COMSATS University Islamabad,
Park Road, Chak Shahzad, Islamabad Pakistan

The Shadow Hunter

By

Kawish Ali Khan	**CUI/FA16-BSE-055/ISB**
Haris Gul	**CUI/FA16-BSE-053/ISB**
Taimoor Fraz Butt	**CUI/FA16-BSE-128/ISB**

Supervisor

Dr. Masoom Alam

Bachelor of Science in Software Engineering (2016-2020)

The candidate confirms that the work submitted is their own and appropriate credit has been given where reference has been made to the work of others.

COMSATS University Islamabad,
Park Road, Chak Shahzad, Islamabad Pakistan

The Shadow Hunter

A project presented to

COMSATS University, Islamabad

In partial fulfillment

of the requirement for the degree of

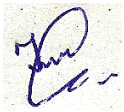
Bachelor of Science in Software Engineering (2016-2020)

By

Kawish Ali Khan	**CUI/FA16-BSE-055/ISB**
Haris Gul	**CUI/FA16-BSE-053/ISB**
Taimoor Fraz Butt	**CUI/FA16-BSE-128/ISB**

DECLARATION

We hereby declare that this software, neither whole nor as a part has been copied out from any source. It is further declared that we have developed this software and accompanied report entirely on the basis of our personal efforts. If any part of this project is proved to be copied out from any source or found to be reproduction of some other. We will stand by the consequences. No Portion of the work presented has been submitted of any application for any other degree or qualification of this or any other university or institute of learning.

Kawish Ali Khan	Taimoor Fraz Butt	Haris Gul
		
----------	----------	----------

CERTIFICATE OF APPROVAL

It is to certify that the final year project of BS (SE) "The Shadow Hunter" was developed by **Kawish Ali Khan (CIIT/FA16-BSE/055)** and **Taimoor Fraz Butt (CIIT/FA16-BSE/128)** and **Haris Gul (CIIT/FA16-BSE/053)** under the supervision of "Dr Masoom Alam" and co supervisor "CO-SUPERVISOR NAME" and that in (their/his/her) opinion; it is fully adequate, in scope and quality for the degree of Bachelors of Science in Computer Sciences.

Supervisor

External Examiner

Head of Department
(Department of Computer Science)

Executive Summary

As the technology is developing and the use of internet is increasing, a highly secure system is the basic need of modern times. It is very necessary for an organization to have honeypots deployed in them. However, the attackers are also getting stronger and more intelligent day by day. With a little intelligence they can easily attack on network infrastructure of an organization. As of now, organizations have only low interaction or high interaction honeypots deployed in their network. Our system would consist of both high interaction honeypots and low interaction services (projection of high interaction honeypots).

Low interaction services will be part of the production system of the organization. However, high interaction honeypots would not be the part of our production network. As the intruder comes inside the production system of the organization, he will be trapped by low interaction services and these low interaction services would send the attacker to the high interaction honeypots (outside of the production network). At this point the attacker thinks that he is in the organization network though in reality he is not. All this movement of the attacker would be shown to the user through the web interface. The system will also generate less but accurate threat intelligence report for making the system more mature in terms of detecting attacks and the nature of the attacker.

Acknowledgement

All praise is to Almighty Allah who bestowed upon us a minute portion of His boundless knowledge by virtue of which we were able to accomplish this challenging task.

We are greatly indebted to our project supervisor “Dr, Masoom Alam”. Without their personal supervision, advice and valuable guidance, completion of this project would have been doubtful. We are deeply indebted to them for their encouragement and continual help during this work.

And we are also thankful to our parents and family who have been a constant source of encouragement for us and brought us the values of honesty & hard work.

Kawish Ali Khan Taimoor Fraz Butt Haris Gul

---------- ---------- ----------

Abbreviations

SRS	Software Require Specification
SDS	Software Design Specification
STS	Software Testing Specification
UC	Use Case
FR	Functional requirements
NFR	Non-Functional Requirements
UT	Unit Testing
FT	Functional Testing
IT	Integration Testing
OVS	Open virtual switch
IP	Internet protocol
Mac address	Media Access Control address
HTTP	Hypertext transfer protocol
SSH	Secure Shell
ONET	Operational network
DNET	Deception network
VM	Virtual Machine

Table of Contents

List of Figures

1. Introduction

1.1 Brief

Deception technology changes the asymmetry of an attack by preparing an organization regardless of the type of cyber-attack. It provides early detection unconcerned of the attack surface. Through deception we can collect the information about the attacker and his goals. Different honey pots are used to trap the attacker and gain his maximum information regarding tool techniques and procedures used by him. For this purpose, deception system provides attack analysis that empowers the attacker to act decisively. Automated responses are also generated to get control over the attacker. Security orchestration integrates different technologies and security tools. This improves incident response. These systems range from static to dynamic. Dynamic work on the services provided to them by the organizations.

1.2 Relevance to Course Modules

There are majority of courses that helped us a lot in making our Final Year Project possible. As if we consider Web Engineering it helped us in developing our front end and we learn React Native through it. Data Base course played a great role in learning the essentials of database systems which allow us to maintain the databases of our project using Mongo DB, Whereas SDA(Software Design Architecture),SRE(Software Requirement Specification) these courses helped us in our documentation process. Software Testing played a major role throughout our testing process. As our project is related to networking CCN helped us in learning the essentials of networking. As HCI course gives us the understanding to design our front end and consistent user interface.

1.3 Project Background

The main purpose of our project is to keep the attacker outside of the production network and get as much information as possible. This would decrease the amount of time an attacker would spend in our production network and so avoiding the losses that can be caused by the attack. The low interaction decoys would directly take the attacker to the high interaction honeypots (outside of the system production network) through SDN tunnel. This makes the infrastructure of an organization strong. High interaction honey pots are deployed in different virtual machines. As soon as the attacker gets in the high interaction honey pots, the activities performed by the attacker will generate threat intelligence and will be reported. This report will help the system to know about the attacker and his goals and techniques. It is up to the organization that how they will use the threat intelligence report to make the organization's security system more mature. This report might be used by the firewall or the security manager of the organization's system to make the system mature. Our system has provided solution to specified security concerns and issues.

1.4 Literature Review

Due to increased cyber-attacks in this era most of the organizations have honeypots for saving their system from any data loss. Most of the organizations have high interaction honeypots to secure their infrastructure and prevent data loss. As the attacker becomes part of organization network he moves in the production network from one PC to other. This movement can cause the damage to the infrastructure of the system. In our system there would be one PC in a single network containing all the services inside it. Less mature systems would be unable to detect the unknown and unaddressed attacks (zero-day attacks). There is need of system that would be intelligent and mature enough to detect every kind of attack and intrusion. Two of the organization that have worked on this system are Acalvio and Fidelis. The reimplementation of this project will help us to understand the behaviour of the intruder, network specific services and generate threat intelligence. The skill that we expect to learn while the implementation of this system is: intrusion detection, intrusion behavior analysis, web development, server's management, networking and cloud computing.

1.5 Analysis of Literature Review

As soon as the attacker interacts with low interaction services as part of organization network, the low interaction decoys would redirect the attacker to an isolated environment, away from the organization's production network. This isolation is important for a secure environment. This would help us to stop the attacker from spending most of the time in an organization's production network. This technique helps us to deceive the attacker because according to the attacker's perspective, he is still inside the system and his attack is going successful. He has no knowledge that he is taken outside of the production network, in deception network. This system would have less deployment cost because a network will consist of all the required low interaction decoys. Attack Analysis will be a main functionality of this project. The threat intelligence generated by our system could be sent to the firewall of the organization's system and this would make the firewall more mature. So, if any familiar attacker with same TTPs would come inside the organization's system, the firewall will block it. By monitoring the TTPs (Tactics, Techniques and Procedures) of the attacker the system will not only protect the organization network but also deceive the attacker towards the deception network. Our system will monitor all the attackers coming inside the production network of an organization. In some of the situations, if the activities of the attackers move out control then our system would stop the attacker by simply closing the session. Web interface would be used to show the user, the literal movement of the attacker.

1.6 Methodology and Software Lifecycle for This Project

For this project we will be using object-oriented methodology with iterative and incremental process model.

1.6.1 **Rationale behind Selected Methodology**

This is a research project so the requirements are not completely known at initial stages and are changing with time. After each iteration, the system will be evaluated and changes will be implemented in the next iteration.

2. Problem Definition

This chapter discusses the precise problem to be solved. It should extend to include the outcome.

2.1 Problem Statement

Due to increased cyber-attacks in this era most of the organizations have honeypots for saving their system from any data loss. Most of the organizations have high interaction honeypots to secure their infrastructure and prevent data loss. As the attacker becomes part of organization network he moves in the production network from one PC to other. This movement can cause the damage to the infrastructure of the system. In our system there would be one PC in a single network containing all the services inside it. Less mature systems would be unable to detect the unknown and unaddressed attacks (zero-day attacks). There is need of system that would be intelligent and mature enough to detect every kind of attack and intrusion. Two of the organization that have worked on this system are Acalvio and Fidelis. The reimplementation of this project will help us to understand the behaviour of the intruder, network specific services and generate threat intelligence. The skill that we expect to learn while the implementation of this system is: intrusion detection, intrusion behavior analysis, web development, server's management, networking and cloud computing.

2.2 Deliverables and Development Requirements

Deliverables	**Development Requirements**
Documentation	Complete document including scope, SRS, SDS, testing
User interface	Understanding of user interaction with system and using libraries like react
Scanner	Complete understanding of nmap and ip scheme selection and scan result report
OVS structure building	It requires ovs complete installation along with tunnels and proper ip selection
Open Flow rules	It requires ip, mac, port and transport layer protocol to implements rules
VM deployments	It needs vagrant, ansible and automated scripts along with vagrant boxes
MongoDB	It requires understating of noSQL database, formation of JSON schemas, schema design choices
Dashboard	It requires visualization, JavaScript libraires like react, redux and visualization eUT
Monitoring	It requires OVS, sFlow, pcap, snort to properly collect, compile and analysis data
Intruder interaction	It needs to have a vulnerable service deployed and attacker interacts with these services

2.3 Current Systems

Application Name	Weakness	Proposed Project Solution
Glastopf	• Low interaction honeypot • No proposed Dashboard • Implementation is slower and complicated. • Not a complete Solution	• High level interaction honeypot • A complete Dashboard • Easy to use • A complete solution.
Kippo	• Medium level interaction honeypot • No complete logs are recorded. • No proper dashboard is provided. • Not fully secured.	• High level interaction of dashboard • Complete logs are provided. • Dashboard can be used. • Fully secured. • A complete solution
mysql-honeypot	• Low level interaction honeypot • No proper logs are maintained • Not secured.	• Fully secured • Scalability • Proper logs are maintained • High level interaction honeypot

3. Requirement Analysis

The following parts of Software Requirements Specification (SRS) report should be included in this chapter.

