**CIT 485 ADVANCED CYBERSECURITY-**

**Lab3: Vulnerability Scanners**

The purpose of this lab is:

**Lab3-1: Infrastructure Vulnerability Scanners**

After completing this lab, you will be able to:

* Perform a Scan Using the following scanners:
* Nessus
* OpenVAS

**Lab3-2: Web Application Scanners and Vulnerability Identification and Remediation**

After completing this lab, you will be able to:

* Use OWASP Zed Attack Proxy (ZAP)
* Use Nikto
* Install Updates Manually
* Enable Automatic Updates

Lab Instructions:

We assume you have completed lab0 and have created and activated your practice labs account. If you have not done that yet, please refer to lab0 instructions in Canvas, Week1, Lab0 section.

**1) Lab3-1: Infrastructure Vulnerability Scanners (50-point)**

- Enter your credentials and the domain name at: [www.practice-labs.com/login.aspx](http://www.practice-labs.com/login.aspx)

- On the “your available practice labs”, select CS0-002- CompTIA Cybersecurity Analyst

- From the lab guide, select Enumeration

- When the lab module’s exercise opens, click Start

- Follow instruction and make sure you understand and go through all the provided information.

Lab **Submission**

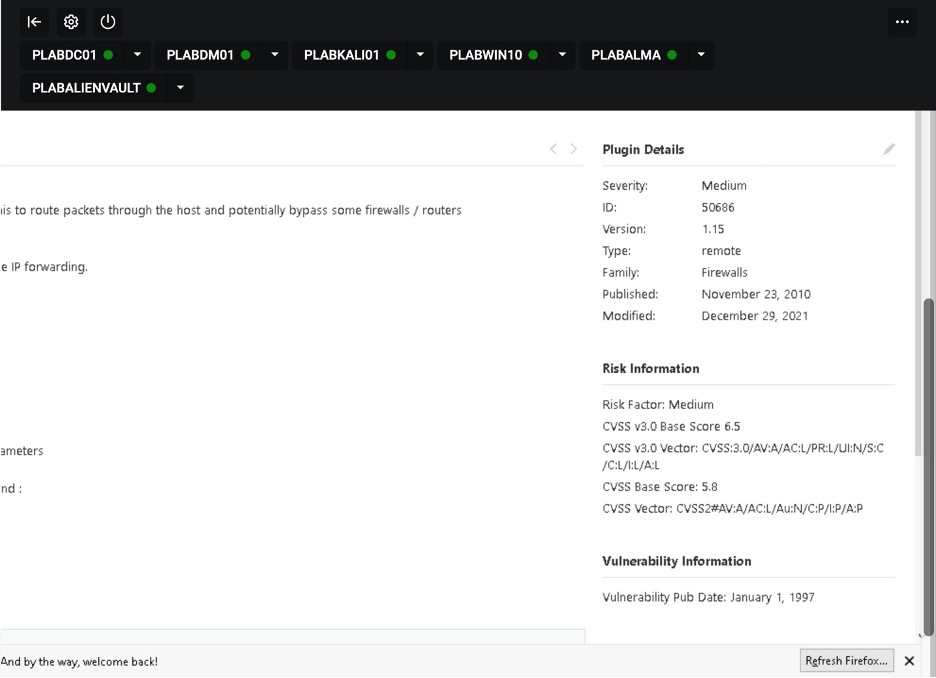
Please make sure to do all the exercises.

