

**Network Incident
Response and
Management**


Module 14





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.

```
===== http://www.alienvault.com =====
=====
==== Access the AlienVault web interface using the following URL: =====
                https://10.10.10.14/
=====

AlienVault USM 5.2.5 - x86_64 - tty1

alienvault login: root
Password: _
```

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.

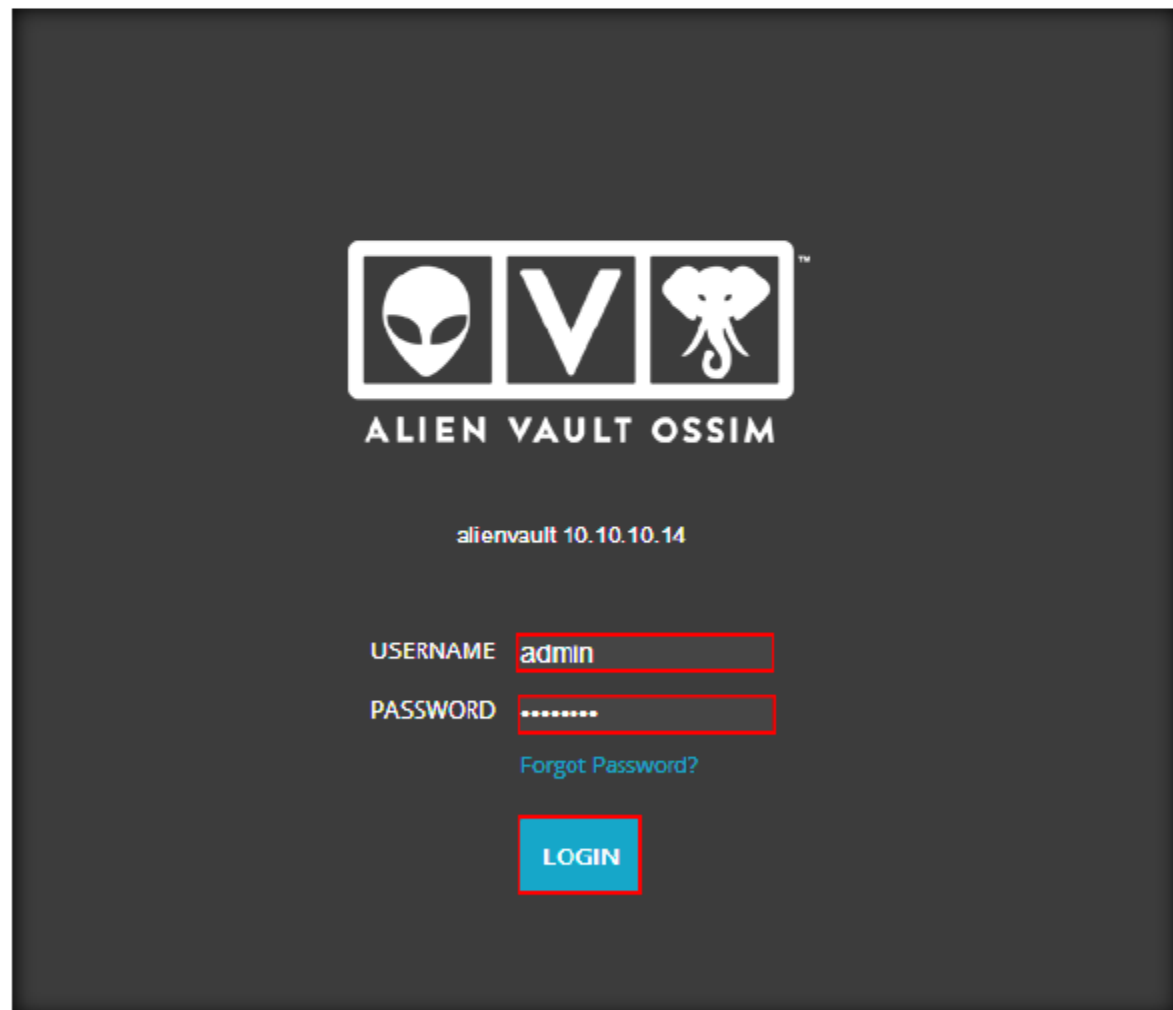


FIGURE 1.2: Logging in to OSSIM

TASK 2
Create or Open Tickets

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

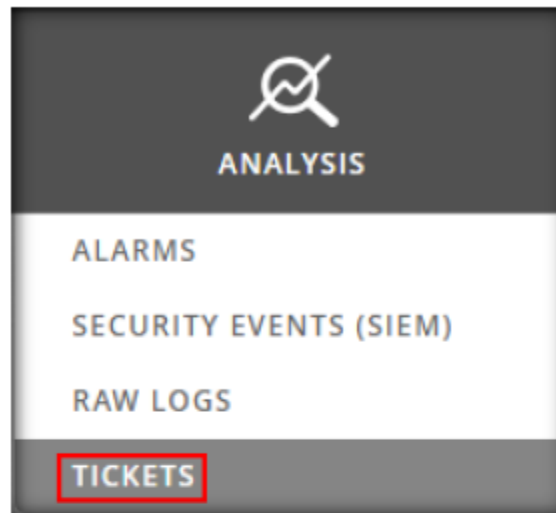


FIGURE 1.3: Navigating to Tickets

5. The existing tickets can be viewed.

A screenshot of the 'TICKETS' page. At the top, there are filter options for 'Class' (set to 'ALL'), 'Type' (set to 'ALL'), 'Search text', 'In charge', 'Status' (set to 'Open'), and 'Priority' (set to 'ALL'). A 'CLOSE SELECTED' button is visible. Below the filters is a table of tickets with columns: TICKET, TITLE, PRIORITY, CREATED, LIFE TIME, IN CHARGE, SUBMITTER, TYPE, STATUS, and EXT. The table contains several rows of vulnerability tickets and one 'EVE01' ticket.

