Practice Labs - Ethical Hacker v10

Enumeration

- **Introduction**
- **Lab Topology**
- **Exercise 1 - Enumeration Techniques using Windows-based Tools**
- **Exercise 2 - Enumeration Techniques using Kali Linux Tools**
- **Exercise 3 - Enumeration Prevention Techniques**
- **Review**

Introduction

Enumeration
SNMP
NetBIOS
MIB
LDAP
Hyena
SuperScan
IP Network Browser
Softerra LDAP Administrator
Dnsenum
Nmap
SMB
Ethical Hacking

Welcome to the **Enumeration** 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 - Enumeration Techniques using Windows-based Tools
- Exercise 2 - Enumeration Techniques using Kali Linux Tools
- Exercise 3 - Enumeration Prevention Techniques

After completing this lab, you will be able to:

- Use SuperScan for NetBIOS Enumeration
- Use Hyena for Enumeration
- Perform LDAP Enumeration using Softerra LDAP Administrator
- Perform SNMP Enumeration using IP Network Browser
- Perform DNS Enumeration
- Perform Windows Host Enumeration using Rpcclient
- Perform Linux Host Enumeration using Nmap
- Perform Website Enumeration using Nmap
- Perform Server Message Block (SMB) Enumeration
- Prevent Web Applications Enumeration
- Prevent SNMP Enumeration
- Prevent LDAP Enumeration
- Prevent DNS Enumeration
- Prevent Windows Enumeration

Exam Objectives

The following exam objectives are covered in this lab:

- **5.2** Information Security Assessment Methodologies

> ***Note:*** *Our main focus is to cover the practical, hands-on aspects of the exam objectives. We 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.

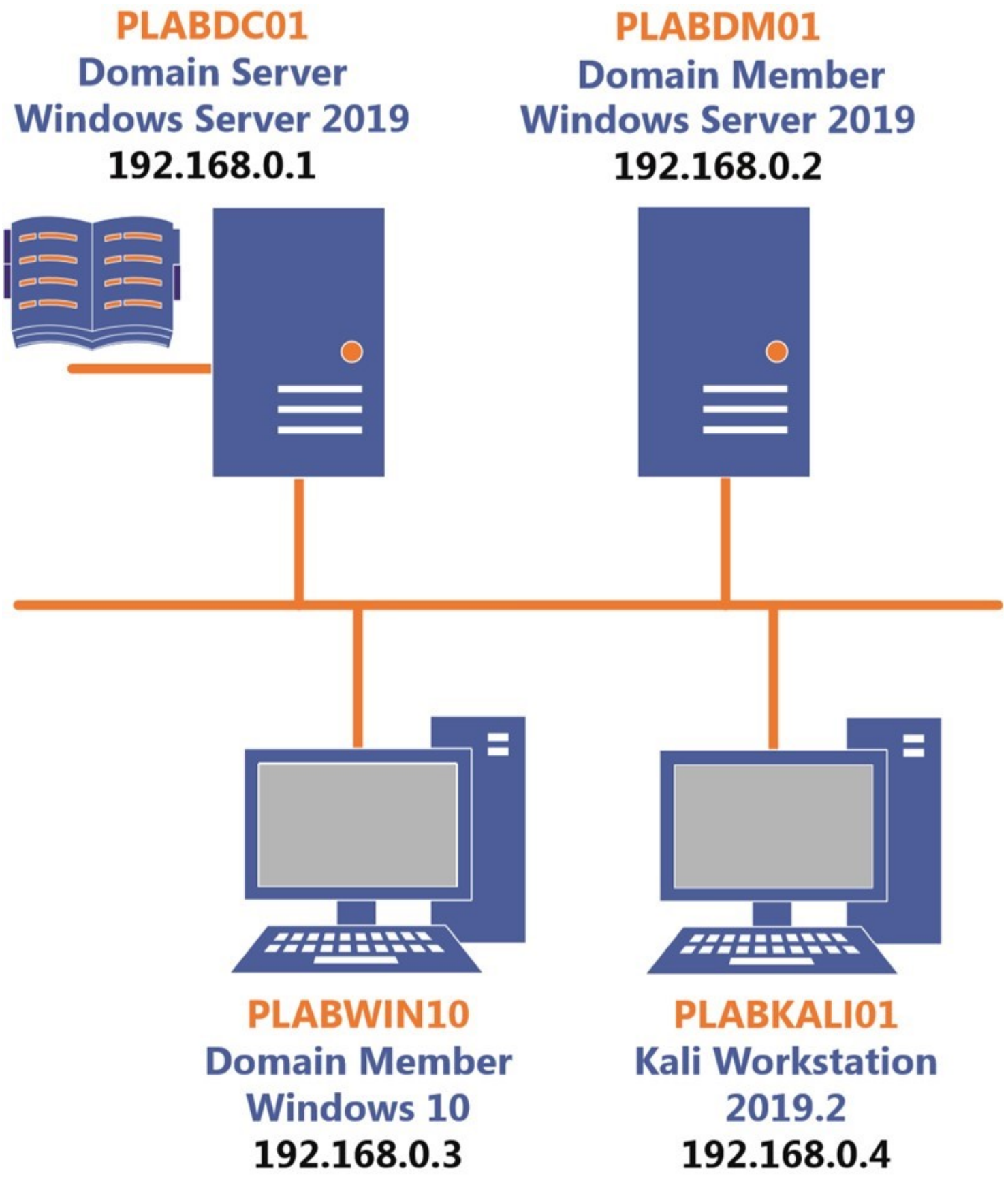
Help and Support

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 Member)
- **PLABWIN10 -** (Windows 10 - Workstation)
- **PLABKALI01 -** (Kali 2019.2 - Linux Kali Workstation)

Click **Next** to proceed to the first exercise.

Exercise 1 - Enumeration Techniques using Windows-based Tools

Enumeration allows you to establish an active connection with a target. Your intent is to extract different types of information from the target. Some of the information that you can extract is:

- Usernames
- Group names
- Hostnames
- Network shares and services
- Routing tables
- Web application
- Web servers
- SNMP information
- DNS information

There are various types of enumerations that can be performed. Some of these are:

- Windows Enumeration
- Linux Enumeration
- NetBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP Enumeration
- SMTP Enumeration

- DNS Enumeration

In this exercise, you will learn to use some of the enumeration techniques using Windows-based tools.

Learning Outcomes

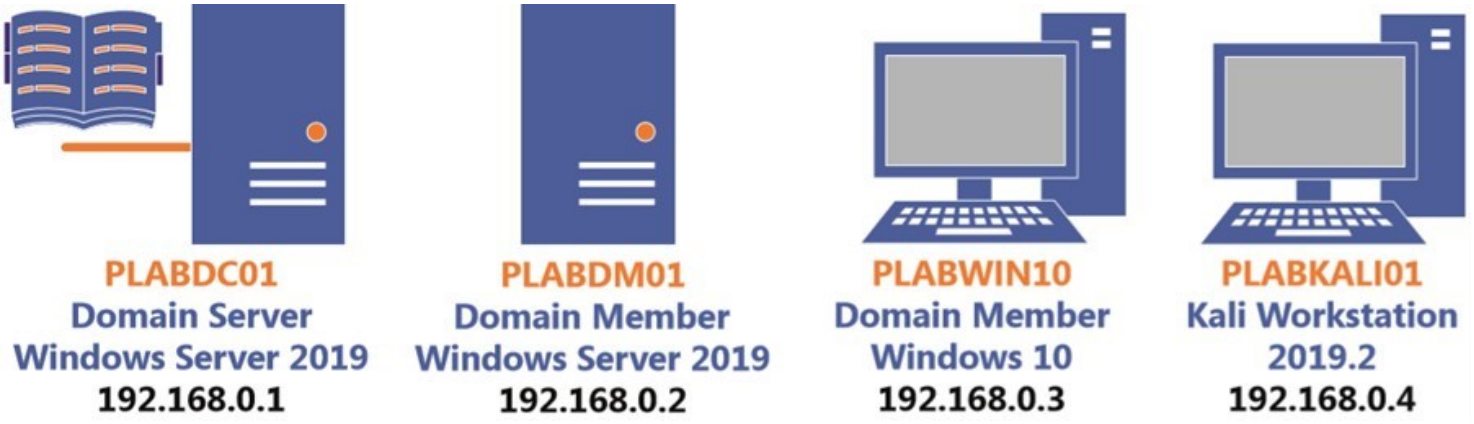
After completing this exercise, you will be able to:

- Use SuperScan for NetBIOS Enumeration
- Use Hyena for Enumeration
- Perform LDAP Enumeration using Softerra LDAP Administrator
- Perform SNMP Enumeration using IP Network Browser

Your Devices

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

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



Task 1 - Use SuperScan for NetBIOS Enumeration

SuperScan is a network management tool that has the following capabilities:

- NetBIOS information

- User and group accounts
- Network shares
- Services status

To use SuperScan, for NetBIOS enumeration perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABWIN10**. In the **Type here to search** text box, type the following:

```
Internet Explorer
```

From the search results, select **Internet Explorer**.

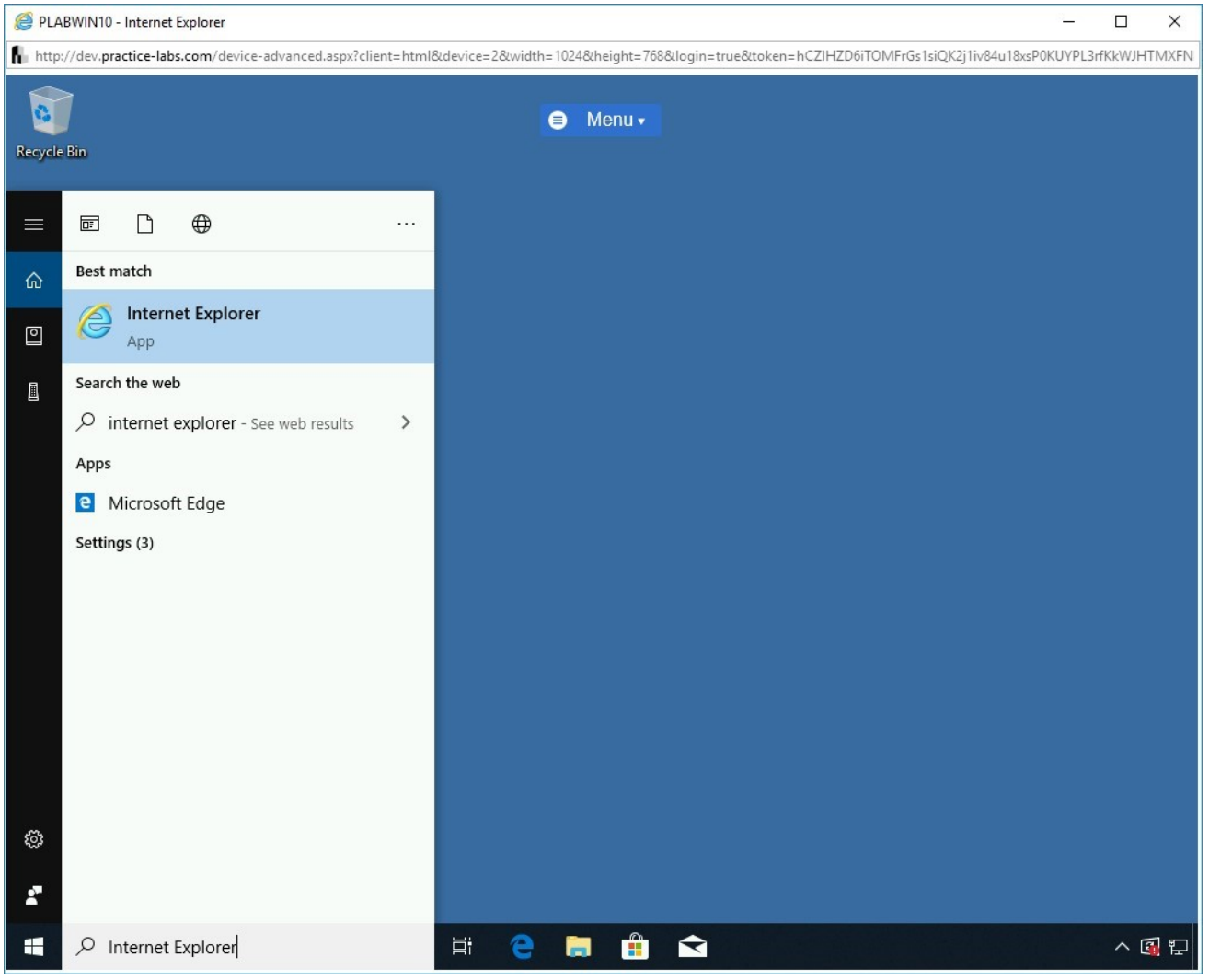


Figure 1.1 Screenshot of PLABWIN10: Selecting Internet Explorer from the search results.

Step 2

Internet Explorer opens the **Tools and resources** webpage.

Click **Tools**.

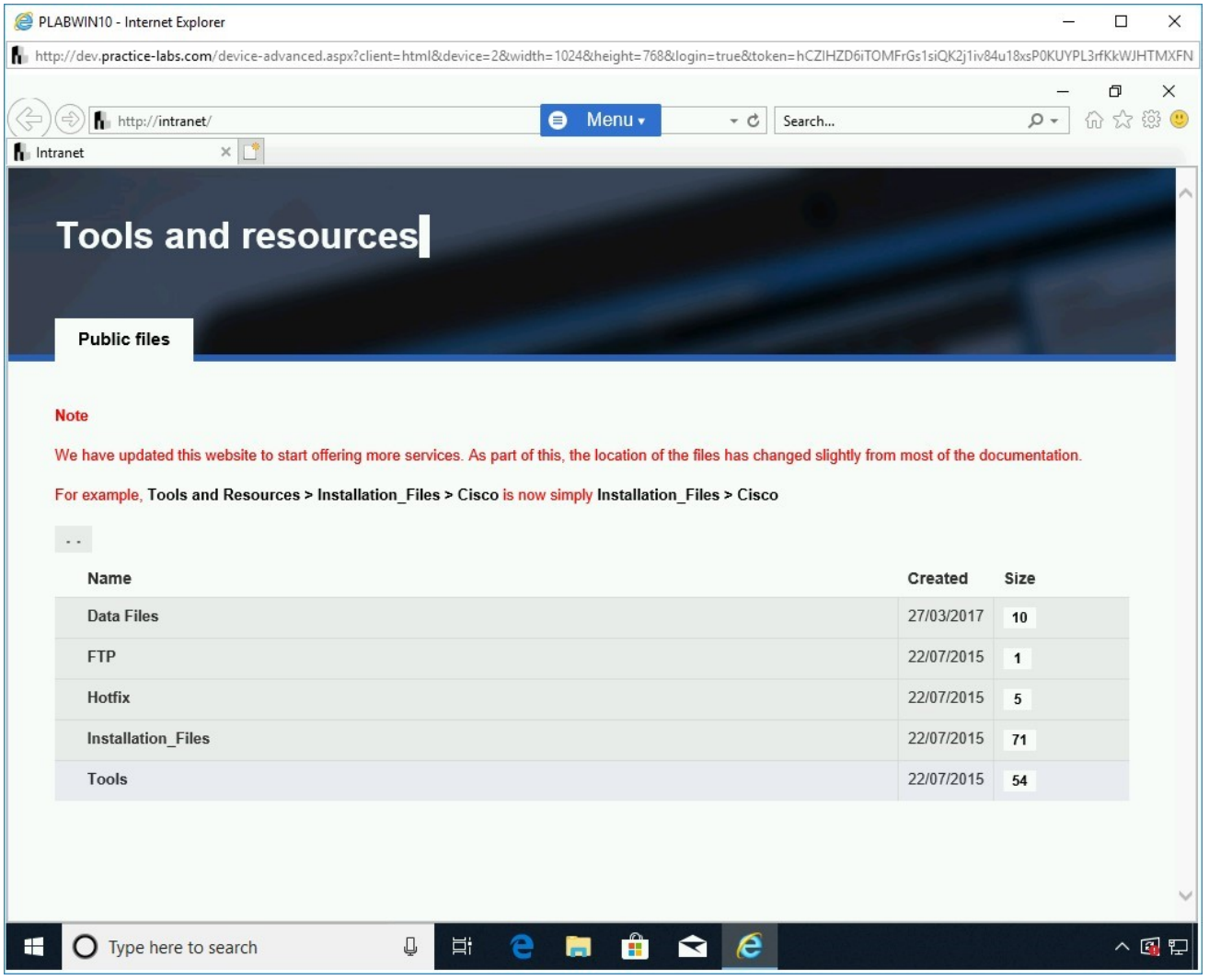


Figure 1.2 Screenshot of PLABWIN10: Clicking the Tools option on the Tools and resources page.

Step 3

You will be directed to **[..] > Tools**.

Scroll down a bit and locate **Hacking Tools**.

Click **Hacking Tools**.

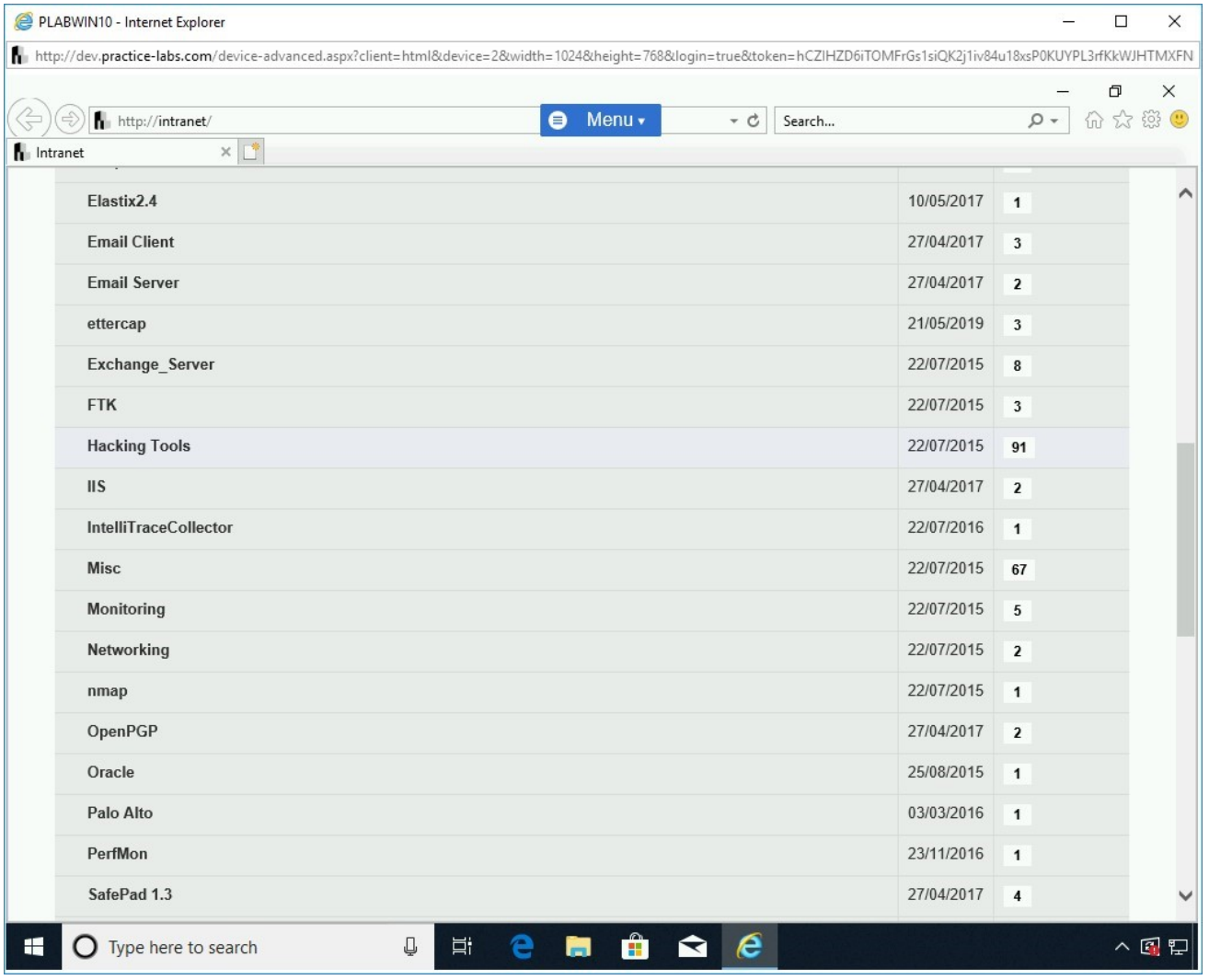


Figure 1.3 Screenshot of PLABWIN10: Clicking the Hacking Tools option.

Step 4

On the **[..] > Tools > Hacking Tools** page, scroll down the page and locate **superscan-4.1.zip**.

Click **superscan-4.1.zip**.

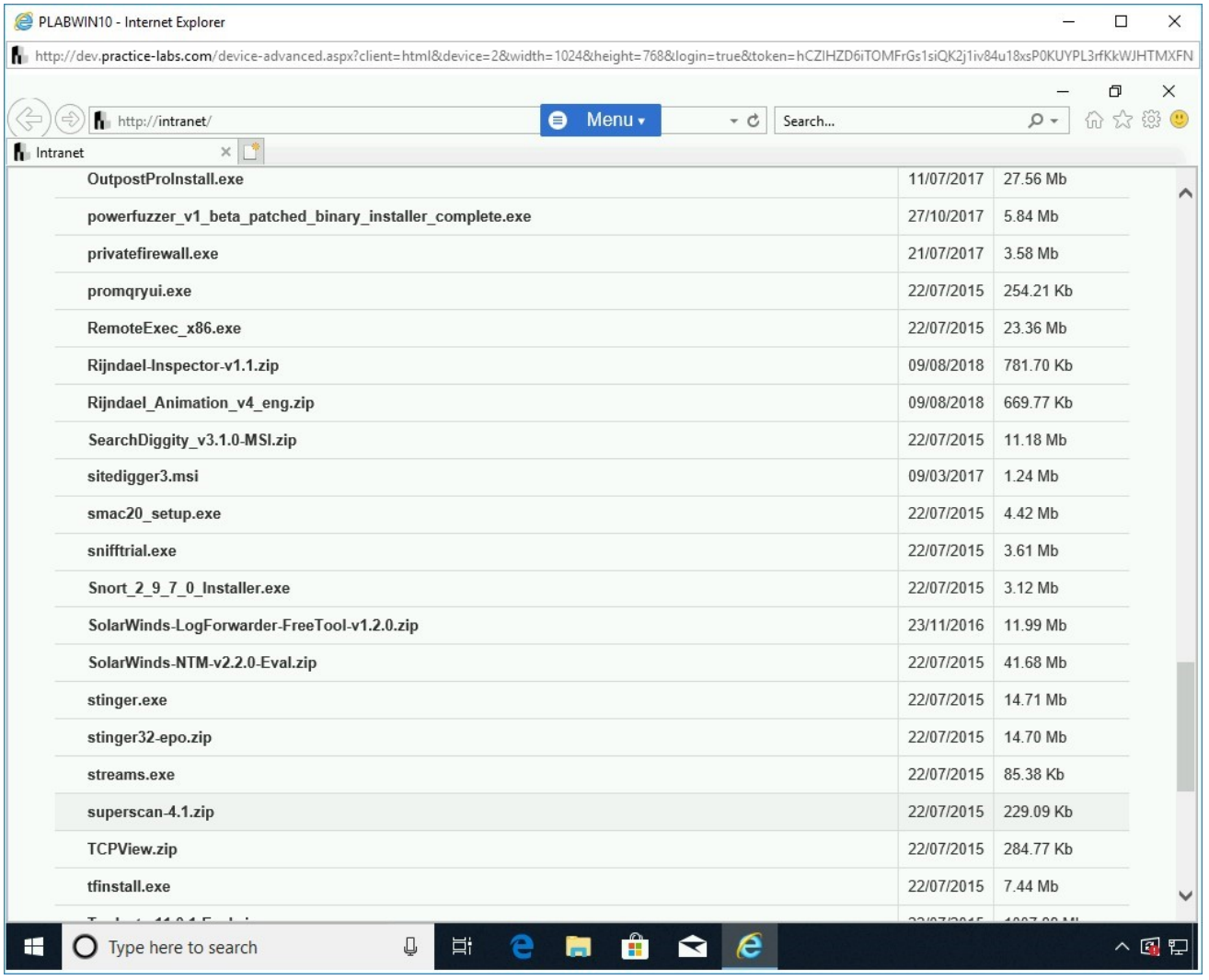


Figure 1.4 Screenshot of PLABWIN10: Clicking the SuperScan-4.1.zip option.

Step 5

In the notification bar, click **Save**.

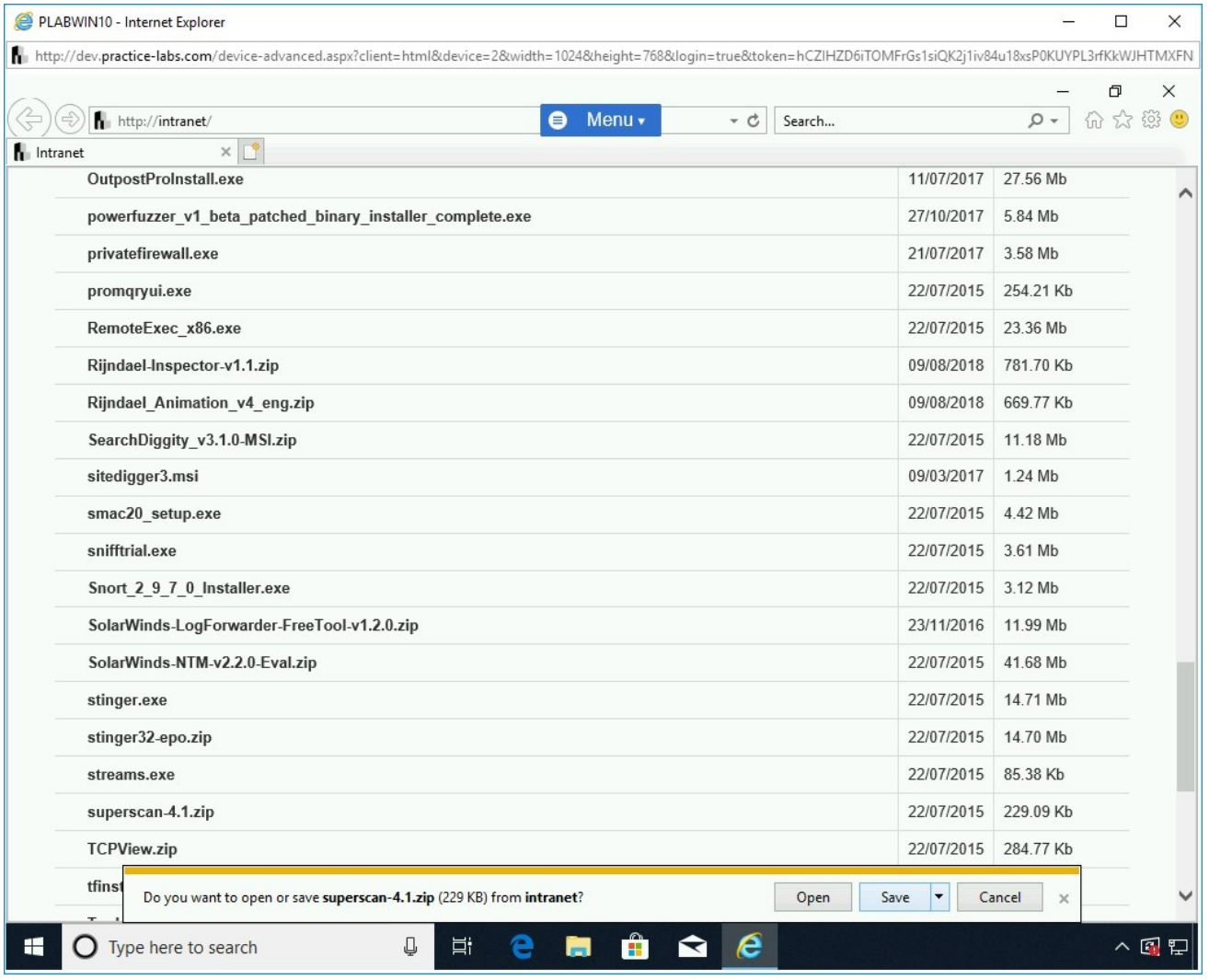


Figure 1.5 Screenshot of PLABWIN10: Clicking Save in the notification bar.

Step 6

When the file download is successfully completed, in the notification bar, click **Open folder**.

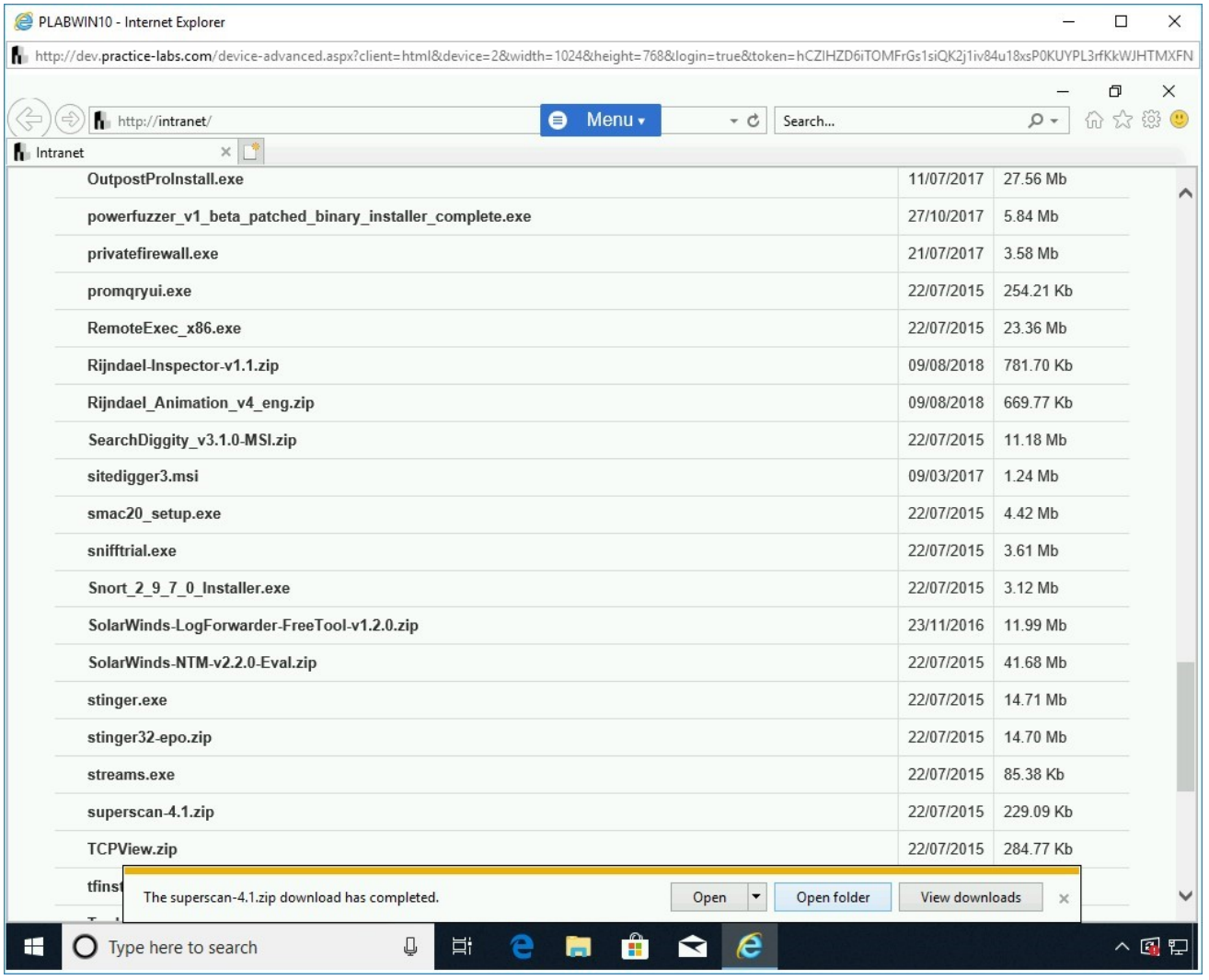


Figure 1.6 Screenshot of PLABWIN10: Clicking Open folder in the notification bar.

Step 7

File Explorer opens the **Downloads** folder that contains the **superscan-4.1.zip** file.

Right-click **superscan-4.1** and select **Extract All**.

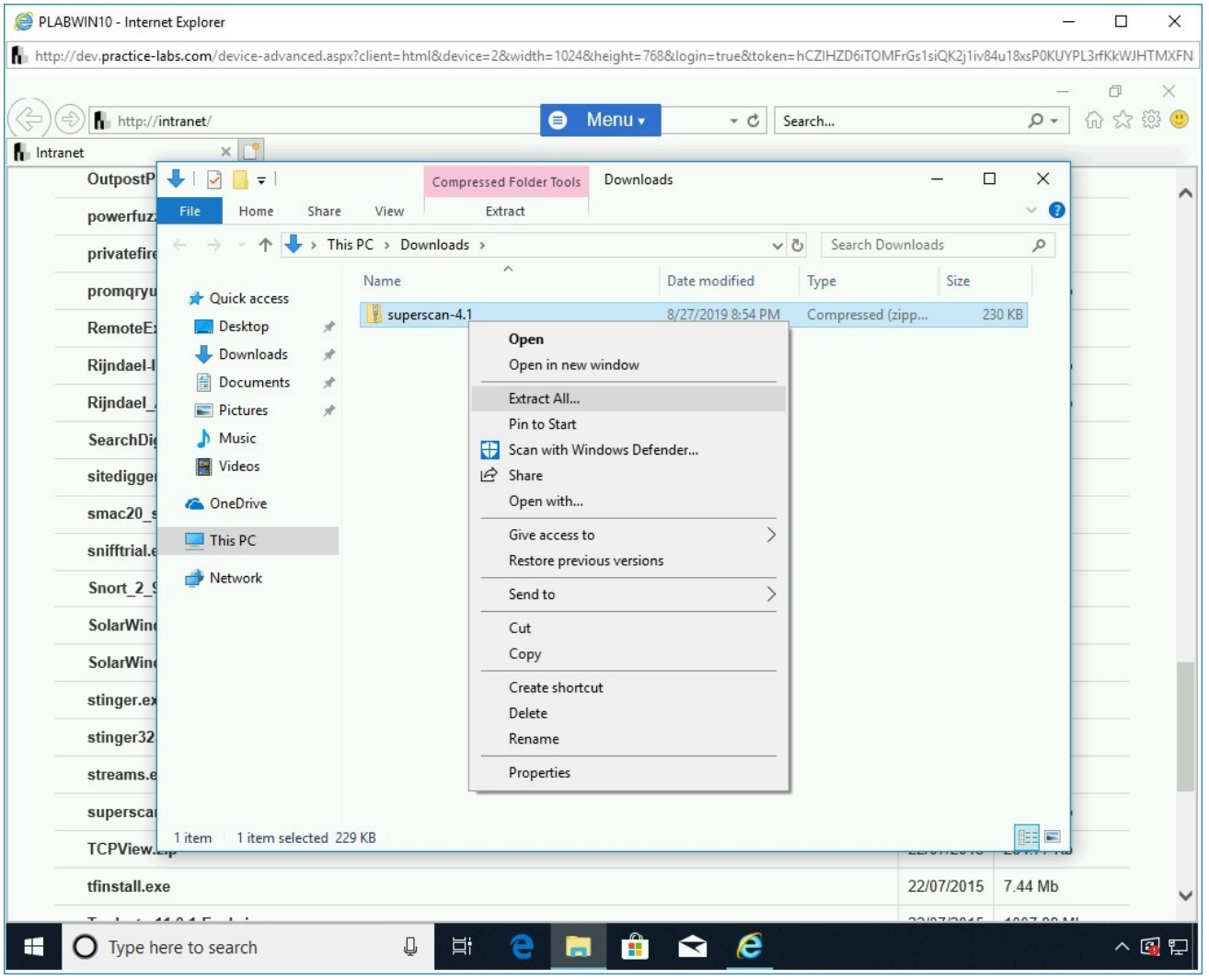


Figure 1.7 Screenshot of PLABWIN10: Right-clicking the superscan-4.1.zip file and selecting Extract All from the context menu.

Step 8

In the **Extract Compressed (Zipped) Folders** dialog box, keep the default path and click **Extract**.

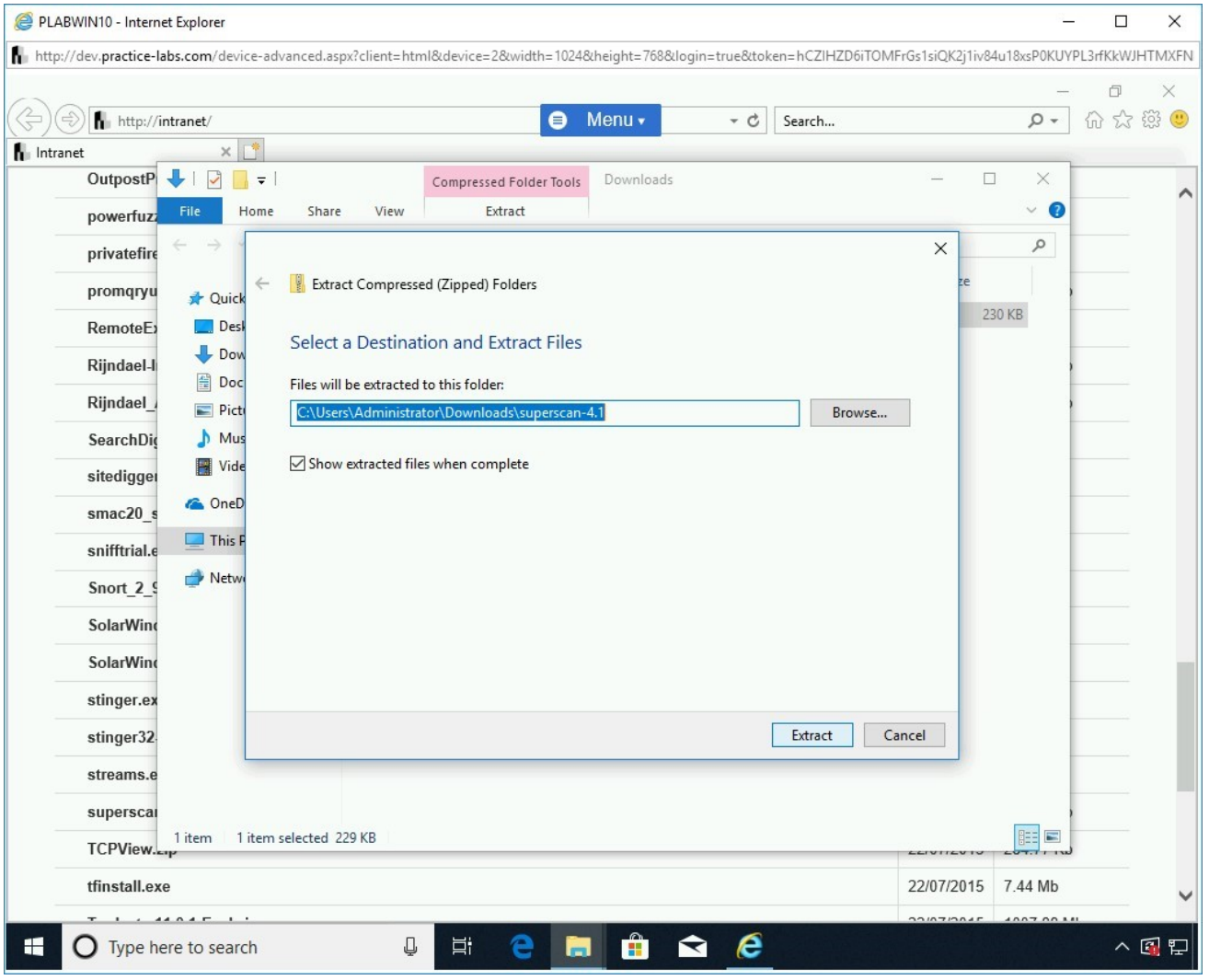


Figure 1.8 Screenshot of PLABWIN10: Clicking the Extract option in the Extract Compressed (Zipped) Folders dialog box.

Step 9

A new **File Explorer** window opens with the extracted files. Double-click **SuperScan4.1**.

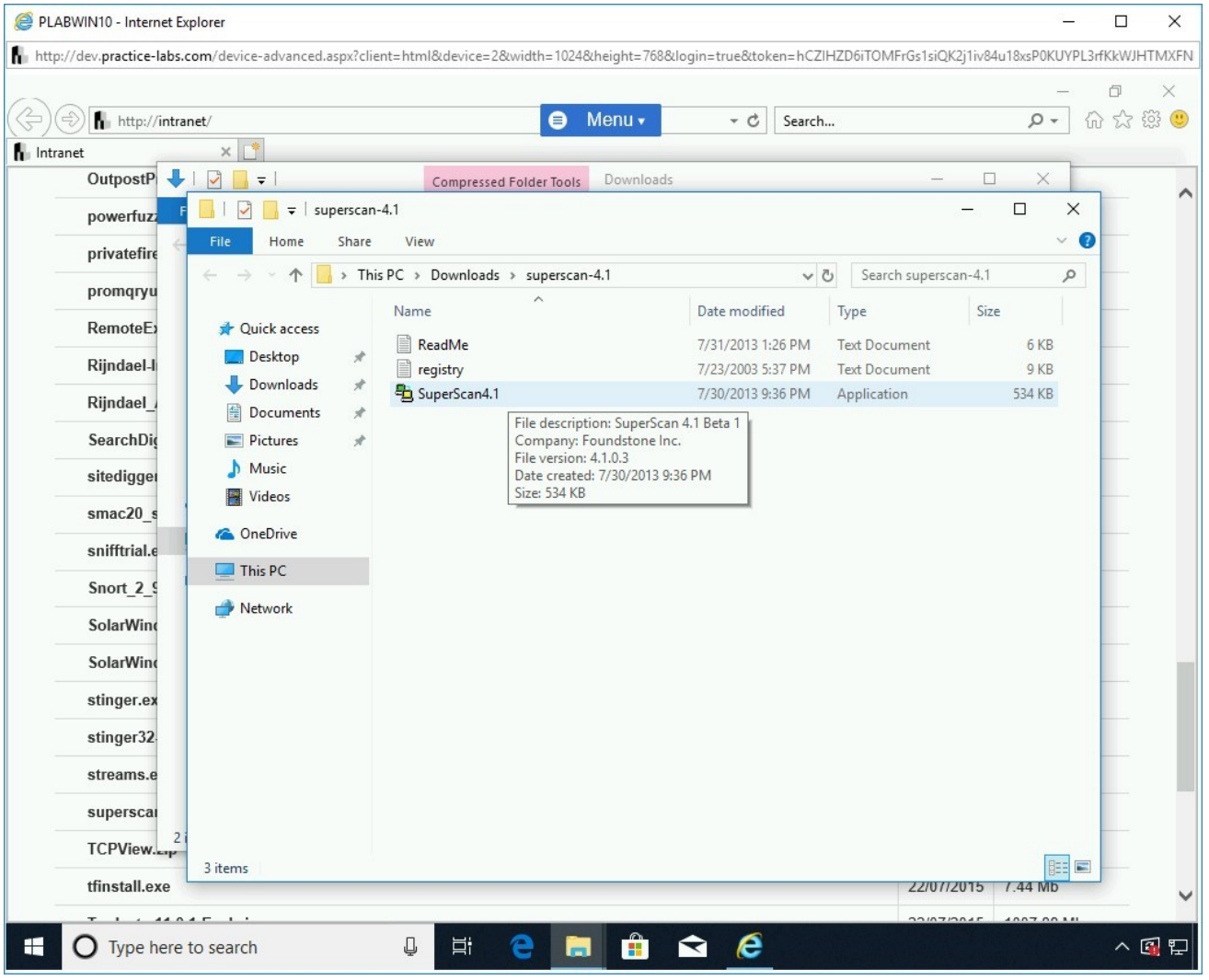


Figure 1.9 Screenshot of PLABWIN10: Showing the extracted files and clicking the SuperScan4.1 file.

Step 10

The **SuperScan 4.1** window is displayed.

In the **SuperScan 4.1** window, click the **Windows Enumeration** tab.

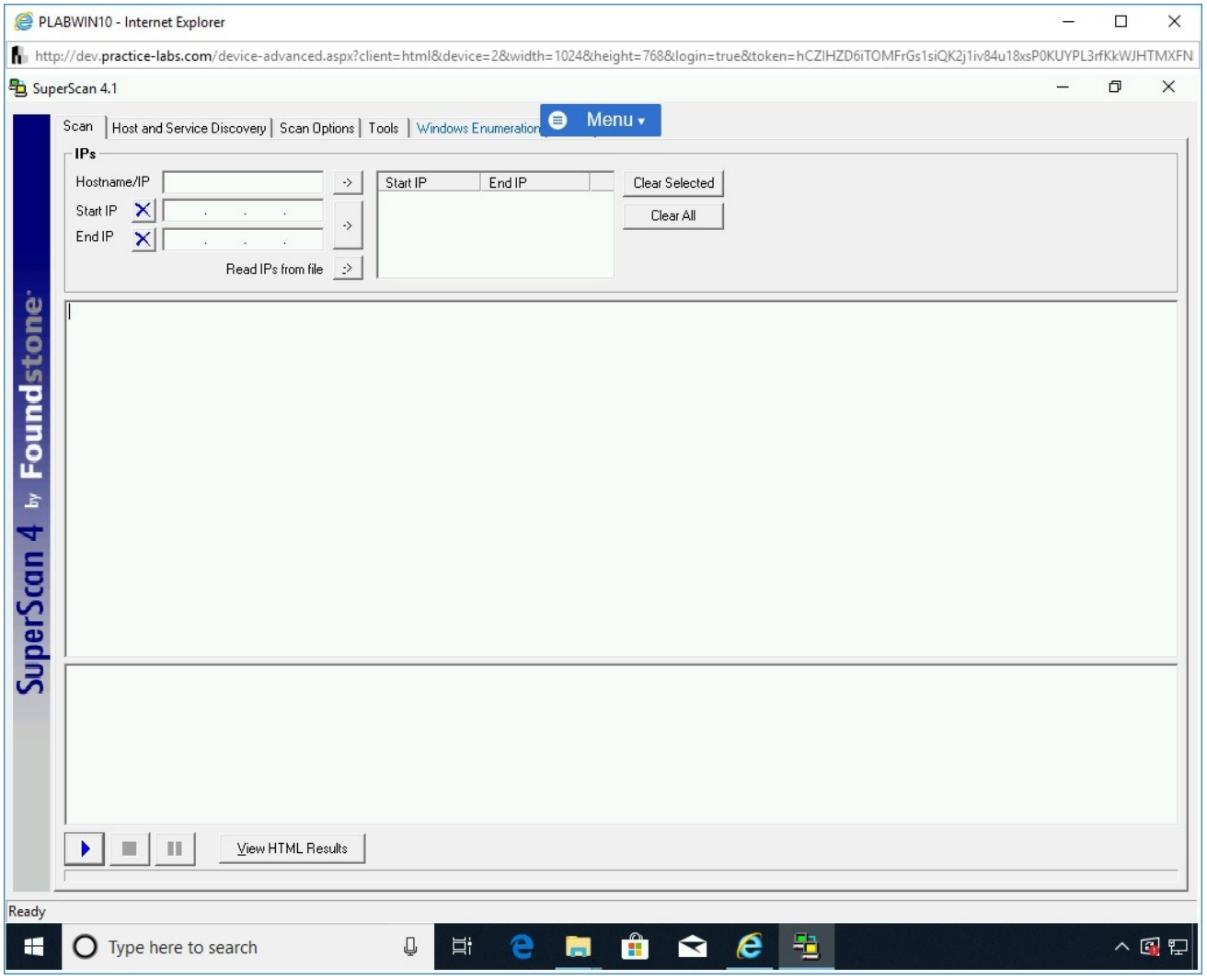


Figure 1.10 Screenshot of PLABWIN10: Clicking the Windows Enumeration tab.

Step 11

There are two panes in the **Windows Enumeration** tab. The left pane contains the Enumeration types, and the right pane will display the result of the enumeration. In the **Hostname/IP/URL** text box, type the following IP address:

```
192.168.0.1
```

Click **Enumerate**.

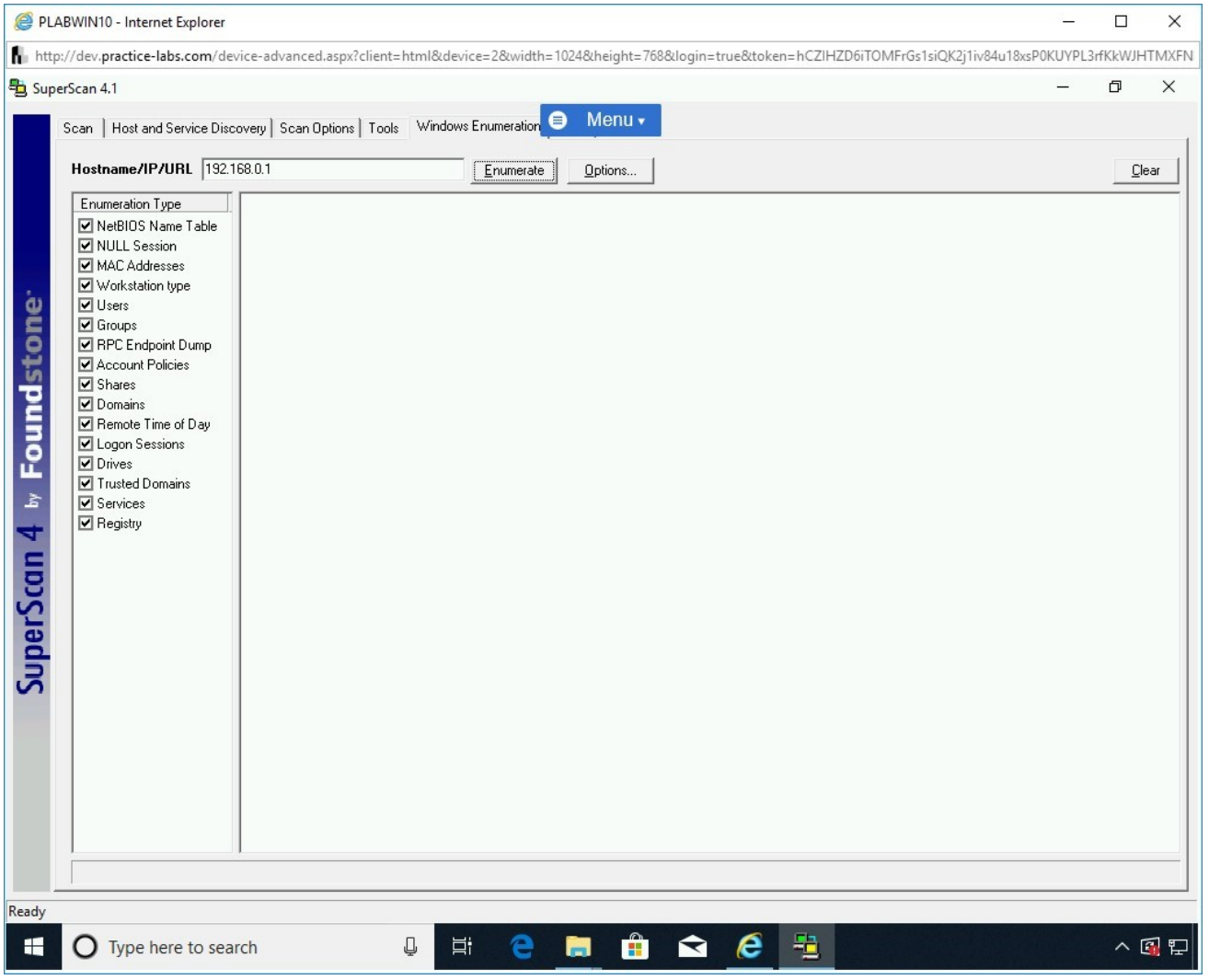


Figure 1.11 Screenshot of PLABWIN10: Entering the target's IP address and clicking Enumerate.

Step 12

The results are displayed in the right pane. Scroll up to view the results from the beginning.

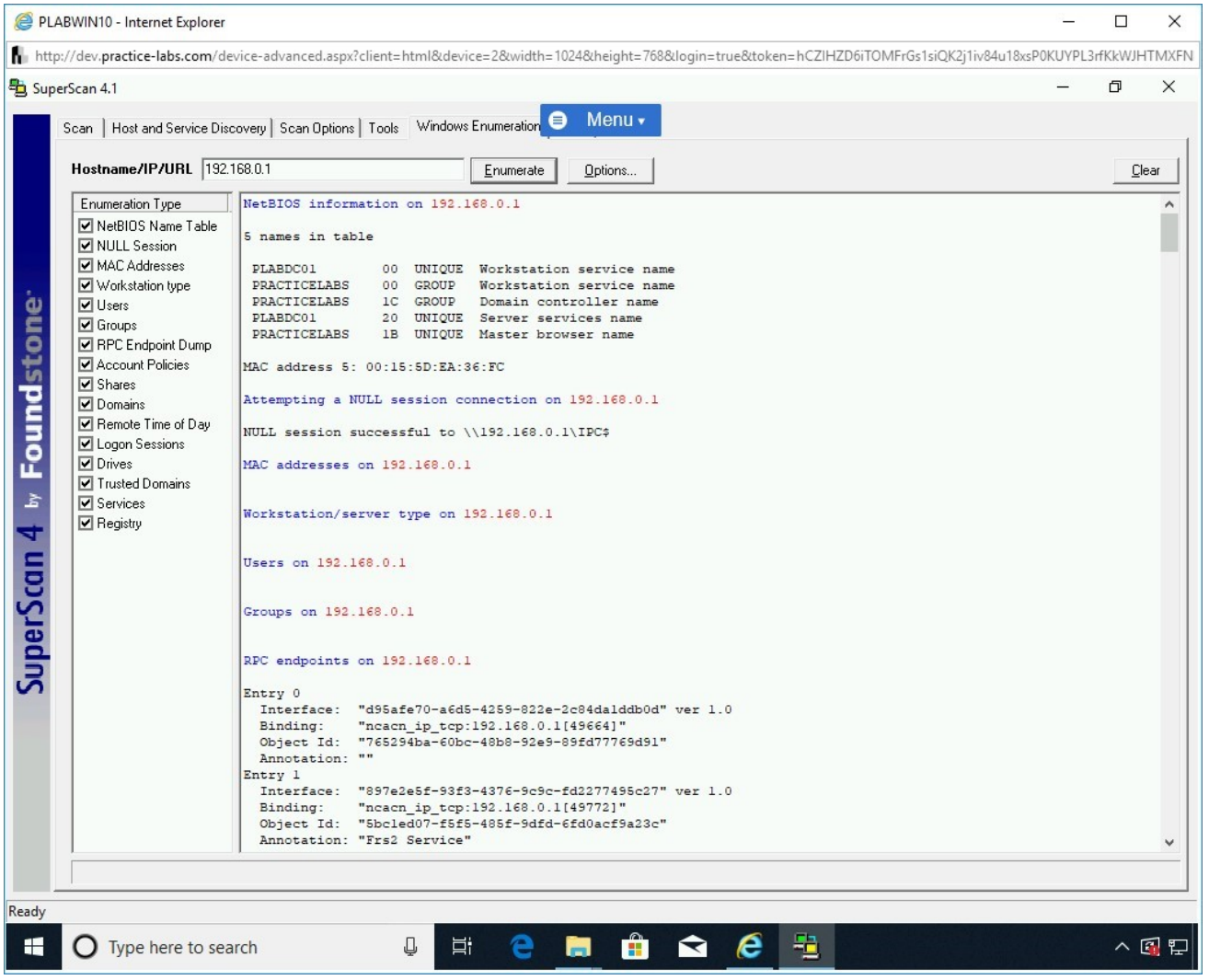


Figure 1.12 Screenshot of PLABWIN10: Showing the results of the enumeration in the right pane.

Step 13

You can view the complete results by scrolling down.

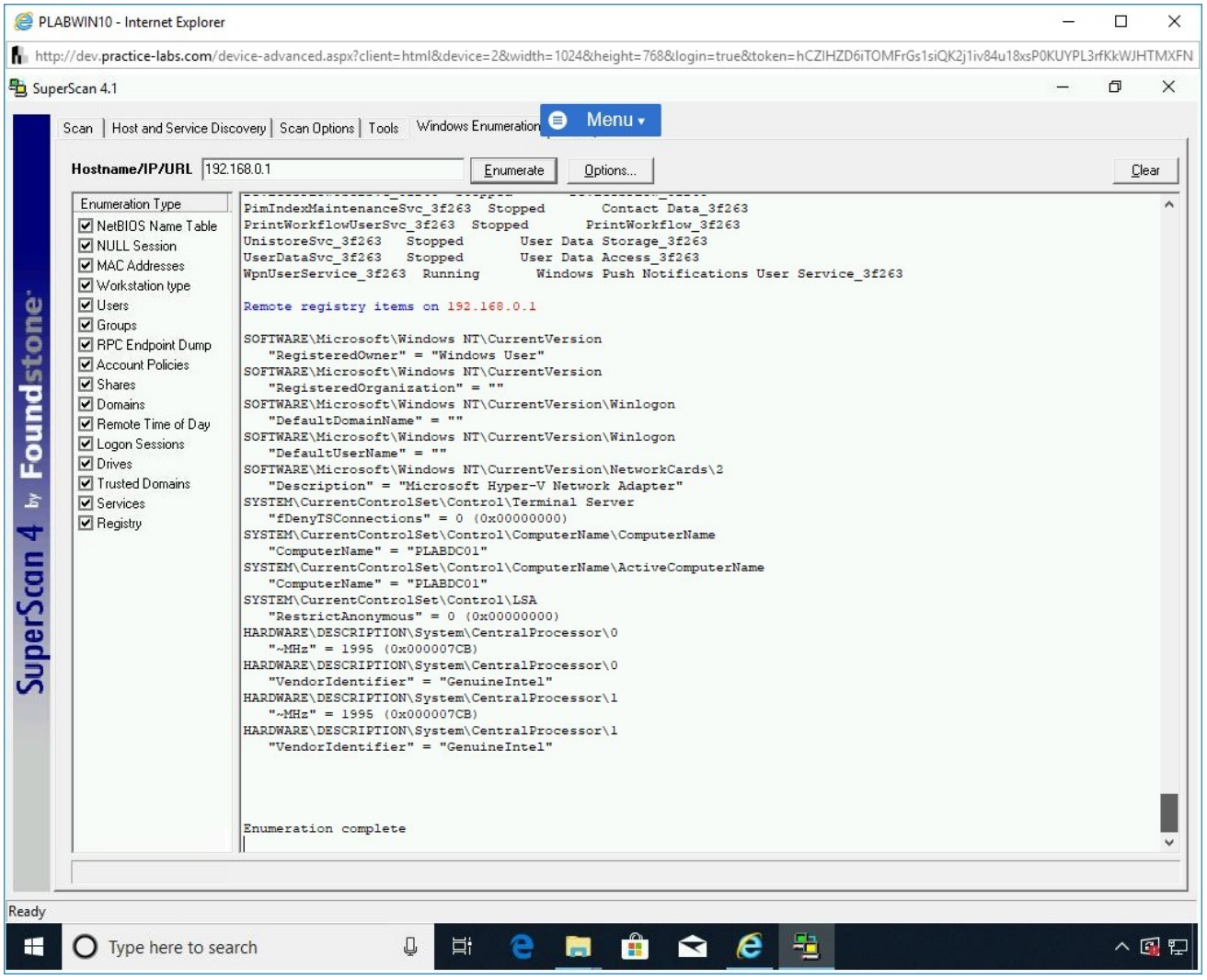


Figure 1.13 Screenshot of PLABWIN10: Showing the results of the enumeration in the right pane.

Step 14

Using **SuperScan**, you can also perform a network scan.

From the **SuperScan 4.1** window, select the **Scan** tab.

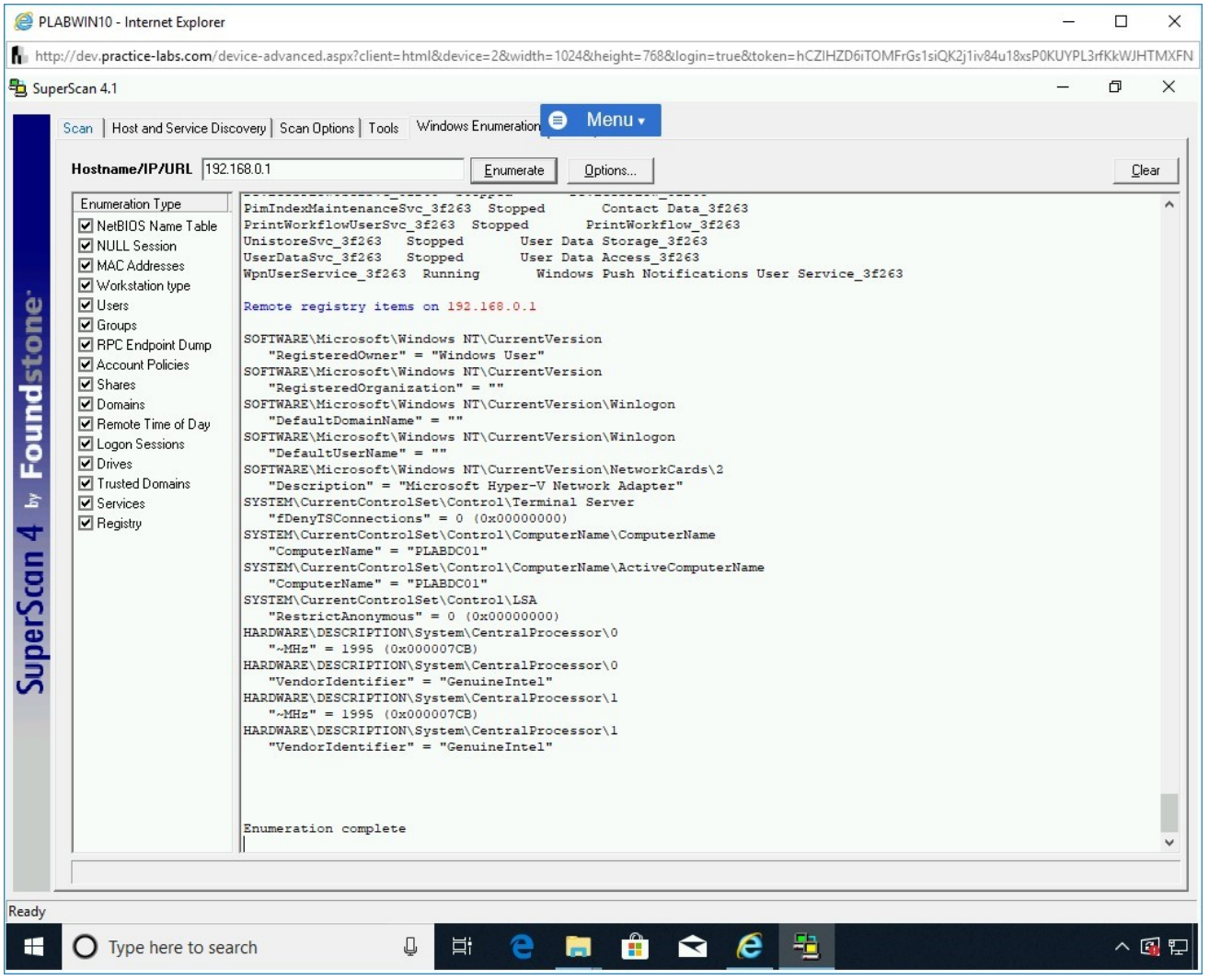


Figure 1.14 Screenshot of PLABWIN10: Clicking the Scan tab.

Step 15

On the **Scan** tab, in the **Start IP** text box, type the following IP address:

```
192.168.0.1
```

Click inside the **End IP** text box. Notice that the **End IP** text information is automatically populated with the following IP address:

```
192.168.0.254
```

Click the middle right arrow to add information in the right text box.

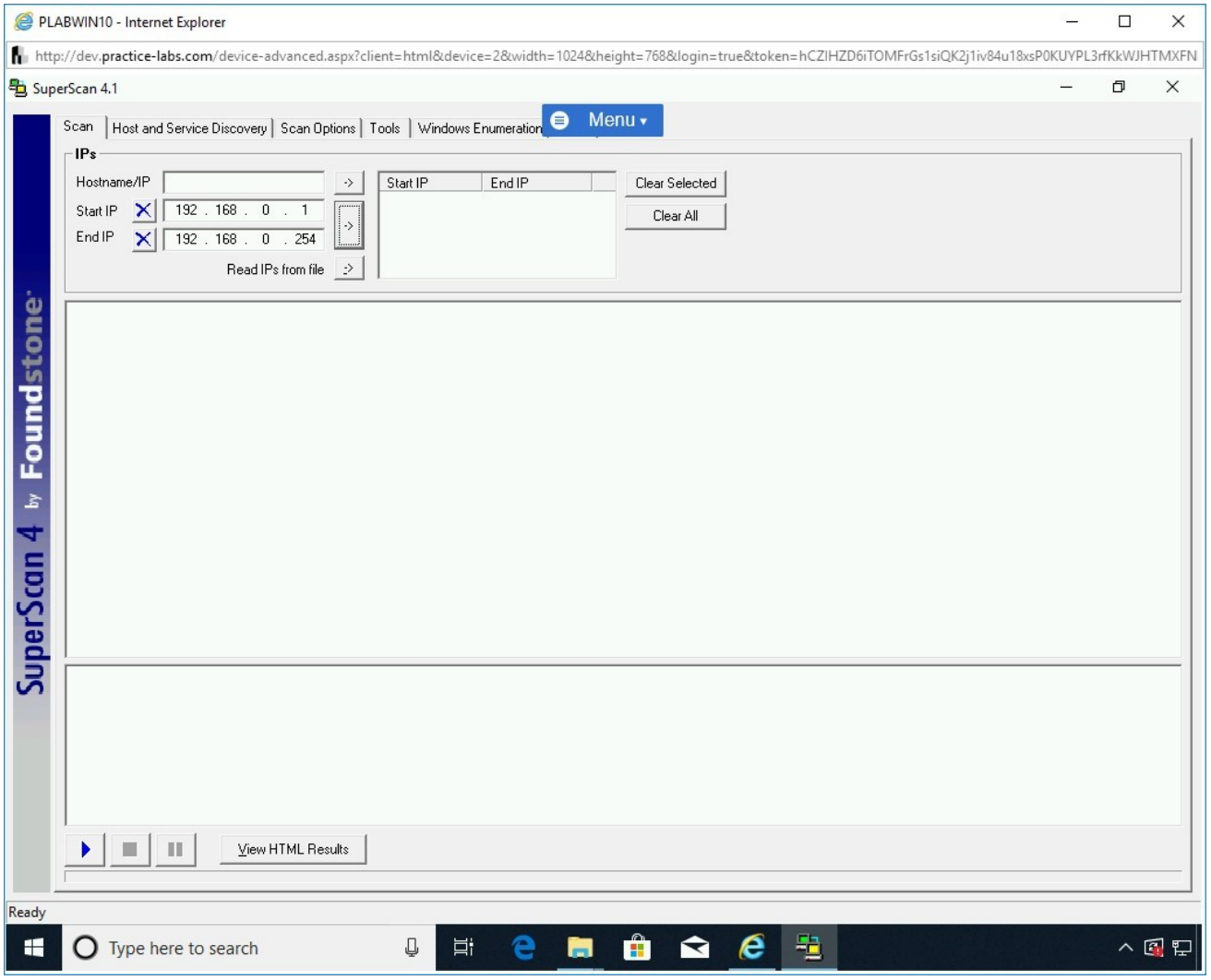


Figure 1.15 Screenshot of PLABWIN10: Entering the range of IP addresses to be scanned.

Step 16

The IP address range is now added in the right text box.

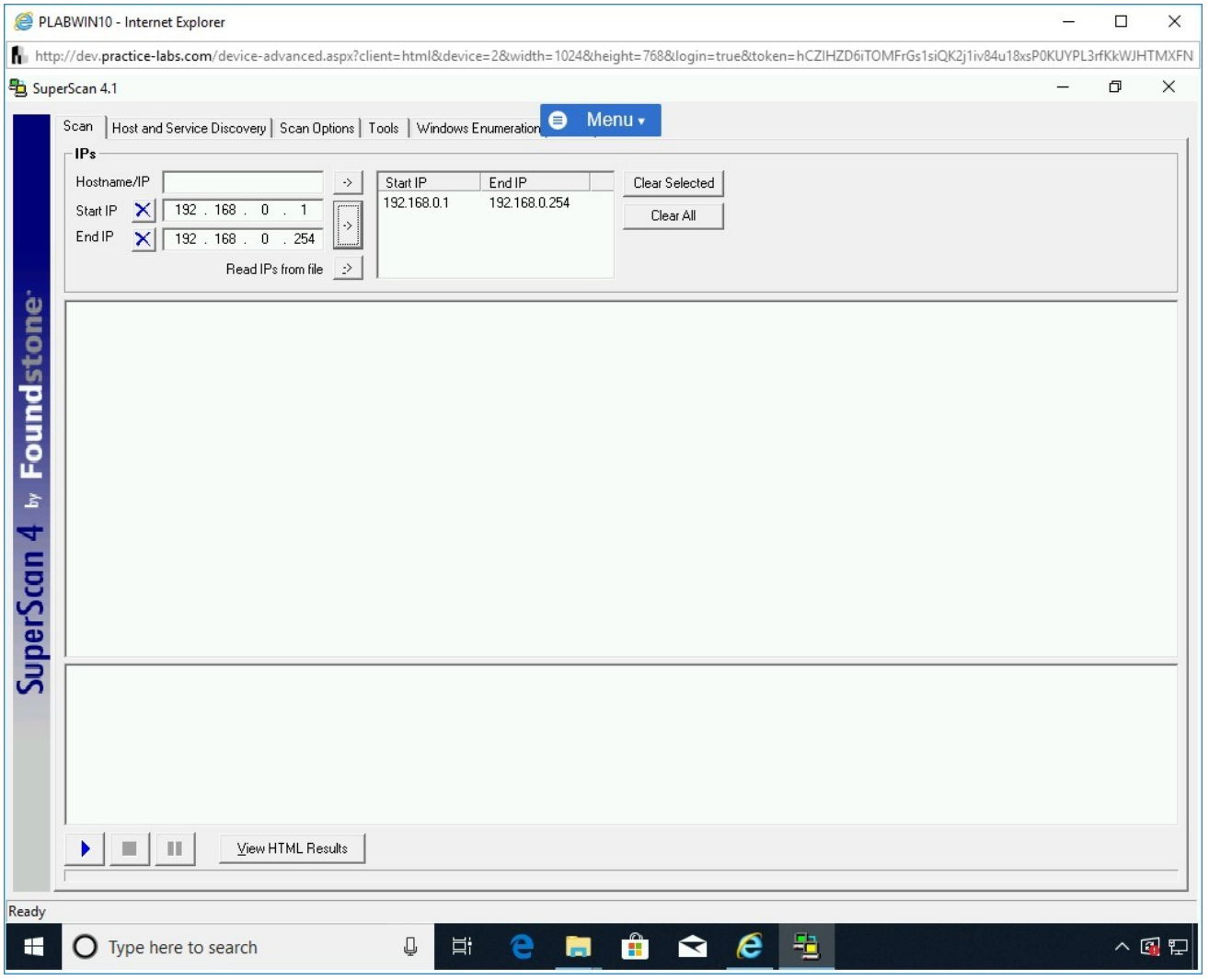


Figure 1.16 Screenshot of PLABWIN10: Adding the range of IP addresses in the right box.

