CompTIA Cybersecurity Analyst (CySA+)

Vulnerability Scanner MBSA

Introduction

The **Vulnerability Scanner MBSA** module provides you with the instructions and devices to develop your hands-on skills in the following topics.

- Introduction to Microsoft Security Baseline Analyzer
- Implementing Recommendations
- Saving Microsoft Security Baseline Analyzer Reports
- Reviewing Configuration Changes

Lab time: It will take approximately 30 minutes to complete this lab.

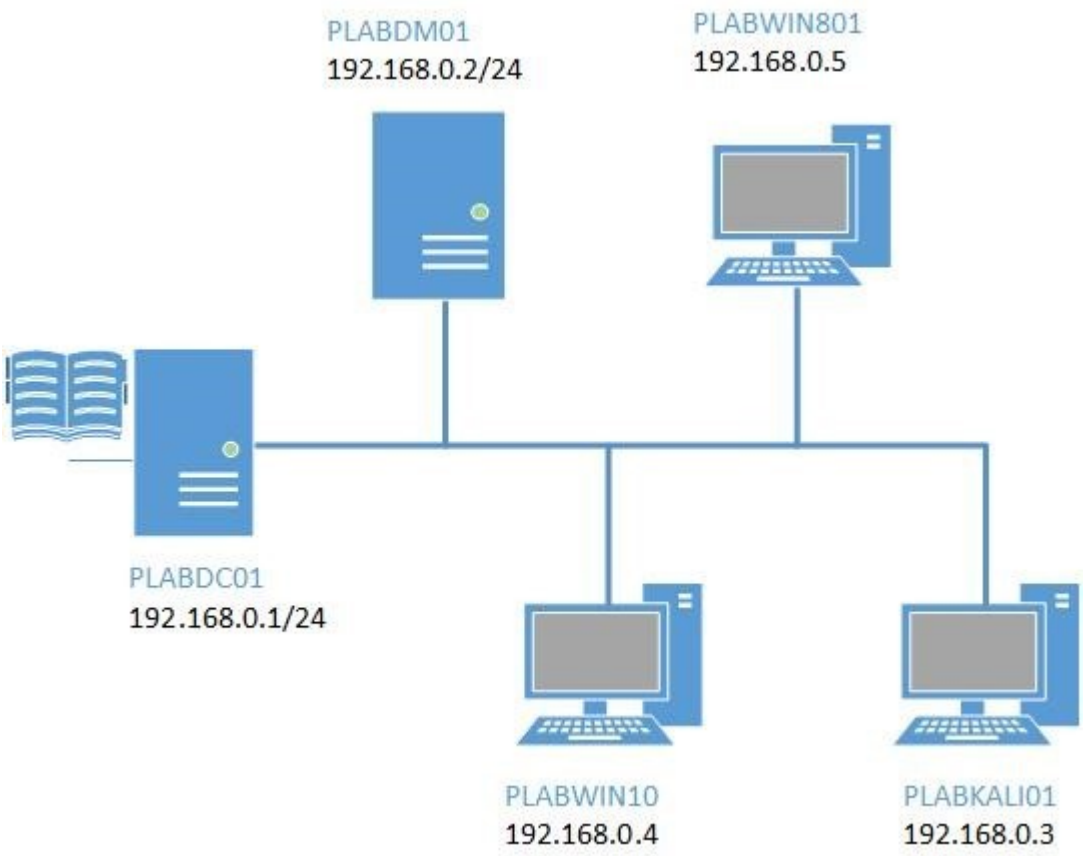
Exam Objectives

The following exam objectives are covered in this lab:

- **CS0-001 2.1** Given a scenario, implement an information security vulnerability management process
- **CS0-001 2.2** Given a scenario, analyze the output resulting from a vulnerability scan
- **CS0-001 2.3** Compare and contrast common vulnerabilities found in the following targets within an organization

Lab Diagram

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.



Connecting to your lab

In this module, you will be working on the following equipment to carry out the steps defined in each exercise.

- **PLABDC01** (Windows Server 2012 R2 - Domain Controller)
- **PLABDM01** (Windows Server 2012 R2 - Member Server)
- **PLABWIN801** (Windows 8.1 - Domain Member)
- **PLABWIN10** (Windows 10 - Domain Member)
- **PLABKALI01** (Kali 2016.2)

To start, simply choose a device and click **Power on**. In some cases, the devices may power on automatically.

For further information and technical support, please see our Help and Support page.

Exercise 1 - Introduction to Microsoft Baseline Security Analyser

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 complete the following tasks:

- Configuration
- Scanning
- Results

Please refer to your course material or use your favorite search engine to research for more information about this topic.

Task 1 - Configuration

Configuration specifications can take place against a single computer or multiple machines within a domain or range of IP's. We will be focusing using an IP range but focusing on the results on PLABDM01 once the scan has been completed.

Step 1

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

Connect to **PLABDM01**.

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

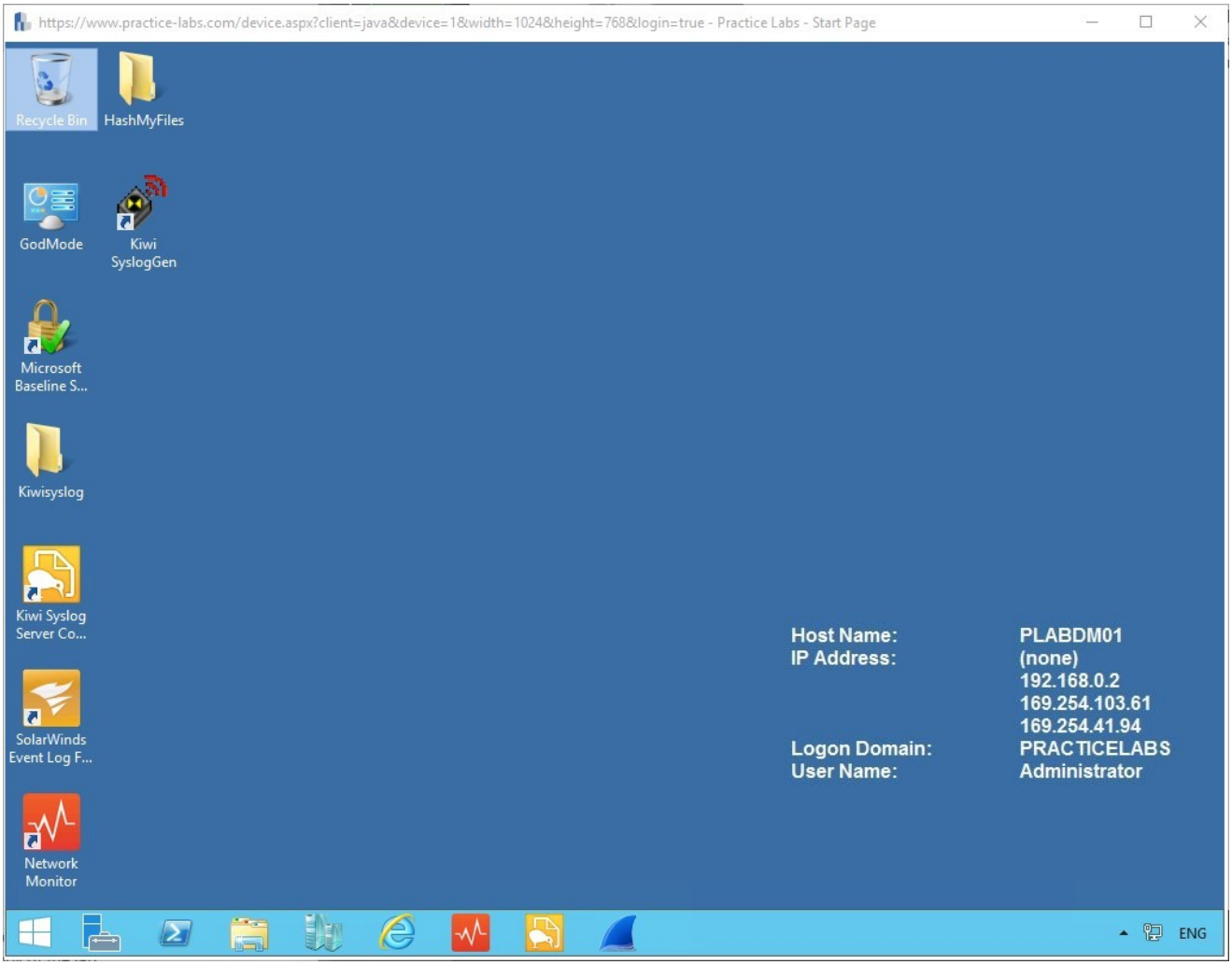


Figure 1.1 PLABDM01: the Desktop.

Step 2

The **Microsoft Baseline Security Analyzer** application launches.

Click on **Scan multiple computers**.

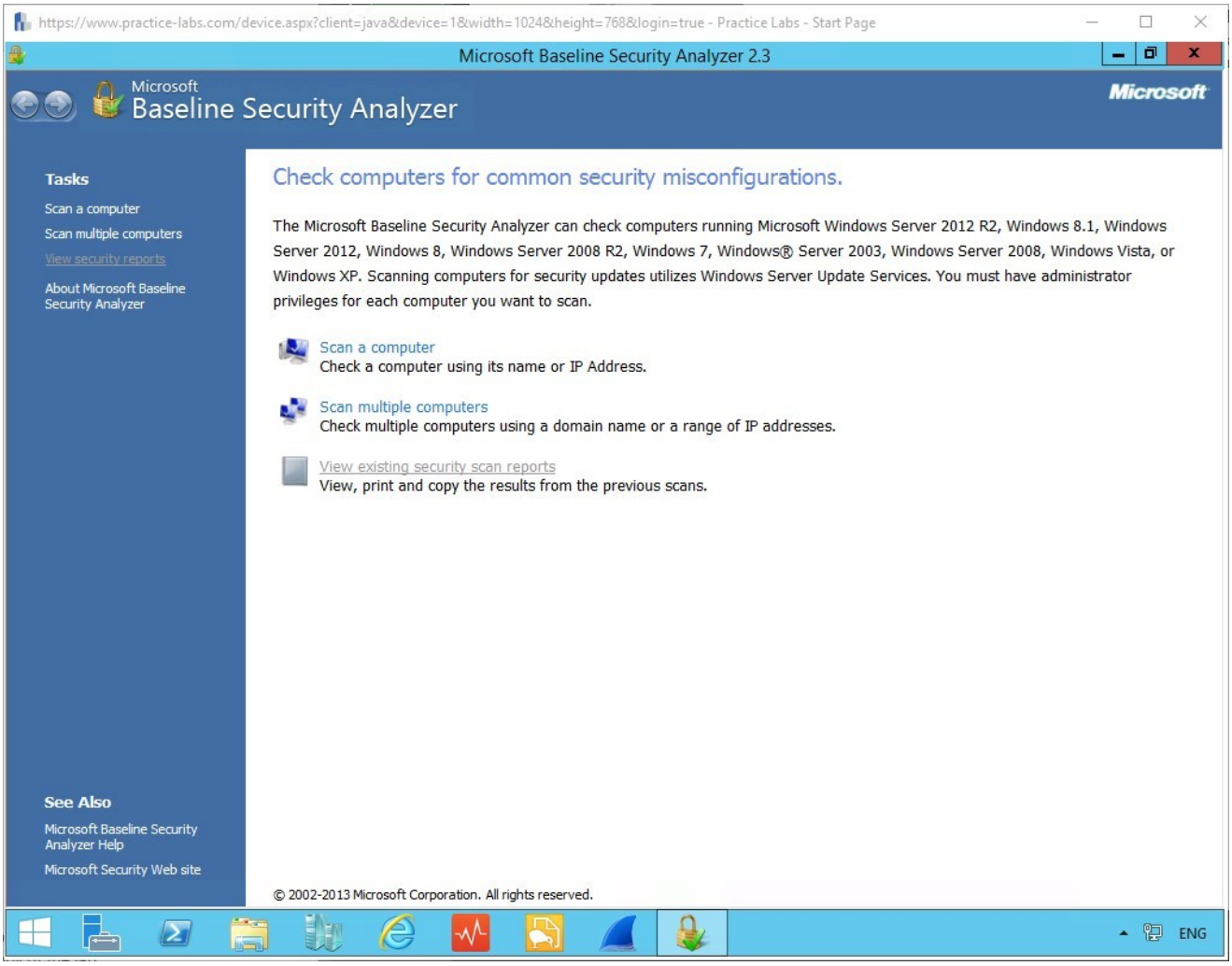


Figure 1.2 PLABDM01: MBSA screen.

Step 3

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

In the IP address range field enter the following:

```
192.168.0.1 to 192.168.0.2
```

Here we could either enter the details of the computer name we are interested in checking or enter an IP range to be checked for example the device itself is

```
PRACTICELABS\PLABDM01
```

However, in this instance, we have entered an IP range.

