# Network Incident Response and Management

## Module 14

Lab 1

# Working with Incident Tickets in OSSIM

*OSSIM (Open Source Security Information Management) is an open source security information and event management system.*

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

## Lab Scenario

A ticket is an element of AlienVault that contains information about detected alarms or any other issues that you want to track in a workflow. Tickets can be used to delegate tasks to other administrators and to track the progress of investigations into specific alarms and events. Tickets can be created or opened in a number of ways either manually or automatically.

As a chief network defense architect, you need to know how to create or open tickets that are generated in AlienVault OSSIM.

## Lab Objectives

The objective of this lab is to demonstrate how to create or open tickets that are generated in AlienVault OSSIM.

## Lab Environment

To carry out the lab, you need:

- OSSIM virtual machine
- A virtual machine running Windows Server 2012
- A Web browser with an Internet connection
- **Administrative** privileges to run tools

## Lab Duration

Time: 15 Minutes

## Overview of OSSIM

OSSIM (Open Source Security Information Management) is an open source security information and event management system which is integrated with a

selection of tools designed to aid network administrators in computer security, intrusion detection, and prevention.

## Lab Tasks

**TASK 1**

**Login to OSSIM**

1. Start the **OSSIM Server** and login with **root** and **toor** as the credentials.

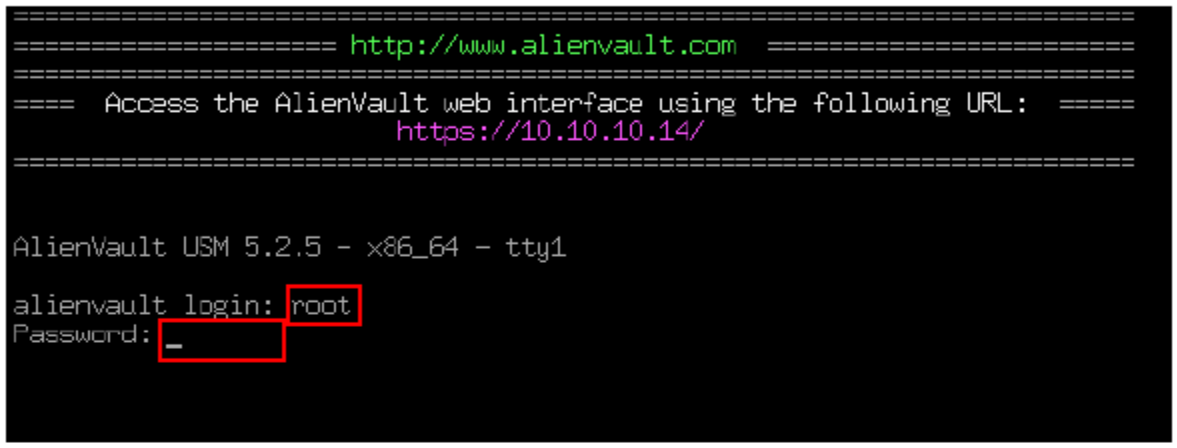


FIGURE 1.1: Logging in to alien vault

2. Launch **Windows Server 2012**. Open a web browser and type https://10.10.10.14 in the address bar and press Enter.
3. Login to **OSSIM** with **admin** and **qwerty@123** as the credentials.