TICKET	TITLE	PRIORITY	CREATED	LIFE TIME	IN CHARGE	SUBMITTER	TYPE	STATUS	EXT
VUL35	Vulnerability - Use LDAP search request to retrieve information from NT Directory Services (10.10.10.220)	3	2016-07-27 09:31:20	5 Days 00:00	Administrator	openstc	Vulnerability	Open	Alert/Inc, W
VUL36	Vulnerability - Use LDAP search request to retrieve information from NT Directory Services (10.10.10.220)	3	2016-07-27 09:31:20	5 Days 00:00	Administrator	openstc	Vulnerability	Open	Alert/Inc, W
VUL37	Vulnerability - TCP timestamps (10.10.10.8)	3	2016-07-27 09:31:20	5 Days 00:00	Administrator	openstc	Vulnerability	Open	Alert/Inc, W
VUL34	Vulnerability - DCE Services Enumeration (10.10.10.8120)	3	2016-07-27 09:31:19	5 Days 00:00	Administrator	openstc	Vulnerability	Open	Alert/Inc, W
VUL32	Vulnerability - Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability (10.10.10.6440)	3	2016-07-27 09:31:18	5 Days 00:00	Administrator	openstc	Vulnerability	Open	Alert/Inc, W
VUL33	Vulnerability - Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468) (10.10.10.8125)	3	2016-07-27 09:31:18	5 Days 00:00	Administrator	openstc	Vulnerability	Open	Alert/Inc, W
EVE01	Welcome to AlienVault	3	2016-07-28 03:50:06	8 Days 15:41	Administrator		Generic	Open	