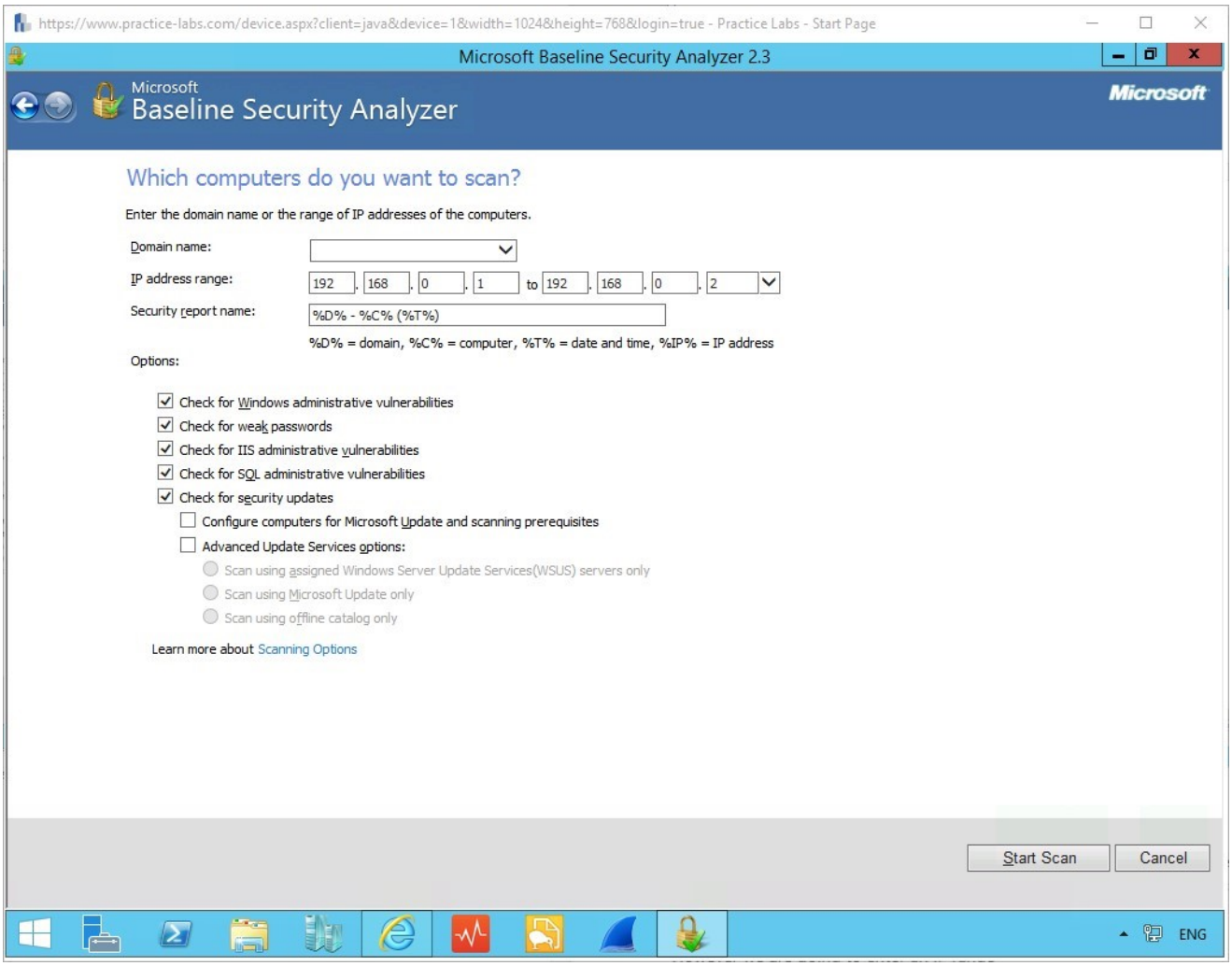


Figure 1.3 PLABDM01: MBSA configuration menu with IP range added.

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.

Task 2 - Scanning an IP range

When working on a live system, we can scan for the following problems within a Windows environment.

- Windows administrative vulnerabilities
- Weak passwords
- IIS administrative vulnerabilities
- SQL administrative vulnerabilities

In this task, we will scan an IP range for vulnerabilities.

Step 1

Next press the **Start Scan** button on the bottom right-hand side of the screen.

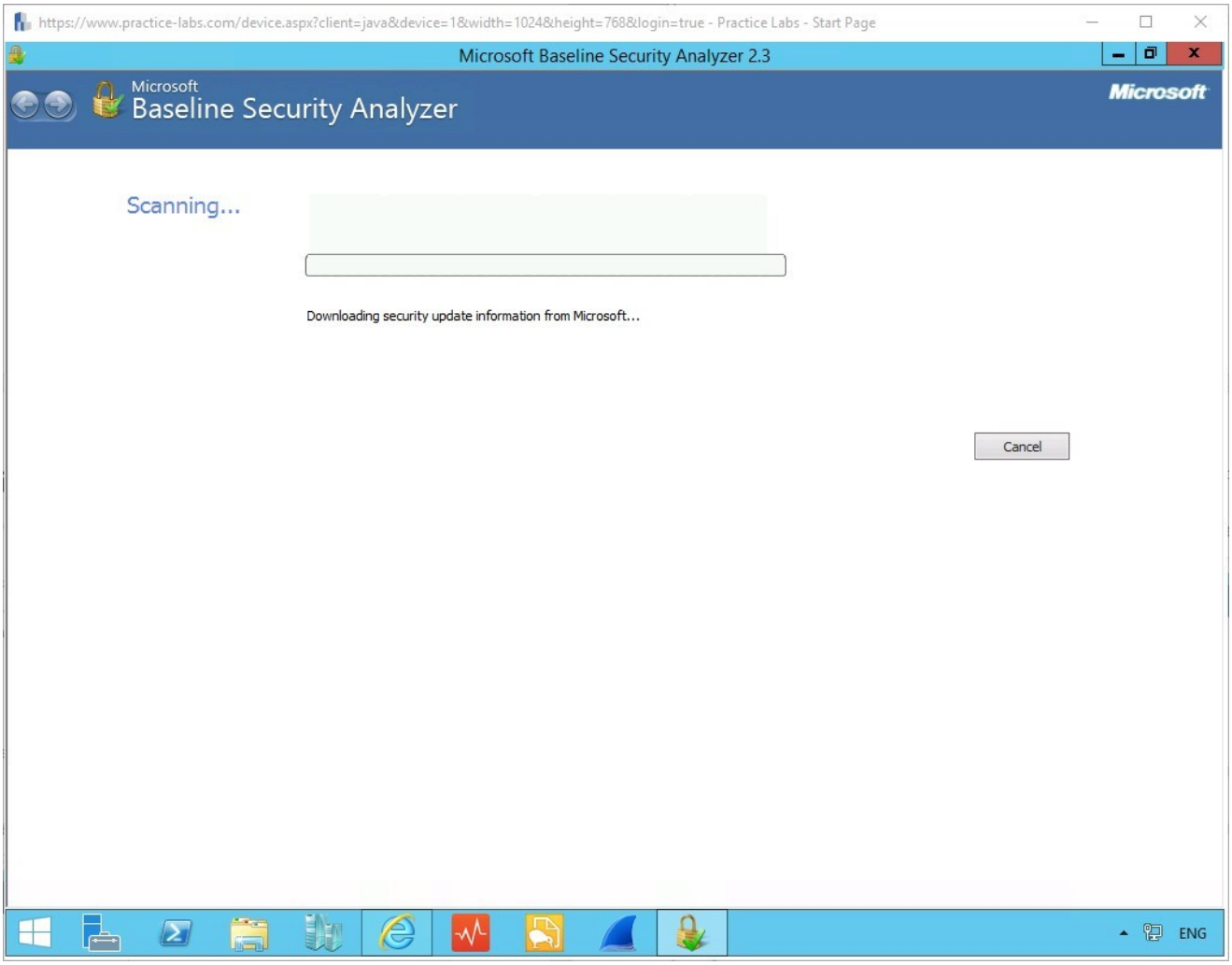


Figure 1.4 PLABDM01: MBSA performing the scan.

You will notice that Windows begins the scanning process by updating security information and downloading data from the Windows site.

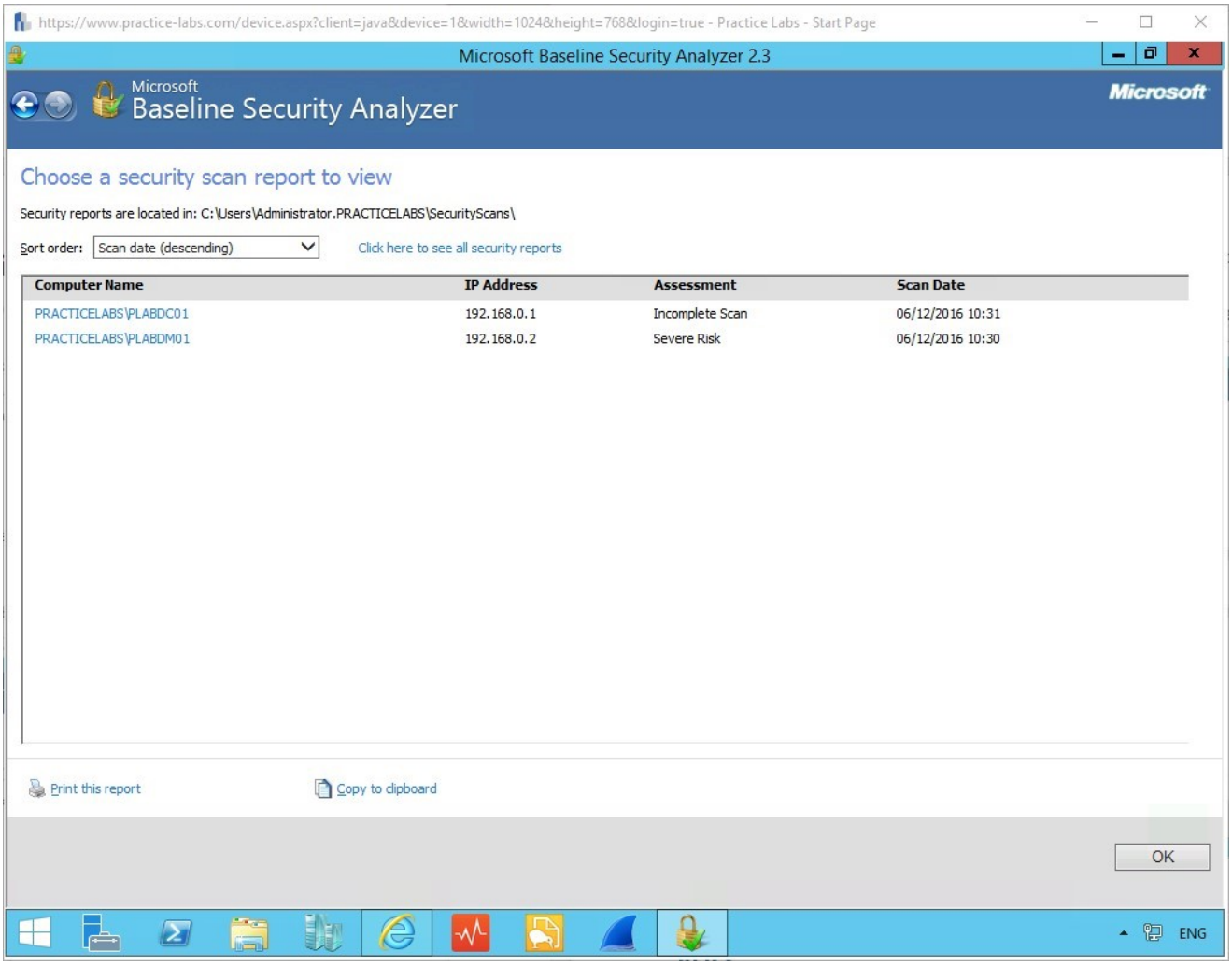


Figure 1.5 PLABDM01: MBSA results summary menu.

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

We will focus on the results of for PLABDM01, therefore click on the **PRACTICELABS\PLABDM01** assessment which is rated as **Severe Risk.**

> ***Note:*** *Scores cannot be changed or reassigned for system configuration checks.*

Task 3 - Reviewing the results of the scan

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

- **A red exclamation mark** is used when a critical check failed (for example, a user has a blank password) for the administrative vulnerability checks.

- **A yellow exclamation mark** is used when a non-critical check failed (for example, an account has a password that does not expire).
- **A green checked mark** shows a check pass.
- **A blue asterisk** presents information on best practice checks (for example, checking if auditing is enabled).
- **A blue informational icon** is used for checks that simply provide information about the computer being scanned (for example, the operating system version of the scanned computer).

When reviewing security updates:

- **A red exclamation mark** confirms a security update is missing or a security check was not performed on the scanned computer.
- **A yellow X** is used for warning messages (for example, the computer does not have the latest service pack or update rollup).
- **A blue star** is used for informational messages indicating that an update is not available to the computer because it has not been approved on the Update Services server.