**Exercise 1 - Use Nessus**

**Task 1 - Perform a Basic Scan**

#### **Perform the Step 1 - Step 29 Perform a Basic Scan and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.**

**Basic PLAB Scan**



## 

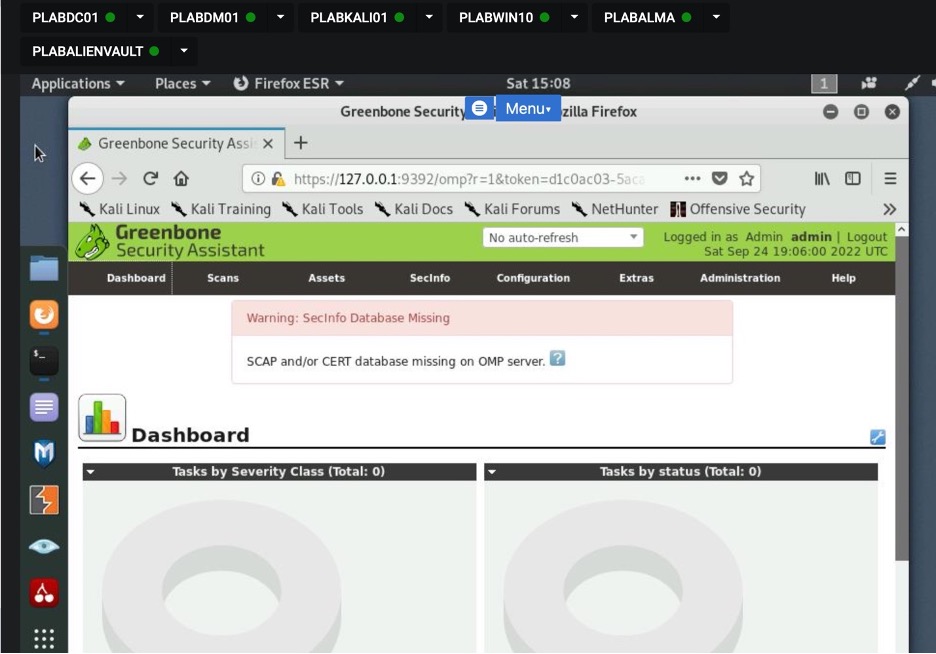
## 

## **Exercise 2 - Use OpenVAS**

**Task 1 - Starting up OpenVAS**

#### **Perform the Step 1 - Step 4 Starting up OpenVAS and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.**

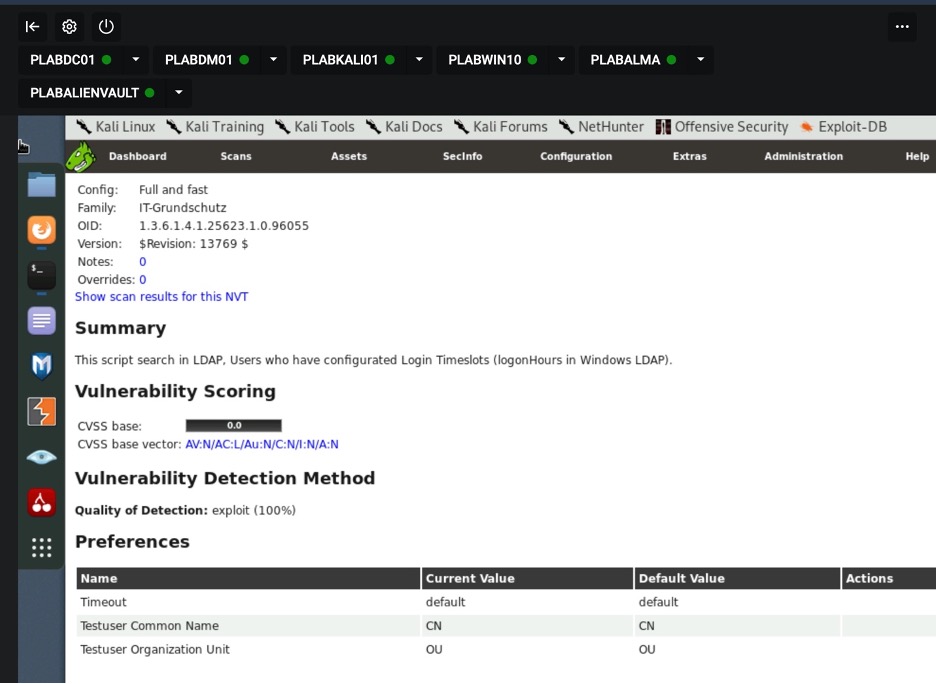
**Opening VAS/Start up**



**Task 2 - Using OpenVAS**

#### **Perform the Step 1 - Step 14 Using OpenVAS and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.**

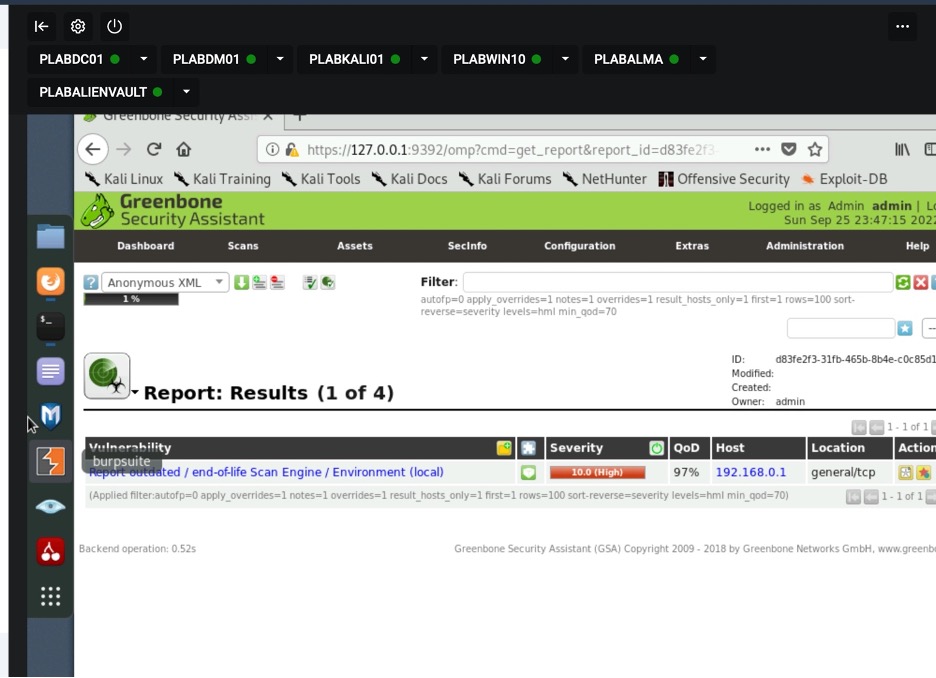
**Using OpenVAS/ Scan config NFT Details**



**Task 3 - Scanning Using OpenVAS**

Perform the Step 1 - Step 10 **Scanning Using OpenVAS** and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.

