HONEYPOTS IN CYBERSECURITY– A SECURITY MECHANISM THAT CREATS A VIRTUAL TRAP TO LURE ATTACKERS

BY

Marina Naznin
ID: 221-25-122

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Master of Computer science and Engineering (Major in Data Science)

Supervised By

Mr. Narayan Ranjan Chakraborty
Associate Professor
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

JANUARY 2023

APPROVAL

This Project/Thesis titled **"HONEYPOTS IN CYBERSECURITY– A SECURITY MECHANISM THAT CREATS A VIRTUAL TRAP TO LURE ATTACKERS"**, submitted by **Marina Naznin**, ID No: **221-25-122** to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on **17-01-2023**.

BOARD OF EXAMINERS

Chairman

Dr. S M Aminul Haque, PhD
Associate Professor & Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Ms. Naznin Sultana
Associate Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Mr. Md. Sadekur Rahman
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

External Examiner

Dr. Mohammad Shorif Uddin, PhD
Professor
Department of Computer Science and Engineering
Jahangirnagar University

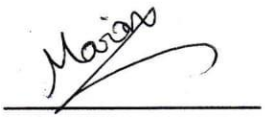
DECLARATION

I hereby declare that, this project has been done by us under the supervision of **Mr. Narayan Ranjan Chakraborty**,Associate Professor, Dept. of CSE, Daffodil International University. I also declare that neither this project nor any part of this project has been submitted elsewhere for the award of any degree or diploma.

Supervised by:

Mr. Narayan Ranjan Chakraborty
Associate Professor
Department of Computer Science and Engineering
Daffodil International University

Submitted by:



Marina Naznin
ID:221-25-122

Department of Computer Science and Engineering
Daffodil International University

ACKNOWLEDGEMENT

And first foremost, I offer our heartfelt appreciation and gratitude to Almighty God for His divine gift, which has enabled us to successfully finish the final year proposal.

I really grateful and wish our profound our indebtedness to **Mr. Narayan Ranjan Chakraborty, Associate Professor,**Department of CSE Daffodil International University, Dhaka. Our supervisor has extensive knowledge and a great interest in the subject of Computer Networks, Cryptography and Information Security. Honey pots will be used to complete this project. His unending patience, scholarly guidance, constant encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stages, and reading many inferior drafts and correcting them at all stages enabled us to complete this project.

I would like to express our heartiest gratitude to Professor Dr. Touhid Bhuiyanand Head, Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

I would like to thank everyone of our Daffodil International University classmates who participated in this discussion while completing their course work.

ABSTRACT

As the popularity of wireless networks soars, maintaining their security is a significant challenge. Wi-Fi networks are susceptible to Rogue Access Points because of the open medium, inadequate software implementation, potential for hardware deficiencies, and inappropriate configuration (RAP). Unauthorized access points known as "rogue access points" can be installed by end users without the security administrator's knowledge. When this malicious device is linked to the Internet, an attacker can utilize it to compromise the network's security. I ran various port and service script configurations, simulated operating systems, and tested which formats worked best as a research honey pot and which formats worked best as a decoy to safeguard other network users. In order to get better results for both goals in the coming weeks, we examined the results. However, configurations successful for one objective were not always successful for the other.Nevertheless, I did uncover promising setups for both purposes. Additionally, I determined the most typical attacks, the most typical ports utilized by attackers, and the level of effectiveness of decoy service scripts. I'll examine the system's architecture, configuration, and operation. After the system's operational phases are complete, I'll look at how the results are pulled from the database and how they're analyzed. In order to create new rules that might prevent them in the future, I must mine through the retrieved results to try to locate the harmful data. I will have a solid understanding of the network traffic that has been recorded and what makes up some of the more intriguing packets at the project's conclusion.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Since honey pots were created in the last ten years to detect, deflect, or counterattack an unauthorized use of information systems, attackers have been compelled to create methods to recognize and deactivate honey pots when they attempt to attack networks. Some security experts believe that the employment of honey pots is now obsolete as a result of the success of some of these tactics. There are, however, defenses against this anti-honey pot technology as well.

Security is a huge issue right now. One such technique to lessen these threats is the use of cloud computing and intrusion detection and prevention systems. Various researchers have periodically presented various IDSs, some of which combine aspects of two or more IDSs and are referred to as hybrid IDSs. The majority of researchers combine the benefits of signature-based and anomaly-based detection methodologies. Any normal network, whether it be wired or wireless, faces a serious security risk from the unlikely and unwelcome admission of malevolent users and/or data packets. The fundamental building blocks of all communication systems are data packets. Thus, network security also entails data packet security. The most fundamental building unit of communication, a data packet streamlines the flow of its countless duplicates to send information from one device to another.

Protecting systems, networks, and programs from cyberattacks is the practice of cybersecurity. These hacks typically try to disrupt regular corporate operations, extort money from users, or access, alter, or delete important information. Nowadays malicious attacks are increasing very badly. It's like it's common to leak anyone’s personal information daily. It has become a serious issue in our country. We’ve also seen that Amazon, and eBay's servers were down for the malicious attack. Stunt has also been used in sophisticated malware strikes against vital infrastructure. So we need to secure our online presence. Organizations use a variety of mainstream, conventional security technologies to identify and stop attacks. These solutions have the drawback of only

being effective against known vulnerabilities. Antivirus and anti-malware software can identify specific worms, Trojan horses, and other viruses if they have signatures for them in their database; otherwise, they are unable to do so. The manual production of signatures and their analysis take a lot of time. A computer security tool called a honey pot is used to spot, block, or otherwise thwart attempts at unwanted access to information systems. Honey pots are used to gather data from unauthorized attackers who get access to them after being duped into thinking they are a legitimate component of the network. As part of their network defense plan, security teams use these traps. Additionally, honey pots are utilized to study the actions and communications of online attackers. There are different types of honey pots. In this study, a novel modular strategy for using honey pots for cyber security is introduced. A cyber security infrastructure also includes numerous other security technologies, such as firewalls, IDS, anti-malware, and antivirus software. A relatively new and developing field of study is honey pot technology, which is being developed to address new security concerns and difficulties.

1.2 Motivation

- It increases system performance by lowering the false alarm rate.
- It can easily be integrated to detect multiple attacks by using several honey pots.
- It can fool attackers to a greater extent.
- It can keep the workload of the honey pot to a minimum.

1.3 Research Question

- How much the wire shark can catch cyber-attacks?
- Is it possible to detect Phishing site with their IP& other details info?
- What'll be the Effectiveness of The Wire shark?
- Could it be able to mislead the assailants?
- Will it can keep the honey pot's total workload to a minimal?
- Can we implement it to identify of attacks?

1.4 Expected Outcome

- Good knowledge about honey pots.
- Know about the wire shark& The KF-Sensor.
- Can secure network from cyber security

1.5 Report Layout

This report varied in a total of six different chapters. Which are capable of extending the understanding of “Honey pots in Cyber security” more briefly.In the first chapter, we’ll mention introduction, motivation, rational study, research questions and the last one is the expected outcome.In the second chapter, we’ll brief about some related works, which types of challenges that we had faced and about the research summary.In the third chapter, we’ll talk about our research subject and instrumentation, workflow of the model, how we’ve installed and configured thewire shark& KF-sensor.In the fourth chapter, we’ll talk about the result that we got, the evaluation of our Honey pots. In the fifth chapter,we’ll describe its impact on our society, impact on our environment and sustainability.In the sixth chapter, which is our last chapter, we’ll mention the conclusion and our future works.

CHAPTER 2

BACKGROUND STUDY

2.1 Introduction

To create a strong, secure platform, honey pots are incorporated into networks together with firewalls and intrusion detection systems. With the largest database in the world, Amazon uses database honey pots to trick attackers into accessing its honey pots. By reducing the number of false positives and false negatives, honey pots enhance IDS. When the word "security" is employed, it refers to reducing the vulnerabilities of resources and assets. As the term "information security" suggests, protecting assets and establishing controls and procedures to prevent harm or potential impact on the system(s) under examination have always been its core purposes. As is, this definitionunderstood in security circles can be interpreted in a number of different ways, but it is frequently used defensively. The list of things to secure is endless and includes the server, the network, and the logs. However, due to expanding demands, applications, and utilities like wireless LANs, remote locations, working from home, and VPNs, in today's environment and systems where you never know where your network starts and ends, this technique becomes a little too onerous.In order to acquire information on new threats, honey pots can be employed as early warning systems, slowing down automated assaults and catching new vulnerabilities. They might be login and password information, Excel files, or credit card details. Additionally, honey pots may be attacked and hacked without ever being computerized, much like networks. Here, we'll get to know about honey pots, types of honey pots. Also, will get to know about the attackers, types of attackers.