Step 1

After clicking the outcome of the report for PLABDM01, we can see a generated report for this device.

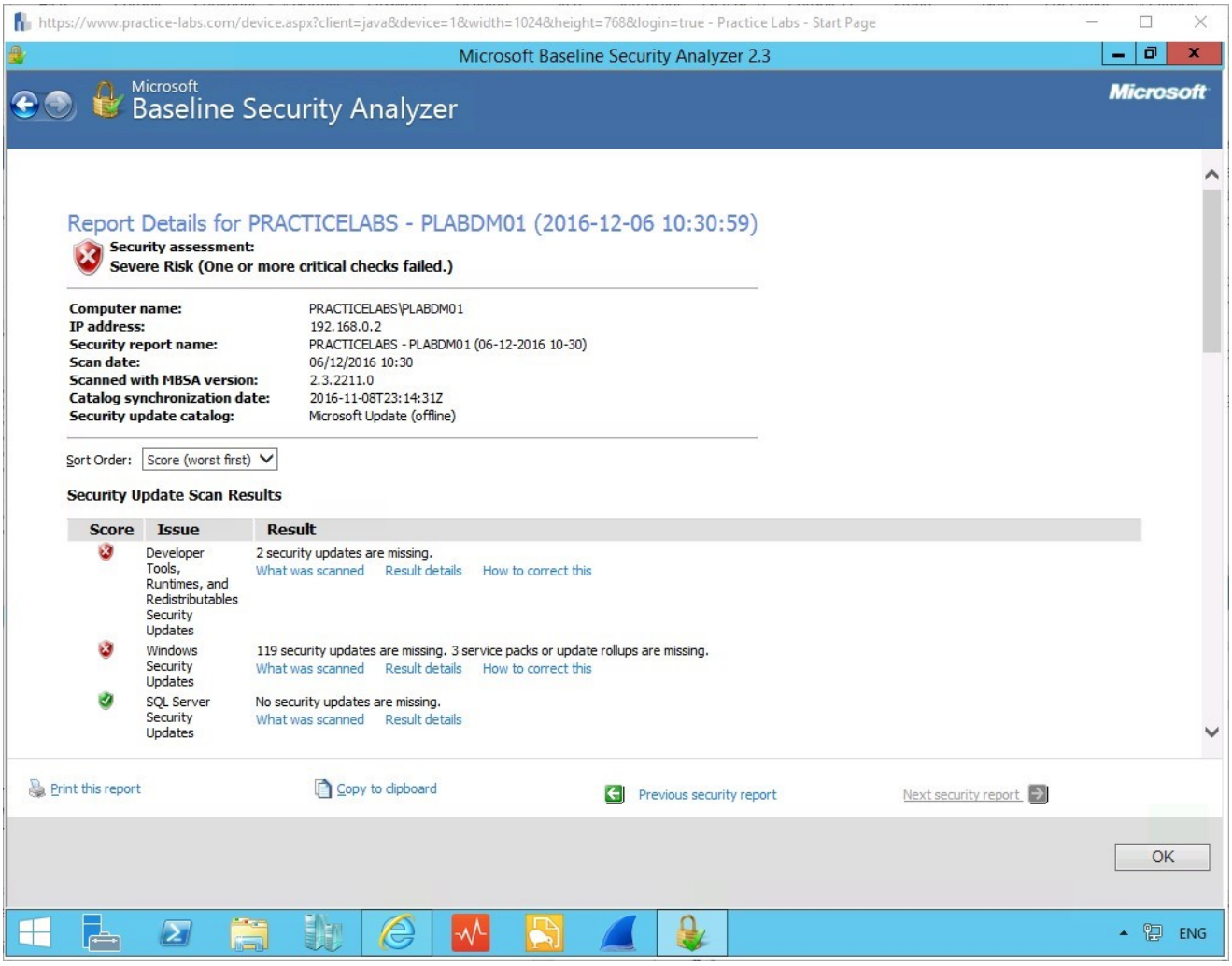


Figure 1.6 PLABDM01: MBSA report screen.

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”.

> ***Note:*** *We have turned off updates that’s why the first Score of Security Updates.*

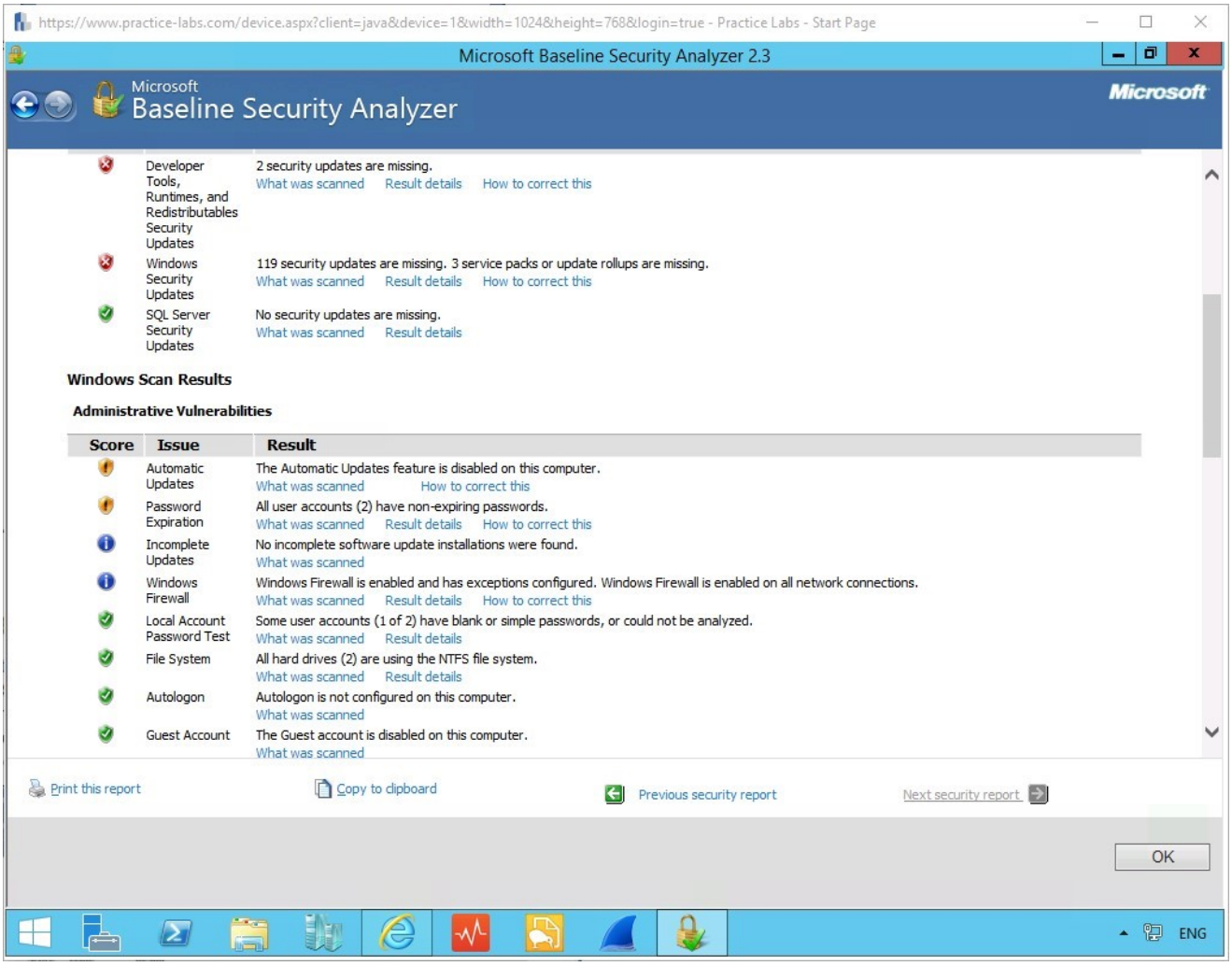


Figure 1.7 PLABDM01: MBSA report screen.

Under the **Windows Scan Results for Administrative Vulnerabilities** click on the result for **Password Expiration**.

There are 3 tabs which we will explore in turn.

Step 3

Let's display the initial results of checked.

Click on **"What was Scanned**". This will automatically open up a page in Internet Explorer where further information can be read.

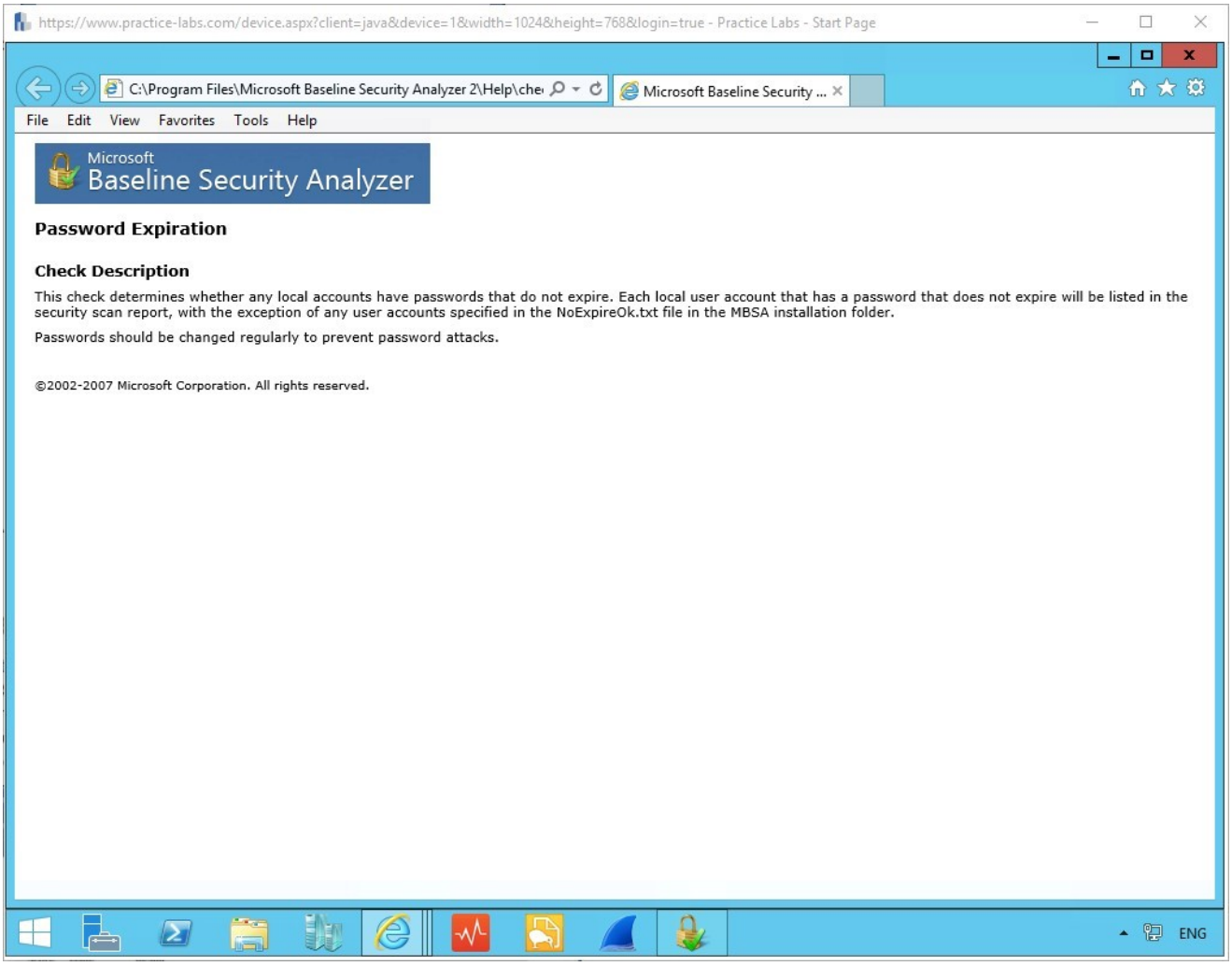


Figure 1.8 PLABDM01: MBSA description page of a result.

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

Step 4

Now exit this screen by clicking on the red cross and click on **Result Details**.

