Defend Against Ransomware Detection Using Intrusion Detection System (IDS)

Fahad Omar Alomary

Information Technology Department, College of Computer and Information Sciences,
Al-Imam Mohammad Ibn Saud Islamic University, Riyadh, Saudi Arabia

Summary

Ransomware is currently one of the most impactful forms of cyber-attacks available. One of the greatest challenges posed by ransom ware is the extremely large number and diversity of ransom ware families, and the fact that new ransom ware variants are being released by cybercriminals on a regular basis. In this paper, studied different ransom ware families, and identified several distinctive characteristics and attributes that could be used in early detection of ransom ware based on network traffic analysis. Intrusion Detection System (IDS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations. Institution network is a complex infrastructure consisting of multiple virtual local area networks "VLANs" separating the different departments, laboratories and facilities according to their functions. Institution Network border consists of a firewall which oversees the ingoing and outgoing traffic and also has a manual monitoring system which logs intrusion attempts. To perform any action against an intrusion the administrator has to perform any action manually. The aim of this paper is to provide an intrusion detection system to be deployed on the Institution Network infrastructure. The IDS will be in the form of an Agent which is located on the network's border acting as the second line of defense behind the firewall, the agent will analyze network traffic by comparing the behavior with a database containing certain measures hence classifying the user.

Key words:

Ransomware, Intrusion Detection System, Intrusion Prevention System, SNORT and WannaCry.

1. Introduction

Systems and networks are subject to electronic attacks. Today's information systems in government and commercial sectors are distributed and highly interconnected via local area and wide area networks. While indispensable, these networks provide potential avenues of attack by hackers, international competitors, and other adversaries [1]. The world has experienced a massive global ransom ware cyber-attack known as "WannaCrypt" or "WannaCry" (Ransom: Win32/WannaCrypt) since Friday, May 12 2017 [2]. Hundreds of thousands computers worldwide have been hit and affected more than 150 countries. WannaCry is far more dangerous than other common ransom ware types because of its ability to spread itself across an organization's network by exploiting a critical vulnerability in Windows computers, which was patched by Microsoft in March 2017. The exploit, known as "Eternal Blue," was released online in April in the latest of a series of leaks by a group known as the Shadow Brokers, who claimed that it had stolen the data from the Equation cyber espionage group [2].

The malware has the capability to scan heavily over Transmission Control Protocol (TCP) port 445 (Server Message Block/SMB), spreading similar to a worm, compromising hosts, encrypting files stored on them then demanding a ransom payment in the form of Bit coin [3]. It is important to note that this is not a threat that simply scans internal ranges to identify where to spread, it is also capable of spreading based on vulnerabilities it finds in other externally facing hosts across the internet.

Intrusion Detection System (IDS) are Hardware and Software Systems that monitor events which occurred on computers and computer networks in order to analyze security problems. IDS have become a key component in ensuring the safety of systems and networks. Intrusions to computer networks are called ''attacks" and these attacks threaten the security of networks by violating privacy, integrity and accessibility mechanisms. Attacks can originate from users who login to the computer using Internet trying to gain administrator rights and other users who misuse the rights they have. IDSs automate monitoring and analyzing the attacks [4].

It might he said a computer system is secure if it is safe from threats, which now a day is feasible only if it lives in an isolation. That is why it is said that a truly secure computer is one that is not plugged into a network or any sort of electricity. In such a case the numbers of exploits are minimized, i.e. existing hidden weaknesses that can hit the system are reduced. But by doing so functionality of the system is severely minimized, which is undesired. It is need of the hour to have computer systems with varying functionalities. Also, these systems should not be placed under isolation, need is to have networked systems connected within a limited domain or sometimes even beyond that. Today, the world is converging into a global village and in the near future, organizations would be even

Manuscript received July 7, 2020
Manuscript revised July 20, 2020

more interconnected, having homogenous or heterogeneous setups. This global scenario leads to an increase in the vulnerabilities to which systems are exposed when connected to the network. Therefore, when there is compelling need to have global reach and maximum clientage, network security becomes utmost concern for the enterprises. The security in computer networks is a rapidly growing area of concern [5]. Most of the valuable information resides on the network, making network an inevitable entity for survival. There is proliferation of the networks in daily lives, he is an academic or business environment.

