 doi:10.20944/preprints202006.0065.v1

Intrusion Detection Systems: A Survey and Taxonomy

Sabah Khaliq
Faculty of Engineering and Informatics
The University of Bradford
Bradford, United Kingdom
skhali16@bradford.ac.uk

***Abstract* — This paper incorporates the definition of Intrusion Detection Systems and the methodologies utilised by these systems. As well as this, this research paper also encompasses a taxonomy and a survey of IDS and the specific strategies and principles. Finally, this paper also includes a discussion amongst other authors for instance what the authors differ and agree on, along with the previously related studies.**

Keywords — Cyber Attacks, Network Security, Network Performance, Network Traffic, Anomaly Detection, Signature Detection

I. INTRODUCTION TO INTRUSION DETECTION SYSTEMS

The act to misuse a system is named 'Intrusion', furthermore due to this, Intrusions often reveal vulnerabilities required to be identified as soon as possible. Intrusion Detection System (IDS) is a security system, in which prevents identified attacks from a computer or a network system. Intrusion Detection Systems has increasingly enhanced with identifying malicious attacks, viruses or activities aimed at a computer or network systems [3]. A diverse number of IDS' can often offer functionalities as well as support. As well as this, IDS' also analyse a network or computer system, in order to discover intrusions or attacks and therefore activate signature or anomaly-based detections systems. Other forms of IDS are also known as network-based and host-based Intrusion Detection Systems.

The aim of Intrusion Detection Systems is to examine and analyse the incoming as well as outgoing network traffic, regarding to the unreliable data activity or possible cyber-attacks; in which can develop from internally or externally of the business or companies network system [5]. Additionally, due to this Intrusion Detection Systems can therefore arise these issues when such activities occur and then inform the user.

A. *Intrusion Detection System Methods and approaches*

There are four main detections methodologies, in which IDS' can prevent hostile attacks. These methodologies are: anomaly detection, signature detection, specification based detection and hybrid detection.

1. *Anomaly based detection*

Anomaly based detection, detects any uncertain algorithm or unreliable data in the computer system or network system. If there is a sudden change within the data, this will then be recognised as an attack from an anomaly-based detection. Anomaly based detection then compares the up to date traffic as oppose to the profile in which is currently produced [8]. Anomaly based detection, also observes the behaviour of a network system and then logs the behaviour; in order to prevent any irregularities or cyber-attacks on the system.

However, this methodology attack rarely detects secret attacks, this is over the reason that anomaly-based detection often hides in huge numerical figures of occurrences which are regarded as 'normal behaviour'**.** Going into further insight as stated previously, if any error occurs before or during the process in an anomaly-based detection this will also increase the alarm rate as well as reducing the enhancement of the detection [4].

2. *Signature based detection*

Signature based detection systems, also referred to as a misuse detection; focuses on the network traffic and therefore attempts to catch any sequences or patterns of an inbound network traffic [7]. However, these sequences or patterns must match an attack signature.

Signatures based detection systems can be exposed by network packets, IP addresses, destination or network packet headers etc. If any of these matches to a known virus, malware detection or any other malicious patterns, the system will then identify and suggest this is an attack. However, any faulty error in this specific detection model will result into an additional false alarm rate and therefore decrease the efficiency of the detection methodology.

3. *Specification Based Detection*

Specification based detection is utilised with a system execution in order to confirm the requirement behaviour. As a substitute instead of learning the systems'

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 June 2020 doi:10.20944/preprints202006.0065.v1

behaviours, the developers as well as professionals' knowledge affects the operating limits on the system; regarding this methodology. Specification based detection focal point is to specific behaviours based upon the least privileged principle.

4. *Hybrid Detection*

A hybrid-based detection consists of a mixture of a signature-based detection and an anomaly-based detection; this detection method is utilised to detect any attack from any network connection event. Additionally, due to this a hybrid-based system offers efficient detection abilities and includes a neural network detection element with a simple pattern matching engine in order to recognise irregularities in a network traffic [9].

Further due to this, this methodology quickly identifies known categories of attacks as well as the unknown attacks. Therefore, since both detection-based systems process simultaneously, one can offer a method to filter a group and can also decrease the security alert.

B. *The benefits and drawback of IDS'*

One of the main benefits is that IDS' detects in real time and maintains fast reactions. Network-based IDS' observe any alteration that may occur in the system. However, this depends on how the system is installed; some attacks can be prevented before gaining access to the host or the system.

Another benefit is IDS' provides ease to the user or company by maintaining regulations. IDS' distributes users with more of a modified view throughout the computer system. Furthermore, due to this, Intrusion Detection System are simpler to meet security rules and regulation.

However, the drawbacks of IDS' is that this system must require an experienced engineer. Intrusion Detection Systems significantly relies on an experienced engineer, in order to manage the information, that the system provides [11]. An engineer holds the responsibility of securing an IDS against any threats, this is because the detection tool provided does not have the ability to prevent, block or to find a solution to difficulties, when an issue arises.

1. *Network Attacks*

The categorisation of attacks has been classified into a few classifications, in which provide more details as listed below:

Virus: A virus is a malicious code that is a self-replicating program. This spreads through a network and additionally affects the system without informing the user.

Worm: A worm is a self-replicating program, which spreads through a network without informing the user. However, the difference between a worm and a virus is that a virus relies on a host program with the intention to spread; a worm is an independent software that does not require a host program, in comparison to a virus.

Password-based attack: A password-based attack is a continuous attempt, which are created to replicate an up to date login or password algorithm. A few examples of password-based attacks are Brute Force Attacks, Phishing, Password Spraying, Keylogger Attacks and Credential stuffing.

Physical attack: A physical attack is also known as a 'kinetic' attack this attack is to expose or destroy a computer or networks physical components.

Trojan: A Trojan or a Trojan Horse is a malware attack that is designed to deceive a user of its true colours [14]. In comparison to other attacks, a Trojan does not propagate itself to other files.

Information gathering attack: This attack includes finding vulnerable information or data on a user's network or computer system [16]. This attack gathers significant information by scanning or examining a user's existing computer network.

Network attack: A network attack manipulates a network protocol, or any method utilised to spitefully attempt to bargain a network security. This can range from the data link layer to the application layer.

I. THE ARCHITECTURE OF INTRUSION DETECTION SYSTEM

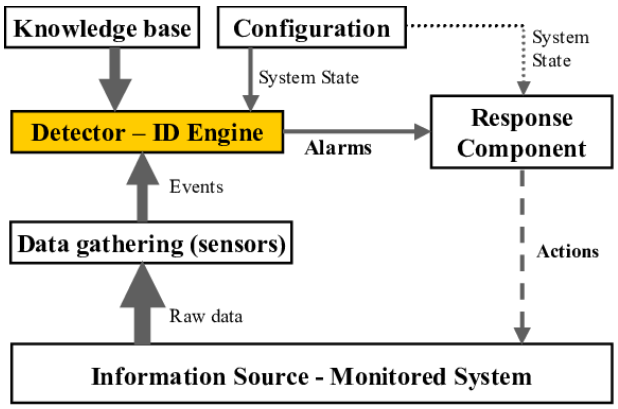

Figure 1: Displays the architecture framework of a common Intrusion Detection System. [17]

Even though these systems are very different in the techniques each system implements, these systems also gather and analyses information [19]. Majority of these systems depend on the common architecture infrastructure (as shown in figure 1). The following fundamental components in the architecture are as described below: -

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 June 2020 doi:10.20944/preprints202006.0065.v1

- Data gathering is accountable for gathering information from network and checked systems
- Detector ID engine develops the information collected from sensors, in order to identify malicious intrusion events.
- Knowledge base includes information gathered by the sensors; this is completed by a 'pre-processed' format filtered data, data profiles etc. This data is often delivered by a security expert or network expert.
- Configuration device gives data regarding the latest state of Intrusion Detection Systems.
- Response component begins when an attack is discovered [21]. These responses can either be automated also known as active or can include a human interaction also named as inactive.

Data source	IDS Type	Type of Response	Architecture	Example of tools
Network Based Intrusion Detection System	Network based	Passive	Distributed	• Bro • SNORT • IBM QRader
Host Based Intrusion Detection System	Host based	Passive and active	Distributed	• SolarWinds Security Manager • OSSEC
Virtual Machine Based IDS'	Host Based	Passive and active	Distributed	• VMware NSX™
Wireless Network IDS'	Network based	Passive and active	Distributed	• OpenWIPS-NG

Table 1: Illustrates the classification of the various forms of IDS' with the accordance of the type of attack and the type of response based on intrusion methods.

II. TAXONOMY OF INTRUSION DETECTION SYSTEM

The table above, classifies the four main type of Intrusion Detection Systems; Network Based Intrusion Detection System analyses network traffic, in order to protect a, computer or network system against any potential threats, this is done by gaining valuable data from the network system and checks every network packet that is active in the system.

C. Network Based Intrusion Detection Systems'

Network based Intrusion Detection Systems can be altered and allows the user the accessibility to customise the network sensors in order to meet the users' own requirements [24]. Additionally, this network-based intrusion detection system, also has a rapid response; in comparison to the Host Based Intrusion Detection System. The implementations on a Network Based System are much comprehensive, easier and less complexed to implement. On the contrary, Network Based Intrusion Systems, include many drawbacks. The first issue is that the Network Based IDS 'must examine every network packet. Furthermore, this particular IDS have difficulties in obtaining high speeds of network data [6].

D. Host Based Intrusion Detection Systems'

Host Based Intrusion Detection System monitors a single system, which is required to be installed, in order to detect any threats. This is completed by analysing the attributes of a host or computer system and the events, in case of a sudden change in the data.

The main benefit of a Host Based Intrusion Detection System is that the system utilises a system log in. This includes the events in which has arisen and can affect whether a threat has befallen or not along with better precision; in comparison to the Network Based Intrusion Detection System. However, the drawbacks of Host Based IDS' are the number of hosts, in which must be implemented in order to prevent any potential threats to the network system.

Host-based Intrusion Detection Systems currently can only protect one host-based system at a time [26]. Therefore, if an organisations system has more than one host and utilises a different operating system this will be more complexed for a host-based intrusion detection system to defend for a single host.

E. Virtual Machine Based Intrusion Detection System

Virtual Machine Based Intrusion Detection Systems utilises a virtual machine to enhance the network security against any potential threats. The main use of Virtual Machine Based Intrusion Detection System is that the VM based application provides a blockade between the IDS and the fraudulent hackers pursuits. The main advantage of this system is the ability to analyse the machine states. The system is additionally more complex for the hacker to attempt to attack the network system [28]. Another benefit is that the Virtual Machine Intrusion Detection System is flexible and is highly efficient, in comparison to other Intrusion Detection Systems.

However, the software implemented and running on this IDS cannot be accessed or altered and therefore will require updating constantly, this issue will make this more time consuming for users and organisations.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 June 2020 doi:10.20944/preprints202006.0065.v1

Name of system	Publ. year	Time of Detection	Granularity	Audit source	Type of response	Data processing	Data collection	Security	Inter-oper.
Haystack	1988	Non-real	Batch	Host	Passive	Centralised	Centralised	Low	low
MIDAS (SSHW88)	1988	Real	Continuous	Host	passive	Centralised	Centralised	Low	Low
IDES(LJL+88)	1988	Real	Continuous	Host	Passive	Centralised	Distributed	Low	low
W&S [VL89]	1989	Real	Continuous	Host	Passive	Centralised	Centralised	Low	Low
COMP-WATCH[DR90]	1990	Non-real	Batch	Host	passive	Centralised	Centralised	Low	Low
NSM[HDL+90]	1990	Real	Continuous	Network	Passive	Centralised	Centralised	Low	Low
NADIR[JDS91]	1991	Non-real	Continuous	Host	Passive	Centralised	Distributed	low	Low
HYPERVIEW[DBS92]	1992	Real	Continuous	Host	Passive	Centralised	Centralised	Low	Low
DIDS[SSTG92]	1992	Real	Continuous	Both	Passive	Distributed	Distributed	Low	Low
ASAX[HCMM92]	1992	Real	Continuous	Host	Passive	Centralised	Centralised	Low	Higher
USTAT[I1G93]	1993	real	Continuous	Host	Passive	Centralised	Centralised	Low	Low
DPEM[KFL94]	1994	Real	Batch	Host	Passive	Distributed	Distributed	Low	Low
IDIOT[KS94b]	1994	Real	Continuous	Host	Passive	Centralised	Centralised	Low	Higher
NIDES [AFV95]	1995	Real	Continuous	Host	Passive	Centralised	Distributed	Low	Higher
GRIDS [fCCCf+96]	1996	Non-real	Batch	Both	Passive	Distributed	Distributed	Low	Low
CSM[WP96]	1996	Real	Continuous	Host	active	Distributed	Distributed	Low	Low
JANUS[GWTB96]	1996	Real	Continuous	Host	Active	Centralised	Centralised	Low	Low
JiNao [JGS+97]	1997	Real	Batch	Host	Passive	Distributed	Distributed	Low	Low
EMERALD[PN97]	1997	Real	Continuous	Both	Active	Distributed	Distributed	Moderate	High
Bro [Pax88]	1998	Real	Continuous	Network	passive	Centralised	Centralised	Higher	Low

Table 2: Classification of the surveyed systems, according to system characteristics [1]

F. Wireless Network Intrusion Detection Systems'

Wireless Intrusion Detection Systems also referred to as WIDS is the prevention of any unlawful malicious network from other wireless devices. WIDS are frequently applied as an overlay to a current wireless Local Area Network (LAN) structure; even though these specific systems can be implemented alone and require no wireless policies within a business [28].

II. A SURVEY OF INTRUSION DETECTION SYSTEMS

In the survey as shown in figure two, Axelsson clearly demonstrates the diverse systems, in which is utilised; and also exemplifies which system has been used by the year, when the time of detection was, the granularity, audit source, the type of response, the data processing and collection as well as, if the security and inter-operations was high, low or moderate on each system.

This survey also compares the different systems to one another and shows the benefits as well as disadvantage of each system. The information below also describes a few of these surveyed systems:

Haystack: The system Haystack is one of the many Intrusion Detection Systems which was initially designed for multiuser Air Force computer systems. This specific system monitors on anomalous activities and examines a user's activities in opposition to predefined security restraints [19].

NADIR: The system NADIR also known as Network Anomaly Detection and Intrusion Reporter is an automated network system, in which identifies network attacks. NADIR focuses on attacks on a network that connects several systems; this system examines the network events though the audit records [6].

EMERALD: The system EMERALD also known as Event Monitoring Enabling Responses to Anomalous Live Disturbances focuses on external and internal attacks. This system uses a signature and statistical analysis asset with a solution that interprets the results [12].

BRO: BRO now known as Zeek is an open source network analysis infrastructure, which focuses on network security and offers a broad platform for other traffic analysis [31].

DIDS: DIDS also known as Distributed Intrusion Detection System: monitors multiple hosts at a time. This systems architecture merges distributed monitoring and data reduction. However, in comparison to other security systems such as Zeek or EMERALD the security is relatively low as well as the inter operations [21].

III. Discussion and Previously Related Studies

Regarding the previously related studies, a few authors such as Stefan Axelsson, Herve Debar, Stephan and Abhijit Sarmah etc, all discuss about one common topic, this is IDS'. Majority of these scholars have all agreed on some key points regarding the Intrusion Detection Systems and hold their own opinions.

Stefan Axelsson as well as Herve Debar both mention that one of the main fundamental issues, in which should be improved on, is the lack of research, in this specific field. Axelsson clearly states that majority of the references in which are utilised do not explain or describe the decision, in which are being illustrated [30]. However, the framework in which the rules can be set out are being demonstrated, as an alternative. Axelsson also discusses, the fact that there is a lack of support on up to date or previous surveys; this is over the reason that majority of the surveys have not been well researched or studied enough, in the case to a more systematic or classified approach.

Another scholar, Abhijit Sarmah, also states that Intrusion Detection Systems are becoming more of a future requirement for many businesses as well as companies. Subsequently installing the firewall technology at the network perimeter. Network perimeter IDS' can therefore provide protection from external and internal hackers, in which traffic does not go past the firewall, under any circumstances provided. Sarmah as well as other authors mention that there must be human intervention. As stated, before in this paper, technology has not yet come to the ultimate peak stage, in which machines as well as technology can independently run tasks by themselves without the requirement of interacting with an individual.

IV. Conclusion

In conclusion, this paper includes the strengths and weaknesses, the analysis and a discussion about the diverse methods of IDS'; along with the main forms of IDS'. This paper also scrutinizes the similarities and differentiations of other authors statements.

In another segment of this paper, this paper includes a description, taxonomy and survey of Intrusion Detection Systems. This paper additionally includes the introduction of IDS' and the specific principles and strategies of IDS.

V. References

[1] Axelsson, S. (2000). Intrusion Detection System: A Survey and Taxonomy. [online] Citeseerx.ist.psu.edu. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.83.3043&rep=rep1&type=pdf [Accessed 9 Nov. 2019].

[2] Dorsz, P. (2004). Intrusion Detection System (IDS) Part 2 - Classification; methods; techniques. [online] TechGenix. Available at: http://techgenix.com/ids-part2-classification-methods-techniques/[Accessed 9 Nov. 2019].

[3] I. Ghafir, V. Prenosil, M. Hammoudeh, F. J. Aparicio-Navarro, K. Rabie and A. Jabban, "Disguised Executable Files in Spear-Phishing Emails: Detecting the Point of Entry in Advanced Persistent Threat." International Conference on Future Networks and Distributed Systems. Amman, Jordan, 2018.

[4] Ghorbani, A., Lu, W. and Tavallaee, M. (2010). Network Intrusion Detection and Prevention. Boston, MA: Springer US [Accessed 5 Dec 2019]

[5] I. Ghafir, V. Prenosil, M. Hammoudeh and U. Raza, "Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[6] Hochburg, J. (1993). NADIR: An automated system for detecting network intrusion and misuse. [online] ScienceDirect. Available at: https://www.sciencedirect.com/science/article/pi 016740489390110Q [Accessed 11 Dec. 2019].

[7] U. Raza, J. Lomax, I. Ghafir, R. Kharel and B. Whiteside, "An IoT and Business Processes Based Approach for the Monitoring and Control of High Value-Added Manufacturing Processes," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[8] Kaur, T. and Kaur, S. (n.d.). Comparative Analysis of Anomaly Based and Signature Based Intrusion Detection System Using PHAD and Snort. [online] Pdfs.semanticscholar.org. Available at: https://pdfs.semanticscholar.org/1d20/35d0cb56018d84ced89b5d235b538ae85420.pdf [Accessed 9 Nov. 2019].

[9] I. Ghafir and V. Prenosil, "Malicious File Hash Detection and Drive-by Download Attacks," International Conference on Computer and Communication Technologies, series Advances in Intelligent Systems and Computing. Hyderabad: Springer, vol. 379, pp. 661-669, 2016.

[10] Kumar, S. (1994). An Application of Pattern Matching in Intrusion Detection. [online] Pdfs.semanticscholar.org. Available at: https://pdfs.semanticscholar.org/73a0/a5c728fcce0aa511f14c580a7781657c7bbd.pdf [Accessed 9 Nov. 2019].

[11] I. Ghafir, V. Prenosil, and M. Hammoudeh, "Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution." International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 7(2), pp. 27-31, 2017.

[12] Leckie, T. (n.d.). The Emerald IDS. [online] Cs.fsu.edu. Available at: http://www.cs.fsu.edu/~yasinsac/group/slides/leckie.pdf [Accessed 11 Dec. 2019].

[13] Liu, Z. (2003). Intrusion Detection System. [online] Pdfs.semanticscholar.org. Available at: https://pdfs.semanticscholar.org/b3ab/f924b92e337bc6f9cd7e67bb4254cb89735f.pdf [Accessed 9 Nov. 2019].

[14] I. Ghafir and V. Prenosil. "Proposed Approach for Targeted Attacks Detection," Advanced Computer and Communication Engineering Technology, Lecture Notes in Electrical Engineering. Phuket: Springer International Publishing, vol. 362, pp. 73-80, 9, 2016.

[15] Lunt, T. (1993). A Survey of Intrusion Detection System. [online] Mathcs.richmond.edu. Available at: http://www.mathcs.richmond.edu/~dszajda/classes/cs334/papers/lunt.pdf [Accessed 9 Nov. 2019].

[16] I. Ghafir, V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid and S. Jaf, "BotDet: A System for Real Time Botnet Command and Control Traffic Detection," IEEE Access (IF=4.098), vol. 6, pp. 1-12, 2018.

 doi:10.20944/preprints202006.0065.v1

[17] Sarmah, A. (2001). Intrusion Detection System: Definition, Need and Challenges. [online] Sans.org. Available at: https://www.sans.org/reading-room/whitepapers/detection/paper/343 [Accessed 9 Nov. 2019].

[18] I. Ghafir, J. Svoboda, V. Prenosil, "A Survey on Botnet Command and Control Traffic Detection," International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 75-80, 2015.

[19] Smaha, S. (1988). Haystack: An intrusion Detection System. [online] People.scs.carleton.ca. Available at: http://people.scs.carleton.ca/~soma/id/readings/smaha-haystack.pdf [Accessed 11 Dec. 2019].

[20] I. Ghafir and V. Prenosil, "Advanced Persistent Threat and Spear Phishing Emails." International Conference Distance Learning, Simulation and Communication. Brno, Czech Republic, pp. 34-41, 2015.

[21] Snapp, S. (n.d.). DIDS (Distributed Intrusion Detection System) − Motivation, Architecture, and An Early Prototype. [online] Seclab.cs.ucdavis.edu. Available at: http://seclab.cs.ucdavis.edu/papers/DIDS.ncsc91.pdf [Accessed 10 Dec. 2019].

[22] Stakhanova, N., Basu, S. and Wong, J. (2006). A Taxonomy of Intrusion Response Systems. [online] Lib.dr.iastate.edu. Available at: https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1193&context=cs_techreports [Accessed 9 Nov. 2019].

[23] J. Svoboda, I. Ghafir, V. Prenosil, "Network Monitoring Approaches: An Overview," International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 88-93, 2015.

[24] Teodoroa, P., Verdejoa, J. and Fernandeza, G. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. [online] Dtstc.ugr.es. Available at: http://dtstc.ugr.es/~jedv/descargas/2009_CoSe09-Anomaly-based-network-intrusion-detection-Techniques,-systems-and-challenges.pdf[Accessed 9 Nov. 2019].

[25] I. Ghafir, M. Husak and V. Prenosil, "A Survey on Intrusion Detection and Prevention Systems," IEEE/UREL conference, Zvule, Czech Republic, pp. 10-14, 2014.

[26] Zhao, F., Yang, W., Jin, H. and Wu, S. (n.d.). VNIDS: A virtual machine-based network intrusion detection system - IEEE Conference Publication. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/4688384 [Accessed 9 Nov. 2019].

[27] I. Ghafir and V. Prenosil, "DNS query failure and algorithmically generated domain-flux detection," International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-5, 2014.

[28] En.wikipedia.org. (2019). Wireless intrusion prevention system. [online] Available at: https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system [Accessed 5 Dec. 2019].

[29] I. Ghafir, J. Svoboda and V. Prenosil, "Tor-based malware and Tor connection detection," International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-6, 2014.

[30] Kumar, V. (2019). Basic architecture of intrusion detection system (IDS). [online] ResearchGate. Available at: https://www.researchgate.net/publication/333705961_A_Survey_of_Network-based_Intrusion_Detection_Data_Sets [Accessed 5 Dec. 2019].

[31] Zeek.org. (2019). Why choose Zeek? [online] Available at: https://www.zeek.org/why_choose_zeek.pdf [Accessed 11 Dec. 2019]