2.1.1 What is a Honey pot?

A network-attached system called a honey pot is set up as a ruse to tempt online attackers. Large businesses utilize honey pots as a crucial tool to mount an active defense against intruders. Large corporations and businesses engaged in cyber security research frequently deploy honey pots. On a network, a demilitarized zone (DMZ) is a common location for honey pots. Honey pots can be taken over by cybercriminals and used against

the company that set them up. The quantity and nature of risks that a network infrastructure is exposed to can be determined by watching and recording activities in the honey pot.

We can use it in very ways. For example: Honeypots have been designed to look like USB storage devices, such as Ghost. It’s sounds quite interesting. That means the honeypot will fool the malware into infecting the emulated device if a PC is compromised with malware that spreads over USB. There are a lots of uses of honey pots. Those are:

- Attackers travel throughout my environment conducting reconnaissance, scanning our network, and looking for susceptible and poorly configured equipment. At this point, they are probably going to trip my honeypot, alerting me to look into it and block access from attackers. [25] By doing this, I can react before an intruder has an opportunity to successfully steal data from my surroundings. Instead of targeting locations with actual data, malicious actors may spend a lot of time trying to work on the honeypot. By directing their attack on a useless system, I can squander cycles and receive early notification of an impending attack. [25]

- They aid in our process testing for incident response. Honeypots are a low-cost way to evaluate our team's preparedness in the event that a honeypot detects unexpected behavior, which can help you improve our security maturity. [25]

- In addition to being simple to download and install, modern honeypots can deliver precise alerts regarding harmful setup errors and attacker activity. It's possible that your team won't even be aware that a honeypot has been set up until someone starts probing your internal network. For honeypots to be effective, known-bad attack signatures and recent threat information are not necessary, unlike intrusion detection systems. [25]

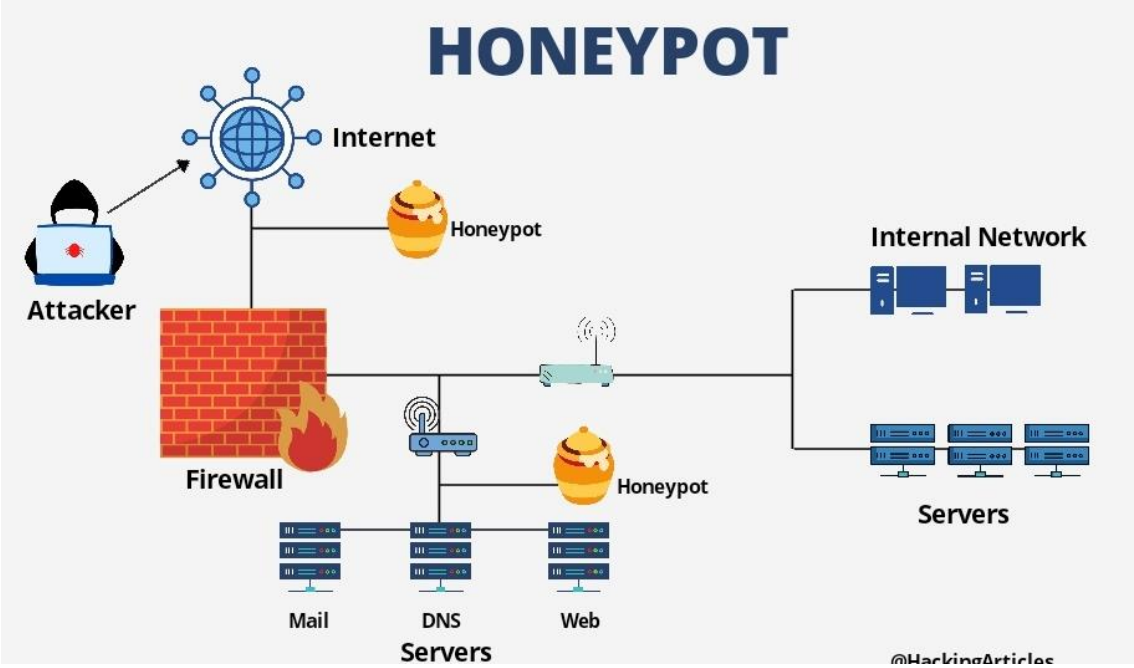


Figure 2.1: Honey pots [19]

2.1.2 Types of Honey pots:

On the basis of Interaction there are 3 types of Honey pots:

- **Pure Honey pot [21:** A full-scale system running on various servers is referred to as a pure honeypot. It mirrors the industrial process in every way. A pure honeypot has "sensitive" user information and data that has been disguised to appear confidential. It also has a variety of sensors that are used to track and monitor attacker activities. [21]

- **High Interaction Honey pot [21]:**A high-interaction honeypot is made to entice intruders to stay inside for as long as feasible. This increases the security team's chances of observing the aims and motives of the attacker and of identifying systemic weaknesses. The attacker might wish to try to get into additional systems, databases, and processes in a honeypot with heavy user involvement. Researchers can see the attacker's search strategy, preferred sources of information, and attempts to increase their access privileges. [21]

- **Mid Interaction Honey pot [21]:** The application layer is mimicked by mid-interaction honeypots, although they lack an operating system. Their goal is to disorient or delay an attacker so that the organization has more time to decide how to respond to the specific type of attack. [21]

- **Low Interaction Honey pot [21]:** Low-interaction honeypots use fewer resources and acquire basic information about the type of threat and its origin. These utilize network services, the Transmission Control Protocol (TCP), the Internet Protocol (IP), and are reasonably easy to set up. However, there is nothing in the honeypot that may keep the attacker's interest for a long period.

On the basis of Purpose there are 2types of Honey pots:

- **Research Honey pot [22]:** It utilized for security improvement and educational reasons. They contain traceable data that can be used to investigate an attack if it is taken. [22]

- **Production Honey pot [22]:**It operate as dummy systems within fully functional networks and servers, frequently as a component of an intrusion detection system (IDS). They divert criminal focus away from the actual system while monitoring malicious activities to help close security holes. [22]

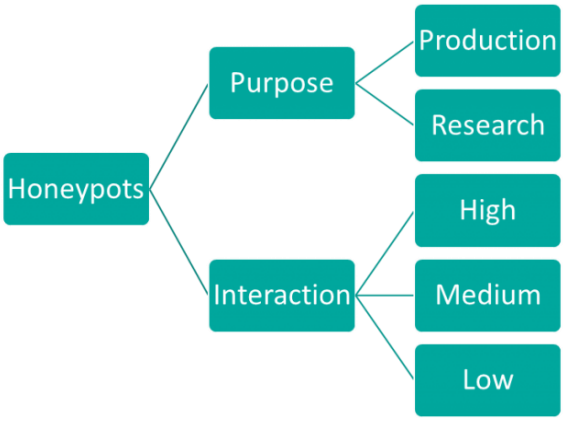


Figure 2.2: Types of Honey pot [23]

2.1.3 How Do Honey pot's Work?

A honeypot resembles a real computer system in many ways. It has the tools and information that cybercriminals use to choose the best targets. For instance, a honeypot could impersonate a system that holds private consumer data, including credit card or personal identification numbers. [20] Decoy data can be introduced into the system to lure in potential attackers wanting to steal, use, or sell it. The IT staff may see the attacker enter the honeypot and follow their steps, noting the different approaches they use and how well or poorly the system's protections work. The network's overall defenses can then be strengthened using this information. [20]