FIGURE 1.4: Viewing the tickets

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

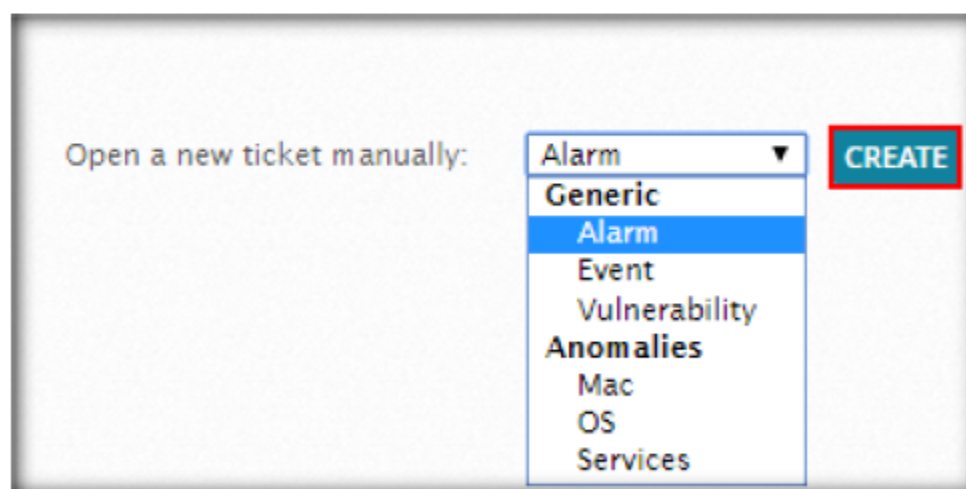


FIGURE 1.5: Creating ticket

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

Values marked with () are mandatory*

NEW TICKET	
TITLE *	<input type="text" value="New Alarm incident"/>
ASSIGN TO *	User: <input type="text" value="Administrator"/>
PRIORITY *	<input type="text" value="1"/>
TYPE *	<input type="text" value="Anomalies"/>
SOURCE IPS	<input type="text"/>
DEST IPS	<input type="text"/>
SOURCE PORTS	<input type="text"/>
DEST PORTS	<input type="text"/>
START OF RELATED EVENTS	<input type="text" value="2016-08-01 06:05:23"/>
END OF RELATED EVENTS	<input type="text" value="2016-08-01 06:05:23"/>

FIGURE 1.6: Entering the ticket details

8. You can see the new ticket details.

TICKETS

SIMPLE FILTERS [\[SWITCH TO ADVANCED\]](#)

Class: Type: Search text: In charge:

TICKET	TITLE	PRIORITY	CREATED	LIFE TIME
<input type="checkbox"/> ALA08	<input type="text" value="New Alarm incident"/>	1	2016-08-01 06:08:51	04:00
<input type="checkbox"/> VUL05	Vulnerability - Use LDAP search request to retrieve information from NT Directory Services (10.10.10.8:389)	7	2016-07-27 09:31:20	5 Days 00:37
<input type="checkbox"/> VUL06	Vulnerability - Use LDAP search request to retrieve information from NT Directory Services (10.10.10.8:3268)	7	2016-07-27 09:31:20	5 Days 00:37
<input type="checkbox"/> VUL07	Vulnerability - TCP timestamps (10.10.10.8)	5	2016-07-27 09:31:20	5 Days 00:37
<input type="checkbox"/> VUL04	Vulnerability - DCE Services Enumeration (10.10.10.8:135)	7	2016-07-27 09:31:19	5 Days 00:37