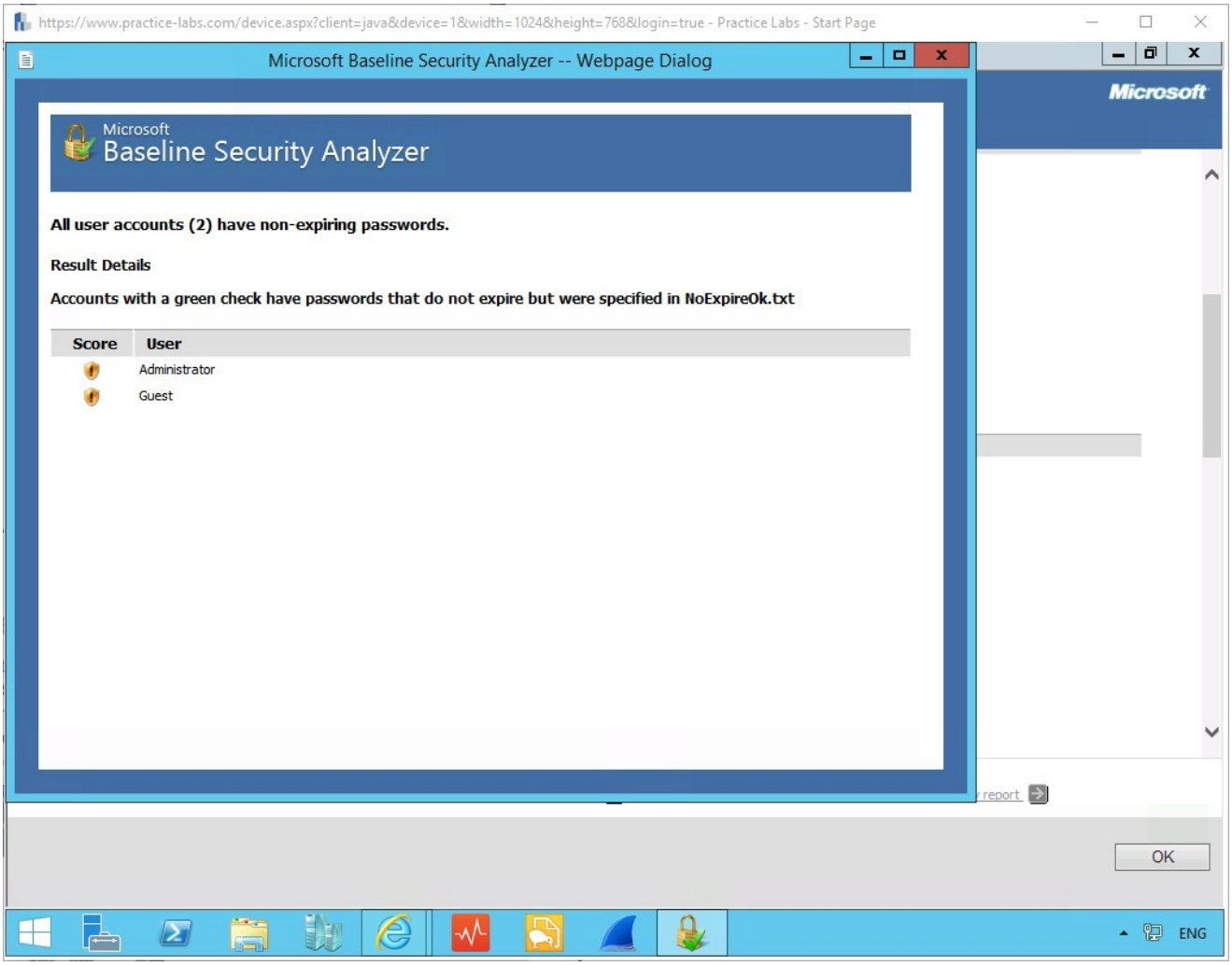


Figure 1.9 PLABDM01: MBSA report result details screen.

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

Step 5

Now click on the button **How to Correct this**.

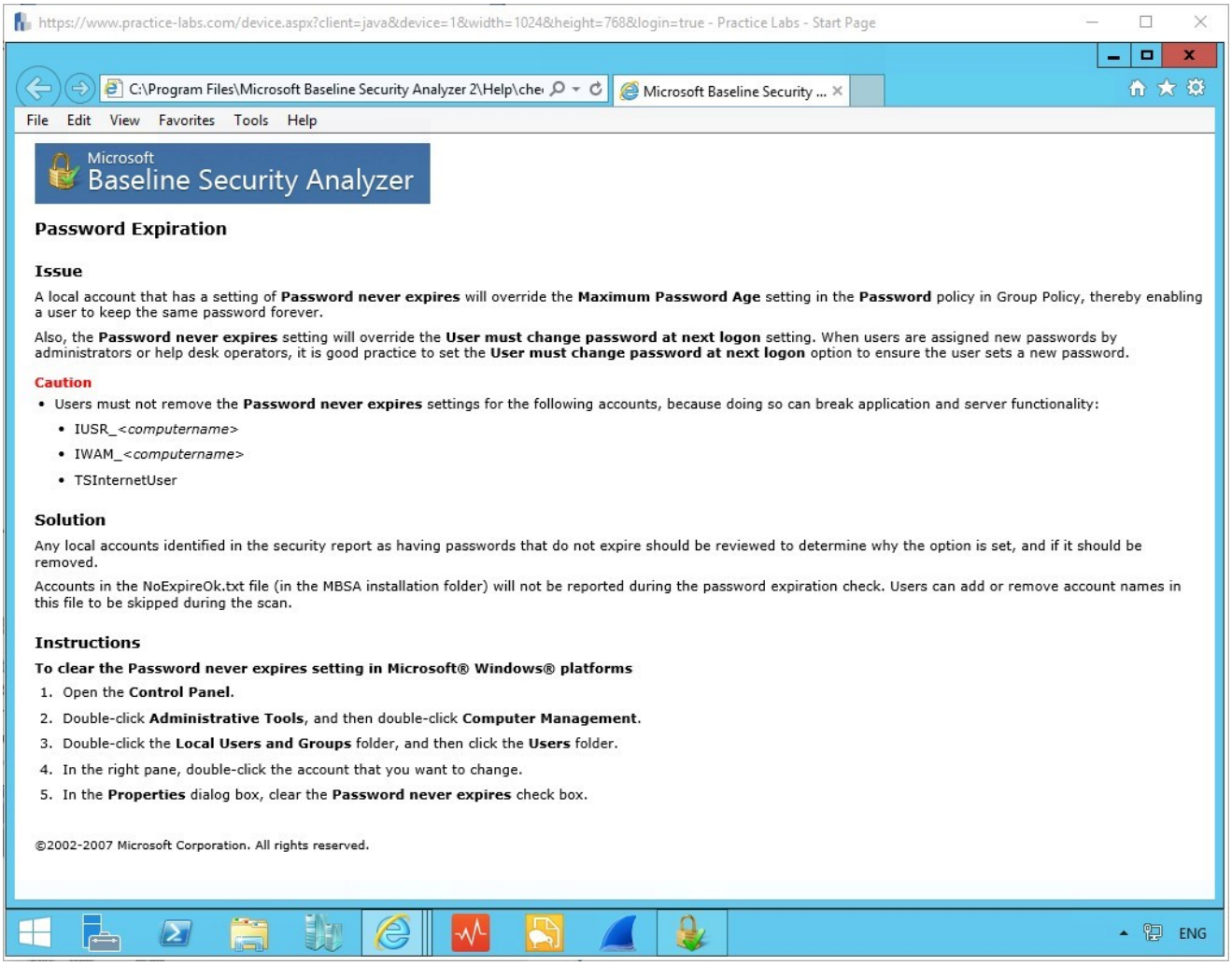


Figure 1.10 PLABDM01: MBSA remediation details.

We are presented with the Issue and even a caution on changing account details for specific situations. Finally we are presented with the solution on correcting the problem.

We will now follow these steps to make sure we are protected against this for the Guest and Administration accounts.

> Leave all devices powered on in their current state and proceed to the next exercise.

Exercise 2 - Implementing Recommendations

Once a result has been confirmed, we must action changes against the configuration recommendations or at least have valid arguments for maintaining the device

specifications. Here we will reset the password controls to keep them in line with best practice.

In this exercise you will complete the following tasks:

- Clearing password settings

Please refer to your course material or use your favorite search engine to research for more information about this topic.

Task 1 - Clearing password settings

We begin by tracking down the area where password controls are stored and edited.

Step 1

Let's open the control panel by right clicking on the **Start** menu icon.

Then click on the **Control Panel** option.

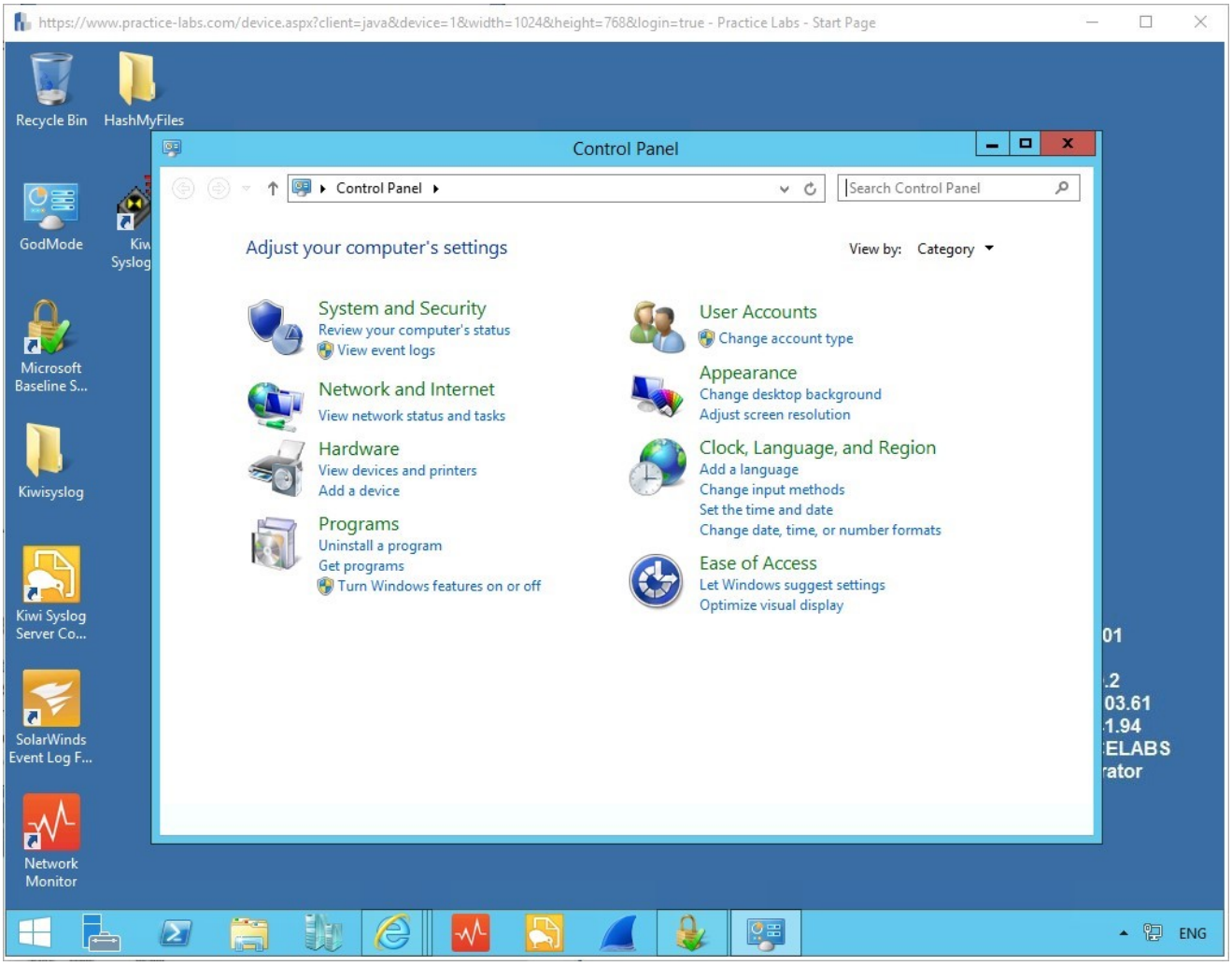


Figure 2.1 PLABDM01: Control Panel

Step 2

Click **Next** on **System and Security,** and you will find **Administrative tools** at the bottom of the menu.