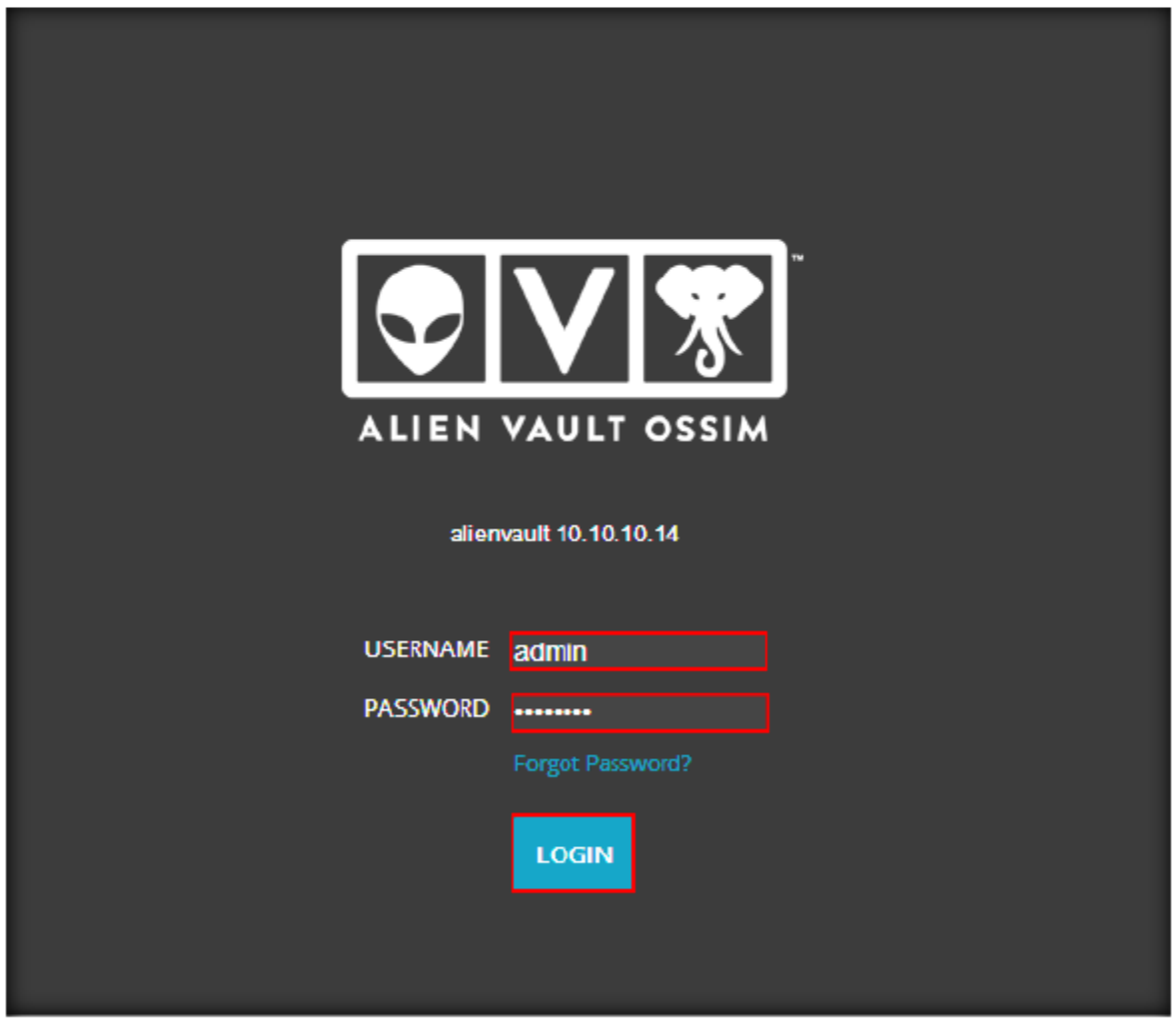


FIGURE 1.2: Logging in to OSSIM

**TASK 2**

**Create or Open Tickets**

4. Hover the mouse on **ANALYSIS** and click **TICKETS**.

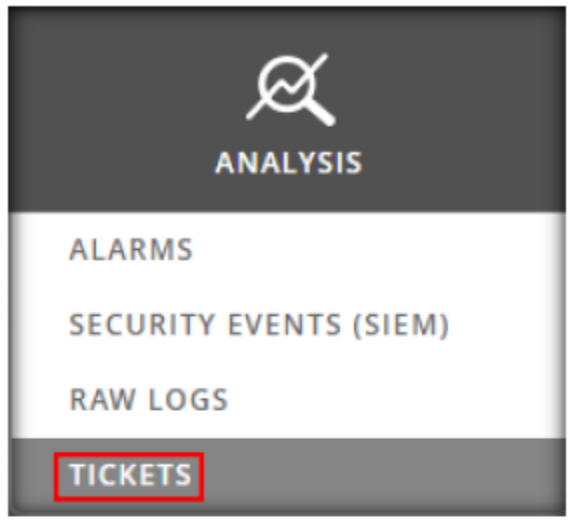


FIGURE 1.3: Navigating to Tickets

5. The existing tickets can be viewed.

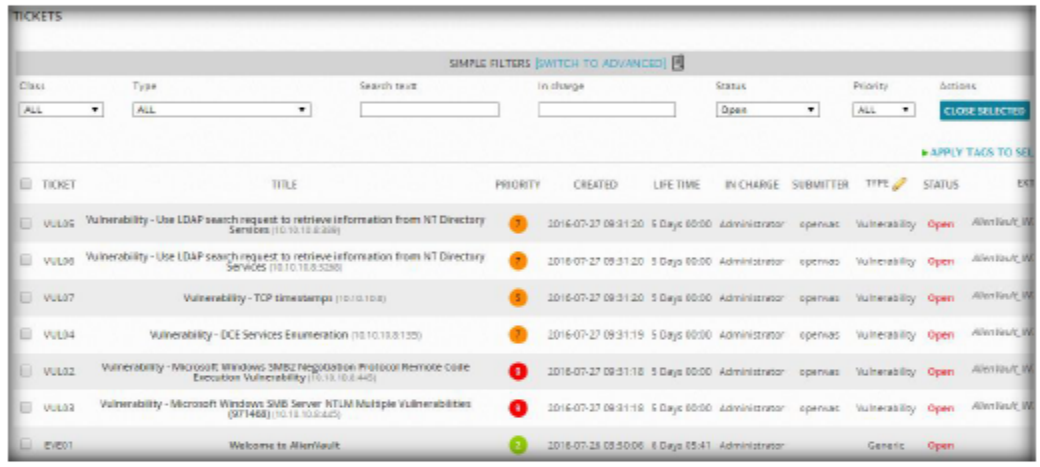


