

UNIVERSITY OF BAHRAIN

College of Information Technology



Zero-day Attacks Detection Using Threat Hunting Intelligence Approach

A Thesis Submitted in Partial Fulfilment of the Requirements for the
Masters of Sciences Degree in Cybersecurity

Submitted By

Yusuf Almahmeed

University ID: 20151648

Supervised By

Dr. Alauddin Al-Omary

Associate professor

University of Bahrain

April 2023



Dissertation Deposit Form

Author Name:	Yusuf Salah Almahmeed		
Email:	20151648 @stu.uob.edu.bh	Contact No:	39197117
College:	Information Technology		
Department:	Computer Science		
Thesis Title:	Detection Using Deception and Threat Hunting Intelligence Approach earning Technique		
Year:	2023		

Author's Declaration: I agree to the following conditions:

The above thesis will be available (in the University of Bahrain library and externally) and reproduced as necessary at the discretion of the University of Bahrain. It may also be digitized by the University of Bahrain and made available via the university's repository or via other parties on the Internet.

This condition shall apply to ALL copies including electronic copies.

The above thesis has been provided on the understanding that it is copyright protected material and that no quotation from this thesis may be published without proper acknowledgement.

Signature of the Author:		Date:	25-Jun-23
--------------------------	--	-------	-----------

DECLARATION

I declare that this work is the result of my own investigation and that it has not already been accepted in substance for any degree, nor is it currently submitted for any degree.

Signed:  Date: 25/06/2023

Yusuf Salah Almahmeed

The Thesis defense committee considers the thesis titled:

Zero-day Attacks Detection Using Deception and Threat Hunting Intelligence Approach

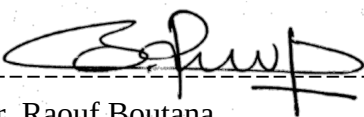
Submitted by Yusuf Salah Almahmeed to the College of Information Technology is satisfactory and acceptable for the Master of Science in Cyber Security.

The Defense Committee:



Dr. Alauddin Al-Omary
(Supervisor)

Department of Computer Engineering
University of Bahrain



Dr. Raouf Boutana
(External Examiner)

University of Waterloo, Canada



Dr. Wael Elmedany
(Internal Examiner)

Department of Computer Engineering
University of Bahrain

ABSTRACT

The swift progression of technology has resulted in a proportional expansion of the attack surface, presenting notable obstacles in the field of threat management and mitigation. Zero-day attacks are widely known as one of the most powerful forms of attacks to address. Zero-day attacks refer to cyber attacks that take advantage of software or hardware vulnerabilities that are not yet recognized by the security vendor. Conventional security measures, including firewalls and antivirus software, may prove inadequate in preventing attacks in instances where the vendor has not yet issued any patches or fixes for the identified vulnerabilities. Consequently, there is a pressing need for more sophisticated detection techniques. The utilization of deception techniques entails the creation of fake systems or data with the aim of attract attackers to expose their presence. Conversely, threat hunting intelligence involves the proactive exploration of potential threats. The present study proposes a methodology that integrates the aforementioned techniques to help the identify zero-day attacks. The efficacy of this methodology is assessed via experiments employing real attack scenarios. The findings indicate that the suggested methodology has the potential to considerably enhance the detection efficacy of zero-day attacks, thereby presenting a viable solution to augment cybersecurity in the wake of swiftly changing security threats.

Contents

APPROVAL	A
DECLARATION	C
ABSTRACT	E
TABLE OF CONTENTS	F
LIST OF FIGURES	I
LIST OF TABLES	K
ACKNOWLEDGMENTS	L
DEDICATION	M
PUBLICATIONS	N
LIST OF ABBREVIATIONS	O
1 Introduction	1
1.1 Overview	1
1.2 Background	2
1.3 Research Problem	3
1.4 Research Objectives	3
1.5 Threat Hunting Intelligence and Traditional Techniques in Detecting Zero-Day Attacks	5
1.6 Contribution to the Field	6
1.7 Thesis Outline	7
2 Literature Review	8
2.1 Literature Review	8

2.1.1	Artificial Intelligence Approaches	9
2.1.2	Deception Approaches	13
2.1.3	Hybrid Approaches	16
2.2	Summary	20
3	Methodology	22
3.1	Introduction	22
3.2	Research Questions	23
3.3	Data collection and analysis	25
3.4	Framework development	27
3.5	Evaluation methods	28
3.6	Description of the proposed framework	30
3.6.1	Strategical Threat Hunting Intelligence	31
3.6.2	Operational Threat Hunting Intelligence	32
3.6.3	Tactical Threat Hunting Intelligence	32
3.6.4	Technical Threat Hunting Intelligence	33
3.6.5	Deception	34
3.7	Components of the framework	35
3.7.1	Management Staff Role	36
3.7.2	Operation Staff Role	37
3.7.3	Technology used	38
3.7.4	Environment Design	39
3.7.5	Implementation	40
3.8	Summary	62
4	Results and Evaluation	63
4.1	Introduction	63
4.2	Description of the evaluation methodology	63
4.3	Results of the evaluation	64
4.4	Discussion of the results	70

4.5	Summary	71
5	Discussion and Analysis	72
5.1	Analysis of the research findings	72
5.2	Discussion of the research implications and limitations . . .	73
5.2.1	Cost	73
5.2.2	Complexity	75
5.2.3	Data	76
5.2.4	Protection Scope	77
5.2.5	Time	78
5.3	Summary	79
6	Conclusion	80
6.1	Summary of the research findings	80
6.2	Future research directions	81
	References	82
	Abstract (in Arabic)	

List of Figures

3.1	Evaluation Flow	30
3.2	SANS survey results	31
3.3	The Main Components of the framework	35
3.4	Threat Hunting Intelligence Approaches	40
3.5	Certificate Domains	41
3.6	Certificate Details	41
3.7	DNS Domain Details	42
3.8	DNS Records	42
3.9	MHN VPC Details	43
3.10	MHN Subnets Details	43
3.11	MHN Route Table Details	45
3.12	MHN IGW Details	46
3.13	EIP Details	47
3.14	Mirror Inbound Filter Details	49
3.15	Mirror Outbound Filter Details	49
3.16	Mirror Target Details	50
3.17	Mirror Sessions Details	50
3.18	Web Servers Target Group Details	53
3.19	Honeypot Target Group Details	53
3.20	MHN ALB Details	53
3.21	MHN ALB Listener Details	54
3.22	MHN ALB Listener Rules Details	54

3.23	Users Table Details	57
3.24	Servers Table Details	58
3.25	Web Server Configuration	59
3.26	Active Directory OU Details	60
3.27	Honeypot Server Configuration	61
4.1	Security Onion 2 High Severity Alerts	66
4.2	NMAP Scan Alert Details	66
4.3	EternalBlue Probe MS17-010 (Generic Flags) Alert Details .	67
4.4	EternalBlue Probe MS17-010 (MSF style) Alert Details . . .	67
4.5	EternalBlue Probe MS17-010 Echo Response Alert Details .	67
4.6	EternalBlue Exploit M2 MS17-010 Alert Details	68
4.7	MVPower DVR Shell UCEs Alert Details	68
4.8	JAWS Webserver Unauthenticated Shell Command Execu- tion Alert Details	69
4.9	Mirai Variant User-Agent Scan Alert Details	69
4.10	Basic Auth Base64 HTTP Password detected unencrypted Alert Details	69
5.1	February 2023 Bill	74
5.2	March 2023 Bill	74
5.3	April 2023 Bill	75
5.4	May 2023 Bill	75

List of Tables

3.1	AWS Servers	51
3.2	AWS Servers Specifications	51
3.3	Security Groups	56
3.4	Active Directory Users	61
4.1	Survey Results	65

ACKNOWLEDGMENTS

I would like to express my deep appreciation to Dr. Alauddin Al-Omary for his valuable guidance and support throughout my thesis project. His expertise and encouragement have been invaluable in shaping the direction of my research, and I am grateful for the opportunity to work with him.

DEDICATION

To my parents, who have always been my guiding light and a source of unwavering support. This thesis project is a testament to your love, encouragement, and sacrifices. Thank you for everything.

PUBLICATIONS

CONFERENCE PAPER

1. (Published) Y. S. AlMahmeed and A. Y. Al-Omay, "Zero-day Attack Solutions Using THI: Extensive Survey," 2022 International Conference on Data Analytics for Business and Industry (ICDABI), Sakhr, Bahrain, 2022, pp. 309-314

URL: <https://ieeexplore.ieee.org/document/10041568>

LIST OF ABBREVIATIONS

THI	Threat Hunting Intelligence
SOC	Security Operations Center
AWS	Amazon Web Services
IOC	Indicators Of Compromise
TTP	Tactics, Techniques, and Procedures
EC2	Elastic Compute Cloud
VPC	Virtual Private Cloud
VPC	Classless Inter-Domain Routing
IP	Internet Protocol
IGW	Internet Gateway
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
ALB	Application Load Balancer
DNS	Domain Name System
ACM	AWS Certificate Manager
URL	Uniform Resource Locator
MHN	Managed Honeypot Network

HTML Hypertext Markup Language

PHP Hypertext Preprocessor

Chapter 1

Introduction

1.1 Overview

The main objective of this research is to tackle the issue of identifying zero-day attacks through the introduction of a new methodology that merges deception and threat hunting intelligence. The proposed strategy entails the development of a hybrid system that incorporates a decoy mechanism that tricks potential attackers into revealing their presence, as well as their techniques, tactics, and procedures. The system has been developed to replicate an authentic system and includes with a range of traps and enticements to mislead intruders. while actively monitors the network for indications of abnormal behaviors and employs advanced analytics to identify unusual anomaly, as an aspect of its threat hunting methodology. The study employs real-world experiments to assess the effectiveness of the suggested methodology. The findings indicate that the methodology exhibits a high degree of effectiveness in identifying zero-day attacks, as evidenced by a high rate of detection and minimal number of false positives. The thesis provides a noteworthy contribution to the domain of cybersecurity by tackling the issue of detecting zero-day attacks, which is a crucial concern in the modern digital world. The suggested methodology presents a practical and efficient improvement that enterprises can employ to safeguard their systems and in-

formation against these highly damaging attacks.

1.2 Background

Zero-day exploits refer to a type of cyber attacks that exploit undisclosed vulnerabilities in software or hardware. Frequently, these vulnerability are detected by individuals with malicious intent, commonly referred to as hackers, who subsequently create and implement methods to gain entry into systems without proper authorization, exfiltrate confidential information, or inflict other types of harm. Zero-day vulnerabilities have the potential to be traded illegally on underground marketplaces or leveraged by state-sponsored threat actors for the purposes of conducting cyber espionage.

In recent years, there has been a rise in both the frequency and complexity of zero-day exploits. This trend has been observed in the context of attacks that are directed towards high-value targets, including critical infrastructure. The significance of proactive measures, such as threat hunting intelligence and deception techniques, in the identification and mitigation of these types of attacks is highlighted in the literature (Shejin & Sudheer, 2023).

Examples of the ramifications of zero-day exploits include the following:

The WannaCry ransomware attack focused on a security vulnerability in Microsoft Windows that had been utilized by the US National Security Agency (NSA) and later revealed to the general public. The hackers successfully leveraged the exploit to propagate ransomware throughout a multitude of systems, resulting in extensive disturbances and financial impacts (Nayak, Tiwari, & Samanthula, 2023).

The Equifax data breach was the result of a security vulnerability in the Apache Struts web application framework that was exploited by malicious actors to obtain confidential information pertaining to a vast number of in-

dividuals (McLoughlin, 2023).

The SolarWinds supply chain attack, a carefully executed cyber intrusion, was brought to light in December of 2020. According to a report on software supply chain attacks, various government agencies and private companies were compromised as a result of attackers exploiting a zero-day vulnerability in the SolarWinds Orion IT management software (Jakob, 2023).

The escalating frequency and magnitude of zero-day exploits underscore the need for entities to embrace preemptive security measures and remain attentive in response to this growing danger.

1.3 Research Problem

Zero-day attacks pose a considerable risk to enterprises, as they leverage security loopholes that remain undisclosed to the security community. The efficacy of conventional security measures in thwarting such attacks is frequently inadequate, rendering their detection and prevention a formidable task. Hence, the main goal of the research lies in devising efficacious methodologies to detect zero-day attacks with the aim of enhancing organizational security. (R. Ahmad, Alsmadi, Alhamdani, & Tawalbeh, 2023).

1.4 Research Objectives

The aim of this study is to propose a Framework methodology that integrates the deception with threat hunting intelligence techniques to detect zero-day attacks. The aforementioned goal will be achieved by means of the following specified objectives:

1. Examine the present status of zero-day attacks and their impact on organizations. The aim of this objective is to perform a thorough ex-

amination of the extant literature related to zero-day attacks in order to determine their extent, and potential consequences for organizations.

2. Examining the notions of deception and threat hunting intelligence (THI) and their viability in the identification of zero-day attacks. This study's aim entails an examination of the notions of deception and THI and their potential use for the detection of zero-day attacks. The present study includes a comprehensive analysis of the extant literature related to the use of deception and THI in detecting zero-day attacks, along with an investigation into their benefits, limitations and efficiency.
3. Propose a framework that utilizes deception and THI methodologies in order to identify zero-day attacks. The process involves the recognition of fundamental components of the framework, such as the roles of organizational personnel, the technological aspects employed in the proof of concept, and the design and execution of the POC environment.
4. Assessing the efficacy of the proposed framework in detecting zero-day attacks. The present aim entails the execution of a proof of concept (POC) to evaluate the efficacy of the suggested framework in identifying zero-day attacks. The proof of concept (POC) will entail the simulation of multiple attacks within a controlled setting, followed by an comparison with other state of the art solutions to determine the framework's efficacy in detecting and responding to these attacks.

The primary objective of this thesis is to make a valuable contribution towards the advancement of security solutions that are more efficient in detecting zero-day attacks. The research focuses on the utilization of deception and THI techniques. The achievement of these objectives will provide significant perspectives and recommendations for entities

seeking to improve their cybersecurity posture and safeguard against the escalating danger of zero-day attacks.

1.5 Threat Hunting Intelligence and Traditional Techniques in Detecting Zero-Day Attacks

In the context of detecting zero-day attacks, the utilization of threat hunting intelligence presents a superior and proactive methodology in contrast to conventional techniques. Zero-day attacks are intended to take advantage of computer system vulnerabilities that are still unknown. Therefore, such attacks frequently do not correspond to any existing signatures or patterns that are relied upon by conventional detection solutions.

The practice of threat hunting intelligence entails the proactive pursuit and detection of possible security risks through the utilization of sophisticated analytics. Through the examination of extensive data collected from diverse sources such as network traffic, logs, and endpoint devices, the practice of threat hunting intelligence has the capacity to detect irregularities and trends that may signify the existence of a zero-day attack. The adoption of a proactive approach enables organizations to identify zero-day attacks in real-time, thereby mitigating the potential for significant harm.

Conversely, conventional methods of detecting zero-day attacks, such as intrusion detection and intrusion prevention systems, depend on established signatures or behavioral patterns to detect possible hazards. Zero-day attacks are capable of evading detection by existing systems due to their lack of complying to established signatures or patterns.

It is noteworthy that conventional methods of detection can still serve a purpose in identifying attacks through the recognition and prevention of established attack vectors or suspicious conduct. Furthermore, the utilization of deception tactics such as honeypots can prove to be efficacious in

the identification of zero-day attacks by enticing malicious actors to expose their identities.

In general, although conventional detection methods retain their utility in identifying zero-day attacks, the implementation of threat hunting intelligence presents a superior and proactive strategy that can enhance an organization's capacity to safeguard against such threats.

1.6 Contribution to the Field

The implementation of deception and threat hunting and intelligence (THI) techniques for the detection of zero-day attacks is a noteworthy contribution to the domain of cybersecurity. Zero-day attacks pose a significant risk to enterprises since they exploit security loopholes that are yet to be discovered by the security experts. Conventional cybersecurity measures, such as firewalls and antivirus software, are insufficient in identifying and thwarting such attacks, rendering it arduous to safeguard against them.

Deception techniques encompass the creation of an environment that is intentionally misleading, with the aim of inducing attackers to commit errors, thus exposing their strategies and motives. On the contrary, Threat Hunting Initiative (THI) entails proactively seeking out indications of malevolent operations within the network of an enterprise. Both methodologies possess the capability to detect zero-day attacks that could have evaded conventional security measures.

This thesis makes a significant contribution to the field of cybersecurity by introducing a framework that incorporates deception and THI to identify zero-day attacks. Initially, it offers a more efficient methodology for identifying zero-day attacks, thereby mitigating the likelihood of data breaches and other cybersecurity occurrences. Furthermore, it underscores the significance of proactive security measures, such as Threat Hunting and Intelli-

gence (THI), which are frequently disregarded in conventional cybersecurity methodologies.

The implementation of the framework can enhance the resilience of organizations against zero-day attacks by facilitating the identification and mitigation of such attacks prior to their infliction of substantial harm. The fourth point pertains to the potential of the proposed framework to function as a fundamental basis for future investigations concerning the utilization of deception and THI in the realm of cybersecurity.

To summarize, the implementation of deception and THI techniques for the detection of zero-day attacks constitutes a significant contribution to the domain of cybersecurity. The framework under consideration exhibits the capacity to enhance the security of institutions by identifying zero-day attacks that conventional security measures frequently overlook, thus mitigating the likelihood of data breaches and other cybersecurity incidents.

1.7 Thesis Outline

The forthcoming sections of this thesis will begin with a literature review that will analyze the current state-of-the-art solutions proposed for detecting zero-day attacks. Subsequently, the methodology section will outline the methodology employed in this study, followed by a framework section that will describe the proposed framework. The results and evaluation section will undertake a discussion of the proposed solution findings and results, followed by a discussion and analysis of the project findings. Lastly, a conclusion section will provide a brief summary of the findings, in addition to outlining future work.

Chapter 2

Literature Review

2.1 Literature Review

The scholarly discourse pertaining to the identification of zero-day attacks through the utilization of deception, THI, machine learning, and other techniques is expanding at a swift pace. Diverse frameworks, algorithms, and methodologies have been suggested by researchers to address this issue. The objective of this literature review is to present a comprehensive summary of the existing research in this field, emphasizing the advantages and drawbacks of various methodologies. This literature review aims to investigate the potential of deception and threat hunting intelligence (THI) in detecting zero-day attacks and evaluate their efficacy in comparison to conventional security measures.

2.1.1 Artificial Intelligence Approaches

Bu and Cho have introduced a novel approach for the identification of zero-day phishing attacks. The approach combines the principles of deep learning with constraints programmed in first-order logic. The technique of deep learning is employed for the purpose of acquiring knowledge about the characteristics of URLs that are associated with phishing activities. Programmed constraints in first-order logic are utilized to represent domain expertise pertaining to phishing attacks. By utilizing a fusion of deep learning and first-order logic programmed constraints, the technique exhibits a remarkable ability to accurately identify zero-day phishing attacks. The methodology incorporates a convolutional neural network (CNN) as its deep learning component. The Convolutional Neural Network (CNN) has been trained using a dataset comprising of URLs associated with phishing activities. The Convolutional Neural Network (CNN) acquires the ability to extract distinctive features from URLs that are indicative of phishing attacks. The method's first-order logic programmed constraints component serves to encode domain knowledge pertaining to phishing attacks. The domain knowledge encompasses details pertaining to the composition, substance, and conduct of phishing URLs. By utilizing a fusion of deep learning and first-order logic programmed constraints, the approach exhibits a remarkable ability to identify zero-day phishing attacks with a high degree of precision. The deep learning module incorporated in the methodology is proficient in extracting distinctive characteristics from phishing URLs that serve as reliable indicators of phishing attacks. The method's component that employs first-order logic programmed constraints has the capability to eliminate erroneous outcomes. The method proposed exhibits promise as a novel approach to identifying zero-day phishing attacks. The approach exhibits a notable capability in identifying nascent phishing attacks with a considerable degree of precision. Additionally, it possesses a low computational overhead and can be

implemented on devices with limited resources (Bu & Cho, 2021).

The utilization of unsupervised algorithms for the identification of zero-day attacks was examined by Zoppi et al. Unsupervised algorithms function by detecting anomalous patterns within data. This technique can be employed to detect and classify attacks that are unfamiliar to the defender. The scholars deliberated on several unsupervised algorithms that have the potential to identify zero-day attacks. The challenges associated with utilizing unsupervised algorithms for the detection of zero-day attacks were also deliberated by the authors. A notable obstacle pertains to the sensitivity of algorithms towards noise present in the data. An additional obstacle pertains to the computational expense of the algorithms. Notwithstanding the difficulties, the authors contended that unsupervised algorithms possess the potential to serve as a valuable instrument for the identification of zero-day attacks. The study conducted by the authors involved the utilization of unsupervised algorithms for the identification of zero-day attacks in a practical context. The findings of the case study indicate that unsupervised algorithms possess the capability to detect zero-day attacks with efficacy, thereby presenting a promising approach for safeguarding against such attacks. Nevertheless, the authors acknowledge the need for further research in this domain (Zoppi, Ceccarelli, & Bondavalli, 2021).

Mbona and Eloffi propose a semi-supervised machine learning methodology that leverages Benford's law to discern noteworthy characteristics that serve as indicators of zero-day attacks. Semi-supervised machine learning methodologies amalgamate both supervised and unsupervised learning paradigms. The application of supervised learning involves the acquisition of knowledge from labeled data, whereas unsupervised learning involves the acquisition of knowledge from unlabeled data. The integration of various pedagogical methodologies can be employed to enhance the identification of zero-day assaults. Benford's law is a statistical principle which posits

that the initial digit of a numerical value is not uniformly distributed. This technique has the potential to detect aberrant actions in the transmission of data across a network. The proposed methodology is assessed through the utilization of the NSL-KDD dataset. The findings indicate that the suggested methodology has the capability to attain a substantial level of detection accuracy for zero-day attacks. The advantages and disadvantages of the proposed approach were also deliberated upon by the authors. The approach boasts of notable benefits such as a superior detection rate and the capability to identify zero-day attacks that are unfamiliar to the defender. The approach is associated with certain drawbacks, such as its dependence on annotated data and its intricate computational requirements (Mbona & Eloff, 2022).

Tang and colleagues introduced a novel methodology for identifying web-based zero-day attacks. The methodology is founded upon the notion that zero-day assaults frequently exhibit syntactic and semantic dissimilarities from innocuous solicitations. ZeroWall employs a self-translation mechanism to acquire knowledge of the syntax and semantics of non-malicious requests. ZeroWall performs real-time translation of a novel request by first converting it into a latent representation and subsequently reconvert-ing it into an output request. A zero-day attack is identified when the output request differs from the input request. The performance of ZeroWall was assessed using a dataset comprising 1.4 billion web requests. The system exhibited a 98% level of accuracy in identifying zero-day attacks. ZeroWall is a proficient method for identifying zero-day web assaults that may evade conventional signature-based web application firewalls (WAFs). ZeroWall is a proficient approach for identifying zero-day web assaults that may evade detection by conventional signature-based Web Application Firewalls (WAFs) (Tang et al., 2020)

Popoola and colleagues have introduced a novel approach called feder-

ated deep learning (FDL) for the identification of zero-day botnet attacks. The FDL method is designed to be both privacy-preserving and efficient, enabling the training of deep learning models for detecting zero-day botnet attacks on IoT edge devices. The FDL approach involves the utilization of deep learning models that are trained on individual IoT edge devices. Subsequently, the regional models are consolidated into a universal model through the utilization of a federated averaging technique. Subsequently, the world-wide model is employed for the identification of botnet attacks that exploit vulnerabilities unknown to the security community. The method under consideration was assessed on two distinct datasets, namely the Bot-IoT and N-BaIoT datasets. The findings indicate that FDL exhibited a notable capability to identify botnet attacks that were previously unknown, achieving a high level of precision. FDL demonstrated the capability to identify botnet attacks that exploit unknown vulnerabilities, commonly referred to as zero-day attacks, while maintaining minimal communication overhead and latency. The FDL method is an efficient and privacy-preserving approach for training deep learning models to detect zero-day botnet attacks on IoT edge devices. FDL exhibited a high degree of precision and low levels of communication overhead and latency in its ability to identify botnet attacks that exploit previously unknown vulnerabilities (Popoola et al., 2022).

Bathala and colleagues have presented a novel approach for email filtering that leverages sophisticated machine learning methodologies to identify zero-day attacks. The approach employs a blend of characteristics, encompassing the textual content of the electronic mail, the electronic mail address of the sender, and the accompanying files, to categorize electronic mails as either unsolicited bulk messages or fraudulent attempts to acquire sensitive information. The method under consideration was assessed using a dataset comprising 100,000 electronic mails. The findings indicate that the employed technique exhibited a 99% precision rate in identifying zero-

day attacks. The method proposed exhibits potential as a novel strategy for safeguarding enterprises and individuals against zero-day assaults (Bathala, Srihitha, Dodla, & Pasala, 2021).

Bathala and colleagues have presented a novel approach for email filtering that leverages sophisticated machine learning methodologies to identify zero-day attacks. The approach employs a blend of characteristics, encompassing the textual content of the electronic mail, the electronic mail address of the sender, and the accompanying files, to categorize electronic mails as either unsolicited bulk messages or fraudulent attempts to acquire sensitive information. The method under consideration was assessed using a dataset comprising 100,000 electronic mails. The findings indicate that the employed technique exhibited a 99% precision rate in identifying zero-day attacks. The method proposed exhibits potential as a novel strategy for safeguarding enterprises and individuals against zero-day assaults (Nandakumar et al., 2022).

