Intrusion Detection a Challenge: SNORT the savior

Gurven Vaseer, Dr. Pushpinder Singh Patheja

Lecturer, OP Jindal University, Raigarh, Chattisgarh, India
Professor, Oriental Institute of Science & Technology, Bhopal, MP, India

***Abstract* —** *Technology has become an integral part of our life. With the incredible advancements in the field of technology encompassing networking and security concepts, we are still lacking in protecting our devices from thefts/attacks. This is becoming a grave challenge for organizations/institutes, hence by this paper we are able to use Snort as a tool for detecting attacks and generating standard rules that can be implemented and thus will minimize security breaches.*

Keywords*—Intrusion Detection System, IP packet, ICMP packet.*

I. INTRODUCTION

In this era of digitization, traditional methods of data storage and manipulation are obsolete. Thus computers have become the crux of handling data. The most important factor thus becomes the immense protection of this data from intruders, and hence intrusion detection systems become all the more important for us. Malicious users or hackers use the organization's internal systems to collect information and cause vulnerabilities like Software bugs, Lapse in administration, leaving systems to default configuration [4]. Intrusion detection System (IDS) is a type of security management system for computers and networks [1]. An intrusion detection system (IDS) monitors all outbound and inbound network action and finds out the doubtful patterns that may point to a network or system intrusion or attack from someone trying to crack into or conciliation a system. IDS gathers and observes information from different areas inside a network of systems to find out probable safety breaches, which contain together called intrusions (attacks exterior from the association) and misuse (attacks from inside the association). IDS use susceptibility assessment, it is an expertise which is designed and developed to appraise the security of a network [2].

SNORT is an open source Intrusion Detection System (IDS), which may also be configured as an Intrusion Prevention system (IPS) for monitoring and prevention of security attacks on networks. It's especially useful in detecting a wide variety of attacks and probes, including buffer overflows, stealth port scans and CGI attacks. In fact, this freeware tool is so capable; it's not a stretch to say that Snort is one of the best network-based intrusion detection systems (IDS), free or otherwise.

II. SNORT : RULES TO DETECT MALICIOUS ACTIVITY

A Snort rule can be broken down into two basic parts, the rule header and options for the rule. The rule header contains the action to perform, the protocol that the rule applies to, and the source and destination addresses and ports. The rule options allow you to create a descriptive message to associate with the rule, as well as check a variety of other packet attributes by making use of Snort's extensive library of plug-ins.

A. IP ping alert

If we want to trigger an alert on seeing any IP packet or ICMP packet this rule set is used. Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages[3].

- go to /etc/snort/snort.conf
- set the HOME_NET variable to the local ip i.e assigned by the n/w administrator .eg. 10.60.18.15
- set the EXTERNAL_NET variable to !HOME_NET
- search for the list of rules variable in that snort.conf file...

  something like this

  #include $RULE_PATH/app-detect.rules

#include $RULE_PATH/attack-responses.rules

#include $RULE_PATH/backdoor.rules

#include $RULE_PATH/bad-traffic.rules

#include $RULE_PATH/blacklist.rules

#include $RULE_PATH/botnet-cnc.rules

#include $RULE_PATH/browser-chrome.rules

#include $RULE_PATH/browser-firefox.rules

#include $RULE_PATH/browser-ie.rules

#include $RULE_PATH/browser-other.rules

- include this lines without quotes "include $RULE_PATH/myrules.rules" in between any of these above rules.

  Note: for a single host system try to comment unused rules by putting '#' at the beginning of the rules path so that the snort work more efficently.

- exit from snort.conf
- go to /etc/snort/rules/ and create a file name 'myrules.rules'
- edit that file and insert the rule for ping alert.

  alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"outside ping"; icode:0; itype:8; sid:10000;)

EXPLANATION

alert- type of action perform by snort(currently used - alert, reject, drop, log, activate ,dynamic, sdrop)

icmp - type of protocol used. (currently used - ip, tcp, udp, icmp)

$EXTERNAL_NET - external network

$HOME_NET -home network

any - port no

-> direction of the packet

msg- message to be printed

icode- the icode field is used to explain icmp redirect packet in details. If the icmp packets has following code then means:

0, it is a network redirect ICMP packet.

1, it is a host redirect packet.

2, the redirect is due to the type of service and network.