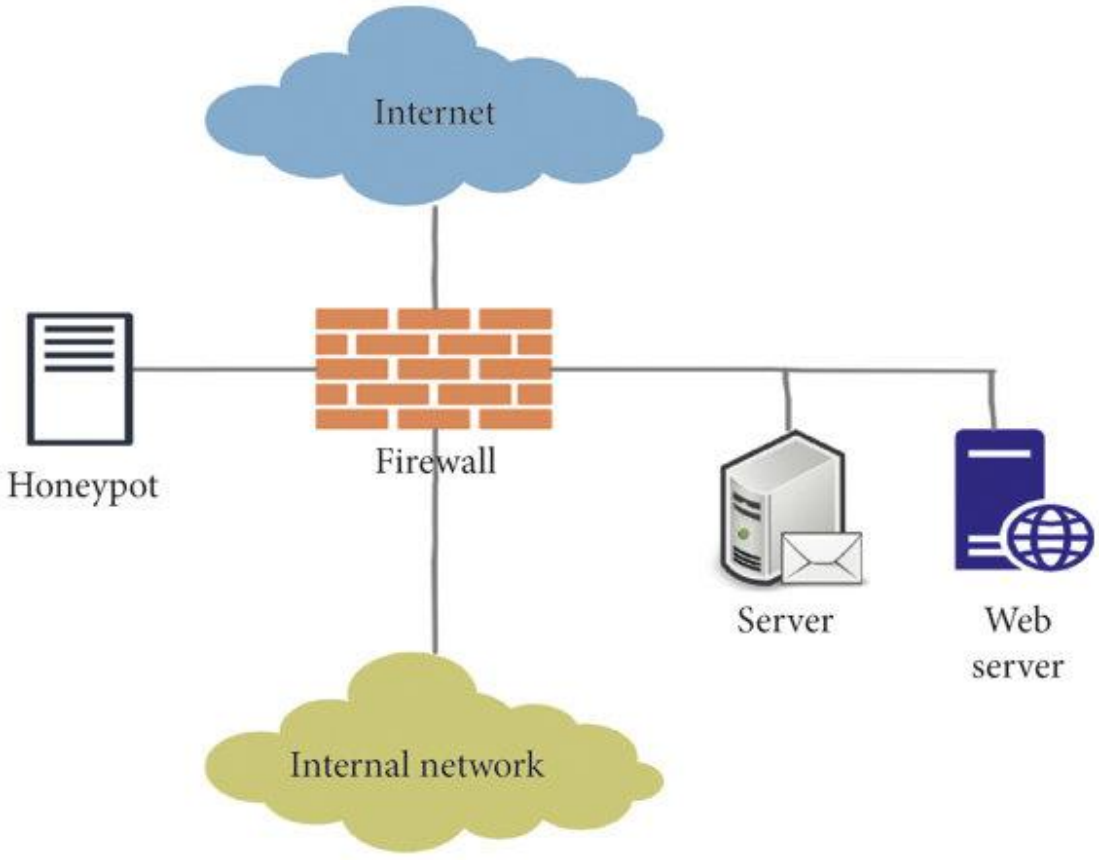


Figure 2.3: Working process of Honey pots [19]

2.1.4 Attackers

The attacker could be anyone who attempts to gain unauthorized access to a network or system without the proper authorization. It could even be someone from space. These attackers are mostly automated bots16 that scour the internet for a public network connection that connects to a private network, though occasionally a human hacker17 may also be involved. These bots attempt to access networks in the hopes of gaining access to information that would be useful or of interest to the boot's owner. The sole objective of certain bots, however, is to disrupt networks, destroy data, and damage hardware.

An attacker in the context of computers and computer networks is a person or a group that engages in malicious actions with the intent to damage, reveal, disable, steal, obtain unauthorized access to, or otherwise misuse, a resource. [26]Each of us spends more time online as Internet access spreads across the globe and as the number of attackers also increases. Attackers employ all the tools and strategies they can to try to get access to our systems without authorization. [26]

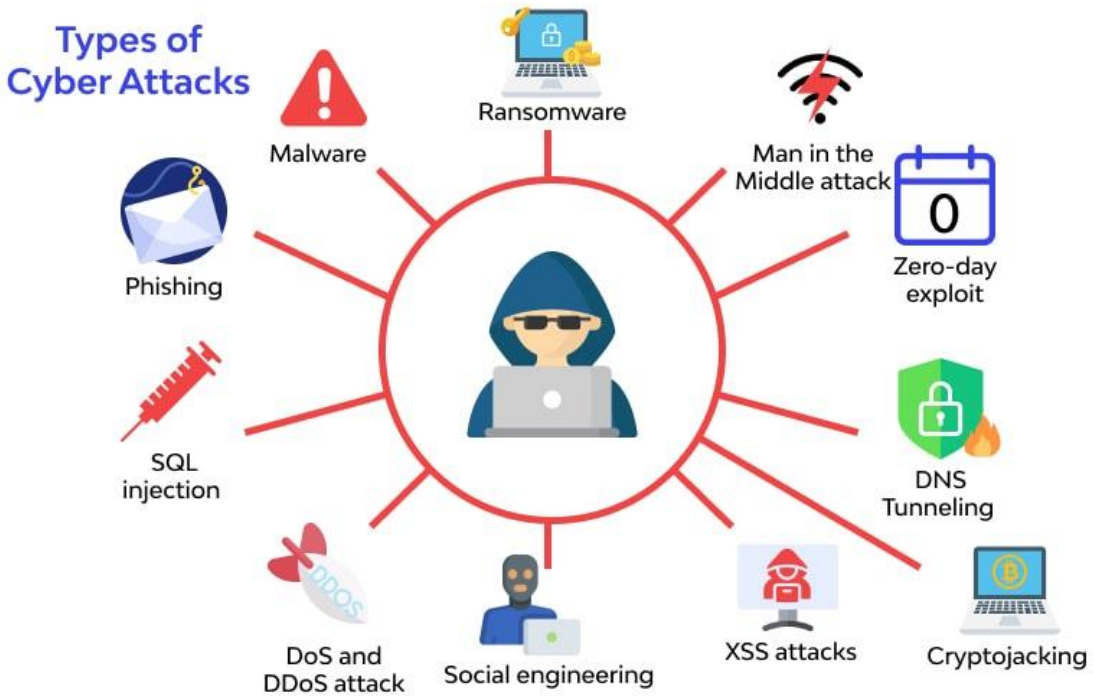


Figure 2.4: Types of Cyber Attacks [24]

- **Trojan:** A Trojan, sometimes known as a Trojan horse, is a sort of malware that hides its true purpose in order to trick a user into believing it to be a benign program. The "payload" carried by a Trojan, like the wooden horse used to capture Troy, is unknown to the user, but it can serve as a delivery system for a number of threats.[12]

- **Rabbit:** Ransom ware of the "drive-by-attack" variety, such as Bad Rabbit, spreads by infecting websites. Vise ion, Dragon, and Rhagae, the dragons from well-known shows and books, are mentioned in the code. Who exactly is behind Bad Rabbit is unknown. It's believed that Bad Rabbit attacked Russian media outlets, forcing servers to fail. Additionally, it affected vital transportation infrastructure organizations in Ukraine. Businesses in the United States have not yet been impacted by the Bad Rabbit virus, but they are advised to be vigilant for any potential breakouts.[13]

- **Spyware:** One of the most popular cyber-attack techniques that are challenging for users and organizations to recognize is spyware. Spyware gathers private and sensitive data that it sells to advertising, data-gathering companies, or unscrupulous individuals in order to make money. Four years ago, spyware impacted the systems of 80% of internet users.[14]

- **Macro:** Malicious attachments in phishing emails are how macro malware is spread. The malware won't be able to infect the device if the macros in a Microsoft Office file are not executed. Reducing the number of interactions between malware and a device is the best strategy to get rid of the threat of macro malware. Do not open any attachments in shady emails from unknown senders. Do not enable macros if a malicious macro command appears to carry out nefarious deeds. Before they have a chance to become victims, teach your coworkers how to spot potential risks. [15]

2.1.3 IDS:

A honey pot is composed of numerous tools, programs, and utilities. On a network protected by a firewall, the IDS itself will open a port. This permits access to the Honey pot while safeguarding the security of the rest of the network. I've used Wire shark and KF-Sensor for my project.

2.2 Related work:

Gurdip Kaur EPL and Jatinder Singh Saini explain white hats & black hats. Black hats and white hats are the two different communities that network security interacts with. This research is based on the use of honey pots with low and high levels of interaction. As a reverse firewall, the Honeywell gateway let's all kinds of traffic—both good and bad—into the system.

Almutairi, et al.'s description of the many traits of the researchers' available high-interaction honey pot technologies [2]. Given that their functioning varies mostly in the data analysis, it distinguishes between them using a detection mechanism. The overall pattern is evident despite the wide variety of honey pots and associated tools: Simple proof of concept tools evolved into more advanced honey pot technologies. Tools for administration and analysis arise when the desired analysis becomes more complicated.[2]

The proper way to compare different protocols in MANETs over a wide range of categories is provided by G. Singh et al.[3]. It aids me in correctly evaluating how to compare various honey pot tools. A lot of businesses employ honey pots to protect their data from outside users. Since so many technologies are open-source and free to use, securing data for enterprises is now considerably more affordable and practical. Readers may find this document useful in protecting their resources from attackers by utilizing the free honey pot tools.[3]

The intrusion detection module is introduced by Dongxia, L.[4], and Yongbo utilizing the IP Trace back approach. By using mobile agents, we can increase the system's capacity. Honey pot Internet of Things (IOT) (HIoTPOT) monitors IOT devices covertly and

analyzes the numerous current risks to IOT devices.[4] All attackers are drawn to IOT since it is accessible and open, making it a prime target.

According to C.H. Yeh and C.H. Yang,[5] a honeyed tool interface may be provided for log checking and SMS operation in a real-world setting. A lightweight container-based deployment called Honeynet imitates common Linux and Windows services for unwary invaders. Results display actual assaults on the installed system[5]. By simulating the physical systems and services existing within the network, Honey-net can aid in preventing access to genuine systems.

According to Z. LiJuan[6], honey pot tools can be utilized to secure the defense system even if they have a number of drawbacks. It’s quite interesting. [6]

The network deception tool built on the Java and honeyed programs is described by R.Upadrashta, et al. By scripting the straightforward honeyed utility in Java, it can now operate on a variety of systems, improving its functionality.

