Practice Labs - Ethical Hacker v10

Vulnerability Analysis

- **Introduction**
- **Lab Topology**
- **Exercise 1 - Performing a Vulnerability Scan**
- **Exercise 2 - Introducing Microsoft Baseline Security Analyzer (MBSA)**
- **Exercise 3 - Implementing Recommendations**
- **Exercise 4 - Saving Microsoft Baseline Security Analyzer Reports**
- **Exercise 5 - Analyze Vulnerability Scan Results and Prioritize Activities**
- **Review**

Introduction

Vulnerability Scanning
Vulnerability Analysis
OpenVAS
Ethical Hacking
Microsoft Baseline Security Analyser (MBSA)
Nikto
Lynis

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.

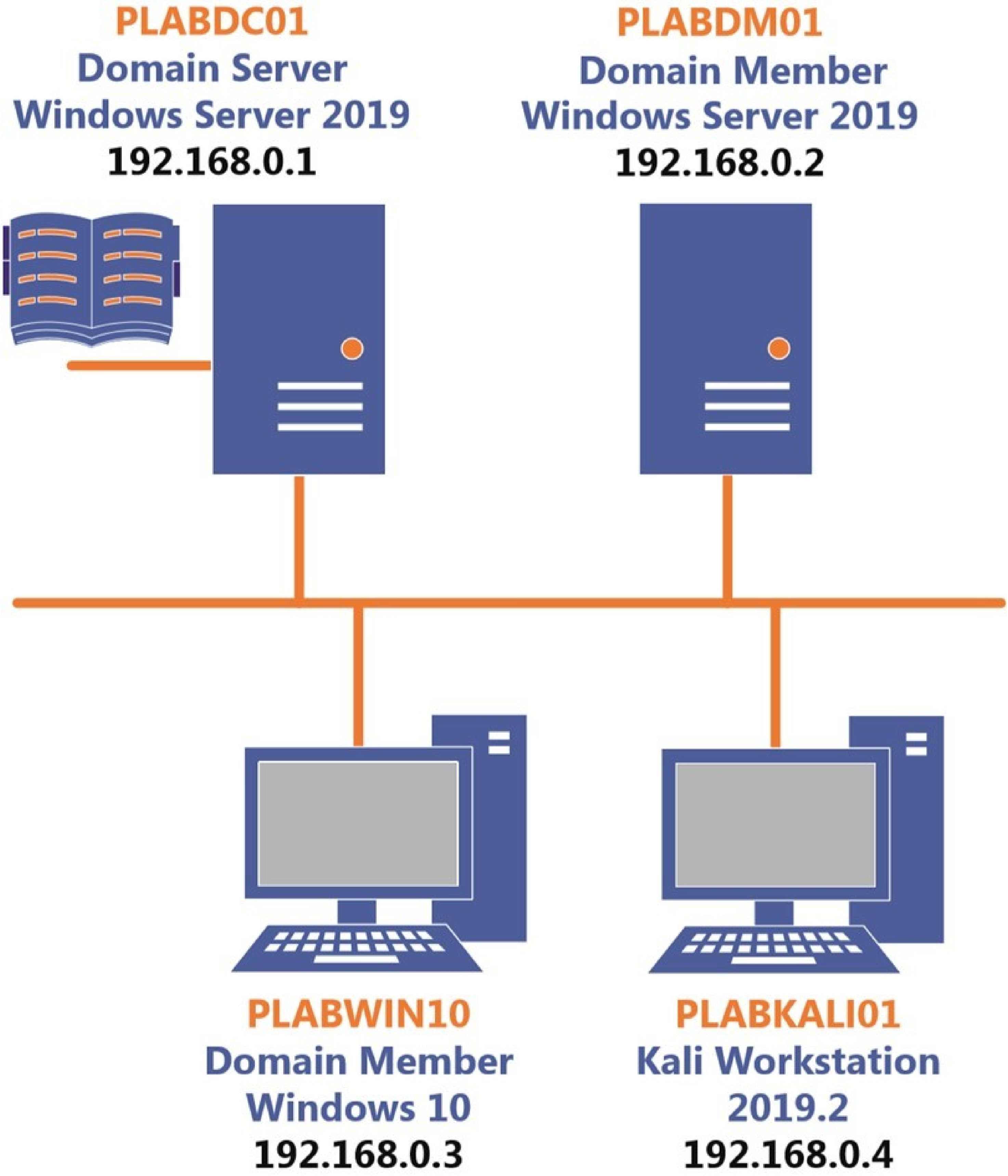
Help and Support

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.

- **PLABDC01 -** (Windows Server 2019 - Domain Server)
- **PLABDM01 -** (Windows Server 2019 - Domain Controller)
- **PLABWIN10 -** (Windows 10 - Workstation)
- **PLABKALI01 -** (Kali 2019.2 - Linux Kali Workstation)

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

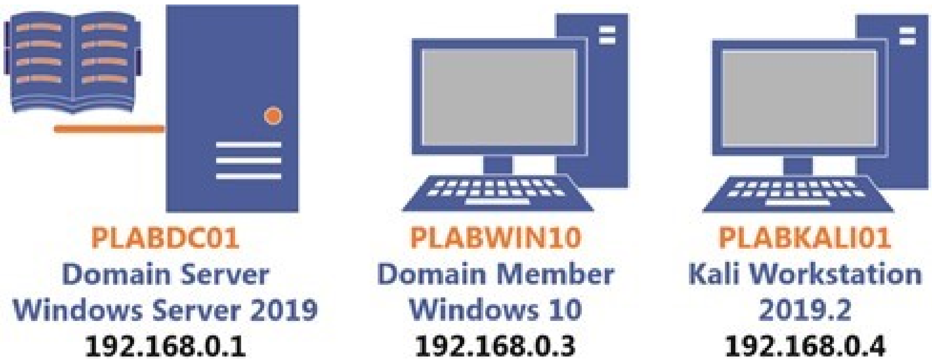
After completing this exercise, you will be able to:

- 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)
- **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 **PLABKALI01**.

Credentials are:

Username:

```
root
```

Password:

```
Passw0rd
```

The desktop of **PLABKALI01** is displayed.

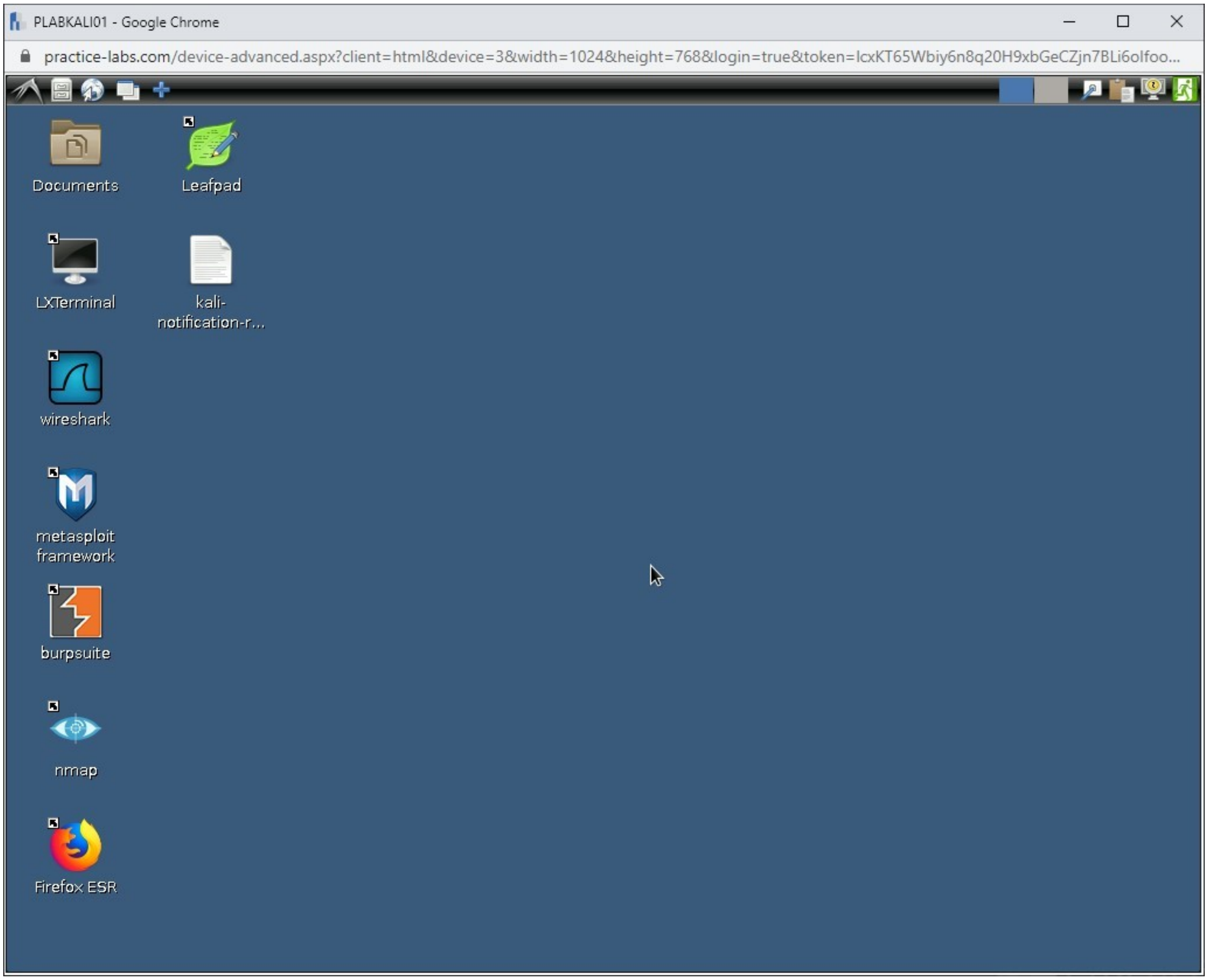

PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
Documents
Leafpad
LXTerminal
kali-notification-r...
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR

Figure 1. 1 Screenshot of PLABKALI01: Showing the desktop of PLABKALI01.

Step 2

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

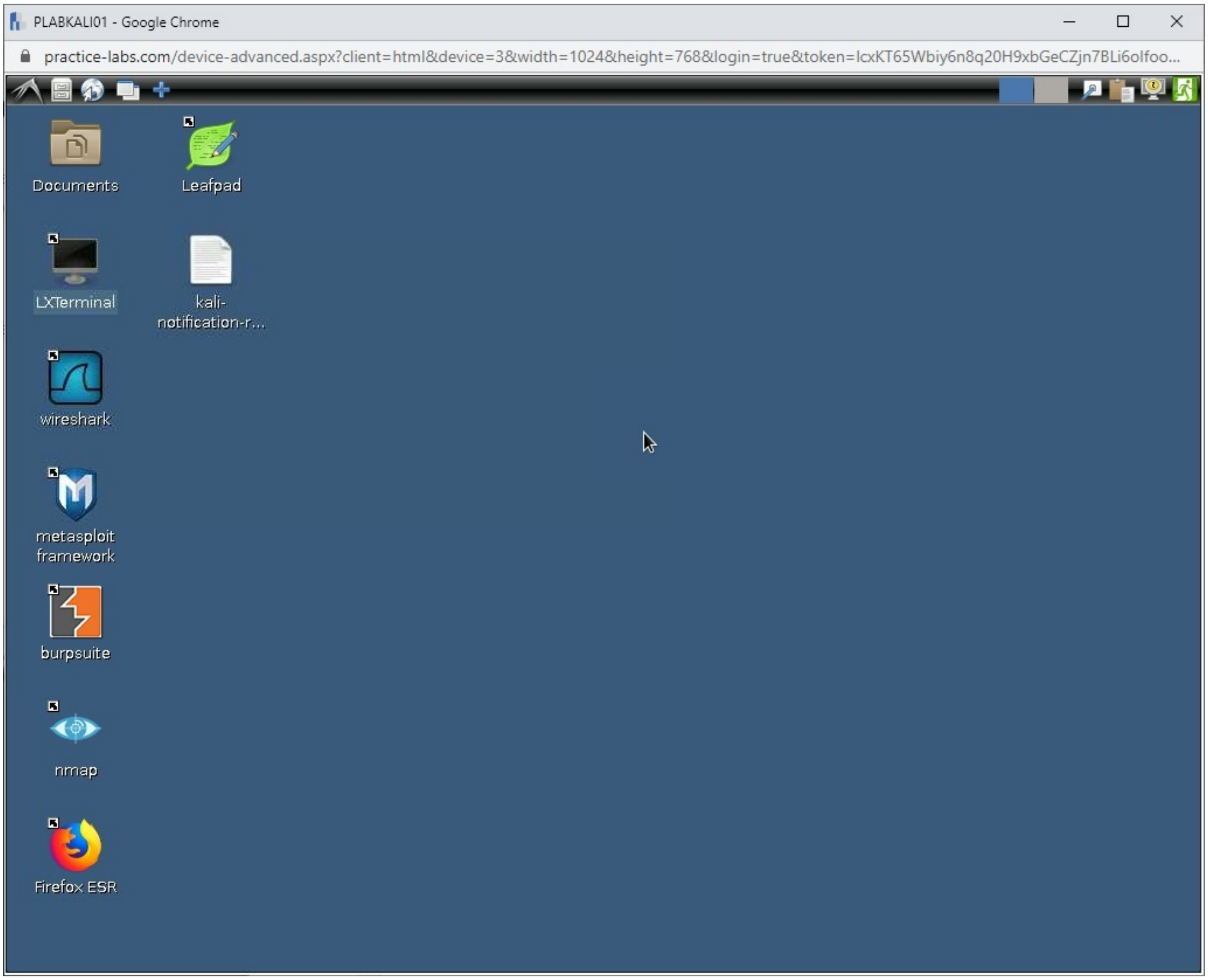

PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
Documents
Leafpad
LXTerminal
kali-notification-r...
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR

Figure 1.2 Screenshot of PLABKALI01: Double-clicking the Terminal icon towards the left side of the screen.

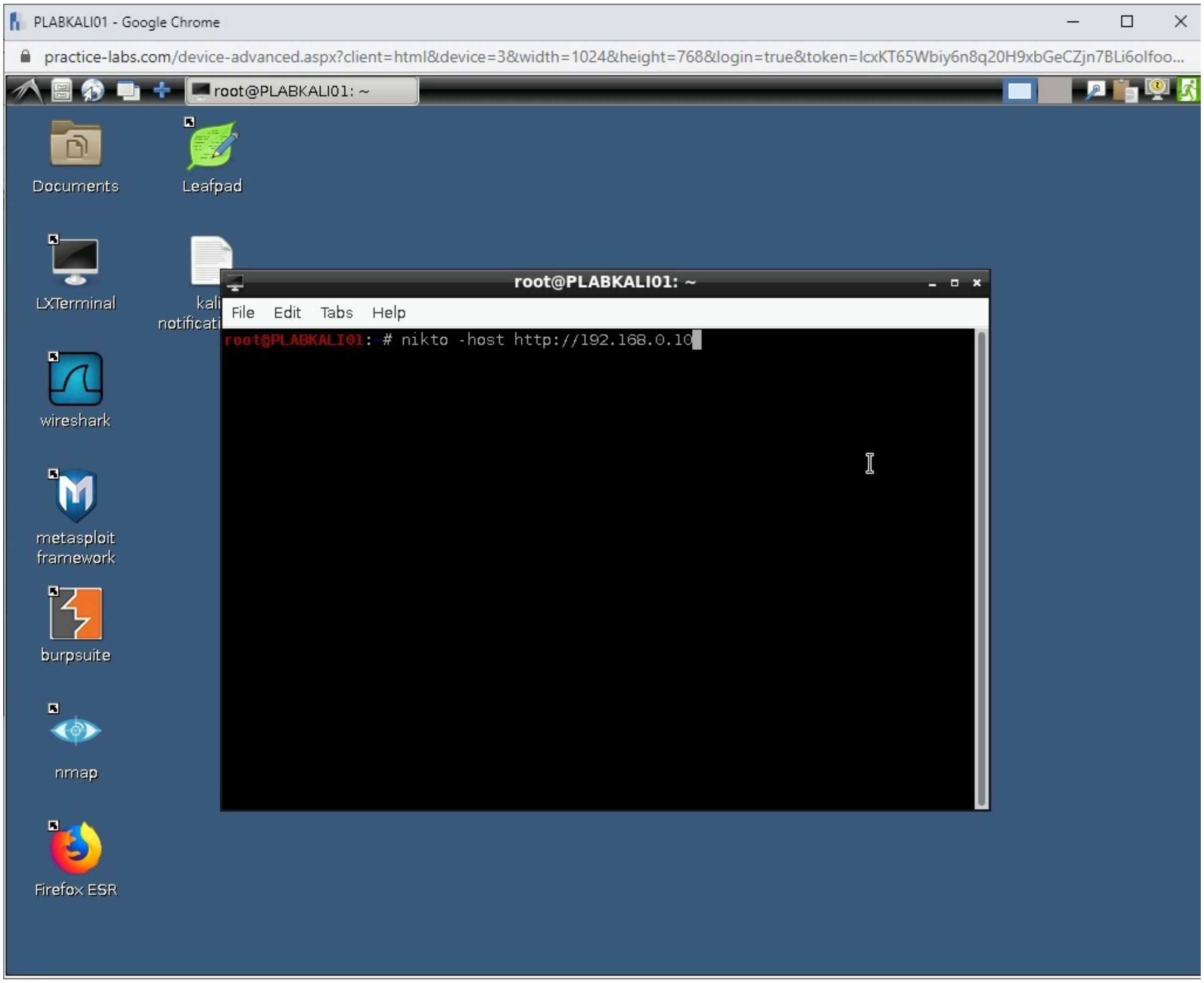
Step 3

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**.



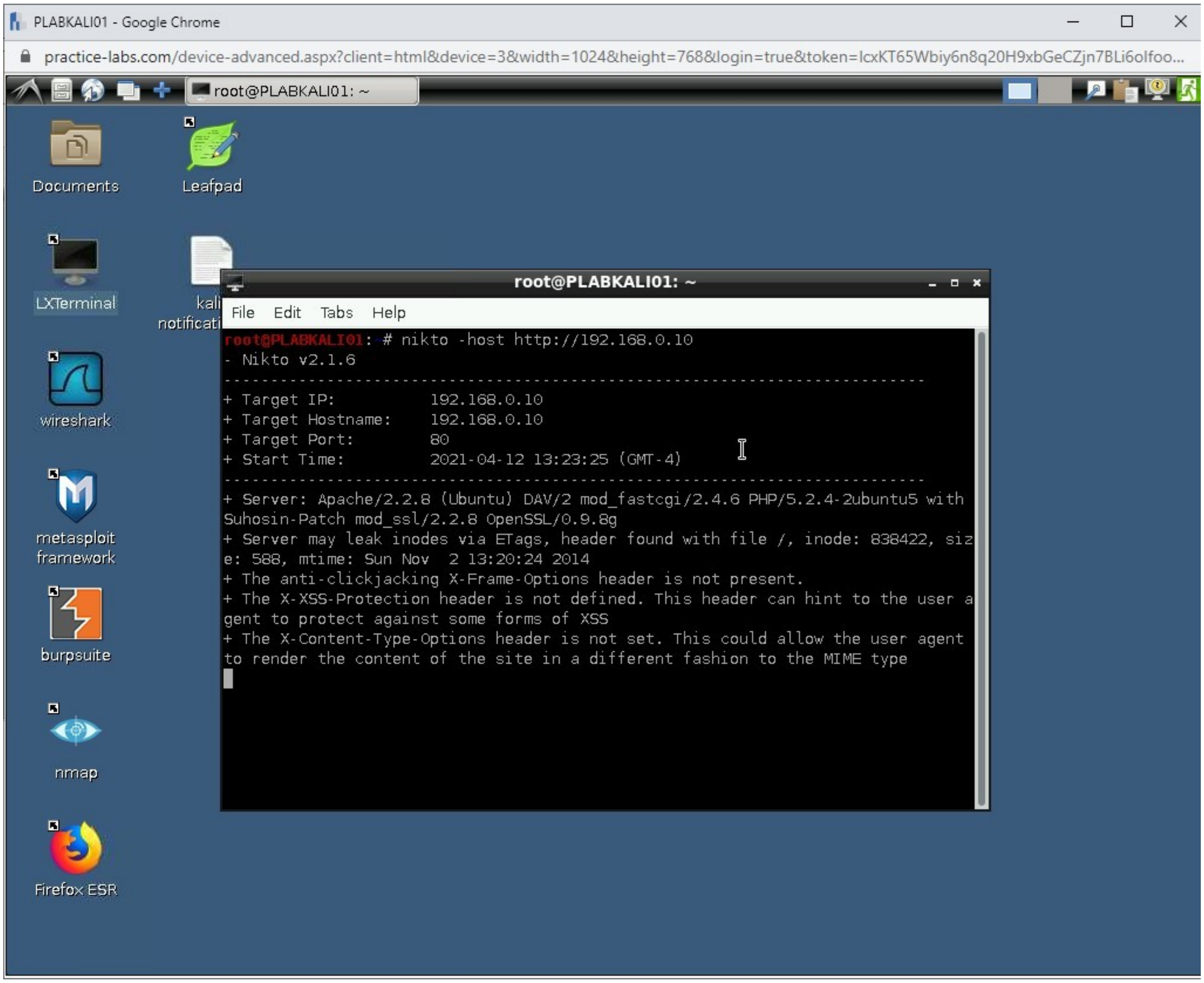
PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
root@PLABKALI01: ~
Documents
Leafpad
LXTerminal
kali notificati
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR
root@PLABKALI01: ~
File
Edit
Tabs
Help

```
root@PLABKALI01: ~# nikto -host http://192.168.0.10
```

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.

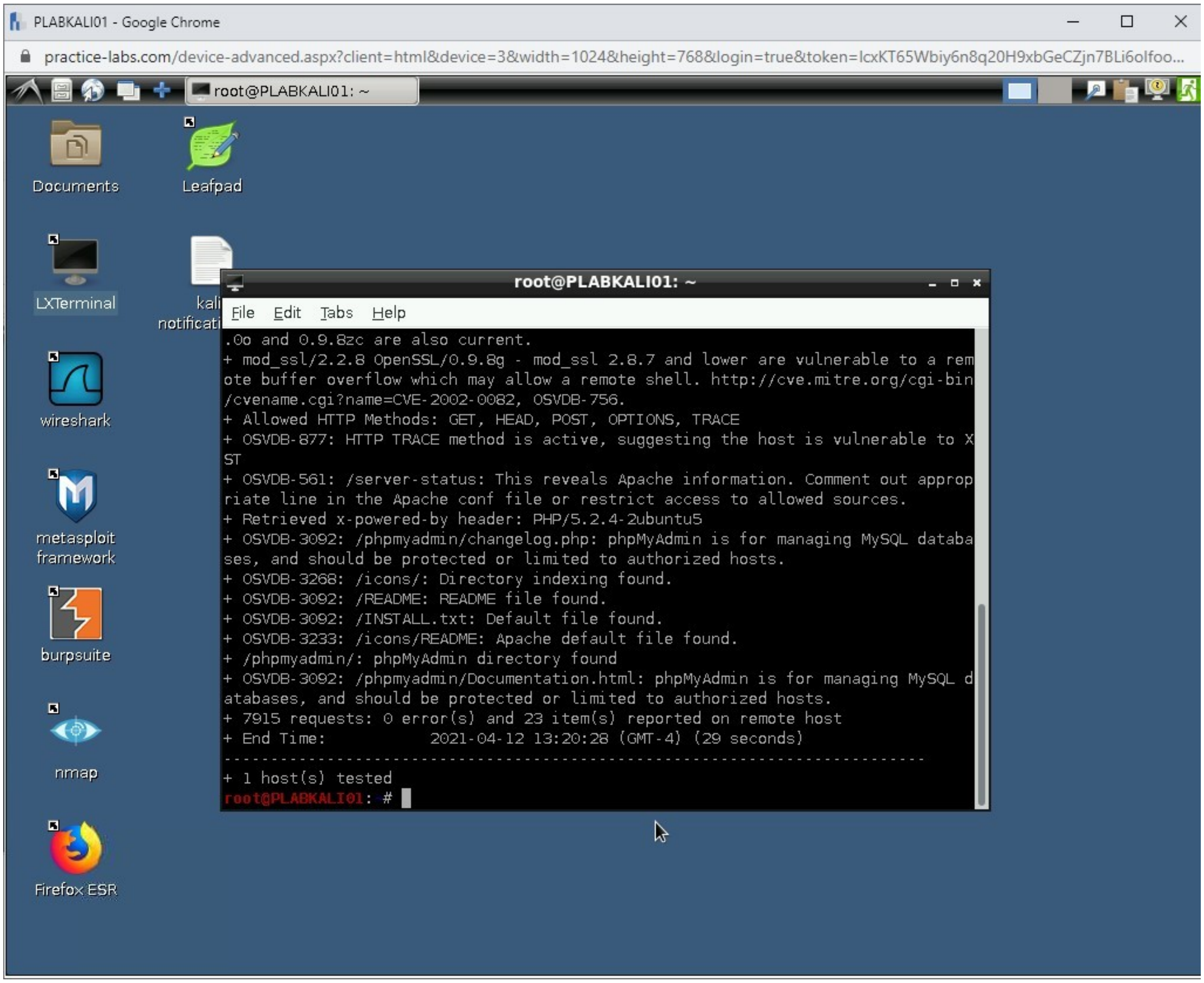

PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
root@PLABKALI01: ~
Documents
Leafpad
LXTerminal
kali notificati
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR
root@PLABKALI01: ~
File
Edit
Tabs
Help

```
root@PLABKALI01: ~# nikto -host http://192.168.0.10
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.10
+ Target Hostname:    192.168.0.10
+ Target Port:        80
+ Start Time:         2021-04-12 13:23:25 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with
Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
+ Server may leak inodes via ETags, header found with file /, inode: 838422, siz
e: 588, mtime: Sun Nov  2 13:20:24 2014
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
```

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.


PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
root@PLABKALI01: ~
Documents
Leafpad
LXTerminal
kali notificati
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR
root@PLABKALI01: ~
File
Edit
Tabs
Help

```
.0o and 0.9.8zc are also current.
+ mod_ssl/2.2.8 OpenSSL/0.9.8g - mod_ssl 2.8.7 and lower are vulnerable to a rem
ote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin
/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
ST
+ OSVDB-561: /server-status: This reveals Apache information. Comment out approp
riate line in the Apache conf file or restrict access to allowed sources.
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databa
ses, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3092: /README: README file found.
+ OSVDB-3092: /INSTALL.txt: Default file found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL d
atabases, and should be protected or limited to authorized hosts.
+ 7915 requests: 0 error(s) and 23 item(s) reported on remote host
+ End Time:           2021-04-12 13:20:28 (GMT-4) (29 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@PLABKALI01:~#
```

Figure 1.5 Screenshot of PLABKALI01: Showing the output of the nikto command.

Step 6

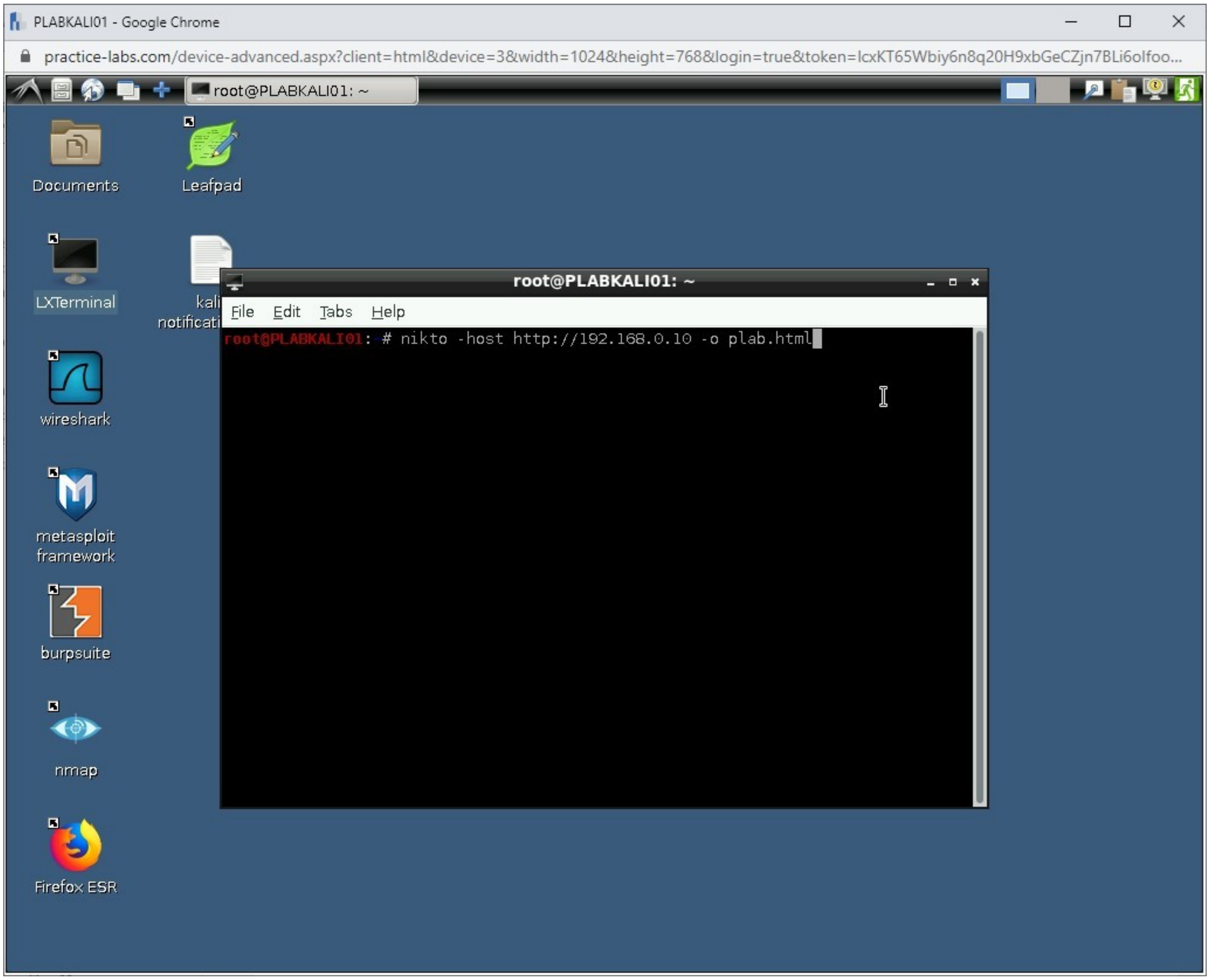
Clear the screen by entering the following command:

```
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**.


PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
root@PLABKALI01: ~
Documents
Leafpad
LXTerminal
kali notificati
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR
root@PLABKALI01: ~
File
Edit
Tabs
Help

```
root@PLABKALI01: # nikto -host http://192.168.0.10 -o plab.html
```

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

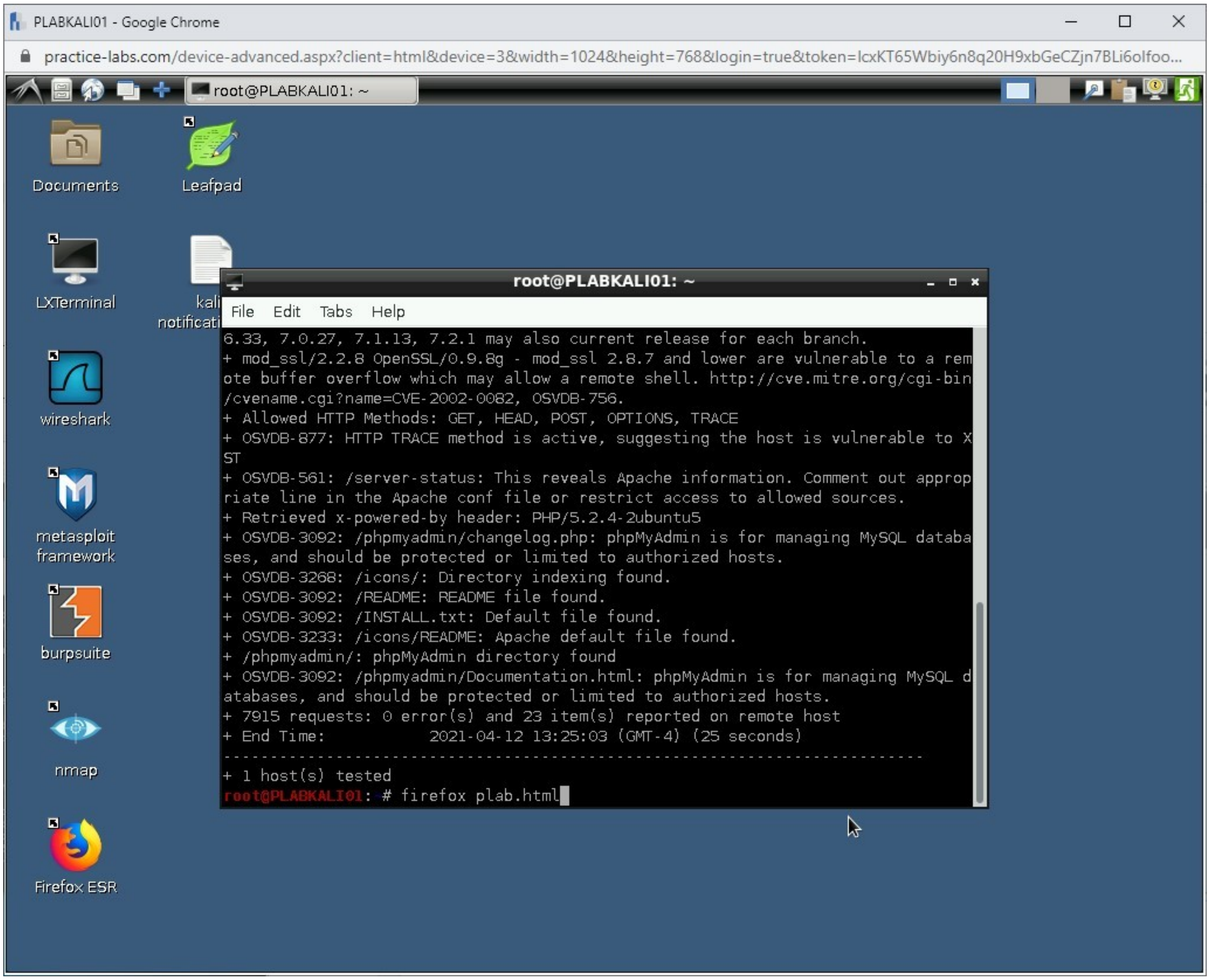
Step 7

Let the vulnerability scanning process complete.

Then, type the following command:

```
firefox plab.html
```

Press **Enter**.

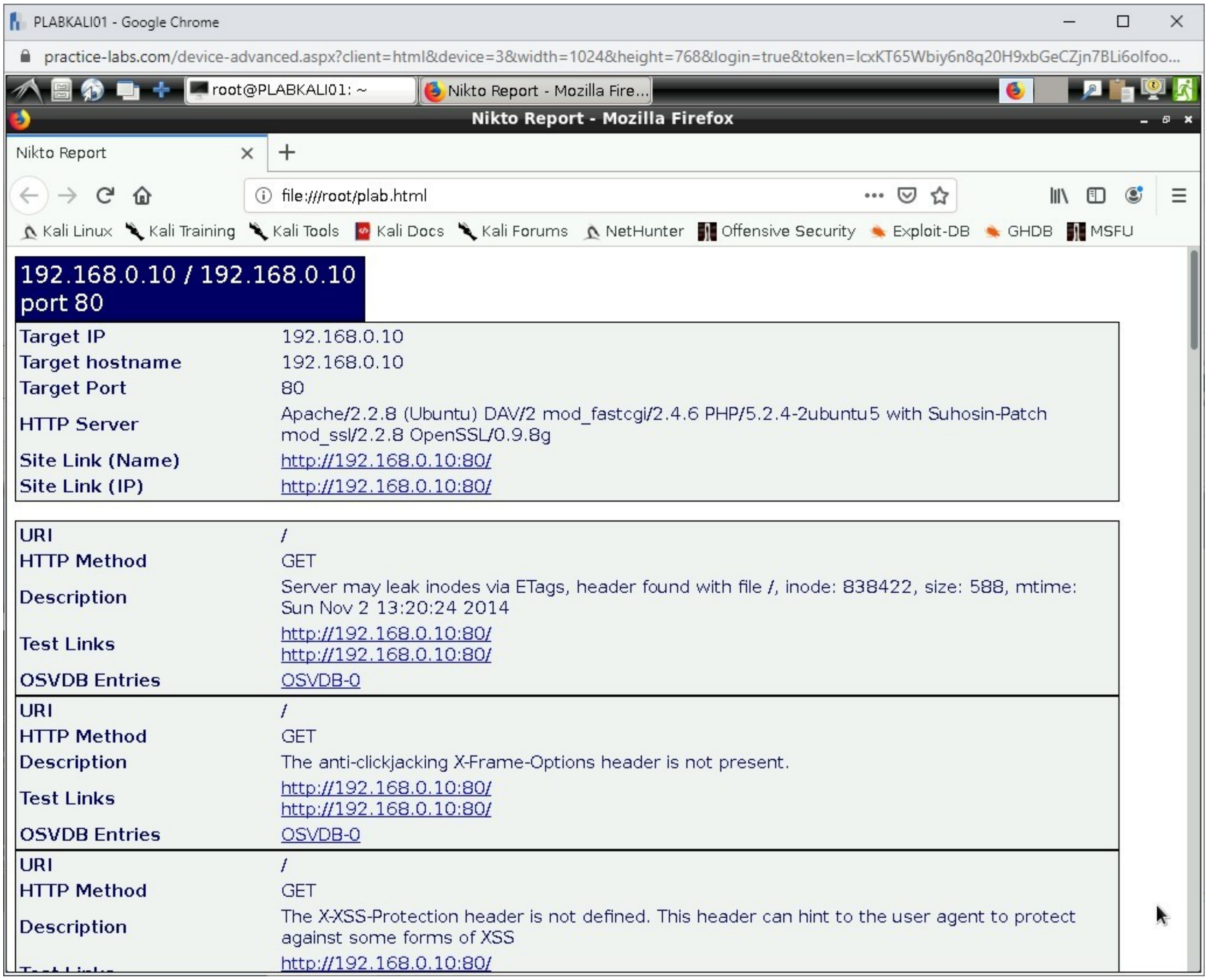

PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=lcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
root@PLABKALI01: ~
Documents
Leafpad
LXTerminal
kali notificati
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR
root@PLABKALI01: ~
File
Edit
Tabs
Help

```
6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
+ mod_ssl/2.2.8 OpenSSL/0.9.8g - mod_ssl 2.8.7 and lower are vulnerable to a rem
ote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin
/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
ST
+ OSVDB-561: /server-status: This reveals Apache information. Comment out approp
riate line in the Apache conf file or restrict access to allowed sources.
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databa
ses, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3092: /README: README file found.
+ OSVDB-3092: /INSTALL.txt: Default file found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL d
atabases, and should be protected or limited to authorized hosts.
+ 7915 requests: 0 error(s) and 23 item(s) reported on remote host
+ End Time:           2021-04-12 13:25:03 (GMT-4) (25 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@PLABKALI01:~# firefox plab.html
```

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.


PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
root@PLABKALI01: ~
Nikto Report - Mozilla Fire...
Nikto Report - Mozilla Firefox
Nikto Report
file:///root/plab.html
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

192.168.0.10 / 192.168.0.10
port 80

Target IP	192.168.0.10
Target hostname	192.168.0.10
Target Port	80
HTTP Server	Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
Site Link (Name)	http://192.168.0.10:80/
Site Link (IP)	http://192.168.0.10:80/

URI	/
HTTP Method	GET
Description	Server may leak inodes via ETags, header found with file /, inode: 838422, size: 588, mtime: Sun Nov 2 13:20:24 2014
Test Links	http://192.168.0.10:80/ http://192.168.0.10:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://192.168.0.10:80/ http://192.168.0.10:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
Test Links	http://192.168.0.10:80/

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 **PLABKALI01**.

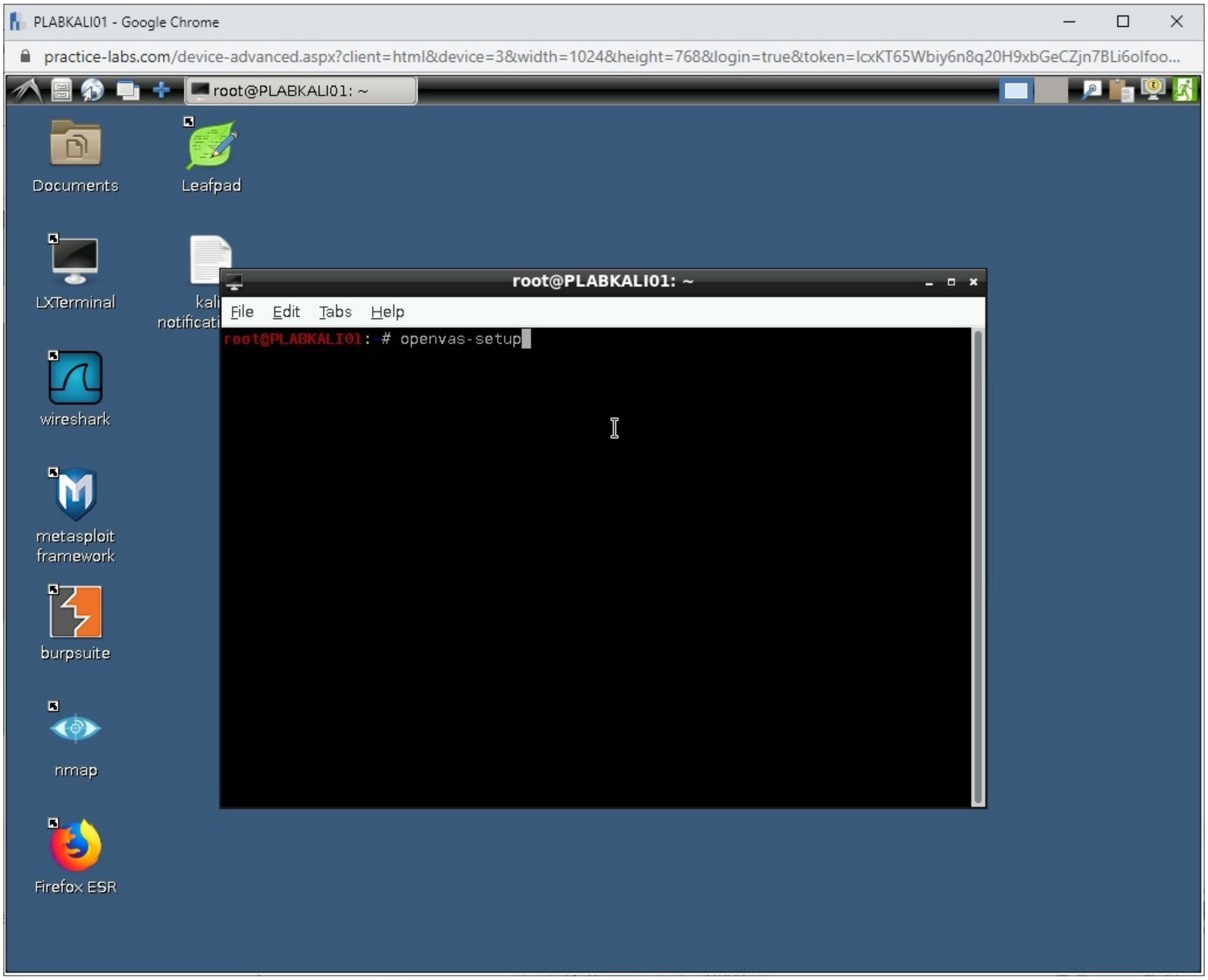
Clear the screen by entering the following command:

```
clear
```

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

```
openvas-setup
```

Press **Enter**.



PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
root@PLABKALI01: ~
Documents
Leafpad
LXTerminal
kali notificati
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR
root@PLABKALI01: ~
File
Edit
Tabs
Help

```
root@PLABKALI01:~# openvas-setup
```

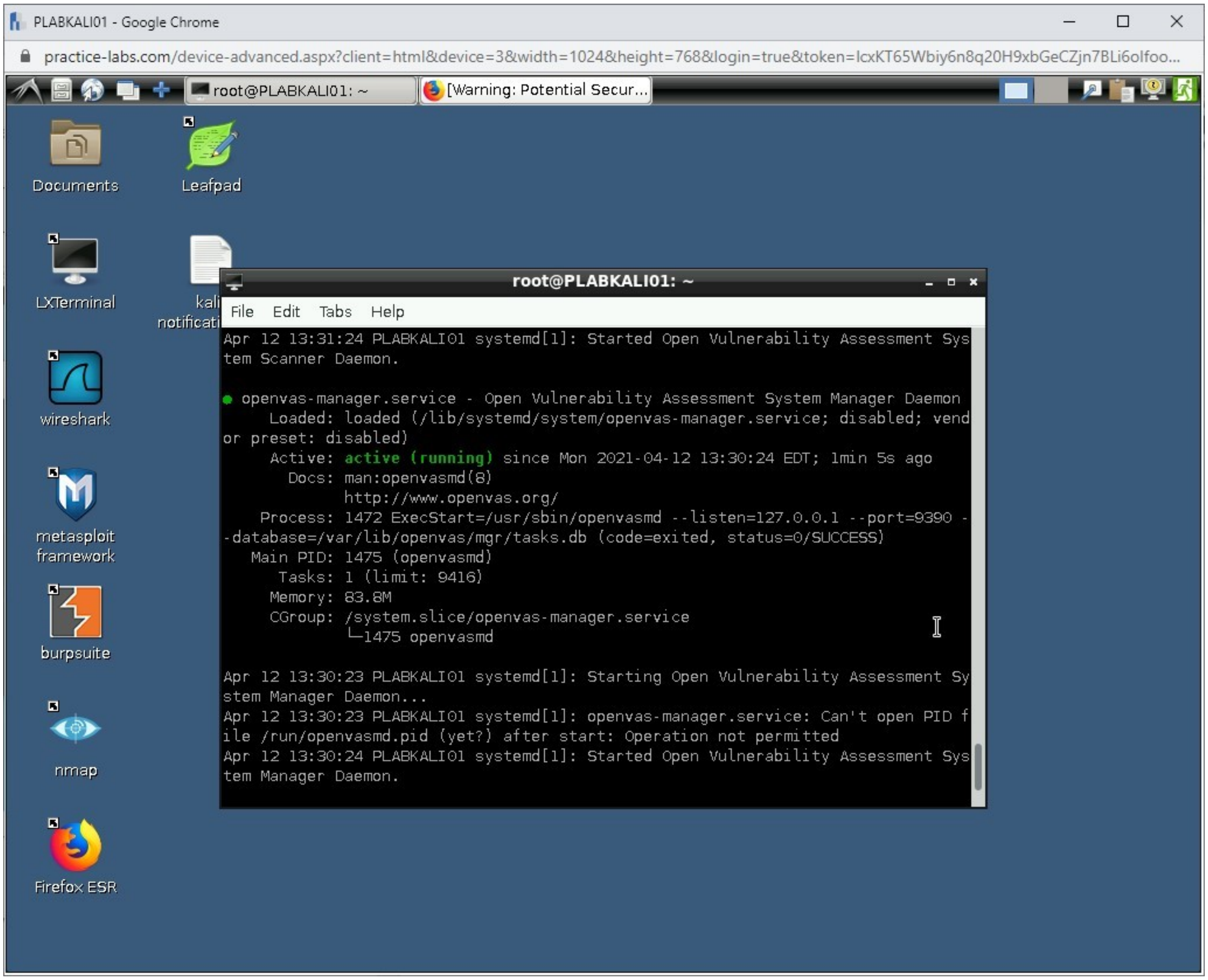
Figure 1.9 Screenshot of PLABKALI01: Entering the openvas-setup script command to setup and configure openvas.

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.


PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
root@PLABKALI01: ~
[Warning: Potential Secur...
Documents
Leafpad
LXTerminal
kali notificati
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR
root@PLABKALI01: ~
File
Edit
Tabs
Help

```
Apr 12 13:31:24 PLABKALI01 systemd[1]: Started Open Vulnerability Assessment Sys
tem Scanner Daemon.