**Scanning using OpenVAS**



**(P.S. I tried to let the OpenVAS scan to 100% but after a half hour it was still at 1% and as I was doing the lab my mouse in the VM stopped working and has to use the tab and enter button in order to get things working properly so this is the best I was able to do during this time)**

## **2) Lab3-2: Web Application Scanners and Vulnerability Identification and Remediation (50-point)**

- From the lab guide, select Enumeration (we assume you are already logged in)

- When the lab module’s exercise opens, click Start

- Follow instruction and make sure you understand and go through all the provided information.

Lab **Submission**

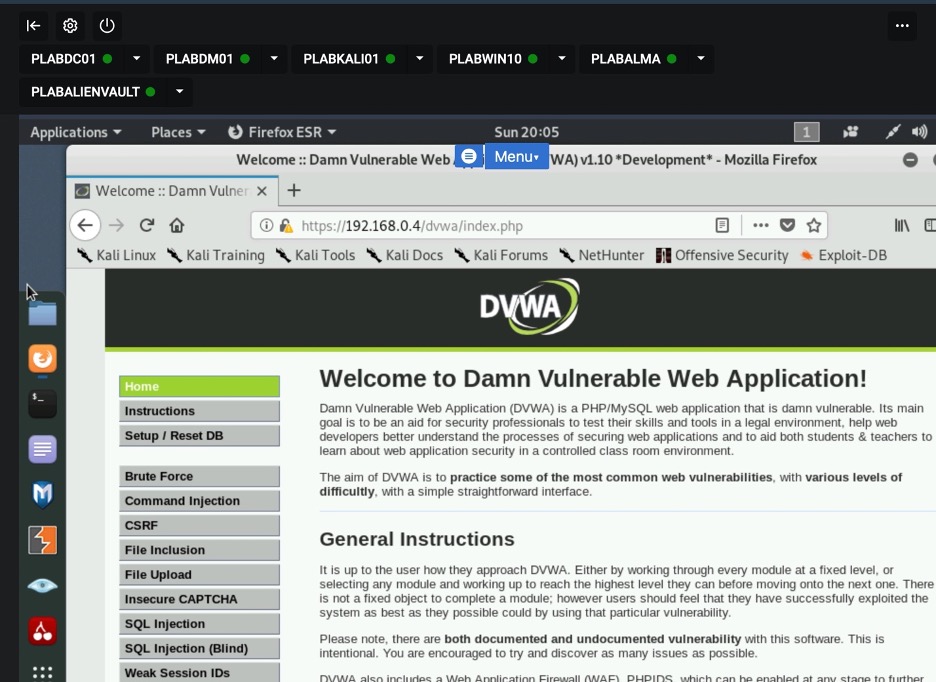
Please make sure to do all the exercises.