Ren-ling LI and colleagues[7] create the SISH (Study of Intrusion Signature based on Honeypot) methodology to fully watch and record the attacker's activity. It examines the data that has been recorded before creating the first signatures to strengthen the security of the system. An efficient and strong network security solution is an intrusion detection system (IDS). The research trends in network-based intrusion detection systems are reviewed in this article. Additionally, it examines benchmark datasets, the current state of NIDS, and popular NIDS approaches.

In light of unaided peculiarities, the creators offer an independent technique for attack characterization. using what has been accumulated by honey pots to learn. This arrangement of stream troupes into traffic classes depends on bunching methods including thickness-based grouping, subspace grouping, and proof collection. This approach has the advantage of not needing a preparation stage. There are several ways that vary based on the problem's nature and the kind and amount of data. There are three types of machine learning: supervised, unsupervised, and reinforcement learning.

In view of AI, the creators propose a shrewd honey pot that upgrades the security of IOT gadgets. A model called IOT Student was prepared to be utilized by the clever honey pot that can streamline a model to answer assailants, and an IOT scanner was introduced to test accessible IOT gadgets on the Web and sweep the Web for each hurtful collaboration.

The administrator network uses the reports created by the antagonistic source to find out about the character, inspirations, and methodologies utilized by the gatecrasher to infiltrate the framework. The executive organization planned to naturally treat every communication distinguished as an unsafe action.

Rather than the main kind of learning, support learning doesn't utilize names; all things being equal, the specialist acquires information from its encounters to get done with the task within reach. This is the means by which support gaining varies from administered learning.

According to Bailey and Holz's[10] research, recent developments in honey pot research have been greatly influenced by the adoption of new types of network applications, geographic diversity in Internet user populations, expansion of underground attacker communities, and technological advancements in networking hardware.

A few surveys on honey pot research have been conducted. Seifert[11] conducted a survey on the various types of honey pots currently in use, highlighting their benefits. A succinct overview of particular kinds of honey pots was provided by Fu and Porras.[11] In order to create effective defenses against Honeyed virtual honey pot detections, Fu's study offers a quick assessment of the existing methodologies and procedures.

2.3 Research Summary

After reviewing some research paper I got to know about the importance of honey pot in cyber-attacks. We are aware that they are employed to gather data from unauthorized intruders who have been duped into accessing them by making them seem like a legitimate component of the network. As part of their network defense plan, security teams use these traps.This paper's major objective is to investigate how The Wire

sharkcatch the cyber-attack.By keeping hackers' focus off of your sensitive data, a honeypot can be a useful tool for securing your personal network. With careful use of this tool, you may strengthen your home network's defenses. Additionally, this study focuses on investigating and putting a current, successful solution for this classification task the Kf-sensor honey pots.

2.4 Scope of the Problem:

I've reviewed some papers & articles. There they mentioned & applied different approaches. But I installed the wire shark& KF-Sensor. So that I can see how they can protect my network from cyber security.

2.5 Challenges:

I've installed The wire shark. But I've a little amount of knowledge aboutHoney pots. So I've to gain more knowledge and practice more & more on those.

On the other hand there was another difficulties that wasthe Kf-Sensor. It was very challenging for to install & take screenshots from it. A few attacks have been seen to appear more frequently in the literature at each stratum. One of the most well-known attacks is MAC flooding, which can target any device in the DER environment that uses Ethernet at the Data Link layer and has a valid MAC address. These devicesinclude but are not limited to synchrophasors, network switches, routers, control systems, smart meters, and other communication gateways. The most effective measures now advocated by the industry to stop such attacks include port security, which takes the form of hardening unused ports and predefining the number of MAC addresses on a specific switch port.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

In this part, I will quickly describe the steps I took to accomplish our study project. A honey pot is composed of numerous tools, programs, and utilities. On a network protected by a firewall, the IDS itself will open a port. This permits access to the Honeypot while safeguarding the security of the rest of the network. I've used Wire shark and KF-Sensor for my project.

3.2 Project Setup:

Table 3.1: Setup for my Project

Mandatory	Optional
IDS	Graphing tool
Capture Tool	Secondary Capture tool
Database	TCP Viewer
Data Miner	Database GUI

Honeypot IDS is the design that combines the best elements of honey pot and intrusion detection systems. The study suggests a three-step honey pot IDS design for rogue access point detection and prevention. The suggested architecture is schematically represented in Figure 1 and is comprised of three phases: filtering, intrusion detection, and honey pot. Unauthorized accesspoints are filtered in the first phase using a filtering component. But it's possible that either an attacker is utilizing an approved AP (inadvertently established and hacked access point) or that they spoof the MAC address of the legal access point using Address Resolution Protocol (ARP)spoofing [19]. The packet will then be sent to

the intrusion detection system after passing through the filtering phase in this scenario. Wire shark [21], and Snort [22] are used in the following step to filter out illegal hosts and to identify different assaults. Here I had to maintain some steps:

1. All visible wireless access points are examined by the filter for their MAC addresses. Any router with a mismatched MAC address is considered to be an unauthorized access point, and the request is rejected.

2. After making it through the first stage, the request is sent to an intrusion detection system, where Wire shark was used to analyze the packets' contents and characteristics.
    - **WireShark [17]:** As the preferred network packet capture tool, Wire shark is one of the most helpful tools for IT professionals. You may capture network packets with Wire shark and view them in detail. You can utilize these packets for offline or real-time analysis after they have been deconstructed. With the help of this application, you can examine your network traffic in detail, filter it, and dive down to find the source of any issues. [17]. This tool also helps with network analysis and, eventually, network security. You can learn how to collect, decipher, filter, and inspect data packets using this free Wire shark tutorial to efficiently troubleshoot.

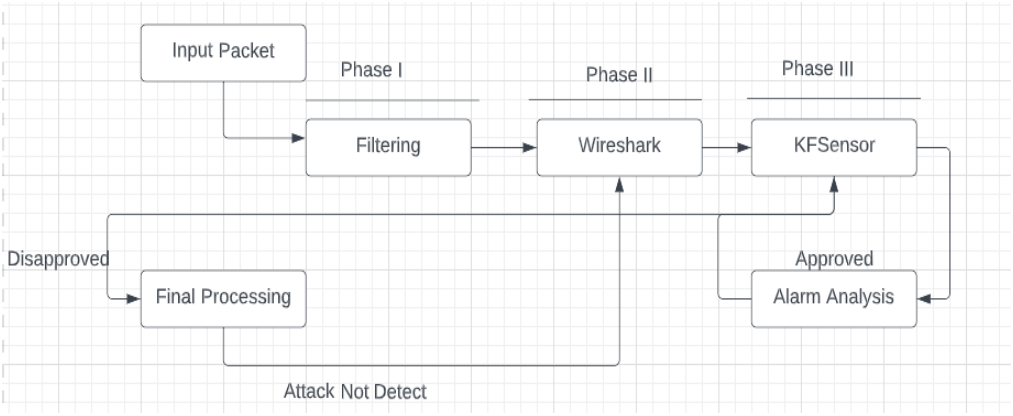


Figure 3.2: Flow chart Proposed Honeypots IDS

According to the given flow chart, two conditions may arise here:

1. If IDS classifies a request as approved, move on to the final processing. That means Attack detection results in a false-negative indication. If no assault is found, the statement "true-negative" is used.
2. If the IDS classifier a request as unauthorized, then it will move to the KF-Sensor.

CHAPTER 4

EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Experimental Setup

One authorized Netis Wireless router is attached to this wireless network. This home network consists of three allowed hosts with the IP addresses 127.0.0.1, 192.168.123.1, and 192.168.1.4, a system with all necessary software that is Wire-shark[17], and a KF-Sensor honey pot [18] system with the IP address 192.168.38.33. The attacker connects to this network using a wireless router and attempts to penetrate it with an IP address of 192.168.38.5. Security.

4.2 Result Analysis

The packet enters this step after passing the first phase and is not detected as an attacker. There could be two outcomes here. The packet either originates from an approved host or an unauthorized host. The packet will be screened using Ettercap if it originates from a hostile user. As seen in Fig. 4, Ettercap displays the IP and MAC addresses of each host connected to the wireless network. Here, the attacker who does not employ ARP spoofing will be quickly detected. On the other hand, if the attacker is employing ARP spoofing, this will not be filtered. The experimental system has been subjected to simulated attacks such as MITM, DOS, DNSSpoofing, and Attacks like MITM and DOS cause rapid variations in packet flow rate, which Wire shark and Snort can identify. From the IP address 192.168.38.35, assaults have been launched. Using Wire shark, MITM attacks can be found by creating IO graphs between the number of packets that flow per unit of time. Figure 5 depicts the usual packet flow rate. As inter-packet separation rises when an attacker uses a MITM assault, as seen in Fig. 6, the packet flow rate falls. As shown in Fig. 7, Snort captures additional packet information and generates alarms based on predetermined rules. Figure 7 displays the Snort-generated messages indicating that a wireless network utilizing a Cisco router at IP address 192.168.38.53 is accessing the Google website. Similarly, Fig. 8 displays the Snort-generated alarm messages indicating that the attacker's IP address, 192.168.38.53, is attempting to launch a DOS assault on the

network in order to disable its services. Thus, the third phase of verification receives all questionable packets.