● openvas-manager.service - Open Vulnerability Assessment System Manager Daemon
     Loaded: loaded (/lib/systemd/system/openvas-manager.service; disabled; vend
or preset: disabled)
     Active: active (running) since Mon 2021-04-12 13:30:24 EDT; 1min 5s ago
       Docs: man:openvasmd(8)
             http://www.openvas.org/
    Process: 1472 ExecStart=/usr/sbin/openvasmd --listen=127.0.0.1 --port=9390 -
-database=/var/lib/openvas/mgr/tasks.db (code=exited, status=0/SUCCESS)
   Main PID: 1475 (openvasmd)
      Tasks: 1 (limit: 9416)
     Memory: 83.8M
     CGroup: /system.slice/openvas-manager.service
             └─1475 openvasmd

Apr 12 13:30:23 PLABKALI01 systemd[1]: Starting Open Vulnerability Assessment Sy
stem Manager Daemon...
Apr 12 13:30:23 PLABKALI01 systemd[1]: openvas-manager.service: Can't open PID f
ile /run/openvasmd.pid (yet?) after start: Operation not permitted
Apr 12 13:30:24 PLABKALI01 systemd[1]: Started Open Vulnerability Assessment Sys
tem Manager Daemon.
```

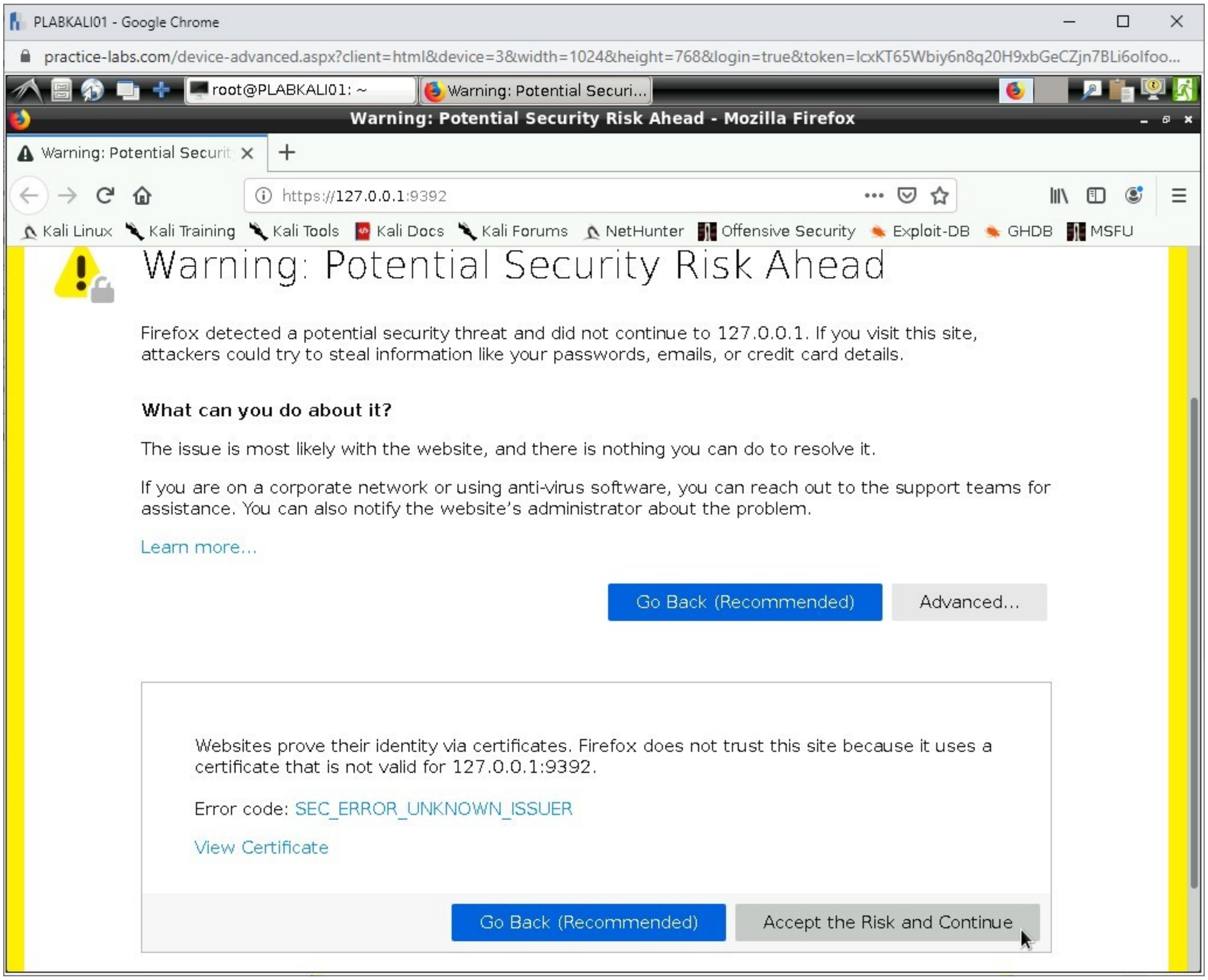
Figure 1.10 Screenshot of PLABKALI01: Showing the signature and vulnerability test downloads.

Step 3

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

Click **Advanced...**

Scroll down and click **Accept the Risk and Continue.**



PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
root@PLABKALI01: ~
Warning: Potential Securi...
Warning: Potential Security Risk Ahead - Mozilla Firefox
Warning: Potential Securit
https://127.0.0.1:9392
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 127.0.0.1. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 127.0.0.1:9392.

Error code: SEC_ERROR_UNKNOWN_ISSUER

Figure 1.11 Screenshot of PLABKALI01: Showing Firefox window with connection not secure message.

Step 4

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

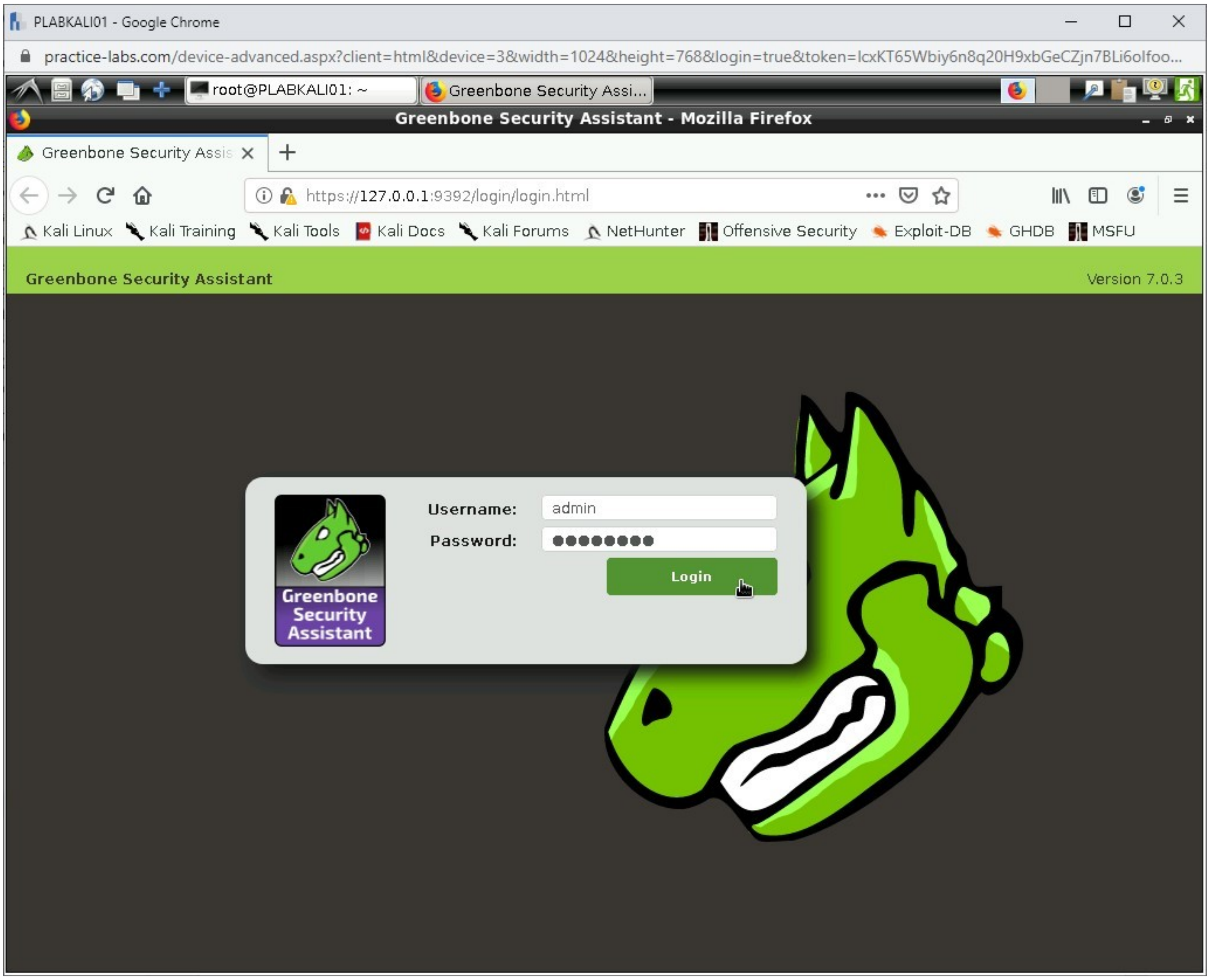
In the **Username** text box, type the following:

```
admin
```

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

```
Passw0rd
```

Click **Login**.



PLABKALI01 - Google Chrome

practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...

Greenbone Security Assistant - Mozilla Firefox

https://127.0.0.1:9392/login/login.html

Greenbone Security Assistant Version 7.0.3

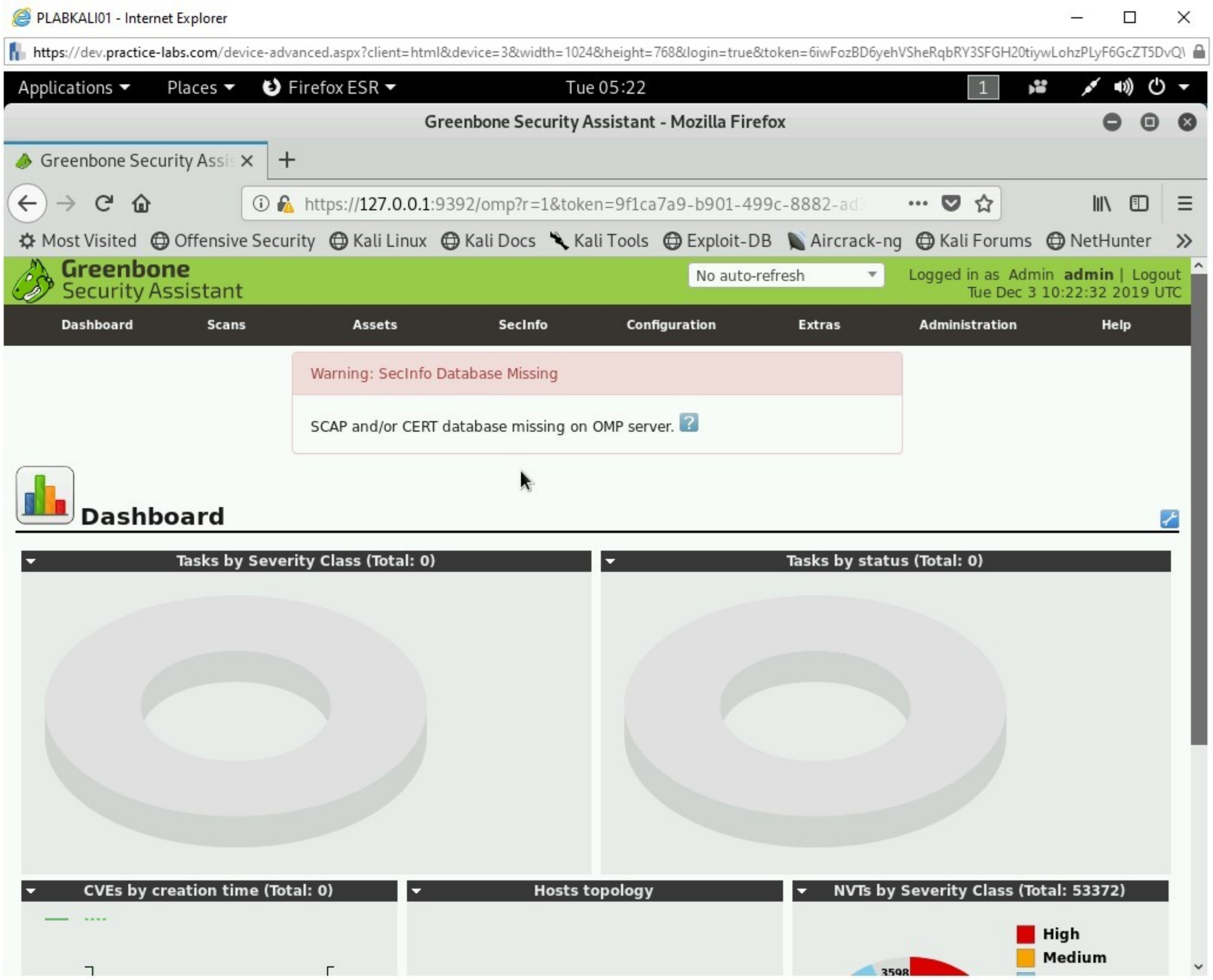
Username: admin

Password: ●●●●●●●●●

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.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=6iwFozBD6yehVSheRqbRY3SFGH20tiywLohzPLyF6GcZT5DvQ\
Applications
Places
Firefox ESR
Tue 05:22
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assis
https://127.0.0.1:9392/omp?r=1&token=9f1ca7a9-b901-499c-8882-ad
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Tue Dec 3 10:22:32 2019 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help

Warning: SecInfo Database Missing

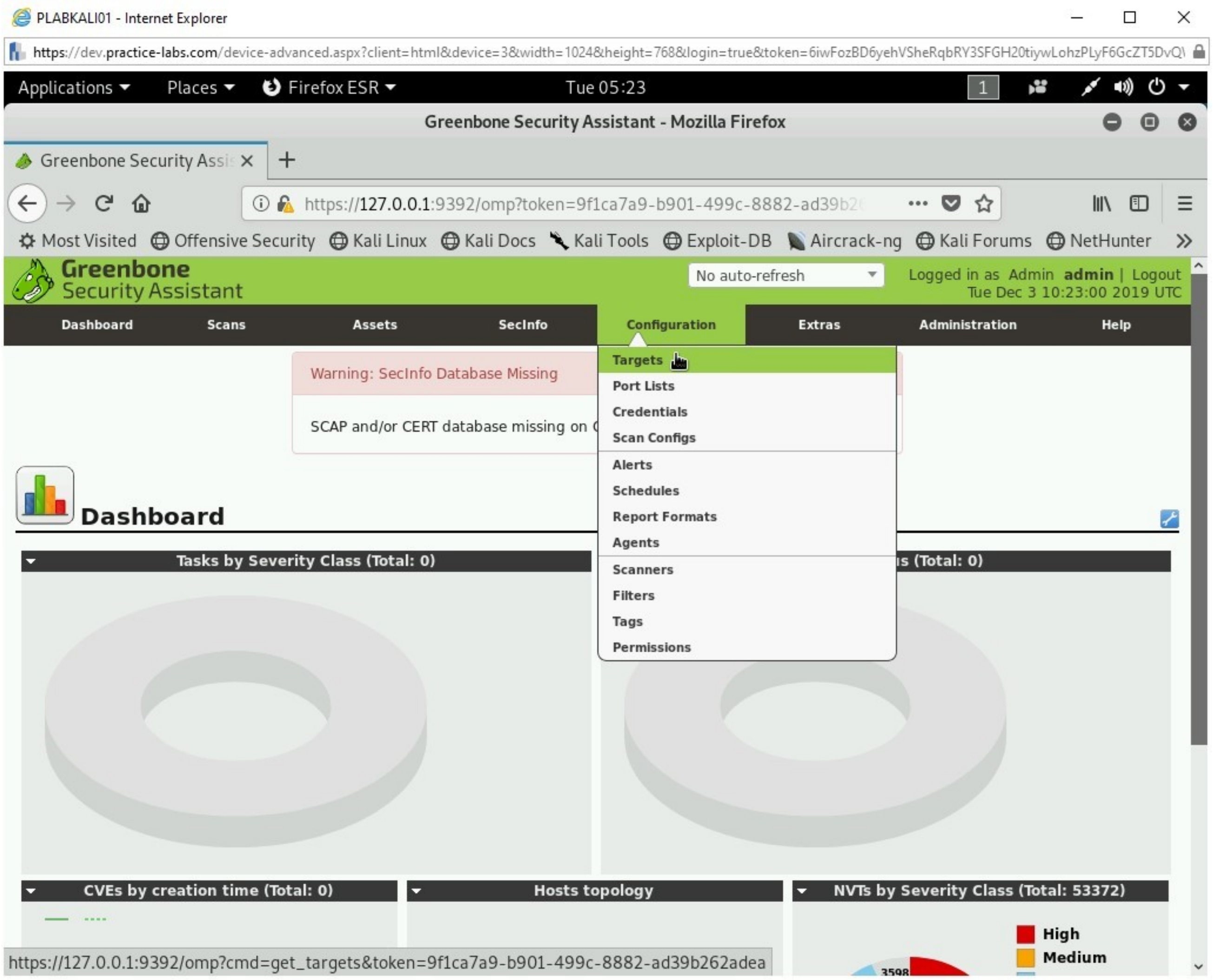
SCAP and/or CERT database missing on OMP server.

Dashboard
Tasks by Severity Class (Total: 0)
Tasks by status (Total: 0)
CVEs by creation time (Total: 0)
Hosts topology
NVTs by Severity Class (Total: 53372)
High
Medium
3598

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**.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=6iwFozBD6yehVSheRqbRY3SFGH20tiywLohzPLyF6GcZT5DvQ\
Applications
Places
Firefox ESR
Tue 05:23
1
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assis
https://127.0.0.1:9392/omp?token=9f1ca7a9-b901-499c-8882-ad39b2
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Greenbone
Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Tue Dec 3 10:23:00 2019 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Targets
Port Lists
Credentials
Scan Configs
Alerts
Schedules
Report Formats
Agents
Scanners
Filters
Tags
Permissions
Dashboard
Tasks by Severity Class (Total: 0)
s (Total: 0)
CVEs by creation time (Total: 0)
Hosts topology
NVTs by Severity Class (Total: 53372)
High
Medium
3598
https://127.0.0.1:9392/omp?cmd=get_targets&token=9f1ca7a9-b901-499c-8882-ad39b262adea

Warning: SecInfo Database Missing

SCAP and/or CERT database missing on (

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.

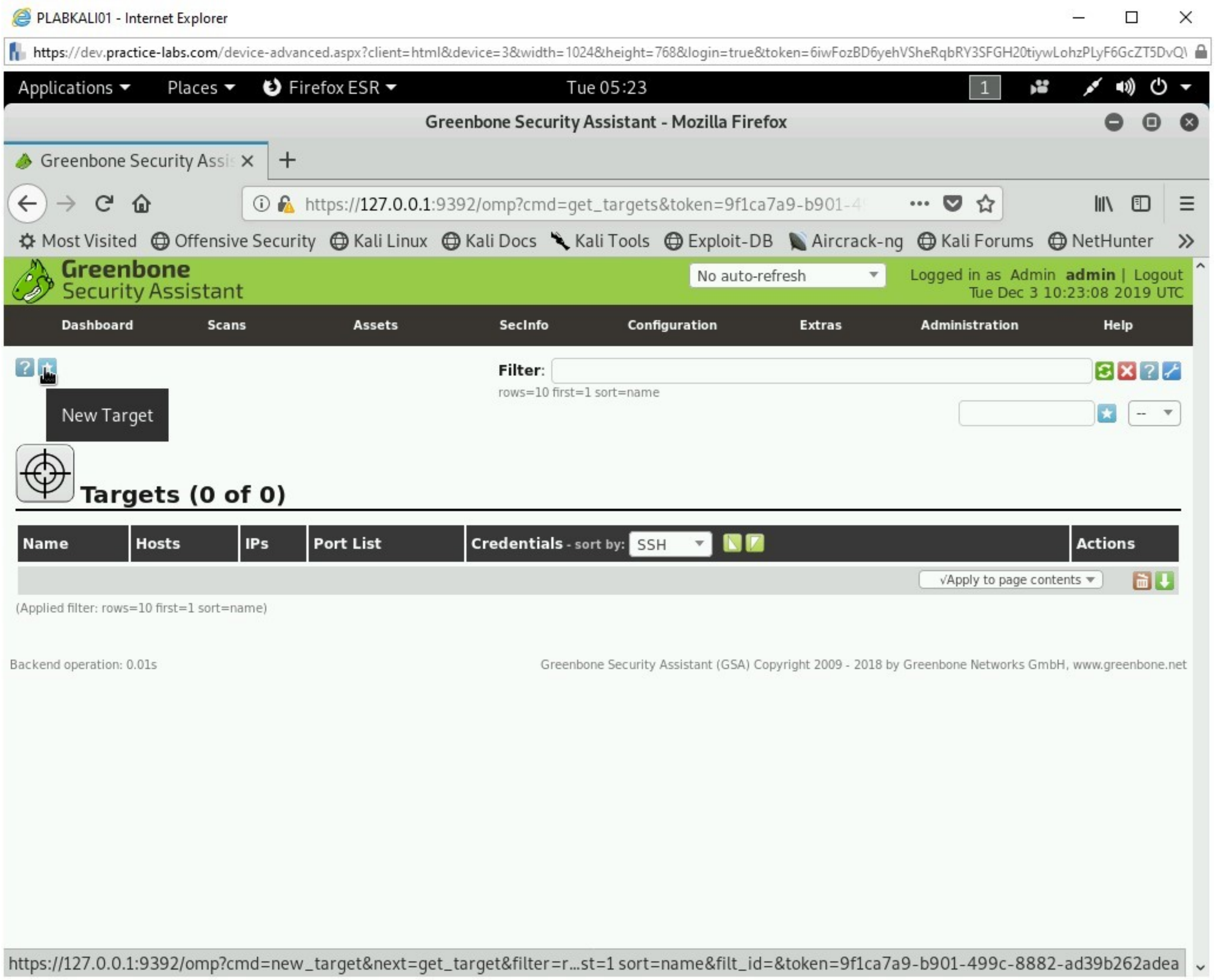

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=6iwFozBD6yehVSheRqbRY3SFGH20tiywLohzPLyF6GcZT5DvQ\
Applications
Places
Firefox ESR
Tue 05:23
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assi
https://127.0.0.1:9392/omp?cmd=get_targets&token=9f1ca7a9-b901-4
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Tue Dec 3 10:23:08 2019 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
New Target
Filter:
rows=10 first=1 sort=name
Targets (0 of 0)
Name
Hosts
IPs
Port List
Credentials - sort by: SSH
Actions
√Apply to page contents
(Applied filter: rows=10 first=1 sort=name)
Backend operation: 0.01s
Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net
https://127.0.0.1:9392/omp?cmd=new_target&next=get_target&filter=r...st=1 sort=name&filt_id=&token=9f1ca7a9-b901-499c-8882-ad39b262adea

Figure 1.15 Screenshot of PLABKALI01: Clicking * or New Target on the Targets page.

Step 8

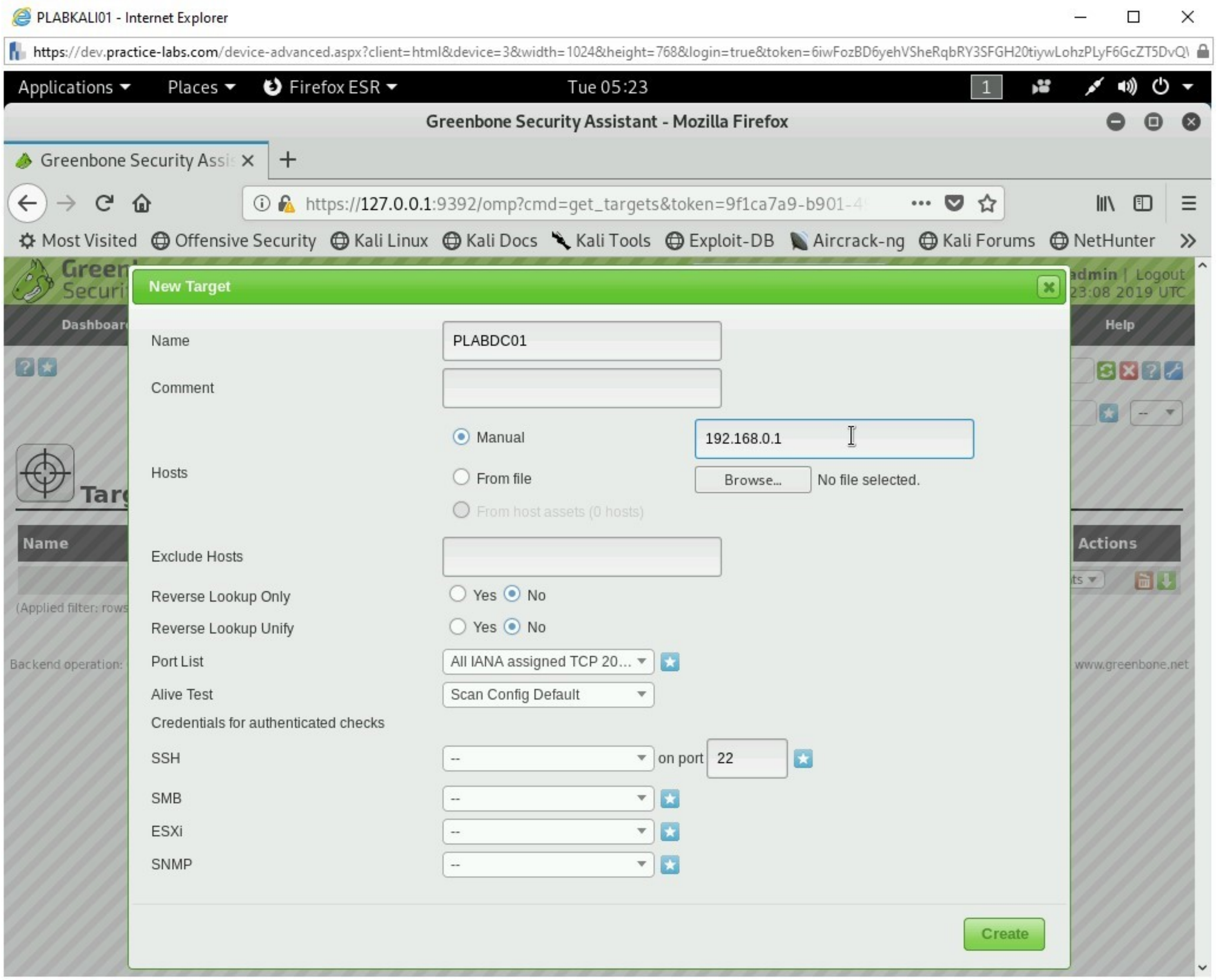
The **New Target** dialog box is displayed. In the **Name** text box, type the following:

```
PLABDC01
```

In the Manual Field text box, type the following:

