :	sig_name 20 Index	32,768 Bytes	Collation latin1_sw	edish_ci
sig_reference	sig_class_id_idx INDE)	(43 🖉 🗙 s	sig_class_id Total	49,152 Bytes	Next Autoindex	44
signature tcohdr	Create an inde	ex on 1 columns	Go		Creation Mar 20, 20	12 at 08:29 PM
udphdr 💊	Pup COL quant/quaria	s on database sport@		Cielde:		
				😝 Internet	- A -	€ 75% ·
Istart 6 6	A Dominist	Mirroré 🖉 I	المحمد المحمد ال			
	a Antoniaus	Photosu 6 DC	anost / localnost /		4 ×××	9 66 1.42 PM
g13: Con	tains all t	he inforn	nation ab	out sig	gnatures	
		SIGNA	TURE			
NE EDOC	E quoru	rachanca	with ttl.	1 min	and no	
	л query	response	with thi.	1 11111	. and no	
ithority		-				
Г CURRI	ENT_EVI	ENTS PC	DLICY D	NS U	pdate Fro	m
xternal ne	t					
T CURRI	ENT EVI	ENTS Ur	known l	Keenal	ive in	
	Spambau		Listed T	raffic 1	nhound	-
T MAI W	ARE Fur	Web Pr	oducts A	gent T	raffic	1
TMALW		Wob Dr	oducts A	nyuwor	a Hear A	ront
T MAI W	ARE FUI	sible Wi	ndows er	py war	ble sent u	then
mote hos	t claims to	o send a '	Text File	uta	one sent w	nen
T MAI W	ARF Pos	sible Wi	ndowser	xecuta	hle sent w	hen
mote hos	t claime t	o send a '	Text File	uta	one sent w	nen
T MAL W		CVS5 T	IDD D.		aund Cr	mast
IMALW	AKE SO	CKSV3 L	DP Proz	xy Inb	ouna Con	nect
eauest (W	/indows S	Source)				

ET RBN Known Russian Business Network IP TCP ET RBN Known Russian Business Network IP UDP

ICMP Destination Unreachable (Fragmentation Needed

ICMP Destination Unreachable (Network Unreachable) ICMP Destination Unreachable (Undefined Code!) ICMP Fragment Reassembly Time Exceeded

FTP Bad login

ICMP PING

and DF bit was set)

ICMP L3retriever Ping

ICMP PING (Undefined Code!)

ICMP PING CyberKit 2.2 Windows

	ICMP PING Windows						
	ICMP superscan echo						
»	ICMP Time-To-Live Exceeded in Transit (Undefined						
	Code!)						
^	ICMP traceroute						
	MISC Large ICMP Packet						
	SHELLCODE x86 NOOP						
	WEB-ATTACKS cc command attempt						
	WEB-ATTACKS mail command attempt						
Ξ	WEB-ATTACKS netcat command attempt						
	WEB-ATTACKS rm command attempt						
	WEB-CGI archie access						
	WEB-CGI calendar access						
	WEB-CGI redirect access						
	WEB-CGI rsh access						
	WEB-CGI wrap access						
	WEB-IIS scripts access						
	WEB-IIS Unauthorized IP Access Attempt						
	WEB-IIS view source via translate header						
v	WEB-MISC 403 Forbidden						
	WEB-MISC backup access						
	WEB-MISC count.cgi access						
	WEB-MISC handler access						
	WEB-MISC http directory traversal						
٦	WEB-MISC Invalid URL						
-	WEB-MISC musicat access						
	WEB-MISC whisker head						
	Table1: Top Triggered Signature						
	Generic Protocol Command Decode						
	Executable code was detected						
	Access to a potentially vulnerable web application						
	Unknown Trattic						
	Network Trojan was detected						
	Potential Corporate Privacy violation						
	Web Application Attack						
	Potentially Red Traffic						
	Attempted Information Leak						
	Mise Attack						
	Table?: Summary of Attacks						
	autor. Summary Of Attacks						

Ankita Tuteja, Ravi Shanker / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.1768-1774



alerts

V. CONCLUSION

Snort is a common Intrusion detection system which for our task was modified to analyze extrusion traffic as well. The proposed work was carried out on Windows XP because of its friendly interface. We have tried our best to optimize Snort so that our network could be made more secure. Different factors from various sources are studied and combined together to come up with efficient system so that our network could be made more secure. With the advantages there are also some drawbacks of Intrusion detection system which will prevail among them are that Intrusion detection system are not a solution to all security concerns, an IDS is not a subsitute for a good security policy and human intervention is required. In the proposed work also human intervention is required once an attack is detected and reported it is our responsibility of the to determine how it occurred, correct the problem and take necessary action to prevent the occurrence of the same attack in future.

REFERENCES

- Charlie Scott, Paul Wolfe, Bert Hayes, Snort For Dummies (Wiley Publishing, Inc., Indianapolis, 2004)
- [2] Karen Scarfone, Peter Mell, *Guide to Intrusion Detection and Prevention Systems* (National Institute of Standards and Technology Special Publication 800-94, 2007)
- [3] Rafeeq Ur Rehman Intrusion Detection Systems with Snort (Pearson Education, Inc., 2003)

- [4] Cecile Lussie, *Signature Based Extrusion Detection*, Institute for Technische Informatik und kommunikationsnetze, MA, 2008
- [5] Farzaneh Izak Shiri, Bharanidharan Shanmugam, Norbik Bashah Idris, A Parallel Technique for improving the performance of Signature-Based Network Intrusion Detection System, *IEEE*,2011
- [6] Mohd Nazri Ismail, Mohd Taha Ismail, Framework of Intrusion Detection System via Snort Application on Campus Network Environment, *International Conference on Future Computer and Communication*, 2009.
- [7] Muhammad Naveed, Shams Un Nihar, Mohammad Inayatullah Babar, Network Intrusion Prevention by Configuring ACLs on the Routers, *International Conference Emerging Technologies (ICET)*,2010
- [8] Rebecca Bacel and Peter Mell2, *NIST Special Publication on Intrusion Detection Systems*, Special Publication 800-94, February 2007.
- [9] SANS Institute-Understanding Intrusion Detection Systems, 2001
- [10] Sunny Behal, Amanpreet Singh Brar, Krishan Kumar, Signature-Based Botnet Detection and Prevention, *Springer*, 2009.
- [11] Sunny Behal, Krishan Kumar, An Experimental Analysis for Malware Detection Using Extrusions, International Conference on Computer and Communication Technology, 2011
- [12] Zhou Zhimin, Chen Zhongwen, Zhou Ti echeng, Guan Xiaohui, The Study of Network Intrusion Detection System of Snort, International Conference on Networking and Digital Society,2010
- [13] http://www.ll.mit.edu/mission/communications/ ist/corpora/ideval/data/index.html
- [15] http://www.streetdirectory.com/travel_guide/15 4241/security/importance_of_network_security_yst em.html
- [16] http://www.brighthub.com/computing/enterprise security /articles/69275.aspx
- [17] http://qualitative.wikidot.com/dimensions-ofresearch
- [18] www.snort.org
- [19] www.emergingthreats.com