Utilizing Machine Learning Algorithms to Detect Zero Day attack in Network Traffic

Project 1

By Sophia Virgo, Jasmine Roberts, and Morgan Smith

Bowie State University

CTEC 402-001 Software & Operating Systems Security

Dr. Haydar Teymourlouei

February 21st, 2023

Table of Contents

[Introduction](#_4d34og8) 3

[Problem Statement](#_99b2gw1b9utc) 3

[Research Questions](#_2evnkhot6kf5) 3

[Purpose of Research](#_2s8eyo1) 4

[Case Study](#_vabg69re7h1m) 4

[Methodologies](#_nr20myshxjyv) 5

[Method 1: Statistical Method](#_jffwxr3n1ybb) 5

[Method 2: Signature-Based Detection](#_biou5pq512a2) 9

Method 3[:](#_b8ozth48c8hf) Large-Scale Intrusion Detection 11

[Method 4: Anomaly-Based Detection](#_9ejmke4szql1) 11

[Method 5: Nessus](#_cejw1iws0fxv) 12

[Method 6:](#_c0adj7qgnm71) Kismet 14

[Method 7:](#_i4b9fujvwgbu) Fog Computing

Method 8: Wireshark 16

[Summary](#_gjqrx5d0tcbj) 21

[References](#_sikiz12tji87) 22

# Introduction

Zero Day Attacks inside of Network Traffic are very prominent in this century as technology advances each year and becomes more vulnerable. Zero Day Attacks within the Network traffic consist of plotting vulnerabilities on any type of software and include damaging leverage that will put networks, and business organizations at risk which will include their data and private business credentials to become vulnerable. For instance, if you work at an enterprise that handles money, the enterprise will be naturally vulnerable because people with malicious intent are drawn to money. In an attack affiliated with Zero Day within Network Traffic, thousands of dollars will be put at risk of being wired tampered with and stolen. As we rely on technology as the way of life and conducting business, people aren’t aware that there are free open-source methods, software, and tools that can be installed on our PCs that can help detect Zero Day Attacks inside of their Network Traffic.

In our research project, we are going to provide information and display credible methods, software, and tools to help detect Zero Day Attacks inside the Network Traffic. These methods, software, and tools are a way of mentoring your Network Traffic. We are going to display easily read instructional steps and screenshots to demonstrate how to use and the benefits of the methods that we conducted. These methods will be descriptive enough to where they can be easily accessible for use at any convenience. Throughout our research project everything that is included is carefully documented, credible, and worth the access.

## Problem Statement

As technology advances, no matter what device you decide to use (PCs, Phones, Health Care Devices, Cars, etc.), we are put more at risk for vulnerabilities that consist of malicious intent inside of our Network Traffic. Technology in this day in time consists of advanced designs and more intermediate development to handle your daily tasks, which can be more attractive to users with malicious intent to cause vulnerabilities. For example, the Tesla Car Company recently recalled a Third-Party software that exposed many Tesla vehicles to remote access and security bugs within the self-drive option. To prevent many security bugs, and malicious remote access, it would be best to access software that can detect such, bad intent to remote access. Enterprise businesses such as Tesla, have plenty of vulnerabilities, to think they are an Enterprise business they would enlist the top security prevention but it's clear that they do not. (Whittaker, 2022)

# Research Questions

1. What necessarily are zero-day attacks?
2. What are the most effective ways to detect zero-day attacks?
3. How harmful can zero-day attacks be to an organization's data?
4. What should be completed routinely to prevent zero-day attacks?
5. What types of organizations are most susceptible to zero-day attacks?
6. What information can be made to the public to raise awareness about zero-day attacks?
7. What security protocols should be enforced/ taught to protect an organization's data?
8. How have new technological innovations advanced security and awareness about zero-day attacks?
9. How effective is the Statistical Method in detecting zero-day attacks using mathematical equations?
10. What is the least effective method for detecting zero-day attacks?