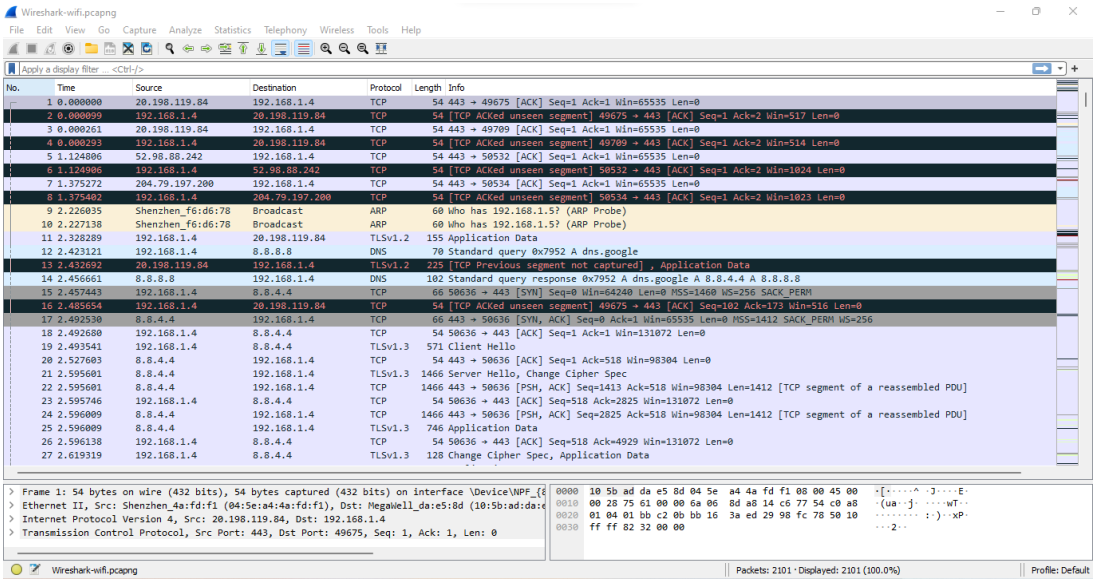


Figure 4.1: Snapshot of Wire shark showing packet rate during an attack

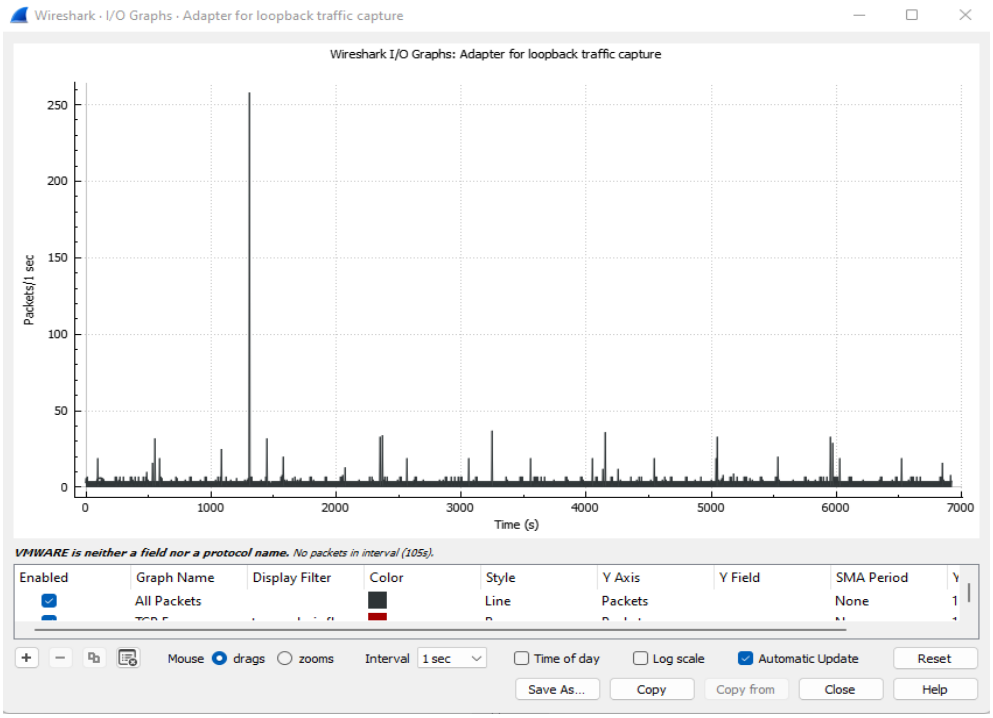


Figure 4.2: Capturing from Adapter for loopback traffic capture

A loopback adapter is a type of network interface that can be used to transfer network traffic from one program to another on the same computer but NOT to any other networked device. Here, I capture for loopback traffic with the help of adapter.

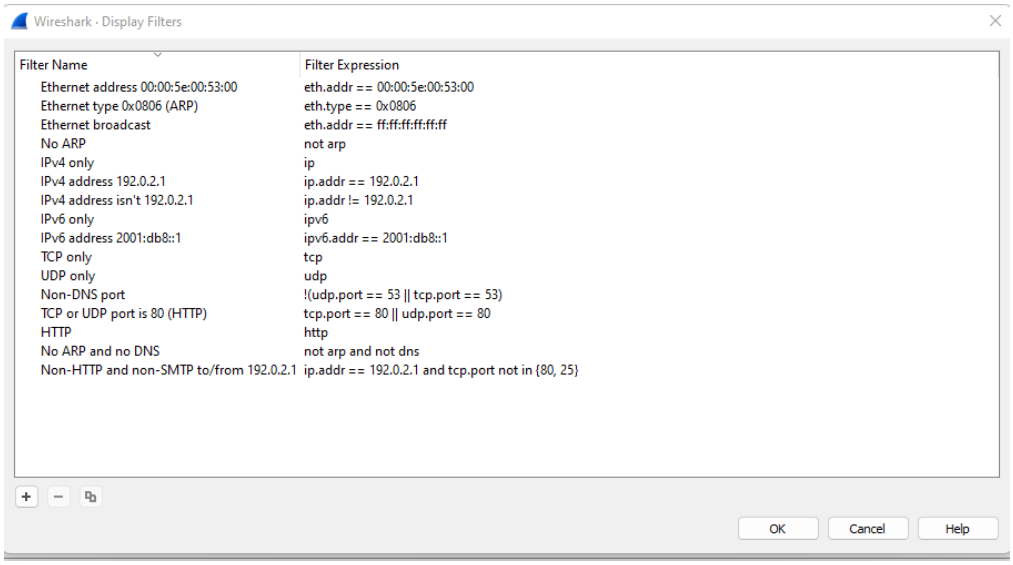


Figure 4.3: Display filter of Wire shark

We can manage the current presentation of packets on Wireshark by using the platform's display filter language. Display filters are frequently used to confirm the existence of a protocol or field. They can also be used to compare packets using logical operators like "and" and "or," though. On the other hand we can precisely manage which packets are displayed with Wireshark's display filter language. They can be used to determine whether a protocol or field is present, its value, or even to compare two fields to one another. In response to the text I have entered in the display filter, Wireshark provides a list of suggestions. The expression has not yet been accepted, and the show filter bar is still red. The expression has been approved and ought to function properly if the display filter bar becomes green. The expression has been accepted if the display filter bar turns yellow, but it probably won't function as intended.

