ISSN 2278-3091

Volume 9 No.2, March - April 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse171922020.pdf

https://doi.org/10.30534/ijatcse/2020/171922020

Performing Forensic Analysis on Network to Identify Malicious Traffic

Jonnadula Bala Harika[1], Dr B. Chaitanya Krishna[2]

[1] M.Tech, Department of CSE, KLEF, Vaddeswaram,, A.P, India, harika07.jonnadula@gmail.com

[2]Associate Professor, Department of CSE, KLEF, Vaddeswaram, A.P, India, chaitu2502@kluniversity.in

ABSTRACT

With the wide range of internet, cybercrime attacks are increased against the networked system and raised the importance of network security. More and more cyber threats are confronting organizations. The malicious threats in an enterprise make use of the network for industrial spying. It is important to examine the data in the context of packets being transmitted across the network to recognize the suspect's behaviors. Network administrators must be able to analyze and examine the networking traffic to understand how the events occur and to execute immediate reactions in case of an unexpected attack. Network forensics is like a camera for monitoring, correlating, checking and investigating network traffic for different objectives such as a gathering of information, forensic evidence, or ids (intrusion detection system). This paper proposes a Network forensics analysis framework to identify malicious threats in network traffic using Wireshark and generate alert using snort. An algorithm is proposed to find the attack intentions. Wireshark is used to diagnosis of the protocols in the network and used to identify network-based attacks such as port scanning, TCP based attacks, and HTTP based attacks. Snort is used to detect network-based attacks using some rules and all activities on network traffic are recorded on Snort are stored in a log file.

Key words : Attacks, Framework, Network Forensics, Network traffic.

1.INTRODUCTION

Because of pervasive computer networks, network security has now become essential in an online society. Today the majority of them use computers, tablets, and smartphones every day for web-based correspondence, and the use of e-mail servers, network servers, and web servers to access multiple applications. These accesses build sand of information across the web. We've long since gone through the internet to analyze its work and to understand it [16]. Nonetheless, the very fact is that we humans have already built a much more strong and complicated framework, we can understand bits and pieces of it and we can develop broad generalization. A whole new field of study emerged during this time, i.e. network forensics (usually refers to scientific research on network evidence).

The forensic network may be an area of study outside of any particular legal case and may recognize many technological advances, devices, and techniques developed for the requirements of the criminal investigation. The Forensic Network provides a way to see the evidence behind a crime scene on the Internet. We will figure out how to discover information that is hidden on the Web in every email, website and web server [17]. Through my ongoing study of other network challenges, we analyze the malicious use of the Internet and its key protocols.

Most of the people's perception, network forensics involves the CIA method. CIA stands for Capturing the packets, Identifying date and time of packets and Analyzing both know and unknown packets.

Network forensics handles data that can be found mainly on inbound and outbound traffic across a network connection. Network forensics tries to examine network traffic logged via IDS or firewalls as well as on network devices such as routers and switches.

Forensics in the network can generally be described as a science of finding and retrieving relevant information from a couple of crimes in the networked world and making them appropriate in court. Typically cybercrime investigation includes cases involving Homeland Security Office, spying for companies, pornography, traditional crimes supported by computer equipment and network technology, monitoring of employees or medical records, in which privacy is a crucial issue.

Forensics in the network involves tracking network traffic and assessing whether there's a traffic anomaly and whether it signals an attack. If an attack is observed, the kind of attack also will be calculated next to that. Network forensic methods allow researchers to follow the criminal(s). The primary objective is to provide solid evidence to enable the prosecution of the criminal.

2.RELATED WORK

Kanti Singh Sangher and Archana Singh[1]have presented a literature review to distinguish the new IDS and a learning-based method is introduced and includes the peer-to-peer technology framework also use internet automata to monitor and record the crime.
Prabhjot Kaur, Anchit Bijalwan, R.C. Joshi and Amit Awasthi [2] have Compared with the existing network forensic process models and systems, they have introduced a software model. Network forensic analysis assesses network traffic to track flooding and investigate how and why the crime occurred.
Nour Moustafa, Jill Slay [3] mainly focuses on capturing, storing network data and selecting essential features of a network utilizing the chi-square method including investigating unexpected events utilizing the corr-entropy technique was explained with a case study.
Desti Mualfah and Imam Riadi [4] have proposed the detection of flooding attacks on a network by performing forensics on the webserver. Snort can be used to find out attacks by using some rules and all activities on network traffic are recorded in snort as log files that are useful for an investigation to find out the evidence.
Akhyar Lubis and Andysah Putera Utama Siahaan [5] are supported to improve the network forensics process. Network Forensics tools are used to find out a crime on network traffic in common cases.
Jingsha He, Chengyue Chang, Peng He, and Muhammad Salman Pathan [6] have Suggested a piece of compromise evidence as well as an algorithm to recreate attack situations and network traceback packets to find the actual evidence.
Suleman Khan, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Muhammad Shiraz, Iftikhar Ahmad [7] have presented a review on network forensics that can track internal and external threats by concentrating on main network weaknesses and interaction channels. They provide a history and analysis of network forensics strategies and transparent challenges.
Barenya Bikash Hazarika and Smriti Priya Medhi [8] explains about network forensics and collect the network traffic. It provides different security mechanisms(Firewall, Email Forensics, Intrusion Detection System, Web forensics) for the investigation purpose.
Hariyanto, AndysahPutera Utama Siahaan[9] have built an intrusion detection system to protect the network from threats. Network administrators have to create a new signature when a problem arises and stay updated with new types of attacks.
Joseph MbuguaChahira, Jane KinanuKiruki, Peter KipronoKemei [10] aimed to find out optimum performance on various known and unknown threats resulting in new alerts to improve alert quality and identify different attack strategy.
Vivens Ndatinya, Zhifeng Xiao Vasudeva Rao Manepalli, Ke Meng and Yang Xiao [11] gives a brief overview of Wireshark for capturing and analyzing the network traffic to find out the malicious packets.
Abhishek Srivastav and Irman Ali [12] are focusing on several techniques and tools to perform network forensics, emerging forensics area, and comparison charts.
Manish Kumar, M.Hanumanthappa and T.V.Suresh Kumar[13] are discussing techniques to overcome IP spoofing. The technique is to find out the source IP address of the intruder on the geographical map.
Natarajan Meghanathan, Sumanth Reddy Allam and Loretta A. Moore[14]discuss several techniques and tools to perform network forensics and detect different attacks by using IP trace back mechanisms.
Sarandis Mitropoulos, Dimitrios Patsos, Christos Douligeris[15] have presented an overview of classification schema for all trace back problems.

3. Extracting evidence from a pcap file:

The analyst must have sturdy knowledge and awareness about the OSI model and packet examination on each layer to finally leverage PCAP as a forensic mechanism. Packet capture (PCAP) is the systematic reporting of data packets passing through capture devices that are characteristic of the network traffic.

Frame signifies the section of transferring into a second layer protocol also consists of a second layer header continued on a packet. The network in a computer uses a frame through digital information transmission. During the HTTP request a protocol header is appended to the packet in the seventh application layer. Application layer header payload Transport layer header and network layer header are included within a packet. Figure 1 explains the different headers of a protocol.