3.1 Use Cases Diagram(s)

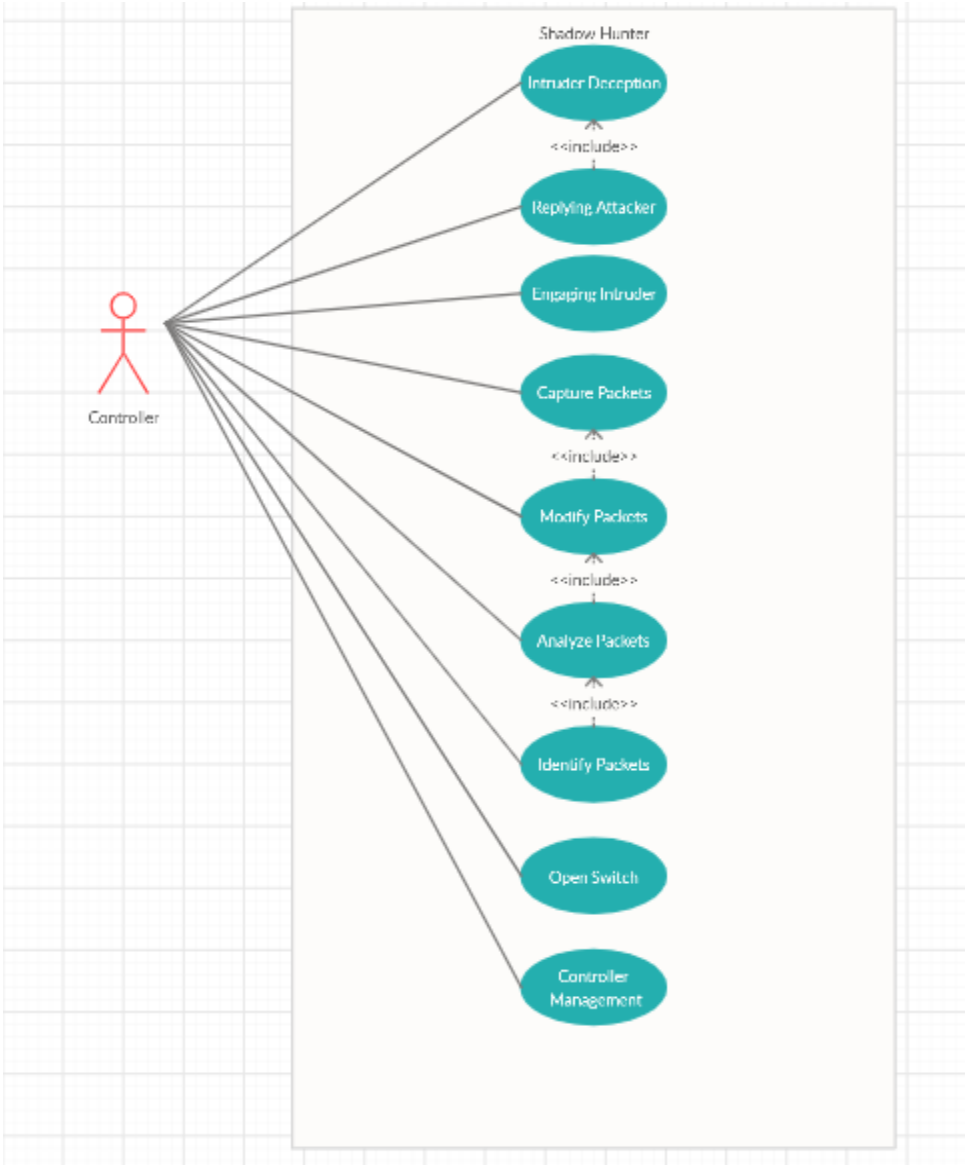


Figure 3.1 UC Diagram 1 - Attacker Parking

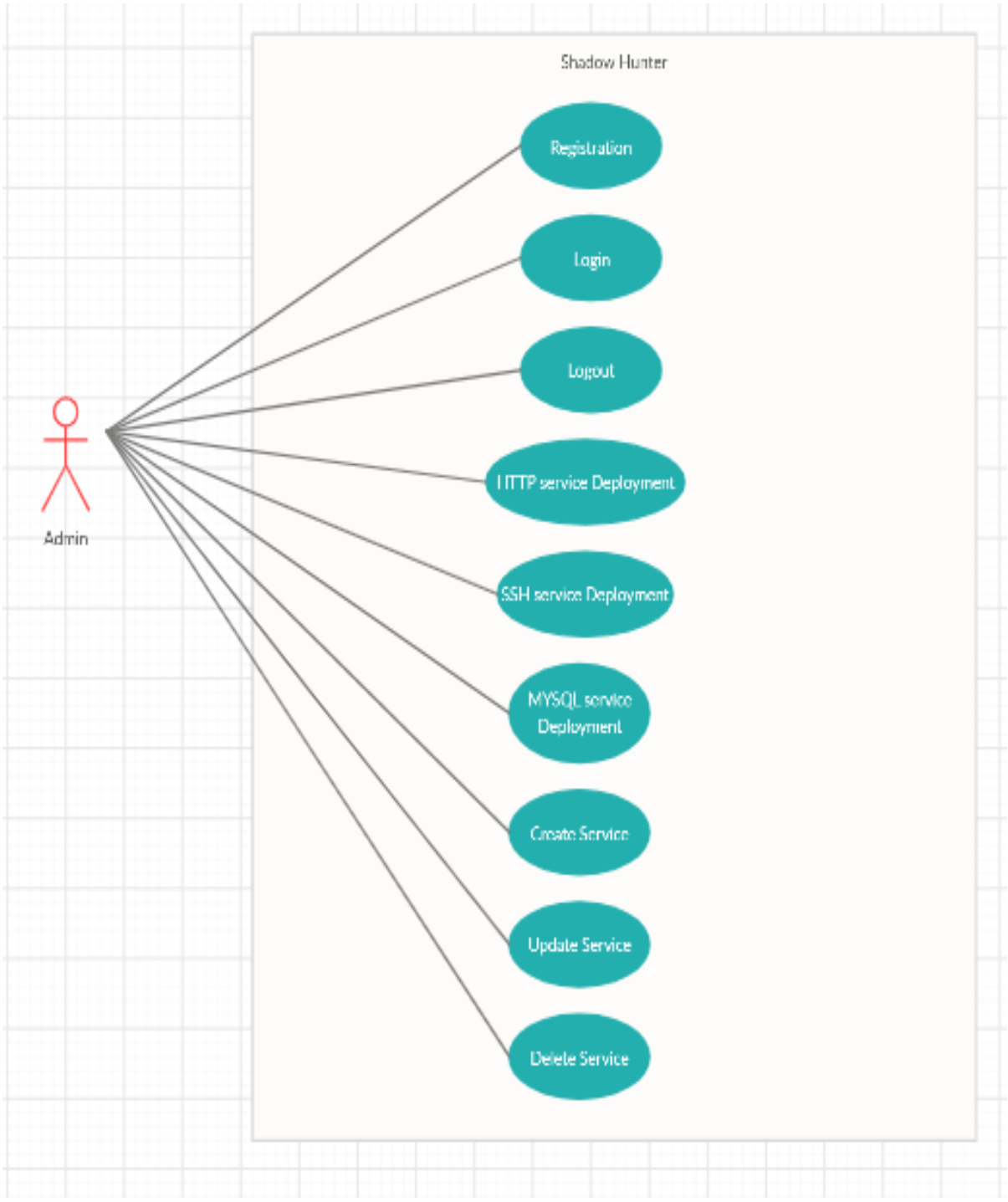


Figure 3.2 UC Diagram 2 - Services Management

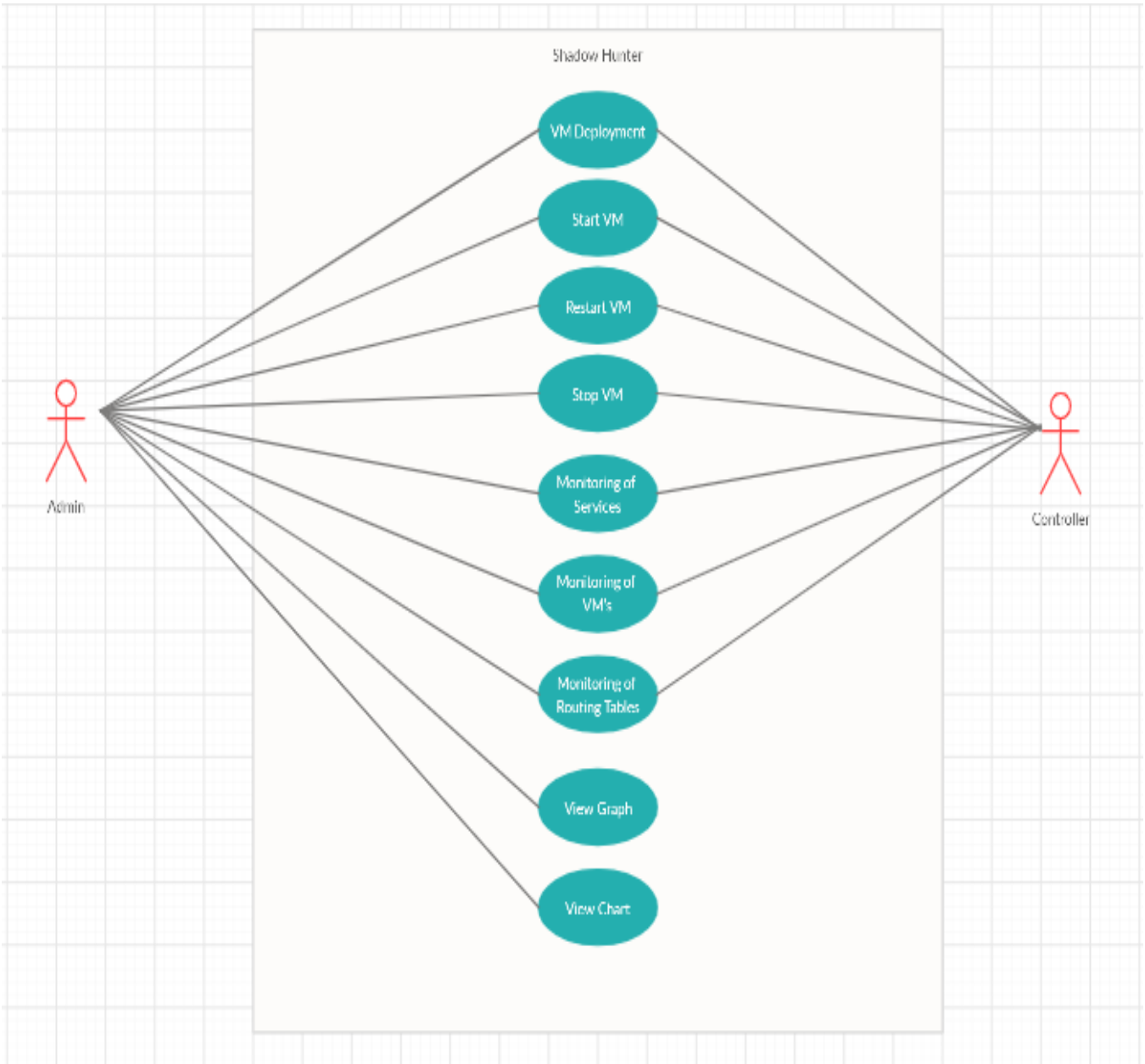


Figure 3.3 UC Diagram 3 – VM Management

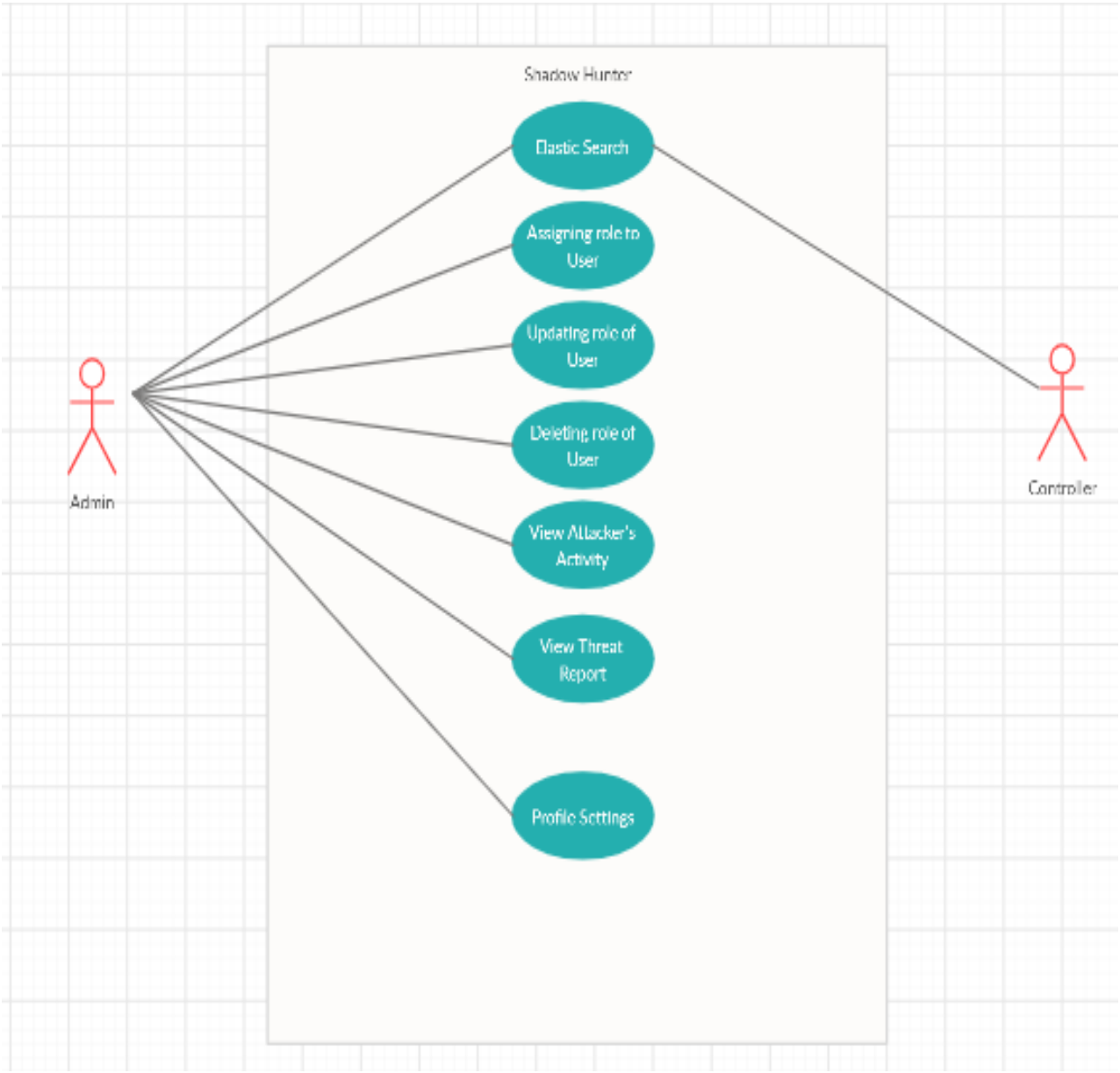


Figure 3.4 UC Diagram 4 – User Management

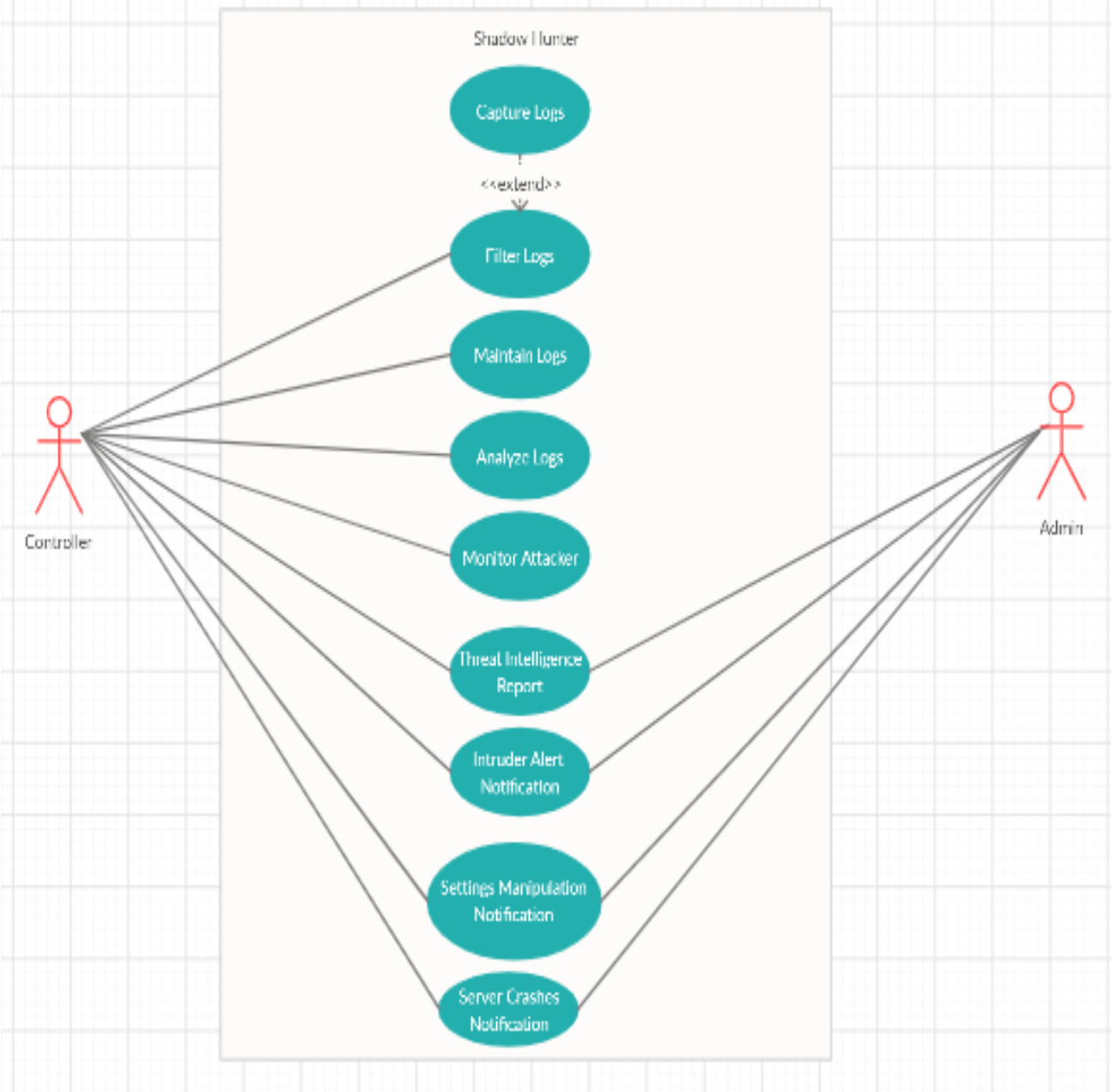


Figure 3.5 UC Diagram 5 – Monitoring

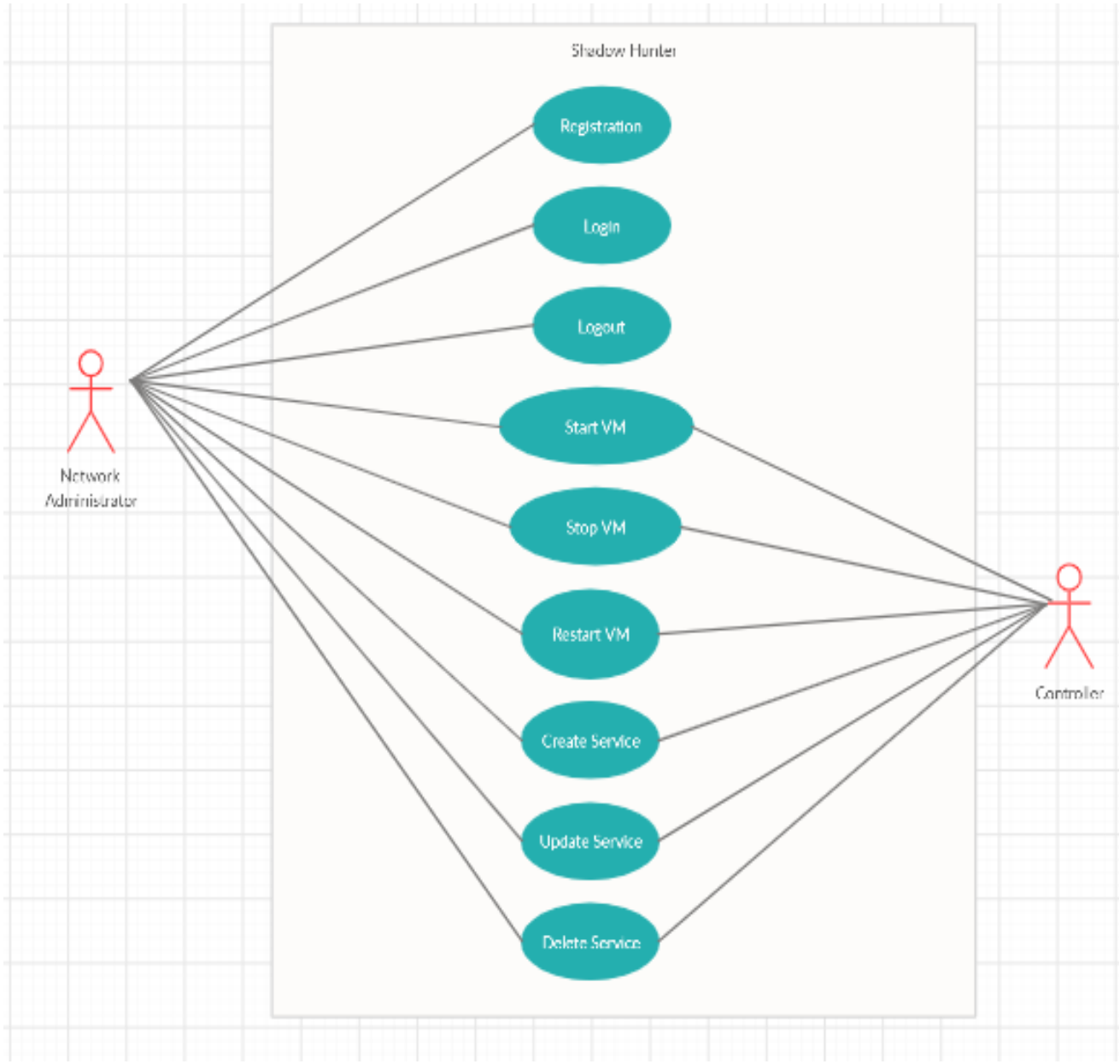


Figure 3.6 UC Diagram 6 – Network Administration

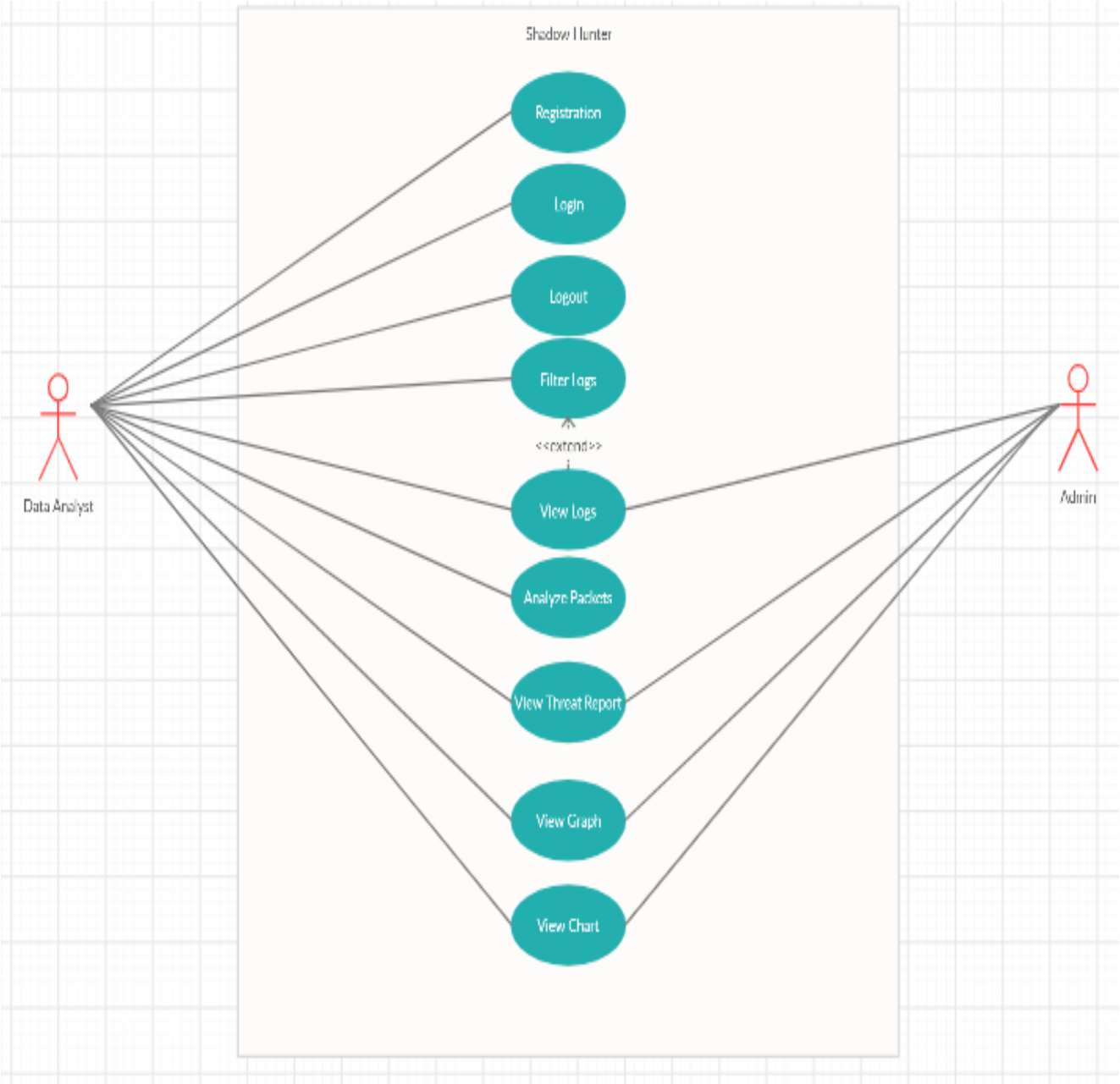


Figure 3.7 UC Diagram 7 – Visualization

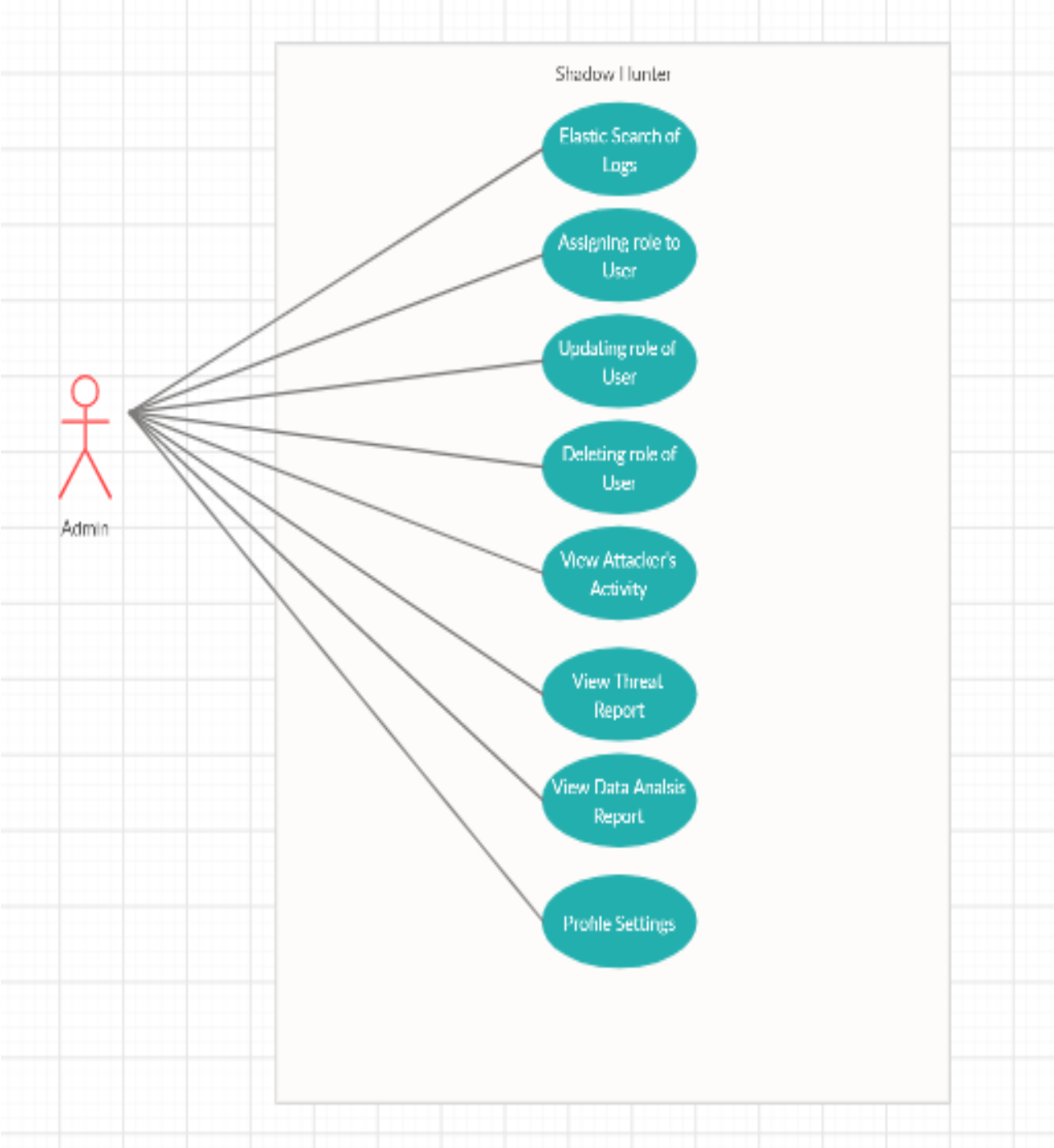


Figure 3.8 UC Diagram 8 – Admin Usage

3.2 Detailed Use Case

Use Case ID	Actors	Use Case Name
UC-001	Admin/User	Admin/User Registration
UC-002	Admin/User	Admin/User login
UC-003	Admin/User	Admin/User logout
UC-004	Admin/User	HTTP service Projection
UC-005	Admin/User	SSH service Projection
UC-006	Admin/User	MySQL service Project
UC-007	Controller	Intruder Deception
UC-008	Controller	Reply Attacker
UC-009	Controller	Engaging Intruder
UC-010	Controller	Packet Capturing
UC-011	Controller	Modify Packets
UC-012	Controller	Network Protocol Preservation
UC-013	Controller	Analyze Packets
UC-014	Controller	Identify Packets
UC-015	Controller	Open vSwitch
UC-016	Controller	Controller Management
UC-017	Admin/User	Create Service
UC-018	Admin/User	Update Service
UC-019	Admin/User	Delete Service
UC-020	Admin/User	Deploy VM
UC-021	Admin/User	Start VM
UC-022	Admin/User	Stop VM
UC-023	Admin/User	Restart VM
UC-024	Controller	Capture Logs
UC-025	Controller	Filter Logs
UC-026	Controller	Maintain Logs
UC-027	Controller	Analyze Logs
UC-028	Controller	Monitor Attacker
UC-029	Admin/User	Monitor Services
UC-030	Admin/User	Monitor VM’s
UC-031	Admin/User	Monitor Routing Tables
UC-032	Admin/User	View Graph
UC-033	Admin/User	View Chart
UC-034	Admin/User	MongoDB for Logs
UC-035	Admin/User	Assign role to User
UC-036	Admin/User	Remove role of User
UC-037	Admin/User	Update role of User
UC-038	Admin/User	View Attacker’s activity

UC-039	Admin/User	View Threat Report
UC-040	Controller	Network Scanner
UC-041	Controller	ONET setup
UC-042	Admin/User	Profile Settings

3.2.1 **Use Case 001: Admin/User Registration**

Use Case ID	UC-001
Use Case Name	Admin/User Registration
Actors	***Admin/User***
Description	The Admin/User will register itself to use this system.
Trigger	Register
Pre-conditions	***PRE-01: A valid Email address.***
Post-conditions	***POST-01: Admin/User Registration will be successful/unsuccessful.***
	Normal flow will be: ***NF-01: Admin/User will click Register button*** ***NF-02: Admin/User will provide his/her bio data*** ***NF-03: Admin/User will input his email address*** ***NF-04: Admin/User will input password*** ***NF-05: Admin/User will accept to terms and conditions*** ***NF-06: Admin/User will click on the signup button to complete the process.***
Alternative Flow	***N/A***
Exceptions	***E-01: An invalid email address.***
Business Rule	***BR-01: Admin/User data will be saved on local database*** ***BR-02: Admin/User must enter valid email address***
Assumptions	Admin/User has verified email address. Admin/User is qualified to use this system.

Table 1: UC-001 Admin/User registration

3.2.2 **Use Case 002: Admin/User Login**

Use Case ID	UC-002
Use Case Name	Admin/User Login
Actors	***Admin/User***
Description	***Admin/User*** will login to the system by giving his credentials.
Trigger	Sign In
Pre-conditions	***PRE-01: Admin/User must have an account on this system.*** ***Admin/User must remember his account name and password***
Post-conditions	***POST-01: Admin/User will be signed in or will be stopped from signing in.***

Normal Flow	Normal flow will be*:* ***NF-01: Admin/User will click on the sign in button*** ***NF-02: Admin/User will give credentials to the system*** ***NF-03: Admin/User will click on the log in button to logged in.***
Alternative Flow	***The Admin/User will sign in using google API*** ***AF-01: The Admin/User is on the login page*** ***AF-02: Admin/User will click on the google button*** ***AF-03: The Admin/User will verify themselves to share google credentials with our system*** ***AF-04: The Admin/User will be log in to our system***
Exceptions	***E-01: Admin/User does not remember his password***
Business Rule	***BR-01: Admin/User must enter the registered email address on the system.*** ***BR-02: Password should be matched with the registered password in the database.***
Assumptions	Admin/User is already registered.

Table 2: UC-002 Admin/user login

3.2.3 Use Case 003: Admin/User Logout

Use Case ID	UC-003
Use Case Name	Admin/User log out
Actors	Admin/User
Description	Admin/User will log out from the system by pressing log out button.
Trigger	Log out button
Pre-conditions	***PRE-01: Admin/User must have an account.*** ***Admin/User must be logged in***
Post-conditions	***POST-01: Admin/User will be logged out of the system.*** ***Admin/User will be redirected to the main page.***
Normal Flow	Normal flow will be*:* ***NF-01: Admin/User will log in to the system*** ***NF-02: Admin/User will visit dashboard to log out from the system.*** ***NF-03: Admin/User will press account button*** ***NF-04: Admin/User will press on log out button*** ***NF-05:***
Alternative Flow	***N/A***
Exceptions	***E-01: Admin/User internet is not working***
Business Rule	***N/A***
Assumptions	Admin/User is login

Table 3: UC-003 Admin/User logout

3.2.4 Use Case 004: Http Service Deployment

Use Case ID	UC-004
Use Case Name	Http Service deployment
Actors	Admin/User
Description	Deploying low interaction decoys in http same as high interaction decoys to deceive the intruder.
Trigger	Deploy Http Service
Pre-conditions	***PRE-01: Admin/User is logged in*** ***PRE-02: Service Projection script should be available.*** ***PRE-03: Machines are accessible to Admin/User*** ***PRE-04: The machine status is ON***
Post-conditions	***POST-01: Service should start working*** ***POST-02: Service will be bind to an IP address*** ***Service should show some errors.***
Normal Flow	Normal flow will be: ***NF-01: Admin/User login to the page.*** ***NF-02: Admin/User will go to the service projection page.*** ***NF-03: Admin/User will select http service type for projection.*** ***NF-04: Admin/User will select the VM*** ***NF-05: Admin/User will deploy the http service projection.***
Alternative Flow	***N/A***
Exceptions	***E-01: Machine is OFF.*** ***E-02: IP Address is duplicated*** ***E-03: Wrong IP address is assigned to a VM*** ***Ansible is not working***
Business Rule	***BR-01: The apache packages shall be in the Linux services.***
Assumptions	Ansible is installed and is working.

Table 4: UC-004 http service deployment

3.2.5 Use Case 005: SSH Service Deployment

Use Case ID	UC-005
Use Case Name	SSH service Deployment
Actors	Admin/User
Description	Deploying low interaction decoys in ssh same as high interaction decoys to deceive the intruder.
Trigger	Deploy SSH service.
Pre-conditions	***PRE-01: Admin/User is logged in*** ***Service Projection script should be available.***
Post-conditions	***POST-01:SSH Server should start working*** ***Service should show some errors.***

Normal Flow	Normal flow will be: ***NF-01: Admin/User login to the page.*** ***NF-02: Admin/User will go to the service projection page.*** ***NF-03: Admin/User will select SSH service type for projection.*** ***NF-04: Admin/User will select the VM*** ***NF-05: Admin/User will deploy the SSH service projection.***
Alternative Flow	***N/A***
Exceptions	***E-01: Machine is OFF.*** ***E-02: IP Address is duplicated*** ***E-03: Wrong IP address is assigned to a VM*** ***Ansible is not working***
Business Rule	***BR-01: The apache packages shall be in the Linux services.***
Assumptions	Ansible is installed and is working

Table 5: UC-005 ssh service deployment

3.2.6 **Use Case 006: MYSQL Service Deployment**

Use Case ID	UC-006
Use Case Name	MYSQL Service Deployment
Actors	Admin/User
Description	Deploying low interaction decoys in mysql same as high interaction decoys to deceive the intruder.
Trigger	Deploy SSH service.
Pre-conditions	***PRE-01: Admin/User is logged in*** ***Service Projection script should be available***
Post-conditions	***POST-01: MYSQL Server should start working*** ***Service should show some errors.***
Normal Flow	Normal flow will be: ***NF-01: Admin/User login to the page.*** ***NF-02: Admin/User will go to the service projection page.*** ***NF-03: Admin/User will select MYSQL service type for projection.*** ***NF-04: Admin/User will select the VM*** ***NF-05: Admin/User will deploy the MYSQL service projection.***
Alternative Flow	***N/A***
Exceptions	***E-01: Machine is OFF.*** ***E-02: IP Address is duplicated*** ***E-03: Wrong IP address is assigned to a VM*** ***Ansible is not working***
Business Rule	***BR-01: The apache packages shall be in the Linux services.***
Assumptions	Ansible is installed and is working

Table 6: UC-006 mySQL service deployment

3.2.7 **Use Case 007: Intruder Deception**

Use Case ID	UC-007
Use Case Name	Intruder Deception
Actors	Controller
Description	Intruder will be deceived by the controller by sending him to high interaction services using packets modification.
Trigger	It's an automated process.
Pre-conditions	***PRE-01: The intruder attempt on the service*** ***PRE-02: We shall have packets of the attacker to modify them.***
Post-conditions	***POST-01: Attacker will be sent to the high interaction services.***
Normal Flow	Normal flow will be: ***NF-01: Attacker will attack on the service*** ***NF-02: Attacker will try to communicate with shadow network*** ***NF-03: Controller will start receiving packets.*** ***NF-04: Controller will modify these packets and will send attacker to high interaction service through tunnel.***
Alternative Flow	***N/A***
Exceptions	***E-01: Controller is down*** ***E-02: No communication between intruder and shadow networks.*** ***E-03: Controller have no access to shadow services*** ***E-04: Controller have no access to high interaction services***
Business Rule	***BR-01: Security should be ensured.***
Assumptions	Attacker is not aware of high interaction services.

Table 7: UC-007 intruder deception

3.2.8 **Use Case 008: Replying to Attacker**

Use Case ID	UC-008
Use Case Name	Intruder Deception
Actors	Controller
Description	Intruder will be deceived by the controller by giving him reply from high interaction decoys using tunnel
Trigger	It's an automated process.
Pre-conditions	***PRE-01: We shall have packets of the attacker to modify them.***
Post-conditions	***POST-01: Attacker will be sent to the high interaction services.***
Normal Flow	Normal flow will be: ***NF-01: Attacker have attacked on the shadow services.*** ***NF-02: Controller will send it to high interaction decoys*** ***NF-03: The high interaction decoys will entertain the attacker*** ***NF-04: Response will be forwarded to attacker's request***

Alternative Flow	***N/A***
Exceptions	***E-01: Controller is down*** ***E-02: Controller have no access to shadow services*** ***E-03: Controller have no access to high interaction services*** ***E-04: No communication between intruder and shadow network.***
Business Rule	***BR-01: Deceiving of the attacker should be possible***
Assumptions	Attacker is not aware of high interaction services.

Table 8: UC-008 replying to attacker

3.2.9 Use Case 009: Engaging Intruder

Use Case ID	UC-009
Use Case Name	Engaging Intruder
Actors	Controller
Description	Intruder will be engaged by setting him up with fake data in high interaction system.
Trigger	It's an automated process.
Pre-conditions	***PRE-01: We shall have fake data in the deception network to keep him engaged.***
Post-conditions	***POST-01: Attacker will be engaged in the high interaction services while the controller will be monitoring him closely.***
Normal Flow	Normal flow will be: ***NF-01: Attacker will attack the system*** ***NF-0 2: Attacker will try to communicate with shadow network*** ***NF-03: Controller will start receiving packets.*** ***NF-04: Controller will modify these packets and will send attacker to high interaction system through tunnel.*** ***NF-05: Attacker will start accessing fake data in the high interaction system.*** ***NF-06: Controller will start monitoring his actions.***
Alternative Flow	***N/A***
Exceptions	***E-01: Less Valuable information to an Attacker*** ***E-02: Not much information to an Attacker***
Business Rule	***N/A***
Assumptions	Attacker is not aware of fake data in high interaction services.

Table 9: UC-009 Engaging intruder

3.2.10 Use Case 010: Packet Capturing

Use Case ID	UC-010
Use Case Name	Packet Capturing

Actors	Controller
Description	The controller will start capturing packets once the intruder enters the system.
Trigger	This will be an automated process. It doesn't need any trigger.
Pre-conditions	***PRE-01: Controller should be working*** ***PRE-02: the attacker should engage itself in the network*** ***PRE-03: The attacker attempt to interact with one of shadow services***
Post-conditions	***POST-01: Packets will be captured***
Normal Flow	Normal flow will be: ***NF-01: Attacker will attack the system*** ***NF-02: Controller will start capturing packets*** ***NF-03: Controller will start sending captured packets to the Admin/User*** ***NF-04: Once the attack is finished the controller will send the details to the Admin/User.***
Alternative Flow	***N/A***
Exceptions	***E-01: No packets captured due to controller fault*** ***E-02: Packets lost due to controller misconfiguration***
Business Rule	***N/A***
Assumptions	Controller is fully functional and working

Table 10: UC-010 Packet Capturing

3.2.11 **Use Case 011: Modify Packets**

Use Case ID	UC-011
Use Case Name	Modify Packets
Actors	Controller
Description	The Controller will inspect packets that are captured, can modify packets they have captured and can view specific packets.
Trigger	It is an automated Process
Pre-conditions	***PRE-01: Packets should be captured.***
Post-conditions	***POST-01: Packet should be modified.***
Normal Flow	Normal flow will be: ***NF-01: Attacker will attack the system*** ***NF-02: Controller will start capturing packets*** ***NF-03: Controller will modify the packets.*** ***NF-04: The traffic will be routed to desired destination***
Alternative Flow	***N/A***
Exceptions	***E-01: No packets captured due to controller fault***

	E-02: Packets lost due to controller
Business Rule	***BR-01: Security should be ensured***
Assumptions	Controller is fully functional and working

Table 11: UC-011 modify packet

3.2.12 **Use Case 012: Network Protocol Preservation**

Use Case ID	UC-012
Use Case Name	Network Protocol Preservation
Actors	Controller
Description	Packets will be manipulated by the controller by keeping its IP address same as the organization network so that attacker will be deceived.
Trigger	It's an automated process.
Pre-conditions	***PRE-01: Attacker shall request some data***
Post-conditions	***POST-01: Network Protocols will be kept identical.***
Normal Flow	Normal flow will be: ***NF-01: Attacker will attack the system*** ***NF-02: Attacker will try to communicate with shadow network*** ***NF-03: The network protocols will be kept identical*** ***NF-03: Deception network will send back reply to the attacker*** ***NF-04: Controller will manipulate these packets header by changing its IP address and will send it to the attacker.***
Alternative Flow	***N/A***
Exceptions	***E-01: Controller is down*** ***E-02: No request sent from attacker***
Business Rule	***BR-01: Manipulation will help controller deceive intruder***
Assumptions	Packets are received by the controller.

Table 12: UC-012 network protocol preservation

3.2.13 **Use Case 013: Analyze Packets**

Use Case ID	UC-013
Use Case Name	Analyze Packets
Actors	Admin/User
Description	The Admin/User will inspect packets that are captured. They can analyze packets they have captured and can view specific packets.
Trigger	View Packets
Pre-conditions	***PRE-01: Admin/User should be logged in*** ***PRE-02: The attempt has been made to the services*** ***PRE-03: The controller has captured the packets*** ***Internet should be stable*** ***Controller should be working***

Post-conditions	***POST-01: Packet should be displayed*** ***System shall show some errors.***
Normal Flow	Normal flow will be: ***NF-01: Attacker will attack the system*** ***NF-02: Controller will start capturing packets*** ***NF-03: Controller will start sending captured packets to the Admin/User*** ***NF-04: Admin/User will start analysis the captured packets.***
Alternative Flow	***N/A***
Exceptions	***E-01: No packets captured due to controller fault*** ***Packets lost due to controller***
Business Rule	***BR-01: understanding attacker through analysis.***
Assumptions	Controller is fully functional and working

Table 13: UC-013 analyzes packets

3.2.14 **Use Case 014: Identify Packets**

Use Case ID	UC-014
Use Case Name	Identify Packets
Actors	Controller
Description	The Controller will receive the packets from high interaction services identify them and will send the packet to required requester.
Trigger	It doesn't need any trigger.
Pre-conditions	***PRE-01: Controller should be started*** ***Attacker must be in the high interaction Service***
Post-conditions	***POST-01: Packets will be sent to the corresponding attacker***
Normal Flow	Normal flow will be: ***NF-01: SDN will trap the attacker*** ***NF-02: Controller will start receiving packets from the attacker's log.*** ***NF-03: Controller will start identifying packets.*** ***NF-04: Controller will sent packets to the corresponding requester.***
Alternative Flow	***N/A***
Exceptions	***E-01: No packets received.***
Business Rule	***N/A***
Assumptions	Attacker is in the high interaction service

Table 14: UC-014 identify packet

3.2.15 **Use Case 015: Open vSwitch**

Use Case ID	UC-015
Use Case Name	Open Switch

Actors	Switch
Description	Open switch will send packets to the controller first time an attack happens. And will maintain the routing between different end-points
Trigger	Packets have been received by the attacker
Pre-conditions	***PRE-01: Attack must have happened***
Post-conditions	***POST-01: Switch will send packets to the controller.***
Normal Flow	Normal flow will be: ***NF-01: Attacker must enter the system.*** ***NF-02: Switch will start sending packets to the controller*** ***NF-03: Switch will start maintaining tables for coming packets routing*** ***NF-04: Next time attack happens the open switch will handle itself.***
Alternative Flow	***N/A***
Exceptions	***E-01:***
Business Rule	***N/A***
Assumptions	***N/A***

Table 15: UC-015 Open vSwitch

3.2.16 **Use Case 016: Controller Management**

Use Case ID	UC-016
Use Case Name	Controller Management
Actors	Controller
Description	Controller will manage all the logs, packets, services and management on its own.
Trigger	This will be an automated process. It Doesn't need any trigger
Pre-conditions	***PRE-01: Attack must happen*** ***PRE-02: Controller scripts shall run fine***
Post-conditions	***POST-01: Controller will be managing all the activities.***
Normal Flow	Normal flow will be: ***NF-01: Attacker will enter the system*** ***NF-02: Switch will send packets to the controller.*** ***NF-03: Controller will start capturing packets*** ***NF-04: It will reroute the traffic to desired destination.*** ***NF-05: Controller will start analyzing logs*** ***NF-06: As soon as an attack finished it will start sending data to the Admin/User.***
Alternative Flow	***AF-01:***
Exceptions	***E-01: No attack happens***
Business Rule	***N/A***

Assumptions	Controller scripts are working

Table 16: UC-016 Controller Management

3.2.17 **Use Case 017: Create Service**

Use Case ID	UC-017
Use Case Name	Create Service
Actors	Admin/User
Description	The Admin/User will create service of his own choice. They can create a service from known options.
Trigger	Create Service
Pre-conditions	***PRE-01: Admin/User shall be logged in*** ***Admin/User should know about service criteria*** ***Admin/User shall have the authority to create service***
Post-conditions	***POST-01: Service should be created*** ***Service should run some errors***
Normal Flow	Normal flow will be: ***NF-01: Admin/User will login to the system*** ***NF-02: Admin/User will go to the services page.*** ***NF-03: Admin/User will select create service*** ***NF-04: Admin/User will fill in the form*** ***NF-05: Admin/User will press the create service button to start it***
Alternative Flow	***N/A***
Exceptions	***E-01: poor internet connection*** ***E-02: Services are not integrated*** ***Admin/User have no access to start service***
Business Rule	***N/A***
Assumptions	Controller is set to project service

Table 17: UC-017 Create service

3.2.18 **Use Case 018: Update Service**

Use Case ID	UC-018
Use Case Name	Update Service
Actors	Admin/User
Description	The Admin/User will update service of his own choice. It will help him in moving shadow service from one VM to another
Trigger	Update Service
Pre-conditions	***PRE-01: Admin/User shall be logged in*** ***PRE-02: The services need to be integrated*** ***Admin/User should know about service criteria*** ***Admin/User shall have the authority to update service***

Post-conditions	***POST-01: Service should be updated*** ***Service should run some errors***
Normal Flow	Normal flow will be: ***NF-01: Admin/User will login to the system*** ***NF-02: Admin/User will go to the services page.*** ***NF-03: Admin/User will select update service*** ***NF-04: Admin/User will fill in the form*** ***NF-05: Admin/User will press the update service button to start it***
Alternative Flow	***N/A***
Exceptions	***E-01: poor internet connection*** ***E-02: The page has no access to that subnet*** ***E-03: The VMs are down*** ***Admin/User have no access to start service***
Business Rule	***N/A***
Assumptions	Controller is set to project service

Table 18 UC-018 update service

3.2.19 **Use Case 019: Delete Service**

Use Case ID	UC-019
Use Case Name	Delete Service
Actors	Admin/User
Description	The Admin/User will delete service of his own choice. It will help him in deleting a service from a subnet
Trigger	Delete Service
Pre-conditions	***PRE-01: Admin/User shall be logged in*** ***PRE-02: The VM's are up*** ***PRE-03: The VM's are connected with dashboard*** ***Admin/User should know about service criteria*** ***Admin/User shall have the authority to delete service***
Post-conditions	***POST-01: Service should be deleted*** ***Service should run some errors***
Normal Flow	Normal flow will be: ***NF-01: Admin/User will login to the system*** ***NF-02: Admin/User will go to the services page.*** ***NF-03: Admin/User will select delete service*** ***NF-04: Admin/User will fill in the form*** ***NF-05: Admin/User will press the delete service button to start it***
Alternative Flow	***N/A***

Exceptions	***E-01: poor internet connection*** ***E-02: The IP addresses can be configured wrong*** ***Admin/User have no access to start service***
Business Rule	***N/A***
Assumptions	Controller is set to project service

Table 19: UC-019 delete service

3.2.20 **Use Case 020: Deploy VM**

Use Case ID	UC-020
Use Case Name	Deploy VM
Actors	Admin/User
Description	Deploy VM will be done by the Admin/User as per organization need. VM's will route the traffic.
Trigger	Deploy VM
Pre-conditions	***PRE-01: Admin/User must be logged in*** ***PRE-02: The machine must have network connectivity*** ***Admin/User shall have knowledge of cloud VM's.*** ***Admin/User shall have the access to cloud management.***
Post-conditions	***POST-01: VM's shall be deployed.*** ***VM's shall show some errors.***
Normal Flow	Normal flow will be: ***NF-01: Admin/User will login to the system*** ***NF-02: Admin/User will go to the cloud management*** ***NF-03: Admin/User will select Deploy VM.*** ***NF-04: Admin/User will fill in the form.*** ***NF-05: Admin/User will deploy VM.***
Alternative Flow	***N/A***
Exceptions	***E-01: internet instability.*** ***E-02: Wrong VM deployment using wrong IP addressing*** ***No access to the cloud management***
Business Rule	***N/A***
Assumptions	VM's are functional and are on standby position.

Table 20: UC-020 deploys VM

3.2.21 **Use Case 021: Start VM**

Use Case ID	UC-021
Use Case Name	Start VM
Actors	Admin/User
Description	Admin/User will start VM services in the Deploy VM page to start a specific VM.
Trigger	Start VM

Pre-conditions	***PRE-01: Admin/User must be logged in*** ***PRE-02: The Machine IP needs to be accessible*** ***Admin/User shall have knowledge of cloud VM's.*** ***Admin/User shall have the access to VM management.***
Post-conditions	***POST-01: VM shall start working*** ***VM shall throw some errors.***
Normal Flow	Normal flow will be: ***NF-01: Admin/User will login to the system*** ***NF-02: Admin/User will go to the cloud management*** ***NF-03: Admin/User will select VM management.*** ***NF-04: Admin/User will select start VM.*** ***NF-05: Admin/User will fill the form.*** ***NF-06: Admin/User will press Start VM***
Alternative Flow	***N/A***
Exceptions	***E-01: internet instability.*** ***No access to the cloud management.***
Business Rule	***N/A***
Assumptions	VM's are functional and are on standby position.

Table 21: UC-021 start VM

3.2.22 **Use Case 022: Stop VM**

Use Case ID	UC-022
Use Case Name	Stop VM
Actors	Admin/User
Description	Admin/User will stop VM services in the Deploy VM page to stop a specific VM.
Trigger	Stop VM
Pre-conditions	***PRE-01: Admin/User must be logged in*** ***PRE-02: The machine must have network connectivity*** ***PRE-03: The Machine IP needs to be accessible*** ***Admin/User shall have knowledge of cloud VM's.*** ***Admin/User shall have the access to VM management.***
Post-conditions	***POST-01: VM shall stop working*** ***VM shall throw some errors.***
Normal Flow	Normal flow will be: ***NF-01: Admin/User will login to the system*** ***NF-02: Admin/User will go to the cloud management*** ***NF-03: Admin/User will select VM management.*** ***NF-04: Admin/User will select stop VM.*** ***NF-05: Admin/User will fill the form.*** ***NF-06: Admin/User will press Stop VM***

Alternative Flow	***N/A***
Exceptions	***E-01: internet instability.*** ***No access to the cloud management.***
Business Rule	***N/A***
Assumptions	VM's are functional and are on standby position.

Table 22: UC-022 stop VM

3.2.23 Use Case 023: Restart VM

Use Case ID	UC-023
Use Case Name	Restart VM
Actors	Admin/User
Description	Admin/User will restart VM services in the Deploy VM page to restart a specific VM.
Trigger	Restart VM
Pre-conditions	***PRE-01: Admin/User must be logged in*** ***PRE-02: The machine must have network connectivity*** ***PRE-03: The Machine IP needs to be accessible*** ***Admin/User shall have knowledge of cloud VM's.*** ***Admin/User shall have the access to VM management.***
Post-conditions	***POST-01: VM shall restart working*** ***VM shall throw some errors.***
Normal Flow	Normal flow will be*:* ***NF-01: Admin/User will login to the system*** ***NF-02: Admin/User will go to the cloud management*** ***NF-03: Admin/User will select VM management.*** ***NF-04: Admin/User will select restart VM.*** ***NF-05: Admin/User will fill the form.*** ***NF-06: Admin/User will press restart VM***
Alternative Flow	***N/A***
Exceptions	***E-01: internet instability.*** ***No access to the cloud management.***
Business Rule	***N/A***
Assumptions	VM's are functional and are on standby position.

Table 23: UC-023 Restart VM

3.2.24 Use Case 024: Capture Logs

Use Case ID	UC-024
Use Case Name	Capture Logs
Actors	Controller

Description	As soon as an attack happens controller will start capturing logs from all over the system and will show it to the Admin/User to perform certain tasks on it.
Trigger	This will be an automated process. It Doesn't need any trigger.
Pre-conditions	***PRE-01: Attack must be happened.*** ***Controller should be in working state.***
Post-conditions	***POST-01: Controller shall start capturing logs*** ***Controller shall throw some errors.***
Normal Flow	Normal flow will be: ***NF-01: The attacker will attack on the system.*** ***NF-02: The controller will send him to the high interaction service*** ***NF-03: The controller will start analyzing its moves.*** ***NF-04: As soon as the attacker start working in the system, controller will start capturing logs*** ***NF-05: the controller will send all the capture logs to the Admin/User.***
Alternative Flow	***N/A***
Exceptions	***E-01: The attacker turn off service logs***
Business Rule	***N/A***
Assumptions	Controller is working fine and is ready to capture logs.

Table 24: UC-024 Capture logs

3.2.25 **Use Case 025: Filter Logs**

Use Case ID	UC-025
Use Case Name	Filter Logs
Actors	Admin/User
Description	Admin/User will filter all the logs as per organization need and will start analyzing them.
Trigger	Filter Logs
Pre-conditions	***PRE-01: Admin/User is logged in*** ***PRE-02: Logs are captured*** ***PRE-03: Admin/User has the authority to filter logs.***
Post-conditions	***POST-01: Logs will be filtered***
Normal Flow	Normal flow will be: ***NF-01: Admin/User will login to the page*** ***NF-02: Admin/User will select logs Engine page.*** ***NF-03: Admin/User will start seeing all the captured logs*** ***NF-04: Admin/User will filter logs as per organization need.*** ***NF-05: Admin/User will trigger filter logs button to filter logs.***
Alternative Flow	***N/A***
Exceptions	***E-01: No proposed options are available in filters***

Business Rule	***N/A***
Assumptions	Admin/User knows how to capture logs.

Table 25: UC-025 filter logs

3.2.26 Use Case 026: Maintain Logs

Use Case ID	UC-026
Use Case Name	Logs Maintenance
Actors	Controller
Description	Controller will maintain the logs by storing them to a database so that can be monitored later.
Trigger	This will be an automated process. It Doesn't need any trigger.
Pre-conditions	***PRE-01: Attack must be happened.*** ***PRE-02: Controller should be in working state.*** ***PRE-03: Logs are captured.***
Post-conditions	***POST-01: Logs will be maintained.***
Normal Flow	Normal flow will be: ***NF-01: The attacker will attack on the system.*** ***NF-02: The controller will send him to the high interaction service*** ***NF-03: The controller will start analyzing its moves.*** ***NF-04: As soon as the attacker start working in the system controller will start capturing logs*** ***NF-05: Controller will start storing these logs on a database.*** ***NF-06: The controller will send all the capture logs to the Admin/User.*** ***NF-07: Controller will maintain these logs from time to time for future use.***
Alternative Flow	***N/A***
Exceptions	***E-01: No logs captured.*** ***E-02: Storing space is full*** ***E-03: Database is not accessible***
Business Rule	***N/A***
Assumptions	Controller is working fine and is ready to maintain logs.

Table 26: UC-026 Maintain logs

3.2.27 Use Case 027: Analyze Logs

Use Case ID	UC-027
Use Case Name	Analyze Logs
Actors	Controller
Description	Controller will analyze the logs to completely understand the intentions of the attacker.
Trigger	This will be an automated process. It Doesn't need any trigger.