Network security issues have been a major challenge on Institution network for a long time. University networks are protected from malicious hackers using firewall. However, firewall does not have the ability to detect hostile intent or identify types of attack on allowed services. All the University Servers are on DMZ (demilitarize Zone) network and all their services are hosted on to these servers. These services are being public to everyone connected to the Internet. Therefore, these servers can anytime be compromise by hackers that may lead to the breach of their security. This problem can be tackled by deploying SNORT Intrusion Detection System on the Institution network for effective monitoring of Intrusion activities or policy violations Specially That the Attacks may not be detected instantly if detected at all Network Administrator is not aware of the network status on a constant basis and All network traffic is considered similar and makes it hard to detect intruders.

The aim of this Project is to evaluate the performance of SNORT IDS in safeguarding demilitarize zone (DMZ) network of Institution. The specific objectives are: To deploy SNORT IDS on Institution Demilitarized Zone (DMZ) network, to perform real-time traffic analysis employing SNORT IDS on Institution DMZ network using Detection Rate performance metric, to create a Database to log network intrusions and to classify network traffic on the basis of their threat level and generate reports/alerts.

2. Literature Review

During the 21st Century the world has seen a vast amendment in our surrounds, this amendment isn’t a physical one, rather it’s a silent one which has affected almost every single person. This change is known to all of us as Technology. These days even the simplest daily tasks have been made easier using the aid of smart phones, laptops and the other technologies. With the profligate up rise of technology and the rely on computer networks is increasing day by day. The dependency and use of networks resources is growing and network infrastructures are gaining in size and complexity. This prolific growth and development is accompanied with a curse which is Security Issues.

New threats and vulnerabilities appear every day and computers are far from being unsecure. Considering the vigorous rise of the technologies and approaches used by black hat community or as they are commonly known as “Underworld of the Web” a solution had to be found [5].

SNORT is an open source intrusion prevention system offered by Cisco. It is capable of real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more [6].

SNORT can be used as a packet sniffer like tcpdump, a packet logger (useful for network traffic debugging, etc.), network file logging device (capturing files in real-time from network traffic), or as a full blown network intrusion prevention system. The mission for SNORT is to deliver the most effective and comprehensive real-time network defense solutions on the planet [6].

Ransomeware threats do not typically spread rapidly. Threats like WannaCrypt (also known as WannaCry, WanaCrypt0r, Crypt, or WCRY) usually leverage social engineering or email as primary attack vector, relying on users downloading and executing a malicious payload. However, in this unique case, the Ransomware perpetrators used publicly available exploit code for the patched SMB 'EternalBlue' vulnerability, CVE-2017-0145, which can be triggered by sending a specially crafted packet to a targeted SMBv1 server. This vulnerability was fixed in security bulletin MS17-010, which was released on March 14, 2017.

WannaCrypt spreading mechanism is borrowed from well-known public SMB exploits, which armed this regular Ransomeware with worm-like functionalities, creating an entry vector for machines still unpatched even after the fix had become available.

The exploit code used by WannaCrypt was designed to work only against unpatched Windows 7 and Windows Server 2008 (or earlier OS) systems, so Windows 10 PCs are not affected by this attack.

Gupta and Tripathi [7] created awareness amongst the unskilled computer users on the risks of ransomware things to do to organizations. The authors listed the viable threat posed with the aid of the malware which consists of system shutdown due to infection, records or records loss, economic price and once in a while loss of life. It proposed quite a few mitigating methods and controls amongst its shield expertise which must consist of e mail security, intrusion prevention, down load insight, browser protection, take advantage of safety and adoption of first-rate practice.

Upadhyaya and Jain [8] mentioned the anatomy and nature of the ransomware household that normally blocks the venture manager, instructions immediate and different executable documents and renders the conceivable system unusable. The paper streamlines its focal point on CTB Locker, analyses its mode of assault and how it creates its Bitcoin pockets per sufferer and mode of fee the use of the Tor gateway. Some physicist proposed the layout of quantum cryptography structures that would be devoid of loopholes which seem to be like a mirage, whilst others advise prior safety of digital asset earlier than assault and everyday backup as the great solution. Furthermore,

Gagneja [9] offers more than a few approaches that ransomware exploits machine safety vulnerabilities to unfold infections thru some walking out of date utility on victims' computer. It as a result eliminates the backup documents and directories to stop machine restored and eventually encrypt the device files. It cautioned ordinary education of personnel on machine protection issues, replace of patches, set up of firewall, e-mail scanning and the use of licensed working machine for prevention in opposition to ransomware attack.

Saiyed [10] talked about a new malware known as crypto ransomware and analysed how it works and the way its encrypt records at relaxation the use of public key structures; it endorsed the proper mixture of understanding the fundamentals of CryptoLocker protection measure coupled with prescriptive coaching for primary prevention, detection, mitigation, and restoration controls that are past the everyday IDS/IPS mechanism.

While Richardson and North [11] deliver to endure the records and evolution of the first ransomware virus known as the AIDS Trojan in 1989 (also recognized as PC Cyborg) to the current CryptoLocker family, it additionally touched on the rating of the usa that is most affected (USA–Turkey) and mentioned the discrepancy for or towards the fee of ransom which mostly relies upon on the significance of the documents and the degree of backup. Similarly, Formby et al. [12] directed their research on the emerging trend in high profile attacks on hospitals by ransomware. It indicated that the perceived absence of threat on the industrial control system (ICS) over a long period of time and lack of regular update of their network systems contributed to the exposure of confidential information to the hackers.

3. Methodology

This section presents an overview of the method, experimental procedure and experimental setup, and performance metrics adopted to deploy and evaluate the performance of SNORT intrusion detection system.

In Detection System (IDS) on demilitarized zone (DMZ) network segment of institution. Two Network traffics will be captured this research paper, a quantitative research method was adopted to evaluate the performance of the SNORT Intrusion, one from the system that initiated the attack from LAN network segment, and another traffic from SNORT-ids system on DMZ network segment. Traffic to be capture on SNORT-ids system will be comparing against suspicious traffic detected by SNORT-Ids System. Detection rate metric will be used to evaluate the performance of SNORT-Ids system to know the rate at which it is able to suspicious traffic.

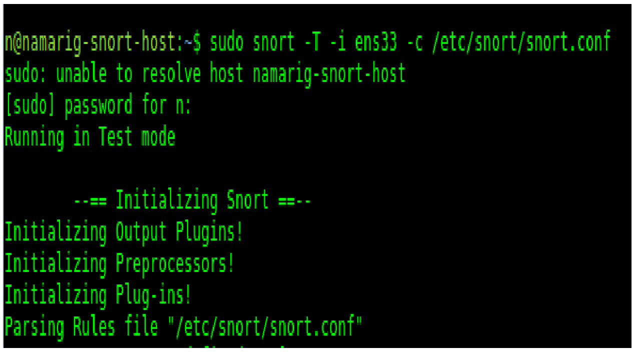
To evaluate the performance of the SNORT Intrusion Detection System (IDS) on demilitarized zone (DMZ) network segment of Institution, A SNORT Server will be configuring and deploy on DMZ network segment. This Server will be connected to the DMZ Switch on interface (ether1), and a Console Monitoring port. The Console monitoring port will be used by network administrator for monitoring Intrusion activities collected by SNORT through web browser.

4. Results and Discussions

4.1 System Implementation

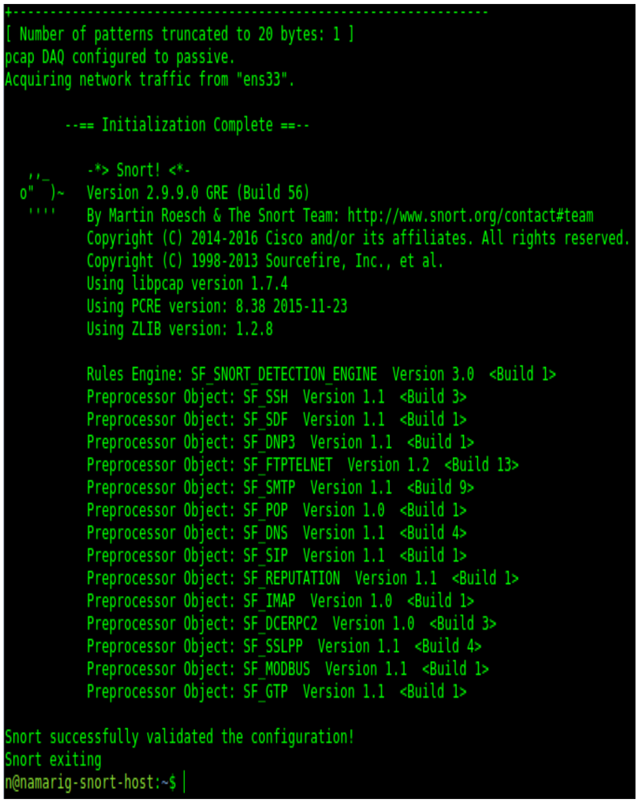
The SNORT IDS was implemented together with various tools such as SNORT Application, Barnyard, Apache, MySQL, PHP, and ADODB to achieve intrusion detection system for analyzing and detecting a malware intrusive attacks.

SNORT application was installed on a server running Ubuntu 16.04 Operating System. SNORT captures attack data through SNORT.conf` file in /etc/SNORT directory. In this file we specified our block of IP address for DMZ network segment and parameters that specified link to our rule files that will be executed whenever there is suspicious traffic on the DMZ network zone. If suspicious traffic is been detected and captures by SNORT.conf file it will be forwarded to SNORT logs file in /var/log/SNORT directory with SNORT.u2 extension. SNORT log file is a directory that keeps track of any suspicious traffic captures by SNORT. SNORT Application installation and configuration procedure are shown in Figure 1 & 2.



```
n@namarig-snort-host:~$ sudo snort -T -i ens33 -c /etc/snort/snort.conf
sudo: unable to resolve host namarig-snort-host
[sudo] password for n:
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
```

Fig. 1 Install SNORT prerequisites.

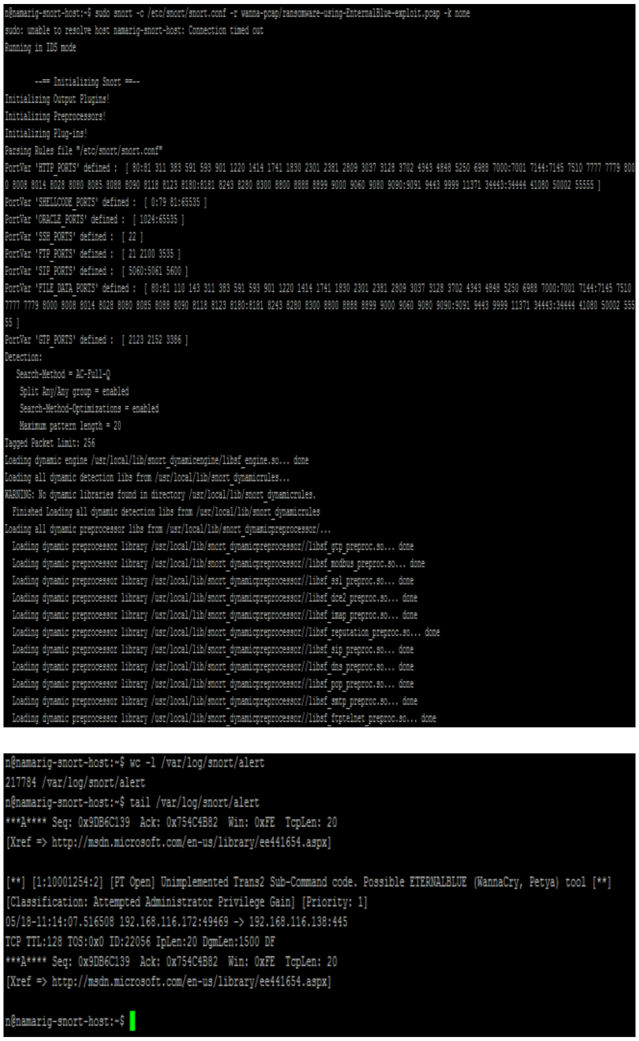


```
+-----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1 ]
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.9.0 GRE (Build 56)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2016 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.7.4
           Using PCRE version: 8.38 2015-11-23
           Using ZLIB version: 1.2.8

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.0  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>

Snort successfully validated the configuration!
Snort exiting
n@namarig-snort-host:~$ |
```

Fig. 2 Install SNORT prerequisites 2.

4.2 System Testing

The following figure shows the malware (wannacray) propagation in the lab environment and how the SNORT alerted these suspicious activities.



```
n@namarig-snort-host:~$ sudo snort -c /etc/snort/snort.conf -r wanna-pcap/ransomware-using-EnternalBlue-exploit.pcap -k none
sudo: unable to resolve host namarig-snort-host: Connection timed out
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 800
0 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510
7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 555
55 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/local/lib/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/local/lib/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/local/lib/snort_dynamicrules.
  Finished Loading all dynamic detection libs from /usr/local/lib/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/local/lib/snort_dynamicpreprocessor/...
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_gtp_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_modbus_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_ssl_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_dce2_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_imap_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_reputation_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_sip_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_dns_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_pop_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_smtp_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_ftptelnet_preproc.so... done
```

```
n@namarig-snort-host:~$ wc -l /var/log/snort/alert
217784 /var/log/snort/alert
n@namarig-snort-host:~$ tail /var/log/snort/alert
***A**** Seq: 0x9DB6C139  Ack: 0x754C4B82  Win: 0xFE  TcpLen: 20
[Xref => http://msdn.microsoft.com/en-us/library/ee441654.aspx]

[**] [1:10001254:2] [PT Open] Unimplemented Trans2 Sub-Command code. Possible ETERNALBLUE (WannaCry, Petya) tool [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
05/18-11:14:07.516508 192.168.116.172:49469 -> 192.168.116.138:445
TCP TTL:128 TOS:0x0 ID:22056 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x9DB6C139  Ack: 0x754C4B82  Win: 0xFE  TcpLen: 20
[Xref => http://msdn.microsoft.com/en-us/library/ee441654.aspx]

n@namarig-snort-host:~$ 
```

Fig. 3 WannaCry propagation.

4.3 System Evaluation

In order to evaluate performance of SNORT-ids, we captured ICMP (Ping) traffic from the initiating System with 172.16.64.238 IP address from LAN network segment for the period of 15 minutes. We initiated ping attempt from System with 172.16.64.238 IP address to the System with 172.16.64.238 IP address on DMZ network segment. This traffic is compared against the ICMP (Ping) traffics captured from SNORT-ids for the period of 15 minutes. ICMP (Ping) traffics captured from SNORT-ids System are compared against suspicious traffics detected by SNORT-ids.ICMP (Ping) traffics from both initiating system and SNORT-ids system were captured through Wire shark. However, ICMP (Ping) Suspicious traffic was detected by SNORT-ids and analyzed using basic analysis and security engine (BASE). These traffics are shown in Table 1 and Figure 4.

Table 1: Summary of ICMP (Ping) Traffic captured on initiating system and traffic captured on SNORT-ids system.

Table 1: ICMP Traffic Ping

Application	Initiating System	SNORT-IDS	% of Total Traffic
ICMP (Ping)	213	213	100%
Total no. of Traffic	213	213	100%

From Table 1, 213 ICMP (Ping)traffic on SNORT-ids system were captured out of 213ICMP (Ping) traffics captured from initiating system for a period of 15 minutes However, ICMP (Ping) traffic captured from SNORT-ids system is 100% of total number of ICMP (Ping) traffic captured from the system that initiate the ping.

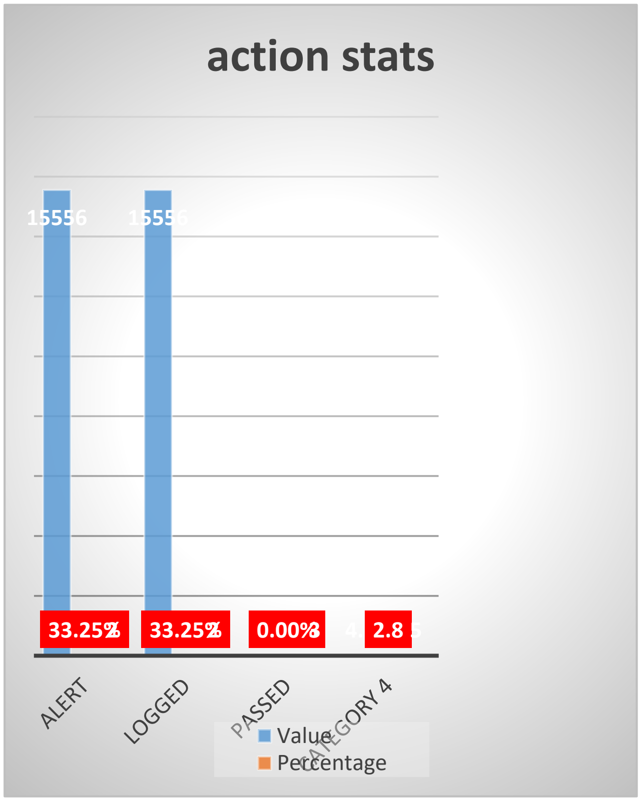


Fig. 4 Result analysis.

5. Conclusion

Using an Intrusion Detection System can optimally increase security of a network or Using this system can provide a mixture of detection and prevention techniques or, alarming system allows the network administrator to be aware of the network intrusions at all times, Reports generated by the system allow efficient and accurate analysis of the security status The GUI provides an easy and attractive platform to assess threats.

The continued researches in the area of compression between classic network and software define network could be made with using other tools to measure this parameter's such trample, apache Meter, apache bench and auto bench

Measuring the other performance parameters such as latency, packet loss. Based on this research, hope to see in the Intuits managing and measuring parameters in other models such as small area or multimedia models or WAN network with different topology.

References

[1] S. Alelyani and H. Kumar, "Overview of cyberattack on saudi organizations," 2018.

[2] P. B. Caliaberah, S. Armoogum, and X. Li, "An Adaptive Security Architecture for Detecting Ransomware Attack Using Open Source Software," in Future of Information and Communication Conference, 2020, pp. 618-633.

[3] A. Zimba and M. Chishimba, "Understanding the Evolution of Ransomware: Paradigm Shifts in Attack Structures," International Journal of Computer Network & Information Security, vol. 11, 2019.

[4] A. Patel, M. Taghavi, K. Bakhtiyari, and J. C. Janior, "An intrusion detection and prevention system in cloud computing: A systematic review," Journal of network and computer applications, vol. 36, pp. 25-41, 2013.

[5] S. Landau, "The real security issues of the iPhone case," Science, vol. 352, pp. 1398-1399, 2016.

[6] W. Bul'ajoul, A. James, and M. Pannu, "Improving network intrusion detection system performance through quality of service configuration and parallel technology," Journal of Computer and System Sciences, vol. 81, pp. 981-999, 2015.

[7] S. Mohurle and M. Patil, "A brief study of wannacry threat: Ransomware attack 2017," International Journal of Advanced Research in Computer Science, vol. 8, 2017.

[8] R. Upadhyaya and A. Jain, "Cyber ethics and cyber-crime: A deep dwelved study into legality, ransomware, underground web and bitcoin wallet," in 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016, pp. 143-148.

[9] K. K. Gagneja, "Knowing the ransomware and building defense against it-specific to healthcare institutes," in 2017 Third International Conference on Mobile and Secure Services (MobiSecServ), 2017, pp. 1-5.

[10] D.-Y. Kao and S.-C. Hsiao, "The dynamic analysis of WannaCry ransomware," in 2018 20th International Conference on Advanced Communication Technology (ICACT), 2018, pp. 159-166.

[11] R. Richardson and M. M. North, "Ransomware: Evolution, mitigation and prevention," International Management Review, vol. 13, p. 10, 2017.

[12] D. Formby, S. Durbha, and R. Beyah, "Out of control: Ransomware for industrial control systems," in RSA conference, 2019.

Fahad Omar Alomary is currently the Executive Director of Center of Cyber Crimes Studies. He is an Assistant Professor in Information Technology Department, College of Computer and Information Sciences at Al-Imam Mohammad Ibn Saud Islamic University, Riyadh, Kingdom of Saudi Arabia (KSA). He holds a Bachelor of Science in Electronics Engineering from College of Technology, Riyadh, Kingdom of Saudi Arabia (2002). Masters of Science in Computer Engineering, and Masters of Science in Engineering Management from Florida Institute of Technology, Melbourne, FL, United State (2008). Doctoral of Science in Computer Engineering in field of Data Networking from Florida Institute of Technology, Melbourne, FL, United State (2013). He has more than 9 years of working experience. Also, he teaches Information Networks, Digital Libraries, and IT Fundamentals, academic advising, and supervising the graduation projects. In addition, he holds some academic positions Chair of IT Department, Chancellor & Director General of Office of Vice Rector, and the Executive Director of Center of Cyber Crimes Studies. His research interests include Computer Networking, Data Management, and Information Security.