FIGURE 1.4: Viewing the tickets

6. To manually open a ticket, scroll down and select a class then click **CREATE**.

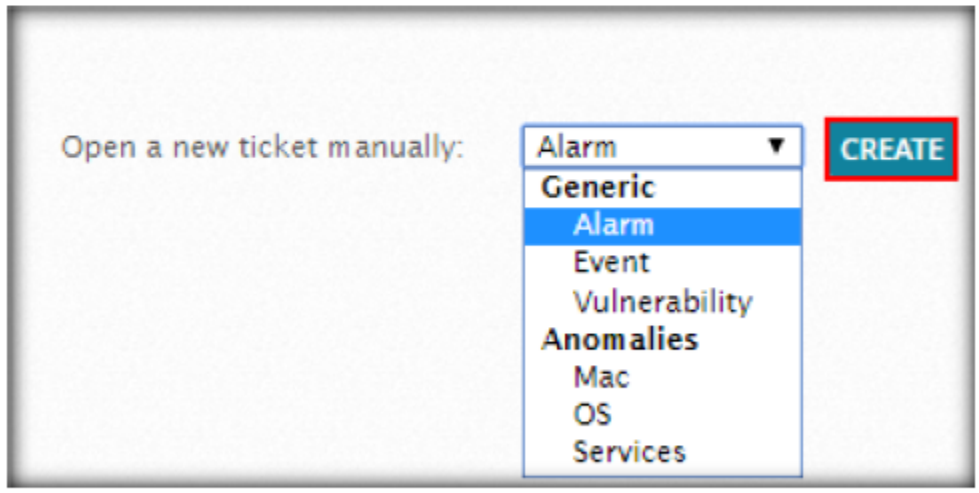


FIGURE 1.5: Creating ticket

7. Enter the highlighted details and click **SAVE**.

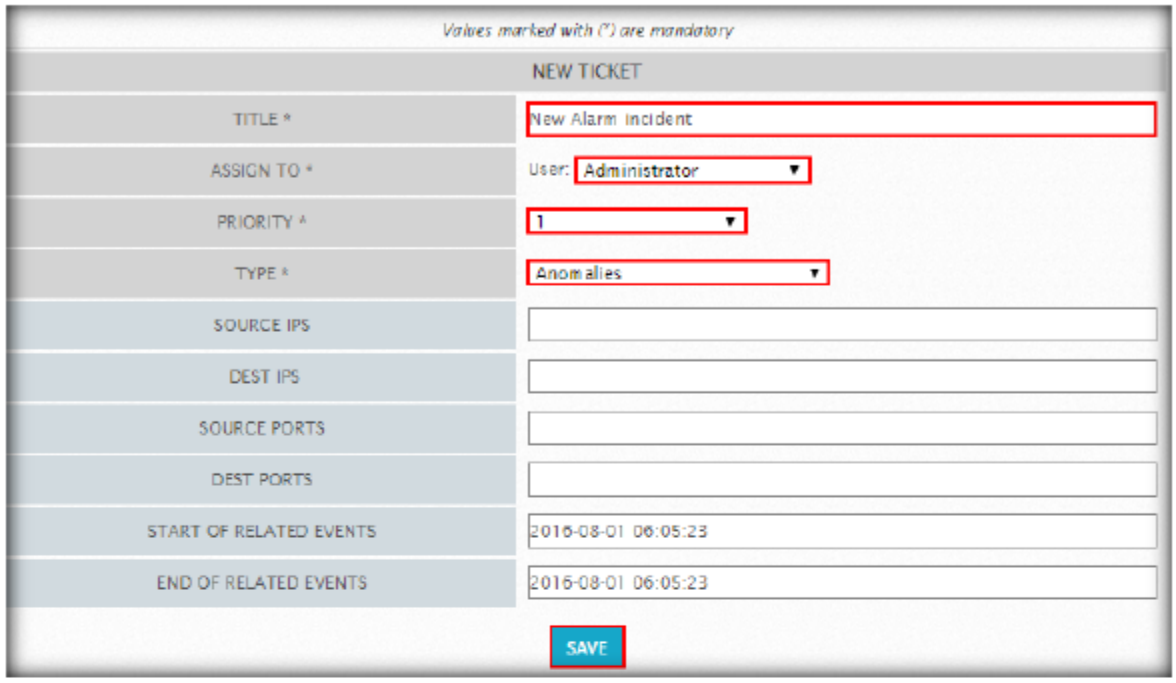


FIGURE 1.6: Entering the ticket details

8. You can see the new ticket details.

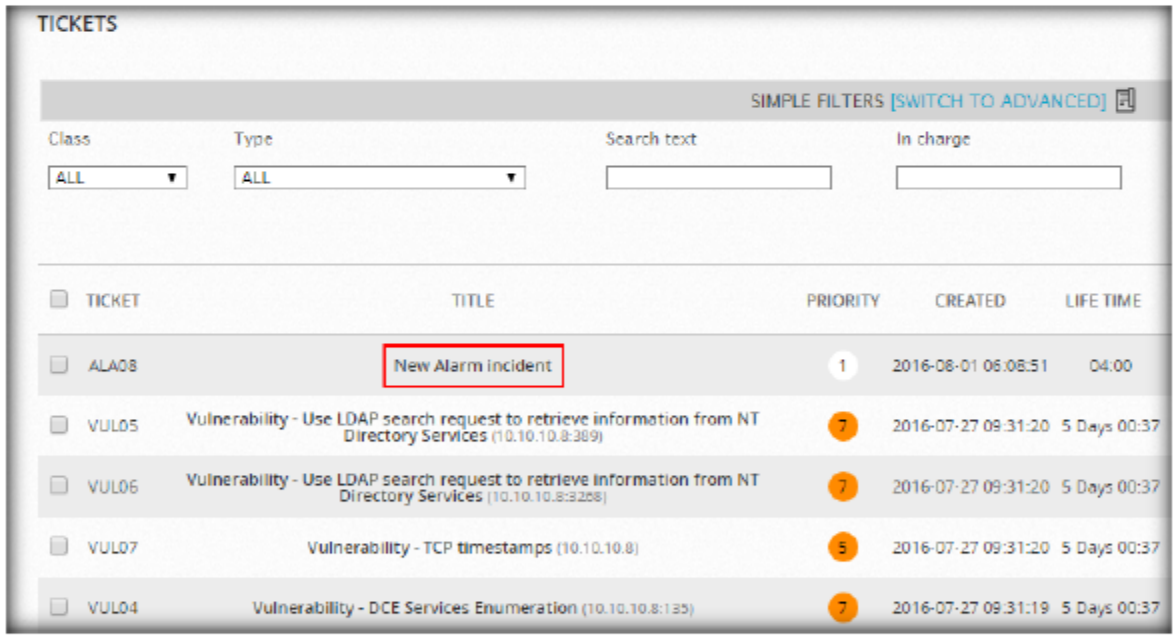


FIGURE 1.7: New ticket created

9. Tickets can be filtered based on a particular class of events using the **Class** drop down menu.

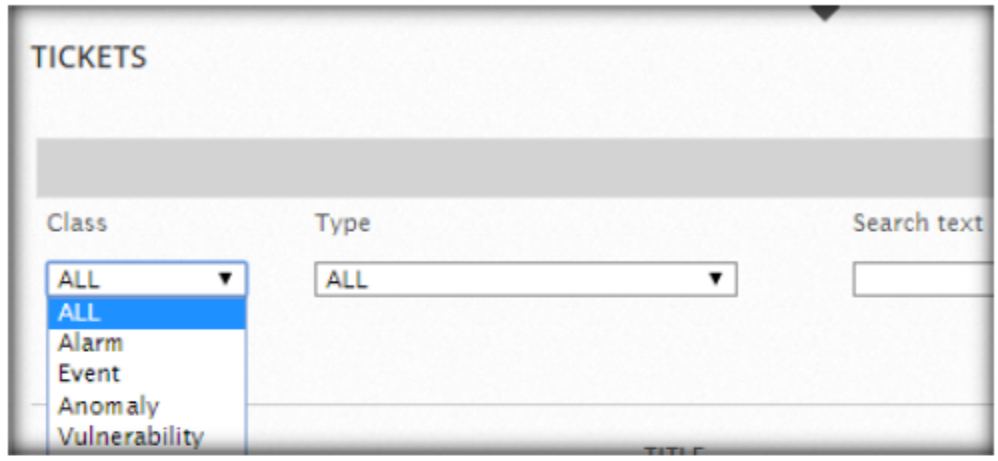


FIGURE 1.8: Filtering tickets

10. You can also select a particular type within a Class from the **Type** drop down menu.

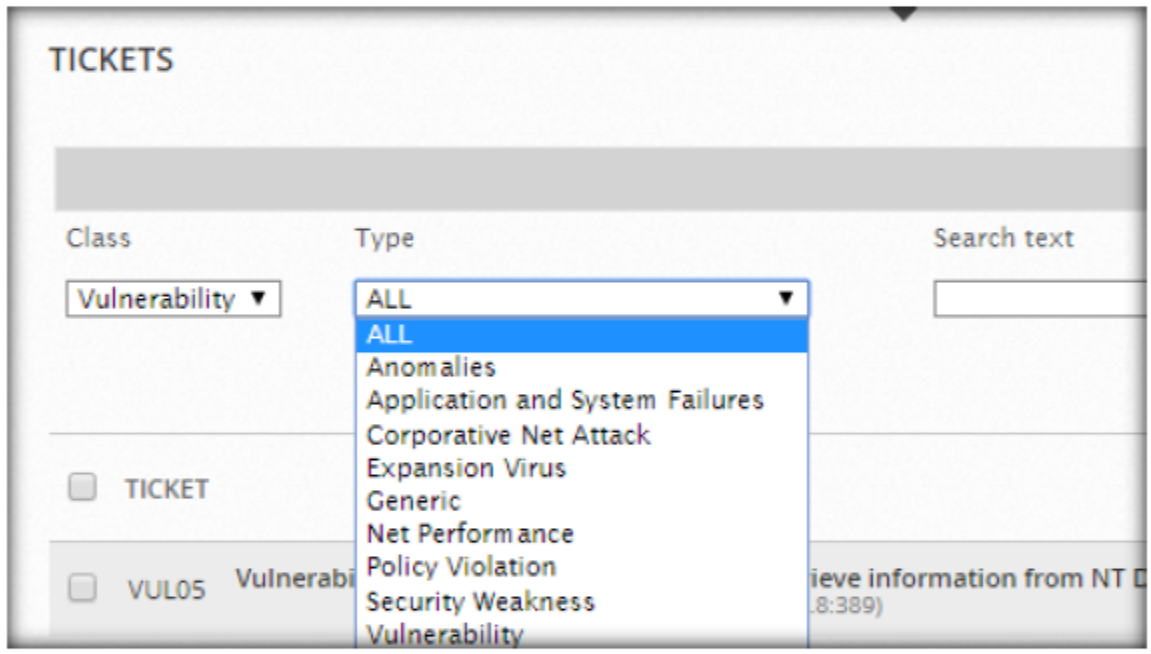


FIGURE 1.9: Selecting the type of document

11. Click any ticket to view its details and edit it.

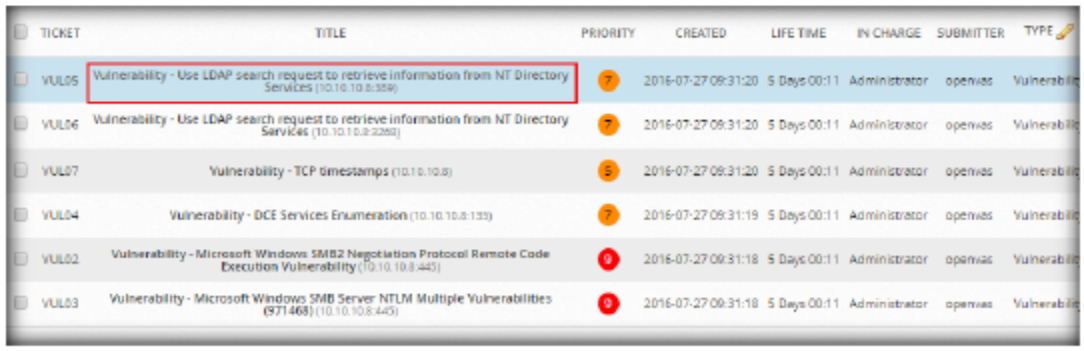


FIGURE 1.10: Viewing a ticket in detail

12. The **TICKET DETAILS** page comes up.


FIGURE 1.11: ticket details

13. Scroll down and make changes to the ticket, then click **SAVE TICKET**.

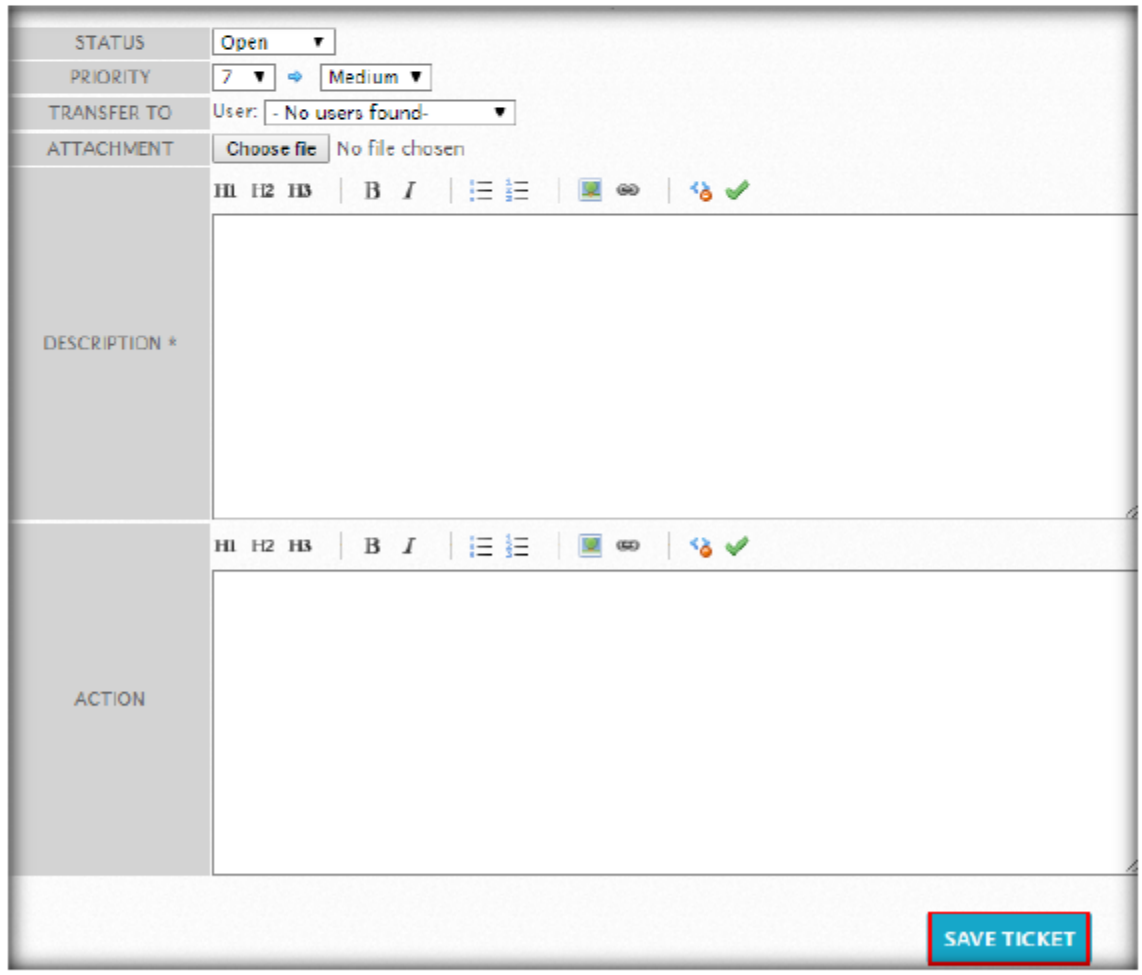


FIGURE 1.12: Edit and save ticket

# Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

| Internet Connection Required | |
|---|---|
| ☐ Yes | ☑ No |
| **Platform Supported** | |
| ☑ Classroom | ☑ iLabs |