FIGURE 1.7: New ticket created

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

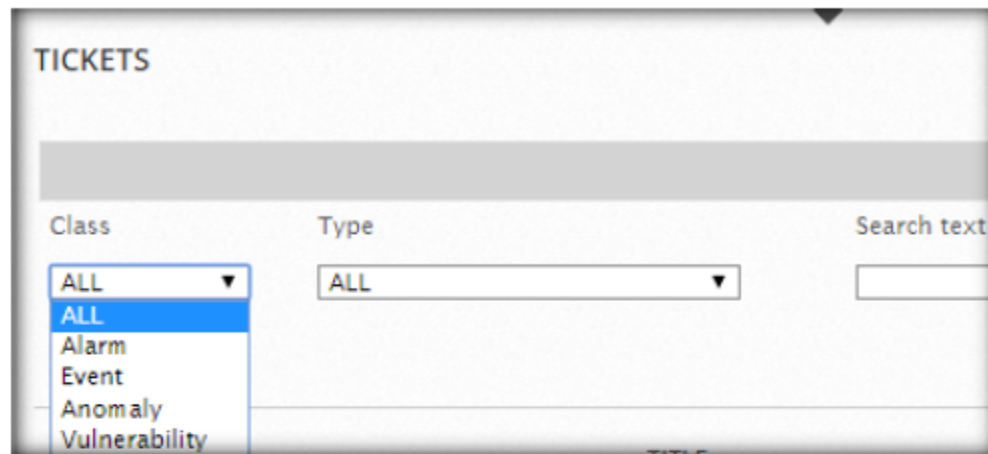


FIGURE 1.8: Filtering tickets

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

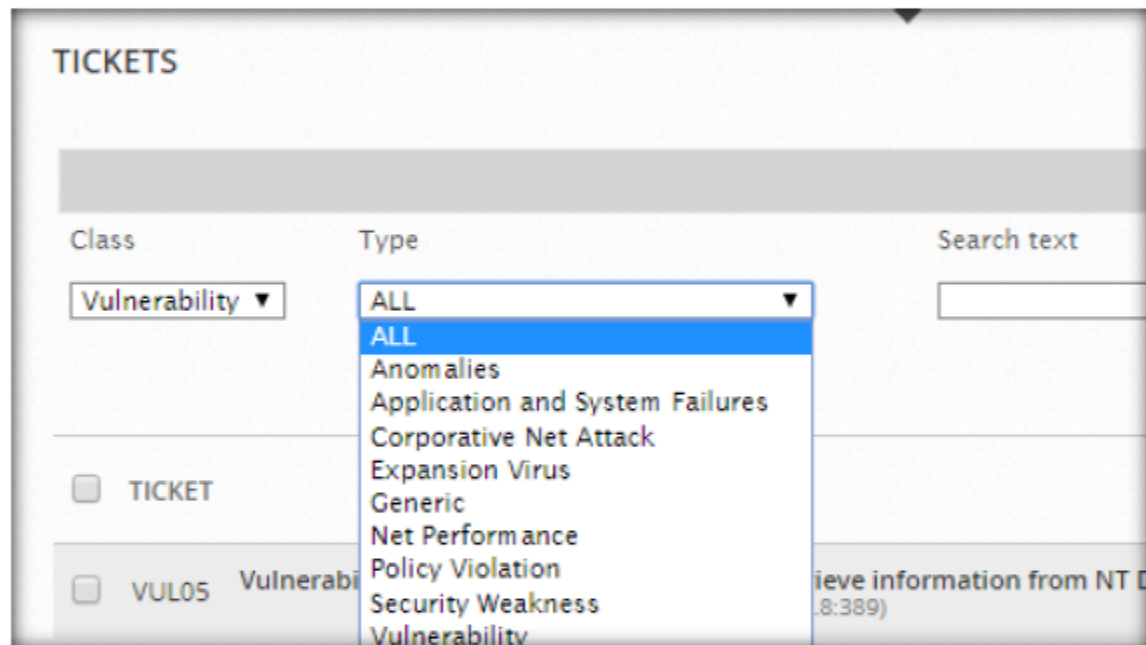


FIGURE 1.9: Selecting the type of document

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

TICKET	TITLE	PRIORITY	CREATED	LIFE TIME	IN CHARGE	SUBMITTER	TYPE
VUL05	Vulnerability - Use LDAP search request to retrieve information from NT Directory Services (10.10.10.8:389)	7	2016-07-27 09:31:20	5 Days 00:11	Administrator	openvas	Vulnerability
VUL06	Vulnerability - Use LDAP search request to retrieve information from NT Directory Services (10.10.10.8:389)	7	2016-07-27 09:31:20	5 Days 00:11	Administrator	openvas	Vulnerability
VUL07	Vulnerability - TCP timestamps (10.10.10.8)	5	2016-07-27 09:31:20	5 Days 00:11	Administrator	openvas	Vulnerability
VUL04	Vulnerability - DCE Services Enumeration (10.10.10.8:135)	7	2016-07-27 09:31:19	5 Days 00:11	Administrator	openvas	Vulnerability
VUL02	Vulnerability - Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability (10.10.10.8:445)	9	2016-07-27 09:31:18	5 Days 00:11	Administrator	openvas	Vulnerability
VUL03	Vulnerability - Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468) (10.10.10.8:445)	9	2016-07-27 09:31:18	5 Days 00:11	Administrator	openvas	Vulnerability

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**.