**Exercise 1 - Web Application Scanner**

**Task 1 - Verify that the DVWA is running**

#### **Perform the Step 1 - Step 15 Verify that the DVWA is running and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.**

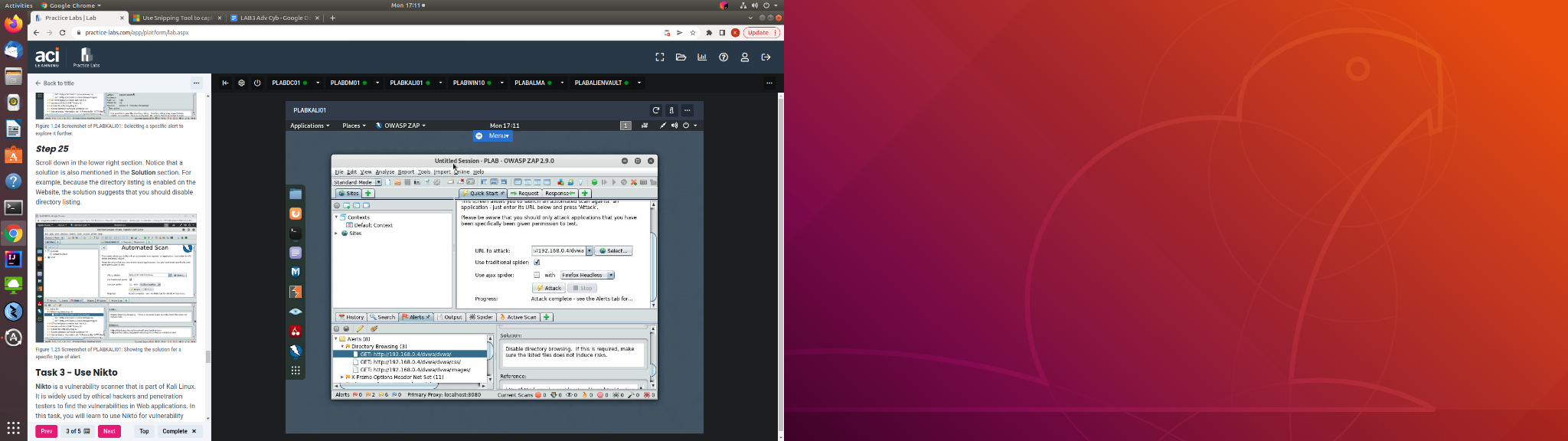
**Verifying that the DVWA is running in both kali and windows**



**Task 2 - Use OWASP Zed Attack Proxy (ZAP)**

#### **Perform the Step 1 - Step 25 Use OWASP Zed Attack Proxy (ZAP) and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.**