```
192.168.0.1
```

Click **Create**.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=6iwFozBD6yehVSheRqbRY3SFGH20tiywLohzPLyF6GcZT5DvQ\
Applications
Places
Firefox ESR
Tue 05:23
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assis
https://127.0.0.1:9392/omp?cmd=get_targets&token=9f1ca7a9-b901-4
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Dashboard
Help
admin | Logout
Name
Actions
www.greenbone.net

New Target

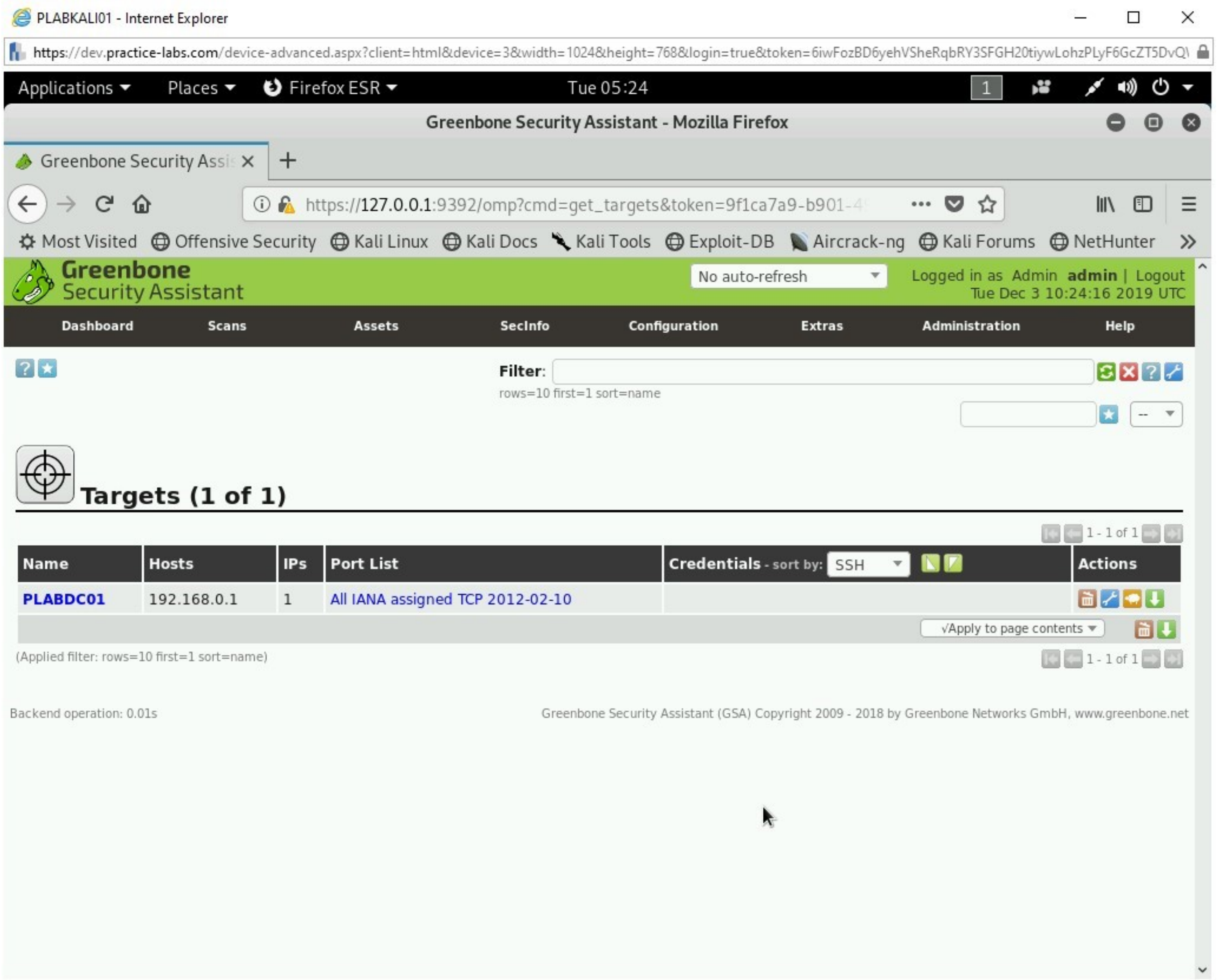
Name	PLABDC01	
Comment		
Hosts	● Manual	192.168.0.1
	○ From file	Browse... No file selected.
	○ From host assets (0 hosts)	
Exclude Hosts		
Reverse Lookup Only	○ Yes ● No	
Reverse Lookup Unify	○ Yes ● No	
Port List	All IANA assigned TCP 20...	
Alive Test	Scan Config Default	
Credentials for authenticated checks		
SSH	--	on port 22
SMB	--	
ESXi	--	
SNMP	--	

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.


PLABKALI01 - Internet Explorer
Applications
Places
Firefox ESR
Tue 05:24
Greenbone Security Assistant - Mozilla Firefox
https://127.0.0.1:9392/omp?cmd=get_targets&token=9f1ca7a9-b901-4
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Tue Dec 3 10:24:16 2019 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Filter:
√Apply to page contents

rows=10 first=1 sort=name

Targets (1 of 1)

1 - 1 of 1

Name	Hosts	IPs	Port List	Credentials - sort by: SSH	Actions
PLABDC01	192.168.0.1	1	All IANA assigned TCP 2012-02-10		

(Applied filter: rows=10 first=1 sort=name)

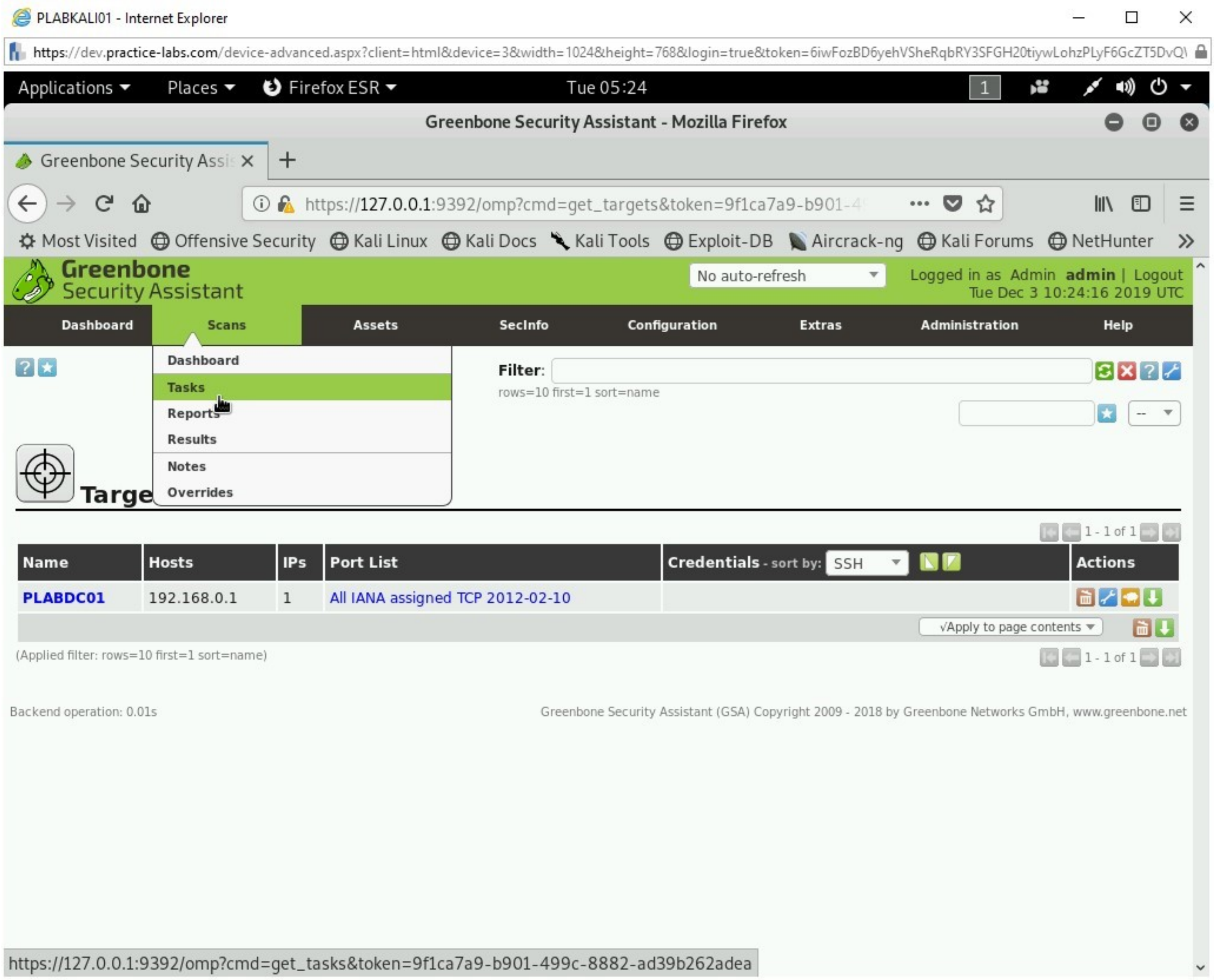
Backend operation: 0.01s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

Figure 1.17 Screenshot of PLABKALI01: Showing the newly created task.

Step 10

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


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=6iwFozBD6yehVSheRqbRY3SFGH20tiywLohzPLyF6GcZT5DvQ\
Applications
Places
Firefox ESR
Tue 05:24
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assis
https://127.0.0.1:9392/omp?cmd=get_targets&token=9f1ca7a9-b901-4
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Tue Dec 3 10:24:16 2019 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Dashboard
Tasks
Reports
Results
Notes
Overrides
Targe
Filter:
rows=10 first=1 sort=name
1 - 1 of 1
√Apply to page contents
(Applied filter: rows=10 first=1 sort=name)
Backend operation: 0.01s
Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net
https://127.0.0.1:9392/omp?cmd=get_tasks&token=9f1ca7a9-b901-499c-8882-ad39b262adea

Name	Hosts	IPs	Port List	Credentials - sort by: SSH	Actions
PLABDC01	192.168.0.1	1	All IANA assigned TCP 2012-02-10		

Figure 1.18 Screenshot of PLABKALI01: Selecting Tasks from the Scans menu.

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**.

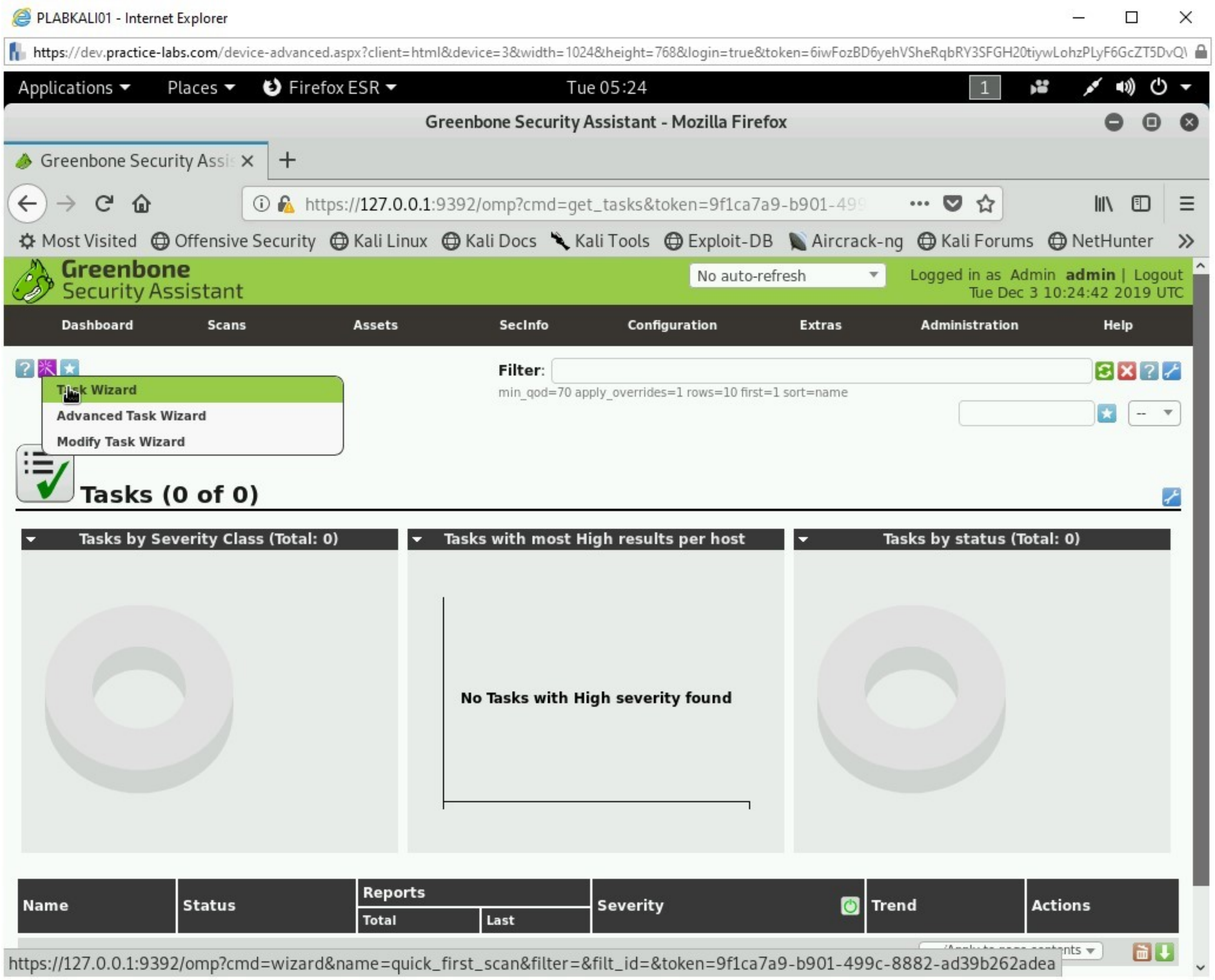
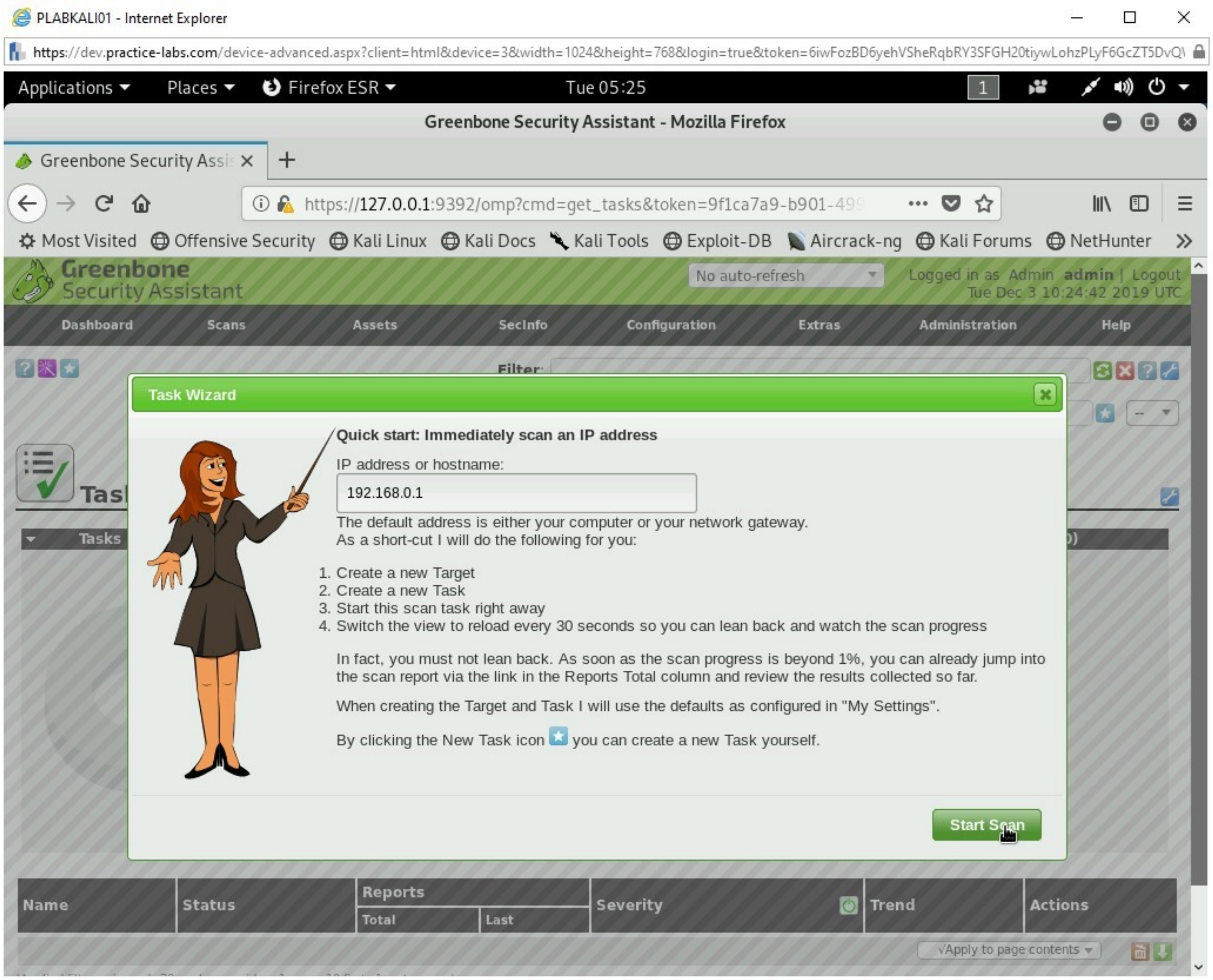

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=6iwFozBD6yehVSheRqbRY3SFGH20tiywLohzPLyF6GcZT5DvQ\
Applications
Places
Firefox ESR
Tue 05:24
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assi
https://127.0.0.1:9392/omp?cmd=get_tasks&token=9f1ca7a9-b901-499
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Tue Dec 3 10:24:42 2019 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Task Wizard
Advanced Task Wizard
Modify Task Wizard
Filter:
min_qod=70 apply_overrides=1 rows=10 first=1 sort=name
Tasks (0 of 0)
Tasks by Severity Class (Total: 0)
Tasks with most High results per host
No Tasks with High severity found
Tasks by status (Total: 0)
Name
Status
Reports
Total
Last
Severity
Trend
Actions
https://127.0.0.1:9392/omp?cmd=wizard&name=quick_first_scan&filter=&filt_id=&token=9f1ca7a9-b901-499c-8882-ad39b262adea

Figure 1.19 Screenshot of PLABKALI01: Selecting Task Wizard from the menu.

Step 12

The **Task Wizard** is displayed. Input the IP address as **192.168.0.1** and click **Start Scan**.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=6iwFozBD6yehVSheRqbRY3SFGH20tiywLohzPLyF6GcZT5DvQ\
Applications
Places
Firefox ESR
Tue 05:25
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assis
https://127.0.0.1:9392/omp?cmd=get_tasks&token=9f1ca7a9-b901-499
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Tue Dec 3 10:24:42 2019 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Filter:
Tas
Tasks
Task Wizard
Start Scan
Name
Status
Reports
Total
Last
Severity
Trend
Actions
√Apply to page contents

Quick start: Immediately scan an IP address

IP address or hostname:

192.168.0.1

The default address is either your computer or your network gateway.
As a short-cut I will do the following for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

When creating the Target and Task I will use the defaults as configured in "My Settings".

By clicking the New Task icon ✱ you can create a new Task yourself.

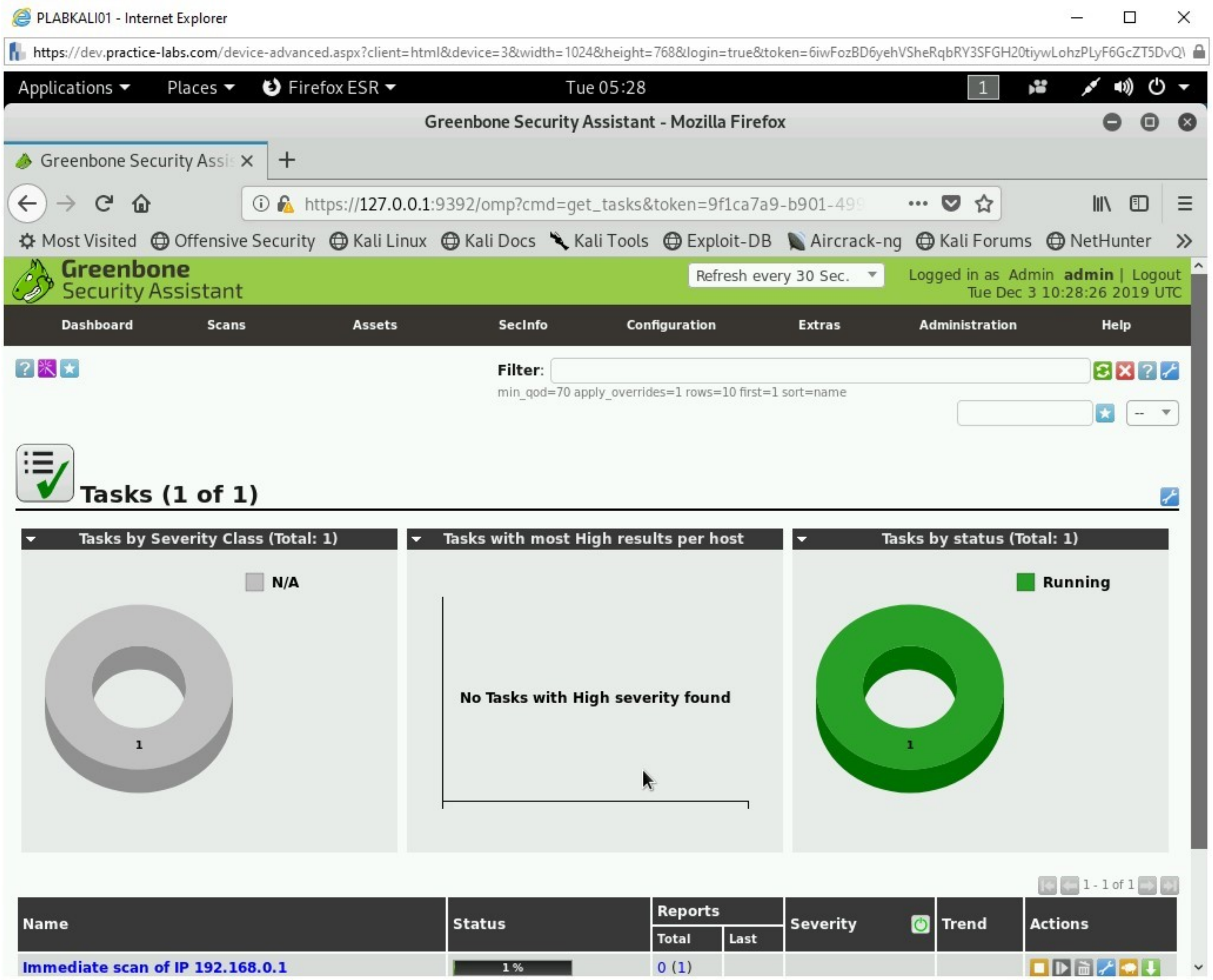
Figure 1.20 Screenshot of PLABKALI01: Clicking Start Scan on the Task Wizard dialog box.

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.*


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=6iwFozBD6yehVSheRqbRY3SFGH20tiywLohzPLyF6GcZT5DvQ
Applications
Places
Firefox ESR
Tue 05:28
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assi
https://127.0.0.1:9392/omp?cmd=get_tasks&token=9f1ca7a9-b901-49
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Greenbone Security Assistant
Refresh every 30 Sec.
Logged in as Admin admin | Logout
Tue Dec 3 10:28:26 2019 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Tasks by Severity Class (Total: 1)
N/A
1
Tasks with most High results per host
No Tasks with High severity found
Tasks by status (Total: 1)
Running
1
1 - 1 of 1

Filter:

min_qod=70 apply_overrides=1 rows=10 first=1 sort=name

Tasks (1 of 1)

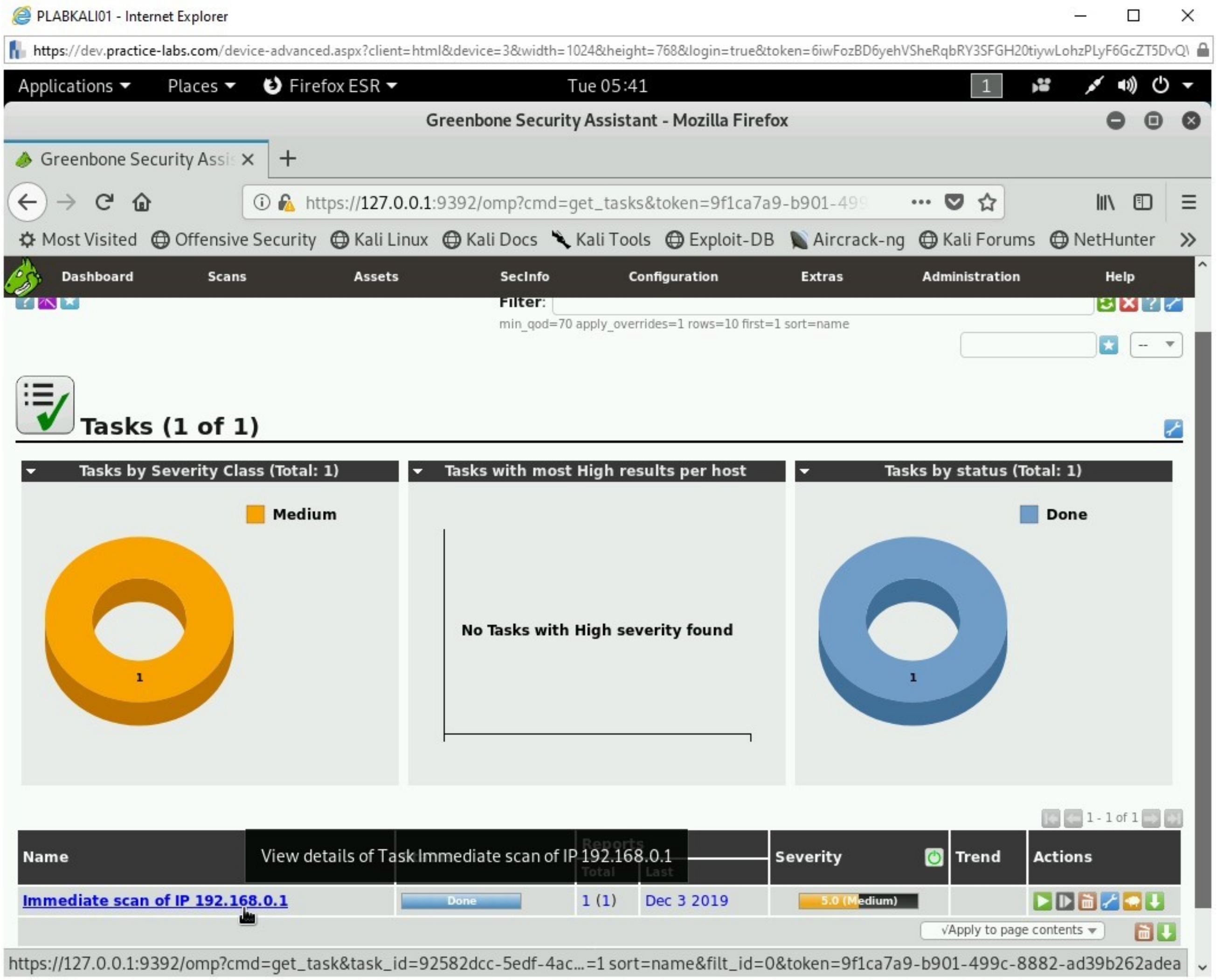
Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.0.1	1 %	0 (1)				

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**.



https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=6iwFozBD6yehVSheRqbRY3SFGH20tiywLohzPLyF6GcZT5DvQ\

https://127.0.0.1:9392/omp?cmd=get_tasks&token=9f1ca7a9-b901-499

min_qod=70 apply_overrides=1 rows=10 first=1 sort=name

Tasks (1 of 1)

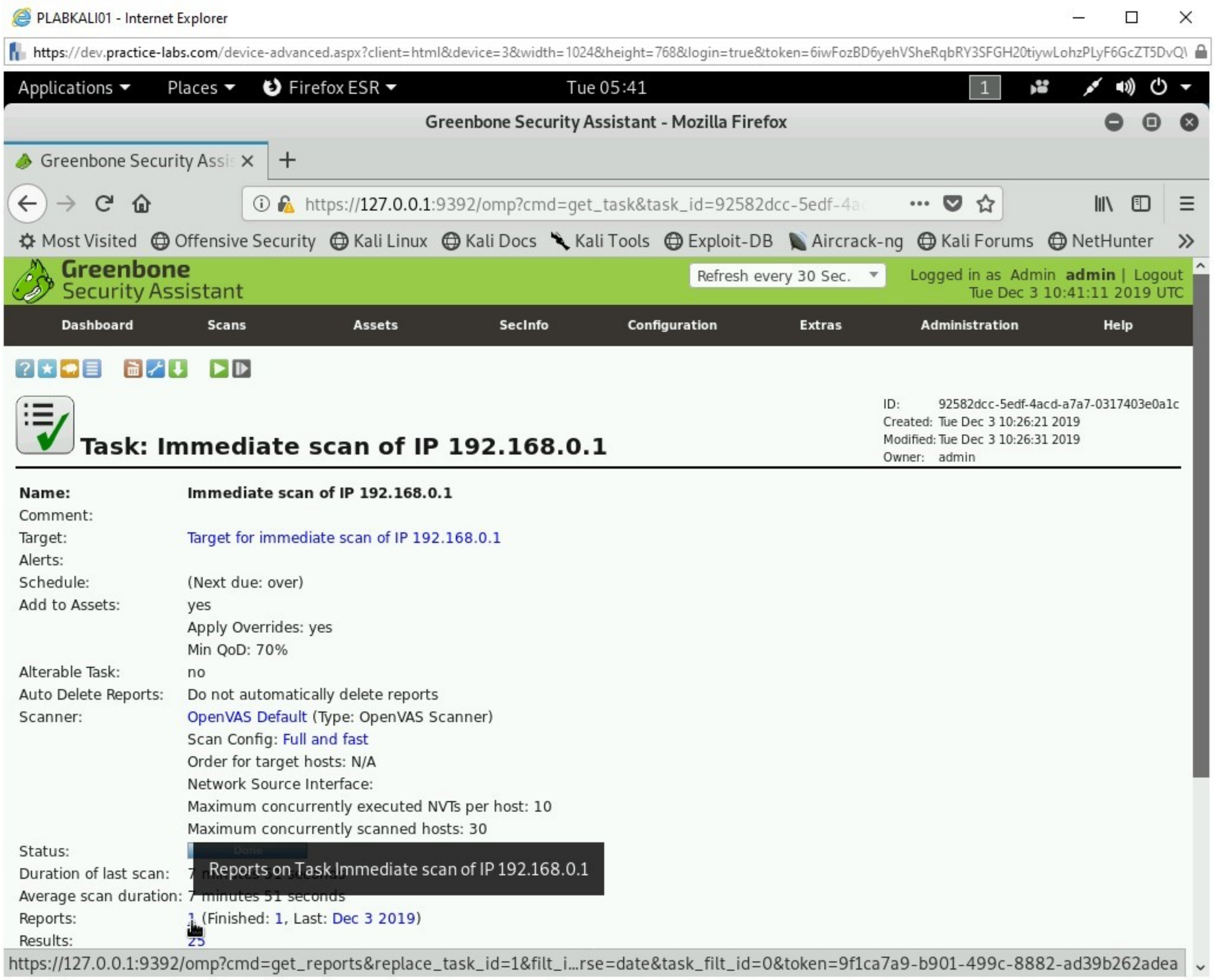
Name	Status	Reports Total	Reports Last	Severity	Trend	Actions
Immediate scan of IP 192.168.0.1	Done	1 (1)	Dec 3 2019	5.0 (Medium)		

https://127.0.0.1:9392/omp?cmd=get_task&task_id=92582dcc-5edf-4ac...=1 sort=name&filt_id=0&token=9f1ca7a9-b901-499c-8882-ad39b262adea

Figure 1.22 Screenshot of PLABKALI01: Showing the completed task on the Tasks page.

Step 15

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


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=6iwFozBD6yehVSheRqbRY3SFGH20tiywLohzPLyF6GcZT5DvQ\
Applications
Places
Firefox ESR
Tue 05:41
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assis
https://127.0.0.1:9392/omp?cmd=get_task&task_id=92582dcc-5edf-4a
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Greenbone Security Assistant
Refresh every 30 Sec.
Logged in as Admin admin | Logout
Tue Dec 3 10:41:11 2019 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help

Task: Immediate scan of IP 192.168.0.1

ID: 92582dcc-5edf-4acd-a7a7-0317403e0a1c
Created: Tue Dec 3 10:26:21 2019
Modified: Tue Dec 3 10:26:31 2019
Owner: admin

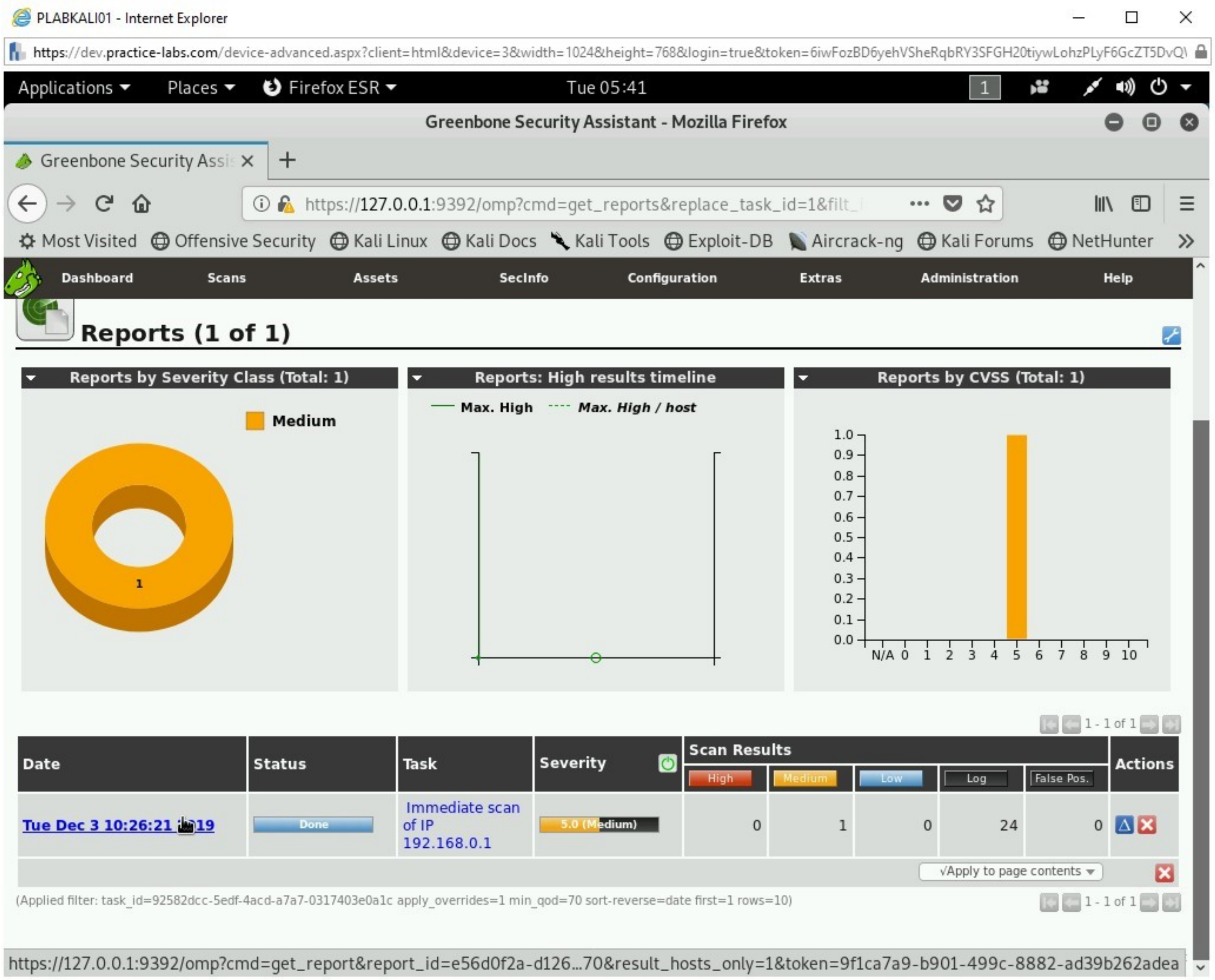
Name: **Immediate scan of IP 192.168.0.1**
Comment:
Target: Target for immediate scan of IP 192.168.0.1
Alerts:
Schedule: (Next due: over)
Add to Assets: yes
Apply Overrides: yes
Min QoD: 70%
Alterable Task: no
Auto Delete Reports: Do not automatically delete reports
Scanner: OpenVAS Default (Type: OpenVAS Scanner)
Scan Config: Full and fast
Order for target hosts: N/A
Network Source Interface:
Maximum concurrently executed NVTs per host: 10
Maximum concurrently scanned hosts: 30
Status: Done
Duration of last scan: 7 minutes 51 seconds
Average scan duration: 7 minutes 51 seconds
Reports: 1 (Finished: 1, Last: Dec 3 2019)
Results: 25

Reports on Task Immediate scan of IP 192.168.0.1
https://127.0.0.1:9392/omp?cmd=get_reports&replace_task_id=1&filt_i...rse=date&task_filt_id=0&token=9f1ca7a9-b901-499c-8882-ad39b262adea

Figure 1.23 Screenshot of PLABKALI01: Clicking 1 next to Reports.

Step 16

Click the link provided under the **Date** column.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=6iwFozBD6yehVSheRqbRY3SFGH20tiywLohzPLyF6GcZT5DvQ\
Applications
Places
Firefox ESR
Tue 05:41
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assi
https://127.0.0.1:9392/omp?cmd=get_reports&replace_task_id=1&filt
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Reports (1 of 1)
Reports by Severity Class (Total: 1)
Medium
1
Reports: High results timeline
Max. High
Max. High / host
Reports by CVSS (Total: 1)
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
N/A 0 1 2 3 4 5 6 7 8 9 10
1 - 1 of 1

Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Tue Dec 3 10:26:21 19	Done	Immediate scan of IP 192.168.0.1	5.0 (Medium)	0	1	0	24	0	

√Apply to page contents
1 - 1 of 1

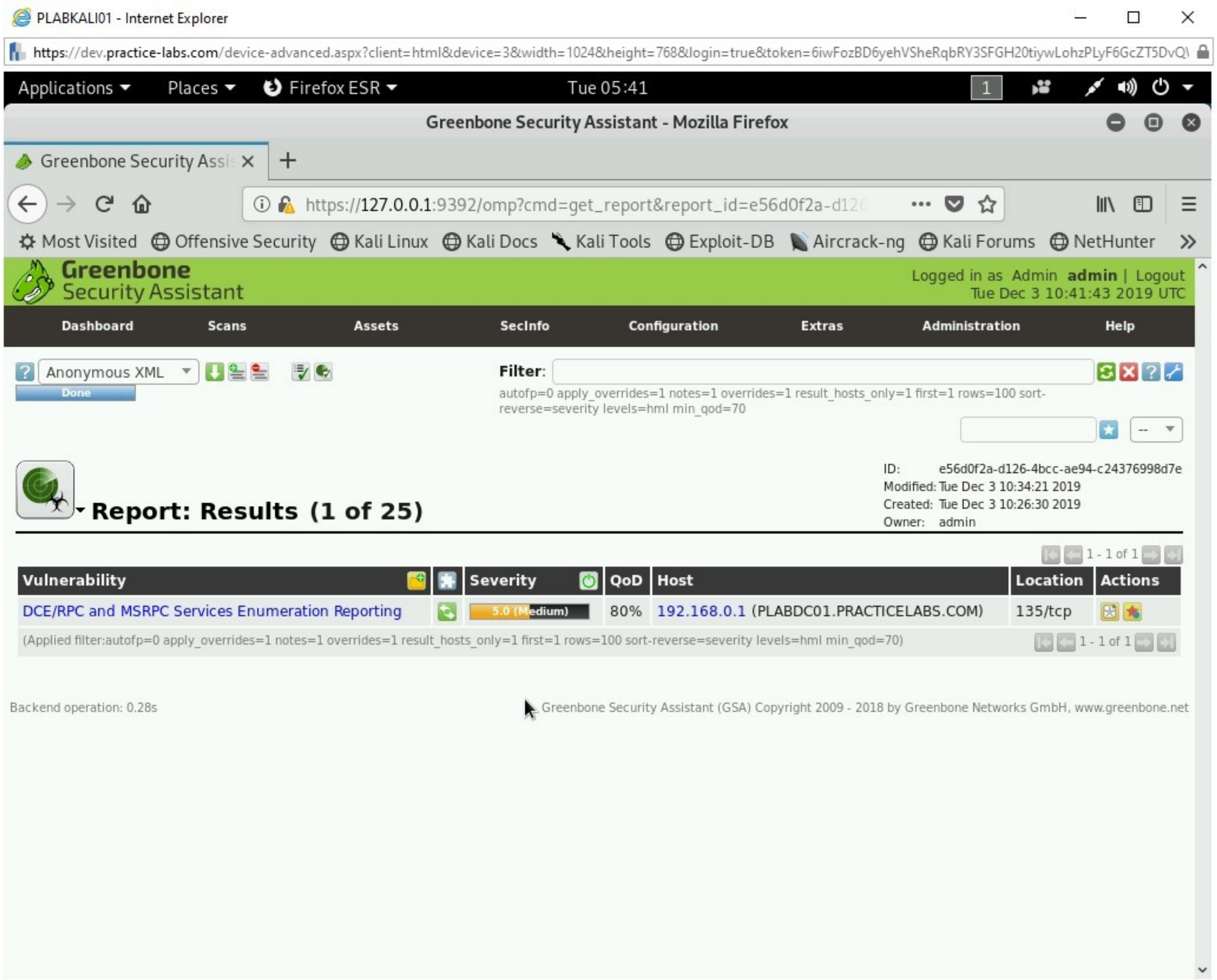
(Applied filter: task_id=92582dcc-5edf-4acd-a7a7-0317403e0a1c apply_overrides=1 min_qod=70 sort-reverse=date first=1 rows=10)

https://127.0.0.1:9392/omp?cmd=get_report&report_id=e56d0f2a-d126...70&result_hosts_only=1&token=9f1ca7a9-b901-499c-8882-ad39b262adea

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.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=6iwFozBD6yehVSheRqbRY3SFGH20tiywLohzPLyF6GcZT5DvQ\
Applications
Places
Firefox ESR
Tue 05:41
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assis
https://127.0.0.1:9392/omp?cmd=get_report&report_id=e56d0f2a-d12
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Greenbone Security Assistant
Logged in as Admin admin | Logout
Tue Dec 3 10:41:43 2019 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Anonymous XML
Done
Filter:
Backend operation: 0.28s
Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

Report: Results (1 of 25)

ID: e56d0f2a-d126-4bcc-ae94-c24376998d7e
Modified: Tue Dec 3 10:34:21 2019
Created: Tue Dec 3 10:26:30 2019
Owner: admin

1 - 1 of 1

Vulnerability	Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.0.1 (PLABDC01.PRACTICELABS.COM)	135/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70) 1 - 1 of 1

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

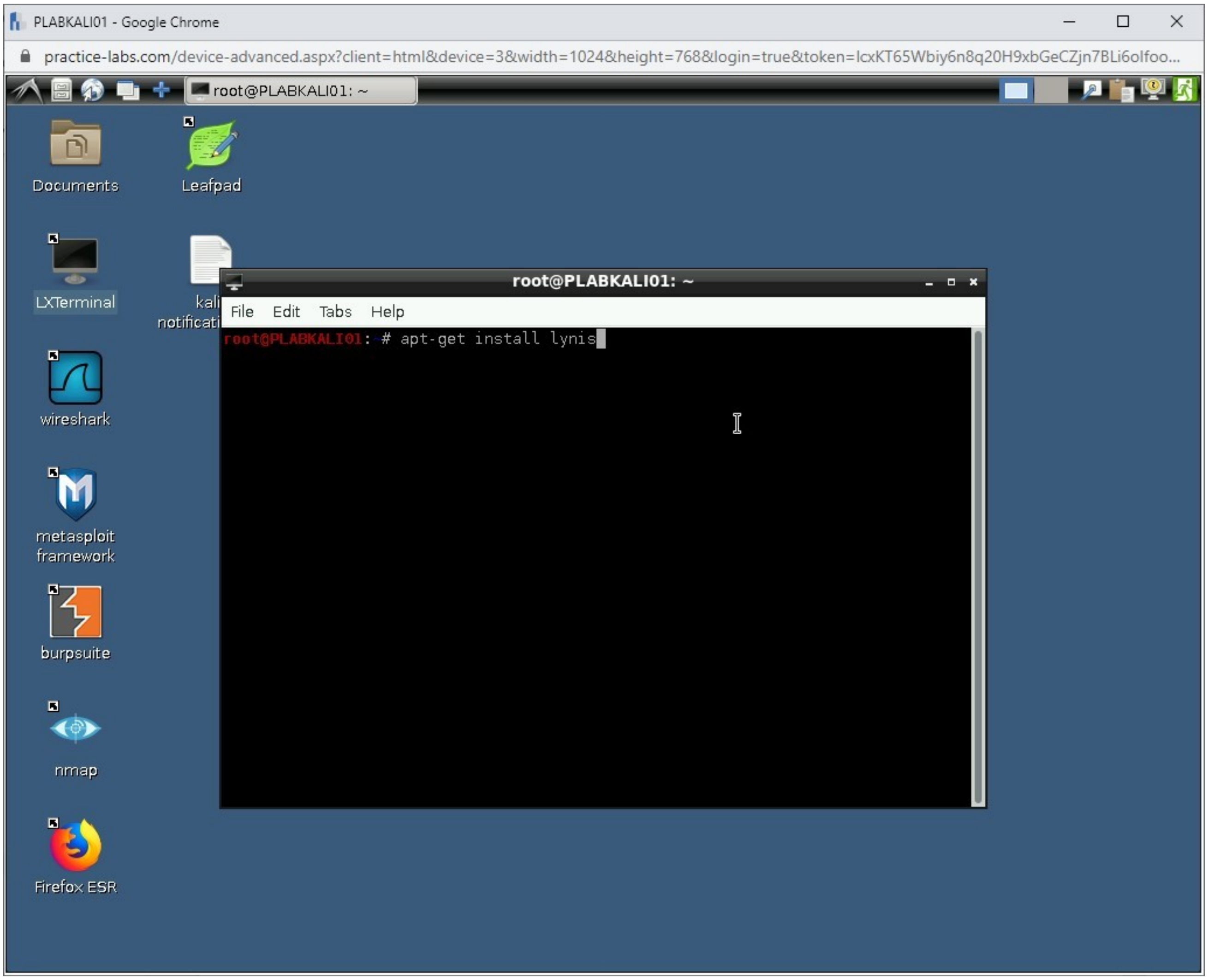
Ensure you have powered on all the devices listed in the introduction and connect to **PLABKALI01**.

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.


PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
root@PLABKALI01: ~
Documents
Leafpad
LXTerminal
kali notificati
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR
root@PLABKALI01: ~
File
Edit
Tabs
Help

```
root@PLABKALI01: # 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
```

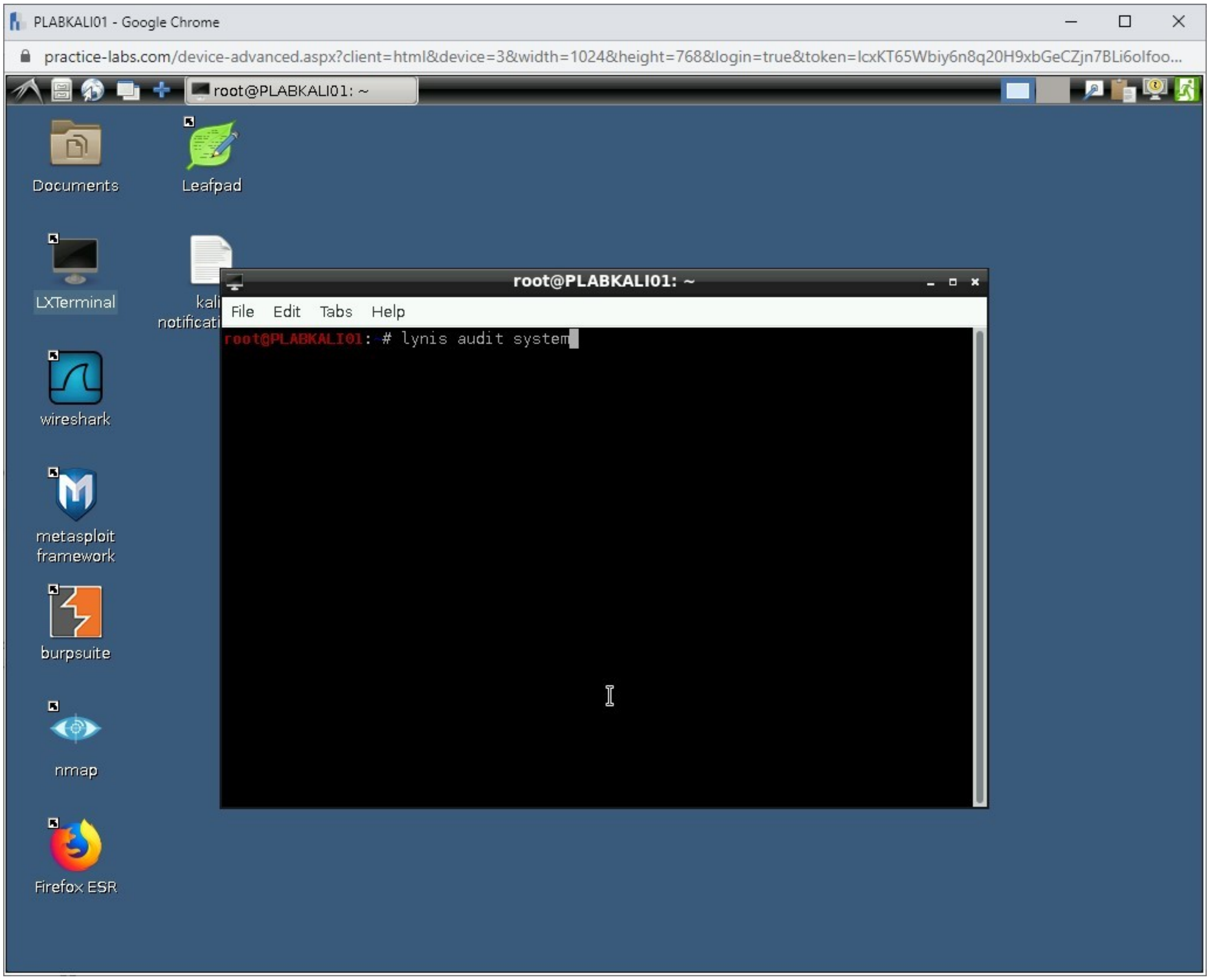
By default, Lynis will perform a local system scan. You have the option to run a normal audit scan or can run the entire system scan.

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.


PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
root@PLABKALI01: ~
Documents
Leafpad
LXTerminal
kali notificati
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR
root@PLABKALI01: ~
File
Edit
Tabs
Help

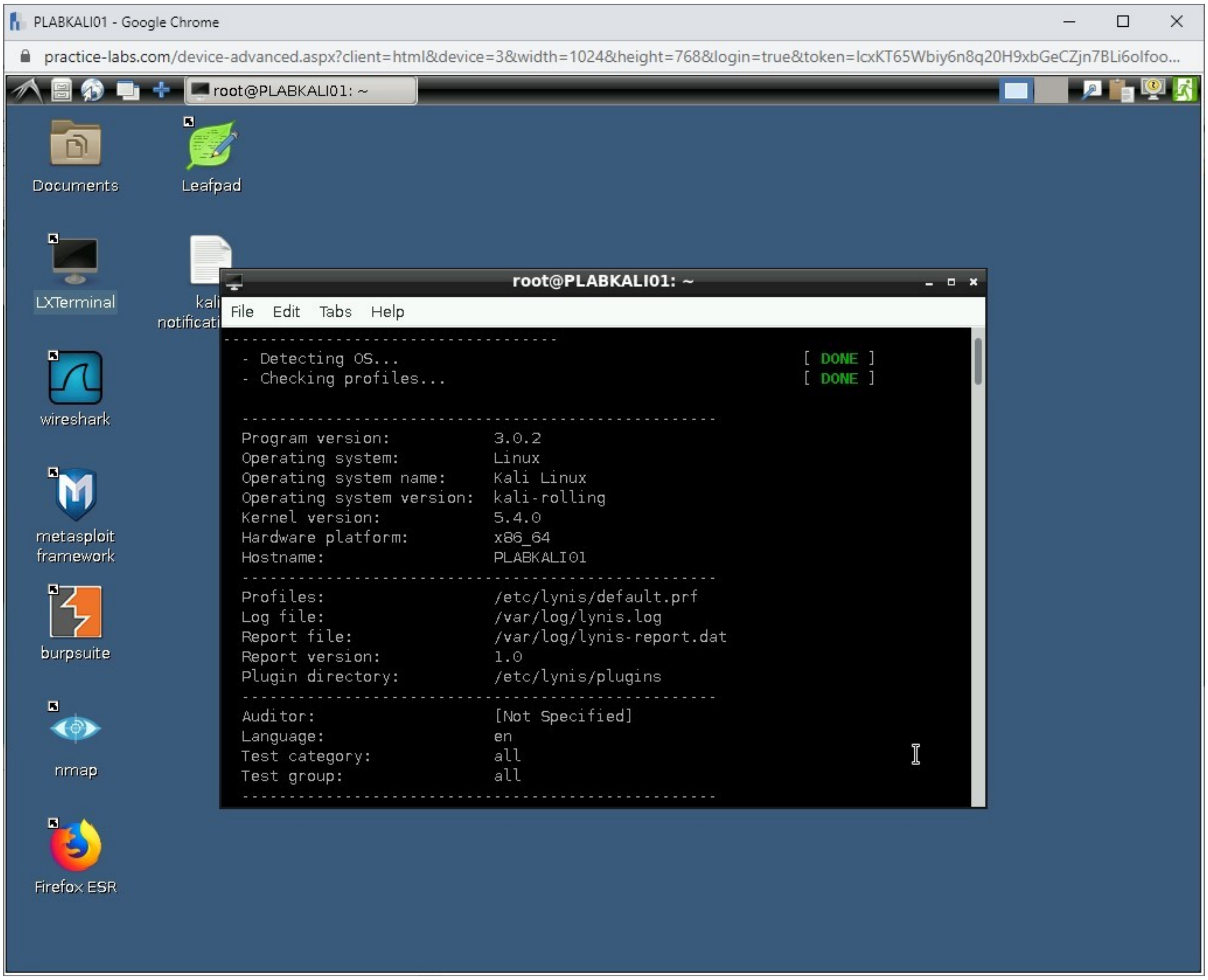
```
root@PLABKALI01: # lynis audit system
```

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.*

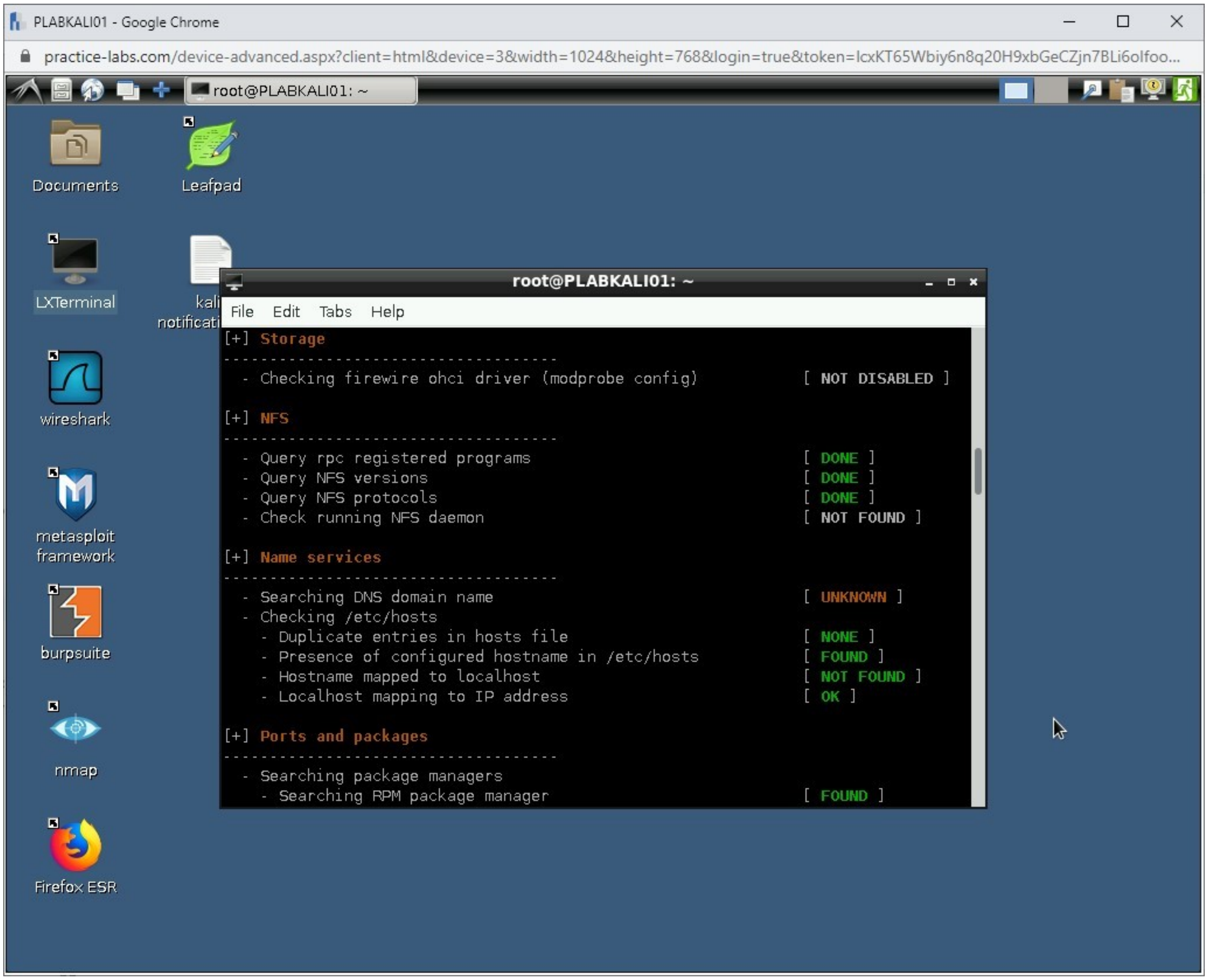

PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
root@PLABKALI01: ~
Documents
Leafpad
LXTerminal
kali notificati
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR
root@PLABKALI01: ~
File
Edit
Tabs
Help

```
-----------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           3.0.2
  Operating system:          Linux
  Operating system name:     Kali Linux
  Operating system version:  kali-rolling
  Kernel version:            5.4.0
  Hardware platform:         x86_64
  Hostname:                  PLABKALI01
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /etc/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
```

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.

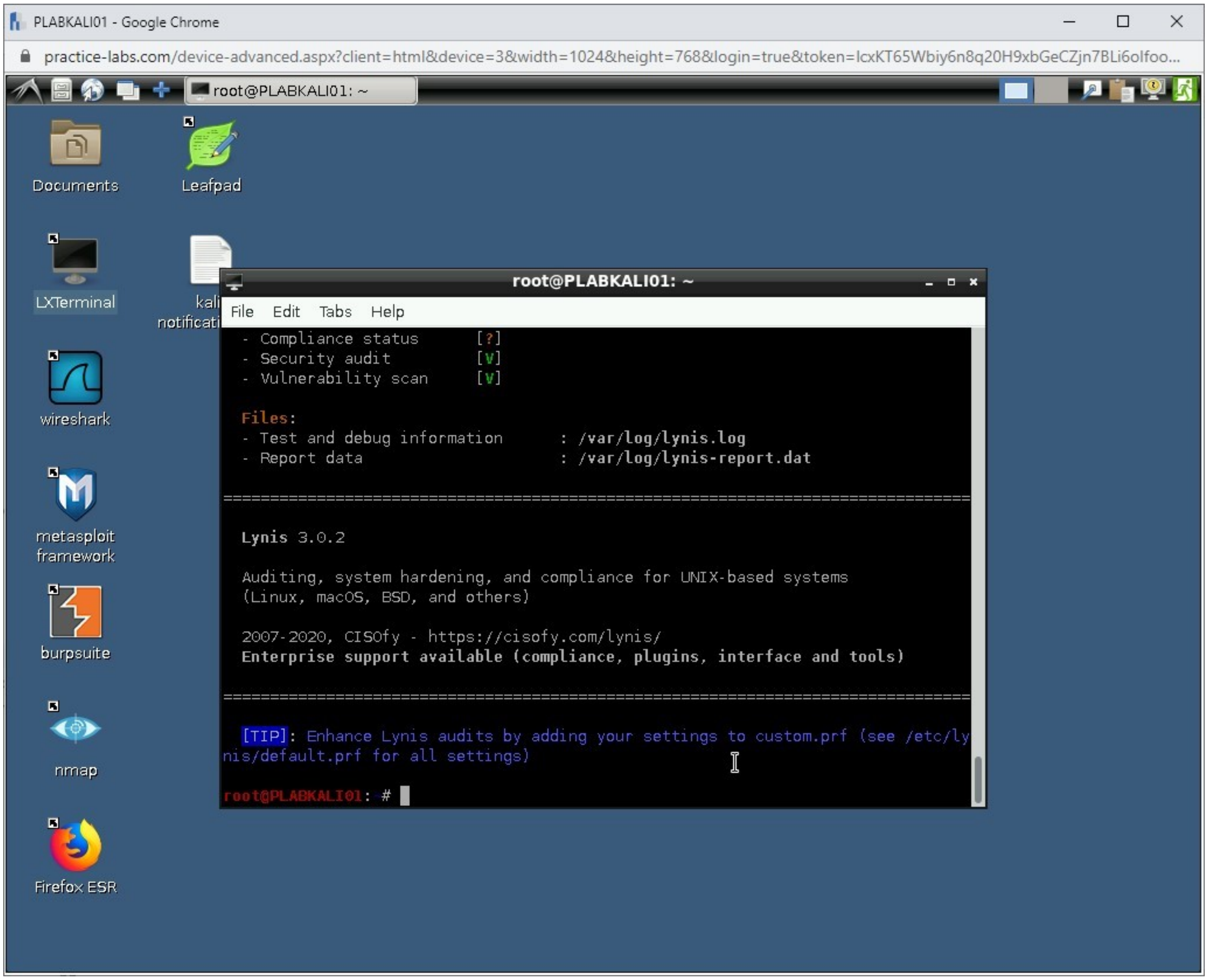

PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
root@PLABKALI01: ~
Documents
Leafpad
LXTerminal
kali notificati
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR
root@PLABKALI01: ~
File
Edit
Tabs
Help

```
[+] Storage
------------------------------------
  - Checking firewire ohci driver (modprobe config)          [ NOT DISABLED ]

[+] NFS
------------------------------------
  - Query rpc registered programs                            [ DONE ]
  - Query NFS versions                                       [ DONE ]
  - Query NFS protocols                                      [ DONE ]
  - Check running NFS daemon                                 [ NOT FOUND ]

[+] Name services
------------------------------------
  - Searching DNS domain name                                [ UNKNOWN ]
  - Checking /etc/hosts
    - Duplicate entries in hosts file                        [ NONE ]
    - Presence of configured hostname in /etc/hosts          [ FOUND ]
    - Hostname mapped to localhost                           [ NOT FOUND ]
    - Localhost mapping to IP address                        [ OK ]

[+] Ports and packages
------------------------------------
  - Searching package managers
    - Searching RPM package manager                          [ FOUND ]
```

Figure 1.29 Screenshot of PLABKALI01: Showing the output of the lynis command.

Step 5

The audit process completes.


PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=IcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
root@PLABKALI01: ~
Documents
Leafpad
LXTerminal
kali notificati
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR
root@PLABKALI01: ~
File
Edit
Tabs
Help

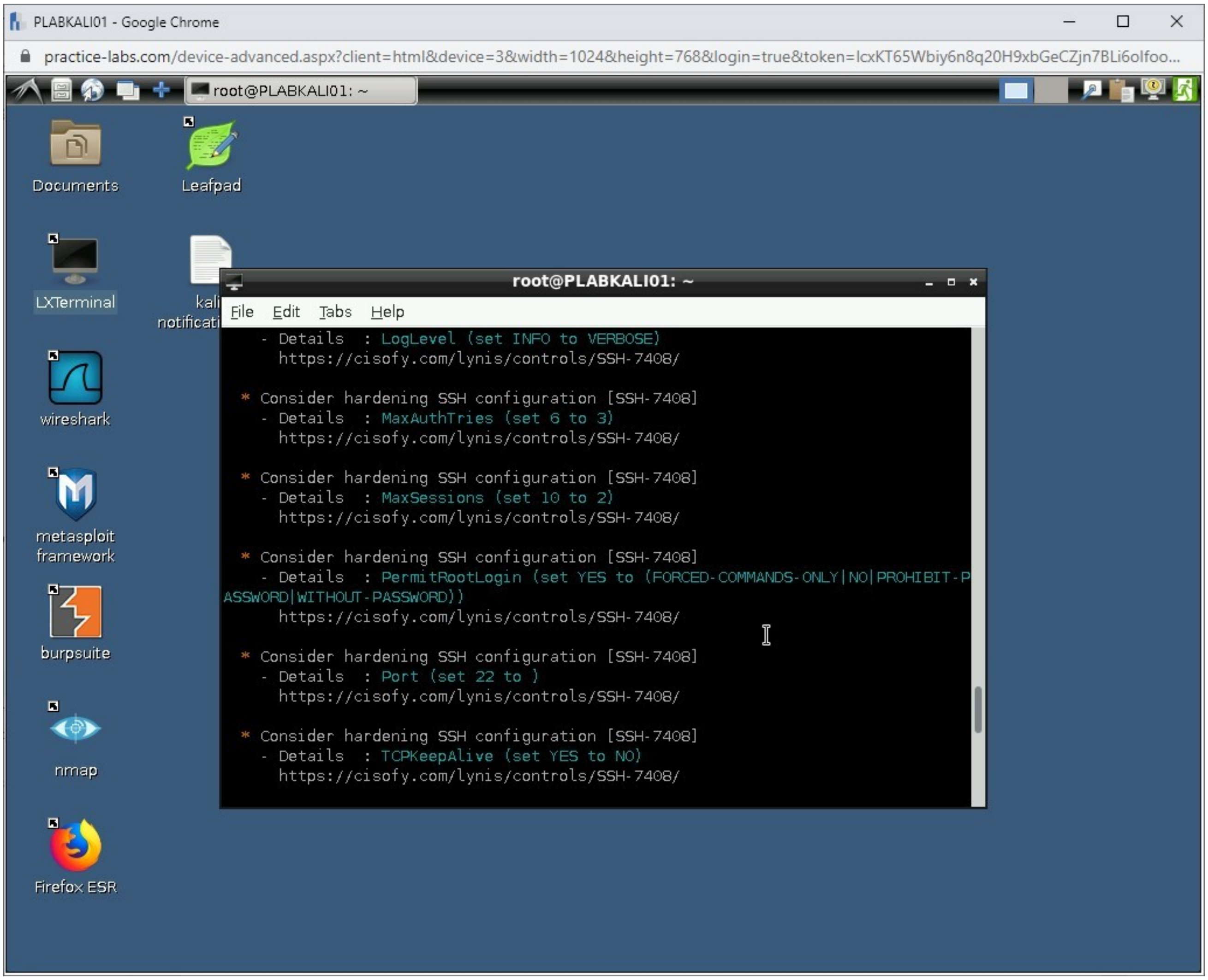
```
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

================================================================================

  Lynis 3.0.2

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2020, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

================================================================================

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/ly
nis/default.prf for all settings)

root@PLABKALI01: #
```

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*


PLABKALI01 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=lcxKT65Wbiy6n8q20H9xbGeCZjn7BLi6olfoo...
root@PLABKALI01: ~
Documents
Leafpad
LXTerminal
kali notificati
wireshark
metasploit framework
burpsuite
nmap
Firefox ESR
root@PLABKALI01: ~
File
Edit
Tabs
Help

```
    - Details  : LogLevel (set INFO to VERBOSE)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxAuthTries (set 6 to 3)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxSessions (set 10 to 2)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitRootLogin (set YES to (FORCED-COMMANDS-ONLY|NO|PROHIBIT-P
ASSWORD|WITHOUT-PASSWORD))
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Port (set 22 to )
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : TCPKeepAlive (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/
```

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

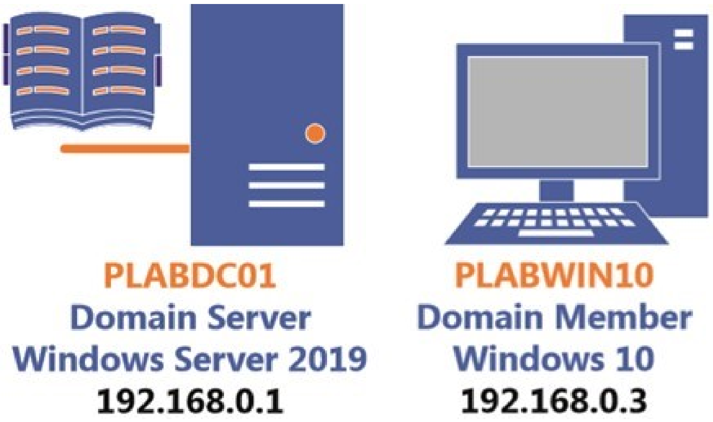
After completing this exercise, you will be able to:

- 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)



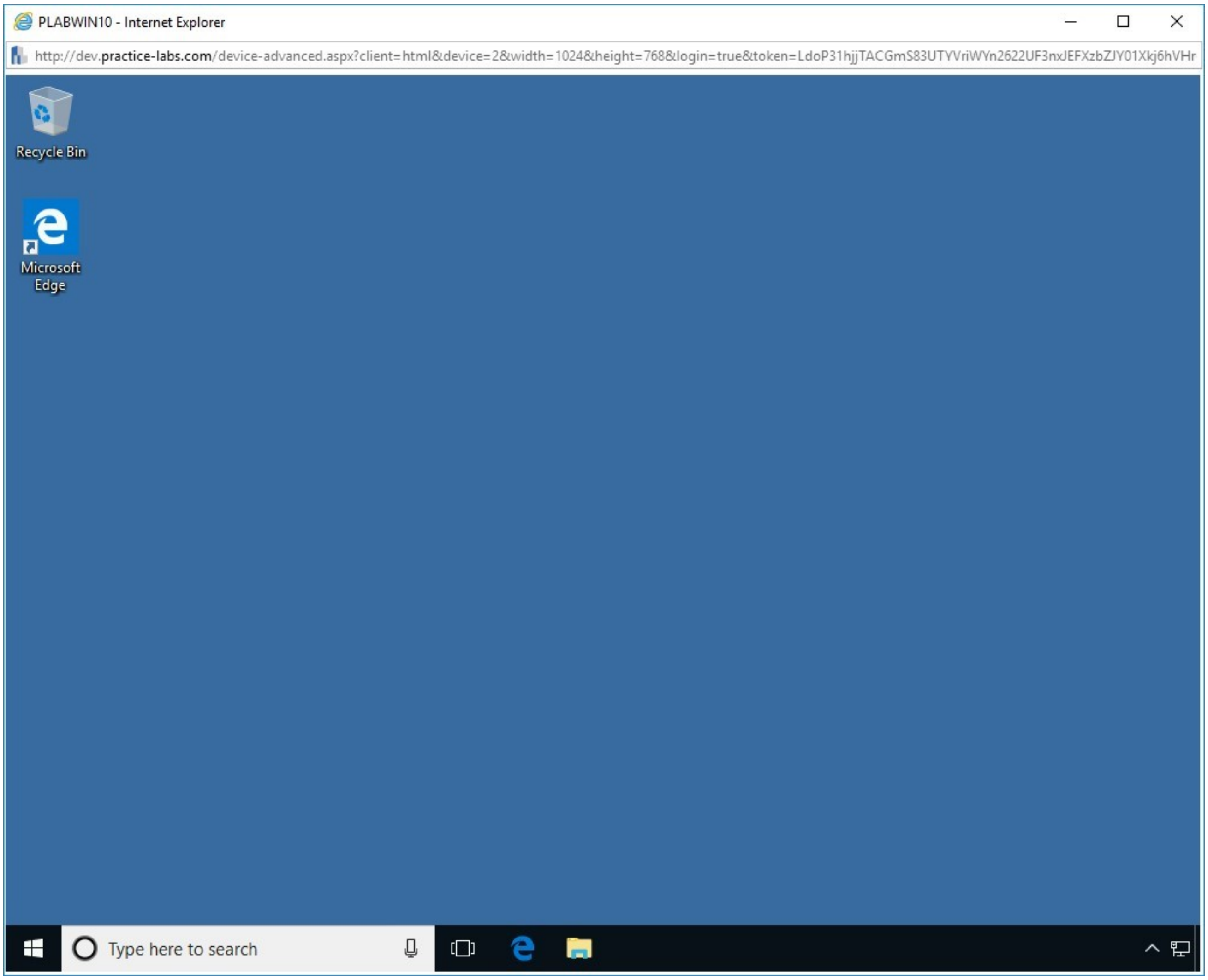
Task 1 - Install MBSA

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.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr

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

Step 2

Click **Microsoft Edge**, located on the taskbar.

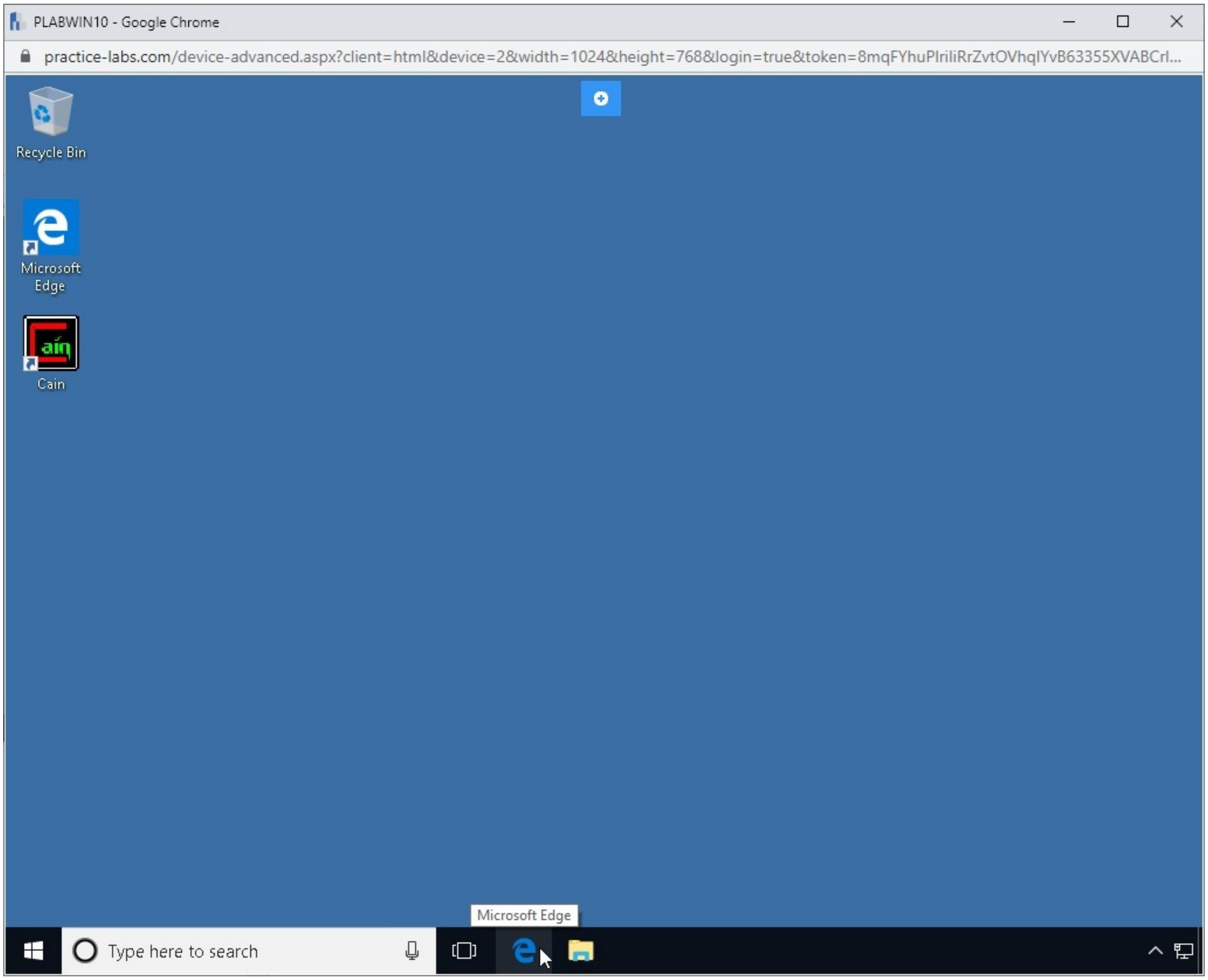
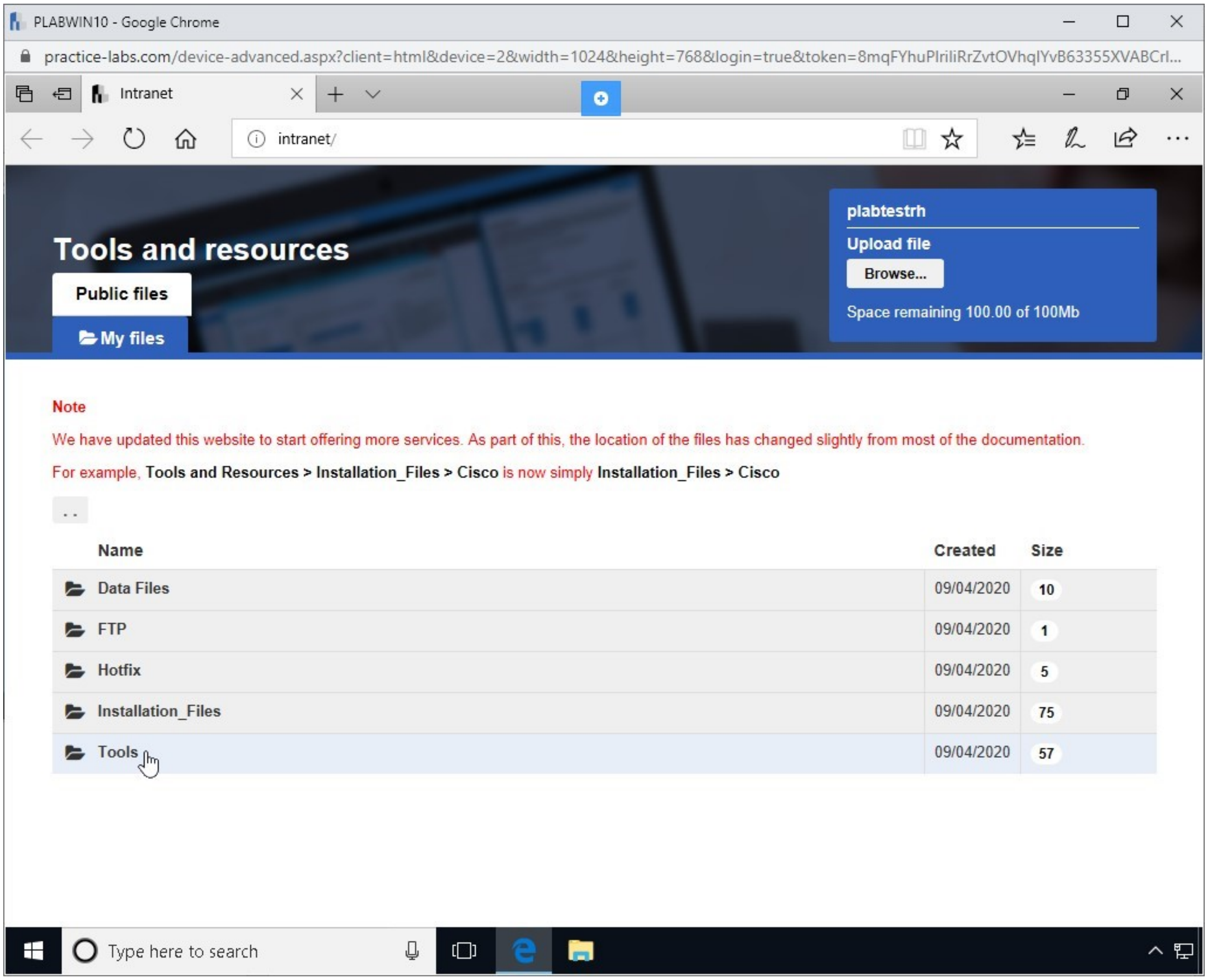

PLABWIN10 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=8mqFYhuPIriliRrZvtOVhqlYvB63355XVABCrl...
Recycle Bin
Microsoft Edge
Cain
Microsoft Edge
Type here to search

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.**


PLABWIN10 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=8mqFYhuPIriliRrZvtOVhqlYvB63355XVABCrl...
Intranet
intranet/
Tools and resources
Public files
My files
plabtestrh
Upload file
Browse...
Space remaining 100.00 of 100Mb
Type here to search

Note

We have updated this website to start offering more services. As part of this, the location of the files has changed slightly from most of the documentation.

For example, **Tools and Resources > Installation_Files > Cisco** is now simply **Installation_Files > Cisco**

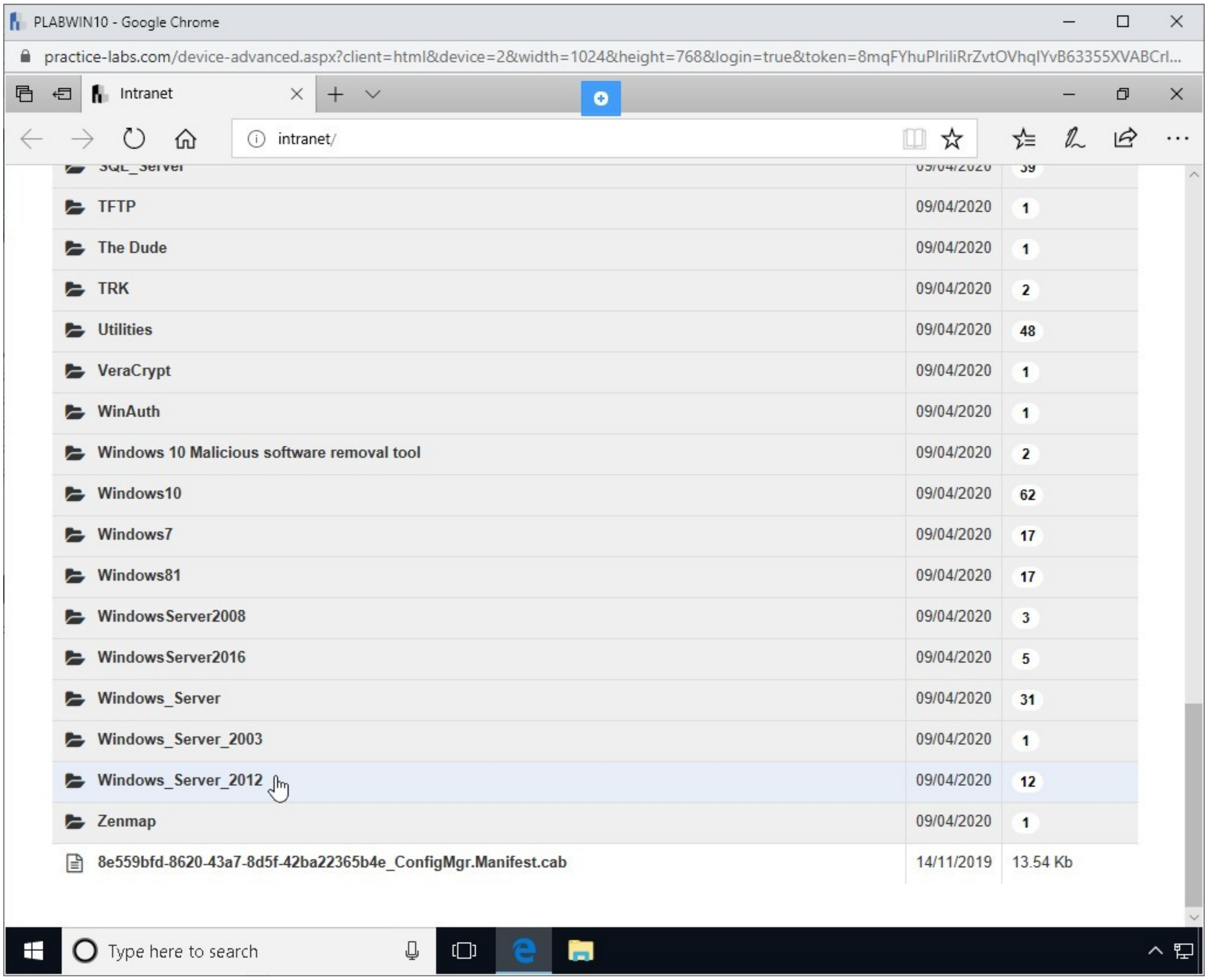
. .

Name	Created	Size
Data Files	09/04/2020	10
FTP	09/04/2020	1
Hotfix	09/04/2020	5
Installation_Files	09/04/2020	75
Tools	09/04/2020	57

Figure 2.3 Screenshot of PLABWIN10: Showing the Intranet page, Tools is highlighted.

Step 4

Scroll down the page and select the link for **Windows_Server_2012.**

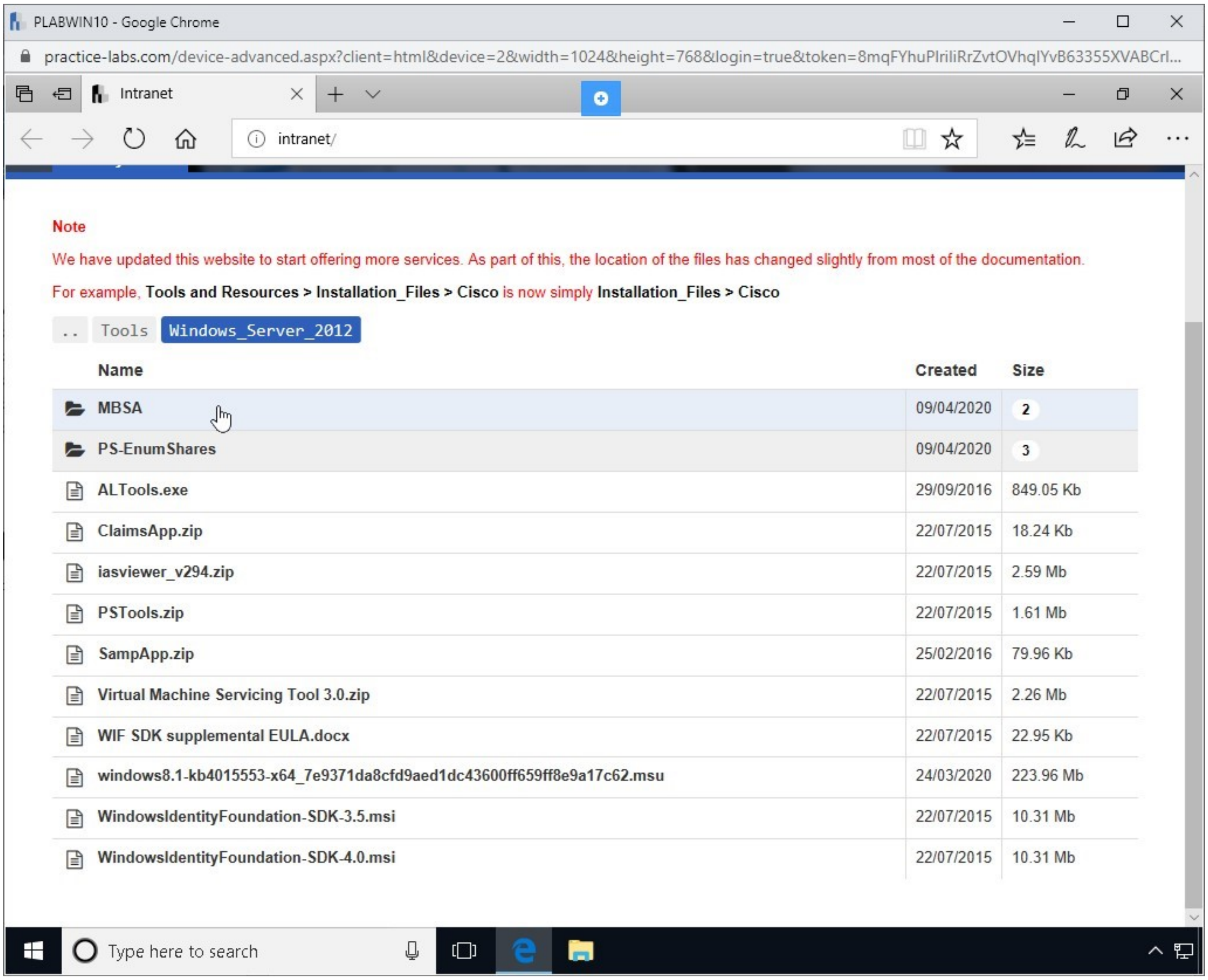

PLABWIN10 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=8mqFYhuPIriliRrZvtOVhqlYvB63355XVABCrl...
Intranet
intranet/
Type here to search

SQL_Server	09/04/2020	39
TFTP	09/04/2020	1
The Dude	09/04/2020	1
TRK	09/04/2020	2
Utilities	09/04/2020	48
VeraCrypt	09/04/2020	1
WinAuth	09/04/2020	1
Windows 10 Malicious software removal tool	09/04/2020	2
Windows10	09/04/2020	62
Windows7	09/04/2020	17
Windows81	09/04/2020	17
WindowsServer2008	09/04/2020	3
WindowsServer2016	09/04/2020	5
Windows_Server	09/04/2020	31
Windows_Server_2003	09/04/2020	1
Windows_Server_2012	09/04/2020	12
Zenmap	09/04/2020	1
8e559bfd-8620-43a7-8d5f-42ba22365b4e_ConfigMgr.Manifest.cab	14/11/2019	13.54 Kb

Figure 2.4 Screenshot of PLABWIN10: Showing the Intranet page, Windows_Server_2012 is highlighted.

Step 5

Click the link for **MBSA.**


PLABWIN10 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=8mqFYhuPlriliRrZvtOVhqlYvB63355XVABCrl...
Intranet
intranet/
Type here to search

Note

We have updated this website to start offering more services. As part of this, the location of the files has changed slightly from most of the documentation.

For example, **Tools and Resources > Installation_Files > Cisco** is now simply **Installation_Files > Cisco**

.. Tools Windows_Server_2012

Name	Created	Size
MBSA	09/04/2020	2
PS-EnumShares	09/04/2020	3
ALTools.exe	29/09/2016	849.05 Kb
ClaimsApp.zip	22/07/2015	18.24 Kb
iasviewer_v294.zip	22/07/2015	2.59 Mb
PSTools.zip	22/07/2015	1.61 Mb
SampApp.zip	25/02/2016	79.96 Kb
Virtual Machine Servicing Tool 3.0.zip	22/07/2015	2.26 Mb
WIF SDK supplemental EULA.docx	22/07/2015	22.95 Kb
windows8.1-kb4015553-x64_7e9371da8cfd9aed1dc43600ff659ff8e9a17c62.msu	24/03/2020	223.96 Mb
WindowsIdentityFoundation-SDK-3.5.msi	22/07/2015	10.31 Mb
WindowsIdentityFoundation-SDK-4.0.msi	22/07/2015	10.31 Mb

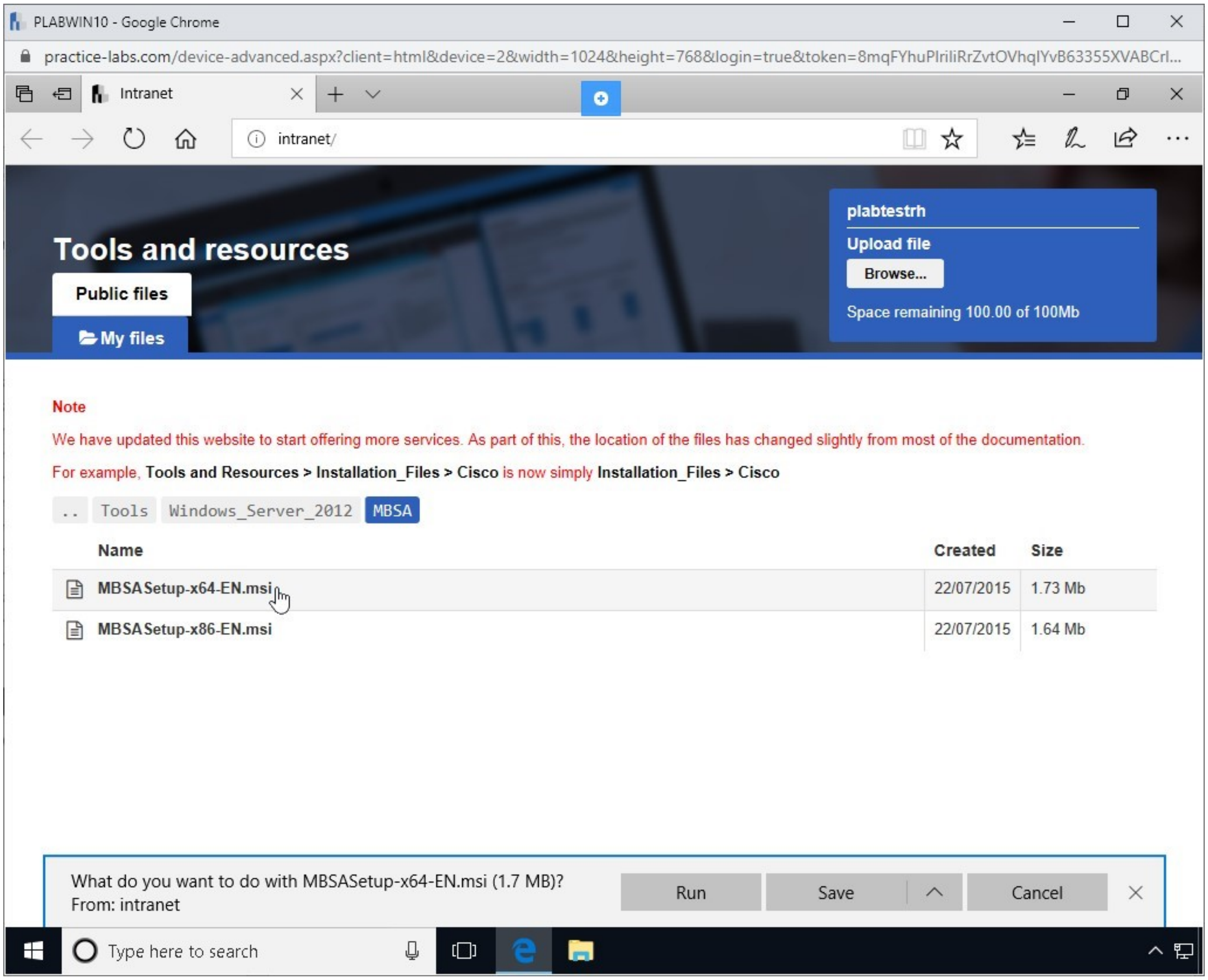
Figure 2.5 Screenshot of PLABWIN10: Showing the Intranet page, MBSA is highlighted.

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.**



PLABWIN10 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=8mqFYhuPIriliRrZvtOVhqIYvB63355XVABCrl...
Intranet
intranet/
Tools and resources
Public files
My files
plabtestrh
Upload file
Browse...
Space remaining 100.00 of 100Mb
.. Tools Windows_Server_2012 MBSA
Run
Save
Cancel
Type here to search

Note

We have updated this website to start offering more services. As part of this, the location of the files has changed slightly from most of the documentation.

For example, **Tools and Resources > Installation_Files > Cisco** is now simply **Installation_Files > Cisco**

Name	Created	Size
MBSASetup-x64-EN.msi	22/07/2015	1.73 Mb
MBSASetup-x86-EN.msi	22/07/2015	1.64 Mb

What do you want to do with MBSASetup-x64-EN.msi (1.7 MB)?
From: intranet

Figure 2.6 Screenshot of PLABWIN10: Showing the Intranet page, MBSA Setup-x64-EN-msi is highlighted and showing the pop-up at the bottom of the Microsoft Edge window.

Step 7

From the taskbar, click **File Explorer**.

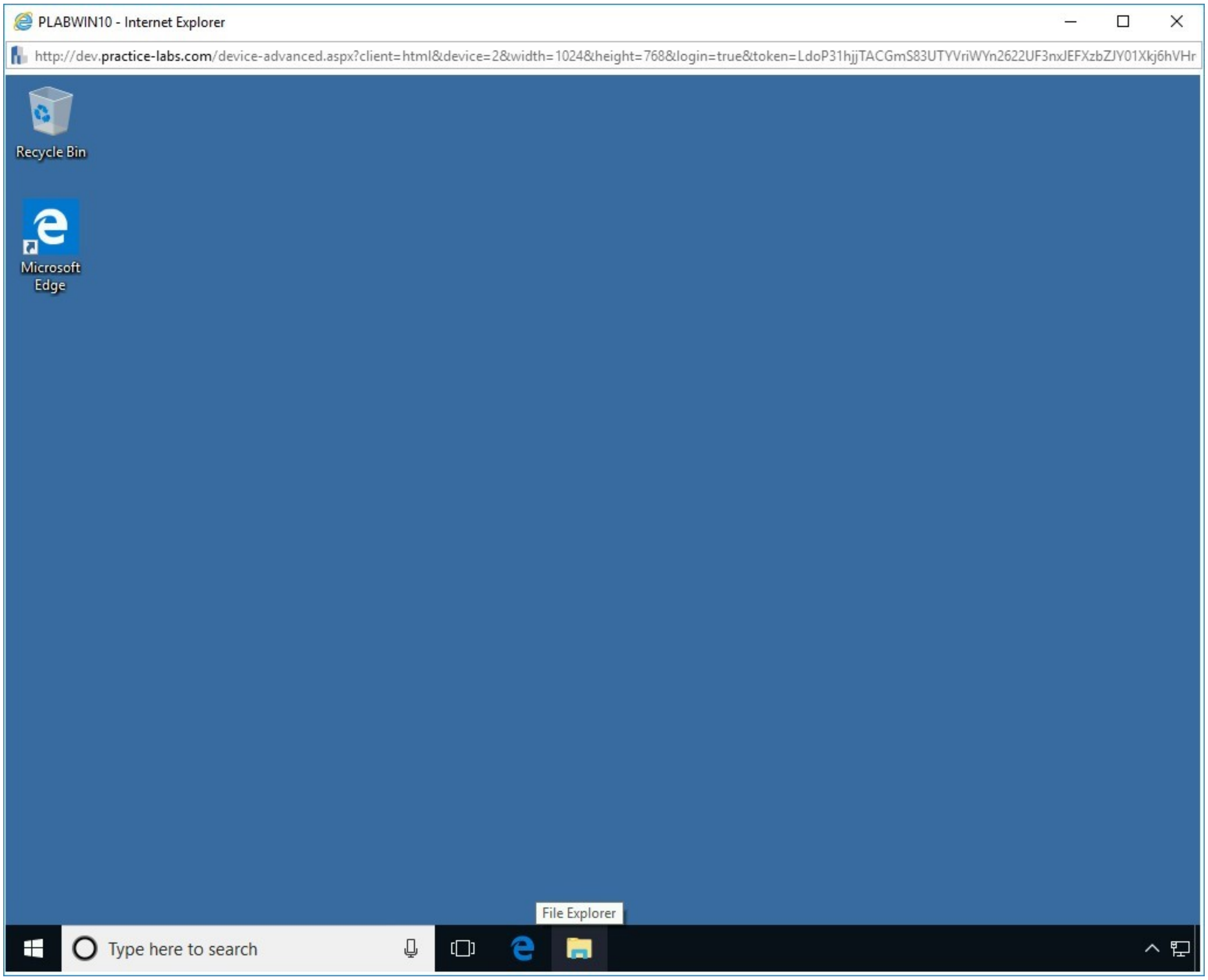
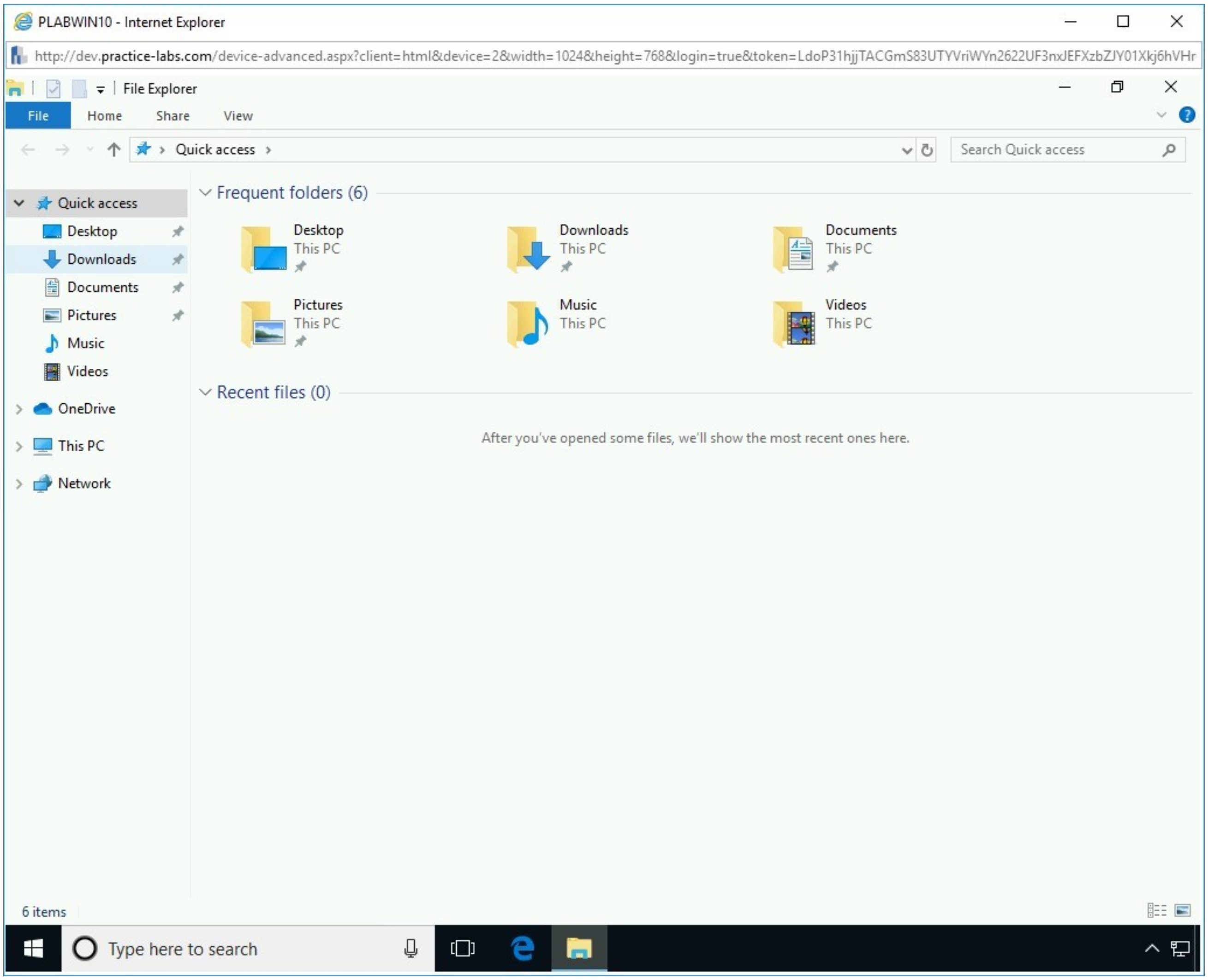

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Recycle Bin
Microsoft Edge
File Explorer
Type here to search

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.



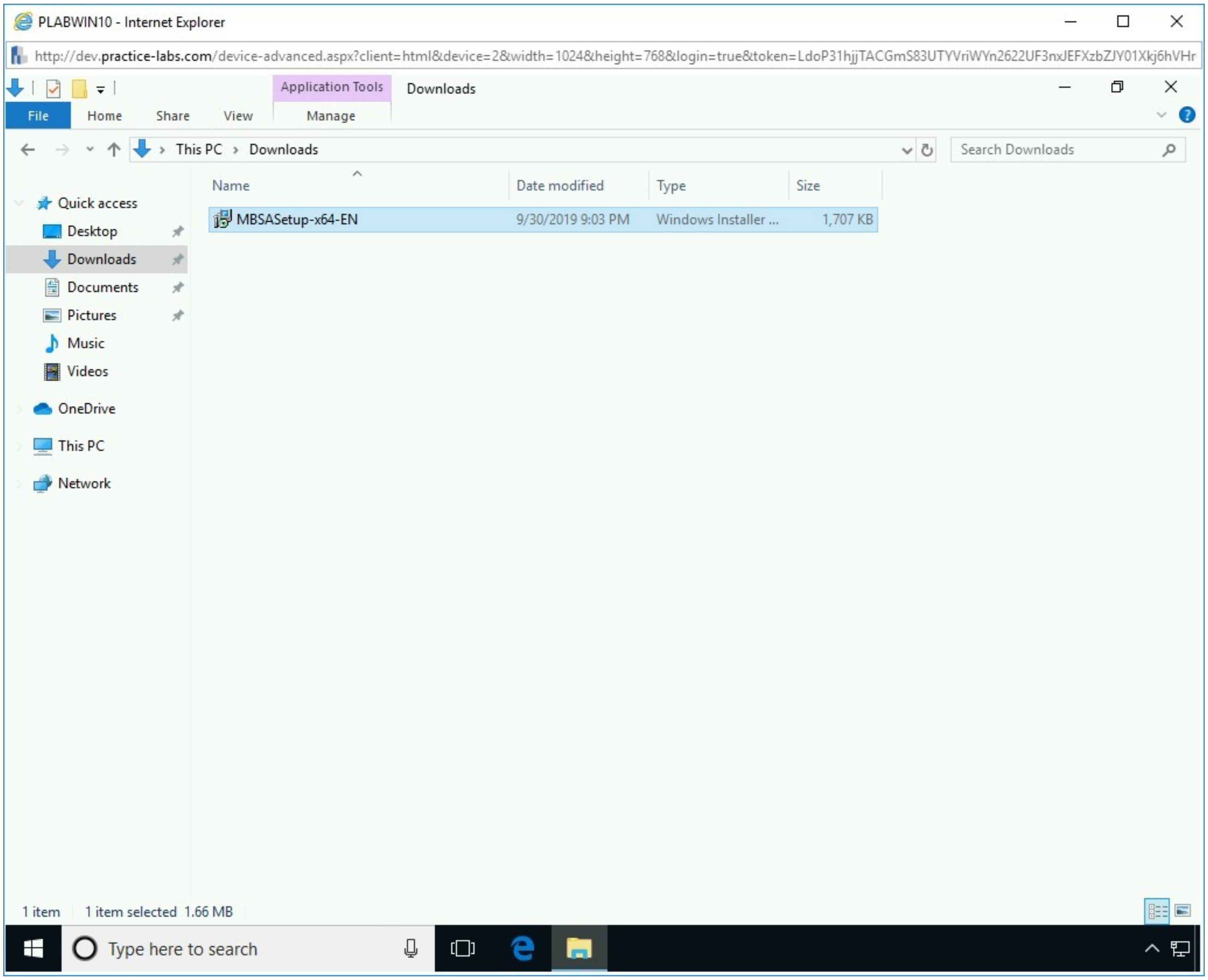
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr

After you've opened some files, we'll show the most recent ones here.

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.

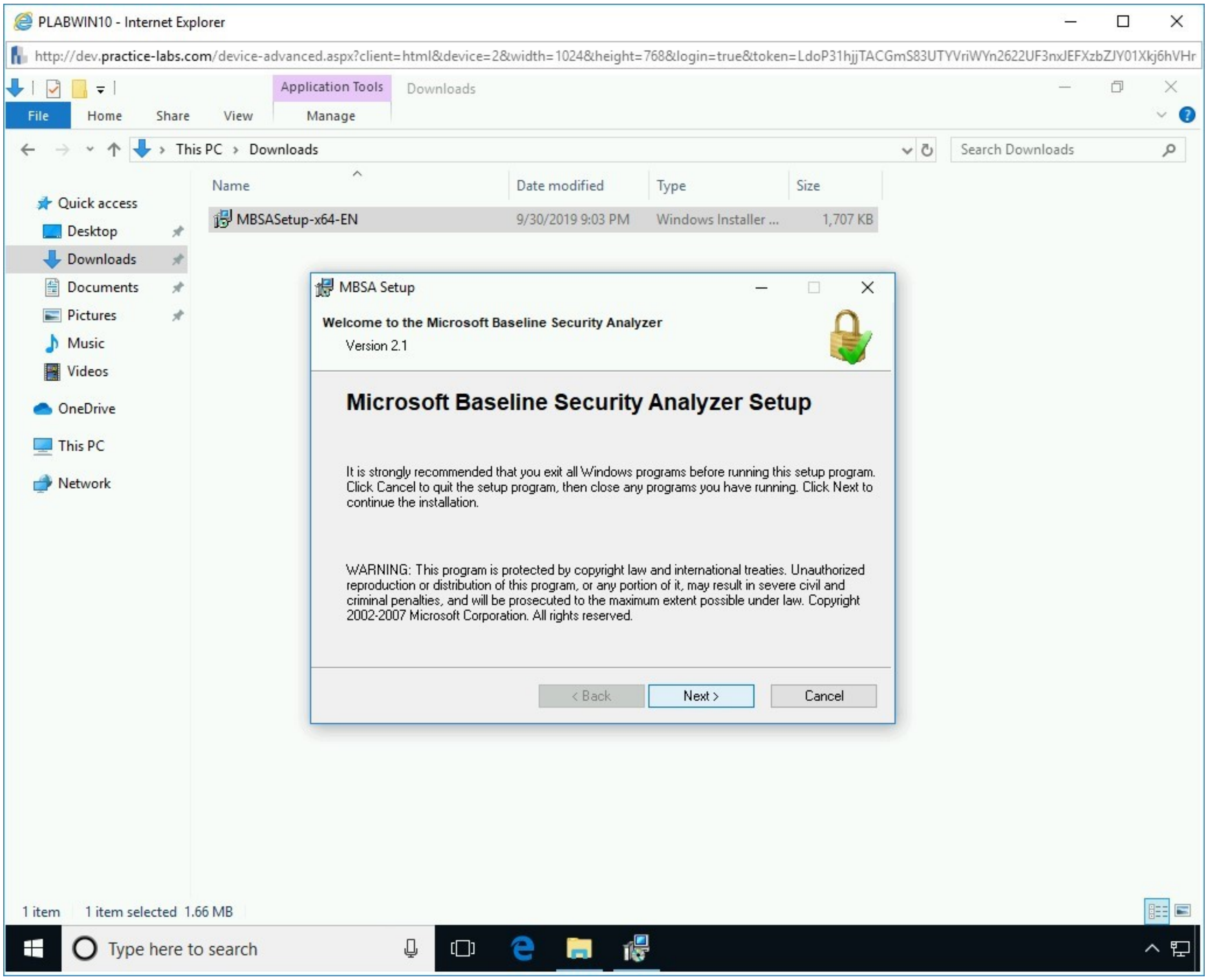


Name	Date modified	Type	Size
MBSASetup-x64-EN	9/30/2019 9:03 PM	Windows Installer ...	1,707 KB

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**.



MBSA Setup

Welcome to the Microsoft Baseline Security Analyzer

Version 2.1

Microsoft Baseline Security Analyzer Setup

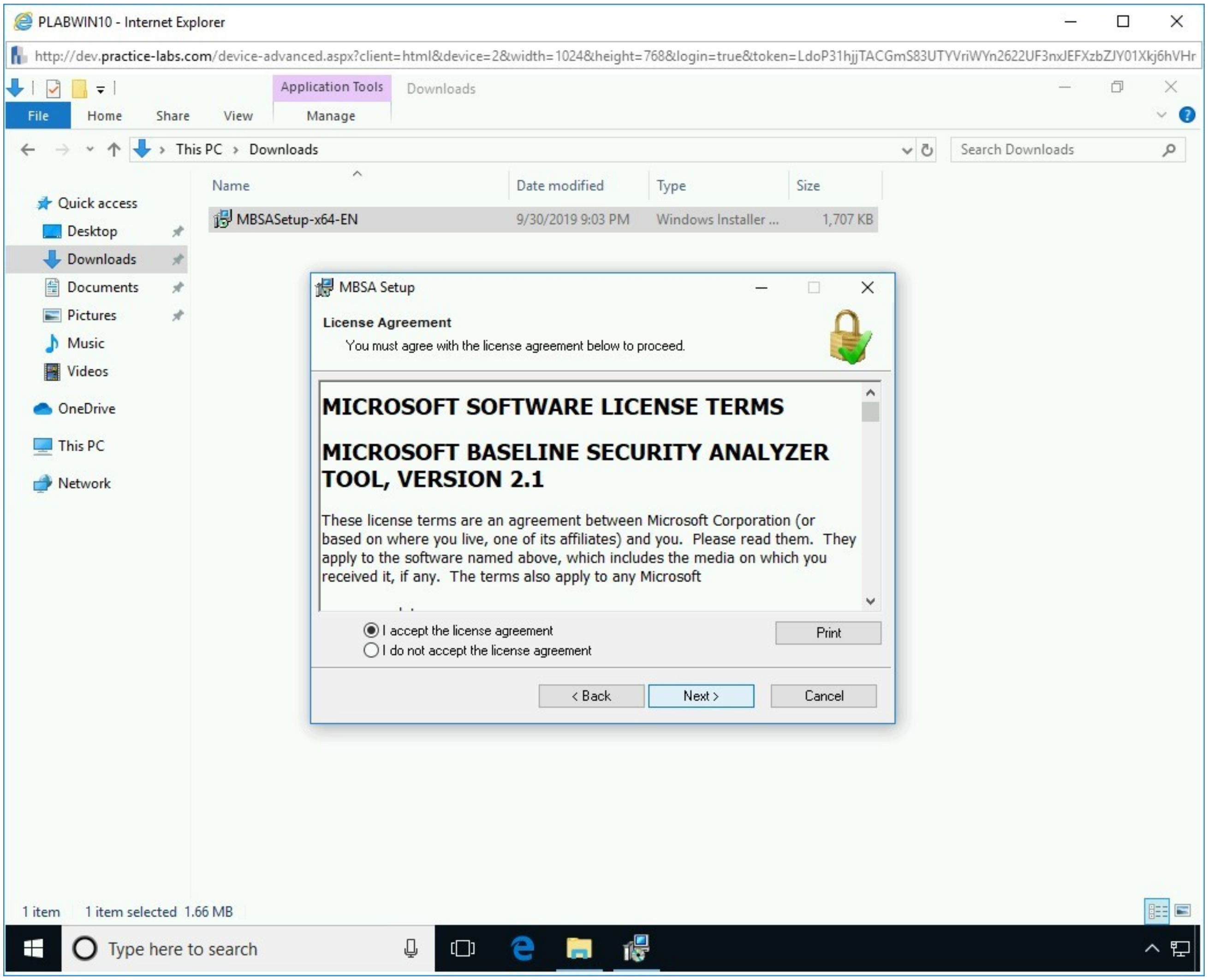
It is strongly recommended that you exit all Windows programs before running this setup program. Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

WARNING: This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law. Copyright 2002-2007 Microsoft Corporation. All rights reserved.

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**.



License Agreement

You must agree with the license agreement below to proceed.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT BASELINE SECURITY ANALYZER TOOL, VERSION 2.1

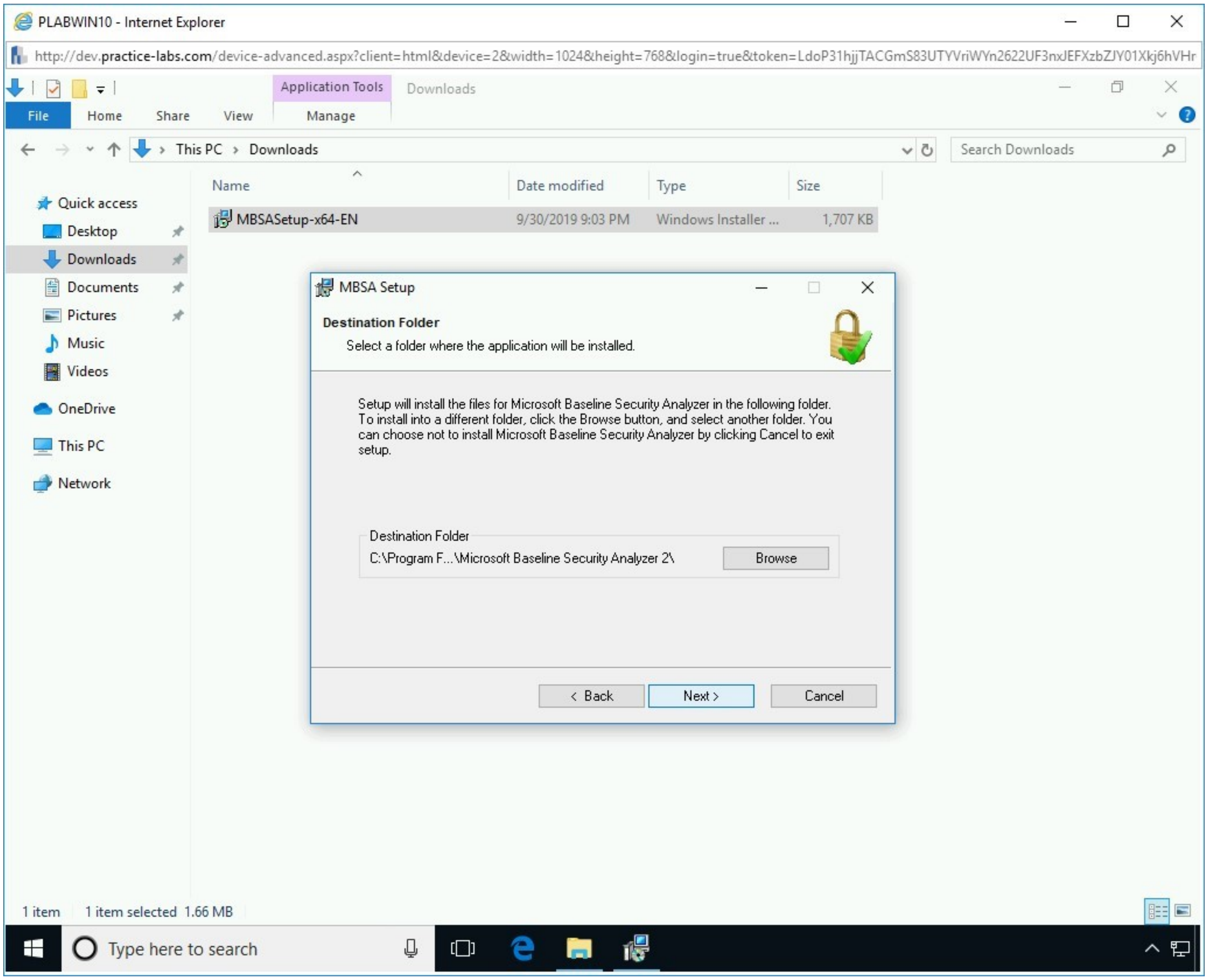
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

● I accept the license agreement
○ I do not accept the license agreement

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**.



MBSA Setup

Destination Folder

Select a folder where the application will be installed.

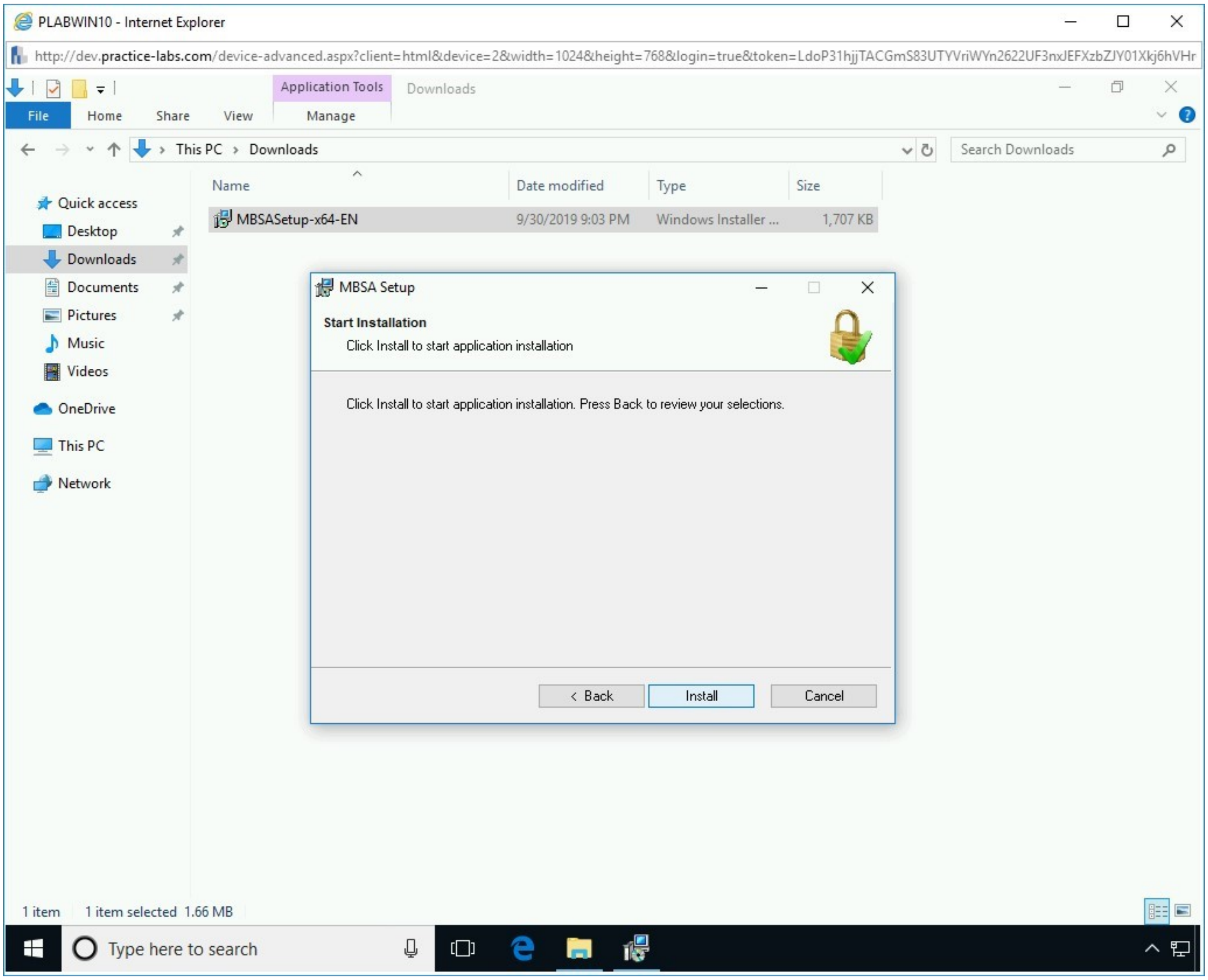
Setup will install the files for Microsoft Baseline Security Analyzer in the following folder. To install into a different folder, click the Browse button, and select another folder. You can choose not to install Microsoft Baseline Security Analyzer by clicking Cancel to exit setup.

Destination Folder
C:\Program F...\Microsoft Baseline Security Analyzer 2\

Figure 2.12 Screenshot of PLABWIN10: Clicking Next on the Destination Folder page.

Step 13

On the **Start Installation** page, click **Install**.



Name	Date modified	Type	Size
MBSASetup-x64-EN	9/30/2019 9:03 PM	Windows Installer ...	1,707 KB

MBSA Setup

Start Installation

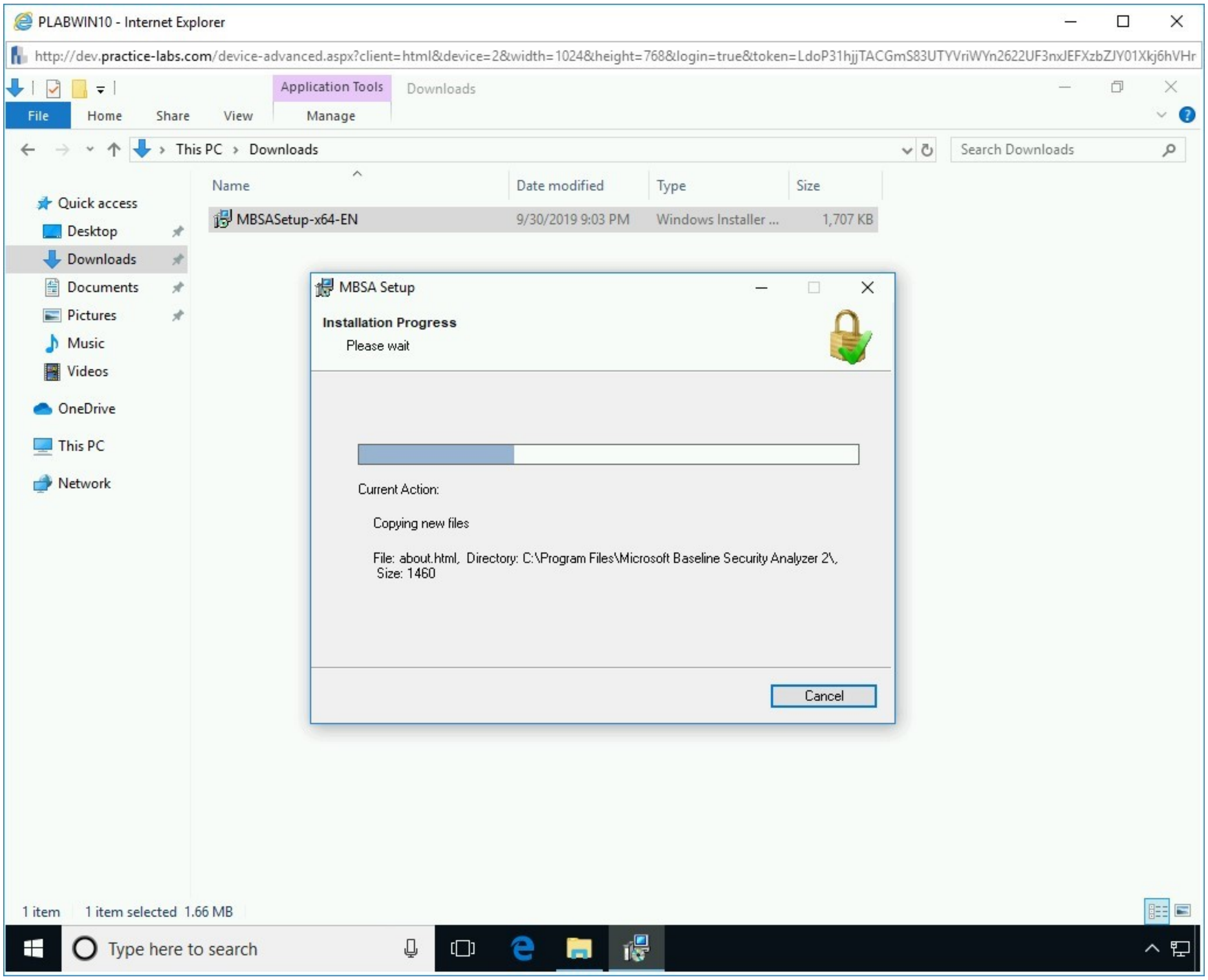
Click Install to start application installation

Click Install to start application installation. Press Back to review your selections.

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.



Name	Date modified	Type	Size
MBSASetup-x64-EN	9/30/2019 9:03 PM	Windows Installer ...	1,707 KB

MBSA Setup

Installation Progress

Please wait

Current Action:

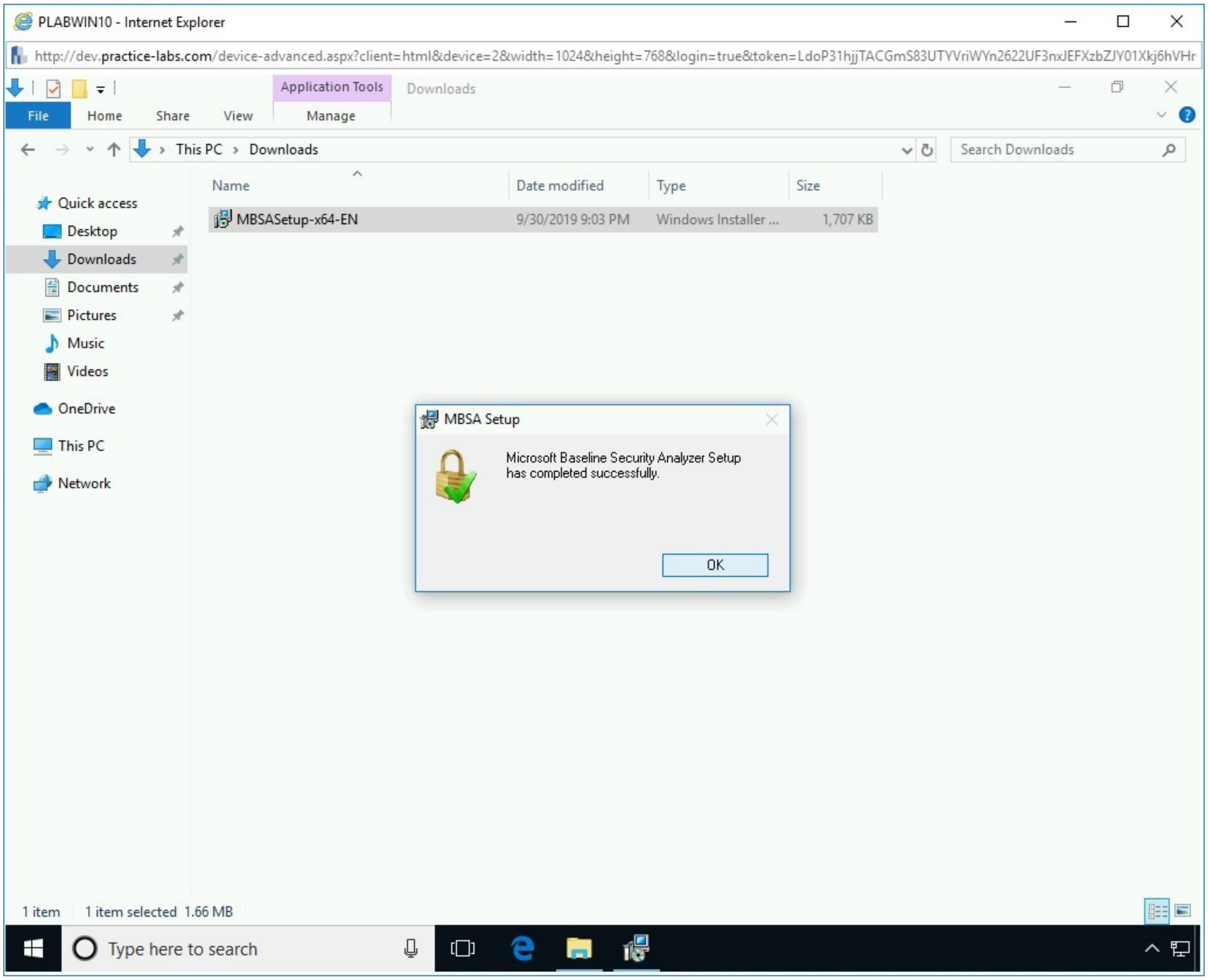
Copying new files

File: about.html, Directory: C:\Program Files\Microsoft Baseline Security Analyzer 2\, Size: 1460

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**.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr

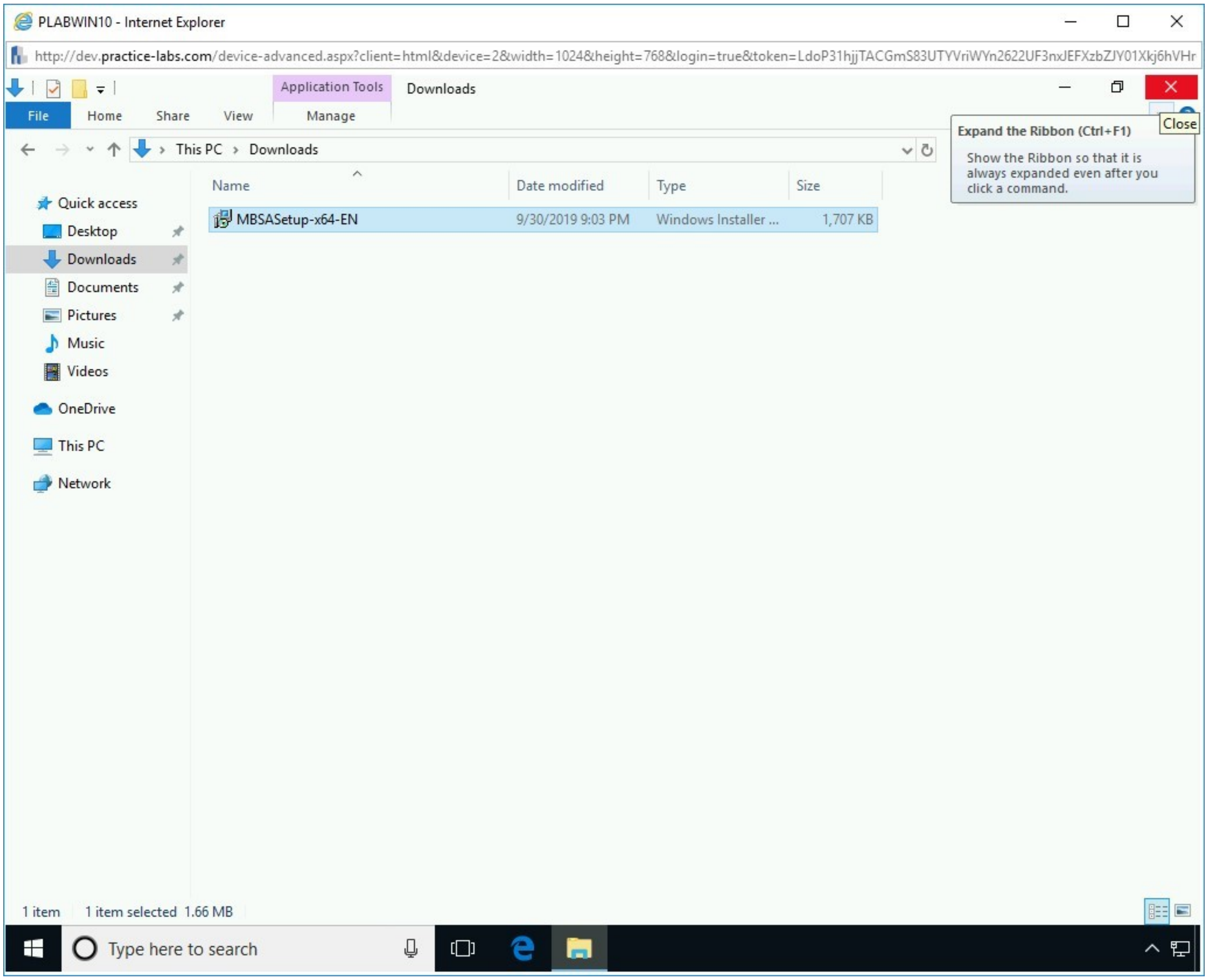
Name	Date modified	Type	Size
MBSASetup-x64-EN	9/30/2019 9:03 PM	Windows Installer ...	1,707 KB

Microsoft Baseline Security Analyzer Setup has completed successfully.

Figure 2.15 Screenshot of PLABWIN10: Clicking OK on the MBSA Setup dialog box.

Step 16

Close the **File Explorer** window.



Expand the Ribbon (Ctrl+F1)

Show the Ribbon so that it is always expanded even after you click a command.

Name	Date modified	Type	Size
MBSASetup-x64-EN	9/30/2019 9:03 PM	Windows Installer ...	1,707 KB

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

Step 17

Notice that the MBSA icon appears on the desktop.

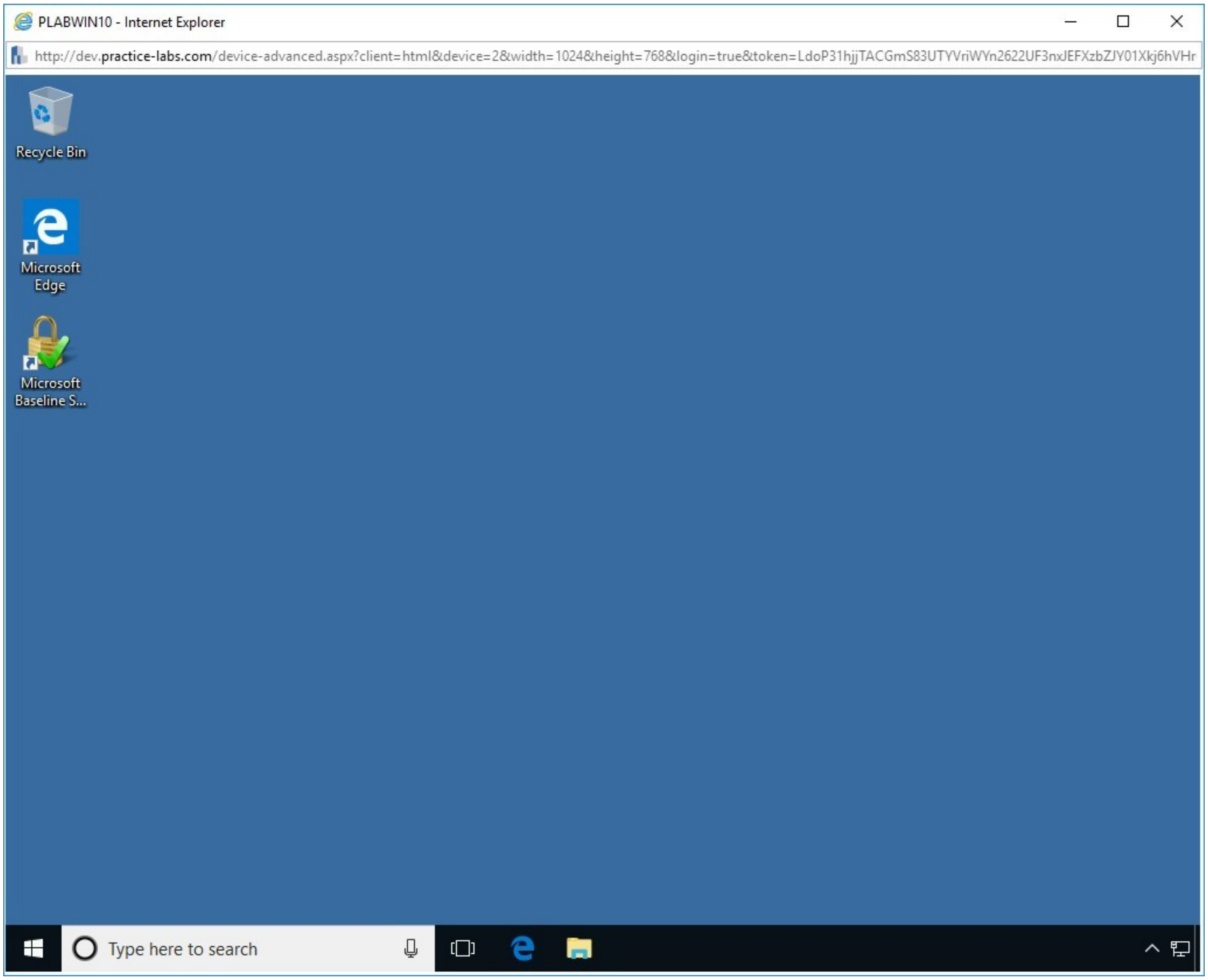

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Recycle Bin
Microsoft Edge
Microsoft Baseline S...
Type here to search

Figure 2.17 Screenshot of PLABWIN10: Showing the MBSA icon 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.

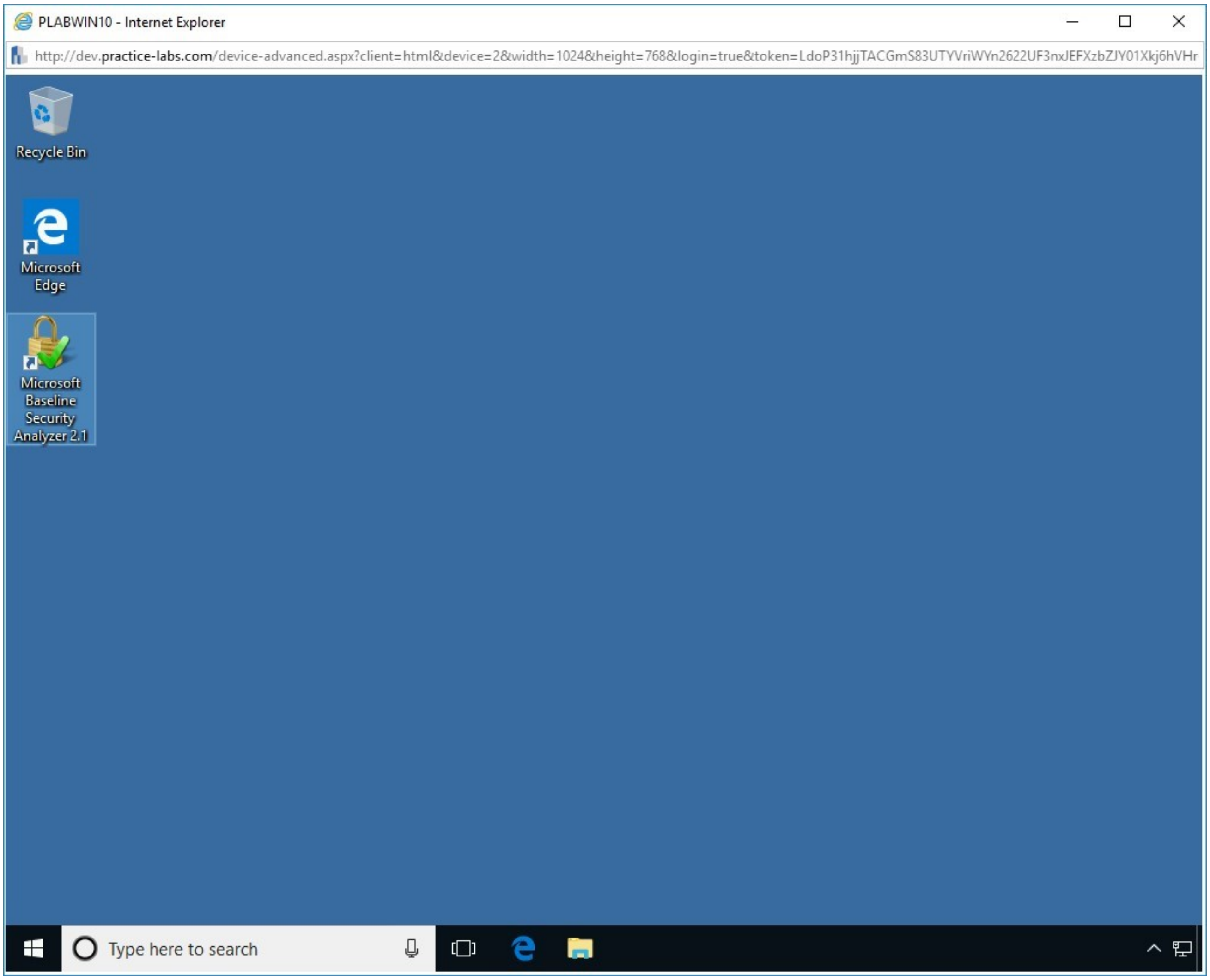
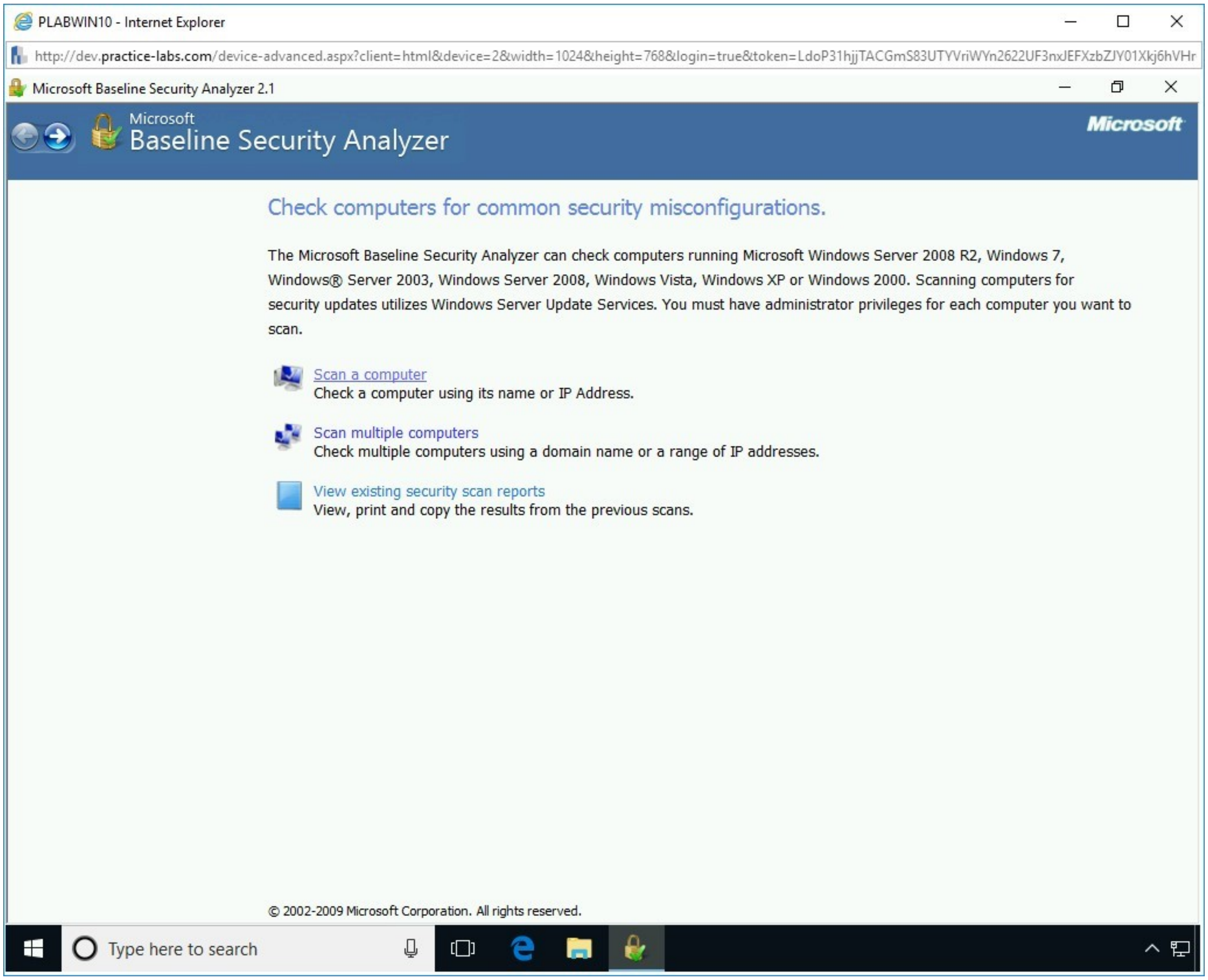

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Recycle Bin
Microsoft Edge
Microsoft Baseline Security Analyzer 2.1
Type here to search

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**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft
Type here to search

Check computers for common security misconfigurations.

The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, Windows XP or Windows 2000. Scanning computers for security updates utilizes Windows Server Update Services. You must have administrator privileges for each computer you want to scan.

Scan a computer
Check a computer using its name or IP Address.

Scan multiple computers
Check multiple computers using a domain name or a range of IP addresses.

View existing security scan reports
View, print and copy the results from the previous scans.

© 2002-2009 Microsoft Corporation. All rights reserved.

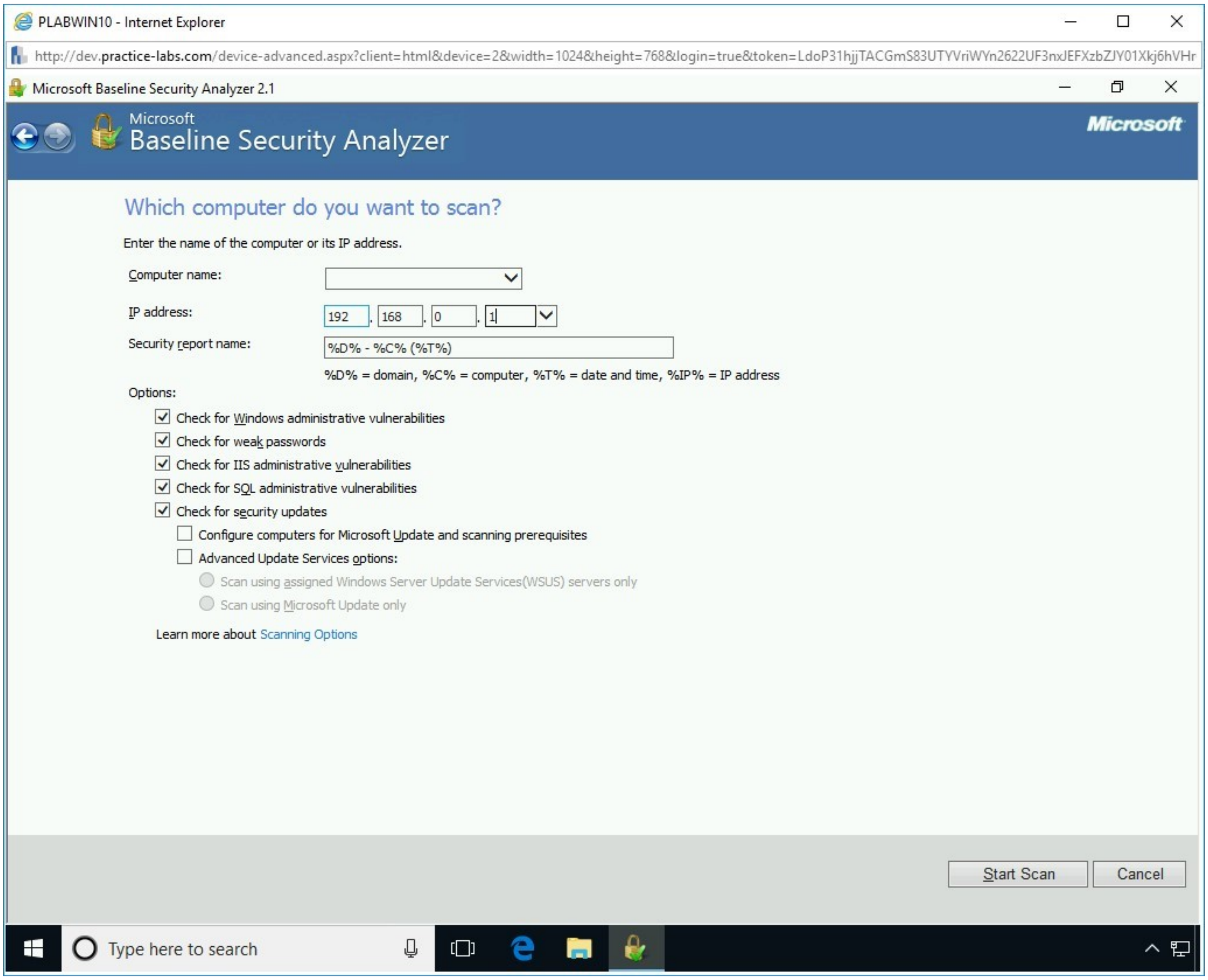
Figure 2.19 Screenshot of PLABWIN10: Selecting the Scan a computer option

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
```



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr

Microsoft Baseline Security Analyzer 2.1

Microsoft
Baseline Security Analyzer

Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name:

IP address: 192 . 168 . 0 . 1

Security report name: %D% - %C% (%T%)

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

Options:

☑ Check for Windows administrative vulnerabilities
☑ Check for weak passwords
☑ Check for IIS administrative vulnerabilities
☑ Check for SQL administrative vulnerabilities
☑ Check for security updates
☐ Configure computers for Microsoft Update and scanning prerequisites
☐ Advanced Update Services options:
○ Scan using assigned Windows Server Update Services(WSUS) servers only
○ Scan using Microsoft Update only

Learn more about Scanning Options

Figure 2.20 Screenshot of PLABWIN10: Showing the MBSA configuration page with IP range added.

Step 4

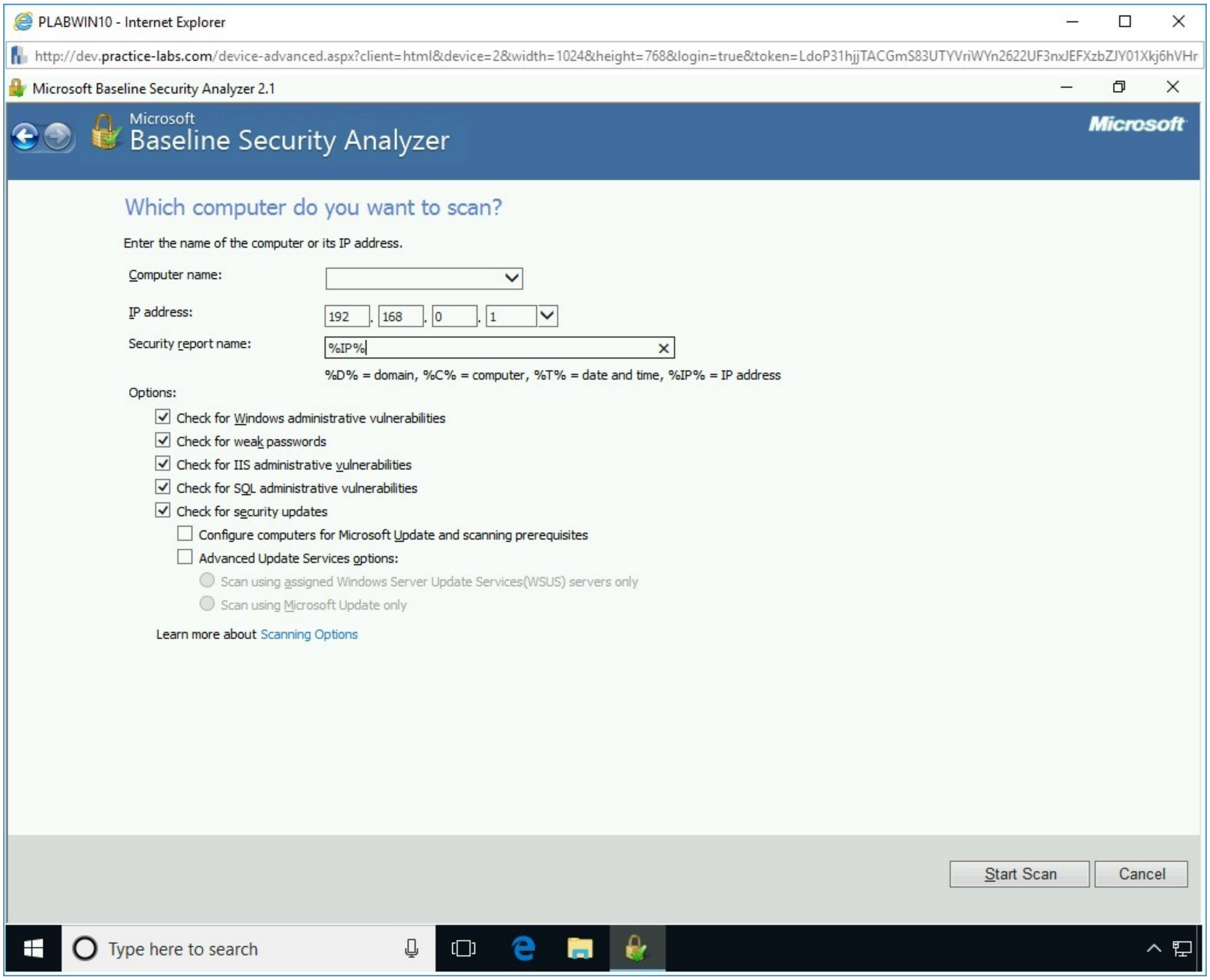
Change the **Security Report Name** to something preferable and identifiable such as:

```
%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


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft
Start Scan
Cancel
Type here to search

Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name:

IP address: 192 . 168 . 0 . 1

Security report name: %IP%

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

Options:

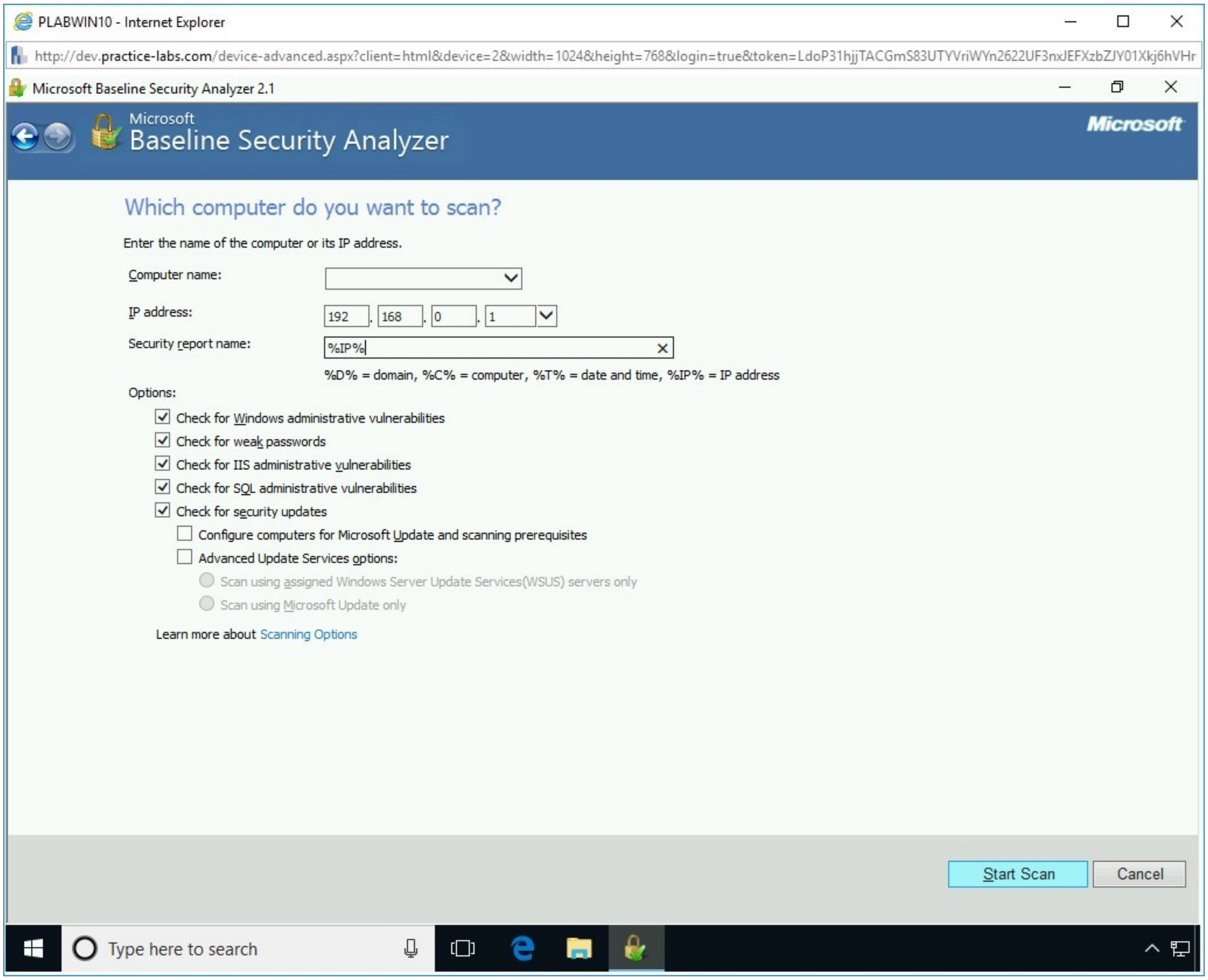
☑ Check for Windows administrative vulnerabilities
☑ Check for weak passwords
☑ Check for IIS administrative vulnerabilities
☑ Check for SQL administrative vulnerabilities
☑ Check for security updates
□ Configure computers for Microsoft Update and scanning prerequisites
□ Advanced Update Services options:
○ Scan using assigned Windows Server Update Services(WSUS) servers only
○ Scan using Microsoft Update only

Learn more about Scanning Options

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.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr

Microsoft Baseline Security Analyzer 2.1

Microsoft
Baseline Security Analyzer

Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name:

IP address: 192 . 168 . 0 . 1

Security report name: %IP%

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

Options:

- ☑ Check for Windows administrative vulnerabilities
- ☑ Check for weak passwords
- ☑ Check for IIS administrative vulnerabilities
- ☑ Check for SQL administrative vulnerabilities
- ☑ Check for security updates
  - ☐ Configure computers for Microsoft Update and scanning prerequisites
  - ☐ Advanced Update Services options:
    - ○ Scan using assigned Windows Server Update Services(WSUS) servers only
    - ○ Scan using Microsoft Update only

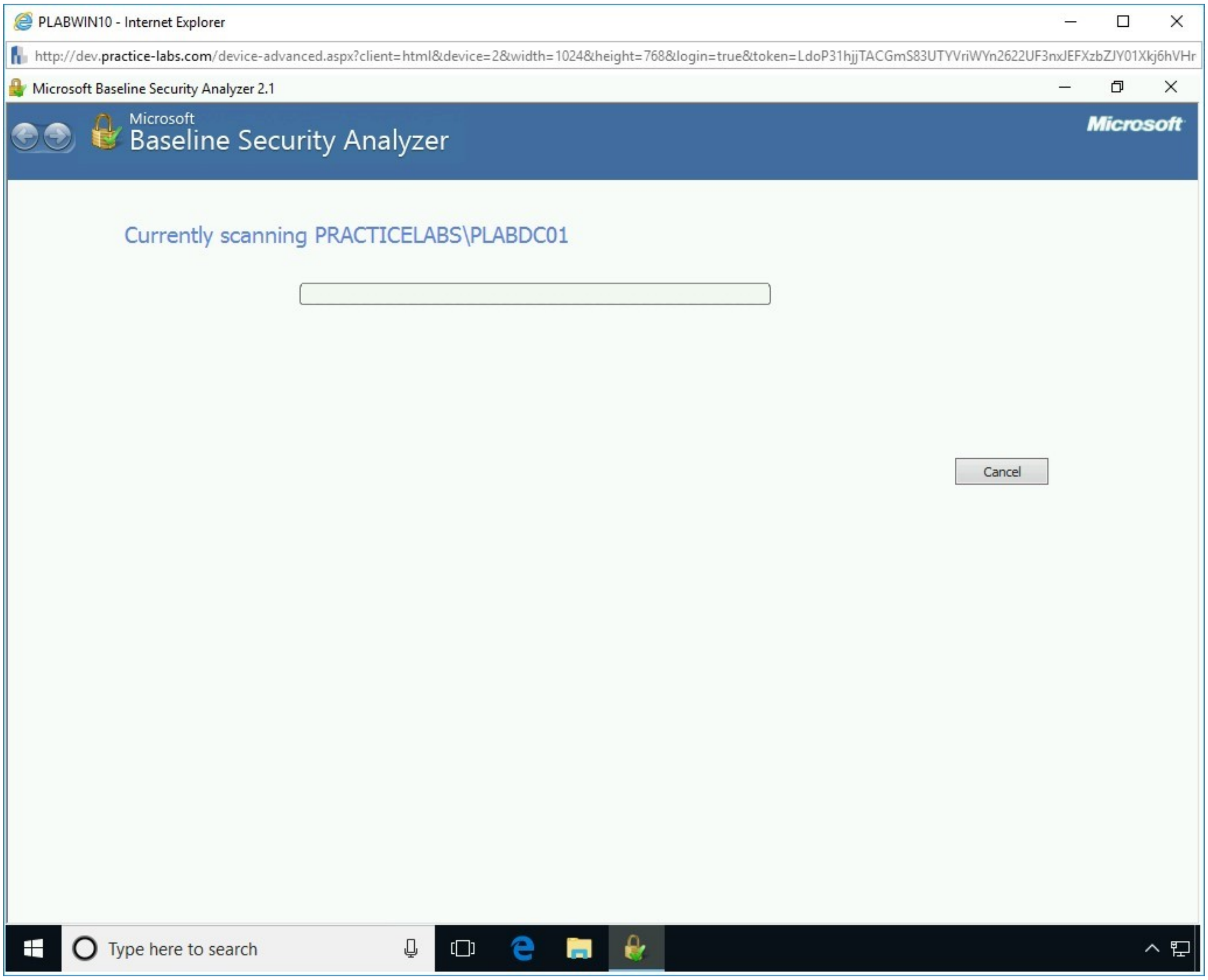
Learn more about Scanning Options

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.*


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft
Cancel
Type here to search

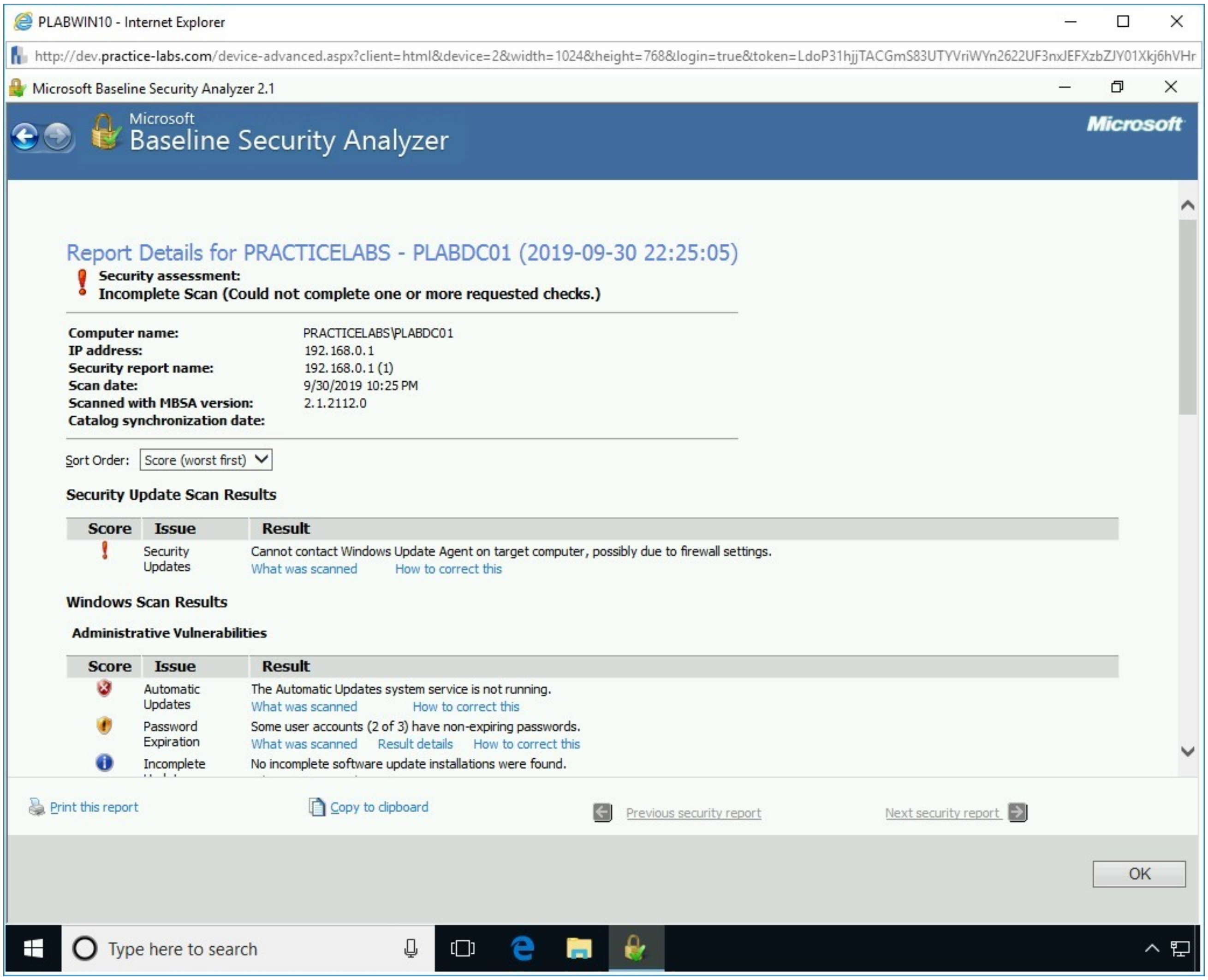
Currently scanning PRACTICELABS\PLABDC01

Figure 2.23 Screenshot of PLABWIN10: Showing the scan progress.

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.*


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft

Report Details for PRACTICELABS - PLABDC01 (2019-09-30 22:25:05)

! Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

Computer name:	PRACTICELABS\PLABDC01
IP address:	192.168.0.1
Security report name:	192.168.0.1 (1)
Scan date:	9/30/2019 10:25 PM
Scanned with MBSA version:	2.1.2112.0
Catalog synchronization date:	

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. What was scanned How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
☒	Automatic Updates	The Automatic Updates system service is not running. What was scanned How to correct this
!	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. What was scanned Result details How to correct this
ⓘ	Incomplete	No incomplete software update installations were found.

Figure 2.24 Screenshot of PLABWIN10: Showing the MBSA scan report.

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

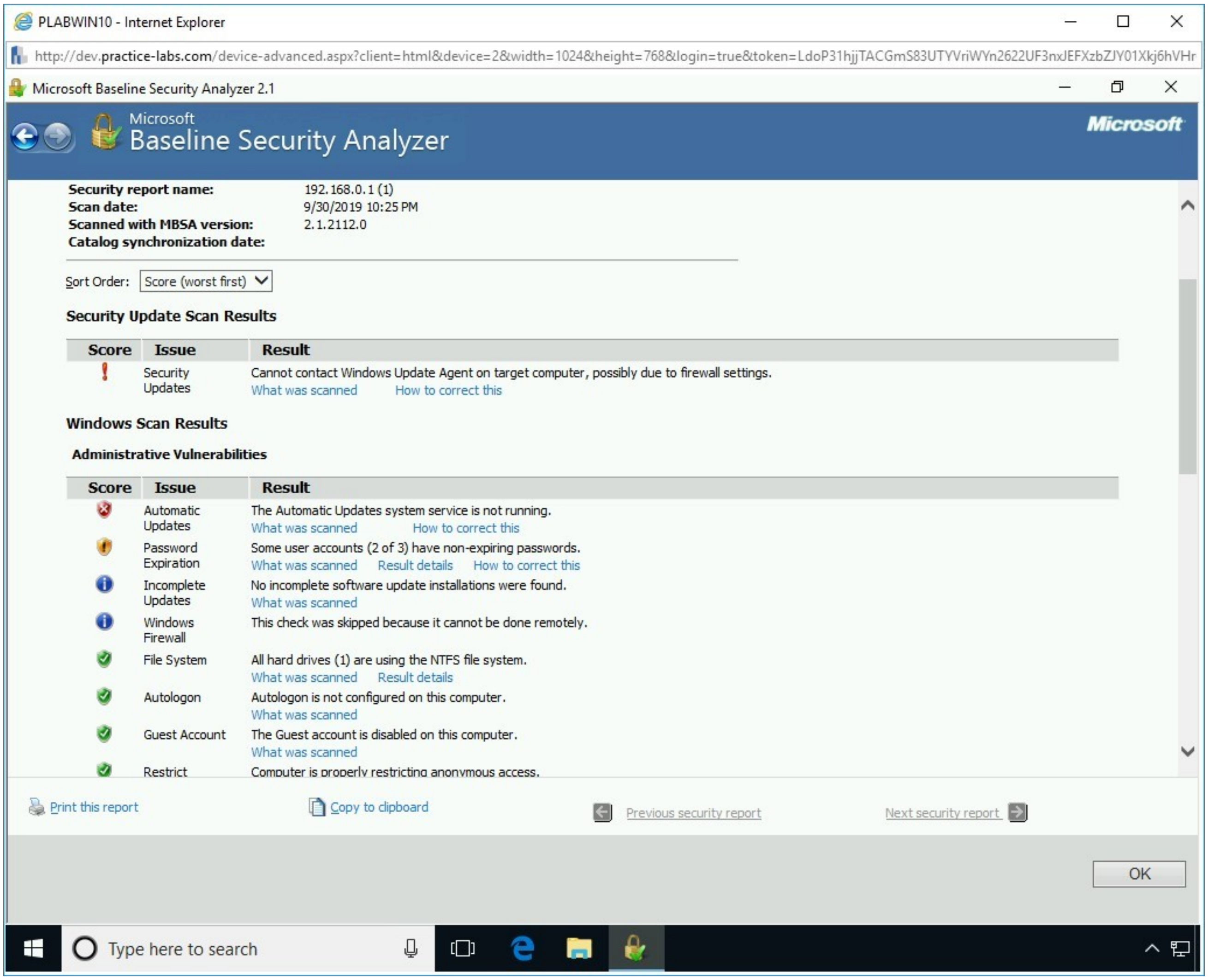
computer.

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.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft
Print this report
Copy to clipboard
Previous security report
Next security report
OK
Type here to search

Security report name: 192.168.0.1 (1)
Scan date: 9/30/2019 10:25 PM
Scanned with MBSA version: 2.1.2112.0
Catalog synchronization date:

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
❗	Security Updates	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. What was scanned How to correct this

Windows Scan Results

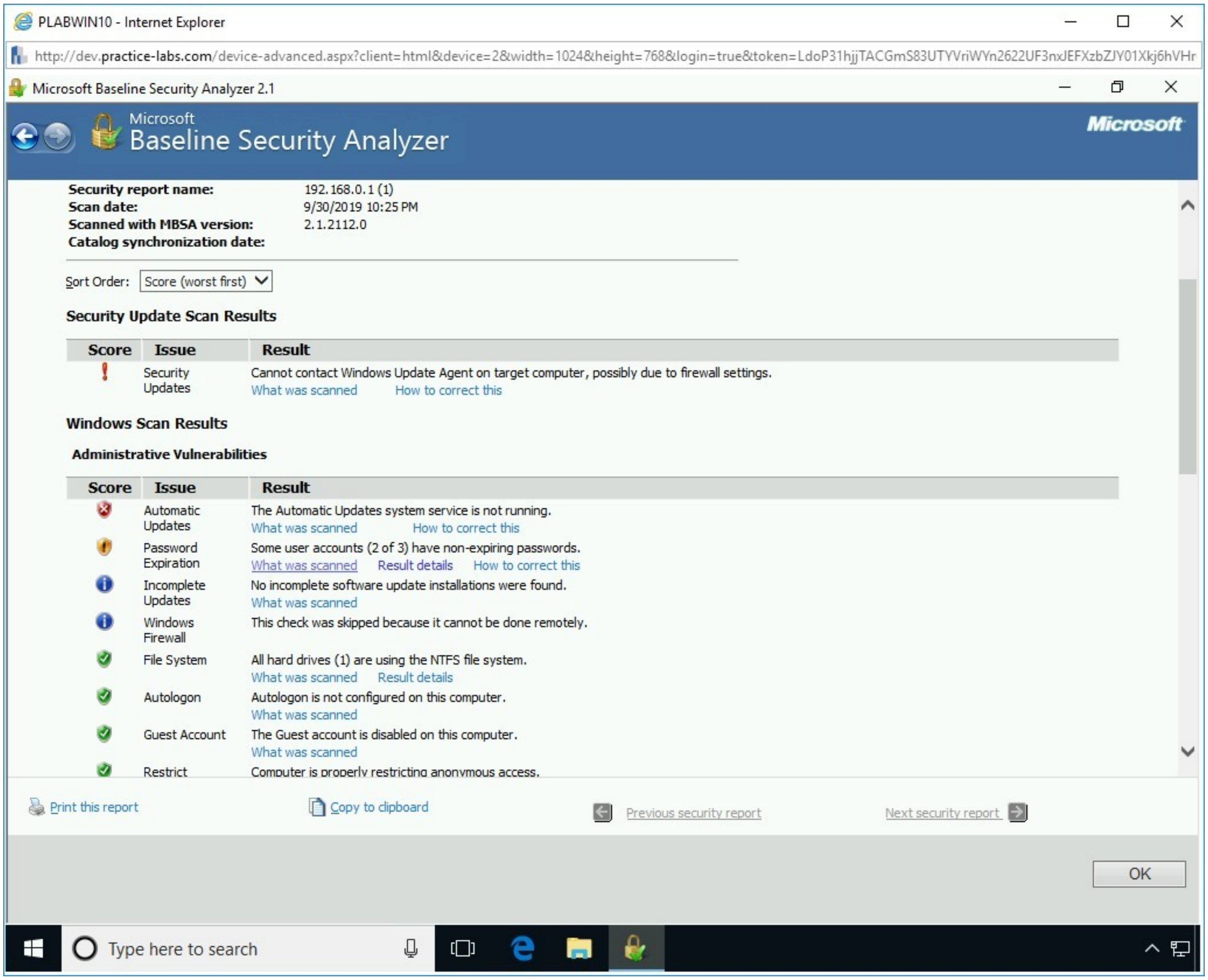
Administrative Vulnerabilities

Score	Issue	Result
✖	Automatic Updates	The Automatic Updates system service is not running. What was scanned How to correct this
⚠	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. What was scanned Result details How to correct this
ℹ	Incomplete Updates	No incomplete software update installations were found. What was scanned
ℹ	Windows Firewall	This check was skipped because it cannot be done remotely.
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict	Computer is properly restricting anonymous access.

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**".


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft

Security report name: 192.168.0.1 (1)
Scan date: 9/30/2019 10:25 PM
Scanned with MBSA version: 2.1.2112.0
Catalog synchronization date:

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. What was scanned How to correct this

Windows Scan Results

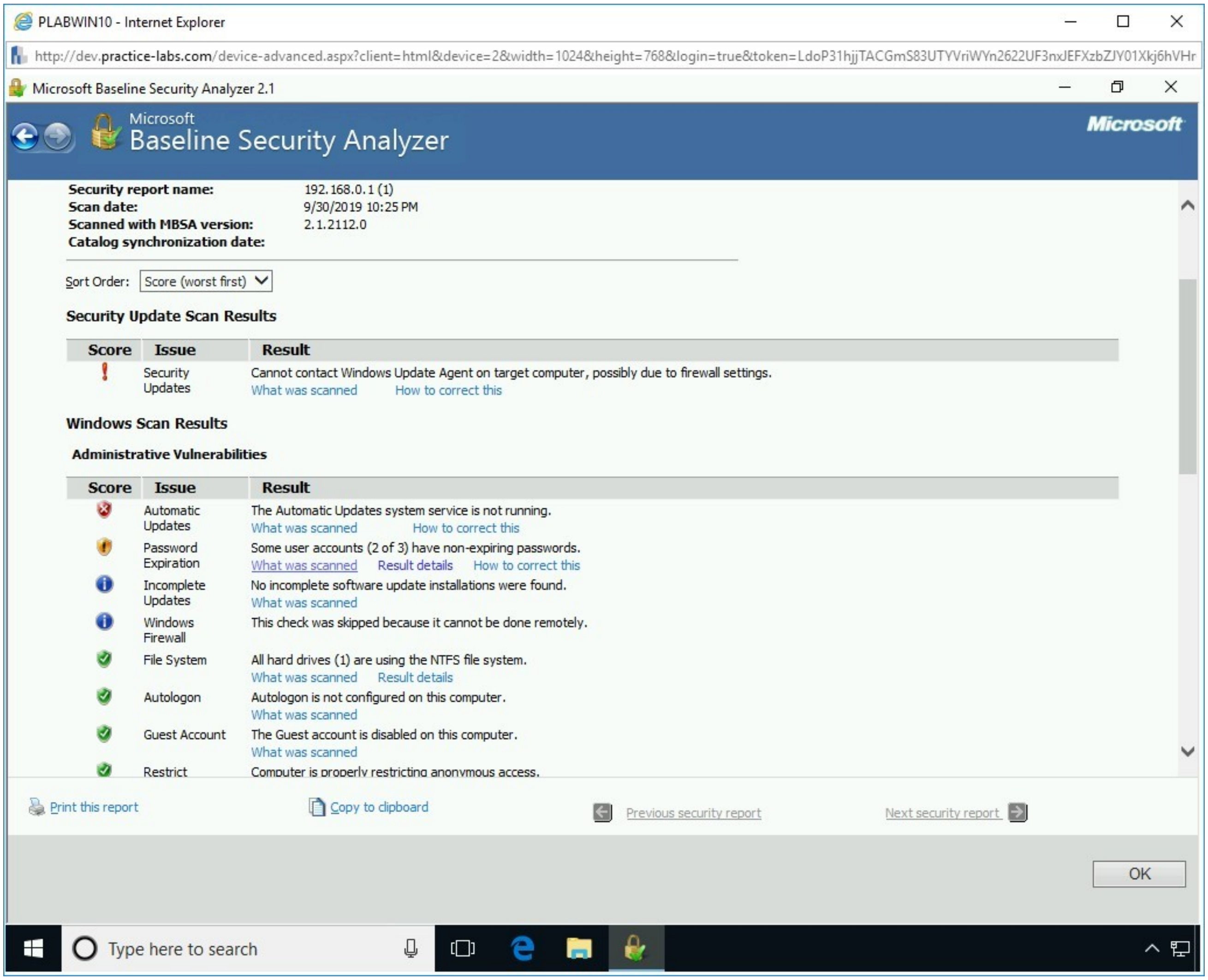
Administrative Vulnerabilities

Score	Issue	Result
☒	Automatic Updates	The Automatic Updates system service is not running. What was scanned How to correct this
!	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. What was scanned Result details How to correct this
i	Incomplete Updates	No incomplete software update installations were found. What was scanned
i	Windows Firewall	This check was skipped because it cannot be done remotely.
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict	Computer is properly restricting anonymous access.

Figure 2.26 Screenshot of PLABWIN10: Showing the MBSA scan report.

Step 3

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


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft

Security report name: 192.168.0.1 (1)
Scan date: 9/30/2019 10:25 PM
Scanned with MBSA version: 2.1.2112.0
Catalog synchronization date:

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. What was scanned How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
☒	Automatic Updates	The Automatic Updates system service is not running. What was scanned How to correct this
!	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. What was scanned Result details How to correct this
i	Incomplete Updates	No incomplete software update installations were found. What was scanned
i	Windows Firewall	This check was skipped because it cannot be done remotely.
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict	Computer is properly restricting anonymous access.

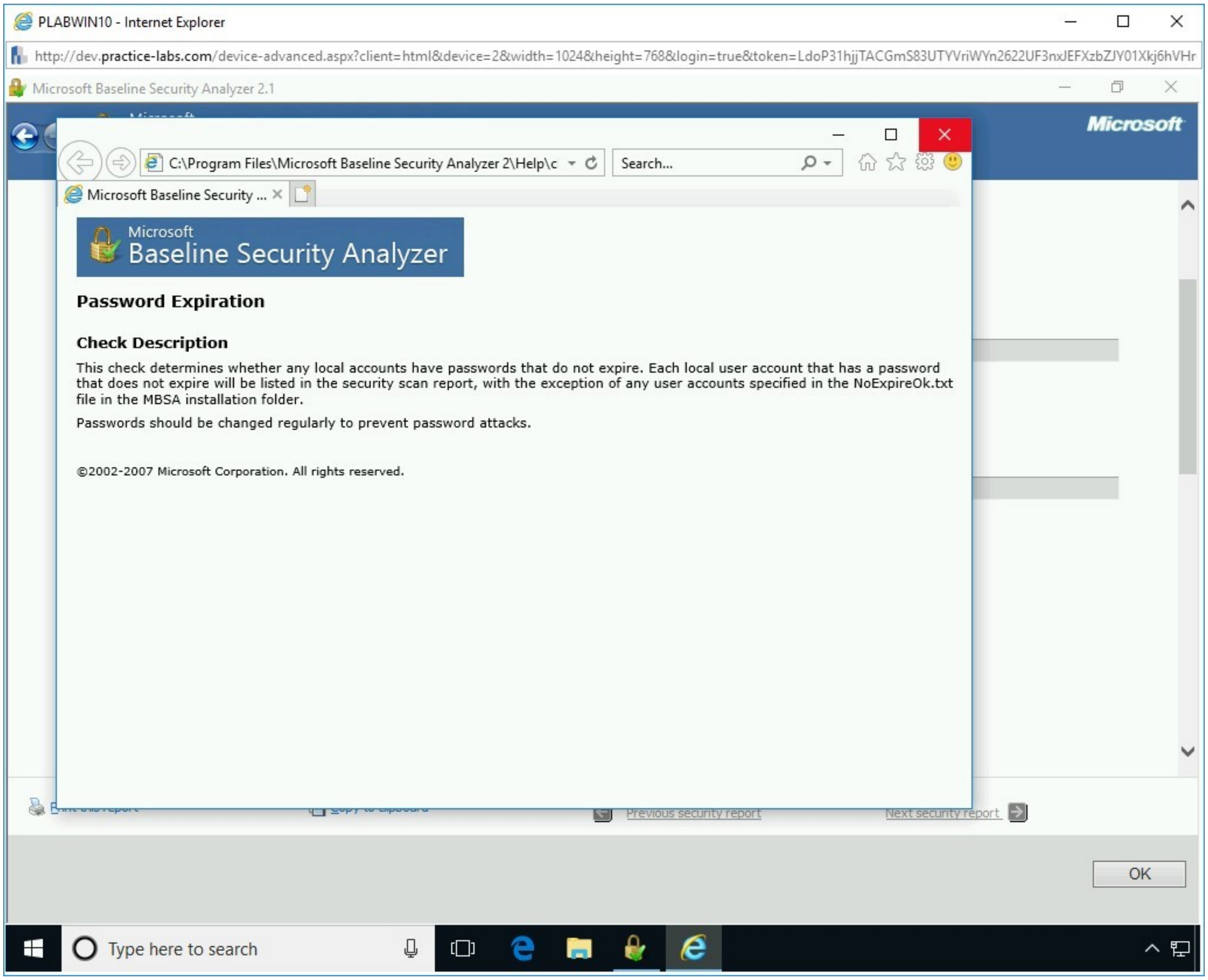
Figure 2.27 Screenshot of PLABWIN10: Clicking the What was scanned option for Password Expiration.

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.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
C:\Program Files\Microsoft Baseline Security Analyzer 2\Help\c
Search...
Microsoft Baseline Security ...
Microsoft
Baseline Security Analyzer
Previous security report
Next security report
OK
Type here to search

Password Expiration

Check Description

This check determines whether any local accounts have passwords that do not expire. Each local user account that has a password that does not expire will be listed in the security scan report, with the exception of any user accounts specified in the NoExpireOk.txt file in the MBSA installation folder.

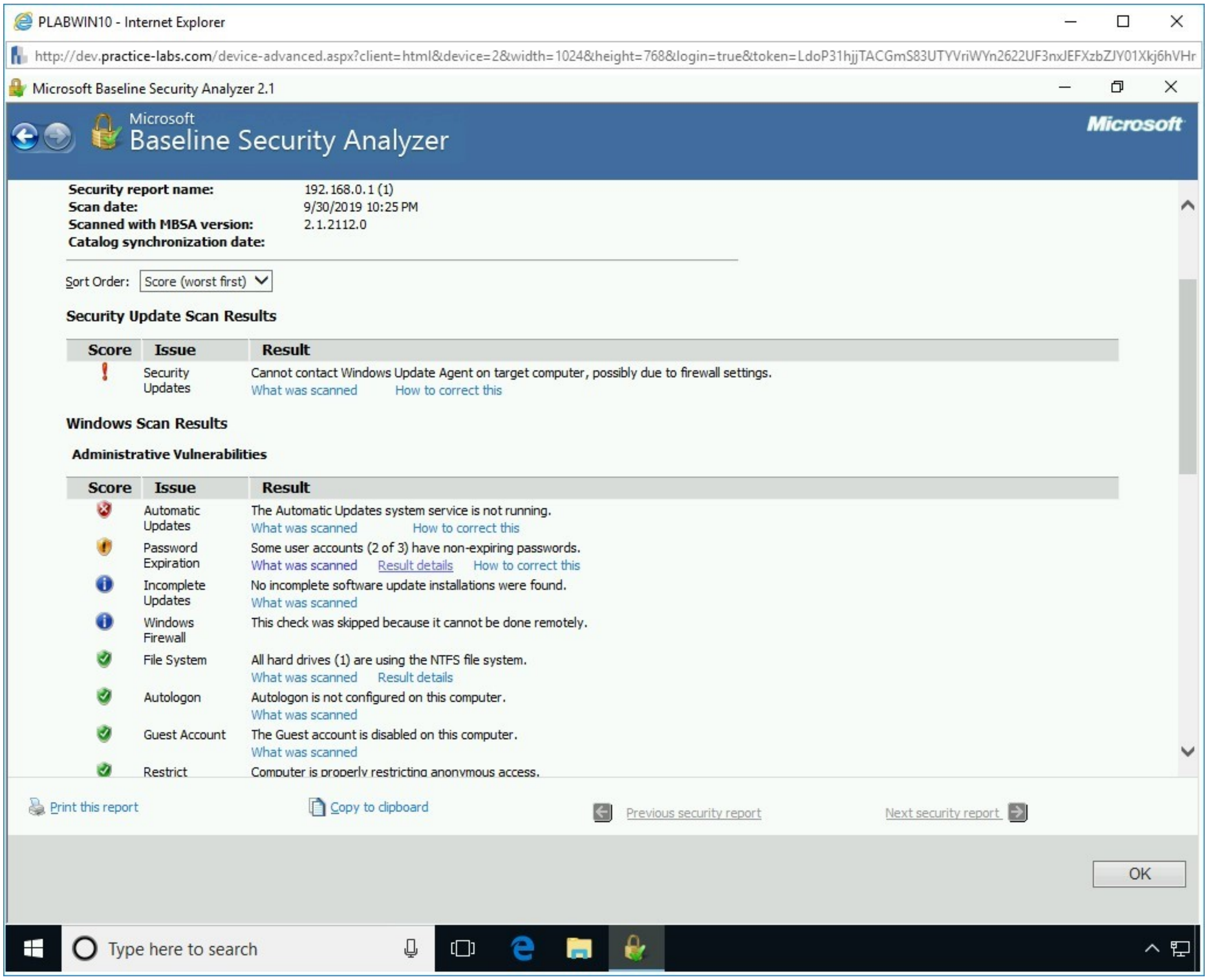
Passwords should be changed regularly to prevent password attacks.

©2002-2007 Microsoft Corporation. All rights reserved.

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

Step 5

Click the **Result details** link.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft
Print this report
Copy to clipboard
Previous security report
Next security report
OK
Type here to search

Security report name: 192.168.0.1 (1)
Scan date: 9/30/2019 10:25 PM
Scanned with MBSA version: 2.1.2112.0
Catalog synchronization date:

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
❗	Security Updates	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. What was scanned How to correct this

Windows Scan Results

Administrative Vulnerabilities

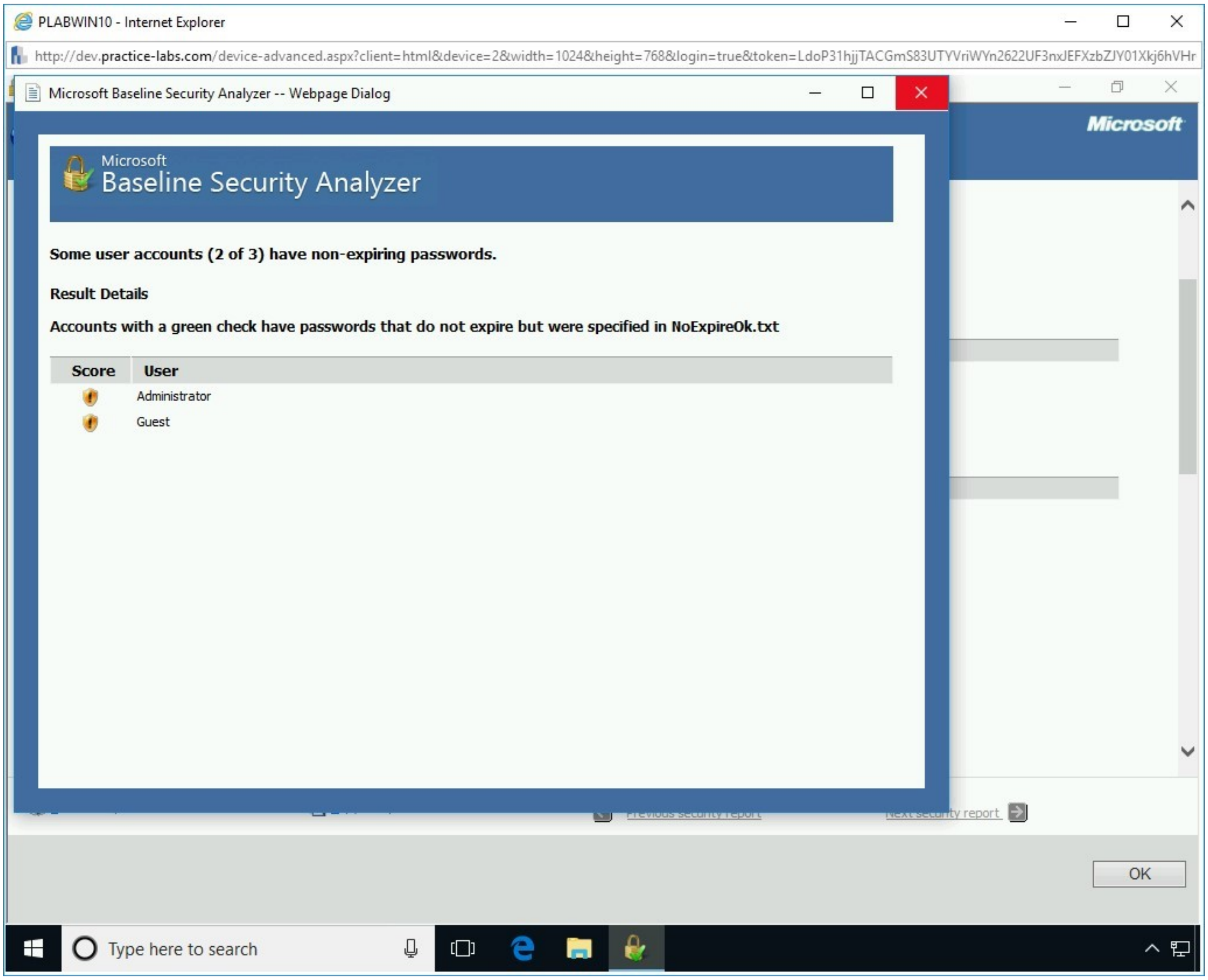
Score	Issue	Result
✖	Automatic Updates	The Automatic Updates system service is not running. What was scanned How to correct this
⚠	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. What was scanned Result details How to correct this
ℹ	Incomplete Updates	No incomplete software update installations were found. What was scanned
ℹ	Windows Firewall	This check was skipped because it cannot be done remotely.
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict	Computer is properly restricting anonymous access.

Figure 2.29 PLABWIN10: Clicking the Result details of Password Expiration.

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.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer -- Webpage Dialog
Microsoft
Microsoft
Baseline Security Analyzer
Previous security report
Next security report
OK
Type here to search

Some user accounts (2 of 3) have non-expiring passwords.

Result Details

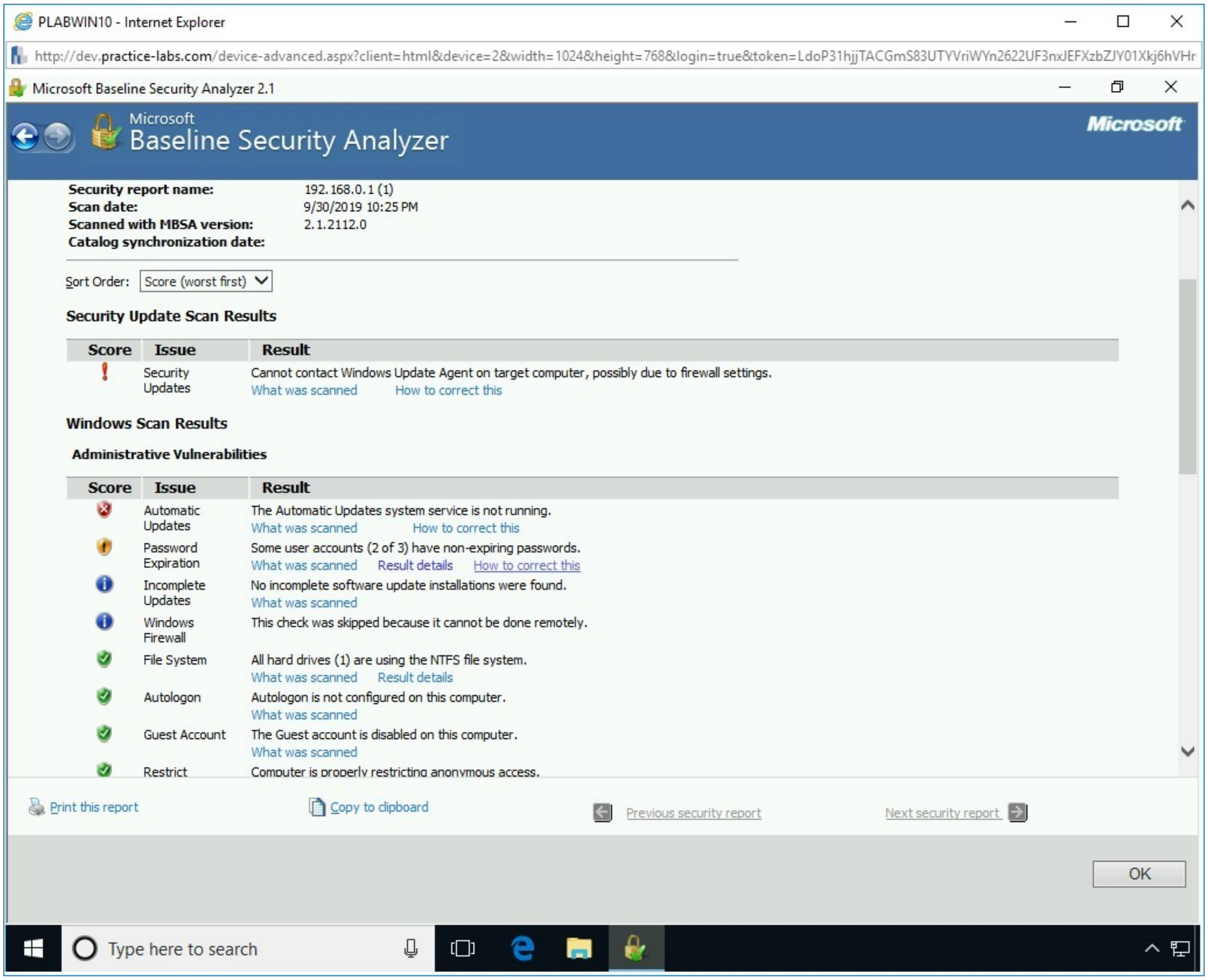
Accounts with a green check have passwords that do not expire but were specified in NoExpireOk.txt

Score	User
!	Administrator
!	Guest

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.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft

Security report name: 192.168.0.1 (1)
Scan date: 9/30/2019 10:25 PM
Scanned with MBSA version: 2.1.2112.0
Catalog synchronization date:

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. What was scanned How to correct this

Windows Scan Results

Administrative Vulnerabilities

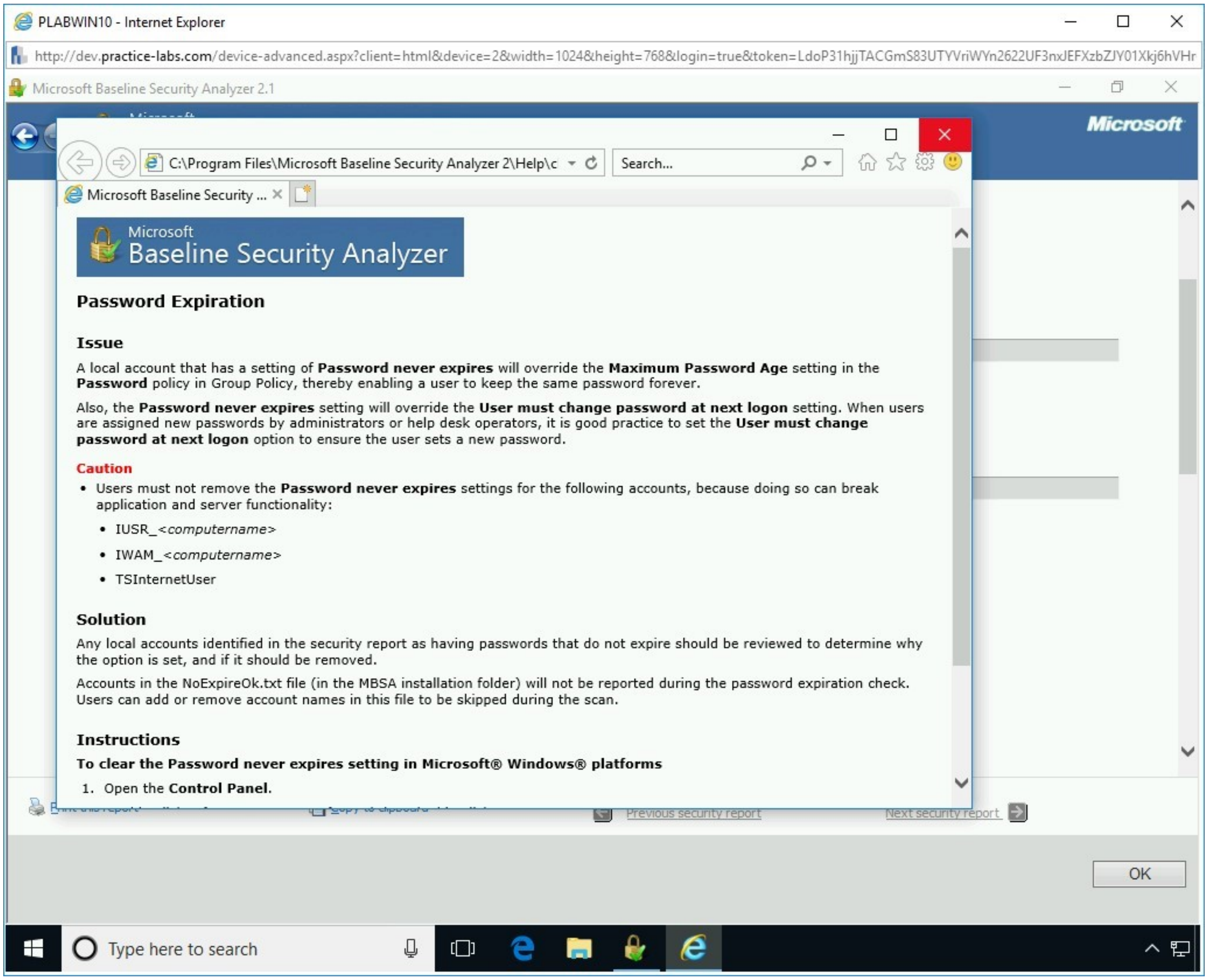
Score	Issue	Result
☒	Automatic Updates	The Automatic Updates system service is not running. What was scanned How to correct this
!	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. What was scanned Result details How to correct this
i	Incomplete Updates	No incomplete software update installations were found. What was scanned
i	Windows Firewall	This check was skipped because it cannot be done remotely.
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict	Computer is properly restricting anonymous access.

Figure 2.31 Screenshot of PLABWIN10: Clicking 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.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
C:\Program Files\Microsoft Baseline Security Analyzer 2\Help\c
Search...
Microsoft Baseline Security ...
Previous security report
Next security report
OK
Type here to search

Microsoft
Baseline Security Analyzer

Password Expiration

Issue

A local account that has a setting of **Password never expires** will override the **Maximum Password Age** setting in the **Password** policy in Group Policy, thereby enabling a user to keep the same password forever.

Also, the **Password never expires** setting will override the **User must change password at next logon** setting. When users are assigned new passwords by administrators or help desk operators, it is good practice to set the **User must change password at next logon** option to ensure the user sets a new password.

Caution

- Users must not remove the **Password never expires** settings for the following accounts, because doing so can break application and server functionality:
  - IUSR_*<computername>*
  - IWAM_*<computername>*
  - TSInternetUser

Solution

Any local accounts identified in the security report as having passwords that do not expire should be reviewed to determine why the option is set, and if it should be removed.

Accounts in the NoExpireOk.txt file (in the MBSA installation folder) will not be reported during the password expiration check. Users can add or remove account names in this file to be skipped during the scan.

Instructions

To clear the Password never expires setting in Microsoft® Windows® platforms

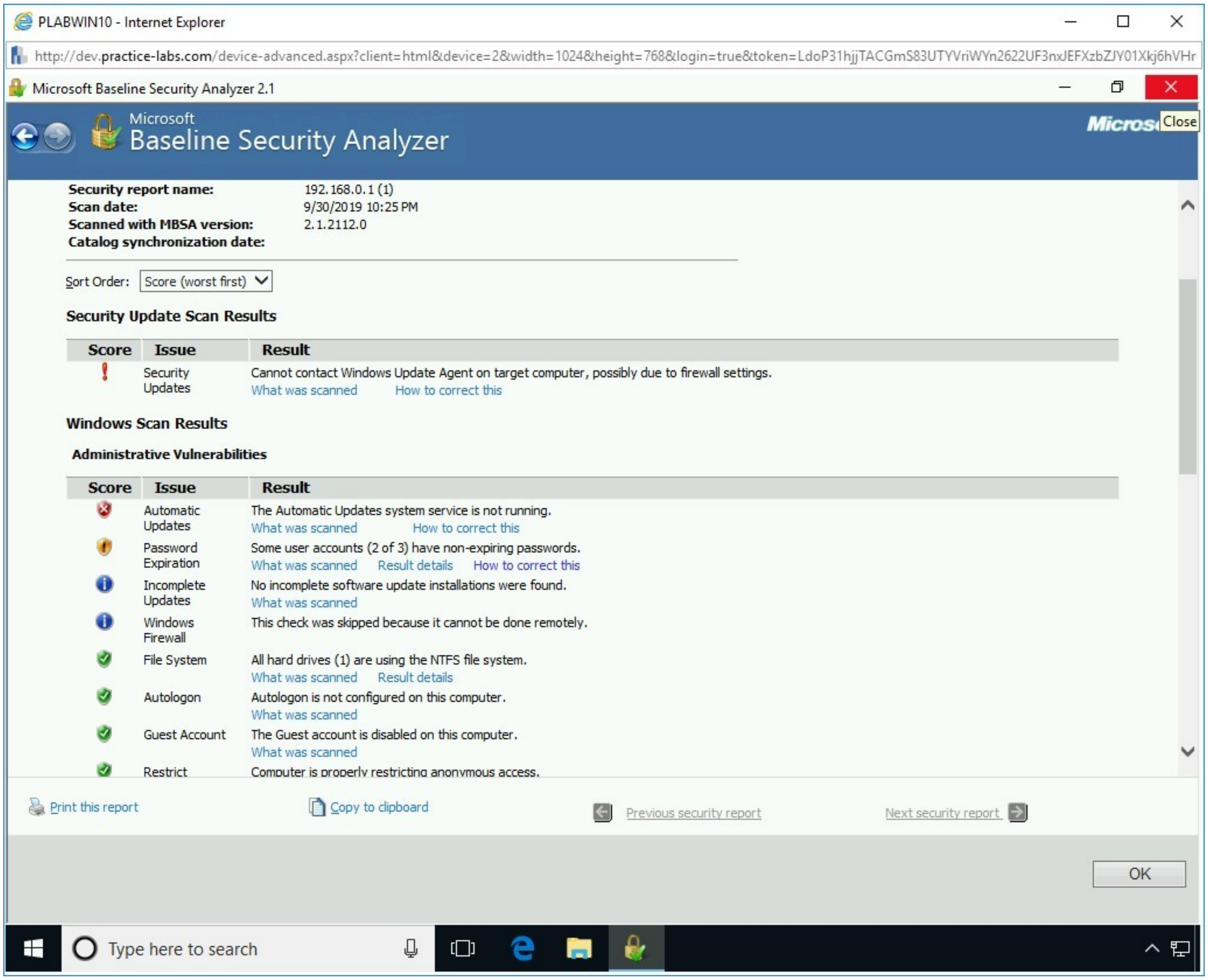
1. Open the **Control Panel**.

Figure 2.32 Screenshot of PLABWIN10: Displaying the Password Expiration remediation page.

Close the **Password Expiration** window.

Step 9

Close the **MBSA** window.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Close

Security report name:	192.168.0.1 (1)
Scan date:	9/30/2019 10:25 PM
Scanned with MBSA version:	2.1.2112.0
Catalog synchronization date:	

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. What was scanned How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✗	Automatic Updates	The Automatic Updates system service is not running. What was scanned How to correct this
!	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. What was scanned Result details How to correct this
i	Incomplete Updates	No incomplete software update installations were found. What was scanned
i	Windows Firewall	This check was skipped because it cannot be done remotely.
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict	Computer is properly restricting anonymous access.

Figure 2.33 Screenshot of PLABWIN10: Closing 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

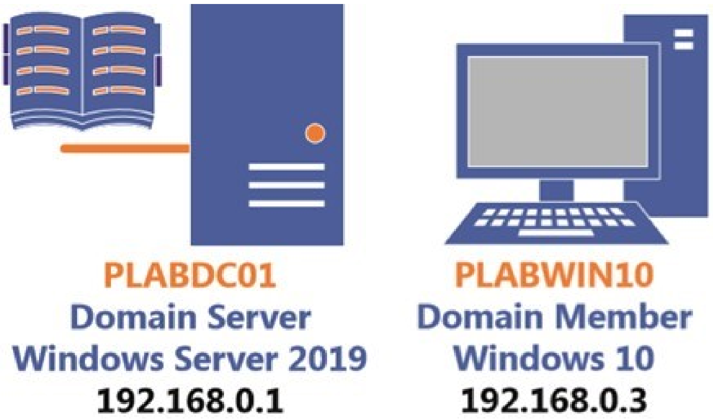
After completing this exercise, you will be able to:

- 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**

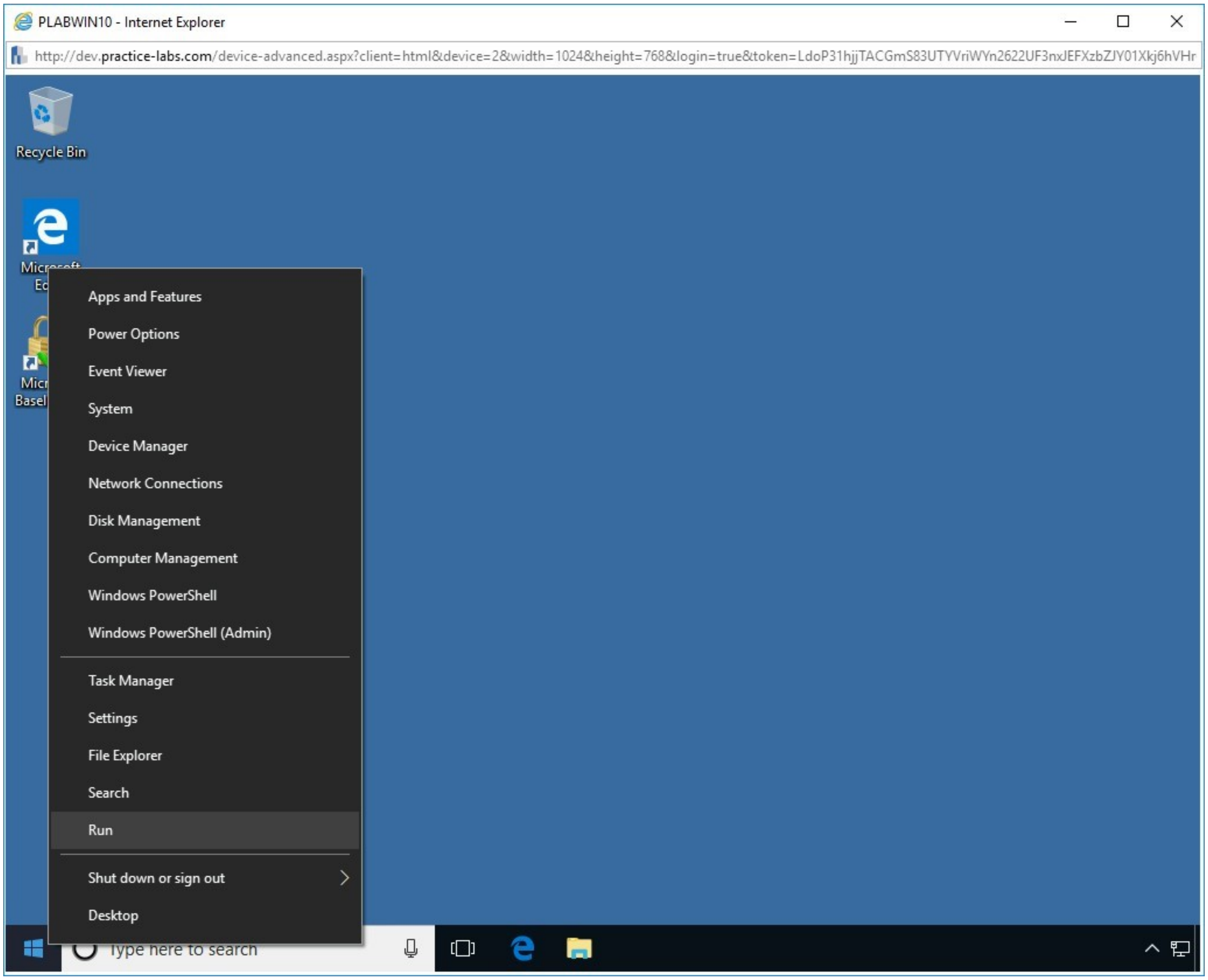


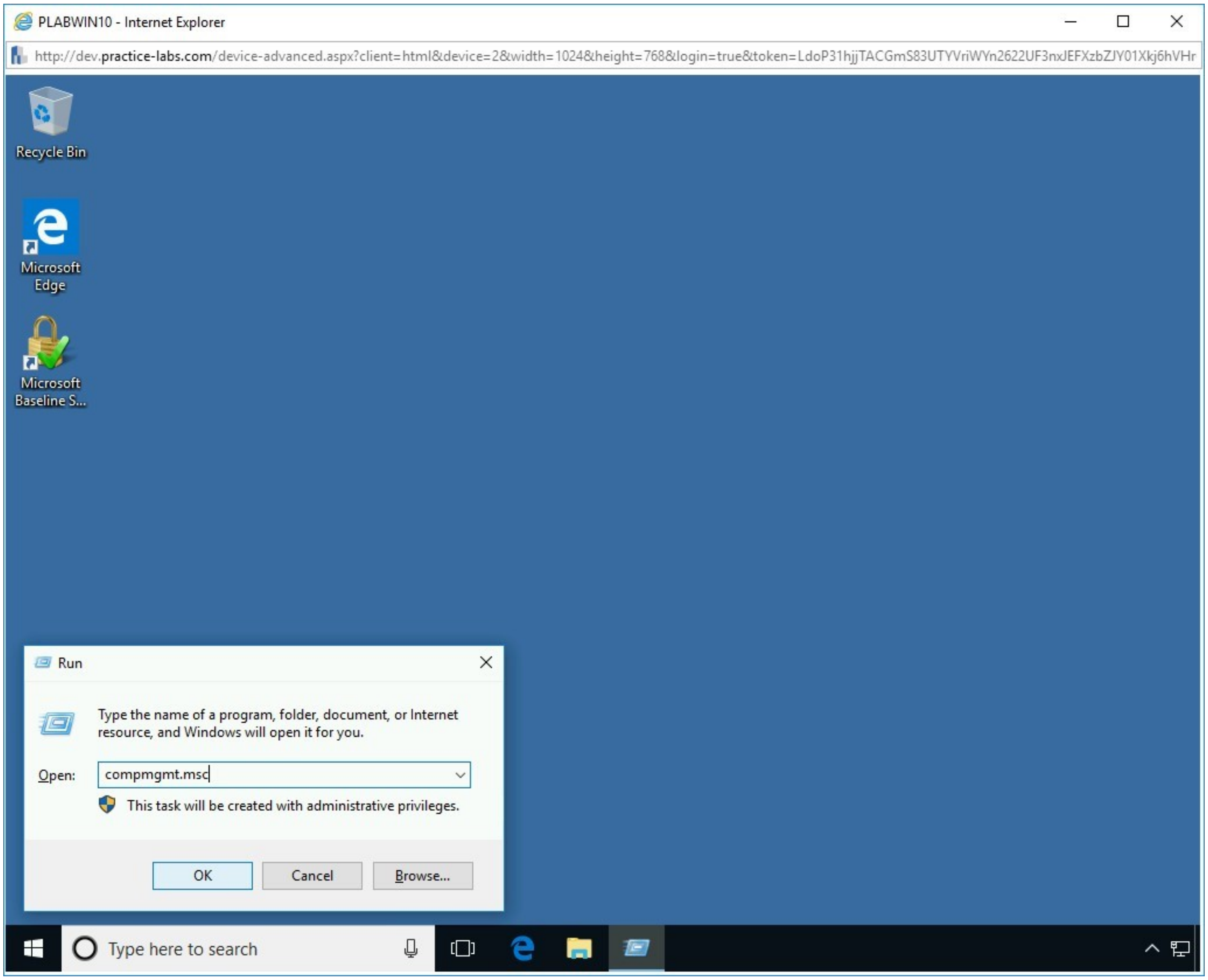
Figure 3.1 Screenshot of PLABWIN10: Selecting the Run option from the Windows charm context menu.

Step 2

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

```
compmgmt.msc
```

Click **OK**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Recycle Bin
Microsoft Edge
Microsoft Baseline S...
Run
OK
Cancel
Browse...
Type here to search

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

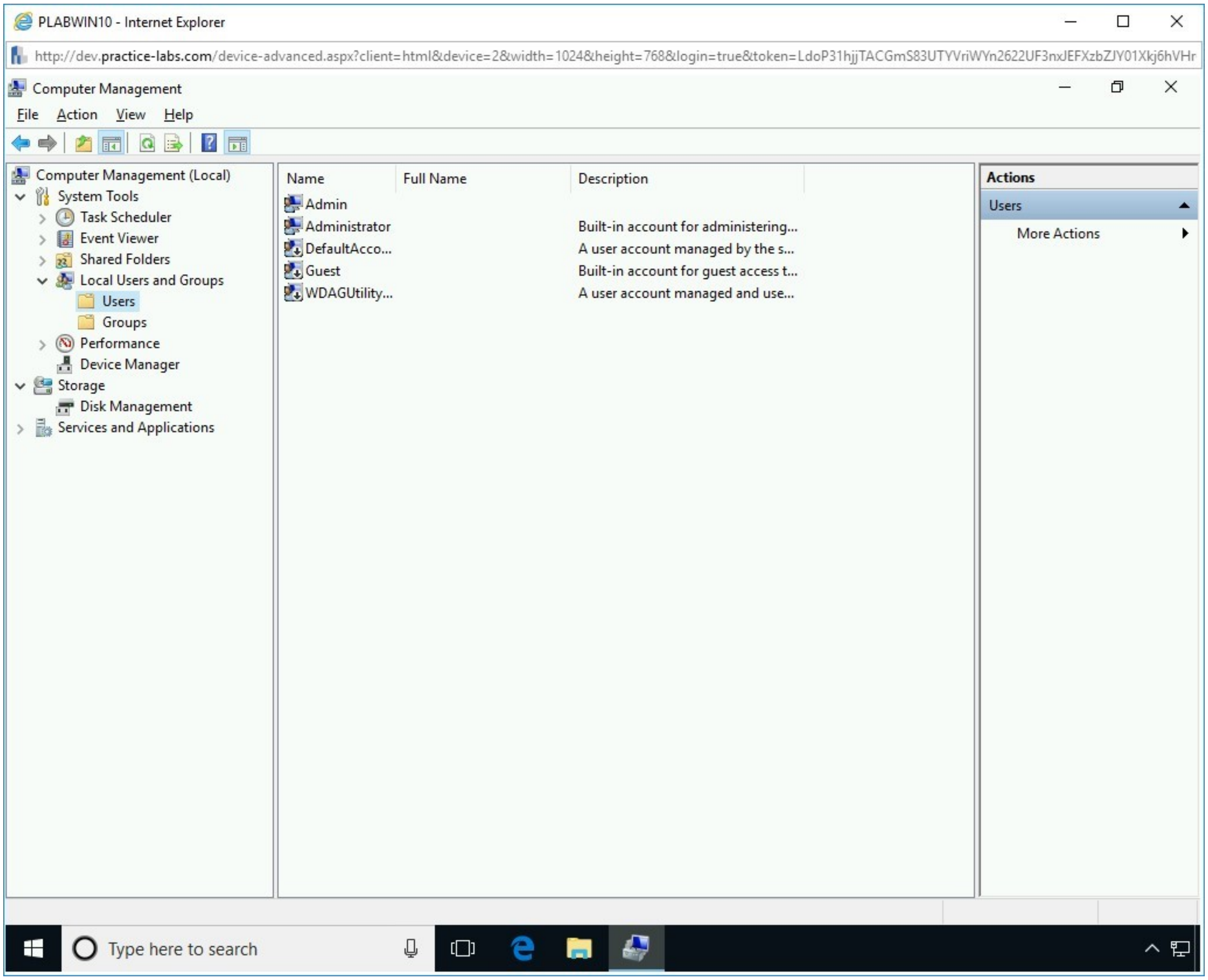
Open: compmgmt.msc

This task will be created with administrative privileges.

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**.

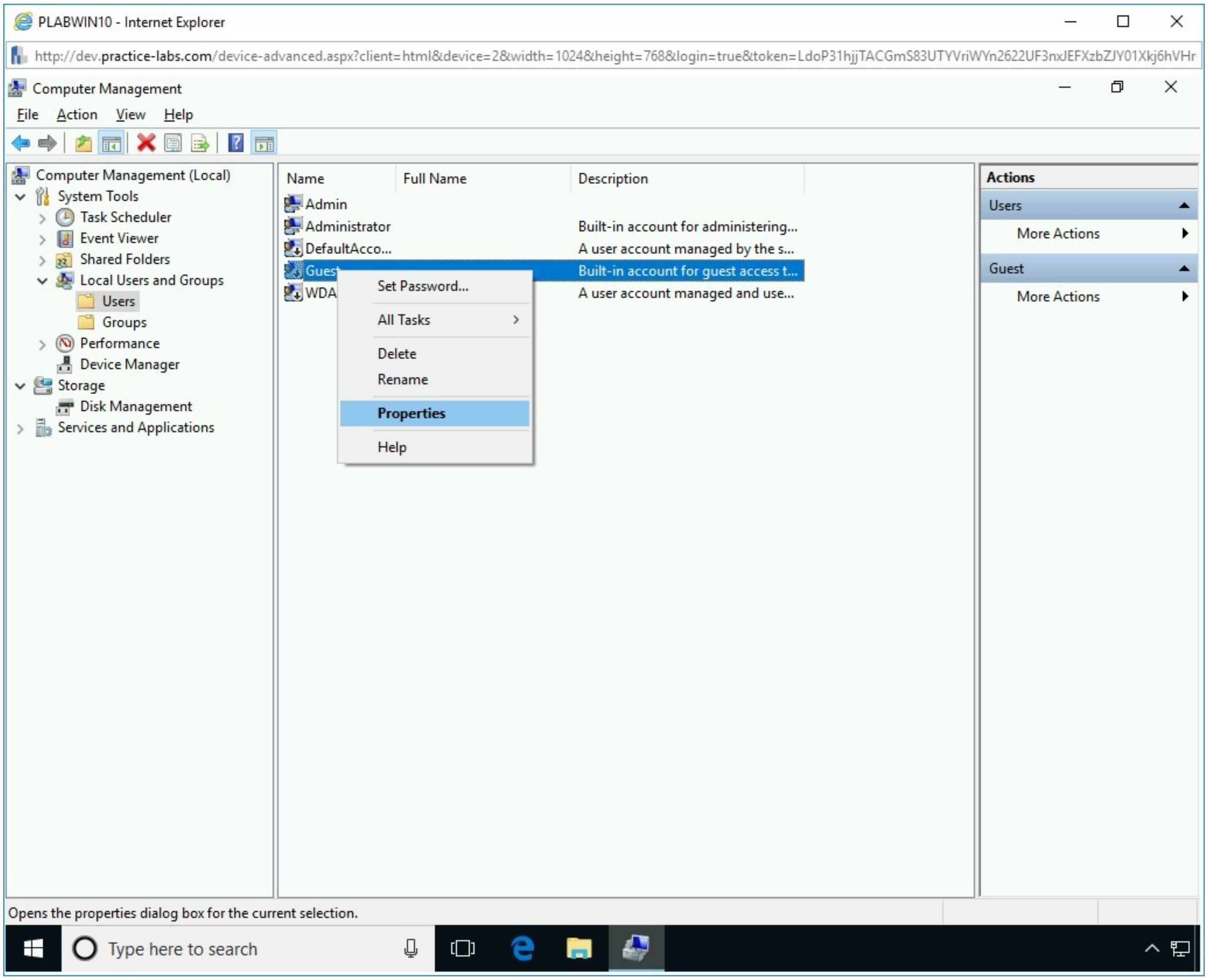

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Computer Management
File
Action
View
Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Actions
Users
More Actions
Type here to search

Name	Full Name	Description
Admin		
Administrator		Built-in account for administering...
DefaultAcco...		A user account managed by the s...
Guest		Built-in account for guest access t...
WDAGUtility...		A user account managed and use...

Figure 3.3 Screenshot of PLABWIN10: Showing the user accounts in the Users node.

Step 4

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



Name	Full Name	Description
Admin		
Administrator		Built-in account for administering...
DefaultAcco...		A user account managed by the s...
Guest		Built-in account for guest access t...
WDA		A user account managed and use...

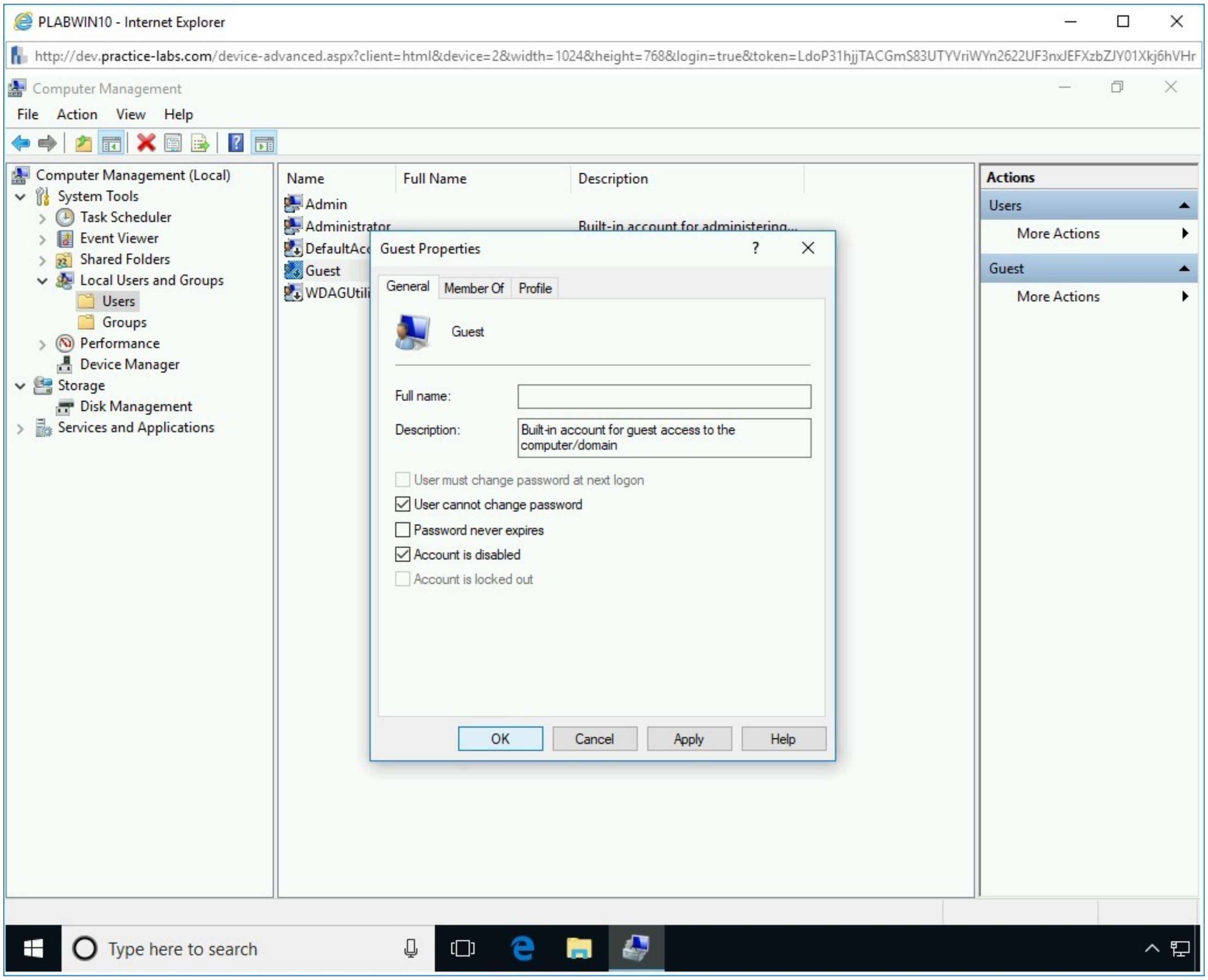
Opens the properties dialog box for the current selection.

Figure 3.4 Screenshot of PLABWIN10: Right-clicking the Guest account and selecting Properties from the context menu.

Step 5

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

Click **OK**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Computer Management
File
Action
View
Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Actions
Users
More Actions
Guest
More Actions
Type here to search

Name	Full Name	Description
Admin		
Administrator		Built-in account for administering...
DefaultAcc		
Guest		
WDAGUtili		

Guest Properties

Guest

Full name:

Description: Built-in account for guest access to the computer/domain

□ User must change password at next logon

☑ User cannot change password

□ Password never expires

☑ Account is disabled

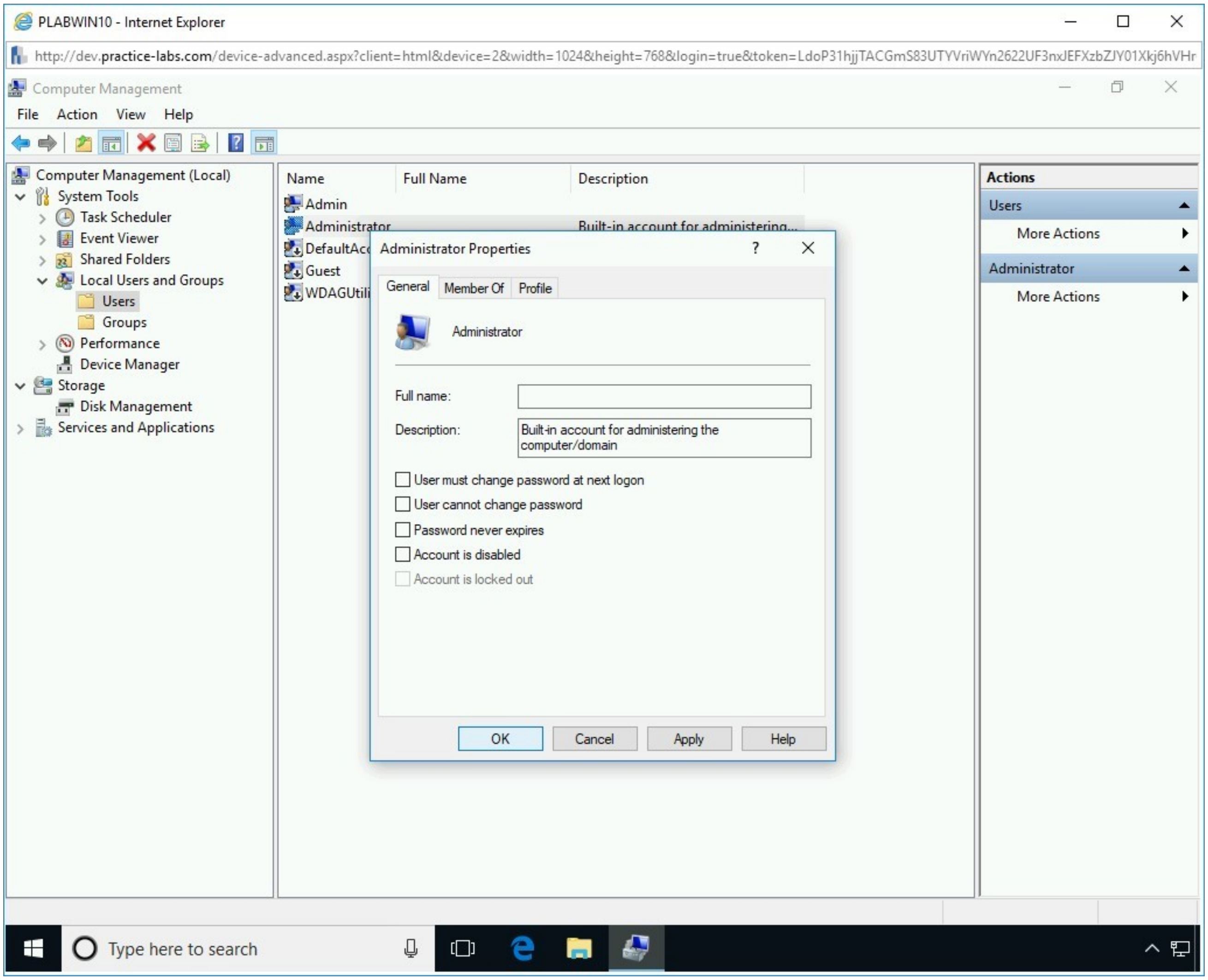
□ Account is locked out

Figure 3.5 Screenshot of PLABWIN10: Showing the Guest Properties dialog box to change the Password Expiration setting.

Step 6

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

Click **OK**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Computer Management
File
Action
View
Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Actions
Users
More Actions
Administrator
More Actions
Type here to search

Name	Full Name	Description
Admin		
Administrator		Built-in account for administering...
DefaultAcc		
Guest		
WDAGUtili		

Administrator Properties

Administrator

Full name:

Description: Built-in account for administering the computer/domain

□ User must change password at next logon

□ User cannot change password

□ Password never expires

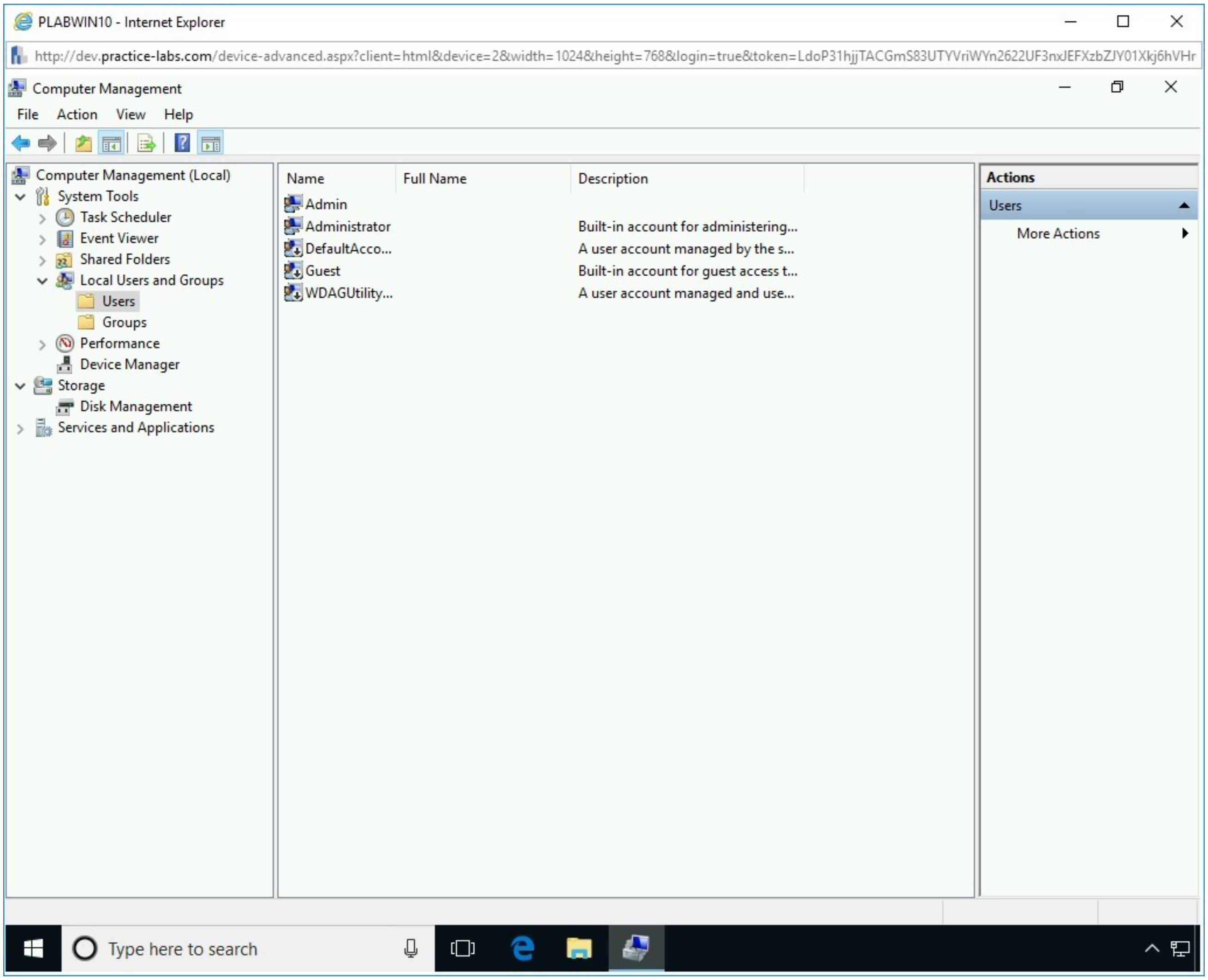
□ Account is disabled

□ Account is locked out

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.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Computer Management
File
Action
View
Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Actions
Users
More Actions
Type here to search

Name	Full Name	Description
Admin		
Administrator		Built-in account for administering...
DefaultAcco...		A user account managed by the s...
Guest		Built-in account for guest access t...
WDAGUtility...		A user account managed and use...

Figure 3.7 Screenshot of PLABWIN10: Closing the Computer Management window.

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

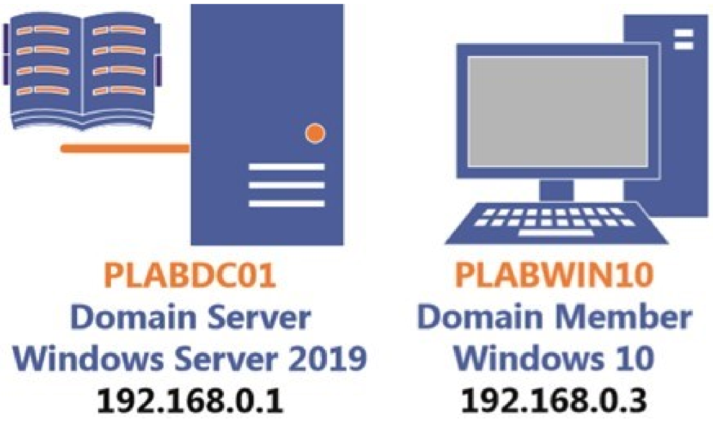
After completing this exercise, you will be able to:

- 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**.

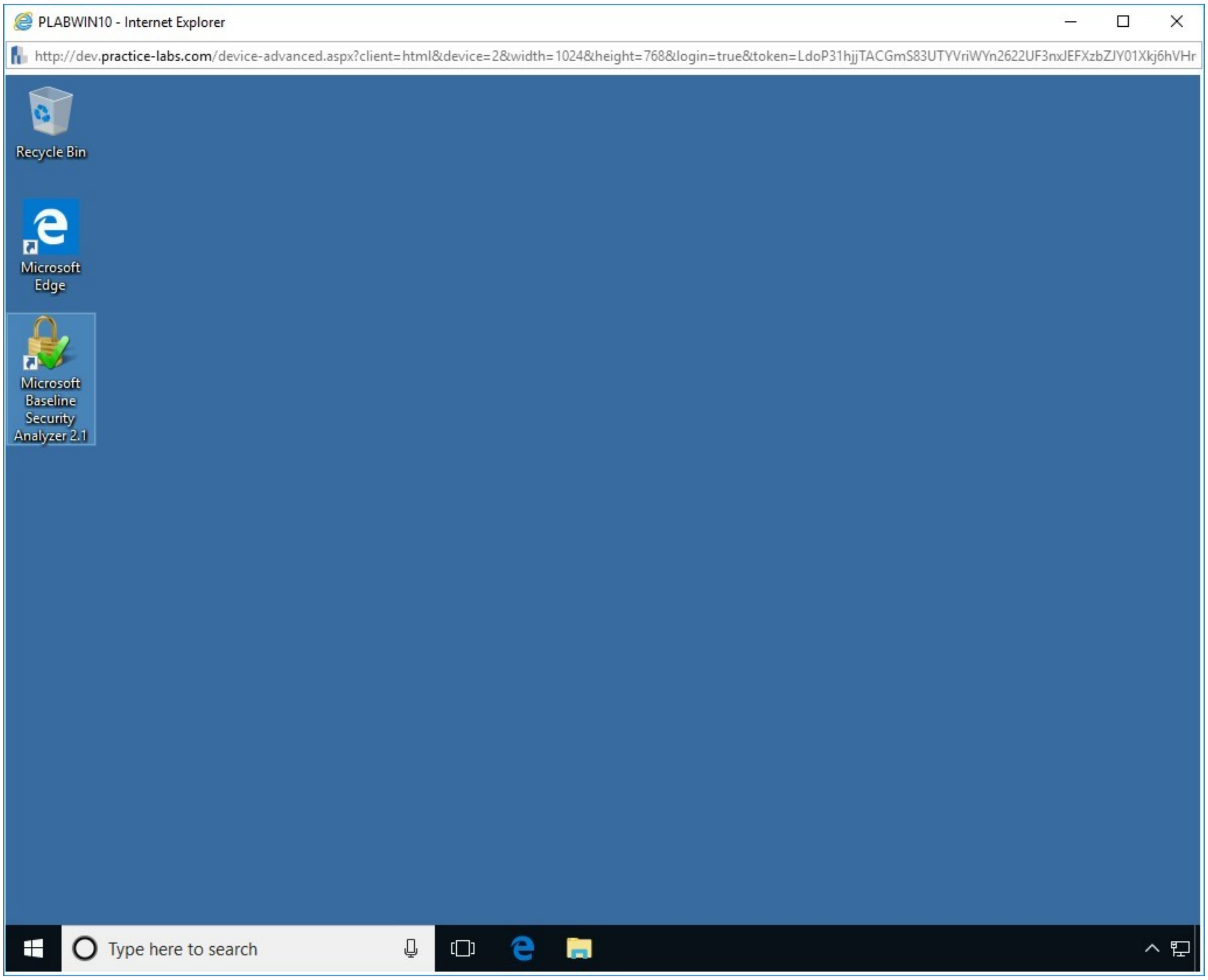
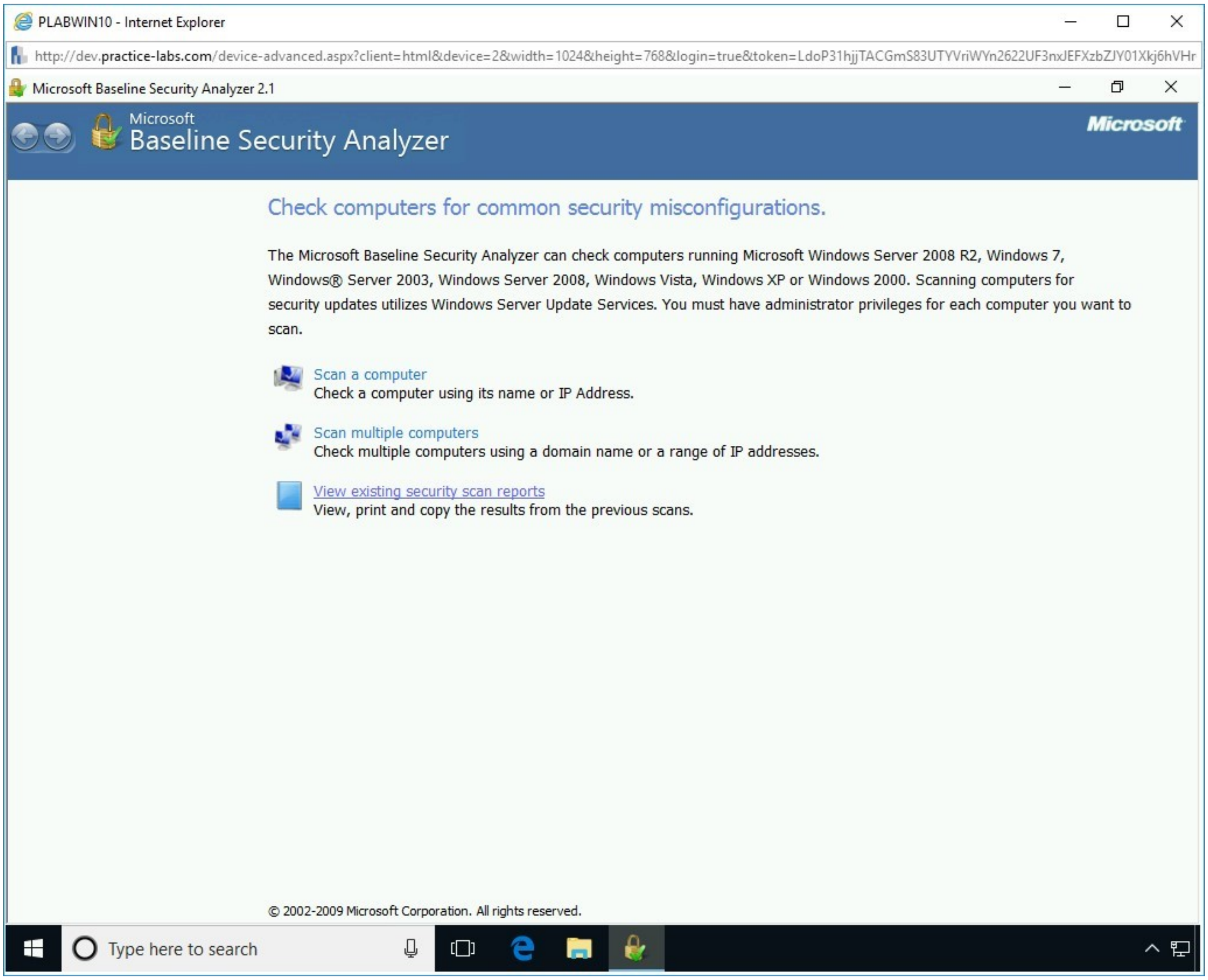

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Recycle Bin
Microsoft Edge
Microsoft Baseline Security Analyzer 2.1
Type here to search

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.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft
Type here to search

Check computers for common security misconfigurations.

The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, Windows XP or Windows 2000. Scanning computers for security updates utilizes Windows Server Update Services. You must have administrator privileges for each computer you want to scan.

Scan a computer
Check a computer using its name or IP Address.

Scan multiple computers
Check multiple computers using a domain name or a range of IP addresses.

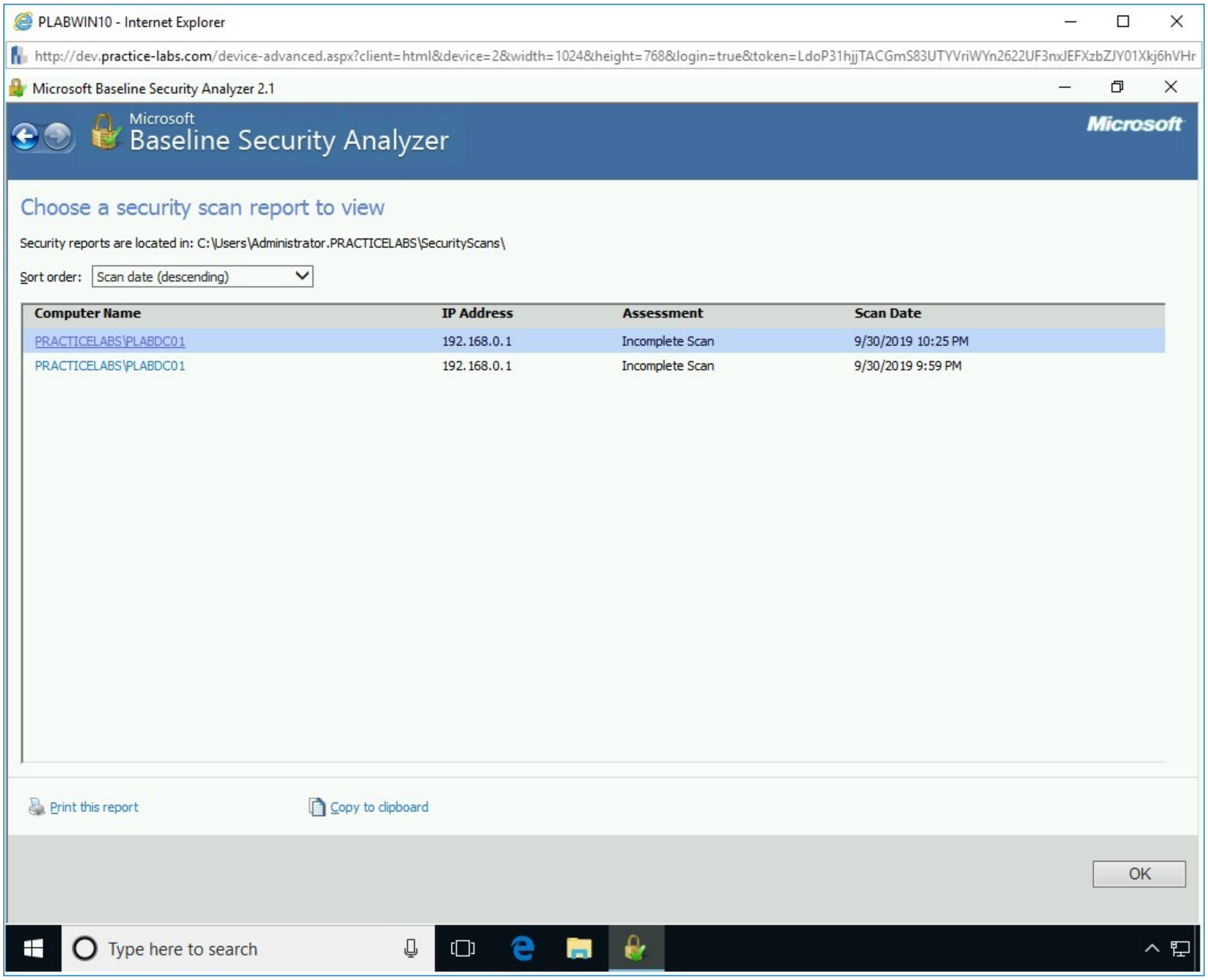
View existing security scan reports
View, print and copy the results from the previous scans.

© 2002-2009 Microsoft Corporation. All rights reserved.

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.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft
Print this report
Copy to clipboard
OK
Type here to search

Choose a security scan report to view

Security reports are located in: C:\Users\Administrator.PRACTICELABS\SecurityScans\

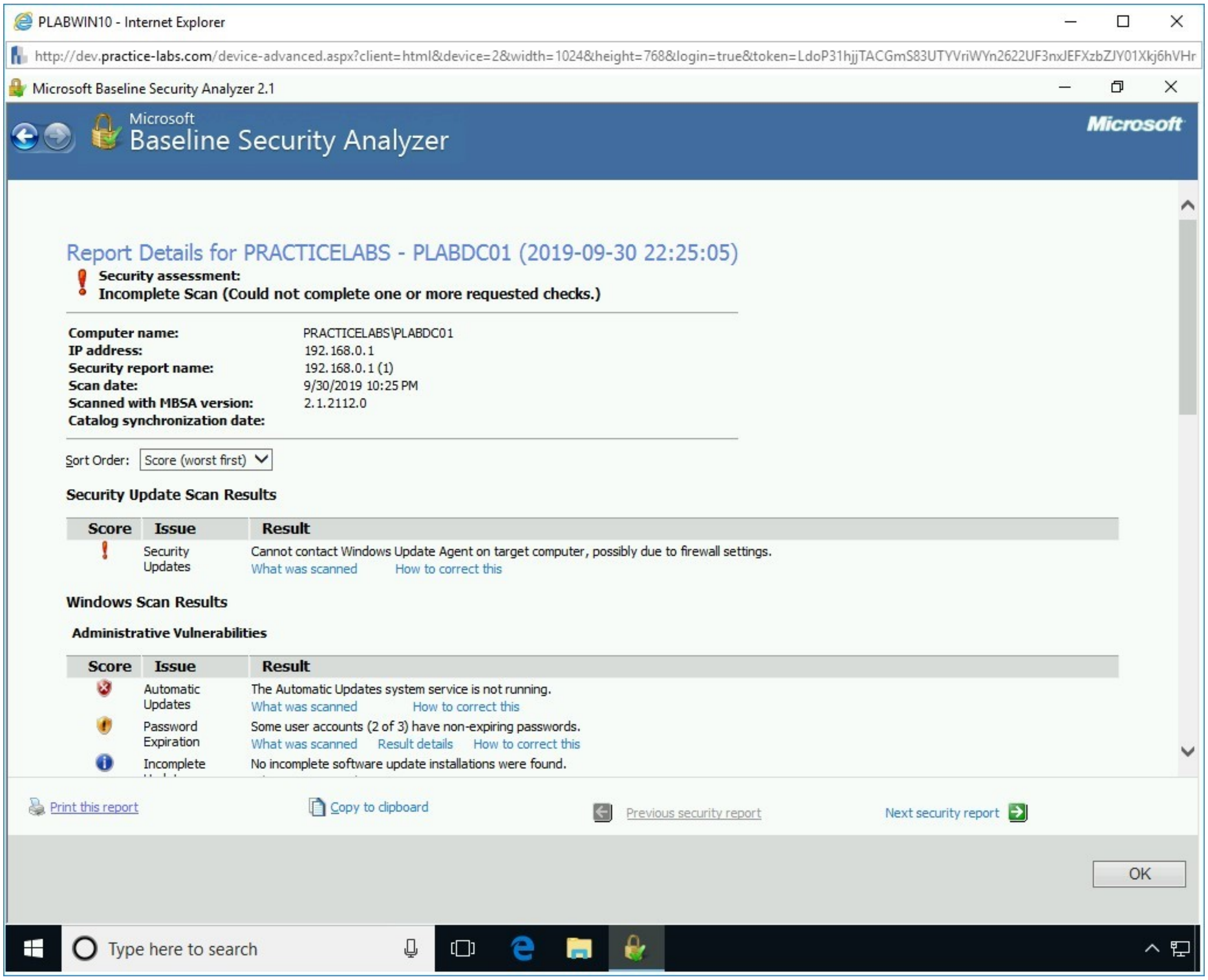
Sort order: Scan date (descending)

Computer Name	IP Address	Assessment	Scan Date
PRACTICELABS\PLABDC01	192.168.0.1	Incomplete Scan	9/30/2019 10:25 PM
PRACTICELABS\PLABDC01	192.168.0.1	Incomplete Scan	9/30/2019 9:59 PM

Figure 4.3 Screenshot of PLABWIN10: Clicking the listed reports.

Step 4

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


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft
Print this report
Copy to clipboard
Previous security report
Next security report
OK
Type here to search

Report Details for PRACTICELABS - PLABDC01 (2019-09-30 22:25:05)

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

Computer name:	PRACTICELABS\PLABDC01
IP address:	192.168.0.1
Security report name:	192.168.0.1 (1)
Scan date:	9/30/2019 10:25 PM
Scanned with MBSA version:	2.1.2112.0
Catalog synchronization date:	

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. What was scanned How to correct this

Windows Scan Results

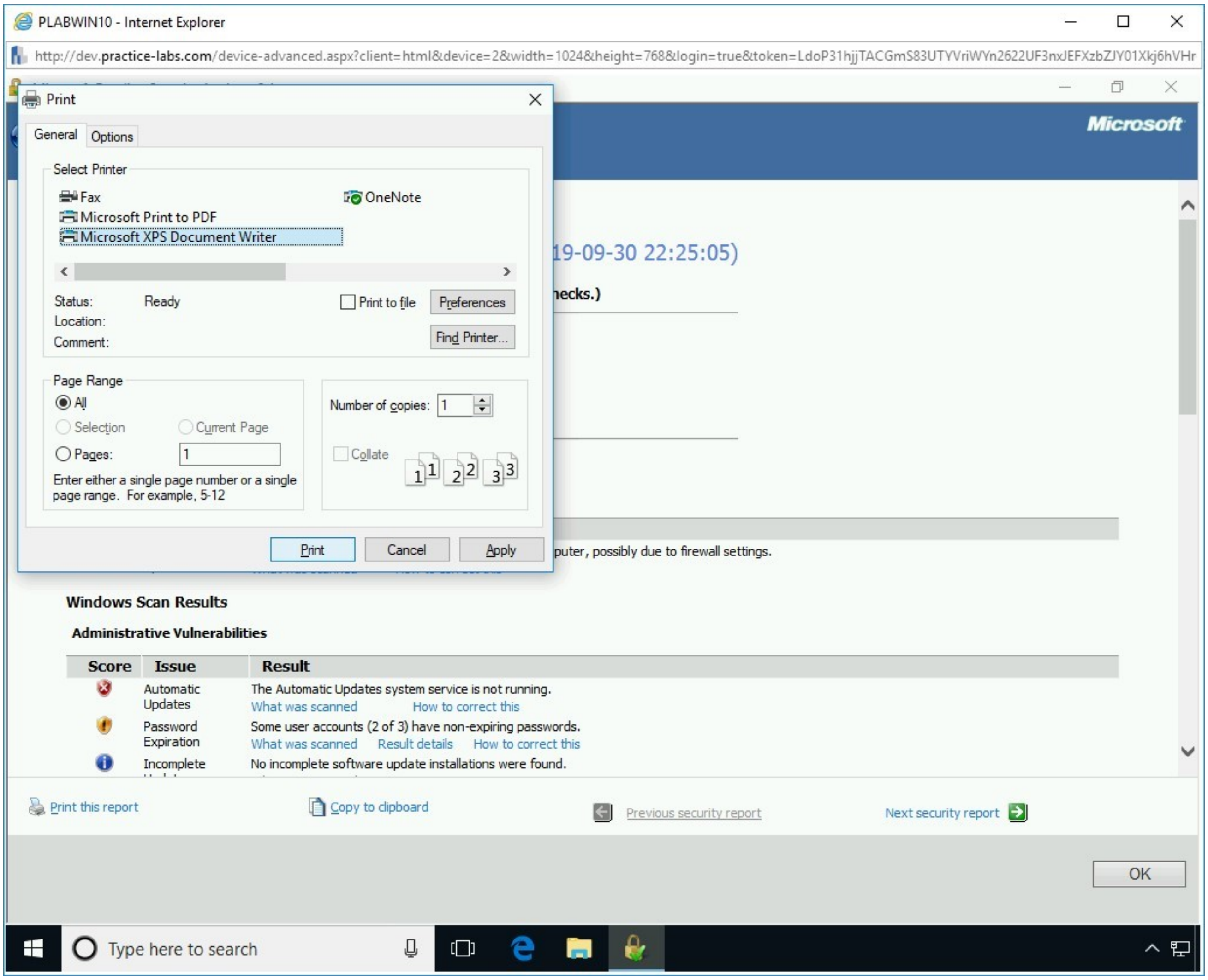
Administrative Vulnerabilities

Score	Issue	Result
☒	Automatic Updates	The Automatic Updates system service is not running. What was scanned How to correct this
!	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. What was scanned Result details How to correct this
i	Incomplete	No incomplete software update installations were found.

Figure 4.4 Screenshot of PLABWIN10: Clicking the Print this report link.

Step 5

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


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft
Print
General
Options
Preferences
Find Printer...
Print
Cancel
Apply
Print this report
Copy to clipboard
Previous security report
Next security report
OK
Type here to search

Select Printer

- Fax
- OneNote
- Microsoft Print to PDF
- Microsoft XPS Document Writer

Status: Ready
Location:
Comment:
□ Print to file

Page Range
● All
○ Selection ○ Current Page
○ Pages: 1
Enter either a single page number or a single page range. For example, 5-12

Number of copies: 1
□ Collate

19-09-30 22:25:05)

hecks.)

puter, possibly due to firewall settings.

Windows Scan Results

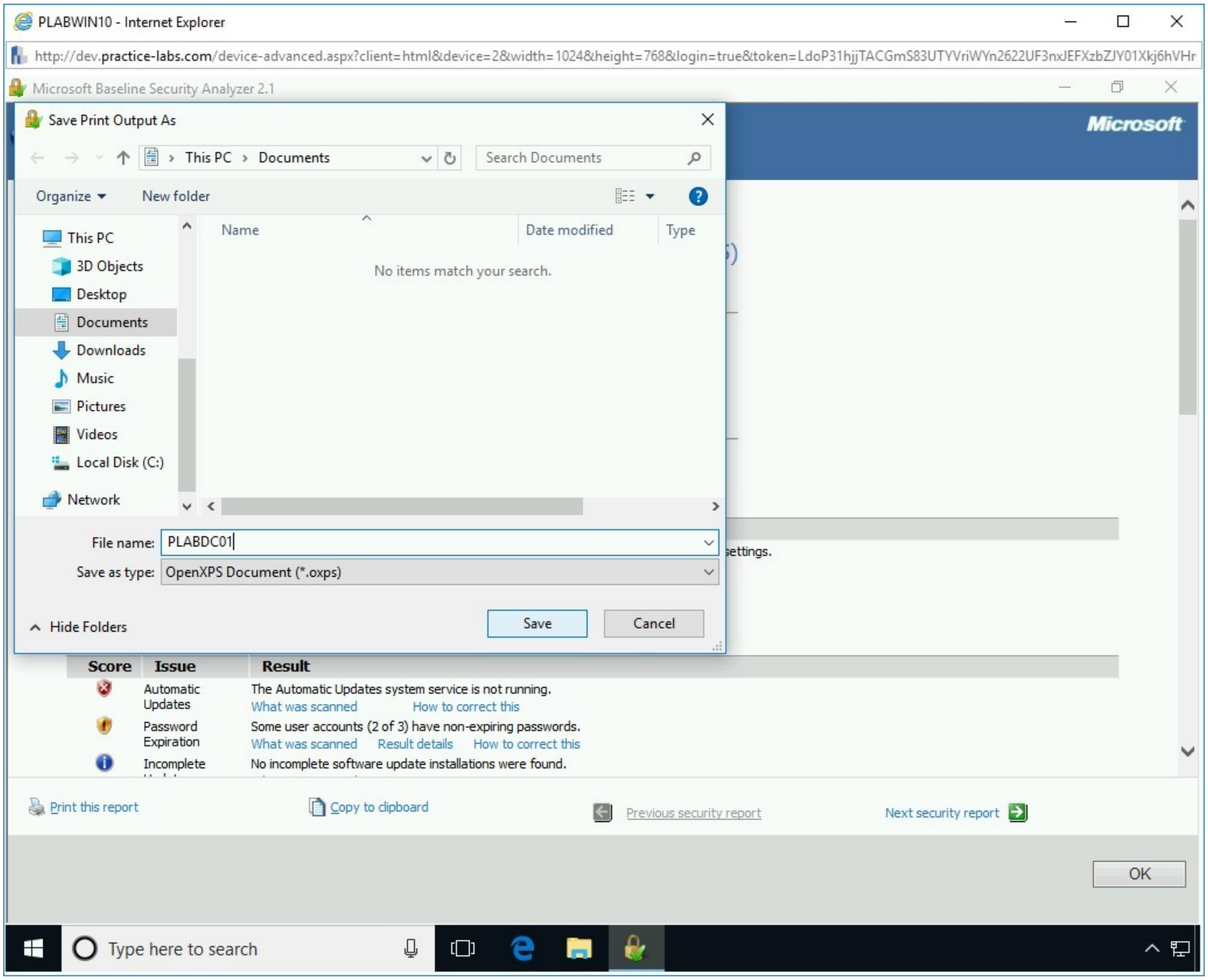
Administrative Vulnerabilities

Score	Issue	Result
✗	Automatic Updates	The Automatic Updates system service is not running. What was scanned How to correct this
!	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. What was scanned Result details How to correct this
i	Incomplete	No incomplete software update installations were found.

Figure 4.5 Screenshot of PLABWIN10: Clicking the Print button in the Print dialog box.

Step 6

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



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr

No items match your search.

File name: PLABDC01

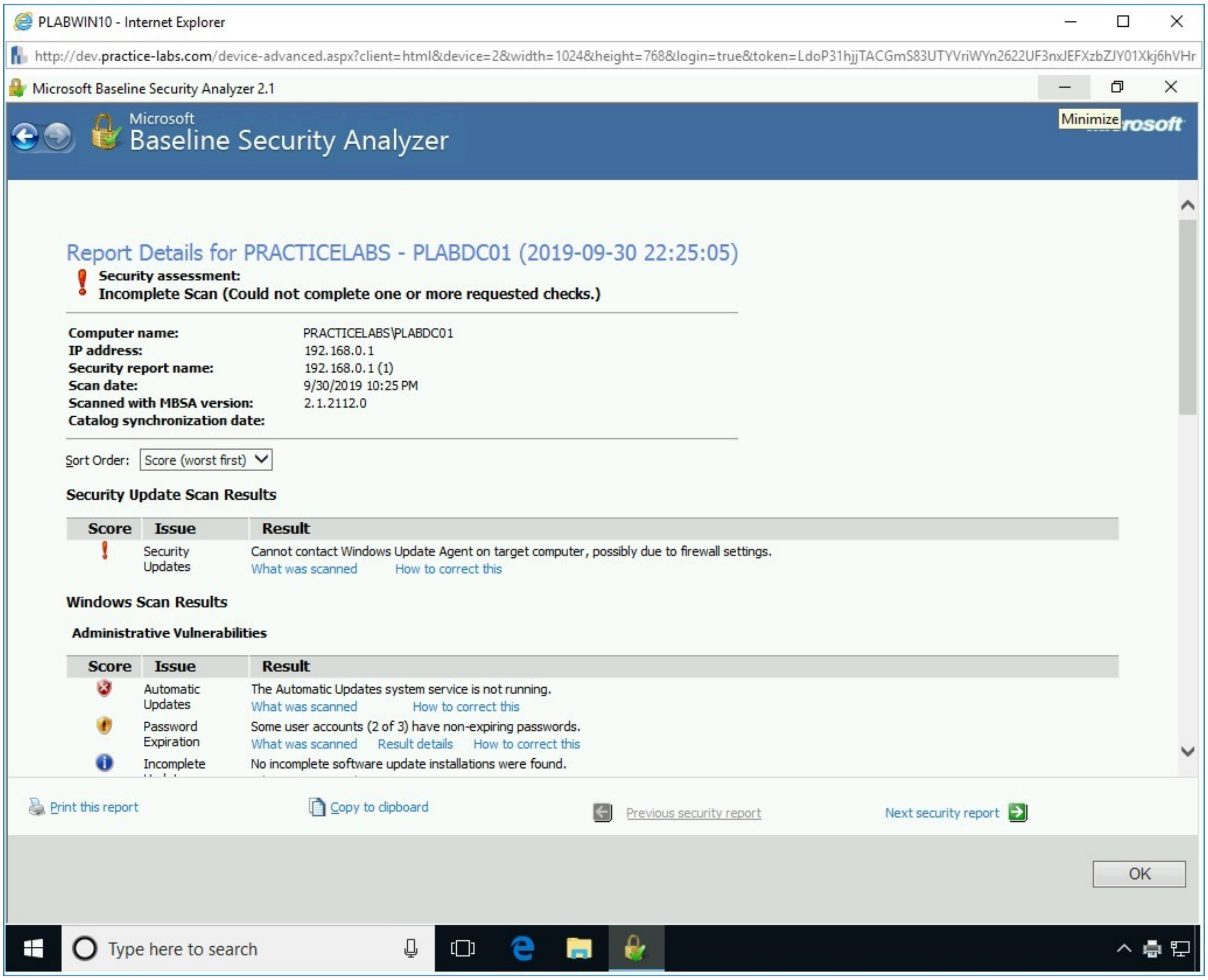
Save as type: OpenXPS Document (*.oxps)

Score	Issue	Result
✖	Automatic Updates	The Automatic Updates system service is not running. What was scanned How to correct this
!	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. What was scanned Result details How to correct this
i	Incomplete	No incomplete software update installations were found.

Figure 4.6 Screenshot of PLABWIN10: Saving the MBSA report in the Save Print Output As dialog box.

Step 7

Now minimize the **MBSA** window.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Minimize
Print this report
Copy to clipboard
Previous security report
Next security report
OK
Type here to search

Report Details for PRACTICELABS - PLABDC01 (2019-09-30 22:25:05)

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

Computer name:	PRACTICELABS\PLABDC01
IP address:	192.168.0.1
Security report name:	192.168.0.1 (1)
Scan date:	9/30/2019 10:25 PM
Scanned with MBSA version:	2.1.2112.0
Catalog synchronization date:	

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. What was scanned How to correct this

Windows Scan Results

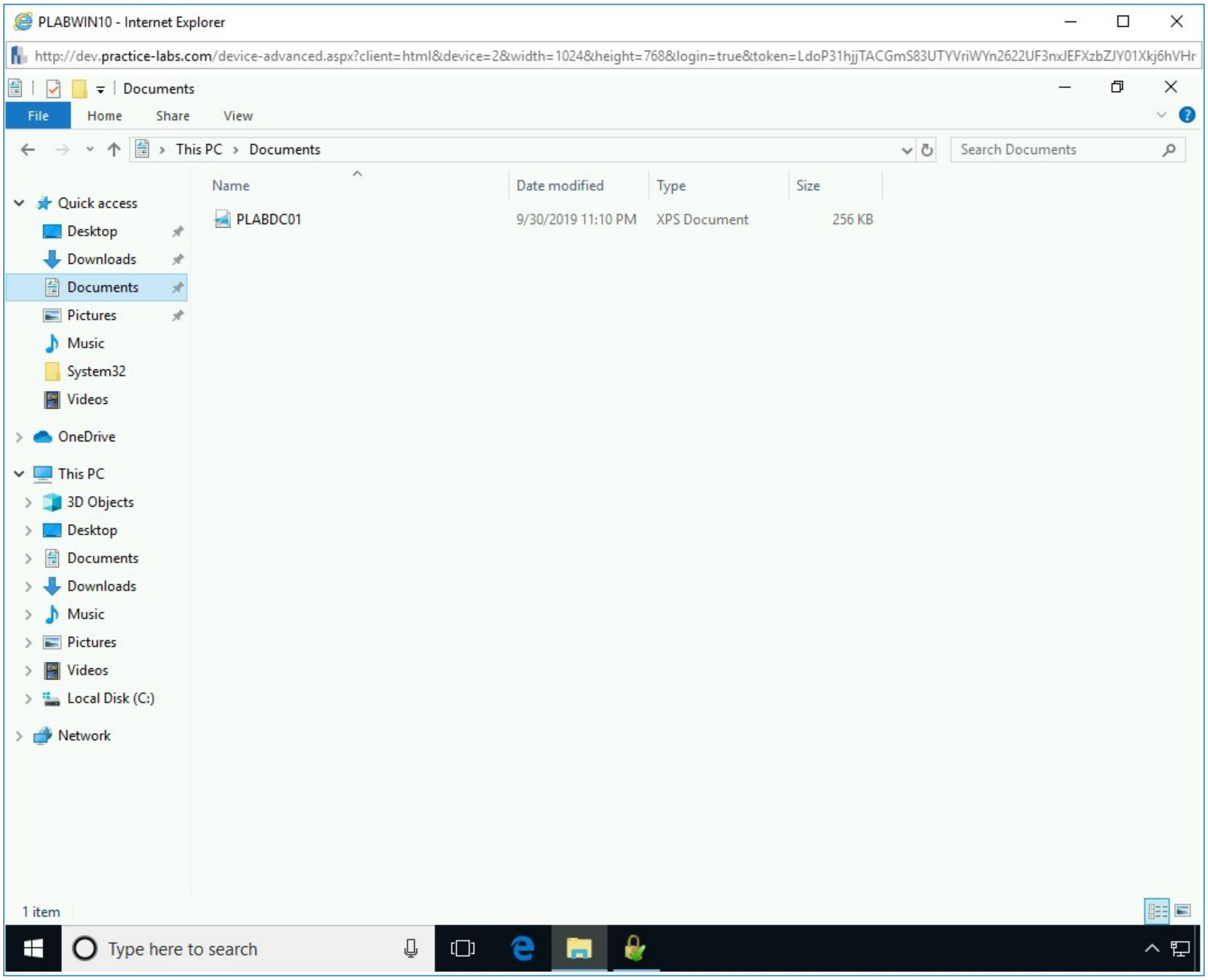
Administrative Vulnerabilities

Score	Issue	Result
✗	Automatic Updates	The Automatic Updates system service is not running. What was scanned How to correct this
!	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. What was scanned Result details How to correct this
i	Incomplete	No incomplete software update installations were found.

Figure 4.7 Screenshot of PLABWIN10: Minimizing the MBSA window.

Step 8

From the taskbar, click **File Explorer** and then navigate to the **Documents** folder in the left pane.



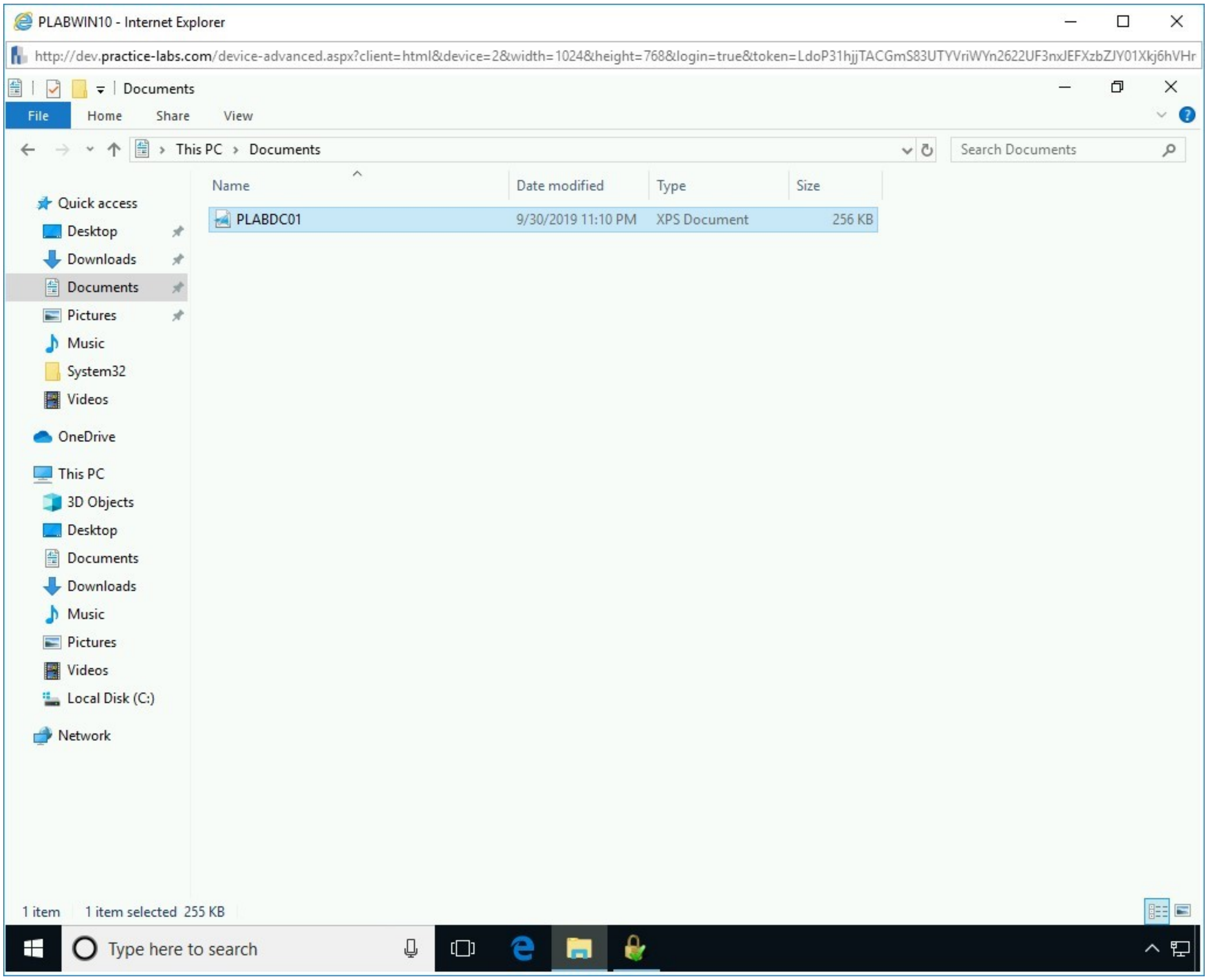
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr

Name	Date modified	Type	Size
PLABDC01	9/30/2019 11:10 PM	XPS Document	256 KB

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.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr

Name	Date modified	Type	Size
PLABDC01	9/30/2019 11:10 PM	XPS Document	256 KB

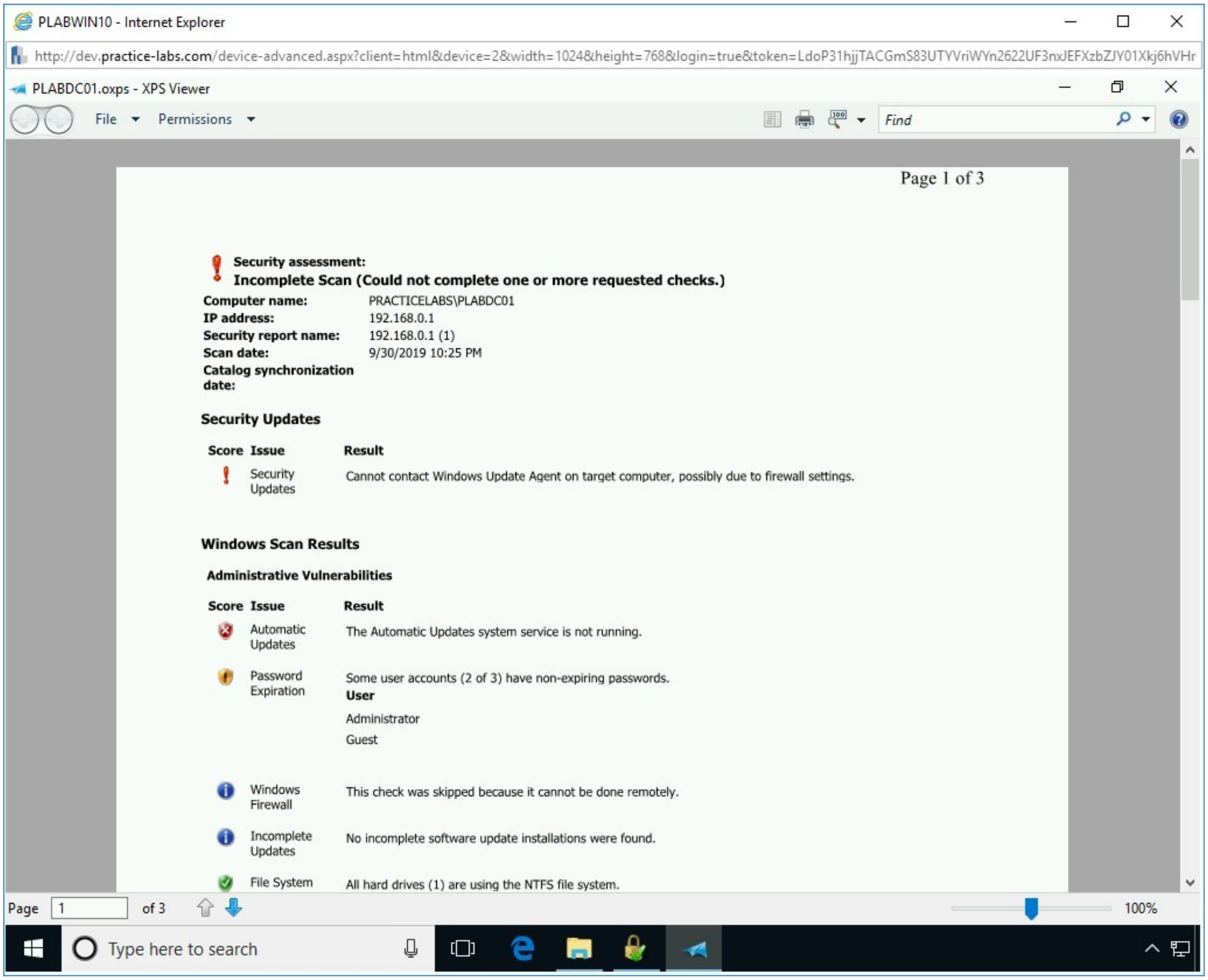
1 item   1 item selected 255 KB

Figure 4.9 Screenshot of PLABWIN10: Double-clicking the scan report in File Explorer.

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.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=LdoP31hjjTACGmS83UTYVriWYn2622UF3nxJEFXzbZJY01Xkj6hVHr
PLABDC01.oxps - XPS Viewer
File
Permissions
Find
Page 1 of 3
Page 1 of 3
100%
Type here to search

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

Computer name:	PRACTICELABS\PLABDC01
IP address:	192.168.0.1
Security report name:	192.168.0.1 (1)
Scan date:	9/30/2019 10:25 PM
Catalog synchronization date:	

Security Updates

Score	Issue	Result
!	Security Updates	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings.

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✗	Automatic Updates	The Automatic Updates system service is not running.
!	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. **User** Administrator Guest
i	Windows Firewall	This check was skipped because it cannot be done remotely.
i	Incomplete Updates	No incomplete software update installations were found.
✓	File System	All hard drives (1) are using the NTFS file system.

Figure 4.10 Screenshot of PLABWIN10: Showing the MBSA report in XPS Viewer.

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.

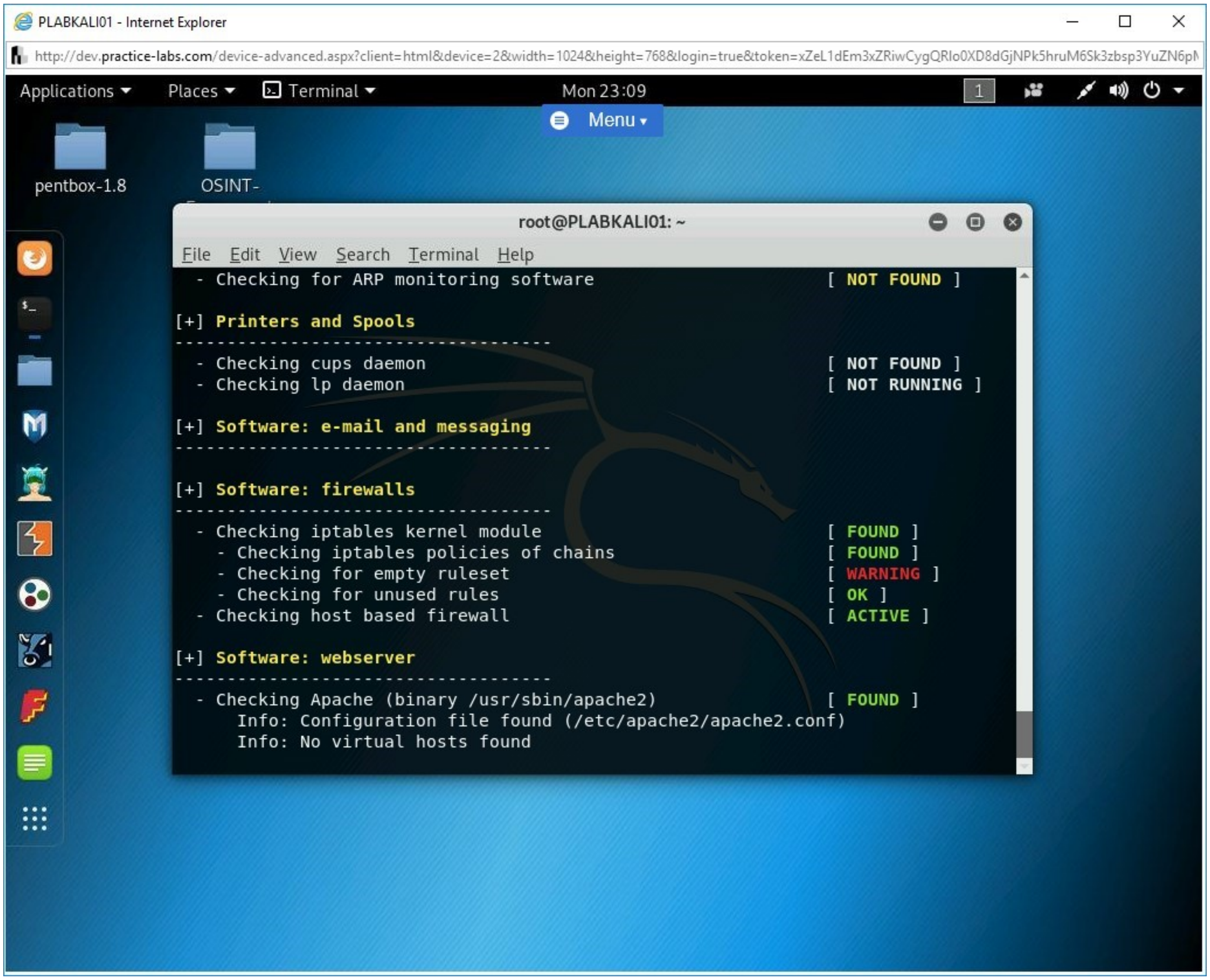
A false positive is a condition, which is typically detected by a scanner, but it actually does not exist. It is about a condition that is considered to be present in a result but it does not exist. For example, a vulnerability may indicate that MySQL has a vulnerability, but, in reality, it does not 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.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xZeL1dEm3xZRiwCygQRlo0XD8dGjNPk5hruM6Sk3zbsp3YuZN6pN
Applications
Places
Terminal
Mon 23:09
1
Menu
pentbox-1.8
OSINT-
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
  - Checking for ARP monitoring software                      [ NOT FOUND ]

[+] Printers and Spools
------------------------------------
  - Checking cups daemon                                      [ NOT FOUND ]
  - Checking lp daemon                                        [ NOT RUNNING ]

[+] Software: e-mail and messaging
------------------------------------

[+] Software: firewalls
------------------------------------
  - Checking iptables kernel module                           [ FOUND ]
    - Checking iptables policies of chains                    [ FOUND ]
    - Checking for empty ruleset                              [ WARNING ]
    - Checking for unused rules                               [ OK ]
  - Checking host based firewall                              [ ACTIVE ]

[+] Software: webserver
------------------------------------
  - Checking Apache (binary /usr/sbin/apache2)                [ FOUND ]
    Info: Configuration file found (/etc/apache2/apache2.conf)
    Info: No virtual hosts found
```

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.