Step 17

Minimize the **SuperScan 4.1** window and all other open windows.

Before proceeding, you will need to disable the firewall, click **Start**.

In the **Type here to search** text box, type the following:

```
Windows Defender Firewall with Advanced Security
```

Click on **Windows Firewall with Advanced Security**.

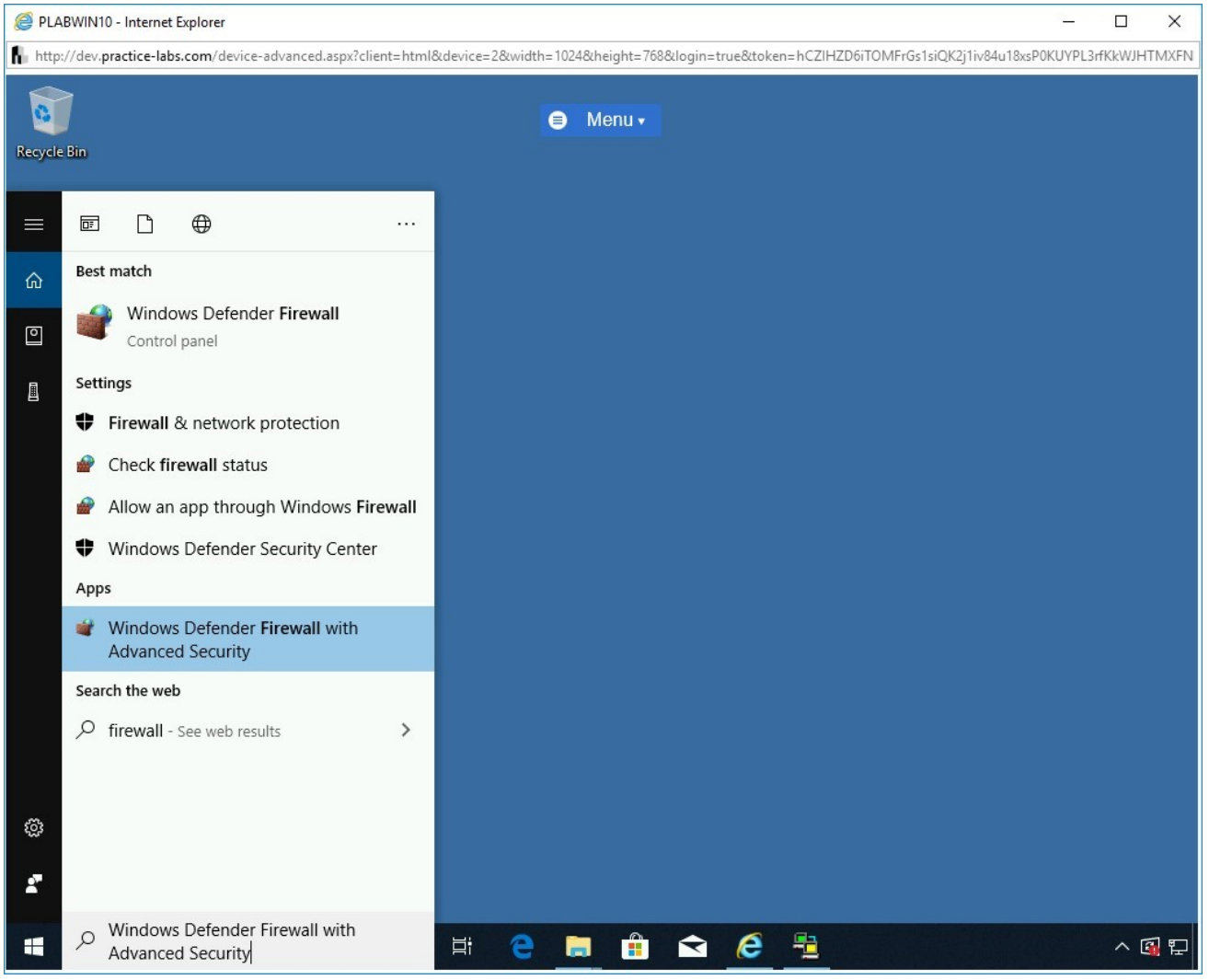


Figure 1.17 Screenshot of PLABWIN10: Selecting Windows Defender Firewall with Advanced Security from the search results.

Step 18

The **Windows Defender Firewall with Advanced Security** window is displayed. You will notice that only the **Domain Profile** is Active, click **Windows Defender Firewall Properties** link in the middle pane.

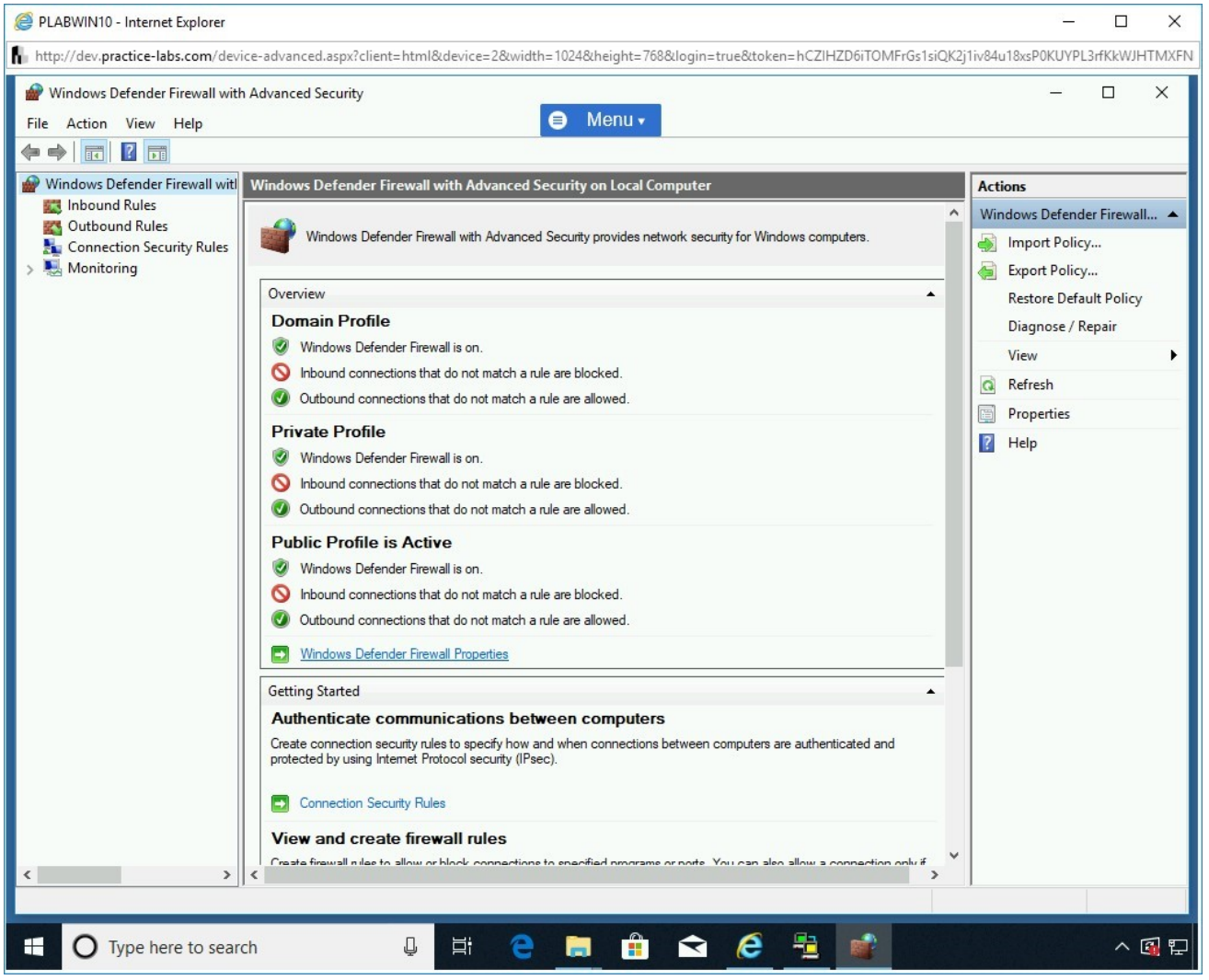


Figure 1.18 Screenshot of PLABWIN10: Clicking Windows Defender Firewall Properties link in the middle pane.

Step 19

On the **Windows Defender Firewall with Advanced Security on Local Computer Properties** dialog box, the **Domain Profile** tab is displayed.

You need to change the **Firewall state** to **Off**. Click the **Firewall state** drop-down and select **Off**.

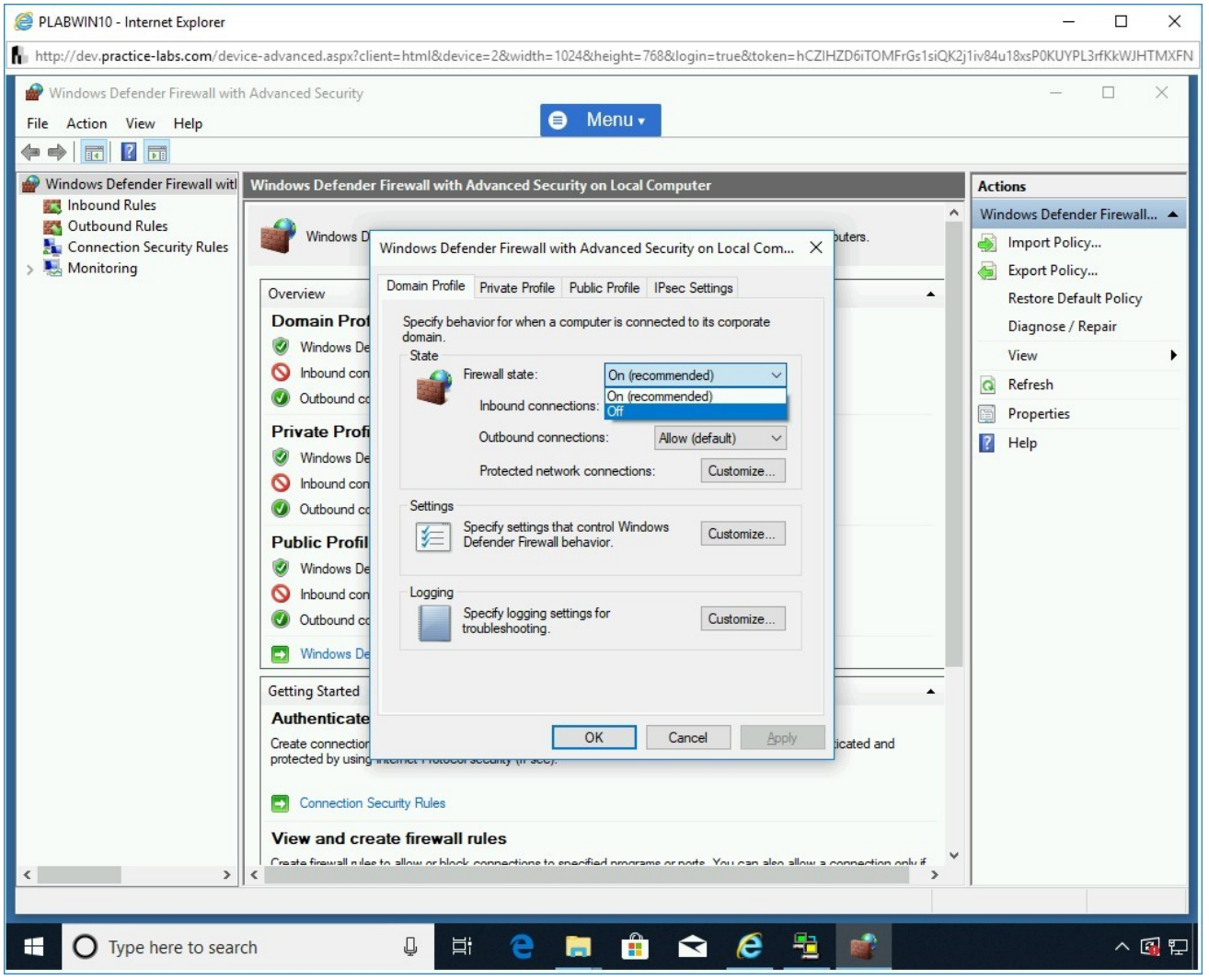


Figure 1.19 Screenshot of PLABWIN10: Turning the firewall off for the Domain profile by selecting Off from the Firewall state drop-down

Step 20

After the Firewall state is set to **Off**, click the **Private Profile** tab.

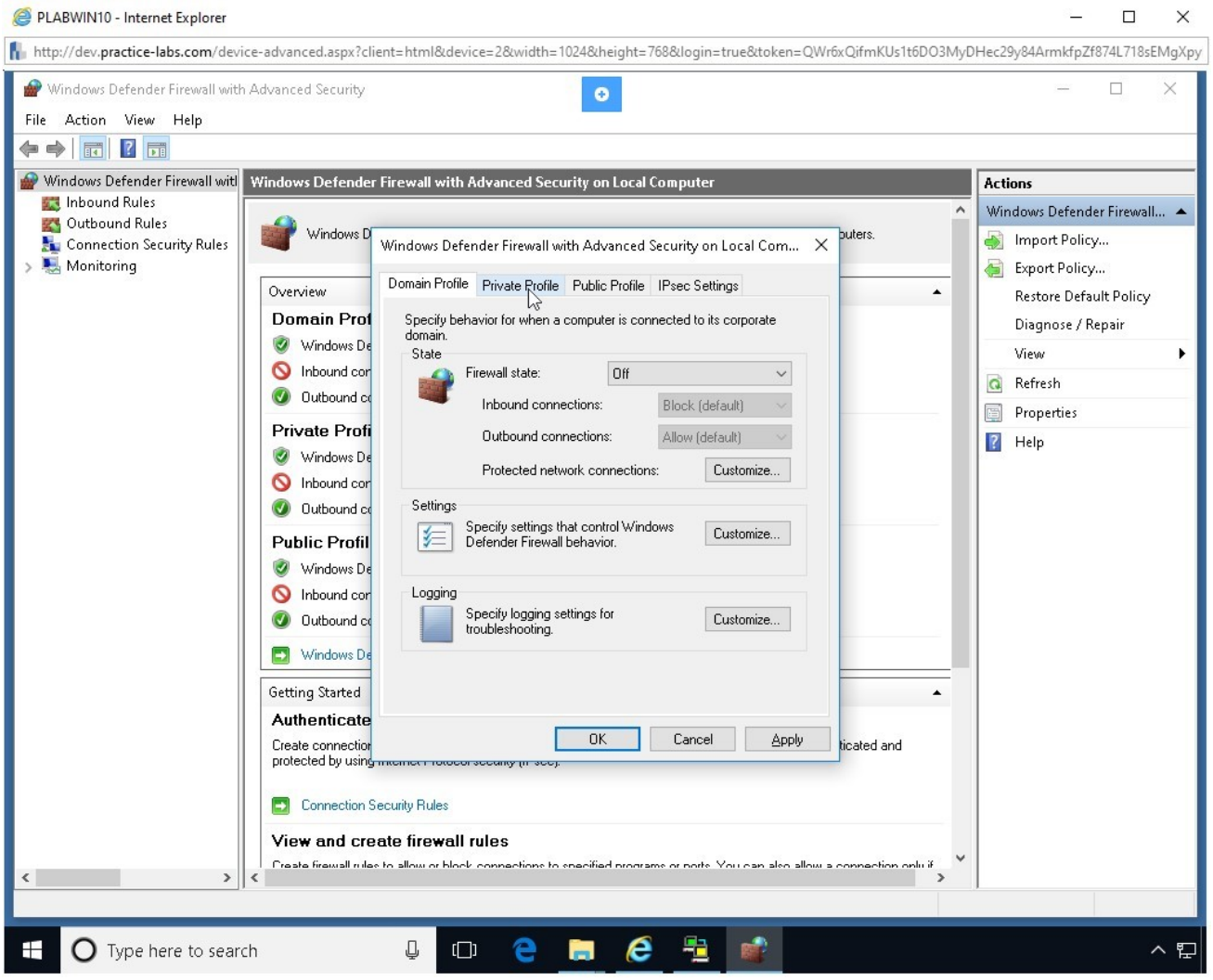


Figure 1.20 Screenshot of PLABWIN10: Displaying the Off status for firewall on the Domain Profile tab and then clicking the Private Profile tab.

Step 21

You need to change the **Firewall state** to **Off**. Click the **Firewall state** drop-down and select **Off**.

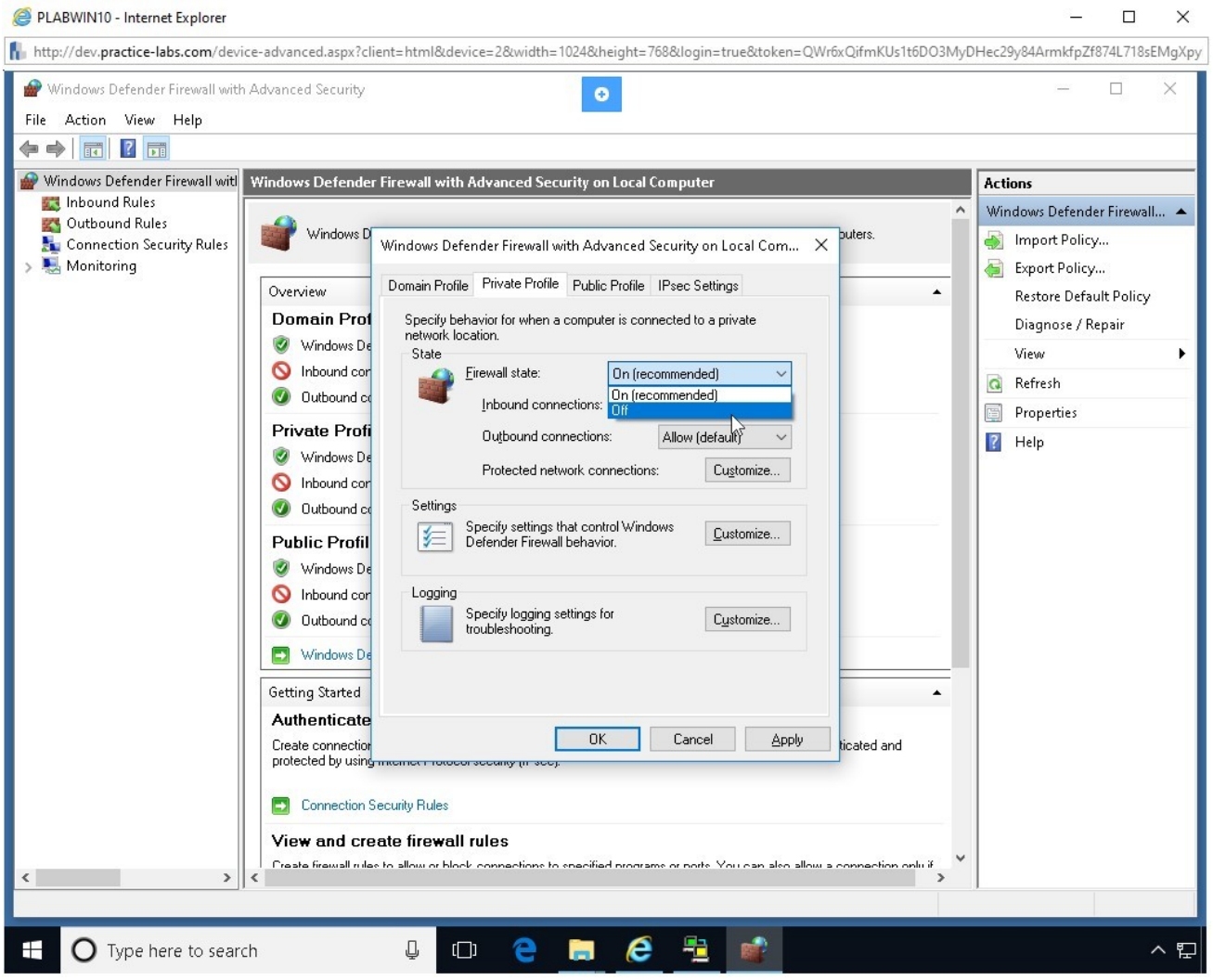


Figure 1.21 Screenshot of PLABWIN10: Turning the firewall off for the Private Profile tab by selecting Off from the Firewall state drop-down.

Step 22

After the Firewall state is set to **Off**, click the **Public Profile** tab.

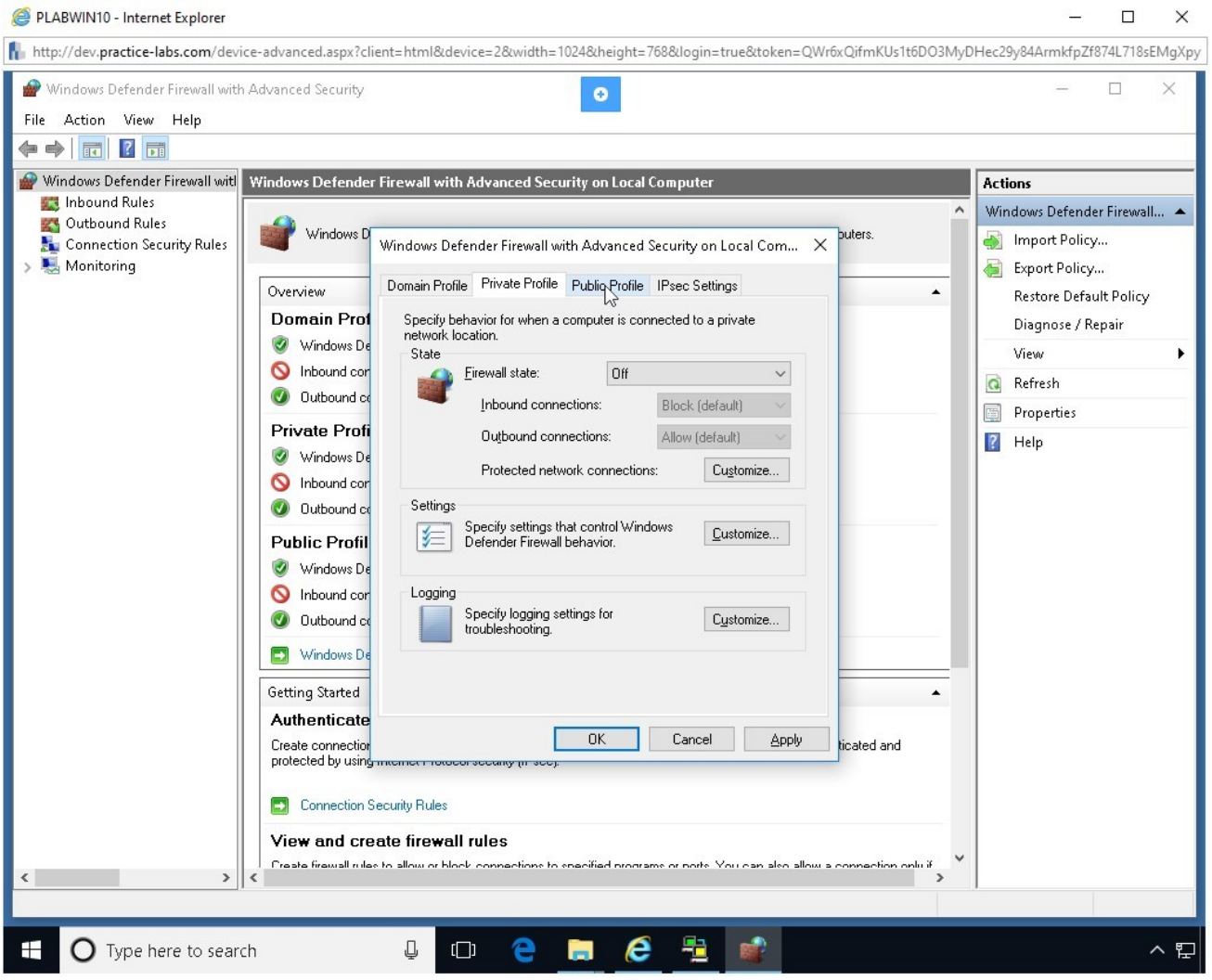


Figure 1.22 Screenshot of PLABWIN10: Displaying the Off status for firewall on the Private Profile tab and then clicking the Public Profile tab.

Step 23

You need to change the **Firewall state** to **Off**. Click the **Firewall state** drop-down and select **Off**.

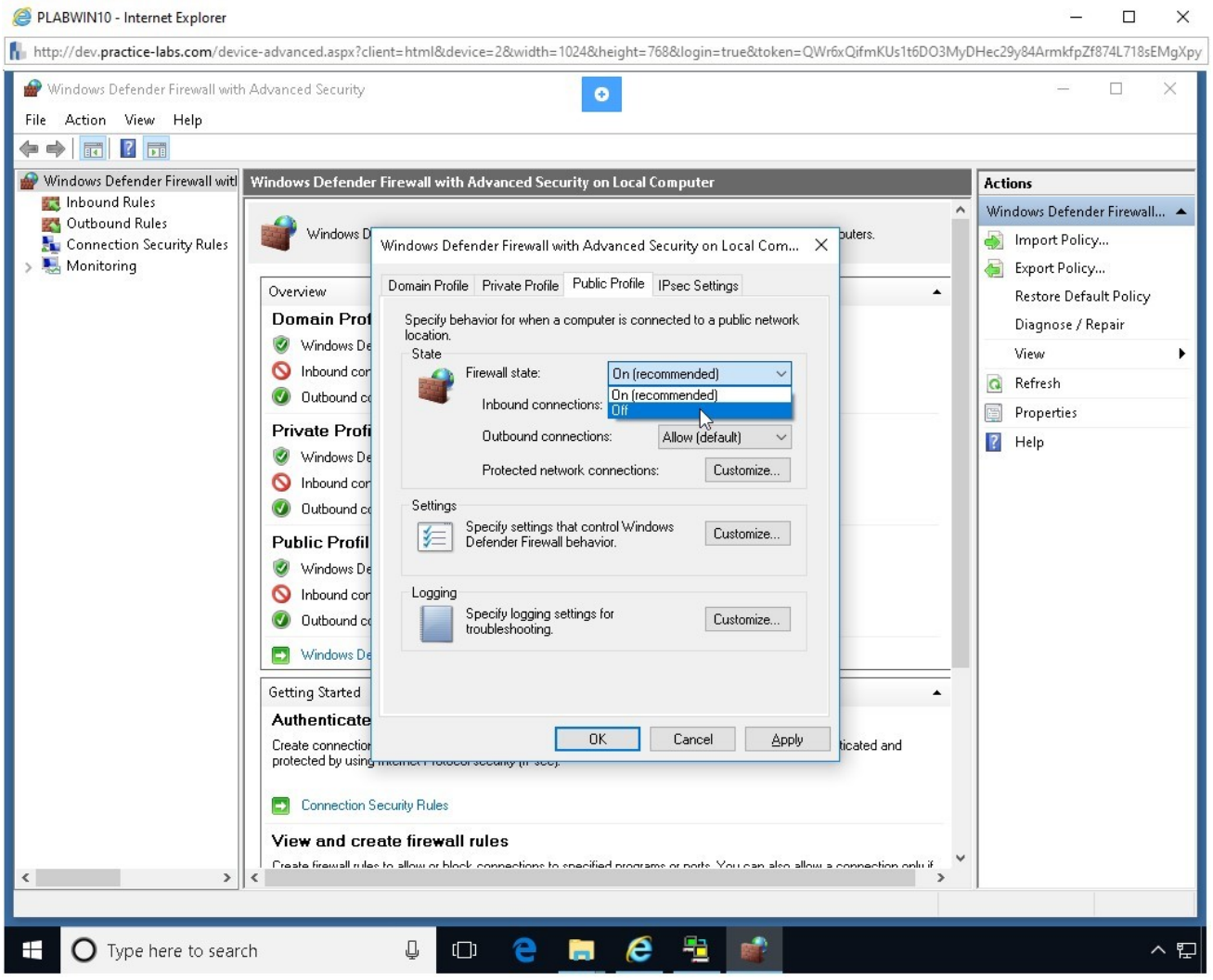


Figure 1.23 Screenshot of PLABWIN10: Turning the firewall off for the Public Profile by selecting Off from the Firewall state drop-down.

Step 24

After the firewall has been turned off on all three tabs, **Domain Profile**, **Private Profile**, and **Public Profile**, click **OK**.

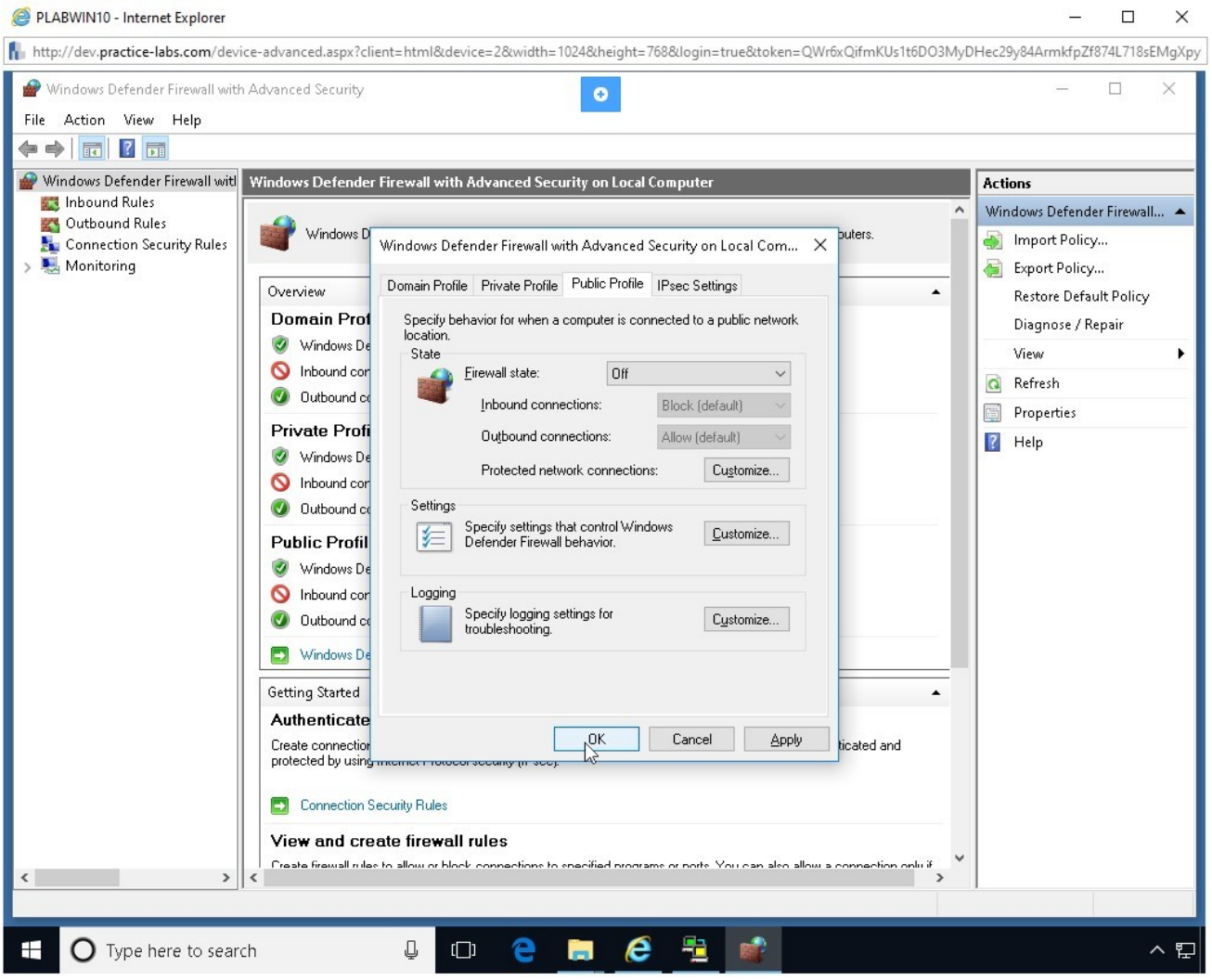


Figure 1.24 Screenshot of PLABWIN10: Clicking OK on the dialog box after turning off the firewall for all three profiles.

Step 25

Close the **Windows Defender Firewall with Advanced Security** window.

> ***Note:*** *In a production environment, you would not do this as it exposes the device to a number of threats.*

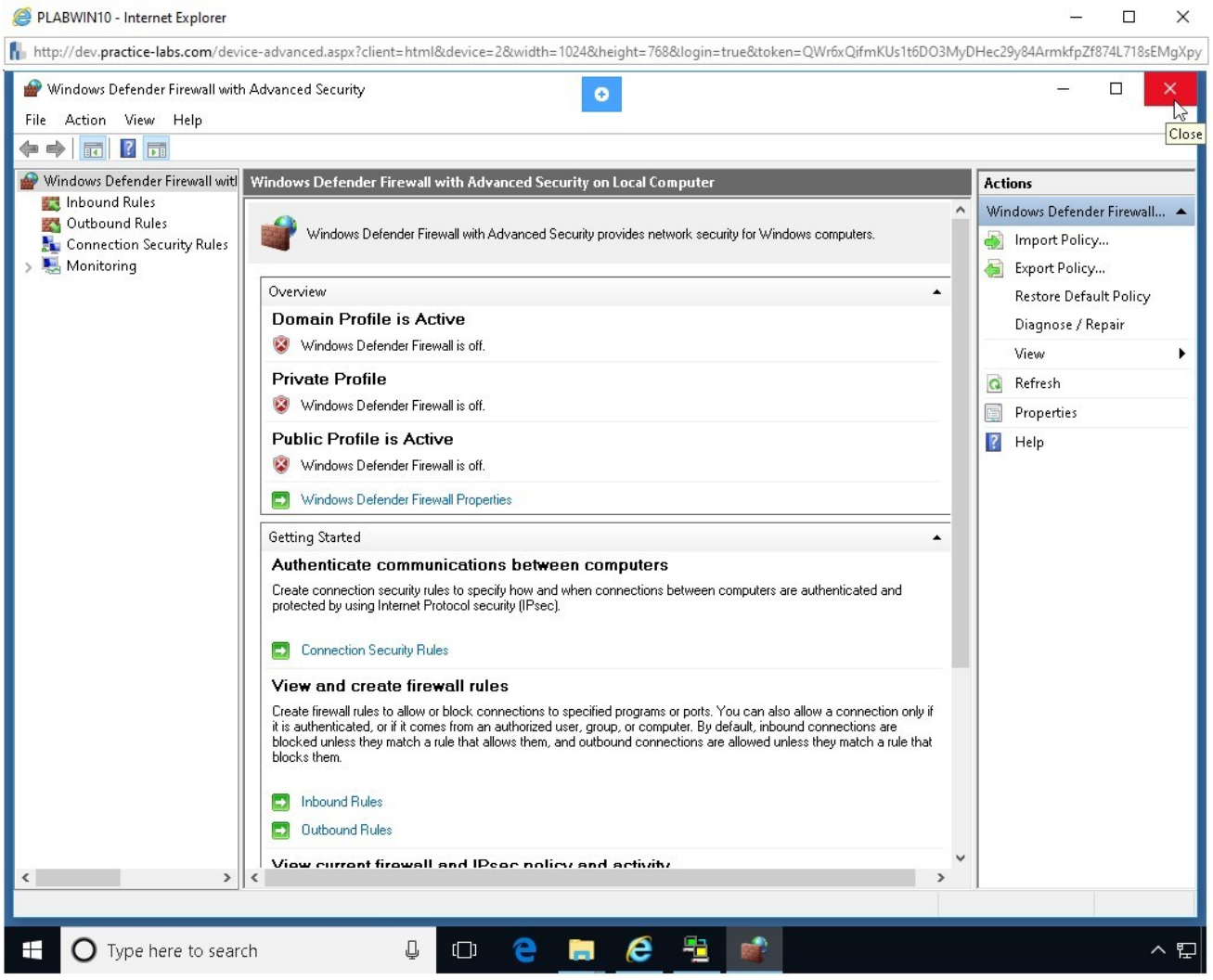


Figure 1.25 Screenshot of PLABWIN10: Closing the Windows Defender Firewall with Advanced Security window.

Step 26

Minimize **PLABWIN10** and connect to **PLABDC01**.

The **Server Manager** window is displayed. Click **Close**.

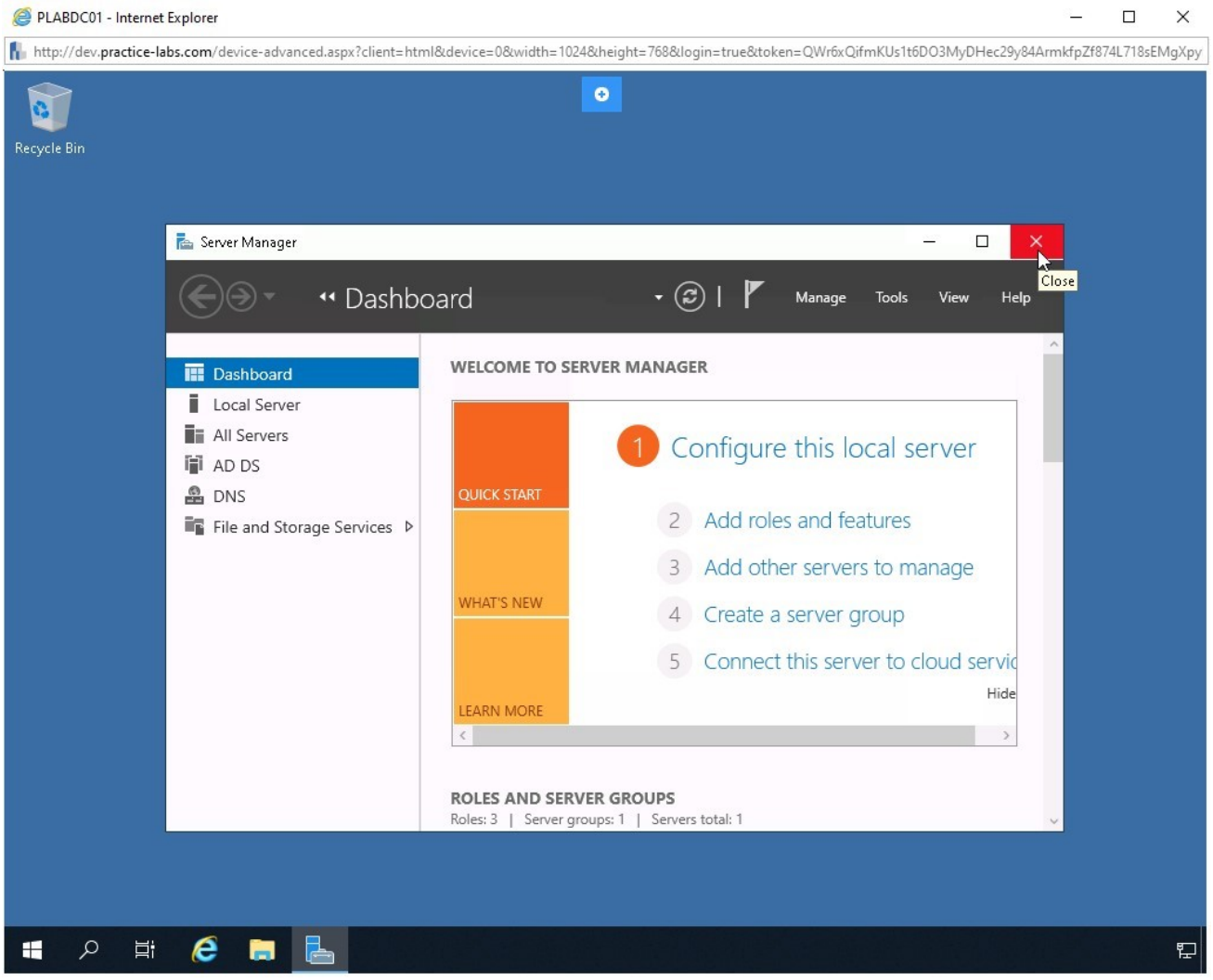


Figure 1.26 Screenshot of PLABDC01: Closing the Server Manager window in PLABDC01.

Step 27

Right-click the Windows charm and select **Windows PowerShell (Admin)**.

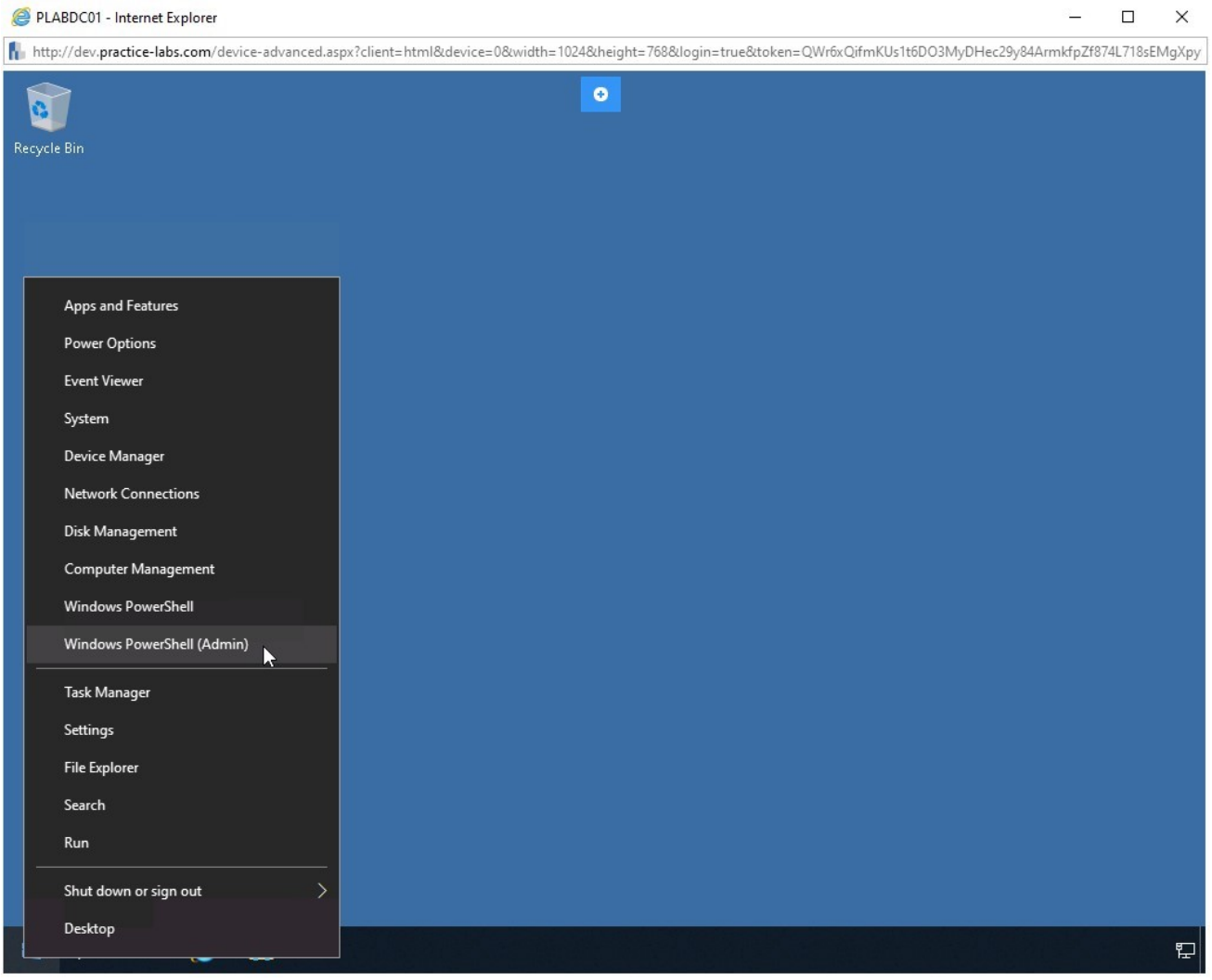


Figure 1.27 Screenshot of PLABDC01: Right-clicking the Windows charm and then selecting Windows PowerShell (Admin).

Step 28

Using a PowerShell cmdlet, you will turn off the firewall on PLABDC01. You can turn off all three profiles using a single command. To do this, type the following command:

```
Set-NetFirewallProfile -Profile Domain,Public,Private -
Enabled False
```

Press **Enter**.

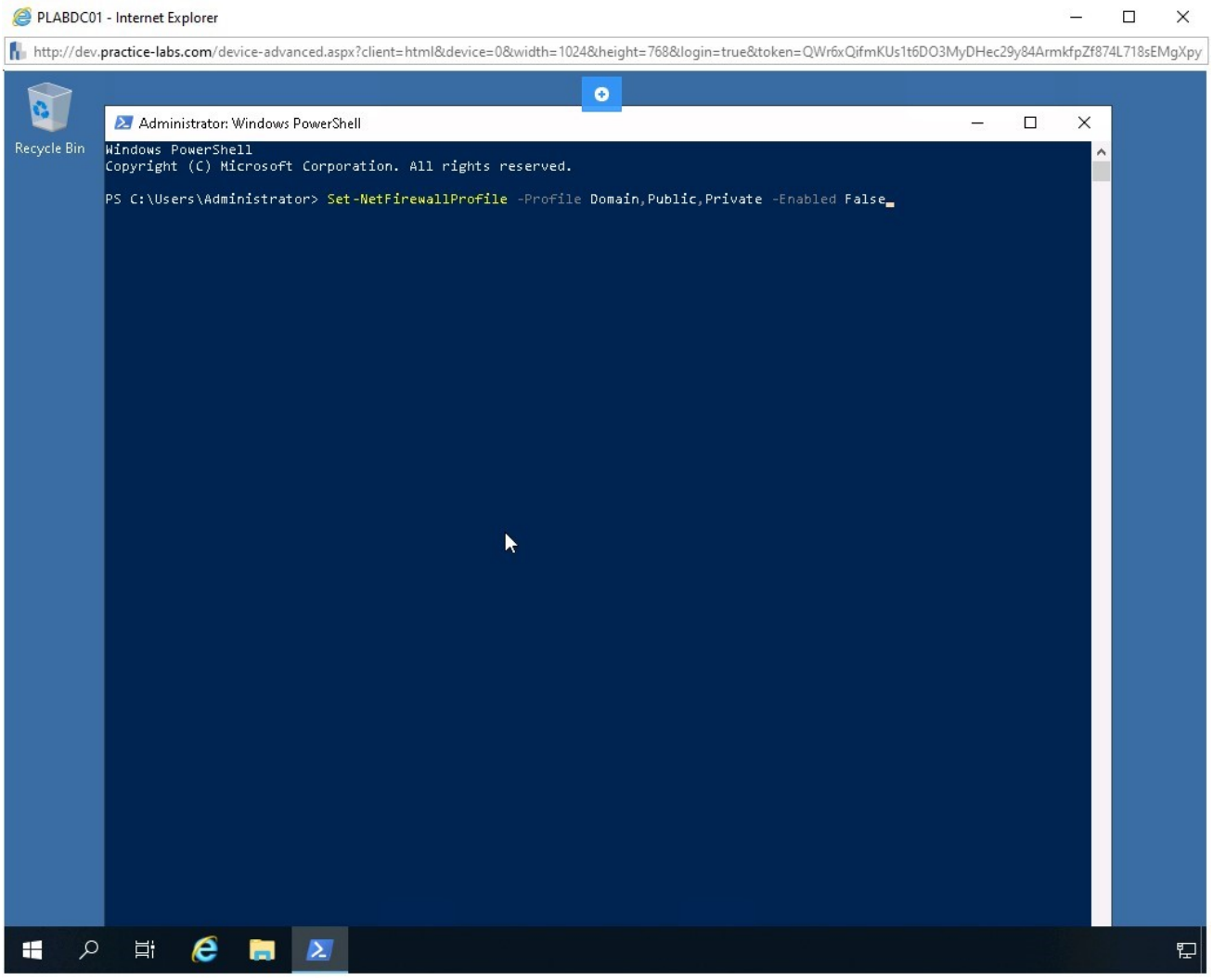


Figure 1.28 Screenshot of PLABDC01: Executing the command to turn off firewall in the PowerShell terminal.

Step 29

Notice that the command does not return any output. Windows Firewall is now switched off.

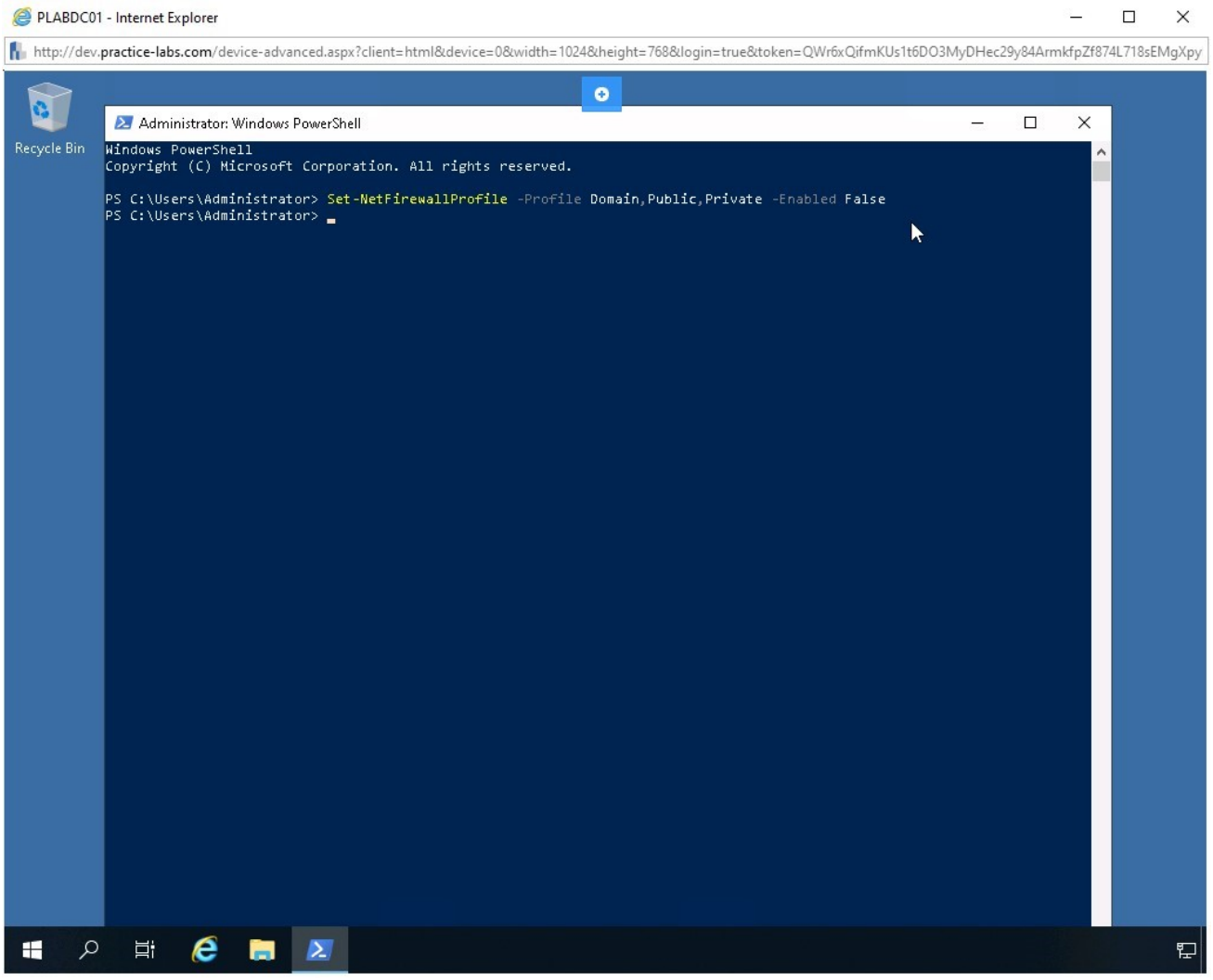


Figure 1.29 Screenshot of PLABDC01: Displaying the successful execution of the command in PowerShell terminal.

Step 30

To exit from the PowerShell window, type the following command:

```
exit
```

Press **Enter**.

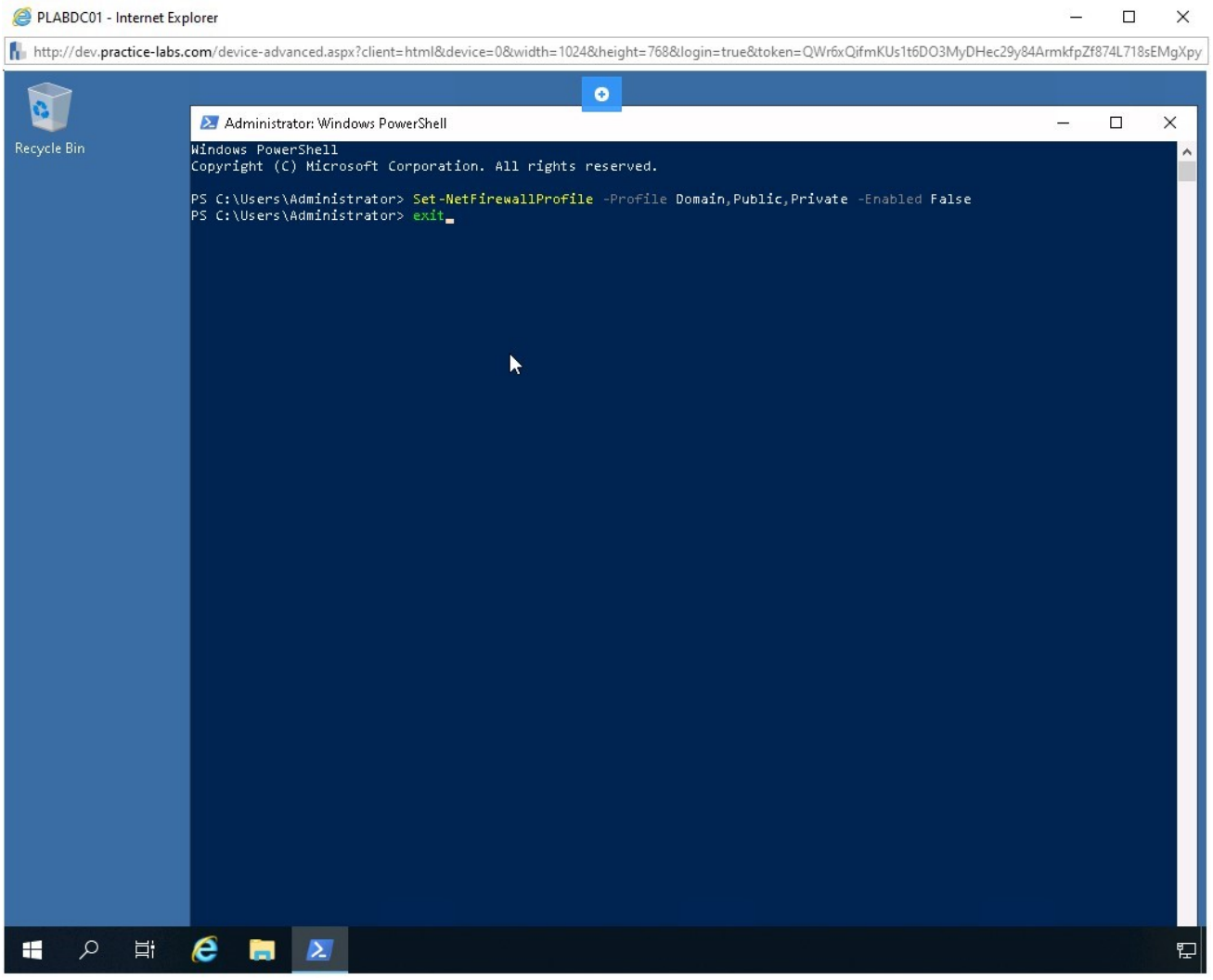


Figure 1.30 Screenshot of PLABDC01: Exiting from the PowerShell terminal by entering the exit command.

Step 31

Minimize **PLABDC01** and connect to **PLABDM01**.

The **Server Manager** window is displayed. Click **Close**.

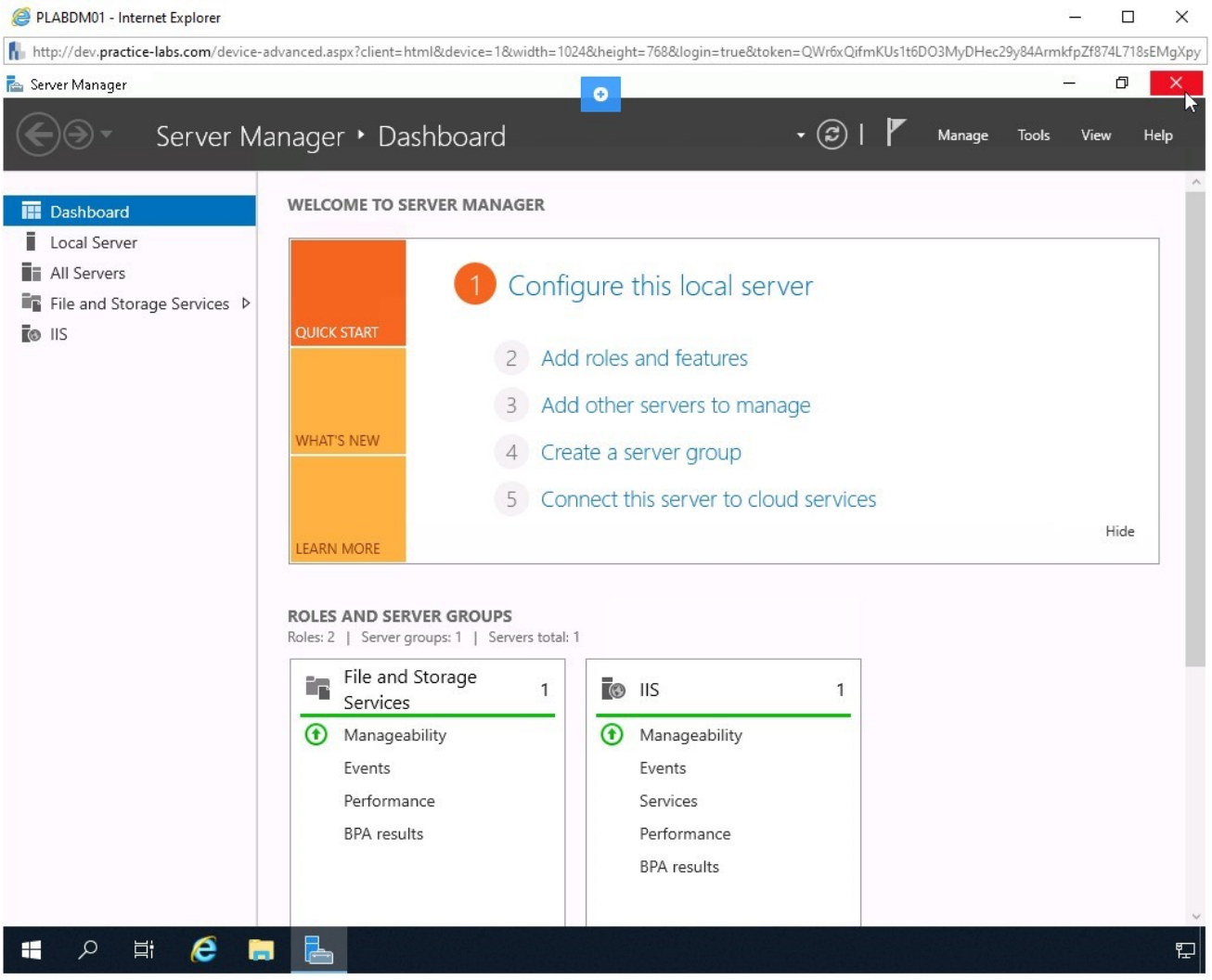


Figure 1.31 Screenshot of PLABDM01: Closing the Server Manager window in PLABDM01.

Step 32

Right-click the Windows charm and select **Windows PowerShell (Admin)**.

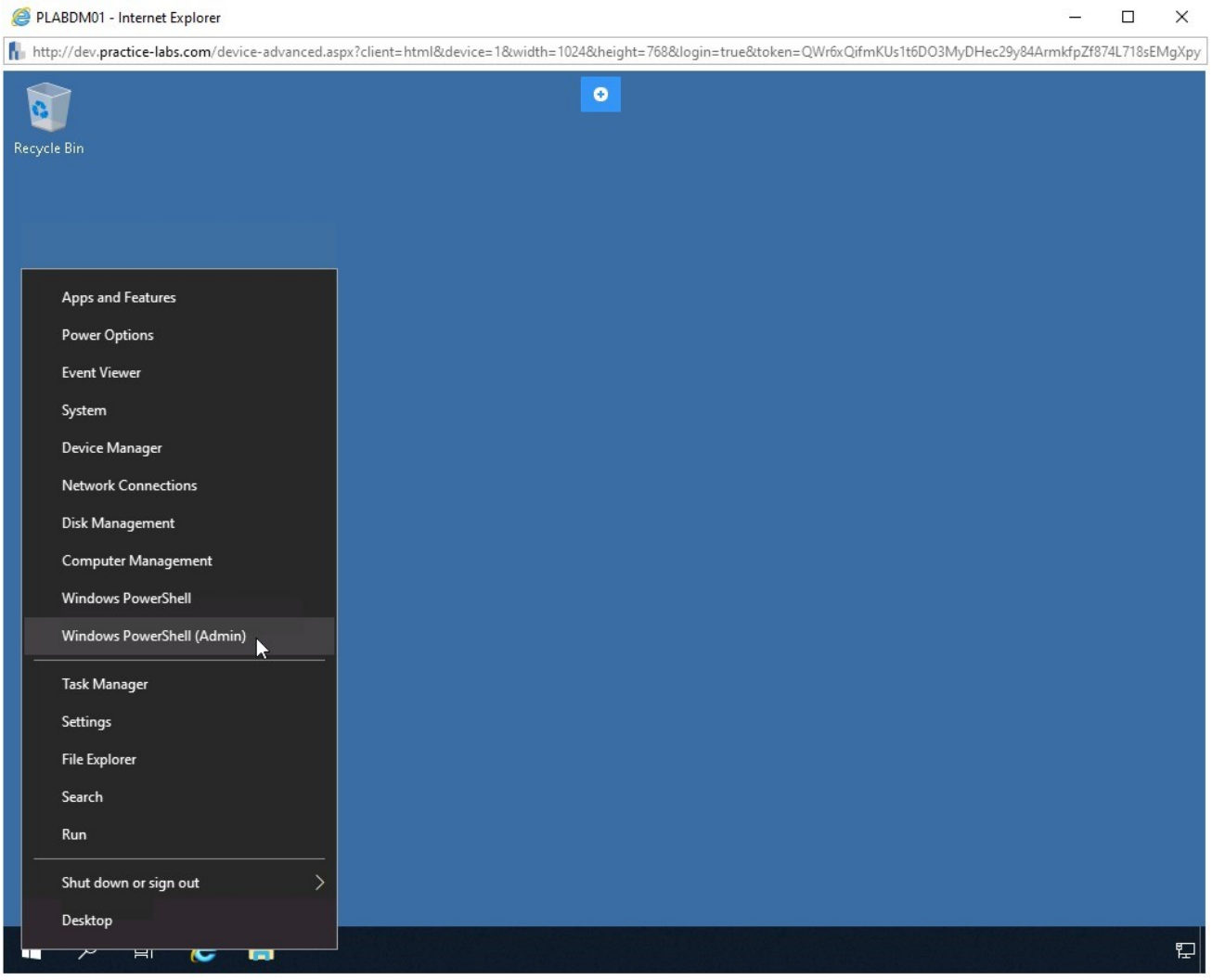


Figure 1.32 Screenshot of PLABDM01: Right-clicking the Windows charm and then selecting Windows PowerShell (Admin).

Step 33

Using a PowerShell cmdlet, you will turn off the firewall on PLABDC01. You can turn off all three profiles using a single command. To do this, type the following command:

```
Set-NetFirewallProfile -Profile Domain,Public,Private -
Enabled False
```

Press **Enter**.

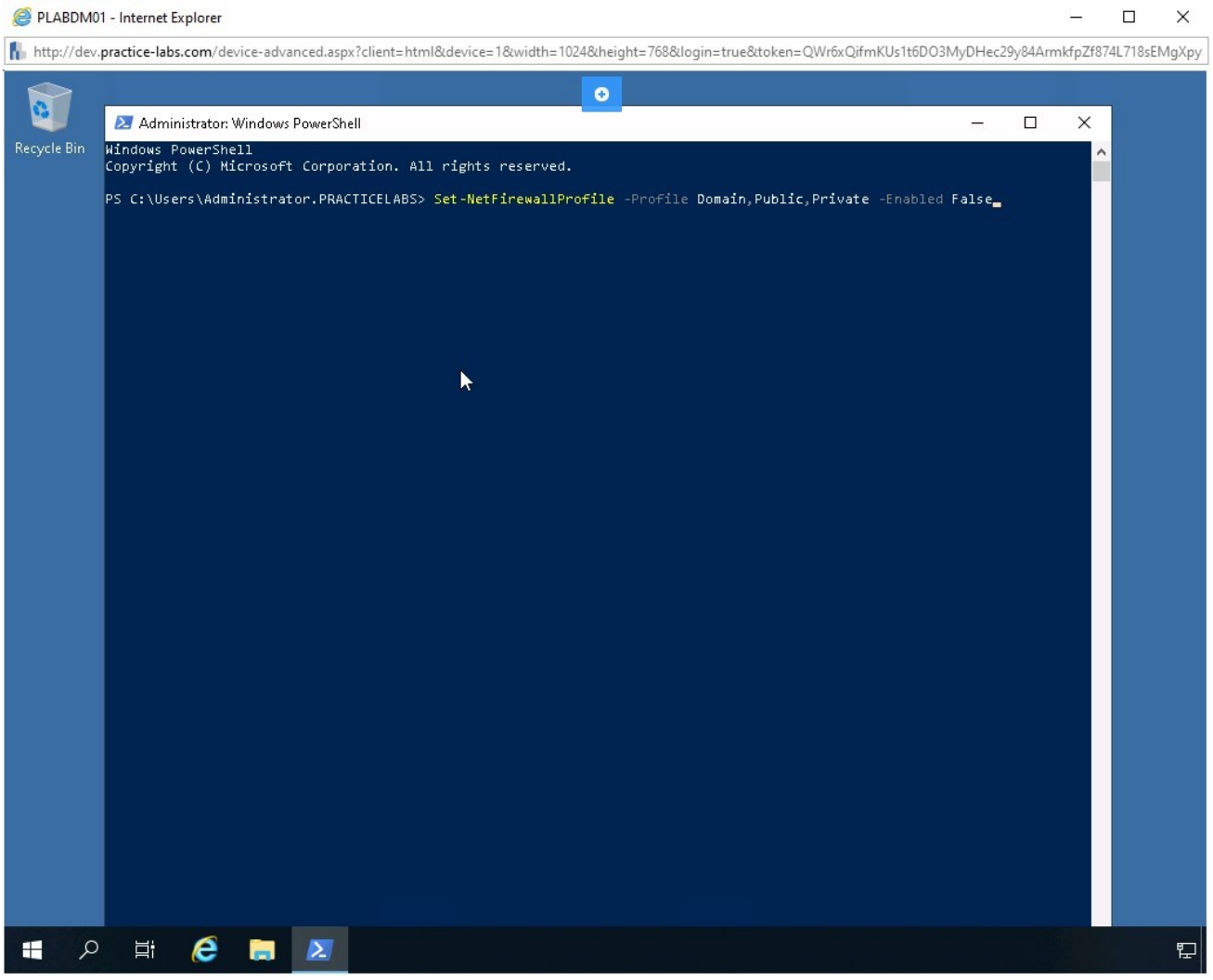


Figure 1.33 Screenshot of PLABDM01: Executing the command to turn off firewall in the PowerShell terminal.

Step 34

Notice that the command does not return any output. Windows Firewall is now switched off.