Pre-conditions	***PRE-01: Attack must be happened.*** ***PRE-02: Controller should be in working state.*** ***PRE-03: Logs are captured.***
Post-conditions	***POST-01: Logs will be analyzed.***
Normal Flow	Normal flow will be: ***NF-01: The attacker will attack on the system.*** ***NF-02: The controller will send him to the high interaction service*** ***NF-03: The controller will start analyzing its moves.*** ***NF-04: As soon as the attacker start working in the system controller will start capturing logs*** ***NF-05: The controller will send all the capture logs to the Admin/User.*** ***NF-06: Controller will start storing these logs on a database.*** ***NF-07: Controller will maintain these logs from time to time for future use.*** ***NF-08: Controller will start analyzing these logs.*** ***NF-09: Controller will get as much information as possible***
Alternative Flow	***N/A***
Exceptions	***E-01: No logs captured.*** ***E-02: No particular matched fields are found***
Business Rule	***N/A***
Assumptions	Controller is working fine and is ready to analyze logs.

Table 27: UC-027 analyze log

3.2.28 **Use Case 028: Monitor Attacker**

Use Case ID	UC-028
Use Case Name	Monitor Attacker
Actors	Admin/User/Controller
Description	The controller will monitor the attacker in detailed possible way. All his tactics techniques and procedures he used to view the system data.
Trigger	This will be an automated process. It Doesn't need any trigger
Pre-conditions	***PRE-01: Attack must be happened.*** ***PRE-02: Controller should be in working state.***
Post-conditions	***POST-01: Attackers will be monitored.***
Normal Flow	Normal flow will be: ***NF-01: Attacker will attack the system.*** ***NF-02: Controller will start its function*** ***NF-03: Controller will start monitoring attacker.*** ***NF-04: Controller will start sending data to the Admin/User.***
Alternative Flow	***N/A***
Exceptions	***E-01: Controller stop working*** ***E-02: Attacks didn't happened***

Business Rule	***N/A***
Assumptions	Attacker is already in the system.

Table 28: UC-028 monitor attacker

3.2.29 **Use Case 029: Monitor Services**

Use Case ID	UC-029
Use Case Name	Monitor Services
Actors	Admin/User
Description	Admin/User will monitor the health of low interaction projected services to make sure that everything is working fine.
Trigger	Start Monitoring
Pre-conditions	***PRE-01: Admin/User must be logged in*** ***PRE-02: Attacker is engaged in the attack.***
Post-conditions	***POST-01: Admin/User will start monitoring the health of projected services.***
Normal Flow	Normal flow will be: ***NF-01: Admin/User will login to the system.*** ***NF-02: Admin/User will go to the Health Monitoring Page.*** ***NF-03: Admin/User will select monitor Projected Services*** ***NF-04: Admin/User will trigger start monitoring to monitor the health of projected Services.***
Alternative Flow	***N/A***
Exceptions	***E-01: Internet instability*** ***E-02: Admin/User has no knowledge of monitoring***
Business Rule	***N/A***
Assumptions	Attack has already happened.

Table 29: UC-029 monitor services

3.2.30 **Use Case 030: Monitor VM's**

Use Case ID	UC-030
Use Case Name	Monitor VM's
Actors	Admin/User
Description	Admin/User will monitor the health of cloud VM's to make sure that everything is working fine.
Trigger	VM status
Pre-conditions	***PRE-01: Admin/User must be logged in*** ***PRE-02: The VM is deployed***
Post-conditions	***POST-01: Admin/User will start monitoring the health of cloud VM's.***
Normal Flow	Normal flow will be: ***NF-01: Admin/User will login to the system.***

	NF-02: Admin/User will go to the Health Monitoring Page. ***NF-03: Admin/User will select monitor cloud VM's.*** ***NF-04: Admin/User will trigger start monitoring to monitor the health of cloud VM's.***
Alternative Flow	***N/A***
Exceptions	***E-01: Internet instability*** ***E-02: Admin/User has no knowledge of monitoring***
Business Rule	***N/A***
Assumptions	Attack has already happened.

Table 30: UC-030 Monitor VM's

3.2.31 Use Case 031: Monitor Routing Tables

Use Case ID	UC-031
Use Case Name	Monitor Routing Tables
Actors	Admin/User
Description	Admin/User will monitor the health of routing tables to make sure that attacker is being diverted from shadow services to High Interaction decoys
Trigger	Start Monitoring
Pre-conditions	***PRE-01: Admin/User must be logged in*** ***PRE-02: Attacker is engaged in the attack.***
Post-conditions	***POST-01: Admin/User will start monitoring the health of routing tables.***
Normal Flow	Normal flow will be: ***NF-01: Admin/User will login to the system.*** ***NF-02: Admin/User will go to the Health Monitoring Page.*** ***NF-03: Admin/User will select monitor routing tables.*** ***NF-04: Admin/User will trigger start monitoring to monitor the health of routing tables.***
Alternative Flow	***N/A***
Exceptions	***E-01: Internet instability*** ***E-02: The flows are wrongly interpreted*** ***E-02: Admin/User has no knowledge of monitoring***
Business Rule	***N/A***
Assumptions	Attack has already happened.

Table 31: UC-031 Monitor routing tables

3.2.32 **Use Case 032: View Graph**

Use Case ID	UC-032
Use Case Name	View Graph
Actors	Admin/User
Description	Admin/User will visualize all the data through dashboard and will see different graphs to analyze the behavior of the attacker and monitor the different activities.
Trigger	View Graph
Pre-conditions	***PRE-01: Admin/User must be logged in*** ***PRE-02: The logs have been captured*** ***PRE-03: The logs has been analyzed***
Post-conditions	***POST-01: Admin/User will see different detailed graphs on the dashboard.***
Normal Flow	Normal flow will be: ***NF-01: Admin/User will login to the system.*** ***NF-02: Admin/User will click on the dashboard*** ***NF-03: Admin/User will see different charts and graphs.*** ***NF-04: Admin/User will click on one of the graphs to have a detailed view of it.***
Alternative Flow	***N/A***
Exceptions	***E-01: Internet is not working*** ***E-02: The data has not been sent to Graphs*** ***E-03: The data is in the wrong format***
Business Rule	***N/A***
Assumptions	Admin/User has the credentials to login to the page

Table 32: UC-032 View Graph

3.2.33 **Use Case 033: View Chart**

Use Case ID	UC-033
Use Case Name	View Chart
Actors	Admin/User
Description	Admin/User will visualize all the data through dashboard and will see different charts to analyze the behavior of the attacker and monitor the different activities.
Trigger	View Chart
Pre-conditions	***PRE-01: Admin/User must be logged in*** ***PRE-02: The logs have been captured*** ***PRE-03: The logs has been analyzed***
Post-conditions	***POST-01: Admin/User will see different detailed charts on the dashboard.***
Normal Flow	Normal flow will be:

	NF-01: Admin/User will login to the system. ***NF-02: Admin/User will click on the dashboard*** ***NF-03: Admin/User will see different charts and graphs.*** ***NF-04: Admin/User will click on one of the charts to have a detailed view of it.***
Alternative Flow	***N/A***
Exceptions	***E-01: Internet is not working*** ***E-02: The data has not been sent to Graphs*** ***E-03: The data is in the wrong format***
Business Rule	***N/A***
Assumptions	Admin/User has the credentials to login to the page

Table 33: UC-033 View charts

3.2.34 **Use Case 034: MongoDB for Logs**

Use Case ID	UC-034
Use Case Name	MongoDB for Logs
Actors	Admin/User
Description	logs captured by log Engine will be stored in elastic search. Logs will be parse, maintain, organize and analyze.
Trigger	Search Logs
Pre-conditions	***PRE-01: Admin/User must be logged in*** ***PRE-02: Admin/User must have the authority to Search logs.***
Post-conditions	***POST-01: Admin/User will successfully search logs.***
Normal Flow	Normal flow will be*:* ***NF-01: Admin/User will login to the system.*** ***NF-02: Admin/User will go the logs section*** ***NF-03: Admin/User will enter to the logs search*** ***NF-04: Admin/User will search any logs he wants*** ***NF-05: Admin/User will trigger search logs to complete the process***
Alternative Flow	***N/A***
Exceptions	***E-01: No logs stored in the database***
Business Rule	***N/A***
Assumptions	Database is connected and is working fine

Table 34: UC-034 MongoDB for logs

3.2.35 **Use Case 035: Assign role to User**

Use Case ID	UC-035
Use Case Name	Assign role to User
Actors	Admin

Description	Admin will add a User by assigning him some role as a User.
Trigger	Add User
Pre-conditions	***PRE-01: Admin must be logged in*** ***PRE-02: Admin has the authority to enter User management section.***
Post-conditions	***POST-01: Admin will successfully add a User.***
Normal Flow	Normal flow will be: ***NF-01: Admin will login to the system*** ***NF-02: Admin will go to the User management section*** ***NF-03: Admin will select add User role.*** ***NF-04: Admin will enter User's name and his role*** ***NF-05: Admin will trigger add User button to successfully add him.***
Alternative Flow	***N/A***
Exceptions	***E-01: User is already added.***
Business Rule	***N/A***
Assumptions	Admin has the authority to enter the section

Table 35: UC-035 assign role to user

3.2.36 **Use Case 036: Remove role of User**

Use Case ID	UC-036
Use Case Name	Remove role of User
Actors	Admin
Description	Admin will remove a User by deleting his role as an User.
Trigger	Remove User
Pre-conditions	***PRE-01: Admin must be logged in*** ***PRE-02: Admin/ has the authority to enter Admin/User management section.***
Post-conditions	***POST-01: Admin will successfully remove a User.***
Normal Flow	Normal flow will be: ***NF-01: Admin will login to the system*** ***NF-02: Admin will go to the User management section*** ***NF-03: Admin will select remove User role.*** ***NF-04: Admin will enter User's name and his role*** ***NF-05: Admin will trigger remove User button to successfully remove him.***
Alternative Flow	***N/A***
Exceptions	***E-01: User is already deleted.***
Business Rule	***N/A***
Assumptions	User has the authority to enter the section

Table 36: UC-036 remove role to user

3.2.37 **Use Case 037: Update role of User**

Use Case ID	UC-037
Use Case Name	Update role of User
Actors	Admin
Description	Admin will update a User by updating his role as an Admin/User.
Trigger	Update User
Pre-conditions	***PRE-01: Admin must be logged in*** ***PRE-02: Admin has the authority to enter User management section.***
Post-conditions	***POST-01: Admin will successfully update a User.***
Normal Flow	Normal flow will be: ***NF-01: Admin will login to the system*** ***NF-02: Admin will go to the User management section*** ***NF-03: Admin will select update User role.*** ***NF-04: Admin will enter User's name and his role*** ***NF-05: Admin will trigger update User button to successfully update him.***
Alternative Flow	***N/A***
Exceptions	***E-01: User is already updated.***
Business Rule	***N/A***
Assumptions	Admin has the authority to enter the section

Table 37: UC-037 update role of user

3.2.38 **Use Case 038: View Attacker's activity**

Use Case ID	UC-038
Use Case Name	View Attacker's activity
Actors	Admin/User
Description	Admin/User can view the attacker's activity from dashboard to see what is happening.
Trigger	Dashboard
Pre-conditions	***PRE-01: Admin/User must be logged in*** ***PRE-02: Attack must be going on***
Post-conditions	***POST-01: Admin/User can successfully see attacker activity.***
Normal Flow	Normal flow will be: ***NF-01: Admin/User will login to the system.*** ***NF-02: Admin/User will go to the dashboard*** ***NF-03: Admin/User will click on the attacker activity viewing to see the activity of the attacker***
Alternative Flow	***N/A***

Exceptions	***E-01: No attack is happening***
Business Rule	***N/A***
Assumptions	Controller is working fine to show activity of the attacker

Table 38: UC-038 view attacker's activity

3.2.39 Use Case 039: View Threat Report

Use Case ID	UC-039
Use Case Name	View Threat Report
Actors	Admin/User
Description	Admin/User can view threat report from dashboard to see what attacker tried to achieve and what were the actions and goals.
Trigger	Dashboard
Pre-conditions	***PRE-01: Admin/User must be logged in*** ***PRE-02: Attack must have happened.*** ***PRE-03: Attack report has been generated***
Post-conditions	***POST-01: Admin/User can successfully see threat report.***
Normal Flow	Normal flow will be: ***NF-01: Admin/User will login to the system.*** ***NF-02: Admin/User will go to the dashboard*** ***NF-03: Admin/User will click on the threat report to see the activity of the attacker***
Alternative Flow	***N/A***
Exceptions	***E-01: No attack has happened.***
Business Rule	***N/A***
Assumptions	Controller is working fine to generate threat report.

Table 39: UC-39 view threat report

3.2.40 Use Case 040: Network Scanner

Use Case ID	UC-040
Use Case Name	Network Scanner
Actors	Controller
Description	Controller will scan the whole network to identify the potential services
Trigger	The admin/user will request the controller to scan the network by clicking on scan button
Pre-conditions	***PRE-01: Nmap needs to be installed***
Post-conditions	***POST-01: Admin/User will receive scan results on dashboard***
Normal Flow	Normal flow will be: ***NF-01: The admin will click on scan button*** ***NF-02: The request will be forwarded to controller***

	NF-03: The controller will scan the whole network using nmap. ***NF-04: The controller will sum-up the result.*** ***NF-05: The result will be sent to admin***
Alternative Flow	***N/A***
Exceptions	***E-01: No internet connection*** ***E-02: Nmap is not installed*** ***E-03: Database is not configured***
Business Rule	***N/A***
Assumptions	The tools are working properly.

Table 40: UC-040 Network Scanner

3.2.41 **Use Case 041: ONET setup**

Use Case ID	UC-041
Use Case Name	ONET setup
Actors	Controller
Description	Controller will setup the whole configuration of ONET on a machine
Trigger	The user/admin will click on add-department to add a new department
Pre-conditions	***PRE-01: The open vSwitch needs to be installed*** ***PRE-02: The machines needs to be accessible***
Post-conditions	***POST-01: The department has been successfully added.***
Normal Flow	Normal flow will be: ***NF-01: A message will be forwarded by admin.*** ***NF-02: Controller will check availability*** ***NF-03: The controller will deploy the department.*** ***NF-04: The user/admin will get a message that department has been successfully added***
Alternative Flow	***N/A***
Exceptions	***E-01: No internet connection*** ***E-02: Machine is not accessible*** ***E-03: Required Tools are not installed***
Business Rule	***N/A***
Assumptions	The ONET setup is not done yet.

Table 41: UC-041 ONET setup

3.2.42 **Use Case 042: Profile Settings**

Use Case ID	UC-042
Use Case Name	Profile Settings
Actors	Admin/User

Description	Admin/User will change his profile settings like his bio or any other personal information.
Trigger	Profile Settings
Pre-conditions	***PRE-01: Admin/User must be logged in***
Post-conditions	***POST-01: Admin/User can successfully update profile settings***
Normal Flow	Normal flow will be: ***NF-01: Admin/User will log in to the system*** ***NF-02: Admin/User will click account*** ***NF-03: Admin/User will click profile setting to enter the profile setting page.*** ***NF-04: Admin/User will update its settings and will trigger update profile to update settings.***
Alternative Flow	***N/A***
Exceptions	***E-01: No internet connection*** ***E-02: Wrong information provided***
Business Rule	***N/A***
Assumptions	N/A

Table 42: UC-042 Profile setting

3.3 Functional Requirements:

Functional Requirements for **Shadow Hunters** are as follows

FR ID.	FR Name	Description
FR-001	User Registration	The user shall be able to fill registration form to get registered.
FR-002	Login	Users must be able to use their username and password to login.
FR-003	Forget Password	In case if user forgot his password he shall be able to restore his password by clicking forget password.
FR-004	Invalid credentials	The user shall not be permitted to login by providing invalid credentials.
FR-005	Logout	User shall be able to logout from the account.
FR-006	Display profile	User shall be able to view their profile
FR-007	Edit profile	User shall be able to edit their profile information.
FR-008	View user profile	Admin shall be able to view the profiles of other users.
FR-009	Show confirmation dialog	Confirmation dialog shall ask user to conduct any critical task or cancel it.
FR-010	Show error dialog	System should display error dialog if there is something incorrect in the implementation or if there is any unwanted circumstances.
FR-011	Show dashboard	Dashboards shows the graphical representation of data and help us to easily visualize huge amount of data and provide us less but accurate information
FR-012	View attacker activity	Admin shall be able to view the attacker's activity.

FR-013	Installing openvpn script	Controller shall be able to install the openvpn script on ONET machine.
FR-014	Running openvpn script	Controller shall be able to run the openvpn script to install the tunnel.
FR-015	Creating tunnel	Controller shall be able to create an openvpn tunnel
FR-016	Monitor attacker activity	Controller shall be able to monitor attacker activity.
FR-017	Create service	Admin shall be able to create different services.
FR-018	Start service	Admin shall be able to up the service within the network.
FR-019	End service	Admin shall be able to down the service from the network.
FR-020	Update service	Admin shall be able to update the network configuration of deployed services.
FR-021	Delete service	Admin shall be able to delete service from the network.
FR-022	Generate alert	System should be able to generate an alert when an intruder try to interact with one of our projected services.
FR-023	Send alert	System shall be able to send an alert to admin when an intruder breaches.
FR-024	View alert	Admin shall be able to view an alert generated by the system.
FR-025	Delete alert	Admin shall be able to make required directories on machines
FR-026	Make Directories	System should be able to generate server crashes notification.
FR-027	Vpn client file creation	System should be able to create client vpn files that includes network information
FR-028	Sending vpn files	System should be able to transfer the vpn files from server to desired clients.
FR-029	Add user	Admin shall be able to add a new user.
FR-030	Assign role	Admin shall be able to assign role to users.
FR-031	Remove role	Admin shall be able to remove role of a user.
FR-032	Update role	Admin shall be able to update the role of a user.
FR-033	Edit IP address	User shall be able to edit IP address to deploy VM.
FR-034	Inspect IP address	Controller shall be able to inspect IP addresses of each incoming and outgoing packets.
FR-035	Inspect switch port	Controller shall be able to inspect arriving packets switch ports.
FR-036	Inspect Vxlan id	Controller shall be able to inspect Vxlan id of incoming packets.
FR-037	Modify IP address	Controller shall be able to modify IP address of incoming and outgoing packets.
FR-038	Modify destination port	Controller shall be able to modify the destination switch port of incoming and outgoing traffic.
FR-039	Modify MAC address	Controller shall be able to modify MAC address of incoming and outgoing traffic.
FR-040	Capture packet	Controller shall be able to capture incoming and outgoing traffic
FR-041	Analyze packet	Controller shall be to analyze the requested services
FR-042	View graph	Admin shall be able to view graph.
FR-043	Edit graph setting	Admin shall be able to edit graph setting.
FR-044	View chart	Admin shall be able to view charts.
FR-045	Search log	Admin shall be able to search specific logs from elastic search.
FR-046	Inspect log	Admin shall be able to inspect logs from the elastic search.
FR-047	Capture log	Controller shall be able to capture logs of different services.
FR-048	Filter log	Admin shall have the ability to apply filter on logs.
FR-049	Analyze log	Admin shall be able to analyze the captured logs.
FR-050	Store log	Elastic search shall be used to store capture logs.

FR-051	View projected services health	Admin shall be able to view health of projected services.
FR-052	View cloud VM's health	Admin shall be able to view health of cloud VM's.
FR-053	View routing table health	Admin shall be able to view flows of routing tables.
FR-054	Setting unique name for vpn clients	Controller shall be able to give unique naming scheme to each vpn clients.
FR-055	Unique IP address for each vpn client	Controller shall be able to assign unique ip addresses to each vpn clients.
FR-056	Deploy HTTP service	Controller shall be able to deploy HTTP service across the network.
FR-057	Deploy SSH service	Controller shall be able to deploy SSH service across the network.
FR-058	Deploy MySQL service	Controller shall be able to deploy MySQL service.
FR-059	Attacker request to HTTP service	Attacker shall be able to request resources from HTTP service.
FR-060	Attacker request to SSH service	Attacker shall be able to request resources from SSH service.
FR-061	Attacker request to MySQL service	Attacker shall be able to request resources from MySQL service.
FR-062	HTTP response to attacker	Controller shall be able to send HTTP response to the attacker.
FR-063	SSH response to attacker	Controller shall be able to send SSH response to the attacker.
FR-064	MySQL response to attacker	Controller shall be able to send MySQL response to the attacker.
FR-065	Deploy VM	Controller shall be able to deploy VM in the cloud infrastructure.
FR-066	Start VM	Admin shall be able to start cloud VM.
FR-067	Stop VM	Admin shall be able to stop cloud VM.
FR-068	Restart VM	Admin shall be able to restart cloud VM in order to resume.
FR-069	Send packet by OpenVswitch	OpenVswitch shall be able to send packet to Controller.
FR-070	Send packet by Controller	Controller shall be able to send packets to OpenVswitch.
FR-071	Receive packet by OpenVswitch	OpenVswitch should be able to receive packets.
FR-072	Receive packet by controller	Controller shall be able to receive packets by OpenVswitch.
FR-073	Scan the network	Controller shall be able to scan the whole network using nmap
FR-074	Scan Data accumulation	Controller shall be able to send accumulate the data of the scan and make a report of it
FR-075	Sending scan data	Controller shall be able to send the scan data to dashboard

3.3.1 **FR-01: User registration**

Identifier	FR-01
Title	User registration
Requirement	The user shall be able to fill registration form to get registered.
Source	Supervisor

Rationale	Keep track of user activities and provide customized experience to secure application.
Business Rule	User must have a valid email address.
Dependencies	N/A
Priority	High

3.3.2 **FR-02: Login**

Identifier	FR-02
Title	Login
Requirement	Users must be able to use their username and password to login.
Source	Supervisor
Rationale	Application integrity and customized experience.
Business Rule	User must have an account.
Dependencies	FR-01
Priority	High

3.3.3 **FR-03: Forget Password**

Identifier	FR-03
Title	Forget Password
Requirement	In case if user forgot his password he shall be able to restore his password by clicking forget password.
Source	Supervisor
Rationale	To let user recover password.
Business Rule	N/A
Dependencies	FR-01
Priority	Low

3.3.4 **FR-04: Invalid credentials**

Identifier	FR-04
Title	Invalid Credentials
Requirement	The user shall not be permitted to login by providing invalid credentials.
Source	Supervisor
Rationale	To inform the user in case of invalid username and password.
Business Rule	N/A
Dependencies	FR-02
Priority	Medium

3.3.5 **FR-05: Logout**

Identifier	FR-05
Title	Logout
Requirement	User shall be able to logout from the account.
Source	Supervisor
Rationale	Let users to logout and go offline completely.
Business Rule	User must be logged in.
Dependencies	FR-02
Priority	High

3.3.6 **FR-06: Display profile**

Identifier	FR-06
Title	Display profile
Requirement	User shall be able to view their profile.
Source	Supervisor
Rationale	Allow users to view their private data.
Business Rule	N/A
Dependencies	FR-02
Priority	Low

3.3.7 **FR-07: Edit profile**

Identifier	FR-07
Title	Edit profile
Requirement	User shall be able to edit their profile information.
Source	Supervisor
Rationale	User may need to update their personal data.
Business Rule	N/A
Dependencies	FR-01
Priority	Medium

3.3.8 **FR-08: View user profile**

Identifier	FR-08
Title	View user profile
Requirement	Admin shall be able to view the profiles of other users.
Source	Supervisor
Rationale	Allow admin to view the profile data of other users
Business Rule	Admin must have to select a profile to view.
Dependencies	FR-02

Priority	Low

3.3.9 **FR-09: Show confirmation dialog**

Identifier	FR-09
Title	Show confirmation dialog.
Requirement	Confirmation dialog shall ask user to conduct any critical task or cancel it.
Source	Supervisor
Rationale	Obtain user approval to conduct or cancel operation.
Business Rule	N/A
Dependencies	N/A
Priority	Low

3.3.10 **FR-10: Show error dialog**

Identifier	FR-10
Title	Show error dialog.
Requirement	System should display error dialog if there is something incorrect in the implementation or if there is any unwanted circumstances.
Source	Supervisor
Rationale	Alert user of any possible errors.
Business Rule	N/A
Dependencies	N/A
Priority	Medium

3.3.11 **FR-11: Show Dashboard**

Identifier	FR-11
Title	Show Dashboard
Requirement	Dashboards shows the graphical representation of data and help us to easily visualize huge amount of data and provide us less but accurate information
Source	Supervisor
Rationale	It provides a quick overview on attacker's activity and provide detailed information about the threat intelligence generated by our system.
Business Rule	Data must be available in dashboard.
Dependencies	FR-02
Priority	Medium

3.3.12 **FR-12: View attacker activity**

Identifier	FR-12
Title	View attacker activity
Requirement	Admin shall be able to view the attacker's activity.

Source	Supervisor
Rationale	When an intruder is interacting with the projected services his activities should be viewable to admin.
Business Rule	N/A
Dependencies	FR-02
Priority	High

3.3.13 **FR-13: Installing openvpn script**

Identifier	FR-13
Title	Installing openvpn script
Requirement	Controller shall be able to install the openvpn script on ONET machine.
Source	Supervisor
Rationale	A network needs to be installed to have in-between communication.
Business Rule	Network is compulsory to have a better way of communication.
Dependencies	FR-02,FR-16
Priority	High

3.3.14 **FR-14: Running openvpn script**

Identifier	FR-14
Title	Running openvpn script
Requirement	Controller shall be able to run the openvpn script to install the tunnel.
Source	Supervisor
Rationale	The tunnel needs to be installed to have a better way of communication.
Business Rule	N/A
Dependencies	FR-02
Priority	High

3.3.15 **FR-15: Creating tunnel**

Identifier	FR-15
Title	Creating tunnel
Requirement	Controller shall be able to create an openvpn tunnel
Source	Supervisor
Rationale	A tunnel is necessary to transfer data from source to destination
Business Rule	N/A
Dependencies	FR-02,FR-16
Priority	High

3.3.16 **FR-16: Monitor attacker activity**

Identifier	FR-16
Title	Monitor attacker activity
Requirement	Controller shall be able to monitor attacker activity.
Source	Supervisor
Rationale	When attacker try to infiltrate into network we should be able to monitor attacker techniques, tactics and procedures.
Business Rule	N/A
Dependencies	FR-02
Priority	High

3.3.17 **FR-17: Create Service**

Identifier	FR-17
Title	Create Service
Requirement	Admin shall be able to create different services.
Source	Supervisor
Rationale	To initiate service of his own choice admin will create the service as per his need.
Business Rule	A service must be deployed before creation.
Dependencies	FR-02
Priority	High

3.3.18 **FR-18: Start Service**

Identifier	FR-18
Title	Start Service
Requirement	Admin shall be able to up the service within the network.
Source	Supervisor
Rationale	To let the user to use the service.
Business Rule	Internet connection is required.
Dependencies	FR-02,FR-17
Priority	High

3.3.19 **FR-19: End Service**

Identifier	FR-19
Title	End Service
Requirement	Admin shall be able to down the service from the network.
Source	Supervisor
Rationale	To make the service unavailable to use.
Business Rule	Internet connection is required.
Dependencies	FR-02,FR-18
Priority	High

3.3.20 **FR-20: Update Service**

Identifier	FR-20
Title	Update Service
Requirement	Admin shall be able to update the network configuration of deployed services.
Source	Supervisor
Rationale	For any modification in service admin will update it as per need.
Business Rule	Internet connection is required.
Dependencies	FR-02,FR-18,FR-56,FR-57,FR-58
Priority	High

3.3.21 **FR-21: Delete Service**

Identifier	FR-21
Title	Delete Service
Requirement	Admin shall be able to delete service from the network.
Source	Supervisor
Rationale	When a service is no longer required it should be deleted by the admin.
Business Rule	Service must be available.
Dependencies	FR-02,FR-18,FR-56,FR-57,FR-58
Priority	High

3.3.22 **FR-22: Generate Alert**

Identifier	FR-22
Title	Generate Alert
Requirement	System should be able to generate an alert when an intruder try to interact with one of our projected services.
Source	Supervisor
Rationale	Alert is generated whenever an intruder tries to interact with projected services.
Business Rule	Alert will be generated when an intruder tries to interact with projected services.
Dependencies	FR-02
Priority	High

3.3.23 **FR-23: Send Alert**

Identifier	FR-23
Title	Send Alert
Requirement	System shall be able to send an alert to admin when an intruder breaches.
Source	Supervisor
Rationale	When an alert is generated it should be sent to admin by the system.
Business Rule	N/A

Dependencies	FR-02,FR-22
Priority	High

3.3.24 **FR-24: View Alert**

Identifier	FR-24
Title	View Alert
Requirement	Admin shall be able to view an alert generated by the system.
Source	Supervisor
Rationale	Admin shall be able to view alert details.
Business Rule	N/A
Dependencies	FR-02,FR-22,FR-23
Priority	High

3.3.25 **FR-25: Delete Alert**

Identifier	FR-25
Title	Delete Alert
Requirement	Admin shall be able to delete alert generated by the system
Source	Supervisor
Rationale	Admin can delete unnecessary or already seen alerts.
Business Rule	N/A.
Dependencies	FR-02,FR-22,FR-23
Priority	High

3.3.26 **FR-26: Make Directories**

Identifier	FR-26
Title	Make Directories
Requirement	System should be able to make directories in ONET and DNET machines
Source	Supervisor
Rationale	In order to make the room for desired files
Business Rule	N/A
Dependencies	FR-02
Priority	High

3.3.27 **FR-27: Vpn client file creation**

Identifier	FR-27
Title	Vpn client file creation
Requirement	System should be able to create client vpn files that includes network information

Source	Supervisor
Rationale	Different client vpn files are created on runtime by controller in order to have a tunnel
Business Rule	N/A
Dependencies	FR-02,FR-26
Priority	High

3.3.28 **FR-28: Sending vpn files**

Identifier	FR-28
Title	Sending vpn files
Requirement	System should be able to transfer the vpn files from server to desired clients.
Source	Supervisor
Rationale	When vpn client is created that needs to be transfer to client from server
Business Rule	N/A
Dependencies	FR-02,FR-26,FR-27
Priority	High

3.3.29 **FR-29: Add user**

Identifier	FR-29
Title	Add user
Requirement	Admin shall be able to add a new user.
Source	Supervisor.
Rationale	A new user should be added to the system by admin with all permissions granted.
Business Rule	Credentials should be valid.
Dependencies	FR-02
Priority	Medium

3.3.30 **FR-30: Assign role**

Identifier	FR-30
Title	Assign role
Requirement	Admin shall be able to assign role to users.
Source	Supervisor
Rationale	Admin can assign specific roles to users.
Business Rule	User should be in system..
Dependencies	FR-02,FR-29
Priority	High

3.3.31 **FR-31: Remove role**

Identifier	FR-31
Title	Remove role

Requirement	Admin shall be able to remove role of a user.
Source	Supervisor
Rationale	When role of a user is over it should be terminated by admin.
Business Rule	N/A
Dependencies	FR-02,FR-29,FR-30
Priority	Low

3.3.32 **FR-32: Update role**

Identifier	FR-32
Title	Update role
Requirement	Admin shall be able to update the role of a user.
Source	Supervisor
Rationale	When we need to modify the role of a user it should be done by an admin.
Business Rule	Role must be assigned.
Dependencies	FR-02,FR-29,FR-30
Priority	Low

3.3.33 **FR-33: Edit IP address**

Identifier	FR-33
Title	Edit IP address
Requirement	User shall be able to edit IP address to deploy VM.
Source	Supervisor
Rationale	In case of any modification user should be free to edit IP address within the same subnet.
Business Rule	Require internet connection
Dependencies	FR-02
Priority	Medium

3.3.34 **FR-34: Inspect IP address**

Identifier	FR-34
Title	IP address inspection
Requirement	Controller shall be able to inspect IP addresses of each incoming and outgoing packets.
Source	Supervisor
Rationale	Packet should be inspected in order to keep track of an attack..
Business Rule	N/A
Dependencies	FR-02
Priority	High

3.3.35 **FR-35: Inspect switch port**

Identifier	FR-35
Title	Switch port inspection
Requirement	Controller shall be able to inspect arriving packets switch ports.
Source	Supervisor
Rationale	Switch ports should be inspected in order to modify the switch port.
Business Rule	N/A
Dependencies	FR-02
Priority	High

3.3.36 **FR-36: Inspect Vxlan id**

Identifier	FR-36
Title	Vxlan id inspection
Requirement	Controller shall be able to inspect Vxlan id of incoming packets.
Source	Supervisor
Rationale	Vxlan id's needs to be inspected in order to transfer traffic to similar Vxlan.
Business Rule	N/A
Dependencies	FR-02,FR-40
Priority	High

3.3.37 **FR-37: Modify IP address**

Identifier	FR-37
Title	Modify IP address
Requirement	Controller shall be able to modify IP address of incoming and outgoing packets.
Source	Supervisor
Rationale	Traffic will be rerouted to the cloud infrastructure.
Business Rule	IP address must be available.
Dependencies	FR-02,FR-34
Priority	High

3.3.38 **FR-38: Modify destination port**

Identifier	FR-38
Title	Destination port modification
Requirement	Controller shall be able to modify the destination switch port of incoming and outgoing traffic.
Source	Supervisor
Rationale	Traffic will be rerouted to the cloud infrastructure.
Business Rule	Port must be available.
Dependencies	FR-02,FR-35,FR-40
Priority	High

3.3.39 **FR-39: Modify MAC address**

Identifier	FR-39
Title	Modify MAC address
Requirement	Controller shall be able to modify MAC address of incoming and outgoing traffic.
Source	Supervisor
Rationale	Traffic will be rerouted to the cloud infrastructure.
Business Rule	MAC address must be available.
Dependencies	FR-02,FR-40
Priority	High

3.3.40 **FR-40: Capture Packet**

Identifier	FR-40
Title	Capture packet
Requirement	Controller shall be able to capture incoming and outgoing traffic
Source	Supervisor
Rationale	Packets are captured in order to get valuable information.
Business Rule	N/A
Dependencies	FR-02
Priority	High

3.3.41 **FR-41: Analyze packet**

Identifier	FR- 41
Title	Analyze packet
Requirement	Controller shall be to analyze the requested services
Source	Supervisor
Rationale	Packet analyzing is carried out to get some services information from it.
Business Rule	Packets must be captured.
Dependencies	FR-02,FR-40
Priority	High

3.3.42 **FR-42: View graph**

Identifier	FR-42
Title	View graph
Requirement	Admin shall be able to view graph.
Source	Supervisor
Rationale	Viewing Graph provides a huge amount of data to admin in an organized manner through dashboard to analyze and monitor the behavior of attacker.
Business Rule	Data must be available.
Dependencies	FR-02

Priority	High

3.3.43 **FR-43: Edit graph setting**

Identifier	FR-43
Title	Edit graph setting
Requirement	Admin shall be able to edit graph setting.
Source	Supervisor
Rationale	In case of any modification admin should be able to edit graph setting.
Business Rule	N/A
Dependencies	FR-02
Priority	Medium

3.3.44 **FR-44: Viewing chart**

Identifier	FR-44
Title	Viewing Chart
Requirement	Admin shall be able to view charts.
Source	Supervisor
Rationale	Viewing Charts provides a huge amount of data to admin in an organized manner through dashboard to analyze and monitor the behavior of attacker.
Business Rule	Data must be available.
Dependencies	FR-02
Priority	High

3.3.45 **FR-45: Search log**

Identifier	FR-45
Title	Search log
Requirement	Admin shall be able to search specific logs from elastic search.
Source	Supervisor
Rationale	It enables us to make reliable search and analyze the data.
Business Rule	Logs must be captured.
Dependencies	FR-02
Priority	High

3.3.46 **FR-46: Inspect log**

Identifier	FR-46
Title	Inspect log
Requirement	Admin shall be able to inspect logs from the elastic search.
Source	Supervisor
Rationale	In order to maintain logs it should be inspected.