# 

# 

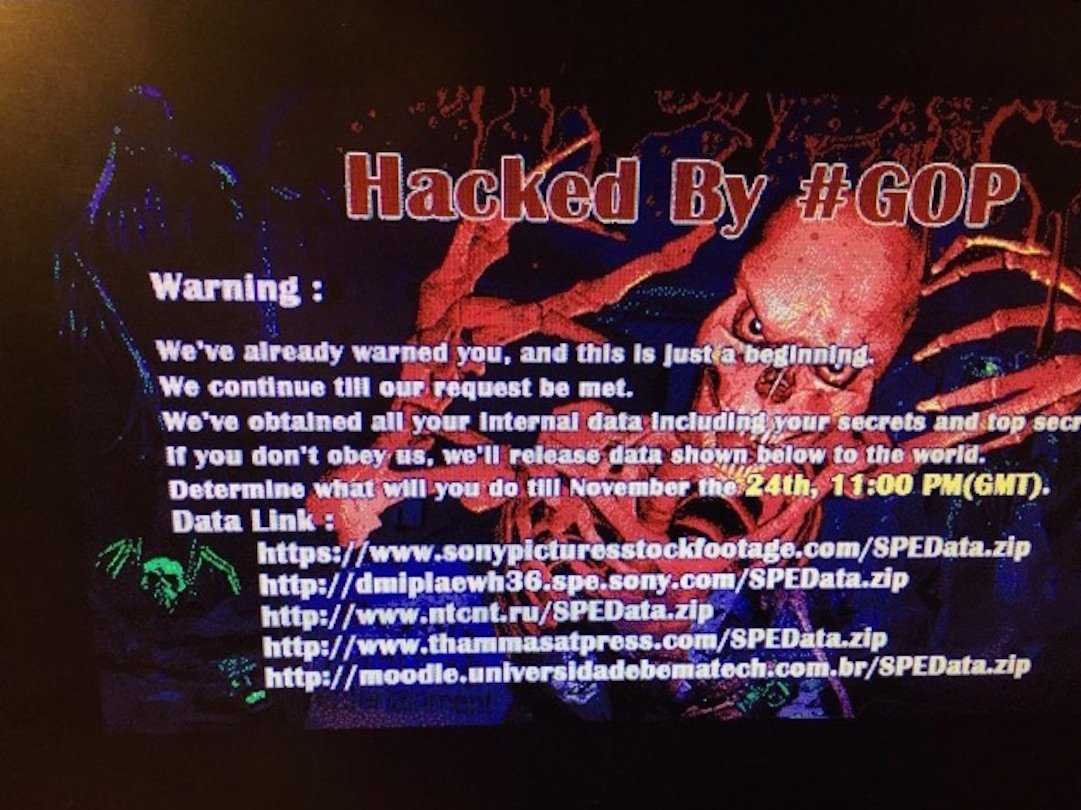
## Purpose of Research

The research purpose of our study is that we are going to supply eight different articles and open-source free methods to help detect Zero Day Attacks within Network Traffic and Vulnerabilities. These attacks and vulnerabilities cause lethal damage to people and the device within itself, but users lack the knowledge of attack prevention, maybe because they don’t feel it’s needed, or they believe they would never be the one that will be attacked initially. Anyone with a device, any device, is not safe from malicious intent without the proper detection or security to monitor your network and path. Our goal is to bring knowledge and awareness that there is open-source free detection and prevent vulnerabilities over the internet developed by top cybersecurity companies. Users aren’t influenced by open-source free methods until they are attacked, it takes for people to be attacked for them to take detection and vulnerability prevention seriously. As we know Zero Day Attacks are very prominent among personal users, Enterprise Businesses, etc., and we need more users to be aware of accessible software that is given to them.

## Case Study

The zero-day attack that will be discussed in this paper is the 2014 Sony hack. This attack took place in November 2014. The attackers called themselves the Guardians of Peace. It had been rumored that the attackers were collaborating with North Korea in some capacity. The attackers managed to commandeer Sony’s network to steal large amounts of information. The information, which included different correspondences Sony’s employees sent to each other was then leaked to different journalists. We have reason to believe that the “Guardians of Peace” collaborated with North Korea because after the information was given to different journalists, one of the hackers communicated through the “Pastebin” website that they were prepared to commit different acts of terrorism against movie theaters. This targeted act was due to the release of the movie “The Interview” which presented a mocked version of Kim Jong Un. Sony responded by canceling the release of the movie.

So, what exactly did the hackers do? The hackers attacked Sony’s corporate network and had taken terabytes of sensitive data, deleted the original documents from all Sony computers, and lastly left threatening messages to release more information if the hacker's demands were not met. You would think that the Sony company would have tighter security protocols to be able to defend itself against zero-day attacks, however, that is the whole idea of these attacks, they are very sudden and almost impossible to prevent once begun. This specific attack happened in 2014 and to this day Sony still does not know the identities of the hackers, working with North Korea. Once the zero-day attack had commenced, Sony’s network had been down for days. Sony’s employees were forced to work on whiteboards. Shortly after the attack, more leaks began to be released. The hackers posted waves of files taken from Sony's computers over the course of several weeks. Four of the five Sony movies that were uploaded by the hackers were still in development. Thousands of private documents were also leaked, including salary and performance information about Sony employees. Below you will find a figure attached of what the Sony employees saw on their screens on Monday, November 24th, 2014. (The 2014 Sony Hacks, Explained, 2015)



*Figure 1: A visual showing a message that appeared on the employee's screens during the zero-day attack with Sony.* (The 2014 Sony Hacks, Explained, 2015)

# 

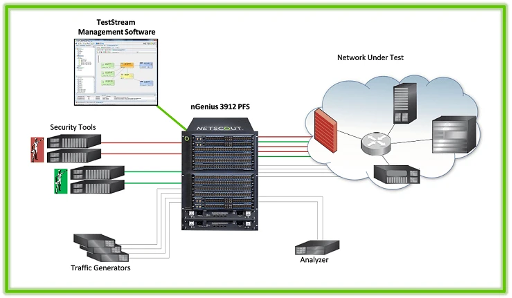
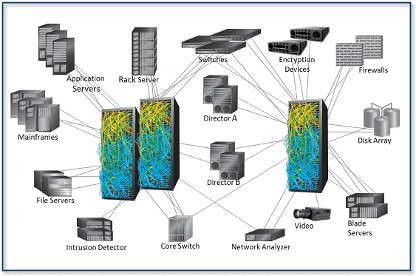
# Methodologies

## Method 1: Statistical Method

Statistical Methods in the Risk-Based Monitoring Article consist of a method called Statistical and its benefits. Usually, statistical methods can be used to detect similarities in the data which can alert users to focus their time based on their findings. It can improve data integrity across devices of users. Typically, a user has multiple devices so they cannot monitor each at once, statistically. There are seven types of Statistical Methods, which are Laboratory Data, Outliers, Univariate, Multivariate, Euclidean, Mahalanobis, Analysis, and Inliers. Each of the seven can handle monitoring for you in their own different way.

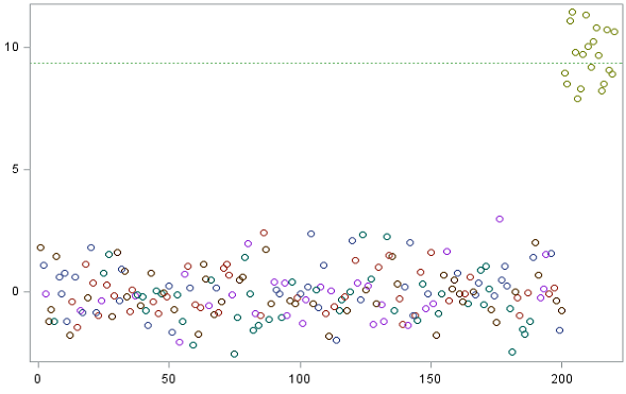
The goal of these statistical math methods is to analyze your data within different math equations, to improve your data so you won’t get any vulnerabilities/breaches, Zero-day attacks within your network, etc. These methods can be used to detect fraud, dangers to your network, attacks, and errors. These methods can also improve data integrity to supply secure and safe data inside your network. They contain mostly visual readings such as bar graphs, line graphs, and math equations. (Statistical Methods in Risk-Based Monitoring, 2018) The seven types of Statistical methods are illustrated below.

***Type 1: Laboratory Data***



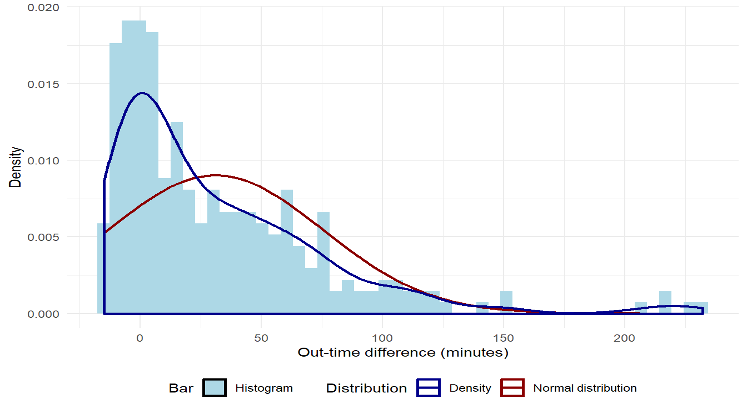
*Figure 2: Consumes multiple items of test equipment to run tests on each appliance. Includes Security tools, Encryption Devices, and Traffic Generators to monitor your Network Traffic inside of a lab.* (Test Lab Automation Solutions for Cyber & Security Test Labs, n.d.)

***Type 2: Outliers***



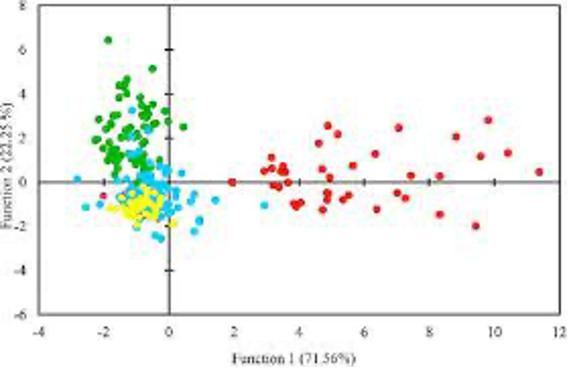
*Figure 3: a graph that consumes numerical scores of your network activity, the score is the result of a particular user database or device. It looks for univariate and multivariate outliers within your device/database.*

***Type 3: Univariate***



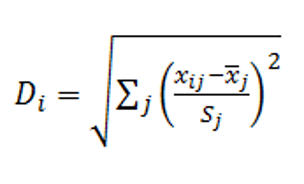
*Figure 4: a bar chart that is showing the results of one variable and its data. The Univariate methods only mentor one variable.* (Achyuthuni, 2019)

***Type 4: Multivariate***



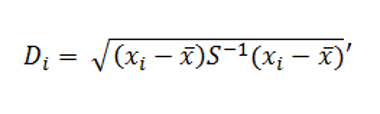
*Figure 5: when more than two variables are to be analyzed, within the system.* (Rai, 2022)

***Type 5: Euclidean***

******

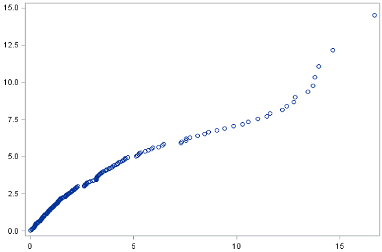
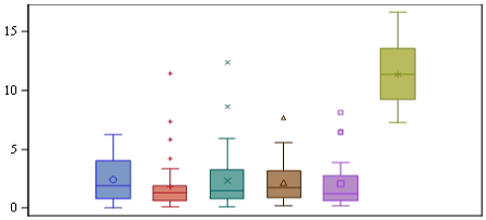
*Figure 6: (ED), Di, from the mean, for each individual, I, can be calculated using the mean, x̄j, and SD, Sj at each site, j* (Statistical Methods in Risk Based Monitoring, 2018)

***Type 6: Mahalanobis***

**

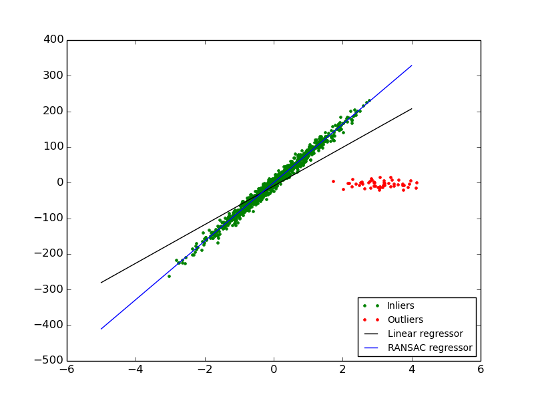
*Figure 7: make use of the correlation structure of the data with the Mahalanobis distance (MD). In this case, Di is calculated by way of where x̄ is the vector of means for the variables, S is the covariance matrix, and xi is the vector of observations for the ith person.* (Statistical Methods in Risk-Based Monitoring, 2018)

***Type 7: Analysis***

******

*Figure 8: a bar graph, allows for further checks, those with large Di values can be identified as outliers if they exceed a critical value, according to the chi-squared distribution at a specified significance level.* (*Statistical Methods in Risk-Based Monitoring*, 2018)