2.1.2 Deception Approaches

A honeypot design is suggested by Ellouh et al. for identifying IoT zero-day attacks. Three basic parts make up the architecture: a honeypot, a sensor, and a controller. A virtual device called a honeypot is made to resemble an IoT device that is weak. The sensor is used to gather information from the honeypot, including the attacker's IP address and the tools they are employing. The data gathered by the sensor is examined by the controller, which also uses it to look for zero-day attacks. The proposed architecture was assessed in the article using data from actual IoT threats. The outcomes demonstrated that the architecture was capable of accurately identifying zero-day assaults (Ellouh, Ghaleb, & Felemban, 2022).

Ahmad et al, presents a honeypot-based approach for detecting and analyzing active attacks. The honeypot system used in this paper is a combi-

nation of a virtual machine and a network sniffer. The virtual machine is used to create a realistic target environment for attackers, while the network sniffer is used to capture traffic between the honeypot and the attacker. The paper describes two methods for detecting active attacks using the honeypot system. The first method is based on the observation that attackers typically use a variety of tools and techniques to carry out their attacks. By monitoring the traffic between the honeypot and the attacker, the honeypot system can identify these tools and techniques and raise an alarm if they are detected. The second method is based on the observation that attackers often make mistakes during their attacks. By monitoring the traffic between the honeypot and the attacker, the honeypot system can identify these mistakes and raise an alarm if they are detected. The paper concludes by discussing the limitations of the honeypot-based approach. One limitation is that honeypots can be expensive to deploy and maintain. Another limitation is that honeypots can be easily detected by attackers, which can reduce their effectiveness (W. Ahmad, Arsalan, Nawaz, & Waqas, n.d.).

Priya and Chakkaravarthy have proposed an architecture for a cloud-based honeypot that is containerized, with the aim of monitoring and tracing attackers. The proposed architecture comprises a collection of honeypots that are strategically positioned in a cloud environment. Each honeypot is designed to simulate a distinct set of vulnerable services, thereby luring potential attackers. Additionally, a central server is incorporated into the architecture to oversee the management of the honeypots and to gather pertinent attack-related information. The utilization of Docker containers for honeypot deployment ensures both ease of deployment and isolation. The collected data is analyzed and visualized through the implementation of Elasticsearch and Kibana on the server. The efficacy of the architecture is assessed through its deployment on a publicly accessible cloud platform, with subsequent observation of the attacks it elicits. The authors conclude

that the architecture effectively draws a diverse range of attacks and furnishes valuable insights into the behavior of attackers. The article delineates various constraints of the suggested framework, such as the potential for malicious actors to detect the honeypots and escape them, the burden of handling and examining substantial volumes of data gathered by the honeypots, and the requirement for persistent revisions to guarantee that the honeypots simulate the most recent susceptibilities. The authors acknowledge that the proposed architecture is mainly intended for the identification and monitoring of malicious actors, and fails to provide proactive defense mechanisms to prevent attacks in real-time (Priya & Chakkaravarthy, 2023)

Machmeier has proposed a comprehensive framework that enables the identification and examination of active attacks. The underlying premise of the framework lies in the recognition that malicious actors often employ a diverse array of instruments and methodologies in the execution of their hostile actions. Through the surveillance of the communication flow between the targeted system and the attacker, the framework has the capacity to discern said assailant's tools and methodologies, and subsequently trigger an alert in the event of their detection. The proposed system comprises a traffic monitoring module that is designed to gather data pertaining to the communication between the victim system and the malevolent entity. The proposed component is designed to detect signatures of various tools and techniques that are commonly employed by malicious actors. A component for detecting anomalies that can potentially signify an attack by identifying atypical traffic patterns. The component responsible for traffic monitoring is tasked with gathering data pertaining to the communication between the targeted system and the perpetrator. Subsequently, the traffic is directed towards the components responsible for signature detection and anomaly detection. The component responsible for detecting signatures is tasked with identifying the specific tools and techniques that are commonly employed by malicious

actors. The process of identifying attacks in the signature detection component is accomplished by utilizing a database consisting of pre-existing attack signatures. The anomaly detection module is responsible for detecting unusual traffic patterns that could potentially signify a security breach. The anomaly detection module employs diverse techniques to detect unusual traffic patterns, including statistical analysis and machine learning. A constraint of the framework is its inability to identify novel attacks that are not present in the repository of recognized attack signatures. An additional constraint pertains to the computational expense of the framework when applied to extensive datasets (Machmeier, 2023).

2.1.3 Hybrid Approaches

Machida and colleagues introduced innovative deception strategies for the purpose of detecting malware in Industrial Control Systems (ICS). The methodologies employed are predicated upon the concept of enticing malware to honeypots, subsequently scrutinizing their conduct to identify any malevolent actions. The authors assess the efficacy of the techniques on a real-world dataset of malware and demonstrate their ability to accurately detect attacks with a high degree of precision. The methodologies employed are founded upon the concept of fabricating honeypots that bear a striking resemblance to authentic industrial control system (ICS) apparatus. Upon malware infection of a honeypot, it initiates communication with the command and control (CC) server of the attacker. Subsequently, the honeypot may be employed to oversee the conduct of the malicious software and amass data concerning the perpetrator. The present study assesses the effectiveness of the suggested methods of deception on an actual dataset of malicious software. The findings indicate that the employed methodologies are proficient in identifying intrusions with a notable level of precision. The study culminates by examining the prospective advantages of the sug-

gested methodologies and the obstacles that necessitate resolution in forthcoming investigations. The results of the study hold great importance as they showcase the viability of employing deception tactics in identifying malware on Industrial Control Systems (ICS). The methodologies are facile to implement and have the capability to identify a diverse spectrum of malicious software incursions. Furthermore, the employed methodologies are non-invasive and do not necessitate any alterations to the Industrial Control System (ICS) network. This renders them a potentially effective strategy for enhancing the security of Industrial Control Systems (ICS) (Machida, Yamamoto, Unno, & Kojima, 2021).

Liu and colleagues have presented a framework comprising three primary components, namely a mimic defense architecture, a zero-day attack detection module, and a response module. The mimic defense architecture has been developed with the purpose of emulating the configuration and actions of the digital realm, thereby creating a challenging environment for potential assailants to differentiate between authentic and counterfeit cyberspace. The module for detecting zero-day attacks employs machine learning methodologies to identify zero-day attacks through the analysis of network traffic and the detection of anomalous behavior. The response module employs a blend of active and passive defensive strategies to address zero-day attacks, including but not limited to obstructing the attack, segregating the impacted system, and alerting the security personnel. The proposed framework was assessed by the authors through the utilization of a dataset comprising actual instances of zero-day attacks in the real world. The findings indicate that the framework exhibits efficacy in identifying and mitigating zero-day attacks, with a notable capacity for detection and a minimal incidence of false positives (Liu et al., 2017).

Misbah and colleagues presented a scholarly article that offers a comprehensive examination of zero-day attacks and their potential ramifications on

computer systems. Subsequently, the text deliberates on the constraints of conventional signature-based detection methods and the necessity for more sophisticated techniques capable of identifying attacks that were previously unknown. The study conducted by the authors involves a comparison of various soft computing techniques for the purpose of detecting zero-day attacks. The techniques that were evaluated include artificial neural networks (ANNs), support vector machines (SVMs), decision trees, and fuzzy logic. The authors assess each approach utilizing multiple criteria, including but not limited to accuracy, false positive rate, and detection time. The findings indicate that Artificial Neural Networks (ANNs) and Support Vector Machines (SVMs) are the most efficacious soft computing methodologies for detecting zero-day attacks. ANNs exhibit a marginally superior accuracy performance compared to SVMs. The authors emphasize the significance of choosing suitable features for model training and the necessity of continuous updates to maintain model efficacy (Anwer, Ahmed, Akhunzada, Hussain, & Khan, 2022).

Jeong and Choi have proposed a hybrid system comprising a Network Intrusion Detection and Prevention System (NIDPS) and a honeypot, which collaborate to identify and avert zero-day attacks. The author initially addresses the constraints of conventional security measures and emphasizes the necessity for sophisticated methodologies to identify and avert zero-day attacks. The Network Intrusion Detection and Prevention System (NIDPS) is a tool utilized for the purpose of monitoring network traffic and identifying potentially malicious behavior through the application of predetermined regulations. Upon detection of a zero-day attack, the system initiates the activation of a honeypot, which has been specifically designed to simulate vulnerable systems that are susceptible to being targeted by malicious attackers. The honeypot serves as a mechanism for gathering information pertaining to the attack, thereby enabling the security team to conduct a

comprehensive analysis of the attack and subsequently devise appropriate countermeasures. The proposed hybrid system is assessed by the authors through the utilization of a dataset comprising of real-world zero-day attacks. The findings indicate that the system exhibits efficacy in identifying and mitigating zero-day attacks, thereby reducing the potential impact of such attacks (Jeong & Choi, 2020).

The authors Pitre et al, The author has put forth a new methodology for identifying zero-day attacks, which involves utilizing a hybrid approach that incorporates both signature-based and anomaly-based detection techniques. The method of signature-based detection is employed for the identification of attacks that are already known, whereas the method of anomaly-based detection is utilized for the detection of attacks that are not yet identified. The article additionally examines the utilization of machine learning techniques to mitigate the occurrence of false positives in the anomaly-based detection approach. The study culminates by assessing the suggested methodology on a corpus of actual network traffic. The findings indicate that the suggested methodology exhibits a capacity to identify zero-day attacks with a notable degree of precision and a minimal occurrence of false positives. (Pitre, Gandhi, Konde, Adhao, & Pachghare, 2022).

Hairab and colleagues have presented a method that employs a convolutional neural network (CNN)-based anomaly detection system for scrutinizing the performance of Internet of Things (IoT) devices. This system is capable of identifying anomalies that could potentially signify a zero-day attack. In order to enhance the precision of the system, the authors have employed regularization techniques, including dropout and L2 regularization, to mitigate the issue of overfitting and enhance generalization. The proposed system is assessed by the authors through the utilization of a dataset comprising of real-world IoT traffic and zero-day attacks. The findings indicate that the suggested system is proficient in identifying zero-day attacks

in IoT networks, exhibiting a substantial detection rate and minimal false positive rate. Regularization techniques enhance the precision of the system and mitigate the likelihood of overfitting (Hairab, Said Elsayed, Jurcut, & Azer, 2022).

An solution that Roshan and Zafar presented makes use of an auto-encoder neural network to find network traffic irregularities that might point to a zero-day assault. The authors suggest an optimization technique that fine-tunes the hyper-parameters of the auto-encoder using evolutionary algorithms in order to increase the system's accuracy. The NSL-KDD dataset and the CICIDS2017 dataset were used to evaluate the suggested methodology. The findings demonstrate that the suggested method has a high detection rate and a low false positive rate for identifying zero-day threats in computer networks. The optimization technique is also portable and usable on devices with limited resources (Roshan & Zafar, 2021).

2.2 Summary

The present section provides a literature review on the subject of mitigating and detecting zero-day attacks, including techniques such as anomaly detection and machine learning. It explores how these methods can be employed to identify such attacks. Although anomaly detection and machine learning have proven to be efficacious in identifying unfamiliar attacks, their implementation necessitates a considerable degree of proficiency and may not be viable for all entities. The segment additionally examines the utilization of a fusion of machine learning and honeypots in the identification of zero-day attacks. The literature pertaining to this approach is examined by the author, who observes that it has the potential to efficiently identify previously unidentified attacks while mitigating the occurrence of false positives. Nevertheless, this methodology necessitates a substantial allocation of resources

and specialized knowledge.

To sum up, the Literature Review segment furnishes a thorough outline of the extant investigations on the identification of zero-day assaults utilizing manifold methodologies. This section elucidates the advantages and drawbacks of various methodologies and furnishes valuable perspectives for scholars and professionals operating in the domain of cybersecurity.

Chapter 3

Methodology

3.1 Introduction

This section presents a comprehensive account of the research methodologies employed to accomplish the study's aims. The present thesis centers on the conception and execution of an innovative strategy for identifying zero-day attacks through the utilization of deception and THI. The methodology section delineates the procedures employed to formulate and execute the investigation, encompassing the methodologies for gathering, scrutinizing, and construing data. The segment additionally examines the methodologies and instruments utilized for assessing the efficacy of the suggested methodology. The methodology section functions as a guide for the research and imparts a lucid comprehension of the measures taken to ensure the accuracy and consistency of the study outcomes.

3.2 Research Questions

1. How effective is the proposed approach in detecting zero-day attacks?

The efficacy of deception and threat hunting intelligence (THI) in identifying zero-day attacks is contingent upon several variables, such as the complexity of the attack, the caliber of the deception and THI, and the proficiency of the security personnel. The integration of deception and THI has the potential to enhance the precision and efficacy of zero-day attack identification by mitigating erroneous alerts and furnishing a more all-encompassing perspective of the network environment. Additionally, it is noteworthy to acknowledge that the utilization of deception and the use of truth-inducing techniques (THI) is not a panacea. The utilization of deception techniques and threat hunting initiatives in tandem with supplementary security measures, such as firewalls, intrusion detection systems, and antivirus software, holds significant importance. to determine the effectiveness of the proposed approach a real attacks will be conducted by security specialist targeting the proof of concept environment in order to proof it accuracy.

2. How does the proposed approach compare to existing methods in terms of accuracy and efficiency?

The utilization of Deception and Threat Hunting Intelligence (THI) has been found to exhibit greater precision and efficacy in the identification of zero-day attacks in comparison to conventional techniques, such as signature-based detection. The reason for this is that deception and threat hunting intelligence (THI) possess the capability to identify attacks that have not yet been recognized by either the vendor or the user. Moreover, they are capable of identifying attacks that have not yet been encompassed by signature-based detection. Nonetheless,

it is worth noting that the implementation and maintenance of deception and THI techniques may pose greater financial and logistical challenges compared to conventional methods. Conversely, it has the potential to diminish instances of erroneous positive identifications, a task that can demand significant amounts of time and resources to scrutinize. The proposed approach will be compared with the existing method by establishing its effectiveness and by proving that the proof of concept is working as required.

3. What are the limitations of the proposed approach and how can they be addressed in future research?

Although deception and Threat Hunting and Intelligence (THI) have demonstrated efficacy in detecting zero-day attacks, it is imperative to acknowledge their inherent limitations. The aforementioned constraints encompass:

Complexity: The implementation of deception and threat hunting infrastructure (THI) necessitates a considerable degree of technical proficiency and resource allocation, which may pose a difficulty for smaller entities.

Limited coverage: The employment of deception techniques provides protection solely to the assets that have been deliberately targeted, thereby rendering the remaining network susceptible to potential attacks.

Sophisticated attackers: Highly skilled attackers possess the ability to discern and evade deceitful tactics, thereby diminishing their efficacy against sophisticated assailants.

In order to overcome these constraints, forthcoming investigations may concentrate on the advancement of more intricate Deception and THI methodologies that can more accurately emulate authentic sys-

tems and data. Furthermore, it is worth investigating the potential of employing machine learning algorithms in order to mitigate the occurrence of false positives and enhance the precision of Deception and THI. Subsequent studies may explore the amalgamation of Deception and THI with additional security measures, including endpoint protection and network segmentation, to furnish a more all-encompassing strategy for detecting zero-day attacks. Subsequently, further investigation may be directed towards the advancement of Deception and THI methodologies that are more attainable and economical for less sizable establishments that possess restricted resources.

3.3 Data collection and analysis

This section will discuss the various types of data that can be gathered to initiate the process of threat hunting.

1. Network traffic data: Network traffic can be utilized for the purpose of detecting suspicious activities, such as establishing connections with IP addresses that are recognized as malicious. Various tools can be used to help with network traffic and event capturing such as Qradar, splunk and security onion 2. The POC presented in this study will include AWS session mirroring to foreword all the network traffic to security solution that will be later used to analyze the traffic and demonstrate the effectiveness of the proposed framework by examining the targeted IP address.
2. Endpoint data: The data obtained at the endpoint can be utilized for the purpose of detecting potentially malicious behavior, such as the launching of harmful executable files. Various tools, including antivirus software, endpoint security suites, and file integrity monitoring tools, can be utilized to gather endpoint data. In this POC this

type of data will be out of scope as the network traffic data can be a sufficient evidence of intrusion as whoever is trying to access the deception environment will be triggered in the network traffic data.

3. User Behavior data: The utilization of user behavior data can facilitate the detection of potentially fraudulent actions, such as the occurrence of a login attempt from an atypical geographical location. The collection of user behavior data will be facilitated in this POC through the utilization of VPC flow logs and Security Onion 2 to understand which attacks and techniques are being utilized by the attackers.
4. Threat intelligence data: The utilization of threat intelligence information can facilitate the identification of potential threats, including but not limited to recognized malevolent IP addresses and file signatures. The collection of threat intelligence data can be sourced from multiple channels, including but not limited to government entities, security vendors, and open-source intelligence (OSINT) feeds. In this POC this type of data will be out of scope.

Data analysis:

1. Statistical analysis: The utilization of statistical analysis will be employed to detect potential zero-day attacks through the identification of discernible patterns within the data, such as anomalous surges in network traffic or the implementation of malevolent files.

Human analysis: The utilization of human analysis shall be employed to detect any anomalous behavior that could potentially signify a zero-day attack. The SOC team is capable of scrutinizing the data for any anomalous activities, such as atypical network traffic or the implementation of malevolent commands.

3.4 Framework development

The present study will adopt a framework that integrates multiple frameworks, including:

- A framework for deception strategy will be formulated as an integral component of the primary framework, with the aim of ascertaining the optimal deception techniques for the detection of zero-day attacks. The proposed framework will encompass a comprehensive categorization of deception tactics, including but not limited to honeypots, honeytokens, and decoys. Additionally, the framework will offer a set of criteria for determining the optimal deception technique to be employed in a given environment.
- A framework for threat intelligence will be established within the primary framework with the aim of detecting and predicting novel and emerging threats. The proposed framework comprises a categorization of threat intelligence sources, encompassing open-source intelligence, strategic, operational, tactical, and technical sources. In addition, the provision of guidelines for the selection of the most pertinent sources of threat intelligence for the environment under consideration is imperative.
- A framework for Threat Hunting will be established as an integral component of the primary framework with the aim of actively seeking out concealed threats and vulnerabilities within the network. The proposed framework entails a systematic categorization of threat hunting methodologies, including but not limited to log analysis, network forensics, and endpoint analysis. Additionally, it aims to furnish recommendations for the optimal selection of a technique that aligns with the specific requirements of the environment under consideration.

- The development of an incident response framework is proposed as an integral component of the overarching framework, with the aim of furnishing a set of directives for effectively addressing zero-day attacks. The proposed framework encompasses a taxonomy of incident response protocols, namely containment, analysis, eradication, and recovery, and furnishes recommendations for determining the optimal protocols for the network environment.
- A framework for evaluation will be established as an integral component of the primary framework, with the aim of appraising the efficacy of the suggested methodology for identifying zero-day attacks. The proposed framework encompasses a categorization of assessment techniques, comprising of metrics such as false positive and false negative rates, detection time, and coverage. Additionally, it furnishes recommendations for the optimal selection of evaluation methods, tailored to the specific network environment. It is imperative that the Evaluation Framework incorporates directives for juxtaposing the proposed methodology against pre-existing techniques and furnishing discernment into the advantages and drawbacks of the proposed approach.

3.5 Evaluation methods

- False Positive and False Negative Rates

The false positive rate is a metric that quantifies the ratio of system-generated alerts that do not correspond to genuine zero-day attacks, whereas the false negative rate is a metric that quantifies the ratio of zero-day attacks that remain undetected by the system. The efficacy of a system in detecting zero-day attacks is positively correlated with the reduction of false positive and false negative rates. in the proposed

POC the false positive will be consider as when a non attacker try to access the depiction environment but in the following section it will be demonstrated that whoever tried to access the depiction environment tried to conduct an attack, in addition a normal user will not be able to navigate to the depiction environment without enumerating the whole POC environment.

- Detection Time

The duration required for a system to identify a zero-day attack is referred to as the detection time. A system's efficacy in detecting zero-day attacks increases with a decrease in its detection time. Once an attack is launched a measurement of the time it takes for the proposed security system to detect and respond to the attack will be conducted. This will be done using the logs and alerts generated by the security system, as well as by monitoring the behavior of the attack itself.

- Coverage

The scope of the system's ability to identify zero-day attacks throughout the network is evaluated through coverage metrics. The efficacy of the system in detecting zero-day attacks increases proportionally with the level of coverage. the POC is covering more than the one infrastructure zone as it covers the Demilitarized Zone (DMZ) with a deployment of a web server and the CORE zone with the deployment of a database and active directory server.

- Comparison to Existing Methods

The efficacy of the proposed approach can be assessed by means of a comparative analysis with established methodologies. Conventional techniques for detecting zero-day attacks encompass signature-based detection methods, intrusion detection systems, and other existing

methods. The evaluation of the performance can be conducted by utilizing various metrics, including but not limited to, false positive and false negative rates, detection time, and coverage.

- Expert Analysis

The efficacy of the suggested approach can be assessed through the utilization of specialized analysis conducted by professionals in the field. Professionals specialized in the domain of cybersecurity possess the ability to scrutinize the system's output and offer valuable observations regarding its efficacy in identifying zero-day attacks.

- Evaluation Flow

Figure 3.1 represent the flow of the evaluation that will be taken to determine the effectiveness of the proposed framework.

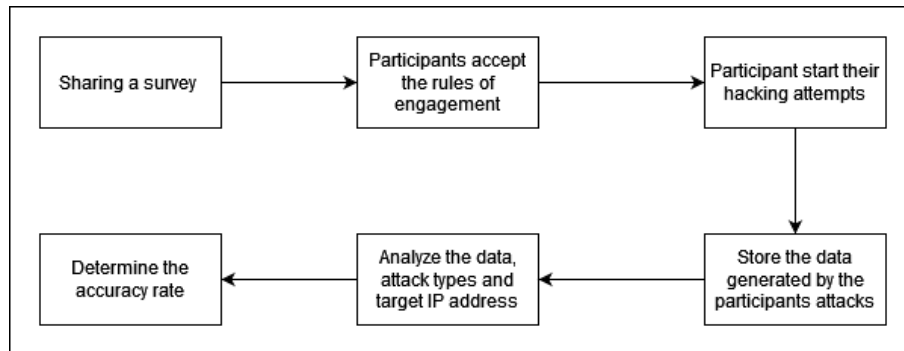


Figure 3.1: Evaluation Flow

3.6 Description of the proposed framework

The proposed framework combines several frameworks. As a result, it will be divided into the two following parts, High level which contains Strategic and Operational THI in addition to the deception planing, and the other part is the low level which contains Tactical and Technical THI in addition the exaction of the deception plan.

3.6.1 Strategic Threat Hunting Intelligence

The strategic approach to THI involves the acquisition of data from various sources such as meeting minutes, briefings, reports, and conversations. This data assists decision-makers in the fields of cyber and information security in recognizing and comprehending both current and potential hazards. This information encompasses both historical and contemporary data pertaining to cyberattacks, as well as the financial ramifications of such occurrences. The intended recipients of this category of threat hunting are individuals who lack technical expertise (Rahman, Mahdavi-Hezaveh, & Williams, 2021).

According to a survey carried out by the SysAdmin, Audit, Network, and Security (SANS) Institute (Brown & Lee, 2021), strategic information is predominantly utilized in formats such as PowerPoint presentations, spreadsheets, and emails. Diagram 3.2 presented depicts the outcomes of the inquiry posed to the participants regarding the manner in which their organization employs or circulates CTI information. Please indicate all options that are applicable.

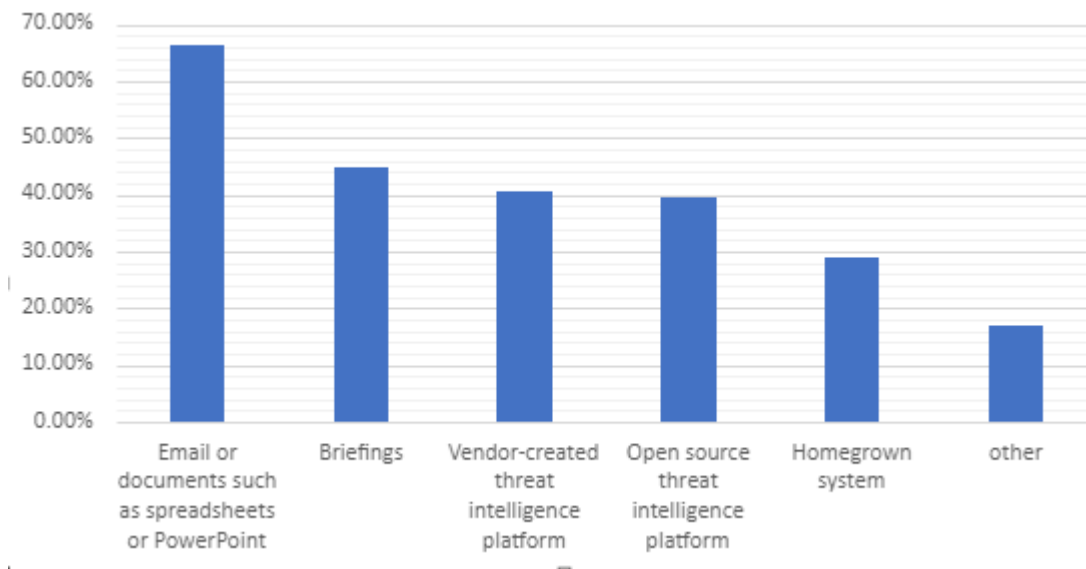


Figure 3.2: SANS survey results

3.6.2 Operational Threat Hunting Intelligence

The aforementioned approach bears resemblance to the Strategic approach in that both hinge on the acquisition of information. However, the disparity lies in the nature of the information procured and the means by which it is obtained. The utilized data in this methodology comprises of precise details regarding imminent attacks, encompassing attack motives, temporal aspects, characteristics, and threat assessments. This particular THI variant is designed for examination and implementation by expert security personnel operating within a SOC (Varatharaj, Rupasinghe, & Liyanapathirana, 2021).