### **Using ZAP**

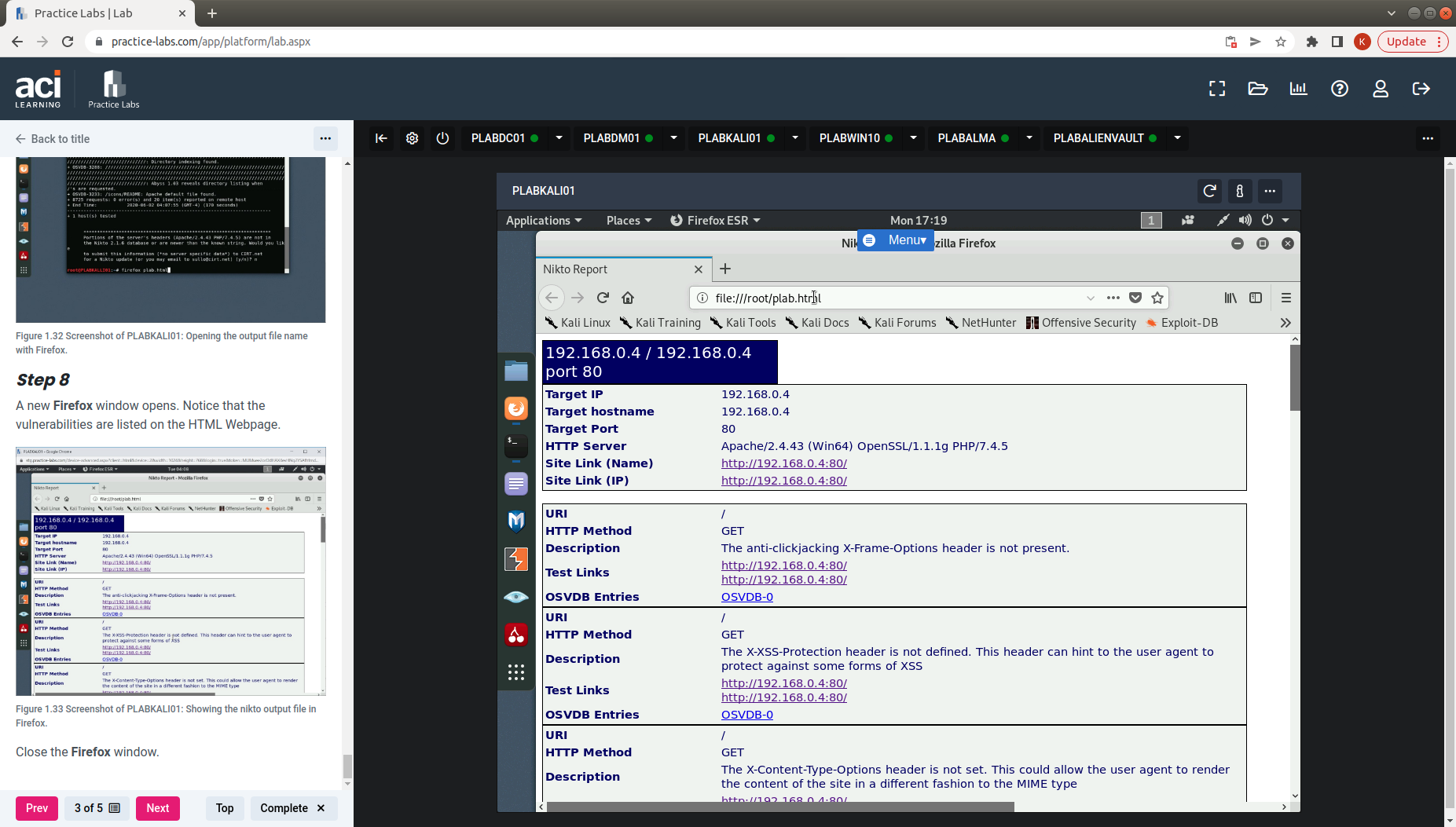


### 

**Task 3 - Use Nikto**

#### **Perform the Step 1 - Step 8 Use Nikto and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.**

Using Nikto



## **Vulnerability Identification and Remediation**

Lab **Submission**

Please make sure to do all the exercises.