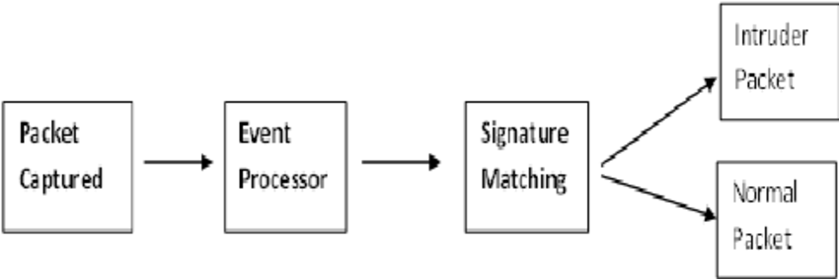
***Type 8: Inliers***

******

*Figure 9: Di is closest to zero and a good way of detecting these by eye is by taking the negative of the log* (*Statistical Methods in Risk Based Monitoring*, 2018)

## *Method 2: Signature-Based Detection*

A Signature-Based Detection consists of a valid signature for each of the files that you create, and with that signature, it can detect if it has been stored or previously detected (used). Anti-virus products such as Norton, MCAFEE, and more all use signature-based detection to detect attacks, malware, threats, etc. One unique fact about SBD is that it can quickly discover attacks. SBD can help identify many threats and attacks with the same pattern just by its signature. If a match is found within a potential attack or threat SBD will inform the police and further investigation will be conducted. (What Is Signature-Based Detection? — Techslang, n.d.). Also, is an approach to identify a specific code, or the hash of known malicious activity, associated with a piece of malware. (Signature-Based Detection Definition - Cybersecurity Terms, n.d.)

**

*Figure 10: The Event Processor initiates Signature Matching Detection, and it can detect the difference between malicious intent and normal safe intent.*

*Method 3: Large-scale intrusion detection*

Coordinated attacks, such as extensive stealthy scans, worm outbreaks, and DDoS attacks, appear on multiple networks at once. Traditional intrusion detection systems frequently only monitor a small portion of the network, which makes it difficult for them to identify these attacks. Instead, large-scale intrusion detection systems can scale better because they divide the computational load among numerous detection agents and have a global view of the network. There are two significant intrusion detection system strategies. The initial intrusion detection system strategy entails placing flow collectors across various subnetworks and using an aggregated data set to run a central detection engine.

The flow collectors send unprocessed packets to the detection engine. There are ways to get around the collection traffic overhead, which generates and sends the detector brief packet summaries. To achieve an acceptable true positive rate, which is still crucial, one must reach a bandwidth overhead of 35%. The collaborative intrusion detection system, a two-level anomaly detection system where monitors are physically divided in the network to carry out local detection, makes up the second intrusion detection strategy. They produce low-level alerts, which are then combined to create high-level intrusion reports.

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

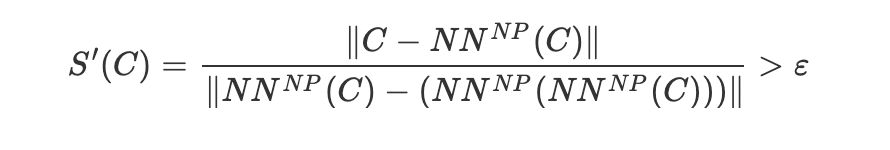
## 

## *Figure 11: Central Correlation Engine*

## *Method 4: Anomaly-Based Detection*

In the fourth article, named the Anomaly Detection Module approach, the algorithm that is used is the one-class nearest neighbor algorithm. This algorithm is put into place with the responsibility of revealing zero-day attacks before it becomes too late. The definition of distance or similarity functions between instance features is necessary for nearest neighbor anomaly detection techniques. There are a number of distance measures that can be used, but Euclidian distance is one of the most popular ones for anomaly detection and has produced excellent results in this field. A model for the class that corresponds to the context of typical behavior is first developed. A sample of typical connection profiles taken from the Audit Network connections repository served as the basis for the model that we created.

A connection record "C" that partially matches attack context profiles can be passed to the anomaly detection module as such a model is developed. Such a connection is recognized by the anomaly detection module as a zero-day attack and is disregarded as a regular activity. When the nearest neighbor selected from the standard connection profiles has a local density that is lower or equal to its own. For estimating local densities, the first nearest neighbor is typically used. The acceptance function is shown below, which computes the connection record "C's" anomaly score "S" and compares it to a user-defined threshold "E'' Based on the ratio between d1 and d2, experts can identify and classify the connection record "C" as a zero-day attack. In this instance, the one-class nearest neighbor algorithm was modified in a number of ways to speed up computation time, including sampling, computing normal sample nearest neighbors in advance, and dimensionality reduction using singular value decomposition. The number of numerical dimensions for connection "C" and the regular profiles connections was decreased using SVD. In order to predict zero-day attacks, the profile similarity score "S" and the anomaly score "S" of a connection record are combined at the end.