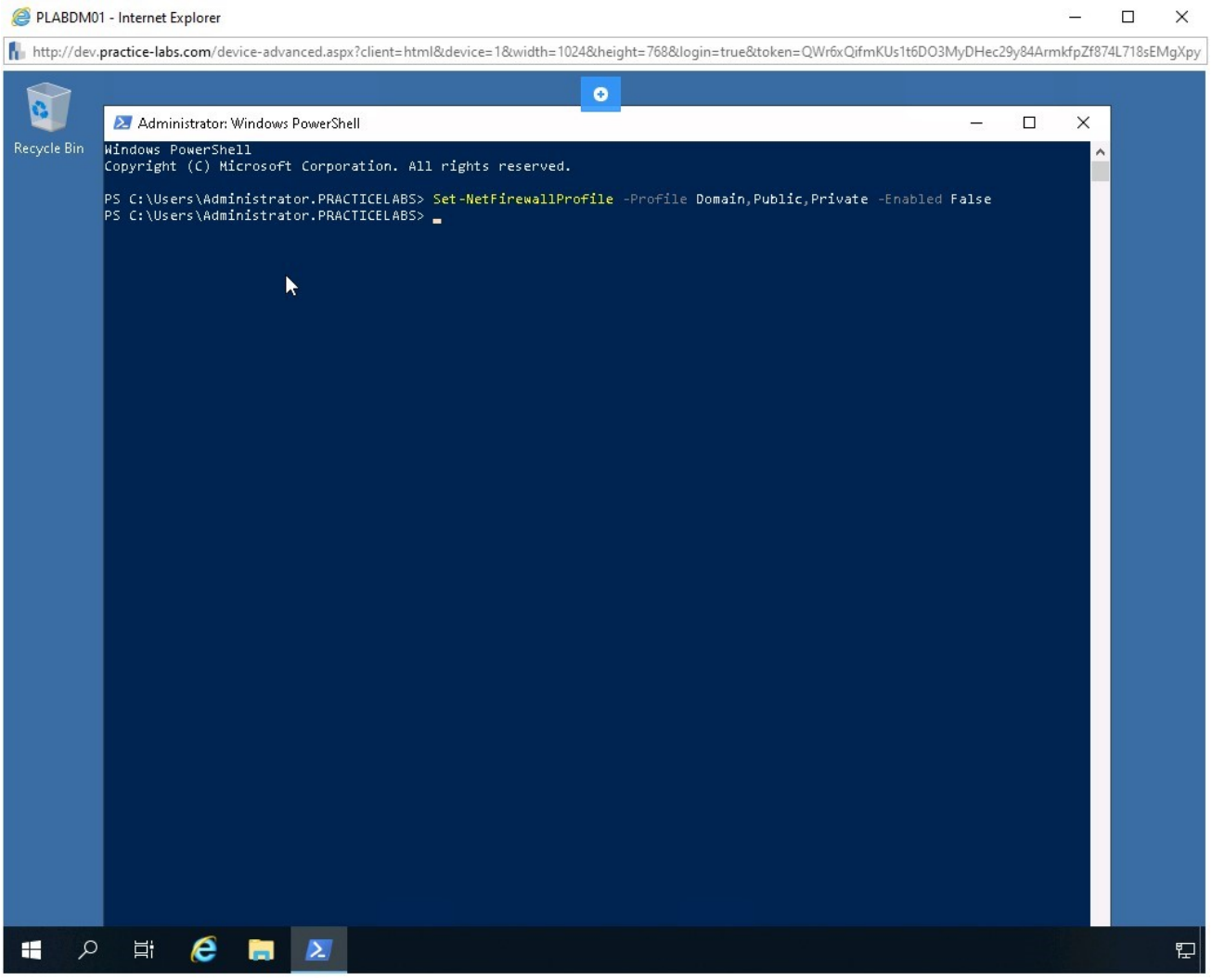


Figure 1.34 Screenshot of PLABDM01: Displaying the successful execution of the command in PowerShell terminal.

Step 35

To exit from the PowerShell window, type the following command:

```
exit
```

Press **Enter**.

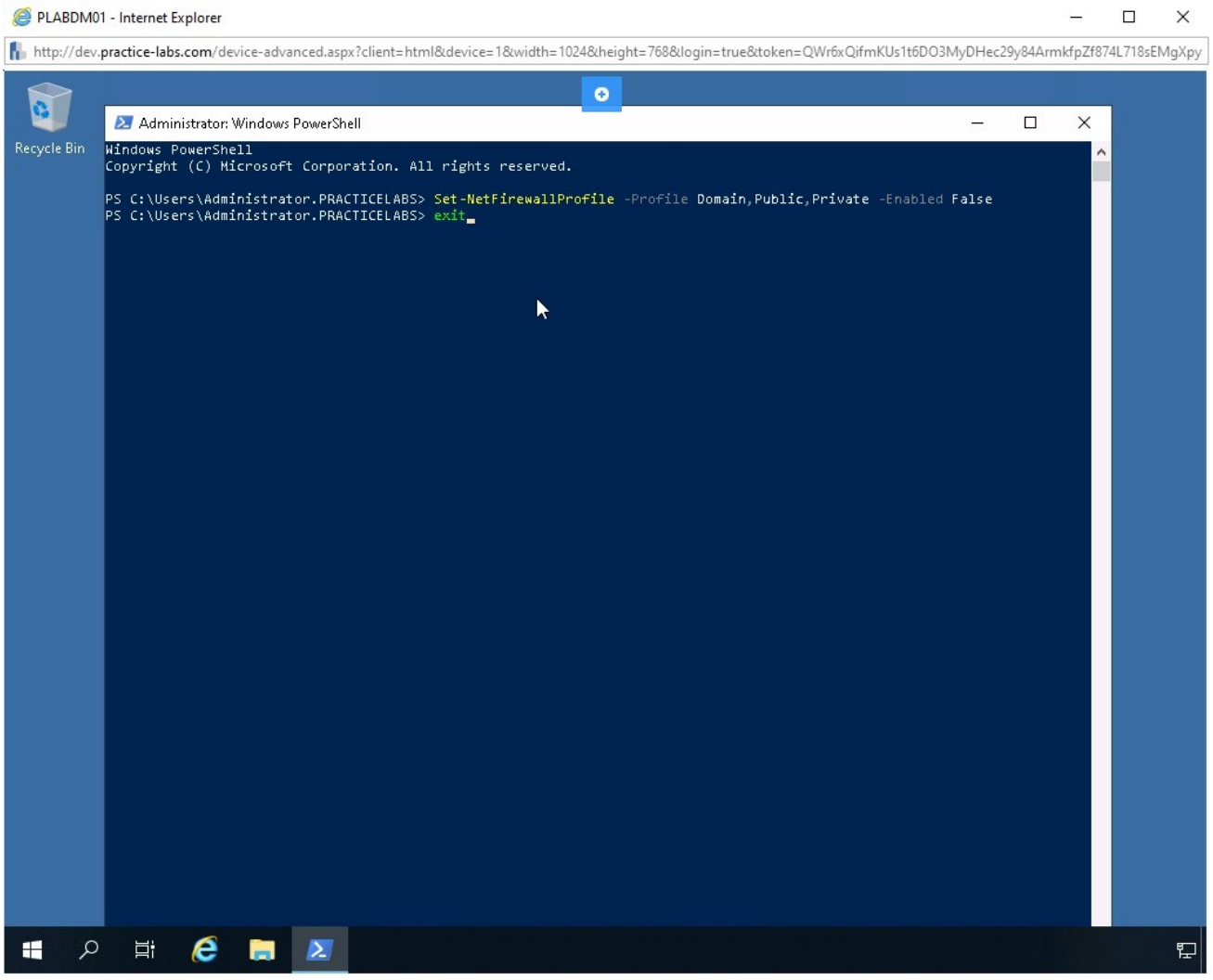


Figure 1.35 Screenshot of PLABDM01: Exiting from the PowerShell terminal by entering the exit command.

Step 36

Switch back to **PLABWIN10**. Restore the **SuperScan 4.1** window from the taskbar and click the **Play** button in the bottom section.

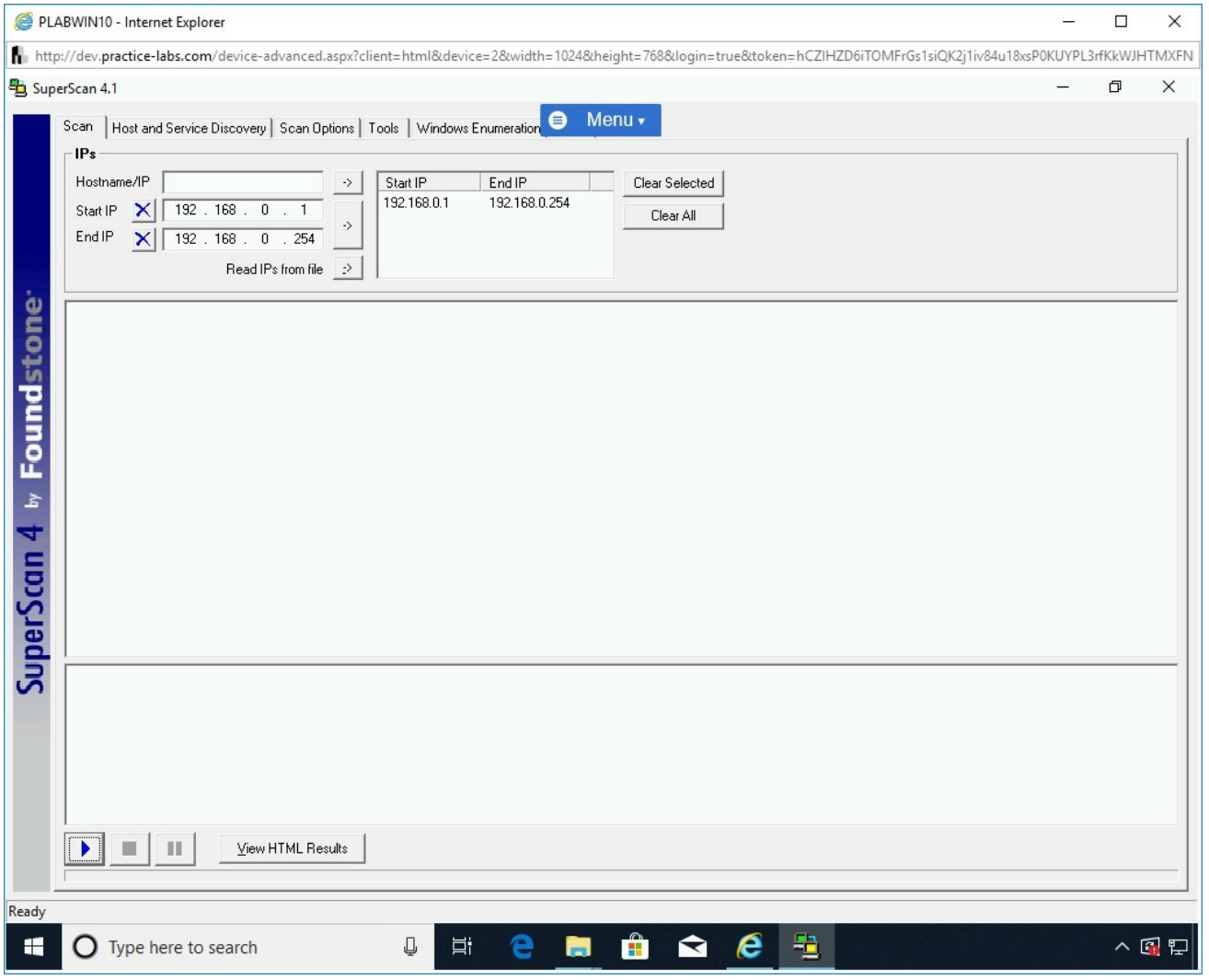


Figure 1.36 Screenshot of PLABWIN10: Restoring the SuperScan 4.1 window from the taskbar and clicking the Play button in the bottom section.

Step 37

Note that the network scan of the defined IP address range has started.

Once the scan is completed, and the progress bar has reached the end, a detailed report is displayed.

You need to read through the generated report by **SuperScan**.

Click the **Tools** tab to proceed to the next step.

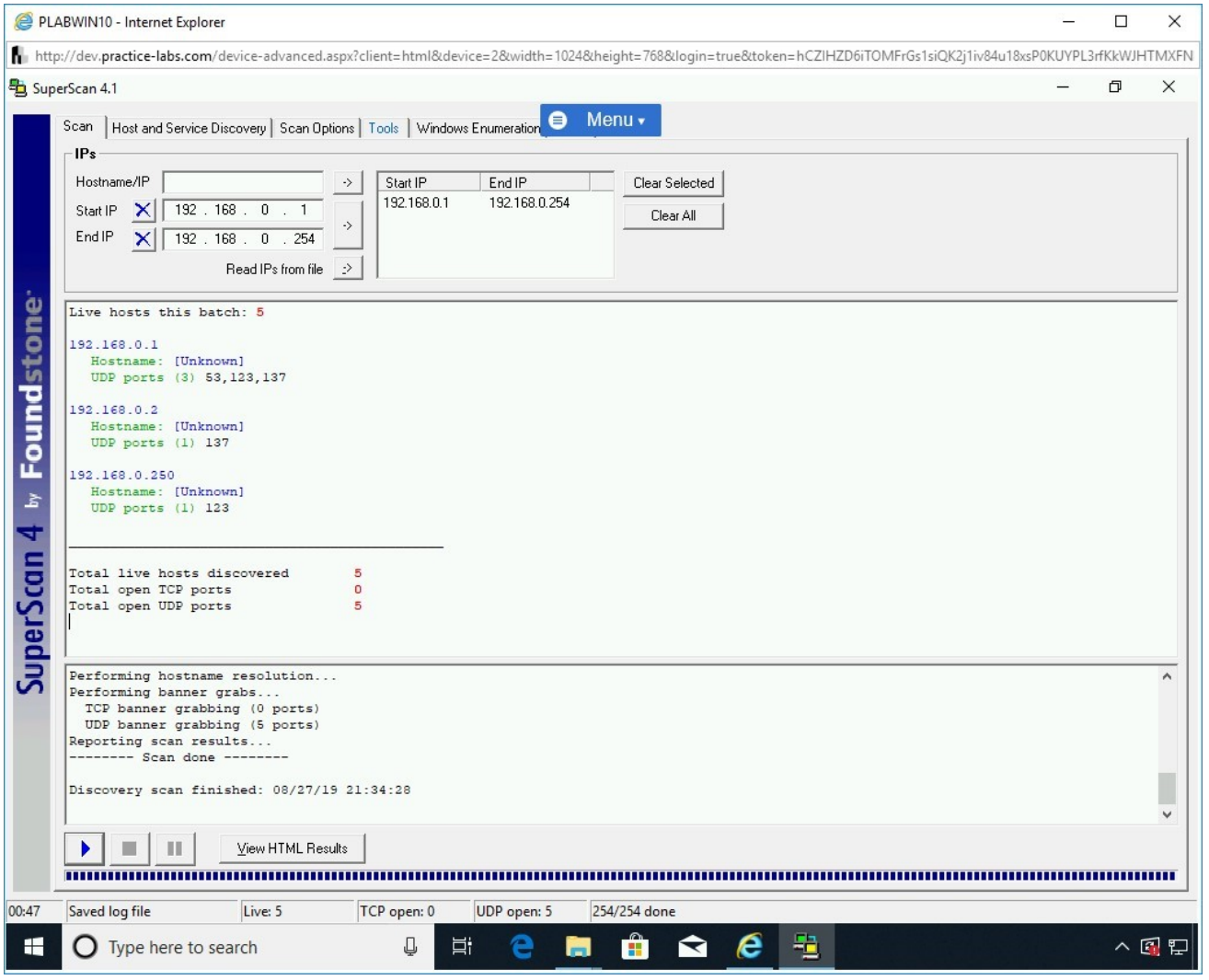


Figure 1.37 Screenshot of PLABWIN10: Showing the results on the Scan tab and then clicking the Tools tab.

Step 38

On the **Tools** tab, click inside the **Hostname/IP/URL** textbox, type the following name:

```
PLABDC01
```

Click the **Hostname/IP Lookup** button.

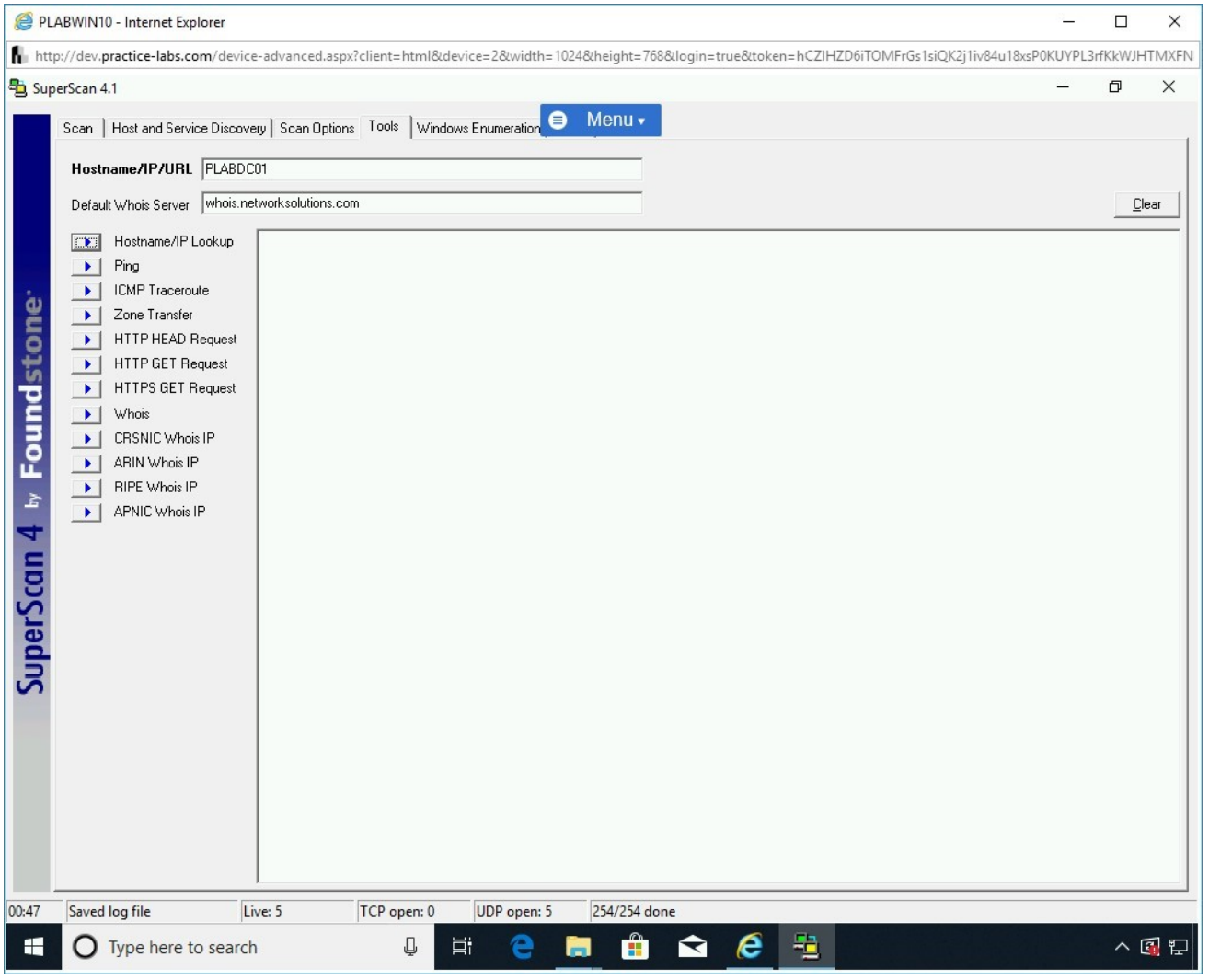


Figure 1.38 Screenshot of PLABWIN10: Entering the IP address as the target and clicking the Hostname/IP Lookup button.

Step 39

Note that the results of the hostname will be now resolved to its IP address in the right pane.

Click the **Ping** button.

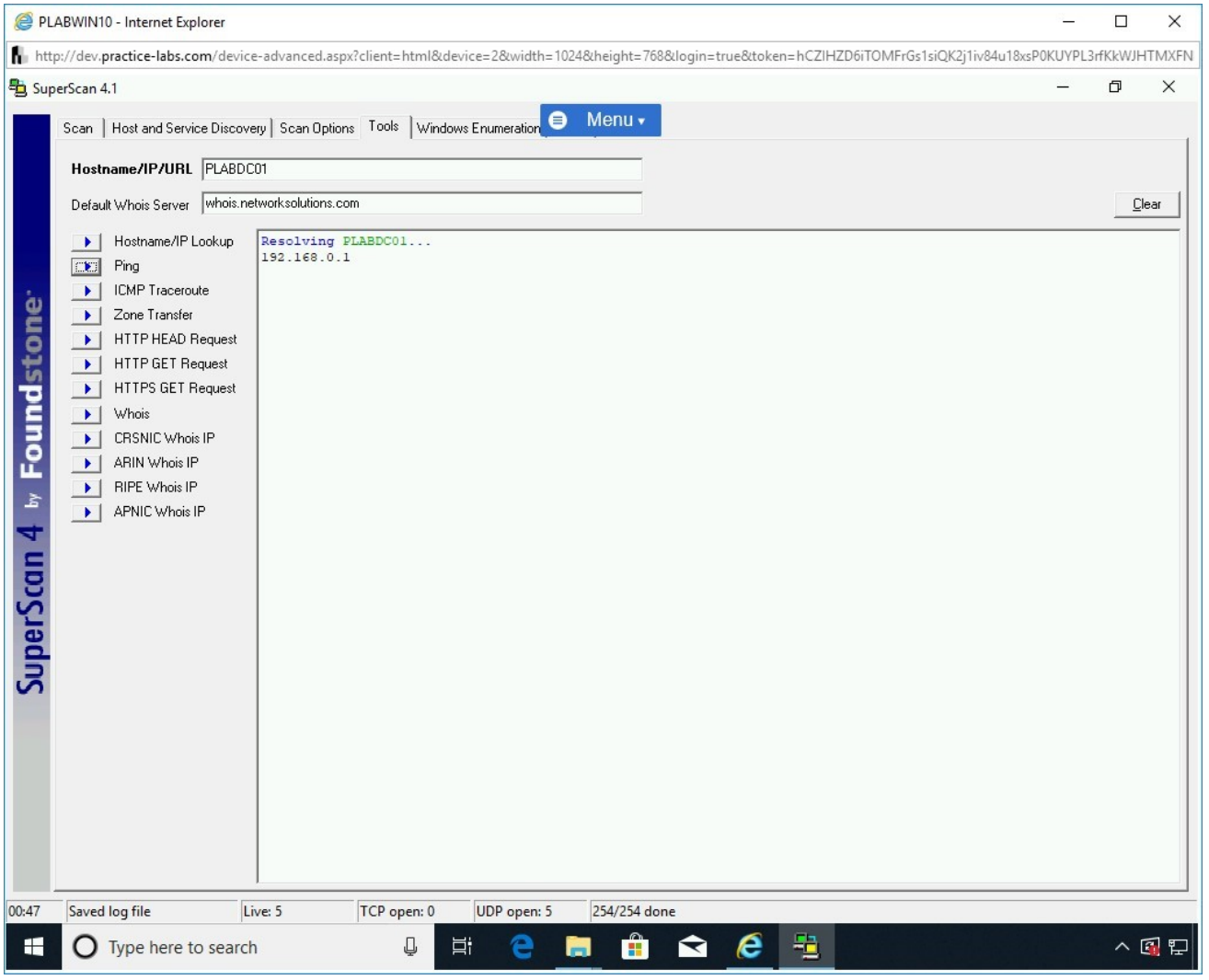


Figure 1.39 Screenshot of PLABWIN10: Clicking the Ping button from the left pane.

Step 40

The ping response from **PLABDC01** is received.

Click the **ICMP Traceroute** button.

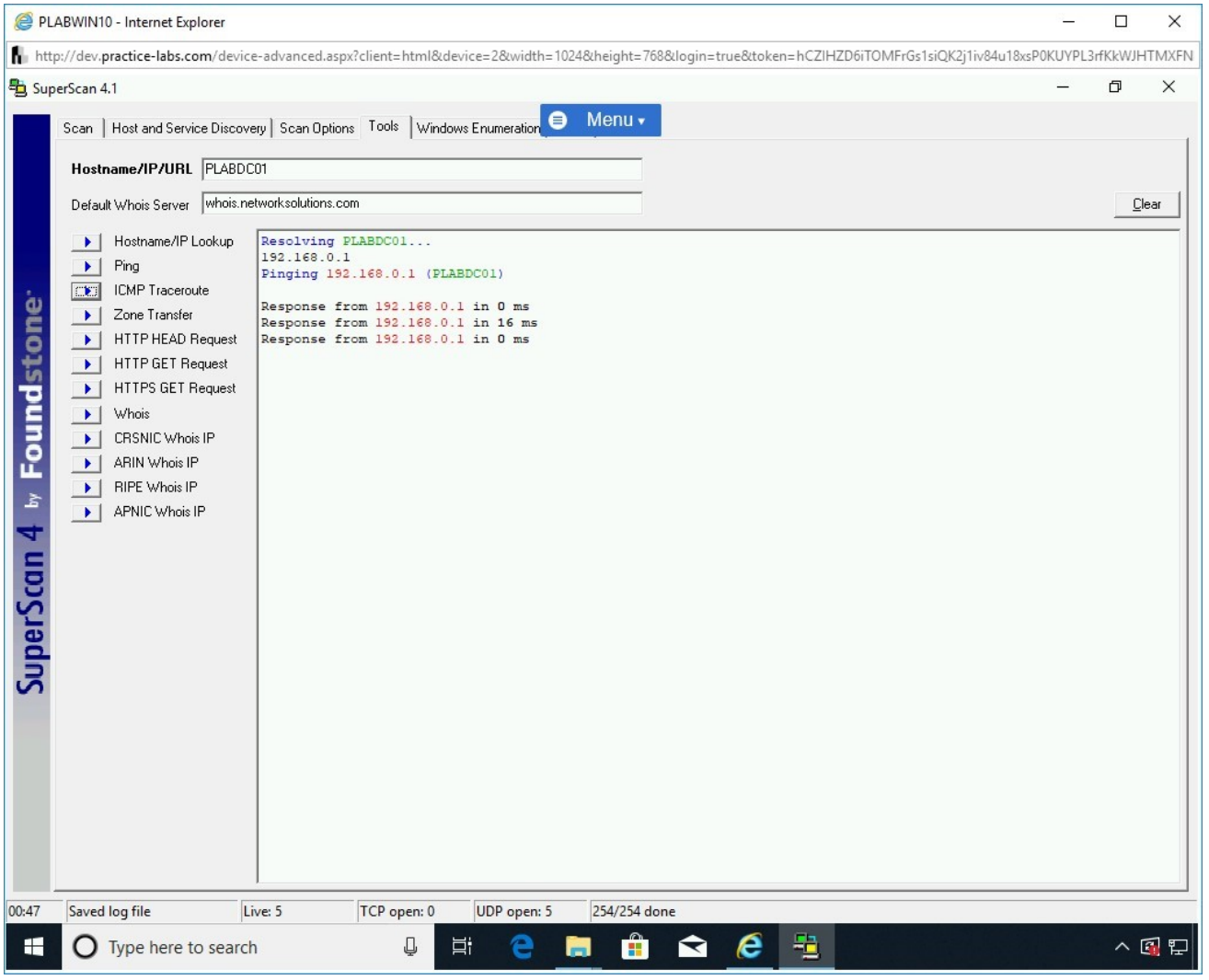


Figure 1.40 Screenshot of PLABWIN10: Clicking the ICMP Traceroute button in the left pane.

Step 41

Note that the results are displayed.

There is a single hop to **PLABDC01**.

> ***Note**: You can try the remaining options if time permits.*

Close the **SuperScan 4.1** window.

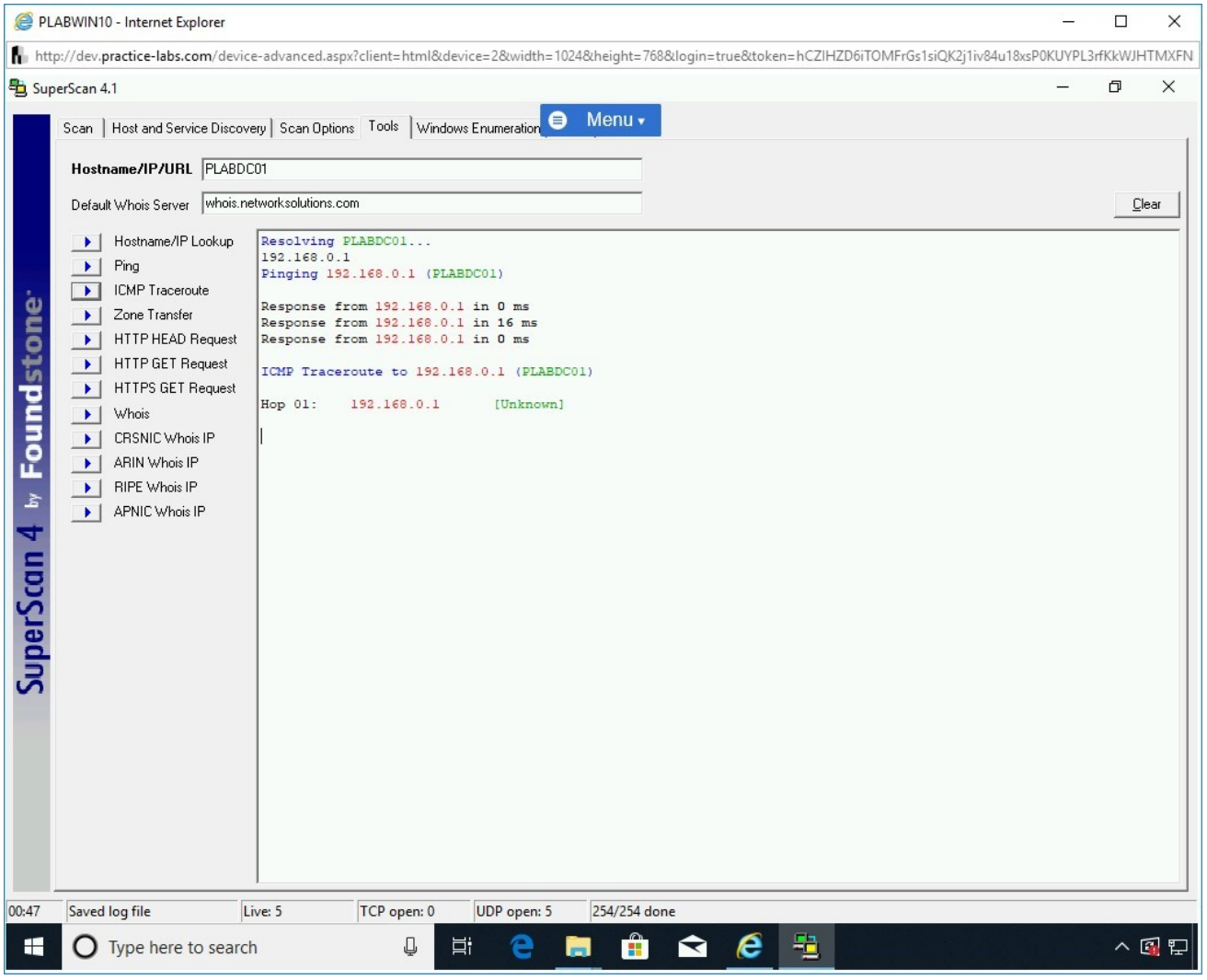


Figure 1.41 Screenshot of PLABWIN10: Showing the results in the right pane and then closing the SuperScan 4.1 window.

Close the **File Explorer** windows and keep **Internet Explorer** open.

Task 2 - Use Hyena for Enumeration

Hyena is one of the most renowned tools for system management used by network administrators. Hyena with its system management capabilities can perform enumeration of various types of information:

- users
- shares
- services

In this task, you will learn to use Hyena for enumeration. To use Hyena, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABWIN10.** Ensure that **Internet Explorer** is open, and you are on the **Hacking Tools** page.

> ***Note:*** *If you closed Internet Explorer in the previous task, please ensure you follow the steps provided in Task 1 to reach the Hacking Tools page.*

On the **Hacking Tools** Webpage, scroll to locate **hyena.zip**. Click **hyena.zip**.

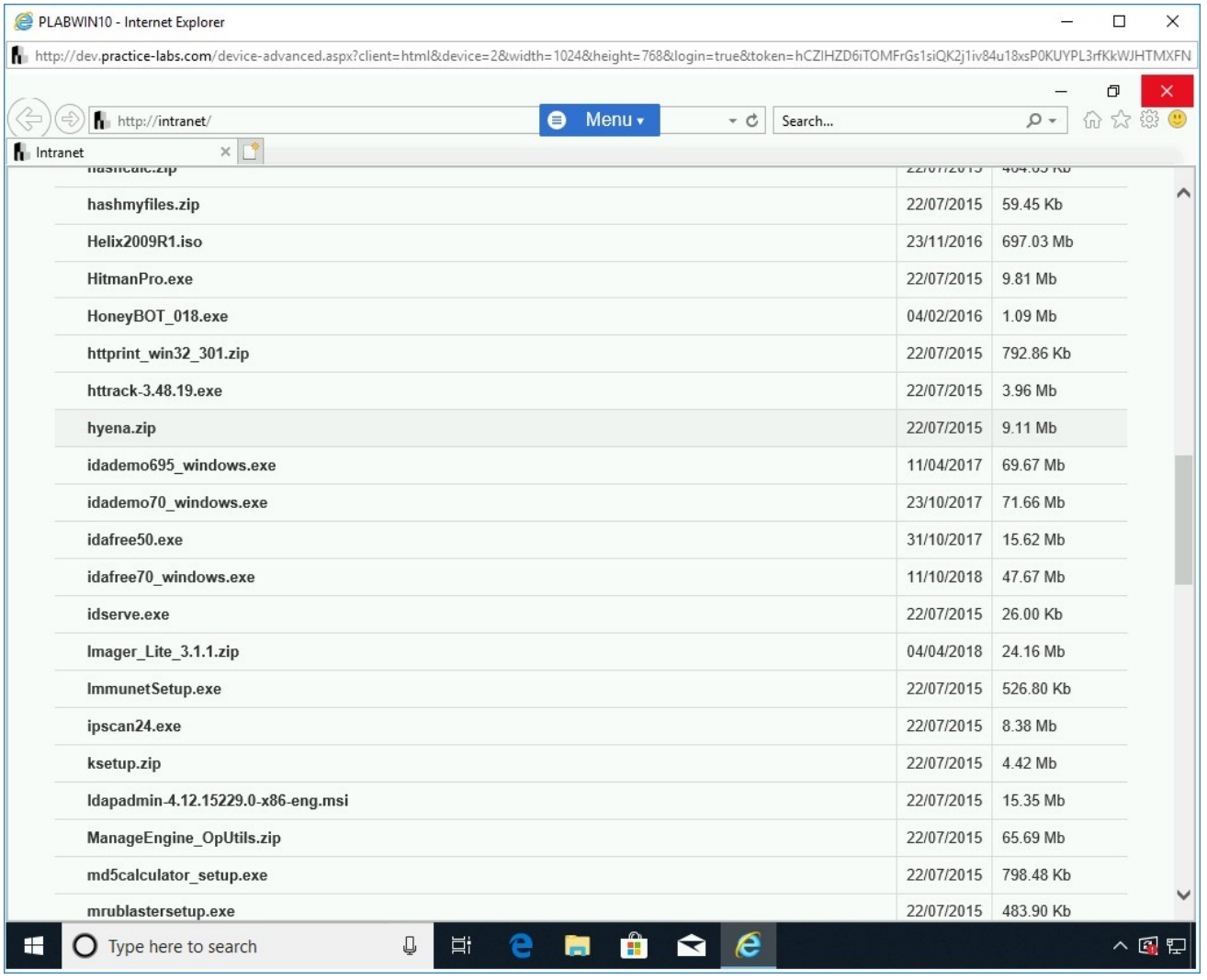


Figure 1.42 Screenshot of PLABWIN10: Clicking hyena.zip on the Hacking Tools page.

Step 2

In the notification bar, click **Save**.

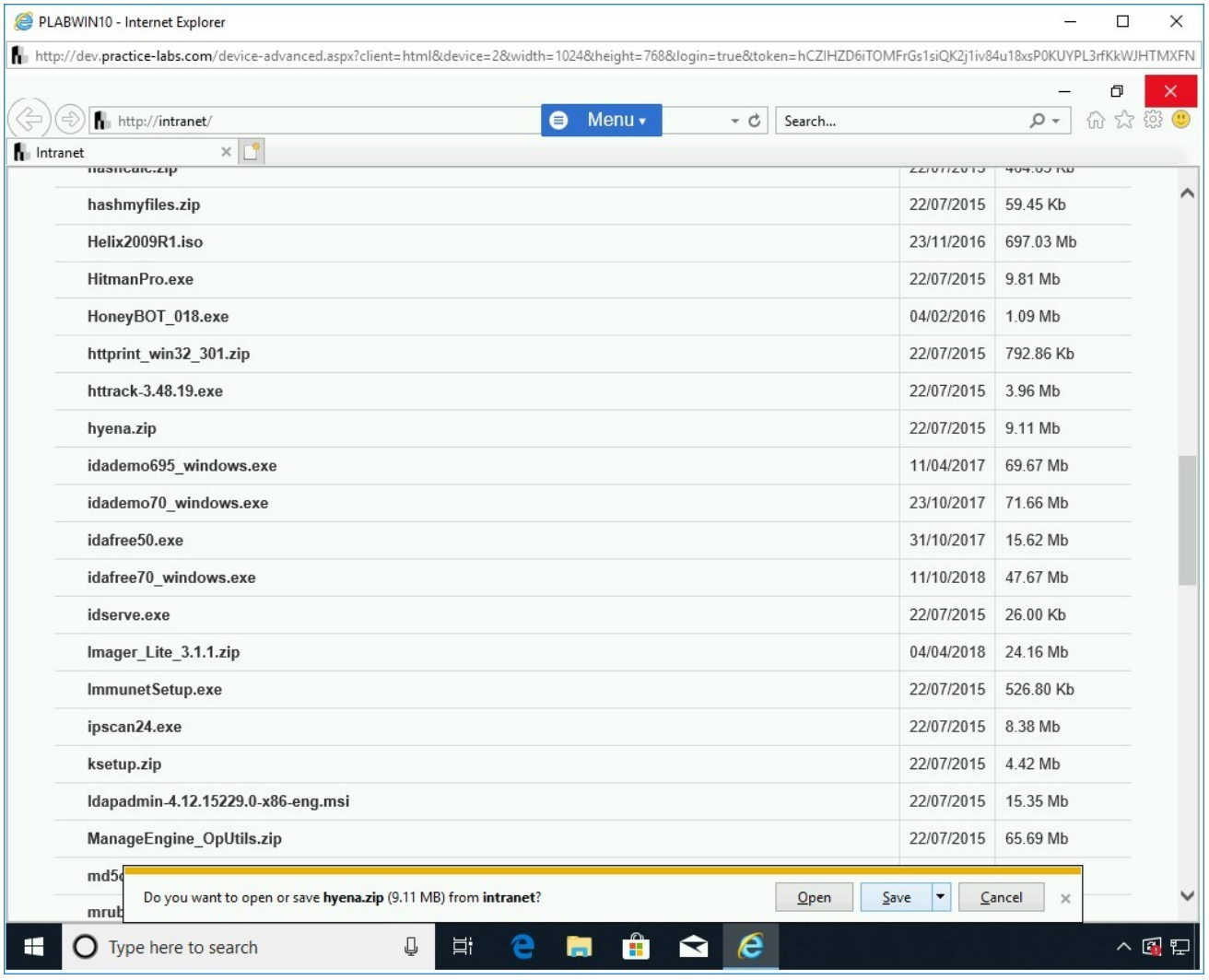


Figure 1.43 Screenshot of PLABWIN10: Clicking Save in the notification bar.

Step 3

When the file is successfully downloaded, in the notification bar, click **Open folder**.

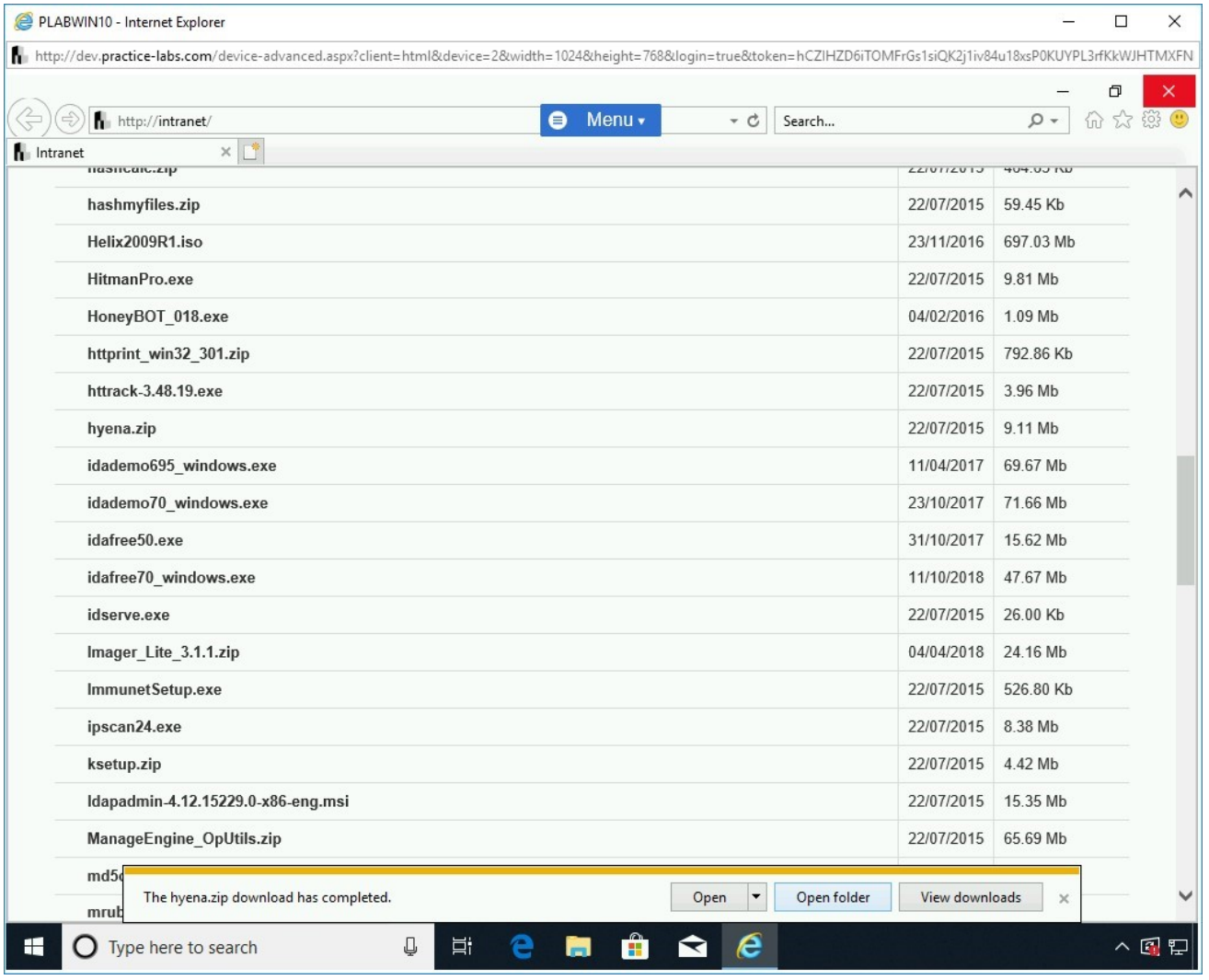


Figure 1.44 Screenshot of PLABWIN10: Clicking Open folder in the notification bar.

Step 4

In the **File Explorer** window, right-click **hyena.zip** and select **Extract All**.

> ***Note:*** *The files in the download folder may differ in your lab environment.*

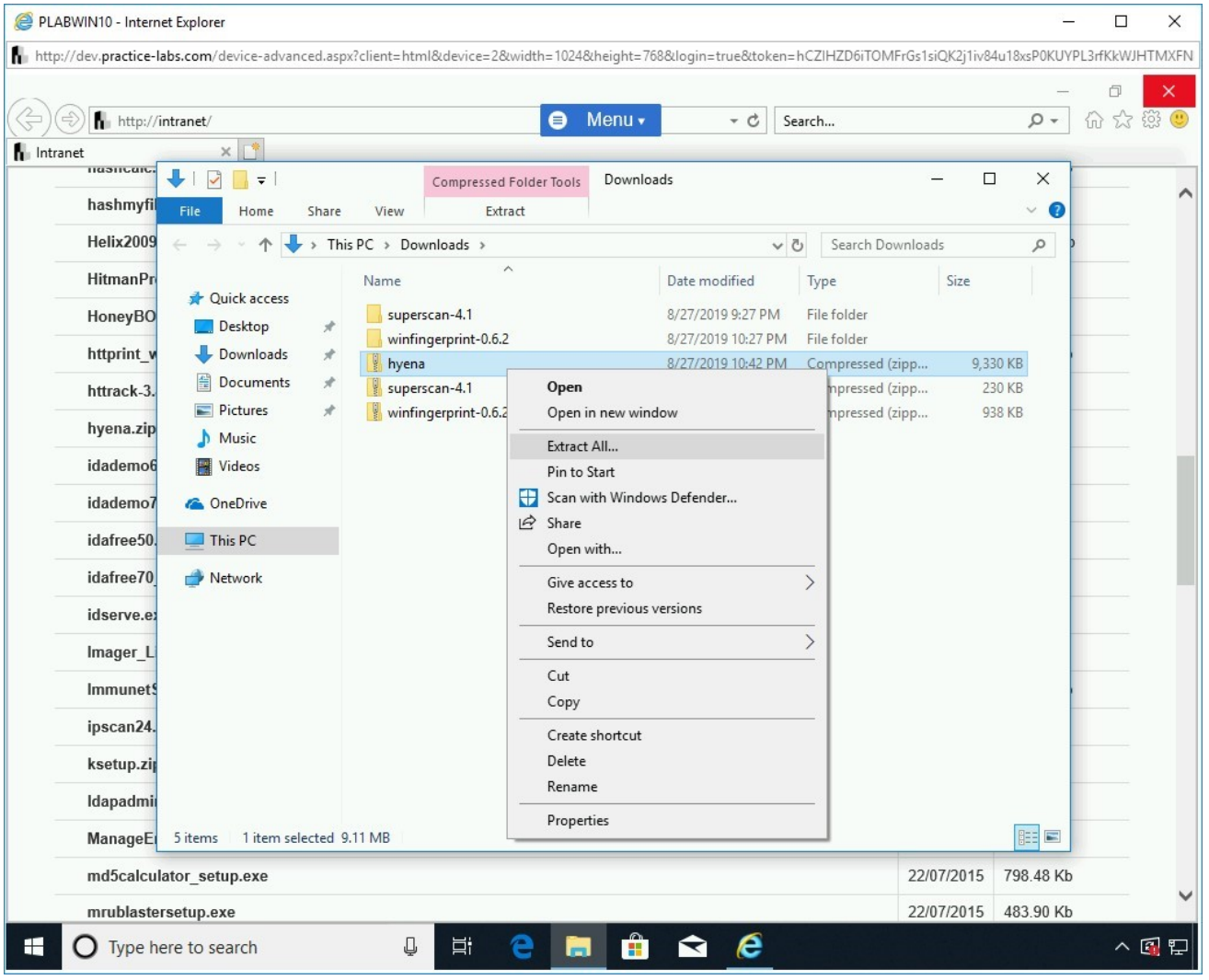


Figure 1.45 Screenshot of PLABWIN10: Right-clicking hyena.zip and selecting Extract All from the context menu.

Step 5

In the **Extract Compressed (Zipped) Folders** dialog box, keep the default path and click **Extract**.

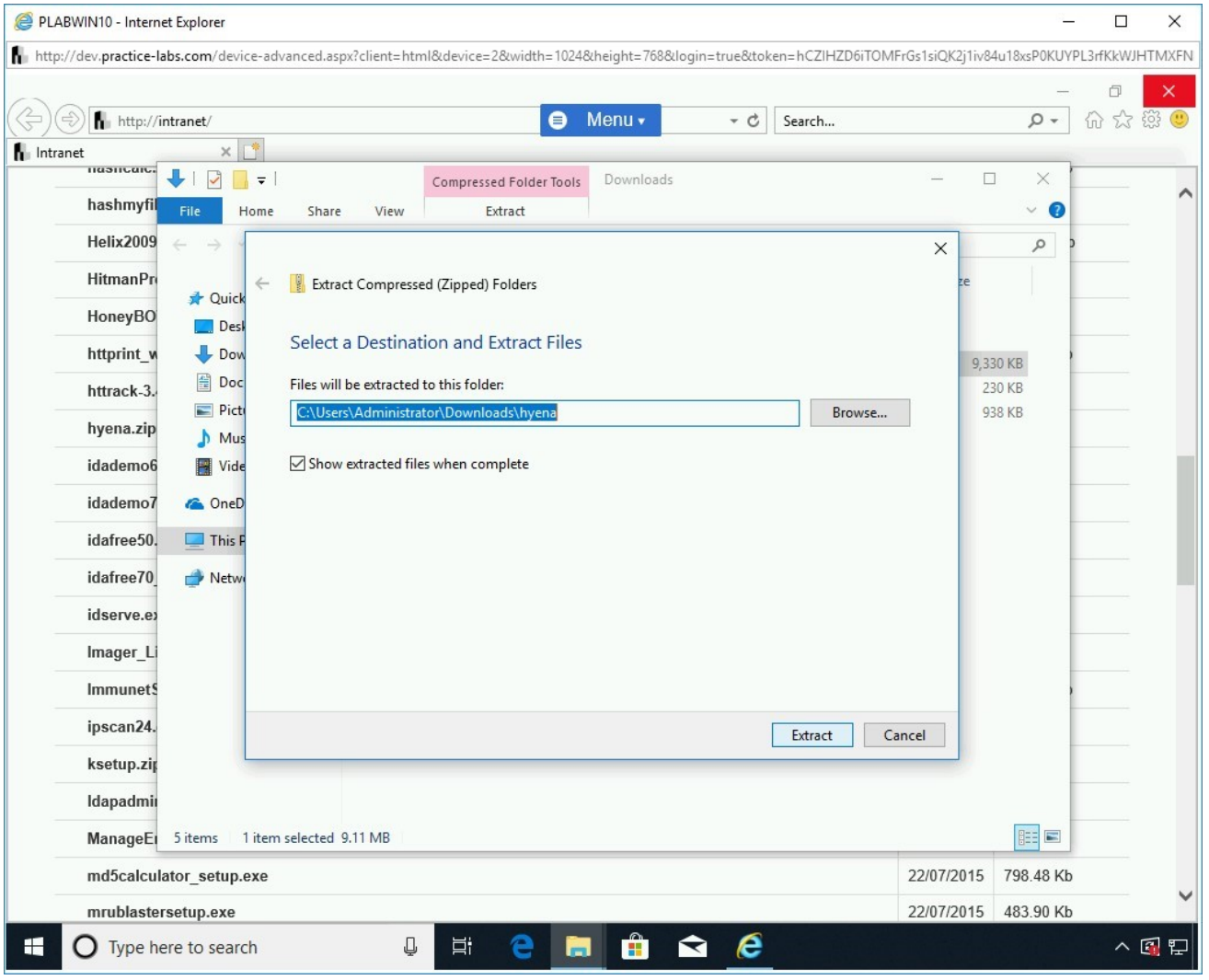


Figure 1.46 Screenshot of PLABWIN10: Clicking Extract in the Extract Compressed (Zipped) Folders dialog box.

Step 6

A new **File Explorer** window is displayed with the **Hyena_English_x86** file. Double-click the **Hyena_English_x86** file.

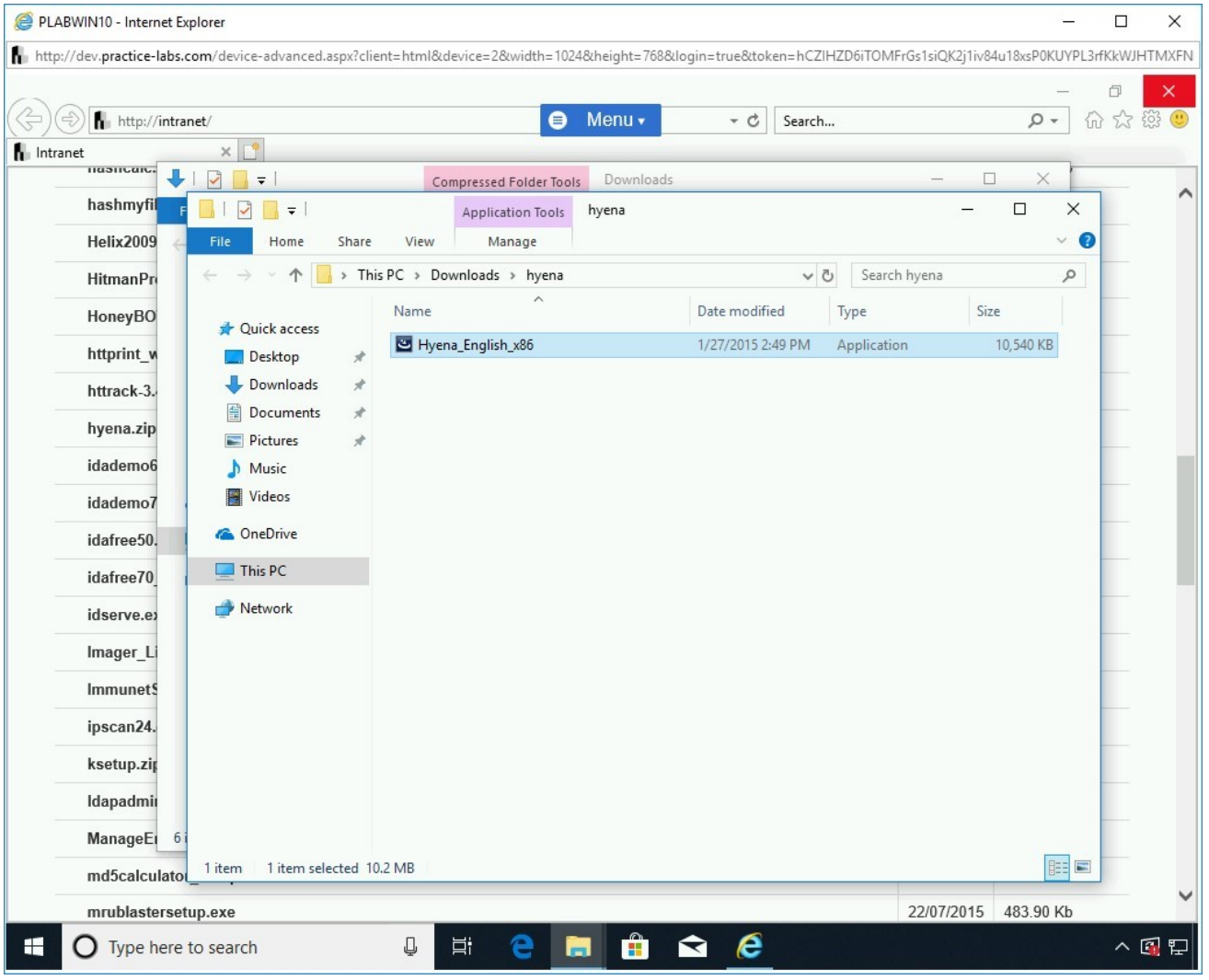


Figure 1.47 Screenshot of PLABWIN10: Double-clicking the Hyena_English_x86 file.

Step 7

The **Hyena v11.2 - InstallShield Wizard** is displayed. It prompts with a pre-requisite application, which is **Microsoft Visual C++ 2008 SP1**, to be installed before installing Hyena. To begin the installation of **Microsoft Visual C++ 2008 SP1**, click **Install**.

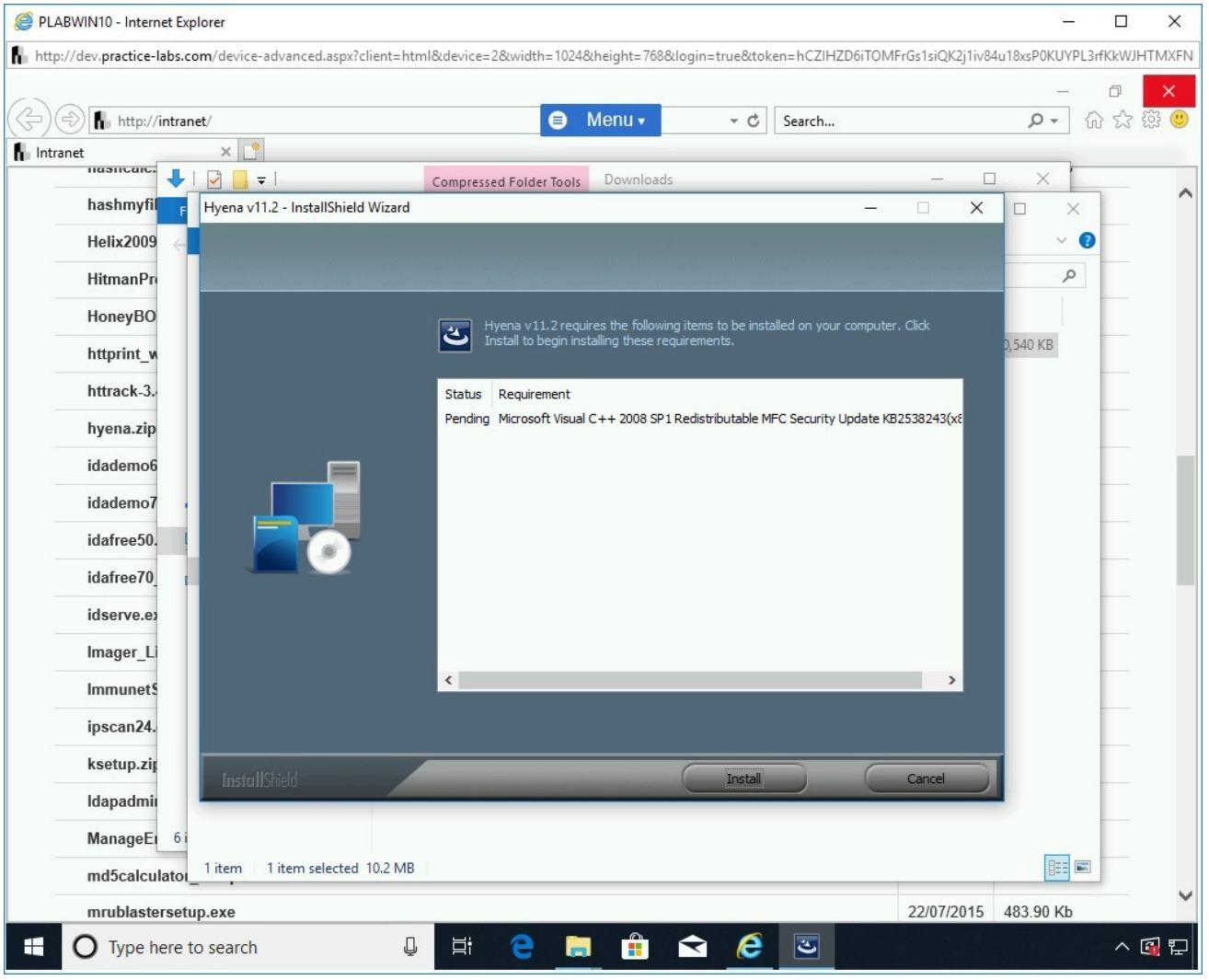


Figure 1.48 Screenshot of PLABWIN10: Showing the Hyena v11.2 - InstallShield Wizard dialog box and clicking Install.

Step 8

The installation of the required application starts.

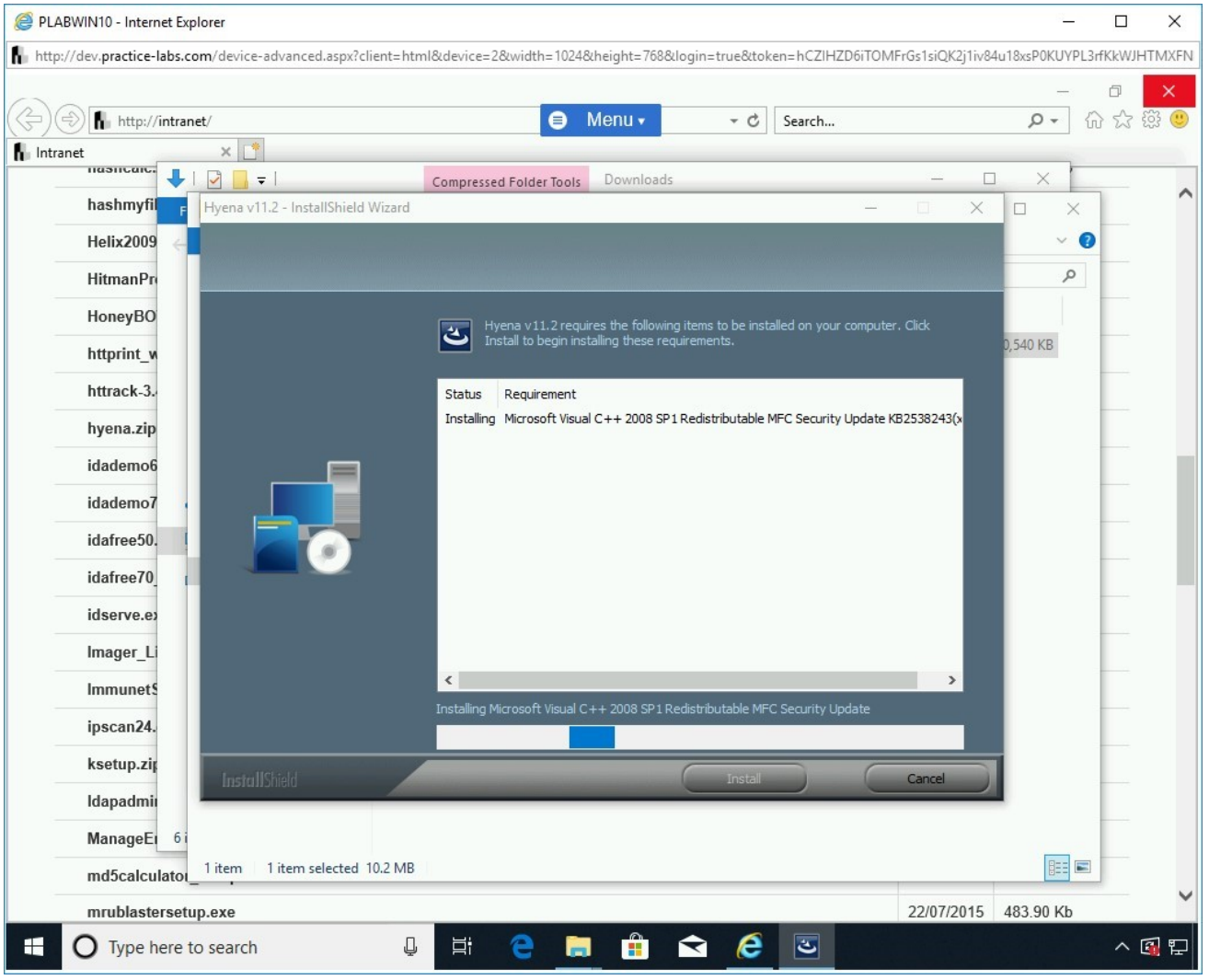


Figure 1.49 Screenshot of PLABWIN10: Showing the installation of Microsoft Visual C++.

Step 9

After the required application is installed, you are navigated to the **Welcome to the InstallShield Wizard for Hyena v11.2** page. Click **Next**.

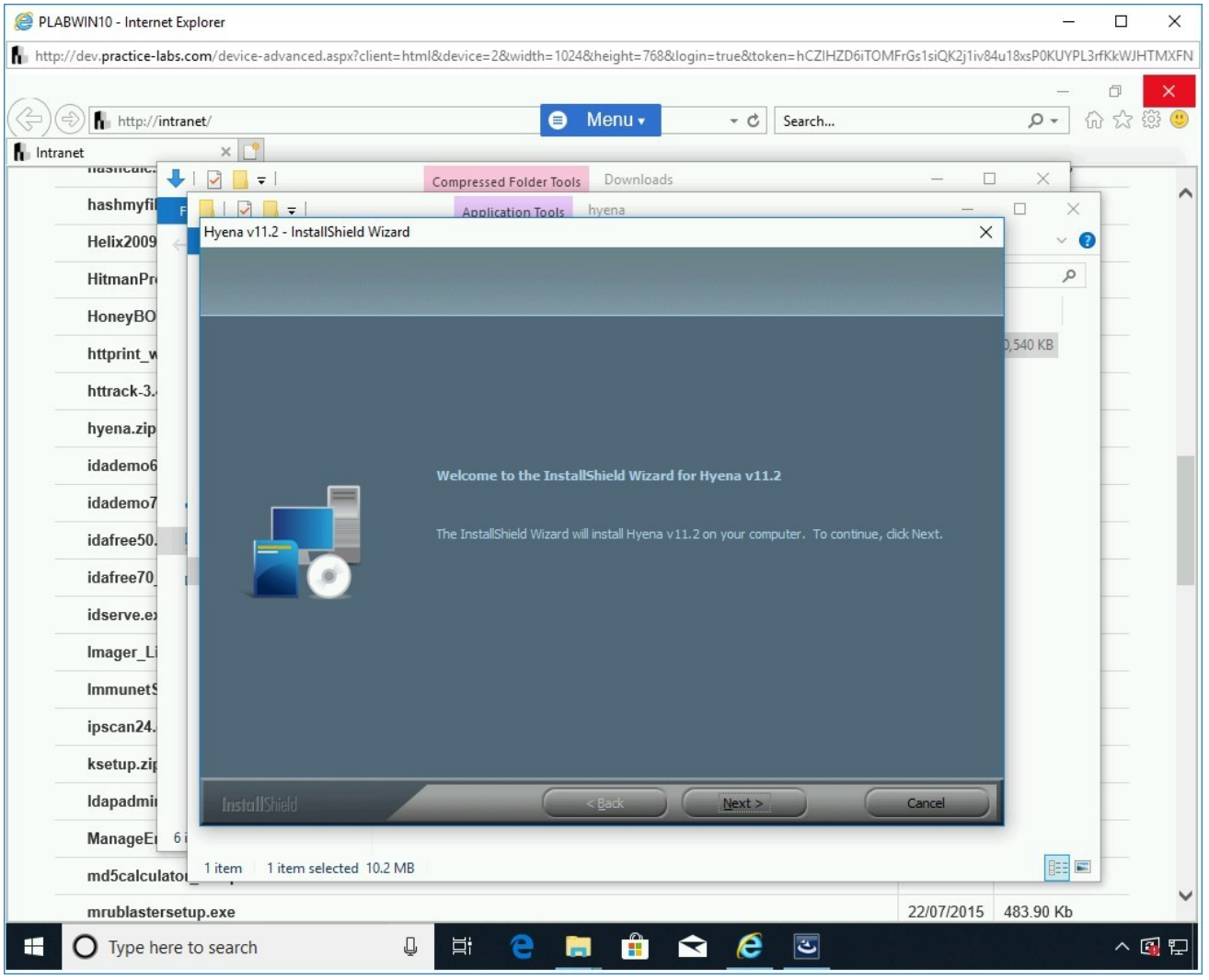


Figure 1.50 Screenshot of PLABWIN10: Clicking Next on the Welcome to the InstallShield Wizard for Hyena v11.2 page.

Step 10

On the **License Agreement** page, select **I accept the terms of the license agreement** and click **Next**.

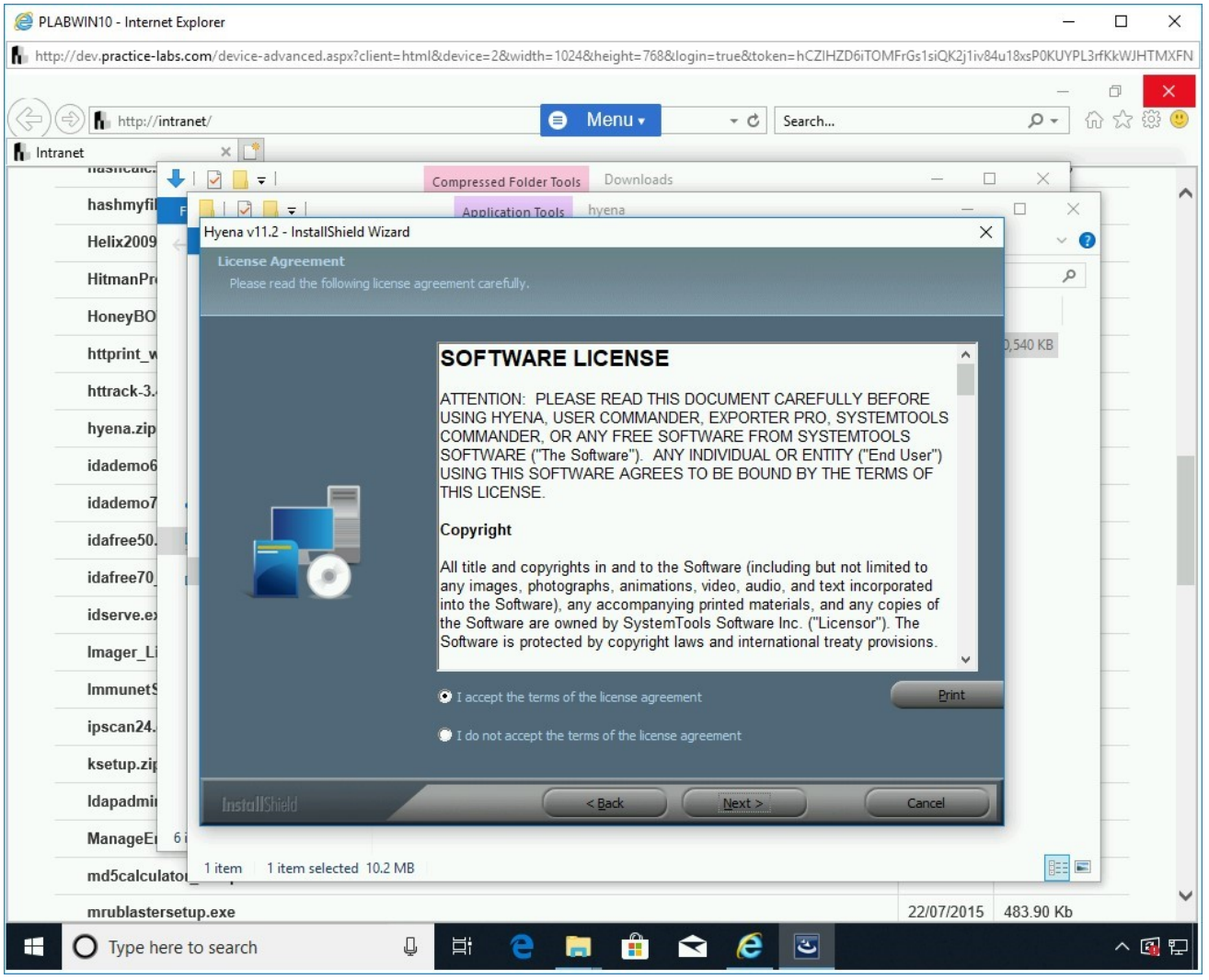


Figure 1.51 Screenshot of PLABWIN10: Selecting I accept the terms of the license agreement and clicking Next.