3, the redirect is due to type of service and host.

itype: it denotes the icmp type field

0, echo reply

3, destination unreachable

4, source quench

5, redirect

8, echo request

sid= snort rule id aka signature id (Note: use 10000 or greater value for creating own rules)

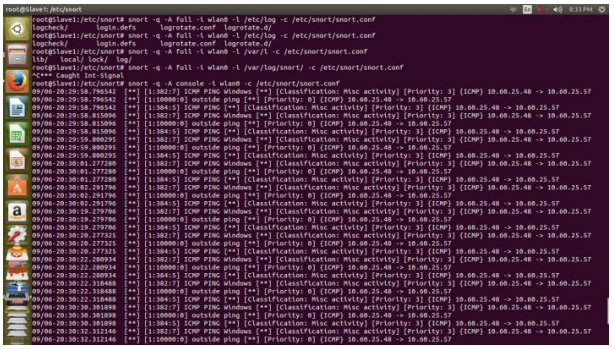

Figure 1: Shows an IP ping alert

B. SYN FIN Attack

Sneaky-Firewall Bypass Attack

Checks any syn flood attack from source to destination i.e check amount of connections permissible in a particular time period.

alert tcp any any -> $HOME_NET any (flags: SF; msg: "SYNC-FIN packet detected";)

EXPLANATION
flags- flag on the tcp header file...
S - SYN flag used for connection establishing
F - FIN finish flag

C. Content based filteration

If we want to check any malicious access to a website or any other relevant content we can use the below mentioned rules.

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"facebook accessed"; content:"facebook"; nocase; sid:10002;)

EXPLANATION
content- the string through website is accessed.
nocase - check on both UPPERCASE and lowercase.

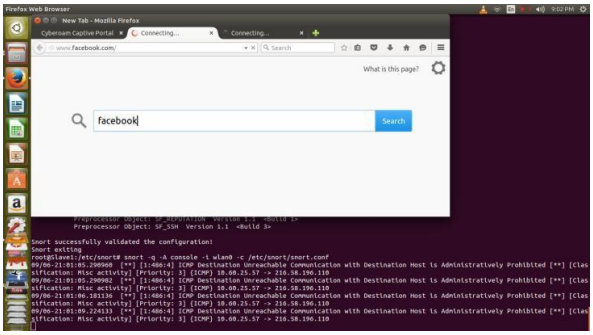

Figure 2: shows user access to facebook website

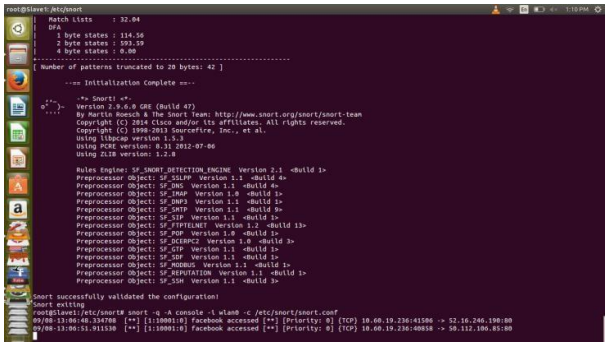

Figure 3: shows how by rules facebook access is detected

D. Incoming FTP connection

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"incoming ftp connection";flags:S;sid:10001)

EXPLANATION:

flags - S is used to check tcp SYN flag which is responsible for connection creation.

E. Testing of rules:

In order to test the above mentioned rules we need to:

exit from gedit.open the terminal and enter the following commands

snort -c /etc/snort/snort.conf -T /etc/snort/rules/myrules.rules

then restart the snort

/etc/init.d/snort restart

and run the rules
snort -q -A console -i wlan0 -c /etc/snort/snort.conf

III. CONCLUSION

Intrusion detection study has gained momentum since the past 10 years in order to protect our valuable data from malicious attempts. Snort however needs to be explored in order to detect complicated problems. The motive of this paper is to develop preliminary rules for detecting basic attacks like ip ping alert etc. and to make the device secure. It is also used for detecting accessing of websites which is the main area of concern for organizations/institutes these days. Further work will be done to proceed in this direction and detect even more complex attacks in large data.

REFERENCES

[1] K. Jungwon, J. B. Peter, A. Uwe, G. Julie, T. Gianni and T. Jamie, "Immune System Approaches to Intrusion Detection – A Review", Natural Computing: an international journal, vol. 6, Issue 4, **(2007)** December.

[2] E. J. Derrick, R. W. Tibbs and L. L. Reynolds, "Investigating New Approaches to Data Collection, Management and Analysis for Network Intrusion Detection", ACMSE, Winston-Salem, N. Carolina, USA, (2007) March 23-24, pp. 283-287.

[3] Forouzan, Behrouz A. (2007). Data Communications And Networking (Fourth ed.). Boston: McGraw-Hill. pp. 621–630. ISBN 0-07-296775-7.

[4] Christopher Low –"Understanding Wireless attacks &detection "-GIAC Security Essentials Certification (GSEC) Practical Assignment 13 April 2005 -SANS Institute InfoSec Reading Room.