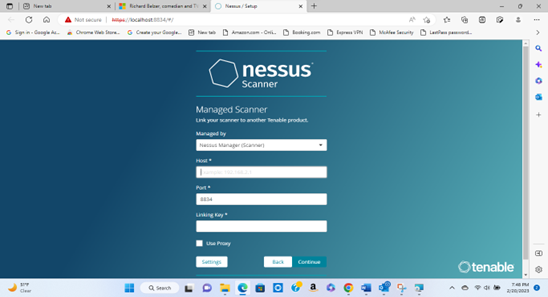


*Figure 12: The One Class Nearest Neighbor Algorithm*

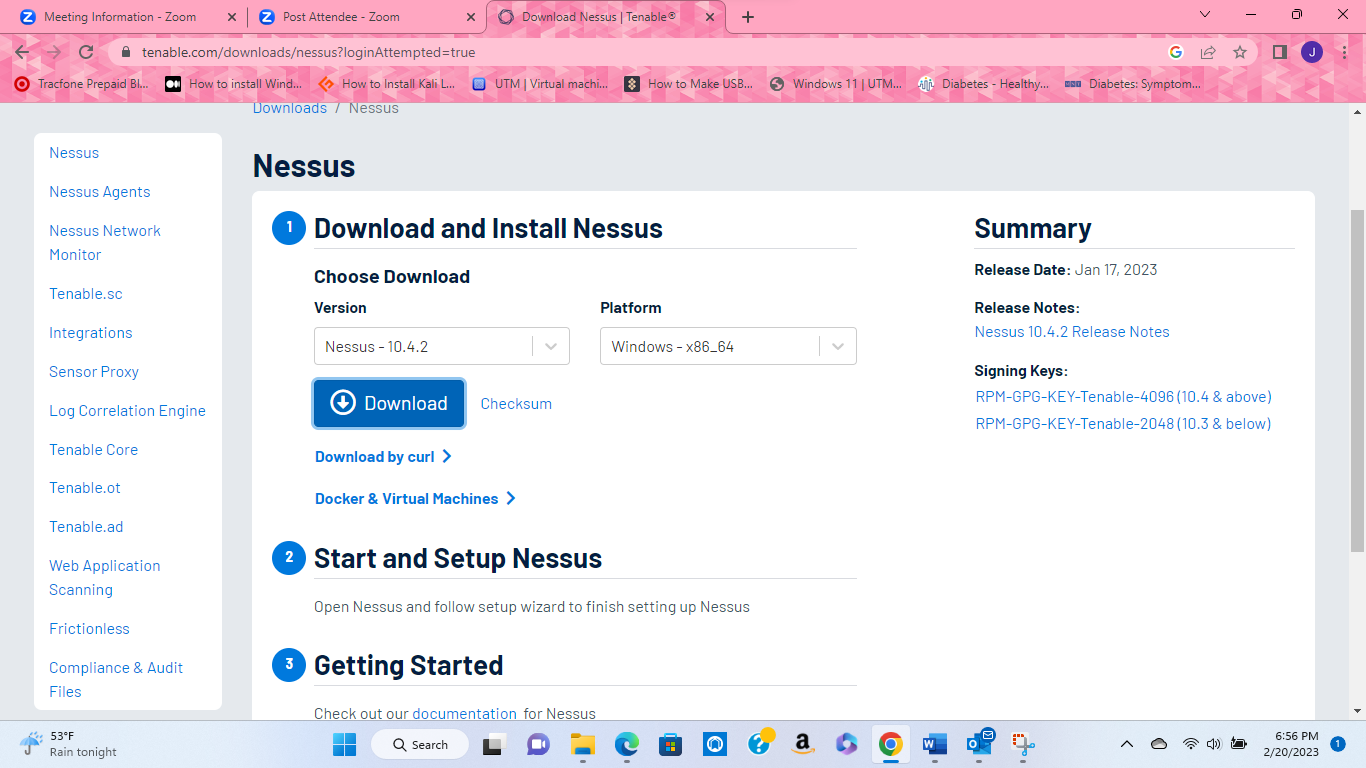
## *Method 5: Nessus*

Using Nessus can help protect against zero-day attacks. Nessus can test each port on a computer and detect what service is running, then test out its service if it has vulnerabilities that could be used for malicious intent. Nessus is what’s known as a remote scanner; it does not need to be installed on a computer for it to test a computer. It is very secure since it doesn’t assume that the computer is using port 80 because if it did that it could skip over other vulnerabilities. If it notices a vulnerability it has patching assistance and suggests a way to patch up the vulnerabilities. Nessus also allows for scripting language so, you can write different tests specific to your own system. When you understand the scripting tool more it also allows you to get a plug-in which they do have a website for and these plug-ins are meant to detect common viruses and vulnerabilities.

It also has up-to-date information about new vulnerabilities and attacks. The Nessus team adds updates to the list of what type of vulnerabilities to check on; it does this on a daily basis to lower the chance of the exploit coming into view and it is detected with the Nessus. Nessus finds vulnerabilities and exploits by scanning the computer and will alert the user if it notices anything. This tool is best used for an administrator that has to be in charge of a computer or even a group of computers. Nessus isn’t the computer security solution but will help out a lot.