Step 11

On the **Choose Destination Location** page, keep the default installation path and click **Next**.

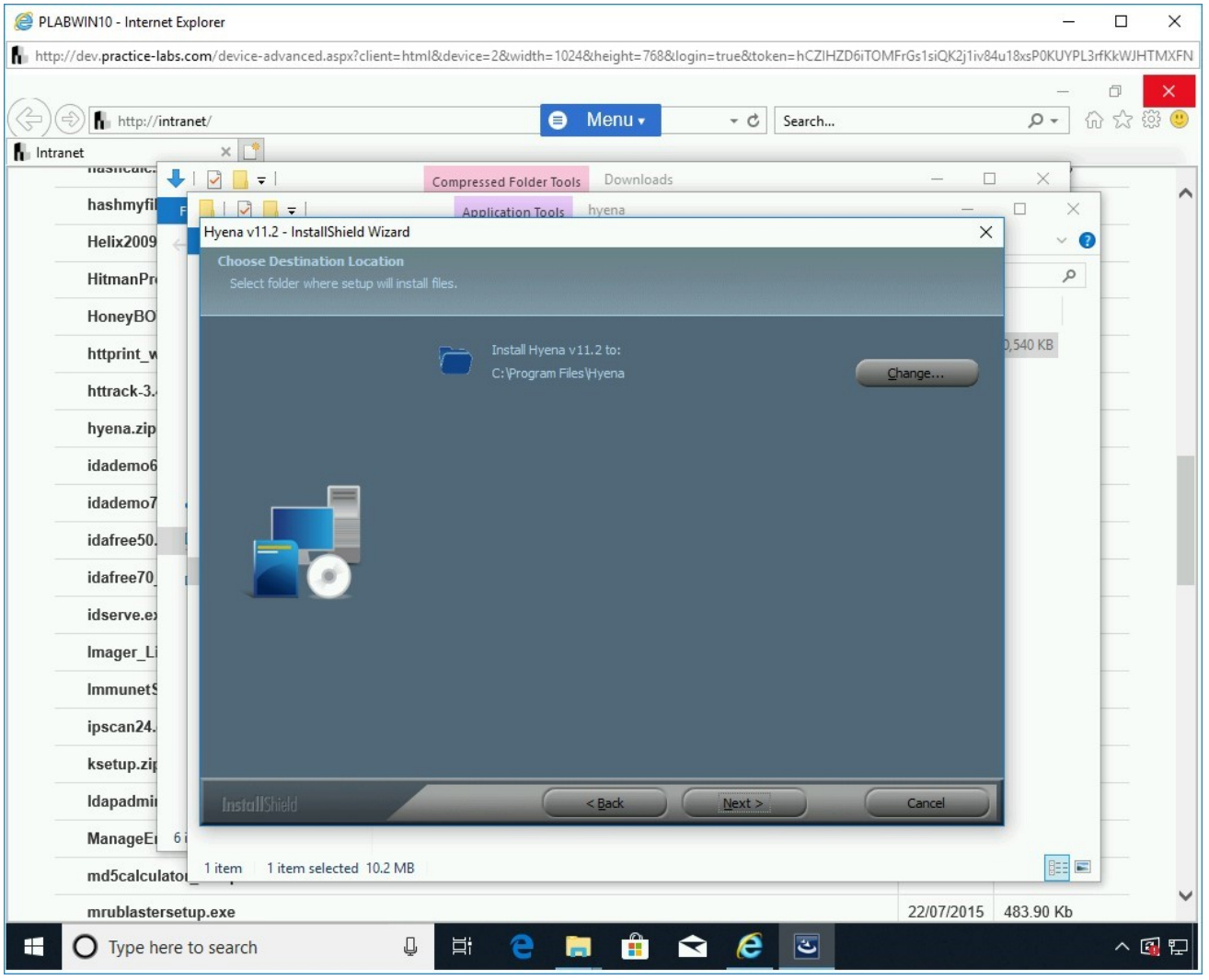


Figure 1.52 Screenshot of PLABWIN10: Keeping the default installation path and clicking Next.

Step 12

On the **Ready to Install the Program** page, click **Install**.

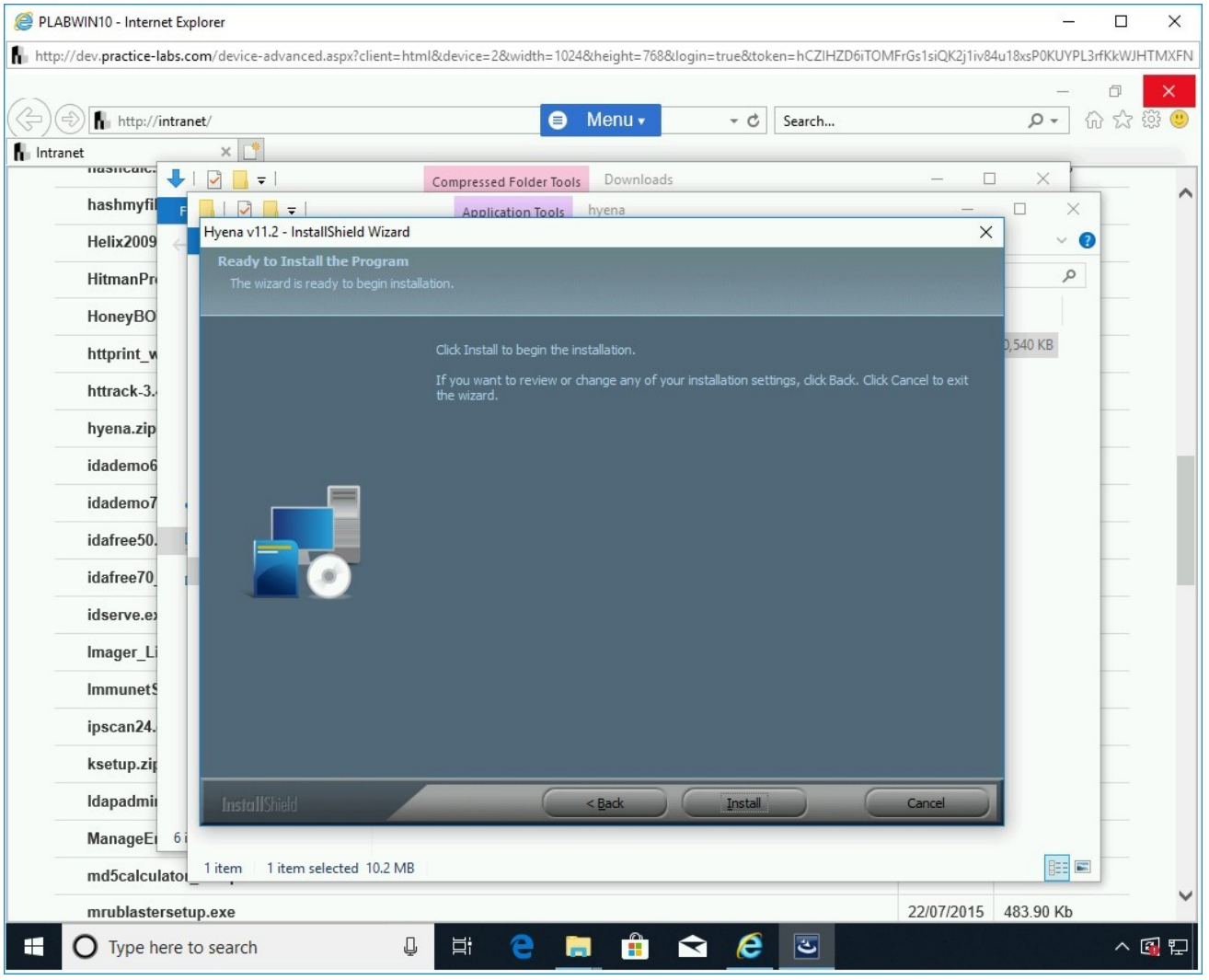


Figure 1.53 Screenshot of PLABWIN10: Clicking Install on the Ready to Install the Program page.

Step 13

On the **InstallShield Wizard Complete** page, click **Finish**.

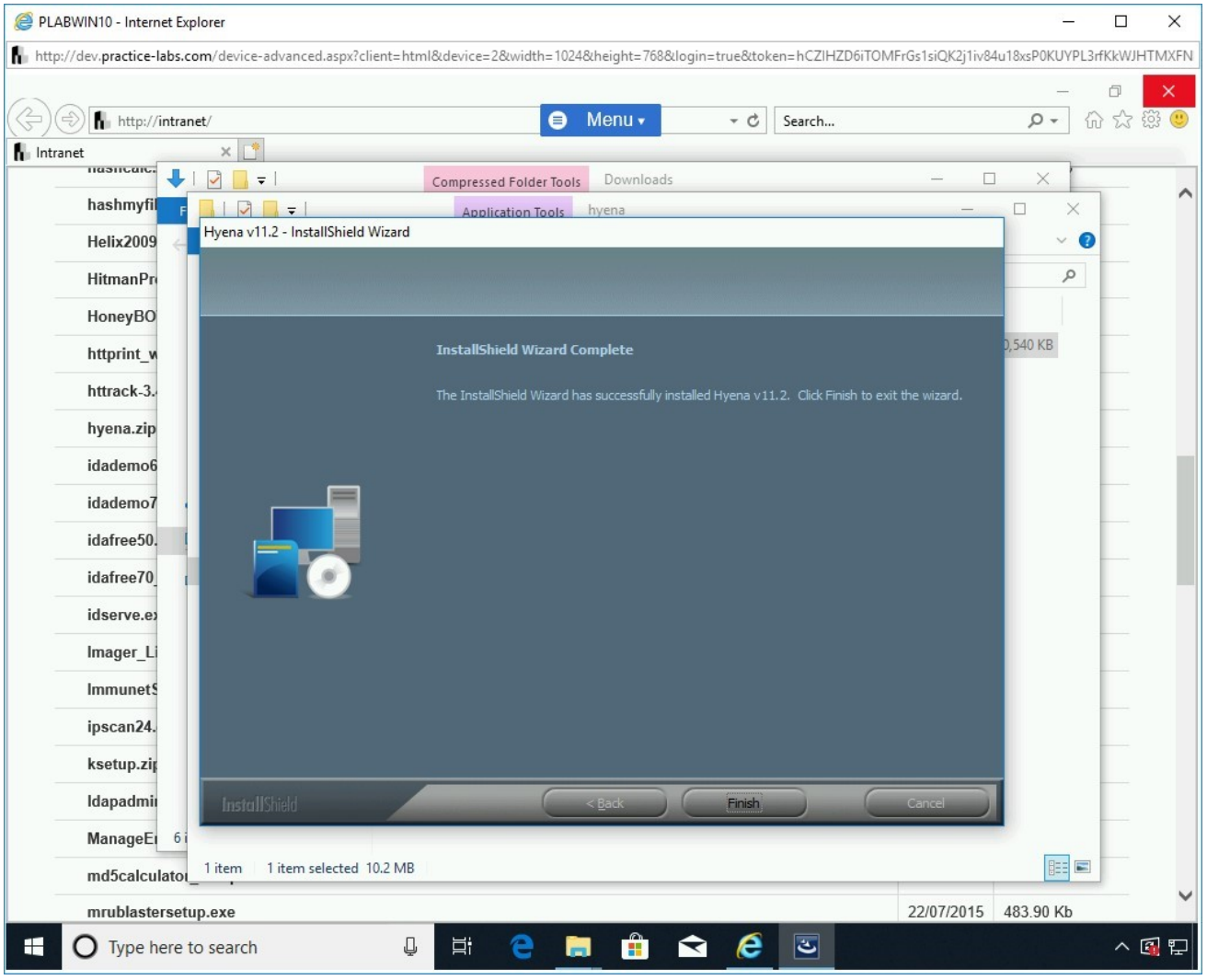


Figure 1.54 Screenshot of PLABWIN10: Clicking Finish on the InstallShield Wizard Complete page.

Step 14

Close all instances of **File Explorer** windows. Minimize the **Internet Explorer** window.

In the **Type here to search** text box, type the following:

```
hyena
```

From the search results, select **Hyena**.

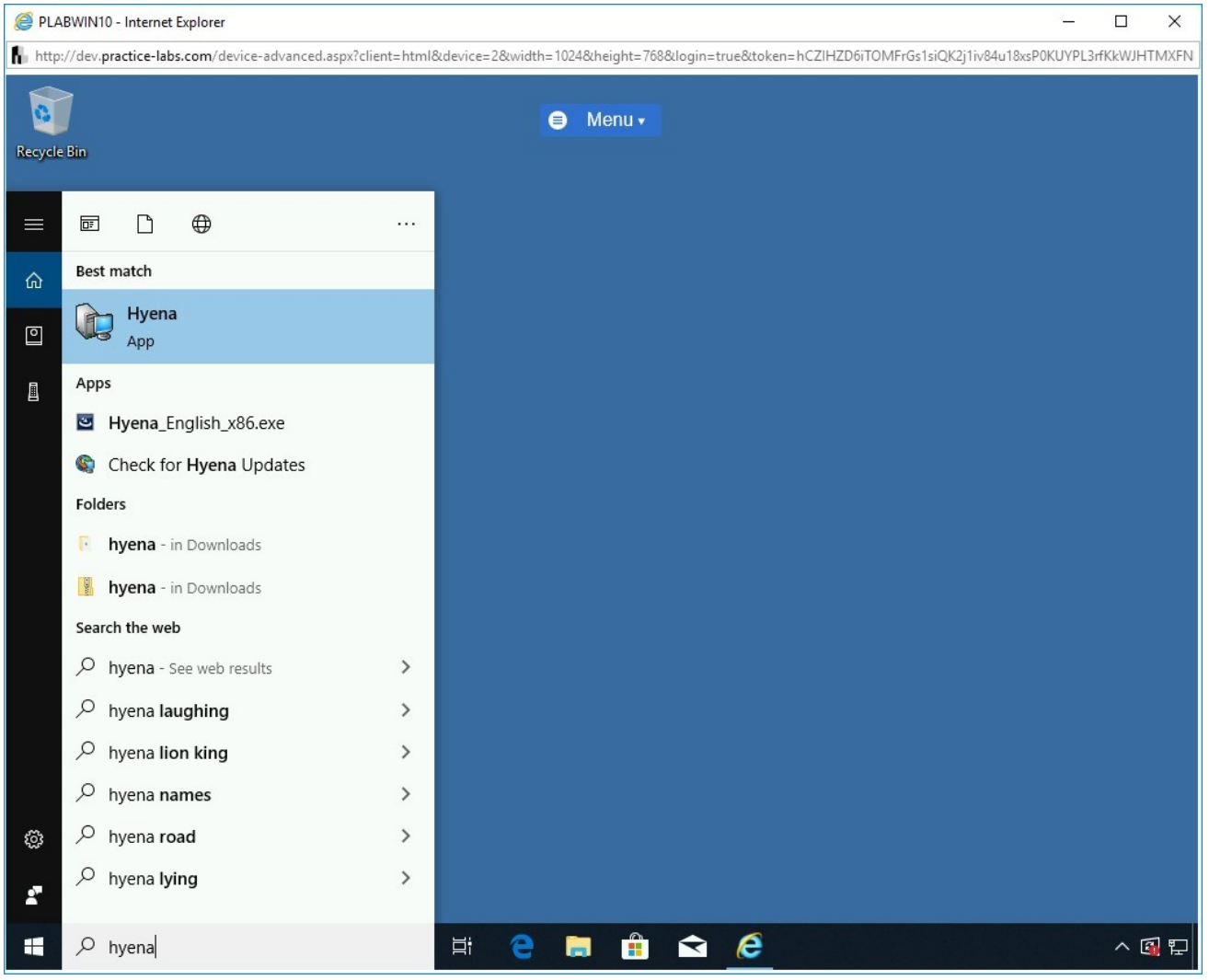


Figure 1.55 Screenshot of PLABWIN10: Selecting Hyena from the search results.

Step 15

The **SystemTools Update Notification Utility** dialog box is displayed.

Click **Close**.

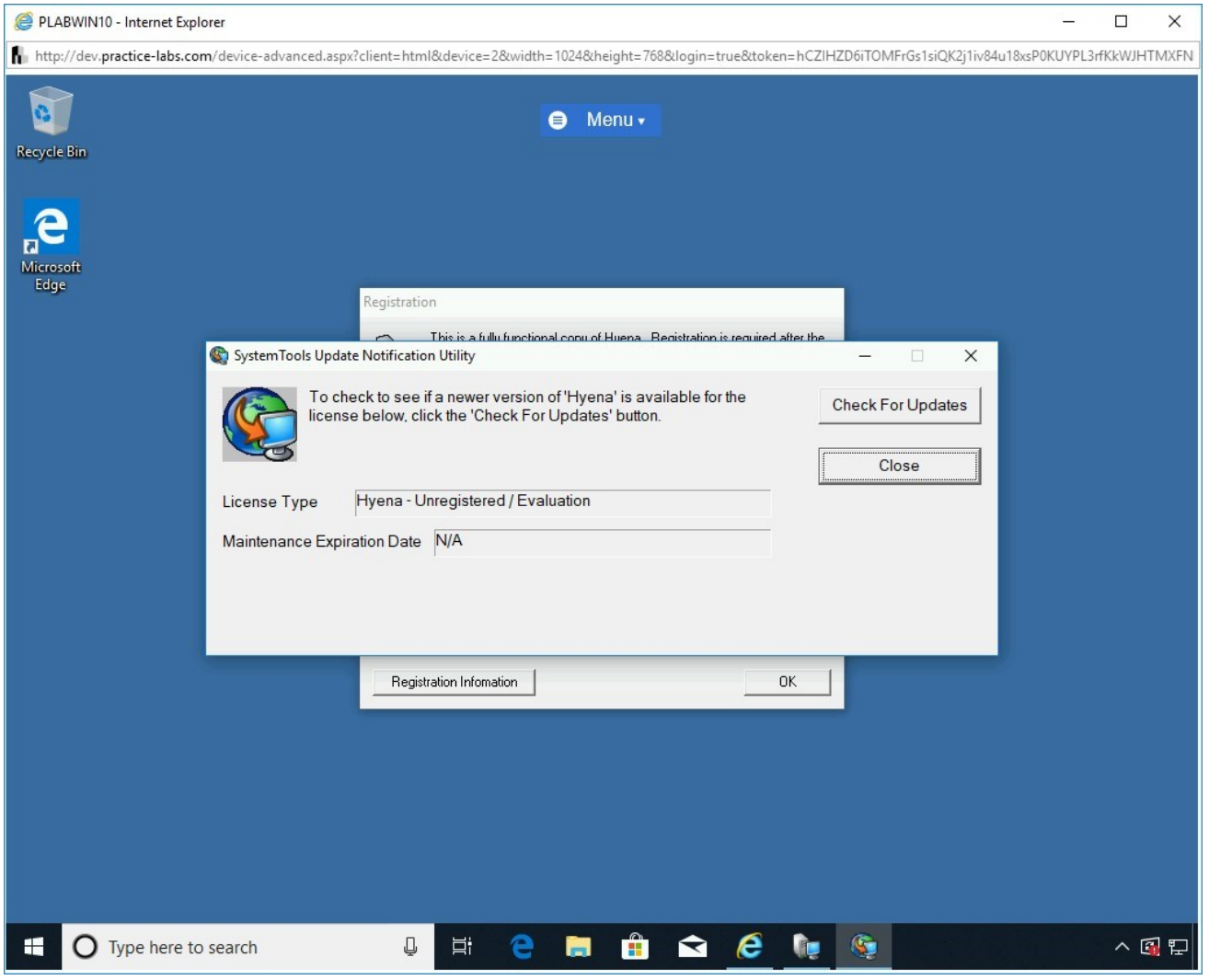


Figure 1.56 Screenshot of PLABWIN10: Clicking Close on the SystemTools Update Notification Utility.

Step 16

On the **Registration** dialog box, click **OK**.

You can skip the registration process.

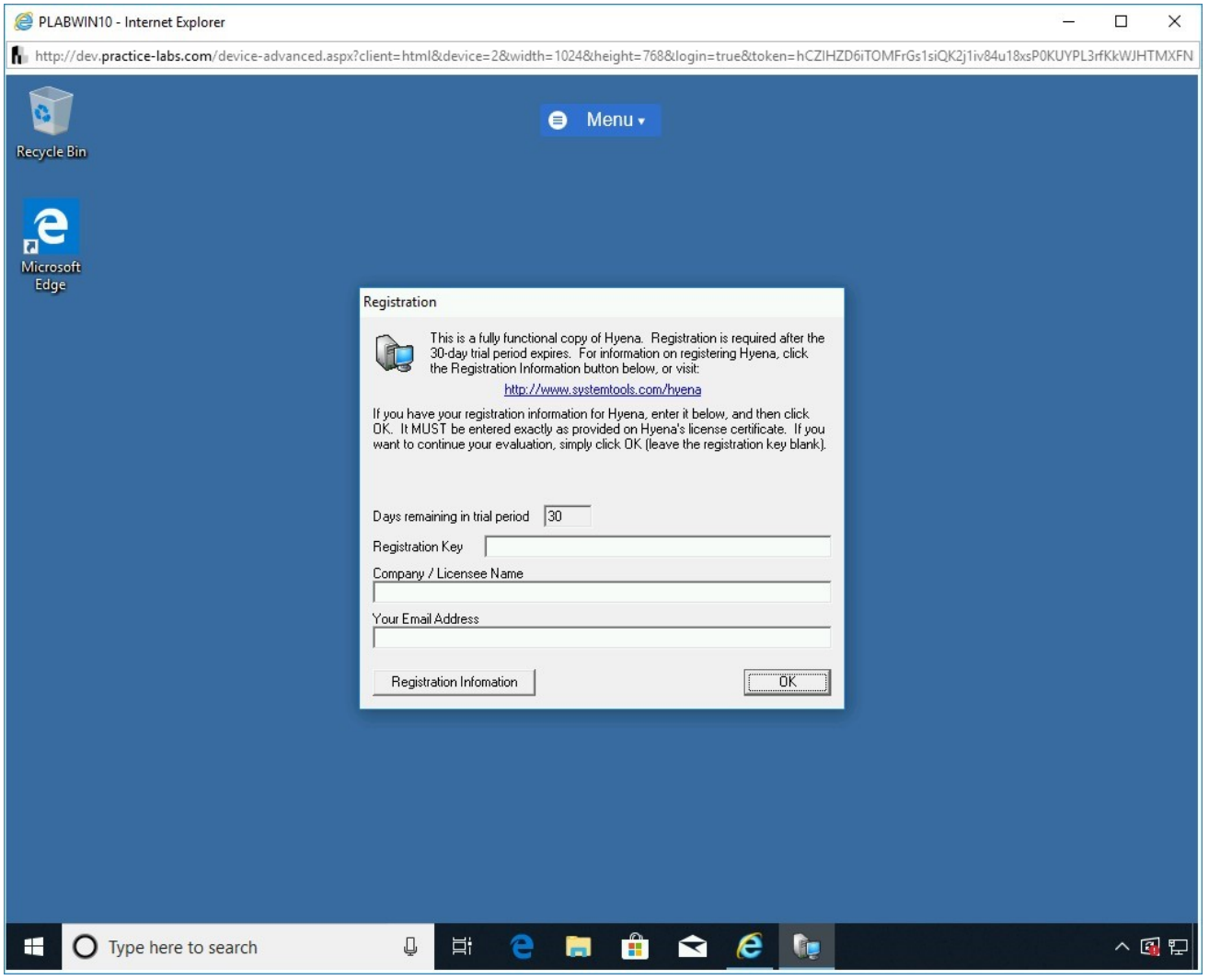


Figure 1.57 Screenshot of PLABWIN10: Clicking OK on the Registration dialog box.

Step 17

On the **Hyena** dialog box, click **No**.

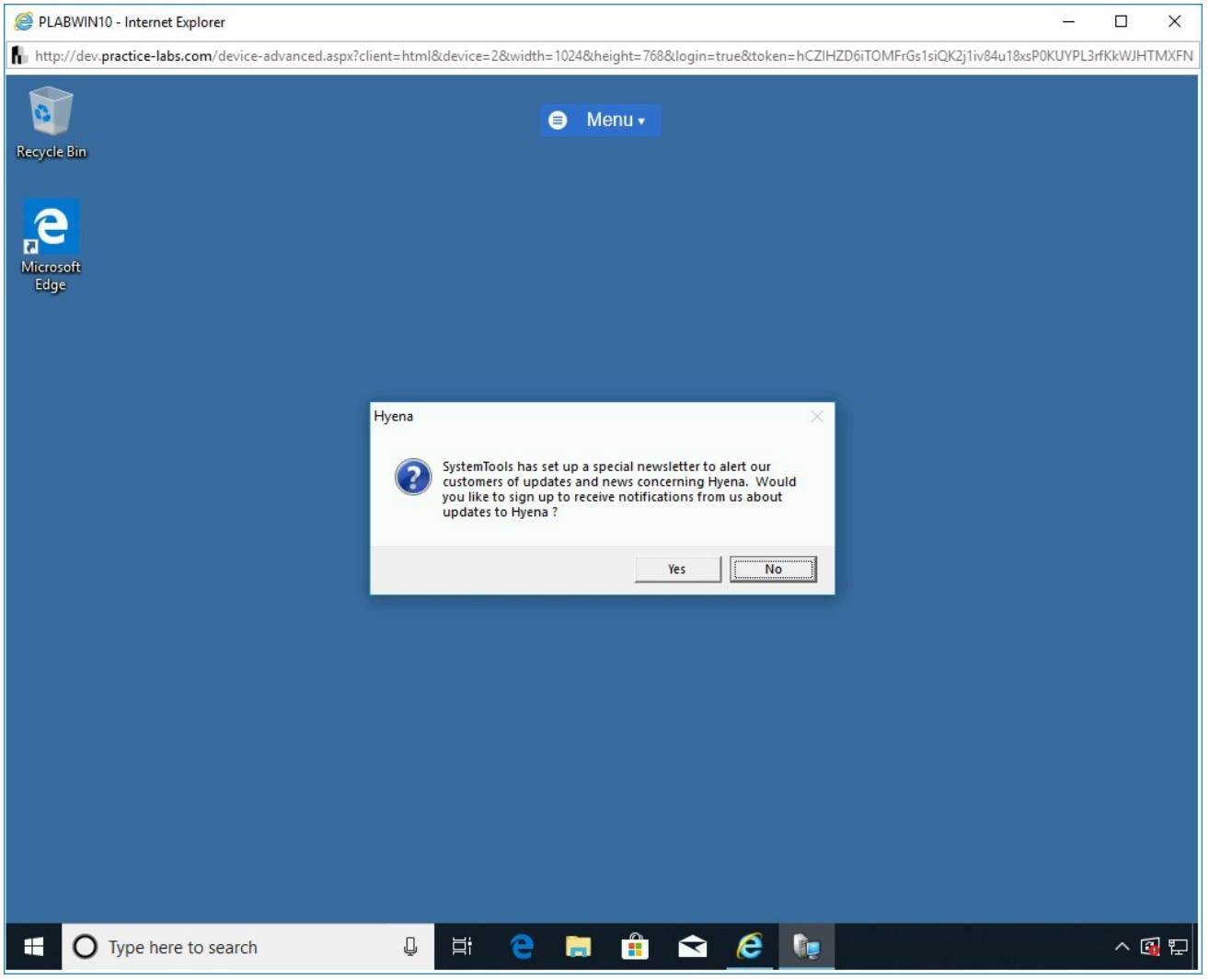


Figure 1.58 Screenshot of PLABWIN10: Clicking No on the Hyena dialog box.

Step 18

The **Hyena v11.2** window is displayed. It is divided into the left and right pane.

In the left pane, the **PRACTICELABS.COM** domain has already been added automatically.

To remove a domain, click **File** and then select **Manage object View.**

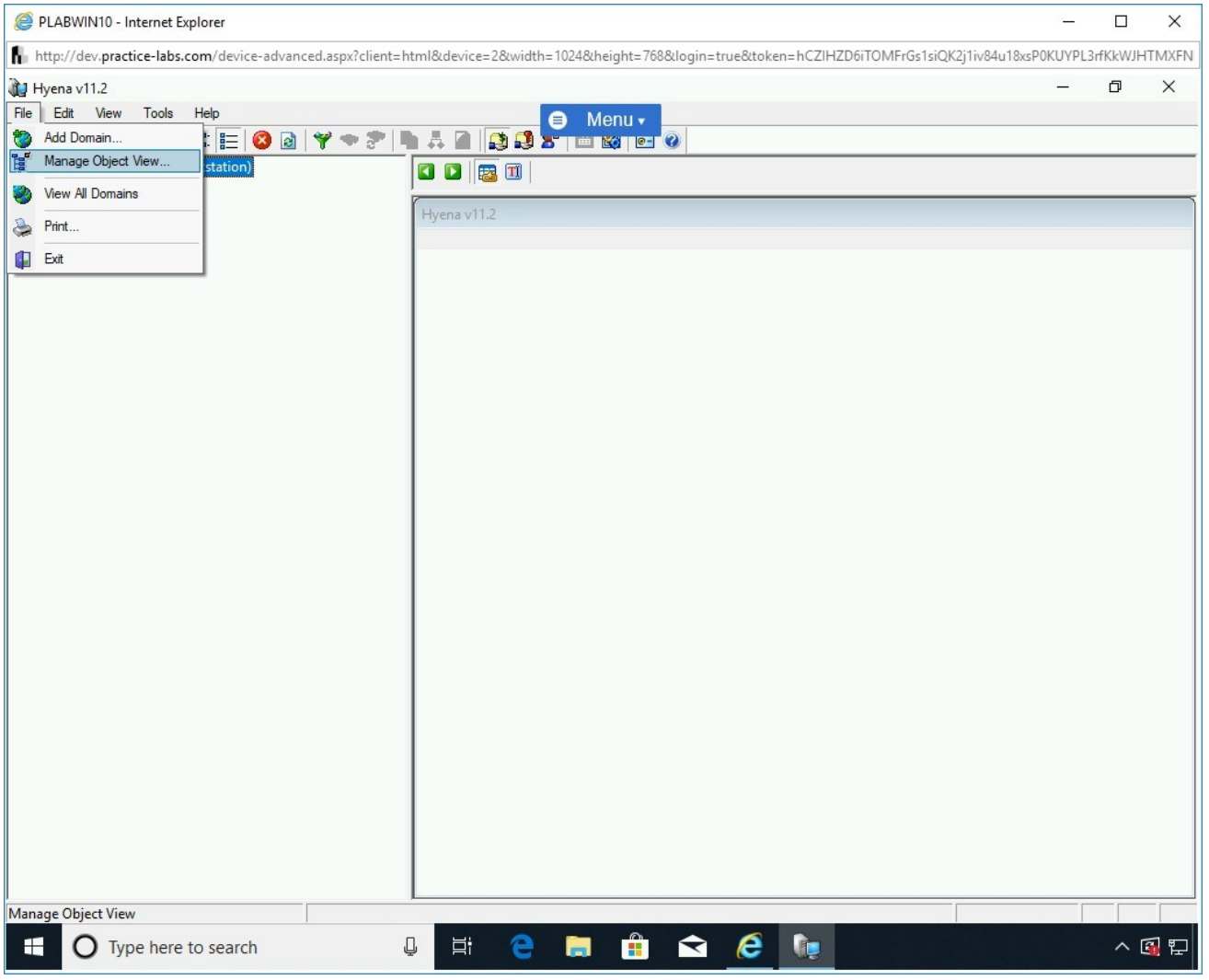


Figure 1.59Screenshot of PLABWIN10: Clicking File and then selecting Manage object view.

Step 19

In the **Object Manager Configuration** dialog box, select the **PRACTICELABS.COM** domain under the **Object Name** column and then click **Delete**.

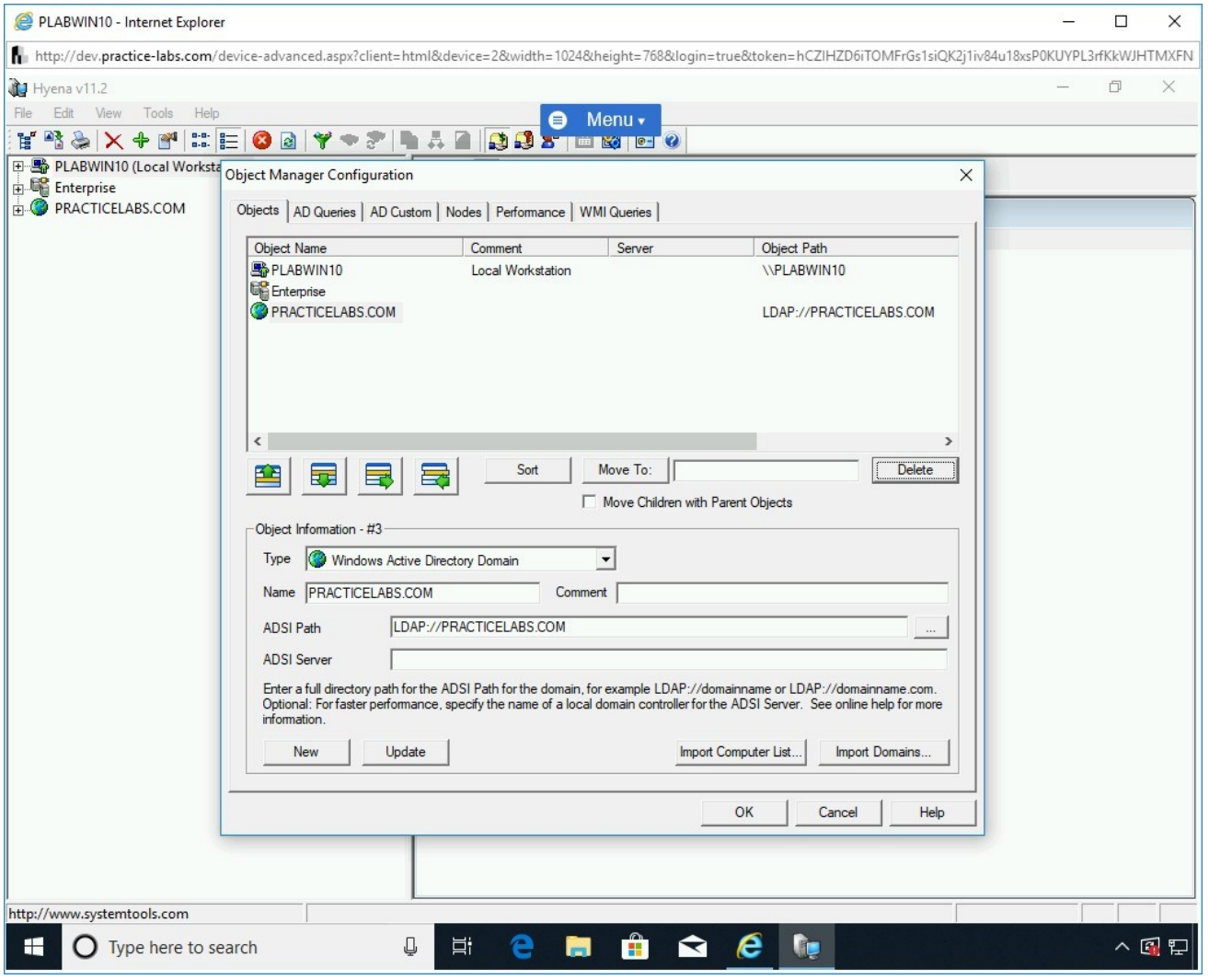


Figure 1.60 Screenshot of PLABWIN10: Selecting and deleting the domain on the Objects tab.

Step 20

The **PRACTICELABS.COM** domain is removed now. Click **OK** to close the **Object Manager Configuration** dialog box.

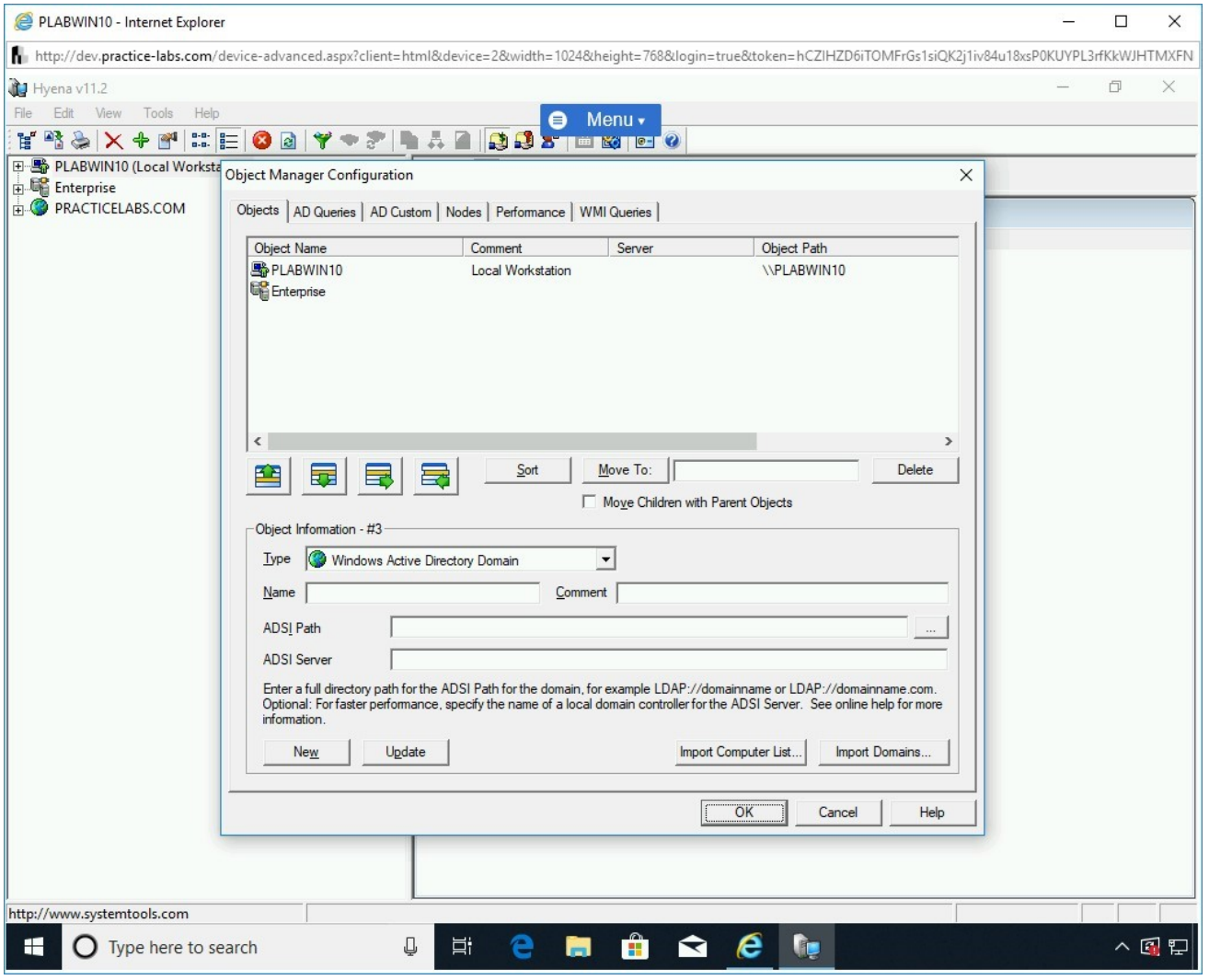


Figure 1.61 Screenshot of PLABWIN10: Clicking OK to close the Object Manager Configuration dialog box.

Step 21

You are back on the **Hyena v11.2** window. Notice that the **PRACTICELABS.COM** domain is no longer listed in the left pane. To add a domain, click **File** and select **Add Domain**.

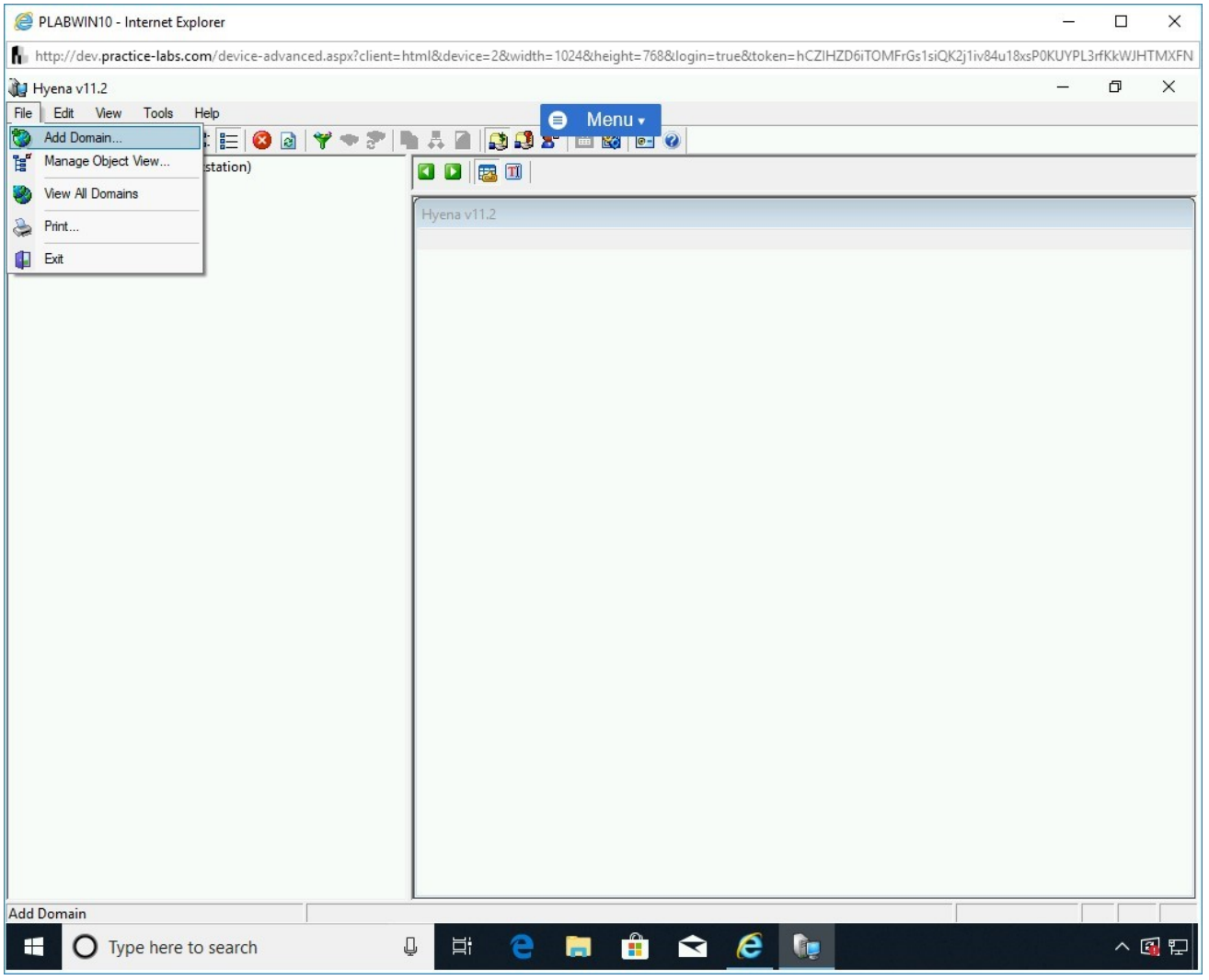


Figure 1.62 Screenshot of PLABWIN10: Adding a domain by clicking File and selecting Add Domain.

Step 22

The **Add Domain(s) to View** dialog box is displayed. In the **Domain Name** text box, type the following domain name:

```
PRACTICELABS.COM
```

Click **OK**.

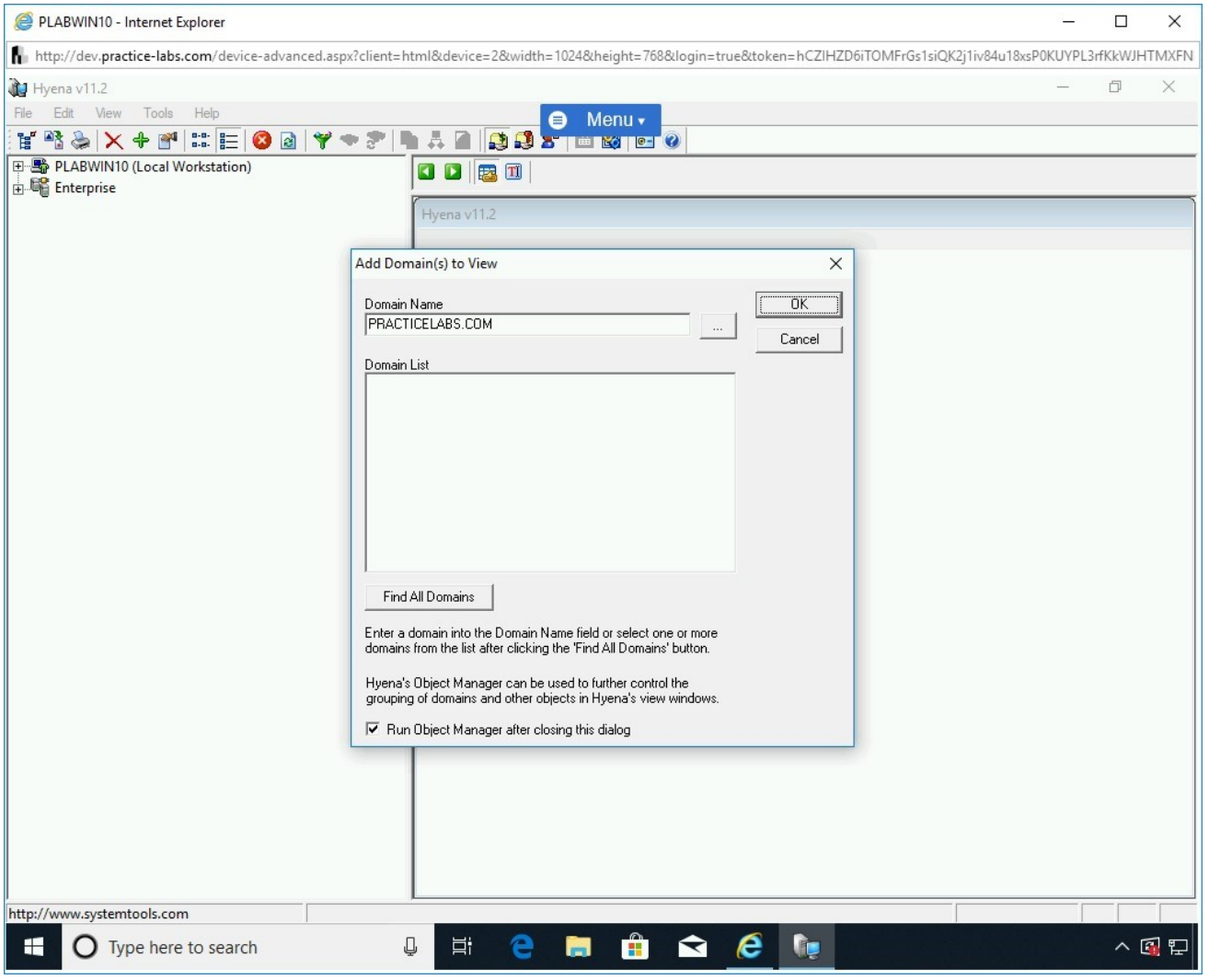


Figure 1.63 Screenshot of PLABWIN10: Typing the domain name in the Domain Name text box and clicking OK.

Step 23

The **PRACTICELABS.COM** domain appears in the left pane. Along with this, the **Object manager Configuration** opens automatically.

Click **OK** to close it.

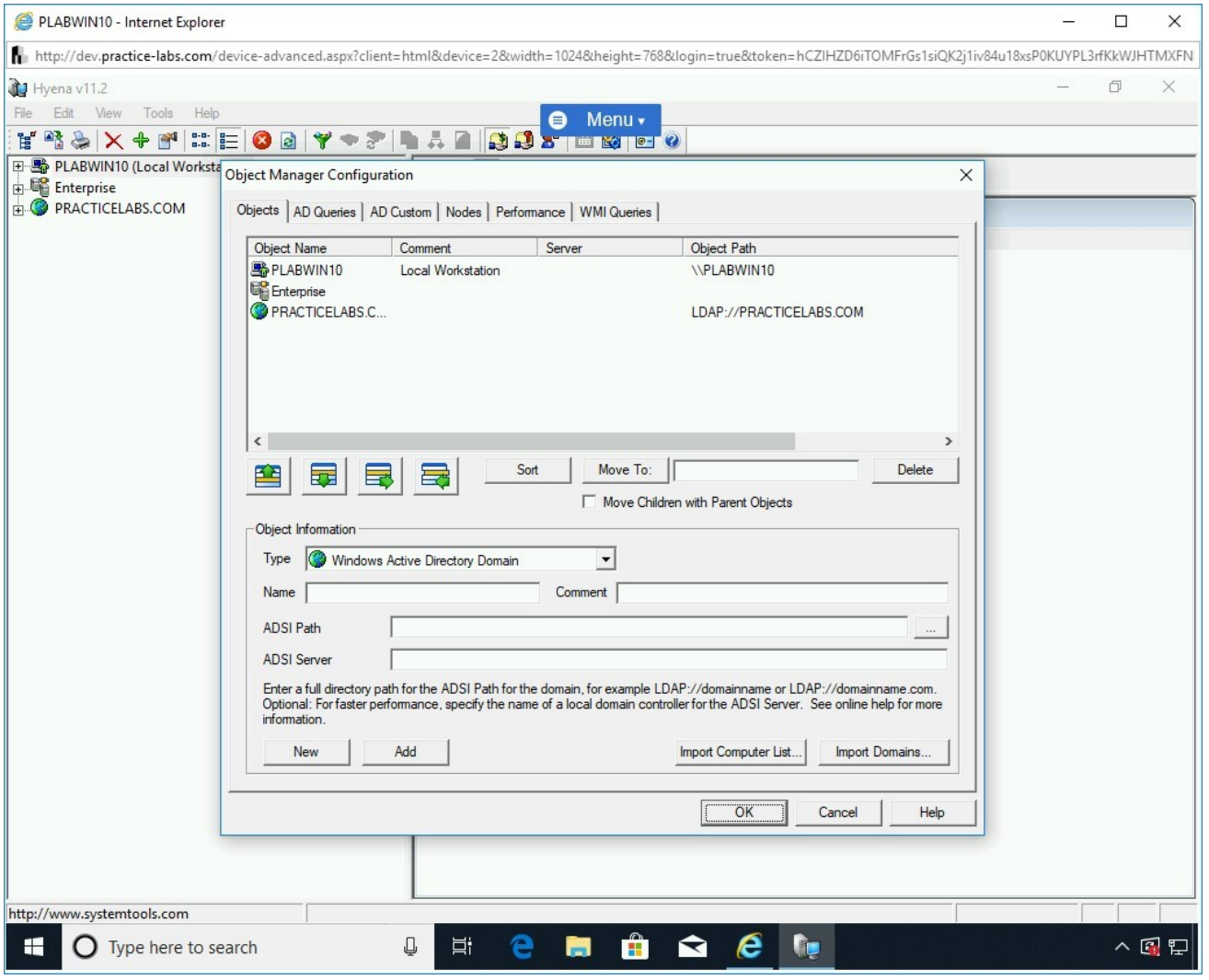


Figure 1.64 Screenshot of PLABWIN10: Showing the added domain name and clicking OK.

Step 24

In the left pane, expand **PRACTICELABS.COM**. The **Admin Tools Reminder** dialog box is displayed. Click **OK**.

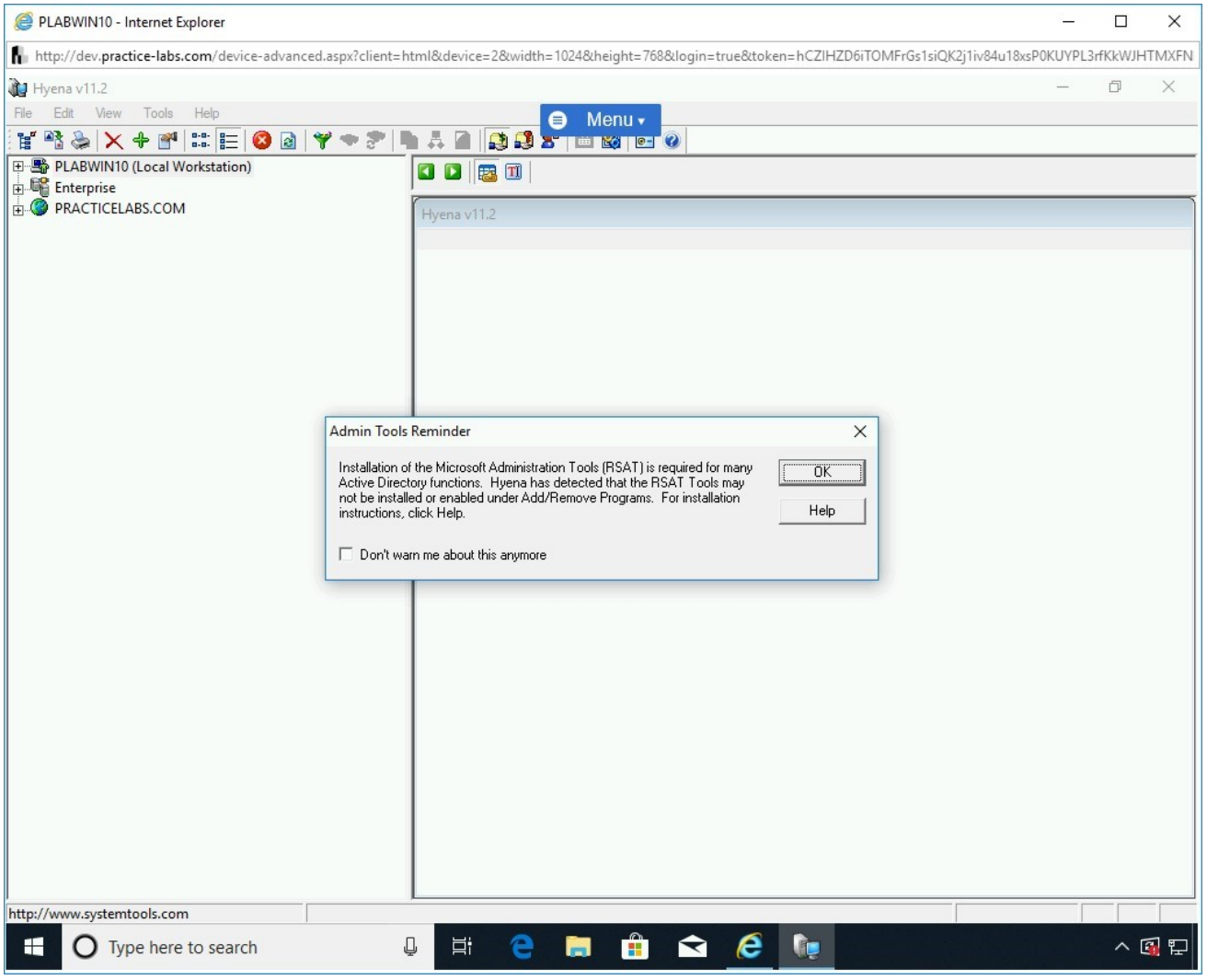


Figure 1.65 Screenshot of PLABWIN10: Clicking OK on the Admin Tools Reminder dialog box.

Step 25

You should now notice several nodes that are now visible below **PRACTICELABS.COM**.

Expand **Domain Controllers**, expand **PLABDC01**, and then double-click **Services**.

> ***Note**: You can click on various nodes and view information.*

Notice that a list of services running on **PLABDC01** is displayed. You can also view their current status.

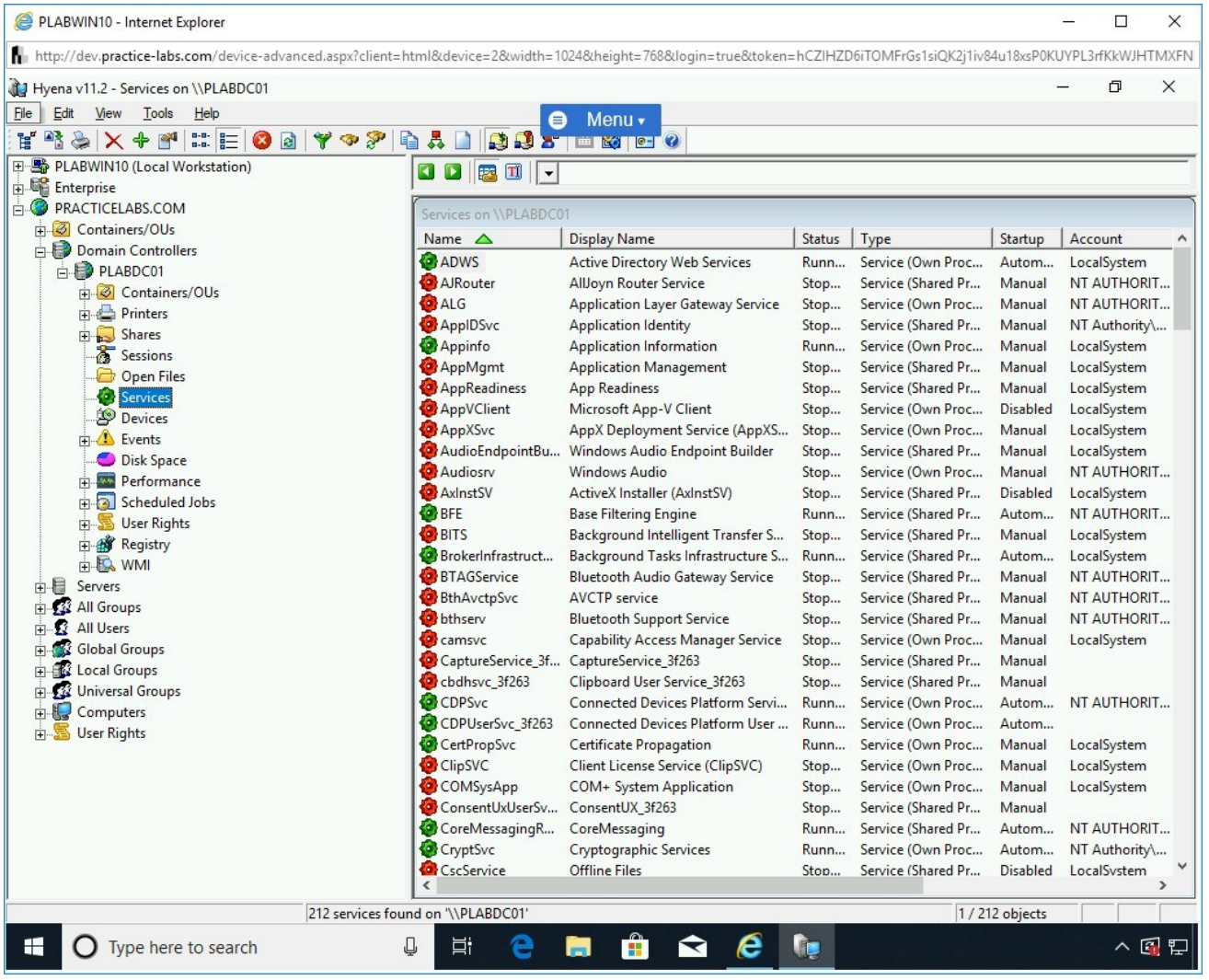


Figure 1.66 Screenshot of PLABWIN10: Double-clicking Services in the left pane and showing the services in the right pane.

Step 26

Double-click **Sessions**.

The right pane displays the number of established sessions.

> ***Note**: The current number of users may vary from the screenshot below.*

At present, there is only one session, which is established by the **Administrator**.

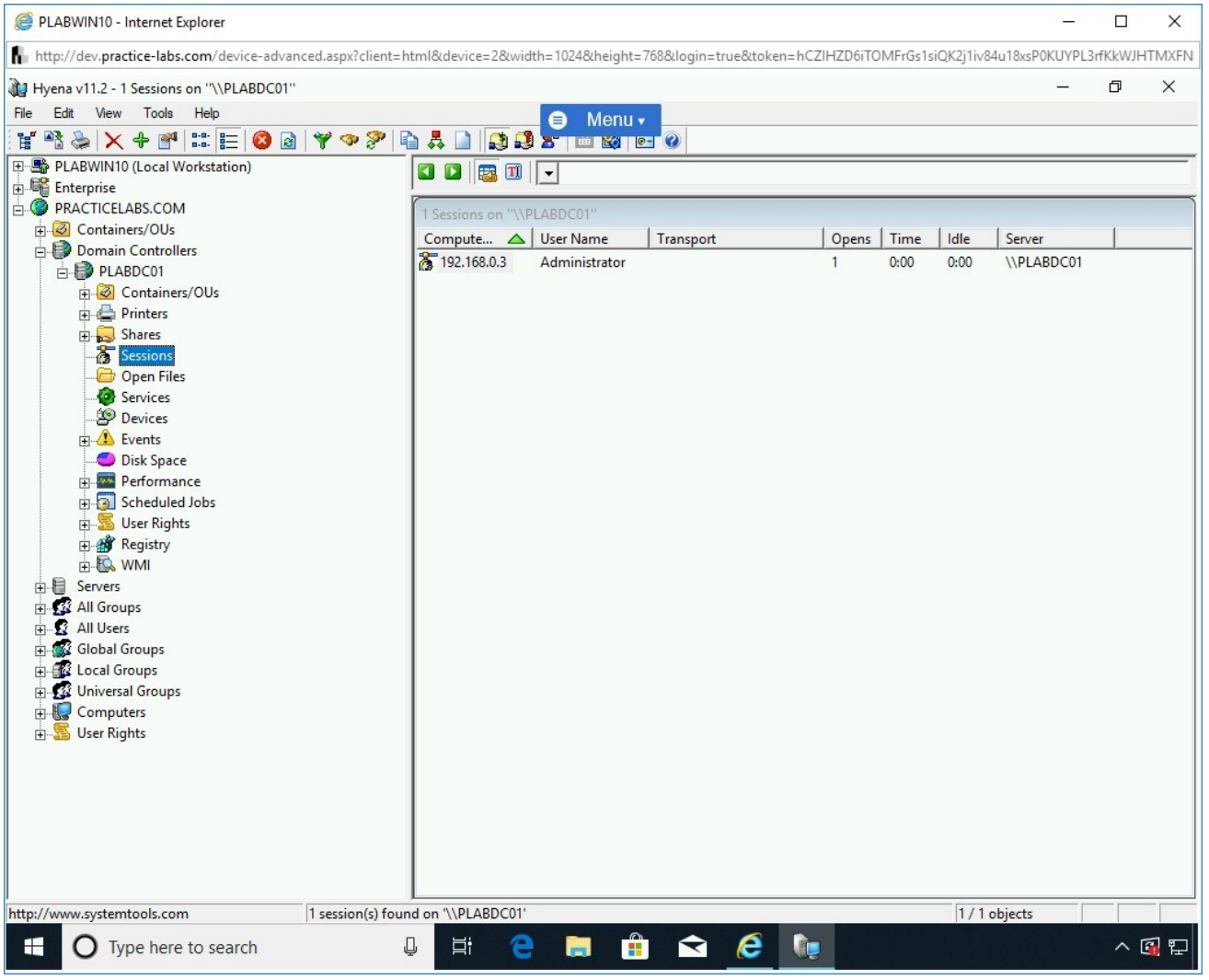


Figure 1.67 Screenshot of PLABWIN10: Double-clicking Sessions in the left pane and showing the live sessions in the right pane.

Step 27

Double-click **Disk Space**.

The right pane displays the available drives and information on disk space, such as total, free, and used space.

Close the **Hyena v11.2** window.

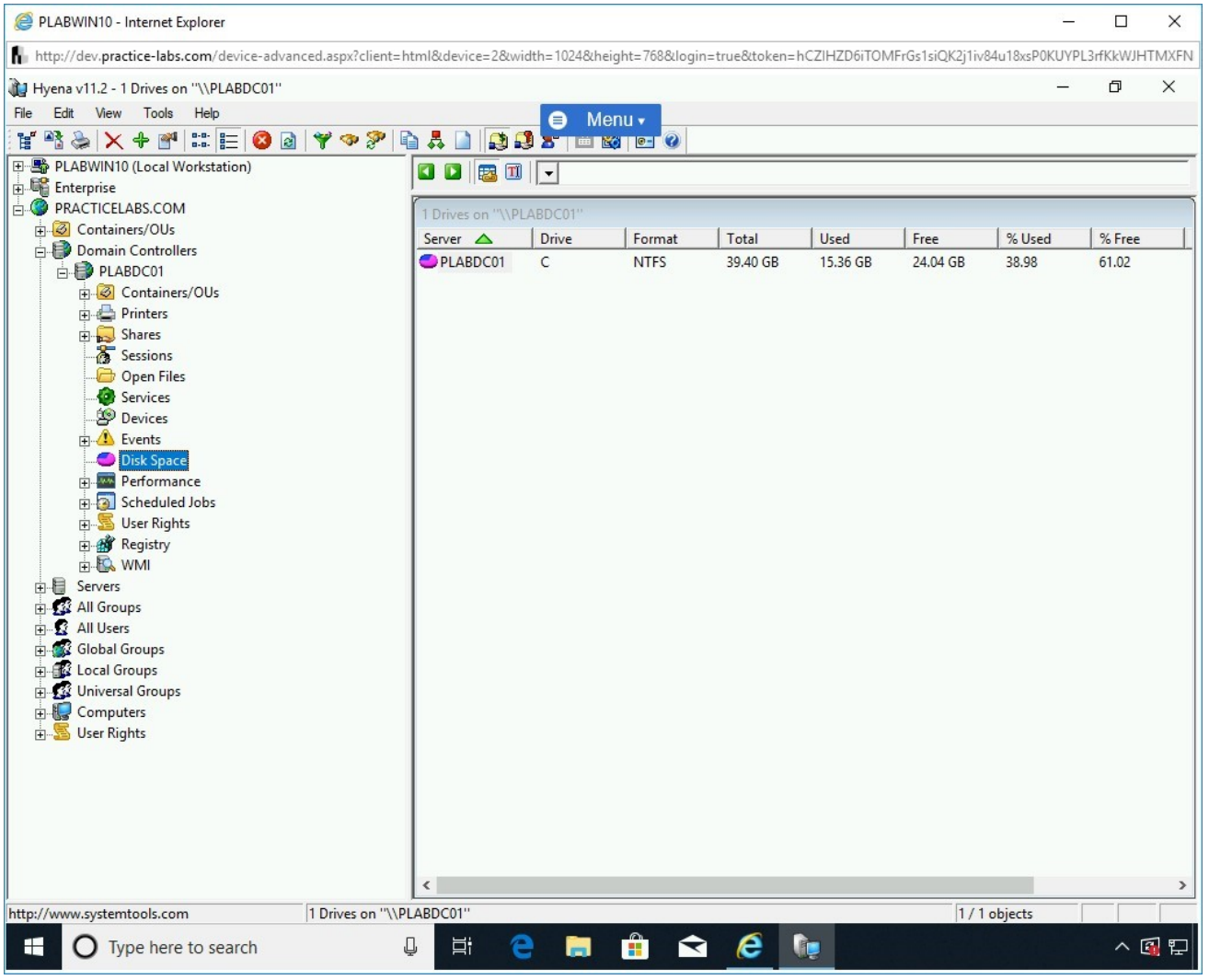


Figure 1.68 Screenshot of PLABWIN10: Double-clicking Disk Space in the left pane and showing the disk status in the right pane.

Keep the **Internet Explorer** window open.

Task 3 - Perform LDAP Enumeration Using Softerra LDAP Administrator

Softerra LDAP Administrator is an LDAP management tool. You can use it to perform various LDAP operations.

In this task, you will perform LDAP enumeration using Softerra LDAP Administrator. 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.**

Ensure that **Internet Explorer** is open, and you are on the Hacking Tools page.

> ***Note:*** *If you closed Internet Explorer in the previous task, please ensure you follow the steps provided in Task 1 to reach the Hacking Tools page.*

On the **Hacking Tools** Webpage, scroll to locate **ldapadmin-4.12.15229.0-x86-eng.msi**. Click **ldapadmin-4.12.15229.0-x86-eng.msi**.

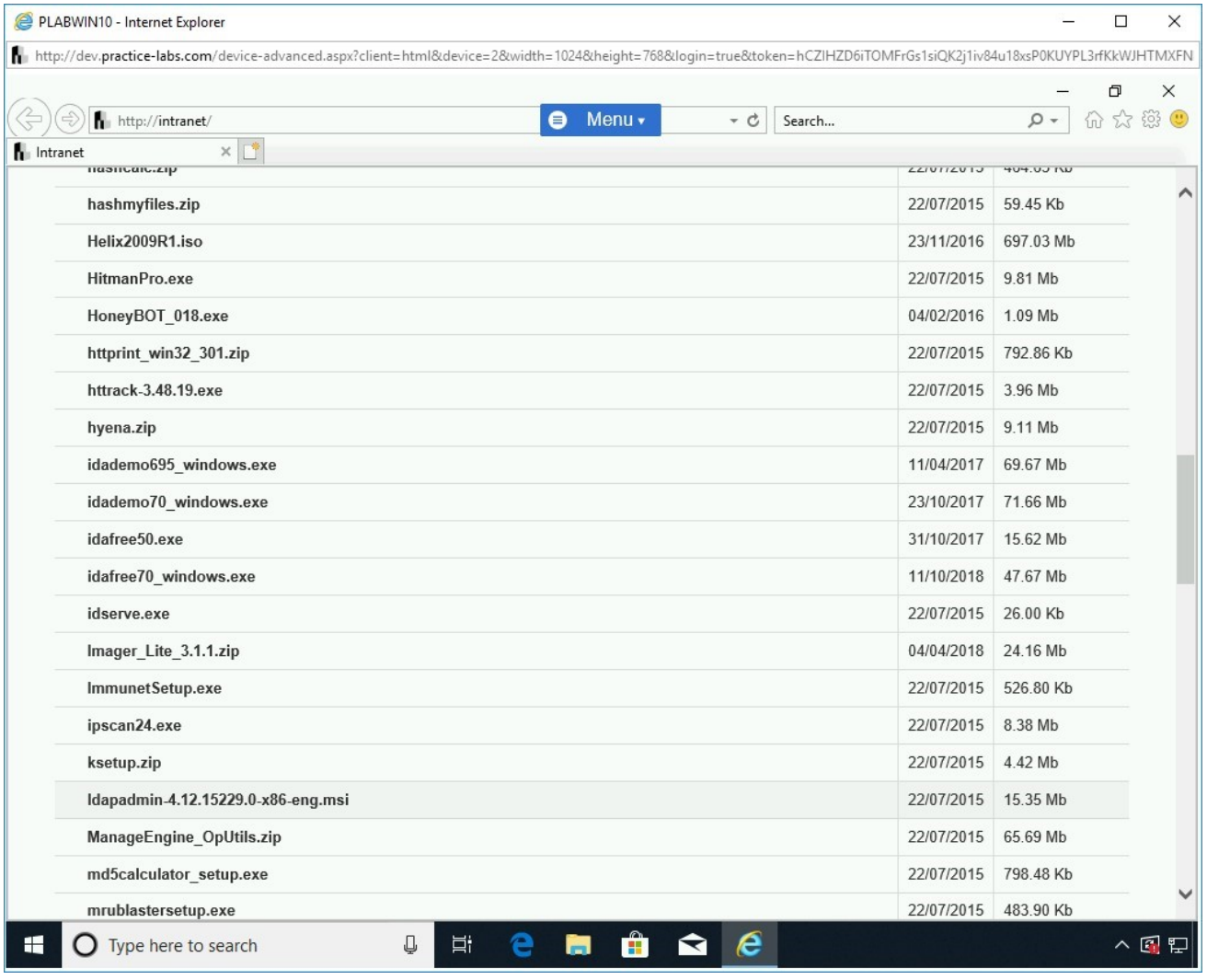


Figure 1.69 Screenshot of PLABWIN10: Clicking ldapadmin-4.12.15229.0-x86-eng.msi on the Hacking Tools page.

Step 2

In the notification bar, click **Save.**

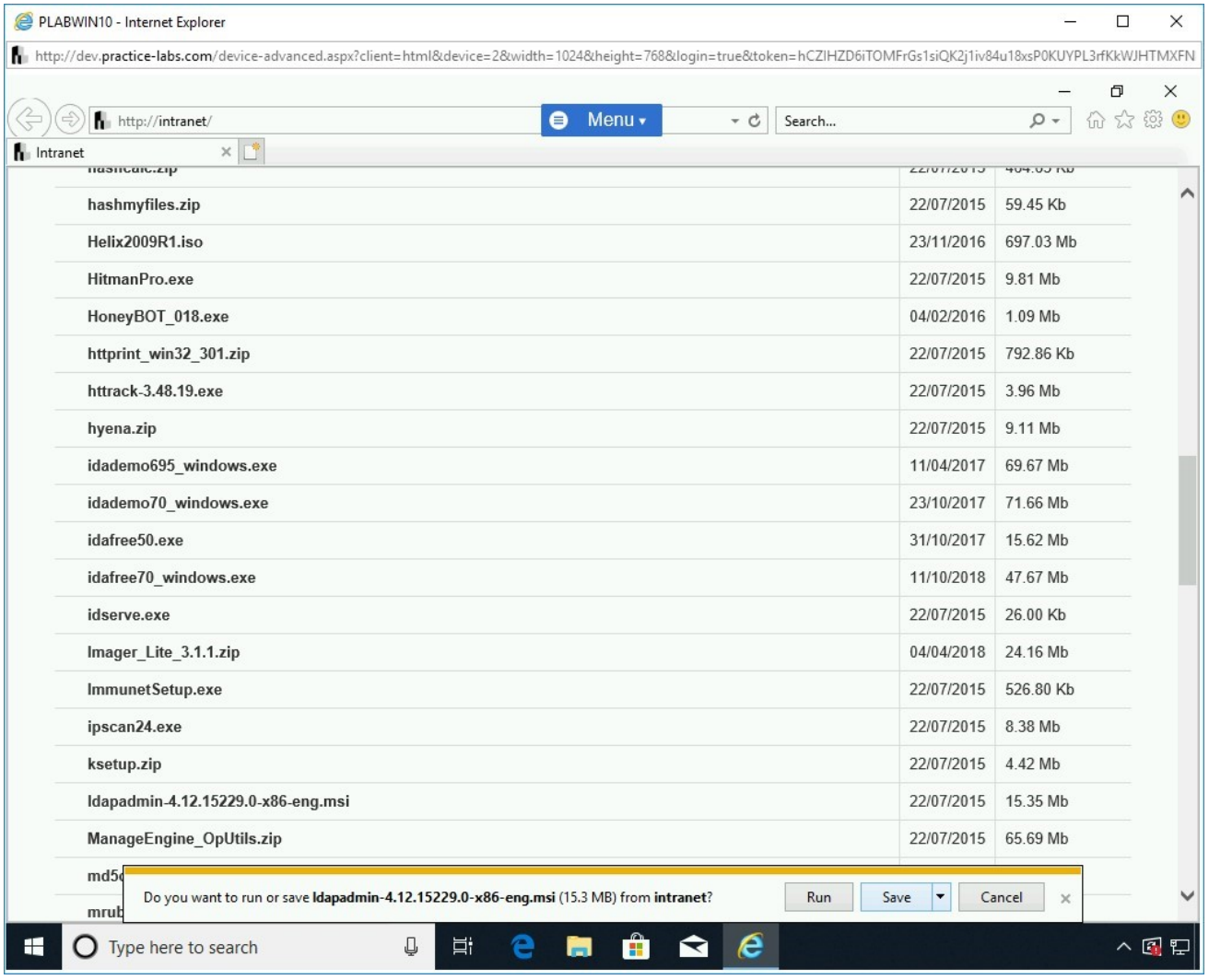


Figure 1.70 Screenshot of PLABWIN10: Clicking Save on the notification bar.

Step 3

In the notification bar, click **Run**.

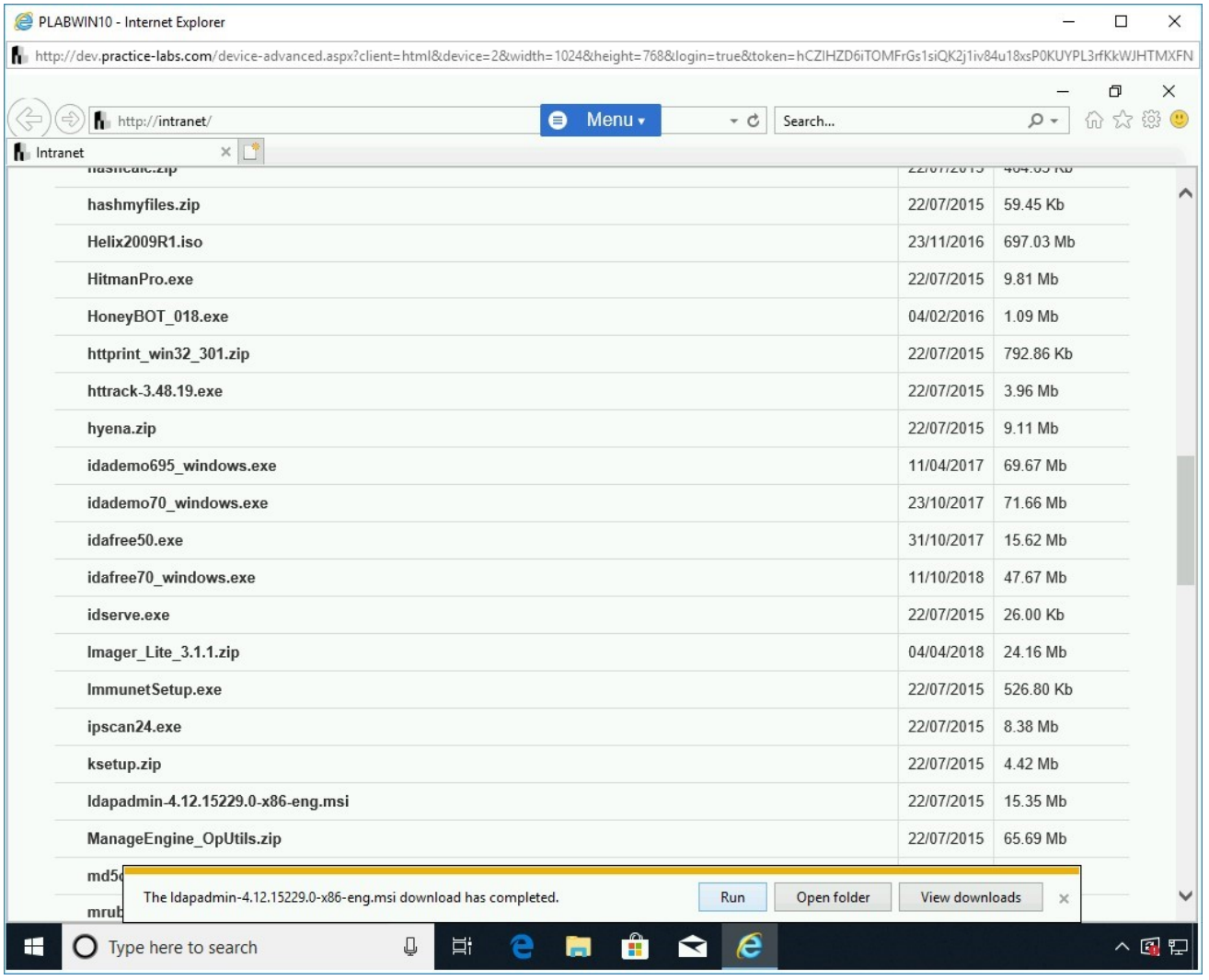


Figure 1.71 Screenshot of PLABWIN10: Clicking Run on the notification bar.

Step 4

On the **Welcome to the Softerra LDAP Administrator 2015.1 Installation Wizard** page of the **Softerra LDAP Administrator 2015.1 Setup** wizard, click **Next**.

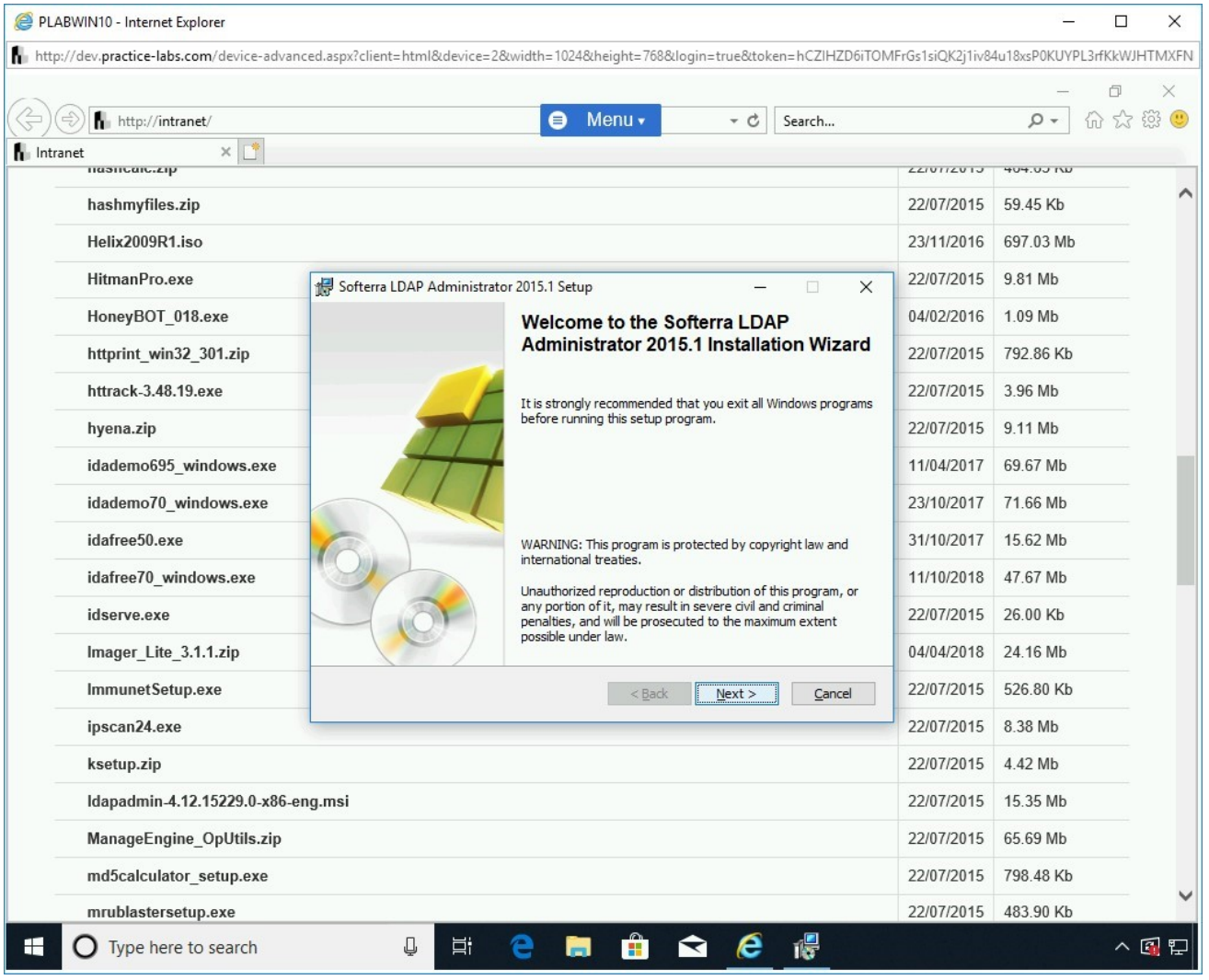


Figure 1.72 Screenshot of PLABWIN10: Clicking Next on the Softerra LDAP Administrator 2015.1 Setup Wizard page.

Step 5

On the **License Agreement** page, select **I accept the license agreement** and click **Next**.

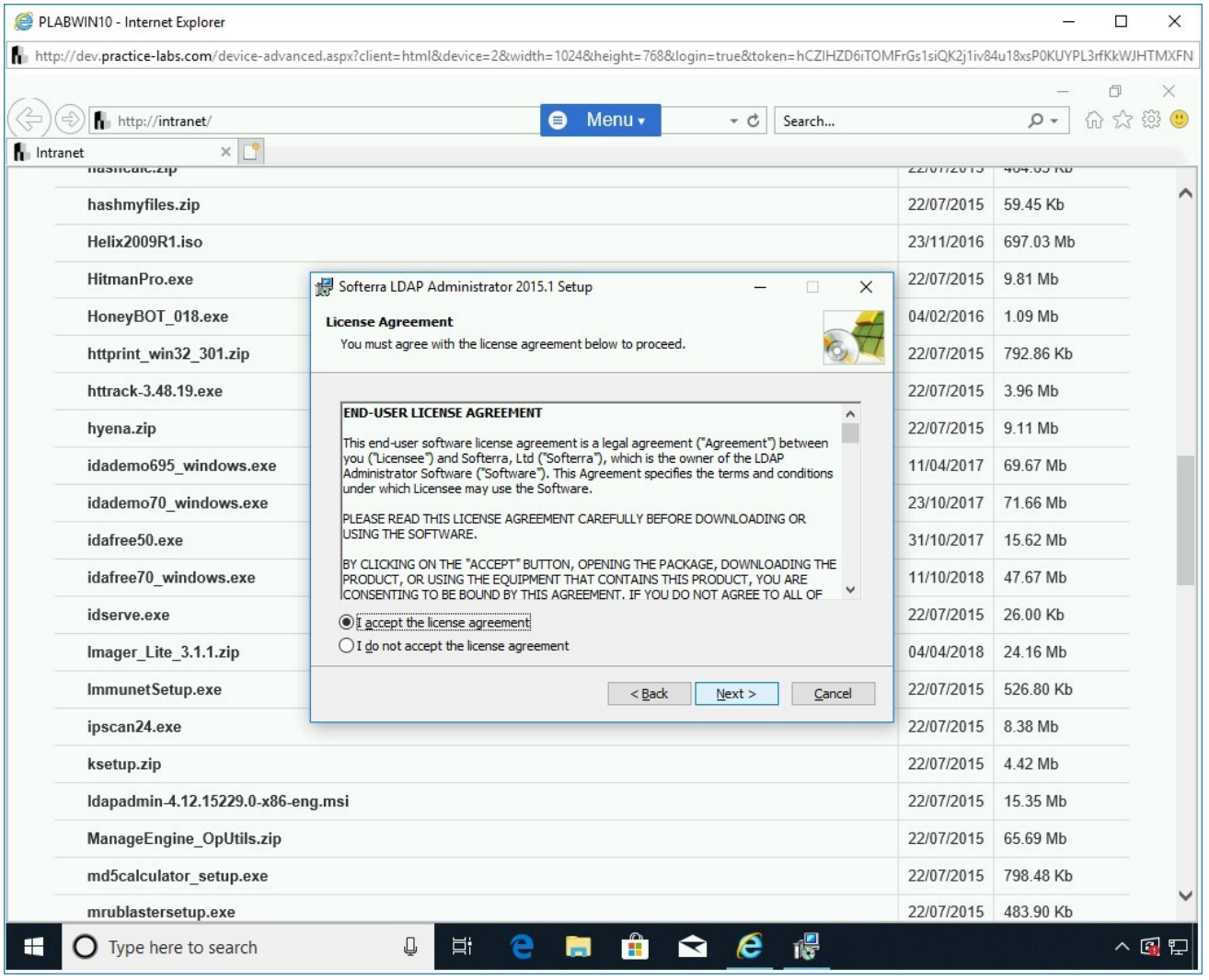


Figure 1.73 Screenshot of PLABWIN10: Selecting I accept the license agreement and clicking Next.

Step 6

On the **Readme Information** page, scroll and read through the information. Click **Next**.

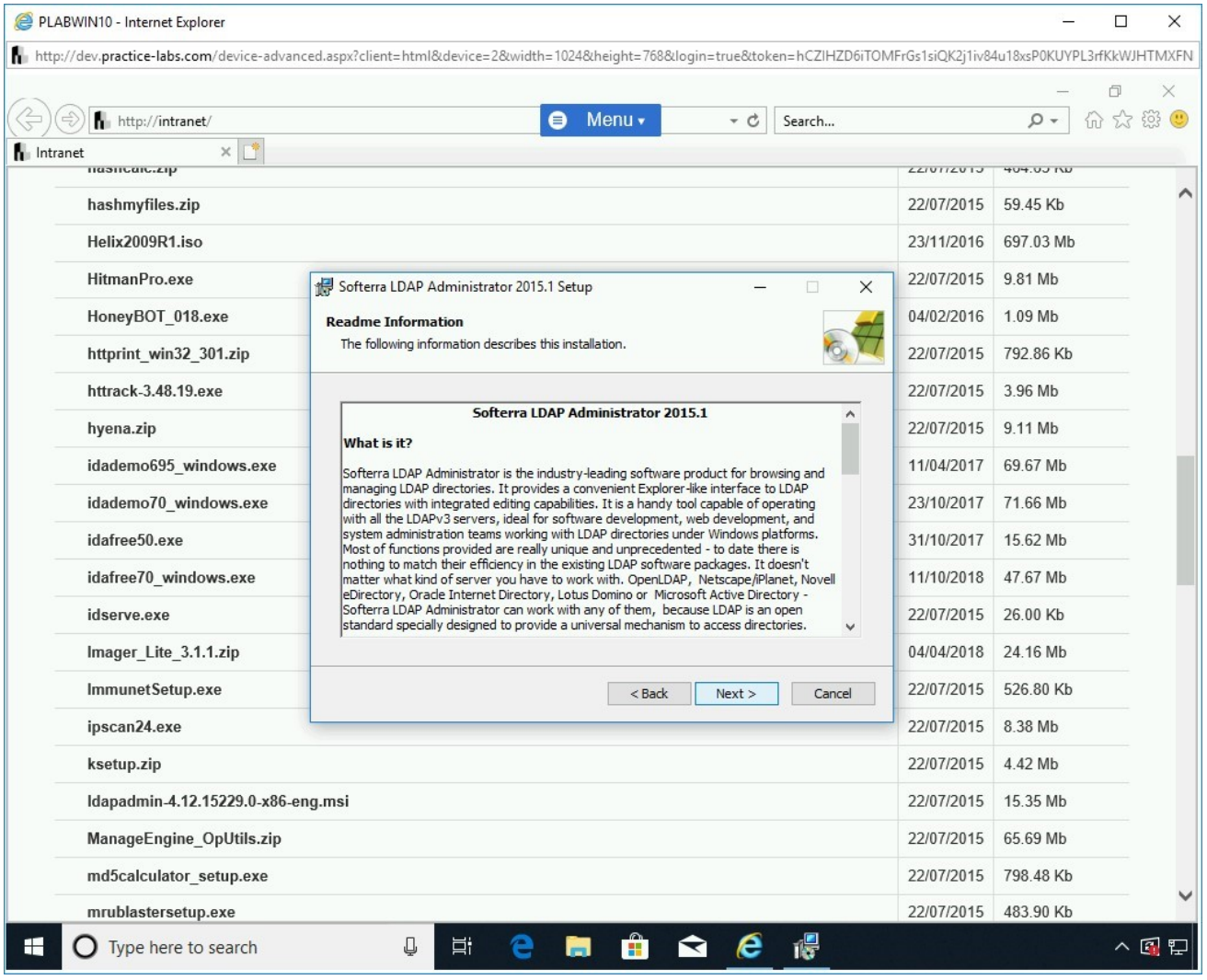


Figure 1.74 Screenshot of PLABWIN10: Clicking Next on the Readme Information page.

Step 7

On the **Destination Folder** page, keep the default installation path and click **Next**.

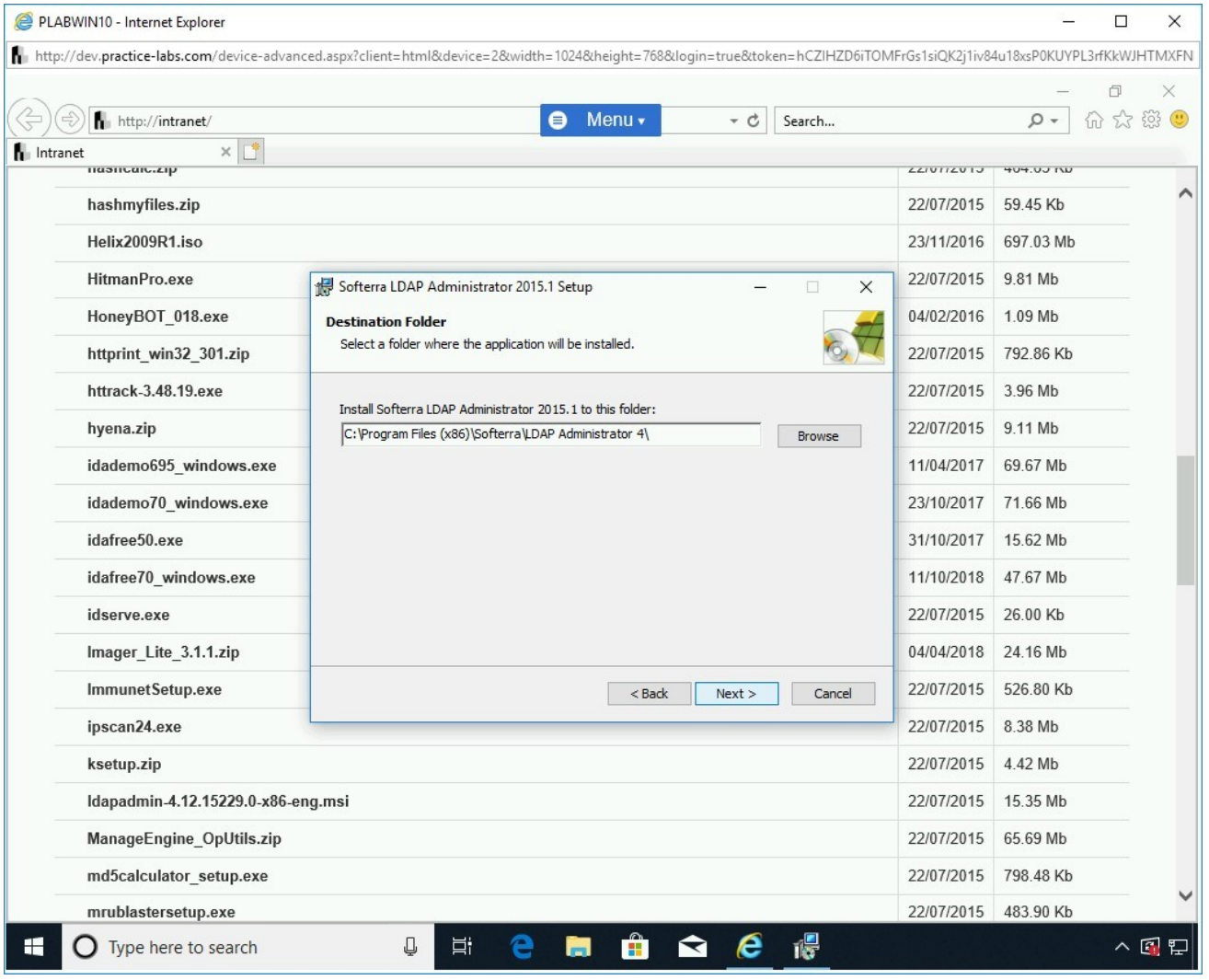


Figure 1.75 Screenshot of PLABWIN10: Keeping the default installation path on the Destination Folder page and clicking Next.

Step 8

On the **Select Installation Type** page, **Typical** is selected by default. Keep the default selection, click **Next**.

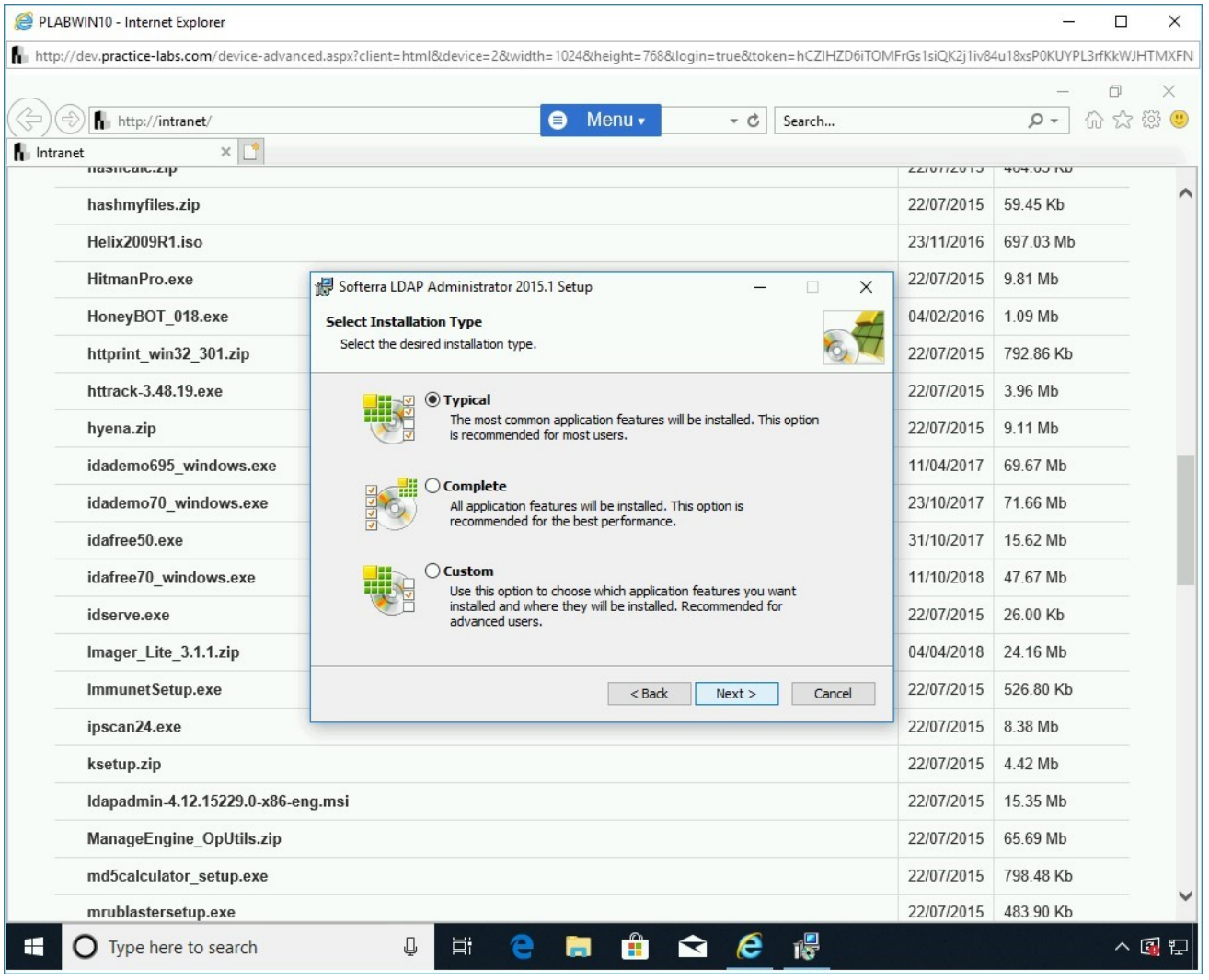


Figure 1.76 Screenshot of PLABWIN10: Keeping the default selection and clicking Next on the Select Installation Type page.

Step 9

On the **Ready to Install the Application** page, click **Next**.

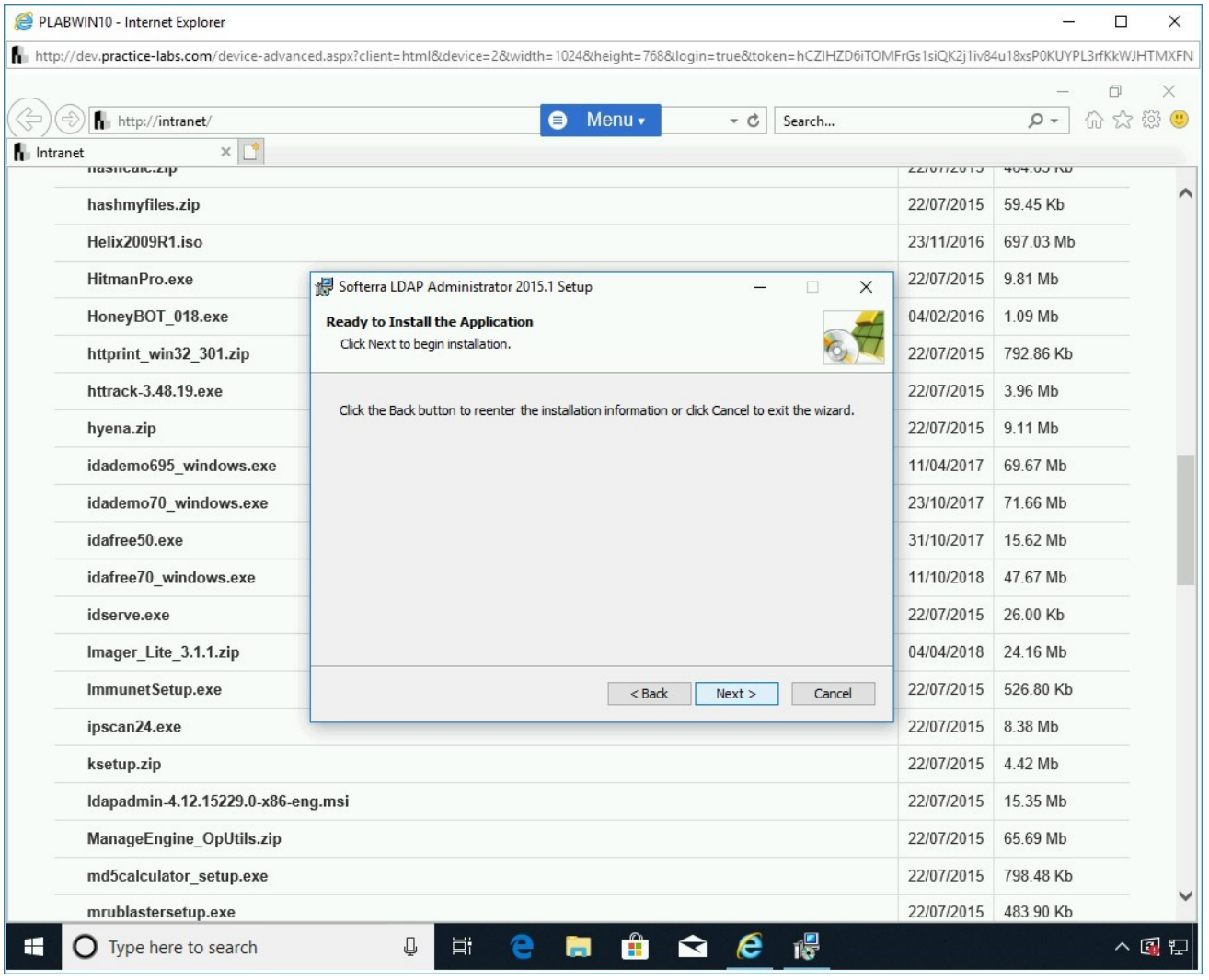


Figure 1.77 Screenshot of PLABWIN10: Clicking Next on the Ready to Install the Application page.

Step 10

On the **Updating System** page, installation progress is displayed.

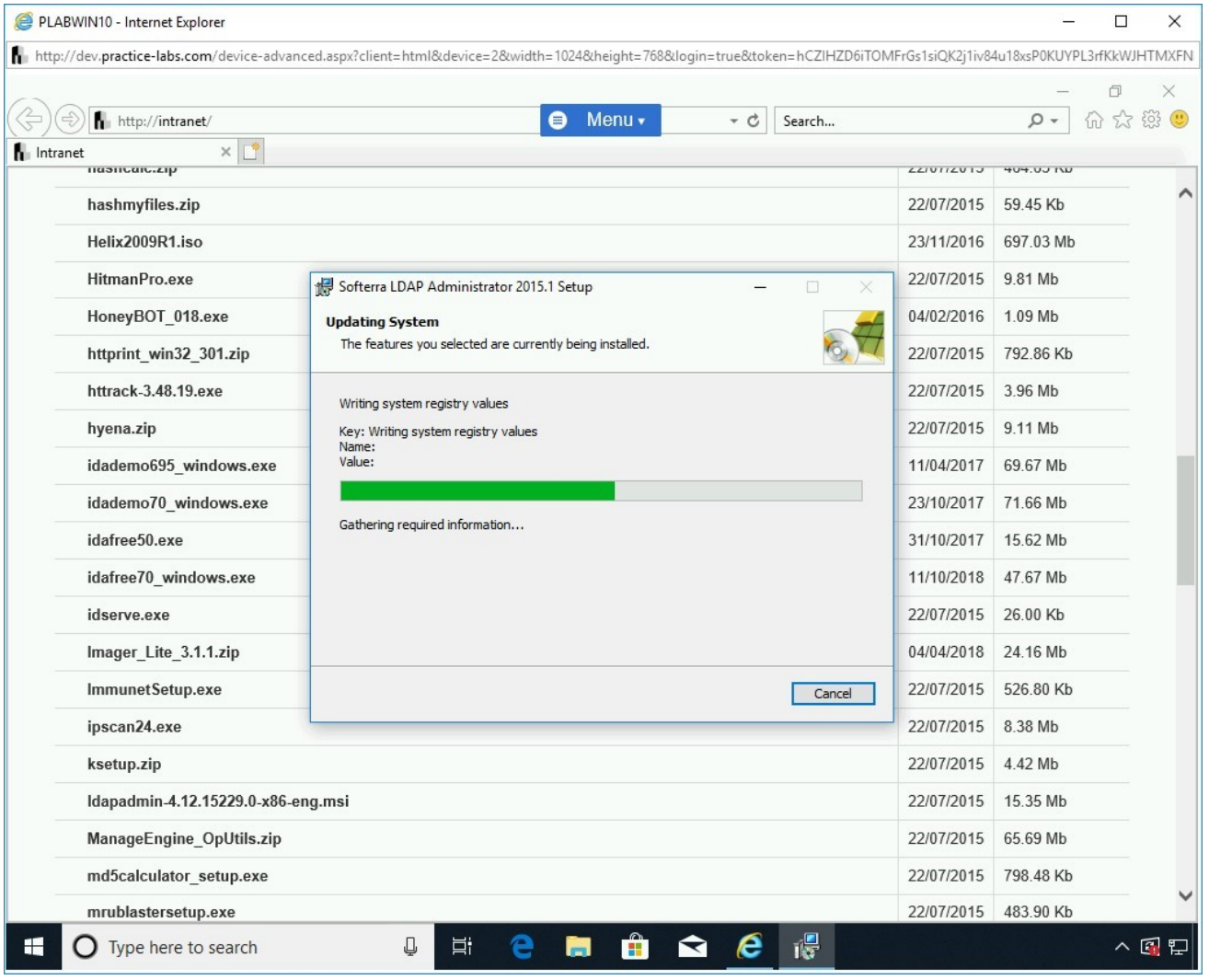


Figure 1.78 Screenshot of PLABWIN10: Showing the installation progress on the Updating System page.

Step 11

On the **Softerra LDAP Administrator 2015.1 has been successfully installed** page, click **Finish**.

Minimize the **Internet Explorer** window.

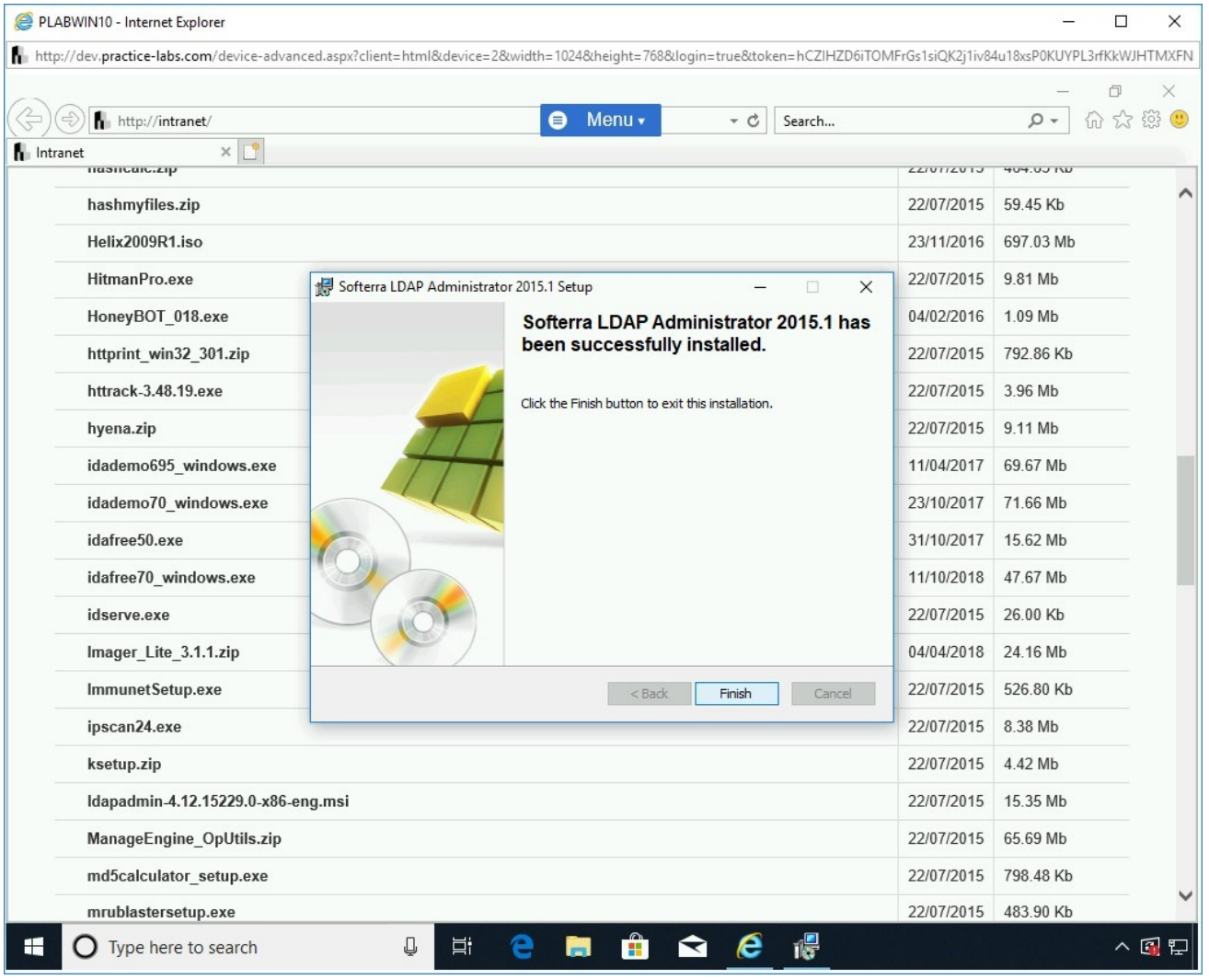


Figure 1.79 Screenshot of PLABWIN10: Clicking Finish on the Softerra LDAP Administrator 2015.1 has been successfully installed page.

Step 12

Double-click the **Softerra LDAP Administrator 2015.1** icon on the desktop.

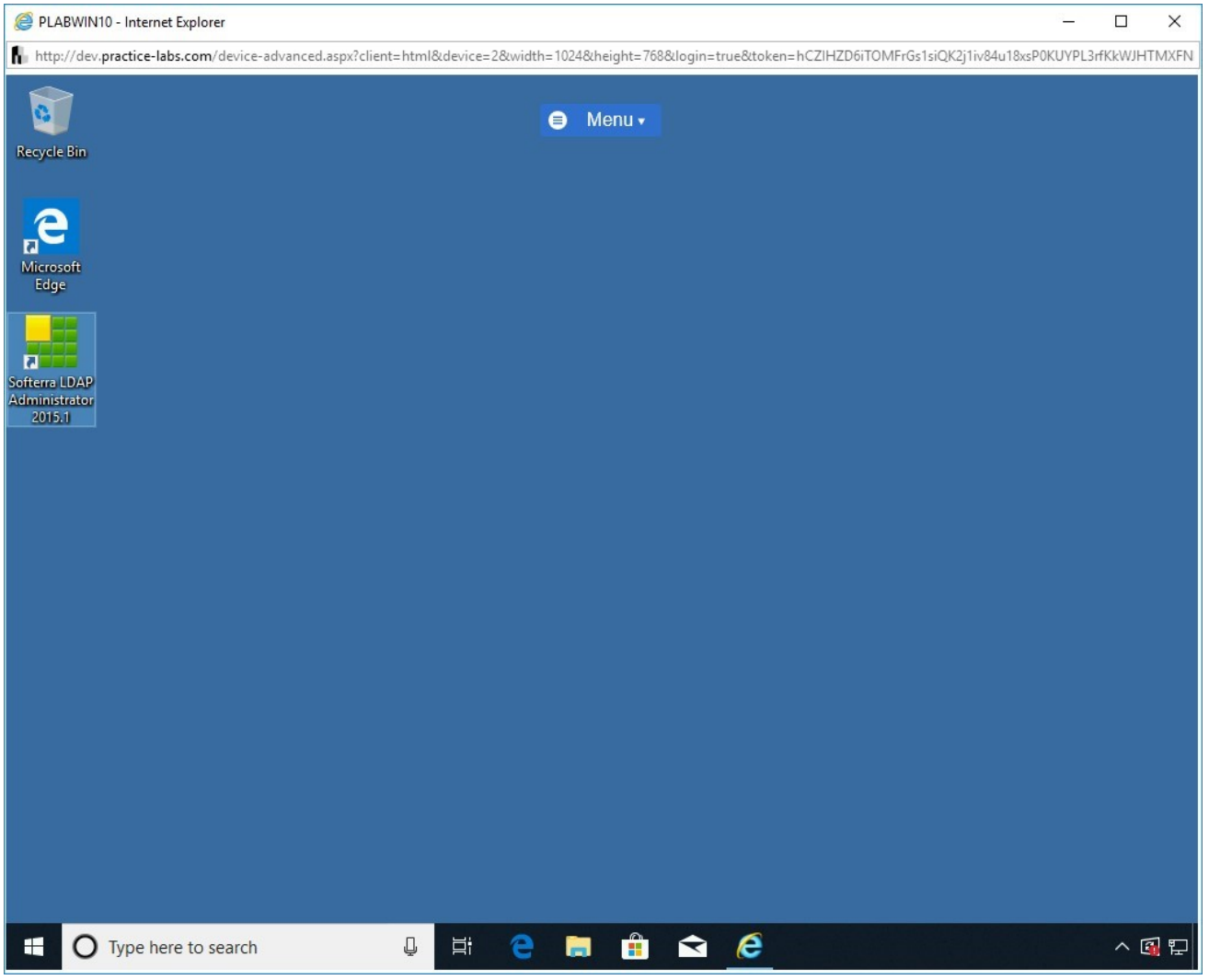


Figure 1.80 Screenshot of PLABWIN10: Double-clicking the Softerra LDAP Administrator 2015.1 icon on the desktop.

Step 13

The **Softerra LDAP Administrator 2015.1** window is displayed.

Select **Remember my preference** and click **Yes**.

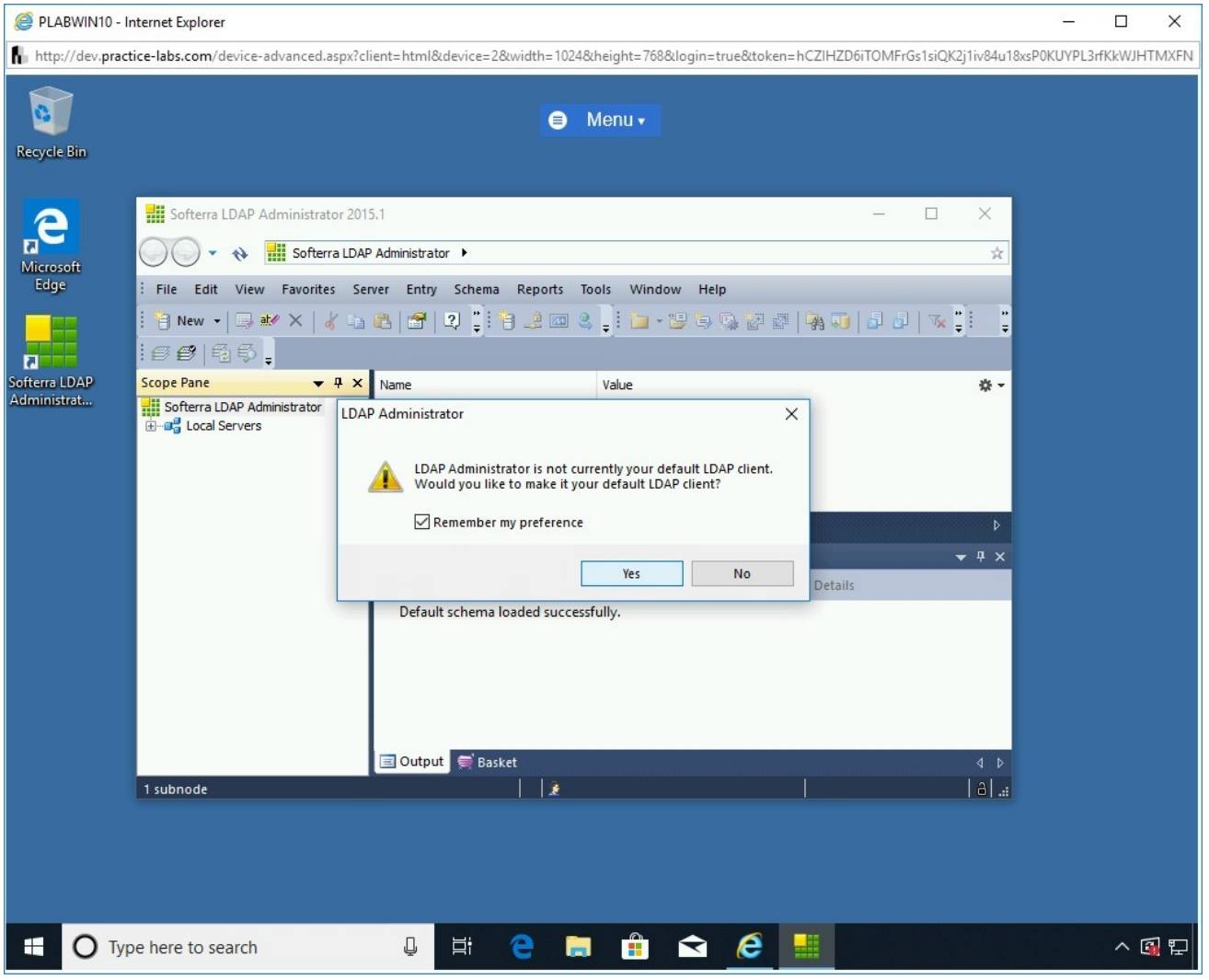


Figure 1.81 Screenshot of PLABWIN10: Selecting Remember my preference and clicking Yes.

Step 14

From the top menu bar, click **Server** and select **New Profile**.

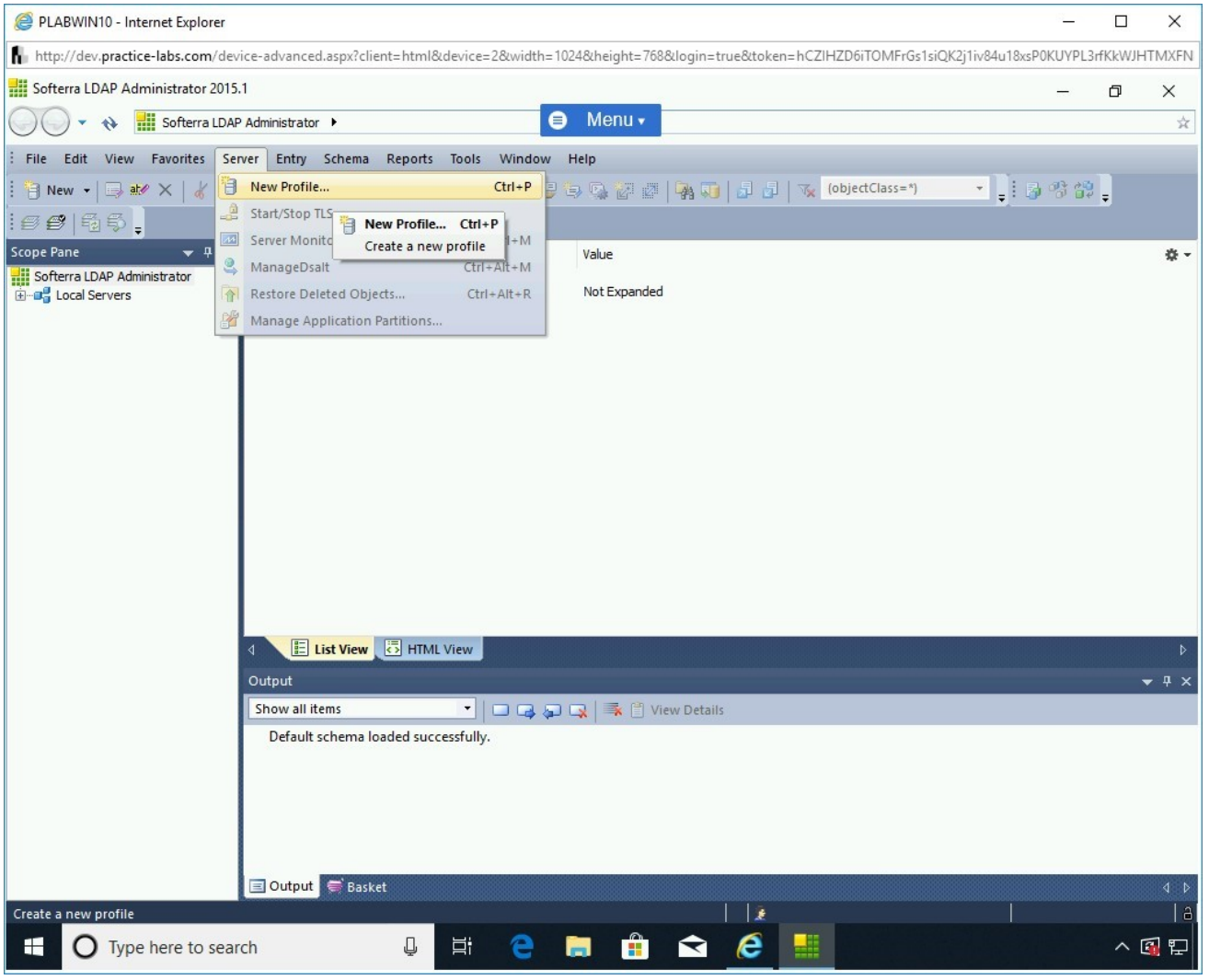


Figure 1.82 Screenshot of PLABWIN10: Clicking Server and selecting New Profile.

Step 15

The **Profile Creation Wizard - Step 1** wizard is displayed. On the **Server Profile Name** page, enter the following in the **Profile Name** textbox:

PLAB

Click **Next**.

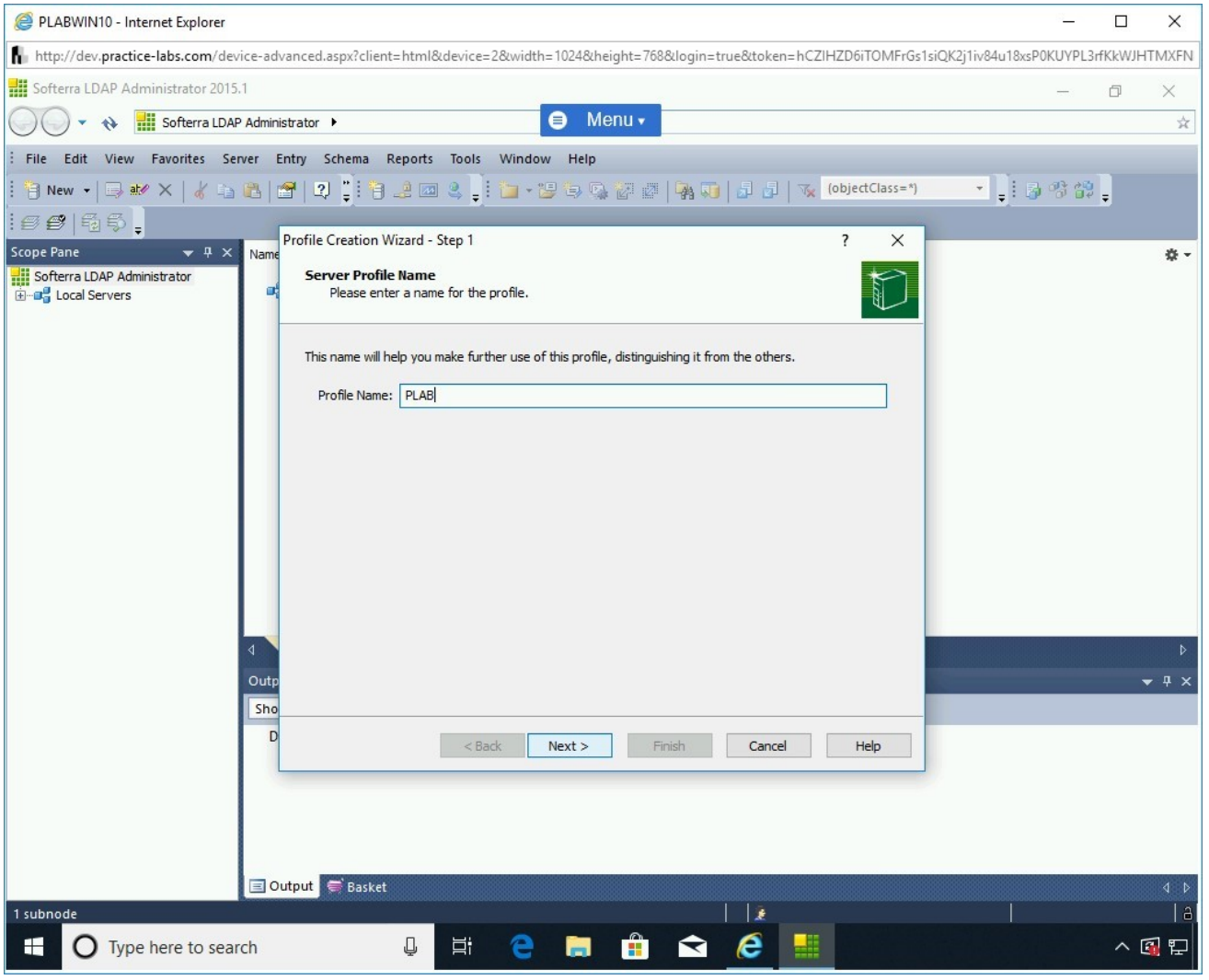


Figure 1.83 Screenshot of PLABWIN10: Entering PLAB in the Profile Name textbox and clicking Next on the Server Profile Name page.

Step 16

On the **Profile Generation Information** page, in the **Host** text box, type the following name:

```
PLABDC01
```

Click **Lookup Servers**.

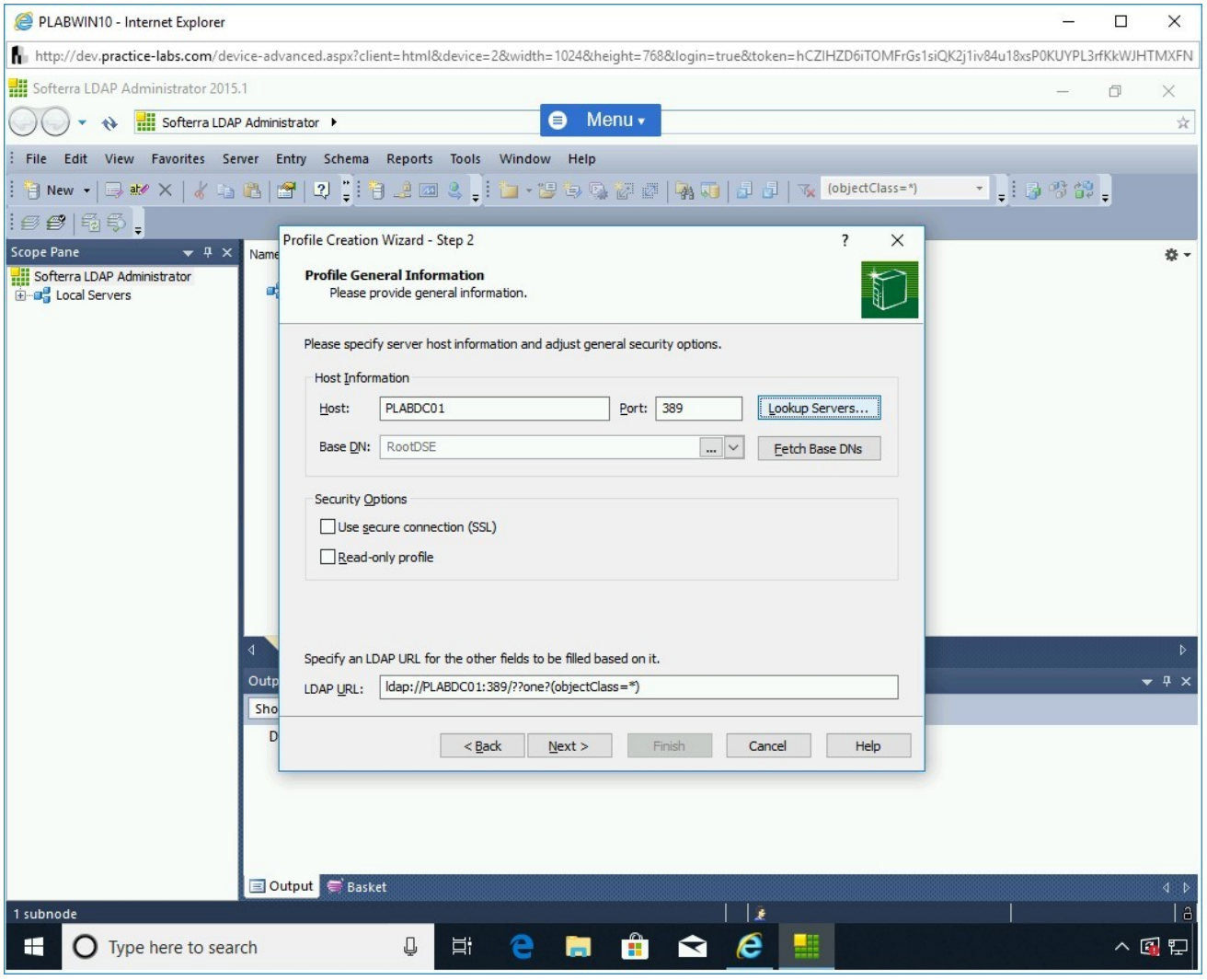


Figure 1.84 Screenshot of PLABWIN10: Entering the hostname and clicking Lookup Servers.

Step 17

The **Lookup LDAP Servers** dialog box is displayed. **PRACTICELABS.COM** will be populated automatically in the **Lookup in domain** textbox.

The **Available servers** textbox displays **PLABDC01.PRACTICELABS.COM:389**. Select it and click **Select**.

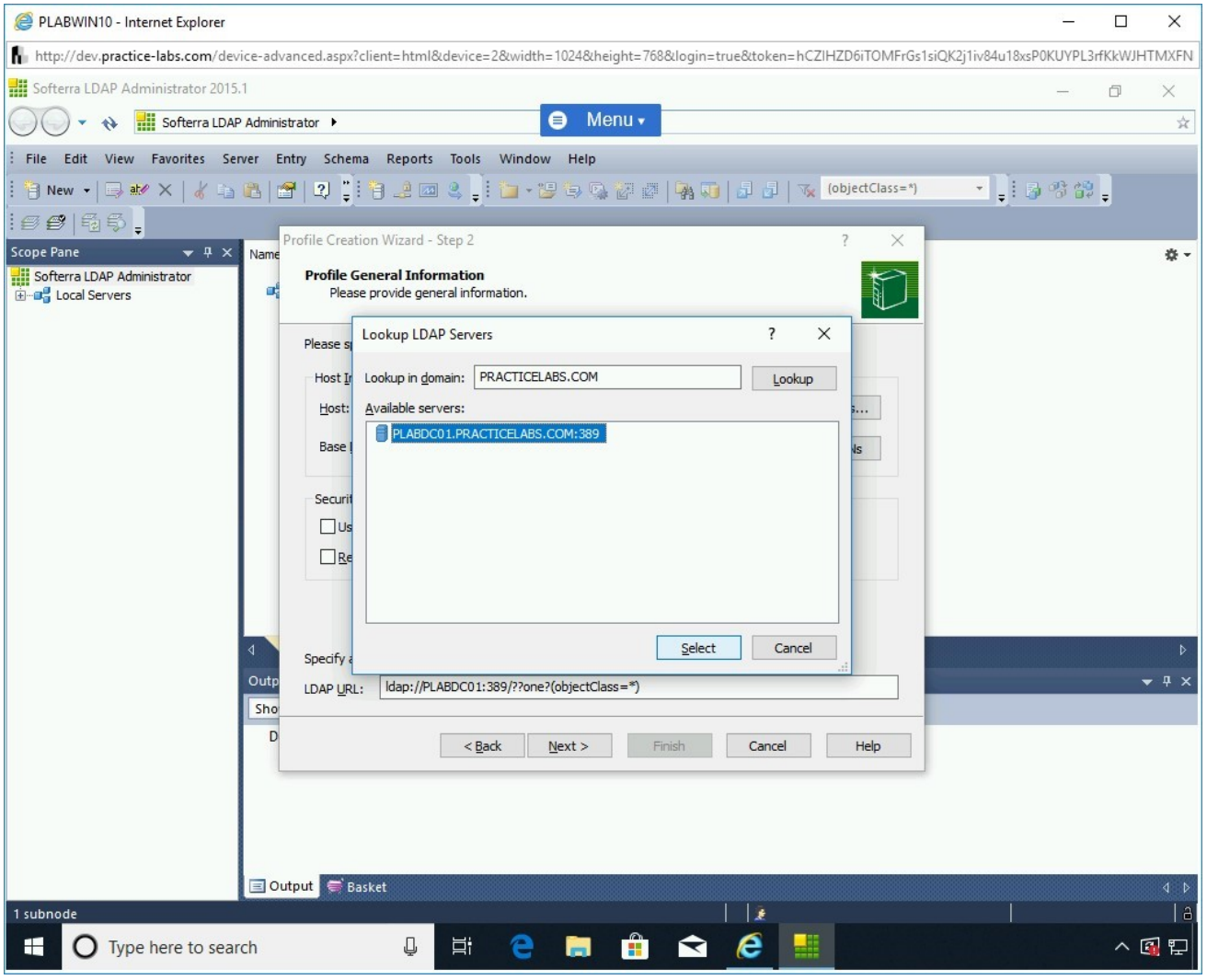


Figure 1.85 Screenshot of PLABWIN10: Selecting PLABDC01.PRACTICELABS.COM:389 and clicking Select.

Step 18

You are back on the **Profile Creation Wizard**. Note that all the information is now populated. Click **Next**.

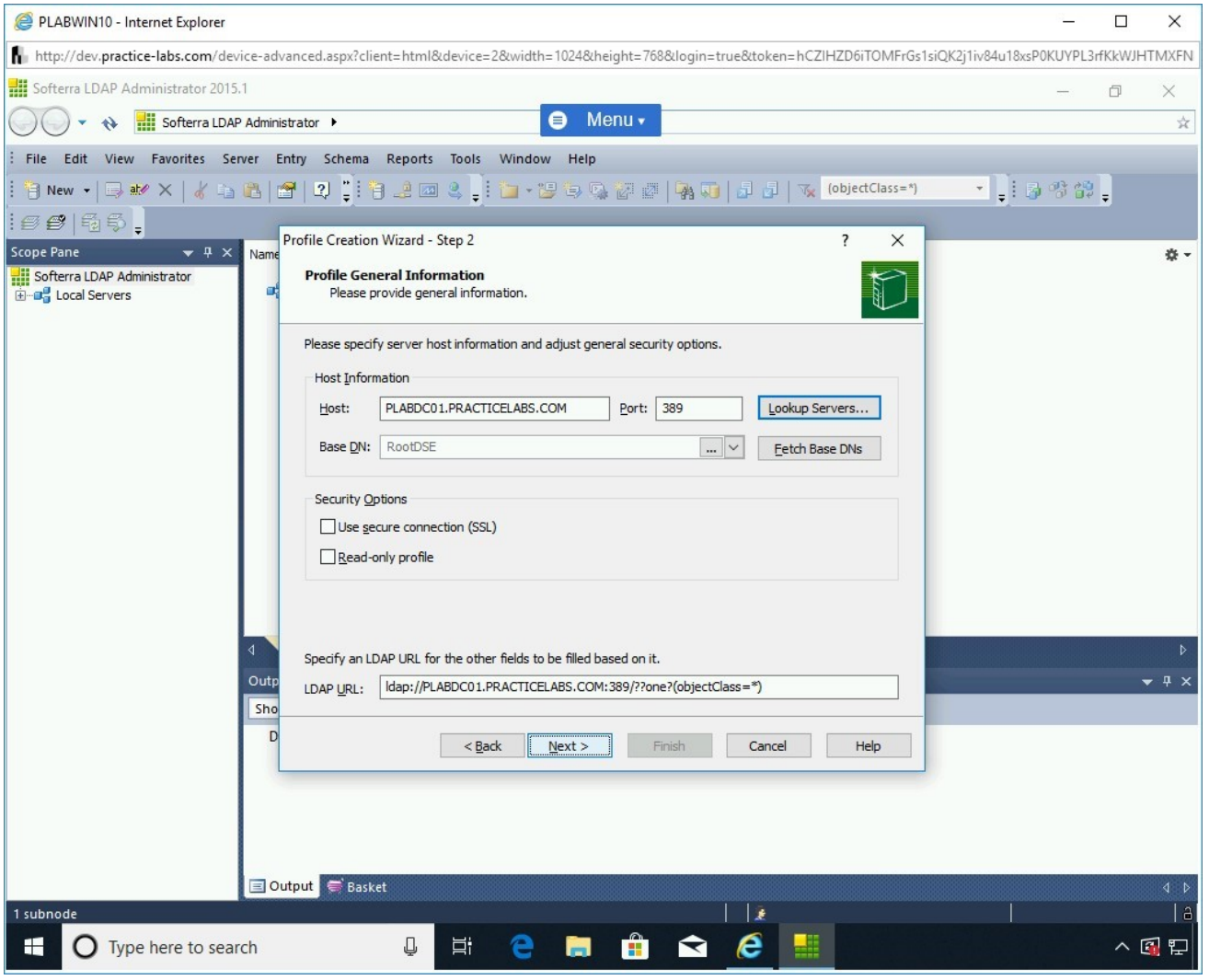


Figure 1.86 Screenshot of PLABWIN10: Clicking Next on the Profile General Information page.

Step 19

On the **User Authentication Information** page, select **Currently logged on user (Active Directory only)** and click **Next**.

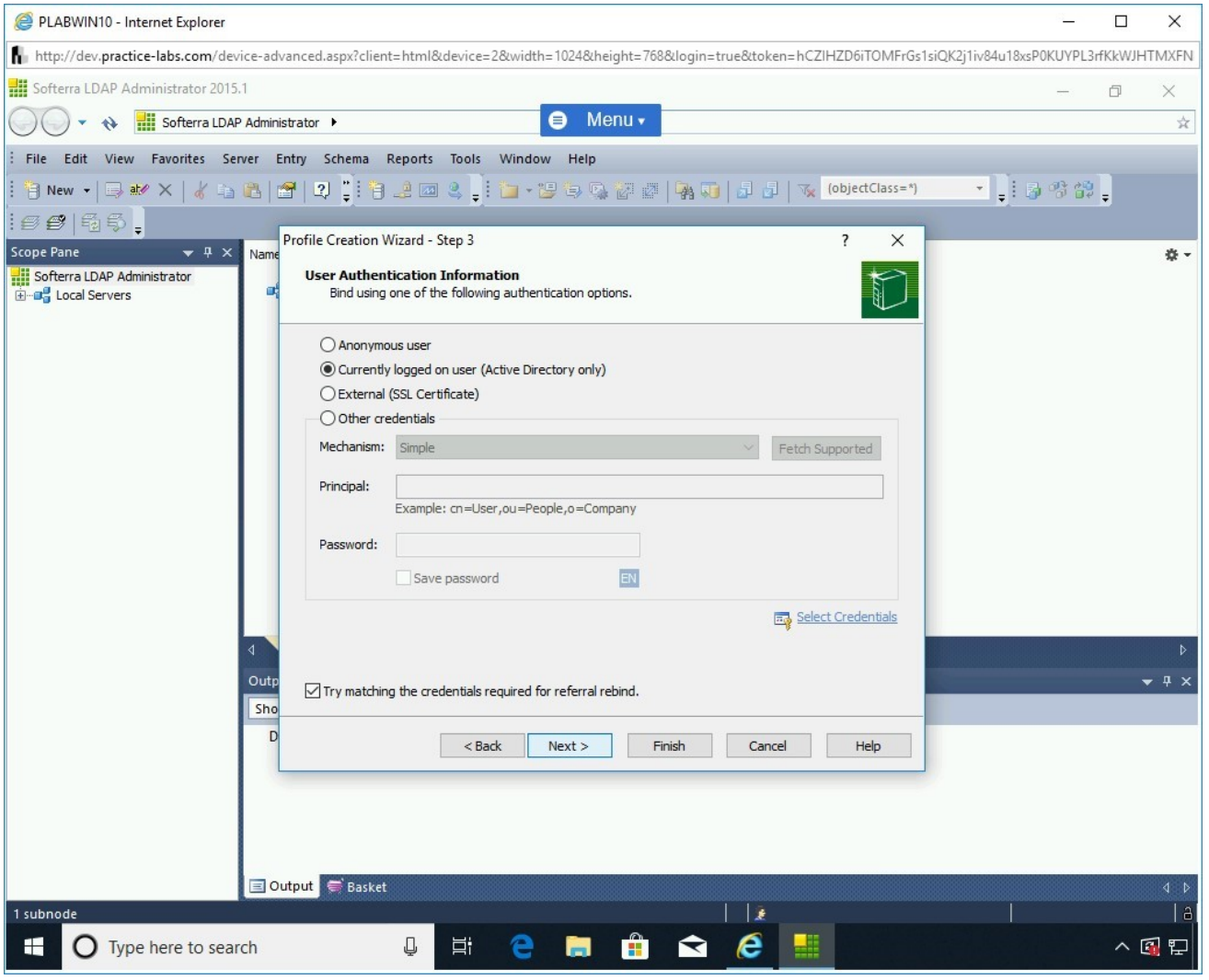


Figure 1.87 Screenshot of PLABWIN10: Selecting Currently logged on user (Active Directory only) and clicking Next.

Step 20

On the **LDAP Settings** page, keep the default settings and click **Finish**.

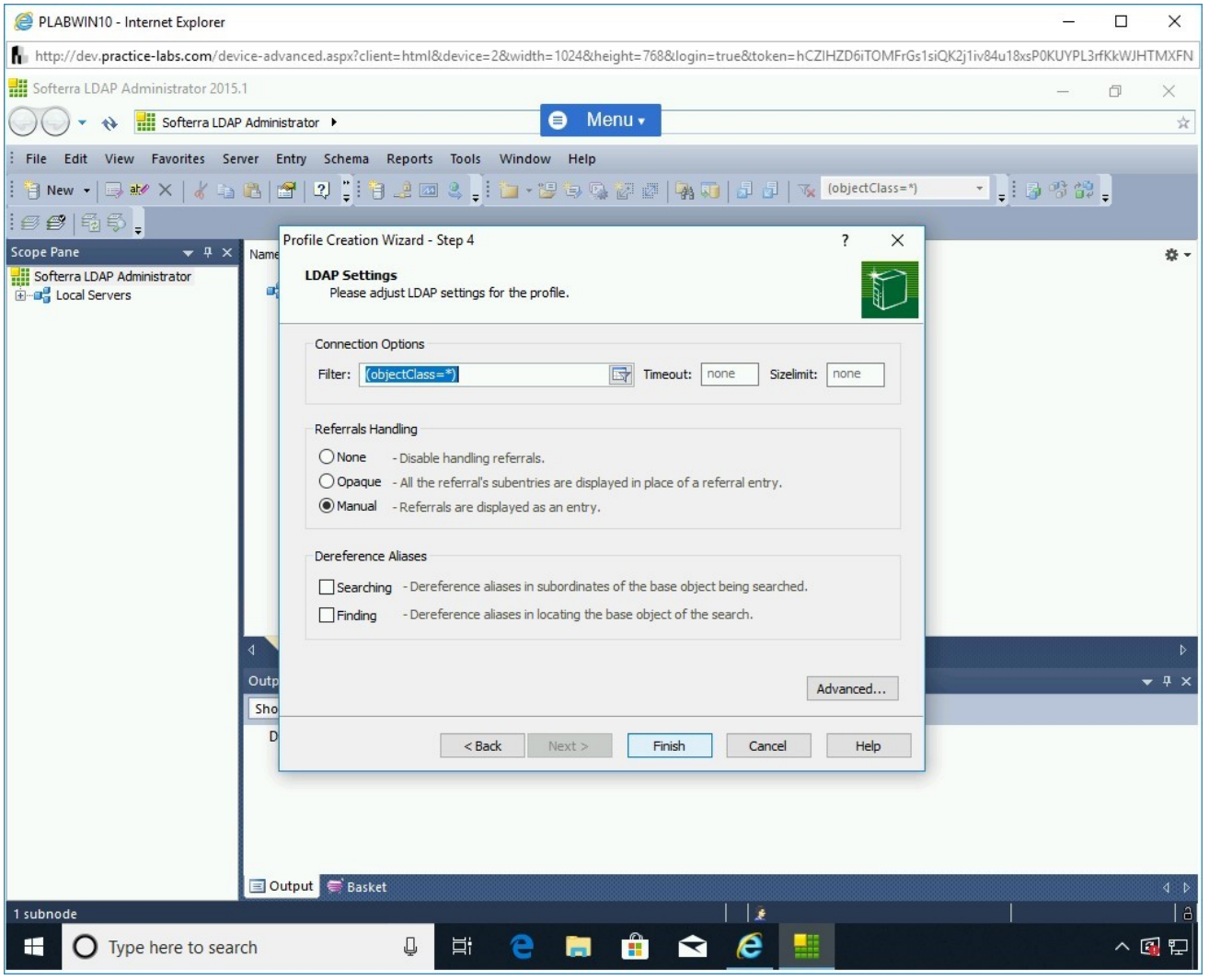


Figure 1.88 Screenshot of PLABWIN10: Clicking Finish on the LDAP Settings page with the default settings.

Step 21

The left pane displays several nodes under **PLAB**. The right pane displays various attributes.

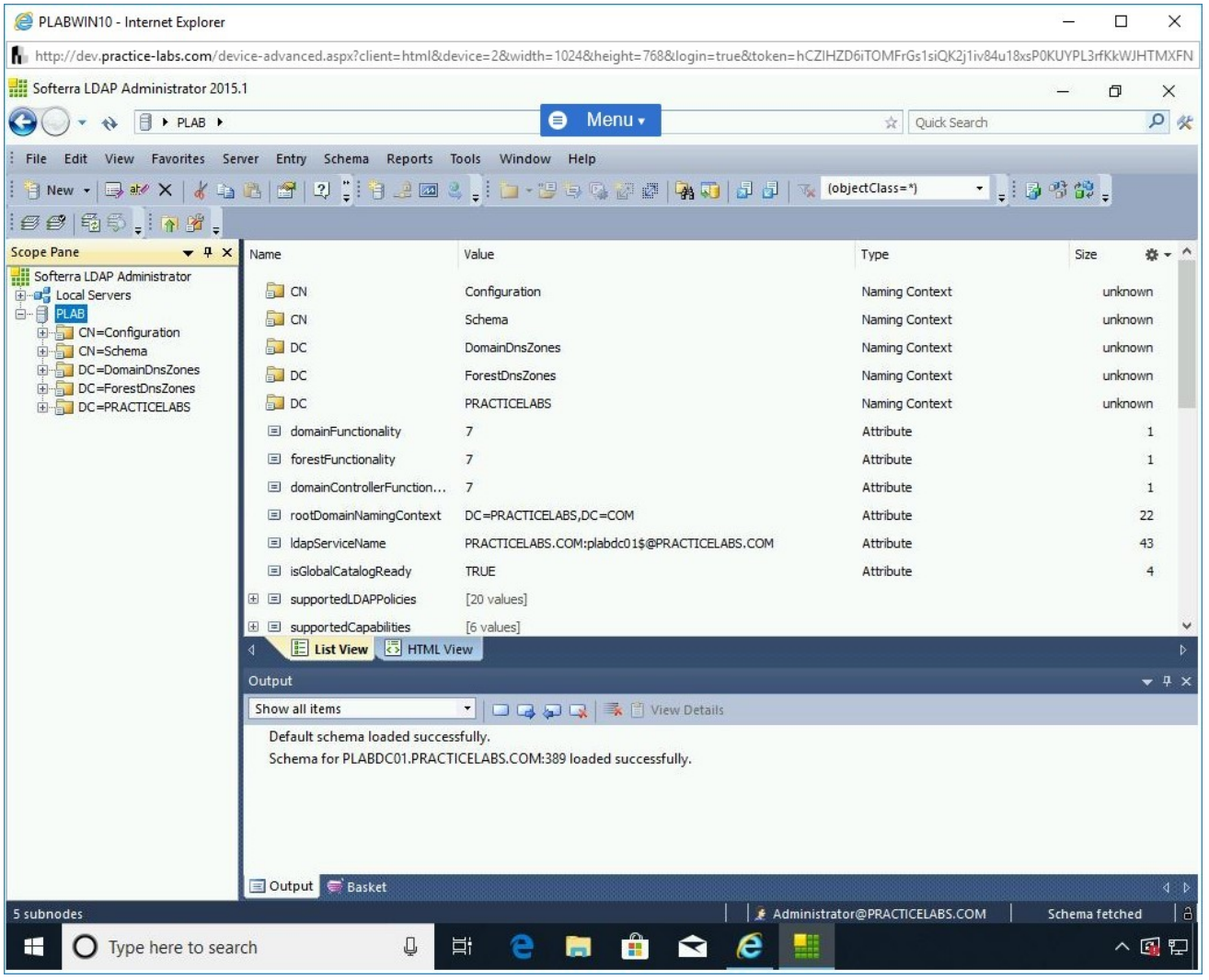


Figure 1.89 Screenshot of PLABWIN10: Selecting PLAB in the left pane and showing its attributes in the right pane.

Step 22

In the left pane, expand **DC=PRACTICELABS** and then expand **CN=Users** and select it.

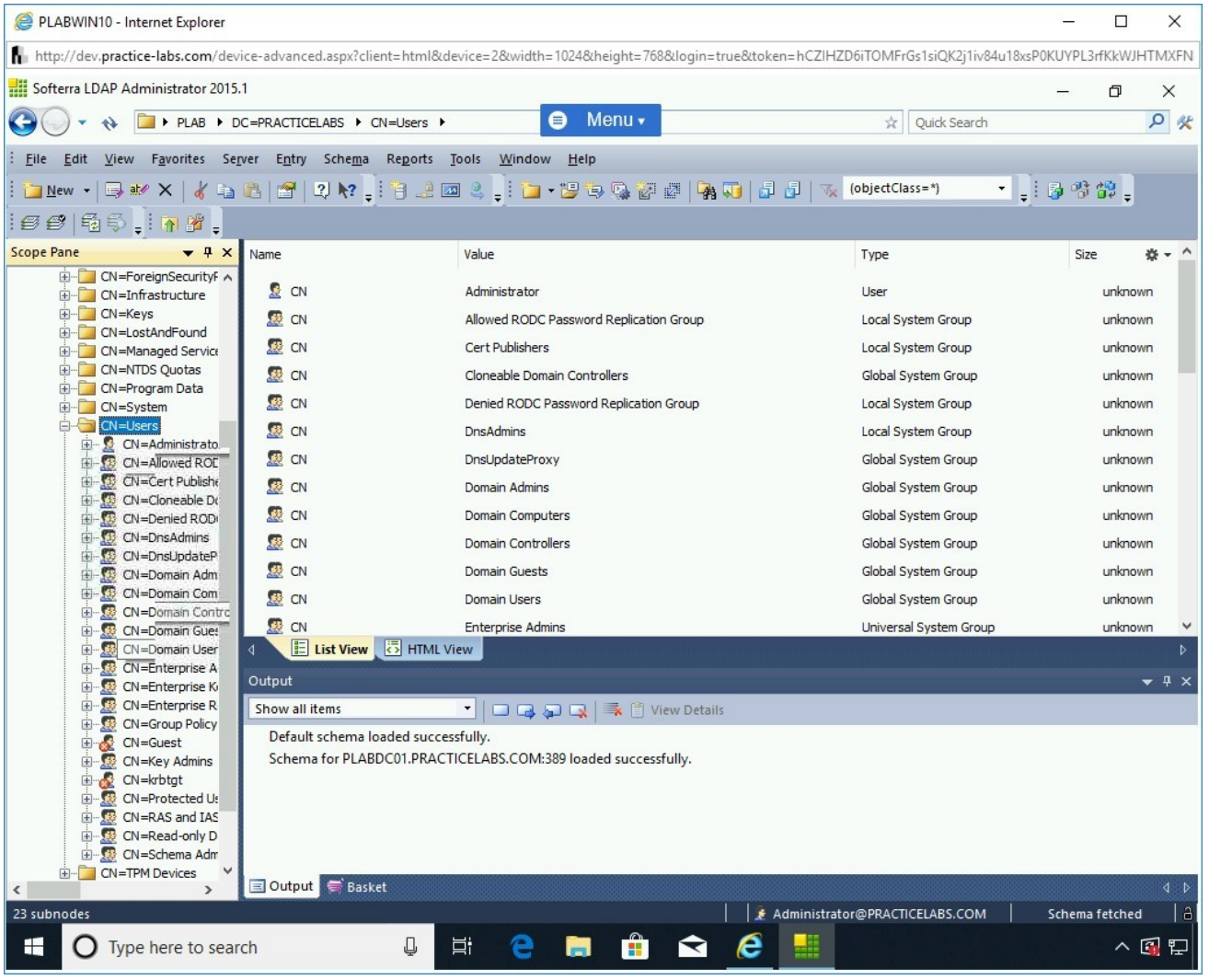


Figure 1.90 Screenshot of PLABWIN10: Expanding DC=PRACTICELABS and then expanding and selecting CN=Users.

Step 23

The quickest method to locate information in **LDAP Administrator** is by using search.

You can use **Quick Search**, which is located on the right side above the menu bar, to find the required information.

Click on **PLAB** at the top of the **Scope** pane and enter the following in **Quick Search**:

```
administrator
```

Once entered, click the search button adjacent to the search box.

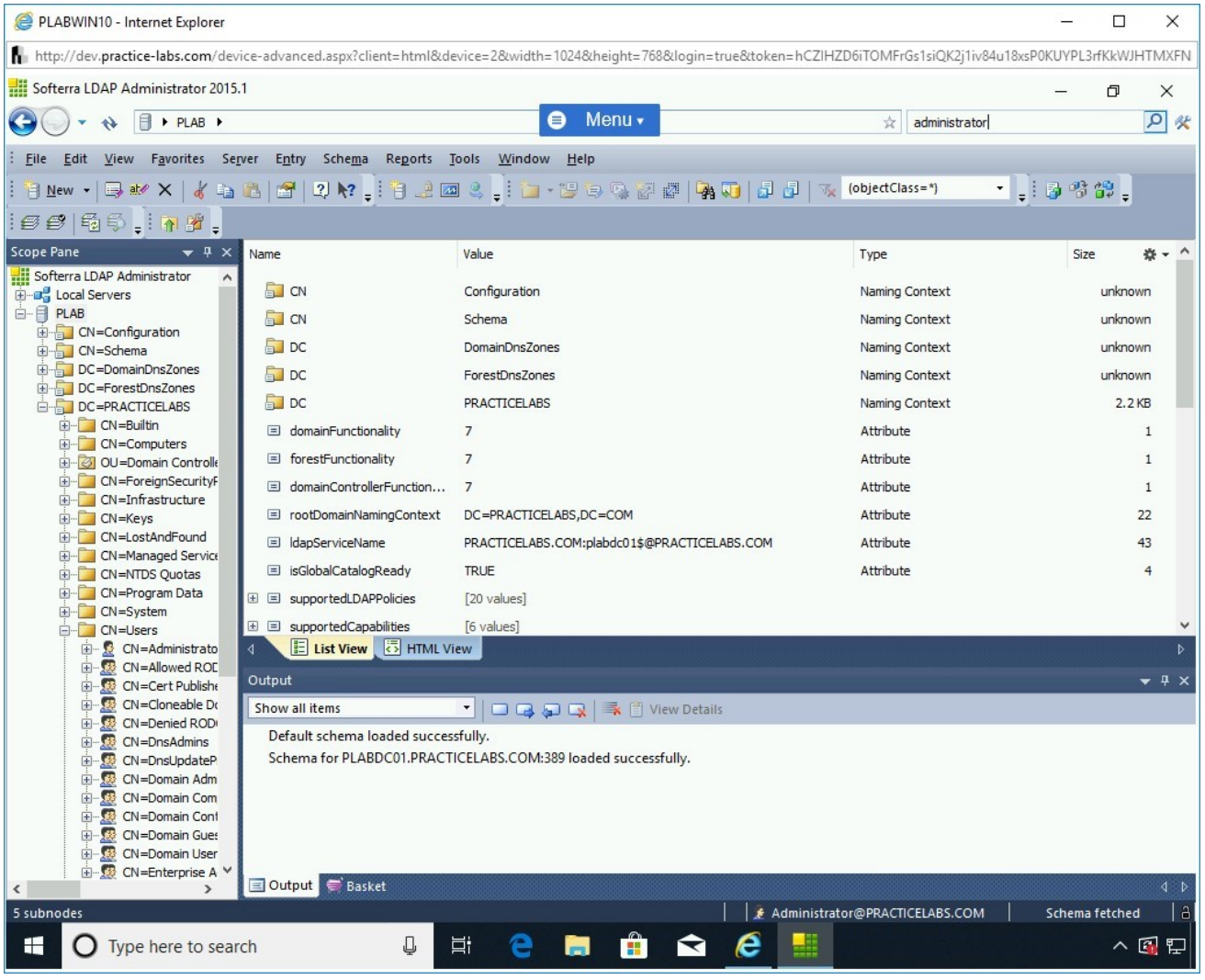


Figure 1.91 Screenshot of PLABWIN10: Entering the administrator name in the Quick Search text box and clicking the search button.

Step 24

The search result is displayed. Now, only the **Administrator** account is listed in the search result.

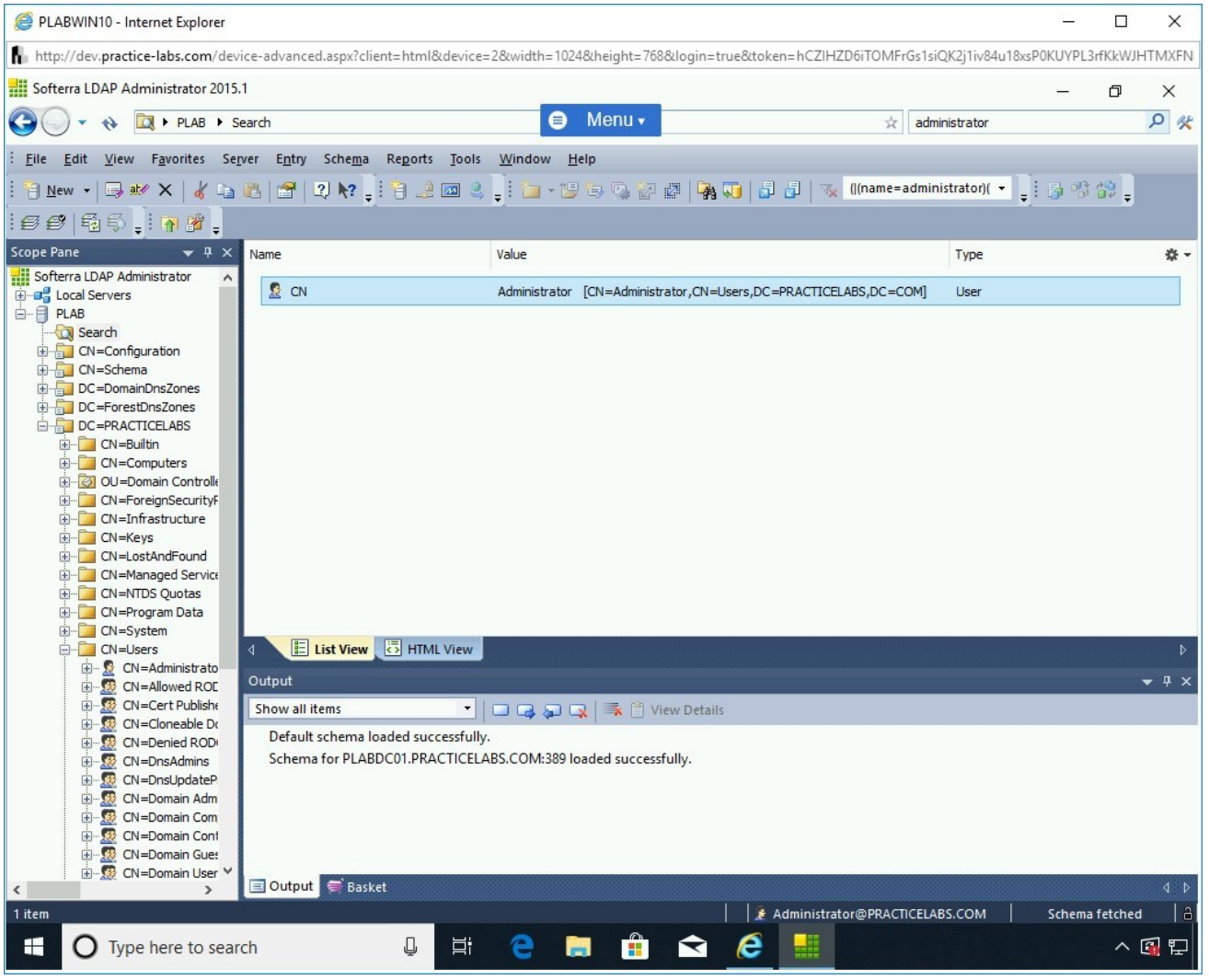


Figure 1.92 Screenshot of PLABWIN10: Showing the Administrator account in the right pane.

Step 25

Right-click the result and select **Locate in Tree**.

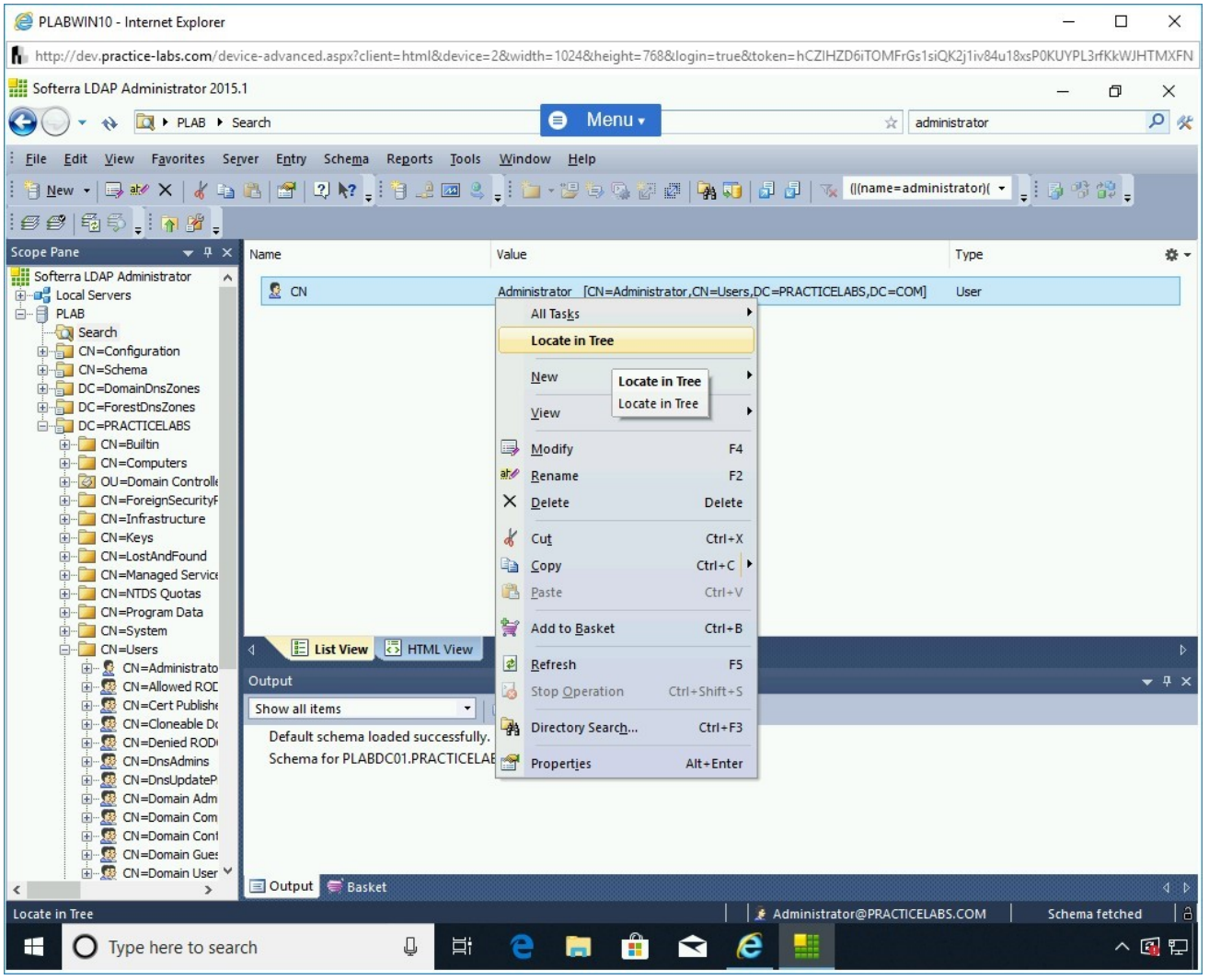


Figure 1.93 Screenshot of PLABWIN10: Right-clicking the result and selecting Locate in Tree.

Step 26

Note that the nodes in the left pane are automatically expanded, and **CN=Administrator** is highlighted.

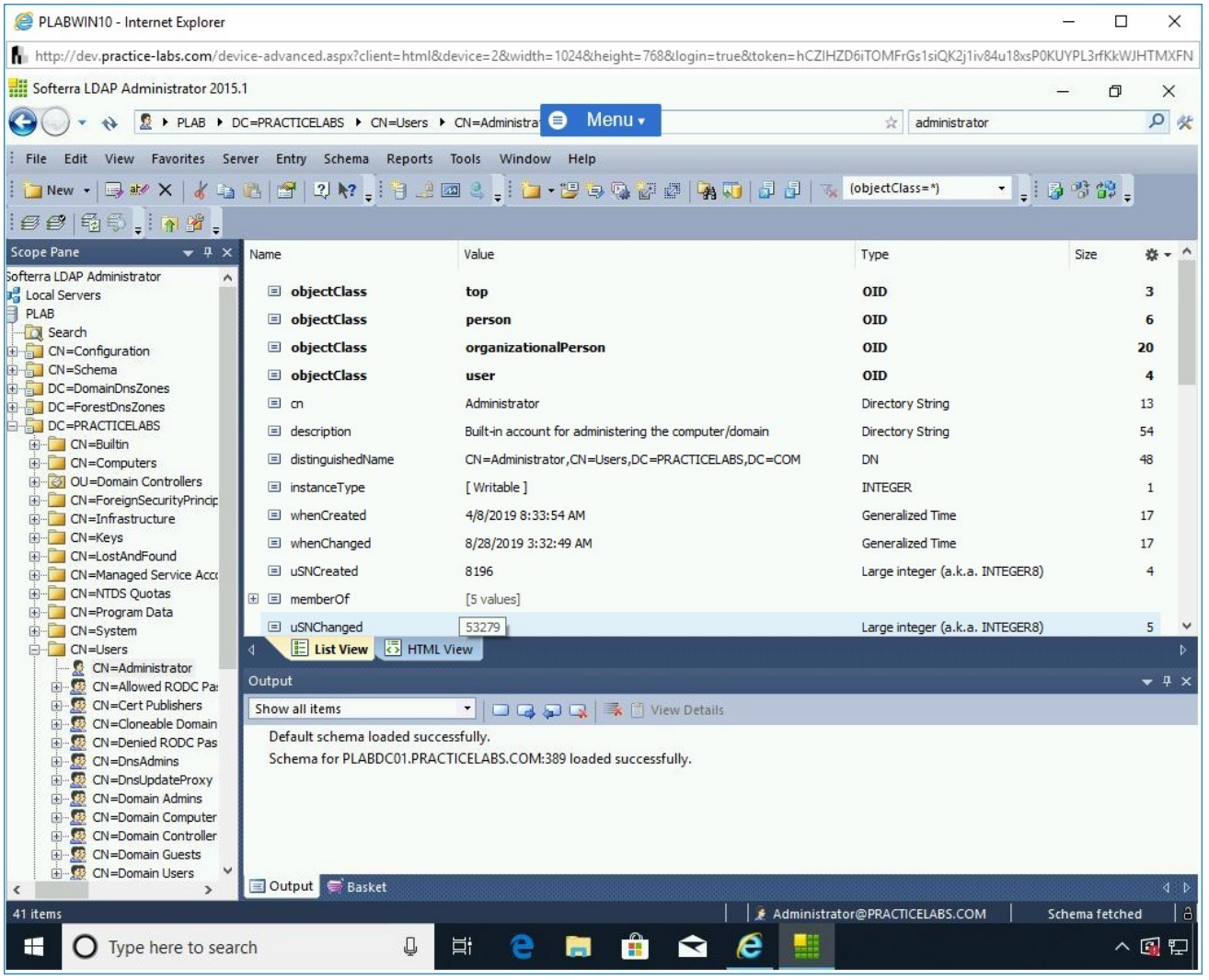


Figure 1.94 Screenshot of PLABWIN10: Showing the outcome of the Locate in Tree option.

Step 27

You can also perform several tasks on LDAP, which is Active Directory in this case. For example, you can modify a user.

> ***Note**: If you would like to try the other available tasks/options, you can perform at your own pace.*

In the left pane, right-click **CN=Administrator**, select **All Tasks**, and then select **Reset Password**.

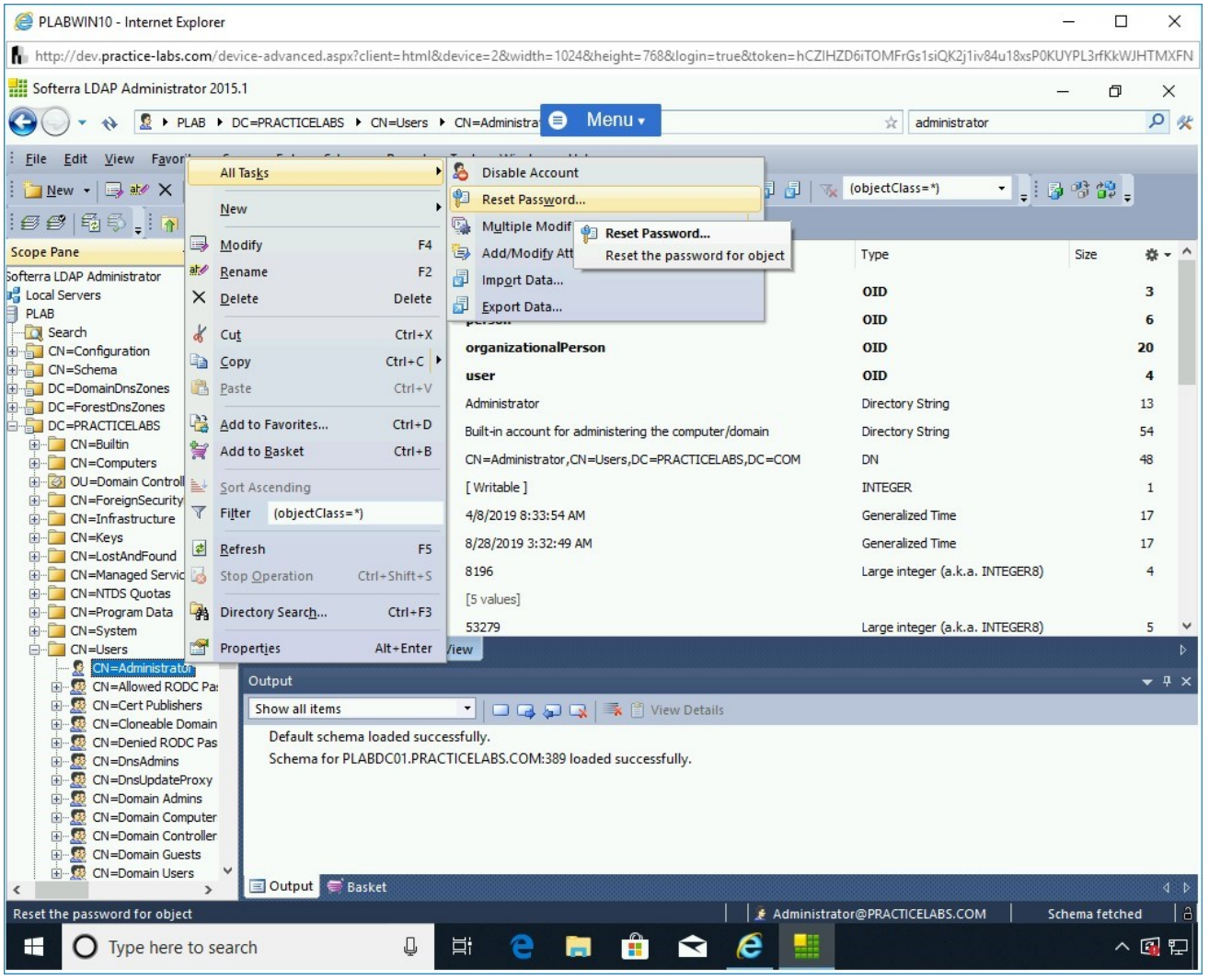


Figure 1.95 Screenshot of PLABWIN10: Right-clicking Administrator, selecting All Tasks, and then selecting Reset Password.

Step 28

The **Reset Password for Administrator** dialog box is displayed.

In the **New password** text box, type the following password:

```
Passw0rd
```

In the **Confirm password** text box, type the following password:

```
Passw0rd
```

Click **OK**.

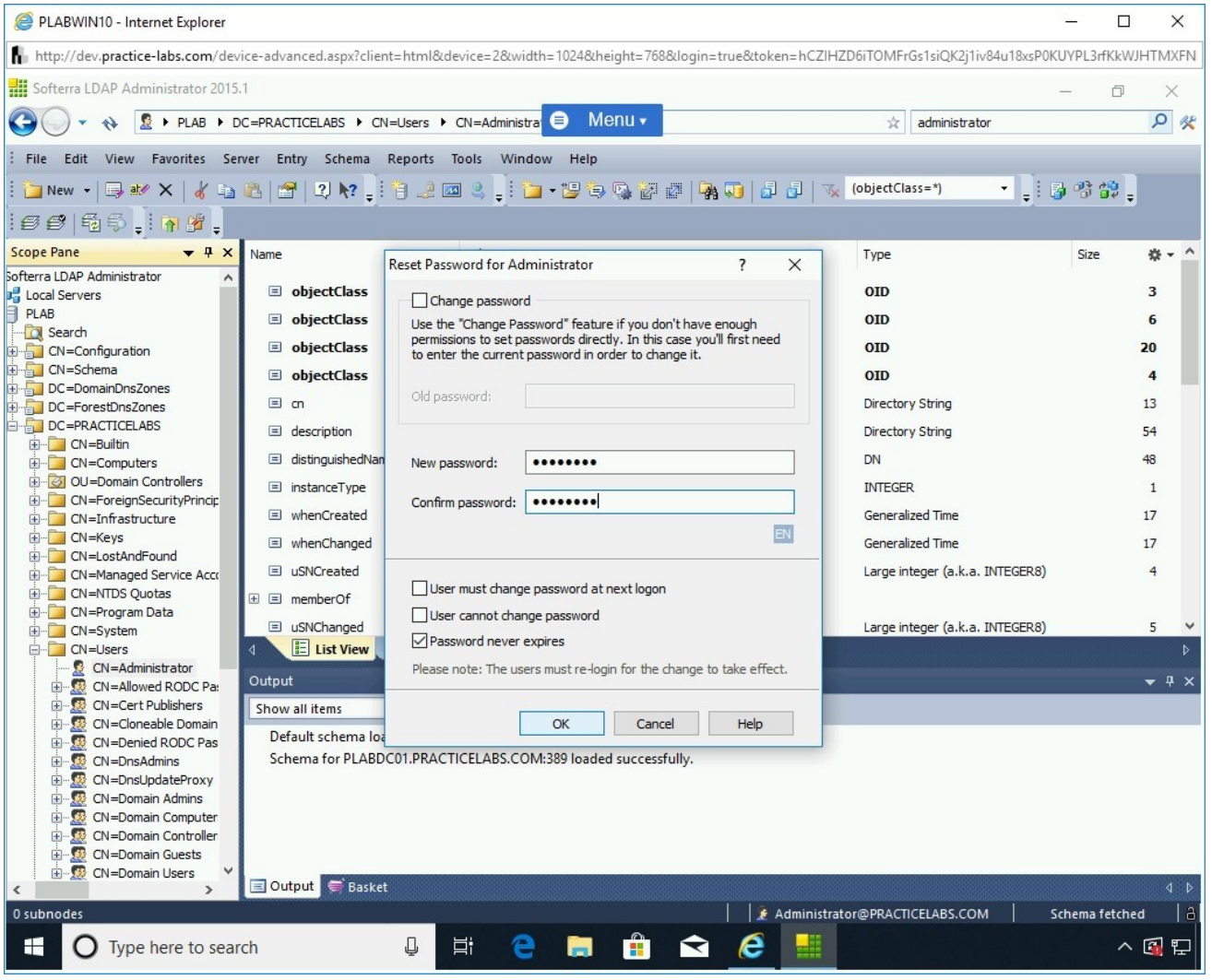


Figure 1.96 Screenshot of PLABWIN10: Entering and confirming the password and clicking OK.

Step 29

The **Reset Password** dialog box is displayed. Note that the status is now marked as **Completed**. Click **Close**. The password for the **Administrator** user is now changed.

Note: *This tool has many more capabilities than just the ones demonstrated in the lab environment, you can explore these if you have time.*

Close the **Softerra LDAP Administrator 2015.1** window.

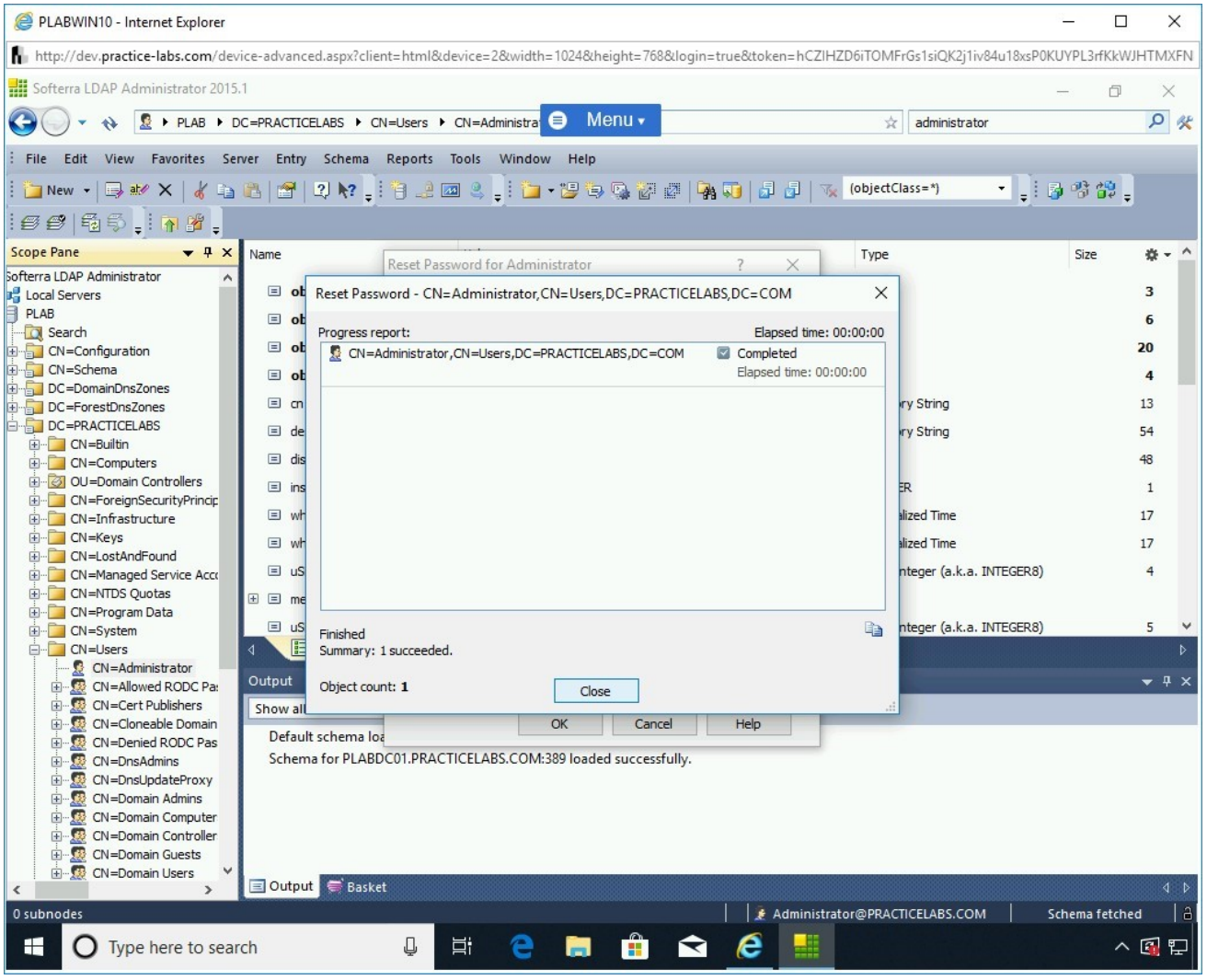


Figure 1.97 Screenshot of PLABWIN10: Clicking Close button after a successful password change.

Keep **Internet Explorer** window open.

Task 4 - Perform SNMP Enumeration Using IP Network Browser

There are various tools available in the market for SNMP enumeration. Two key tools are:

- SolarWind's IP Network Browser
- ManageEngine OpUtils

IP Network Browser is a that is used for performing network discovery. It can use either ICMP or SNMP to perform network discovery. In this task, you will use the IP Network Browser. 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.**

Ensure that **Internet Explorer** is open, and you are on the Hacking Tools page.

> ***Note:*** *If you closed Internet Explorer in the previous task, please ensure you follow the steps provided in Task 1 to reach the Hacking Tools page.*

On the **Hacking Tools** Webpage, scroll to locate **Toolset-v11.0.1-Eval.zip**. Click **Toolset-v11.0.1-Eval.zip**.

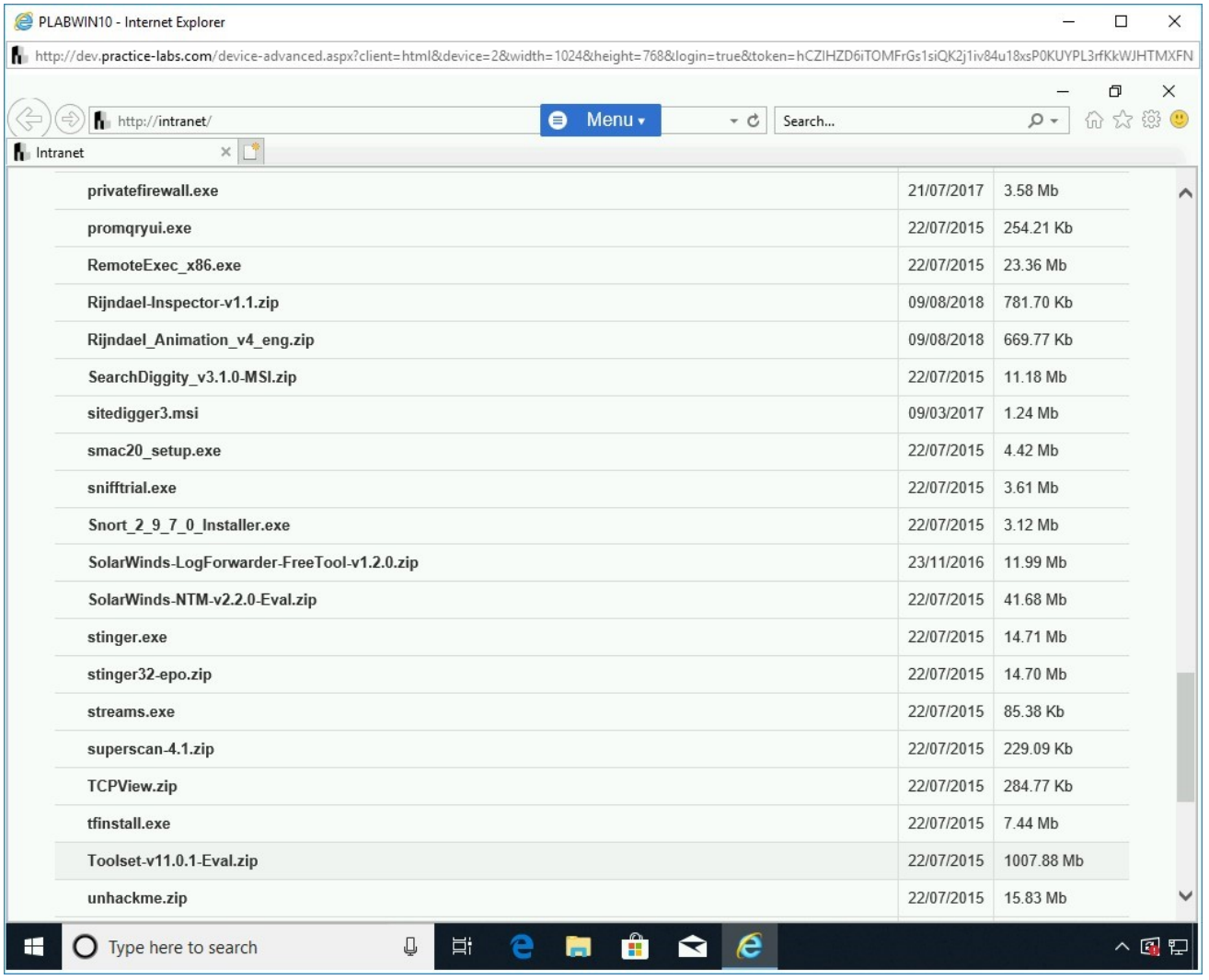


Figure 1.98 Screenshot of PLABWIN10: Clicking Toolset-v11.0.01-Eval.zip on the Hacking Tools page.

Step 2

In the notification bar, click **Save**.

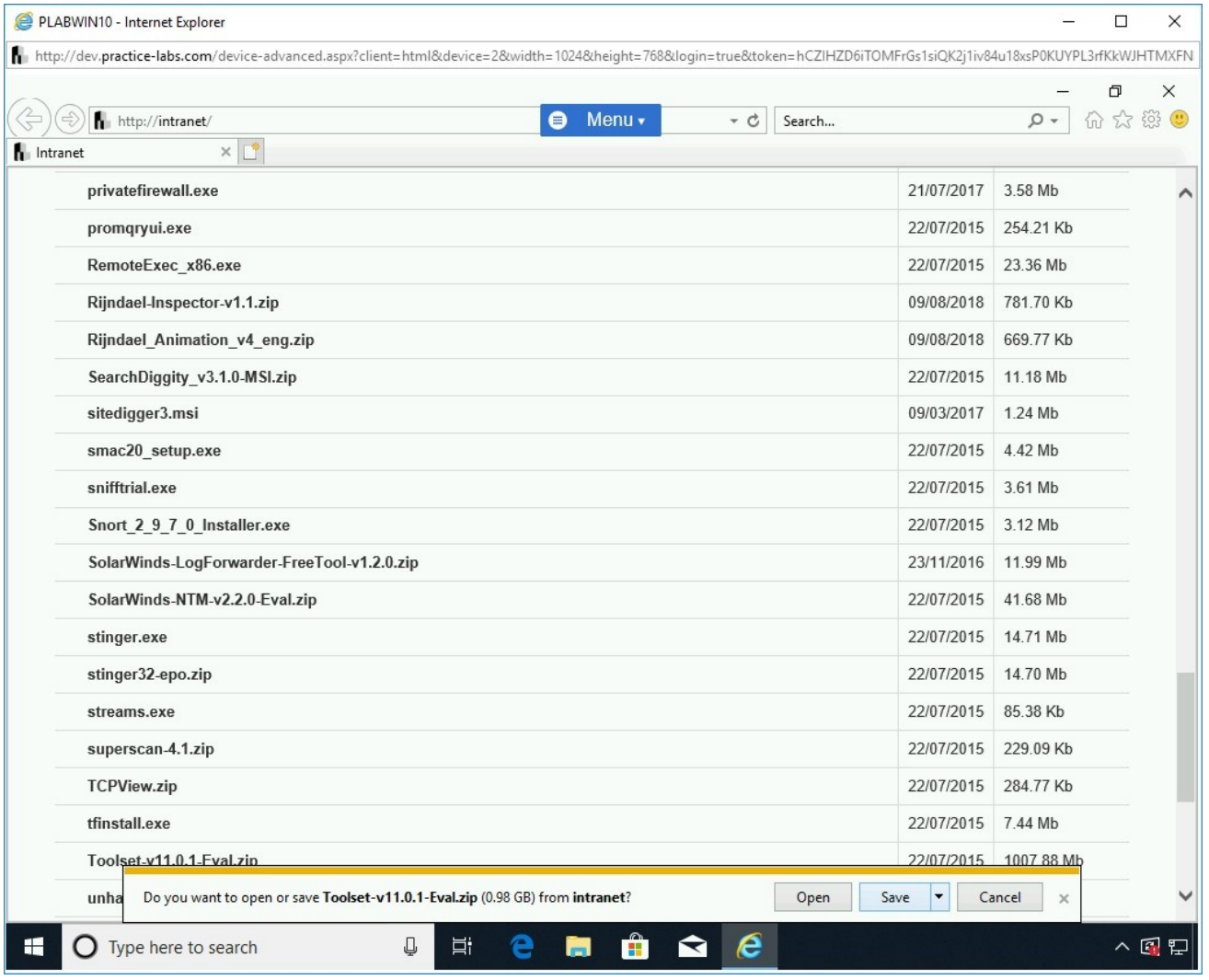


Figure 1.99 Screenshot of PLABWIN10: Clicking Save on the notification bar.

Step 3

When the file download is successfully completed, in the notification bar, click **Open folder.**

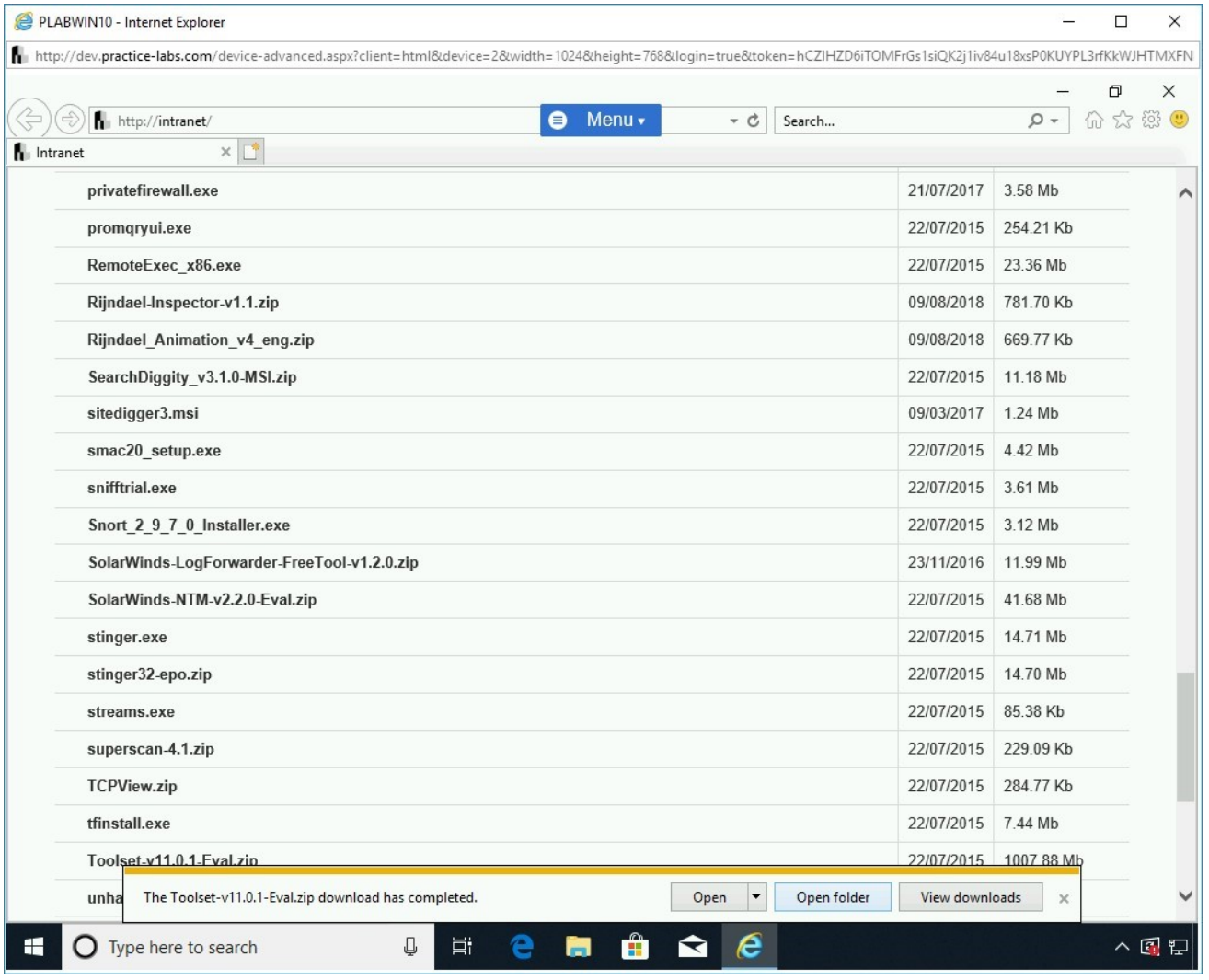


Figure 1.100 Screenshot of PLABWIN10: Clicking Open folder on the notification bar.

Step 4

In the **File Explorer** window, right-click **Toolset-v11.0.1-Eval.zip** and select **Extract All**.

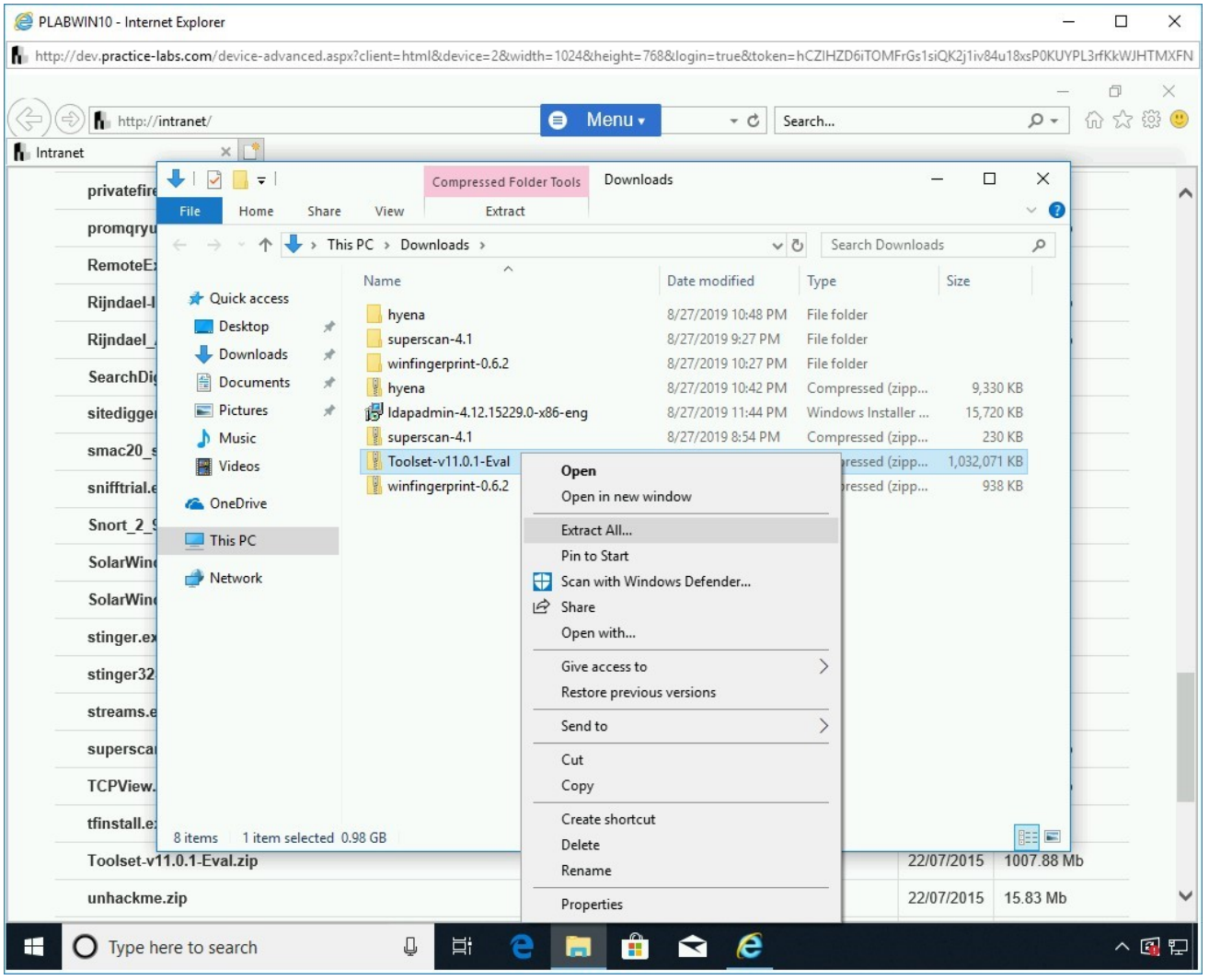


Figure 1.101 Screenshot of PLABWIN10: Right-clicking Toolset-v11.0.01-Eval.zip and selecting Extract All.

Step 5

In the **Extract Compressed (Zipped) Folders** dialog box, keep the default path and click **Extract**.

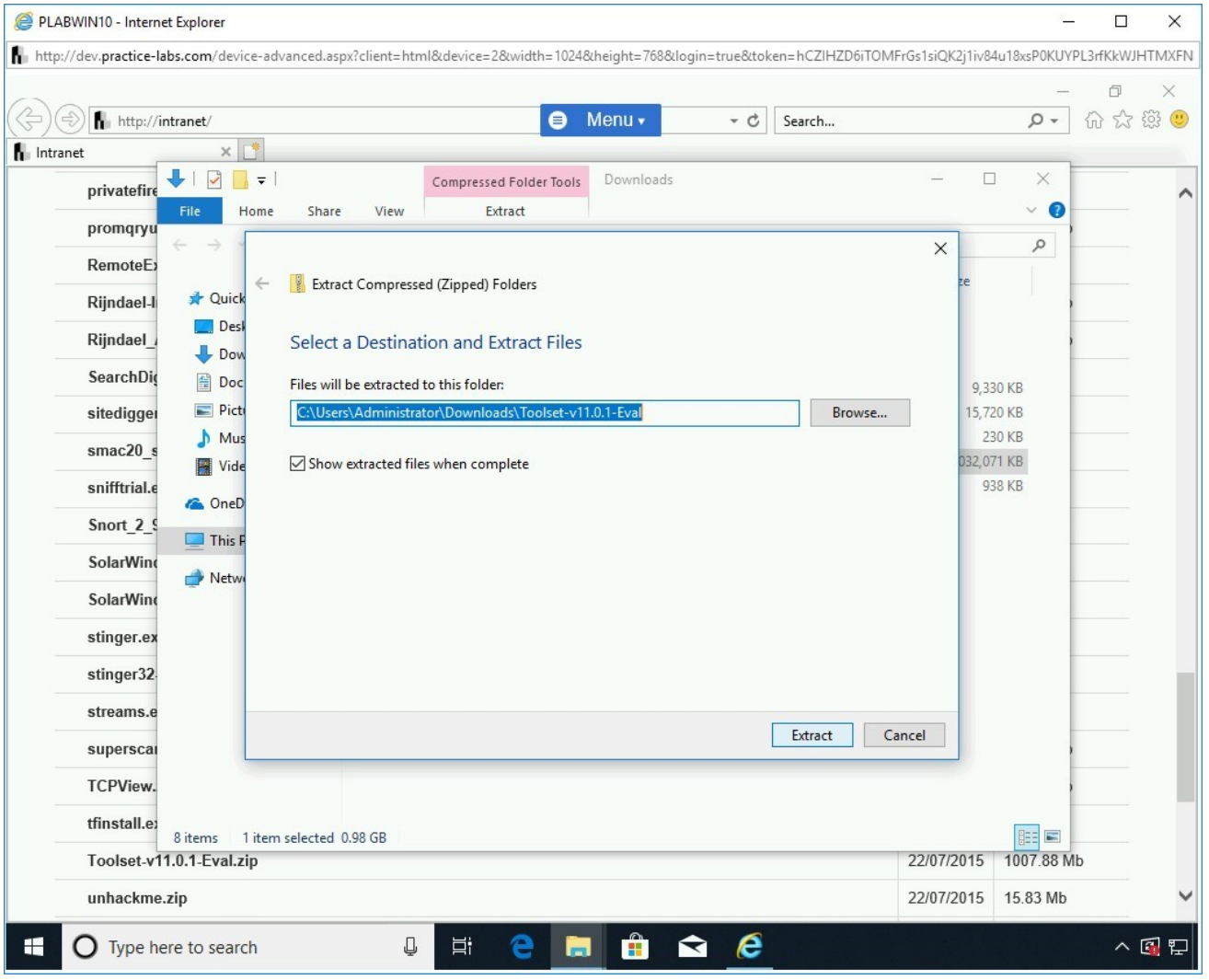


Figure 1.102 Screenshot of PLABWIN10: Clicking Extract in the Extract Compressed (Zipped) Folders dialog box.

Step 6

A file copying dialog box will be displayed. After the file copying process is complete, a new **File Explorer** window is displayed with various files. Double-click the **SolarWinds-DesktopToolset-v11** file.

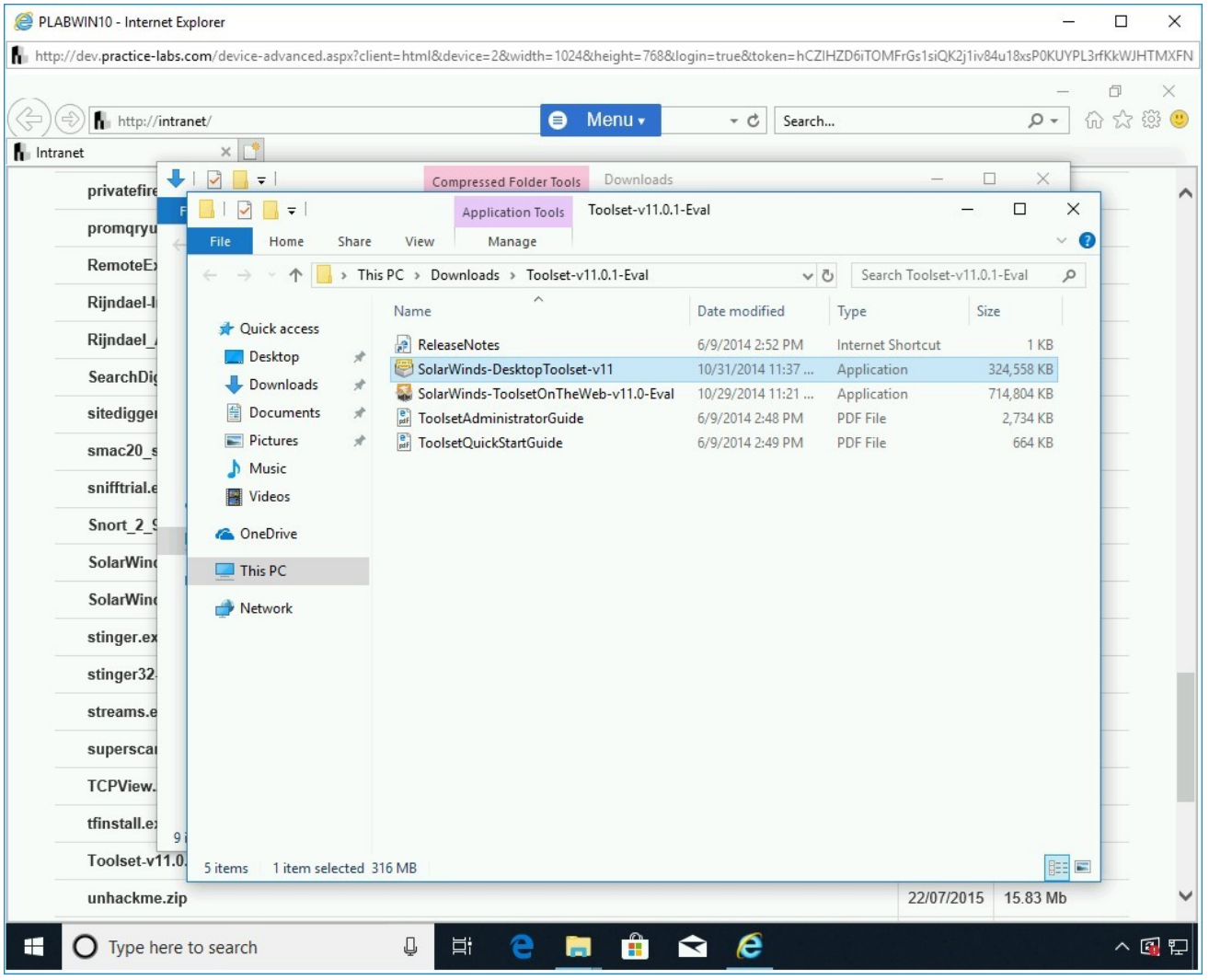


Figure 1.103 Screenshot of PLABWIN10: Double-clicking the SolarWinds-DesktopToolset-v11 file.

Step 7

The **Solarwinds Toolset v11.0.1 Setup** dialog box is displayed. It displays a message that **Microsoft .Net Framework 3.5 SP1 is being installed**.

Alert: In your lab environment, if .Net Framework is already installed, this step will not appear.

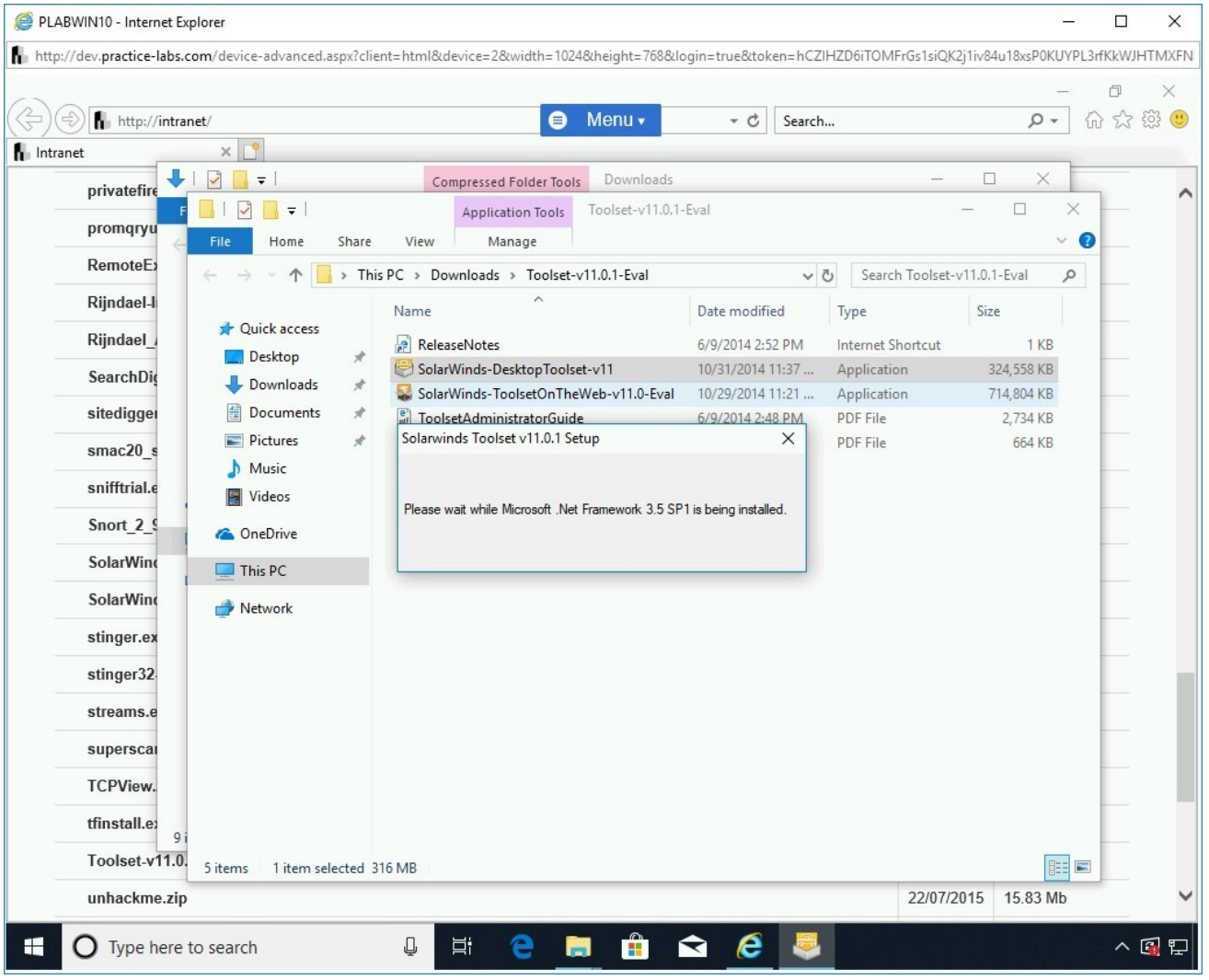


Figure 1.104 Screenshot of PLABWIN10: Showing the progress of the Microsoft .Net Framework installation.

Step 8

After the **Microsoft .Net** installation is complete, **Toolset** installation will start.

On the **Welcome to the SolarWinds Toolset v11.0.1 Setup Wizard** page of the **Solarwinds Toolset v11.0.1 Setup**, click **Next**.

Figure 1.105 Screenshot of PLABWIN10: Clicking Next on the Welcome to the SolarWinds Toolset v11.0.1 Setup Wizard page of the Solarwinds Toolset v11.0.1 Setup.

Step 9

On the **End-User License Agreement** page, select **I Accept the terms in the License Agreement** and click **Next**.

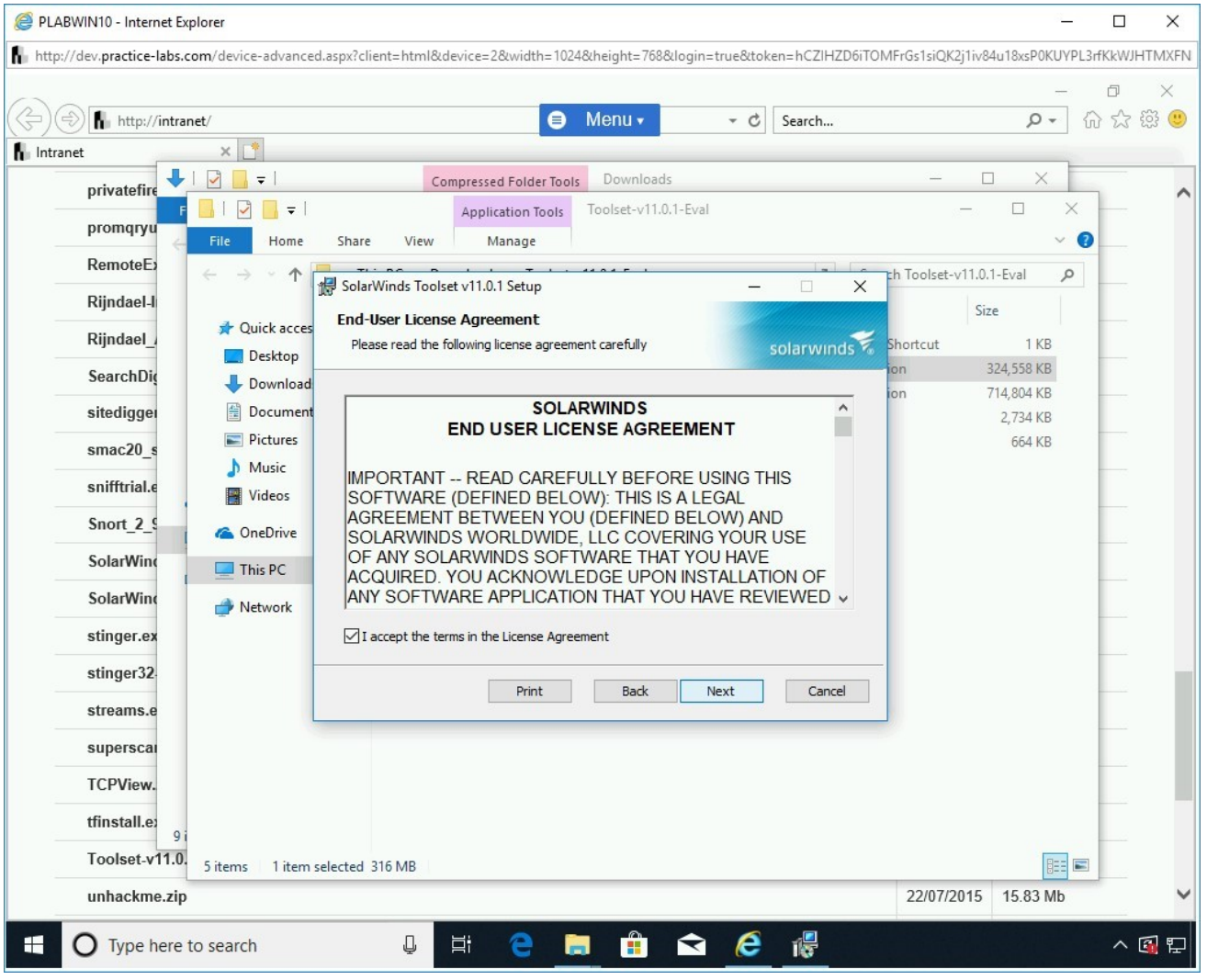


Figure 1.106 Screenshot of PLABWIN10: Selecting I accept the terms in the License Agreement and clicking Next.

Step 10

On the **Destination Folder** page, keep the default path and click **Next**.

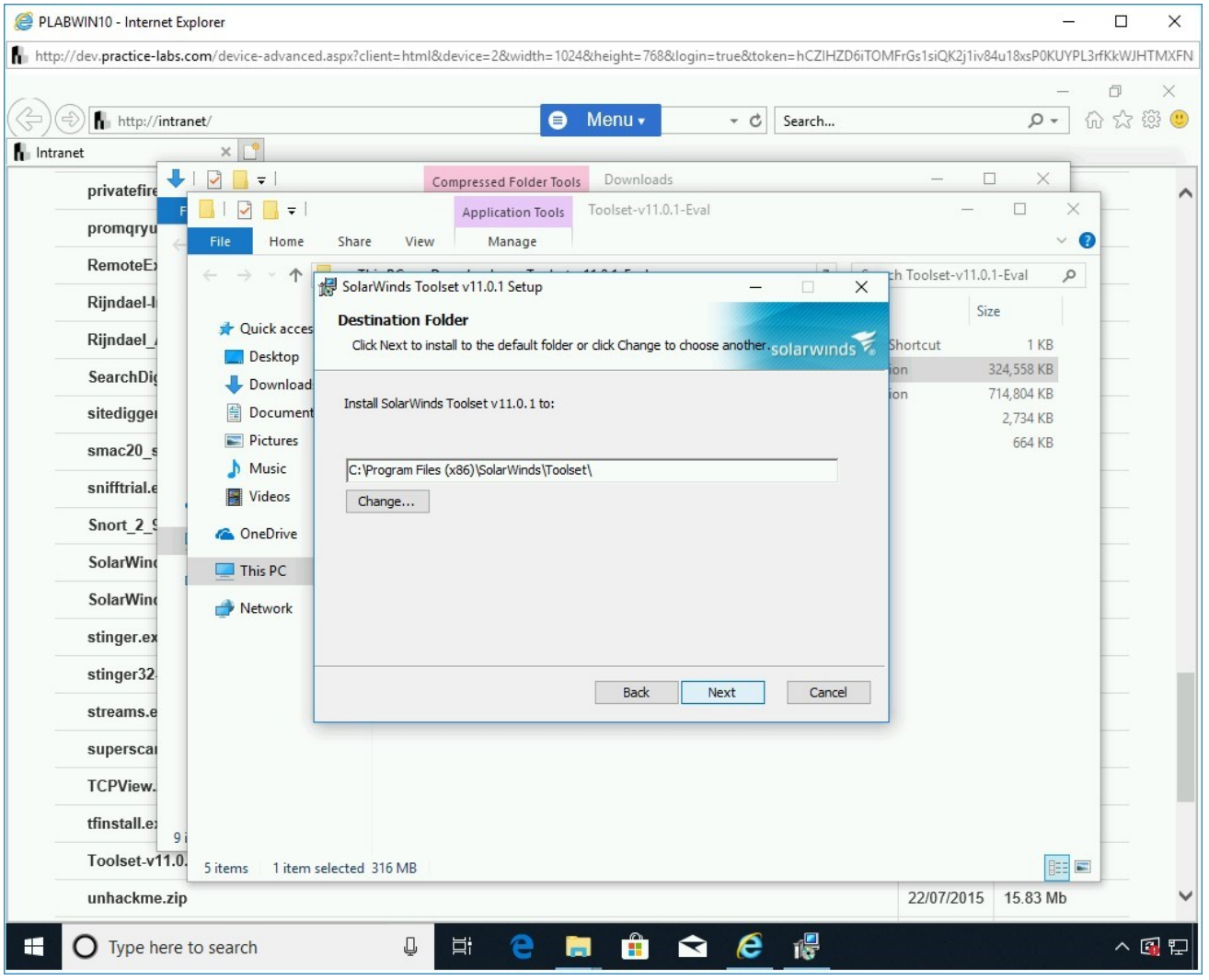


Figure 1.107 Screenshot of PLABWIN10: Clicking Next on the Destination Folder page.

Step 11

On the **Ready to install SolarWinds Toolset v11.0.1** page, click **Install**.

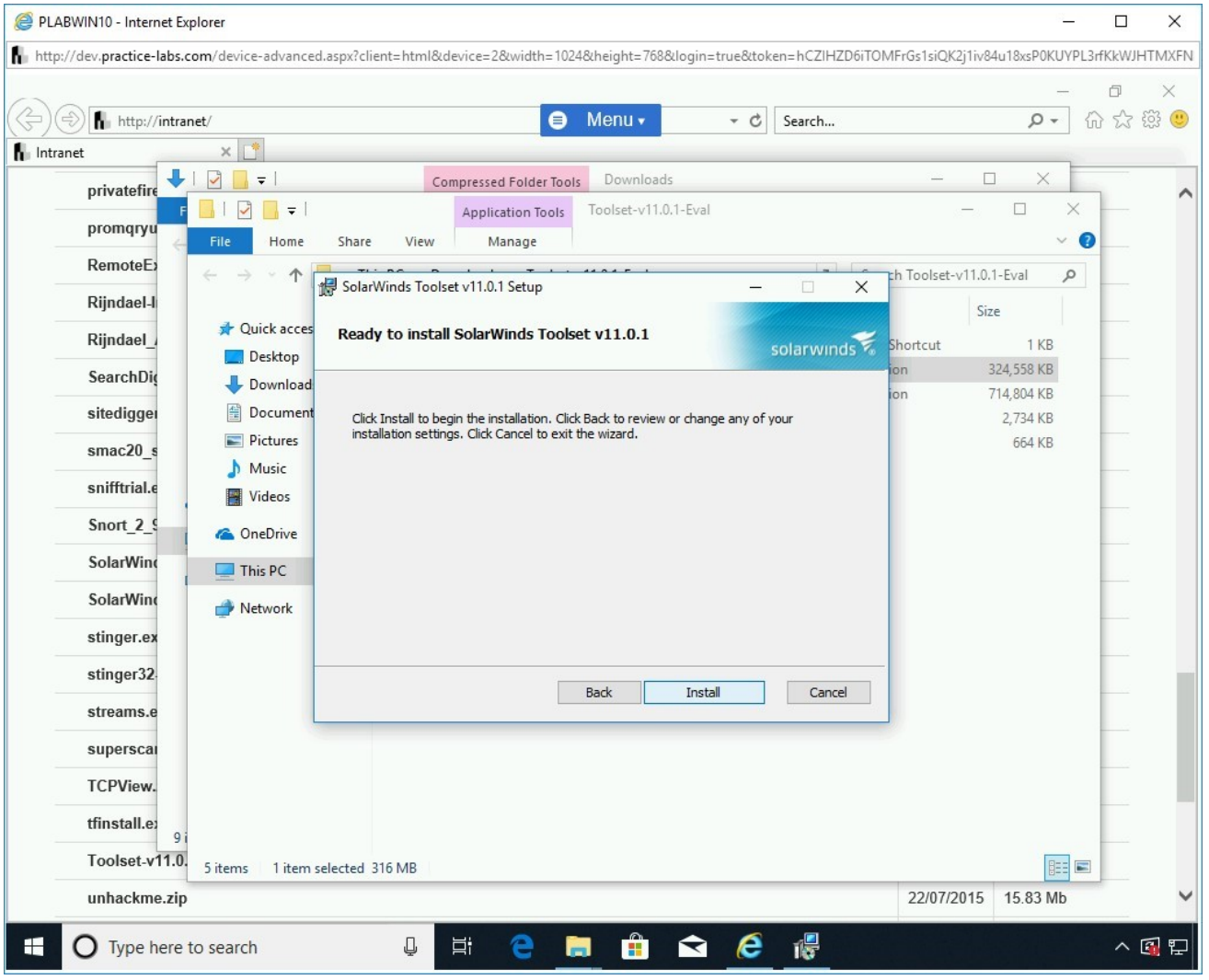


Figure 1.108 Screenshot of PLABWIN10: Clicking Install on the Ready to install SolarWinds Toolset v11.0.1 page.

Step 12

The installation will now begin; it should take a few minutes to complete.

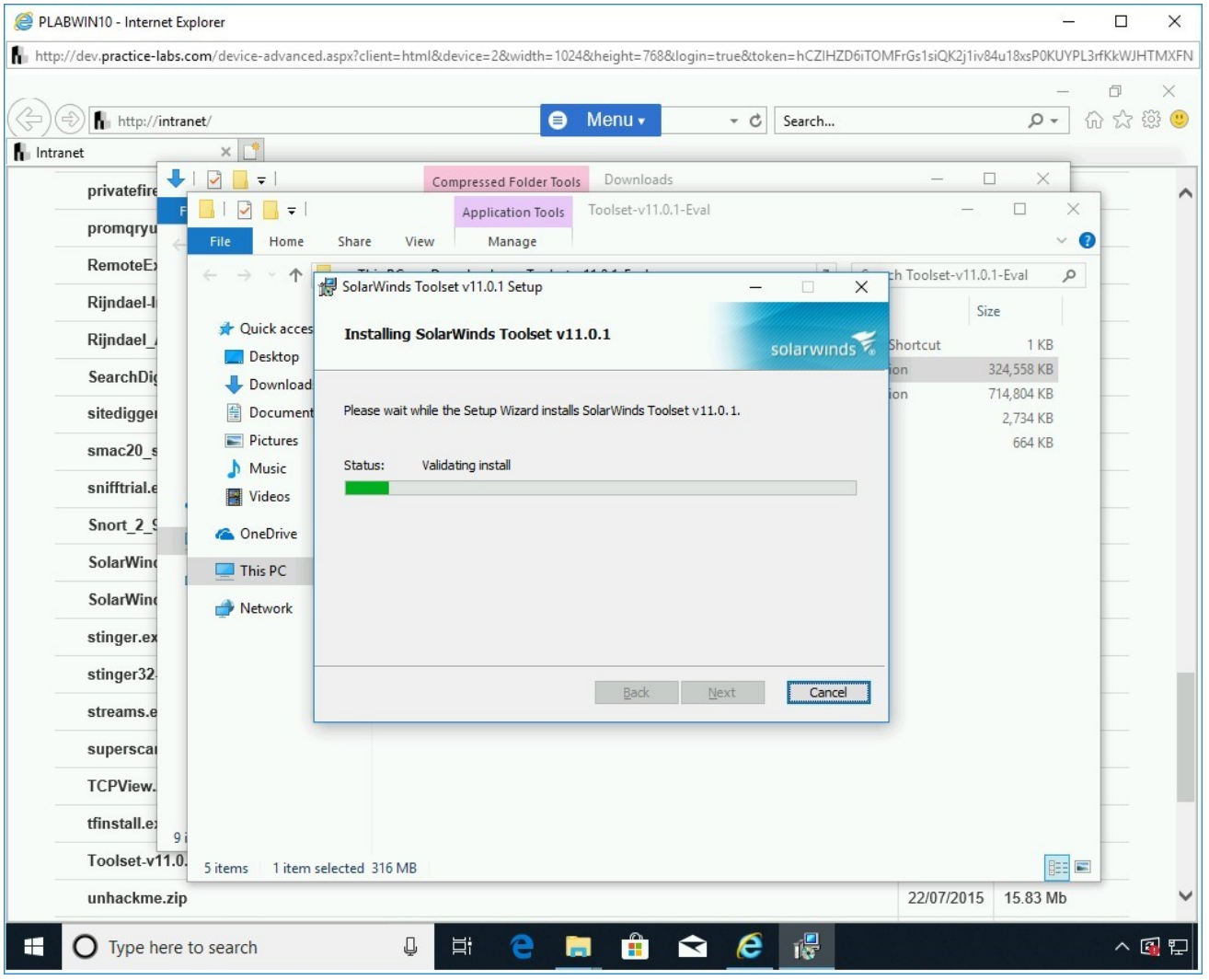


Figure 1.109 Screenshot of PLABWIN10: Showing the installation progress.

Step 13

After the installation has completed, on the Toolset dialog box, click **Continue Evaluation**.

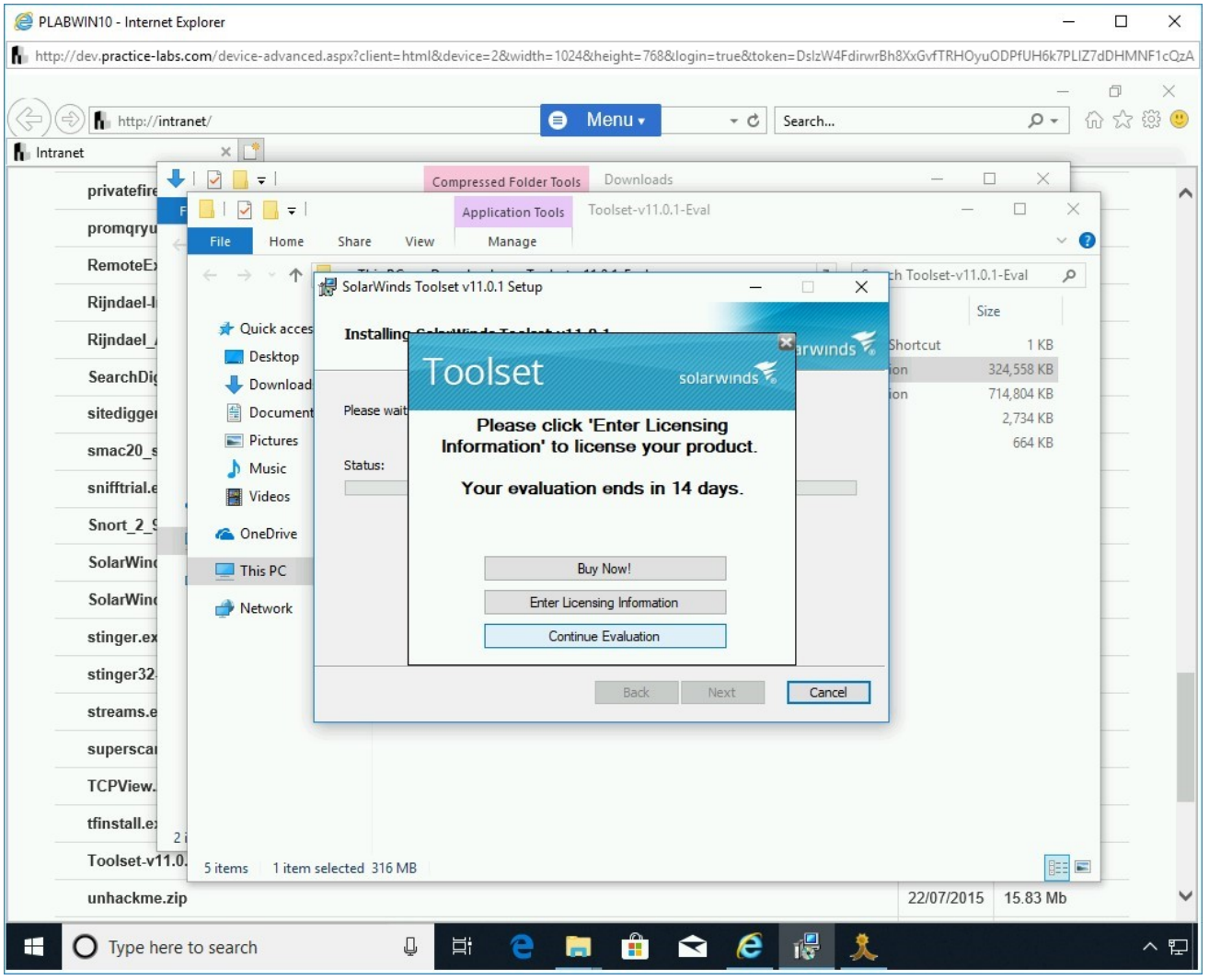


Figure 1.110 Screenshot of PLABWIN10: Clicking Continue Evaluation on the Toolset dialog box.

Step 14

You will finally be asked if you would like to send solar winds anonymous data, select **No, I would not like to participate,** and then click **OK**.

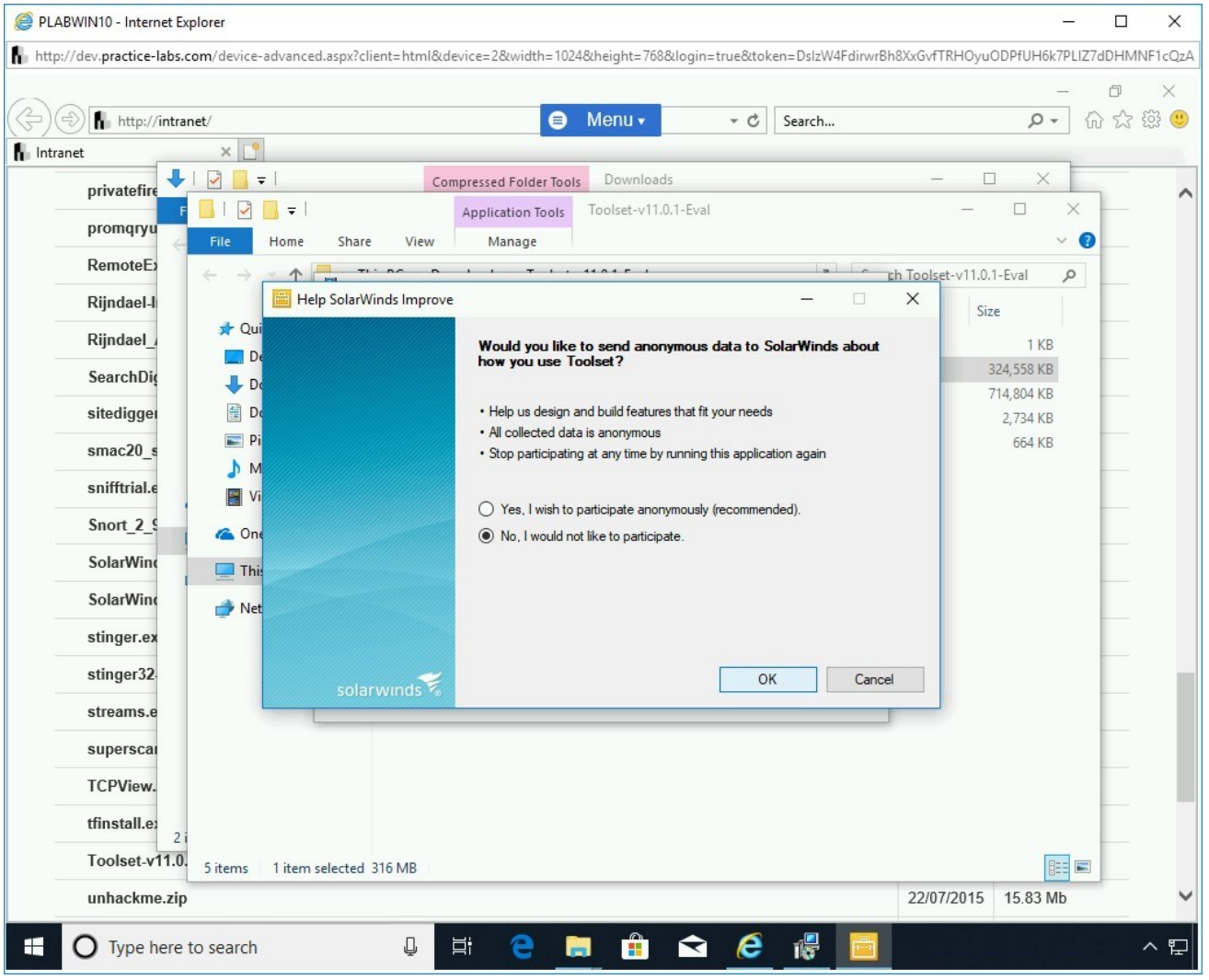


Figure 1.111 Screenshot of PLABWIN10: Selecting No, I would not like to participate and then clicking OK.

Step 15

The installation is now in progress.

When setup is successfully completed, click **Finish**.

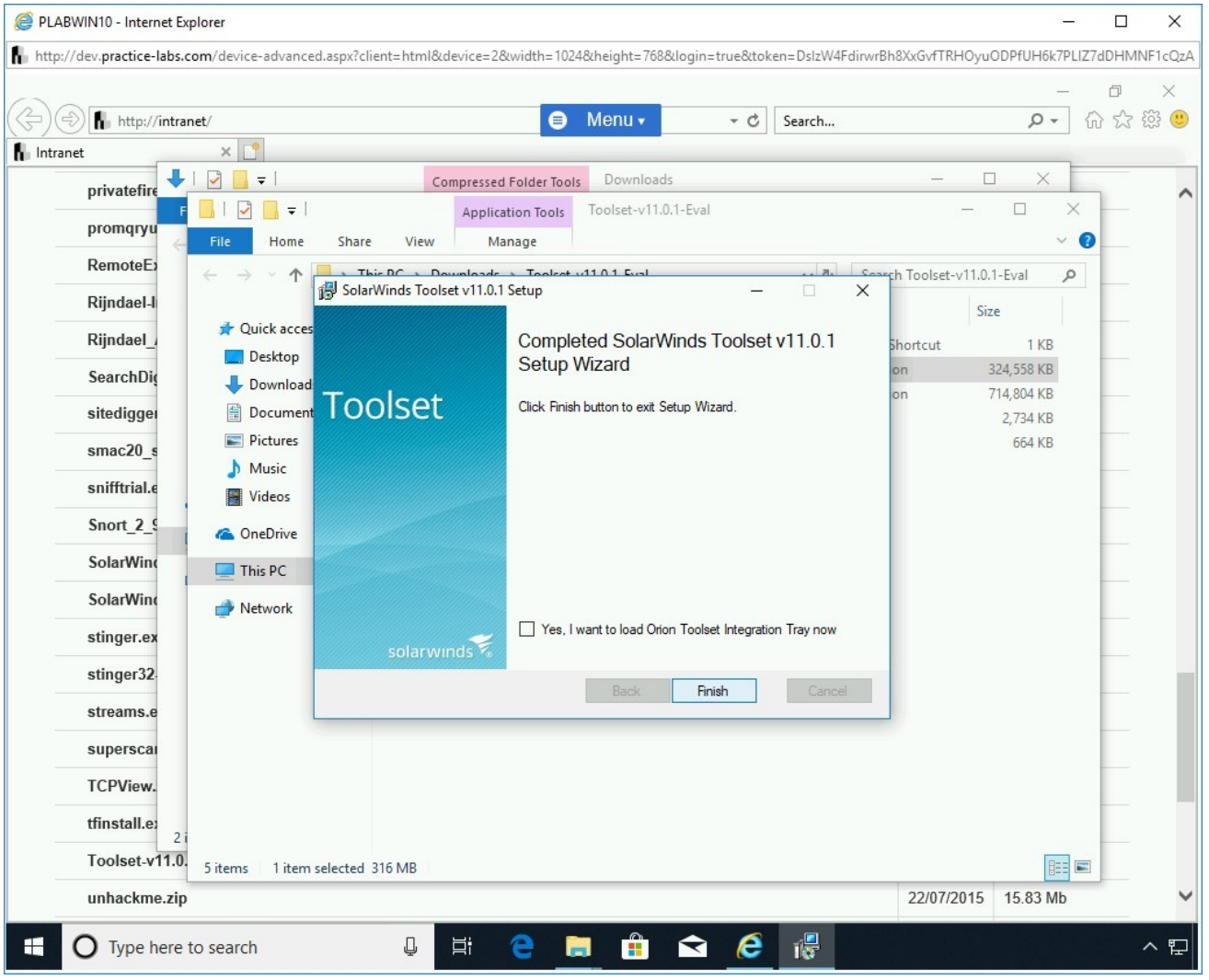


Figure 1.112 Screenshot of PLABWIN10: Clicking Finish on the Completed SolarWinds Toolset v11.0.1 Setup Wizard page.

Close all instances of **File Explorer**.

Minimize the **Internet Explorer** window.

Step 16

The **Toolset Launch pad** will now be displayed.

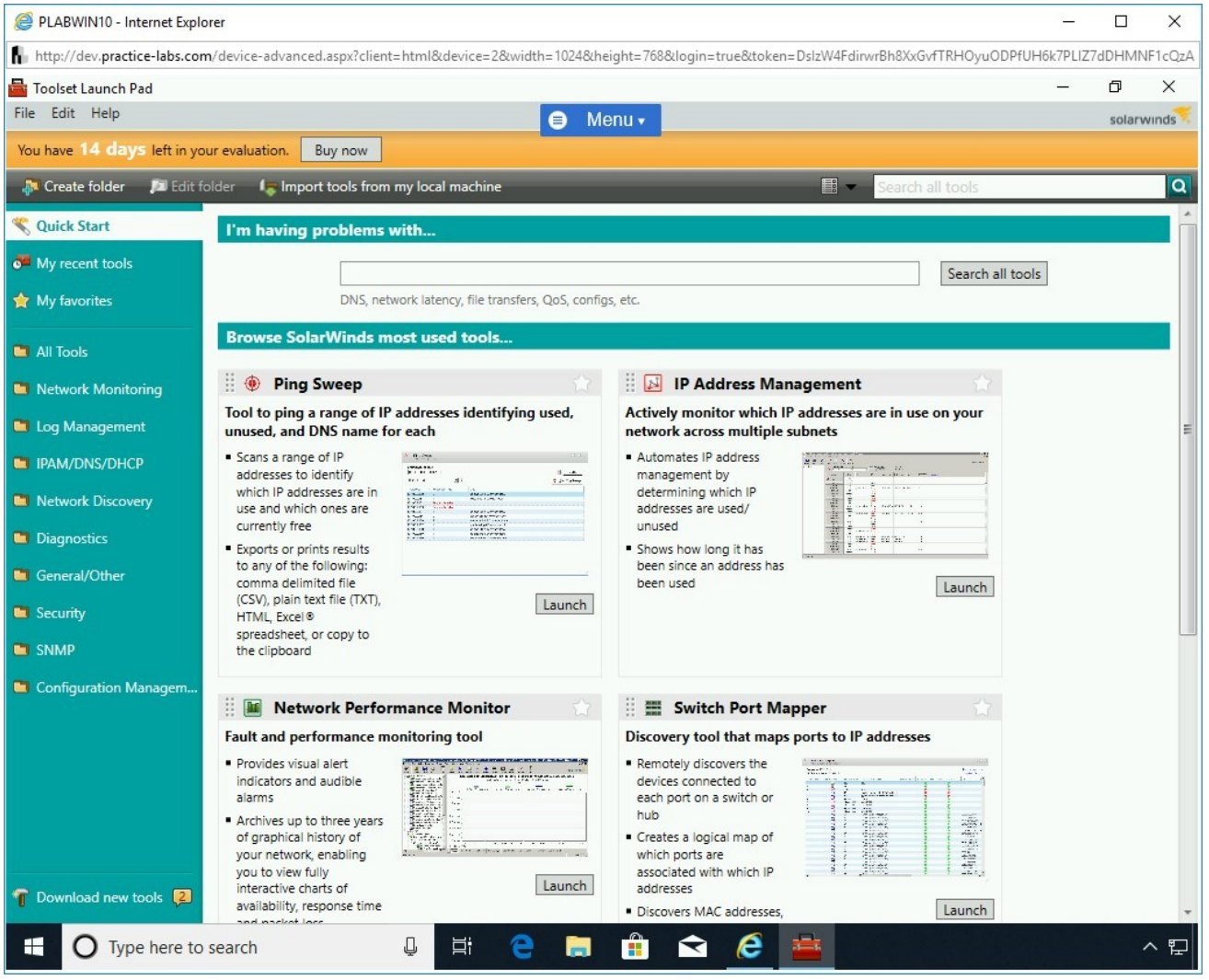


Figure 1.113 Screenshot of PLABWIN10: Showing the Toolset Launch Pad page.

Step 17

Before performing SNMP enumeration, you need to ensure that the target machine is set to accept requests.

In this task, you will configure **PLABDC01** for accepting the requests.

Connect to **PLABDC01**. The desktop is displayed.

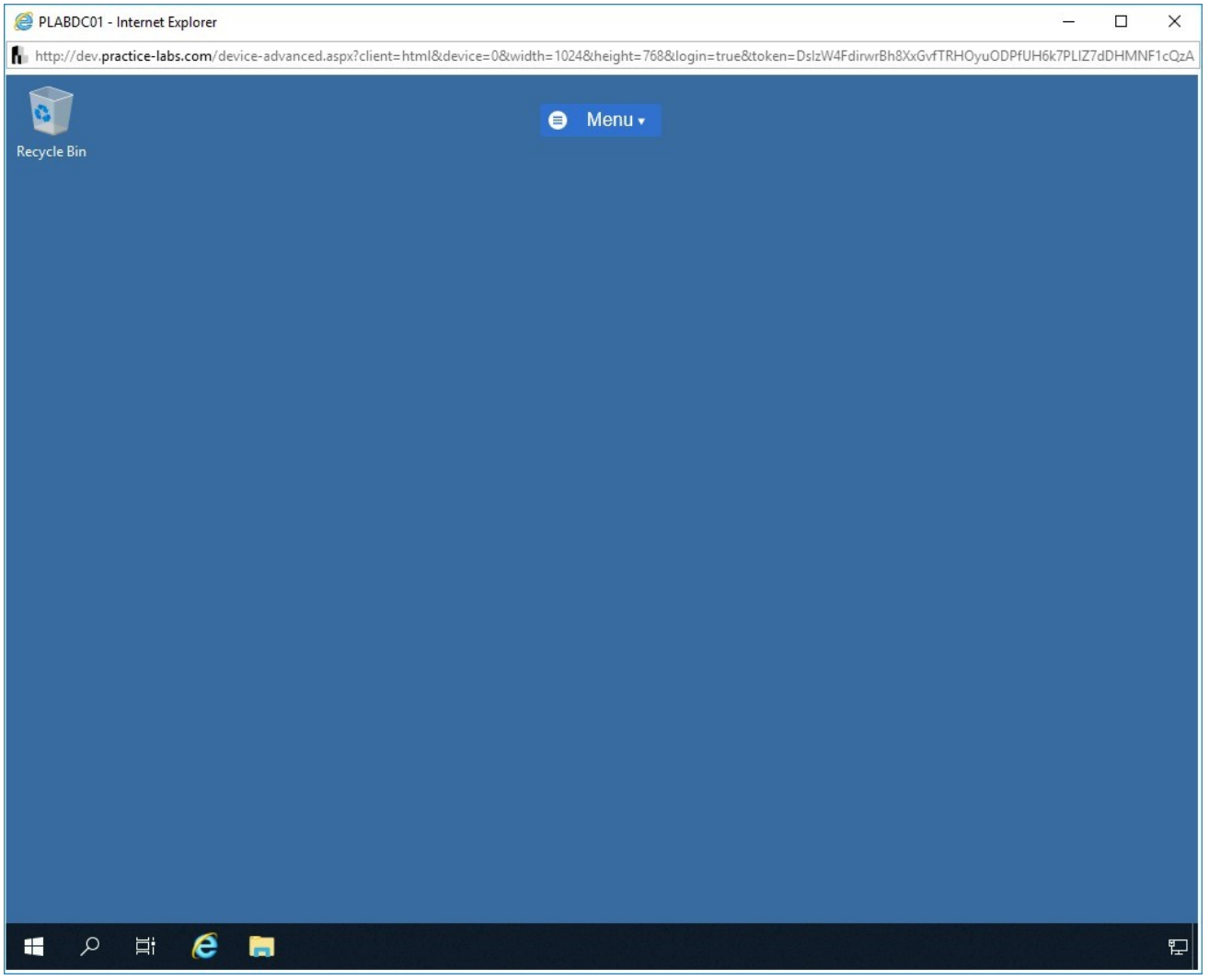


Figure 1.114 Screenshot of PLABDC01: Showing the desktop of PLABDC01.

Step 18

Click the **Start charm**, click **Windows Administrative Tools**, and then select **Services**.

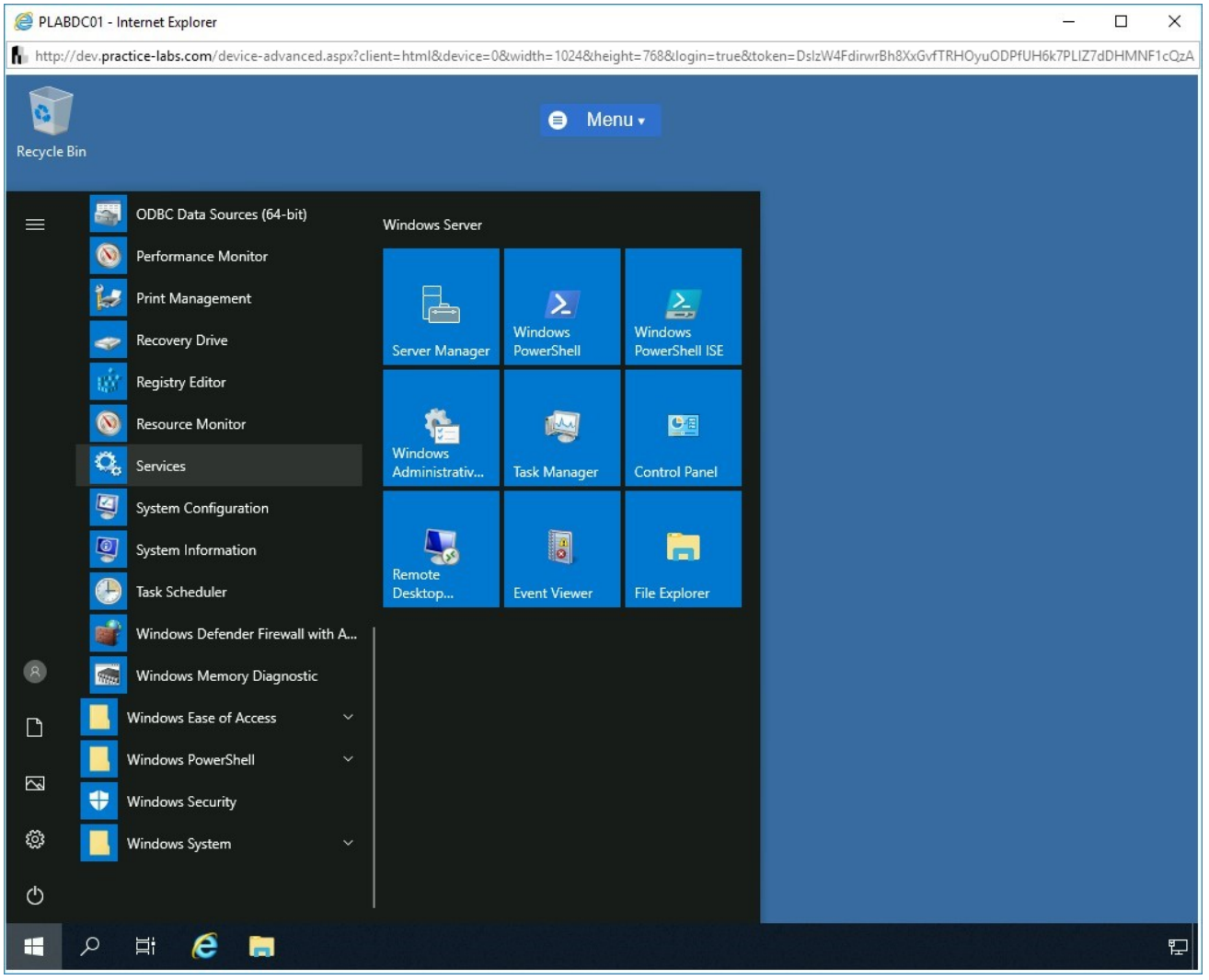


Figure 1.115 Screenshot of PLABDC01: Clicking Services from the Start -> Windows Administrative Tools menu.

Step 19

The **Services** snap-in is displayed.

Scroll down and select **SNMP Service**.

Double-click **SNMP Service**.

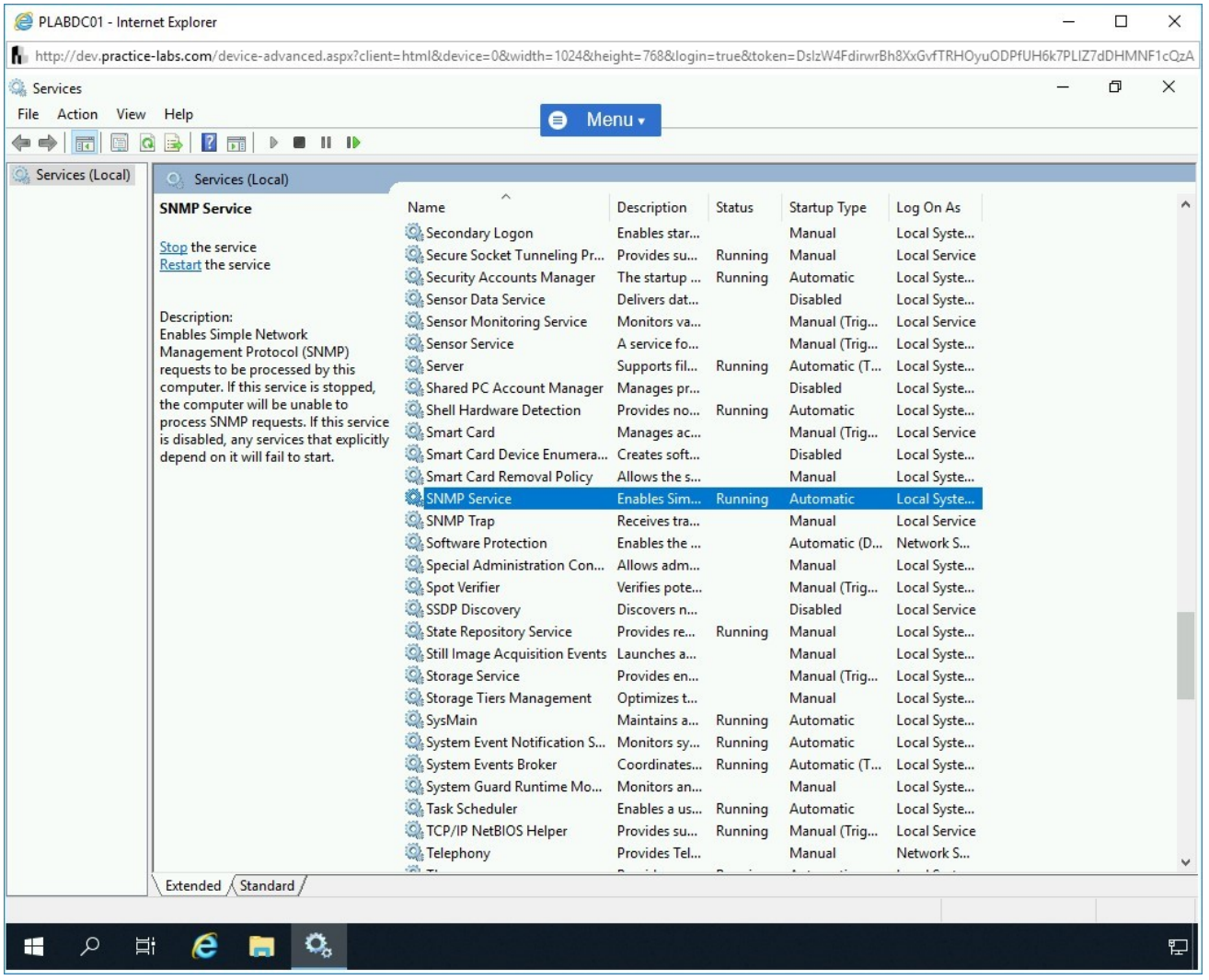


Figure 1.116 Screenshot of PLABDC01: Double-clicking the SNMP service in the Services console.

Step 20

The **SNMP Service Properties (Local Computer)** dialog box is displayed.

Click the **Security** tab.

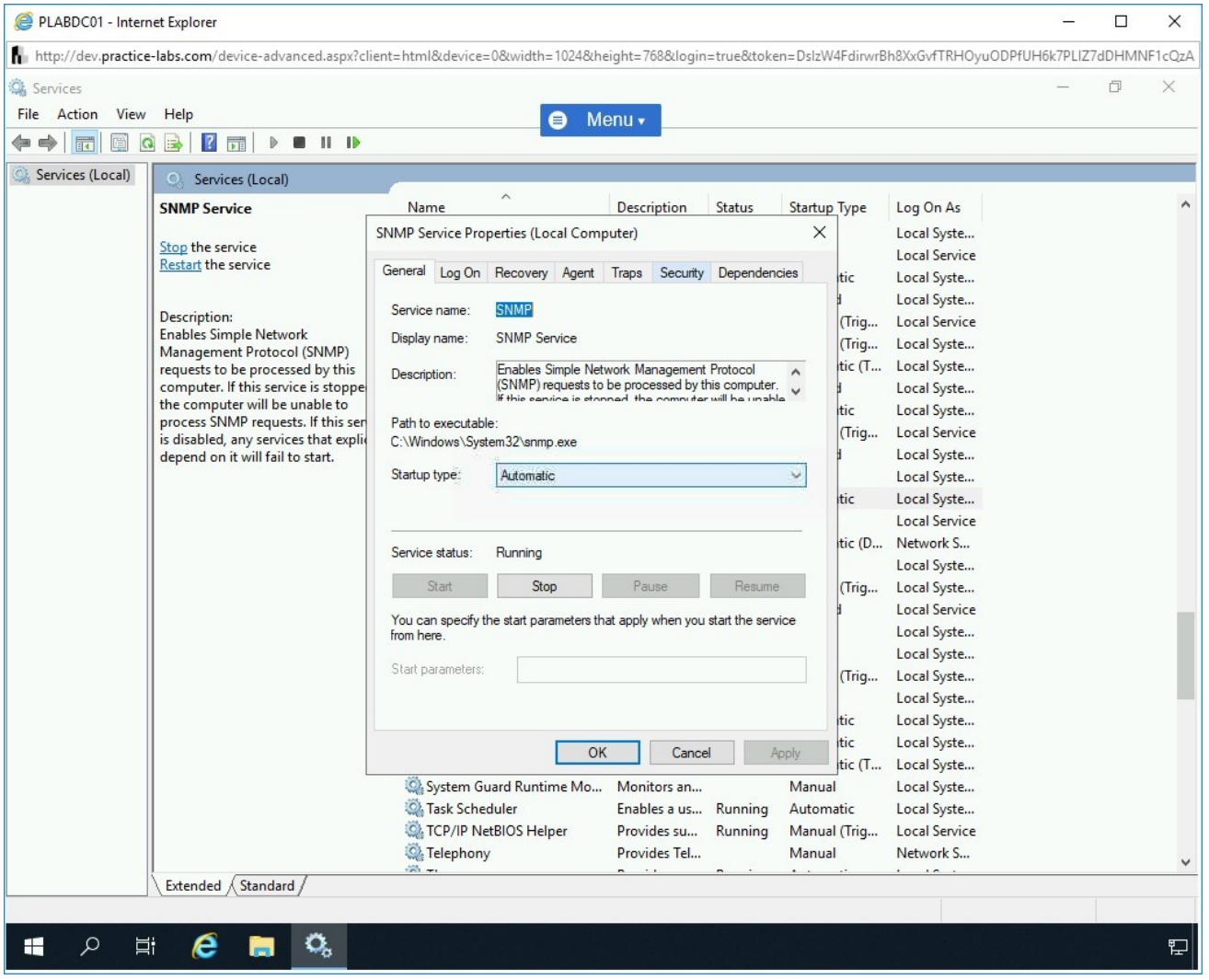


Figure 1.117 Screenshot of PLABDC01: Clicking the Security tab.

Step 21

Here, you will define a community and allow this system to accept SNMP packets from other systems.

Click **Add** under the **Accepted community names** section.

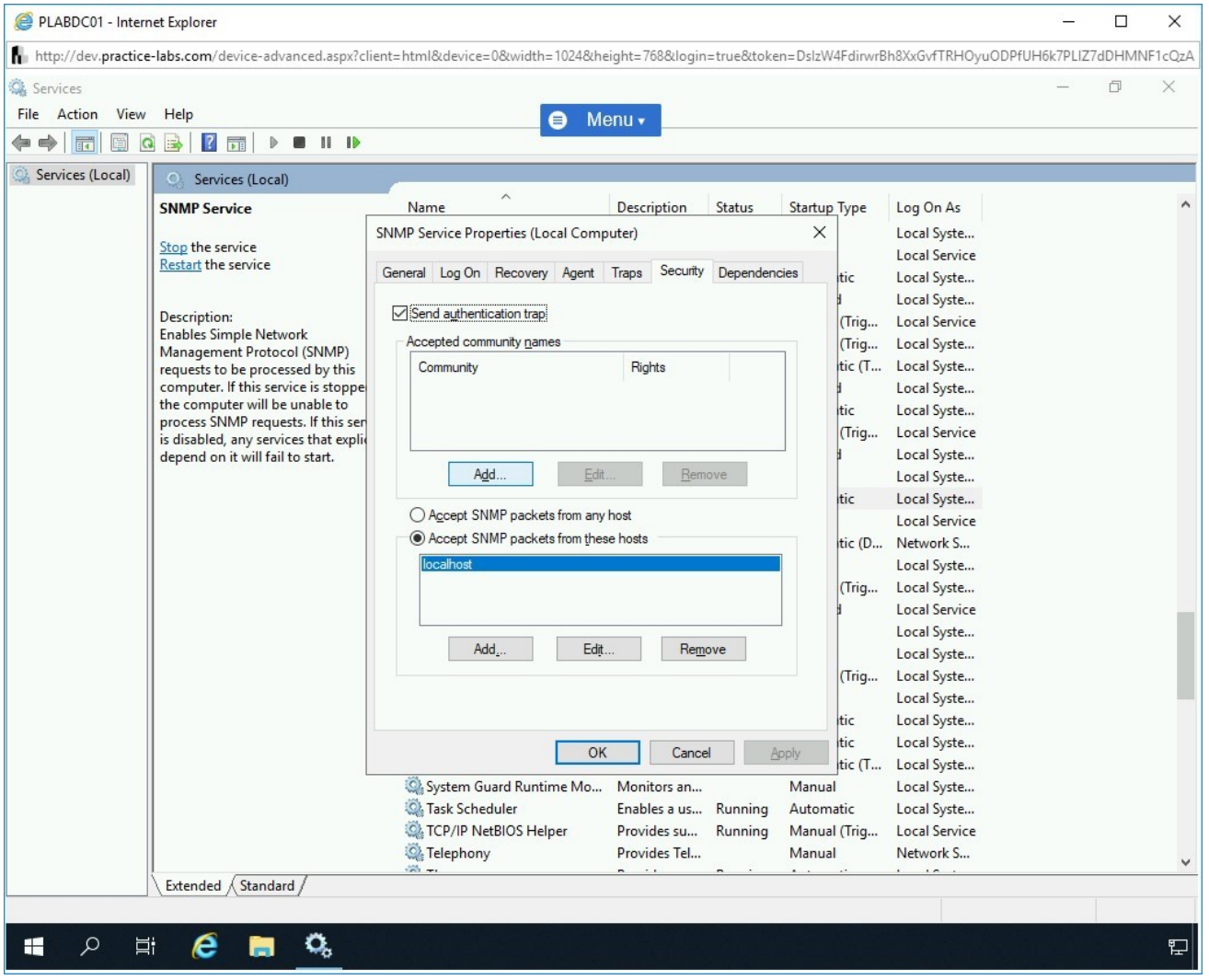


Figure 1.118 Screenshot of PLABDC01: Clicking Add under the Accepted community names section.

Step 22

The **SNMP Service Configuration** dialog box is displayed.

In the **Community Name** text box, type the following name:

```
public
```

Click **Add**.

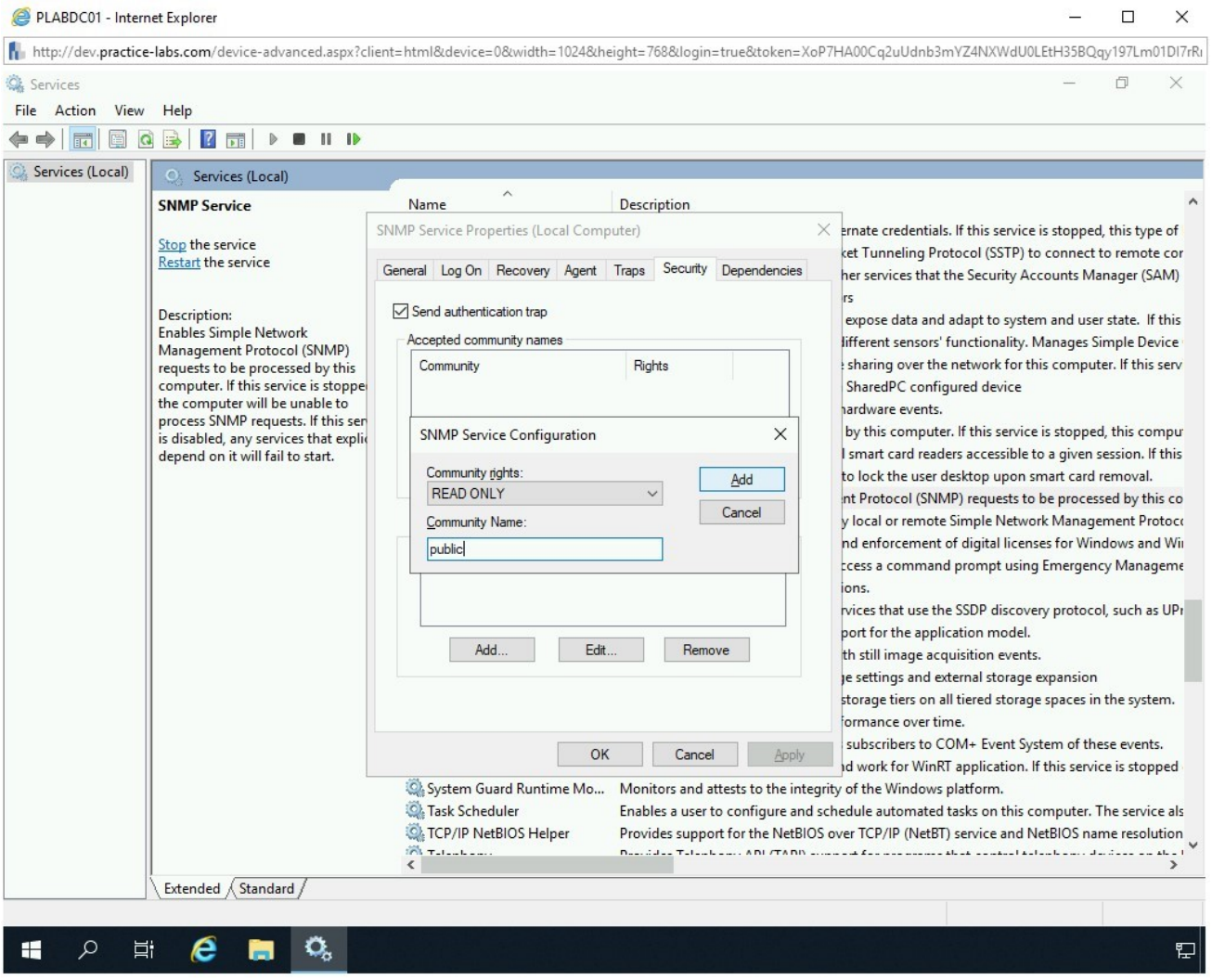


Figure 1.119 Screenshot of PLABDC01: Clicking Add in the SNMP Service Configuration dialog box.

Step 23

Notice that the community public appears in the Accepted Community names section. Select **Accept SNMP packets from any host** and click **OK**.

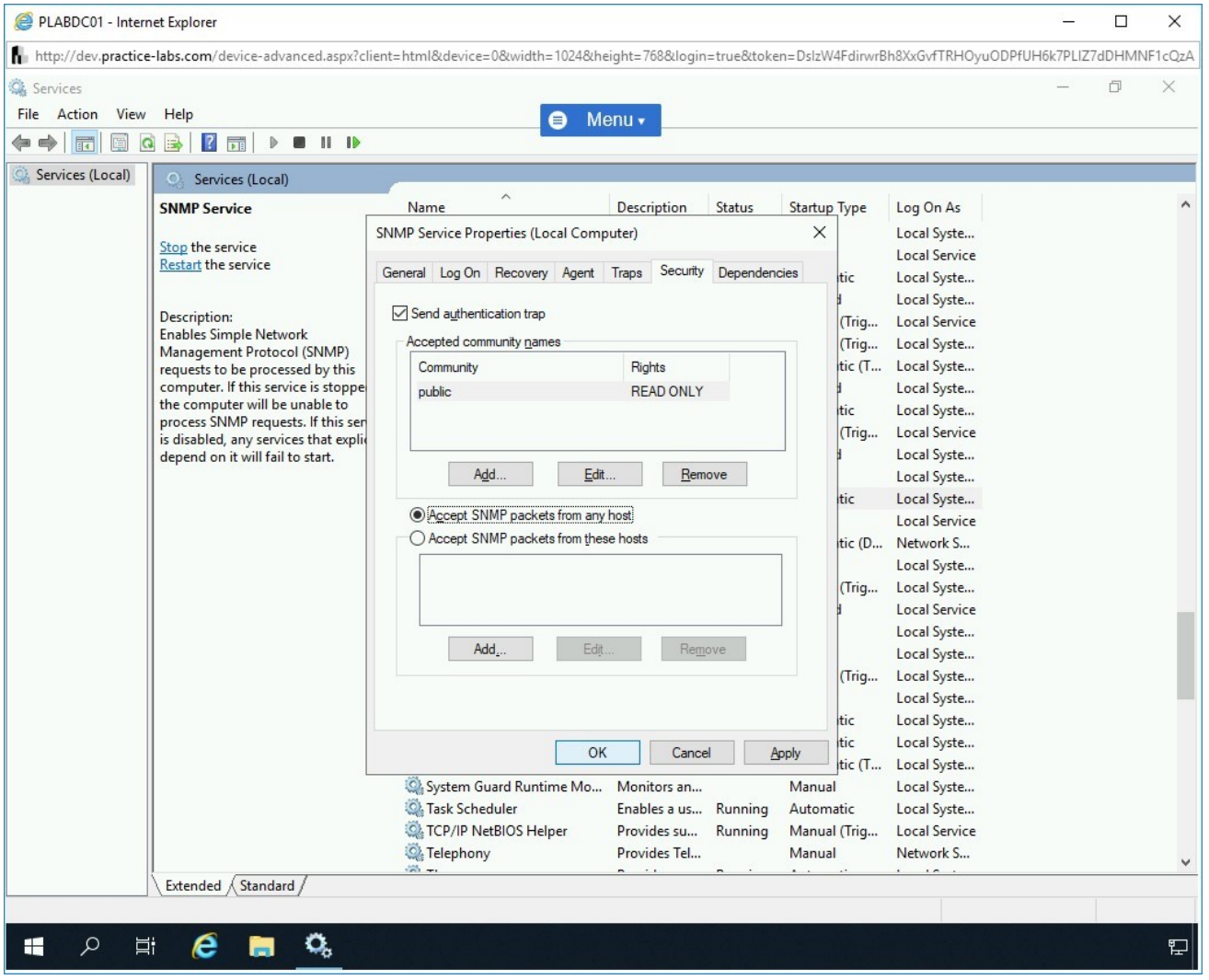


Figure 1.120 Screenshot of PLABDC01: Selecting Accept SNMP packets from any host and clicking OK.

Step 24

Connect to **PLABWIN10**. The **Toolset LaunchPad** window is already open. Click **SNMP** in the left pane.

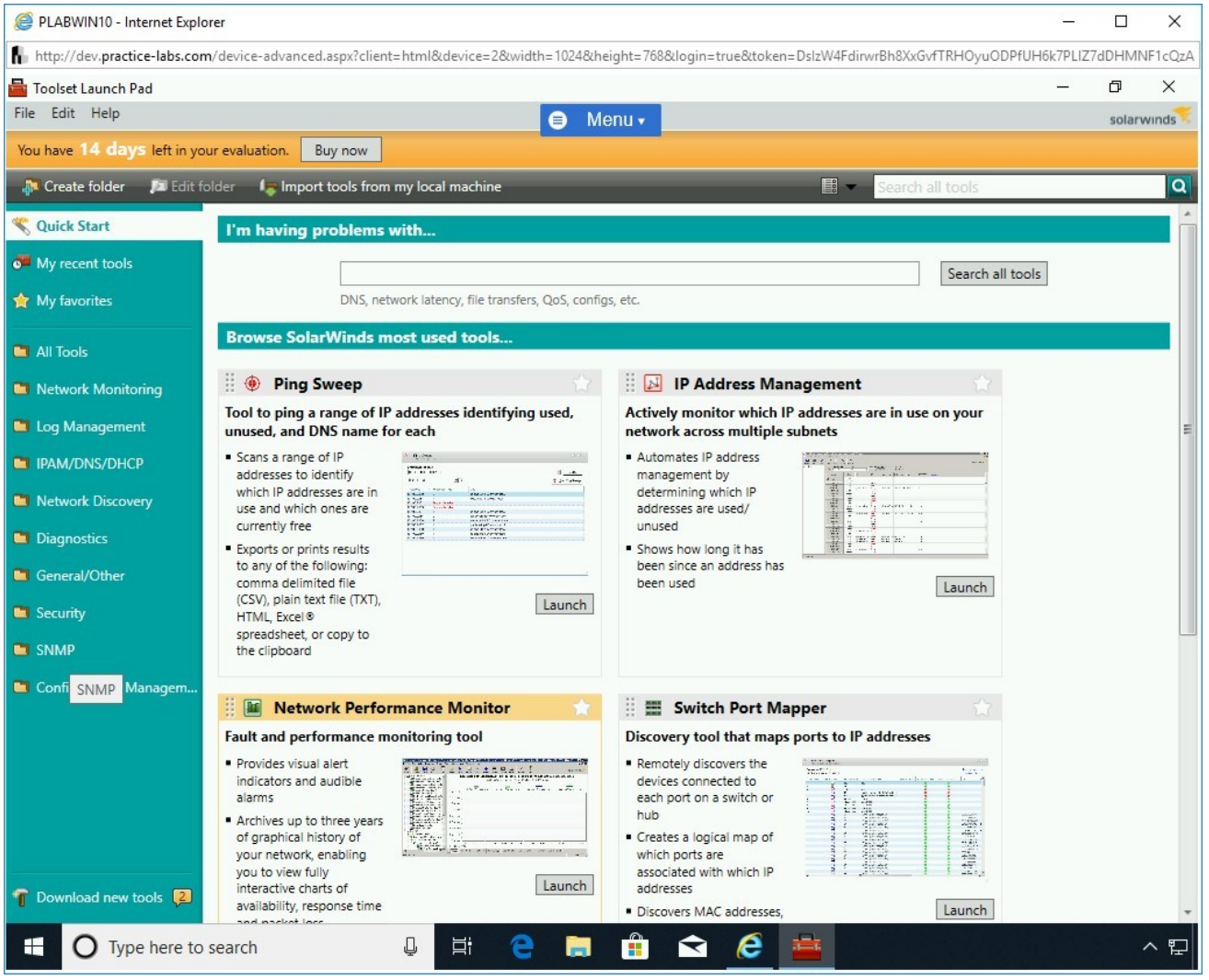


Figure 1.121 Screenshot of PLABWIN10: Clicking SNMP in the left pane.

Step 25

The right pane lists several SNMP related tools.

Click **Launch** under **MIB Viewer**.

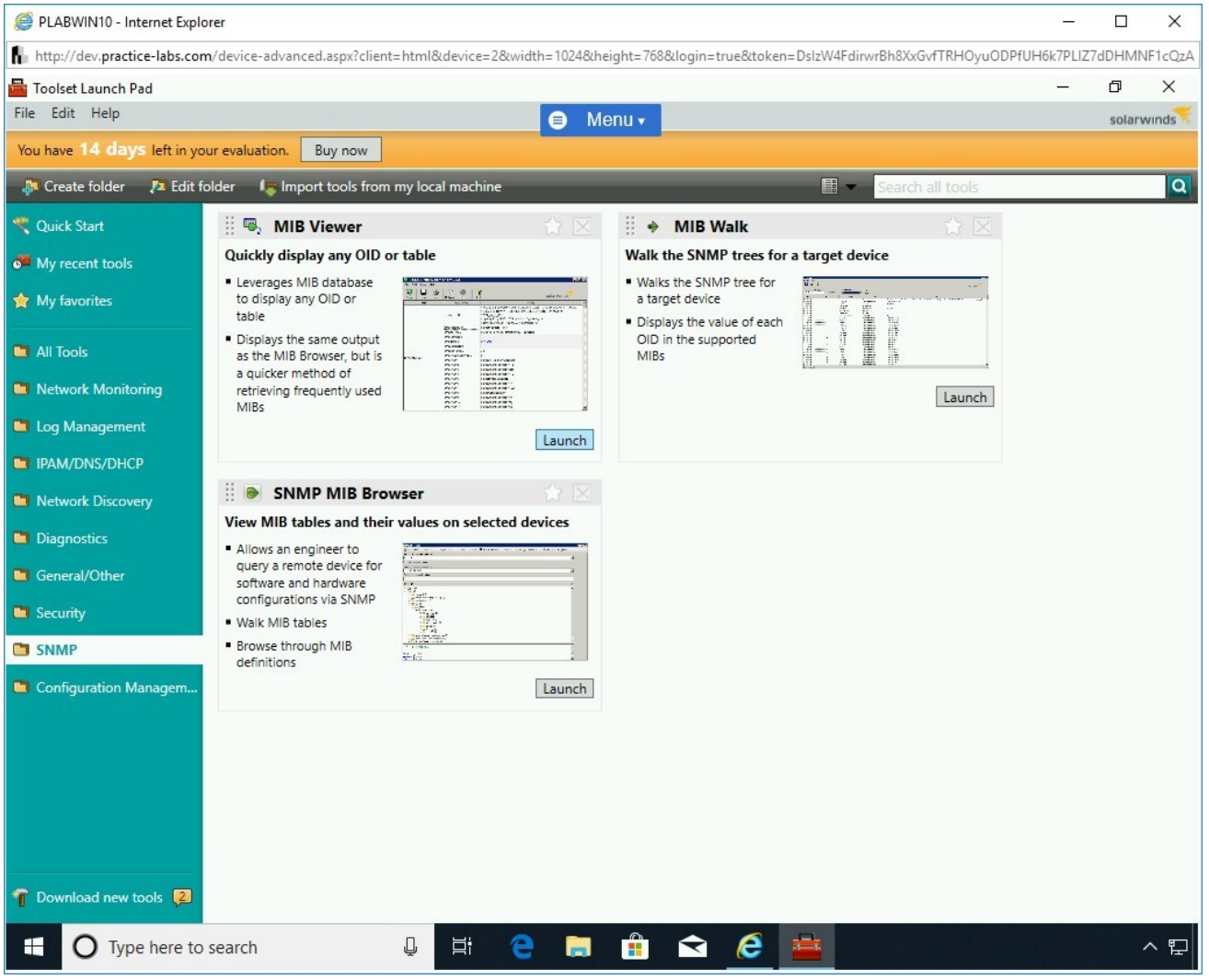


Figure 1.122 Screenshot of PLABWIN10: Clicking Launch under MIB Viewer.

Step 26

The **Toolset** dialog box is displayed.

Click **Continue Evaluation**.