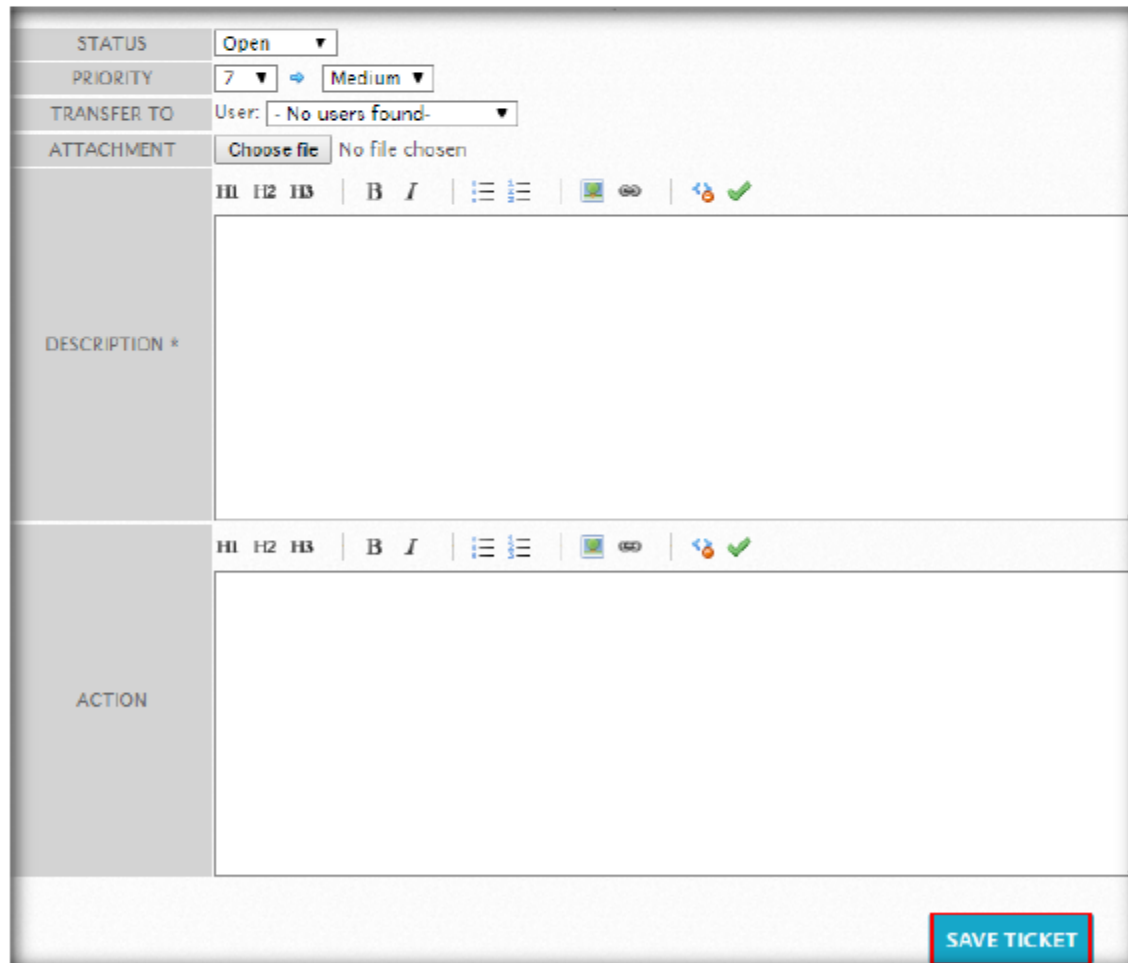


FIGURE 1.12: Edit and save ticket

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs