Welcome to the **Vulnerability Analysis** Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

**Learning Outcomes**

In this module, you will complete the following exercises:

- Exercise 1 - Performing a Vulnerability Scan
Exercise 2 - Introducing Microsoft Baseline Security Analyser
Exercise 3 - Implementing Recommendations
Exercise 4 - Saving Microsoft Baseline Security Analyzer Reports
Exercise 5 - Analyze Vulnerability Scan Results and Prioritize Activities

After completing this lab, you will be able to:

- Use Nikto for Vulnerability Scanning
- Perform Vulnerability Scanning using OpenVAS
- Use Lynis for System Vulnerability Scanning
- Install MBSA
- Configure MBSA
- Review the Results of the Scan
- Clear the Password Settings
- Save the MBSA Report
- Explain False Positive
- Map Vulnerabilities

Exam Objectives

The following exam objectives are covered in this lab:

- 3.1 Information Security Controls

Note: Our main focus is to cover the practical, hands-on aspects of the exam objectives. You recommend referring to course material or a search engine to research theoretical topics in more detail.

Lab Duration

It will take approximately 1 hour to complete this lab.

Help and Support

For more information on using Practice Labs, please see our Help and Support page. You can also raise a technical support ticket from this page.
Click **Next** to view the Lab topology used in this module.

---

**Lab Topology**

During your session, you will have access to the following lab configuration.
Depending on the exercises, you may or may not use all of the devices, but they are shown here in the layout to get an overall understanding of the topology of the lab.
Click Next to proceed to the first exercise.

---

**Exercise 1 - Performing a Vulnerability Scan**

There is a wide variety of resources that should be made available to the ethical hacker, depending on the scope of the ethical hacking project. For example, these resources may include Nikto, OpenVAS, and Lynis. These tools enable vulnerability scanning, which is used to find vulnerabilities in Web applications.

In this exercise, you will learn to perform vulnerability scanning.

**Learning Outcomes**

After completing this exercise, you will be able to:

- Use Nikto for Vulnerability Scanning
- Perform Vulnerability Scanning using OpenVAS
- Use Lynis for System Vulnerability Scanning

**Your Devices**

You will be using the following devices in this lab. Please power these on now.

- **PLABDC01** - (Windows Server 2019 - Domain Server)
- **PLABDM01** - (Windows Server 2019 - Domain Controller)
- **PLABWIN10** - (Windows 10 - Workstation)
- **PLABKALI01** - (Kali 2019.2 - Linux Kali Workstation)
Task 1 - Use Nikto for Vulnerability Scanning

Nikto is a vulnerability scanner that is part of Kali Linux. It is widely used by ethical hackers and penetration testers to find the vulnerabilities in Web applications. In this task, you will learn to use Nikto for vulnerability scanning.

To do this, perform the following steps:

**Step 1**

Ensure you have powered on all the devices listed in the introduction and connect to **PLABKALIo1**.

Credentials are:

Username: **root**

Password: **Passw0rd**

The desktop of **PLABKALIo1** is displayed.
Figure 1. 1 Screenshot of PLABKALI01: Showing the desktop of PLABKALI01.

**Step 2**

On the desktop, double-click the **Terminal** icon
Step 3

To scan a Website for vulnerabilities, type the following command:

```
Note: Instead of the -host parameter, you can also use the -h parameter. Both provide the same result.
```

```
nikto -host http://192.168.0.10
```

Press Enter.
Figure 1.3 Screenshot of PLABKALI01: Entering the nikto command with a host IP.

**Step 4**

The vulnerability scanning process starts. Depending on the number of vulnerabilities, the process may run for a few minutes.
Figure 1.4 Screenshot of PLABKALI01: Showing the running process of the nikto command.

**Step 5**

A detailed list of vulnerabilities is listed as the output.
Step 6

Clear the screen by entering the following command:

```
clear
```

To scan a Website for vulnerabilities and save the output to an HTML file, type the following command:

```
```
nikto -host http://192.168.0.10 -o plab.html

Press Enter.

Figure 1.6 Screenshot of PLABKALI01: Entering the nikto command with a host IP and output file name.

**Step 7**

Let the vulnerability scanning process complete.

Then, type the following command:
Press Enter.

![Firefox window opening a file](image)

**Figure 1.7** Screenshot of PLABKALI01: Opening the output file name with Firefox.

**Step 8**

A new Firefox window opens. Notice that the vulnerabilities are listed on the HTML Webpage.
Figure 1.8 Screenshot of PLABKALI01: Showing the nikto output file in Firefox.

Close the Firefox window.

**Task 2 - Perform Vulnerability Scanning using OpenVAS**

Kali Linux provides a tool named the Open Vulnerability Assessment System (OpenVAS) for vulnerability scanning. OpenVAS is a framework that consists of multiple services and tools. The first step is getting information about a Web server. The Footprinting process can also help you grab banners on the Web server.

To perform vulnerability scanning using OpenVAS, perform the following steps:

**Step 1**
Ensure you have powered on all the devices listed in the introduction and connect to PLABKAL101.

Clear the screen by entering the following command:

```
clear
```

Next, you need to setup OpenVAS. To do this, type the following command:

```
openvas-setup
```

Press Enter.
Step 2

The setup process for OpenVAS now starts. This process will setup OpenVAS and download many signatures and vulnerability tests.

Note: This process may take a while to complete.

Alert: If openvas fails to start or if a Firefox window is not opened as indicated in the following step, please reattempt executing the openvas-setup command.
**Step 3**

After the setup process is complete, a Firefox window is opened.

Click **Advanced**...

Scroll down and click **Accept the Risk and Continue**.
Figure 1.11 Screenshot of PLABKALI01: Showing Firefox window with connection not secure message.

**Step 4**

The **Greenbone Security Assistant** login page is displayed.

In the **Username** text box, type the following:

```
admin
```

In the **Password** text box, type the following:
Click **Login**.

![Screenshot of PLABKALI01: Entering the user credentials on the login screen and clicking Login.](image)

**Figure 1.12** Screenshot of PLABKALI01: Entering the user credentials on the login screen and clicking Login.

**Step 5**

The dashboard for OpenVAS is displayed.
Figure 1.13 Screenshot of PLABKALI01: Showing the dashboard screen for OpenVAS.

**Step 6**

You will now perform a scan. Hover over **Configuration** and select **Targets**.
Figure 1.14 Screenshot of PLABKALI01: Selecting Targets from the Configuration menu.

**Step 7**

The **Targets** page is displayed. First, you need to define a target.

Click **New Target** (*) on the upper left side - just below the menu.
Step 8

The **New Target** dialog box is displayed. In the **Name** text box, type the following:

```
PLABDC01
```

In the Manual Field text box, type the following:

```
192.168.0.1
```
Click Create.

Figure 1.16 Screenshot of PLABKALI01: Enter the name in the Name text box and click Create.

**Step 9**

Notice that the target is now created.
Figure 1.17 Screenshot of PLABKALI01: Showing the newly created task.

**Step 10**

Next, create a task. Hover over **Scans** and then select **Tasks**.
Step 11

The **Tasks** page is displayed.

**Note:** A dialog box will appear for 10 seconds and then disappear automatically.

Click the **Task** icon just below the menu bar and select **Task Wizard**.
Step 12

The Task Wizard is displayed. Input the IP address as **192.168.0.1** and click **Start Scan**.
Figure 1.20 Screenshot of PLABKALI01: Clicking Start Scan on the Task Wizard dialog box.

**Step 13**

Notice that a new task is created.

After a few minutes, the task starts to run. The **Status** column now shows the percentage of task run.

**Note:** This task will take around 10 minutes to complete.
Figure 1.21 Screenshot of PLABKALI01: Showing the running task with the percentage completed.

**Step 14**

Finally, the scan completes, and the **Tasks** page displays the status.

Click **Immediate scan of IP 192.168.0.1**.
Figure 1.22 Screenshot of PLABKALIO1: Showing the completed task on the Tasks page.

**Step 15**

The finished task details are displayed. Click 1 next to Reports.
**Step 16**

Click the link provided under the **Date** column.
Figure 1.24 Screenshot of PLABKALI01: Clicking the link in the Date column.

**Step 17**

Notice that the vulnerability is now displayed. It also displays the **Severity** level of vulnerability.
Figure 1.25 Screenshot of PLABKALI01: Showing the vulnerability with the severity level.

Close the Firefox window.

Task 3 - Use Lynis for System Vulnerability Scanning

Lynis is a built-in tool in Kali Linux that is a multi-purpose tool. It is designed to perform the following tasks:

- Security auditing
- Compliance testing
- Penetration testing
- Vulnerability detection
- System hardening
It can perform several types of system auditing, such as system binaries, boot loaders, startup services, run level, loaded modules, kernel configuration, core dumps, and so on.

In this task, you will learn to use Lynis for system vulnerability scanning. To do this, perform the following steps:

**Step 1**

Ensure you have powered on all the devices listed in the introduction and connect to **PLABKALIo1**.

In the terminal window, enter the following command to install Lynis.

```
apt-get install lynis
```

Press **Enter**.

**Note:** If you are shown an error such as 404 not found in the output, execute the command `apt-get update` and then reattempt the command at this step being `apt-get install lynis`. 
Figure 1.26 Screenshot of PLABKALI01: Showing the command apt-get install lynis inputted to install lynis.

**Step 2**

After the installation has completed and you are shown the next prompt.

Clear the screen by entering the following command:

```
clear
```

By default, Lynis will perform a local system scan. You have the option to run a normal audit scan or can run the entire system scan.
Let’s first run the normal audit scan. Type the following command:

```
lynis audit system
```

Press Enter.

**Alert:** If you are shown a not found error, please reattempt Step 1 following the alert located within.

Figure 1.27 Screenshot of PLABKALI01: Entering the lynis command to perform a local system security audit.

**Step 3**
The auditing process starts. Notice that it has already detected the operating system version, its hostname, and so on.

**Note:** The audit process will take a few minutes to complete.

![Screenshot of PLABKALI01](image)

**Figure 1.28** Screenshot of PLABKALI01: Showing the running audit process.

**Step 4**

During the scan process, you will notice that the results are categorized under different categories.
Figure 1.29 Screenshot of PLABKALI01: Showing the output of the lynis command.

**Step 5**

The audit process completes.
Figure 1.30 Screenshot of PLABKALI01: Showing the completed status of lynis command.

**Step 6**

You will need to scroll up to review the results. Notice that there are vulnerabilities that are located. Lynis also provides a suggestion to close the vulnerabilities. For example, it is hardening the SSH configuration. It has a setting `PermitRootLogin` set to Yes. Lynis audit suggests that it should be set to No.

**Note:** Take a few minutes and go through the audit report. If time permits, then you should use the following command to perform a full audit scan: `lynis audit system -c`
Figure 1.31 Screenshot of PLABKALI01: Showing the list of vulnerabilities.

Close the terminal window.

Exercise 2 - Introducing Microsoft Baseline Security Analyzer (MBSA)

Microsoft Baseline Security Analyzer (MBSA) checks for available updates to the operating system, Microsoft Data Access Components (MDAC), MSXML (Microsoft XML Parser), .NET Framework, and SQL Server. MBSA also scans a computer for insecure configuration settings. When MBSA checks for Windows service packs and patches, it includes in its scan Windows components, such as Internet Information Services (IIS) and COM+. 
In this exercise, you will learn about MBSA.

The PLABWIN10 system does not have MBSA installed. MBSA will be installed from the Intranet within the following task.

**Learning Outcomes**

After completing this exercise, you will be able to:

- Install MBSA
- Configure MBSA
- Review the results of the scan

**Your Devices**

You will be using the following devices in this lab. Please power these on now.

- **PLABDC01** - (Windows Server 2019 - Domain Server)
- **PLABWIN10** - (Windows 10 - Workstation)

**Task 1 - Install MBSA**

You can use MBSA to track the missing updates and security misconfiguration on a Windows system. MBSA does not come installed by default. You need to download and install it on a Windows system.

In this task, you will learn to install MBSA on PLABWIN10. To do this, perform the following steps:
Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABWIN10**. The desktop of **PLABWIN10** is displayed.

![Screenshot of PLABWIN10](image)

Figure 2.1 Screenshot of PLABWIN10: Showing the desktop of PLABWIN10.

Step 2

Click **Microsoft Edge**, located on the taskbar.
Figure 2.2 Screenshot of PLABWIN10: Showing the desktop of PLABWIN10. Microsoft Edge is highlighted.

**Step 3**

The Intranet page is opened by default.

Click the link for **Tools.**
Step 4

Scroll down the page and select the link for **Windows_Server_2012**.
Figure 2.4 Screenshot of PLABWIN10: Showing the Intranet page, Windows_Server_2012 is highlighted.

**Step 5**

Click the link for MBSA.
Step 6

Click the link for **MBSA Setup-x64-EN.msi**

Click **Save** on the pop-up at the bottom of the window.

Once indicated that the setup has finished downloading, close the notification and close **Microsoft Edge**.
Step 7

From the taskbar, click **File Explorer**.
Figure 2.7 Screenshot of PLABWIN10: Clicking the File Explorer icon in the taskbar.