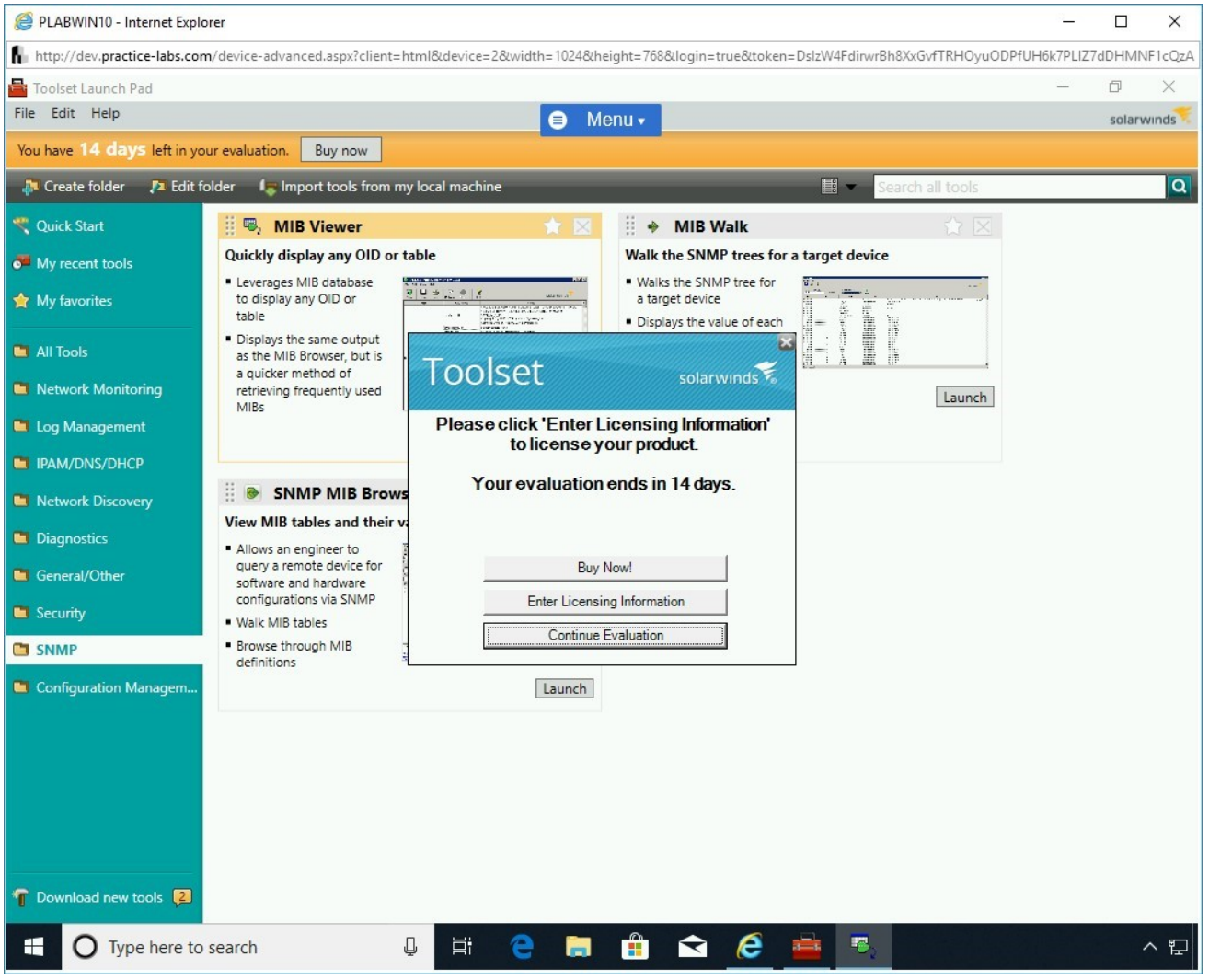


Figure 1.123 Screenshot of PLABWIN10: Clicking Continue Evaluation in the Toolset dialog box.

Step 27

The **MIB Viewer** dialog box is displayed.

Click inside the **Hostname or IP Address** textbox.

The **Device Credentials** dialog box is displayed. in the **Device or IP address** drop-down, enter:

```
192.168.0.1
```

From the **Community string** drop-down, type:

```
public
```

Click **OK**.

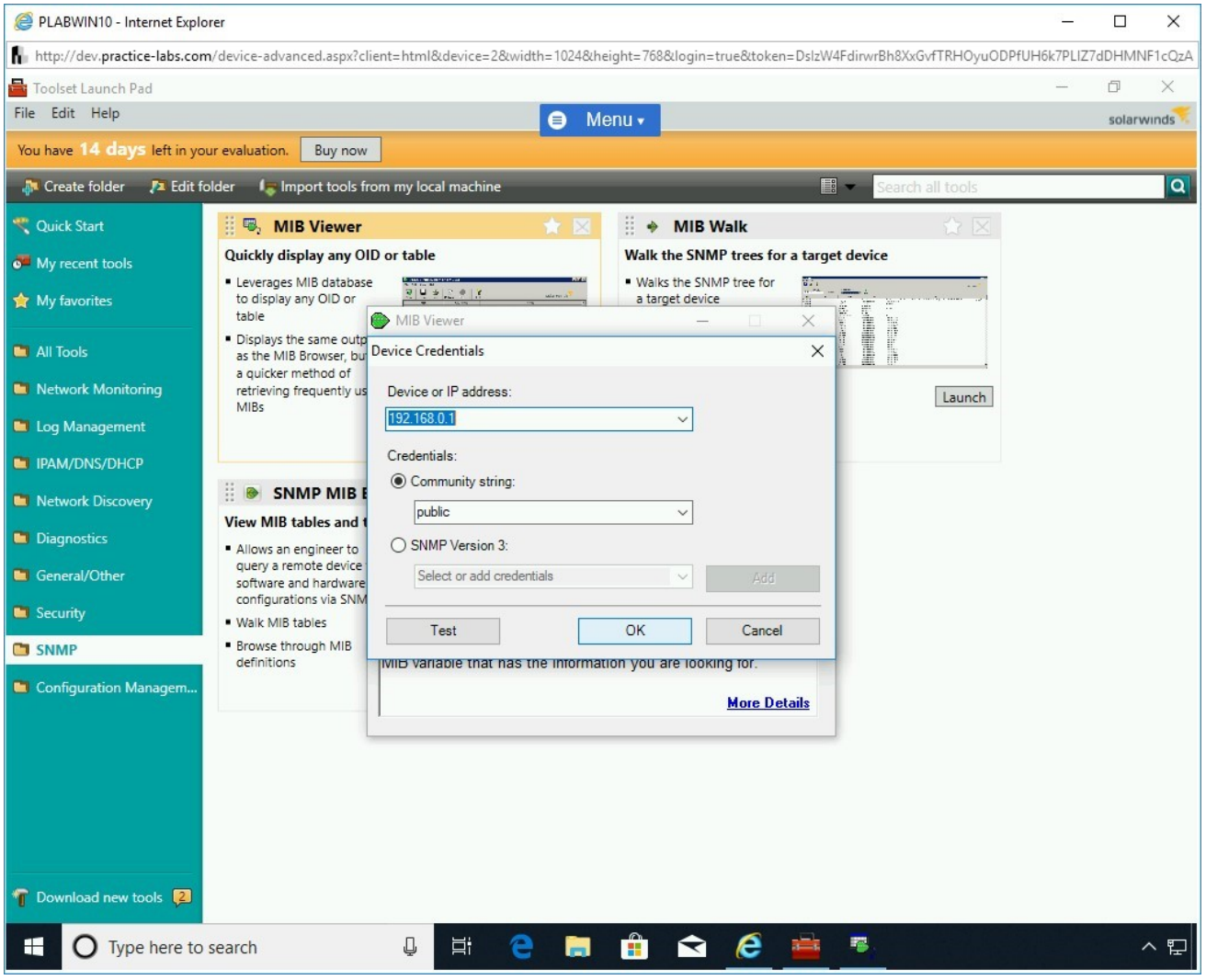


Figure 1.124 Screenshot of PLABWIN10: Configuring the target properties and clicking OK.

Step 28

You will then be prompted to **store the Community string,** click **Yes.**

Note that the name is now populated in the **Hostname or IP Address** textbox.

From the **MIB Table to download** drop-down, select any of the given MIB Table names.

Click **Download MIB Table**.

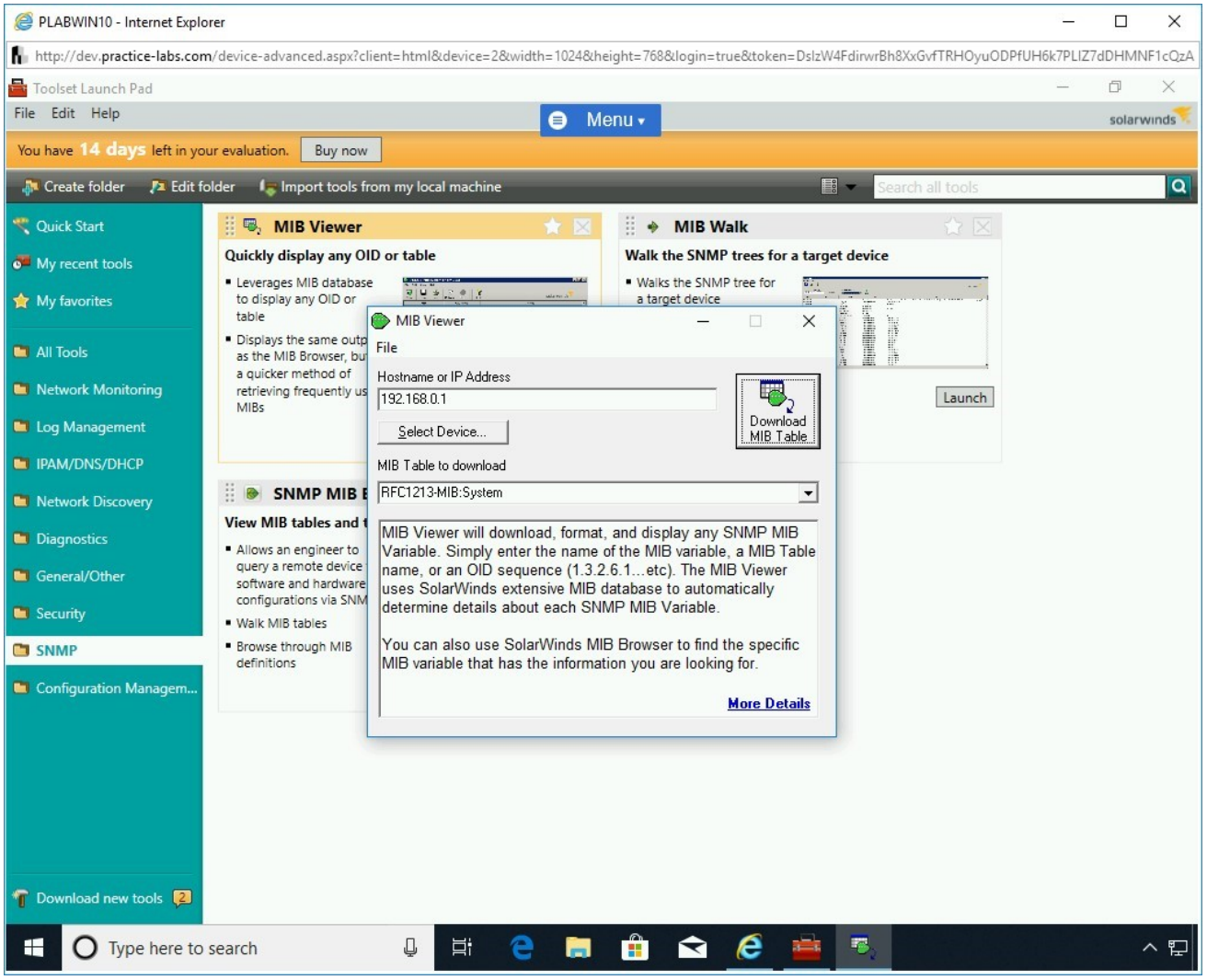


Figure 1.125 Screenshot of PLABWIN10: Clicking Download MIB Table in the MIB Viewer dialog box.

Step 29

The **RFC1213-MIB:system on PLABDC01.PRACTICELABS.COM** dialog box is displayed. The required information is displayed. Similar to this tool, you can try other listed tools.

Close the MIB table.

Close the **Toolset Launch Pad**.

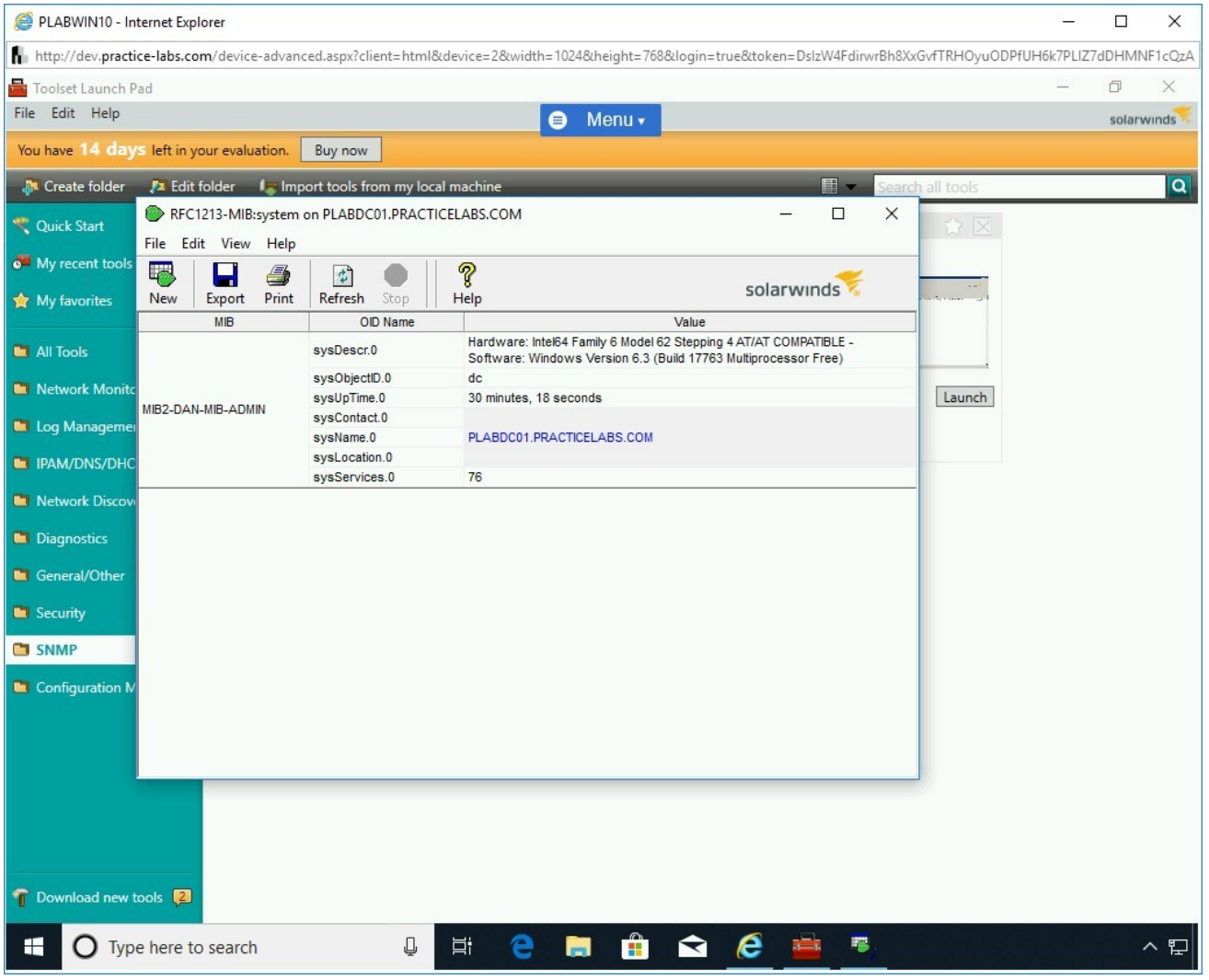


Figure 1.126 Screenshot of PLABWIN10: Showing the download MIB Table and then closing Toolset Launch Pad.

Exercise 2 - Enumeration Techniques using Kali Linux Tools

Just like the Windows-based tools, there are several enumeration tools available in Kali Linux. Some of the key tools are rpcclient, dnsenum, and nmap. With the help of these tools, you can perform different types of enumeration, such as web application, web server, Domain Name Service (DNS), and so on.

In this exercise, you will learn about enumeration techniques using Kali Linux tools.

Learning Outcomes

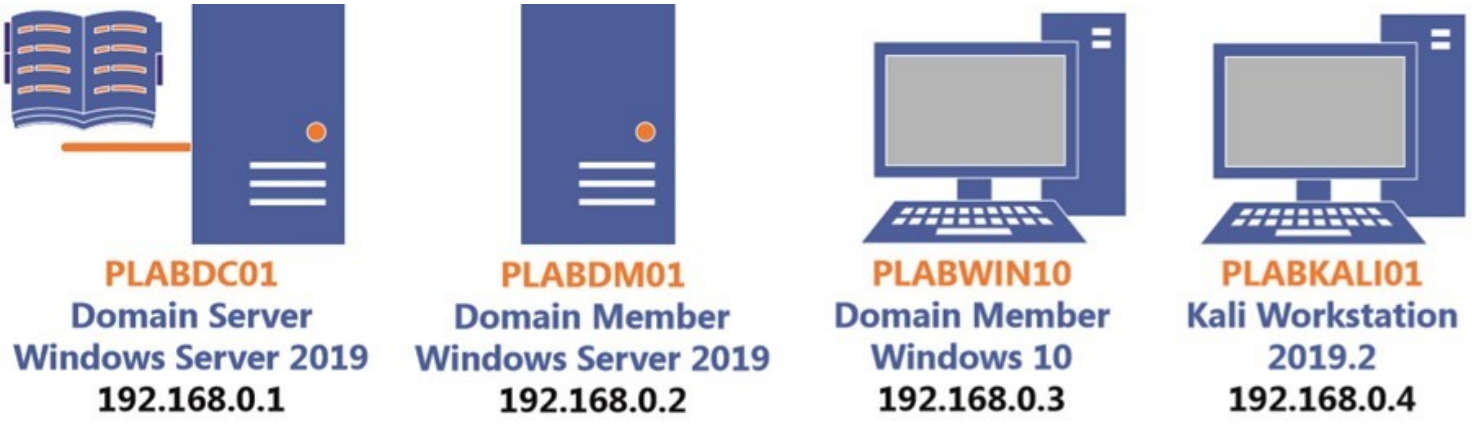
After completing this exercise, you will be able to:

- Perform DNS Enumeration
- Perform Windows Host Enumeration using Rpcclient
- Perform Linux Host Enumeration using Nmap
- Perform Website Enumeration using Nmap
- Perform Server Message Block (SMB) Enumeration

Your Devices

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

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



Task 1 - Perform DNS Enumeration

DNS plays a vital role on the Internet. It translates a domain name to an IP address. By probing a DNS, you can find information about the DNS and mail servers for a specific domain.

In this task, you will perform DNS enumeration. 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
```

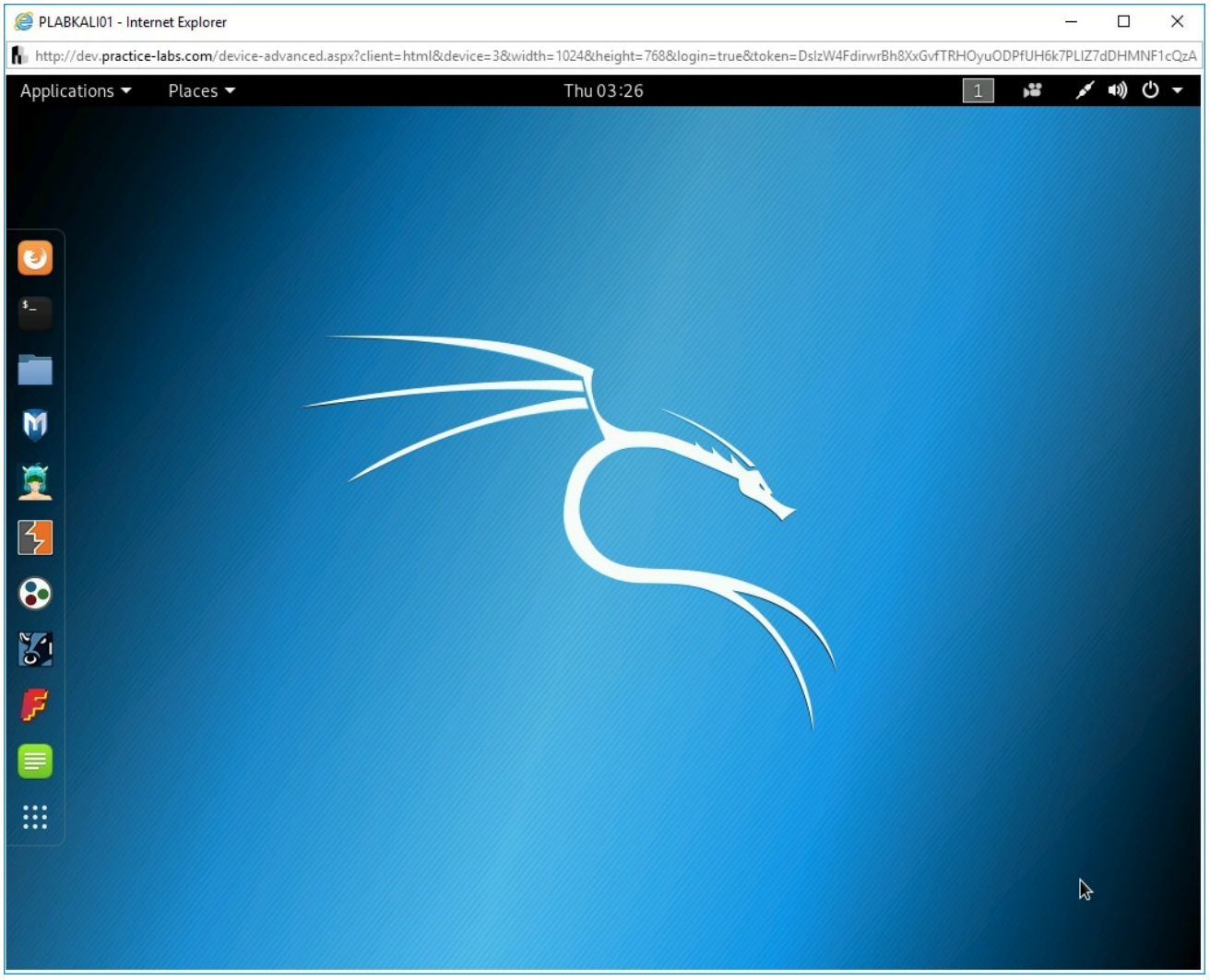


Figure 2.1 Screenshot of PLABKALI01: Showing the desktop of PLABKALI01.

Step 2

On the desktop, in the left pane, click the **Terminal** icon.

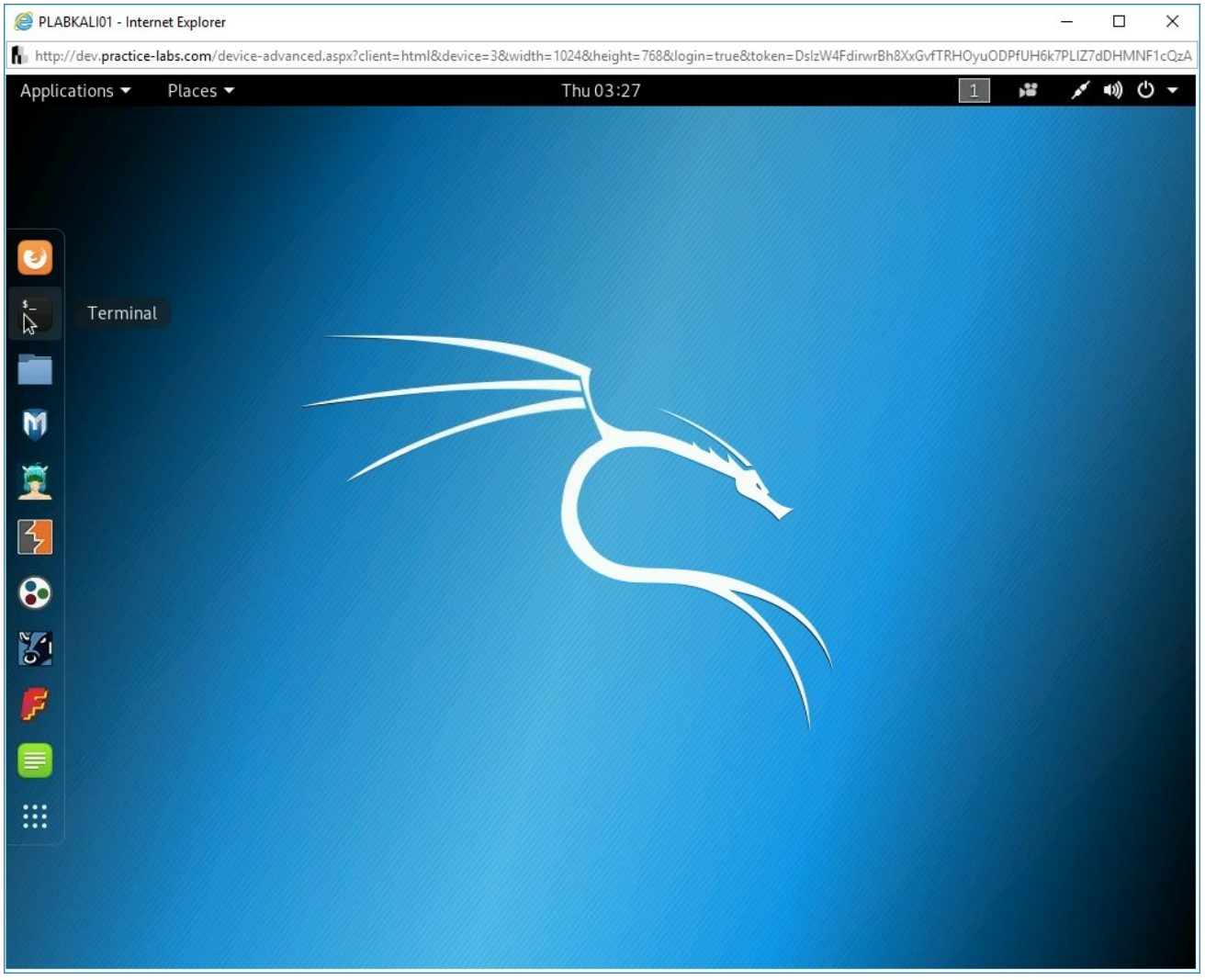


Figure 2.2 Screenshot of PLABKALI01: Clicking the Terminal icon in the left pane.

Step 3

The terminal window is displayed. Let's first find the nameserver for the **practicelabs.com** domain. You can use the **host** command with the **-t** parameter to do the same. The **ns** parameter is for the nameserver. Type the following command:

```
host -t ns practicelabs.com
```

Press **Enter**.

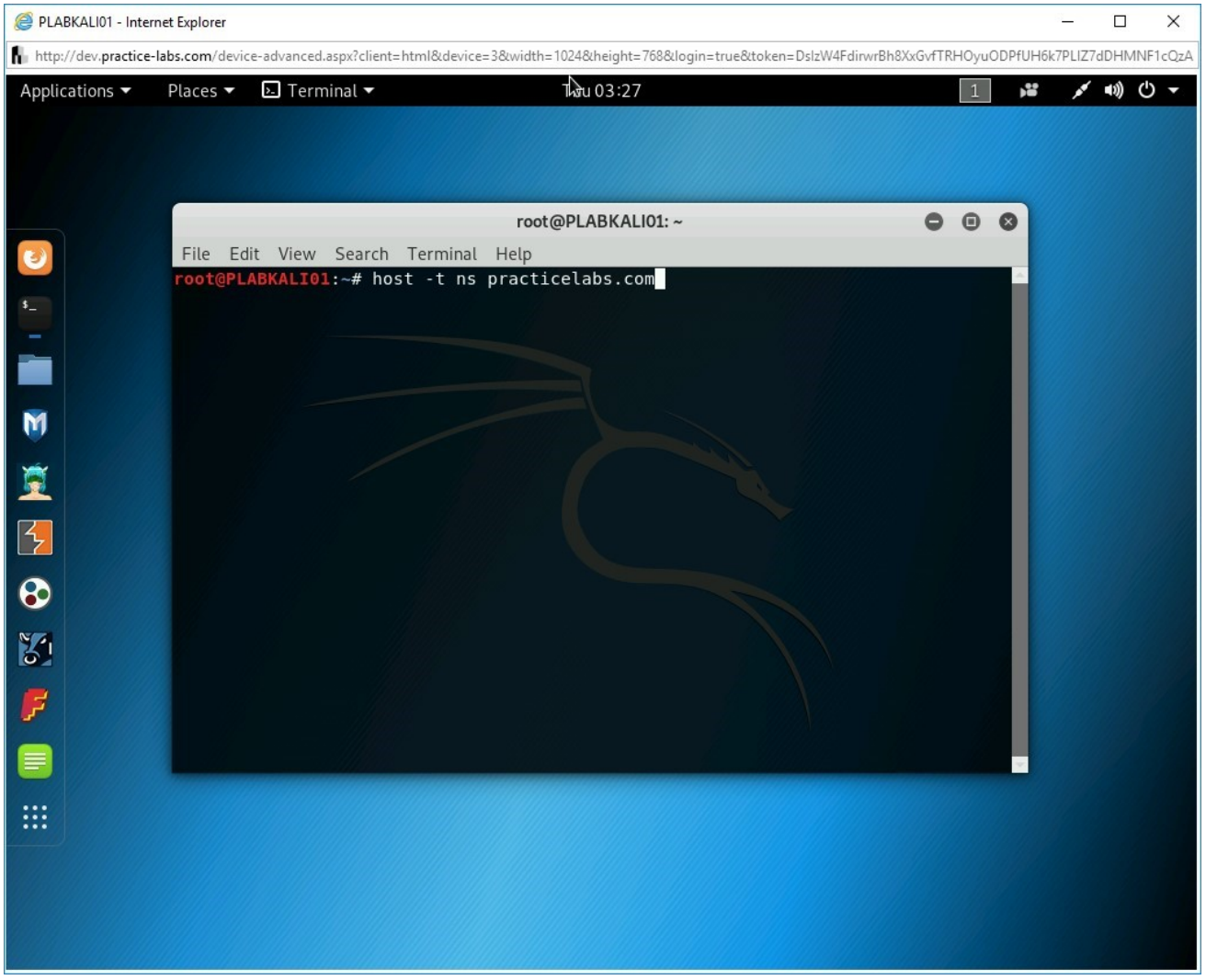


Figure 2.3 Screenshot of PLABKALI01: Entering the host command to find the nameserver for practicelabs.com.

Step 4

Notice that the name server details are displayed.

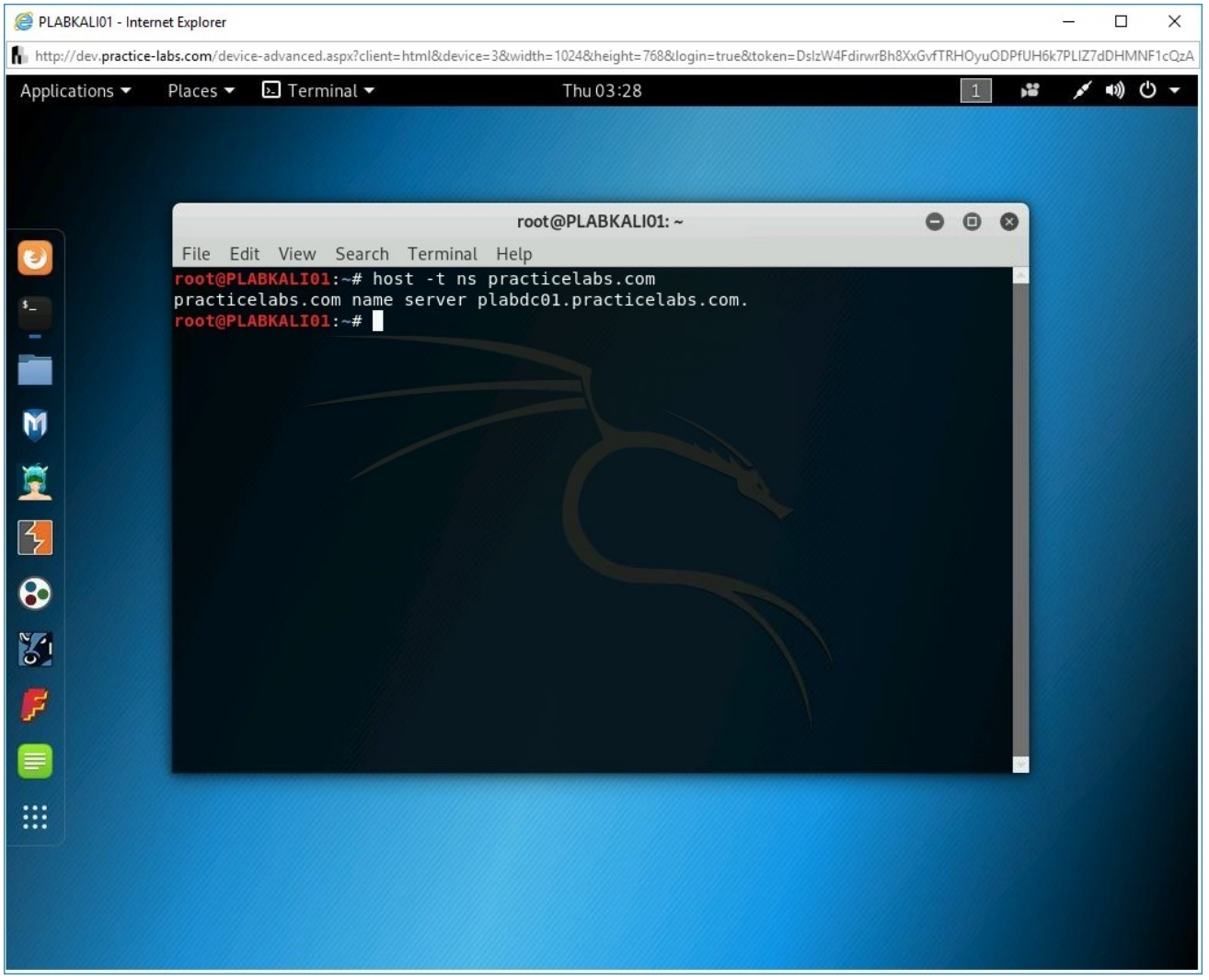


Figure 2.4 Screenshot of PLABKALI01: Showing the name of the nameserver for practicelabs.com.

Step 5

Let's now find the mail server for the **practicelabs.com** domain. You can use the host command with the **-t** parameter to do the same. The **mx** parameter is for the mail server. Type the following command:

```
host -t mx practicelabs.com
```

Press **Enter**.

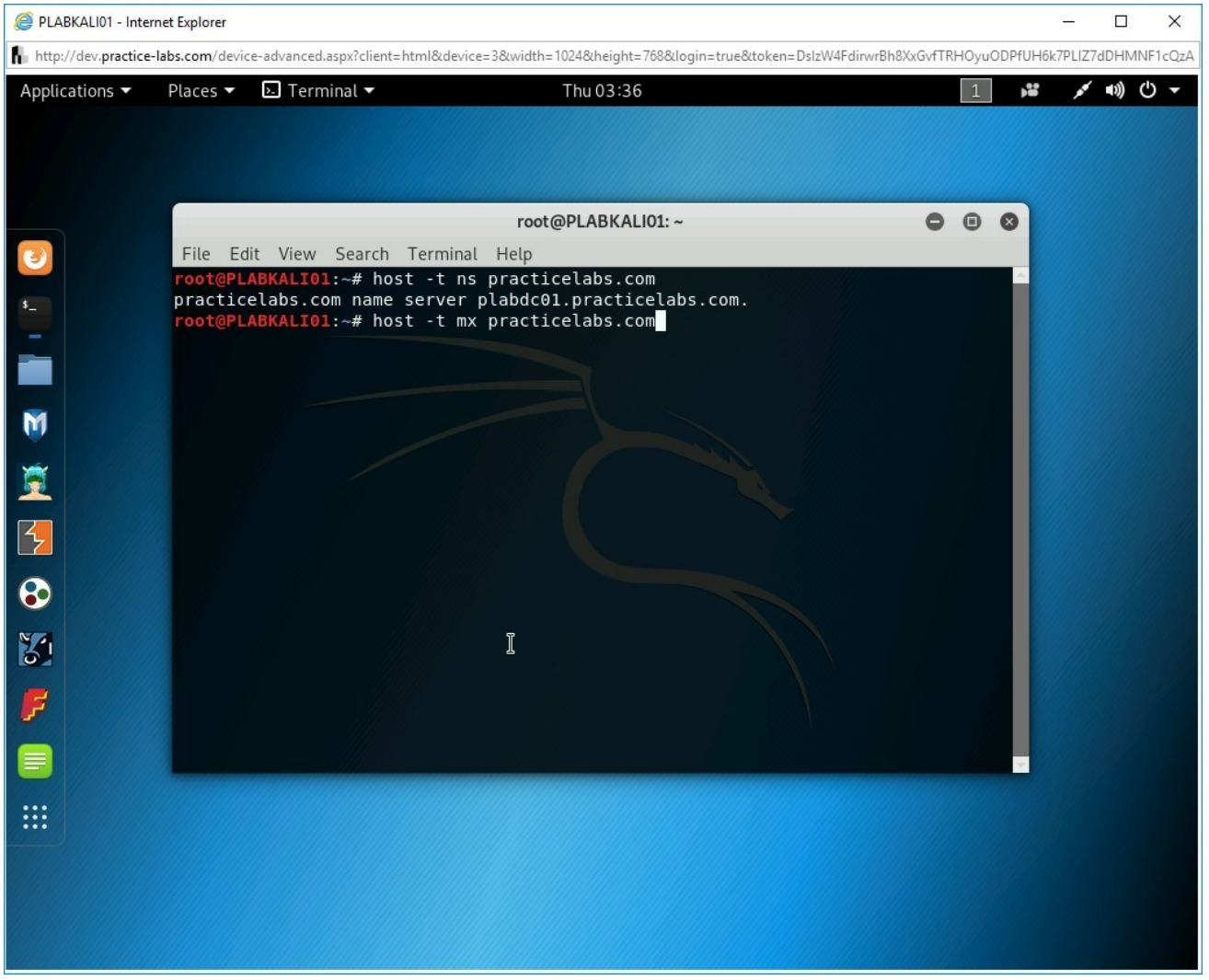


Figure 2.5 Screenshot of PLABKALI01: Entering the host command to find the mail server for practicelabs.com.

Step 6

Notice that there are no messaging servers.

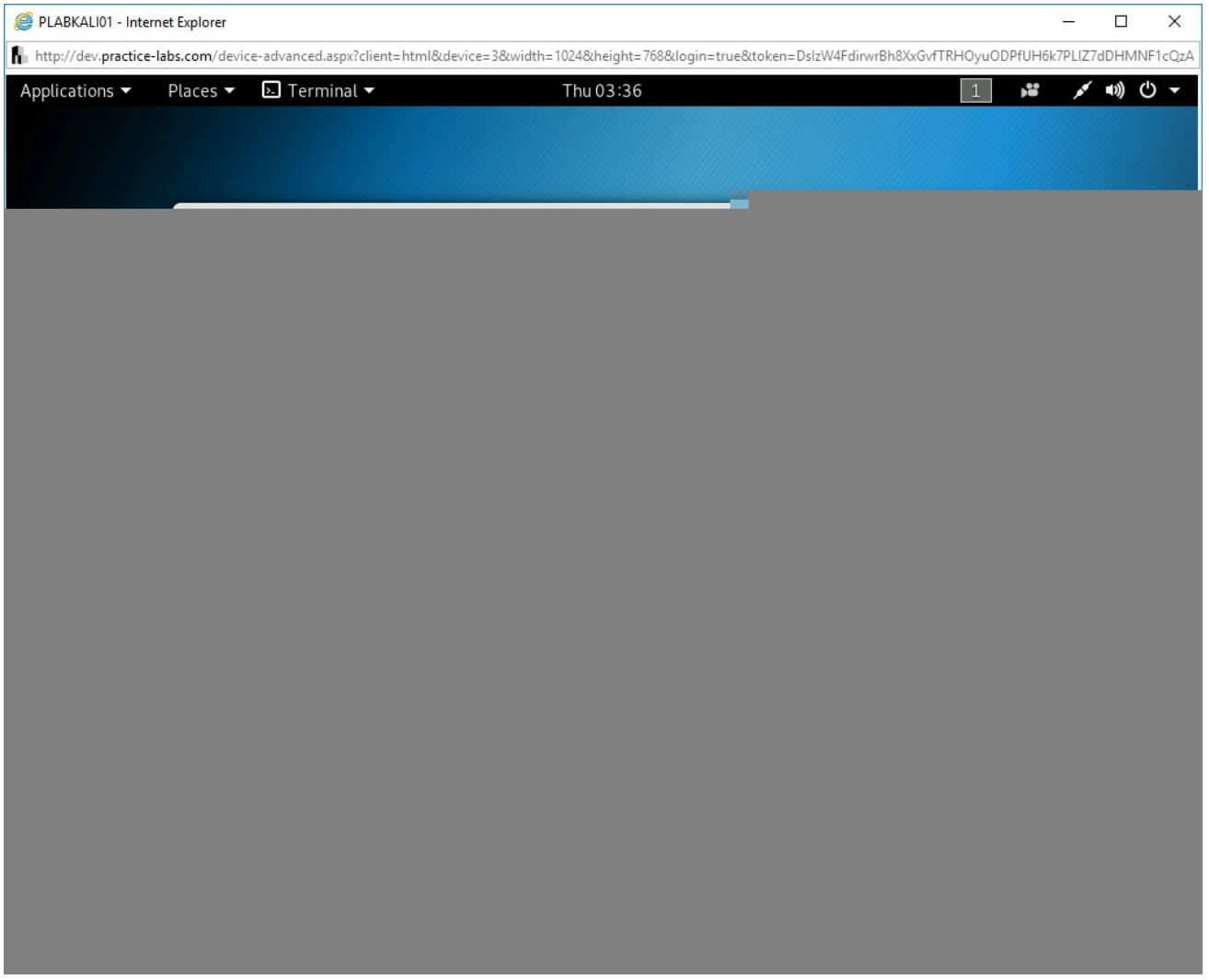


Figure 2.6 Screenshot of PLABKALI01: Showing the output of the host command with no messaging server.

Step 7

Clear the screen by entering the following command:

```
clear
```

You will now gather the information about various services in a text file named **plab.txt**. Later, you will create a loop with the hostname and display the details of each service if it exists.

Note: *The first command will write the output of the echo command in a file named plab.txt using the > operator. The second to the last command will append the output to the plab.txt file using the >> operator.*

Type the following commands:

```
echo www > plab.txt
echo ftp >> plab.txt
echo mail >> plab.txt
echo proxy >> plab.txt
```

Press **Enter** after each command.

Figure 2.7 Screenshot of PLABKALI01: Using the echo command to gather the information about various services in a text file named plab.txt.

Step 8

Next, you will create a for loop to generate the list of services with their IP addresses. In this command, you are automating the **Forward DNS Lookup** using the host command in a script. You can attempt to guess valid names for the servers using this script. For example, if there is a web server configured as www.practicelabs.com, you will be able to find it using this script.

Type the following command:

```
for ip in $(cat plab.txt); do host
$ip.practicelabs.com;done
```

Press **Enter**.

Figure 2.8 Screenshot of PLABKALI01: Creating a for loop to generate the list of services with their IP addresses.

Step 9

Notice the output of the loop. None of these services were found.

Figure 2.9 Screenshot of PLABKALI01: Showing the output of the loop.

Step 10

Clear the screen by entering the following command:

```
clear
```

Let's now look at DNS zone transfer. In a secure environment, DNS zone transfer would be limited to authorized slave DNS servers. If you do not configure it properly, then the zone transfer can be configured to any DNS server.

You will now try zone transfer on **plabdc01.practicelabs.com**. To do this, type the following command:

```
host -l practicelabs.com plabdc01.practicelabs.com
```

Press **Enter**.

Figure 2.10 Screenshot of PLABKALI01: Entering the command to perform DNS zone transfer.

Step 11

The outcome of this command is displayed. In this outcome, the **plabdc01.practicelabs.com** nameserver has refused the zone transfer request.

Figure 2.11 Screenshot of PLABKALI01: Showing the outcome with an error for the DNS zone transfer.

Step 12

Clear the screen by entering the following command:

```
clear
```

Kali Linux also contains a DNS enumeration tool named **DNSRecon**. To use **DNSRecon**, type the following command:

Note: *The -d parameter defines the domain name. The -t parameter defines the type of the enumeration.*

```
dnsrecon -d practicelabs.com -t axfr
```

Press **Enter**.

Figure 2.12 Screenshot of PLABKALI01: Entering the dnsrecon command to perform DNS enumeration.

Step 13

Notice the output of this command. It tests the zone transfer, which fails, and lists the **NS** servers. It also provides the open ports on the server.

Figure 2.13 Screenshot of PLABKALI01: Showing the output of the dnsrecon command.

Step 14

Clear the screen by entering the following command:

```
clear
```

Next, you can also use another tool named **DNSEnum**, which also provides similar information to the **DNSRecon** tool. Type the following command:

```
dnsenum practicelabs.com
```

Press **Enter**.

Figure 2.14 Screenshot of PLABKALI01: Entering the dnsenum command for DNS enumeration.

Step 15

Notice that the output nameserver name and IP address and mail server. It also shows zone transfer results.

Figure 2.15 Screenshot of PLABKALI01: Showing the output of the dnsenum command.

Keep the **terminal** window open.

Task 2 - Perform Windows Host Enumeration using Rpcclient

There are different ways to enumerate a Windows host. Using enumeration, you can discover information, such as:

- OS version
- Users
- Services
- Groups
- Privileges
- Shares
- Configuration settings

A Windows host can be enumerated using different methods. For example, you can enumerate a Windows host using:

- Built-in commands
- Nmap
- Rpcclient
- Metasploit framework

Note: *In the previous modules, you have already looked at the Metasploit framework and Nmap. This module will focus on built-in commands of Windows and Rpcclient.*

Other than the commands, Nmap also contains ready-made scripts that can be used for various reasons, such as enumerating a Windows host. For example, consider the following command:

```
nmap 192.168.0.10 --script smb-os-discovery.nse
```

You can find hundreds of ready-made scripts in the **/usr/share/nmap/scripts** directory.

Figure 2.16 Screenshot of PLABKALI01: Showing the listing of the nmap scripts.

Some of the built-in commands in Windows that are commonly used are :

- dir
- ipconfig
- arp
- route
- net share
- net user

Other than the Windows command, Windows PowerShell also offers several built-in cmdlets that can be used. Some of the key cmdlets are:

- Get-Website
- Get-LocalUser
- Get-LocalGroup
- Get-Command

This is not an exhaustive list. You can get a detailed list by searching your favorite search engine.

In this task, you will learn to perform Windows host enumeration. To do this, perform the following steps:

Alert: Before performing this task, ensure the Windows Defender Firewall on **PLABWIN10** Is turned off.

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
```

First, you will work with **Rpcclient**. Type the following command to connect to **PLABWIN10**:

```
rpcclient 192.168.0.3 -U admin
```

Press **Enter**.

Figure 2.17 Screenshot of PLABKALI01: Entering the rpcclient command to connect to a remote system.

Step 2

You are now prompted for the admin password. Type the following:

```
Passw0rd
```

Press **Enter**.

Note: *Password, when entered, will not be visible.*

Figure 2.18 Screenshot of PLABKALI01: Showing the password prompt for the user admin.

Step 3

Notice that the **rpcclient** prompt appears. This indicates that you have connected to **PLABWIN10** successfully.

Figure 2.19 Screenshot of PLABKALI01: Showing the rpcclient prompt after successful login.

Step 4

To display the **PLABWIN10** details, type the following command:

```
srvinfo
```

Press **Enter**.

Figure 2.20 Screenshot of PLABKALI01: Entering the srvinfo command.

Step 5

Notice the output of the **srvinfo** command. It displays the IP address, type of operating system, its version, and so on.

Figure 2.21 Screenshot of PLABKALI01: Showing the output of the srvinfo command.

Step 6

Let's find out the **Security ID (SID)** of the **admin** account. Type the following command:

```
lookupnames admin
```

Press **Enter**.

Figure 2.22 Screenshot of PLABKALI01: Entering the command to find the SID for the admin account.

Step 7

Notice that the **SID** for the admin account is now displayed. **SID** for the **admin** account ends with **1001**.

Note: *If this was the built-in administrator account, then its SID will always end with 500. SID will never change even if you rename the administrator account.*

Figure 2.23 Screenshot of PLABKALI01: Showing the SID for the admin account.

Step 8

To clear the screen, press **Ctrl + l**.

You can also list the privileges that are known in this domain. Type the following command:

```
enumprivs
```

Press **Enter**.

Figure 2.24 Screenshot of PLABKALI01: Entering the command to list the privileges that are known in this domain.

Step 9

The output for the enumprivs command is displayed.

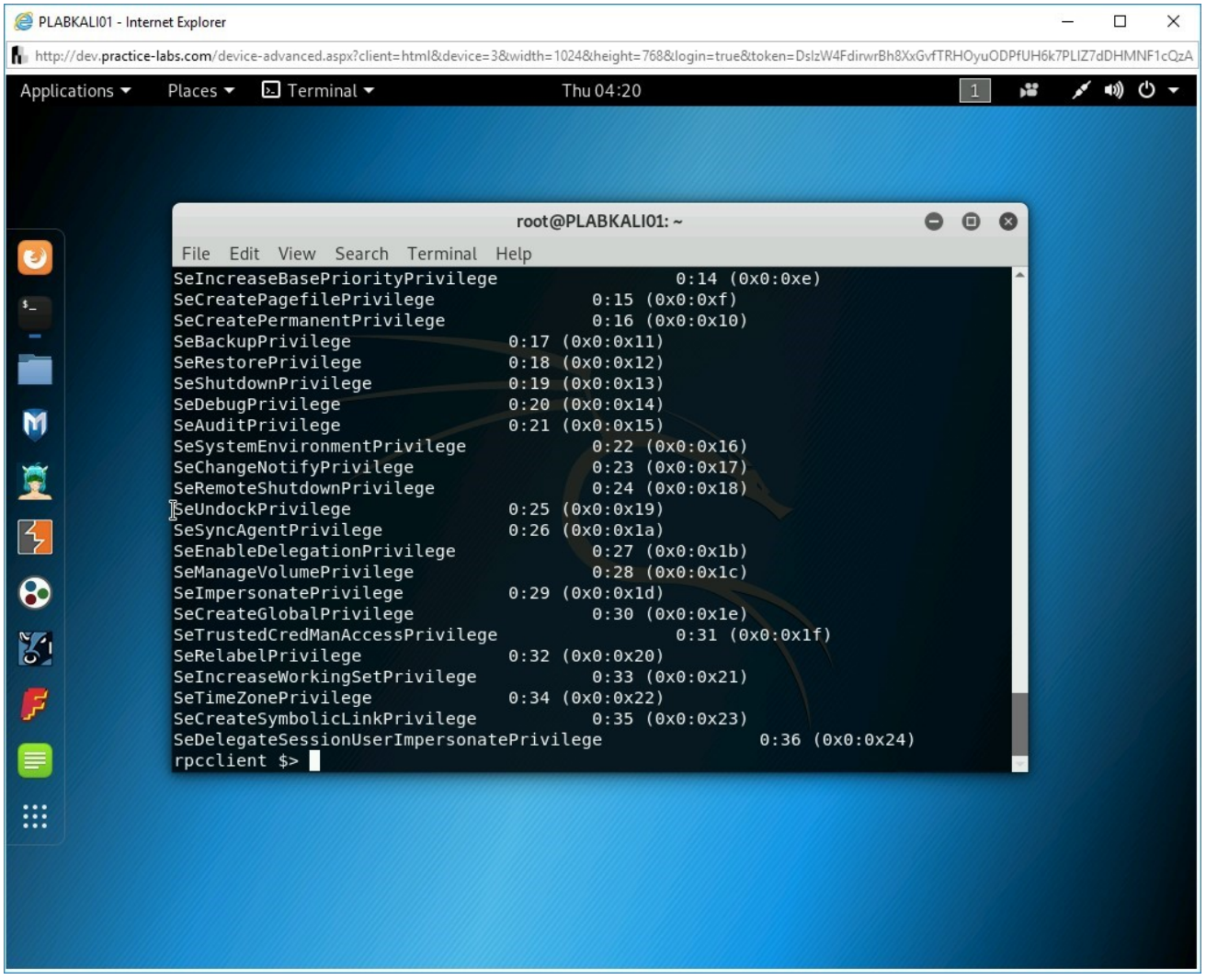


Figure 2.25 Screenshot of PLABKALI01: Showing the output for the enumprivs command.

Step 10

To clear the screen, press **Ctrl + l**.

You can also list the SIDs for the local LSA. Type the following command:

```
lsaenumsid
```

Press **Enter**.

Figure 2.26 Screenshot of PLABKALI01: Entering the command to list the SIDs for the local LSA.

Step 11

Notice that the SIDs for the local LSA is now listed.

Figure 2.27 Screenshot of PLABKALI01: Showing the list of SIDs for the local LSA.

Step 12

To exit from the **rpcclient**, type the following command:

```
exit
```

Press **Enter**.

Figure 2.28 Screenshot of PLABKALI01: Entering the exit command to exit from rpcclient.

Step 13

You are now back on the terminal prompt.

Figure 2.29 Screenshot of PLABKALI01: Showing the root prompt in the terminal window.

Keep the **terminal** window open.

Task 3 - Perform Linux Host Enumeration using Nmap

Just like Windows, you can also perform Linux host enumeration. Linux also offers several built-in commands that can be useful in the enumeration. Some of the key commands are:

- uname -a
- hostname
- route
- arp
- ifconfig
- mount
- whoami

An example of the **uname -a** command:

Figure 2.30 Screenshot of PLABKALI01: Showing the output of the uname-a command.

In a situation where you are inside the system and want to find information about the installed packages, you can run the **dpkg** command.

An example of **dpkg -l** command:

Figure 2.31 Screenshot of PLABKALI01: Showing the output of the dpkg -l command.

In this task, you will use nmap to enumerate a Linux host. 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**.

Clear the screen by entering the following command:

```
clear
```

You will first perform operating system detection. Type the following command:

```
nmap -O intranet
```

Press **Enter**.

Figure 2.32 Screenshot of PLABKALI01: Entering the nmap command to perform operating system detection.

Step 2

Notice that the output provides several pointers. It lists the open ports along with TCP/IP fingerprint.

Figure 2.33 Screenshot of PLABKALI01: Showing the output of the nmap command.

Step 3

Clear the screen by entering the following command:

```
clear
```

You can perform detailed enumeration, such as list the running services on a Linux host. Type the following command:

```
nmap -sV intranet
```

Press **Enter**.

Figure 2.34 Screenshot of PLABKALI01: Entering the nmap command for detailed operating system enumeration.

Step 4

Notice the output lists the open ports, running services, and their versions.

Figure 2.35 Screenshot of PLABKALI01: Showing the output of the nmap command.

Step 5

Clear the screen by entering the following command:

```
clear
```

You can also use several built-in commands to extract information that can be useful in ethical hacking. For example, you can find all SUID files. To do this, type the following command:

```
find / -perm -4000 -type f 2>/dev/null
```

Press **Enter**.

Figure 2.36 Screenshot of PLABKALI01: Entering the find command to find all SUID files.

Step 6

The output lists several files.

Figure 2.37 Screenshot of PLABKALI01: Showing the output of the find command.

Step 7

Clear the screen by entering the following command:

```
clear
```

You might also want to list services that are running as **root**. Type the following command:

```
ps aux | grep root
```

Press **Enter**.

Figure 2.38 Screenshot of PLABKALI01: Entering the ps and grep command to list services that are running as root.

Step 8

A set of services is listed as the output.

Figure 2.39 Screenshot of PLABKALI01: Showing the output of the ps and grep command with the services that are running as root.

Keep the **terminal** window open.

Task 4 - Perform Website Enumeration using Nmap

There are different methods to enumerate a Website. For example, you can use a manual method using a Web browser. You can try:

http://www.plab.com/admin

After the URL, you can add a directory name, such as admin. You are likely to get one of the following responses:

- **200** - OK
- **401** - Unauthorized
- **402** - Payment Required

- **403** - Forbidden
- **404** - Not Found

If the admin does not return **404** error but something else, such as **403**, it indicates clearly that this directory exists.

You can also enumerate a website using Nmap, which provides several scripts to enumerate different types of websites, such as WordPress or Drupal.

In this task, you will perform website enumeration using Nmap. 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**.

Clear the screen by entering the following command:

```
clear
```

To perform a website enumeration, type the following command:

```
nmap -script=http-enum intranet
```

Press **Enter**.

> ***Note:*** *This command may take a few minutes to provide an output.*

Figure 2.40 Screenshot of PLABKALI01: Entering the nmap command to perform a website enumeration.

Step 2

Notice the output. It has been able to list the open ports and a possible admin folder.

Figure 2.41 Screenshot of PLABKALI01: Showing the output of the nmap command.

Close the **terminal** window.

Task 5 - Perform Server Message Block (SMB) Enumeration

The SMB protocol is used by operating systems, such as Windows, to share files and printers. It is known to be a weak protocol, and there have been various versions that have been included in different versions of Windows.

- **SMB1** - Windows 2000, Windows XP, and Windows Server 2003
- **SMB2** - Windows Vista SP1 and Windows Server 2008
- **SMB2.1** - Windows 7 and Windows Server 2008 R2
- **SMB3** - Windows 8 and above, Windows Server 2012 and above

In this task, you will perform SMB enumeration. 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**.

Clear the screen by entering the following command:

```
clear
```

You can use **Nmap** to perform **SMB NetBIOS** enumeration. To do this, type the following command:

> ***Note:*** *SMB uses TCP ports 139 and 445. When using the nmap command, you should specify both ports.*

```
nmap -v -p 21,139,445 intranet
```

Press **Enter**.

Figure 2.42 Screenshot of PLABKALI01: Entering the nmap command to perform SMB NetBIOS enumeration.

Step 2

Notice the outcome of this command.

Figure 2.43 Screenshot of PLABKALI01: Showing the output of the nmap command for SMB NetBIOS enumeration.

Step 3

Clear the screen by entering the following command:

```
clear
```

To identify the **NetBIOS** information, you can use the **nbtscan** command. Type the following command:

```
nbtscan -r 192.168.0.0/24
```

Press **Enter**.

Figure 2.44 Screenshot of PLABKALI01: Running the nbtscan command.

Step 4

The output reveals the **NetBIOS** information.

Figure 2.45 Screenshot of PLABKALI01: Showing the output of the nbtscan command.

Step 5

Clear the screen by entering the following command:

```
clear
```

You can check the security level of the SMB server using **Nmap** script. To do this, type the following command:

```
nmap -v -p 139,445 -script=smb-security-mode intranet
```

Press **Enter**.

Figure 2.46 Screenshot of PLABKALI01: Entering the nmap command to check the security level of the SMB server using Nmap script.

Step 6

Notice the output as it details out the SMB security details.

Figure 2.47 Screenshot of PLABKALI01: Showing the output of the Nmap script.

Exercise 3 - Enumeration Prevention Techniques

Since there are different types of enumerations, such as SNMP, DNS, and so on, you need to use different prevention methods. For example, a web application enumeration can be prevented by using a Web Application Firewall (WAF).

In this exercise, you will learn about enumeration prevention techniques using Kali Linux tools.

Learning Outcomes

After completing this exercise, you will be able to:

- Prevent Web Applications Enumeration
- Prevent SNMP Enumeration
- Prevent LDAP Enumeration
- Prevent DNS Enumeration
- Prevent Windows Enumeration

Your Devices

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

- **PLABKALI01 -** (Kali 2019.2 - Linux Kali Workstation)

Task 1 - Prevent Web Applications Enumeration

A Web application enumeration can be prevented by using a Web Application Firewall (WAF). The wafw00f tool helps to determine whether the Web application is behind a WAF.

In the most typical scenario, a hacker performs the reconnaissance on the Web application, which is simply analyzing it. Then, after collecting enough information, the hacker will perform the attack using various tools, **wafw00f** is one such tool that can be used. It helps you to detect if the web application is being protected by a firewall.

In this task, you will learn to use wafw00f. 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**.

Clear the screen by entering the following command:

```
clear
```

You will attempt to find out whether a web application is behind the **Web Application Firewall (WAF**). You will use a tool named **wafw00f** for this purpose. Type the following command:

```
wafw00f http://intranet
```

Press **Enter**.

Figure 3.1 Screenshot of PLABKALI01: Entering the wafw00f command.

Step 2

Notice that the output has detected a **WAF**.

Figure 3.2 Screenshot of PLABKALI01: Showing the output of the wafw00f command with a WAF detected.

Close the **terminal** window.

Task 2 - Prevent SNMP Enumeration

In Exercise 1, Task 4 - Perform SNMP Enumeration Using IP Network Browser, you learned that with the small configuration of SNMP service, you were able to enumerate it using the IP Network Browser. This can be easily prevented.

To prevent SNMP enumeration, you need to stop the SNMP service. An alternate method is to restrict it to the localhost. You can open the **Services** console by typing **services.msc** in the **Run** prompt. In the **Services** console, locate the **SNMP** Service and double-click to open its properties dialog box.

Figure 3.3 Screenshot of PLABDC01: Configuring the SNMP service properties.

There might be a possibility that your organization is using an application that uses SNMP agents. You can remove the agent to prevent SNMP enumeration.

Some of the other methods to prevent SNMP enumeration are:

- Never use the default public community string
- Ensure that you use SNMPv3 to encrypt the community strings and messages
- Restrict anonymous connections using Group Policy
- Enable firewall and block access to TCP/UDP ports 161

Task 3 - Prevent LDAP Enumeration

Any authenticated user in Active Directory domain can send a query to the domain controller and retrieve a list of the all users, which means the user information. You can also retrieve the information about the security groups and the members they have. You can also retrieve a list of computers that are listed in the domain.

There are tools that can help you enumerate LDAP. Some of these tools are:

- Softerra LDAP Administrator
- LDAP Admin Tool
- LDAP Administrator tool
- Jxplorer

There are methods that can be used to prevent LDAP enumeration. Some of the key methods are:

- Always use SSL to encrypt LDAP communication.
- Use Kerberos to restrict access only to known users.
- Enable account lockout policy.

In this task, you will enable account lockout policy. To do this, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABDC01**.

Click the **Type here to search** icon in the taskbar.

Figure 3.4 Screenshot of PLABDC01: Showing the desktop of PLABDC01.

Step 2

In the search text box, type the following:

```
Group Policy Management
```

From the search results, select **Group Policy Management**.

Figure 3.5 Screenshot of PLABDC01: Selecting Group Policy Management from the search results.

Step 3

If already not expanded, expand **Domains**, then expand **PRACTICELABS.COM**, and then right-click **Default Domain Policy** to select **Edit**.

Figure 3.6 Screenshot of PLABDC01: Right-clicking the Default Domain Policy and selecting Edit.

Step 4

The **Group Policy Management Editor** window is displayed. In the left pane, under the **Computer Configuration** node, expand **Policies**, then expand **Windows Settings**. Further, you need to expand **Security Settings** and then select **Account Lockout Policy**.

Notice that the right pane displays three policies.

Figure 3.7 Screenshot of PLABDC01: Selecting the Account Lockout Policy node under Account Policies in the Group Policy Management Editor.

Step 5

In the right pane, double-click the **Account lockout duration** policy.

Figure 3.8 Screenshot of PLABDC01: Double-clicking the Account lockout duration policy.

Step 6

The **Account lockout duration Propeties** dialog box is displayed. Select **Define this policy** setting. Notic that **minutes** listbox is enabled by default and has a default value of **30**. Keep the default setting and click **OK**.

Figure 3.9 Screenshot of PLABDC01: Selecting the Define this policy checkbox and then clicking OK.

Step 7

The **Suggested Value Changes** dialog box is displayed. Review the suggested status of the remaining two policies and click **OK**.

Figure 3.10 Screenshot of PLABDC01: Reviewing the suggested changes for two policies and clicking OK on the Suggested Value Changes dialog box.

Step 8

Notice that the remaining two policies, **Account lockout threshold** and **Reset account lockout counter after** policies are enabled with the default values. You can either choose to keep the default values or change them as required.

For this task, you can keep the default values.

Figure 3.11 Screenshot of PLABDC01: Showing the status of the policies in Account Lockout Policy.

Step 9

Close the **Group Policy Management Editor** window.

Figure 3.12 Screenshot of PLABDC01: Closing the Group Policy Management Editor window.

Step 10

Close the **Group Policy Management** window.

Figure 3.13 Screenshot of PLABDC01: Closing the Group Policy Management window.

Step 11

You should now be on the desktop.

Figure 3.14 Screenshot of PLABDC01: Showing the desktop of PLABDC01.

Task 4 - Prevent DNS Enumeration

DNS enumeration can reveal sensitive DNS information. In this process, the DNS servers of an organization are tracked and certain requests are made to them to reveal their records and zone information.

There are various tools that can be used for DNS enumeration. Some of these tools are:

- Nslookup
- DNS Dumpster
- DNS Recon

An organization must use certain methods to protect their DNS servers from revealing critical information. Some of the method that can be used to prevent DNS enumeration:

- DNS zone transfers should be performed with the authenticated and known DNS servers.
- DNS zone transfers must not include HINFO information.

Along with the two suggested methods, you should ensure that DNS zone files include only the necessary information. These files should not be able to reveal extra information.

In this task, you will configure DNS zone transfer with the known servers. To do this, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABDC01**.

Click the **Type here to search** icon in the taskbar.

Figure 3.15 Screenshot of PLABDC01: Showing the desktop of PLABDC01.

Step 2

In the search text box, type the following:

```
DNS
```

From the search results, select **DNS**.

Figure 3.16 Screenshot of PLABDC01: Selecting DNS from the search results.

Step 3

The **DNS Manager** window is displayed. In the left pane, expand **PLABDC01** if not expanded already. Then, expand **Forward Lookup Zones** and then select **PRACTICELABS.COM**.

Figure 3.17 Screenshot of PLABDC01: Expanding PLABDC01, then expanding Forward Lookup Zones and then selecting PRACTICELABS.COM..

Step 4

In the left pane, right-click **PRACTICELABS.COM** and select **Properties**.

Figure 3.18 Screenshot of PLABDC01: Right-clicking the PRACTICELABS.COM zone and then selecting Properties from the context menu.

Step 5

The **PRACTICELABS.COM Properties** dialog box is displayed. Click the **Zone Transfers** tab.

Figure 3.19 Screenshot of PLABDC01: Clicking the Zone Transfers tab on the PRACTICELABS.COM Properties dialog box.

Step 6

The **Zone Transfers** tab is displayed. Select **Allow zone transfers** and then select **Only to the following servers**.

Click **Edit**.

Figure 3.20 Screenshot of PLABDC01: Selecting the Allow zone transfers checkbox and then selecting the Only to the following servers option.

Step 7

The **Allow Zone Transfers** dialog box is displayed.

> ***Note:*** *In the lab environment, there is only one DNS Server available. Therefore, if you add the IP address here, you will be prompted with an error. However, in the real environment, you can add the IP address or name of the DNS server and it should get resolved.*

Figure 3.21 Screenshot of PLABDC01: Displaying the Allow Zone Transfers dialog box.

Step 8

On the **Allow Zone Transfers** dialog box, click **Cancel**.

Figure 3.22 Screenshot of PLABDC01: Clicking Cancel on the Allow Zone Transfers dialog box.

Step 9

Click **Cancel** on the **PRACTICELABS.COM Properties** dialog box.

Figure 3.23 Screenshot of PLABDC01: Clicking Cancel on the PRACTICELABS.COM Properties dialog box.

Step 10

Close the **DNS Manager** window.

Figure 3.24 Screenshot of PLABDC01: Closing the DNS Manager window.

Task 5 - Prevent Windows Enumeration

Windows Enumeration helps you locate information about a system that is running Windows. You can find information, such as open ports and running services. This type of information can be used to exploit a Windows system.

For example, running a simple Nmap command will scan all ports on a system with the IP address, 192.168.0.1.

nmap -p 1-65535 192.168.0.1

You can also perform operating system detection using the following command:

nmap -A -T4 192.168.0.1

Various tools can be used in Windows enumeration:

- PsExec
- PsInfo
- PsList
- PsFile
- PsLoggedOn
- PsLogList

- PsGetSid
- PsKill

Windows enumeration can be prevented with the following methods:

- Stop unnecessary services from running.
- Configure a firewall on the Windows host.

In this task, you will take a look at the unnecessary services running on Windows 10. 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.**

In the **Type here to search** text box, type the following:

```
services.msc
```

From the search results, select **Services**.

Figure 3.25 Screenshot of PLABWIN10: Selecting Services from the search results.

Step 2

The **Services** window is displayed. In the right pane, click the **Status** header twice to list the services with the **Running** status.

Figure 3.26 Screenshot of PLABWIN10: Clicking the Status header to list the services with their status.

Step 3

Notice that the services with the **Running** status are listed on the top of the window.

Figure 3.27 Screenshot of PLABWIN10: Displayng the services with the Running status.

Step 4

You will now need to find services that you can shut down as they will not be required on **PLABWIN10**.

Scroll down to locate the **Print Spooler** service. Notice that the service is running currently. Double-click the **Print Spooler** service.

Figure 3.28 Screenshot of PLABWIN10: Locating and then double-clicking the Print Spooler service.

Step 5

The **Print Spooler Properties (Local Computer)** dialog box is displayed. Click **Stop**.

Figure 3.29 Screenshot of PLABWIN10: Clicking Stop to stop the Print Spooler service from running.

Step 6

Notice that the service status has changed to **Stopped**.

Figure 3.30 Screenshot of PLABWIN10: Displaying the Stopped status for the Print Spooler service.

Step 7

You also want to ensure that the service does not start automatically when you reboot the system. You should change the startup type to **Disabled**. From the **Startup type** drop-down, select **Disabled**.

Figure 3.31 Screenshot of PLABWIN10: Selecting the Disabled status from the Startup type drop-down for the Print Spooler service.

Step 8

Notice that the **Startup type** is now set to **Disabled**. Click **OK**.

> ***Note:*** *Just like* ***Print Spooler*** *service, you can find more services that you do not require to run in Windows. You can then stop these services and disable them so that they do not start automatically when you reboot the system.*

Figure 3.32 Screenshot of PLABWIN10: Setting the Disabled status for the Print Spooler service and clicking OK.

Step 9

Back on the **Services** window, click **Startup Type** header and then locate **Print Spooler**. Notice that it is now set to **Disabled**.

Figure 3.33 Screenshot of PLABWIN10: Displaying the Disabled status for the Print Spooler service.

Step 10

Close the **Services** window.

Figure 3.34 Screenshot of PLABWIN10: Closing the Services window.

Review

Well done, you have completed the **Enumeration** Practice Lab.

Summary

You completed the following exercises:

- Exercise 1 - Enumeration Techniques using Windows-based Tools
- Exercise 2 - Enumeration Techniques using Kali Linux Tools
- Exercise 3 - Enumeration Prevention Techniques

You should now be able to:

- Use SuperScan for NetBIOS Enumeration
- Use Hyena for Enumeration
- Perform LDAP Enumeration using Softerra LDAP Administrator
- Perform SNMP Enumeration using IP Network Browser
- Perform DNS Enumeration
- Perform Windows Host Enumeration using Rpcclient
- Perform Linux Host Enumeration using Nmap
- Perform Website Enumeration using Nmap
- Perform Server Message Block (SMB) Enumeration
- Prevent Web Applications Enumeration
- Prevent SNMP Enumeration
- Prevent LDAP Enumeration
- Prevent DNS Enumeration
- Prevent Windows Enumeration

Feedback

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