CEH v12 Lesson 3 : NetBIOS, SNMP & LDAP Network Enumeration

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 — Enumeration Concepts
- Exercise 2 — NetBIOS Enumeration
- Exercise 3 — SNMP Enumeration
- Exercise 4 — LDAP Enumeration

After completing this module, you will be able to:

- Use SuperScan for NetBIOS Enumeration
- Perform NetBIOS Enumeration Using Nbtstat
- Perform NetBIOS Enumeration using Nmap
- Perform SNMP Enumeration Using IP Network Browser
- Perform SNMP Enumeration Using Snmp-check
- Perform LDAP Enumeration Using Softerra LDAP Administrator

After completing this module, you will have further knowledge of:

- Defining Enumeration
- Enumeration Methods
- TCP and UDP Port Enumeration
- Methods to Prevent SNMP Enumeration
- Methods to Prevent LDAP Enumeration

Lab Duration

It will take approximately **1 hour** to complete this lab.

Exercise 1 — Enumeration Concepts

Enumeration is a method of gathering information by connecting directly with the systems. The attacker connects with the system and identifies the vulnerabilities that can be exploited to access the system.

In the enumeration phase, an attacker attempts to gain information about various network components. The core intent of enumeration is to look for possible attack vectors which can exploit one or more systems. The attacker can enumerate the following:

- Network shares
- Routing tables
- Simple Network Management Protocol (SNMP)
- Fully Qualified Domain Name (FQDN)
- System names
- User and group names
- Applications
- Services

In this exercise, you will learn about the enumeration concepts.

Learning Outcomes

After completing this exercise, you will have further knowledge of:

- Define Enumeration
- Enumeration Methods
- TCP and UDP Port Enumeration

Your Devices

This exercise contains supporting materials for **Ethical Hacker v11**.

Enumeration Methods

An attacker can use various enumeration methods to collect information about a target, individual system, user, or organization. There is no hard and fast rule about selecting a specific method; instead, it is mainly driven by a situation or the attacker's objective that they may choose a specific enumeration method.

Let's look at some key methods:

- **Enumerate usernames from email IDs**: understand the naming convention. For example, john.smith@example.com.
- **Enumerate default credentials**: Almost all network appliances and applications have default credentials. Users often do not change default credentials, making things easier for an attacker. After an attacker has determined the type of application or device, it is easy to find the default credentials on the Internet.
- **Enumerate Active Directory**: An attacker can enumerate the Active Directory using tools such as KerBrute. Enumerating the usernames can help in password spraying attacks as the attacker has valid usernames.
- **Enumerate DNS servers**: An attacker can enumerate the zone information if the DNS servers are not properly configured for zone transfer. For example, suppose a DNS server is configured to transfer zone information to any DNS server. In that case, an attacker can leverage this and replicate all zone information to a rogue DNS server.
- **Enumerate user's groups:** If the target network is a Windows domain, it is easy to determine groups to which the user belongs. This can be done using different methods, such as the command line.
- **Enumerate using SNMP:** An attacker can enumerate the devices managed using SNMP. They can enumerate information, such as usernames, passwords, and groups.

TCP and UDP Port Enumeration

In a network, several services use either TCP or UDP ports. These ports can be enumerated to extract different types of information.

Here are some of the key TCP and UDP ports that becomes the target for enumeration:

- **TCP 20/21:** File Transfer Protocol (FTP)

- **TCP 22:** Secure Shell (SSH)
- **TCP 23:** Telnet
- **TCP 25:** SMTP
- **TCP/UDP 53:** DNS Zone Transfer
- **UDP 69:** Trivial File Transfer Protocol (TFTP)
- **UDP 123:** Network Time Protocol
- **TCP/UDP 135:** Microsoft RPC Endpoint Mapper
- **UDP 137:** NetBIOS Name Service
- **TCP 139:** NetBIOS Session Service
- **UDP 161:** SNMP
- **TCP/UDP 162:** SNMP Trap
- **TCP/UDP 389:** LDAP
- **TCP/UDP 445:** SMB Over TCP
- **UDP 500:** Internet Key Exchange (IKE)
- **TCP 2049:** Network File System (NFS)

Exercise 2 — NetBIOS Enumeration

NetBIOS enumeration can reveal a great deal of information to an attacker. With the NetBIOS enumeration, the attacker can gain sensitive information about the domain systems by listing them, network shares, and network passwords. NetBIOS enumeration can be performed on a file and printer sharing feature enabled.

In this exercise, you will learn to perform NetBIOS enumeration.

Learning Outcomes

After completing this exercise, you will be able to:

- Use SuperScan for NetBIOS Enumeration
- Perform NetBIOS Enumeration Using Nbtstat

- Perform NetBIOS Enumeration using Nmap

Your Devices

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

PLABDC01Domain Controller192.168.0.1/24PLABWIN10Domain MemberWorkstation192.168.0.3/24PLABKALI01Domain MemberWorkstation192.168.0.5/24PLABDM01Domain Member Server192.168.0.2/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABDM01

Windows Server 2019 — Domain Member192.168.0.2/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

Task 1 — Use SuperScan for NetBIOS Enumeration

SuperScan is a tool that you can use to scan ports, ping a system, or resolve machine names. SuperScan has the following capabilities:

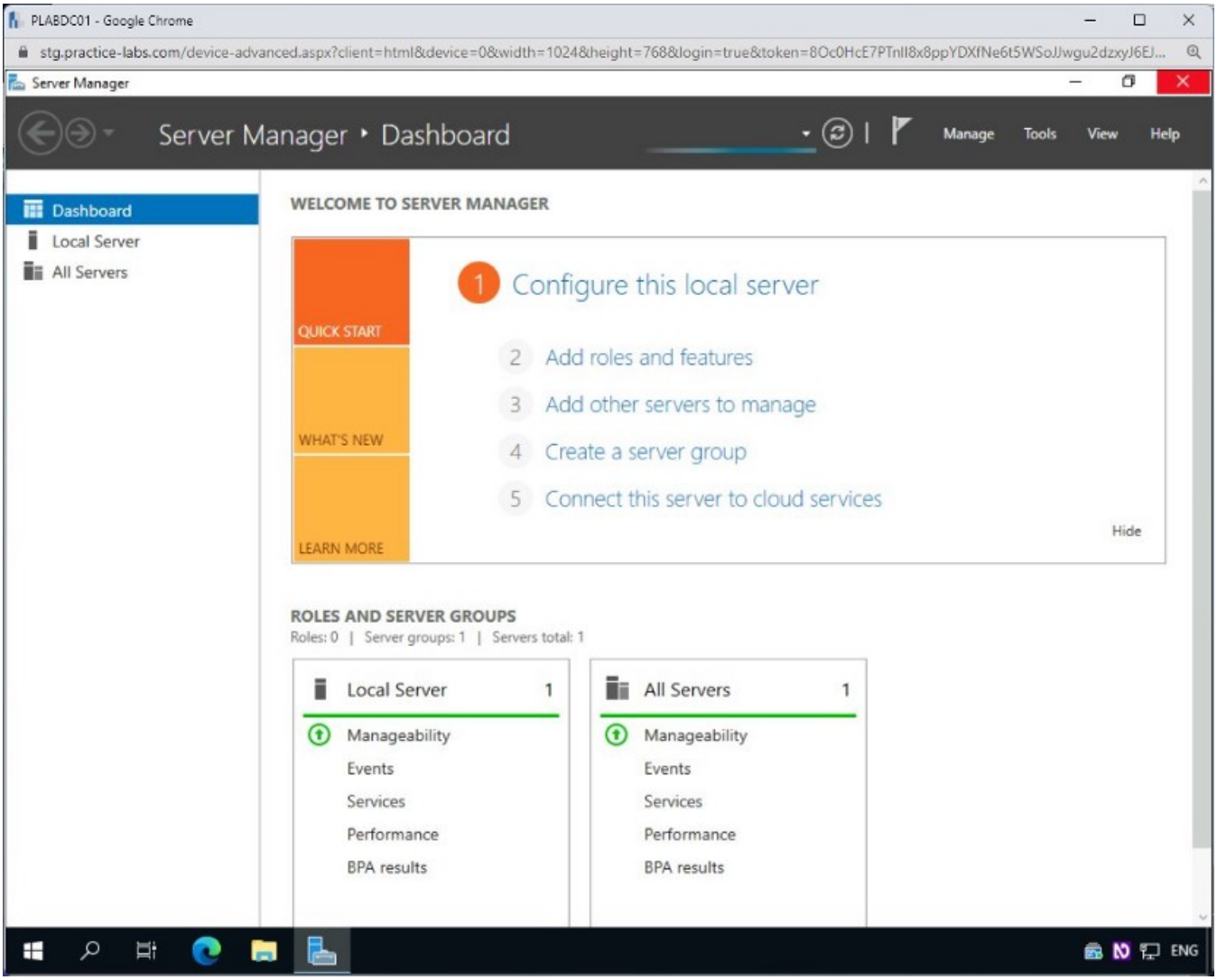
- NetBIOS information
- User and Group Accounts
- Network shares
- Services status

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

Step 1

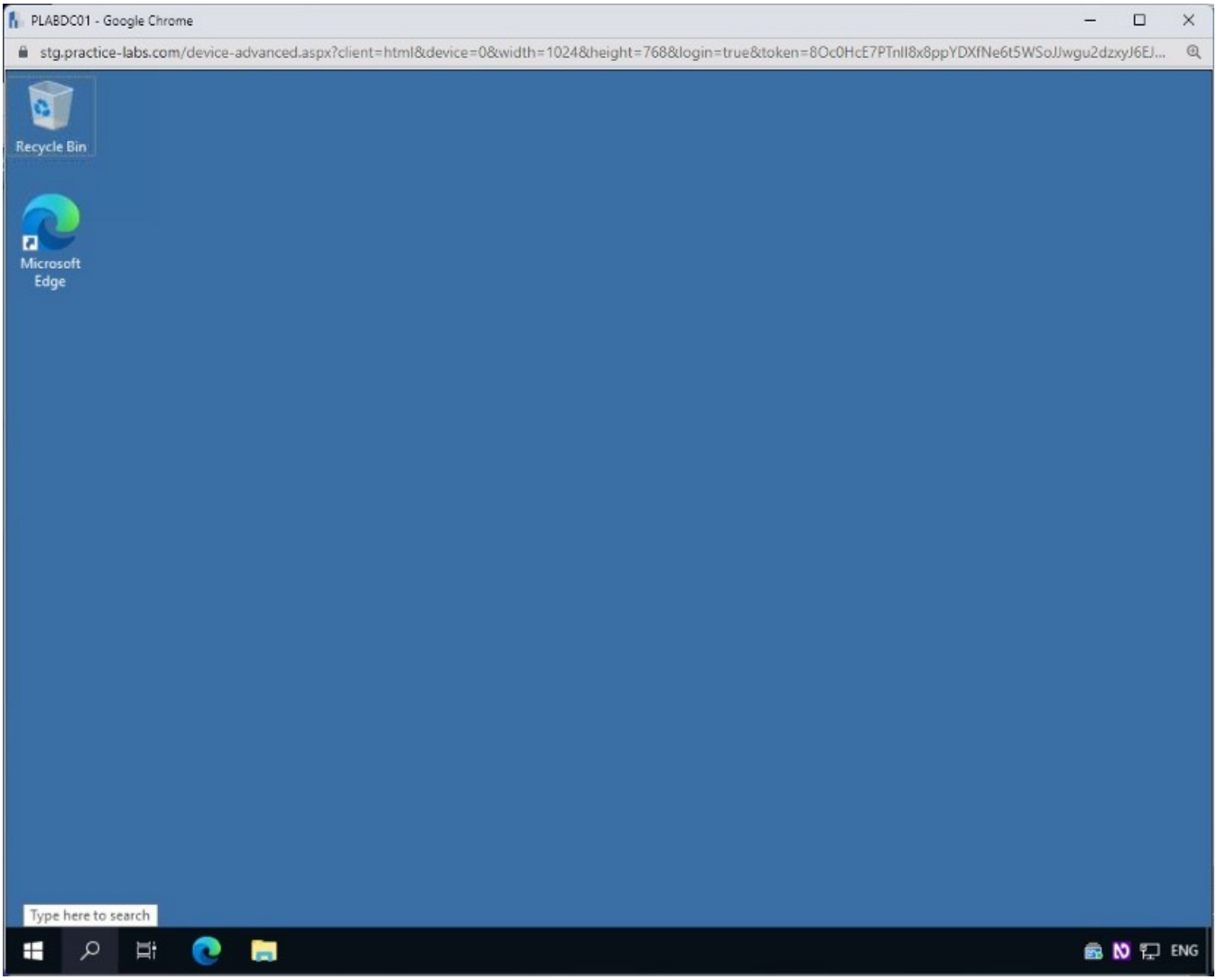
Ensure you have powered on all devices listed in the introduction and connect to **PLABDC01.**

Close the **Server Manager** window.