Business Rule	N/A
Dependencies	FR-02,FR-47
Priority	Medium

3.3.47 **FR-47: Capture log**

Identifier	FR-47
Titlen	Capture log
Requirement	Controller shall be able to capture logs of different services.
Source	Supervisor
Rationale	When attack happens the controller begins to capture logs in an entire system and will send it to admin to perform operations on it.
Business Rule	N/A
Dependencies	FR-18
Priority	High

3.3.48 **FR-48: Filter log**

Identifier	FR-48
Title	Filter log
Requirement	Admin shall have the ability to apply filter on logs.
Source	Supervisor
Rationale	Admin will filter captured logs according to his need.
Business Rule	Logs must be available..
Dependencies	FR-02,FR-47
Priority	Medium

3.3.49 **FR-49: Analyze log**

Identifier	FR-49
Title	Analyze log
Requirement	Admin shall be able to analyze the captured logs.
Source	Supervisor
Rationale	Admin should be able to analyze the captured logs to understand the intentions of the attacker.
Business Rule	Logs must be maintained.
Dependencies	FR-02,FR-47
Priority	High

3.3.50 **FR-50: Store log**

Identifier	FR-50
Title	Store log
Requirement	MongoDB shall be used to store capture logs.

Source	Supervisor
Rationale	Logs are stored in MongoDB in order to retrieve them according to need.
Business Rule	N/A
Dependencies	FR-02,FR-47
Priority	High

3.3.51 **FR-51: View projected services health**

Identifier	FR-51
Title	View projected services health
Requirement	Admin shall be able to view health of projected services.
Source	Supervisor
Rationale	Admin will view the projected services health to ensure the availability of the projected services.
Business Rule	N/A
Dependencies	FR-02
Priority	High

3.3.52 **FR-52: View cloud VM's health**

Identifier	FR-52
Title	View cloud VM's health
Requirement	Admin shall be able to view health of cloud VM's.
Source	Supervisor
Rationale	Admin will view the projected services health to ensure the availability of the cloud VM's..
Business Rule	N/A
Dependencies	FR-02
Priority	High

3.3.53 **FR-53: View routing table health**

Identifier	FR-53
Title	View routing table health
Requirement	Admin shall be able to view flows of routing tables.
Source	Supervisor
Rationale	To make sure everything is working well admin will view the routing tables health.
Business Rule	N/A
Dependencies	FR-02
Priority	High

3.3.54 **FR-54: Setting unique name for vpn clients**

Identifier	FR-54
Title	Setting unique name for vpn clients
Requirement	Controller shall be able to give unique naming scheme to each vpn clients
Source	Supervisor
Rationale	Whenever a client vpn is needed, controller will generate new vpn clients
Business Rule	N/A.
Dependencies	FR-02
Priority	High

3.3.55 **FR-55: Unique IP address for each vpn client**

Identifier	FR-55
Title	Unique IP address for each vpn client
Requirement	Controller shall be able to assign unique ip addresses to each vpn clients.
Source	Supervisor
Rationale	Whenever a client needs vpn tunnel, controller will generate it with unique IP address
Business Rule	N/A
Dependencies	FR-02,FR-54
Priority	High

3.3.56 **FR-56: Deploy HTTP service**

Identifier	FR-56
Title	Deploy HTTP service
Requirement	Controller shall be able to deploy HTTP service across the network.
Source	Supervisor
Rationale	Deploying low interaction decoys as HTTP to deceive the intruder.
Business Rule	Require internet connection.
Dependencies	FR-02,FR-18
Priority	High

3.3.57 **FR-57: Deploy SSH service**

Identifier	FR-57
Title	Deploy SSH service
Requirement	Controller shall be able to deploy SSH service across the network.
Source	Supervisor
Rationale	Deploying low interaction decoys as SSH to deceive the intruder.
Business Rule	Require internet connection.
Dependencies	FR-02,FR-18
Priority	High

3.3.58 **FR-58: Deploy MySQL service**

Identifier	FR-58
Title	Deploy MySQL service
Requirement	Controller shall be able to deploy MySQL service.
Source	Supervisor
Rationale	Deploying low interaction decoys as MySQL to deceive the intruder.
Business Rule	Require internet connection.
Dependencies	FR-02,FR-18
Priority	High

3.3.59 **FR-59: Attacker request to HTTP service**

Identifier	FR-59
Title	Attacker request to HTTP service
Requirement	Attacker shall be able to request resources from HTTP service.
Source	Supervisor
Rationale	Attacker request to the shadow network to acquire resources from HTTP service.
Business Rule	Service must be available.
Dependencies	FR-18
Priority	High

3.3.60 **FR-60: Attacker request to SSH service**

Identifier	FR-60
Title	Attacker request to SSH request
Requirement	Attacker shall be able to request resources from SSH service.
Source	Supervisor
Rationale	Attacker request to the shadow network to acquire resources from SSH service.
Business Rule	Service must be available.
Dependencies	FR-18
Priority	High

3.3.61 **FR-61: Attacker request to MySQL service**

Identifier	FR-61
Title	Attacker request to MySQL service
Requirement	Attacker shall be able to request resources from MySQL service.
Source	Supervisor
Rationale	Attacker request to the shadow network to acquire resources from MySQL service.
Business Rule	Service must be available.
Dependencies	FR-18
Priority	High

3.3.62 **FR-62: HTTP response to attacker.**

Identifier	FR-62
Title	HTTP response to attacker
Requirement	Controller shall be able to send HTTP response to the attacker.
Source	Supervisor
Rationale	When the attacker tries to infiltrate the HTTP service, he will get a response from deception system.
Business Rule	Attacker connection with our service.
Dependencies	FR-18, FR-59
Priority	High

3.3.63 **FR-63: SSH response to attacker.**

Identifier	FR-63
Title	SSH response to attacker
Requirement	Controller shall be able to send SSH response to the attacker.
Source	Supervisor
Rationale	When the attacker tries to infiltrate the SSH service he will get a response from deception system.
Business Rule	Attacker connection with our service.
Dependencies	FR-18, FR-60
Priority	High

3.3.64 **FR-64: MySQL response to attacker.**

Identifier	FR-64
Title	MySQL response to attacker
Requirement	Controller shall be able to send MySQL response to the attacker.
Source	Supervisor
Rationale	When the attacker tries to infiltrate the MySQL service he will get a response from deception system.
Business Rule	Attacker connection with our service.
Dependencies	FR-18,FR-61
Priority	High

3.3.65 **FR-65: Deploy VM**

Identifier	FR-65
Title	Deploy VM
Requirement	Controller shall be able to deploy VM in the cloud infrastructure.
Source	Supervisor
Rationale	VM's should be deployed as per organization need.
Business Rule	Require internet connection.

Dependencies	N/A
Priority	High

3.3.66 **FR-66: Start VM**

Identifier	FR-66
Title	Start VM
Requirement	Admin shall be able to start cloud VM.
Source	Supervisor
Rationale	To initiate a specific VM admin will visit deployment page to start VM.
Business Rule	VM availability.
Dependencies	FR-02
Priority	High

3.3.67 **FR-67: Stop VM**

Identifier	FR-67
Title	Stop VM
Requirement	Admin shall be able to stop cloud VM.
Source	Supervisor
Rationale	To stop a specific VM admin will visit VM deployment page to stop VM.
Business Rule	VM availability.
Dependencies	FR-02
Priority	High

3.3.68 **FR-68: Restart VM**

Identifier	FR-68
Title	Restart VM
Requirement	Admin shall be able to restart cloud VM in order to resume.
Source	Supervisor
Rationale	To restart a specific VM admin will visit VM deployment page to restart VM.
Business Rule	VM availability.
Dependencies	FR-02
Priority	High

3.3.69 **FR-69: Send packet by OpenvSwitch**

Identifier	FR-69
Title	Send packet by OpenvSwitch
Requirement	OpenvSwitch shall be able to send packet to Controller.
Source	Supervisor
Rationale	When packets are received by OpenvSwitch he will be unaware of the packets for understanding the packets will be forwarded to Controller.

Business Rule	OpenvSwitch must be installed.
Dependencies	FR-40
Priority	High

3.3.70 **FR-70: Send packets by Controller**

Identifier	FR-70
Title	Send packets by controller
Requirement	Controller shall be able to send packets to OpenVswitch.
Source	Supervisor
Rationale	After analyzing packets it should be sent to OpenVswitch.
Business Rule	Stable connection between switches and controller.
Dependencies	FR-69
Priority	High

3.3.71 **FR-71: Receive packets by OpenVswitch**

Identifier	FR-71
Title	Receive packets by OpenVswitch
Requirement	OpenVswitch should be able to receive packets.
Source	Supervisor
Rationale	Packets forwarded by controller after analyzing should be received by OpenVswitch to proceed further.
Business Rule	OpenvSwitch must be installed.
Dependencies	FR-70
Priority	High

3.3.72 **FR-72: Receive packets by controller**

Identifier	FR-72
Title	Receive packets by controller
Requirement	Controller shall be able to receive packets by OpenVswitch.
Source	Supervisor
Rationale	When packets are forwarded by OpenVswitch it should be received by controller.
Business Rule	Stable connection between switches and controller.
Dependencies	FR-02
Priority	High

3.3.73 **FR-73: Scan the network**

Identifier	FR-73
Title	Scan the network
Requirement	Controller shall be able to scan the whole network using nmap
Source	Supervisor

Rationale	The controller have to recognize the potential services
Business Rule	Nmap should be installed and properly configured
Dependencies	N/A
Priority	High

3.3.74 **FR-74: Scan Data accumulation**

Identifier	FR-74
Title	Scan Data accumulation
Requirement	Controller shall be able to send accumulate the data of the scan and make a report of it
Source	Supervisor
Rationale	The controller have to accumulate date in order to have better understanding
Business Rule	Nmap should be installed and properly configured
Dependencies	FR-73
Priority	High

3.3.75 **FR-75 Scan Data accumulation**

Identifier	FR-75
Title	Sending scan data
Requirement	Controller shall be able to send the scan data to dashboard
Source	Supervisor
Rationale	The controller have to send the data to user to view it
Business Rule	Nmap should be installed and properly configured
Dependencies	FR-73
Priority	High

3.4 Non-Functional Requirements

Following are the non-functional Requirements of our system:

NFR ID	Category	Name	Description
UR-1	Usability	Efficiency	Performance shall be good.
UR-2		Operability	System shall be in a safe and reliable functioning Condition
UR-3		Admin/User manual	A Admin/User guide for the Admin/User to understand system.
PR-1	Performance	Web Response Time	Time taking to connect to the internet
PR-2		System Response Time	Time taking to interact with Admin/User
RR-1	Reliability	Availability	Availability at Peak time.
RR-2		Maintenance	Easy to maintain throughout the life.

SR-1	Supportability	System Support	Shall be supportable at the time of system problem
SR-1		Supported Platform	Shall support the required platform easily.

Table : Non-Functional Requirements

3.4.1 Usability:

3.4.1.1 Efficiency

Identifier	UR-1
Title	Efficiency
Requirement	The system shall be efficient enough to perform a task without a delay.

Table 1: UR-1 efficiency

3.4.1.2 Operability

Identifier	UR-2
Title	Operability
Requirement	The system shall be in good functioning condition. Incase of any fault, it should notify the Admin/User about a certain error.

Table 2: UR-2 operability

3.4.1.3 Admin/User Manual:

Identifier	UR-3
Title	Admin/User Manual
Requirement	A Admin/User guide shall be provided in the form of “how to use” button. It should display all the important stuff that can help the Admin/User in running that system.

Table 3: UR-3 user manual

3.4.2 Performance:

3.4.2.1 Web Response Time

Identifier	PR-1
Title	Web Response Time
Requirement	The response time of connecting to the internet of the system shall be quick.

Table 4: PR-1 web response time

3.4.2.2 System Response Time

Identifier	PR-1
Title	System Response Time
Requirement	The system response time to some task performed by the Admin/User shall be quick.

Table 5: PR-2 system response time

3.4.3 Reliability:

3.4.3.1 Availability:

Identifier	RR-1
Title	Availability
Requirement	The system shall be available all the time. The system shall not be down if it is using at its peak time during organization working hours.

Table 6: RR-1 availability

3.4.3.2 Maintenance:

Identifier	RR-2
Title	Maintenance
Requirement	The system shall be easily maintained. If a fault occurs in the system that shall be easily removed from the system and it should not be complicated.

Table 7: RR-2 maintenance

3.4.4 Supportability:

3.4.4.1 Supported Platform:

Identifier	SR-1
Title	Supported Platform
Requirement	The system shall work in all the required environment and shall work fine on required supported platforms like windows.

Table 8: SR-2 supportability

4. Design and Architecture

The following parts of Software Design Description (SDD) report should be included in this chapter.

4.1 System Architecture

4.1.1 Multi-tier Architecture

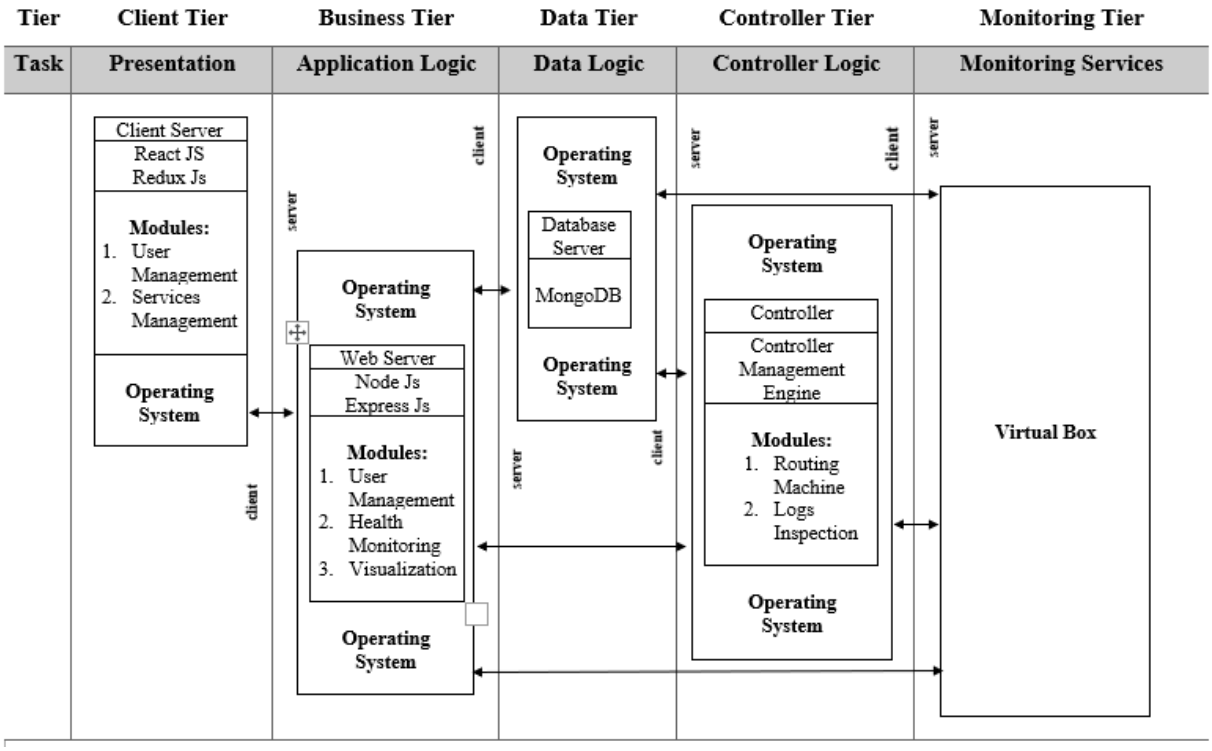


Figure 4.1 Architecture Diagram

4.1.1.1 Multi-tier Architecture Description

A *Multi-Tier Architecture* is a software architecture in which different software components, organized in tiers (layers), provide dedicated functionality. Basically, it is n-tier architecture which act as client-server architecture in which numbers of tiers can be used for different systems. We are using 5-tiers to explains our system architecture. First-tier is a "client-tier" which is used for presentation of our system and represents the system interface functionalities. Second tier is a "business-tier" whose task is the application logic. It acts as a web server which contains the complete logics and explanation of a system. Third tier is the "data tier" and explains the data logic. It acts as a data server and its main task is to manage the database of the system. Fourth tier is an "Controller tier" which explains the attack logic. It acts as a controller server.
Conceptually, a multi-tier architecture results from a repeated application of the client/server paradigm. A component in one of the tiers is client to the next lower tier and at the same time acts as server to the next higher tier.

4.2 Data Representation

```
const mongoose = require( 'mongoose' )
mongoose.set('useCreateIndex', true);
const Schema = mongoose.Schema

// Create Schema
const UserSchema = new Schema({
  username: {
    type: String,
  },

  email: {
    type: String,
    required: true,
    unique:true,
    // minlength: 5,
    // maxlength: 255,
  },
  password: {
    type: String,
    required: true,

  },

  avatar: {
    type: String,
  },
  date: {
    type: Date,
    default: Date.now
  }
})
module.exports = User = mongoose.model('users', UserSchema)
```

Figure 4.2 Schema - 01 Admin

```
const mongoose = require('mongoose')
mongoose.set('useCreateIndex', true);
const Schema = mongoose.Schema

// Create Schema
const ServiceSchema = new Schema({
  IPaddress: {
    type: String,
  },

  account: {
    type: String,
    required: true,
    // minlength: 5,
    // maxlength: 255,
  },
  password: {
    type: String,
    required: true,
  },
  service:{
type: String,
required: true,
  },
  date: {
    type: Date,
    default: Date.now
  }
})

module.exports = Service = mongoose.model('services', ServiceSchema)
```

Figure 4.3 Schema - 02 VM deployment

models > JS Scanner.js > ScannerSchema > name

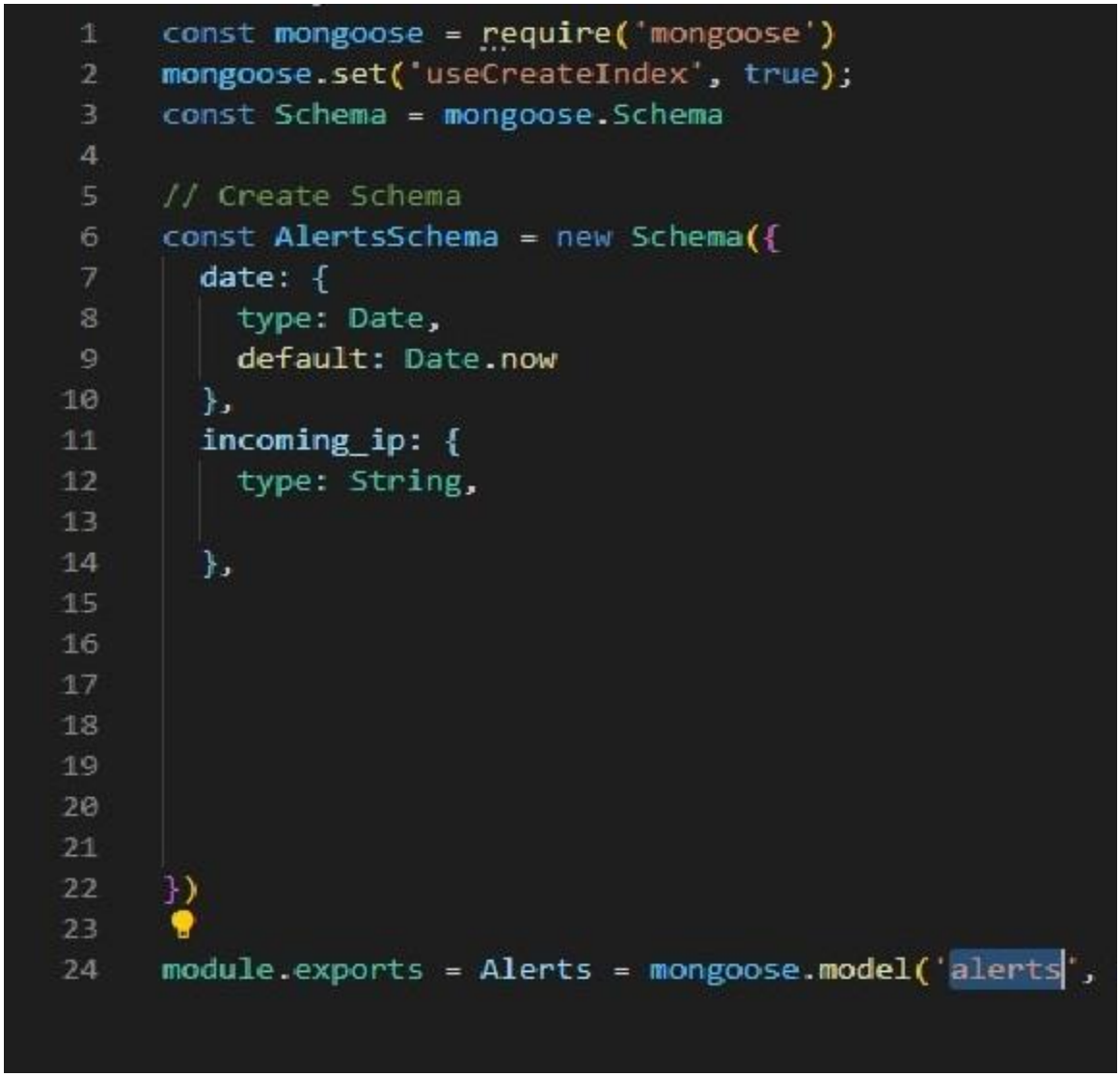
```
1   const mongoose = require('mongoose')
2   mongoose.set('useCreateIndex', true);
3   const Schema = mongoose.Schema
4
5   // Create Schema
6   const ScannerSchema = new Schema({
7     ip_address:{
8       type: mongoose.Schema.Types.String,
9     },
10    port: {
11      type: Number,
12
13    },
14    name: {
15      type: String,
16    },
17    state: {
18      type: String,
19    },
20    product: {
21      type: String,
22
23    },
24    version: {
25      type: String,
26    },
27    date: {
28      type: Date,
29      default: Date.now
30    }
31  })
32  module.exports = Scanner = mongoose.model('scanner', ScannerSchema)
```

Figure 4.4 Schema - 03 Scanner

models > JS SubManager.js > SubManagerSchema > email

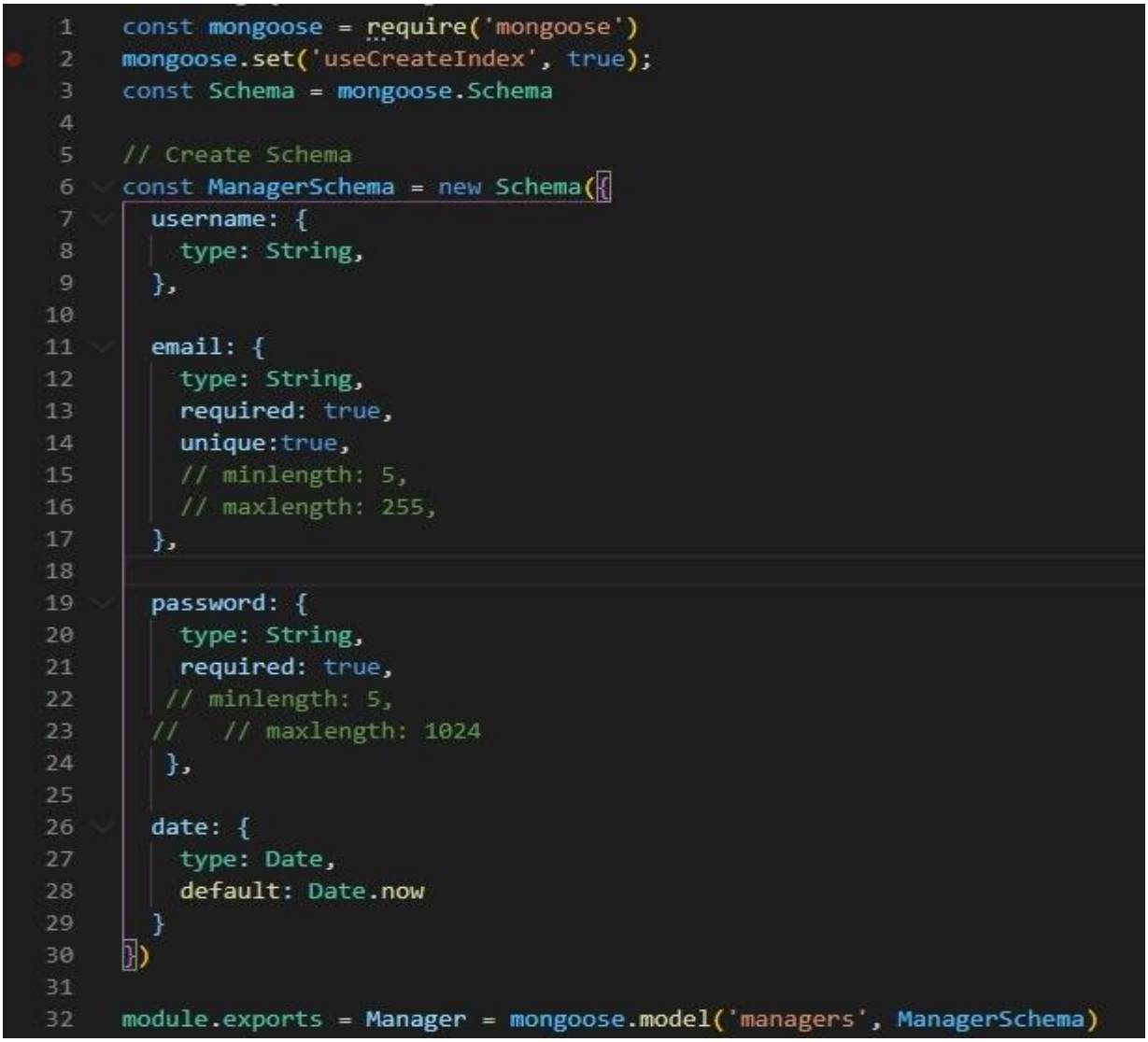
```
1   const mongoose = require('mongoose')
2   mongoose.set('useCreateIndex', true);
3   const Schema = mongoose.Schema
4
5   // Create Schema
6   const SubManagerSchema = new Schema({
7     username: {
8       type: String,
9     },
10
11    email: {
12      type: String,
13      required: true,
14      unique:true,
15
16    },
17    password: {
18      type: String,
19      required: true,
20
21    },
22
23    avatar: {
24      type: String,
25    },
26    date: {
27      type: Date,
28      default: Date.now
29    }
30  })
31
32  module.exports = SubManager = mongoose.model('submanagers', SubManagerSchema)
```

Figure 4.5 Schema - 04 SubManager



```
const mongoose = require('mongoose')
mongoose.set('useCreateIndex', true);
const Schema = mongoose.Schema

// Create Schema
const AlertsSchema = new Schema({
  date: {
    type: Date,
    default: Date.now
  },
  incoming_ip: {
    type: String,

  },



})
module.exports = Alerts = mongoose.model('alerts',
```

Figure 4.6 Schema - 05 Alerts



```
const mongoose = require('mongoose')
mongoose.set('useCreateIndex', true);
const Schema = mongoose.Schema

// Create Schema
const ManagerSchema = new Schema({
  username: {
    type: String,
  },

  email: {
    type: String,
    required: true,
    unique:true,
    // minlength: 5,
    // maxlength: 255,
  },

  password: {
    type: String,
    required: true,
   // minlength: 5,
  //   // maxlength: 1024
   },

  date: {
    type: Date,
    default: Date.now
  }
})

module.exports = Manager = mongoose.model('managers', ManagerSchema)
```

Figure 4.7 Schema - 06 Manager

```
const mongoose = require('mongoose')
mongoose.set('useCreateIndex', true);
const Schema = mongoose.Schema

// Create Schema
const RoleSchema = new Schema({
  user_id:{
    type: mongoose.Schema.Types.ObjectId,
    required: true,
    ref: 'users'
  },
  username: {
    type: String,
  },

  email: {
    type: String,
    required: true,
    unique:true,
    // minlength: 5,
    // maxlength: 255,
  },
  role: {
    type: String,
    required: true,
  },
  date: {
    type: Date,
    default: Date.now
  }
})
module.exports = Role = mongoose.model('roles', RoleSchema)
```

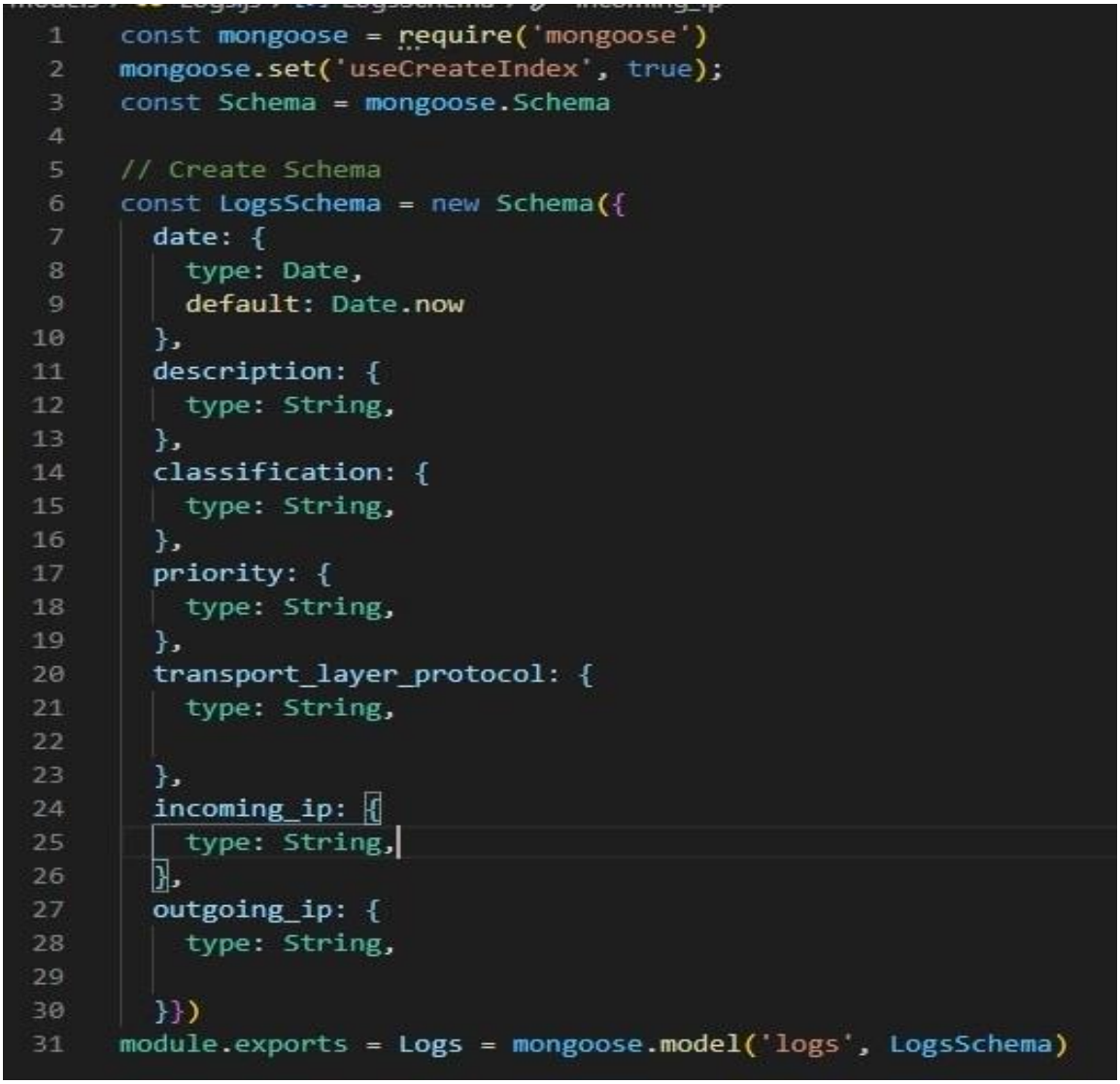
Figure 4.8 Schema - 07 Role

```
const mongoose = require('mongoose')
mongoose.set('useCreateIndex', true);
const Schema = mongoose.Schema
const NotificationSchema = new Schema({
  sender:{
    type: mongoose.Schema.Types.String,
    default: "System"
  },reciever_role:{
    type: mongoose.Schema.Types.String,
  },notification_id:{
    type: mongoose.Schema.Types.String,
    required: true
  }, broadcast:{
    type: mongoose.Schema.Types.Boolean,
    default: false
  }, reciever_email:{
    type: mongoose.Schema.Types.String,
  }, notification_type:{
    type: mongoose.Schema.Types.String,
    required: true
  }, message: {
    type: mongoose.Schema.Types.String,
    required: true
  },url:{
    type: mongoose.Schema.Types.String,
    default: ""}, readBy: [  {
    type: mongoose.Schema.Types.String
  }],  date: {
    type: Date,
    default: Date.now
  }})
module.exports = Notification = mongoose.model('notifications', NotificationSchema)
```

Figure 4.9 Schema - 08 Notification

```
const mongoose = require('mongoose')
mongoose.set('useCreateIndex', true);
const Schema = mongoose.Schema

// Create Schema
const DepartmentSchema = new Schema({
  IPaddress: {
    type: String,
    required: true,
  },

  account: {
    type: String,
    required: true,
    // minlength: 5,
    // maxlength: 255,
  },
  password: {
    type: String,
    required: true,
  },

  date: {
    type: Date,
    default: Date.now
  }
})

module.exports = Department = mongoose.model('department', DepartmentSchema)
```

Figure 4.10 Schema - 09 Department



```
const mongoose = require('mongoose')
mongoose.set('useCreateIndex', true);
const Schema = mongoose.Schema

// Create Schema
const LogsSchema = new Schema({
  date: {
    type: Date,
    default: Date.now
  },
  description: {
    type: String,
  },
  classification: {
    type: String,
  },
  priority: {
    type: String,
  },
  transport_layer_protocol: {
    type: String,

  },
  incoming_ip: {
    type: String,
  },
  outgoing_ip: {
    type: String,

  }})
module.exports = Logs = mongoose.model('logs', LogsSchema)
```

Figure 4.11 Schema - 10 Logs

4.3 Process Flow/Representation

4.3.1 Activity diagram 01: User Profile

(UC001-003)

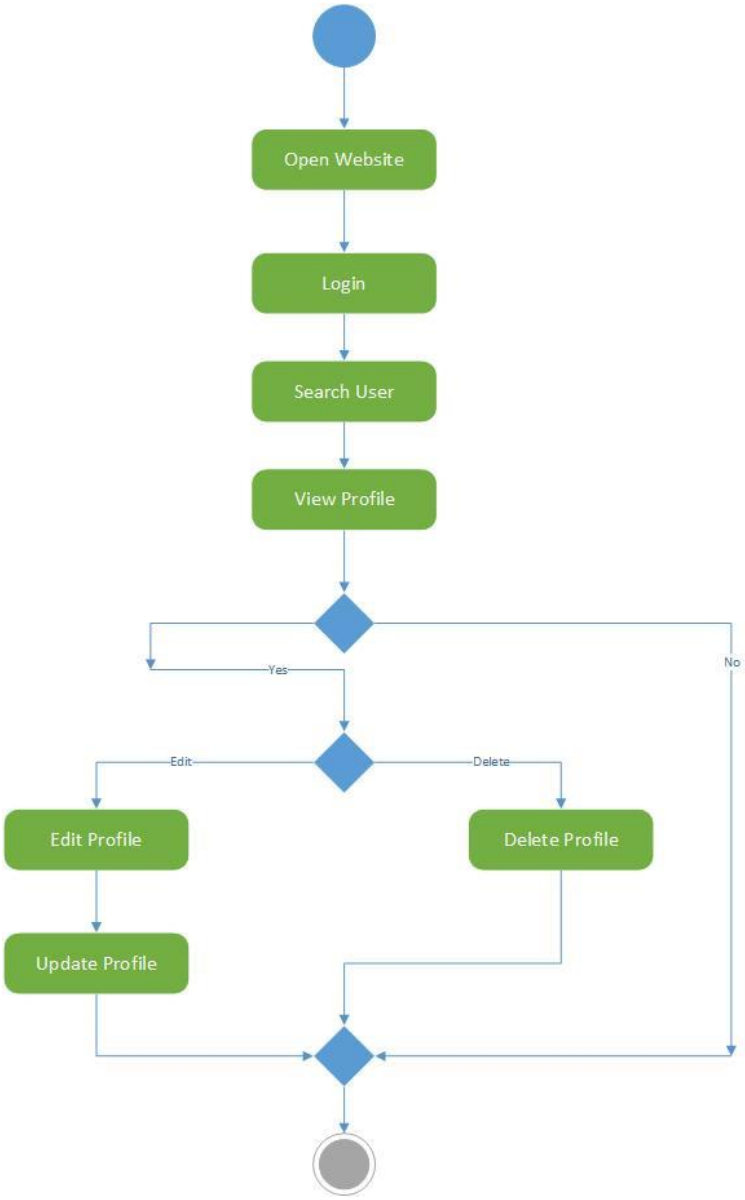


Figure 4.12 Activity Diagram – 1 User Profile

4.3.2 Activity Diagram 02: User Management

(UC036-038)

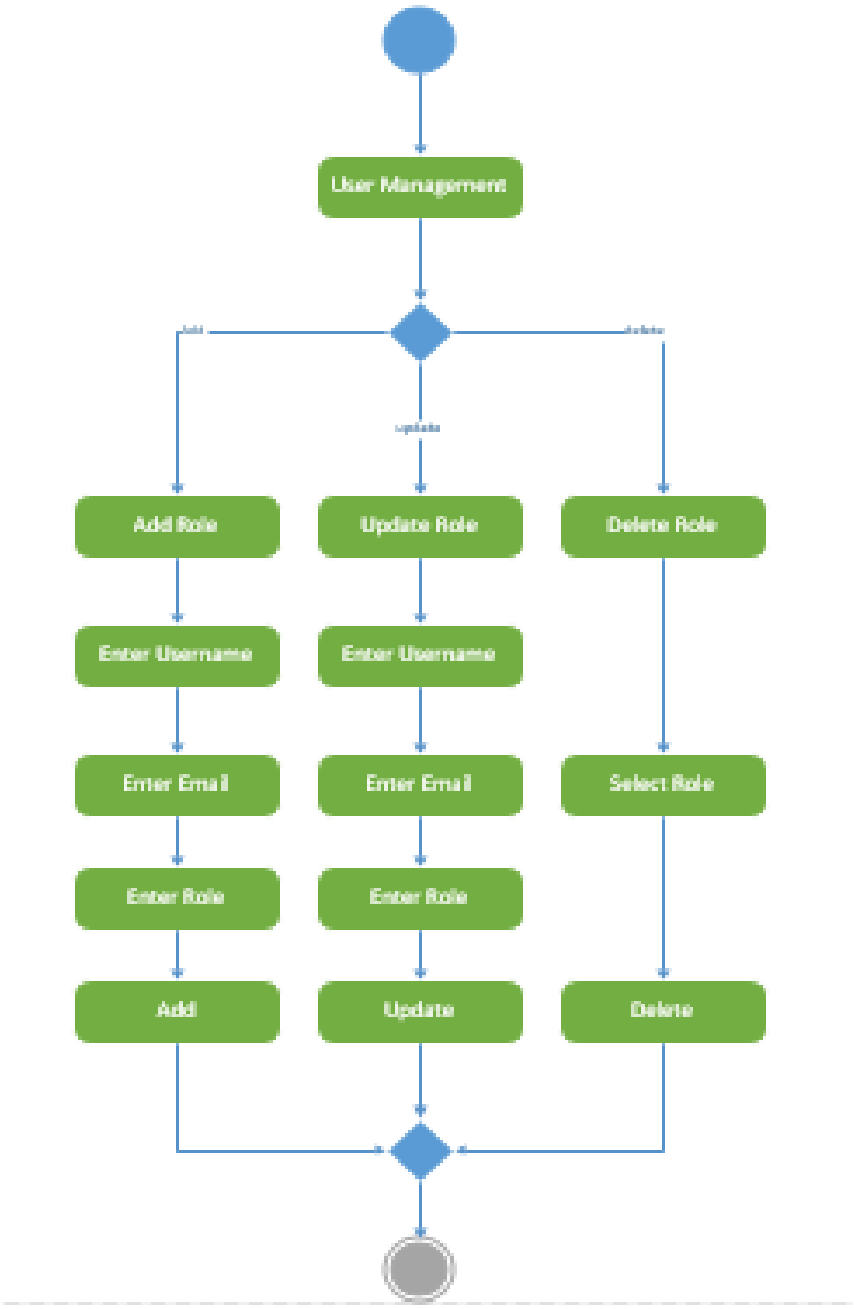


Figure 4.13 Activity Diagram - 2 User Management

4.3.3 Activity Diagram 03: Services Management

(UC004-006)

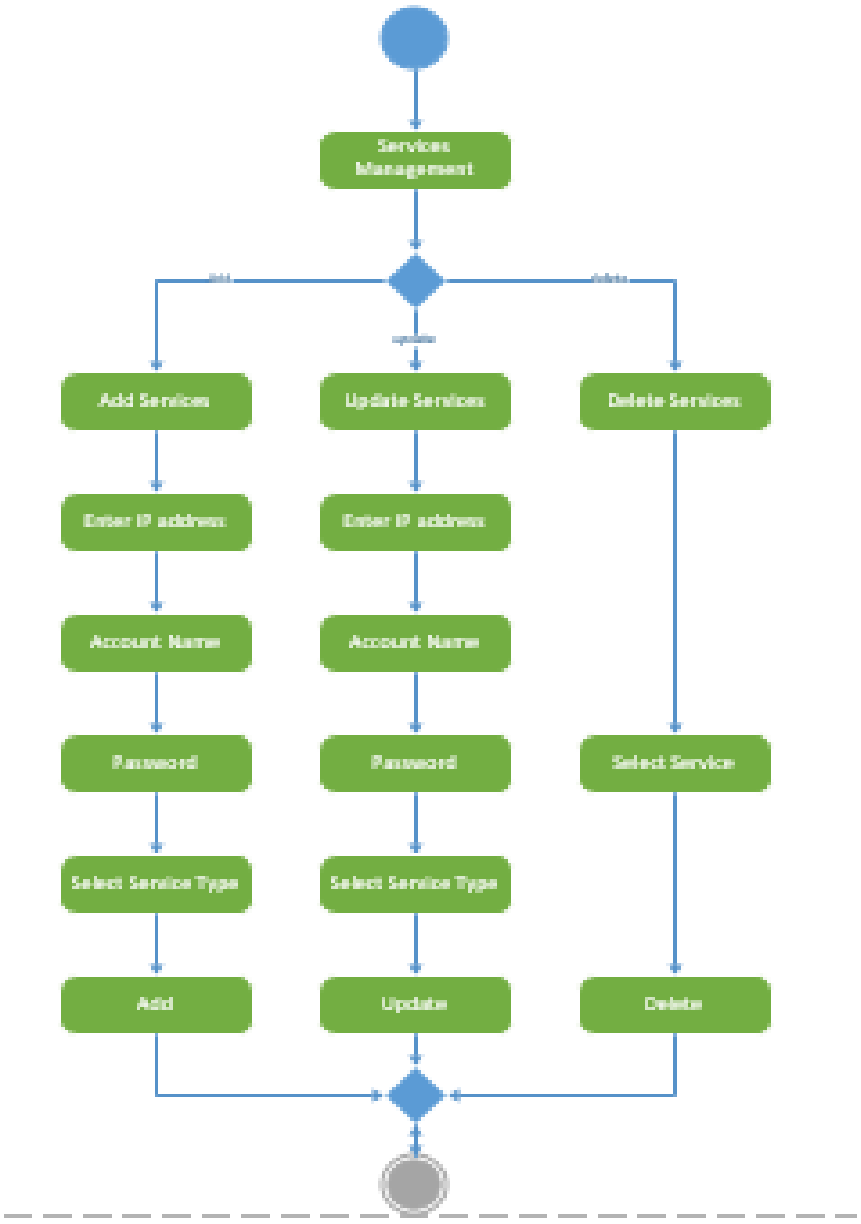


Figure 4.14 Activity Diagram - 3 Services Management

4.3.4 Activity Diagram 04 Filter Logs

(UC035)

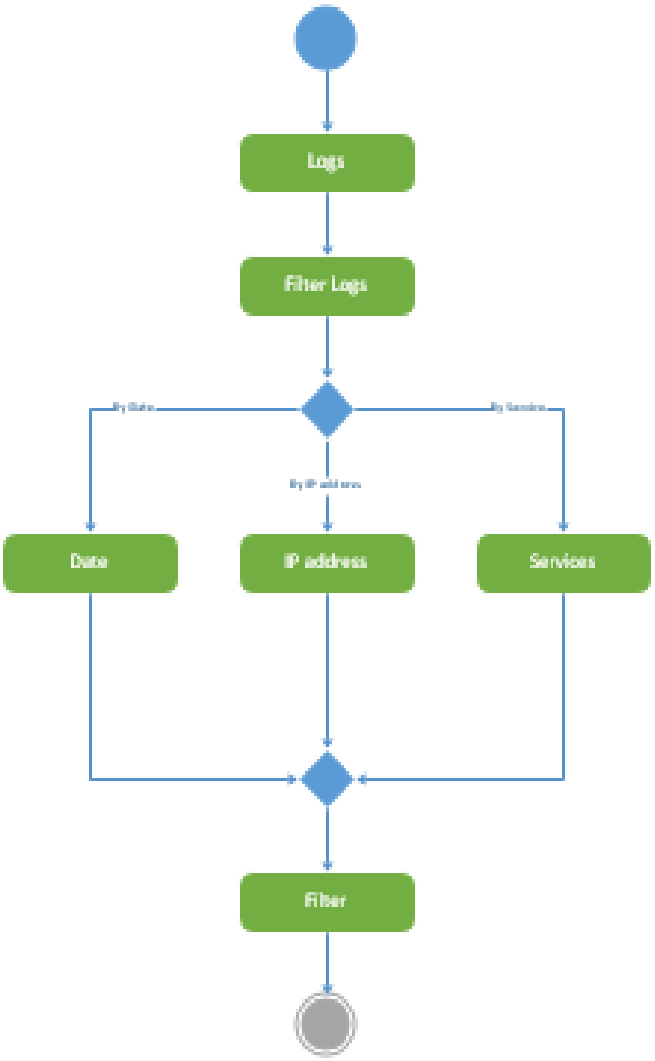


Figure 4.15 Activity Diagram - 4 Filter Logs

4.3.5 Activity Diagram 05: Monitor Services

(UC031)

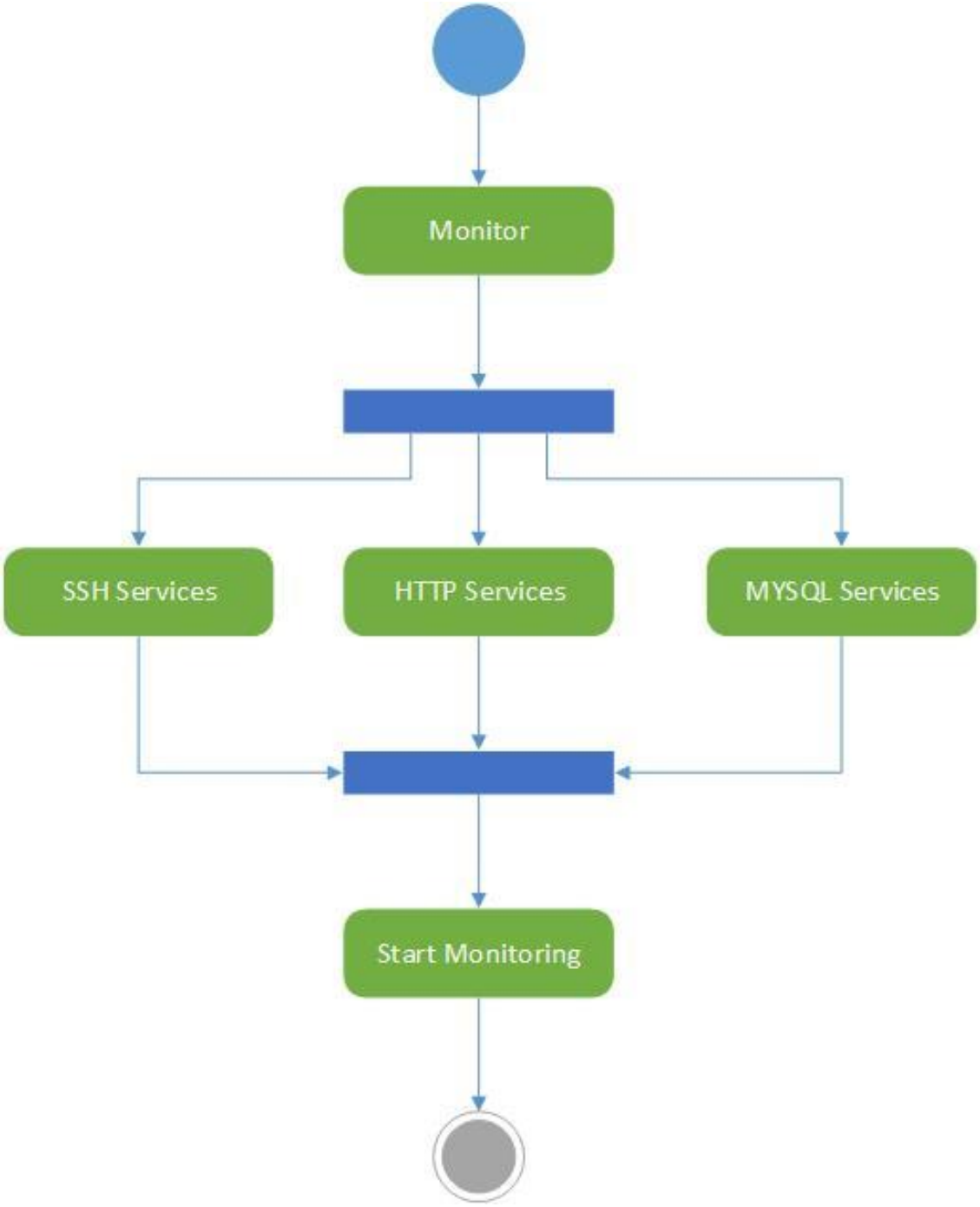


Figure 4.16 Activity Diagram - 5: Monitor Services

4.4 Class Diagram

4.4.1 Class Diagram 01: Frontend

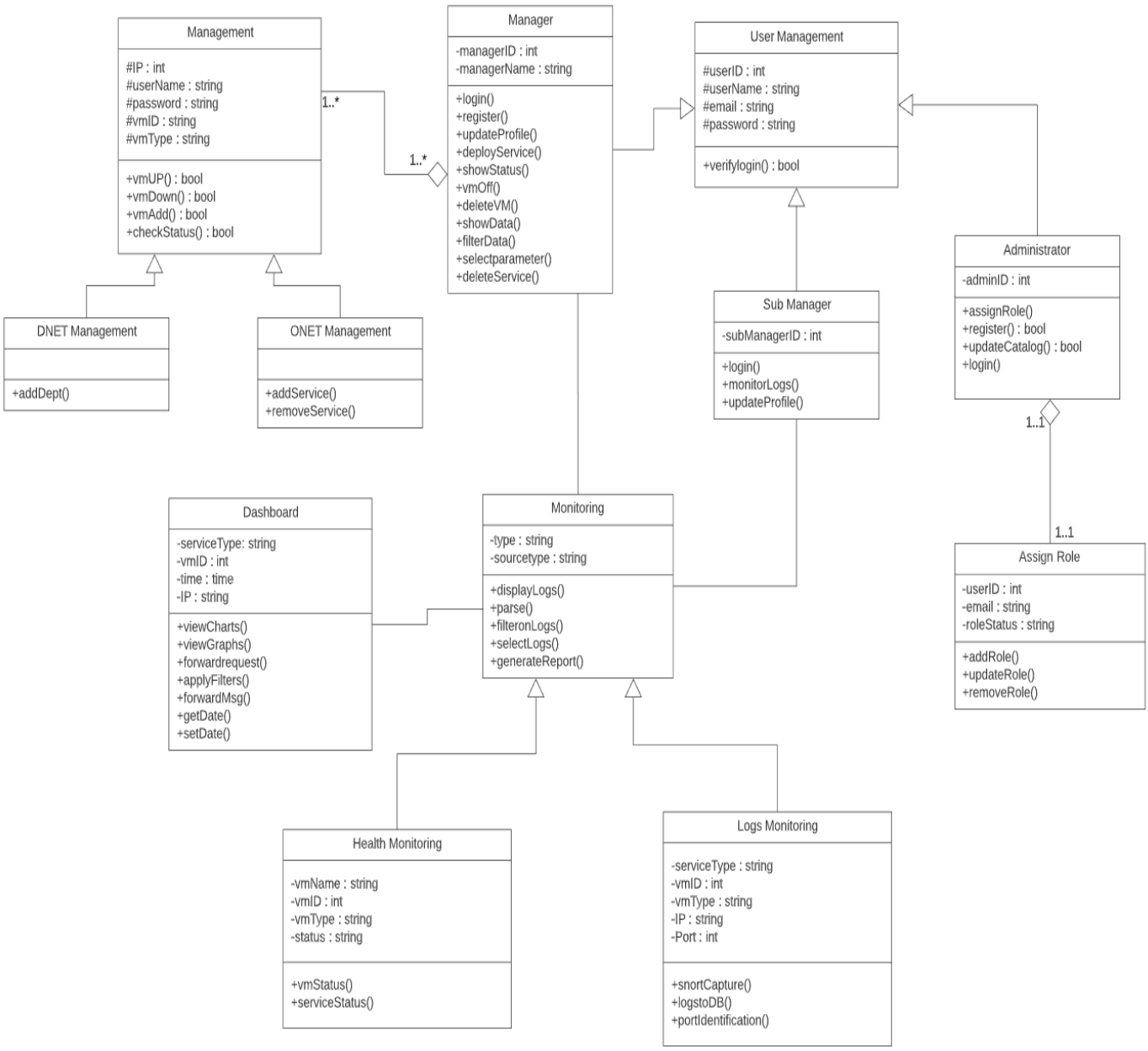


Figure 4.17 Class Diagram - 1: Frontend

4.4.2 **Class Diagram 02: Backend**

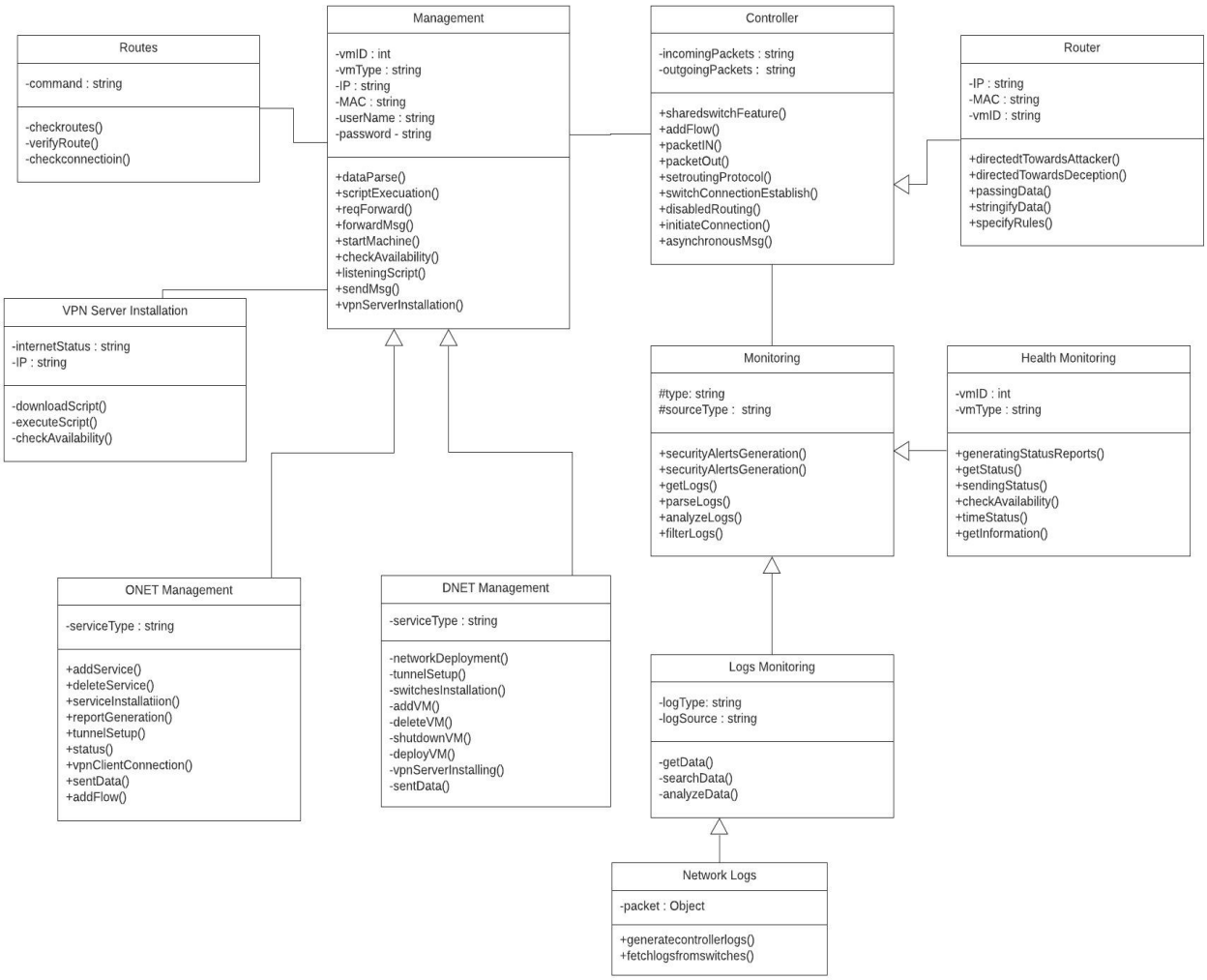


Figure 4.18 Class Diagram - 2 Backend

4.5 Sequence Diagram

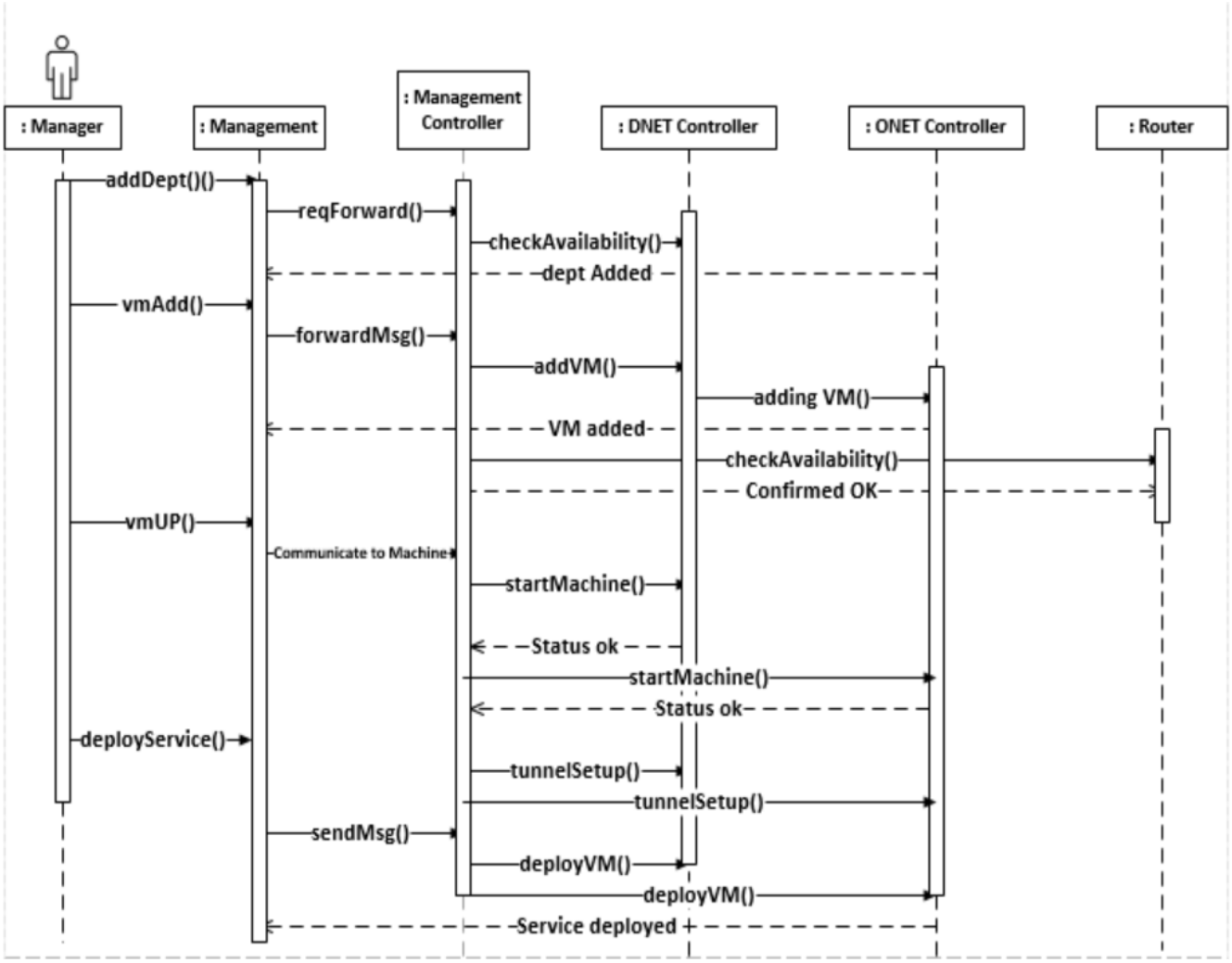


Figure 4.19 Sequence Diagram - 01 Add department

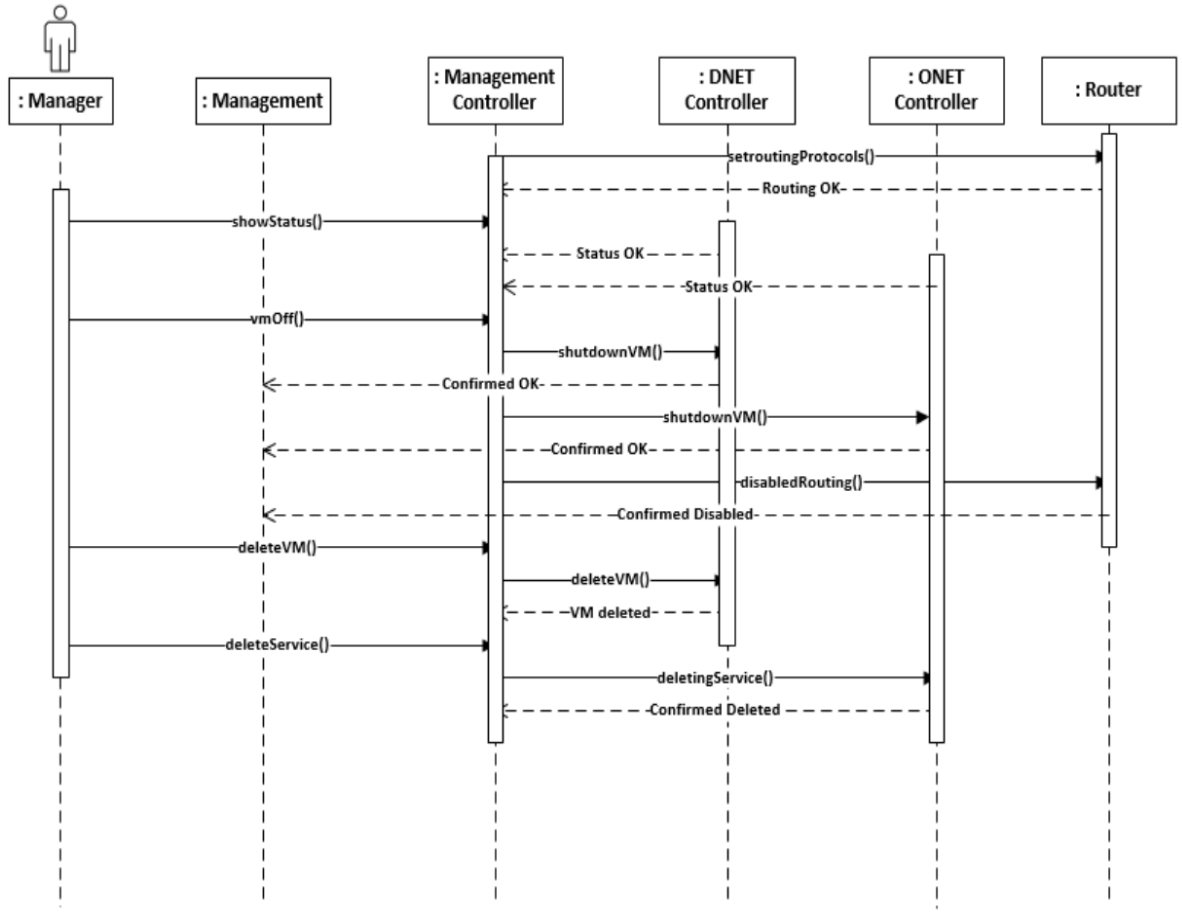


Figure 4.20 Sequence Diagram - 02 VM deployment

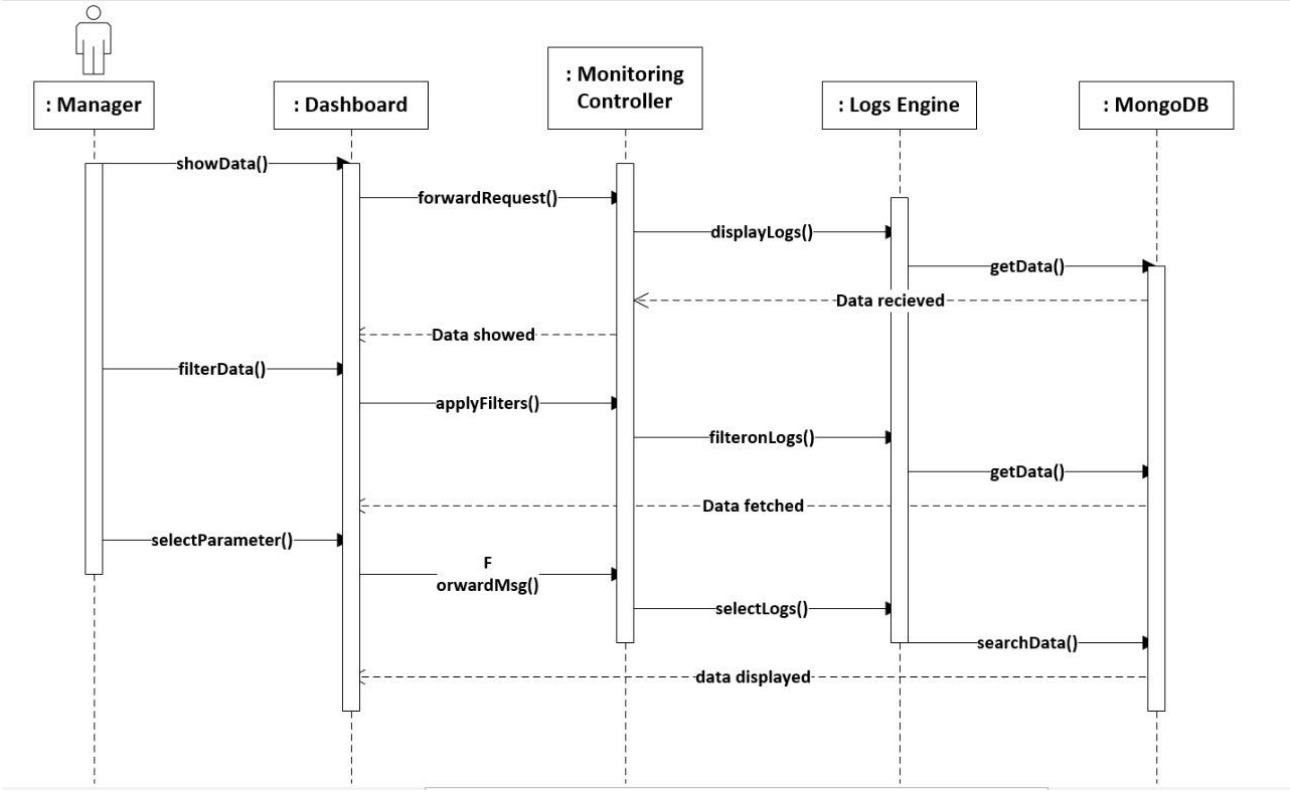


Figure 4.21 Sequence Diagram - 03 Monitoring

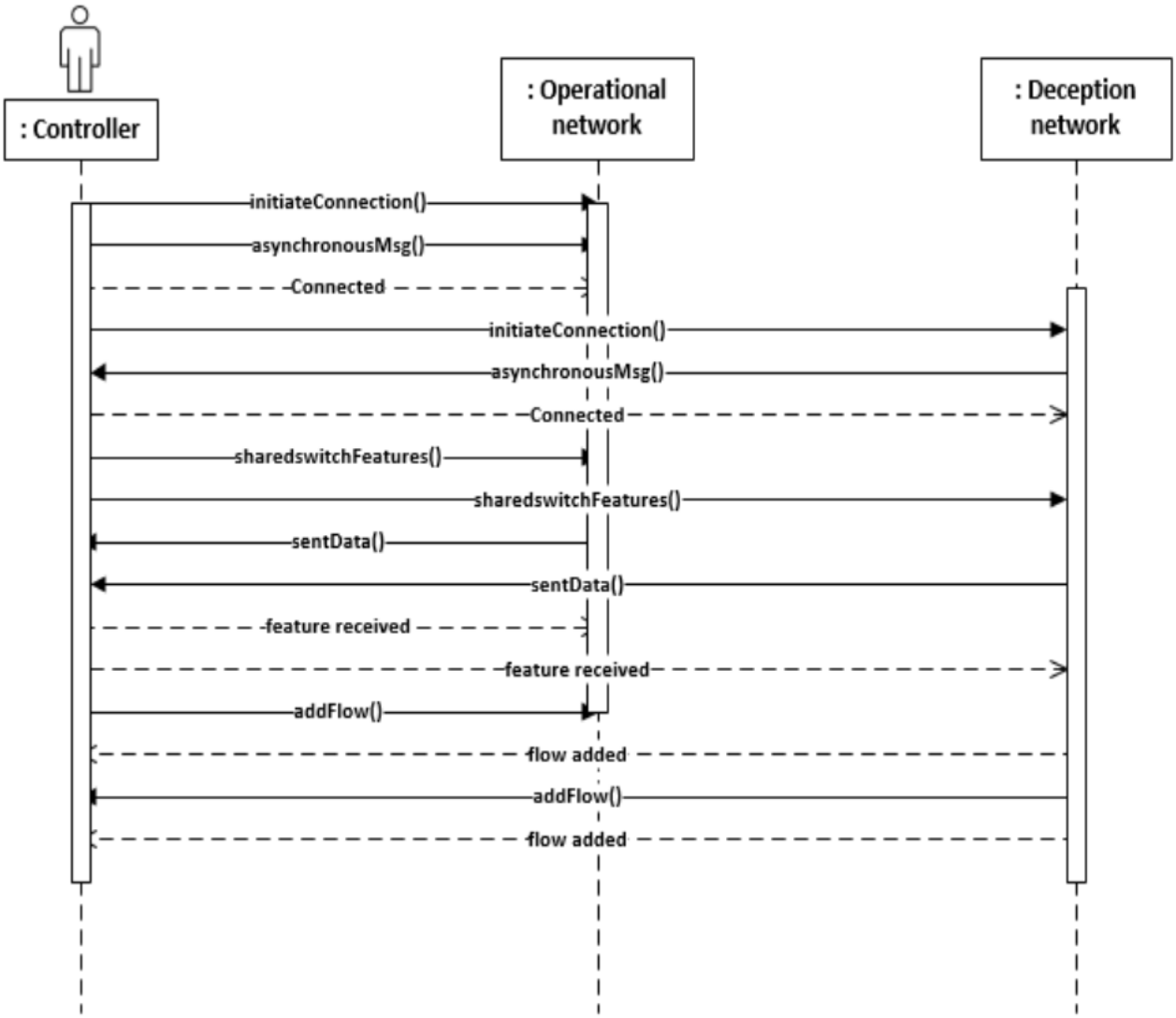


Figure 4.22 Sequence Diagram - 04 Open Flow rules implantation

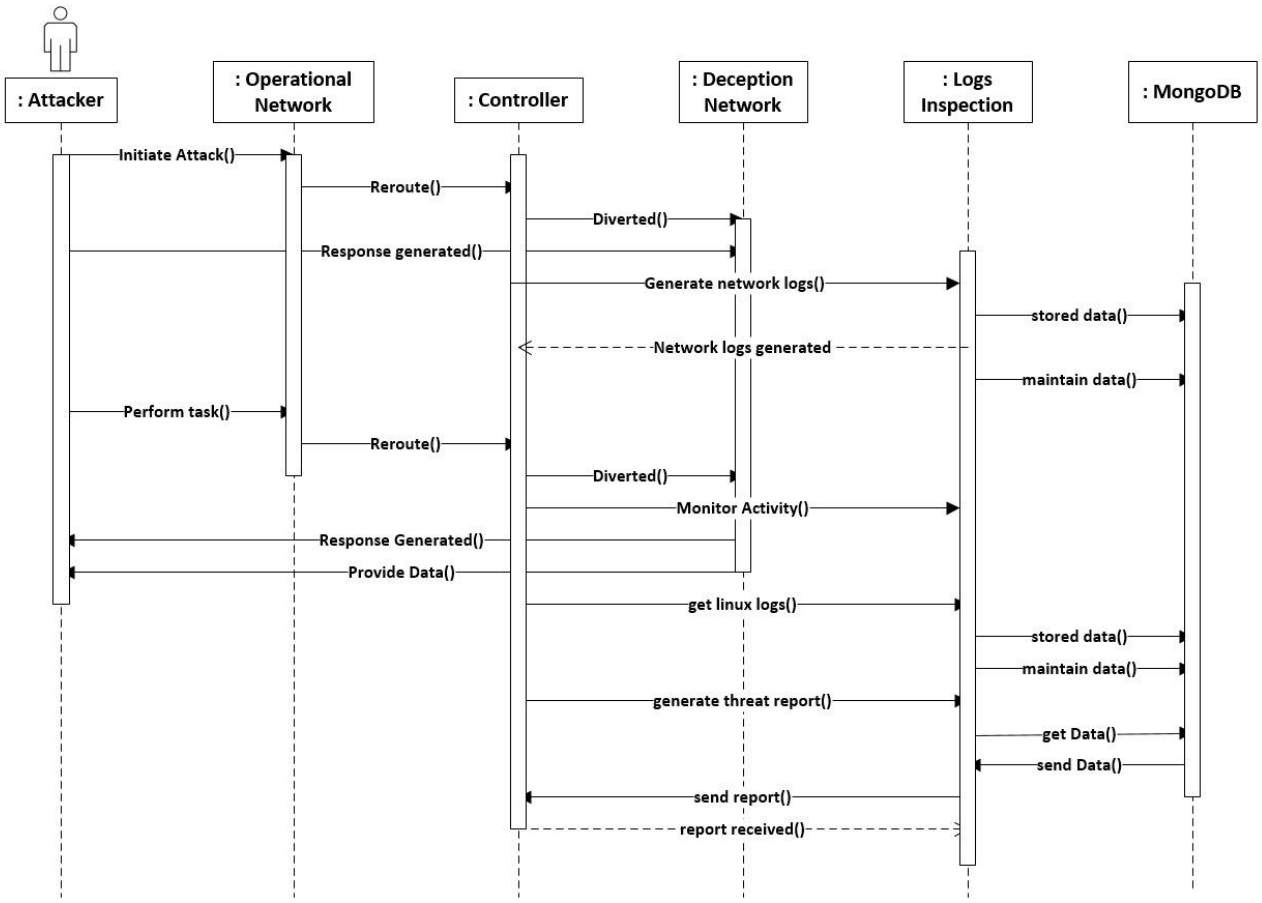


Figure 4.23 Sequence Diagram - 05 Attacker

Management Controller:

It handles the request from user and create a channel with backend controller

DNET Controller:

It handles all the configuration of Deception network along with switches routing tables

ONET Controller:

It handles request of user and perform deployments according to it along with access of database.

Dashboard:

It provides the data in visual form and gather data from different machines

Monitoring Controller:

It setup the ports for monitoring data along with capturing network logs in realtime

Logs Inspection:

It inspects the captured logs, gather it, assembled it and sent to user/admin

5. Implementation

This chapter will discuss implementation details supported by UML diagrams (if applicable). You will not put your source code here. Any of the following sections may be included based on your project.

5.1 Algorithm

5.1.1 Controller Class

```
While(system.running){
if (serviceisup) & (machine is displayed)
Attackerattacks=true
Reroutethetraffic=true
Generateresponse=true
Else
print("no service found")
or
print("no machine found")
ENDIF
while (Attacking){
if(Attacksuccessful){
generatelogs=true
analyzelogs=true
storelogs=true
generatereport=true
sendtoui=true
else
print("Attack unsuccessful")
ENDIF
```

5.1.2 Ansible Class

Ansible:

```
Function SetPurpose (taskType, winCommand=None)
Set task according to taskType
Set command as winCommand if required
Function SelectFile (taskType)
```

```
Select File according to taskType
Function ReadFile ()
Load data from FILE as ymlScript
Function WriteFile ()
Create new temporaryFile
Write the changed ymlScript to temporaryFile
Function PreparePlaybook ()
FOR tags in ymlScript
FOR params in in tags
Change ymlScript with GetDynamicProperty() from Configuration
ENDFOR
ENDFOR
WriteFile()
Function ExecutePlaybook ()
spawn ansible as childProcess
Interact with childProcess to see output
Del temporaryFile


Function SignIn (user, pass)

If user in d
if
 password of user equals pass
return
success
else
return
invalid credentials
end if
else
return
invalid credentials
end if


Function SingUp(user,pass)

if
user in db
return
user already exist
else
Add user && password to db
return
Success
end if
```

5.2 User Interface

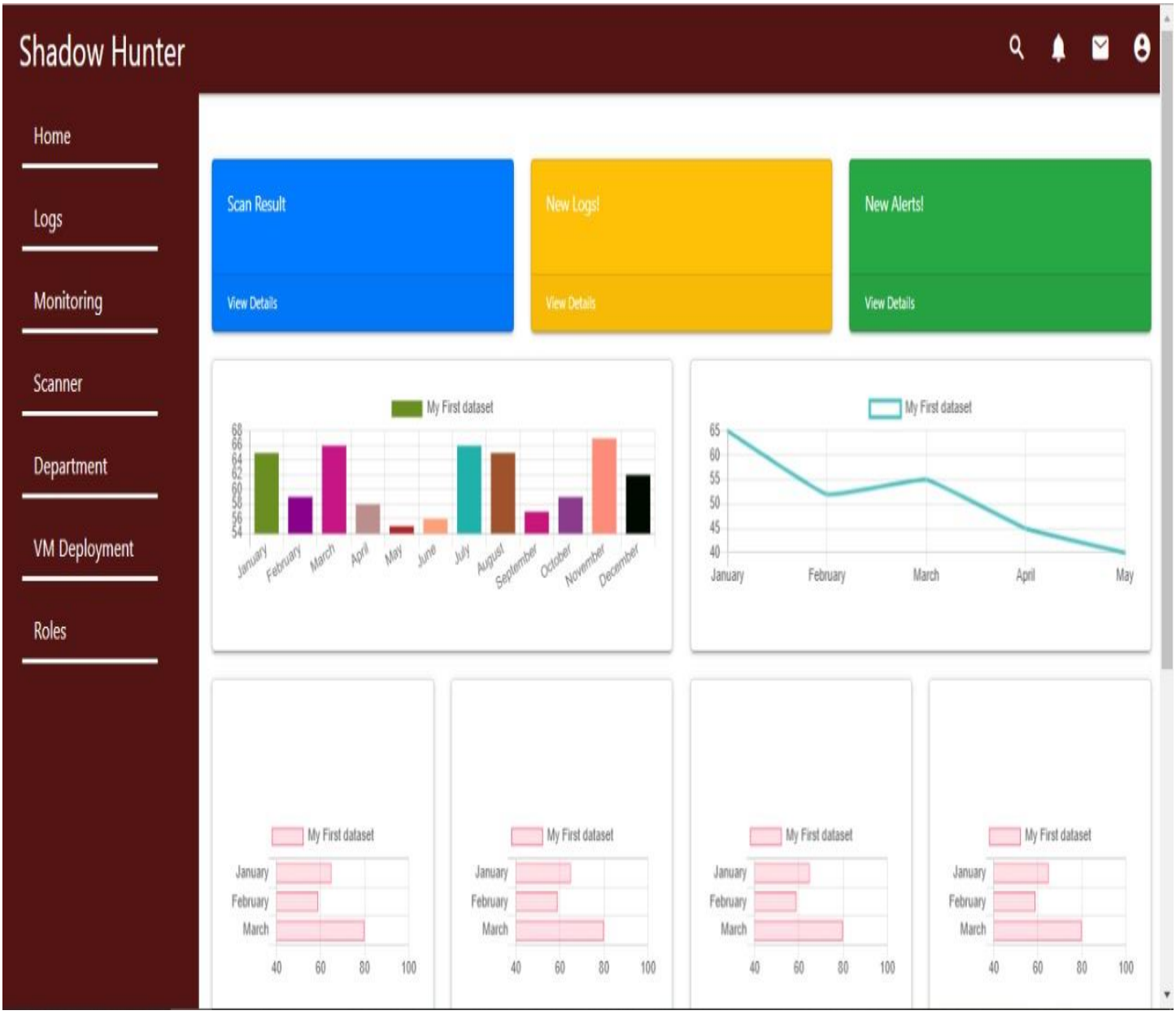


Figure 5.1 User Interface 01 - dashboard

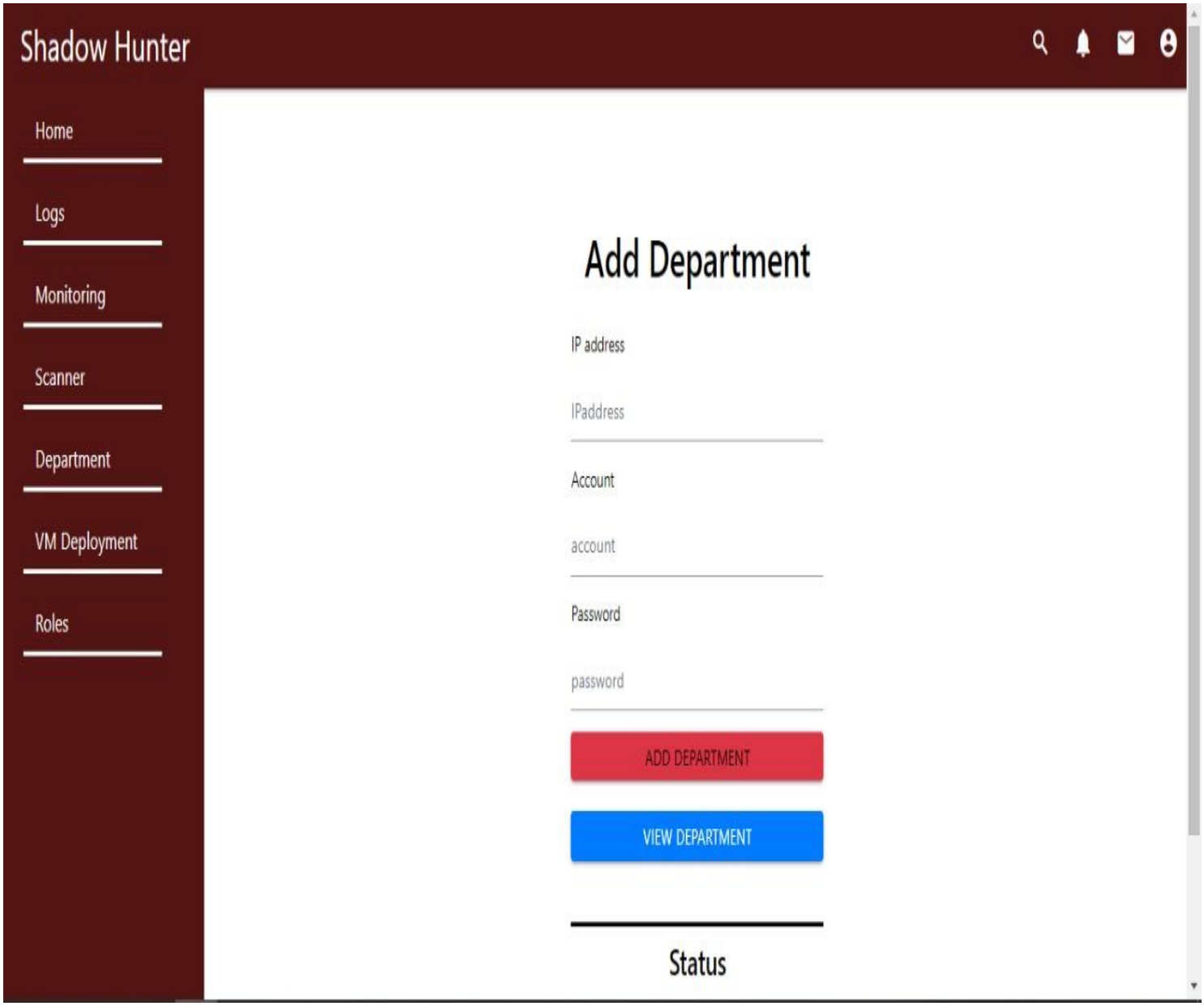


Figure 5.2 User Interface 02 – Add a department

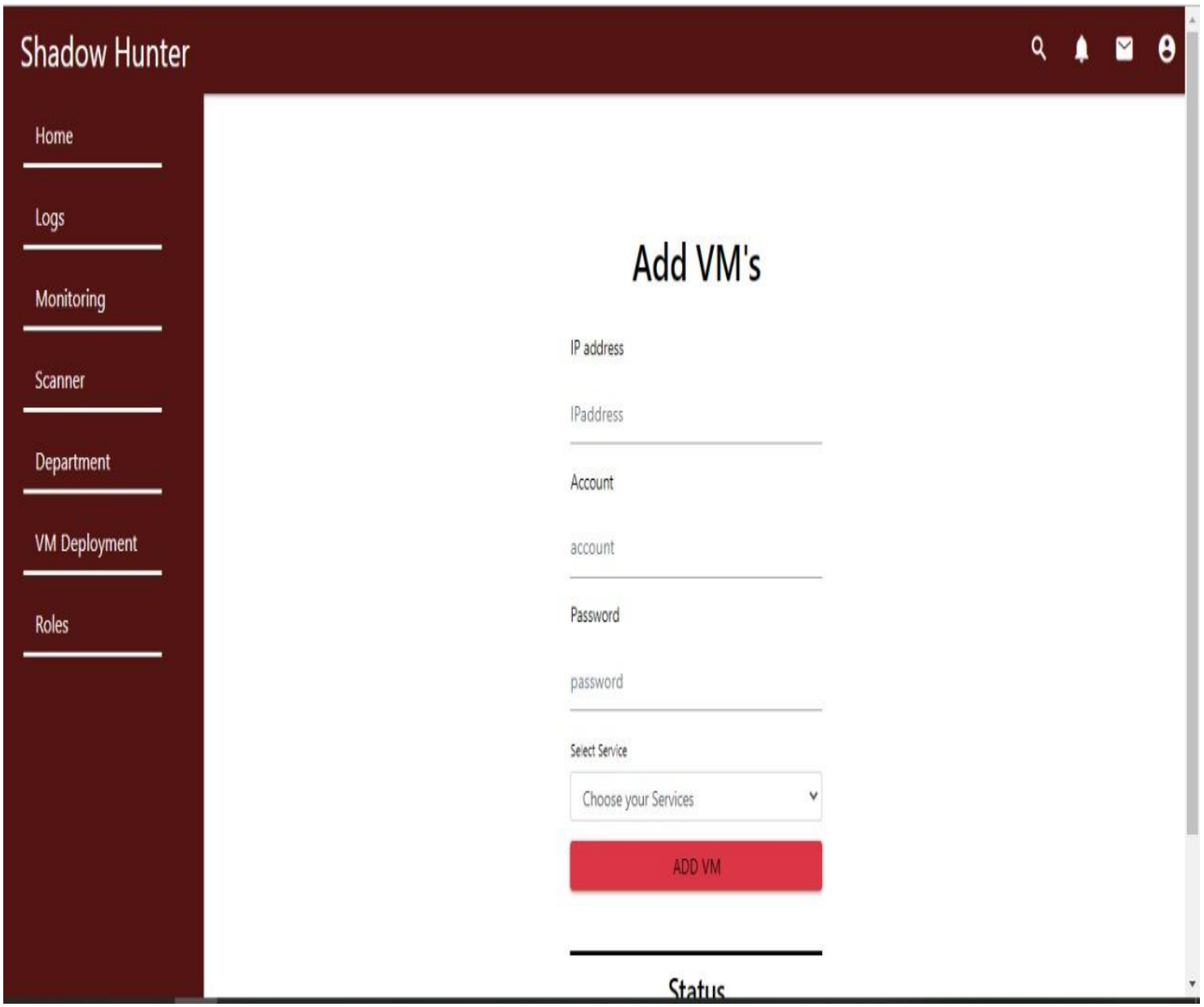


Figure 5.3 User Interface 03 – Add VM

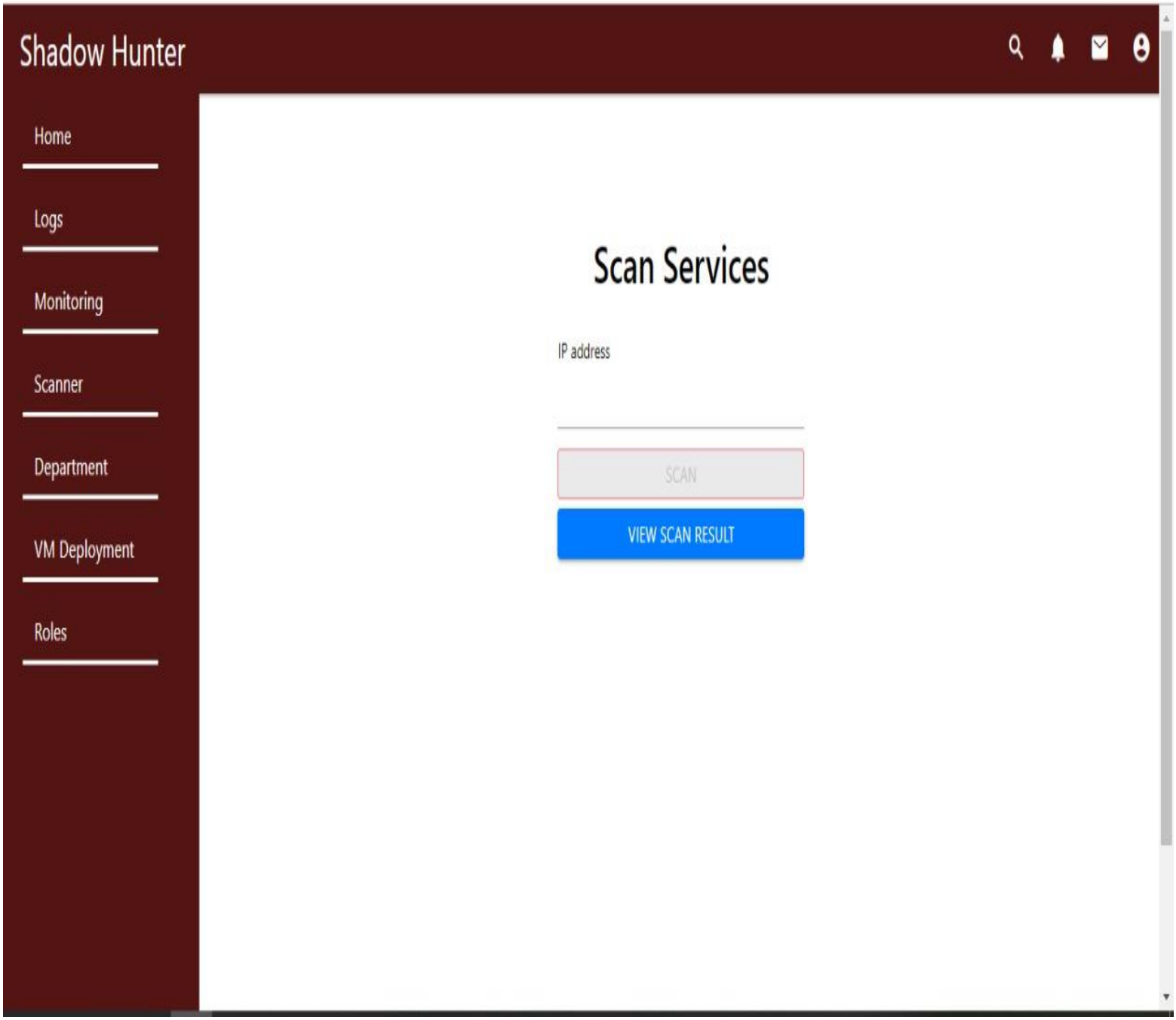


Figure 5.4 User Interface 04 – Scanner

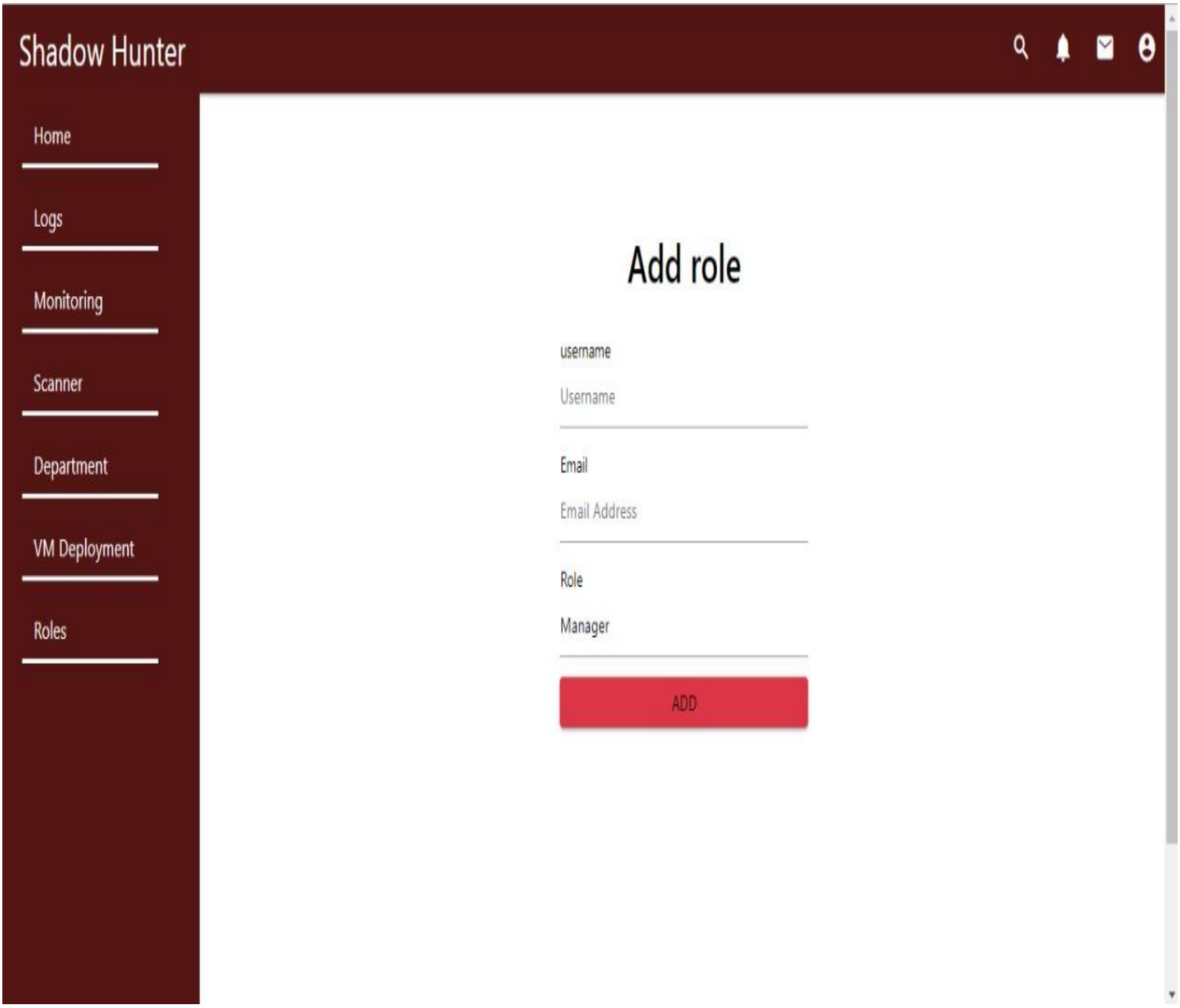


Figure 5.5 User Interface 05 – Add role

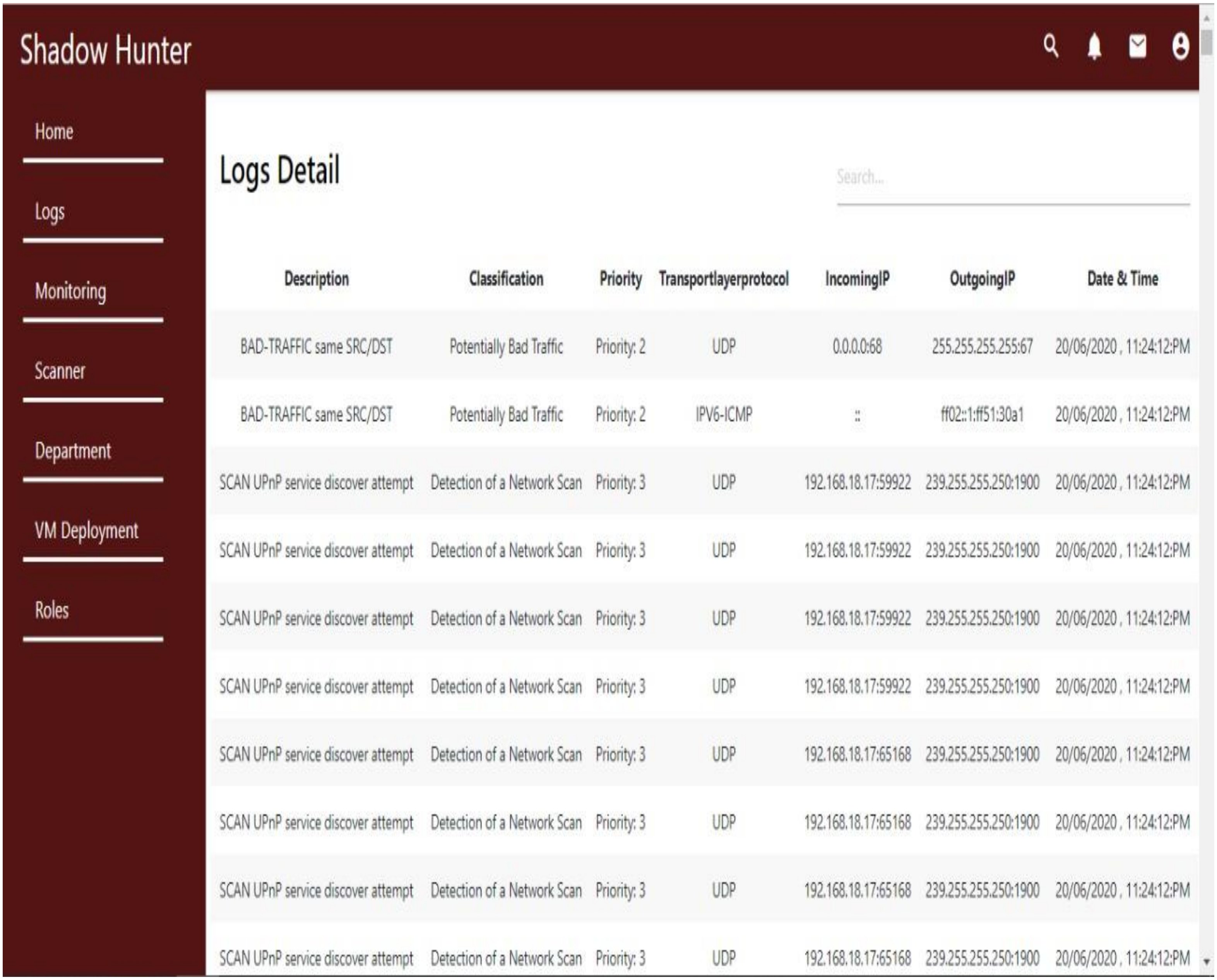


Figure 5.6 User Interface 06 – Logs Detail

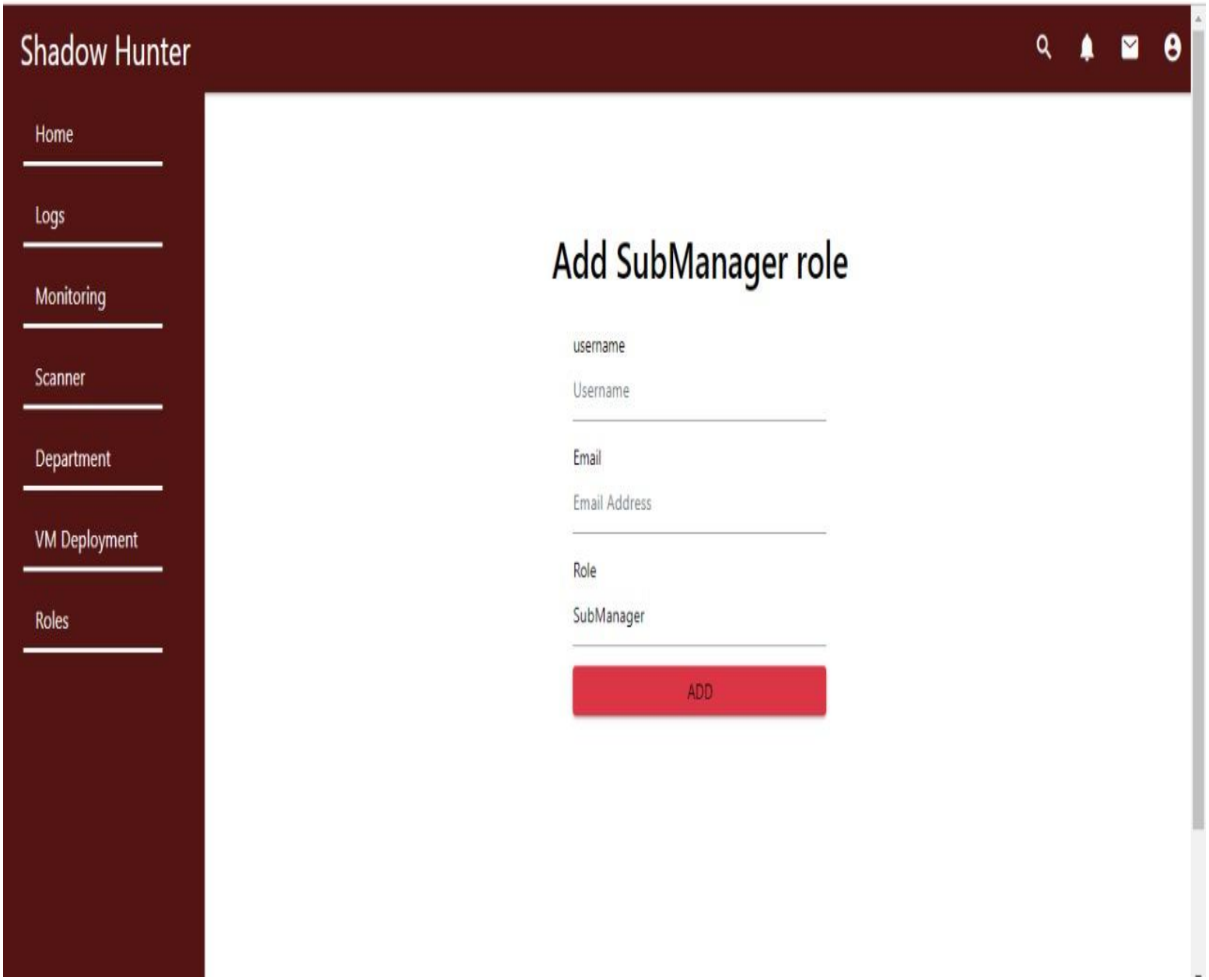


Figure 5.7 User Interface 07 – Add sub-manager role

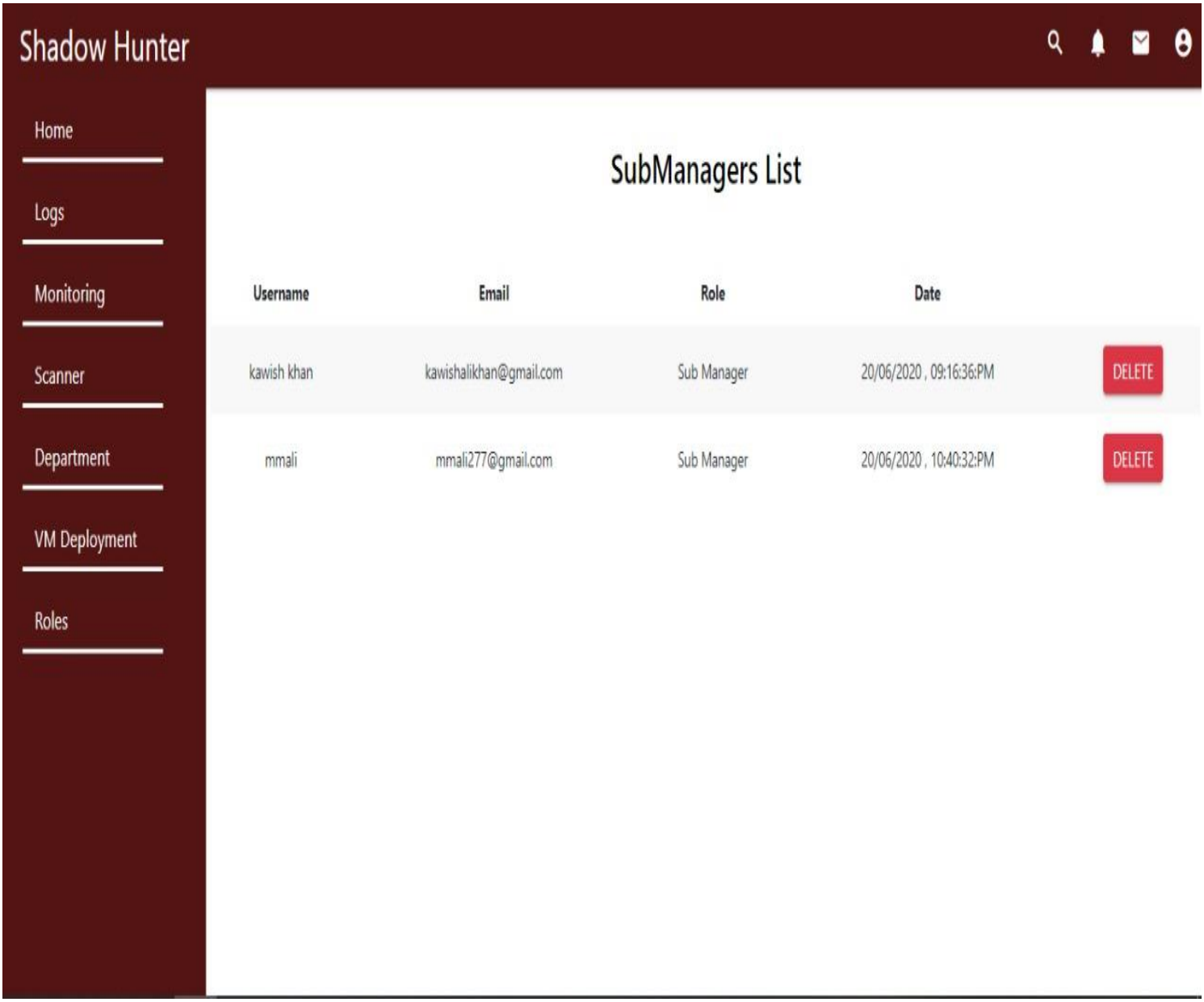


Figure 5.8 User Interface 08 – Sub-Manager list

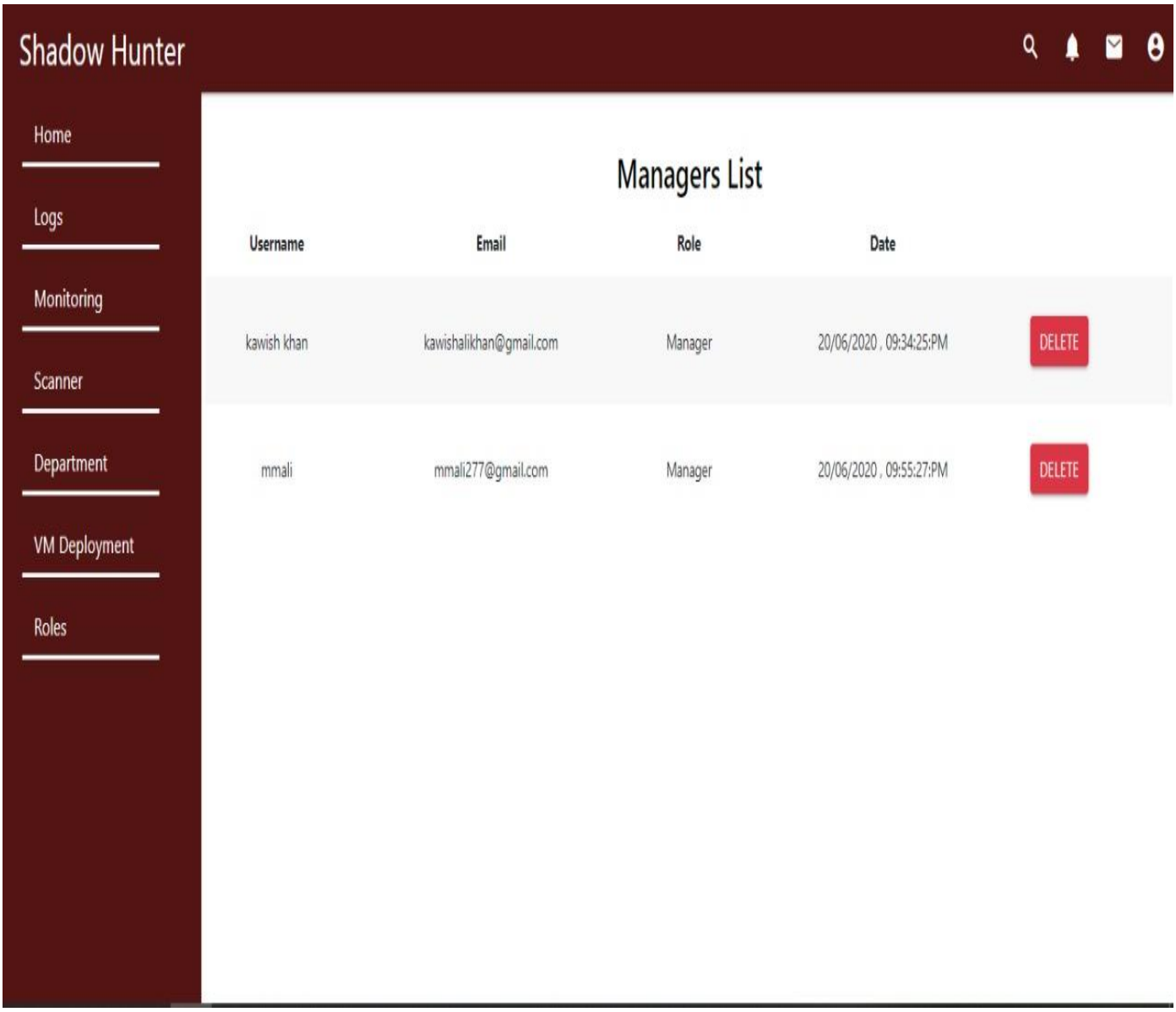


Figure 5.9 User Interface 09 – Managers List

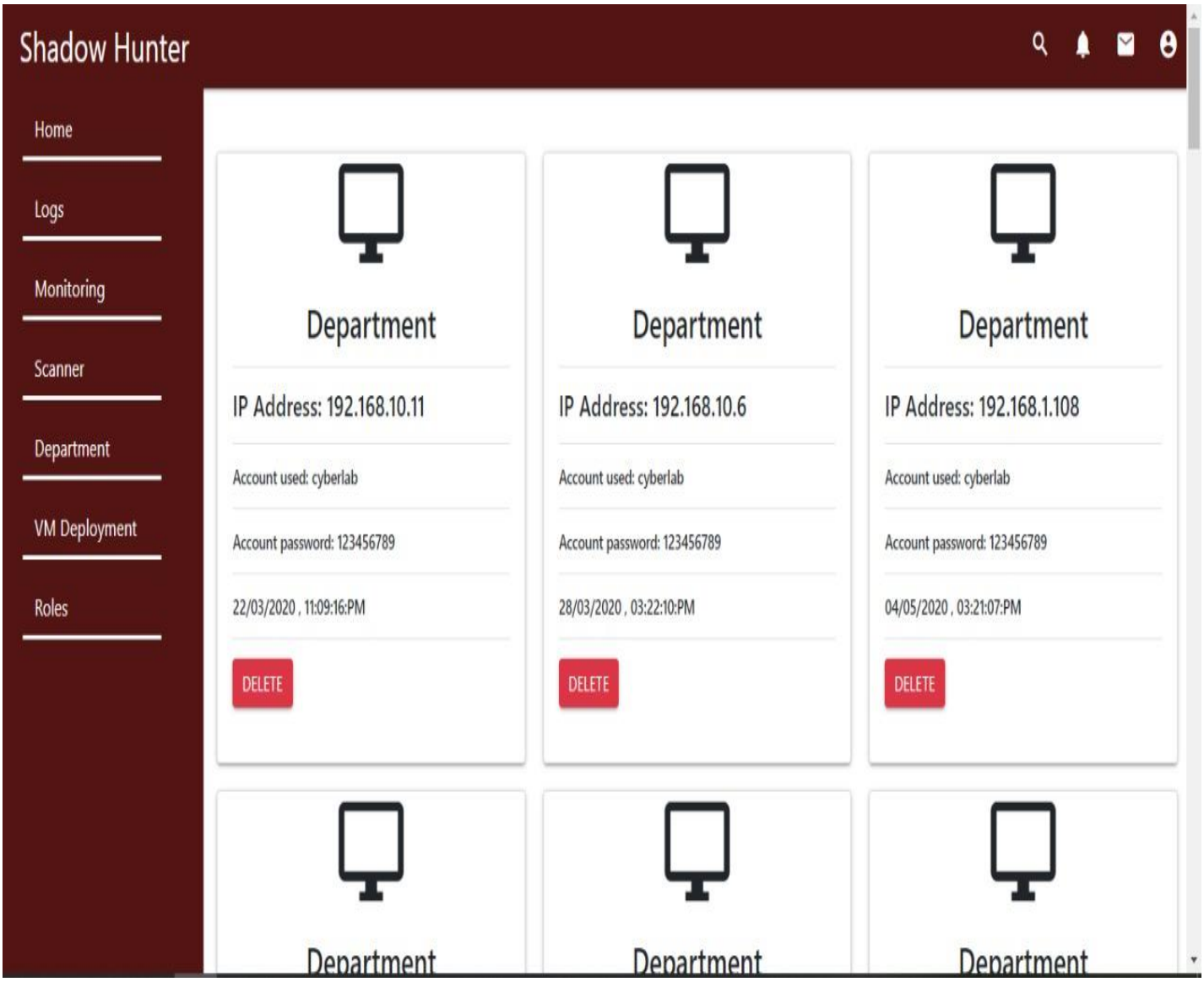


Figure 5.10 User Interface 10 – Departments List

6. Testing and Evaluation

This chapter may include the following sections. (Students are required to perform the testing both manually and automated).

6.1 Manual Testing

6.1.1 System testing

Admin Panel:

The admin will be assigned by our system for specific organization. The admin has higher authority, he/she can assign role to different users and can alter it when it's needed. The admin can scan the whole network and discover the potential services. For which the admin can deploy the deployment and after deployments, the admin can add machines to these deployments and monitor the machines health furthermore admin can monitor network logs of these machines and different alerts will also be sent to admin.

Manager Panel:

The manager will be assigned by admin. The manager has the privileges to scan the network and view the result and find the potential services. For these services deployments can be done by manager. He/She can deploy the departments consisting of whole network setup based upon SDN model. Then manager can add VM's to these departments and monitor the attackers' activity and status of these machines will also be observed by these managers.

Sub-Manager Panel:

The sub-manager will also be assigned by admin. The sub-manager has the privileges to view the result the scans. Apart from this, sub-managers will be assigned to view the network log of machines and identify potential hackers along with this, these sub-managers have privilege to monitor the machine and identify in case of failure.

6.1.2 Unit Testing

Test Case: 001 User Registration

Unit Testing 001: User Registration

Testing Objective: To ensure user registration is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Verify that the Registration form contains username, email, password submit, login (If you already have an account).	-	All fields are visible and working.	As expected	Pass

2.	Verify that system generates a validation message when clicking on submit button without filling all the mandatory fields.	**Username:** **Email:** **Password:** Enter **submit** button.	Validation error is displayed against mandatory field.	As expected	Pass
3.	Verify that system generates a validation message on missing a mandatory field when clicking on submit button.	**Username:** Masoom Alam **Email:** masoomalam @comsats.edu.pk.com **Password:** Enter **submit** button.	Validation error is displayed against Manager name i.e. "Password" Password is required."	As expected	Pass
4.	Verify that entering blank spaces on mandatory fields lead to validation error.	**Username:** **Email:** **Password:** Enter **submit** button.	Validation error is displayed against mandatory field.	As expected	Pass
5.	Verify that system generates a validation message when entering existing email.	**Username:** Masoom Alam **Email:** harisgul101@gmail.com **Password**: haris@123 Enter **submit** button.	Validation error is displayed. i.e. "email already exists."	As expected	Pass
6.	Verify that the validation of email field by entering incorrect email id.	**Username:** Masoom Alam **Email:** masoomalam comsats.edu.pk.com	Validation error is displayed. i.e. "email is required."	As expected	Pass

		Password: haris@123 Enter **submit** button.			
7.	Verify that all the fields have a valid placeholder.	-	All fields have placeholders	As expected	pass
8.	Verify user registration after click on the Submit button on registration form with correct input data.	**Username:** Masoom Alam **Email:** masoomalam @comsats.edu.pk.com **Password:** masoom@123 Enter **submit** button.	Registration completed successfully.	As expected	Pass
9.	Verify that Enter key works as a substitute for the Submit button.	**Username:** Masoom Alam **Email:** masoomalam @comsats.edu.pk.com **Password:** masoom@123 Press **Enter** button.	Enter key works same as a submit button.	As expected	Pass
10.	Verify that clicking on submit button after entering all the mandatory fields, stores data in database.	**Username:** Masoom Alam **Email:** masoomalam @comsats.edu.pk.com **Password:** masoom@123 Click **Submit** button.	Data is stored in Database.	As expected	Pass
11.	Verify the link "Already have Account, Signin."	Click on the link "Already have Account, Signin."	Signin page is loaded.	As expected.	Pass

Table 001: Test Cases for User Registration

Testing Environment: Windows 10, Google Chrome

Tested By: haris gul

Date: February 20, 2020

Test Case: 002 Enter Credentials

Unit Testing 002: Enter Credentials

Testing Objective: To check the field is only valid for official Manager email.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Verify that system generates a validation message when entering existing email.	**Username:** Masoom Alam **Email:** masoomalam @comsats.edu.pk.com **Password:** masoom@123 Click **Submit** button.	Validation error is displayed. i.e. "email already exists."	As expected	Pass
2.	Verify that the validation of email field by entering incorrect email id.	**Username:** Masoom Alam **Email:** masoomalam comsats.edu.pk.com **Password:** masoom@123 Click **Submit** button	Validation error is displayed. i.e. "Invalid Email."	As expected	Pass

Table 002: Test Cases for Entered Credentials

Testing Environment: Windows 10, Google Chrome

Tested By: haris gul

Date: February 20, 2020

Test Case: 003 Send Verification Email

Unit Testing 003: Send Verification Email

Testing Objective: To check the verification email functionality is working correctly.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Verify the user receives an email on their registered account.	System sends an email to entered email.	Generated email is received by the Manager.	As expected	Pass
2.	Verify the valid credentials are placed in email.	**Email:** masoomalam @comsats.edu.pk **Password:** Ab3f	Valid credentials are present in email	As expected	Pass
3.	Verify the system generates a random password for Manager.	**Password:** Ab3f	Random password is included in email.	As expected	Pass
4.	Verify the randomly generated password contains 4 characters.	**Password:** Ab3f	Password contains 4 characters including numbers, capital and small alphabets.	As expected	Pass

Table 003: Test Cases for Send Verification Email

Testing Environment: Windows 10, Google Chrome

Tested By: haris gul

Date: February 20, 2020

Test Case: 004 Register Manager

Unit Testing 004: Register Manager

Testing Objective: To ensure that the admin can add/register accounts of their employees.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Verify that only Manager have an option to register an account for manager.	"Add Manager" link.	Add Manager link is only found	As expected	Pass

			in admin panel.		
2.	Verify that the Registration form contains username email and role field along with the add button.	-	All fields are visible and working.	As expected	Paas
3.	Verify that system generates a validation message when clicking on add button without filling all the mandatory fields.	**username:** **Email:** **role:** Press **add** button.	Validation error is displayed against mandatory field.	As expected	Pass
4.	Verify that system generates a validation message on missing a mandatory field when clicking on add button.	**username:** **Email:** taimoor@gmail.com **role: manager** Press **add** button..	Validation error is displayed against username i.e. "username is required."	As expected	Pass
5.	Verify that entering blank spaces on mandatory fields lead to validation error.	**username:** **Email:** **role:** Press **add** button.	Validation error is displayed against mandatory field.	As expected	Pass
6.	Verify that system generates a validation message when entering existing email.	**username:** mmali **Email:** mmali277@gmil.com **role:** manager Press **add** button.	Validation error is displayed. i.e. "email already exists."	As expected	Pass
7.	Verify that the validation of email field by entering incorrect email id.	**username:** mmali **Email:** mmali277gmil.com **role:** manager Press **add** button.	Validation error is displayed. i.e. "email is required."	As expected	Pass
8.	Verify that all the fields have a valid placeholder.	-	All fields have placeholders	As expected	pass

9.	Verify manager's registration after click on the "Add Manger" button/link on add manager form with correct input data.	**username:** mmali **Email:** mmali277@gmil.com **role:** manager Enter **Add Manager** button.	Registration is done successfully	As expected	Paas
10.	Verify that Enter key works as a substitute for the Add Manager button.	**username:** mmali **Email:** mmali277@gmil.com **role:** manager Press **Enter** key.	Enter key works same as a submit button.	As expected	Pass
11.	Verify that clicking on submit button after entering all the mandatory fields, stores data in database.	**username:** mmali **Email:** mmali277@gmil.com **role:** manager Enter **Add Manager** button	Data is stored in Database.	As expected	Pass

Table 004: Test Cases for Register Manager

Testing Environment: Windows 10, Google Chrome

Tested By: haris gul

Date: February 20, 2020

Test Case: 005 Register Sub Manager

Unit Testing 005: Register Sub manager

Testing Objective: To ensure that the managers can add/register accounts of their Sub managers.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1	Verify that only admin has an option to register an account for Sub manager.	"Add Sub Manager" link.	Add Manager link is only found in admin panel.	As expected	Pass
2	Verify that the Registration form contains username email and role field	-	All fields are visible and working.	As expected	Paas

	along with the add button.				
3	Verify that system generates a validation message when clicking on add button without filling all the mandatory fields.	**username:** **Email:** **role:** Press **add** button.	Validation error is displayed against mandatory field.	As expected	Pass
4	Verify that system generates a validation message on missing a mandatory field when clicking on add button.	**username:** **Email:** submanager@gmail.com **role:** submanager Press **add** button.	Validation error is displayed against username i.e. "username is required."	As expected	Pass
5	Verify that entering blank spaces on mandatory fields lead to validation error.	**username:** **Email:** **role:** Press **add** button.	Validation error is displayed against mandatory field.	As expected	Pass
6	Verify that system generates a validation message when entering existing email.	**username:** mmali **Email:** mmali277@gmail.com **role:** submanager Press **add** button.	Validation error is displayed. i.e. "email already exists."	As expected	Pass
7	Verify that the validation of email field by entering incorrect email id.	**username:** abc **Email:** abcgmail.com **role:** submanager Press **add** button.	Validation error is displayed. i.e. "email is required."	As expected	Pass
8	Verify that all the fields have a valid placeholder.	-	All fields have placeholders	As expected	pass
9	Verify sub manager registration after click on the "Add role" button/link on add role form with correct input data.	**Firstname:** abc **Lastname:** def **Email:** abc1 @comsats.edu.pk Enter **Add** button.	Registration is done successfully	As expected	Paas

1	Verify that Enter key works as a substitute for the Add role button.	**Firstname:** abc **Lastname:** def **Email:** abc1 @comsats.edu.pk Press **Enter** key.	Enter key works same as a submit button.	As expected	Pass
1	Verify that clicking on submit button after entering all the mandatory fields, stores data in database.	**Firstname:** abc **Lastname:** def **Email:** abc1 @comsats.edu.pk Enter **Add** button	Data is stored in Database.	As expected	Pass

Table 005: Test Cases for Register Sub manager

Testing Environment: Windows 10, Google Chrome

Tested By: haris gul

Date: February 20, 2020

Test Case: 006 Create Credentials

Unit Testing 006: Create Credentials

Testing Objective: To check the create credentials functionality successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Verify admin can create credentials for manager.	**Firstname:** abc **Lastname:** def **Email:** abc1 @comsats.edu.pk Press **add** button.	Random password is generated by system and received in email.	As expected	Pass
2.	Verify admin can create credentials for sub manager.	**Firstname:** abc **Lastname:** def **Email:** def1 @comsats.edu.pk Press **add** button.	Random password is generated by system and received in email.	As expected	Pass
3.	Verify random password is generated after clicking the add button	System generates random password.	An email contains random password.	As expected	Pass
4.	Verify the system generates a random	**Password:** b93f	Random password is	As expected	Pass

	password on admin request for Manger's account.		generated in email.		
5.	Verify the system generates a random password on admin's request for sub manager account.	**Password:** L3ba	Random password is generated in email.	As expected	Pass
6.	Verify the randomly generated password contains 4 characters.	**Password:** L3ba	Password contains 4 characters including numbers, capital and small alphabets.	As expected	Pass

Table 006: Test Cases for Create Credentials

Testing Environment: Windows 10, Google Chrome

Tested By: haris gul

Date: February 20, 2020

Test Case: 007 Send Confirmation Email

Unit Testing 007: Send Confirmation Email

Testing Objective: To check the confirmation email functionality is working correctly.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Verify the system generates an email on Add Manager button.	**Firstname:** Manager **Lastname:** One **Email:** manager1 @comsats.edu.pk Press **add** button.	Email is generated by the system.	As expected	Pass
2.	Verify the system generates an email on Add Sub manager button.	**Firstname:** sub manager **Lastname:** One **Email:** submanager1 @comsats.edu.pk Press **add** button.	Email is generated by the system.	As expected	Pass

3.	Verify the manager receives an email on their registered account.	System sends an email.	Generated email is received by the manager.	As expected	Pass
4.	Verify the sub manager receives an email on their registered account.	System sends an email.	Generated email is received by the submanager.	As expected	Pass
5.	Verify the valid credentials are placed in manager's email.	**Email:** manager1 @comsats.edu.pk **Password:** b93f	Valid credentials are present in email	As expected	Pass
6.	Verify the valid credentials are placed in sub manager's email.	**Email:** submanager1 @comsats.edu.pk **Password:** L3ba	Valid credentials are present in email	As expected	Pass
7.	Verify the randomly generated password contains 4 characters.	**Password:** Ab3f	Password contains 4 characters including numbers, capital and small alphabets.	As expected	Pass

Table 007: Test Cases for Send Confirmation Email

Testing Environment: Windows 10, Google Chrome

Tested By: haris gul

Date: February 20, 2020

Test Case: 008 Login as Admin

Unit Testing 008: Login as Admin

Testing Objective: To ensure that the login as admin is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Verify that the login screen contains elements such as email, password, sign in	-	All fields are present	As expected	Pass

	button, remember password check box, forgot password link.				
2.	Verify that Admin is not able to Login with invalid Email and invalid Password.	**Email:** kawish@gmail.com **Password:** kawishkhan1 Enter **Submit** button	Validation error is displayed, "Invalid Credentials"	As expected	Pass
3.	Verify that Admin is not able to Login with any invalid field.	**Email:** kawish@gmail.com **Password:** kawishkhan1 Enter **Submit** button	Validation error is displayed, "Invalid Credentials"	As expected	Pass
4.	Verify that Admin is not able to Login with blank Email or Password.	**Email:** **Password:**	Validation error is displayed, "Invalid Credentials"	As expected	Pass
5.	Verify Admin login by clicking the 'Sign In button on sign in form with correct input data.	**Email:** harisgul101@gmail.com **Password:** Haris@12345 Enter **Submit** button	User Loaded Successfully	As expected	Pass
6.	Verify the password can be copy-pasted.	**Email:** harisgul101@gmail.com **Password:** Haris@12345 Enter **Submit** button	User Loaded Successfully	As expected	Pass
7.	Verify that Enter key works as a substitute for the Sign in button.	**Email:** harisgul101@gmail.com **Password:** Haris@12345 **Enter** key	User Loaded Successfully	As expected	Pass
8.	Verify that clicking on browser back button after successful login should not take Admin to log out mode.	Click browser back button.	User state remains same.	As expected	Pass
9.	Verify that whether Admin is still logged in after series of actions	**Email:** harisgul101@gmail.com **Password:** Haris@12345	User is still loaded.	As expected	Pass

	such as sign in, close browser and reopen the application.	Enter **Submit** button Load different pages. Close browser Reopen browser			
10.	Verify that Admin is redirected to appropriate page after successful login.	**Email:** harisgul101@gmail.com **Password:** Haris@12345 Enter **Submit** button	Redirected to Dashboard.	As expected	Pass
11.	Verify the logs for the login session.	-	Logs are maintained		Not executed

Table 008: Test Cases for Login as Admin

Testing Environment: Windows 10, Google Chrome

Tested By: haris gul

Date: February 20, 2020

Test Case: 009 Login as Manager

Unit Testing 009: Login as Manager

Testing Objective: To ensure that the login as manager is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Verify that the login screen contains elements such as email, password, sign in button, remember password check box, forgot password link.	-	All fields are present	As expected	Pass
2.	Verify that Manager is not able to Login with invalid Email and invalid Password.	**Email:** harisgul101@gmail.com **Password:** Ab3f Enter **Submit** button	Validation error is displayed, “Invalid Credentials”	As expected	Pass

3.	Verify that Manager is not able to Login with any invalid field.	**Email:** harisgul101@gmail.com **Password:** Absas	Validation error is displayed, "Invalid Credentials"	As expected	Pass
4.	Verify that Manager is not able to Login with blank Email or Password.	**Email:** **Password:**	Validation error is displayed, "Invalid Credentials"	As expected	Pass
5.	Verify Manager login by clicking the 'Sign In button on sign in form with correct input data.	**Email:** kawishalikhan@gmail.com **Password:** vz8L Enter **Submit** button	User Loaded Successfully	As expected	Pass
6.	Verify the password can be copy-pasted.	**Email:** kawishalikhan@gmail.com **Password:** vz8L Enter **Submit** button	User Loaded Successfully	As expected	Pass
7.	Verify that Enter key works as a substitute for the Sign in button.	**Email:** kawishalikhan@gmail.com **Password:** vz8L **Enter** key	User Loaded Successfully	As expected	Pass
8.	Verify that clicking on browser back button after successful login should not take Manager to log out mode.	Click browser back button.	User state remains same.	As expected	Pass
9.	Verify that whether Manager is still logged in after series of actions such as sign in, close browser and reopen the application.	**Email:** kawishalikhan@gmail.com **Password:** vz8L Enter **Submit** button Load different pages. Close browser Reopen browser	User is still loaded.	As expected	Pass
10.	Verify that Manager is redirected to appropriate page after successful login.	**Email:** kawishalikhan@gmail.com **Password:** vz8L Enter **Submit** button	Redirected to Dashboard.	As expected	Pass

11.	Verify the logs for the login session.	-	Logs are maintained		Not executed

Table 009: Test Cases for Login as Manager

Testing Environment: Windows 10, Google Chrome

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 010 Login as Sub Manager

Unit Testing 010: Login as Sub Manager

Testing Objective: To ensure that the login as sub manager is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Verify that the login screen contains elements such as email, password, sign in button, remember password check box, forgot password link.	-	All fields are present	As expected	Pass
2.	Verify that Sub Manager is not able to Login with invalid Email and invalid Password.	**Email: sub** manager1@ comsats.edu.pk **Password:** b93f Enter **Submit** button	Validation error is displayed, "Invalid Credentials"	As expected	Pass
3.	Verify that Sub Manager is not able to Login with any invalid field.	**Email:** submanager1 comsats.edu.pk **Password:** b93f Enter **Submit** button	Validation error is displayed, "Invalid Credentials"	As expected	Pass
4.	Verify that Sub Manager is not able to Login with blank Email or Password.	**Email:** **Password:**	Validation error is displayed, "Invalid Credentials"	As expected	Pass

5.	Verify Sub Manager login by clicking the 'Sign In button on sign in form with correct input data.	**Email:** taimoorbutt7447@gmail.com **Password:** 3rTc Enter **Submit** button	User Loaded Successfully	As expected	Pass
6.	Verify the password can be copy-pasted.	**Email:** taimoorbutt7447@gmail.com **Password:** 3rTc Enter **Submit** button	User Loaded Successfully	As expected	Pass
7.	Verify that Enter key works as a substitute for the Sign in button.	**Email:** taimoorbutt7447@gmail.com **Password:** 3rTc **Enter** key	User Loaded Successfully	As expected	Pass
8.	Verify that clicking on browser back button after successful login should not take Sub Manager to log out mode.	Click browser back button.	User state remains same.	As expected	Pass
9.	Verify that whether Sub Manager is still logged in after series of actions such as sign in, close browser and reopen the application.	**Email:** taimoorbutt7447@gmail.com **Password:** 3rTc Enter **Submit** button Load different pages. Close browser Reopen browser	User is still loaded.	As expected	Pass
10.	Verify that Sub Manager is redirected to appropriate page after successful login.	**Email:** taimoorbutt7447@gmail.com **Password:** 3rTc Enter **Submit** button	Redirected to Dashboard.	As expected	Pass
11.	Verify the logs for the login session.	-	Logs are maintained		Not executed

Table 010: Test Cases for Login as Manager

Testing Environment: Windows 10, Google Chrome

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 011 Installing openvpn script

Unit Testing 0:11 Installing openvpn script

Testing Objective: To ensure Installing openvpn script is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The openvpn scripts needs to be installed inorder to perform	Wget:file.com	The script will be downloaded	A script is downloaded	Pass
2.	The openvpn scripts needs to be installed inorder to perform	Wget:file.com	The script will be downloaded	An error occurred while downloading	Not Executed

Table 11: Test Cases for Installing openvpn script

Testing Environment: Ubuntu 18, RYU

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 012 Running openvpn script

Unit Testing 012: Running openvpn script

Testing Objective: To ensure that Running openvpn script is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The controller needs to run the openvpn script on server	Sudo ./script --parameter	Script will run	Fetching details	Pass
2.	The controller needs to run the openvpn script on server	Sudo ./script --parameter	Script will run	Wrong parameter. Run Again	Fail

Table 12: Test Cases for Running openvpn script

Testing Environment: Ubuntu 18, RYU

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 013 Creating tunnel

Unit Testing 013: Creating tunnel

Testing Objective: To ensure that Creating tunnel is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The Controller shall be able to create tunnel between server and client	Nmcli – client.ovpn	The tunnel is successfully created	The tunnel is created (with an icon)	Pass
2.	The Controller shall be able to create tunnel between server and client	Nmcli – client.ovpn	The tunnel is successfully created	The tunnel is still loading (icon is blur)	Fail

Table 13: Test Cases for Creating tunnel

Testing Environment: Ubuntu 18

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 014 Monitor attacker activity

Unit Testing 014: Monitor attacker activity

Testing Objective: To ensure that monitor attacker activity is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The attacker activity needs to be monitored 24/7 by collecting logs	Logs	Logs needs to be generated	Logs are generated	Pass

2.	The attacker activity needs to be monitored 24/7 by collecting logs	logs	Logs needs to be generated	Logs are not generated because service is off	Not Executed

Table 14: Test Cases for Monitor attacker activity

Testing Environment: Ubuntu 18

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 015 Create service

Unit Testing 015: Create service

Testing Objective: To ensure that create service is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The user needs to select a service from services menu to up that VM	http/ssh/mysql option from menu	The service will be created	The service created	Pass

Table 15: Test Cases for create service

Testing Environment: Ubuntu 18, Virtual box, VMware

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 016 Start service

Unit Testing 016: Start service

Testing Objective: To ensure that start service is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The admin/user can start the	Select one of the service and click on start button	The required service will be start	The service is updated	Pass

	selected service for desired VM				

Table 16: Test Cases for start service

Testing Environment: Ubuntu 18, virtual box, VMware

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 017 Stop service

Unit Testing 019: End service

Testing Objective: To ensure that end service is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The admin/user needs to select a service that will be stop from VM and end the VM to perform its tasks	Ssh MySQL Http	The selected service will be stop and will not be functional	The service is stop	Pass

Table 17: Test Cases for end service

Testing Environment: Ubuntu 18, VMware, virtual box

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 018 Update service

Unit Testing 018: Update service

Testing Objective: To ensure that update service is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The admin/user can update the selected service for desired VM	Select one of the service and click on update button	The required service will be updated	The service is updated	Pass

Table 18: Test Cases for update service

Testing Environment: Ubuntu 18, virtual box

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 019 Delete service

Unit Testing 019: Delete service

Testing Objective: To ensure that delete service is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The admin/user can delete the selected service for desired VM	Select one of the service and click on delete button	The required service will be deleted	The service is deleted	Pass
2.	The user will stop the VM and its state will be changed	Ubuntu 16 server	VM will be stop	VM power off	Pass

Table 19: Test Cases for delete service

Testing Environment: Ubuntu 18, virtual box

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 020 Generate alert

Unit Testing 020: Generate alert

Testing Objective: To ensure that generate alert is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The system needs to generate an alert when user tries to intercept with one of the decoys	Sudo ssh osboxes@172.20.16.245	An alert will be generated	Alert is generated	Pass

Table 20: Test Cases for generate alert

Testing Environment: Ubuntu 18, virtual box

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 021 Send alert

Unit Testing 021: Send alert

Testing Objective: To ensure that send alert is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	When a decoy is interacted an alert is sent to admin	Sudo ssh osboxes@172.20.16.245	An alert needs to be sent	An alert is sent	Pass

Table 21: Test Cases for send alert

Testing Environment: Ubuntu 18, virtual box

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 022 View alert

Unit Testing 022: View alert

Testing Objective: To ensure that view alert is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	When an alert is generated by system that needs to be viewed by admin	Sudo service apache2 restart	An alert is viewed by admin	Admin is notified	Pass

Table 22: Test Cases for view alert

Testing Environment: Ubuntu 18, services

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 023 Delete alert

Unit Testing 023: Delete alert

Testing Objective: To ensure that delete alert is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The admin can delete the specific alerts when he/she is notified	Click on delete button to delete the specific alerts	The alerts will be deleted	The alerts get deleted	Pass

Table 23: Test Cases for delete alert

Testing Environment: Ubuntu 18, services

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 024 Make Directories

Unit Testing 024: Make Directories

Testing Objective: To ensure Make Directories is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The system make the required directories in required machine	Sudo mkdir vagrantboxes	The directories will successfully created	The directories are created successfully	Pass
2.	The system make the required directories in required machine	Sudo mkdir vagrantboxes	The directories will successfully created	Machines are not accessible	Not Executed

Table 24: Test Cases for Make Directories

Testing Environment: Ubuntu 18, services

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 025 Vpn client file creation

Unit Testing 025: Vpn client file creation

Testing Objective: To ensure that Vpn client file creation is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The controller will create a ovpn file for each client	Client.ovpn file is created	The client will be created successfully	Client.ovpn is created successfully	Pass
2.	The controller will create a ovpn file for each client	Client.ovpn file is created	The client will be created successfully	Client name is already existed. Try again	Suspended

Table 25: Test Cases for Vpn client file creation

Testing Environment: Ubuntu 18, services

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 026 Sending vpn files

Unit Testing 026: Sending vpn files

Testing Objective: To ensure that Sending vpn files is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The controller will transfer the created vpn files to ONET machine	Sending... Client.ovpn	The file has been sent to ONET machine	The file has been sent	Pass
2.	The controller will transfer the created vpn files to ONET machine	Sending... Client.ovpn	The file has been sent to ONET machine	The file is not found	Fail

Table 26: Test Cases for Sending vpn files

Testing Environment: Ubuntu 18, RYU

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 027 Add user

Unit Testing 027: Add user

Testing Objective: To ensure that add user is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The admin shall be able to add user to the system	Username=Haris Gul Password:1234567	The user will be added successfully	The user is added successfully	Pass
2.	The admin shall be able to add user to the system	Username=Haris Gul Password:	The user will not be added as the password is not mentioned	As expected	Pass

Table 27: Test Cases for add user

Testing Environment: Windows 10, Google Chrome, Firefox

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 028 Assign role

Unit Testing 028: Assign role

Testing Objective: To ensure that assign role is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The admin has the ability to assign roles to the users	Assign user as manager Press **Submit** button	The role has been assigned successfully	As expected	Pass
2.	The admin has the ability to	Press **Submit** button	The role will not be assigned	As expected	Pass

	assign roles to the users		as it is not selected		

Table 28: Test Cases for assign role

Testing Environment: Windows 10, Google Chrome, Firefox

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 029 Remove role

Unit Testing 029: Remove role

Testing Objective: To ensure that remove role is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The admin has the ability to remove role of the user	User: Haris Gul Press **Remove** button	The role has been removed from the user	As expected	Pass
2.	The admin has the ability to remove role of the user	Press **Remove** button	The role is not been removed from the user as user is not selected	As expected	Pass

Table 29: Test Cases for Remove role

Testing Environment: Windows 10, Google Chrome, Firefox

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 030 Update role

Unit Testing 030: Update role

Testing Objective: To ensure that update role is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The admin has the ability to	User: Haris Gul Role: manager Press **update** button	The role of the user has been	As Expected	Pass

	update role of a specific user		successfully updated		
2.	The admin has the ability to update role of a specific user	User: Haris Gul Press **update** button	The role of the user has not been updated as role is not been selected	As expected	Pass
3.	The admin has the ability to update role of a specific user	Role: manager Press **update** button	The role of the user has not been updated as user is not been selected	As expected	Pass

Table 30: Test Cases for update role

Testing Environment: Windows 10, Google Chrome, Firefox

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 031 Edit IP address

Unit Testing 031: Edit IP address

Testing Objective: To ensure that edit IP address is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The admin can edit the IP of the deployed VM	IP address= 172.20.16.245	The VM needs to be deployed on given IP address	The VM is deployed	Pass
2.	The admin can edit the IP of the deployed VM	IP address= 172.20.16.245	The VM needs to be deployed on given IP address	The VM is not deployed because IP is not accessible	Fail
3.	The admin can edit the IP of the deployed VM	IP address= 172.20.16.245	The VM needs to be deployed on given IP address	The VM is not deployed because IP in wrong format	Fail

Table 31: Test Cases for edit IP address

Testing Environment: Windows 10, Google Chrome, Opera

Tested by: Haris Gul

Date: February 20, 2020

Test Case: 032 Inspect IP address

Unit Testing 032: Inspect IP address

Testing Objective: To ensure that inspect IP address is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The given IP address needs to inspected to check for the format	IPaddress=172.20.16.142	The given IPaddress needs to be valid	The given IP address is valid	Pass
2.	The given IP address needs to inspected to check for the format	IPaddress=172.20.16.142	The given IPaddress needs to be valid	Not valid because in wrong format	Fail

Table 32: Test Cases for inspect IP address

Testing Environment: Windows 10, Google Chrome, Opera

Tested By:

Date: February 20, 2020

Test Case: 033 Inspect switch port

Unit Testing 033: Inspect switch port

Testing Objective: To ensure that inspect switch port is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The arriving packets need to be inspected for switch ports	Port=vxlan0	The switch packets are inspected	The switch port is inspected	Pass

Table 33: Test Cases for inspect switch port

Testing Environment: Mongo dB

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 034 Inspect Vxlan id

Unit Testing 034: Inspect Vxlan id

Testing Objective: To ensure that inspect Vxlan id is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The incoming packets ID's are needed to be inspected in order to route it to desired vxlan	incomingID=2, outgoingID=5	The ID's are inspected	Checked for specific ID's	Pass
2.	The incoming packets ID's are needed to be inspected in order to route it to desired vxlan	incomingID=2, outgoingID=5	The ID's are inspected	The packets donot arrived so ID's are not inspected	Fail

Table 34: Test Cases for inspect Vxlan id

Testing Environment: Windows 10, Google Chrome, Opera

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 035 Modify IP address

Unit Testing 035: Modify IP address

Testing Objective: To ensure that Modify IP address is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The incoming packets header IP needs to be identified in order to modified the packet	IP of every packet	Identified, checked	Identified and rerouted	Pass
2.	The incoming packets header IP needs to be	IP of every packet	Identified, checked	Packets get drop	Fail

	identified in order to modified the packet				

Table 35: Test Cases for Modify IP address

Testing Environment: Windows 10, Google Chrome, Opera

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 036 Modify destination port

Unit Testing 036: Modify destination port

Testing Objective: To ensure that modify destination port is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The incoming packets header needs to be identified in order to modified the packet	Desired port of every incoming and outgoing packet	Identified, checked	Identified and rerouted	Pass
2.	The incoming packets header needs to be identified in order to modified the packet	Desired Port of every incoming and outgoing packet	Identified, checked	Packets get drop	Fail

Table 36: Test Cases for modify destination port

Testing Environment: Windows 10, Google Chrome, Opera

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 037 Modify MAC address

Unit Testing 037: Modify MAC address

Testing Objective: To ensure that modify MAC address is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The incoming packets header needs to be identified in order to modified the packet	MAC of every incoming and outgoing packet	Identified, checked	Identified and rerouted	Pass
2.	The incoming packets header needs to be identified in order to modified the packet	MAC of every incoming and outgoing packet	Identified, checked	Packets get drop	Fail

Table 37: Test Cases for modify MAC address

Testing Environment: Windows 10, Google Chrome, Opera

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 038 Capture packet

Unit Testing 038: Capture packet

Testing Objective: To ensure that capture packet is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Once the attacker tries to interact with one of decoys, his packets will be capture	Interaction with one of the decoys	All the packets will be captured	Packets are being captured	Pass

Table 38: Test Cases for capture packet

Testing Environment: Ryu, Ubuntu

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 039 Analyze Packets

Unit Testing 039: Analyze packet

Testing Objective: To ensure that Analyze packet is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The packets of incoming and outgoing packets are needed to be analyzed to deployed VM for requested service	IPaddress=172.20.16.124 Port=22 Service=SSH MAC=cd:22:33:rw:rf:87	The packets will be analyzed for the service	The packets are analyzed	Pass
2.	The packets of incoming and outgoing packets are needed to be analyzed to deployed VM for requested service	IPaddress=172.20.16.124 Port=22 Service=SSH MAC=cd:22:33:rw:rf:87	The packets will be analyzed for the service	The packets are not analyzed because connection get terminated	Fail
3.	The packets of incoming and outgoing packets are needed to be analyzed to deployed VM for requested service	IPaddress=172.20.16.124 Port=22 Service=SSH MAC=cd:22:33:rw:rf:87	The packets will be analyzed for the service	The packets are not analyzed because packets are forwarded towards wrong IPaddress	Fail

Table 39: Test Cases for analyze packet

Testing Environment: Ryu, Ubuntu

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 040 View graph

Unit Testing 040: View graph

Testing Objective: To ensure that view graph is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Admin can successfully view graph along with manager and sub manager	Click on the dashboard button to view graph.	Admin shall see graph along with manager and sub manager.	Admin can see graph along with manager and sub manager.	pass

Table 40: Test Cases for view graph

Testing Environment: Windows 10, Google Chrome, Opera

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 041 Edit graph setting

Unit Testing 041: Edit graph setting

Testing Objective: To ensure that edit graph setting is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Admin can successfully edit graph along with manager and sub manager	Click on the dashboard button to view graph and then click on the graph to edit.	Admin shall edit graph along with manager and sub manager.	Admin can edit graph along with manager and sub manager	pass

Table 41: Test Cases for edit graph setting

Testing Environment: Windows 10, Google Chrome, Opera

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 042 Search log

Unit Testing 042: Search log

Testing Objective: To ensure that search log is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The admin will be able to search for specific logs	Search=SSH	The specific logs will be displayed	The logs are displayed	Not Executed
2.	The admin will be able to search for specific logs	Search=SSH	The specific logs will be displayed	The logs not displayed because logs are not captured	Not Executed

Table 42: Test Cases for search log

Testing Environment: Windows 10, Google Chrome, Opera

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 043 Inspect log

Unit Testing 043: Inspect log

Testing Objective: To ensure that inspect log is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The logs needed to be inspected and get suggested parameters	Service=SSH Port=22 IPaddress=172.20.16.45 MAC=22:11:55:88:33:66	The logs will be inspected	The logs are inspected	Pass

Table 43: Test Cases for inspect log

Testing Environment: Snort, Ryu

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 044 Capture log

Unit Testing 044: Capture log

Testing Objective: To ensure that capture log is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The controller needs to capture logs as soon as the attack initiate	Snort –I eth0	The logs will be started capturing	The logs are captured	Pass
2.	The controller needs to capture logs as soon as the attack initiate	Snort –I eth0	The logs will be started capturing	The logs are not captured because packets are not forwarded	Fail
3.	The controller needs to capture logs as soon as the attack initiate	Snort –I eth0	The logs will be started capturing	The logs are not captured because interface is incorrect	Fail
4.	The controller needs to capture logs as soon as the attack initiate	Snort –I eth0	The logs will be started capturing	The logs are not captured because command is not found	Fail

Table 44: Test Cases for capture log

Testing Environment: snort, Ubuntu

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 045 Filter log

Unit Testing 045: Filter log

Testing Objective: To ensure that filter log is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended

1.	The admin/user can filter the desired logs from captured logs	Logs by time	The logs are being filtered from option "time"	Filtered	Pass

Table 45: Test Cases for filter log

Testing Environment: Windows 10, Google Chrome, Opera

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 046 Analyze log

Unit Testing 046: analyze log

Testing Objective: To ensure that analyze log is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Logs needed to be analyzed to get out attacker information from it	IPaddress=172.20.16.56 MAC=11:22:33:44:55:66 Port=22 Time:22:12:33	Logs will be analyzed	Logs are analyzed	Pass
2.	Logs needed to be analyzed to get out attacker information from it	IPaddress=172.20.16.56 MAC=11:22:33:44:55:66 Port=22 Time:22:12:33	Logs will be analyzed	Not analyzed because controller is off	Fail
3.	Logs needed to be analyzed to get out attacker information from it	IPaddress=172.20.16.56 MAC=11:22:33:44:55:66 Port=22 Time:22:12:33	Logs will be analyzed	Not analyzed because service is poweroff	Fail

Table 46: Test Cases for analyze logs

Testing Environment: Windows 10, Google Chrome, Opera

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 047 Store log

Unit Testing 047: Store log

Testing Objective: To ensure that store log is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The captured logs needs to be maintained in database	Logs.json	The logs are being stored in database	Logs are stored	Pass
2.	The captured logs needs to be maintained in database	Logs.json	The logs are being stored in database	Logs are not stored because database is not accessible	Fail
3.	The captured logs needs to be maintained in database	Logs.json	The logs are being stored in database	Logs are not stored because format is incorrect	Pass

Table 47: Test Cases for store log

Testing Environment: MongoDB

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 048 View projected services health

Unit Testing 048: View projected services health

Testing Objective: To ensure that view projected services health is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The services health needs to be monitored	Service=SSH	Service is active	Service is active	Pass
2.	The services health needs to be monitored	Service=SSH	Service is active	Service is unactive	Fail

3.	The services health needs to be monitored	Service=SSH	Service is active	Service is not loaded	Fail
4.	The services health needs to be monitored	Service=SSH	Service is active	Service deployed IP is wrong	Fail

Table 48: Test Cases for view projected services health

Testing Environment: Vmware, virtualbox

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 049 View Deception VM's health

Unit Testing 049: View deception VM's health

Testing Objective: To ensure that view deception VM's health is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The VM health needs to be monitored	VM=ONET	VM is active	VM is active	Pass
2.	The VM health needs to be monitored	VM=ONET	VM is active	VM is halt	Fail
3.	The VM health needs to be monitored	VM=ONET	VM is active	VM is not loaded	Fail

Table 49: Test Cases for view deception VM's health

Testing Environment: Windows 10, Google Chrome, Virtualbox

Tested By: Haris Gul

Date: February 20, 2020

Test Case: 050 Setting unique name for vpn clients

Unit Testing 050: Setting unique name for vpn clients

Testing Objective: To ensure that Setting unique name for vpn clients is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The controller should assign unique names to each ovpn file	Client name: client	The suggested name will be assigned	The file is generated with unique name	Pass
2.	The controller should assign unique names to each ovpn file	Client name: client	The suggested name will be assigned	The name is duplicated already found	Not Executed

Table 50: Test Cases for Setting unique name for vpn clients

Testing Environment: Ryu, openvpn

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 051 Unique IP address for each vpn client

Unit Testing 051: Unique IP address for each vpn client

Testing Objective: To ensure that Unique IP address for each vpn client is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The controller should assign unique IP address to each ONET machine	IP address: 10.8.0.2	The IP address will assigned to ONET machines	The IP address is set with given value	Pass
2.	The controller should assign unique IP address to each ONET machine	IP address: 10.8.0.2	The IP address will assigned to ONET machines	The IP address is not correct	Fail

Table 51: Test Cases for Unique IP address for each vpn client

Testing Environment: Ubuntu, Ryu

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 052 Deploy HTTP service

Unit Testing 052: Deploy HTTP service

Testing Objective: To ensure that deploy HTTP service is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Deploy the http server in one of VM on both servers once deployed a http VM button is clicked	Username:root Password:toor IP:192.168.1.1	Deployed the http service in both VM's	http service is deployed	Pass
2.	Deploy the http server in one of VM on both servers once deployed a http VM button is clicked	Username:root Password:toor IP:192.168.1.265	Deployed the http service in both VM's	Not deployed because of wrong IP address	Not Executed

Table 52: Test Cases for deploy HTTP service

Testing Environment: Virtualbox, Ansible

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 053 Deploy SSH service

Unit Testing 053: Deploy SSH service

Testing Objective: To ensure that deploy SSH service is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Deploy the ssh server in one of VM on both servers once deployed a ssh VM button is clicked	Username:admin Password:toor IP:192.168.1.1	Deployed the ssh service in both VM's	Not deployed because of wrong username	Not executed

2.	Deploy the ssh server in one of VM on both servers once deployed a ssh VM button is clicked	Username:root Password:toor IP:192.168.1.1	Deployed the ssh service in both VM's	Deployed ssh service in VM from internet	pass

Table 53: Test Cases for deploy SSH service

Testing Environment: Virtualbox, Ansible

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 054 Deploy MySQL service

Unit Testing 054: Deploy MySQL service

Testing Objective: To ensure that deploy MySQL service is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	Deploy the MySQL server in one of VM on both servers once deployed a MySQL VM button is clicked	Username:root Password:toor IP:192.168.1.1	Deployed the MySQL service in both VM's	MySQL service is deployed	pass
2.	Deploy the MySQL server in one of VM on both servers once deployed a MySQL VM button is clicked	Username:root Password:root IP:192.168.1.1	Deployed the MySQL service in both VM's	Not deployed because of wrong password	Not Executed

Table 54: Test Cases for deploy MySQL service

Testing Environment: Virtualbox, Ansible

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 055 Attacker request to HTTP service

Unit Testing 055: Attacker request to HTTP service

Testing Objective: To ensure that attacker request to HTTP service is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The attacker will interact with the shadow HTTP service	http:172.20.16.245:80	Introduction page is Displayed	Introduction Page is Displayed	Pass
2.	The attacker will interact with the shadow HTTP service	http:172.20.16.245:80	Introduction page is Displayed	Page not found	Fail
3.	The attacker will interact with the shadow HTTP service	wget http:172.20.16.245:80	Fetch successful	Page not found	Fail
4.	The attacker will interact with the shadow HTTP service	wget http:172.20.16.245:80	Fetch successful	Fetch successful	Pass

Table 55: Test Cases for attacker request to HTTP service

esting Environment: Ryu, Open vSwitch, Ubuntu

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 056 Attacker request to SSH service

Unit Testing 056: attacker request to SSH service

Testing Objective: To ensure that attacker request to SSH service is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended

1.	The attacker will interact with the shadow SSH service	sudo ssh osboxes@172.20.16.45	Login successful	Login successful	Pass
2.	The attacker will interact with the shadow SSH service	sudo ssh osboxes@172.20.16.45	Login successful	Login unsuccessful, server not found	Fail

Table 56: Test Cases for attacker request to SSH service

Testing Environment: Ryu, Open vSwitch, Ubuntu

Tested By: Kawish Ali khan

Date: February 20, 2020

Test Case: 057 Attacker request to MySQL service

Unit Testing 057: Attacker request to MySQL service

Testing Objective: To ensure that attacker request to MySQL service is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The attacker will interact with the shadow MySQL service	sudo mysql –u osboxes –h 172.20.16.45	Login successful	Login successful	Pass
2.	The attacker will interact with the shadow MySQL service	sudo mysql –u osboxes –h 172.20.16.45	Login successful	Login unsuccessful	Fail

Table 57: Test Cases for attacker request to MySQL service

Testing Environment: Ryu, Open vSwitch, Ubuntu

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 058 HTTP response to attacker

Unit Testing 058: HTTP response to attacker

Testing Objective: To ensure that HTTP response to attacker is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The controller will send a response from deception http service	http:172.20.16.245:80	Login successful	Login successful	Pass
2.	The controller will send a response from deception http service	http:172.20.16.245:80	Login successful	Login unsuccessful	Fail
3.	The controller will send a response from deception http service	wget http:172.20.16.245:80	Login successful	File received	Pass

Table 58: Test Cases for HTTP response to attacker

Testing Environment: Ryu, Open vSwitch, Ubuntu

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 059 SSH response to attacker

Unit Testing 059: SSH response to attacker

Testing Objective: To ensure that SSH response to attacker is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The controller will send a response from deception ssh service	sudo ssh osboxes@172.20.16.45	Login successful	Login successful	Pass
2.	The controller will send a response from deception ssh service	sudo ssh osboxes@172.20.16.45	Login successful	Login unsuccessful, server not found	Fail

Table 59: Test Cases for SSH response to attacker

Testing Environment: Ryu, Open vSwitch, Ubuntu

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 060 MySQL response to attacker

Unit Testing 060: MySQL response to attacker

Testing Objective: To ensure that MySQL response to attacker is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The controller will send a response from deception mysql service	sudo mysql –u osboxes –h 172.20.16.45	Login successful	Login successful	Pass
2.	The controller will send a response from deception mysql service	sudo mysql –u osboxes –h 172.20.16.45	Login successful	Login unsuccessful	Fail

Table 60: Test Cases for MySQL response to attacker

Testing Environment: Ryu, Open vSwitch, Ubuntu

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 061 Start VM

Unit Testing 061: Start VM

Testing Objective: To ensure that start VM is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The admin/user will select a VM and that will be deployed with selected service	Ubuntu 16 with ssh service	VM will be deployed	Deployed	Pass
2.	The user can start the VM	Ubuntu 16 server	The VM will be started	VM's started	Pass

	from already deployed VM's				
3.	The user can start the VM from already deployed VM's	Ubuntu 16 server	The VM will be started	VM's not started because of wrong IP address	Not Executed

Table 61: Test Cases for start VM

Testing Environment: Ansible, virtualbox

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

Test Case: 062 Restart VM

Unit Testing 062: Restart VM

Testing Objective: To ensure that restart VM is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The user needs to restart the VM so that it changes its state	Ubuntu 16 server	The VM will be restarted	VM restarted	Pass
2.	The user needs to restart the VM so that it changes its state	Ubuntu 16 server	The VM will be restarted	VM is poweroff	Fail
3.	The user needs to restart the VM so that it changes its state	Ubuntu 16 server	The VM will be restarted	VM is not accessible	Fail

Table 62: Test Cases for restart VM

Testing Environment: Ansible, virtualbox

Tested By: Taimoor faraz Butt

Date: February 20, 2020

Test Case: 063 Send packet by Open vSwitch

Unit Testing 063: Send packet by Open vSwitch

Testing Objective: To ensure that send packet by Open vSwitch is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The packets needs to be routed between different OVS instances	Packets	Packets get rerouted	Packets get rerouted	Pass
2.	The packets needs to be routed between different OVS instances	Packets	Packets get rerouted	Packets get drops	Fail
3.	The packets needs to be routed between different OVS instances	Packets	Packets get rerouted	Packets get drops, no tunnel found	Fail

Table 63: Test Cases for send packet by Open vSwitch

Testing Environment: Ryu,, Open vSwitch

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 064 Send packet by Controller

Unit Testing 064: Send packet by Controller

Testing Objective: To ensure that send packet by Controller is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The controller needs to send the flows to OVS instances	Openflow packets	Flows are dumped	Flows are dumped	Pass
2.	The controller needs to send the flows to OVS instances	Openflow packets	Flows are dumped	OVS instance is not connected	Fail
3.	The controller needs to send	Openflow packets	Flows are dumped	Flows are in wrong format	Fail

	the flows to OVS instances				
4.	The controller needs to send the flows to OVS instances	Openflow packets	Flows are dumped	Wrong OVS instance is connected	Fail
5.	The controller needs to send the flows to OVS instances	Openflow packets	Flows are dumped	Flows are incomplete	Fail

Table 64: Test Cases for send packet by Controller

Testing Environment: Ryu, open vSwitch

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 065 Receive packet by Open vSwitch

Unit Testing 065: Receive packet by Open vSwitch

Testing Objective: To ensure that receive packet by Open vSwitch is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The OVS instance needs to receive the packets from controller	Packets	Reply is sent	Reply is sent	Pass
2.	The OVS instance needs to receive the packets from controller	Packets	Reply is sent	Waiting for reply	Fail

Table 65: Test Cases for receive packet by Open vSwitch

Testing Environment: Ryu, open vSwitch

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 066 Receive packet by controller

Unit Testing 066: receive packet by controller

Testing Objective: To ensure that receive packet by controller is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The packets forwarded by ovs instance needs to be listened by controller	Openflow packets	Packet received	Packet received	Pass
2.	The packets forwarded by ovs instance needs to be listened by controller	Openflow packets	Packet received	Waiting for reply	Fail
3.	The packets forwarded by ovs instance needs to be listened by controller	Openflow packets	Packet received	Packets get drop	Fail
4.	The packets forwarded by ovs instance needs to be listened by controller	Openflow packets	Packet received	Packets are forwarded to wrong IP	Fail

Table 66: Test Cases for receive packet by controller

Testing Environment: Ryu, open vSwitch

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 067 Scan the network

Unit Testing 067: Scan the network

Testing Objective: To ensure that Scan the network is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended

1.	The controller needs to scan the network to look for potential services	Nmap – 192.168.0.1/24	Network will be scan	Network is scan	Pass
2.	The controller needs to scan the network to look for potential services	Nmap – 192.168.8.1/24	Network will be scan	Wrong ip range is taken	Fail

Table 67: Test Cases for Scan the network by Open vSwitch

Testing Environment: Ryu, Nmap

Tested By: Kawish Ali Khan

Date: February 20, 2020

Test Case: 068 Sending scan data

Unit Testing 068: Sending scan data

Testing Objective: To ensure that Sending scan data is working successfully.

Test Scenario:

No.	Test Case/Test Script	Test Data	Expected Result	Actual Result	Pass/Fail/Not Executed/ Suspended
1.	The controller should sent the scan data report to dashboard to be understand by admin	{“IP”:”192.168.10.55”, “services”:”SSH,HTTP”}	The data will be successfully sent	As expected	Pass
2.	The controller should sent the scan data report to dashboard to be understand by admin	{“IP”:”192.168.10.55”, “services”:”SSH,HTTP”	The data will be successfully sent	The format is wrong, check it again	Fail

Table 68: Test Cases for Sending scan data by Open vSwitch

Testing Environment: Ryu, Nmap, Windows 10, google chrome

Tested By: Taimoor Faraz Butt

Date: February 20, 2020

6.1.3 Functional Testing

The functional testing will take place after the unit testing. In this functional testing, the functionality of each of the module is tested. This is to ensure that the system produced meets the specifications and requirements.

Functional Testing 1: Login with different roles
Objective: To ensure that different users have login successfully.

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The user will login as manager, sub-manager, admin	Username: admin Password: admin	The desired dashboard needs to be shown	pass
2.	The user will login as manager, sub-manager, admin	Username: admin Password: user	Error is shown to user	Pass

Functional Testing 2: Scan network
Objective: To scan the whole network and look for potential services

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The controller shall scan the whole network and find the services onto which VM's needed to be deployed upon user call's	IP address: 192.168.0.1/24	The network will be scan for potential services	Pass
2.	The controller shall scan the whole network and find the services onto which VM's needed to be deployed upon user call's	IP address: 192.168.0.1/24	The network will be scan for not potential services as network is not accessible	Pass

Functional Testing 3: Add a department
Objective: To ensure that multiple departments can easily be added

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The user shall request for a new department to be added.	Username: admin Password: admin IPaddress: 192.168.0.15	The desired department is added and configured	pass
2.	The user shall request for a new department to be added.	Username: admin Password: admin	The desired department is	Fail

		IPaddress: 192.168.0.259	added and configured	

Functional Testing 4: Add a VM
Objective: To ensure that a VM can easily be added to department

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The user shall request for a new VM to be added in already configured departments	Username: admin Password: admin IPaddress: 192.168.0.15 Service: SSH	The desired VM is added and configured	pass
2.	The user shall request for a new VM to be added.	Username: admin Password: admin IPaddress: 192.168.0.259 Service: SSH	The desired department is added and configured	Fail

Functional Testing 5: Enable Routing between machines
Objective: To ensure that a VM can easily be added to department

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The controller shall enable routing between corresponding machines with desired credentials	Incoming IP: 192.168.10.15 Outgoing IP: 192.168.10.16 In-port: 1 Outport: 2	The traffic needs to be rotated	pass
2.	The controller shall enable routing between corresponding machines with desired credentials	Incoming IP: 192.168.10.15 Outgoing IP: 192.168.10.16 In-port: 1 Outport: 2	The traffic needs to be rotated	Fail

Functional Testing 6: Enable log Engine
Objective: To ensure that a logs are being captured correctly

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The user shall start the log engine to start capturing the logs	Logs	The logs are being captured	pass
2.	The user shall start the log engine to start capturing the logs	logs	The logs are being captured	Fail b/c the listening on wrong port

Functional Testing 7: Sent logs to MongoDB
Objective: To ensure that a logs are being captured correctly

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The controller shall send all the desired logs to MongoDB database	Date: 18/6/2020 Time: 3:42 Protocol: icmp Attack type: flood	Data has been stored	pass
2.	The controller shall send all the desired logs to MongoDB database	Date: 18/6/2020 Time: 3:42 Protocol: icmp Attack type: flood	Data has been stored	Fail, Database is not running

Functional Testing 8: View data on dashboard
Objective: To ensure that a logs are being captured correctly

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The user shall be able to view all the data on dashboard of an intrusion attack	Date: 18/6/2020 Time: 3:42 Protocol: icmp Attack type: flood	The data is shown on dashboard	Pass
2.	The user shall be able to view all the data on dashboard of an intrusion attack	Date: 18/6/2020 Time: 3:42 Protocol: icmp Attack type: flood	The data is not shown as the database is empty	Pass

Functional Testing 9: Sending alerts to dashboard
Objective: To ensure that a logs are being captured correctly

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The controller shall send an alert whenever an intrusion tries to infiltrate our machine	Date: 18/6/2020 Time: 3:42 IP address: 192.168.10.5	The data sent to dashboard and is shown	Pass
2.	The controller shall send an alert whenever an intrusion tries to infiltrate our machine	Date: 18/6/2020 Time: 3:42 IP address: 192.168.10.5	Attacker didn't interact with our machines so no alert is generated	Pass

Functional Testing 10: Logout with different roles
Objective: To ensure that different users have logout successfully

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The user will logout as manager, sub-manager, admin	Signut button	The user have successfully logout	pass

2.	The user will logout as manager, sub-manager, admin	Signout button	The user have not successfully logout	Pass

6.1.4 **Integration Testing**

Integration Testing 1: ONET configuration
Objective: To ensure that ONET configuration is working successfully.

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The user will request will required details to deploy a switch configuration	Account: Cyberlab IP: 192.168.10.11 Password: 1234657	The configuration is done successfully	Pass
2.	The user will request will required details to deploy a switch configuration	Account: Cyberlab IP: 192.168.10.11 Password: 1234657 Service: "SSH"	The configuration is done successfully	Pass

Integration Testing 2: Tunnel Creation
Objective: To ensure that Tunnel Creation is working successfully.

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The controller will quickly make the necessary tunnels and make connections on the spot	Network port= eth0 IP=192.168.1.16	The Tunnel will be constructed easily	Pass
2.	The controller will quickly make the necessary tunnels and make connections on the spot	Network port= eth0 IP=192.168.1.16	The port is not found on device	Pass

Integration Testing 3: Vagrant Configuration
Objective: To ensure that Vagrant Configuration is working successfully.

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The controller will make interaction with deployed VM's in the network and fetch information from it	Vagrant init –file –provider	The vagrant VM's are updated	Pass
2.	The controller will make interaction with deployed VM's in the	Vagrant init –file –provider	The file location is not entered correctly	Pass

	network and fetch information from it			

Integration Testing 4: Open vSwitch setup
Objective: To ensure that Open vSwitch setup is working successfully.

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The controller will setup the whole connection with open vSwitch and also setup the Routing Table flows along with transferring data	Datapath.id = 0x0072fd88e9	The flow rules are updated correctly	Pass
2.	The controller will setup the whole connection with open vSwitch and also setup the Routing Table flows along with transferring data	Datapath.id = 0x0072fd88	The flows are not set as the id is wrong	Pass

Integration Testing 5: snort logs engine
Objective: To ensure that snort logs engine is working successfully.

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The controller will setup the snort to enable it to capture logs from ports and log it	Snort --start	The logs are capturing as it needed	Pass
2.	The controller will setup the snort to enable it to capture logs from ports and log it	Snort --start	The logs are not captured as the snort is not listening on right interface	Pass

Integration Testing 6: MongoDB interaction testing
Objective: To ensure that MongoDB interaction testing is working successfully.

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The program data is logged and captured in MongoDB in order to access it	{“username”:”cyberlab”, ”IP”:”192.168.0.15”}	The data is being entered correctly	Pass
2.	The program data is logged and captured in MongoDB in order to access it	{“username”:cyberlab, ”IP”:”192.168.0.455”}	The format is wrong so data is not entered	Pass

Integration Testing 6: Alerts Notification
Objective: To ensure that alerts notification testing is working successfully.

No.	Test Case/Test Script	Attribute and value	Expected Result	Result
1.	The controller will send alerts to dashboard whenever an attack is happened	Date: 19/6/2020 Time: 1:50 IP: 192.168.0.15	The alert is sent to dashboard	Pass
2.	The controller will send alerts to dashboard whenever an attack is happened	Date: 19/6/2020 Time: 1:50 IP: 192.168.0.15	The alert is not passed as the internet was not working.	Pass

6.2 Automated Testing:

6.2.1 Tools used:

Tool Name	Tool Description	Applied on [list of related test cases / FR / NFR]	Results
Hping3	hping is a free packet generator and analyzer for the TCP/IP protocol distributed by Salvatore Sanfilippo. It is a one type of a tester for network security.	Attacker request to SSH service SSH response to attacker	Pass
Nmap	Nmap is a free and open-source network scanner. Nmap is used to discover hosts and services on a computer network by sending packets	Scan the network Scan Data accumulation Sending scan data	Pass

7. Conclusion and Future Work

7.1 Conclusion

In short, our proposed solution is helpful for many organizations who specifically work on our focused services. This system will scan the network and suggest the admin about service deployment and then the system will make the services available in network and any attempt on these services will divert the intruder to a separate machine with similar configuration which lies outside the organization network and hence this system will help the organization to track the movement of the attacker in the network.

7.2 Future Work

As this is an industrial project so it is up to them whether they want to enhance the project or they wanted to stay with the current version. The source code of our project is available on GitHub and the repositories of both front end and back end are there if anyone wants to collaborate with us or want to improve our code then he/she is welcome from our side.

8. References

Cybersecurity, F. (n.d.). *10 Deployment Considerations for Your Deception Strategy.*

Cybersecurity, F. (n.d.). 4 Keys to Automating Threat Detection, Threat Hunting and Response.

Cybersecurity, F. (n.d.). Capture the Flag With Deception Defenses.

Cybersecurity, F. (n.d.). Fidelis Endpoint: A Technical Deep Dive.

Cybersecurity, F. (n.d.). Network DLP Buyer's Guide.

Cybersecurity, F. (n.d.). Overcoming Detection Gaps of Deep Packet Inspection Tools.

Cybersecurity, F. (n.d.). Prevent Threats and Data Loss in Proxied Web Traffic. *Fidelis Network Web Sensor*.

Cybersecurity, F. (n.d.). See More Across Your Environment: Align Visibility for Post-Breach Detection and Response.

Cybersecurity, F. (n.d.). Utilizing Deception for Effective Breach Detection.

Cybersecurity, F. (n.d.). What's Hiding Within Your Metadata.

Mohammad, H. A., & Spafford, E. H. (n.d.). Cybersecurity Deception. 29.

Rouse, M. (2016, August). *Docker Swarm* . Retrieved from Search it Operation:

https://searchitoperations.techtarget.com/definition/Docker-Swarm

Technologies, A. (2017). *Definitive Guide to Deception 2.0.* Acalvio Technologies.

Technologies, A. (n.d.). Three Minutes Until the Apocalypse.

https://ryu.readthedocs.io/en/latest/

Acalvio_Deception_Cyberdefense_Manual

Acalvio_WP___Three_Minutes_Until_the_Apocalypse

https://www.opennetworking.org/

https://en.wikipedia.org/wiki/NETCONF

https://en.wikipedia.org/wiki/OpenFlow