- From the lab guide, select Enumeration (we assume you are already logged in)

- When the lab module’s exercise opens, click Start

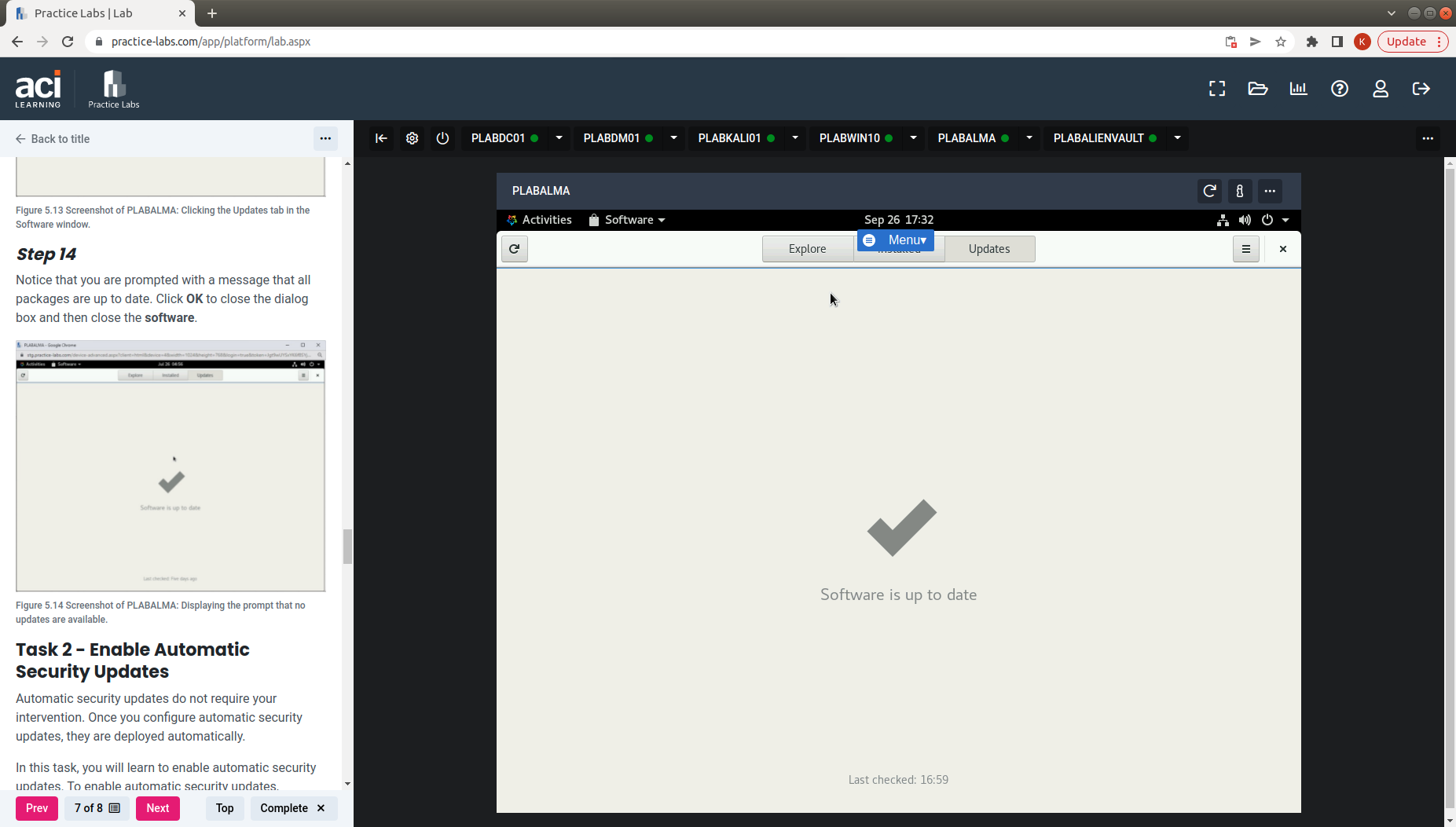
- Follow instruction and make sure you understand and go through all the provided information.