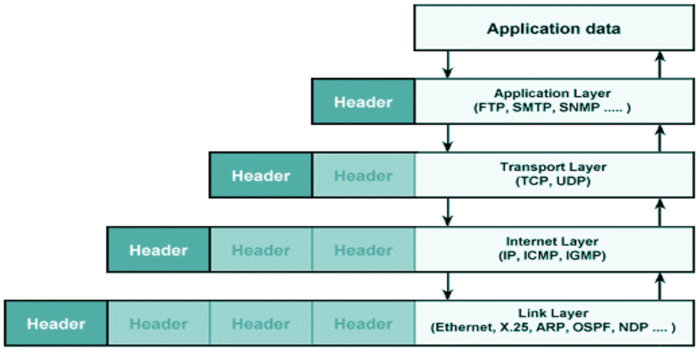

Application data
Header
Application Layer (FTP, SMTP, SNMP .....)
Header
Header
Transport Layer (TCP, UDP)
Header
Header
Header
Internet Layer (IP, ICMP, IGMP)
Header
Header
Header
Header
Link Layer (Ethernet, X.25, ARP, OSPF, NDP ....)

Figure 1: OSI Model

This part presents the investigation of the DNS, HTTP, TLS packets to obtain the evidence. To identify the malicious packets, a framework is proposed based on the packet analysis.

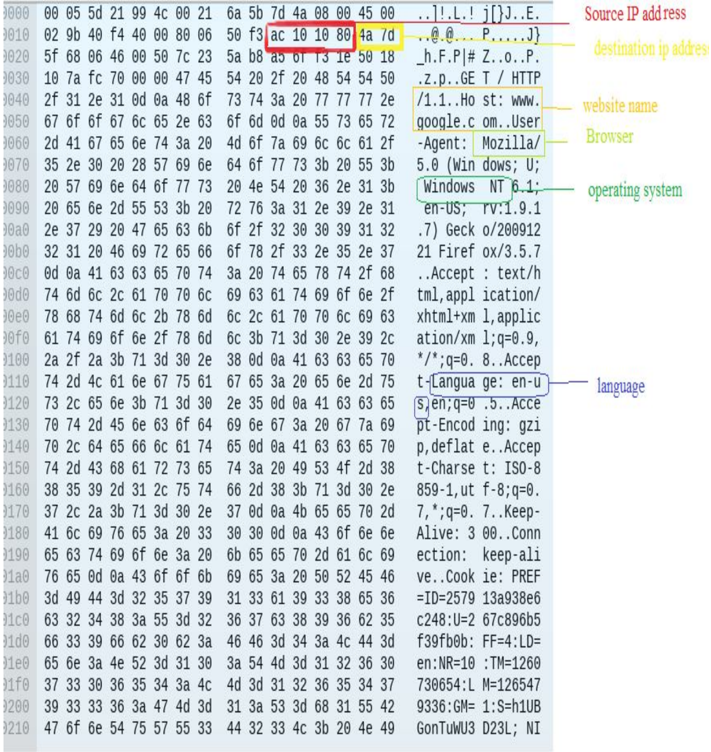
3.1 HTTP

In order to download the websites or web pages on the host system, web browsers utilize the HTTP to interact with this remote server. The HTTP is unprotected because it transfers the data without encrypting them in plain text. That increases the attacker's possibilities of data theft. we can use the HTTP header to analyze the client details and the server details. It is likely to identify the website which the user accesses at the client system. By carrying out the HTTP packet analysis, the forensic investigator will be able to recognize the evidence of the Internet activities carried out.

The application layer within the OSI model utilizes the HTTP to interact with these remote servers. The resulting forensic details from the intercepted HTTP packets can be identified.

a. Features of the client system:

Through examining the HTTP packets, one can learn about the different client system specifics like the type of web browser being used, the client-side configured operating system and the client device language package. Figure 2 displays the picture of the HTTP packet recorded with the specifics of the client device. While the client device is claimed to give the features thereof to the server of which the data is to be retrieved and this message exists in plain text.



```
0000  00 05 5d 21 99 4c 00 21  6a 5b 7d 4a 08 00 45 00   ..]!.L.! j[}J..E.
0010  02 9b 40 f4 40 00 80 06  50 f3 ac 10 10 80 4a 7d   ..@.@... P.....J}
0020  5f 68 06 46 00 50 7c 23  5a b8 a5 6f f3 1e 50 18   _h.F.P|# Z..o..P.
0030  10 7a fc 70 00 00 47 45  54 20 2f 20 48 54 54 50   .z.p..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  67 6f 6f 67 6c 65 2e 63  6f 6d 0d 0a 55 73 65 72   google.c om..User
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0070  35 2e 30 20 28 57 69 6e  64 6f 77 73 3b 20 55 3b   5.0 (Win dows; U;
0080  20 57 69 6e 64 6f 77 73  20 4e 54 20 36 2e 31 3b    Windows  NT 6.1;
0090  20 65 6e 2d 55 53 3b 20  72 76 3a 31 2e 39 2e 31    en-US;  rv:1.9.1
00a0  2e 37 29 20 47 65 63 6b  6f 2f 32 30 30 39 31 32   .7) Geck o/200912
00b0  32 31 20 46 69 72 65 66  6f 78 2f 33 2e 35 2e 37   21 Firef ox/3.5.7
00c0  0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 68   ..Accept : text/h
00d0  74 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   tml,appl ication/
00e0  78 68 74 6d 6c 2b 78 6d  6c 2c 61 70 70 6c 69 63   xhtml+xm l,applic
00f0  61 74 69 6f 6e 2f 78 6d  6c 3b 71 3d 30 2e 39 2c   ation/xm l;q=0.9,
0100  2a 2f 2a 3b 71 3d 30 2e  38 0d 0a 41 63 63 65 70   */*;q=0. 8..Accep
0110  74 2d 4c 61 6e 67 75 61  67 65 3a 20 65 6e 2d 75   t-Langua ge: en-u
0120  73 2c 65 6e 3b 71 3d 30  2e 35 0d 0a 41 63 63 65   s,en;q=0 .5..Acce
0130  70 74 2d 45 6e 63 6f 64  69 6e 67 3a 20 67 7a 69   pt-Encod ing: gzi
0140  70 2c 64 65 66 6c 61 74  65 0d 0a 41 63 63 65 70   p,deflat e..Accep
0150  74 2d 43 68 61 72 73 65  74 3a 20 49 53 4f 2d 38   t-Charse t: ISO-8
0160  38 35 39 2d 31 2c 75 74  66 2d 38 3b 71 3d 30 2e   859-1,ut f-8;q=0.
0170  37 2c 2a 3b 71 3d 30 2e  37 0d 0a 4b 65 65 70 2d   7,*;q=0. 7..Keep-
0180  41 6c 69 76 65 3a 20 33  30 30 0d 0a 43 6f 6e 6e   Alive: 3 00..Conn
0190  65 63 74 69 6f 6e 3a 20  6b 65 65 70 2d 61 6c 69   ection:  keep-ali
01a0  76 65 0d 0a 43 6f 6f 6b  69 65 3a 20 50 52 45 46   ve..Cook ie: PREF
01b0  3d 49 44 3d 32 35 37 39  31 33 61 39 33 38 65 36   =ID=2579 13a938e6
01c0  63 32 34 38 3a 55 3d 32  36 37 63 38 39 36 62 35   c248:U=2 67c896b5
01d0  66 33 39 66 62 30 62 3a  46 46 3d 34 3a 4c 44 3d   f39fb0b: FF=4:LD=
01e0  65 6e 3a 4e 52 3d 31 30  3a 54 4d 3d 31 32 36 30   en:NR=10 :TM=1260
01f0  37 33 30 36 35 34 3a 4c  4d 3d 31 32 36 35 34 37   730654:L M=126547
0200  39 33 33 36 3a 47 4d 3d  31 3a 53 3d 68 31 55 42   9336:GM= 1:S=h1UB
0210  47 6f 6e 54 75 57 55 33  44 32 33 4c 3b 20 4e 49   GonTuWU3 D23L; NI
```

Figure 2: HTTP GET request

b. About Port

During the information is transmitted across the system the transport layer joins its header being displayed in fig 1. The transport layer header is made up of the sender port number and the recipient. Through understanding the port numberof the packet and a forensic investigator may determine the kind of services that the server offers in communication. The server's source port number equals 80 which means the web service of HTTP.

c. Examining the Web Site

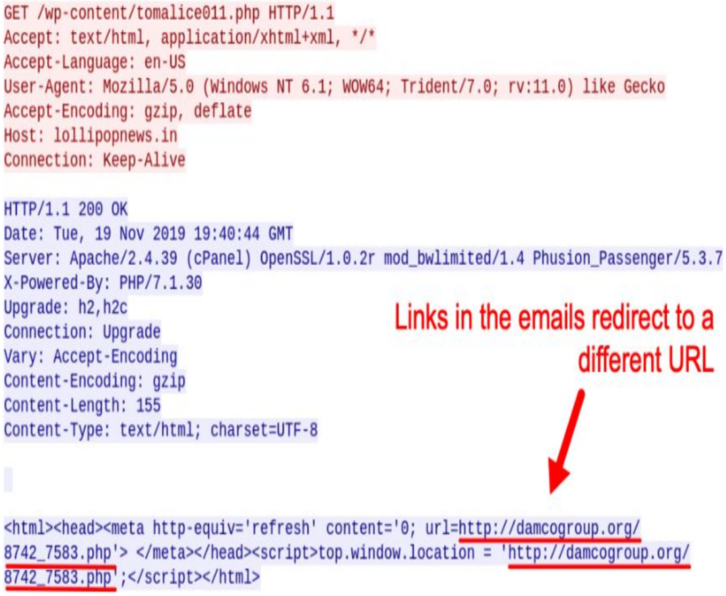
The host websites can be detected by analyzing the header of HTTP protocol in a LAN. To access a specific website of the server the client utilizes the HTTP protocol GET request form. Using the HTTP protocol POST form the server replies to the client's web page. HTTP is the headline of the website concerned. Figure 2 displays the HTTP GET request method.

d. IP address

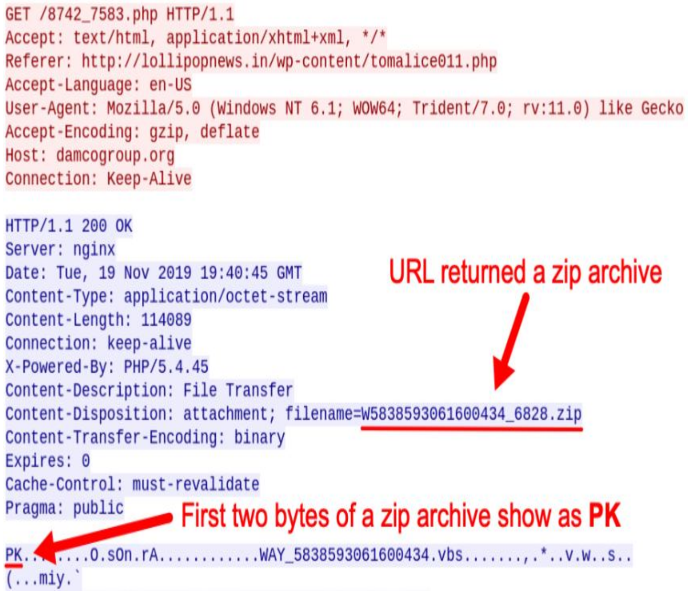
As presented in figure 1 the Bottom layer of the OSI model is effective adding the IPheader to every layer and the information moved off to the top laye. This IPheader provides source and destination information. The forensic investigator will find the devices that are section of the interaction by knowing certain addresses.

e. Attached Document

The malicious threats can send via e-mail and grabs the sensitive documents in an organization, which can be detected by packet analysis. Figure 3 explains the document attached to the mail. The links in the mail are redirected to a different URL



```
GET /wp-content/tomalice011.php HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: lollipopnews.in
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 19 Nov 2019 19:40:44 GMT
Server: Apache/2.4.39 (cPanel) OpenSSL/1.0.2r mod_bwlimited/1.4 Phusion_Passenger/5.3.7
X-Powered-By: PHP/7.1.30
Upgrade: h2,h2c
Connection: Upgrade
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 155
Content-Type: text/html; charset=UTF-8


<html><head><meta http-equiv='refresh' content='0; url=http://damcogroup.org/
8742_7583.php'> </meta></head><script>top.window.location = 'http://damcogroup.org/
8742_7583.php';</script></html>
```



```
GET /8742_7583.php HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://lollipopnews.in/wp-content/tomalice011.php
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: damcogroup.org
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 19 Nov 2019 19:40:45 GMT
Content-Type: application/octet-stream
Content-Length: 114089
Connection: keep-alive
X-Powered-By: PHP/5.4.45
Content-Description: File Transfer
Content-Disposition: attachment; filename=W5838593061600434_6828.zip
Content-Transfer-Encoding: binary
Expires: 0
Cache-Control: must-revalidate
Pragma: public

PK.......O.sOn.rA...........WAY_5838593061600434.vbs.......,.*..v.w..s..
(...miy.`
```

URL returned a zip archive

First two bytes of a zip archive show as **PK**

Figure 3:TCP stream

3.2 DNS

The Domain Name System (DNS) is composed of messages including request (query) and response. Through examining request messages, the sites accessed can be identified using the secure (https) protocol. The server's IP address that hosts the website together with the client's IP address that accesses the website is known for the response message.

3.3 TLS

Transport layer security (TLS) observes and secure every interaction between a client and a server. The root and target IP address and using port information is given by the TLS packet. While the TLS packet is carried across the network HTTPS is resolved based upon the port number. TLS is encrypted while the application data is being transferred and data is secure.