Numerous resources and solutions are accessible for open source or commercial use. One instance of an innovative system is available. Samtani and colleagues introduced a new tinnitus handicap inventory (THI) system called AZSecure. The aforementioned system is designed to gather data from the dark web, including newly developed hacking tools, content, and knowledge that is shared by hackers on both the dark web market and social media platforms (Samtani, Li, Benjamin, & Chen, 2021).

3.6.3 Tactical Threat Hunting Intelligence

This methodology provides security teams with insights into the tactics, techniques, and procedures employed by threat actors. Stated differently, it furnishes valuable insights to the security personnel, thereby expanding their scope and comprehension of the vulnerabilities present in their network (*The Necessity of Cyber Threat Intelligence - ProQuest*, n.d.). Numerous techniques are employed, including:

- (i) Threat Actor Tactics: Comprehending the methods employed by attackers to detect and pinpoint the susceptibilities of organizational assets can aid in the identification of countermeasures to alleviate such

attacks (Yeboah-Ofori et al., 2021).

- (ii) Threat Actor Techniques: This factor pertains to the techniques and instruments employed by malevolent actors to take advantage of a security flaw, potentially impacting entities within an organization (Bahrami et al., 2019).
- (iii) Threat Actor Procedures: Upon satisfying the initial two criteria, the security team will be equipped to educate producers on each potential attack, outlining the appropriate response in the event of an occurrence, or the necessary measures to prevent its manifestation (Maschmeyer, Deibert, & Lindsay, 2021).

3.6.4 Technical Threat Hunting Intelligence

The technical methodology heavily relies on the Security Operations Center (SOC). The Security Operations Center (SOC) can be defined as a specialized unit dedicated to conducting security analyses and monitoring an organization's network. The term SOC is commonly understood as a department that assumes responsibility for overseeing security operations, including but not limited to threat intelligence, incident response, and management (Vielberth, Bohm, Fichtinger, & Pernul, 2020). Numerous Security Information and Event Management (SIEM) solutions are at the disposal of the SOC team. One such solution, as proposed by Eswaran et al (Eswaran, Rani, D., Ramakrishnan, & Selvakumar, 2021), has been designed to detect malicious crawlers that target a bank portal with minimal false positive alerts.

3.6.5 Deception

- (i) Identify high-value assets: Identify the assets that are of the highest value to the organization. This could include sensitive data, intellectual property or critical infrastructure (X. Ren, Liang, & Liu, 2020).
- (ii) Plan for deception: Develop a comprehensive plan to use deception techniques to detect zero-day attacks. This plan should include a range of techniques, such as honeytokens, honeyfiles, and honeycredentials, as well as active defense measures like intrusion deception (Islam & Al-Shaer, 2020).
- (iii) Set up decoys: Create decoy systems, data, and other resources that look and feel like real assets but are designed to trap attackers. These decoys can be used to detect and analyze the behavior of attackers, and to gather intelligence on their tactics and techniques (Liebowitz et al., 2021).
- (iv) Monitor and analyze: Continuously monitor the decoys and other deception assets for any signs of attack. Use machine learning algorithms and other analytical tools to detect anomalies and patterns that may indicate a zero-day attack. Advanced techniques like deep learning and adversarial machine learning can also be used to enhance detection capabilities (Amin, Shetty, Njilla, Tosh, & Kamhoua, 2021).
- (v) Respond and remediate: Take immediate action to isolate the attacker and limit the damage of any detected attacks. Use the information gathered during the attack to improve the deception strategy and overall security posture of the organization. This can include sharing intelligence with other organizations to build a collective defense against zero-day attacks (Shahriar, Ashiqur Rahman, Haque, & Chowdhury, 2021).

3.7 Components of the framework

This section will outline the fundamental components of the proposed solution. This section explores the various components of the framework, covering the responsibilities of the organizational staff, the technological aspects employed in the proof of concept (POC), and the configuration and execution of the POC environment. The section begins by identifying the duties and obligations of the personnel of the organization who are engaged in executing the framework. Subsequently, this section breaks down the technological components employed in the proof of concept (POC) of the framework. The aforementioned includes both the requisite software and hardware components for executing the framework, alongside any third-party tools or services that may be deemed necessary. The segment additionally examines the different features and functionalities of the technology, and its role in enhancing the efficacy of the framework. The section concludes by presenting the details of the POC environment's design and implementation for the framework. This involves the setting up of the system's configuration and the setting up of any necessary monitoring or alerting mechanisms. Figure 3.3 illustrates the two different threat hunting methodologies employed within the proposed framework, as well as the allocation of each staff role to each respective approach. The management team will determine the tactics, techniques, and procedures (TTPs) that necessitate attention for the long-term strategy. Meanwhile, the operational team will establish the necessary resources to initiate the deception of the attackers for short-term planning.



Figure 3.3: The Main Components of the framework

3.7.1 Management Staff Role

The deployment of a deception and threat hunting intelligence framework for the detection of zero-day attacks is dependent upon the crucial involvement of the management staff. Initially, it is incumbent upon them to recognize the requirement for the required framework and to allocate the necessary resources for its execution. It is essential for the management to comprehend the possible risks and ramifications associated with zero-day attacks, as well as the constraints of conventional security measures in detecting them. Subsequently, it is important to make sure that the framework is in line with the security strategy and risk management policies of the organization. The process entails delineating the boundaries of the framework, ascertaining the categories of data to be observed, and establishing the suitable degrees of admittance and permission. Thirdly, it is imperative to ensure that the framework is seamlessly integrated with the pre-existing security systems and processes. This entails engaging in collaboration with the IT department to establish the configuration and deployment of essential hardware and software elements, while also delineating protocols for the oversight and management of alert notifications. Ultimately, it is imperative that the framework undergoes consistent updates and testing to verify its efficacy in mitigating emerging security risks. The aforementioned task entails the surveillance of the framework's functionality, evaluation of the outcomes of threat hunts, and implementation of modifications to the setup and protocols as deemed appropriate. In the context of detecting zero-day attacks, the effective deployment and operation of a deception and threat hunting intelligence framework is contingent upon the critical contribution of management.

3.7.2 Operation Staff Role

The deployment of a deception and threat hunting intelligence framework for the detection of zero-day attacks is reliant on the pivotal involvement of the operational staff. Initially, their responsibility entails the implementation and configuration of both hardware and software components within the framework. The process entails the implementation and customization of the decoy systems, establishment of the monitoring and logging framework, and configuration of the threat hunting and analysis instruments. In addition, it is their duty to oversee the framework and promptly address any notifications. The process entails vigilant surveillance of both the data and decoy systems to identify any anomalous behavior, examining the notifications produced by the system, and examining any plausible security risks. In addition, it is their responsibility to perform threat hunts in order to actively seek out possible threats. The process entails leveraging threat intelligence to detect plausible attack vectors and executing focused searches for indicators of compromise. Ultimately, it is imperative that they establish a close collaboration with the management personnel to guarantee that the framework is in line with the enterprise's comprehensive security strategy and policies for risk management. This entails adhering to established protocols for incident response and communication, cooperating with other teams to address security incidents, and providing evaluations on the efficacy of the framework. In the context of detecting zero-day attacks, the effective deployment and operation of a deception and threat hunting intelligence framework is contingent upon the essential contribution of the operational staff. The efficacy of the framework is contingent upon the individual's technical proficiency and capacity to proficiently oversee and address possible risks.

3.7.3 Technology used

- AWS

The cloud computing platform AWS, offers an extensive range of services, such as computing capabilities, storage, database administration, analytics, and machine learning, among other services. The aforementioned services are tailored to enhance the operational efficiency, security, and cost-effectiveness of organizations across diverse sizes and industries. And it has been used to host the proposed solution of this study. Moreover, AWS have regions where it is hosting its data centers and in each region it has three different data centers referred to as availability zones, and in this study Bahrain region was chosen with two of its availability zones me-south-1a and me-south-1b (Abdoulaye, 2022)

- Security Onion 2

The AWS Security Onion 2 is a security platform that operates in the cloud and is specifically designed to detect, analyze, and respond to threats within AWS environments. The virtual machine (VM) image is deployable as an Amazon EC2 instance and offers a collection of open-source security tools and functionalities for overseeing and safeguarding AWS infrastructure. Security Onion 2 comprises a diverse range of security tools, including Suricata, Zeek (previously referred to as Bro), Wazuh, Elasticsearch, and Kibana. These tools can be utilized to oversee network traffic, identify and examine security events, and explore security breaches. The package includes set dashboards and visual representations which enable the prompt detection of security risks and anomalies. Furthermore, Security Onion 2 has the ability to integrate with various other Amazon Web Services (AWS) offerings, including Amazon CloudWatch and Amazon S3, in order

to furnish centralized capabilities for log management and analysis. The previously mentioned capability allows the aggregation, retention, and examination of logs emanating from AWS infrastructure and security equipment within a unified repository, thereby expediting the detection and remediation of security breaches. Security Onion 2 is equipped with automated functionalities that can be leveraged to optimize security operations and minimize the resources and duration needed for identifying and addressing security risks. The previously mentioned tool consists of automated scripts that facilitate the deployment and configuration of security tools, alongside pre-existing playbooks that cater to the resolution of typical security incidents. In summary, AWS Security Onion 2 is a powerful and adaptable security platform that can effectively oversee and safeguard AWS infrastructure through the utilization of various open-source security tools and functionalities. The implementation of real-time threat detection and analysis, centralized log management and analysis, and automation capabilities can enhance the security posture of an organization by enabling faster incident response (Babu, 2022).

3.7.4 Environment Design

To demonstrate the efficacy of the proposed solution, a simulated bank environment was established to emulate an unreal environment. The simulated financial institution, Middle East International Bank, features a compact demonstration of its environment in figure 3.4. The strategy employed to lure potential attackers involves the utilization of URL path redirection, whereby authorized users are directed to real servers while attackers are redirected to a honeypot environment.

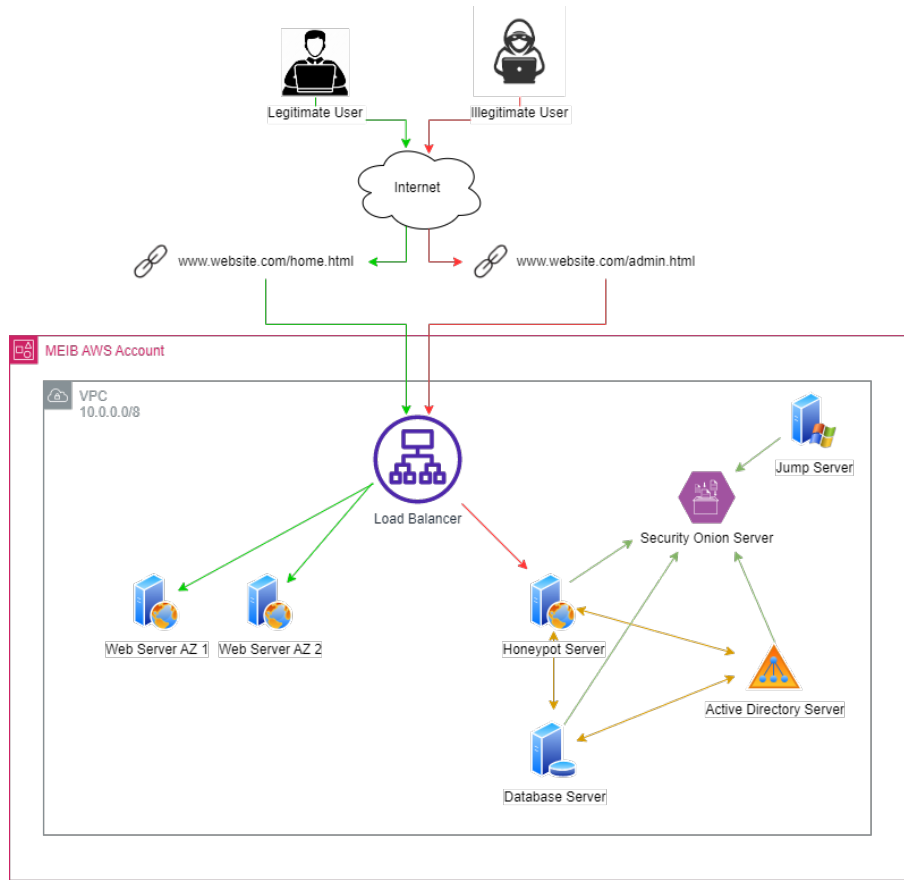


Figure 3.4: Threat Hunting Intelligence Approaches

3.7.5 Implementation

- Certificate

A valid certificate was generated through the use of ACM to verify the simulated environment, and the corresponding certificate configurations are presented in figure 3.5 and figure 3.6, respectively.

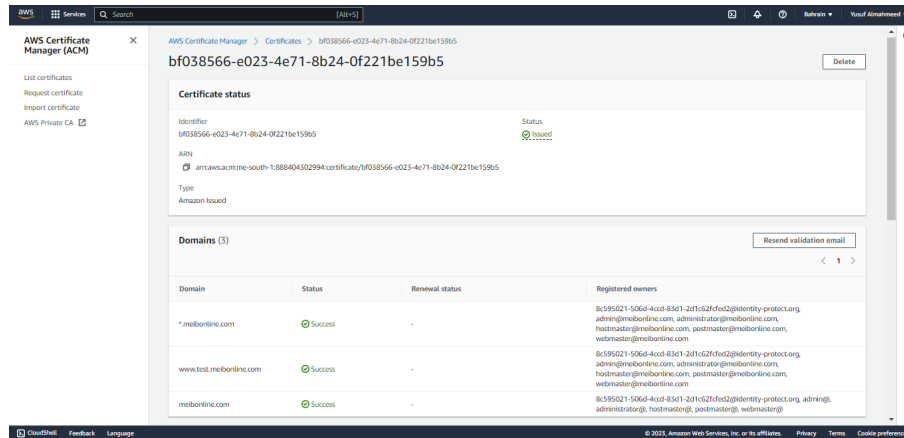


Figure 3.5: Certificate Domains

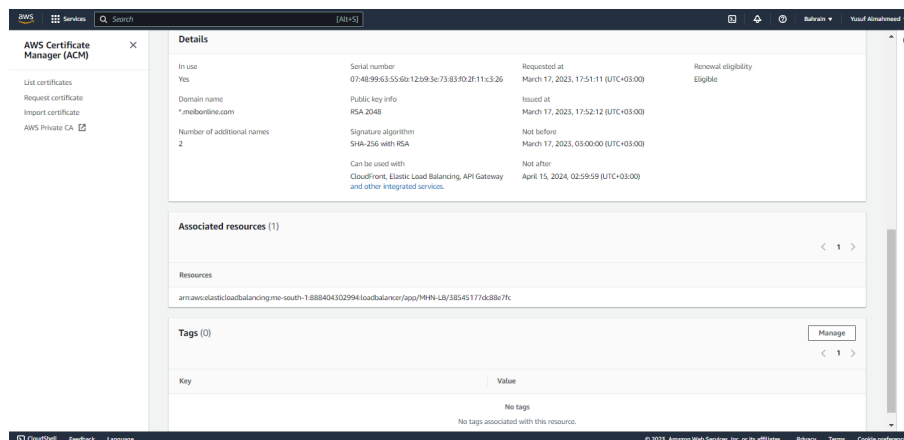


Figure 3.6: Certificate Details

- DNS

DNS entries have been created for the domain meibonline.com using Route 53. As illustrated in figure 3.7, www.test.meibonline.com was directed towards the ALB, as evidenced in figure 3.8.

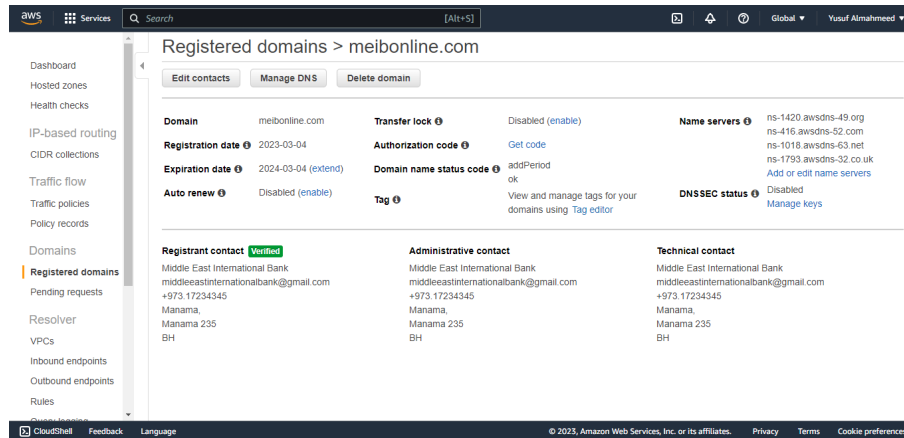


Figure 3.7: DNS Domain Details

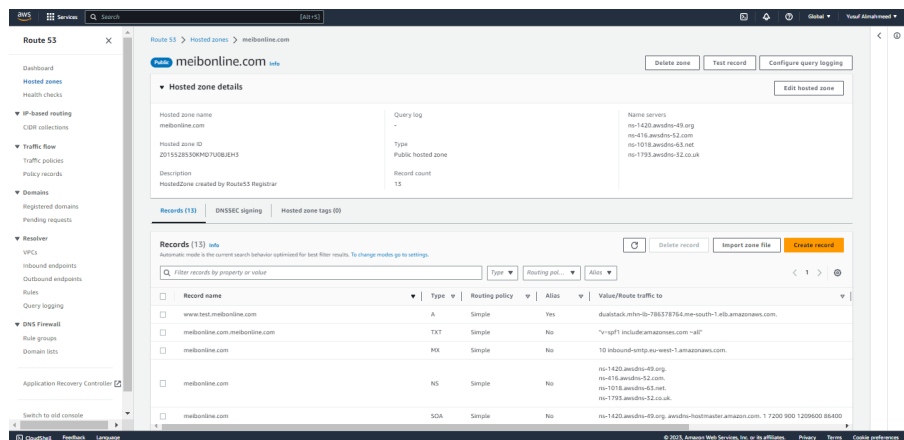


Figure 3.8: DNS Records

- VPC

VPC is a network component part of the components offered by AWS which enables customers to build their own private virtual networks inside the AWS cloud. Resources like instances, databases, and storage can run in a secure and segregated environment by utilizing the VPC component. Administrators of a VPC have total control over the IP address range, subnets, route tables, and network gateways of their virtual network. To manage who has access to their resources, administrators can also configure security settings like security groups and network access control lists. Within an AWS region, a VPC can span

multiple Availability Zones, giving applications high availability and fault tolerance. Additionally, administrators can use VPN or Direct link connections to link their VPC to another VPC or an on-premises data center (Sawant & Sengamedu, 2022). The configuration of the VPC is presented in figure 3.9, with the selection of the 10.10.0.0/16 IPv4 CIDR.

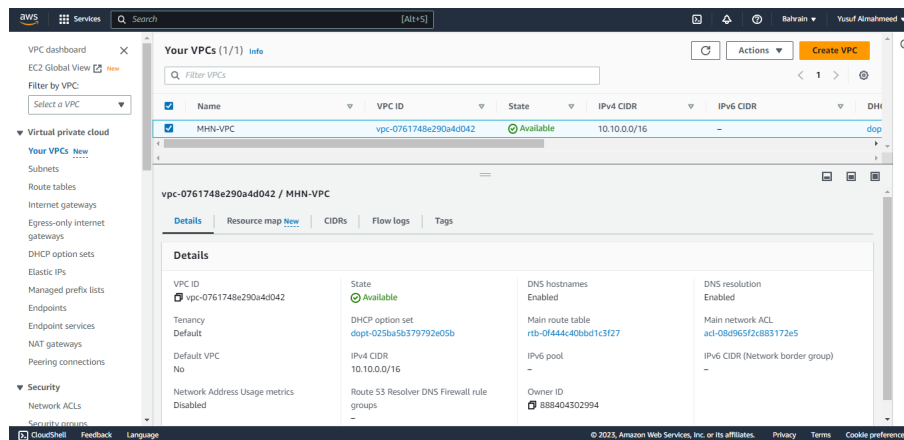


Figure 3.9: MHN VPC Details

Figure 3.10 displays the subnets allocation from the previously created VPC with the 10.10.0.0/16 IPv4 CIDR .

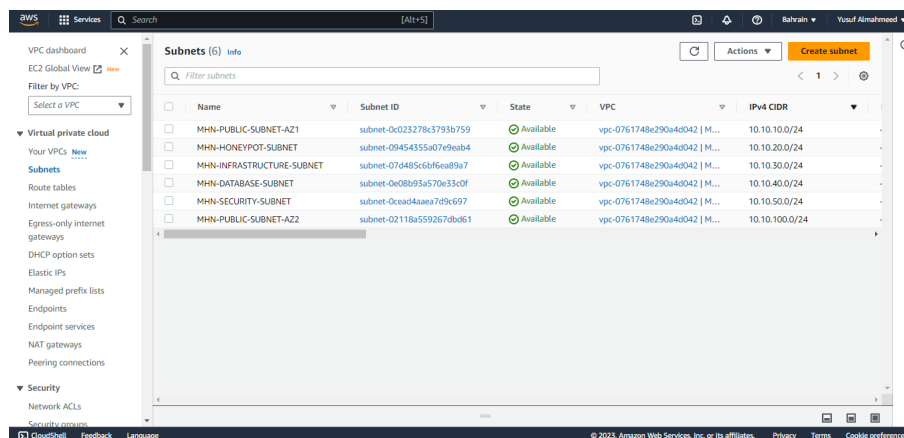


Figure 3.10: MHN Subnets Details

- Route Table

The routing table in AWS is a virtual construct that operates within a VPC and governs the routing of network traffic. Upon the creation of a VPC in AWS, a routing table is automatically generated by the platform as a default setting. The routing table facilitates the routing of network traffic both within the VPC and towards the IGW. It is possible to generate additional routing tables for the VPC in order to accommodate diverse traffic routing needs. Every routing table comprises a collection of rules, commonly known as routes, which determine the appropriate path for network traffic. Every pathway comprises of a destination network and a target. The target network may take the form of a CIDR block, a designated IP address, or a specialized term, such as "local," which refers to VPC-local traffic. The potential targets for a given operation may include various types of network components, such as an IGW, a virtual private gateway, a network address translation (NAT) gateway, or a network interface. In general, routing tables provide a means of managing the direction of network traffic within a VPC and between the VPC and external networks, including the internet (Singh, Arifi, Harikrishnan, Datta, & Wagle, 2022). The route table used for the MHN VPC can be seen in figure 3.11. The first route directs all traffic towards the IGW, whereas the second route directs traffic for the 10.10.0.0/16 subnet to the local VPC.

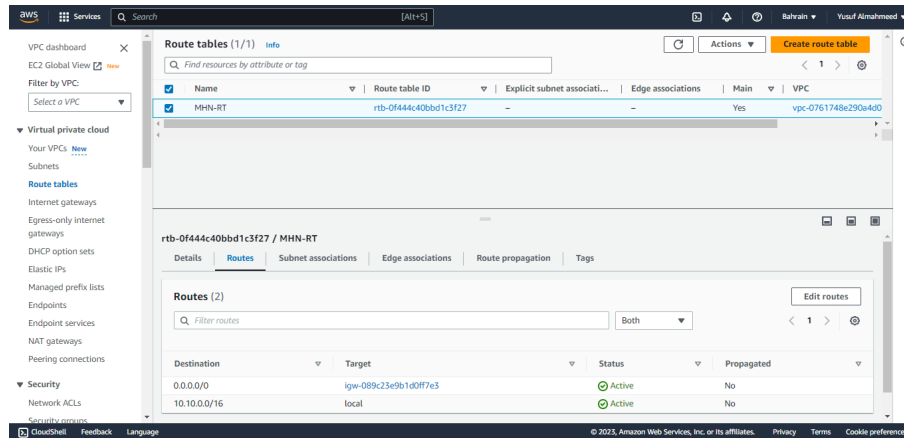


Figure 3.11: MHN Route Table Details

- IGW

The IGW is a VPC component that facilitates communication between instances within a VPC and the internet, with horizontal scalability, redundancy, and high availability. As a default configuration, VPC instances are not directly reachable from the internet. In order to establish internet connectivity for instances within a VPC, it is necessary to connect an IGW to the VPC. The IGW functions as the ingress and egress point for communication between a VPC and the public internet. When a VPC instance transmits a packet to the internet, the packet is routed to the IGW, which subsequently forwards it to the internet. Likewise, in the context of networking, upon dispatch of a packet from the internet to an instance located within a VPC, the packet is routed to the IGW, which subsequently directs it to the pertinent instance. The IGW, or Internet Gateway, is a device that maintains the state of connections between instances within a VPC and the internet, thereby exhibiting stateful behavior. The feature of Network Address Translation (NAT) is also facilitated by the system, enabling the instances located within a VPC to establish communication with the internet through the utilization of the public IP address of the IGW. In general, an IGW is an essential element that facilitates

internet connectivity for instances within a VPC, and it offers a secure and adaptable approach to communication between a VPC and the internet (Lee, Oh, Shon, & Moon, 2023). Figure 3.12 illustrates the configuration implemented for the attachment of the IGW to the VPC.

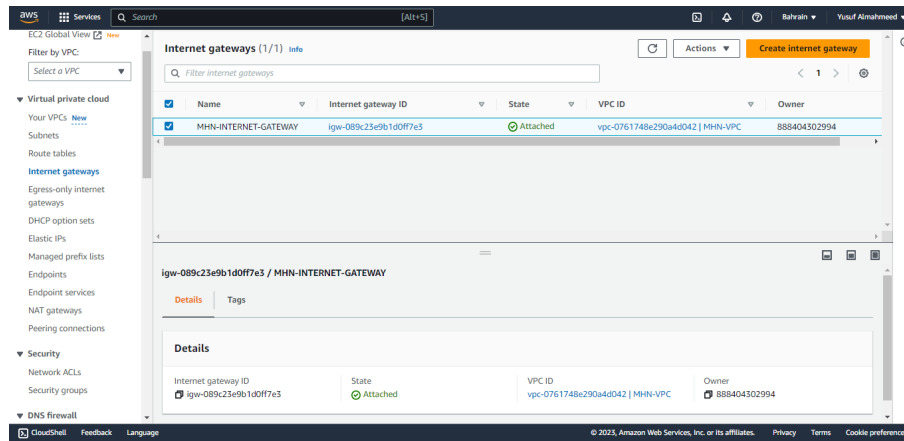


Figure 3.12: MHN IGW Details

- Elastic IP Address

Amazon Elastic IP addresses (EIPs) are static, publicly accessible IPv4 addresses that are provided by AWS and can be assigned to various AWS resources, including Amazon EC2 instances, Elastic Load Balancers, and Network Address Translation (NAT) gateways. The Elastic IP addresses have been specifically designed to demonstrate persistence and can be easily linked or unlinked with various AWS resources as per the requirement. This feature allows the process of remapping public IP addresses to distinct instances or services, without requiring the modification of DNS records or the reconfiguration of other settings. The utilization of Elastic IP addresses offers a significant advantage in that it facilitates the separation of an instance or service from its underlying IP address. This feature can prove to be advantageous in situations where there is a need to transfer an instance

or service from one Availability Zone or region to another, or when it becomes necessary to substitute an instance owing to hardware malfunction or other related concerns. Elastic IP addresses offer a means of allocating a persistent IP address to AWS resources, thereby facilitating applications that necessitate a stable IP address for licensing or security motives. It is noteworthy that AWS imposes a small hourly charge for each Elastic IP address that lacks association with a functional instance. Therefore, it is crucial to dispose any unutilized Elastic IP addresses to evade unnecessary expenses. In general, Elastic IP addresses serve as a valuable resource for effectively managing and preserving the network connectivity of one's AWS resources, while also guaranteeing the accessibility of applications and services from the global internet (Singhal, Khatri, & Singhal, 2022). Figure 3.13 illustrates the configuration implemented for attaching the EIP to the EC2 instance designated as the honeypot.

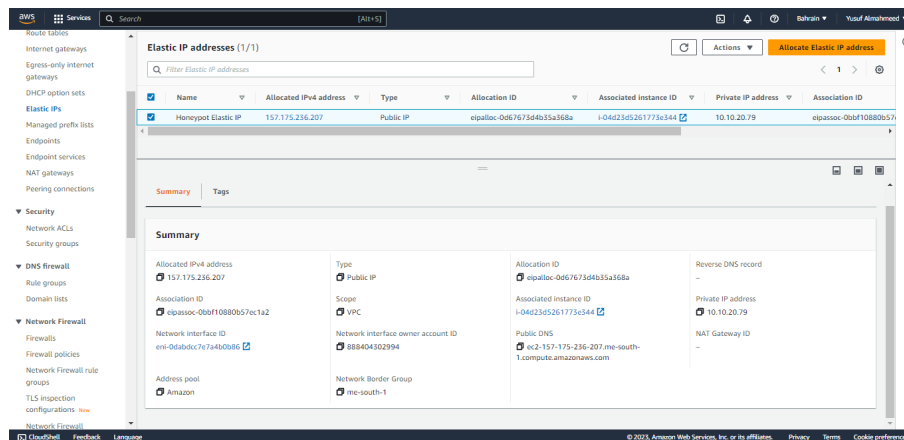


Figure 3.13: EIP Details

- Traffic Mirroring

The Traffic Mirroring functionality offered by AWS enables the replication of network traffic from an Elastic Network Interface (ENI) associated with an Amazon EC2 instance, and its subsequent trans-

mission to an Amazon VPC destination, such as an Amazon Elastic Load Balancer, a network appliance, or an Amazon S3 bucket. Traffic Mirroring enables the monitoring and analysis of network traffic of EC2 instances in almost real-time, without requiring the installation of additional software or agents on the instances. The utilization of this approach may prove useful in the identification and resolution of network-related problems, the evaluation of network efficiency, and the guarantee of adherence to security and regulatory standards. The Traffic Mirroring feature facilitates the mirroring of inbound and outbound traffic, and enables the selection of particular Elastic Network Interfaces (ENIs) and traffic categories for mirroring purposes. Filters can be customized to selectively intercept solely the network traffic that satisfies particular conditions, such as the source or destination IP address, port number, or protocol. The integration of Traffic Mirroring with additional AWS services, namely Amazon CloudWatch and Amazon S3, facilitates the provision of extensive monitoring and analysis functionalities. One possible application of Amazon CloudWatch Logs is to facilitate the storage and analysis of mirrored traffic, while Amazon S3 can be utilized to archive such traffic for extended periods of storage and analysis. In general, Traffic Mirroring is a potent and adaptable mechanism for observing and evaluating the network traffic of EC2 instances, which can enhance the efficiency, dependability, and protection of AWS infrastructure (Sutriyan, Sunaryadi, & Sinambela, 2022). To facilitate the mirroring of traffic from the EC2 interfaces to the Security Onion 2 sniffing interface, a three-step process must be executed. Firstly, a mirror filter should be established, as shown in figure 3.14 and figure 3.15.

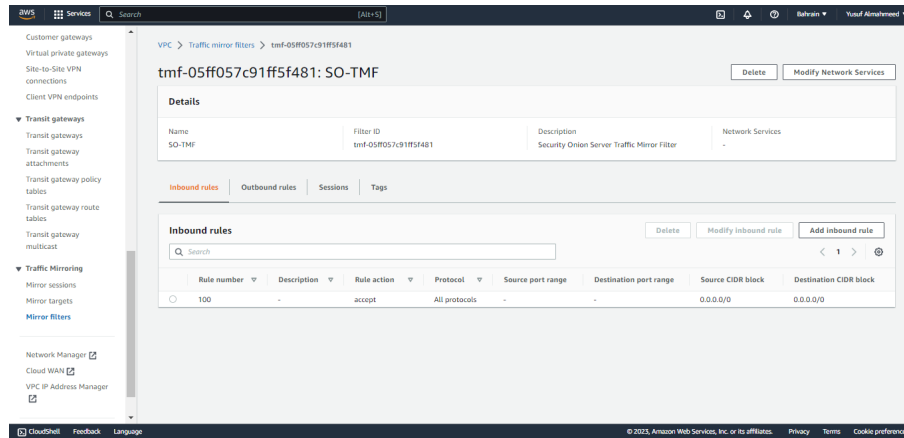


Figure 3.14: Mirror Inbound Filter Details

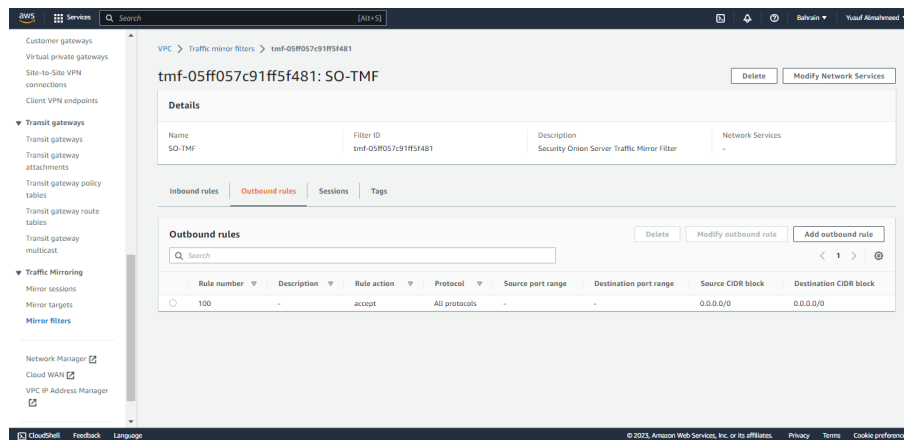


Figure 3.15: Mirror Outbound Filter Details

Subsequently, a mirror target must be created, wherein the Security Onion 2 sniffing interface is designated as the recipient for the mirrored traffic, as illustrated in figure 3.16. Finally, it is necessary to identify the EC2 interfaces within the mirror sessions, as illustrated in figure 3.17.

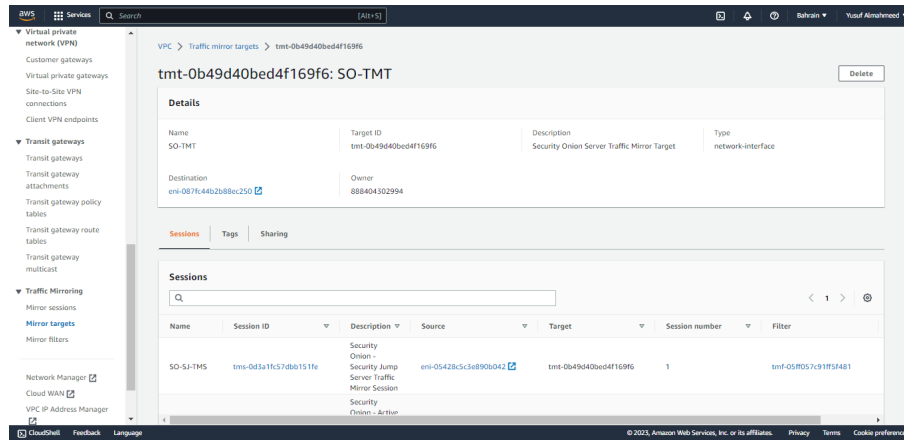


Figure 3.16: Mirror Target Details

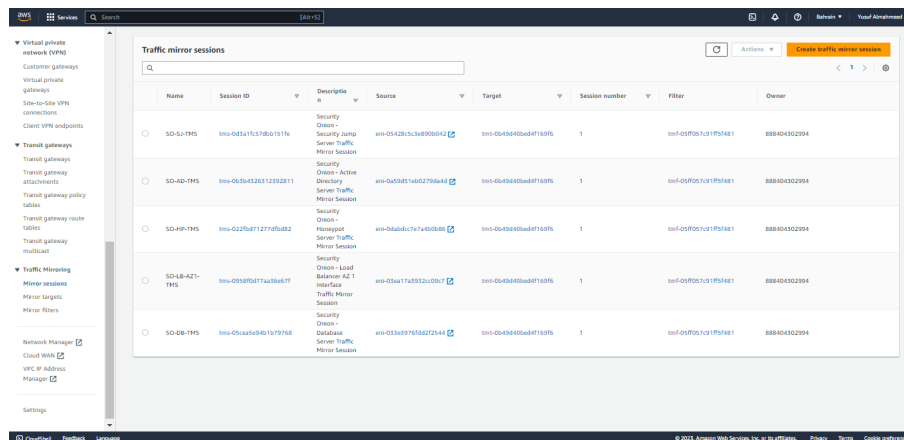


Figure 3.17: Mirror Sessions Details

- Servers

The main service offered by AWS that offers scalable processing capability in the cloud is called EC2. With a variety of configuration choices, EC2 enables customers to launch and operate virtual servers, also known as instances, on demand (Y. Ren, Zhao, Qin, & Zhu, 2020). Table 3.1 presents the servers that were used, while Table 3.2 provides information on their respective specifications.

- ALB

- Application Load Balancer

Table 3.1: AWS Servers

Name	OS	Type	IP Address	Security Group
Active Directory	Windows Server 2012 R2 Standard	t3.micro	10.10.30.36	Active Directory
Database Server			10.10.40.35	Database
Honeypot Server			10.10.20.79	Honeypot
Security Jump	10.10.50.44		Jump Server	
Web Server AZ1	Windows Server 2022 Datacenter		10.10.100.105	WEB
Web Server AZ2			10.10.10.128	
Security Onion 2	CentOS Linux release 7.9.2009 (Core)	t3.2xlarge	10.10.50.117	Security Onion 2 Server

Table 3.2: AWS Servers Specifications

Type	vCPU	CPU Credits/hour	Mem (GiB)	Storage	Network Performance (Gbps)
t3.micro	2	12	1	EBS-Only	Up to 5
t3.2xlarge	8	192	32	EBS-Only	Up to 5

The Amazon Web Services (AWS) platform offers an Application Load Balancer (ALB) service that facilitates the distribution of incoming application traffic among multiple targets, including but not limited to Elastic Compute Cloud (EC2) instances, Elastic Container Service (ECS) tasks, Lambda functions, or Internet Protocol (IP) addresses, across one or more Availability Zones. The Application Load Balancer (ALB) functions at Layer 7 of the Open Systems Interconnection (OSI) model. This implies that it has the capability to direct network traffic by taking into account application-level content, such as the URL path, host, or header fields. ALB is considered to be well-suited for the purpose of load balancing HTTP and HTTPS traffic, along with other application protocols that employ TCP or SSL/TLS. Several notable characteristics of ALB comprise: Periodic health assessments can be conducted by ALB through the transmission of requests to targets, followed by the verification of their response status codes to ensure their expected functionality. The Automatic Load Balancer (ALB) has the capability to dynamically modify the quantity of targets in response to fluctuations in traffic demand. This is

achieved through the utilization of either AWS Auto Scaling or EC2 Auto Scaling. The Application Load Balancer (ALB) has the capability to perform content-based routing, whereby it can direct incoming traffic to different target groups based on the characteristics of the request, such as the host header or URL path. The Application Load Balancer (ALB) has the capability to uphold affinity between a client and a designated target throughout a session by means of cookies or other techniques. This is commonly referred to as sticky sessions. The Application Load Balancer (ALB) has the capability to perform TLS termination, whereby it can effectively terminate SSL/TLS connections and decrypt the traffic prior to relaying it to the intended targets. This functionality can alleviate the targets from the responsibility of TLS processing, thereby reducing their workload. In general, ALB offers a solution that is capable of being scaled, highly accessible, and adaptable in order to effectively allocate incoming application traffic among numerous targets within the AWS environment. The integration of this particular element is deemed essential in numerous AWS frameworks as it has the potential to enhance the accessibility, expandability, and efficacy of various applications (Saraswat & Tripathi, 2020). In order to establish an ALB, it is necessary to generate a target group that identifies the EC2 instances. As depicted in figure 3.18, there have developed two target groups. The initial cluster consists of real web servers, whereas the subsequent cluster include the honeypot server as shown in figure 3.19.

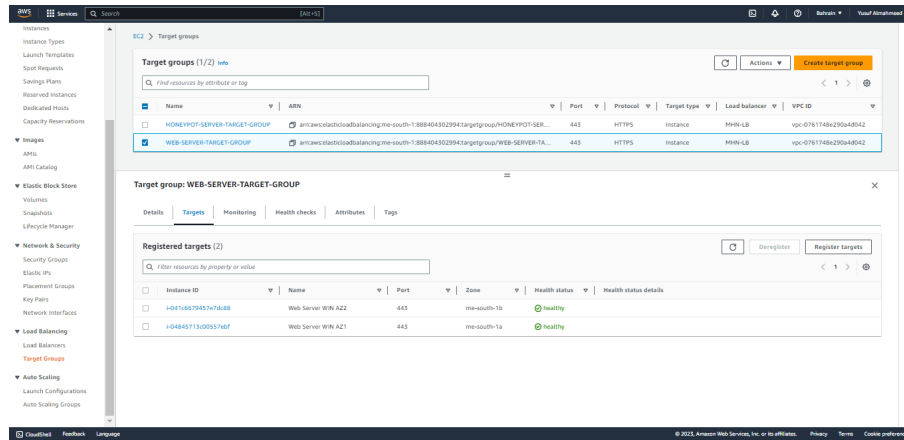


Figure 3.18: Web Servers Target Group Details

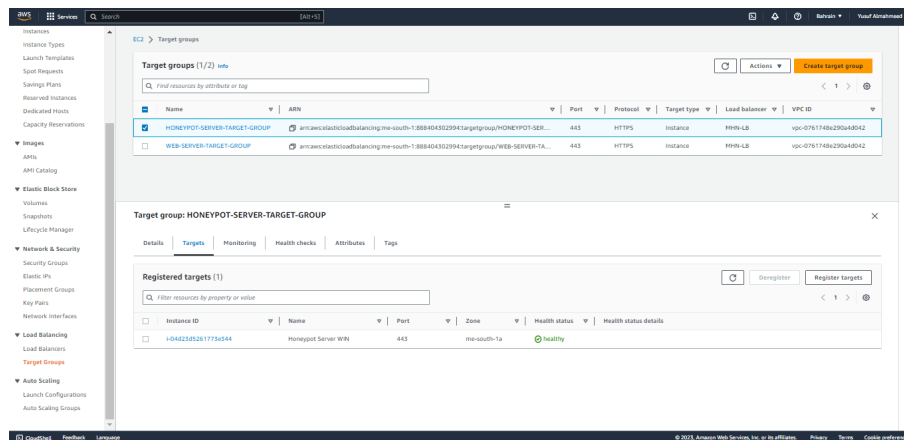


Figure 3.19: Honeypot Target Group Details

Figure 3.20 and figure 3.21 show the details of the MHN-LB.

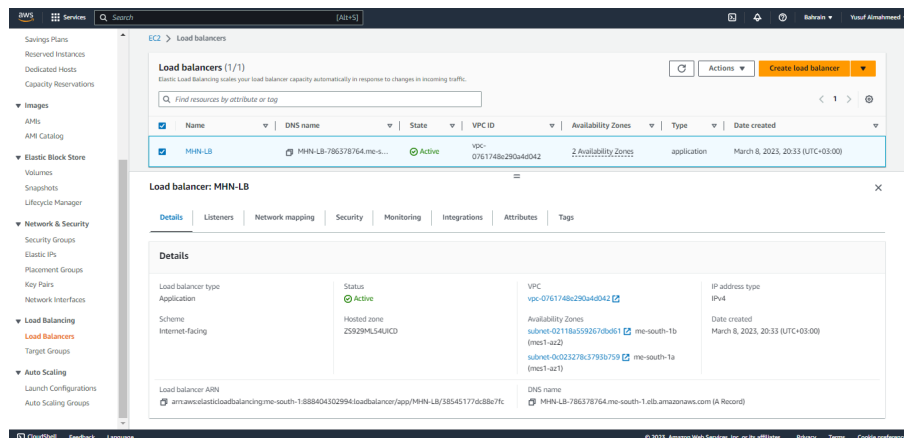


Figure 3.20: MHN ALB Details

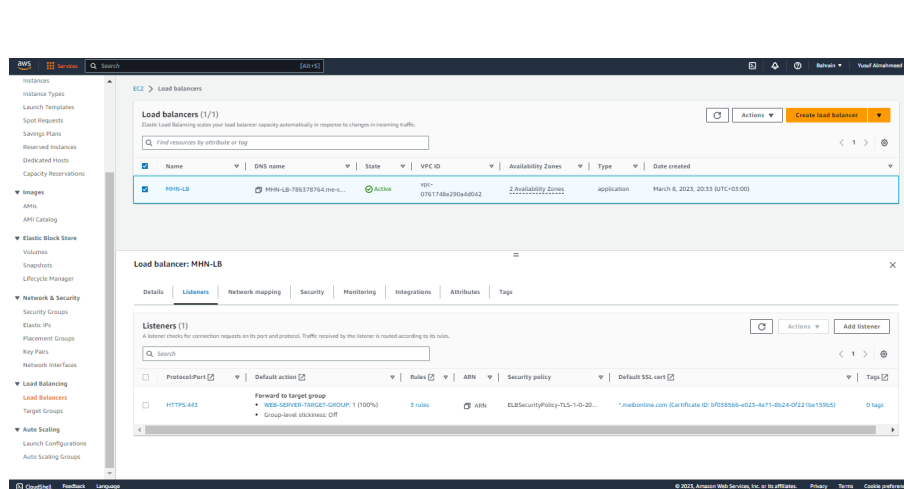


Figure 3.21: MHN ALB Listener Details

Figure 3.22 illustrates the configuration of the URL path rule and as can be seen the first two rules point the traffic to the honeypot target group which was showcased in figure 3.19 while the last rule forward the traffic to the real servers target group which was illustrated in figure 3.20

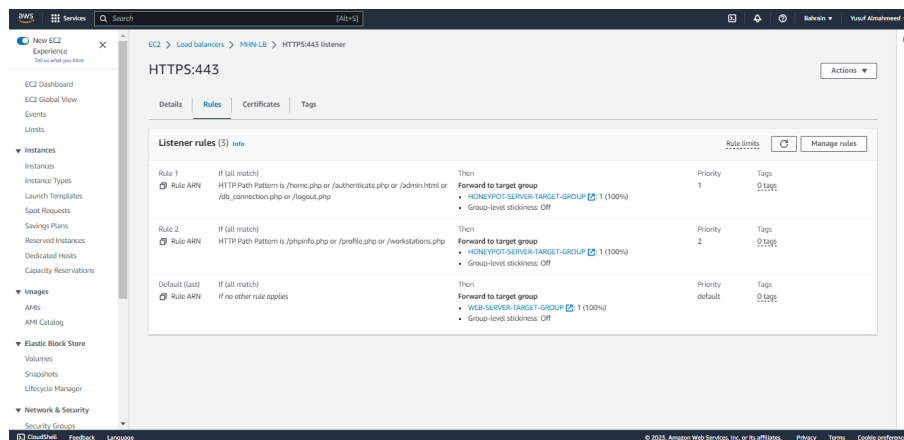


Figure 3.22: MHN ALB Listener Rules Details

• Security Groups

A security group functions as a virtual firewall that regulates the network traffic for one or multiple instances. When an instance is deployed in a VPC, it can be assigned one or more security groups to

the instance. Each security group contains a set of rules that determine what traffic is allowed to reach the instances associated with the security group. The rules for a security group can be configured to allow or deny traffic based on the following parameters: The protocol employed by the traffic, such as TCP, UDP, or ICMP. Port Range: The port or range of ports used by the traffic (e.g., 80 for HTTP traffic or 22 for SSH traffic). Source or Destination: The IP address range or security group allowed to send or receive the traffic. In addition to inbound and outbound rules, security groups also have an implicit "deny all" rule that blocks all traffic that is not explicitly allowed by a rule. As a default, AWS furnishes a security group for each VPC that permits all outbound traffic and inbound traffic only from instances linked with the corresponding security group. It is possible to generate additional security groups and link them to instances in accordance with particular security prerequisites. In general, security groups offer an effective and adaptable mechanism for managing the flow of network traffic to and from instances within the AWS environment. They are a key component of the AWS security model and help to protect instances from unauthorized access (Neto et al., 2021). Table 3.3 displays the security groups that have been configured.

Table 3.3: Security Groups

Name	Rule Type	Protocol	Port	IP Address	Description
Security Onion 2 Server	Inbound/Ingress	All traffic	All	10.10.50.44/32	Jump Server Access
	Inbound/Ingress	tcp	22	87.237.194.169/32	Aministrative Access
	Outbound/Egress	All traffic	All	0.0.0.0/0	Internet Access
Database	Inbound/Ingress	All traffic	All	10.10.30.0/24	Active Directory Access
	Inbound/Ingress	All traffic	All	10.10.20.0/24	Honeypot Access
	Inbound/Ingress	tcp	3389	87.236.142.34/32	Aministrative Access
	Outbound/Egress	All traffic	All	0.0.0.0/0	Internet Access
Jump Server	Inbound/Ingress	tcp	3389	87.237.194.169/32	Aministrative Access
	Outbound/Egress	All traffic	All	0.0.0.0/0	Internet Access
Load Balancer	Inbound/Ingress	tcp	443	0.0.0.0/0	Public Users HTTPS Access
	Outbound/Egress	All traffic	All	0.0.0.0/0	Internet Access
Web	Inbound/Ingress	tcp	80	0.0.0.0/0	Public Users HTTP Access
	Inbound/Ingress	All traffic	All	89.148.30.100/32	Aministrative Access
	Inbound/Ingress	tcp	443	0.0.0.0/0	Public Users HTTPS Access
	Outbound/Egress	All traffic	All	0.0.0.0/0	Internet Access
Active Directory	Inbound/Ingress	All traffic	All	10.0.0.0/8	Active Directory Access
	Inbound/Ingress	tcp	3389	109.63.89.174/32	Aministrative Access
	Outbound/Egress	All traffic	All	0.0.0.0/0	Internet Access
Honeypot	Inbound/Ingress	tcp	80	0.0.0.0/0	Public Users HTTP Access
	Inbound/Ingress	All traffic	All	10.10.30.0/24	Active Directory Access
	Inbound/Ingress	tcp	3389	0.0.0.0/0	Public Users RDP Access
	Inbound/Ingress	tcp	443	0.0.0.0/0	Public Users HTTPS Access
	Outbound/Egress	All traffic	All	0.0.0.0/0	Internet Access
Sniffing Interface	Inbound/Ingress	udp	4789	10.10.30.0/24	Infrastructure Subnet VXLAN Traffic Log Access
	Inbound/Ingress	udp	4789	10.10.100.0/24	Load Balancer Subnet VXLAN Traffic Log Access
	Inbound/Ingress	udp	4789	10.10.10.0/24	Public Subnet VXLAN Traffic Log Access
	Inbound/Ingress	udp	4789	10.10.40.0/24	Database Subnet VXLAN Traffic Log Access
	Inbound/Ingress	udp	4789	10.10.20.0/24	Honeypot Subnet VXLAN Traffic Log Access
	Outbound/Egress	All traffic	All	0.0.0.0/0	Internet Access

- Database

MySQL is a popular Relational Database Management System (RDBMS) utilized in web and application development, which operates as an open-source system. The software is both developed and maintained by Oracle Corporation. MySQL is a widely adopted option for the storage and administration of organized data, such as customer records, product inventories, and financial information. The software offers extensive support for various data types, such as numeric, textual, temporary, and binary data. Additionally, it incorporates robust functionalities for querying, indexing, and administering vast data collections. MySQL is renowned for its high level of performance, scalabil-

ity, and dependability. The system has been specifically engineered to manage workloads characterized by high volume and high transaction rates. It is adaptable in its applicability, being suitable for deployment in various situations ranging from modest web applications to extensive enterprise-level systems. MySQL facilitates the integration with diverse programming languages, such as PHP, Java, Python, and C++, by offering language-specific connectors and libraries. MySQL is a highly customizable and extensible database management system that benefits from a large and active community of developers and users who contribute to its ongoing development and maintenance. The software is obtainable under an open-source license, thereby rendering it free of charge for utilization and distribution. In general, MySQL is a robust and adaptable database management system that has the capability to cater to a variety of web and application development scenarios. It offers a dependable and expandable approach to handling organized data (Zoratti, 2006). Using MySQL two distinct tables were generated within the admins schema. The initial table includes to users and is presented in figure 3.23, while the second table includes to servers and appears in figure 3.24.

id	username	password	email	first_name	last_name
1	Muhammad.Abd...	\$2\$10\$R0eJA...	Muhammad.Abd...	Muhammad	Abdolan
2	Ahmed.Ah	\$2\$10\$BauH7T...	Ahmed.Ah@web...	Ahmed	Ah
3	Fatma.Khalifa	\$2\$10\$0GJ4UQ...	Fatma.Khalifa@...	Fatma	Khalifa
4	Omar.Mahmoud	\$2\$10\$1p34B...	Omar.Mahmoud@...	Omar	Mahmoud
5	Alaha.Hassan	\$2\$10\$Eq15p...	Alaha.Hassan@...	Alaha	Hassan

Figure 3.23: Users Table Details

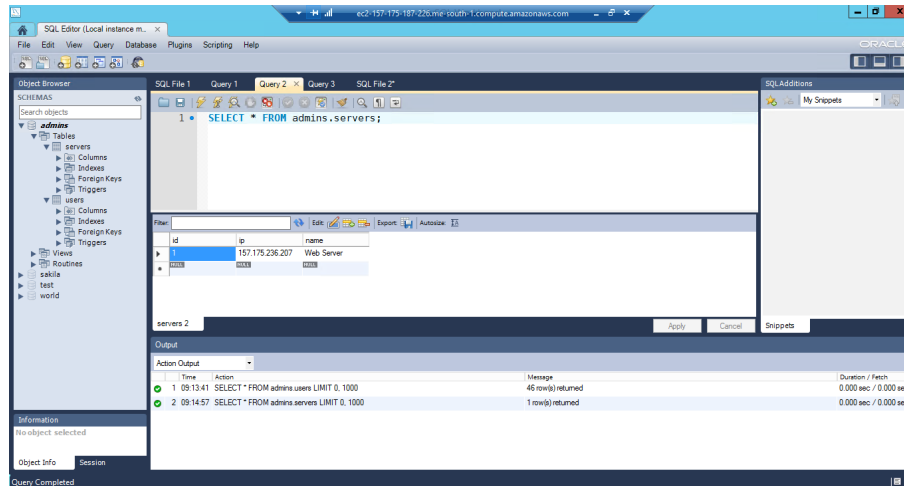


Figure 3.24: Servers Table Details

- Web Servers

Apache Friends has developed XAMPP, which is a web server solution that is both free and open-source. The package offers a convenient installation process that includes the Apache HTTP Server, MySQL database, PHP scripting language, and additional tools that are beneficial for web development and testing. XAMPP is a self-contained and cross-platform web server solution that is intended to be installed and utilized on diverse operating systems, such as Windows, Linux, and macOS. Local development and testing of web applications and websites is a common practice among developers and web designers, prior to their deployment on a live server. XAMPP offers a straightforward interface for administering the web server and its components, and includes pre configurations for prevalent web development situations. In addition, the software package encompasses the PHPMyAdmin utility, which facilitates the administration of MySQL databases, alongside additional beneficial tools, including the FileZilla FTP client and the Mercury Mail Transport System. XAMPP is extremely helpful due to its user-friendly interface and adaptable nature. The software can be swiftly installed and con-

figured, and may be customized to meet the requirements of diverse web development activities. Furthermore, it offers a mobile and independent environment for the development of web-based applications, thereby facilitating the examination and modification of web applications and websites. In general, XAMPP is a widely utilized and useful instrument for web development and experimentation, offering a practical and user-friendly approach to configuring a web server environment locally (Joshi et al., 2022). The latest version of the XAMPP application which is version 8.2.0 have been used in the real web servers. The web servers were configured on the most current operating system, specifically Windows Server 2022 Datacenter, and The HTML files possess the structure represented in figure 3.25.

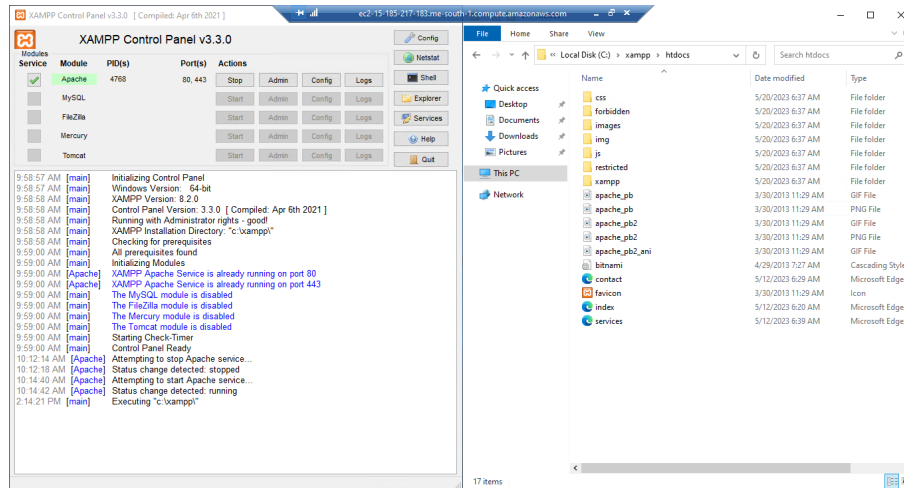
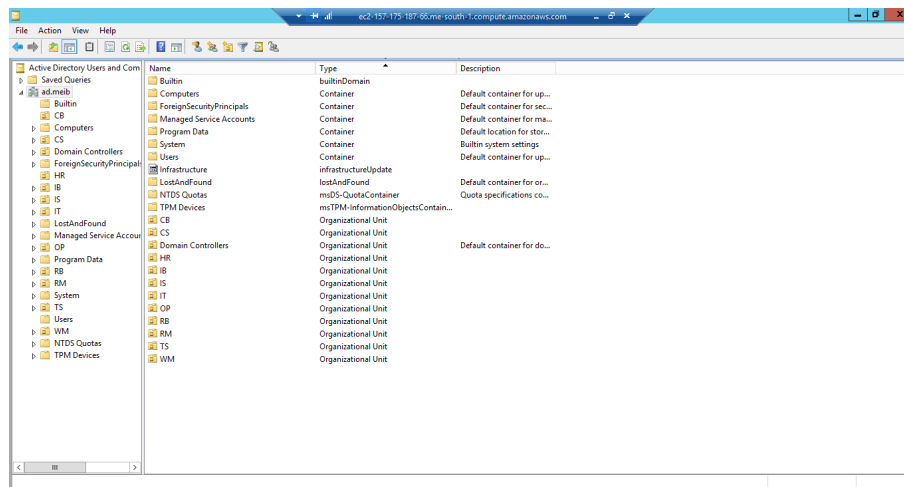


Figure 3.25: Web Server Configuration

- Active Directory

The Active Directory (AD) is a directory service that has been created by Microsoft. It serves as a centralized database for the purpose of managing and storing information about various network resources, including but not limited to users, computers, and applications, within a Windows domain network. Active Directory offers a structured,

object-based hierarchy for the purpose of arranging and administering network assets. The system is founded on the Lightweight Directory Access Protocol (LDAP) and offers a range of functionalities and services for the purpose of administering security, authentication, and access control within a Windows domain setting. User and group management is considered to be a fundamental aspect of Active Directory. Active Directory facilitates the creation and administration of user and group accounts, as well as the allocation of access rights and permissions to resources in accordance with their respective roles and responsibilities. In general, Active Directory is a robust and adaptable directory service that can aid establishments of different sizes in administering and safeguarding their network resources, while guaranteeing that users and computers possess the requisite levels of authorization and access to execute their duties (Srinivasa, Pedersen, & Vasilomanolakis, 2022). The environment's active directory comprised 10 distinct Organization Units figure 3.26 and a total of 46 unique users, as displayed in Table 3.4.



Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
ForeignSecurityPrincipals	Container	Default container for sec...
Managed Service Accounts	Container	Default container for msa...
Program Data	Container	Default location for stor...
System	Container	Builtin system settings
Users	Container	Default container for up...
Infrastructure	infrastructureUpdate	
LostAndFound	lostAndFound	Default container for or...
NTDS Quotas	msDS-QuotaContainer	Quota specifications co...
TPM Devices	msTPM-InformationObjectsContain...	
CB	Organizational Unit	
CS	Organizational Unit	
Domain Controllers	Organizational Unit	Default container for do...
HR	Organizational Unit	
IB	Organizational Unit	
IS	Organizational Unit	
IT	Organizational Unit	
OP	Organizational Unit	
RB	Organizational Unit	
RM	Organizational Unit	
TS	Organizational Unit	
WM	Organizational Unit	

Figure 3.26: Active Directory OU Details

Table 3.4: Active Directory Users

First Name	Initials	Last Name	Username	Email	Street Address	City	Zip Code	State	Country	Department	Password	Telephone	Job Title	Company	OU
Muhammad	MA	Abdullah	Muhammad.Abdullah	Muhammad.Abdullah@meibonline.com	Road 2835, Building 2672	Manama	428	Capital Governorate	BH	IT	Spring_2023	33678901	Engineer	MEIB	OU=IT
Ahmed	AA	Ali	Ahmed.Ali	Ahmed.Ali@meibonline.com	Road 84, Building 261	Juffair	408	Capital Governorate	BH	IT	blu3berry5!	39876543	Manager	MEIB	OU=IT
Fatima	FK	Khalifa	Fatima.Khalifa	Fatima.Khalifa@meibonline.com	Road 1803, Building 470	Muharraq	318	Muharraq Governorate	BH	IT	5am0ou3r@	66789012	Engineer	MEIB	OU=IT
Omair	OM	Mahmoud	Omair.Mahmoud	Omair.Mahmoud@meibonline.com	Road 4659, Building 2746	Riffa	346	Southern Governorate	BH	IT	cr@ry8all	22345678	Teamleader	MEIB	OU=IT
Aisha	AH	Hassan	Aisha.Hassan	Aisha.Hassan@meibonline.com	Road 3601, Building 1097	Adliya	536	Capital Governorate	BH	IT	p@nt2day	55567890	Engineer	MEIB	OU=IT
Hassan	HM	Mohammed	Hassan.Mohammed	Hassan.Mohammed@meibonline.com	Road 5412, Building 722	Hidd	554	Muharraq Governorate	BH	IT	4wedn3u3!	78901234	Manager	MEIB	OU=IT
Mariam	MA	Abdullah	Mariam.Abdullah	Mariam.Abdullah@meibonline.com	Road 3417, Building 93	Isa Town	634	Central Governorate	BH	IT	0b3y3#1	33345678	Engineer	MEIB	OU=IT
Khalid	KS	Salah	Khalid.Salah	Khalid.Salah@meibonline.com	Road 1705, Building 1597	Muharraq	317	Muharraq Governorate	BH	IT	2gethe@	44467890	Engineer	MEIB	OU=IT
Hala	HA	Al-Saud	Hala.Al-Saud	Hala.Al-Saud@meibonline.com	Road 1010, Building 24	Saunabis	410	Capital Governorate	BH	IT	r@inbow#7	77789012	Engineer	MEIB	OU=IT
Nasser	NA	Al-Mansour	Nasser.Al-Mansour	Nasser.Al-Mansour@meibonline.com	Road 2801, Building 2750	ecf	428	Capital Governorate	BH	IT	b0d&dk@ve	22349012	Engineer	MEIB	OU=IT
Rania	RA	Al-Amin	Rania.Al-Amin	Rania.Al-Amin@meibonline.com	Road 1511, Building 140	Jidhafs	215	Capital Governorate	BH	RB	s3cret5auce	55567890	Teller	MEIB	OU=RB
Ali	AA	Ahmed	Ali.Ahmed	Ali.Ahmed@meibonline.com	Road 2503, Building 618	Tubli	425	Capital Governorate	BH	RB	9!wes&k!@ugh5	67891234	Analyst	MEIB	OU=RB
Khalifa	KF	Fatima	Khalifa.Fatima	Khalifa.Fatima@meibonline.com	Road 5726, Building 240	Hamala	257	Northern Governorate	BH	RB	c@ndyShop	33347890	Manager	MEIB	OU=RB
Mahmoud	MO	Omair	Mahmoud.Omair	Mahmoud.Omair@meibonline.com	Road 407, Building 69	Isa Town	704	Central Governorate	BH	RB	6dowcV5	44479012	Accountant	MEIB	OU=RB
Hassan	HA	Aisha	Hassan.Aisha	Hassan.Aisha@meibonline.com	Road 1701, Building 277	Muharraq	317	Muharraq Governorate	BH	RB	l@q@h@l@b@l	77761234	Advisor	MEIB	OU=RB
Mohammed	MH	Hassan	Mohammed.Hassan	Mohammed.Hassan@meibonline.com	Road 1412, Building 109	Muharraq	314	Muharraq Governorate	BH	CS	won&cland#	22347890	Loan Officer	MEIB	OU=CS
Abdullah	AM	Mariam	Abdullah.Mariam	Abdullah.Mariam@meibonline.com	Road 3623, Building 432	Adliya	536	Capital Governorate	BH	CS	1&and3im3	55569012	Underwriter	MEIB	OU=CS
Salah	SK	Khalid	Salah.Khalid	Salah.Khalid@meibonline.com	Road 2801, Building 563	Seef	428	Capital Governorate	BH	CS	gr33a3y3a!	67891234	Clerk	MEIB	OU=CS
Hala	HA	Al-Saud	Khalid.Al-Saud	Khalid.Al-Saud@meibonline.com	Road 1504, Building 249	Muharraq	315	Muharraq Governorate	BH	CB	z3be@pint	33341234	Auditor	MEIB	OU=CB
Nasser	NA	Al-Mansour	Muhammad.Al-Mansour	Muhammad.Al-Mansour@meibonline.com	Road 1125, Building 1237	Mahoor	341	Capital Governorate	BH	CB	7h3arh&at	44465678	Consultant	MEIB	OU=CB
Sara	SA	Al-Amin	Sara.Al-Amin	Sara.Al-Amin@meibonline.com	Road 2825, Building 2431	Seef District	428	Capital Governorate	BH	CB	m@nlight5	77789012	Trader	MEIB	OU=CB
Youssef	YS	Salim	Youssef.Salim	Youssef.Salim@meibonline.com	Road 3622, Building 27	Adliya	536	Capital Governorate	BH	CB	tr@v3ld@ry	22347890	Branch Manager	MEIB	OU=CB
Muna	MA	Ahmed	Muna.Ahmed	Muna.Ahmed@meibonline.com	Road 436, Building 180	Isa Town	704	Central Governorate	BH	TS	c@ptain@merica	55561234	Compliance Officer	MEIB	OU=TS
Samir	SH	Haddad	Samir.Haddad	Samir.Haddad@meibonline.com	Road 3802, Building 7	Mahoor	338	Capital Governorate	BH	TS	3y3o@h3ig3r	67879012	Risk Manager	MEIB	OU=TS
Sara	SA	Al-Salem	Sara.Al-Salem	Sara.Al-Salem@meibonline.com	Road 2124, Building 23	Muharraq	321	Muharraq Governorate	BH	IB	h&ll&st&6	33341234	Investment Banker	MEIB	OU=IB
Tarek	TA	Abadi	Tarek.Abadi	Tarek.Abadi@meibonline.com	Road 2508, Building 812	Seef	428	Capital Governorate	BH	IB	U3mon&3@	44467890	Actuary	MEIB	OU=IB
Laila	LA	Abdel-Aziz	Laila.Abel-Aziz	Laila.Abel-Aziz@meibonline.com	Road 1510, Building 342	Muharraq	315	Muharraq Governorate	BH	IB	4th@july#	77791234	Credit Officer	MEIB	OU=IB
Ziad	ZK	Khalid	Ziad.Khalid	Ziad.Khalid@meibonline.com	Road 5718, Building 200	Hamala	257	Northern Governorate	BH	IB	2f@z2f&urhus	22347890	Economist	MEIB	OU=IB
Mona	MA	Al-Omari	Mona.Al-Omari	Mona.Al-Omari@meibonline.com	Road 2513, Building 686	Seef District	428	Capital Governorate	BH	IS	k3&ur&cl3b3@st	55561234	Financial Planner	MEIB	OU=IS
Ahmed	AA	Al-Khatib	Ahmed.Al-Khatib	Ahmed.Al-Khatib@meibonline.com	Road 4023, Building 530	Saar	940	Northern Governorate	BH	IS	s@ndc@sd3s	67879012	Operations Specialist	MEIB	OU=IS
Fatima	FA	Al-Jaber	Fatima.Al-Jaber	Fatima.Al-Jaber@meibonline.com	Road 2707, Building 113	Muharraq	327	Muharraq Governorate	BH	WM	5@r@gh3r	33347890	Portfolio Manager	MEIB	OU=WM
Omair	QA	Al-Rashid	Omair.Al-Rashid	Omair.Al-Rashid@meibonline.com	Road 3841, Building 100	Mahoor	338	Capital Governorate	BH	WM	fl3cr@h3r3	44467890	Quantitative Analyst	MEIB	OU=WM
Aisha	AA	Al-Zahrani	Aisha.Al-Zahrani	Aisha.Al-Zahrani@meibonline.com	Road 2508, Building 1124	Seef	428	Capital Governorate	BH	WM	m@p&c@77	77791234	Relationship Manager	MEIB	OU=WM
Hassan	HA	Al-Mahdi	Hassan.Al-Mahdi	Hassan.Al-Mahdi@meibonline.com	Road 1803, Building 379	Muharraq	318	Muharraq Governorate	BH	WM	9&1&3@	22349012	Trust Officer	MEIB	OU=WM
Mariam	MA	Al-Qubani	Mariam.Al-Qubani	Mariam.Al-Qubani@meibonline.com	Road 2512, Building 998	Seef District	428	Capital Governorate	BH	RM	r&ck3m&as	55567890	Wealth Advisor	MEIB	OU=RM
Khalid	KA	Al-Ghandi	Khalid.Al-Ghandi	Khalid.Al-Ghandi@meibonline.com	Road 302, Building 10	Manama	320	Capital Governorate	BH	RM	b3&ff&3&@p	67891234	Teamleader	MEIB	OU=RM
Hala	HA	Al-Harbi	Hala.Al-Harbi	Hala.Al-Harbi@meibonline.com	Road 1801, Building 164	Muharraq	318	Muharraq Governorate	BH	OP	c@piv@t3m#	33345678	Operations Specialist	MEIB	OU=OP
Nasser	NA	Al-Qassim	Nasser.Al-Qassim	Nasser.Al-Qassim@meibonline.com	Road 2514, Building 26	Seef District	428	Capital Governorate	BH	OP	1c3cr3@n&5	44467890	Relationship Manager	MEIB	OU=OP
Rania	RA	Al-Abdulwahed	Rania.Al-Abdulwahed	Rania.Al-Abdulwahed@meibonline.com	Road 311, Building 144	Muharraq	331	Muharraq Governorate	BH	OP	s1v3&ur&er	77789012	Wealth Advisor	MEIB	OU=OP
Ali	AA	Al-Dossari	Ali.Al-Dossari	Ali.Al-Dossari@meibonline.com	Road 122, Building 15	Mahoor	336	Capital Governorate	BH	OP	g@mingfl3r3r	22347890	Financial Planner	MEIB	OU=OP
Khalifa	KA	Al-Shammari	Khalifa.Al-Shammari	Khalifa.Al-Shammari@meibonline.com	Road 2408, Building 24	Seef District	428	Capital Governorate	BH	OP	6r@ndom3s	55567890	Credit Officer	MEIB	OU=OP
Mahmoud	MA	Al-Mohsen	Mahmoud.Al-Mohsen	Mahmoud.Al-Mohsen@meibonline.com	Road 1703, Building 164	Muharraq	317	Muharraq Governorate	BH	OP	4&gryb3rd3	67891234	Auditor	MEIB	OU=OP
Hassan	HA	Al-Faris	Hassan.Al-Faris	Hassan.Al-Faris@meibonline.com	Road 2508, Building 28	Seef	428	Capital Governorate	BH	HR	t3&h33&#	33349012	Consultant	MEIB	OU=HR
Mohammed	MA	Al-Sulaiman	Mohammed.Al-Sulaiman	Mohammed.Al-Sulaiman@meibonline.com	Road 2503, Building 9	Tubli	425	Capital Governorate	BH	HR	7&un&h3	44467890	Trader	MEIB	OU=HR
Abdullah	AA	Al-Qurashi	Abdullah.Al-Qurashi	Abdullah.Al-Qurashi@meibonline.com	Road 201, Building 52	anama	320	Capital Governorate	BH	HR	0@r&g3&rd3s	77761234	Branch Manager	MEIB	OU=HR
Salah	SA	Al-Zaidi	Salah.Al-Zaidi	Salah.Al-Zaidi@meibonline.com	Road 3420, Building 175	Isa Town	634	Central Governorate	BH	HR	p3p3&3&mm@	22347890	Financial Planner	MEIB	OU=HR

• Honeypot Server

The honeypot server was established on an outdated vulnerable operating system, specifically Windows Server 2022 Datacenter, and an obsolete XAMPP application, version 1.8.3. The HTML and PHP files possess a structure as shown in figure 3.27.

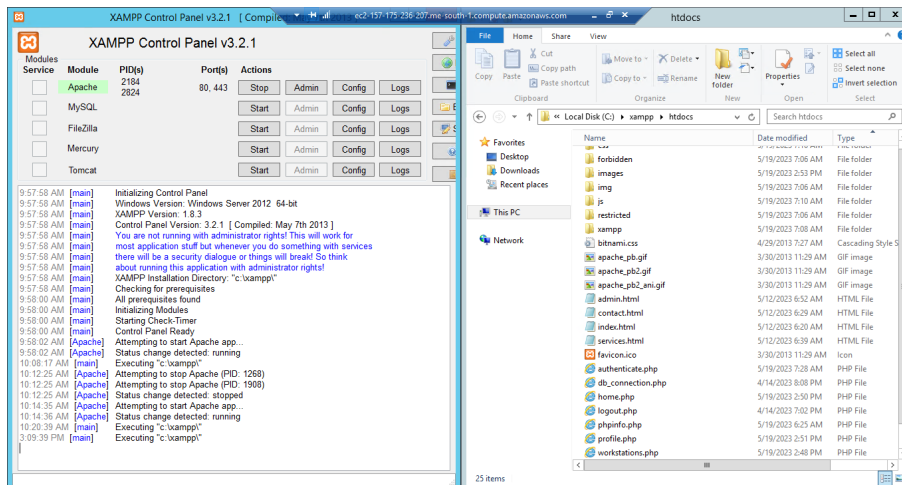


Figure 3.27: Honeypot Server Configuration

3.8 Summary

In conclusion, the proposed methodology for the thesis entails a meticulous and methodical research design that encompasses data collection, analysis, evaluation, and interpretation. The design of the study is aimed at ensuring the validity and reliability of the research methodology, as well as the practical applicability and significance of the obtained results. In addition This section of the thesis presents a thorough description of the proposed framework, which comprises four main components: The study presents a comprehensive overview of a proposed framework, including its components, design, and implementation. The initial two segments expounded upon the framework's structure, with a particular emphasis on the significance of inter-team collaboration and communication throughout the detection and response procedures. The design segment defines the configuration of every layer within the framework, along with the diverse tools and methodologies that can be employed in each layer. Furthermore, the segment addresses the execution of the framework, encompassing the setup of the MHN, the utilization of threat intelligence feeds, and the creation of a mechanism for identifying suspicious activity. In summary, the framework put forth offers an integrated plan for identifying and addressing zero-day attacks, incorporating proactive and responsive tactics to bolster system security. The successful implementation of the framework requires inter-team collaboration and the utilization of diverse tools and methodologies to efficiently identify and counter zero-day attacks.