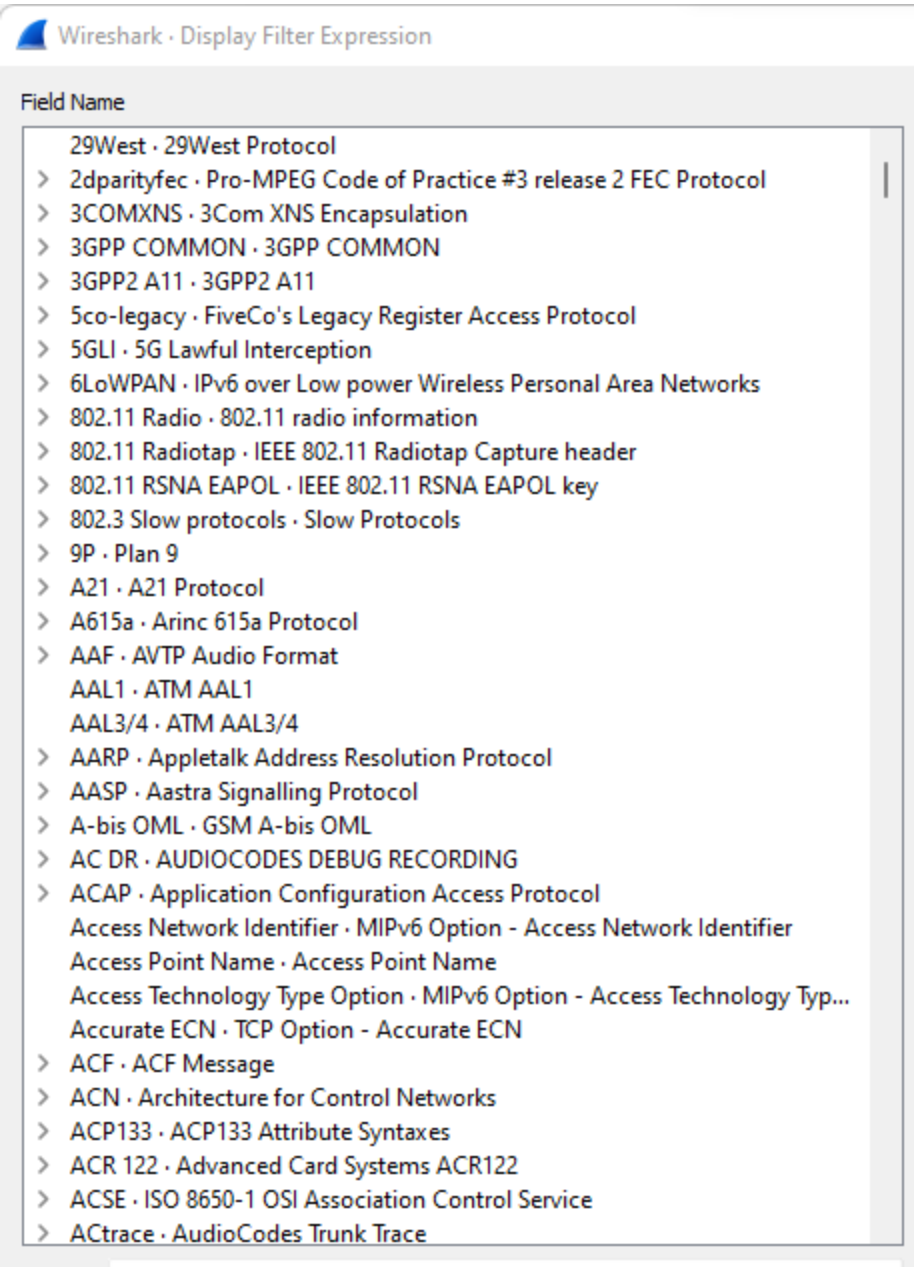


Figure 4.4: Display Filter Expression

I can precisely manage which packets are displayed with Wireshark's display filter language. They can be used to determine whether a protocol or field is present, its value, or even to compare two fields to one another. Complex expressions can be made by combining these comparisons with logical operators like "and" and "or."

KF-Sensor:

In this phase, KF-Sensor is used to scan the suspicious packets that were received from the second phase. A FreeBSD-based open-source firewall and router are called KF-Sensor. Malicious traffic is redirected from Wire-Shark to the KF-Sensor honey pot for an in-depth examination. Figure 6 depicts the router's main pane, which shows system data and the number of interfaces connected to the KF-Sensor honey pot during testing. NAT (Network Address Translation) and rules for rerouting malicious traffic to the KF-Sensor honey pot are required. Prior to creating NAT rules for packet redirection, it first establishes aliases for the destination devices and non-standard destination ports.

KF-Sensor simulates trojans and susceptible system services in order to draw in and find hackers and worms. KF-Sensor comes pre-configured to monitor all ICMP, TCP, and UDP ports. Additionally, it has common services emulated in its configuration. It immediately begins monitoring after installation and is easily customizable to subsequently add more client services.[18].KF-Sensor can reveal the type of attack while preserving ultimate control and minimizing the danger of compromise by reacting with an imitation of real service. KF-Sensor detects and responds to port scans and denial of service (DOS) assaults in addition to targeted service attacks, and it guards against overloading itself. KF-Sensor is able to reveal the type of attack while simultaneously keeping complete control over the occurrence and minimizing the danger of compromise by responding with the imitation of real service. KF-Sensor monitors and responds to individual service attacks as well as port scans and denial of service (DOS) attempts; it also guards against overloading itself.[18]

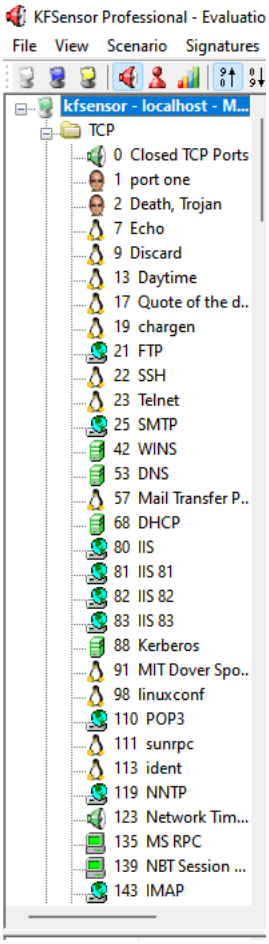


Figure 4.5: Snapshot of the Main scenario of KF-Sensor

As you can see, a list of port numbers and their typical uses are located in the column on the left. If there is a green indicator to the left of a port listing, KF-Sensor is actively monitoring that port.port for assaults If the symbol is blue, there has been a problem and KF-Sensor is not keeping an eye out for exploits targeted at that specific port.

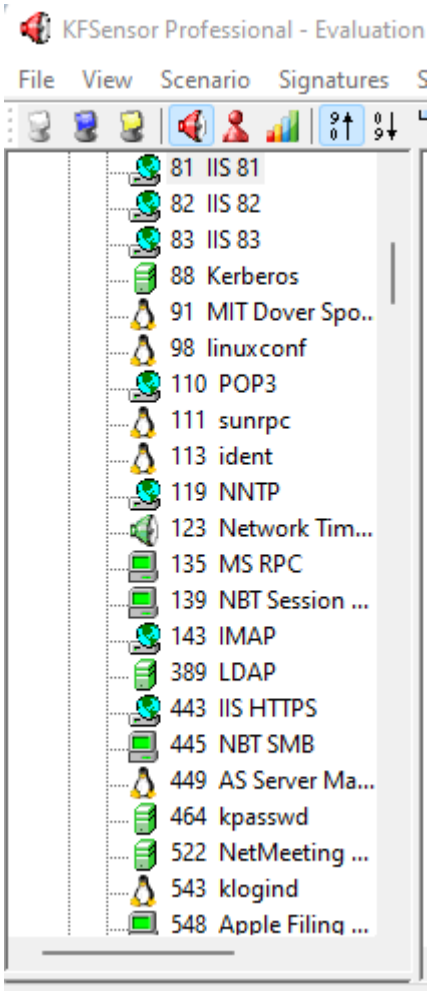


Figure 4.6: Snapshot of the Main scenario of KF-Sensor

If you're wondering why my system displays blue error state icons, it's because I installed KF-Sensor on a Windows 2003 Server that also has a copy of Exchange Server 2003. The error-displaying ports are already in use by Exchange. However, I do not advise running KF-Sensor on an Exchange Server. KF-Sensor is being run on a lab machine, not a server that will be used in a live environment.

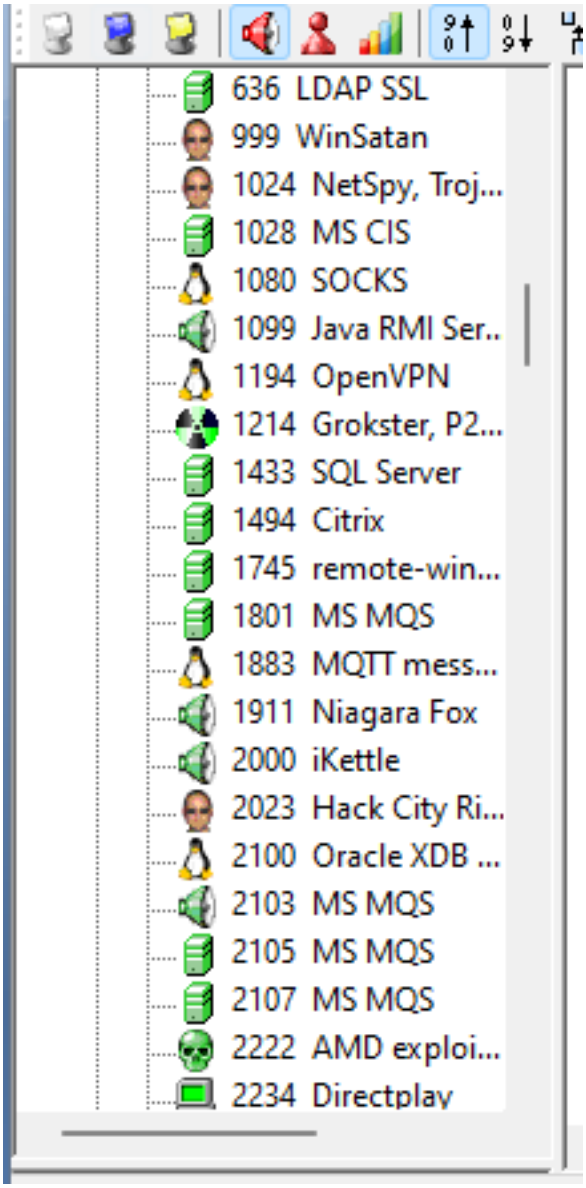


Figure 4.7: Snapshot of the Main scenario of KF-Sensor

One of the finest things you can do after the program is installed and operational is to test it by executing a port scan against the computer hosting KF-Sensor. I'm using a shareware program named HostScan for the port scan that I downloaded from download.com. It only checks a block of IP addresses to see if any ports are open.