4. PROPOSED SYSTEM

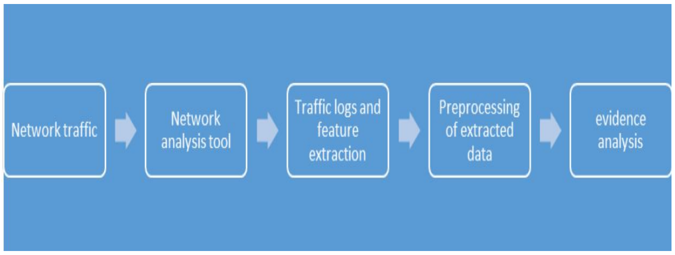

Network traffic
Network analysis tool
Traffic logs and feature extraction
Preprocessing of extracted data
evidence analysis

Figure 4: Proposed Framework

During the Initial Stage, examine the network traffic using network analysis tools. The Analysis stage will perform different analyses such as web request analysis, packet analysis, troubleshooting network problems, etc. After completion of the analysis stage, a report is going to generate any kinds of traffic records including many pieces of the network-based Application Program Interfaces(API) calls which may be suspicious. At the fourth stage, the extracted data are preprocessed as not all data present within the report are going to be suspicious data. During the final stage, investigate the collected evidence to find out the suspicious data. To present an analysis of the network forensics, the tools used three necessary skills: traffic capturing and logging data, identifying data, and examining data.

•Traffic Capturing and Logging Data: This is the ability to capture and store multiple terabytes of data from high throughput networks (including 10G and even 40G networks) without dropping or missing any packets. Every network forensic solution has its limitations, including sustainable throughput, packets per second, data management, search functions, etc. These limitations can and should be determined through practical lab tests, and the results should be repeatable and documented.

• Identifying Data: Once data are recorded on the storage media, the solution should provide a means of filtering particular items of interest, for example, by IP address, application, context, etc. IT engineers rely on discovery tools for sifting through terabytes of data to find specific network conversations or individual packets in a timely fashion.

• Examine Data: To further accelerate discovery and analysis, IT engineers benefit from a forensics solution's built-in assistance for examining the patterns and anomalies found during the discovery process. Automated analysis, including Expert analysis that explains the context of network events, helps IT engineers quickly identify anomalous or otherwise significant network events.

There are various tools employed for network traffic monitoring and analysis such as:

- TCPDUMP
- SNORT
- WIRESHARK

However, we are mainly focused on using a tool called SNORT, an open-source tool for Network Intrusion Detection System.

4.1 SNORT

Different network based attacks cannot be identified by rule matching and they don't either present a signature or a pattern into the payload various payloads can be utilized for every attack so that rule matching method breaks To detect various attacks a different approach must be used The first approach is to write the rule to identify the attack and the next one is to examine the packet headers that may show anomalies providing the evidence regarding a crime or a probe may occur Snort rule consists of the rule header and rule options

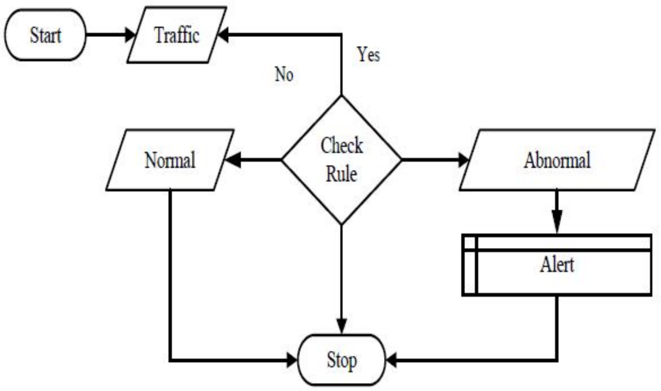


Figure 5: Snort

4.1.1 Rule Header

alert – Rule action. Snort will generate an alert when the set condition is met.
any – Source IP. Snort will look at all sources.
any – Source port. Snort will look at all ports.
-> – Direction. From source to destination.
$HOME_NET – Destination IP. We are using the HOME_NET value from the snort.conf file.
any – Destination port. Snort will look at all ports on the protected network.

4.1.2 Rule Options

msg: "ICMP test" – Snort will include this message with the alert.
sid:1000001 – Snort rule ID. Remember all numbers < 1,000,000 are reserved, this is why we are starting with 1000001 (you may use any number, as long as it's greater than 1,000,000).
rev:1 – Revision number. This option allows for easier rule maintenance.
class type: Icmp-event – Categorizes the rule as an "ICMP-event", one of the predefined Snort categories. This option helps with the rule organization.

To know the attack intentions, an **algorithm** is proposed.

```
Input: Attacks with their evidence and potential intentions.
Output: Estimation of attack intention probability.
Begin
    Let A a set of conditional independence attacks {a1,a2,a3…an} each one has a state between [0,1]
    Define Ak where Ak ϵ A, with a state of accurate ratio.
    Let EV a set of conditional dependence attack evidences {ev1,ev2,ev3…evn}
    Define EVs for Ak where EVs ϵ EV, Ak ϵ A, and Ak has one or more EVs
    Let I a set of all possible of conditional dependence intentions {i1,i2,i3…in}
    For each EVs ϵ EV related to Ak ϵ A do
        Define Ip for each EVs where Ip ϵ I
    End For
    Let C be a causal network to present an attack intention, where Ak is an apparent node connected with their EVs and Ip connected with EVs
    Let H is a set of hypothesis {h1,h2,h3…hn} that related to the attack detection accuracy and collection of evidence
    For each Ak ϵ A that has EVs ϵ EV do
        For each EVs do
            Compute P(EVs| Ip) and its complement
            Compute P(EVs)
        End For
        For each Ip ϵ I do
            Select EVs ϵ EV
            Compute P(Ip |EVs)
            Assign HX for each Ip where HX ϵ H
            Compute BPA(Ip) for Ip where ∑ BPA(Ip) =1
            Compute Be(Ip)
            Compute Pl(Ip)
            Select ix as an attack intention where ix ϵ Ip and ix is the highest degree of Be(Ip)
        End For
    End For
End
```

5. EXPERIMENTAL RESULTS

This is the point where malware attempts to enter the victim's system. This could be done by clicking a link in an e-mail, which could result in a browser hijack that directs the victim to where the attacker wants them to go. The moment the victim connects to a malicious website, the site directs the victim seamlessly to a Traffic Distribution Server (TDS). This determines the victim's OS and browser. A TDS can be quite sophisticated and can filter out connection requests based on the browser type, OS, IP addresses, and other criteria. The TDS can be set to drop or redirect requests to decoy sites from known IP addresses of security researchers, antivirus, or malware firms. These IP addresses that meet the preset criteria are directed to the exploit. The attacker's objectives are to gain undetected access to the victim's computer. Based on the data gleaned about the victim's environment, the exploit kit will identify a vulnerability in the browser or browser plugins and direct the victim to a server running the specific exploit required to compromise their machine and gain a foothold in the system. The malicious payload is downloaded to the victim's computer and the system is infected. The insider tends to take advantage of the compromised or exploited system. During this stage, the malware may call home and establish a connection to exfiltrate sensitive data or act as part of a botnet. It may even encrypt a victim's data and attempt to extort money to decrypt it.

Flow diagram of malicious threat:

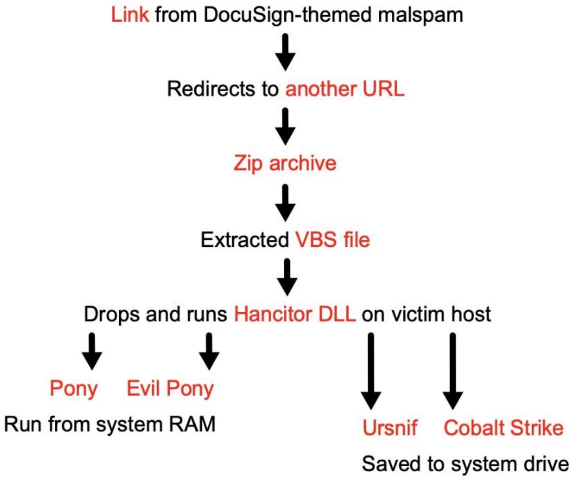
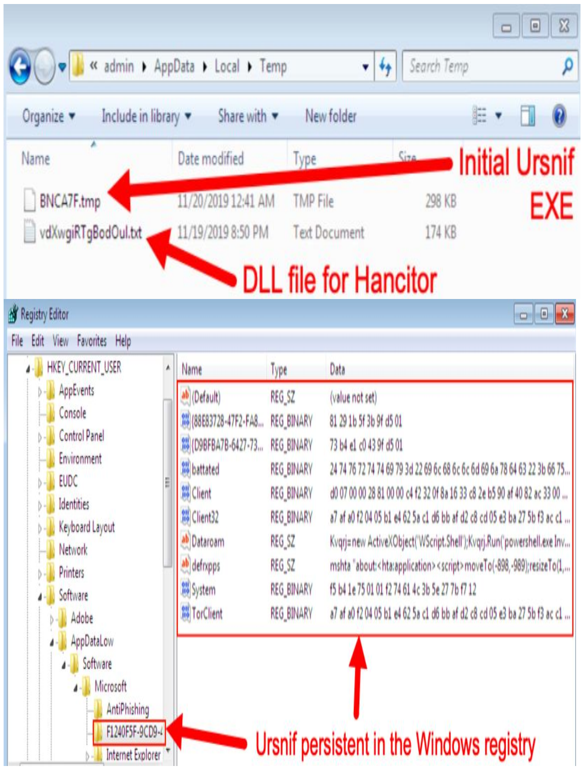


Figure 6: Flow chart

5.1 Indicators of Compromise



Name	Date modified	Type	Size
BNCA7F.tmp	11/20/2019 12:41 AM	TMP File	298 KB
vdXwgiRTgBodOul.txt	11/19/2019 8:50 PM	Text Document	174 KB

Initial Ursnif EXE

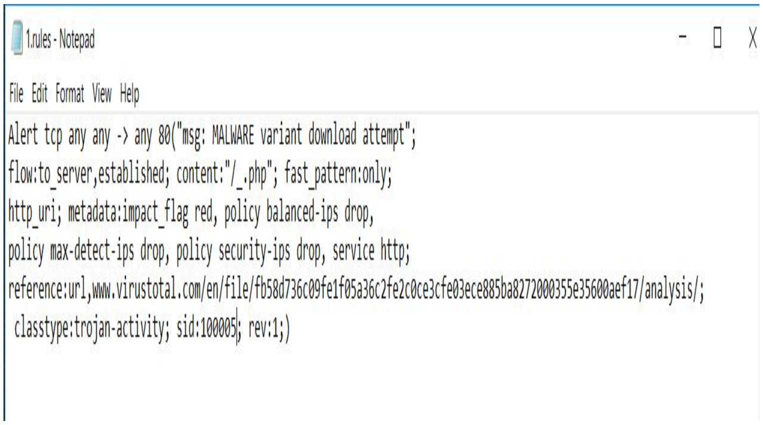
DLL file for Hancitor

Name	Type	Data
(Default)	REG_SZ	(value not set)
{88E83728-47F2-FA8...	REG_BINARY	81 29 1b 5f 3b 9f d5 01
{D9BFBA7B-6427-73...	REG_BINARY	73 b4 e1 c0 43 9f d5 01
battated	REG_BINARY	24 74 76 72 74 74 69 79 3d 22 69 6c 68 6c 6c 6d 69 6a 78 64 63 22 3b 66 75...
Client	REG_BINARY	d0 07 00 00 28 81 00 00 c4 f2 32 0f 8a 16 33 c8 2e b5 90 af 40 82 ac 33 00 ...
Client32	REG_BINARY	a7 af a0 f2 04 05 b1 e4 62 5a c1 d6 bb af d2 c8 cd 05 e3 ba 27 5b f3 ac c1 ...
Dataroam	REG_SZ	Kvqrj=new ActiveXObject('WScript.Shell');Kvqrj.Run('powershell.exe Inv...
defrxpps	REG_SZ	mshta "about:<hta:application><script>moveTo(-898,-989);resizeTo(1,...
System	REG_BINARY	f5 b4 1e 75 01 01 f2 74 61 4c 3b 5e 27 7b f7 12
TorClient	REG_BINARY	a7 af a0 f2 04 05 b1 e4 62 5a c1 d6 bb af d2 c8 cd 05 e3 ba 27 5b f3 ac c1 ...

Ursnif persistent in the Windows registry

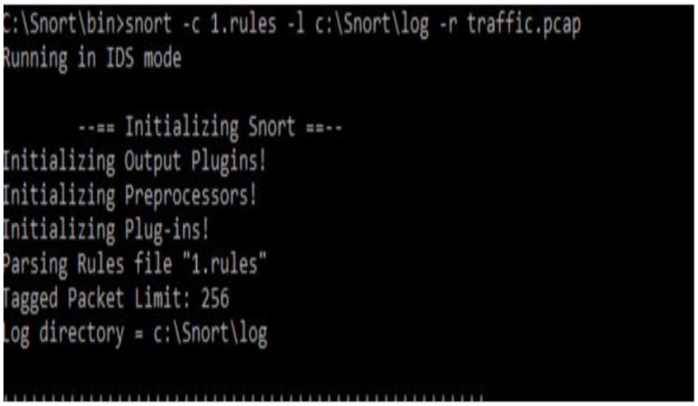
Fig 7: IOC

5.2 Rule for hancitor malware



```
Alert tcp any any -> any 80("msg: MALWARE variant download attempt";
flow:to_server,established; content:"/_.php"; fast_pattern:only;
http_uri; metadata:impact_flag red, policy balanced-ips drop,
policy max-detect-ips drop, policy security-ips drop, service http;
reference:url,www.virustotal.com/en/file/fb58d736c09fe1f05a36c2fe2c0ce3cfe03ece885ba8272000355e35600aef17/analysis/;
 classtype:trojan-activity; sid:100005; rev:1;)
```

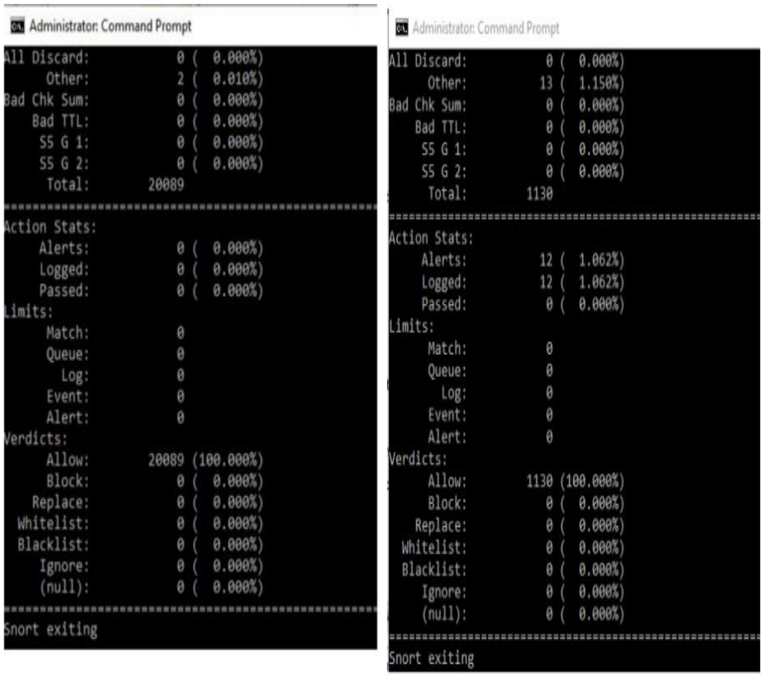
To generate alerts, following command is used.



```
:\Snort\bin>snort -c 1.rules -l c:\Snort\log -r traffic.pcap
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "1.rules"
Tagged Packet Limit: 256
Log directory = c:\Snort\log
```

Fig 8: Snort command

Before and after the rule writing, alert counts.

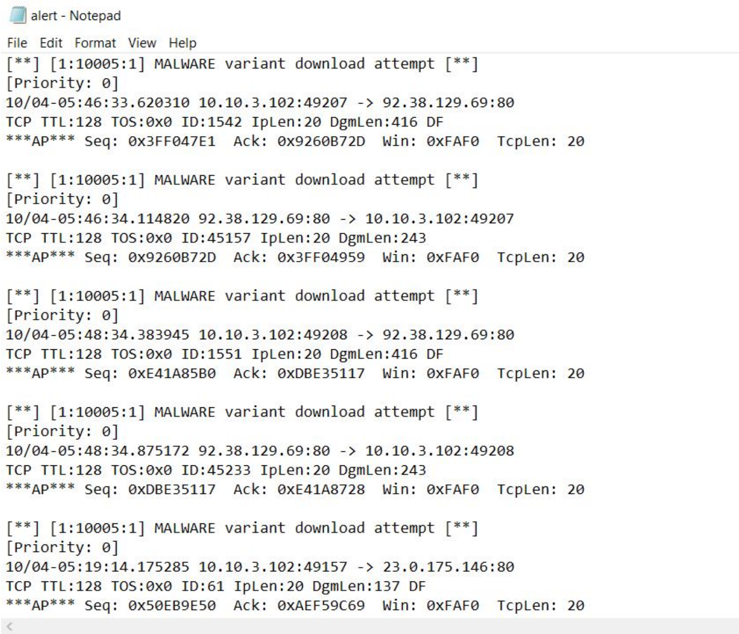


```
All Discard:             0 (  0.000%)
      Other:             2 (  0.010%)
Bad Chk Sum:             0 (  0.000%)
    Bad TTL:             0 (  0.000%)
     S5 G 1:             0 (  0.000%)
     S5 G 2:             0 (  0.000%)
      Total:         20089
===============================================================
Action Stats:
     Alerts:             0 (  0.000%)
     Logged:             0 (  0.000%)
     Passed:             0 (  0.000%)
Limits:
      Match:             0
      Queue:             0
        Log:             0
      Event:             0
      Alert:             0
Verdicts:
      Allow:         20089 (100.000%)
      Block:             0 (  0.000%)
    Replace:             0 (  0.000%)
  Whitelist:             0 (  0.000%)
  Blacklist:             0 (  0.000%)
     Ignore:             0 (  0.000%)
     (null):             0 (  0.000%)
===============================================================
Snort exiting
```

```
All Discard:             0 (  0.000%)
      Other:            13 (  1.150%)
Bad Chk Sum:             0 (  0.000%)
    Bad TTL:             0 (  0.000%)
     S5 G 1:             0 (  0.000%)
     S5 G 2:             0 (  0.000%)
      Total:          1130
===============================================================
Action Stats:
     Alerts:            12 (  1.062%)
     Logged:            12 (  1.062%)
     Passed:             0 (  0.000%)
Limits:
      Match:             0
      Queue:             0
        Log:             0
      Event:             0
      Alert:             0
Verdicts:
      Allow:          1130 (100.000%)
      Block:             0 (  0.000%)
    Replace:             0 (  0.000%)
  Whitelist:             0 (  0.000%)
  Blacklist:             0 (  0.000%)
     Ignore:             0 (  0.000%)
     (null):             0 (  0.000%)
===============================================================
Snort exiting
```

Figure 9: alert count

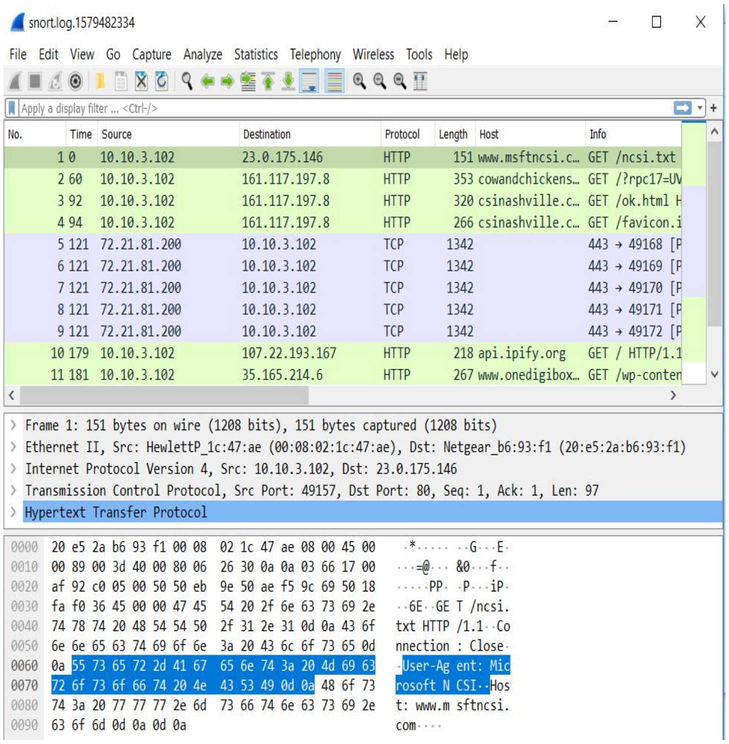
A alert message is generated in .txt format.



```
[**] [1:10005:1] MALWARE variant download attempt [**]
[Priority: 0]
10/04-05:46:33.620310 10.10.3.102:49207 -> 92.38.129.69:80
TCP TTL:128 TOS:0x0 ID:1542 IpLen:20 DgmLen:416 DF
***AP*** Seq: 0x3FF047E1  Ack: 0x9260B72D  Win: 0xFAF0  TcpLen: 20

[**] [1:10005:1] MALWARE variant download attempt [**]
[Priority: 0]
10/04-05:46:34.114820 92.38.129.69:80 -> 10.10.3.102:49207
TCP TTL:128 TOS:0x0 ID:45157 IpLen:20 DgmLen:243
***AP*** Seq: 0x9260B72D  Ack: 0x3FF04959  Win: 0xFAF0  TcpLen: 20

[**] [1:10005:1] MALWARE variant download attempt [**]
[Priority: 0]
10/04-05:48:34.383945 10.10.3.102:49208 -> 92.38.129.69:80
TCP TTL:128 TOS:0x0 ID:1551 IpLen:20 DgmLen:416 DF
***AP*** Seq: 0xE41A85B0  Ack: 0xDBE35117  Win: 0xFAF0  TcpLen: 20

[**] [1:10005:1] MALWARE variant download attempt [**]
[Priority: 0]
10/04-05:48:34.875172 92.38.129.69:80 -> 10.10.3.102:49208
TCP TTL:128 TOS:0x0 ID:45233 IpLen:20 DgmLen:243
***AP*** Seq: 0xDBE35117  Ack: 0xE41A8728  Win: 0xFAF0  TcpLen: 20

[**] [1:10005:1] MALWARE variant download attempt [**]
[Priority: 0]
10/04-05:19:14.175285 10.10.3.102:49157 -> 23.0.175.146:80
TCP TTL:128 TOS:0x0 ID:61 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x50EB9E50  Ack: 0xAEF59C69  Win: 0xFAF0  TcpLen: 20
```

Figure 10: Alert msg

The results of Snort log file is viewed to obtain evidence. After the Snort log files are recorded, the log file will be taken and analyzed using Wireshark to have this forensic evidence. When detected, the Snort rules will give a warning message in the alerts as shown in figure.


snort.log.1579482334
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

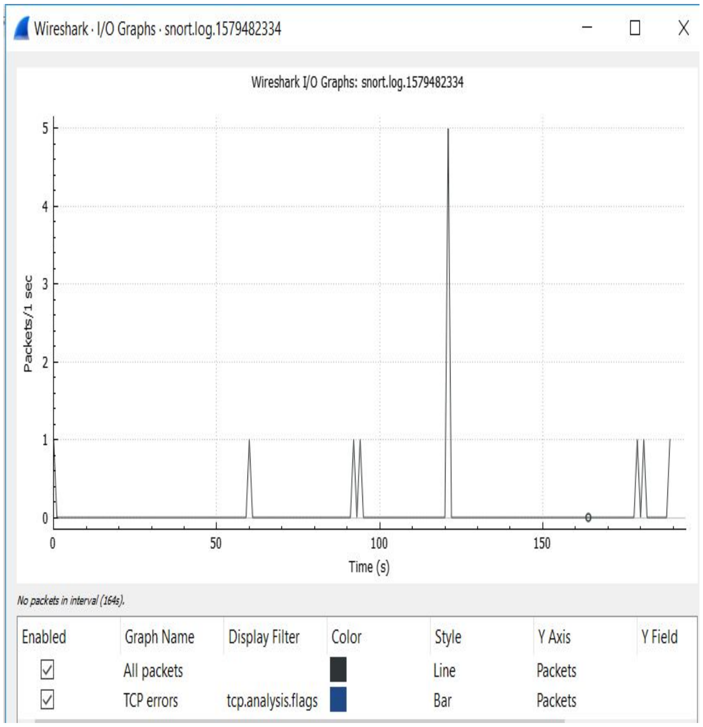
No.	Time	Source	Destination	Protocol	Length	Host	Info
1	0	10.10.3.102	23.0.175.146	HTTP	151	www.msftncsi.c…	GET /ncsi.txt
2	60	10.10.3.102	161.117.197.8	HTTP	353	cowandchickens…	GET /?rpc17=UV
3	92	10.10.3.102	161.117.197.8	HTTP	320	csinashville.c…	GET /ok.html H
4	94	10.10.3.102	161.117.197.8	HTTP	266	csinashville.c…	GET /favicon.i
5	121	72.21.81.200	10.10.3.102	TCP	1342		443 → 49168 [P
6	121	72.21.81.200	10.10.3.102	TCP	1342		443 → 49169 [P
7	121	72.21.81.200	10.10.3.102	TCP	1342		443 → 49170 [P
8	121	72.21.81.200	10.10.3.102	TCP	1342		443 → 49171 [P
9	121	72.21.81.200	10.10.3.102	TCP	1342		443 → 49172 [P
10	179	10.10.3.102	107.22.193.167	HTTP	218	api.ipify.org	GET / HTTP/1.1
11	181	10.10.3.102	35.165.214.6	HTTP	267	www.onedigibox…	GET /wp-conten

```
> Frame 1: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)
> Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
> Internet Protocol Version 4, Src: 10.10.3.102, Dst: 23.0.175.146
> Transmission Control Protocol, Src Port: 49157, Dst Port: 80, Seq: 1, Ack: 1, Len: 97
> Hypertext Transfer Protocol
```

```
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00   .*····· ··G···E·
0010  00 89 00 3d 40 00 80 06  26 30 0a 0a 03 66 17 00   ···=@··· &0···f··
0020  af 92 c0 05 00 50 50 eb  9e 50 ae f5 9c 69 50 18   ·····PP· ·P···iP·
0030  fa f0 36 45 00 00 47 45  54 20 2f 6e 63 73 69 2e   ··6E··GE T /ncsi.
0040  74 78 74 20 48 54 54 50  2f 31 2e 31 0d 0a 43 6f   txt HTTP /1.1··Co
0050  6e 6e 65 63 74 69 6f 6e  3a 20 43 6c 6f 73 65 0d   nnection : Close·
0060  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 69 63   ·User-Ag ent: Mic
0070  72 6f 73 6f 66 74 20 4e  43 53 49 0d 0a 48 6f 73   rosoft N CSI··Hos
0080  74 3a 20 77 77 77 2e 6d  73 66 74 6e 63 73 69 2e   t: www.m sftncsi.
0090  63 6f 6d 0d 0a 0d 0a                               com····
```

Figure 11: Snort.log

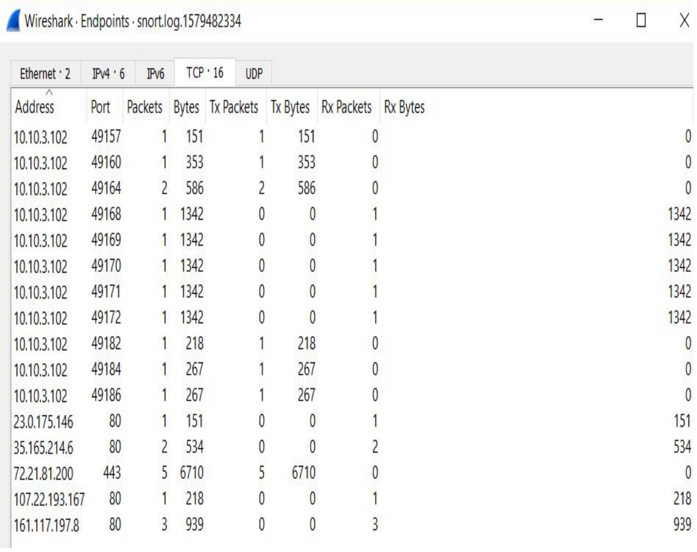
The graph shows the snort.log file overview.



Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field
☑	All packets		■	Line	Packets	
☑	TCP errors	tcp.analysis.flags	■	Bar	Packets	

Figure 12: Graph

In addition, the analysis continued with statistics module endpoint in Wireshark used to collect attack packets contained in log files Intrusion Detection System (IDS) Snort during the attack simulation.



Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.10.3.102	49157	1	151	1	151	0	0
10.10.3.102	49160	1	353	1	353	0	0
10.10.3.102	49164	2	586	2	586	0	0
10.10.3.102	49168	1	1342	0	0	1	1342
10.10.3.102	49169	1	1342	0	0	1	1342
10.10.3.102	49170	1	1342	0	0	1	1342
10.10.3.102	49171	1	1342	0	0	1	1342
10.10.3.102	49172	1	1342	0	0	1	1342
10.10.3.102	49182	1	218	1	218	0	0
10.10.3.102	49184	1	267	1	267	0	0
10.10.3.102	49186	1	267	1	267	0	0
23.0.175.146	80	1	151	0	0	1	151
35.165.214.6	80	2	534	0	0	2	534
72.21.81.200	443	5	6710	5	6710	0	0
107.22.193.167	80	1	218	0	0	1	218
161.117.197.8	80	3	939	0	0	3	939

Figure 13: End points

6.CONCLUSION AND FUTURE WORK

In this paper, we tried to improve network-based attack detection rates using the new 1.Rules. We had seen that it had the full capacity to recognize all of the attacks, which have a defined rule for the matching signature after the usage of SNORT as an intrusion detection system. Today's hackers are very creative and they create the new symbol for different attacks so sometimes, but not always, they can be effective because we have a gun like rules and snort. our purpose to detect stubborn TCP, ICMP and UDP malicious packets during snorting. As a result of this, we have found snort to be capable of detecting attacks and of producing warnings based on installation guidelines. Therefore, to detect and generate alerts based on the rule-based intrusion detection method we have to use the latest rules such that we can generate for zero-days based network attacks also.

In the future, we plan to create an automated solution where we can detect those attacks for which there is no rule mentioned in the configuration file. With the help of the machine learning concept, Using the alert generation file as a training data set we will train our platform to detect the zero-days based network attacks. We also plan to integrate various methods of network intrusion detection (i.e. rule-based, Anomaly-based, Behavior-based) on the same data and observe whether the integrated approach performs better than the individual approach or not.

REFERENCES

[1] Kanti Singh Sangher & Archana Singh. "**A Systematic Review – Intrusion Detection Algorithms Optimisation for Network Forensic Analysis and Investigation**". *International conf. Automation, Computational and Technology Management.* Pp.132-136,2019. doi:10.1109/ICACTM.2019.8776801

[2] Prabhjot Kaur, Anchit Bijalwan, R.C. Joshi and Amit Awasthi. "**Network Forensic Process Model and Framework: An Alternative Scenario**". *Advances in Intelligent Systems and Computing 624*, Pp.493-502, 2018. Doi:https://doi.org/10.1007/978-981-10-5903-2_50

[3] Nour Moustafa, Jill Slay. "**RCNF: Real-time Collaborative Network Forensic Scheme for Evidence Analysis**". *arXiv-Cornell University.* 2017.doi:https://arxiv.org/abs/1711.02824

[4] Desti Mualfah and Imam Riadi. "**Network Forensics For Detecting Flooding Attack On Web Server**". *International Journal of Computer Science and Information Security, Vol.15, No. 2, February 2017.* Pp.326-331. doi:https://sites.google.com/site/ijcsis/ISSN 1947-5500 PaperID:31011770

[5] Akhyar Lubis and Andysah Putera Utama Siahaan. "**Network Forensic Application in General Cases**". *IOSR Journal of Computer Engineering (IOSR-JCE)* Volume 18, Issue 6, Ver. IV (Nov.-Dec. 2016), Pp 41-44. doi:10.31227/osf.io/93zgm

[6] Jingsha He, Chengyue Chang, Peng He, and Muhammad Salman Pathan. "**Network Forensics Method Based on Evidence Graph and Vulnerability Reasoning**". Future Internet 2016, 8, 54;Pp.1-18 doi:10.3390/fi8040054

[7] Suleman Khan, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Muhammad Shiraz, Iftikhar Ahmad."**Network forensics: Review, taxonomy, and open challenges**". *Journal of Network and Computer Applications.*Volume 66, May 2016, Pp 214-235. doi:https://doi.org/10.1016/j.jnca.2016.03.005

[8] Barenya Bikash Hazarika and Smriti Priya Medhi. "**Survey on Real Time Security Mechanisms in Network Forensics**". *International Journal of Computer Applications (0975 – 8887)* Volume 151 – No.2, October 2016. Pp.1-4

[9] Hariyanto, AndysahPutera Utama Siahaan. "**Intrusion Detection System in Network Forensic Analysis and Investigation** ". *IOSR Journal of Computer Engineering (IOSR-JCE),* Volume 18, Issue 6, Ver. IV (Nov.-Dec. 2016), Pp. 115-121 . doi:10.9790/0661-180604115121

[10] Joseph MbuguaChahira, Jane KinanuKiruki, Peter KipronoKemei. "**A Proactive Approach in Network Forensic Investigation Process**". *International Journal of Computer Applications Technology and Research.* Volume 5– Issue 5, Pp.304 - 311, 2016, ISSN:- 2319–8656

[11] Vivens Ndatinya, Zhifeng Xiao Vasudeva Rao Manepalli, Ke Meng and Yang Xiao. " **Network forensics analysis using Wireshark**". International Journal of Security and Networks. January 2015 .Pp.92-106 doi:10.1504/IJSN.2015.070421

[12] Abhishek Srivastav and Irman Ali. " **Network Forensics an emerging approach to an network analysis**". *International Journal of Computer Science & Engineering Technology.* Vol. 5 No. 02 Feb 2014.Pp.118-123, ISSN : 2229-3345

[13] ManishKumar, M.Hanumanthappa and T.V.Suresh Kumar. "**TRACKING OF INTRUDERS ON GEOGRAPHICAL MAP USING IDS ALERT**". *International Journal of Advances in Engineering & Technology.* Vol 3.Issue 1. March 2012,Pp.48-54.

[14] Natarajan Meghanathan, Sumanth Reddy Allam and Loretta A. Moore. "**Tools and techniques for Network Forensics**". International Journal of Network Security & Its Applications (IJNSA), Vol .1, No.1,April 2009, Pp.14-25.

[15] Sarandis Mitropoulos, Dimitrios Patsos, Christos Douligeris. "**Network Forensics: Towards a classification of traceback mechanisms**". *International Conference on Security and Privacy for Emerging Areas in Communication Networks,* 2005.doi:10.1109/SECCMW.2005.1588288

[16] Sanjay K S and Ajit Danti. " **Online Fake Review Identification based on Decision Rules**". *International Journal of Advanced Trends in Computer Science and Engineering,* Volume 8, No 2, March-April 2019. pp: 140-143. doi:https://doi.org/10.30534/ijatcse/2019/07822019

[17] Johan Reimon Batmetan et al., "**Information Security Governance in small Cities in Developing Countries**". *International Journal of Advanced Trends in Computer Science and Engineering.* Volume 8 No 1.5, 2019. pp-182-191.doi:https://doi.org/10.30534/ijatcse/2019/3581.5 2019