Chapter 4

Results and Evaluation

4.1 Introduction

The results section is a crucial element of a research study as it presents the research findings and evaluates the hypothesis's validity. This section presents the outcomes of the study, covering the effectiveness of the suggested approach, the accuracy of the detection mechanism, and the capacity to reduce false positives. The assessment conducted offers a thorough evaluation of the feasibility and efficacy of our methodology, showcasing its capacity to improve the security posture of organizations against zero-day attacks.

4.2 Description of the evaluation methodology

The methodology for evaluation covers an in-depth assessment of the efficacy of the suggested solution in identifying zero-day attacks. The assess-

ment methodology consists of three primary components, including data gathering, experimentation, and performance evaluation.

The process of data collection includes gathering and preparing a diverse set of network traffic data, comprising both normal and malicious traffic. Subsequently, the gathered data is used to evaluate the effectiveness of the suggested solution in identifying zero-day attacks.

The phase of experimentation entails the execution of the proposed solution on the gathered data and evaluation of its efficacy in comparison to various forms of attacks. The metrics included in this study comprise of the detection rate, false-positive rate, and the duration required to identify a zero-day attack. The experiment is repeated on several occasions to ascertain the precision and uniformity of the outcomes.

The process of performance evaluation entails the comparison of the performance of a proposed solution with that of other solutions already available in the market. This comparative analysis is conducted utilizing a consistent set of metrics in order to determine the viability of the proposed solution in relation to alternative solutions.

The evaluation methodology employed in this thesis endeavors to present a thorough evaluation of the efficacy of the proposed solution in detecting zero-day attacks, its accuracy in reducing false positives, and its capacity to improve the security posture of organizations against zero-day attacks.

4.3 Results of the evaluation

The data collection process is currently underway, facilitated by a survey that has been designed and disseminated among cybersecurity experts to evaluate the hypotheses.

Table 4.1 displays the results of the survey. It is clear that a majority of the respondents are situated in Bahrain, with the remaining are from India.

Table 4.1: Survey Results

First Name	Last Name	Country	Email Address	Access to the Survey	Years of Experience	Operating System
Sehrish	Riaz	Bahrain	Sehrish.riaz92@gmail.com	LinkedIn	1	Linux
Hamad	Alnakal		info@hamadalnakal.tech		5	
Qusai	Alhaddad		qusai.alhaddad@gmail.com		23	
Mohamed	Ismaeel		Mohd89ali@gmail.com	Social media	2	Linux and Windows
Muhammad	Afaq		aafaq86@gmail.com	LinkedIn	15	
Husain	Almahhari		Hussainalmahari@gmail.com		2	Kali Linux
Hasan	Alsaibai		Lealsaibai@outlook.com		7	
Mohamed	Ali		overpassthehash@gmail.com		4	
Saad	Alhiddi		S.alhiddi@gmail.com	Social media	2	
Faiyaz	Ahmed		faiyazahmad.online@gmail.com		3	
Naveen	Kumar	India	snaveenk1171@gmail.com	Referral	3	Kali Linux
Syed	Aslam khan		aslam.khan7666@yahoo.com		2	
Faiyaz	Ahmed		faiyazahmad.online@gmail.com		3	
Kishan	Kumar		Kishan.cyberhack@gmail.com		3	Windows

Additionally, the participants' experience in penetration testing spans from one to fifteen years, which makes them suitable for this study.

The report by Mohamed Ismaeel presents his findings, which are included in the appendix section located at the end of this report. The report submitted by Mohamed outlines the methods employed by him to successfully breach the MHN environment. The most important aspect of the report is that the Mohamed shared the report and believed that he had successfully breached the authentic production environment. However, it was subsequently determined that he had only compromised the MHN environment and subsequently stopped his hacking activities. This outcome serves as compelling evidence of the efficacy of the proposed solution, thereby corroborating the thesis hypothesis.

The analysis of figure 4.1 reveals a significant number of alerts with high severity levels, indicating ongoing attempts to attack the honeypot environment.

Count	rule name	event module	event severity_label
28	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	snortcata	high
14	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	snortcata	high
14	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	snortcata	high
6	ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response	snortcata	high
5	ET EXPLOIT MvPower DVR Shell UCE	snortcata	high
5	ET SCAN JAWS Webserver Unauthenticated Shell Command Execution	snortcata	high
5	ET SCAN Mirai Variant User-Agent (Inbound)	snortcata	high
3	ET POLICY Incoming Basic Auth Basic64 HTTP Password detected unencrypted	snortcata	high
2	ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010	snortcata	high
2	ET SCAN Torrcat admin blank login credentials	snortcata	high
1	ET EXPLOIT D-Link Devices Home Network Administration Protocol Command Execution	snortcata	high
1	ET EXPLOIT XiangmaHIScan DVR - Request for User Details - Possible CVE-2017-7577 Exploit Attempt	snortcata	high
1	ET HUNTING Suspicious Chmod Usage in URI (Inbound)	snortcata	high
1	ET POLICY PE EXE or DLL Windows file download HTTP	snortcata	high
1	ET WEB_SERVER Tilde in URI - potential php-source disclosure vulnerability	snortcata	high
1	ET WEB_SERVER WGET Command Specifying Output in HTTP Headers	snortcata	high

Figure 4.1: Security Onion 2 High Severity Alerts

In order to demonstrate that the attacks are directed towards the honeypot environment rather than a real environment, the ensuing figures will exhibit the destination/source private IP address of each alert. It is evident that none of the private IP addresses are associated with the real web servers.

As can be seen in figure 4.2 the Network Mapper (NMAP) scan is targeting 10.10.20.79 which is the Honeypot Server.

Timestamp	rule name	event severity_label	source ip	source port	destination ip	destination port
2023-05-23 18:42:11.041 +00:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	102.38.229.79	56348	10.10.20.79	80
2023-05-23 18:42:09.545 +00:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	102.38.229.79	53614	10.10.20.79	80
2023-05-23 18:52:38.823 +00:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	185.205.204.183	52582	10.10.20.79	80
2023-05-23 18:52:38.296 +00:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	185.205.204.183	52982	10.10.20.79	80
2023-05-23 18:52:37.582 +00:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	185.205.204.183	51888	10.10.20.79	80
2023-05-23 18:52:36.091 +00:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	185.205.204.183	50888	10.10.20.79	80
2023-05-23 18:52:35.618 +00:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	185.205.204.183	50622	10.10.20.79	80
2023-05-23 18:42:07.678 +00:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	102.38.229.79	58174	10.10.20.79	80
2023-05-23 18:48:44.360 +00:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	185.205.204.183	49888	10.10.20.79	80
2023-05-23 18:48:43.883 +00:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	185.205.204.183	49608	10.10.20.79	80
2023-05-23 18:42:06.648 +00:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	102.38.229.79	48344	10.10.20.79	80
2023-05-23 18:48:41.196 +00:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	185.205.204.183	48044	10.10.20.79	80
2023-05-23 18:42:04.942 +00:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	102.38.229.79	45382	10.10.20.79	80
2023-05-23 18:42:04.344 +00:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	102.38.229.79	44128	10.10.20.79	80

Figure 4.2: NMAP Scan Alert Details

In figure 4.3, figure 4.4 and figure 4.5 are related to EternalBlue and as can be seen is targeting 10.10.30.36 which is the Active Directory Server.

Security Onion - Alerts - Custom

Rule name: ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)

Timestamp	rule name	event severity_label	source ip	source port	destination ip	destination port
2023-05-23 21:07:12.371 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	high	101.225.68.26	49705	10.10.30.36	445
2023-05-23 20:29:29.655 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	high	178.205.246.217	4730	10.10.30.36	445
2023-05-24 04:52:05.322 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	high	103.126.240.158	50187	10.10.30.36	445
2023-05-24 05:43:40.862 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	high	105.106.144.129	56197	10.10.30.36	445
2023-05-24 05:48:42.179 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	high	14.249.188.204	51585	10.10.30.36	445
2023-05-24 06:13:05.591 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	high	190.121.233.212	63782	10.10.30.36	445
2023-05-24 06:26:35.647 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	high	178.211.17.154	5719	10.10.30.36	445
2023-05-24 04:58:51.213 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	high	14.141.236.56	46868	10.10.30.36	445
2023-05-24 06:32:17.570 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	high	117.247.92.4	57151	10.10.30.36	445
2023-05-24 08:01:21.078 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	high	82.207.94.18	52114	10.10.30.36	445
2023-05-24 07:06:45.293 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	high	178.134.39.10	62906	10.10.30.36	445
2023-05-24 04:07:27.278 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	high	119.40.80.130	64846	10.10.30.36	445
2023-05-24 01:04:38.473 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	high	177.36.200.93	55868	10.10.30.36	445
2023-05-24 03:09:02.317 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	high	103.135.96.50	61892	10.10.30.36	445

Version: 2.3.210 © 2023 Security Onion Solutions, LLC

Figure 4.3: EternalBlue Probe MS17-010 (Generic Flags) Alert Details

Security Onion - Alerts - Custom

Rule name: ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)

Timestamp	rule name	event severity_label	source ip	source port	destination ip	destination port
2023-05-23 21:07:12.371 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	high	101.225.68.26	49705	10.10.30.36	445
2023-05-23 20:29:29.655 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	high	178.205.246.217	4730	10.10.30.36	445
2023-05-24 04:52:05.322 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	high	103.126.240.158	50187	10.10.30.36	445
2023-05-24 05:43:40.862 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	high	105.106.144.129	56197	10.10.30.36	445
2023-05-24 05:48:42.179 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	high	14.249.188.204	51585	10.10.30.36	445
2023-05-24 06:13:05.591 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	high	190.121.233.212	63782	10.10.30.36	445
2023-05-24 06:26:35.647 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	high	178.211.17.154	5719	10.10.30.36	445
2023-05-24 04:58:51.213 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	high	14.141.236.56	46868	10.10.30.36	445
2023-05-24 06:32:17.570 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	high	117.247.92.4	57151	10.10.30.36	445
2023-05-24 08:01:21.078 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	high	82.207.94.18	52114	10.10.30.36	445
2023-05-24 07:06:45.293 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	high	178.134.39.10	62906	10.10.30.36	445
2023-05-24 04:07:27.278 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	high	119.40.80.130	64846	10.10.30.36	445
2023-05-24 01:04:38.473 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	high	177.36.200.93	55868	10.10.30.36	445
2023-05-24 03:09:02.317 +00:00	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	high	103.135.96.50	61892	10.10.30.36	445

Version: 2.3.210 © 2023 Security Onion Solutions, LLC

Figure 4.4: EternalBlue Probe MS17-010 (MSF style) Alert Details

Security Onion - Alerts - Custom

Options: Custom

Time Range: 2023/12/07 00:07:32 AM - 2023/05/24 08:07:32 AM

Rule name: ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response

Timestamp	rule name	event severity_label	source ip	source port	destination ip	destination port
2023-05-24 00:40:30.463 +00:00	ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response	high	10.10.30.36	445	118.167.89.179	52550
2023-05-24 00:40:37.625 +00:00	ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response	high	10.10.30.36	445	118.167.89.179	52550
2023-05-24 00:40:30.016 +00:00	ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response	high	10.10.30.36	445	118.167.89.179	52550
2023-05-24 00:50:18.119 +00:00	ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response	high	10.10.30.36	445	118.167.89.179	52863
2023-05-24 00:50:18.558 +00:00	ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response	high	10.10.30.36	445	118.167.89.179	52863
2023-05-24 00:50:25.734 +00:00	ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response	high	10.10.30.36	445	118.167.89.179	52863

Rows per page: 1000 1 of 6

Version: 2.3.210 © 2023 Security Onion Solutions, LLC

Figure 4.5: EternalBlue Probe MS17-010 Echo Response Alert Details

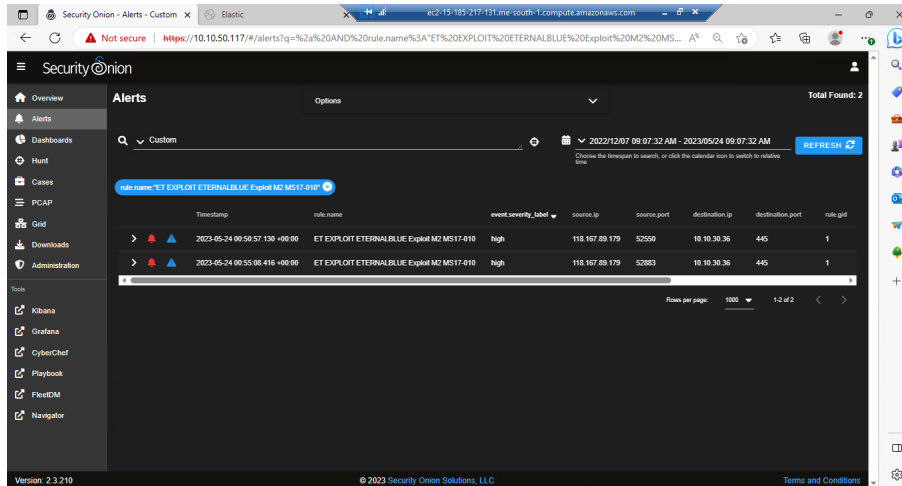


Figure 4.6: EternalBlue Exploit M2 MS17-010 Alert Details

The following figures show multiple attacks targeting 10.10.20.79 which is the Honeypot Server.

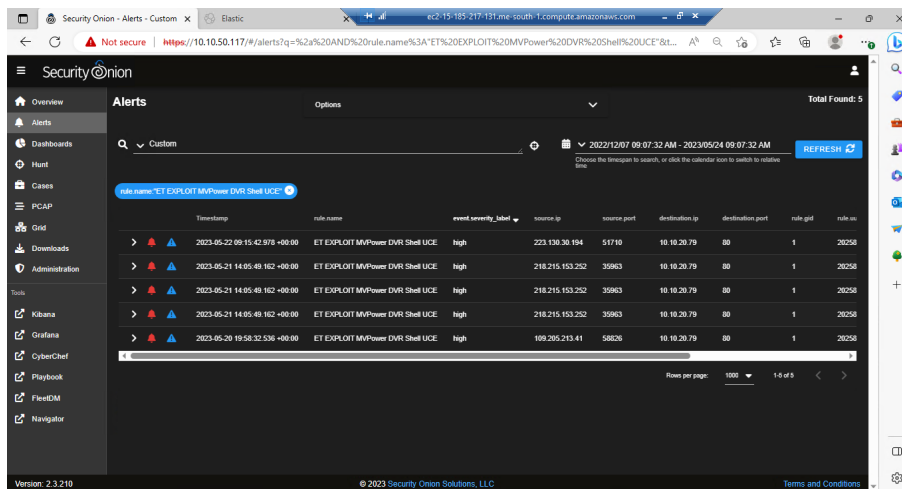


Figure 4.7: MvPower DVR Shell UCEs Alert Details

The screenshot shows the Security Onion Alerts page with a filter for 'Rule name: ET SCAN JAWS Webserver Unauthenticated Shell Command Execution'. The table displays 5 alerts with the following data:

Timestamp	Rule Name	Event Severity Label	Source IP	Source Port	Destination IP	Destination Port	Rule ID
2023-05-22 09:15:42.978 +00:00	ET SCAN JAWS Webserver Unauthenticated Shell Command Execution	high	223.130.30.194	51710	10.10.20.79	80	1
2023-05-21 14:05:49.102 +00:00	ET SCAN JAWS Webserver Unauthenticated Shell Command Execution	high	218.215.153.252	35963	10.10.20.79	80	1
2023-05-21 14:05:49.102 +00:00	ET SCAN JAWS Webserver Unauthenticated Shell Command Execution	high	218.215.153.252	35963	10.10.20.79	80	1
2023-05-21 14:05:49.102 +00:00	ET SCAN JAWS Webserver Unauthenticated Shell Command Execution	high	218.215.153.252	35963	10.10.20.79	80	1
2023-05-20 19:58:32.536 +00:00	ET SCAN JAWS Webserver Unauthenticated Shell Command Execution	high	109.205.213.41	58026	10.10.20.79	80	1

Figure 4.8: JAWS Webserver Unauthenticated Shell Command Execution Alert Details

The screenshot shows the Security Onion Alerts page with a filter for 'Rule name: ET SCAN Mirai Variant User-Agent (Inbound)'. The table displays 5 alerts with the following data:

Timestamp	Rule Name	Event Severity Label	Source IP	Source Port	Destination IP	Destination Port	Rule ID
2023-05-22 09:15:42.978 +00:00	ET SCAN Mirai Variant User-Agent (Inbound)	high	223.130.30.194	51710	10.10.20.79	80	1
2023-05-21 14:05:49.102 +00:00	ET SCAN Mirai Variant User-Agent (Inbound)	high	218.215.153.252	35963	10.10.20.79	80	1
2023-05-21 14:05:49.102 +00:00	ET SCAN Mirai Variant User-Agent (Inbound)	high	218.215.153.252	35963	10.10.20.79	80	1
2023-05-21 14:05:49.102 +00:00	ET SCAN Mirai Variant User-Agent (Inbound)	high	218.215.153.252	35963	10.10.20.79	80	1
2023-05-20 19:58:32.536 +00:00	ET SCAN Mirai Variant User-Agent (Inbound)	high	109.205.213.41	58026	10.10.20.79	80	1

Figure 4.9: Mirai Variant User-Agent Scan Alert Details

The screenshot shows the Security Onion Alerts page with a filter for 'Rule name: ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted'. The table displays 3 alerts with the following data:

Timestamp	Rule Name	Event Severity Label	Source IP	Source Port	Destination IP	Destination Port	Rule ID
2023-05-23 08:05:52.789 +00:00	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	high	106.47.102.251	55067	10.10.20.79	80	1
2023-05-23 08:05:52.789 +00:00	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	high	106.47.102.251	55067	10.10.20.79	80	1
2023-05-21 12:16:11.431 +00:00	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	high	195.170.172.138	55046	10.10.20.79	80	1

Figure 4.10: Basic Auth Base64 HTTP Password detected unencrypted Alert Details

4.4 Discussion of the results

The preceding findings offer compelling proof of the efficacy of the suggested approach in safeguarding authentic servers against zero-day assaults. The 100% protection rate achieved by the solution, combined with the fact that high alerts were only targeting the MHN environment, highlights the solution's ability to effectively isolate the MHN environment from the real servers and detect potential attacks in a targeted and efficient manner.

Furthermore, the 0% false positive rate achieved by the solution is a significant benefit, as false positives can be time-consuming and costly to investigate, and can also lead to complacency among security personnel, potentially leaving systems vulnerable to attack. The solution's capacity to produce alerts that are precisely aimed at the honeypot environment, which is exclusively accessible to attackers, guarantees that any alerts generated are highly probable to be suggestive of a genuine attack, thereby diminishing the probability of false positives.

Apart from the advantages conferred by the proposed solution, the utilization of Security Onion 2 as a framework for executing the solution presents various benefits. Security Onion 2 is an open-source platform that offers a variety of cybersecurity tools and capabilities, rendering it a remarkably adaptable and customizable solution that can be customized to suit the unique requirements of distinct organizations. Furthermore, Security Onion 2 has been developed with a user-friendly interface and streamlined deployment process, resulting in decreased time and resources necessary for the establishment and upkeep of a comprehensive cybersecurity framework.

In summary, the integration of the suggested resolution with the Security Onion 2 framework presents a robust and efficient approach to safeguard genuine servers against zero-day assaults. The targeted alerting capabilities of the solution, when combined with the flexibility and ease of use of Security Onion 2, offer a dependable and comprehensive cybersecurity solution

that can assist organizations in proactively addressing emerging threats and safeguarding their systems. Through the utilization of Security Onion 2 and the suggested approach, enterprises can enhance their network visibility, expedite and enhance the accuracy of potential attack detection, and promptly and efficiently respond to incidents, thereby enhancing their cybersecurity stance holistically.

4.5 Summary

The present section expounded upon the outcomes of the study that was carried out to assess the effectiveness of utilizing deception and threat hunting intelligence in the identification of zero-day attacks. This section presents the outcomes of various experiments and analyses. The findings suggest that the utilization of deception-based techniques is more efficacious in safeguarding real servers against zero-day attacks compared to signature-based methods. This approach offers a considerable degree of protection for real servers while maintaining a low rate of false positives. The section provide results and evaluation that presents evidence of the potential success of deception and threat hunting intelligence in enhancing cybersecurity, particularly in the identification of zero-day attacks. The results indicate that the utilization of deception-based techniques can offer a reliable means of detection while minimizing the occurrence of false positives. This makes them a viable option for cybersecurity experts who aim to protect their systems from the ever-evolving and persistent threats.

Chapter 5

Discussion and Analysis

5.1 Analysis of the research findings

The results of the study demonstrate the efficacy of employing deception and threat hunting intelligence for the identification of zero-day assaults. The implementation of these methodologies can aid organizations in identifying and addressing sophisticated threats that may have evaded their conventional security protocols. The study's results emphasize the potential advantages of employing these methodologies. Deception techniques and threat hunting intelligence offer a notable benefit of being cost-effective in comparison to alternative security measures. The implementation of these solutions does not mandate substantial investments in costly hardware or software, thereby rendering them achievable to a diverse spectrum of organizations, including smaller enterprises with restricted resources. Furthermore, these solutions have the potential to be exceedingly effective in identifying zero-day attacks, which can prove to be difficult to detect through

conventional security measures. Zero-day attacks are frequently crafted to avoid identification by conventional security mechanisms. Deception tactics and threat hunting intelligence are preventative measures that proactively seek out possible threats, such as zero-day assaults. Additionally, the results of the study indicate that these methodologies possess the capability to promptly identify possible risks, thereby mitigating the consequences of security breaches. Organizations can mitigate the expenses and disruptions associated with addressing a security incident by preemptively identifying and addressing potential threats.

5.2 Discussion of the research implications and limitations

5.2.1 Cost

The figures presented in this section provide an overview of the timeline and cost associated with the project. The project was initiated in February 2023 and continued until the end of May 2023, with a total cost of approximately 375.89 USD. It is noteworthy that the project did not receive sponsorship from either AWS or the university, thereby constraining the resources available for project implementation and testing. This limitation on resources had a significant impact on the project timeline, as the more the project environment was running, the more it cost. As a result, the time available for implementing and testing the project was constrained, which in turn limited the scope of the project and the number of experiments and analyses that could be conducted.

Figure 5.1 showcase the month of February total bill which is the lost bill in comparison to the other months as the project was in the instill setup phase during this month.

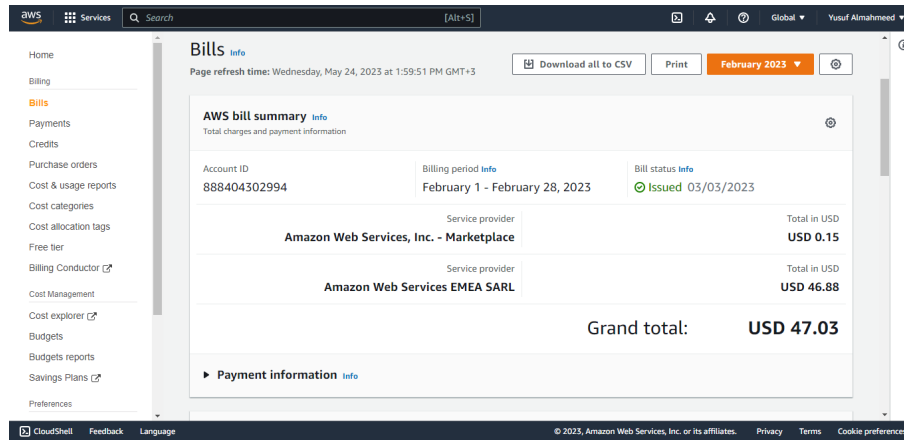


Figure 5.1: February 2023 Bill

As can be seen in figure 5.2 the total bill amount increased as more AWS components were being used and operating.

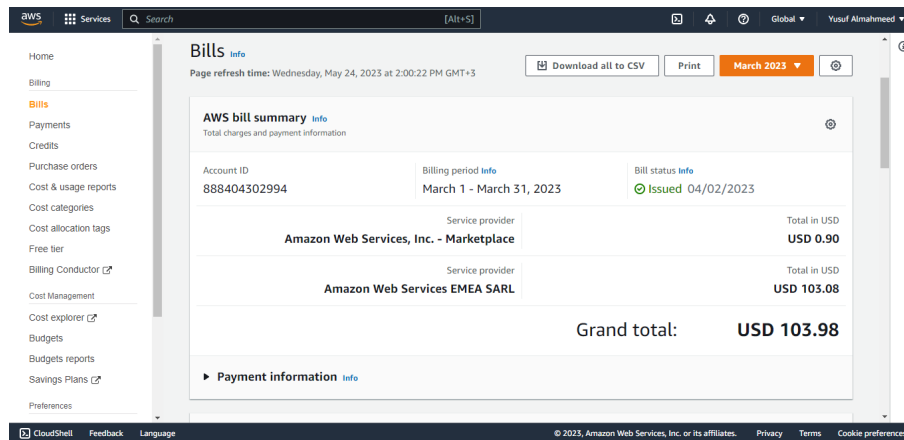


Figure 5.2: March 2023 Bill

Figure 5.3 showcase the amount spent in the month of April which was the modest amount in n comparison to the other months.

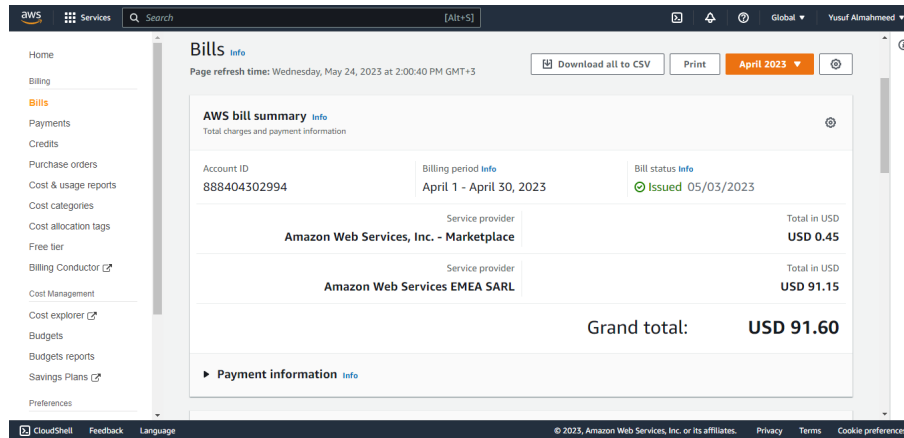


Figure 5.3: April 2023 Bill

The month of May had the highest billing amount as it can be seen in figure 5.4 as it was the project was published to the participants thus the network traffic increased.

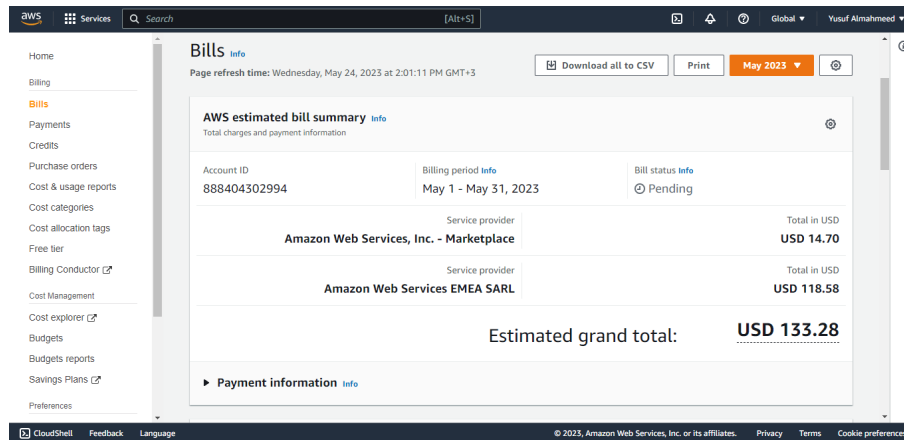


Figure 5.4: May 2023 Bill

5.2.2 Complexity

The project's AWS implementation have been a challenging procedure that required careful preparation and execution. The complexity of this process is influenced by a number of factors, such as the requirement to choose and configure the proper security solutions, the requirement to scale and manage resources efficiently, and the requirement to guarantee compliance with applicable laws and best practices. The selection and configuration of proper

security tools is one of the main obstacles to developing a solution to detect zero-day attacks employing deception and threat hunting intelligence on AWS. It can be challenging to choose the tools that are best suited to the unique demands of an organization because there is a large variety of tools available, each with distinct strengths and shortcomings. Additionally, setting up these technologies to function well together can be a difficult and time-consuming procedure that calls for knowledge in networking, system administration, and data analysis. Scaling and successfully managing resources present another difficulty. Although AWS offers a platform that is very scalable and versatile for managing and deploying security solutions, this flexibility can also make it difficult to make sure that resources are allocated wisely and managed successfully. It may become more challenging to monitor and manage resources as the system's size and complexity increase, which could result in performance and security problems.

5.2.3 Data

Undertaking near-real environmental testing with the aim of data collection can present imposing difficulties, particularly in the field of cybersecurity. The successful execution of this task requires the participation of individuals possessing specialized expertise in the domains of penetration testing and ethical hacking. The professionals possess the necessary knowledge and skills to simulate real-life attacks in a controlled environment, providing valuable insights into the effectiveness of the proposed solution. Locating personnel possessing the necessary skills and knowledge can pose a challenge, particularly in instances where the undertaking is constrained by time. Moreover, it can be challenging to ensure that the individuals selected to conduct the testing are trustworthy and will adhere to the agreed-upon rules and regulations. In order to tackle this challenge, a survey has been distributed through various social media platforms as well as cybersecurity-

oriented Discord servers and forums. The objective of the survey was to identify the individuals who possess the necessary knowledge and skills to carry out authentic environmental attacks. This approach helped the team to identify a pool of potential candidates who possessed the necessary skills and expertise to execute the project successfully.

5.2.4 Protection Scope

Implementing a solution that involves deception techniques and threat hunting intelligence can be complex, particularly in organizations that provide multiple services and have multiple network layers such as DMZ and core. To ensure the effectiveness of such solutions, it is crucial to have a thorough planning process that takes into consideration the organization's specific requirements and the potential risks and challenges. A key consideration when implementing such solutions is the placement of the solution within the network architecture. The placement of the solution within the DMZ layer may not offer sufficient safeguarding for the core layer, which could be of greater significance and worth to the enterprise. Hence, it is imperative to carefully strategize the positioning of the solution, while considering the network architecture of the establishment, the significance of diverse systems and data, and the plausible attack vectors. Before developing such solutions, it is essential to convene the risk management, information security, and information technology teams to ensure that all relevant stakeholders are involved in the planning process. This approach facilitates the identification of prospective hazards and obstacles, and guarantees that the solution is formulated to encompass the most extensive expanse of the environment while preserving its efficacy. Furthermore, it is crucial to ensure that the solution is regularly updated and maintained to ensure its effectiveness over time. Attackers are constantly evolving their techniques and tactics, and the solution must be able to adapt to these changes to remain effective. Therefore, it is essen-

tial to have a comprehensive maintenance plan that includes regular updates and testing of the solution to ensure that it remains effective in detecting and mitigating potential threats.

5.2.5 Time

The time limitation encountered during the project posed a considerable obstacle that impacted multiple phases of the project. A significant amount of time was spent in the preliminary phase of the project, which involved planning, designing, and conducting research. This was necessary to ensure having access to the requisite resources and tools to execute the project successfully. Moreover, the establishment of an appropriate setting for the project constituted a crucial element that demanded significant duration and effort to fulfilling project's prerequisites. The implementation of a solution involving deception tactics and threat hunting intelligence in real-world situations requires a substantial investment of time and resources to establish and sustain the decoy systems and data. The task at hand demands the verification of the authenticity and effectiveness of the decoy systems, with the aim of attracting potential attackers, while simultaneously ensuring their safety and non-threatening nature towards the real systems. Furthermore, the practice of threat hunting entails examining extensive quantities of data in order to detect patterns or anomalies that could potentially signify a security breach. The aforementioned procedure can be a lengthy task and requires specialized abilities and skills to execute proficiently. In order to successfully identify potential threats and vulnerabilities, it is essential that analysts possess a comprehensive comprehension of the organization's network and system architecture, as well as the most current threats and attack methodologies. To conclude, the limitation of time poses a noteworthy obstacle when carrying out projects that entail the utilization of deception tactics and the gathering of threat hunting intelligence. The successful execution of a project requires

Careful planning, thorough preparation, and specialized expertise. However, entities that allocate sufficient time and resources towards the implementation of the stated solutions can enhance their security stance and mitigate the likelihood of security incidents. Adopting a proactive approach towards security is crucial requiring the conduct of periodic evaluations of potential threats, vulnerability scanning, and the implementation of risk management strategies. This practice can aid organizations in recognizing possible vulnerabilities and implementing measures to alleviate them prior to their exploitation by malicious actors.

5.3 Summary

In conclusion, it can be determined that the implementation of deception techniques and threat hunting intelligence can prove to be a financially viable and efficacious approach towards enhancing an organization's security posture and rapidly identifying potential threats, including zero-day attacks. The highlighted section laid out the potential advantages of employing deception tactics and threat hunting intelligence, While also emphasizing some of the limitations and challenges encountered.

Chapter 6

Conclusion

6.1 Summary of the research findings

The study's results confirmed the underlying hypothesis of the study, which posits that the integration of deception and threat hunting intelligence can enhance any organization security maturity level and establish a proactive mechanism for identifying zero-day attacks. The effectiveness of deception and threat hunting technologies in diverse real-world scenarios was assessed by a collection of cybersecurity professionals who generated real-world attack attempt which lead to collecting research findings and data. The study discovered that the integration of these technologies effectively identified and addressed various types of security breaches, including those that exploit of zero-day vulnerabilities. The implementation of deception and threat hunting technologies can yield substantial enhancements to an organization's security posture and a corresponding reduction in the likelihood of being targeted by malicious actors.

6.2 Future research directions

The results of this study highlight the imperative for ongoing investigation into deception strategies and threat detection intelligence. Subsequent studies might focus on enhancing the efficiency of the employed methodologies and developing novel strategies that can more adeptly identify and counter sophisticated risks, such as zero-day attacks. Moreover, forthcoming investigations may concentrate on formulating more comprehensive security solutions that combine deception tactics and threat hunting intelligence with other security measures, such as machine learning and artificial intelligence. Moreover, it is imperative for researchers to conduct a study on the ethical and legal ramifications associated with the utilization of deception tactics and threat hunting intelligence in the field of IT. The study has the potential to establish a set of standards and optimal procedures for the implementation of these methodologies, thereby guaranteeing their ethical and careful utilization. Furthermore, future studies may concentrate on creating more efficient approaches to training and educating cybersecurity experts. One potential opportunity for exploration involves the creation of novel training curricula and certifications that center on the acquisition of skills related to deception tactics and the gathering of threat hunting intelligence.

References

- Abdoulaye, P. (2022). Digitizing the business model using aws. In *Transforming your business with aws: Getting the most out of using aws to modernize and innovate your digital services* (p. 75-76).
- Ahmad, R., Alsmadi, I., Alhamdani, W., & Tawalbeh, L. (2023, Feb). *Zero-day attack detection: a systematic literature review - artificial intelligence review*. Retrieved from <https://link.springer.com/article/10.1007/s10462-023-10437-z> doi: 10.1007/s10462-023-10437-z
- Ahmad, W., Arsalan, M., Nawaz, S., & Waqas, F. (n.d.). Detection and analysis of active attacks using honeypot. *International Journal of Computer Applications*, 975, 8887.
- Amin, M. A. R. A., Shetty, S., Njilla, L., Tosh, D. K., & Kamhoua, C. (2021). Hidden markov model and cyber deception for the prevention of adversarial lateral movement. *IEEE Access*, 9, 49662-49682. doi: 10.1109/ACCESS.2021.3069105
- Anwer, M., Ahmed, G., Akhunzada, A., Hussain, S., & Khan, M. (2022). Comparative analysis of soft computing approaches of zero-day-attack detection. In *2022 international conference on emerging trends in smart technologies (icetst)* (p. 1-5). doi: 10.1109/ICETST55735.2022.9922937
- Babu, R. (2022). *Network traffic analysis and anomaly detection: A comparative case study* (Doctoral dissertation). Retrieved from <http://>

urn.kb.se/resolve?urn=urn:nbn:se:hh:diva-48134

- Bahrami, P. N., Dehghantanha, A., Dargahi, T., Parizi, R. M., Choo, K.-K. R., & Javadi, H. H. S. (2019). Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures. *Journal of Information Processing Systems*, 15(4), 865–889. Retrieved from <https://www.koreascience.or.kr/article/JAK0201925462478086.pag> doi: 10.3745/JIPS.03.0126
- Bathala, H. V., Srihitha, P. P., Dodla, S. G. R., & Pasala, A. (2021). Zero-day attack prevention email filter using advanced machine learning. In *2021 5th conference on information and communication technology (cict)* (p. 1-6). doi: 10.1109/CICT53865.2020.9672420
- Brown, R., & Lee, R. M. (2021). *2021 sans cyber threat intelligence (cti) survey*. SANS. Retrieved from <https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt43a990b140efaa96/6112a525f0c97e39497dc96d/40080.pdf>
- Bu, S.-J., & Cho, S.-B. (2021). Integrating deep learning with first-order logic programmed constraints for zero-day phishing attack detection. In *Icassp 2021 - 2021 ieee international conference on acoustics, speech and signal processing (icassp)* (p. 2685-2689). doi: 10.1109/ICASSP39728.2021.9414850
- Ellouh, M., Ghaleb, M., & Felemban, M. (2022). Iotzerojar: Towards a honeypot architecture for detection of zero-day attacks in iot. In *2022 14th international conference on computational intelligence and communication networks (cicn)* (p. 765-771). doi: 10.1109/CICN56167.2022.10008323
- Eswaran, S., Rani, V., D., D., Ramakrishnan, J., & Selvakumar, S. (2021, Sep). An enhanced network intrusion detection system for malicious crawler detection and security event correlations in

- ubiquitous banking infrastructure. *International Journal of Pervasive Computing and Communications*, ahead-of-print(ahead-of-print). Retrieved from <https://www.emerald.com/insight/content/doi/10.1108/IJPCC-04-2021-0102/full/html> doi: 10.1108/IJPCC-04-2021-0102
- Hairab, B. I., Said Elsayed, M., Jurcut, A. D., & Azer, M. A. (2022). Anomaly detection based on cnn and regularization techniques against zero-day attacks in iot networks. *IEEE Access*, 10, 98427-98440. doi: 10.1109/ACCESS.2022.3206367
- Islam, M. M., & Al-Shaer, E. (2020). Active deception framework: An extensible development environment for adaptive cyber deception. In *2020 ieee secure development (secdev)* (p. 41-48). doi: 10.1109/SecDev45635.2020.00023
- Jakob, B. (2023). Cyberdefense report software supply chain attacks an illustrated typological review.
- Jeong, J. H., & Choi, S. G. (2020). Hybrid system to minimize damage by zero-day attack based on nidps and honeypot. In *2020 international conference on information and communication technology convergence (ictc)* (p. 1650-1652). doi: 10.1109/ICTC49870.2020.9289589
- Joshi, K., Kumar, R., Kumar, A., Reshi, J., Sharma, A., & Dumka, A. (2022). A framework optimization in social media using xampp: A systematic approach. In *2022 international conference on fourth industrial revolution based technology and practices (icfirtp)* (p. 1-4). doi: 10.1109/ICFIRTP56122.2022.10059447
- Lee, B., Oh, J., Shon, W., & Moon, J. (2023). A literature review on aws-based cloud computing: A case in south korea. In *2023 ieee international conference on big data and smart computing (bigcomp)* (p. 403-406). doi: 10.1109/BigComp57234.2023.00099

- Liebowitz, D., Nepal, S., Moore, K., Christopher, C. J., Kanhere, S. S., Nguyen, D., ... Rathakumar, K. (2021). Deception for cyber defence: Challenges and opportunities. In *2021 third ieee international conference on trust, privacy and security in intelligent systems and applications (tps-isa)* (p. 173-182). doi: 10.1109/TPSISA52974.2021.00020
- Liu, W., Chen, F., Hu, H., Cheng, G., Huo, S., & Liang, H. (2017). A novel framework for zero-day attacks detection and response with cyberspace mimic defense architecture. In *2017 international conference on cyber-enabled distributed computing and knowledge discovery (cyberc)* (p. 50-53). doi: 10.1109/CyberC.2017.39
- Machida, T., Yamamoto, D., Unno, Y., & Kojima, H. (2021). Novel deception techniques for malware detection on industrial control systems. *Journal of Information Processing*, 29(0), 559–571. Retrieved from <https://doi.org/10.2197/ipsjjip.29.559> doi: 10.2197/ipsjjip.29.559
- Machmeier, S. (2023). Honeypot implementation in a cloud environment. *arXiv preprint arXiv:2301.00710*.
- Maschmeyer, L., Deibert, R. J., & Lindsay, J. R. (2021, Jan). A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology Politics*, 18(1), 1–20. Retrieved from <https://www.tandfonline.com/doi/full/10.1080/19331681.2020.1776658> doi: 10.1080/19331681.2020.1776658
- Mbona, I., & Eloff, J. H. P. (2022). Detecting zero-day intrusion attacks using semi-supervised machine learning approaches. *IEEE Access*, 10, 69822-69838. doi: 10.1109/ACCESS.2022.3187116
- McLoughlin, J. E. (2023). *Standing in the age of data reaches a consumer friendly framework*
- Nandakumar, D., Schiller, R., Redino, C., Choi, K., Rahman, A., Bowen, E., ...

- Shaha, A. (2022). Zero day threat detection using metric learning autoencoders. In *2022 21st IEEE International Conference on Machine Learning and Applications (ICMLA)* (p. 1318-1325). doi: 10.1109/ICMLA55696.2022.00210
- Nayak, S. C., Tiwari, V., & Samanthula, B. K. (2023). Review of ransomware attacks and data recovery framework using autopsy digital forensics platform (p. 0611).
- The Necessity of Cyber Threat Intelligence - ProQuest.* (n.d.). Retrieved 2022-01-11, from <https://www.proquest.com/openview/faef41faeda78972463125b376cf39ea/1?pq-origsite=gscholar&cbl=18750&diss=y>
- Neto, M. Z., Santana, G. A. A., Sapata, F., Munoz, M., Moraes, A. M. S. P., Morais, T., & Goldfarb, D. L. (2021). Creating your security journey in AWS. In *AWS Certified Security Study Guide: Specialty (SCS-C01) Exam* (p. 363-374). doi: 10.1002/9781119658856.ch10
- Pitre, P., Gandhi, A., Konde, V., Adhao, R., & Pachghare, V. (2022). An intrusion detection system for zero-day attacks to reduce false positive rates. In *2022 International Conference for Advancement in Technology (ICONAT)* (p. 1-6). doi: 10.1109/ICONAT53423.2022.9726105
- Popoola, S. I., Ande, R., Adebisi, B., Gui, G., Hammoudeh, M., & Jogunola, O. (2022). Federated deep learning for zero-day botnet attack detection in IoT-edge devices. *IEEE Internet of Things Journal*, 9(5), 3930-3944.
- Priya, V. D., & Chakkaravarthy, S. S. (2023). Containerized cloud-based honeypot deception for tracking attackers. *Scientific Reports*, 13(1), 1437.
- Rahman, M. R., Mahdavi-Hezaveh, R., & Williams, L. A. (2021). What are the attackers doing now? Automating cyber threat intelligence extraction from text on pace with the changing threat landscape: A survey. *CoRR*, abs/2109.06808. Retrieved from <https://arxiv.org/abs/2109.06808>
- Ren, X., Liang, J., & Liu, Q. (2020). A defensive strategy for integrity detection

- in cyber-physical systems subject to deception attacks. In *2020 10th international conference on information science and technology (icist)* (p. 241-246). doi: 10.1109/ICIST49303.2020.9202239
- Ren, Y., Zhao, J., Qin, C., & Zhu, L. (2020). Small signal stability analysis and optimal control of aws based wave energy conversion system. In *2020 12th ieee pes asia-pacific power and energy engineering conference (appec)* (p. 1-5). doi: 10.1109/APPEEC48164.2020.9220706
- Roshan, K., & Zafar, A. (2021). An optimized auto-encoder based approach for detecting zero-day cyber-attacks in computer network. In *2021 5th international conference on information systems and computer networks (iscon)* (p. 1-6). doi: 10.1109/ISCON52037.2021.9702437
- Samtani, S., Li, W., Benjamin, V., & Chen, H. (2021, Dec). Informing cyber threat intelligence through dark web situational awareness: The azsecure hacker assets portal. *Digital Threats: Research and Practice*, 2(4), 1–10. Retrieved from <https://dl.acm.org/doi/10.1145/3450972> doi: 10.1145/3450972
- Saraswat, M., & Tripathi, R. (2020). Cloud computing: Comparison and analysis of cloud service providers-aws, microsoft and google. In *2020 9th international conference system modeling and advancement in research trends (smart)* (p. 281-285). doi: 10.1109/SMART50582.2020.9337100
- Sawant, N., & Sengamedu, S. H. (2022). Learning-based identification of coding best practices from software documentation. In *2022 ieee international conference on software maintenance and evolution (icsme)* (p. 533-542). doi: 10.1109/ICSME55016.2022.00073
- Shahriar, M. H., Ashiqur Rahman, M., Haque, N. I., & Chowdhury, B. (2021). Ddaf: Deceptive data acquisition framework against stealthy attacks in cyber-physical systems. In *2021 ieee 45th annual computers, software, and applications conference (compsac)* (p. 725-734). doi: 10.1109/COMPSAC51774.2021.00104

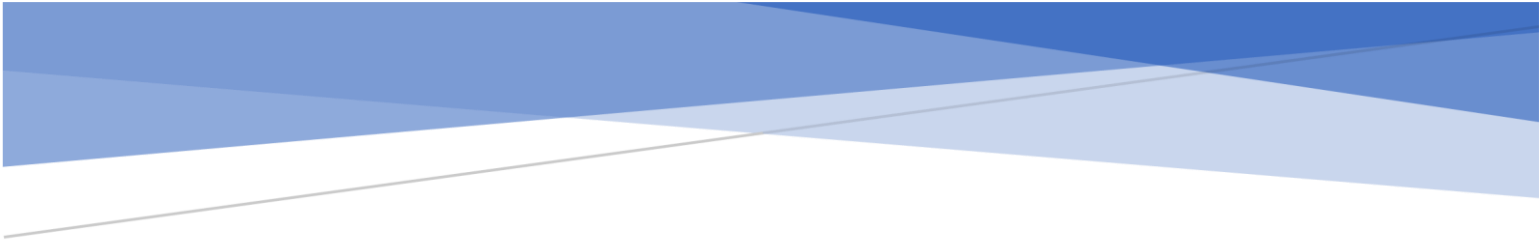
- Shejin, T., & Sudheer, K. (2023). A review on major cyber threats and recommended counter measures.
- Singh, A. K., Arifi, A. A., Harikrishnan, R., Datta, B., & Wagle, S. A. (2022). Iot based home automation using app aws. In *2022 international conference on advances in computing, communication and applied informatics (accai)* (p. 1-9). doi: 10.1109/ACCAI53970.2022.9752635
- Singhal, V., Khatri, K., & Singhal, S. (2022). Risk management by grid computing in aws. In *2022 international conference on machine learning, big data, cloud and parallel computing (com-it-con)* (Vol. 1, p. 874-878). doi: 10.1109/COM-IT-CON54601.2022.9850818
- Srinivasa, S., Pedersen, J. M., & Vasilomanolakis, E. (2022). Deceptive directories and “vulnerable” logs: a honeypot study of the ldap and log4j attack landscape. In *2022 ieee european symposium on security and privacy workshops (eurospw)* (p. 442-447). doi: 10.1109/EuroSPW55150.2022.00052
- Sutriyan, H., Sunaryadi, A., & Sinambela, M. (2022). Blockchain-based multiple server database system prototype on bmkg automatic weather station (aws) center architecture. In *2022 seventh international conference on informatics and computing (icic)* (p. 1-6). doi: 10.1109/ICIC56845.2022.10006923
- Tang, R., Yang, Z., Li, Z., Meng, W., Wang, H., Li, Q., ... Liu, Y. (2020). Zerowall: Detecting zero-day web attacks through encoder-decoder recurrent neural networks. In *Ieee infocom 2020 - ieee conference on computer communications* (p. 2479-2488). doi: 10.1109/INFOCOM41043.2020.9155278
- Varatharaj, A., Rupasinghe, P. L., & Liyanapathirana, C. (2021, Feb). Development of cyber threat intelligence system in a soc environment for real time environment. Retrieved from <http://repo.lib.sab.ac.lk:8080/xmlui/handle/123456789/1741>
- Vielberth, M., Bohm, F., Fichtinger, I., & Pernul, G. (2020). Security operations center: A systematic study and open challenges. *IEEE Access*,

8, 227756–227779. Retrieved from <https://ieeexplore.ieee.org/document/9296846/> doi: 10.1109/ACCESS.2020.3045514

Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber threat predictive analytics for improving cyber supply chain security. *IEEE Access*, 9, 94318–94337. Retrieved from <https://ieeexplore.ieee.org/document/9448097/> doi: 10.1109/ACCESS.2021.3087109

Zoppi, T., Ceccarelli, A., & Bondavalli, A. (2021). Unsupervised algorithms to detect zero-day attacks: Strategy and application. *IEEE Access*, 9, 90603–90615. doi: 10.1109/ACCESS.2021.3090957

Zoratti, I. (2006). Mysql security best practices. In *2006 iet conference on crime and security* (p. 183-198).



MEIB PENETRATION TEST

Mohamed Ismaeel
Mohd89ali@gmail.com

Introduction:

I would like to thank the creators of this challenge, it was awesome 😊 .

Executive Summary:

This summary provides a quick overview of the key findings from the assessment of MEIB's network and systems. Leaked credentials led to unauthorized access to the organization's webmail and compromised a user's workstation. This exposed sensitive information and potentially allowed further unauthorized access within the network. It was also discovered that user privileges were not properly managed, increasing the risk of unauthorized access. Furthermore, the assessment identified potential vulnerabilities in the organization's database server. To address these findings, it is recommended to strengthen password policies, implement additional security measures, review user privileges, and secure the database server. Taking these steps will help improve the organization's overall security posture and protect against future incidents.

Rules of Engagement:

✱

Rules of Engagement:-

- Penetration Test in Scope

Assessing the security measures should only be against domain and URLs that will be mentioned in the next section

- Out of Scope

The following items are not in scope for this assessment:

- Denial of Service (DoS) attacks against the infrastructure
- Phishing / Social Engineering attacks
- Attacks against the third party hosting infrastructure
- Attacks against anything outside of the previously mentioned scope
- Attacks or password changes against the servers/machines local admins

Scope:

Screenshot the below information to have it as a reference

In order to start hacking please find the below:-

- Find the below scope which should only be assessed during testing:

- OSINT on <https://www.test.meibonline.com> and <https://meib.awsapps.com/mail>.
- External Pentest: 10.10.20.0/24.
- Internal Pentest: 10.10.30.0/24 and 10.10.40.0/24.

Leaked credentials:-

muhammad.abdallah work email credentials have been leaked as he was using a weak password **Spring_2023**

Important note:-

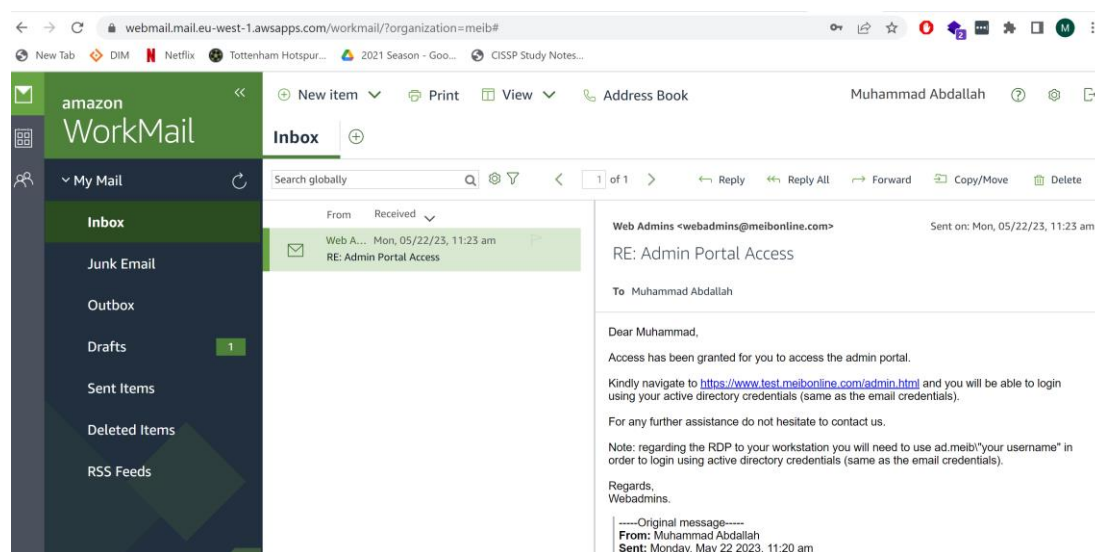
The website and environment were established recently, and they are undergoing a lot of ongoing changes.

For any questions or inquiries, please leave it below with your email address, and we will get back to you as soon as we can.

Findings:

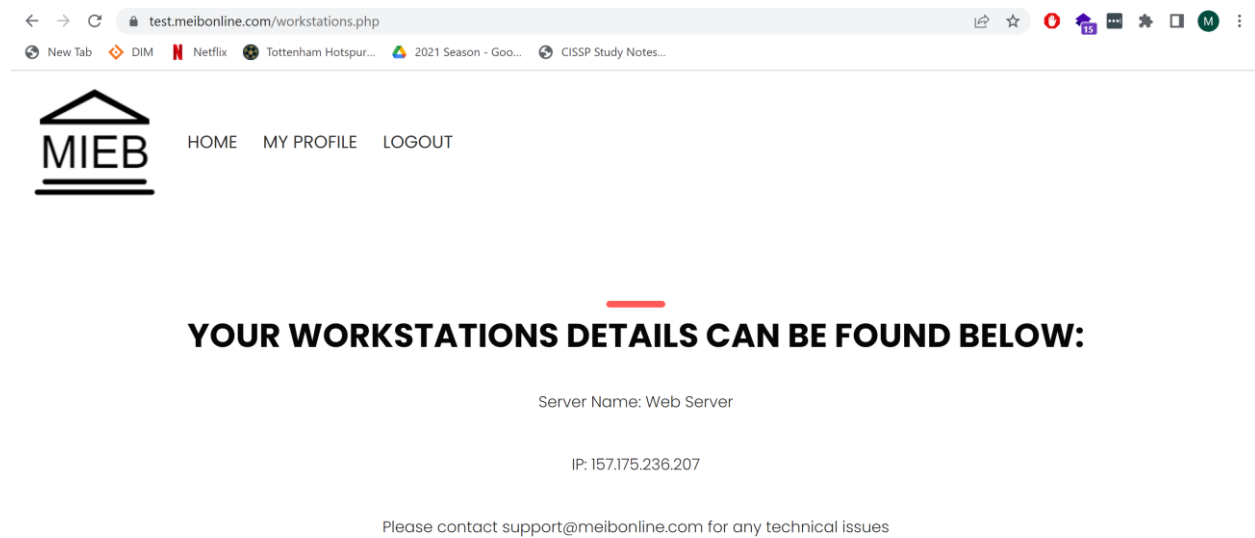
Webmail Compromise

By leveraging the leaked credentials of user "Muhammad.abdallah," unauthorized access was gained to the organization's webmail. An email trail was discovered, containing instructions from an admin on accessing the admin portal of the website. This indicates a potential security lapse, as sensitive information was being exchanged via email.



Workstation Exploitation

The compromised workstation of Muhammad.abdallah revealed a public IP address and evidence of a successful Remote Desktop Protocol (RDP) session using the same leaked credentials. This highlights the importance of securing workstations, as a compromise in a single workstation led to further unauthorized access.



Active Directory Enumeration, several critical details were identified:

Domain and Domain Controller: The domain name and associated domain controller were determined during the enumeration phase.

Users and Computers: A comprehensive list of users and computers within the domain was obtained, aiding in the assessment of potential attack vectors.

Domain Admins: It was discovered that Muhammad.abdallah had administrative privileges, making him a domain admin. This finding raises concerns regarding privilege escalation and unauthorized access.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd ..
PS C:\Windows> cd C:\Tools
PS C:\Tools> ls

Directory: C:\Tools

Mode                LastWriteTime         Length Name
----                -
-a---             5/18/2021   2:59 PM       448187 PowerView.ps1

PS C:\Tools> . .\PowerView.ps1
PS C:\Tools> Get-NetDomain

Forest                : ad.meib
DomainControllers     : {adserver.ad.meib}
Children              : {}
DomainMode            : Windows2012R2Domain
DomainModeLevel       : 6
Parent               : 
PdcRoleOwner          : adserver.ad.meib
RidRoleOwner          : adserver.ad.meib
InfrastructureRoleOwner : adserver.ad.meib
Name                  : ad.meib
```

```
PS C:\Tools> Get-NetDomainController
```

```
Forest                : ad.meib
CurrentTime           : 5/25/2023 3:13:29 PM
HighestCommittedUsn   : 81305
OSVersion              : Windows Server 2012 R2 Standard
Roles                 : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain                : ad.meib
IPAddress             : 10.10.30.36
SiteName              : Default-First-Site-Name
SyncFromAllServersCallback :
InboundConnections    : {}
OutboundConnections   : {}
Name                  : adserver.ad.meib
Partitions             : {DC=ad,DC=meib, CN=Configuration,DC=ad,DC=meib, CN=Schema,CN=Configuration,DC=ad,DC=meib,
                        DC=DomainDnsZones,DC=ad,DC=meib...}
```

```
PS C:\Tools> Get-NetUser * | select cn,description,samaccountname
```

cn	description	samaccountname
Administrator	Built-in account for administering t...	Administrator
Guest	Built-in account for guest access to...	Guest
krbtgt	Key Distribution Center Service Account	krbtgt
mysql server		mysqlserver
web server		webserver
Muhammad Abdallah		Muhammad.Abdallah
Ahmed Ali		Ahmed.Ali
Fatima Khalifa		Fatima.Khalifa
Omar Mahmoud		Omar.Mahmoud
Aisha Hassan		Aisha.Hassan
Hassan Mohammed		Hassan.Mohammed
Mariam Abdullah		Mariam.Abdullah
Khalid Saleh		Khalid.Saleh
Hala Al-Saud		Hala.Al-Saud
Nasser Al-Mansour		Nasser.Al-Mansour
Rania Al-Amin		Rania.Al-Amin
Ali Ahmed		Ali.Ahmed
Khalifa Fatima		Khalifa.Fatima
Mahmoud Omar		Mahmoud.Omar
Hassan Aisha		Hassan.Aisha
Mohammed Hassan		Mohammed.Hassan
Abdullah Mariam		Abdullah.Mariam
Saleh Khalid		Saleh.Khalid
Hala Al-Saud		Khalid.Al-Saud
Nasser Nasser		Muhammad.Al-Mansour
Rania Al-Amin		Sara.Al-Amin
Youssef Salim		Youssef.Salim
Muna Ahmed		Muna.Ahmed
Samir Haddad		Samir.Haddad
Sara Al-Salem		Sara.Al-Salem
Tarek Abadi		Tarek.Abadi
Laila Abdel-Aziz		Laila.Abel-Aziz
Ziad Khalil		Ziad.Khalil
Mona Al-Omari		Mona.Al-Omari
Ahmed Al-Khatib		Ahmed.Al-Khatib
Fatima Al-Jaber		Fatima.Al-Jaber
Omar Al-Rashid		Omar.Al-Rashid
Aisha Al-Zahrani		Aisha.Al-Zahrani
Hassan Al-Mahdi		Hassan.Al-Mahdi
Mariam Al-Qahtani		Mariam.Al-Qahtani
Khalid Al-Ghundi		Al-Ghundi
Hala Al-Harbi		Hala.Al-Harbi
Nasser Al-Qassim		Nasser.Al-Qassim
Rania Al-Abdulwahed		Rania.Al-Abdulwahed
Ali Al-Dossari		Al-Dossari
Khalifa Al-Shammari		Khalifa.Al-Shammari
Mahmoud Al-Mohsen		Mahmoud.Al-Mohsen
Hassan Al-Faris		Hassan.Al-Faris
Mohammed Al-Sulaiman		Mohammed.Al-Sulaiman
Abdullah Al-Qurashi		Abdullah.Al-Qurashi

157.175.236.207 - Remote Desktop Connection

10.10.30.36 - Remote Desktop Connection

Windows PowerShell

```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\muhammad.abdallah> hostname
adserver
PS C:\Users\muhammad.abdallah> whoami
meib\muhammad.abdallah
PS C:\Users\muhammad.abdallah>
```

```
PS C:\Tools> Get-NetUser | select cn,pwdlastset,badpwdcount,logoncount
```

cn	pwdlastset	badpwdcount	logoncount
Administrator	2/15/2023 3:18:41 PM	320	272
Guest	1/1/1601 12:00:00 AM	1	0
krbtgt	2/22/2023 6:25:21 PM	1	0
mysql server	5/23/2023 9:13:14 AM	0	25
web server	5/19/2023 2:36:14 PM	1	38
Muhammad Abdallah	3/25/2023 9:07:57 PM	0	22
Ahmed Ali	5/19/2023 1:59:28 PM	0	0
Fatima Khalifa	5/19/2023 2:06:31 PM	0	0
Omar Mahmoud	5/19/2023 2:06:54 PM	0	0
Aisha Hassan	5/19/2023 2:07:16 PM	0	0
Hassan Mohammed	5/19/2023 2:07:37 PM	0	0
Mariam Abdullah	5/19/2023 2:09:42 PM	0	0
Khalid Saleh	5/19/2023 2:10:02 PM	0	0
Hala Al-Saud	5/19/2023 2:10:24 PM	0	0
Nasser Al-Mansour	5/19/2023 2:10:44 PM	0	0
Rania Al-Amin	5/19/2023 2:11:09 PM	0	0
Ali Ahmed	5/19/2023 2:11:34 PM	0	0
Khalifa Fatima	5/19/2023 2:12:03 PM	0	0
Mahmoud Omar	5/19/2023 2:12:28 PM	0	0
Hassan Aisha	5/19/2023 2:13:06 PM	0	0
Mohammed Hassan	5/19/2023 2:13:33 PM	0	0
Abdullah Mariam	5/19/2023 2:14:37 PM	0	0
Saleh Khalid	5/19/2023 2:15:41 PM	0	0
Hala Al-Saud	5/19/2023 2:16:09 PM	0	0
Nasser Nasser	5/19/2023 2:16:54 PM	0	0
Rania Al-Amin	5/19/2023 2:17:34 PM	0	0
Youssef Salim	5/19/2023 2:18:27 PM	0	0
Muna Ahmed	5/19/2023 2:19:37 PM	0	0
Samir Haddad	5/19/2023 2:20:04 PM	0	0
Sara Al-Salem	5/19/2023 2:20:39 PM	0	0
Tarek Abadi	5/19/2023 2:21:05 PM	0	0
Latifa Abdel-Aziz	5/19/2023 2:21:32 PM	0	0
Ziad Khalil	5/19/2023 2:22:06 PM	0	0
Mona Al-Omari	5/19/2023 2:22:38 PM	0	0
Ahmed Al-Khatib	5/19/2023 2:23:01 PM	0	0
Fatima Al-Jaber	5/19/2023 2:23:34 PM	0	0
Omar Al-Rashid	5/19/2023 2:24:01 PM	0	0
Aisha Al-Zahrani	5/19/2023 2:24:31 PM	0	0
Hassan Al-Mahdi	5/19/2023 2:25:22 PM	0	0
Mariam Al-Qahtani	5/19/2023 2:25:51 PM	0	0
Khalid Al-Ghamdi	5/19/2023 2:26:17 PM	0	0
Hala Al-Harbi	5/19/2023 2:27:22 PM	0	0
Nasser Al-Qassim	5/19/2023 2:27:45 PM	0	0
Rania Al-Abdulwahed	5/19/2023 2:28:20 PM	0	0
Ali Al-Dossari	5/19/2023 2:28:43 PM	0	0
Khalifa Al-Shammari	5/19/2023 2:29:08 PM	0	0
Mahmoud Al-Mohsen	5/19/2023 2:29:31 PM	0	0
Hassan Al-Faris	5/19/2023 2:29:56 PM	0	0
Mohammed Al-Sulaiman	5/19/2023 2:30:26 PM	0	0

The above screen shot determine the active users within the environment.

```
PS C:\Tools> Get-NetGroupMember "domain admins"
```

```
GroupDomain : ad.meib
GroupName   : Domain Admins
MemberDomain : ad.meib
MemberName  : Muhammad.Abdallah
MemberSID   : S-1-5-21-70687330-1375781906-2005314769-1116
IsGroup     : False
MemberDN    : CN=Muhammad Abdallah,OU=IT,DC=ad,DC=meib
```

```
GroupDomain : ad.meib
GroupName   : Domain Admins
MemberDomain : ad.meib
MemberName  : webserver
MemberSID   : S-1-5-21-70687330-1375781906-2005314769-1114
IsGroup     : False
MemberDN    : CN=web server,CN=Users,DC=ad,DC=meib
```

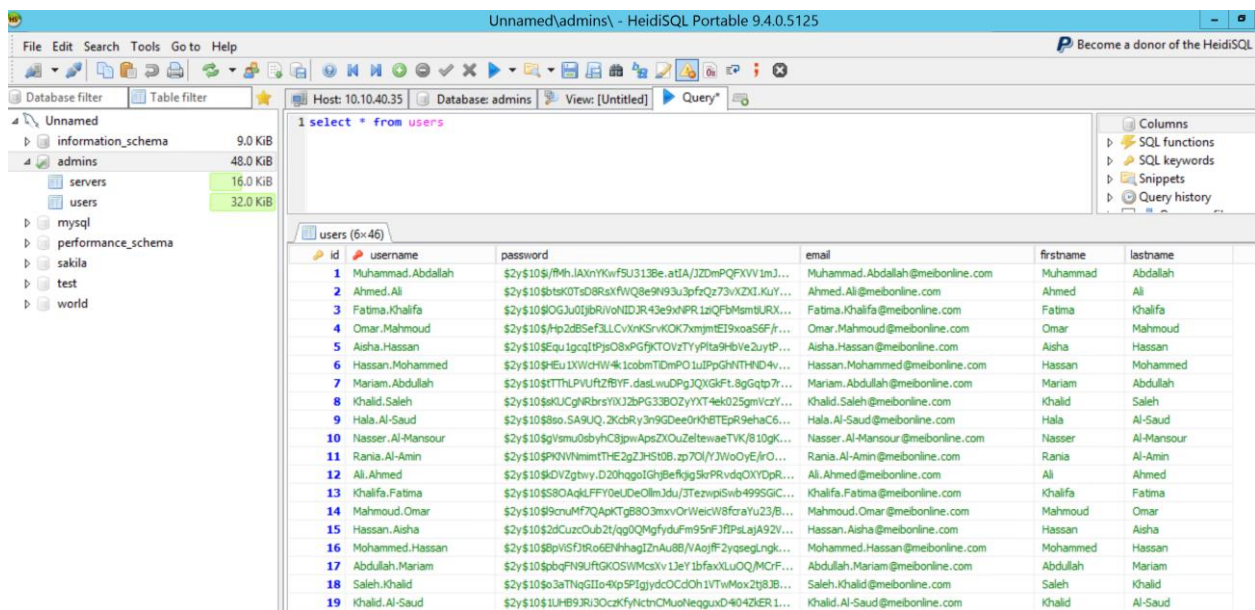
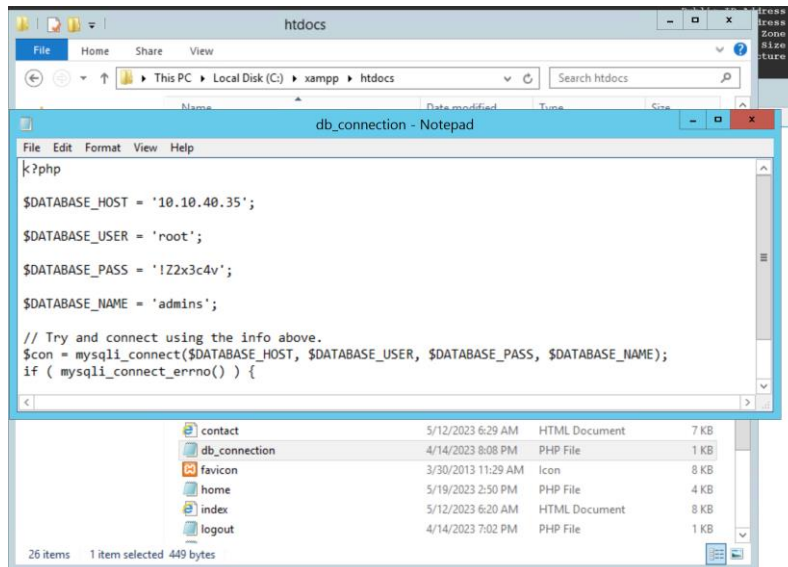
```
GroupDomain : ad.meib
GroupName   : Domain Admins
MemberDomain : ad.meib
MemberName  : mysqlserver
MemberSID   : S-1-5-21-70687330-1375781906-2005314769-1112
IsGroup     : False
MemberDN    : CN=mysql server,CN=Users,DC=ad,DC=meib
```

```
GroupDomain : ad.meib
GroupName   : Domain Admins
MemberDomain : ad.meib
MemberName  : Administrator
```

The above screen demonstrate that Muhammad is a domain admin as well.

Database Server Enumeration

The compromised workstation was found to be running XAMPP, an open-source web server. The website's configuration file revealed credentials for the SQL server and database. Utilizing the obtained credentials, an enumeration of the database server was performed using HeidiSQL.



The above screenshot shows the users table and their secrets.

Host: 10.10.40.35 Database: sakila Query*

1 select * from customer

customer_id	store_id	first_name	last_name	email	address_id	active	create_date	last_update
1	1	MARY	SMITH	MARY.SMITH@sakilacustomer.org	5	1	2006-02-14 22:04:36	2006
2	1	PATRICIA	JOHNSON	PATRICIA.JOHNSON@sakilacustomer.org	6	1	2006-02-14 22:04:36	2006
3	1	LINDA	WILLIAMS	LINDA.WILLIAMS@sakilacustomer.org	7	1	2006-02-14 22:04:36	2006
4	2	BARBARA	JONES	BARBARA.JONES@sakilacustomer.org	8	1	2006-02-14 22:04:36	2006
5	1	ELIZABETH	BROWN	ELIZABETH.BROWN@sakilacustomer.org	9	1	2006-02-14 22:04:36	2006
6	2	JENNIFER	DAVIS	JENNIFER.DAVIS@sakilacustomer.org	10	1	2006-02-14 22:04:36	2006
7	1	MARIA	MILLER	MARIA.MILLER@sakilacustomer.org	11	1	2006-02-14 22:04:36	2006
8	2	SUSAN	WILSON	SUSAN.WILSON@sakilacustomer.org	12	1	2006-02-14 22:04:36	2006
9	2	MARGARET	MOORE	MARGARET.MOORE@sakilacustomer.org	13	1	2006-02-14 22:04:36	2006
10	1	DOROTHY	TAYLOR	DOROTHY.TAYLOR@sakilacustomer.org	14	1	2006-02-14 22:04:36	2006
11	2	LISA	ANDERSON	LISA.ANDERSON@sakilacustomer.org	15	1	2006-02-14 22:04:36	2006
12	1	NANCY	THOMAS	NANCY.THOMAS@sakilacustomer.org	16	1	2006-02-14 22:04:36	2006
13	2	KAREN	JACKSON	KAREN.JACKSON@sakilacustomer.org	17	1	2006-02-14 22:04:36	2006
14	2	BETTY	WHITE	BETTY.WHITE@sakilacustomer.org	18	1	2006-02-14 22:04:36	2006

The above screenshot displays customer details and emails.

Recommendations

Based on the findings of the penetration test, the following recommendations are suggested to enhance the security posture of MEIB:

- Strengthen password policies and enforce regular password changes to mitigate the impact of leaked credentials.
- Implement multi-factor authentication (MFA) for critical systems, including webmail and administrative portals, to add an extra layer of security.
- Conduct security awareness training to educate employees on the risks associated with sharing sensitive information via email.
- Regularly patch and update workstations to address known vulnerabilities and reduce the likelihood of exploitation.
- Review user privileges and restrict administrative access to only those who require it, reducing the potential impact of compromised accounts.
- Secure the database server by implementing strict access controls, regularly updating database software, and removing any unnecessary credentials from configuration files.

ملخص الدراسة

تم في هذا البحث استخدام تقنيات الخداع بإنشاء أنظمة اصطياد ذكية Threat Hunting Intelligence بهدف جذب المهاجمين لفضح وجودهم. تتضمن مطاردة التهديدات الاستكشاف الاستباقي للتهديدات المحتملة. تقترح الدراسة الحالية منهجية تدمج التقنيات الاصطياد الذكية للمساعدة في تحديد هجمات يوم الصفر. تم تقييم فعالية هذه المنهجية من خلال التجارب التي تستخدم سيناريوهات هجوم حقيقي. تشير النتائج إلى أن المنهجية المقترحة لديها القدرة على تعزيز فعالية الكشف بشكل كبير عن هجمات يوم الصفر، وبالتالي تقديم حل قابل للتطبيق لزيادة الأمن السيبراني في أعقاب التهديدات الأمنية المتغيرة بسرعة.

جامعة البحرين

كلية تقنية المعلومات



كشف هجمات اليوم الصفري باستخدام ذكاء الصيد والخداع والتهديد

أطروحة مقدمة كجزء من متطلبات الحصول على
درجة الماجستير في أمن المعلومات

إعداد

يوسف الحميد

الرقم الجامعي: ٢٠١٥١٦٤٨

إشراف

دكتور علاء الدين العمري

أستاذ مساعد

جامعة البحرين

مملكة البحرين

أبريل ٢٠٢٣