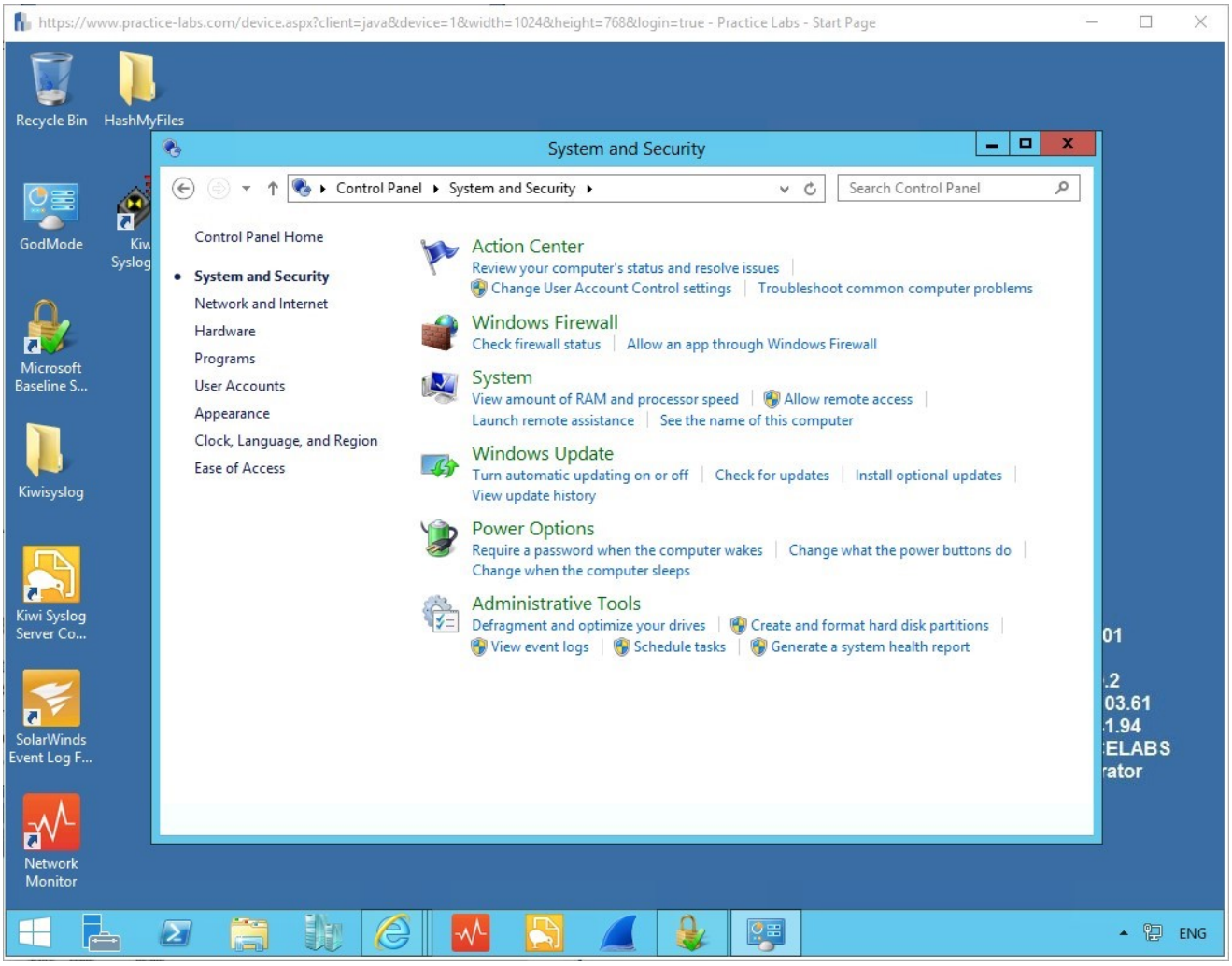


Figure 2.2 PLABDM01: Systems and Security panel.

Note: *Alternatively, you can search for the Administrative tool with the search bar of windows if preferred. Sometimes this can be faster and less convoluted.*

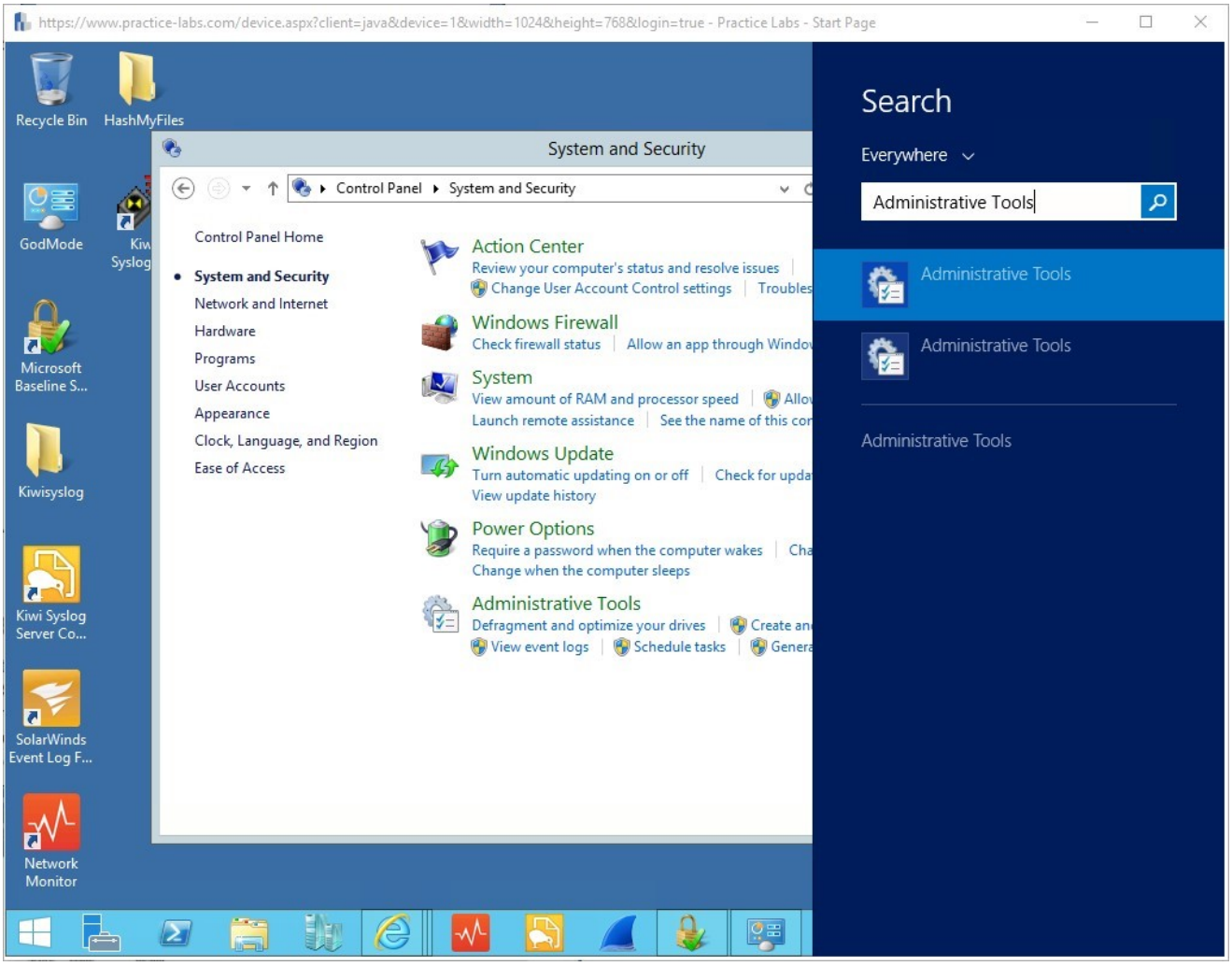


Figure 2.3 PLABDM01: Using the Search Menu for Administrative Tools.

Step 3

Now click on **Computer Management**.

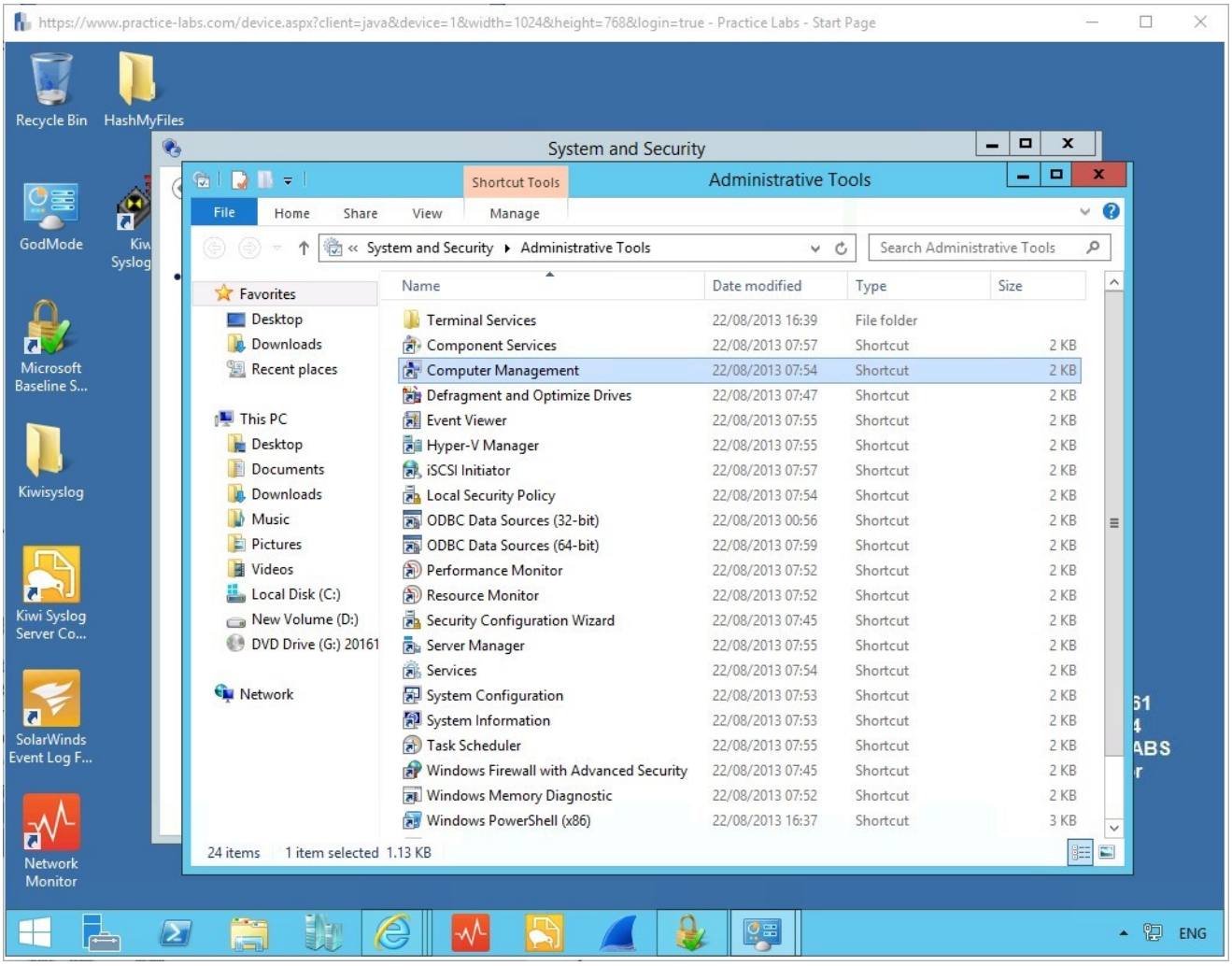


Figure 2.4 PLABDM01: Administrative Tools panel.

Step 4

Navigate to the Local Users and Groups folder found in the left column, and then click the Users folder to display the accounts for Administrator and Guest.

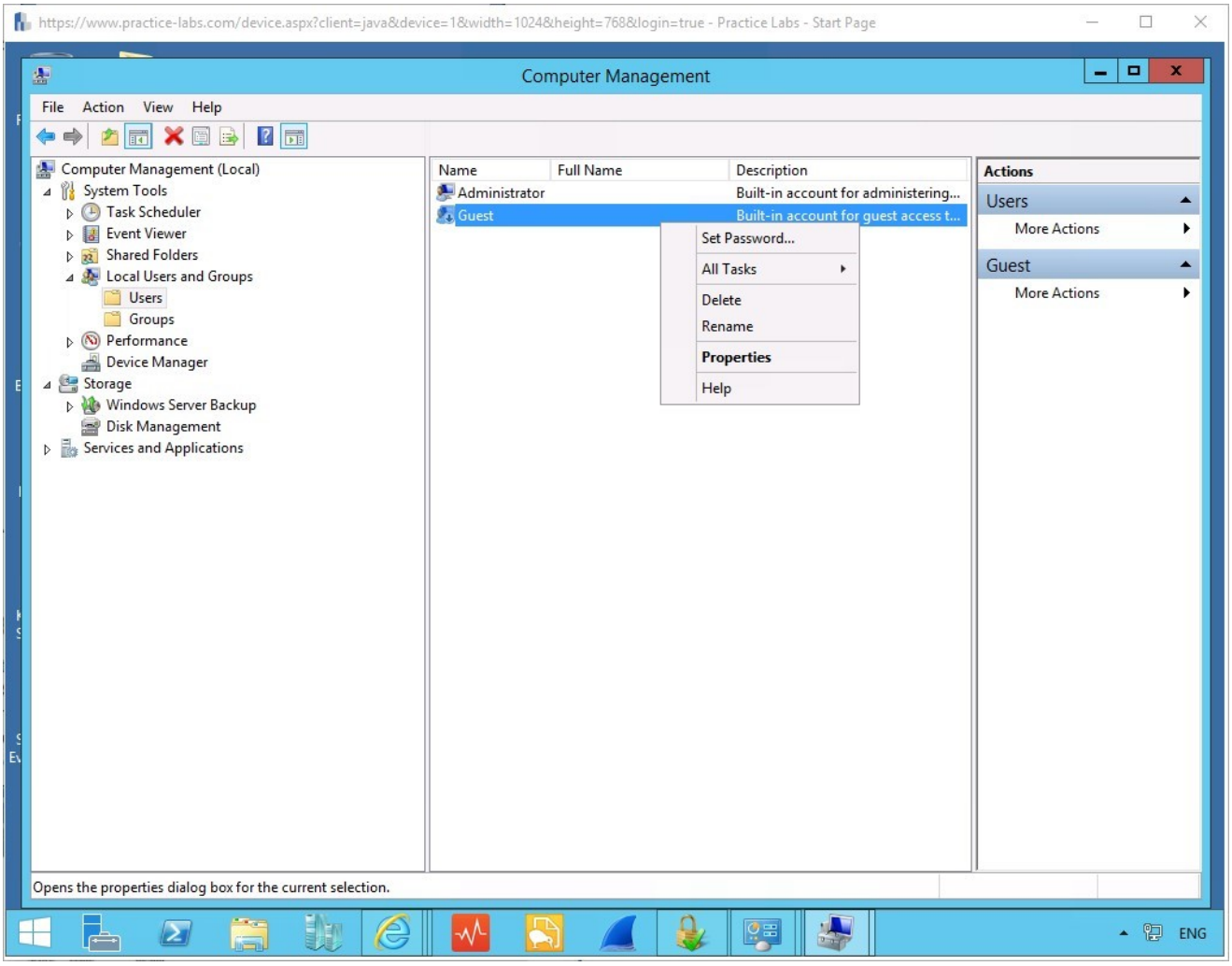


Figure 2.5 PLABDM01: Computer Management interface.

Step 5

Right-click on the **Guest** account and go to **Properties**.

On the **General** tab uncheck the **Password never expires** option.

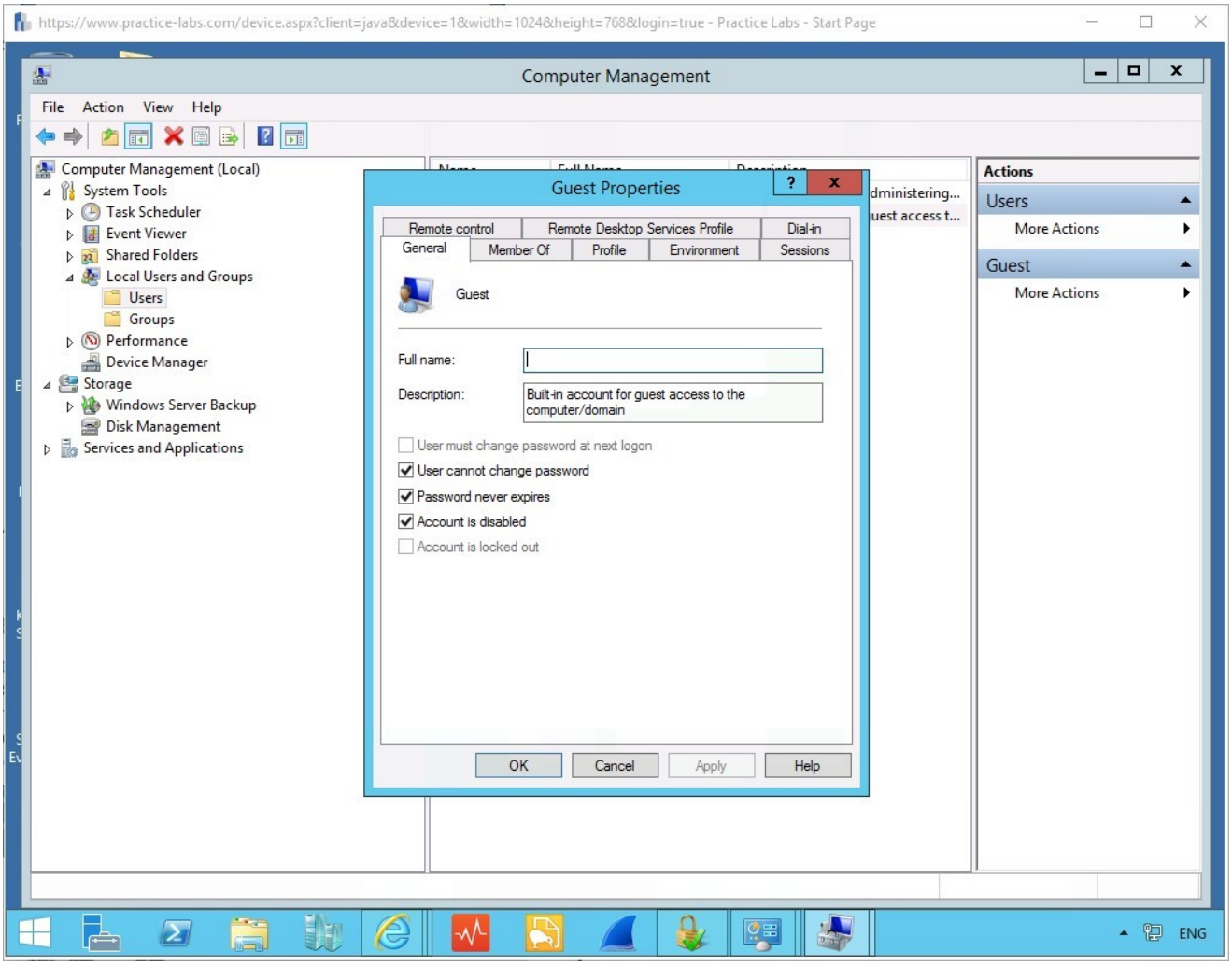


Figure 2.6 PLABDM01: Guest Properties being accessed to change the Password Expiration.

Press the **Apply** button to confirm this action.

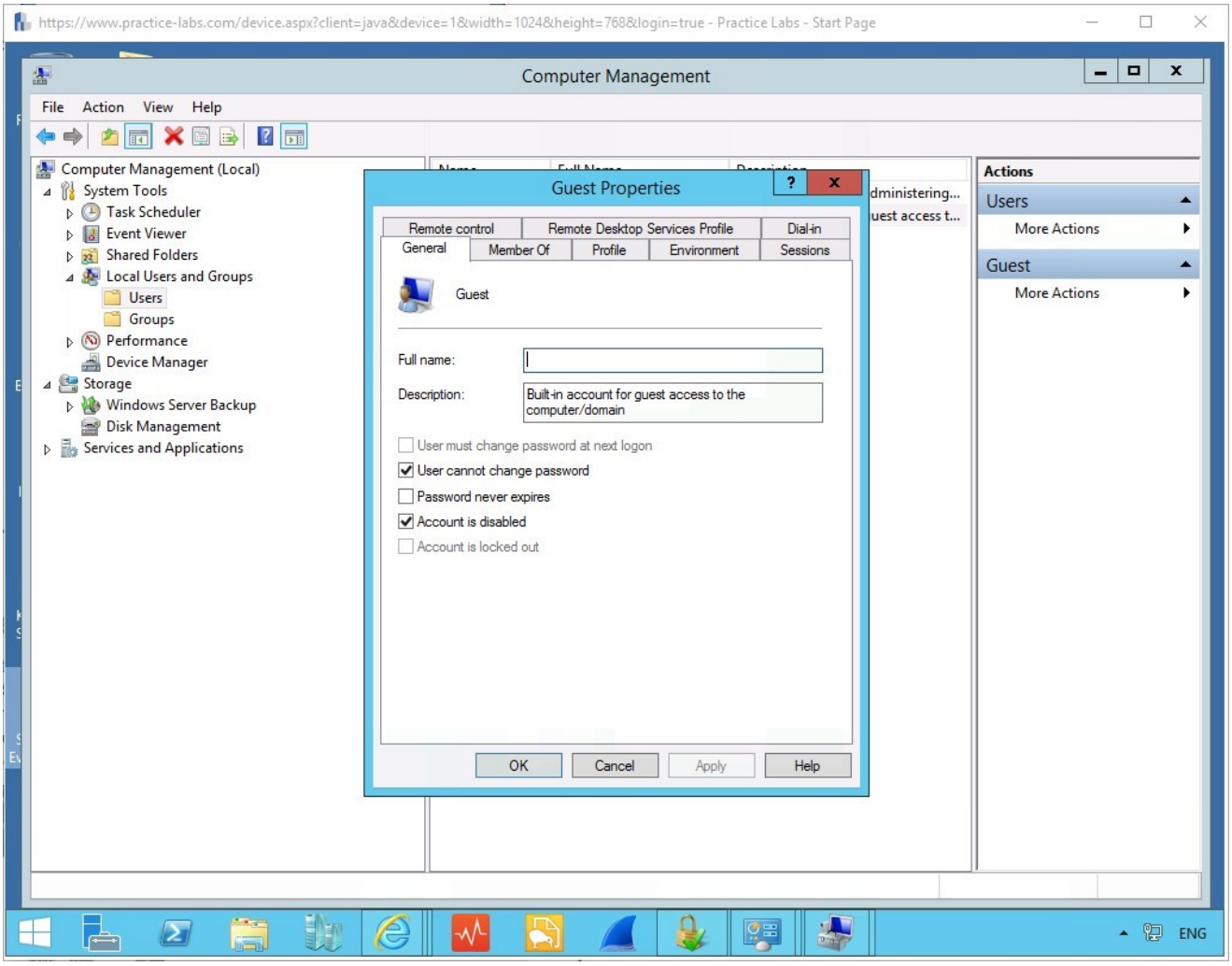


Figure 2.7 PLABDM01: Guest Properties being accessed to change the Password Expiration.

Once completed, perform the same action for the **Administrator** role.

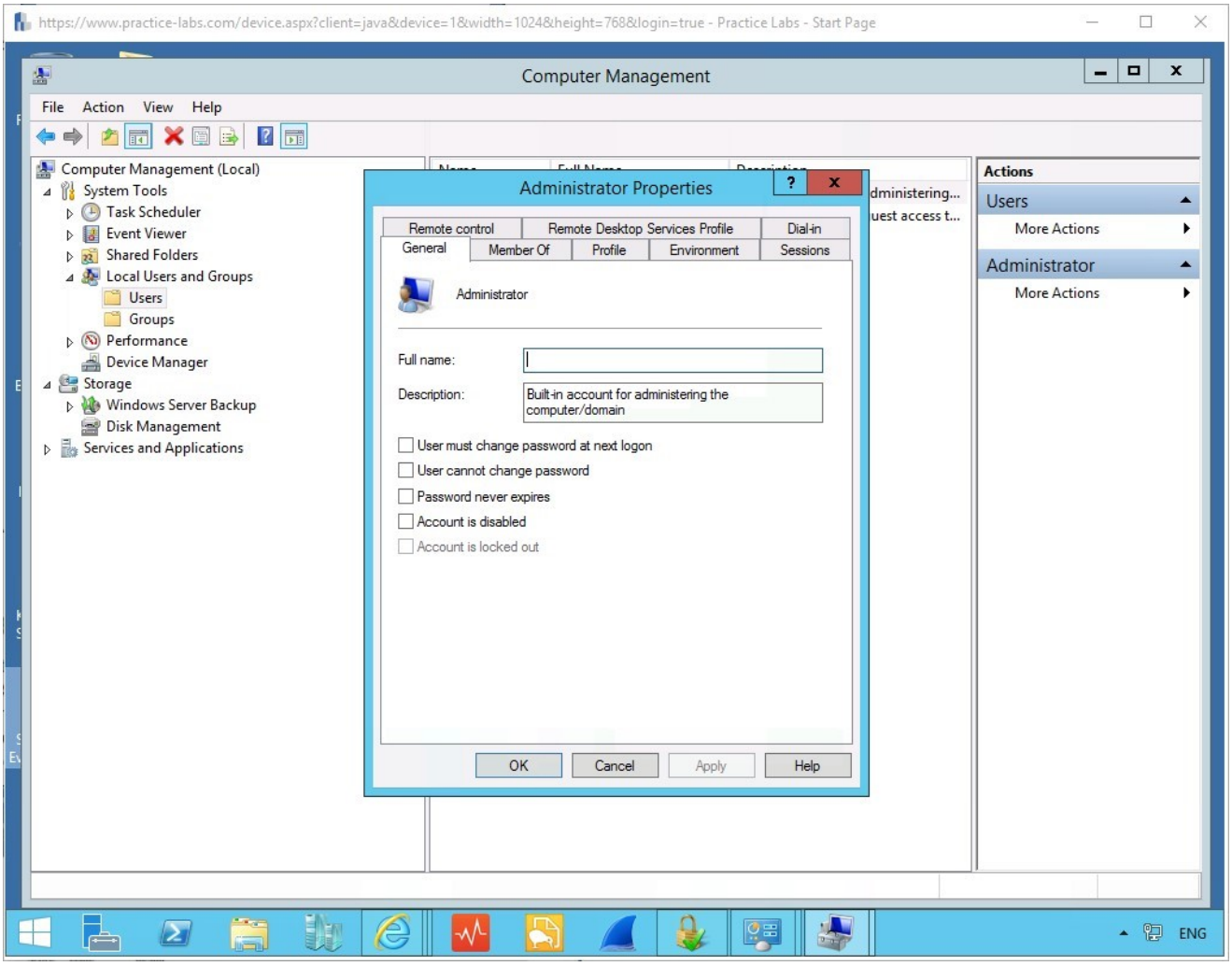


Figure 2.8 PLABDM01: Administrator Properties being accessed to change the Password Expiration.

As seen above we have now completed those security actions for both the Guest and Administrator Roles.

You can now close those screens.

Leave all devices powered on in their current state and proceed to the next exercise.

Exercise 3 - Saving Microsoft Security Baseline Analyzer Reports

Reports are a key feature of the audit trail; here we are auditing the configuration a server device and logging the information for the situation in the future where accountability is

a necessity for tracking changes to the network topology.

In this exercise you will complete the following tasks:

- Saving the report

Please refer to your course material or use your favorite search engine to research for more information about this topic.

Task 1 - Saving the 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

Click on the **Print this report** button, located towards the bottom left-hand corner of the application.

We will be printing to a file for the moment.

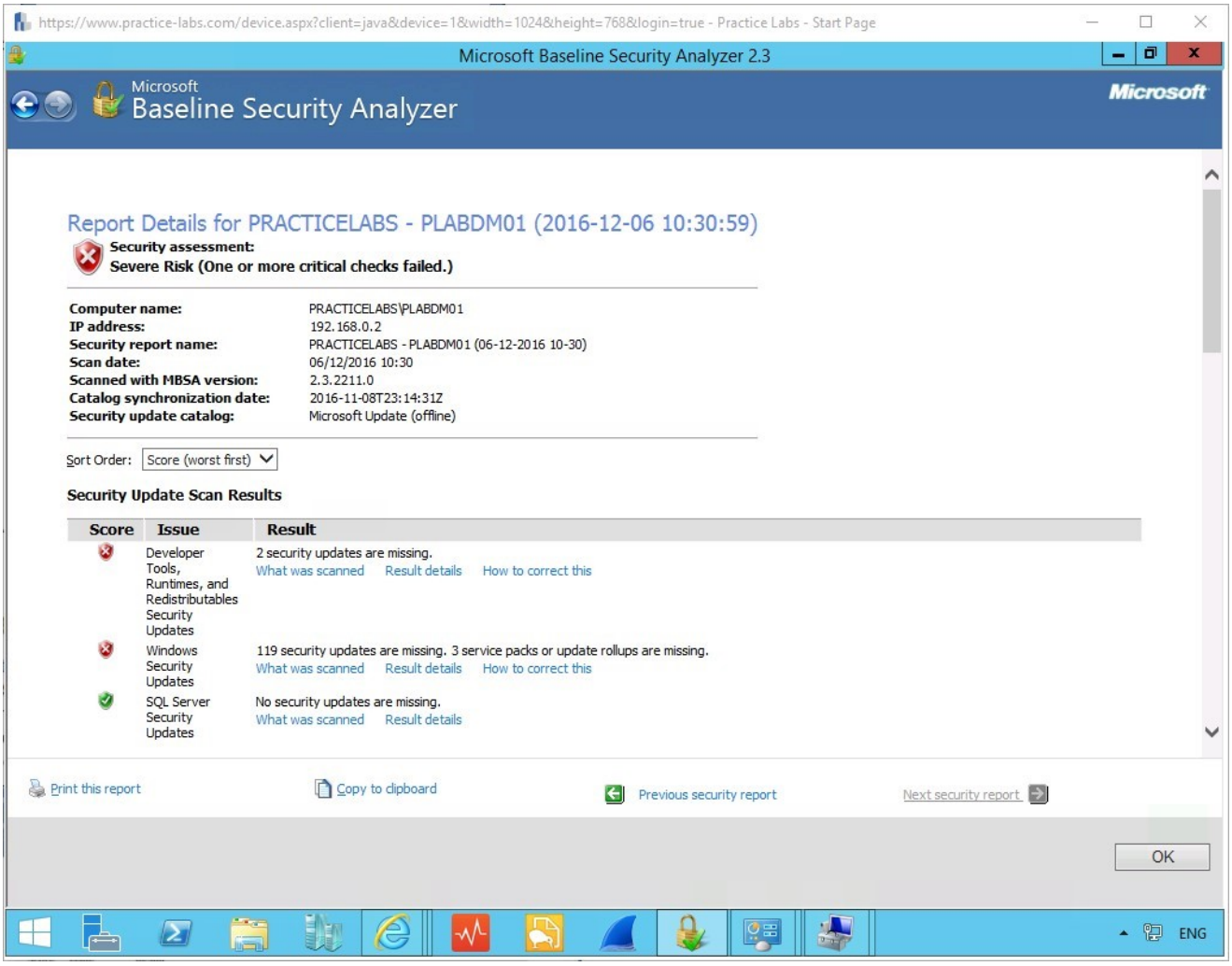


Figure 3.1 PLABDM01: MBSA menu screen with Print this report found bottom left.

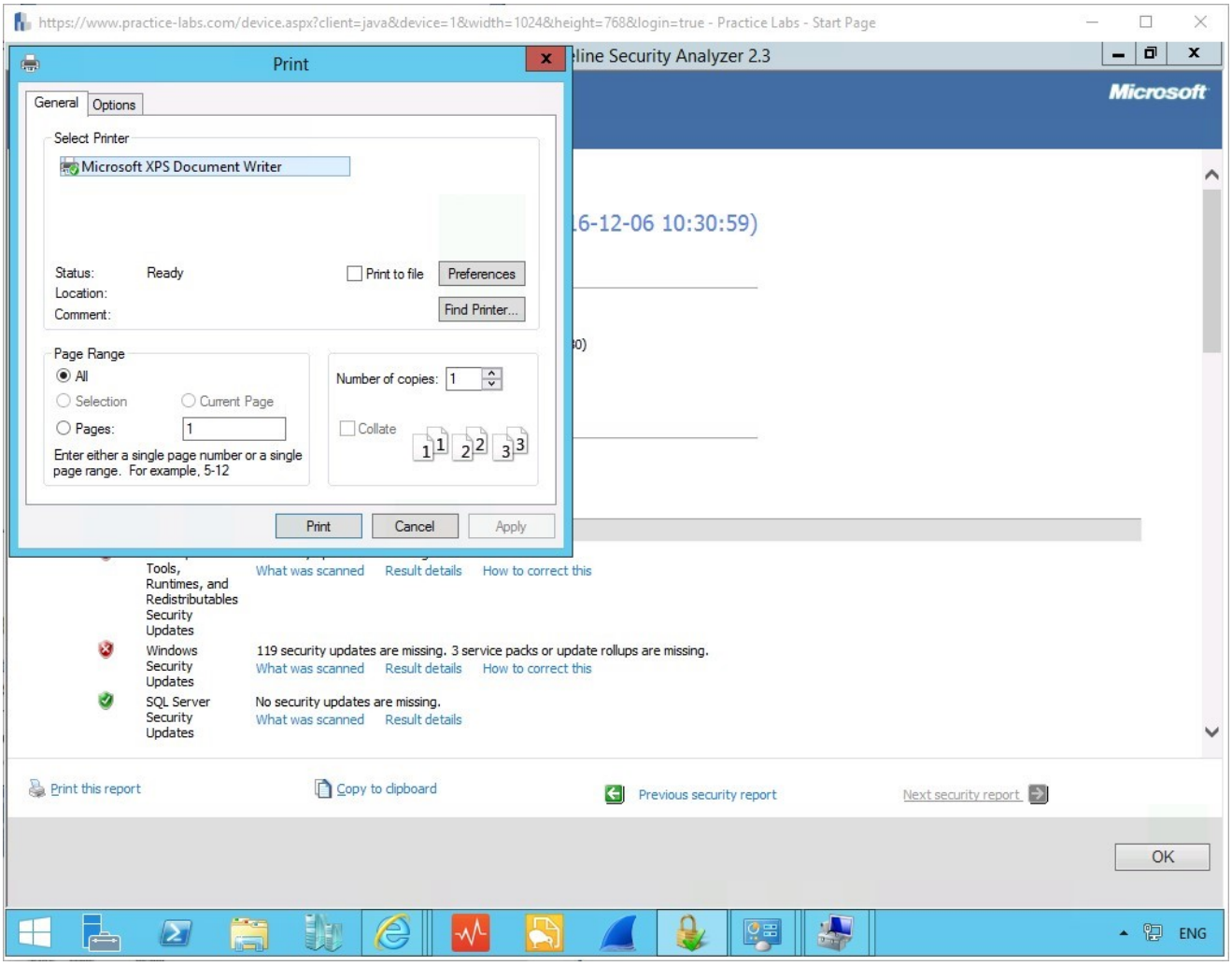


Figure 3.2 PLABDM01: MBSA print interface.

Step 2

Double-click the **Microsoft XPS Document Writer**.

Then click the **Print** button

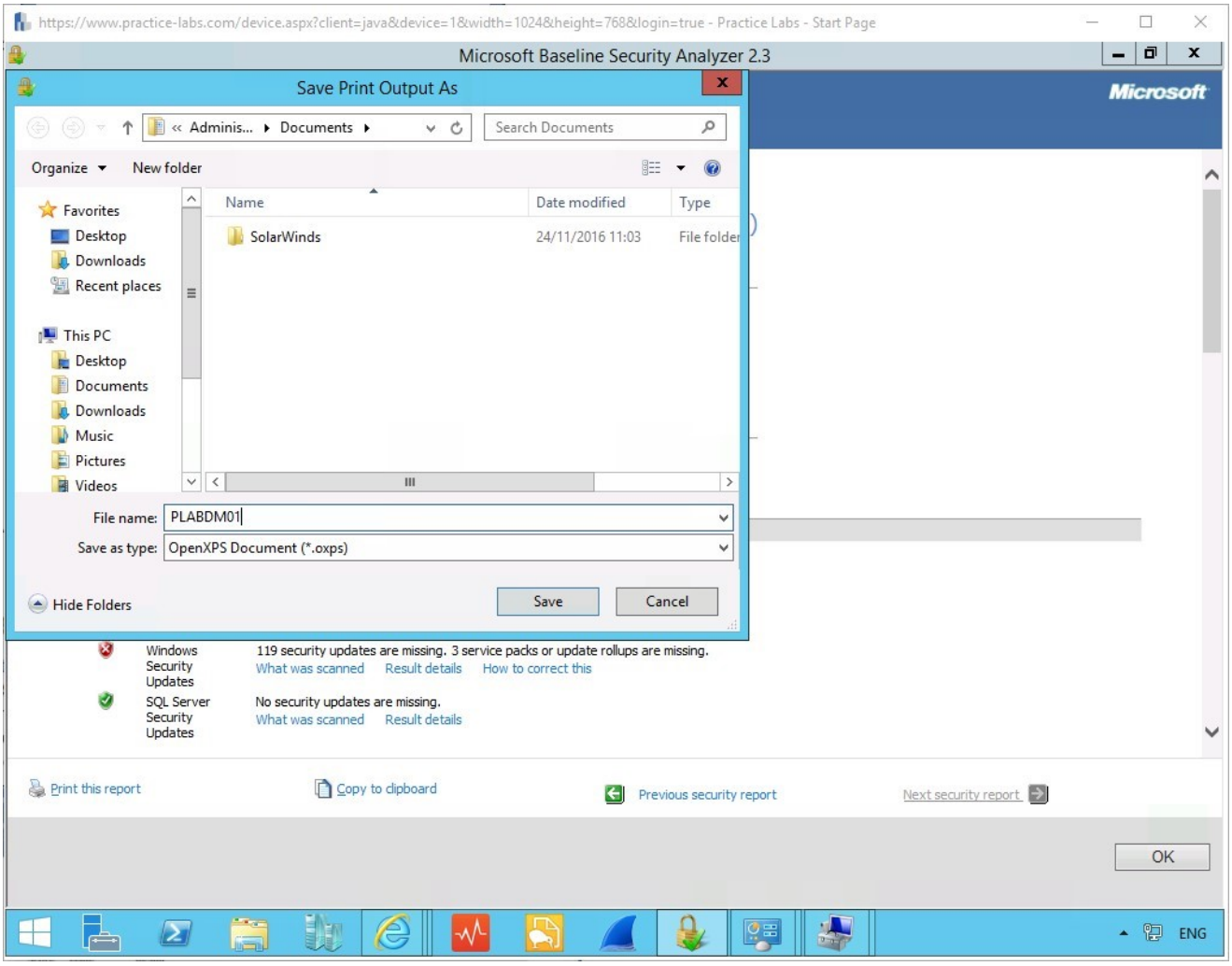


Figure 3.3 PLABDM01: MBSA saving the file to Documents.

Name the file **PLABDM01**, keep the extension as .oxps and save the file to the **Documents**.

Now minimize the application where you should see the file has been saved to the Documents Folder, open it up and confirm the report results.

Step 3

Navigate to the **Documents** folder.

Double-click the file to read the output of the report.

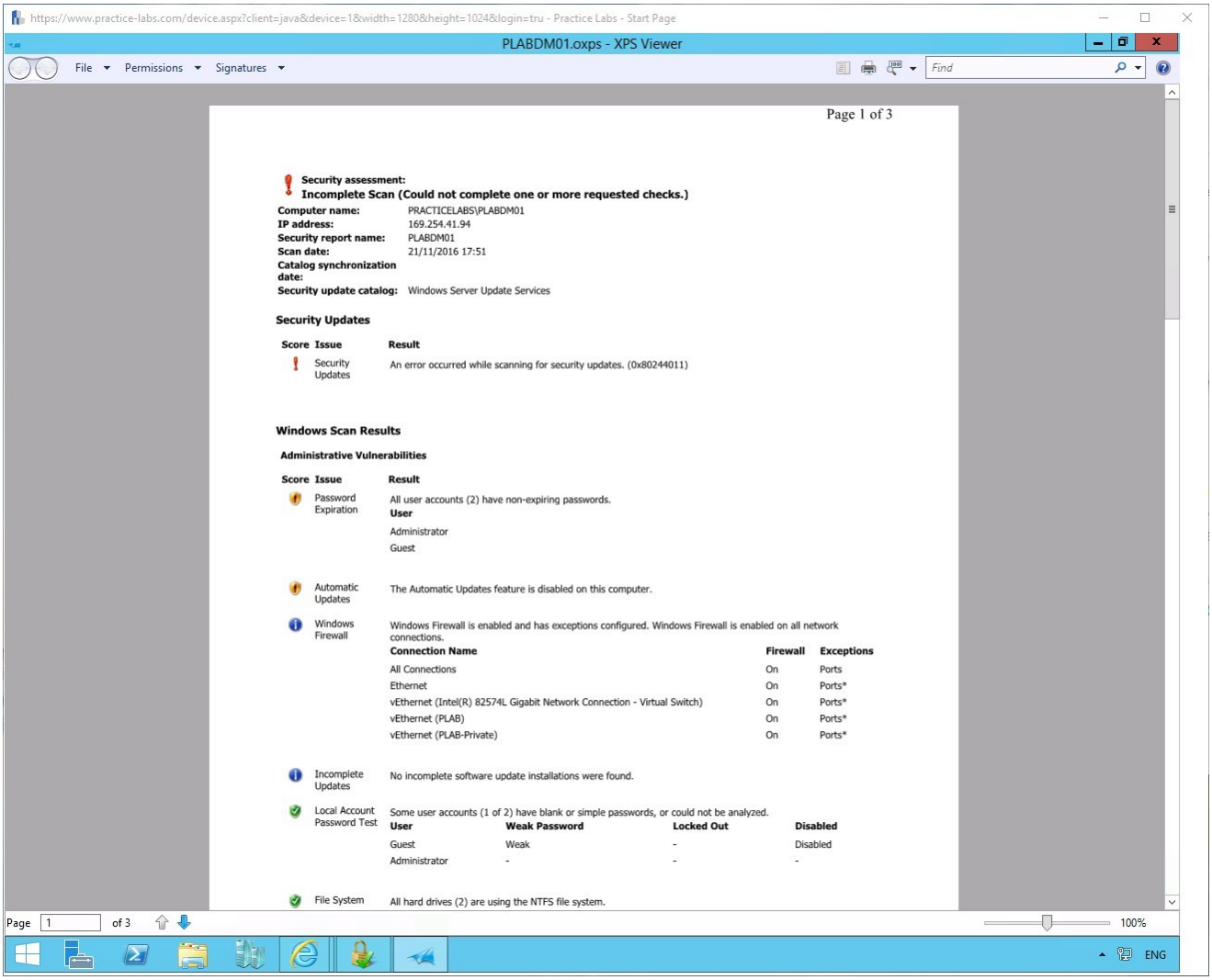


Figure 3.4 PLABDM01: MBSA opening up the report in XPS viewer.

This file is in fact part of the auditing performed against windows machines, and typically it would be kept as a record of actions which have been taken and recognized.

It will provide a verbose amount of information, for example, if you scroll down the page, you will see the Windows updates which are required.

Leave all devices powered on in their current state and proceed to the next exercise.

Exercise 4 - Reviewing Configuration Changes

Once changes have been made to the device, these need to be checked by MBSA to see that they pass the configuration requirements. Therefore, we will move through these

steps more briskly to complete this requirement.

In this exercise you will complete the following tasks:

- Activate the scanner

Please refer to your course material or use your favorite search engine to research for more information about this topic.

Task 1 - Activate the scanner

Maximize the scanner, and use the **Back** button to navigate through the screen results to the Start Scan page where we placed the IP range into the device.

Step 1

Now click on the **Start Scan** button again to activate the scan.

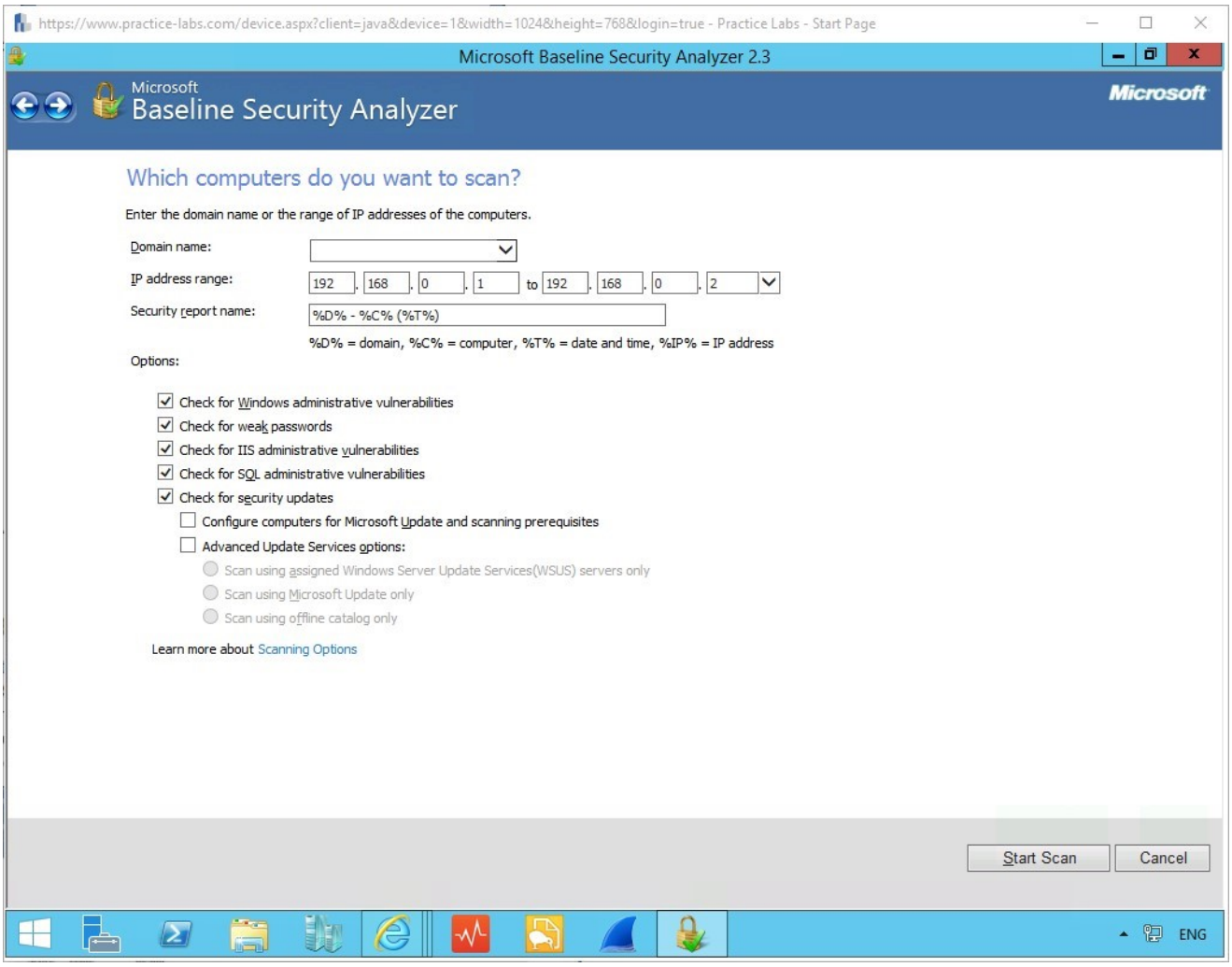


Figure 4.1 PLABDM01: MBSA reactivating the scanner.

Again scroll to the area where we see the results for Administrative Vulnerabilities, if all was completed correctly, we should no longer see that issue.

Step 2

Again following the previous procedure if you look at the scan results, the **Password Expiration** is now in the green. This result shows that we have configured the requirement correctly.

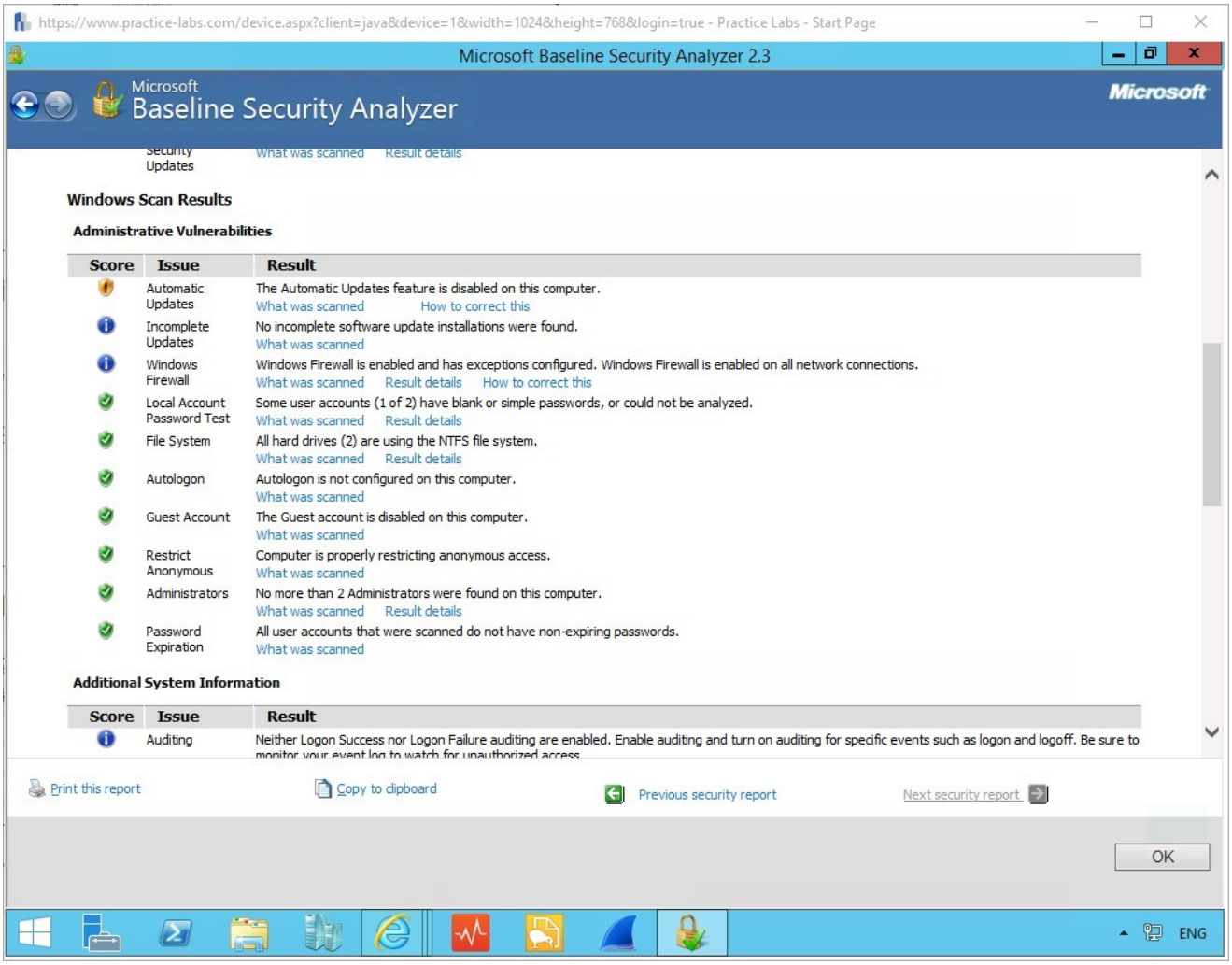


Figure 4.2 PLABDM01: MBSA looking at the results again.

Shut down all virtual machines used in this exercise using Practice Labs power button function to revert these devices to their default settings. Alternatively, you may sign out of the lab portal to power down all devices.

Summary

You covered the following activities in this module:

- Configuration of Microsoft Security Baseline Analyzer
- Remediation Against the Result
- Microsoft Security Baseline Analyzer Saving the Report
- Rechecking after Configuration Changes