**Step 8**

The **File Explorer** window is displayed. In the left pane, click Downloads.
Figure 2.8 Screenshot of PLABWIN10: Selecting the Downloads option in the left pane of File Explorer.

**Step 9**  
In the **Downloads** folder. Double-click the **MBSASetup-x64-EN** file.
Figure 2.9 Screenshot of PLABWIN10: Double-clicking the MBSA installer file.

**Step 10**

The **MBSA Setup** dialog box is displayed. On the **Welcome to the Microsoft Baseline Security Analyzer** page, click **Next**.
Figure 2.10 Screenshot of PLABWIN10: Clicking the Next button on the Welcome to the Microsoft Baseline Security Analyzer page.

**Step 11**

On the **License Agreement** page, select **I accept the license agreement** and click **Next**.
Figure 2.11 Screenshot of PLABWIN10: Selecting the I accept the license agreement option on the License Agreement page.

**Step 12**

On the **Destination folder** page, keep the default path and click **Next**.
Figure 2.12 Screenshot of PLABWIN10: Clicking Next on the Destination Folder page.

**Step 13**

On the **Start Installation** page, click **Install**.
Figure 2.13 Screenshot of PLABWIN10: Clicking Install on the Start Installation page.

**Step 14**

On the **Installation Progress** page, the installation progress is displayed.
Figure 2.14 Screenshot of PLABWIN10: Showing the installation progress on the Installation Progress page.

**Step 15**

After the installation progress is completed, the **MBSA Setup** dialog box is displayed. Click **OK**.
Figure 2.15 Screenshot of PLABWIN10: Clicking OK on the MBSA Setup dialog box.

**Step 16**

Close the **File Explorer** window.
Figure 2.16 Screenshot of PLABWIN10: Closing the File Explorer window.

Step 17

Notice that the MBSA icon appears on the desktop.
Task 2 - Configure MBSA

Configuration specifications can take place against a single computer or multiple machines within a domain or range of IP’s. You will focus on using an IP range and the results on PLABWIN10 after the scan has completed.

To configure MBSA, perform the following steps:

**Step 1**

Ensure all the lab devices stated in the introduction are powered on.

Connect to **PLABWIN10**.
Double-click on the **Microsoft Baseline Security Analyzer 2.3** desktop shortcut.

![Screenshot of PLABWIN10: Double-clicking the MBSA icon on the desktop.](image)

**Figure 2.18** Screenshot of PLABWIN10: Double-clicking the MBSA icon on the desktop.

**Step 2**

The **Microsoft Baseline Security Analyzer 2.1** window is displayed.

Click **Scan a computer**.
Figure 2.19 Screenshot of PLABWIN10: Selecting the Scan a computer option

**Step 3**

The **Which computers do you want to scan?** page is displayed.

In the IP address field, type the following range:

```
192.168.0.1
```
Step 4

Change the **Security Report Name** to something preferable and identifiable such as:

```
%IP%
```

This will bring into effect the IP values as the report name.

When working on a live system, you can scan for the following problems within a Windows environment:
- Windows administrative vulnerabilities
- Weak passwords
- IIS administrative vulnerabilities
- SQL administrative vulnerabilities

Figure 2.21 Screenshot of PLABWIN10: Showing the MBSA configuration page with report name changed.

**Step 5**

Next, press the **Start Scan** button on the bottom right-hand side of the window.
Figure 2.22 Screenshot of PLABWIN10: Clicking the Start Scan button.

**Step 6**

You will notice that Windows begins the scanning process.

*Note:* The scanning process may take a while to complete.
Step 7

After about 5-7 minutes, a summary of scanned devices will be displayed in descending order.

Note: Scores cannot be changed or reassigned for system configuration checks.
Task 3 - Review the Results of the Scan

MBSA generates a report file and sends it to the profile directory under the name titled by the MBSA tool. The results display several Icons.

- **A red exclamation mark** - appears when a critical check has failed. An example is a user account that has a blank password.
- **A yellow exclamation mark** - appears when a non-critical check failed. For example, a user account has a password that does not have expiration date.
- **A green checked mark** - appears when a check has passed.
- **A blue asterisk** - displays information on “best practice” checks. For example, auditing is enabled on the system.
- **A blue informational icon** - displays information about the computer that is being scanned. For example, the operating system version installed on the
When reviewing security updates:

- **A red exclamation mark** - displays information that the computer is missing a security update. It could also appear if it fails to perform a security check on the computer.
- **A yellow X** - displays a warning message computer is missing the most recent service pack.
- **A blue star** - displays a message stating that an update is not installed on the computer because approval for it has not taken place on the Windows Software Update Services (WSUS) server.

**Step 1**

Ensure that the required systems are powered on. Connect to PLABWIN10. After clicking the outcome of the report for **PLABDC01**, you can see a generated report for this device.
Figure 2.25 Screenshot of PLABWIN10: Showing the MBSA scan report.

**Step 2**

On each Issue, you will find a Result tab typically providing 3 options of “What was scanned”, “result details” and “How to correct this”.
**Step 3**

Under the **Administrative Vulnerabilities** subsection of the **Windows Scan Results** section, click the **What was scanned** link for **Password Expiration**.
Step 4

This will automatically open up a page in Internet Explorer where further information can be read.

MBSA gives us some information about Password Expiration results with a description of the issue identified.

Close this window.
Figure 2.28 PLABWIN10: Showing the MBSA description page of a result.

**Step 5**

Click the **Result details** link.
**Step 6**

You are presented with information detailing the user accounts with non-expiring passwords; these accounts will need to be checked.

Close this window.
Figure 2.30 Screenshot of PLABWIN10: Showing the page with the user accounts that have non-expiring passwords.

**Step 7**

Click the **How to correct this** link.
Step 8

You are presented with the issue and even a caution on changing account details for specific situations. Finally, you are presented with the solution to correct the problem.

You will now follow these steps to make sure you are protected against this for the Guest and Administration accounts.
Close the **Password Expiration** window.

**Step 9**

Close the **MBSA** window.
Exercise 3 - Implementing Recommendations

After the MBSA scanning, you need to review the results. There is a probability that the results will require you to perform certain actions to close the security loopholes or vulnerabilities that have been found in the system. The results may also include some recommendations, which are best practices, that you can choose to accept and action or simply ignore them. Here, you will reset the password controls to keep them in line with best practice.

In this exercise, you will learn to implement the recommendations suggested by MBSA.
Learning Outcomes

After completing this exercise, you will be able to:

- Clear the Password Settings

Your Devices

You will be using the following devices in this lab. Please power these on now.

- **PLABDC01** - (Windows Server 2019 - Domain Server)
- **PLABWIN10** - (Windows 10 - Workstation)

Task 1 - Clear the Password Settings

In the previous task, you notice that there are local user accounts that have non-expiring passwords. You need to ensure that these settings are cleared so that the passwords should be changed at a periodic interval. To do this, perform the following steps:

**Step 1**

Ensure that the required devices are powered on. Connect to **PLABWIN10**.

Right-click the Windows charm and select **Run**
Figure 3.1 Screenshot of PLABWIN10: Selecting the Run option from the Windows charm context menu.

**Step 2**

The **Run** dialog box is displayed. In the **Open** text box, type the following:

```
compmgmt.msc
```

Click **OK**.
Figure 3.2 Screenshot of PLABWIN10: Entering compmgmt.msc command in the Open text box of the Run dialog box.

**Step 3**

The **Computer Management** window is displayed. In the left-hand pane, expand **Local Users and Groups** and select **Users**.
Step 4

In the middle pane, right-click **Guest** and select **Properties**.
Step 5

The Guest Properties dialog box is displayed. On the General tab, deselect the Password never expires option.

Click OK.
Step 6

Perform the same action for the **Administrator** role.

Click **OK**.
Figure 3.6 Screenshot of PLABWIN10: Showing the Administrator Properties dialog box to change the Password Expiration setting.

**Step 7**

As seen above, you have now completed security actions for both the **Guest** and **Administrator** roles.
Close the Computer Management window.

Exercise 4 - Saving Microsoft Baseline Security Analyzer Reports

Reports are a key feature of an audit trail; here you are auditing the configuration a server device and logging the information for a situation in the future where accountability is a necessity for tracking changes to a network topology.

In this exercise, you will learn to save MBSA reports.
Learning Outcomes

After completing this exercise, you will be able to:

- Save the MBSA Report

Your Devices

You will be using the following devices in this lab. Please power these on now.

- **PLABDC01** - (Windows Server 2019 - Domain Server)
- **PLABWIN10** - (Windows 10 - Workstation)

Task 1 - Save the MBSA Report

In this task, you will save a generated report as an XPS document, which is an open format designed and supported by Microsoft.

**Step 1**

Ensure that the required devices are powered on. Connect to **PLABWIN10**.

On the desktop, double-click **Microsoft Baseline Security Analyzer 2.1**.
Figure 4.1 Screenshot of PLABWIN10: Double-clicking the MBSA icon on the desktop.

**Step 2**

In the **MBSA** window, click the **View existing security scan reports** link.
Figure 4.2 Screenshot of PLABWIN10: Clicking the View existing security scan reports link.

**Step 3**

On the **Choose a security scan report to view** page, you may get to see one or more reports. The number of reports depends on the time you have run the scan. Click a report.
Step 4

The report contents are displayed. Click the **Print this report** link, located towards the bottom left-hand corner of the window.
Step 5

The **Print** dialog box is displayed. In the **Select Printer** section, scroll across and select **Microsoft XPS Document Writer** and click **Print**.
Step 6

Name the file **PLABDC01**, keep the extension as .oxps and save the file to the **Documents**.
Step 7

Now minimize the MBSA window.
Step 8

From the taskbar, click **File Explorer** and then navigate to the **Documents** folder in the left pane.
Figure 4.8 Screenshot of PLABWIN10: Showing the MBSA scan report in the Downloads folder.

**Step 9**

Notice that a file named **PLABDC01** is present in the **Documents** folder. Double-click the file to read the output of the report.
Step 10

The **PLABDC01.oxps - XPS Viewer** window is displayed. It displays the contents of the **PLABDC01** report.

This file is, in fact, part of the auditing performed against windows machines, and typically it would be kept as a record of actions that have been taken and recognized.
Close the **XPS Viewer** and **File Explorer** windows.

**Note:** You can run MBSA once again to review the vulnerabilities. The password expiration should not appear on the list.

---

**Exercise 5 - Analyze Vulnerability Scan Results and Prioritize Activities**

After you have scanned devices, servers, and Web applications for vulnerabilities, you need to analyze the vulnerability results now. This is because after discovering
vulnerabilities, you need to make good use of them in penetration testing.

In this exercise, you will learn about analyzing the vulnerability scan results.

**Learning Outcomes**

After completing this exercise, you will be able to:

- Explain False Positive
- Know about Mapping Vulnerabilities

**Task 1 - Explain False Positive**

Please connect to **PLABKALI01** to view the list of vulnerability results.

A false positive is a condition, which is typically detected by a scanner, but it actually does not exist. It is about a condition that is considered to be present in a result but it does not exist. For example, a vulnerability may indicate that MySQL has a vulnerability, but, in reality, it does not exist or is not considered a vulnerability. Vulnerability scan results can produce several false positives. A vulnerability scanner may show false positives due to several reasons:

- It is unable to recognize an executable or service.
- To cover up a vulnerability, you may have implemented a compensating control. Therefore, the vulnerability may be shown as false positive even though it is covered by a compensating control.
- The vulnerability scanner does not have updated definitions.
- The scanner configurations are not correct, and therefore, several services or configuration settings may be marked as false positives.

As a pentester, you must be able to identify false positives. Each scan result should be researched and calculated, whether it is a false positive or not. You will not know about every vulnerability that you discover, but researching can certainly prevent wastage of hours of work.

**Task 2 - Map Vulnerabilities**
After generating a list of vulnerabilities, you need to map them. In a network environment, there can be several targets that can have associated vulnerabilities. You may run more than one vulnerability scans. After you are done with the scans, you can collate the vulnerabilities in a single document and map them with the targets. You should update this document as and when you run a vulnerability scan.

![Screenshot of PLABKALI01: Showing the list of vulnerabilities.](image)

Figure 5.1 Screenshot of PLABKALI01: Showing the list of vulnerabilities.

**Review**

Well done, you have completed the **Vulnerability Analysis** Practice Lab.

**Summary**
You completed the following exercises:

- Exercise 1 - Performing a Vulnerability Scan
- Exercise 2 - Introducing Microsoft Baseline Security Analyser
- Exercise 3 - Implementing Recommendations
- Exercise 4 - Saving Microsoft Baseline Security Analyzer Reports
- Exercise 5 - Analyze Vulnerability Scan Results and Prioritize Activities

You should now be able to:

- Use Nikto for Vulnerability Scanning
- Perform Vulnerability Scanning using OpenVAS
- Use Lynis for System Vulnerability Scanning
- Install MBSA
- Configure MBSA
- Review the Results of the Scan
- Clear the Password Settings
- Save the MBSA Report
- Explain False Positive
- Map Vulnerabilities

Feedback

Shutdown all virtual machines used in this lab. Alternatively, you can log out of the lab platform.