**Exercise 5 - Patching**

**Task 1 - Install Updates Manually**

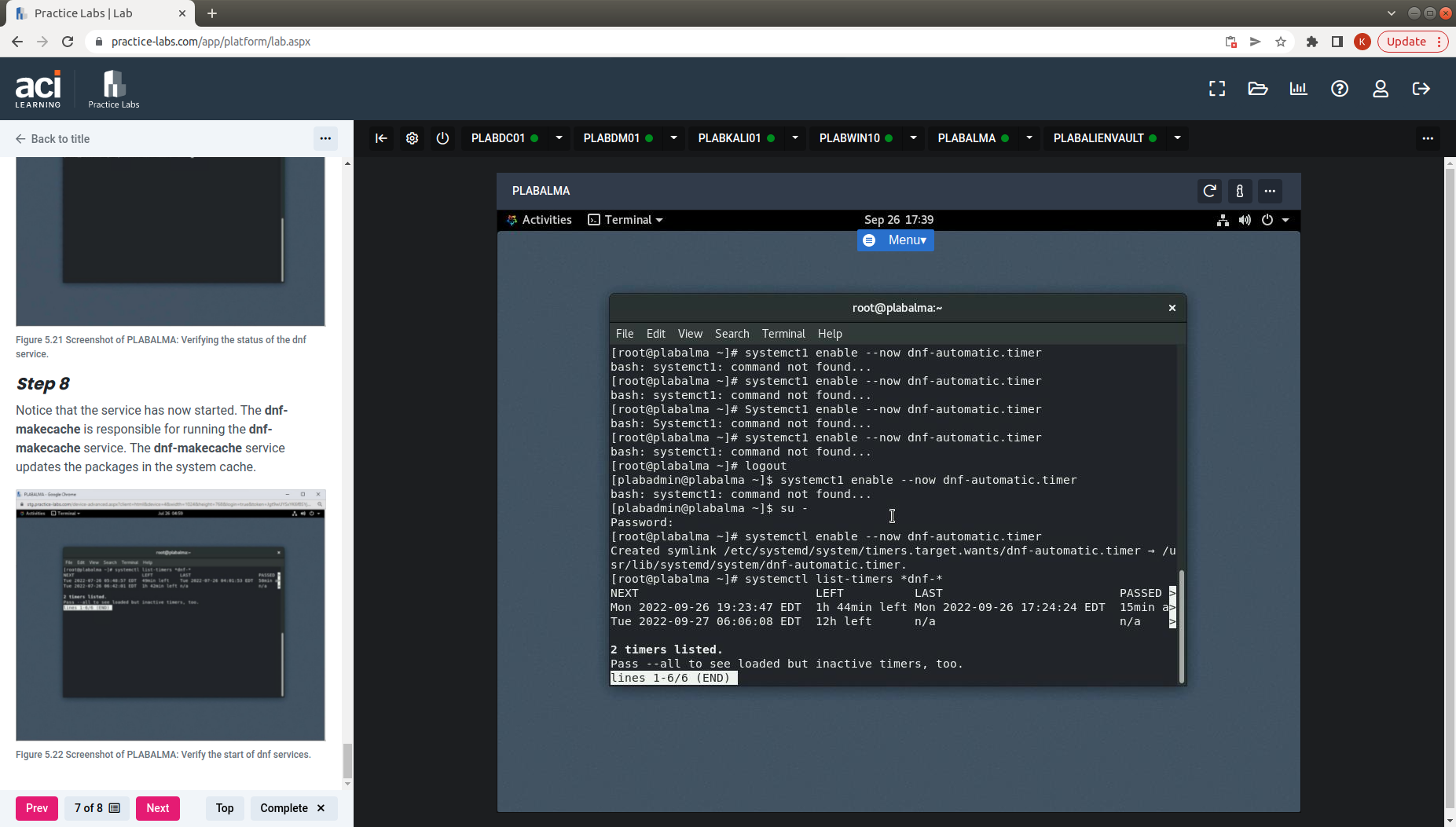
#### **Perform the Step 1 - Step 16 Install Updates Manually and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.**

Updates Manually



**Task 2 - Enable Automatic Security Updates**

#### **Perform the Step 1 - Step 8 Enable Automatic Security Updates and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.**



**Save both Web Application Scanners and Vulnerability Identification and Remediation in one file:**

· Save the report as a docx file (first name and last name: ex. Awad\_Mussa2.docx)

· Keep this file as you will upload it when you take the lab3’s quiz.