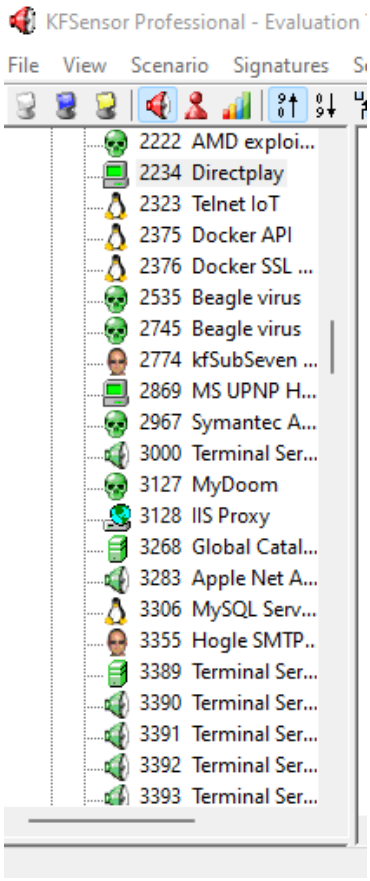


Figure 4.8: Snapshot of the Main scenario of KF-Sensor

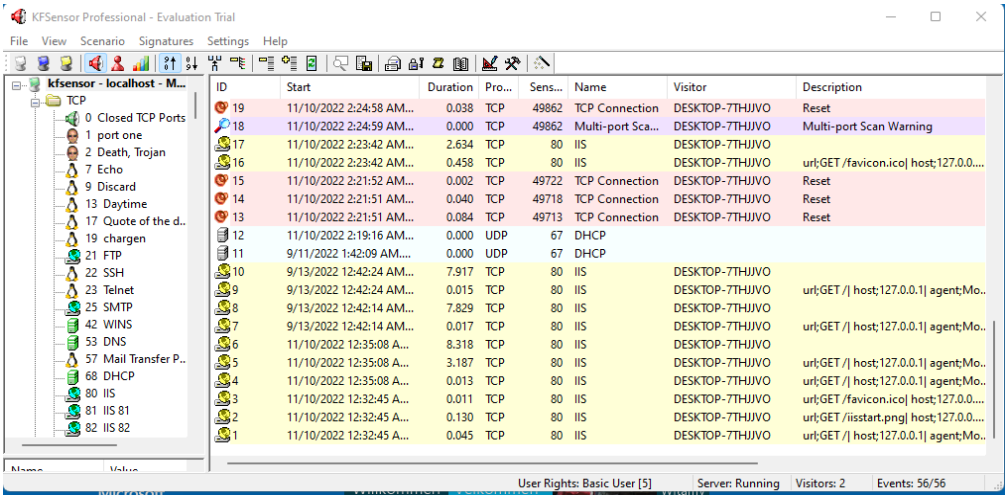


Figure 4.9: Snapshot of DOS Attack detected by KF-Sensor Honeypot

ID	Start	Duration	Pro...	Sens...	Name	Visitor	Description
584	11/24/2022 11:27:19 A...	0.000	UDP	67	DHCP		
583	11/24/2022 10:18:47 A...	0.000	TCP	5985	TCP Closed Port	DESKTOP-7THJJVO	
582	11/24/2022 10:15:14 A...	0.000	TCP	5985	TCP Closed Port	DESKTOP-7THJJVO	
581	11/24/2022 10:14:38 A...	0.000	UDP	67	DHCP		
580	11/24/2022 10:03:48 A...	0.000	TCP	5985	TCP Closed Port	DESKTOP-7THJJVO	
579	11/23/2022 10:17:40 P...	0.000	TCP	5985	TCP Closed Port	DESKTOP-7THJJVO	
578	11/23/2022 3:23:53 PM...	0.000	TCP	5985	TCP Closed Port	DESKTOP-7THJJVO	
577	11/23/2022 10:10:50 A...	0.000	TCP	5985	TCP Closed Port	DESKTOP-7THJJVO	
576	11/23/2022 8:05:34 AM...	0.000	TCP	5985	TCP Closed Port	DESKTOP-7THJJVO	
575	11/23/2022 7:26:10 AM...	0.000	TCP	5985	TCP Closed Port	DESKTOP-7THJJVO	
574	11/23/2022 1:50:26 AM...	0.000	TCP	5985	TCP Closed Port	DESKTOP-7THJJVO	
573	11/23/2022 12:08:56 A...	0.000	TCP	5985	TCP Closed Port	DESKTOP-7THJJVO	
572	11/22/2022 7:07:13 PM...	0.000	TCP	5985	TCP Closed Port	DESKTOP-7THJJVO	
571	11/22/2022 7:06:54 PM...	0.000	UDP	67	DHCP		
570	11/22/2022 12:42:17 P...	0.000	TCP	5985	TCP Closed Port	DESKTOP-7THJJVO	
569	11/22/2022 7:39:37 AM...	0.000	TCP	5985	TCP Closed Port	DESKTOP-7THJJVO	

Figure 4.10: Snapshot of Alert

4.3 Result Discussion

From the capture I got the best results. So now I can say that we can use honey pots in our cyber security problems. From the capture I got the best results. So now I can say that we can use honey pots in our cyber security problems. The first figure illustrates the usual packet flow rate. As inter-packet separation rises when an attacker uses an MITM assault, as seen in Fig. packet flow rate falls. As shown in the figure Snort captures additional packet information and generates alarms based on predetermined rules. Also, displays the Snort-generated messages indicating that a wireless network utilizing a Cisco router at IP address 192.168.38.53 is accessing the Google website. Similarly, displays the Snort-generated alarm messages indicating that the attacker's IP address, 192.168.38.53, is attempting to launch a DOS assault on the network in order to disable its services. All questionable packets are therefore forwarded to the third round of verification. The purpose of KF-Sensor is to defend the genuine thing by acting as a decoy server for the attackers. By opening phony ports on the system where it is installed and gathering data when a connection is made, it fulfills its job flawlessly. This is exactly how a typical server application, such a web server or an SMTP server, accomplishes this. This creates a target, or honeypot server, that will track an attacker's activities. Utilizing KF-Sensor. When I switch on KF-Sensor after downloading and installing it, the dialog below will appear which I've mentioned above.

CHAPTER 5

IMPACT ON SOCIETY, ENVIRONMENTAND SUSTAINABILITY

5.1 Impact on Society

Every human feeling may be linked to the words we view on a daily basis on various online platforms in the digital world. In this case, it is critical for these platforms to have a mechanism in place to discern which are genuine emotions and which are pre-programmed aggressiveness. This is why I've decided to focus on one of the most fascinating genres of all time, By doing so, we can expect to create a more definitive and diverse digital era.

With cyber security measures in place at home, we are fully protected against unauthorized transactions, malware-related data loss, etc. The benefits of cyber security for people are as follows: protection against financial loss, customer data loss, identity theft, and effects on business operations.

5.2 Impact on Environment

Due to the complexity of the network system of openness, sharing of resources, system, linking the variety, the uneven distribution of the terminal, network agnostic, and other barriers, computer networks continue to exhibit their distinctive benefits. Computer's cause. The biggest issue is security, which is one of the numerous issues brought on by the network. Unauthorized access, user impersonation, data integrity destruction, system uptime interference, viruses, malicious attacks, wiretapping, and other safety issues that arise in highly open computer network environments cause significant harm.Cyber-attacks has become a serious issues. Everybody thinks it is a normal issue. But it is not. So that’s why I decided to work on it.

5.3 Ethical Aspects

The internet's media outlets have now become accessible to people of all ages. As a result, the conditions of the user limitations are no longer valid. Because there are insufficient security measures to distinguish between moral and social perspectives. One

must be able to comprehend the overall context of a notion conveyed through platforms. In many circumstances, this has been shown to be harmful to people's moral ideals.

5.4 Sustainability

- There are over 2.3 billion active internet-based life clients worldwide.
- At least two internet-based life cycles are present in 91 percent of large business brands.
- When they can't access their online life profiles, 65 percent of individuals feel uneasy and uncomfortable.
- It will be a helping hand for researcher.
- Able to gain more knowledge about honey pots.

CHAPTER 6

SUMMARY, CONCLUSION, RECOMMENDATION, AND IMPLICATION FOR FUTURE RESEARCH

6.1 Summary of the Study

The purpose of this study was to use a honey pots in cybersecurity. Understanding what honey pots is was first important in order to successfully carry out the research. This topic has been given an overview in order to achieve this. Here, it can be stated that there are various definitions of cyber-attacks, all of which originate from various platforms. Because detecting cyber-attacks falls under the attack detecting, additional literature was examined to better understand the theory underlying honey pots and the use of different techniques.

6.2 Conclusion

With the volume of data that was gathered over the available time period. Because there wasn't really enough variation to get a top-notch result, some of the conclusions may not be totally true or lack clarity or definition. Having said that, the comprehension of the data has much improved, and if more data were collected over a longer period of time, the results would be much better and could even reach a high level.

The use of wireless LAN (802.11) in organizations and the military has dramatically increased over the past several years. As a result, wireless access points are more vulnerable to attacks. The suggested method aims to find all RAPs, beginning with an introduction to Rogue Access Point detection in wireless networks. A rogue access point must be detected and prevented from being installed in order to safeguard wireless networks. In this paper, a novel hybrid approach that combines the best aspects of current honey pots and intrusion detection systems has been proposed. The anticipated concept was put into practice on a modest wireless network. Deploying the model on the cloud and boosting system performance with effective machine learning and optimization approaches are possible future tasks. for preserving a low false alarm rate and honey pot overhead.

6.3 Recommendations

- It will be a contribution.
- More easier.
- More flexible.
- User friendly.

REFERENCES

[1] Kaur, G. and Saini, J. (1970) Implementation of high interaction honeypot to analyze the network traffic and prevention of attacks on protocol/port basis: Semantic scholar, undefined. Available at: https://www.semanticscholar.org/paper/Implementation-of-High-Interaction-Honeypot-to-the-Kaur-Saini/aa715f8f0d3ca1eba0375ffc10204f81a7a17fa4 (Accessed: December 5, 2022).

[2] Nawrocki, M. et al. (1970) [PDF] A survey on honeypot software and data analysis: Semantic scholar, undefined. Available at: https://www.semanticscholar.org/paper/A-Survey-on-Honeypot-Software-and-Data-Analysis-Nawrocki-W%C3%A4hlisch/a5c0c30def10087c3b08935ba4dbe96fec1c9e26 (Accessed: December 5, 2022).

[3] Comparison analysis of Manet routing protocols to identify their ... (no date). Available at: https://www.researchgate.net/profile/Munisha-Devi/publication/331544420_Comparison_analysis_of_MANET_routing_protocols_to_identify_their_suitability_in_smart_environment/links/5c7f39e992851c695058c7b5/Comparison-analysis-of-MANET-routing-protocols-to-identify-their-suitability-in-smart-environment.pdf (Accessed: December 5, 2022).

[4] Hiotpot: Surveillance on IOT devices against recent threats - researchgate (no date). Available at: https://www.researchgate.net/profile/Usha-Gandhi/publication/322649716_HIoTPOT_Surveillance_on_IoT_Devices_against_Recent_Threats/links/5cc28b14299bf120977f95f9/HIoTPOT-Surveillance-on-IoT-Devices-against-Recent-Threats.pdf (Accessed: December 5, 2022).

[5] Yeh, C.-H. and Yang, C. (1970) Design and implementation of honeypot systems based on open-source software: Semantic scholar, undefined. Available at: https://www.semanticscholar.org/paper/Design-and-implementation-of-honeypot-systems-based-Yeh-Yang/23f4e840a3d24697a134ce31a56f9da02f994c27 (Accessed: December 5, 2022).

[6] Honeypot-based Defense System Research and Design | IEEE Conference ... (no date). Available at: https://ieeexplore.ieee.org/document/5234504 (Accessed: December 5, 2022).

[7] Mai, Y., Upadrashta, R. and Su, X. (1970) J-honeypot: A Java-based network deception tool with monitoring and intrusion detection: Semantic scholar, undefined. Available at: https://www.semanticscholar.org/paper/J-Honeypot%3A-a-Java-based-network-deception-tool-and-Mai-Upadrashta/53256d785c1d10d78306acfe16b9c56d29572214 (Accessed: December 5, 2022).

[8] Kwama Leonard Ogweno, Obare Erick Oteyo, Dola Ochieng' henry (no date). Available at: http://www.ijeijournal.com/papers/Vol.4-Iss.5/E04_05-2841.pdf (Accessed: December 5, 2022).

[9] Employee personal page warning - USDA (no date). Available at: https://www.nfc.usda.gov/epps (Accessed: December 5, 2022).

[10] Almutairi, A., Parish, D. and Phan, R. (2012) survey of High Interaction Honeypot tools merits and shortcomings. proceedings of the 13th Annual post-graduate symposium on the convergence of telecommunications, networking and broadcasting, liver-pool, 25-26 june 2012. - references - scientific research publishing. Available at: https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/referencespapers.aspx?referenceid=3300142 (Accessed: December 5, 2022).

[11] Singh, A., Dhaka, V. and Singh, G. (1970) Comparative analysis of dynamic path maintenance routing protocols for mobile ad-hoc networks: Semantic scholar, undefined. Available at: https://www.semanticscholar.org/paper/Comparative-Analysis-of-Dynamic-Path-Maintenance-Singh-Dhaka/0e7a02967b9bcf05287d9c7d68bbfb3a805d7437 (Accessed: December 6, 2022).

[12] What is a trojan virus & how to protect (no date) Webroot. Available at: https://www.webroot.com/us/en/resources/tips-articles/what-is-trojan-virus (Accessed: December 6, 2022).

[13] Limited, S. (no date) Bad rabbit ransomware: What is it?, SiteLock. Available at: https://www.sitelock.com/blog/what-is-bad-rabbit-ransomware/ (Accessed: December 6, 2022).

[14] CyberGlossary guide and definitions (no date) Fortinet. Available at: https://www.fortinet.com/resources/cyberglossary (Accessed: December 6, 2022).

[15] Chris Brook on Wednesday December 5, Brook, C. and Lord, N. (no date) What is Macro malware?, Digital Guardian. Available at: https://digitalguardian.com/blog/what-macro-malware (Accessed: December 6, 2022).

[16] What is wireshark and how to use it: Cybersecurity: Comptia (no date) Default. Available at: https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it (Accessed: December 6, 2022).

[17] Ltd., K.F. (no date) Kfsensor. Available at: https://www.kfsensor.net/kfsensor/ (Accessed: December 6, 2022).

[18] Preventing ARP spoofing in WLAN using SHA-512 (no date). Available at: https://www.researchgate.net/profile/Pradeepkumar-Bhale/publication/269328524_Preventing_ARP_spoofing_in_WLAN_using_SHA-512/links/5a3e4f20aca272d29444ae3f/Preventing-ARP-spoofing-in-WLAN-using-SHA-512.pdf (Accessed: December 5, 2022).

[19] Kamel, N.E. et al. (1970) [PDF] a smart agent design for cyber security based on Honeypot and machine learning: Semantic scholar, undefined. Available at: https://www.semanticscholar.org/paper/A-Smart-Agent-Design-for-Cyber-Security-Based-on-Kamel-Eddabbah/ad300b515191bb8d95369d7e99185a1d4d81baa8 (Accessed: December 6, 2022).

[20] Imperva Learning Center (2022) Learning Center. Available at: https://www.imperva.com/learn/ (Accessed: December 6, 2022).

[21] CyberGlossary guide and definitions (no date) Fortinet. Available at: https://www.fortinet.com/resources/cyberglossary (Accessed: December 6, 2022).

[22] Imperva Learning Center (2022) Learning Center. Available at: https://www.imperva.com/learn/ (Accessed: December 6, 2022).

[23] Tutorial: Build your First project (no date) Tutorial: Build your first project - Sphinx documentation. Available at: https://www.sphinx-doc.org/en/master/tutorial/index.html (Accessed: December 6, 2022).

[24] Wallarm (no date) What is a cyber attack? definition,types and prevention, RSS. Available at: https://www.wallarm.com/what/what-is-a-cyber-attack (Accessed: December 6, 2022).

[25] Fundamentals (no date) Rapid7. Available at: https://www.rapid7.com/fundamentals/ (Accessed: December 6, 2022).

[26] Types of cyber attacks - javatpoint (no date) www.javatpoint.com. Available at: https://www.javatpoint.com/types-of-cyber-attacks (Accessed: December 6, 2022).

CYBER

ORIGINALITY REPORT

20%	7%	1%	15%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	link.springer.com Internet Source	3%
2	Submitted to uwe Student Paper	3%
3	Submitted to University of Greenwich Student Paper	3%
4	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	2%
5	Submitted to Middlesex University Student Paper	1%
6	Submitted to Sim University Student Paper	1%
7	dspace.daffodilvarsity.edu.bd:8080 Internet Source	1%
8	Submitted to CTI Education Group Student Paper	1%
9	Submitted to Purdue University Student Paper	1%