*Figure 13: Nessus scanner UI*

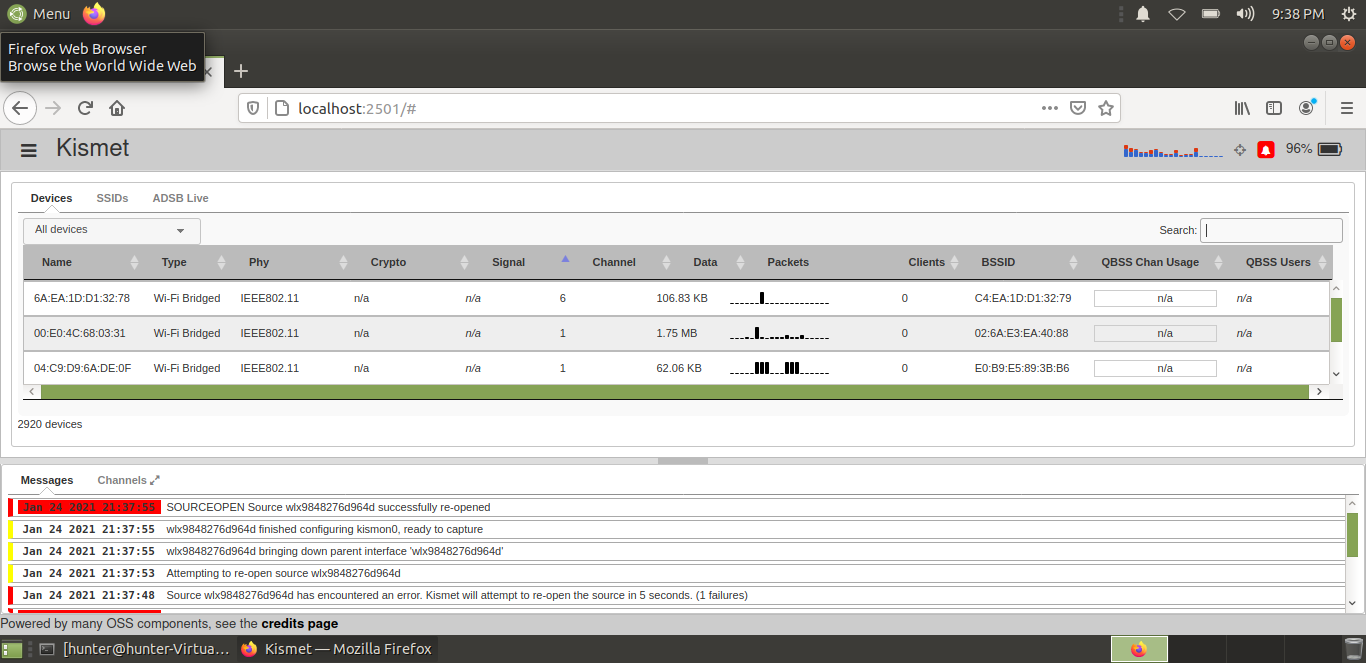


*Figure 14: Example Nessus of a scan report and installation*

## *Method 6: Kismet*

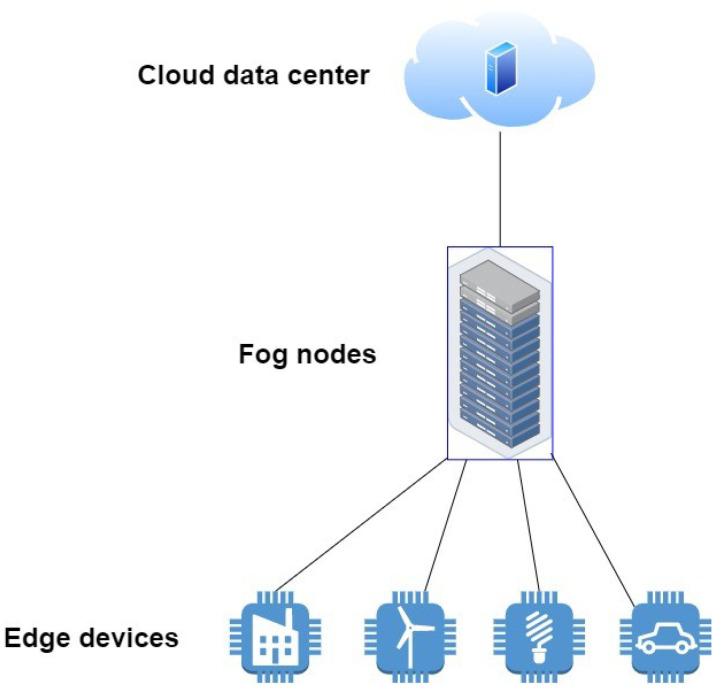
Kismet is a type of tool that can passively act as a network detector, sniffer, wireless intrusion detection framework, and wardriving. When I wrote that kismet works passively it means that it will not send any type of logging packets. Kismet can also work by placing a wireless access card into monitor mode and the program will be able to see all the packets. Kismet is able to capture Bluetooth and can replay pcap pcap-ng files. Kismet can and will allow users to capture packets remotely. This program can also use GPS to give a general idea of where a receiver target is located. It also will allow a user to filter based on MAC addresses and other types of things as well.

This program is a console-based 802.11 layer-2. This program can reveal hidden networks if they're active, it does this by “channel-hopping,” which is a process of scanning each channel in the 2.4 GHz frequency band” ( Dan, 2018). It can log traffic in Wireshark/tcpdump compatible format. This program can plot detected networks and estimate the ranges on downloaded maps. Kismet's uses are that it can be used to identify and audit wireless networks and their configuration. This program can also be used to identify wireless networks that are misconfigured or even unauthorized rogue APs. Some of its components that come with the Kismet server are “(kismet\_server) and the Kismet client (kismet\_client). The Kismet server is what performs the packet sniffing and network detection, while the Kismet client is the GUI” ( Dan, 2018).



*Figure 15: Example of a Kismet interface*

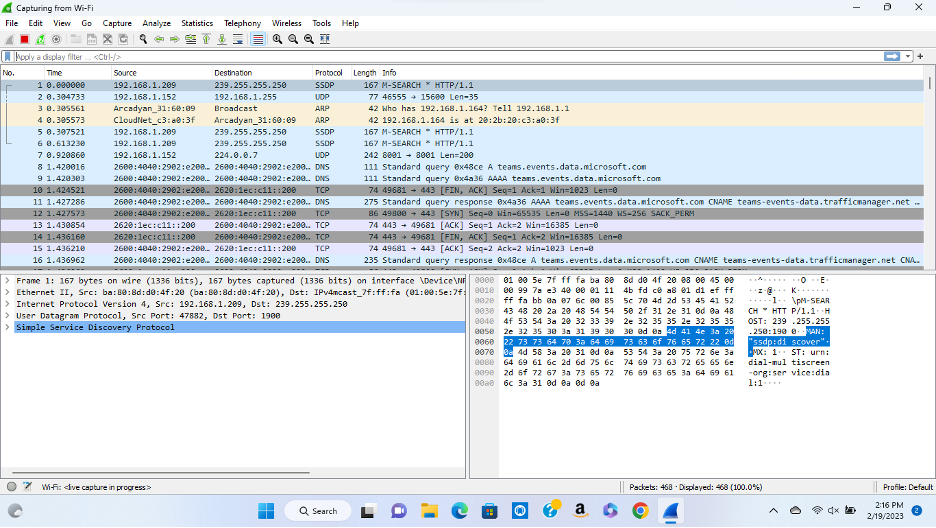
*Method 7: Fog Computing*

According to Cisco Systems, fog computing is a virtual platform that offers computation, storage, and networking services to end devices from cloud computing data centers which are not specifically located at the network edge” ( Yao, 2021). Fog Computing is different from the cloud in that it has got end users closer to it as compared to the cloud, Fog is able to provide the services and then respond to their demands in a small amount of time. Fog computing is known as a distributed computing technology and that maximum operations are performed on it by virtualized and non-virtualized edge devices. Though it is still different from the cloud “It has some similar characteristics with cloud including non-latency aware processing and ability to store useful data for a longer time period by existing between the users and the cloud. The basic architecture of fog computing is similar to cloud computing, but its lower layers contain special components that are able to detect rare time responses efficiently. Due to this feature, fog computing is used to control and improve health care departments, traffic patterns, parking systems and much more” ( Yao, 2021). Fog computing has a disseminated framework that consists of a gadget that does services outside of the system. “Fog computing provides an improved administration and smooth client experience. It is basically a combination of hardware and software systems that has the power to monitor, control and analyze data with extremely low latency. In addition, Fog computing does not provide permanent storage. It reduces the load on the cloud by deleting unnecessary data into its computational storage, which also minimizes the cost” ( Yao, 2021).

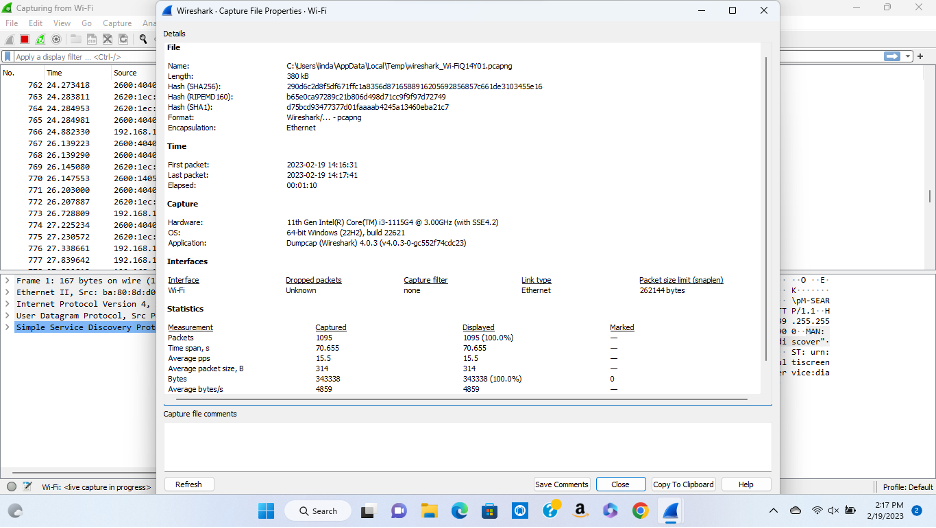
*Figure 16: Diagraph of fog nodes sending data to Edge devices*

*Method 8: Wireshark*

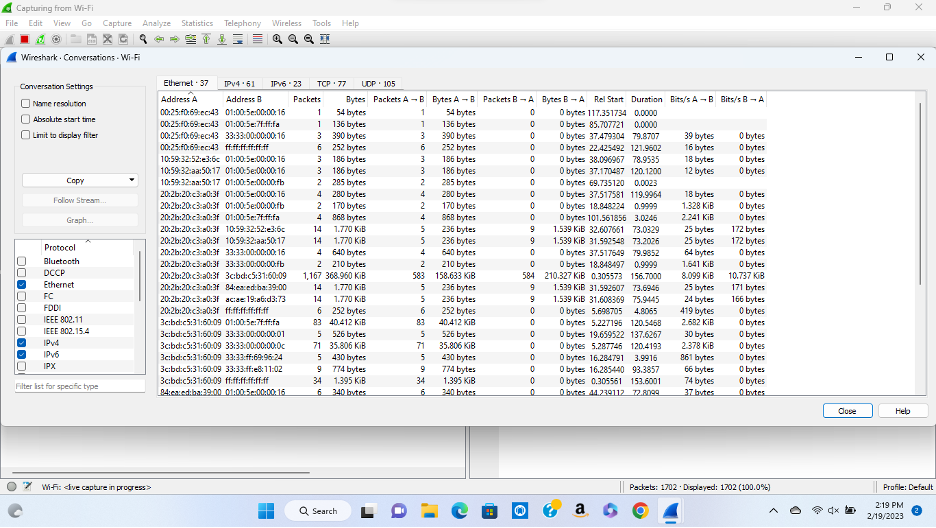
Wireshark is a network-capturing tool, it will help you capture network packets and display them. Wireshark lets you monitor your network traffic under a microscope and filter them. You can easily point out vulnerabilities inside of your network while using Wireshark. (What Is Wireshark and How to Use It | Cybersecurity, n.d.)The way Wireshark captures packets is by your network connection such as from your PC, and the internet. It is basically a packet sniffer and analysis tool to monitor your network traffic. It offers decryption for Wi-Fi and Ip Addresses and captures many file formats so they can also be analyzed. It is compatible with MAC OS, Linux, and Windows OS, practically anyone can access it. (Breeden, 2022). Wireshark can troubleshoot latency issues as well as malicious activity on your network. It consists of displaying how all devices (laptops, PCs, phones, routers, etc.) communicate with each other (Wireshark Tutorial - Javatpoint, n.d.)



*Figure 17: A display of Wireshark capturing packets and IP Addresses inside of an HP Laptop and scanning them from Wi-Fi.*

**

*Figure 18: Wireshark is displaying Capture File Properties from Wi-Fi/ displaying the laptop’s information that is being used to initiate Wireshark. Displaying Name, Length, Hash, Path, Format, First and Last Packet, Elapsed Time, Hardware, OS, Application, Interface, Dropped Packets, Capture Filter, Link Type, Packet Size, and Statistics.*

**

*Figure 19: Wireshark is displaying the Conversation of the Wi-Fi network, consisting of Address A and B, Packets, Bytes, Packets A and B, Bytes A and B, Packets B and A, Bytes B and A, Rel Start, Duration (Time), Bits A and B, and Bits B and A.*

# Summary

# 

The magical thing about technology is that it constantly evolves. As technology becomes more prevalent in the world the need for a more robust security system is heightened. There is always room for learning and improvement within each organization when it comes to keeping up-to-date hardware, software, and security protocols. As discovered in the case study section, If Sony’s network security had been more advanced the organization wouldn’t have had to undergo the loss of private documents or the release of four of their unreleased movies. This paper showed how important it is to stay 10 steps ahead of different hackers. The data has shown how effective zero-day attacks can be when commandeering networks.

The thing that makes zero-day attacks different from other malicious attacks is that it’s a software flaw that fails to announce itself by the vendor but has been used by attackers. Since there is currently no patch available, attackers can easily take advantage of the flaw since there are no safeguards in place. Thus, the importance of keeping your team up to date with new security protocols and new ways to keep the network safe is imperative to keeping the company up and running securely. Numerous machine learning algorithms have been shown to be effective at preventing zero-day attacks through numerous articles and practical experimentation. The statistical approach, signature-based detection, and unsupervised port-based approach, to name a few, are some of the most notable machine learning algorithms. In summary, machine learning is an excellent tool for predicting zero-day attacks and should be used going forward.

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# References

Achyuthuni, H. (2019, July 7). *Univariate analysis*. RPubs. Retrieved February 20, 2023, from https://rpubs.com/harshaash/Univariate\_analysis

Breeden, J. (2022, June 8). *What is Wireshark?* Network World.com. Retrieved February 20, 2023, from https://www.networkworld.com/article/3663021/what-is-wireshark.html

Rai, A. (2022, July 11). *What is Univariate Analysis?* AnalytixLabs. Retrieved February 20, 2023, from https://www.analytixlabs.co.in/blog/univariate-analysis/

*Signature-based Detection Definition - Cybersecurity Terms*. (n.d.). CyberWire. Retrieved February 20, 2023, from https://thecyberwire.com/glossary/signature-based-detection

*Statistical Methods in Risk-Based Monitoring*. (2018, October 2). Quanticate. Retrieved February 20, 2023, from https://www.quanticate.com/blog/statistical-methods-in-risk-based-monitoring

*Test lab automation solutions for Cyber & Security test labs*. (n.d.). Netscout. Retrieved February 20, 2023, from https://www.netscout.com/solutions/cyber-and-security-test-labs

*What is Signature-Based Detection? — Techslang*. (n.d.). Techslang. Retrieved February 20, 2023, from https://www.techslang.com/definition/what-is-signature-based-detection/

*What Is Wireshark and How to Use It | Cybersecurity*. (n.d.). CompTIA. Retrieved February 20, 2023, from https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it

Whittaker, Z. (2022, January 24). *Flaws in third-party software exposed dozens of Teslas to remote access*. TechCrunch. Retrieved February 20, 2023, from https://techcrunch.com/2022/01/24/teslamate-bug-teslas-exposed-remote/

*Wireshark Tutorial - javatpoint*. (n.d.). Javatpoint. Retrieved February 20, 2023, from <https://www.javatpoint.com/wireshark>

Lirim Ashiku, Cihan Dagli, Network Intrusion Detection System using Deep Learning, Procedia Computer Science, Volume 185, 2021, Pages 239-247, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2021.05.025>.

A. G. P. Lobato, M. A. Lopez, I. J. Sanz, A. A. Cardenas, O. C. M. B. Duarte and G. Pujolle, "An Adaptive Real-Time Architecture for Zero-Day Threat Detection," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 2018, pp. 1-6, doi: 10.1109/ICC.2018.8422622.

Agathe Blaise, Mathieu Bouet, Vania Conan, Stefano Secci, Detection of zero-day attacks: An unsupervised port-based approach, Computer Networks, Volume 180, 2020, 107391, ISSN 1389-1286, <https://doi.org/10.1016/j.comnet.2020.107391>.

A. AlEroud and G. Karabatis, "A Contextual Anomaly Detection Approach to Discover Zero-Day Attacks," 2012 International Conference on Cyber Security, Alexandria, VA, USA, 2012, pp. 40-45, doi: 10.1109/CyberSecurity.2012.12.

*Cynet takes cyber threat protection automation to the next level with incident engine*. The Hacker News. (2020, September 9). Retrieved February 20, 2023, from <https://thehackernews.com/2020/09/cynet-cybersecurity-software.html>

*How to use windows defender in windows 10 (creators update)*. YouTube. (2017, May 1). Retrieved February 20, 2023, from <https://youtu.be/HH0xdWpckZ>Y

Nessus. (n.d.). Retrieved February 20, 2023, from <https://www.cs.cmu.edu/~dwendlan/personal/nessus.html#:~:text=Nessus%20works%20by%20testing%20each,carry%20out%20a%20malicious%20attack>.

Team, M. D. A. T. P. (2020, October 8). *Windows defender exploit guard: Reduce the attack surface against next-generation malware*. Microsoft Security Blog. Retrieved February 20, 2023, from <https://www.microsoft.com/en-us/security/blog/2017/10/23/windows-defender-exploit-guard-reduce-the-attack-surface-against-next-generation-malware/>

*The 2014 Sony hacks, explained*. (2015, June 3). Vox. Retrieved February 20, 2023, from <https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea>

Alwakeel, A. M. (2021, December 9). *An overview of fog computing and Edge Computing Security and Privacy Issues*. Sensors (Basel, Switzerland). Retrieved February 21, 2023, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8708798/#:~:text=According%20to%20Cisco%20Systems%2C%20fog,located%20at%20the%20network%20edge.

*Kismet*. Kismet – SecTools Top Network Security Tools. (n.d.). Retrieved February 21, 2023, from https://sectools.org/tool/kismet/

Thecybersecurityman, Published by thecybersecurityman View all posts by thecybersecurityman, thecybersecurityman, P. by, thecybersecurityman, V. all posts by, & (required), N. (2018, March 28). *Pentest Edition: Kismet Wireless*. The Cybersecurity Man. Retrieved February 21, 2023, from https://thecybersecurityman.com/2018/03/22/pentest-edition-kismet-wireless/

VanSickle, R., Abegaz, T., & Payne, B. (n.d.). *Effectiveness of tools in identifying rogue access points on a wireless network*. DigitalCommons@Kennesaw State University. Retrieved February 21, 2023, from https://digitalcommons.kennesaw.edu/ccerp/2019/education/5/