Step 2

Before proceeding, you will need to disable the firewall. Click the **Type here to search** textbox.

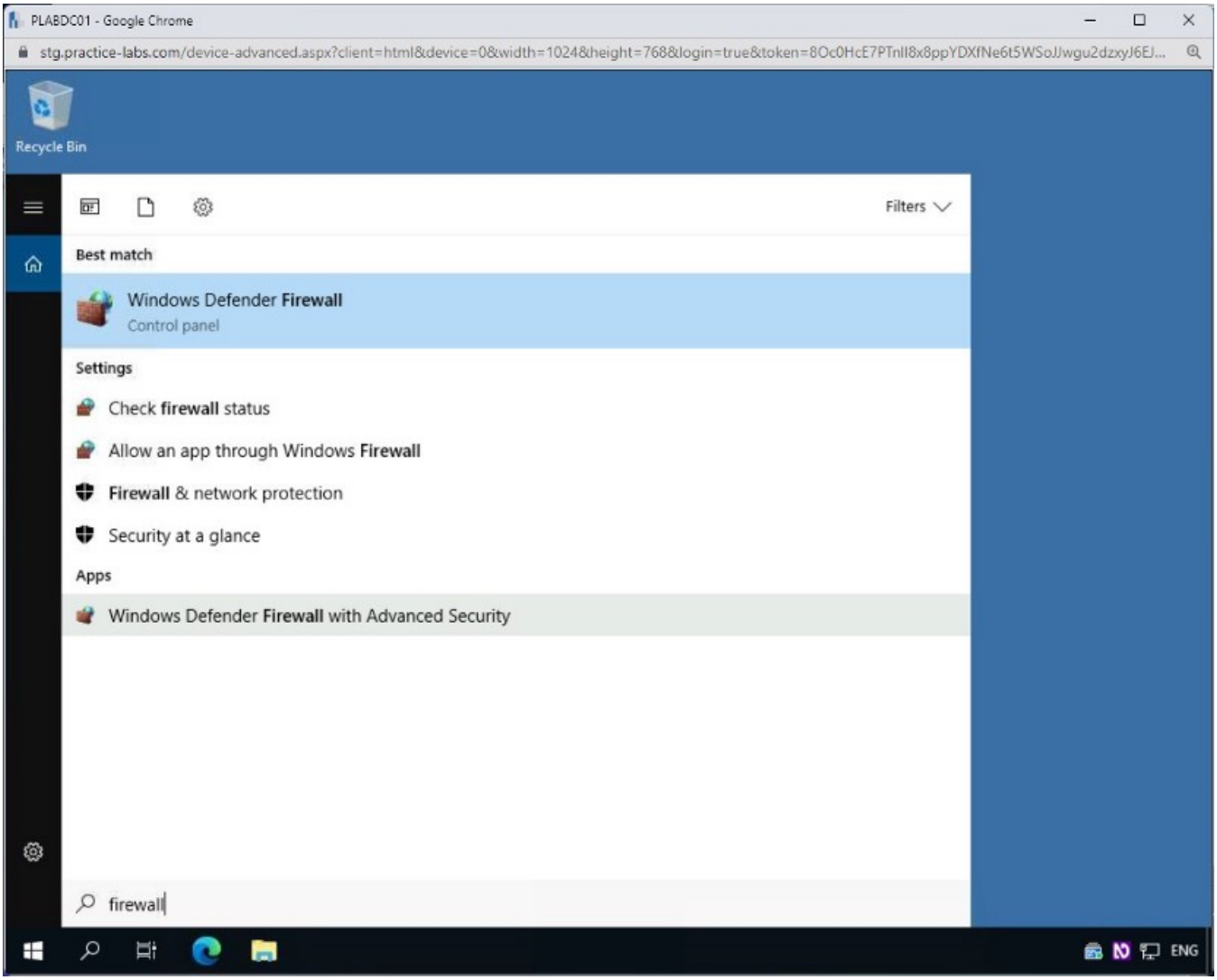


Step 3

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

```
firewall
```

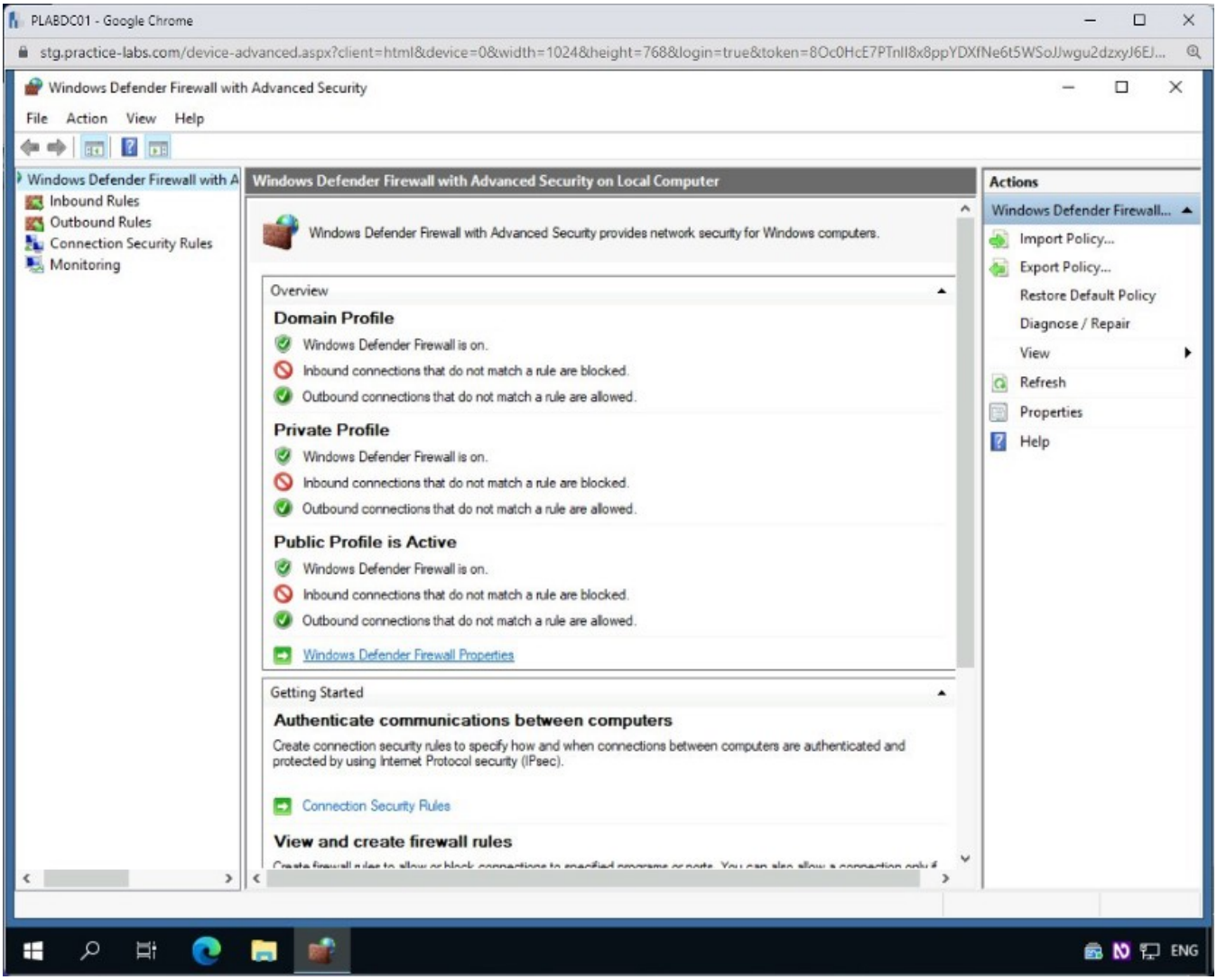
From the bottom of the search results, click **Windows Firewall with Advanced Security**, under **Apps**.



Step 4

Click the **Windows Defender Firewall Properties** link in the middle pane.

The **Windows Defender Firewall with Advanced Security** window will then open. You will notice that only the **Domain Profile** is **Active**.

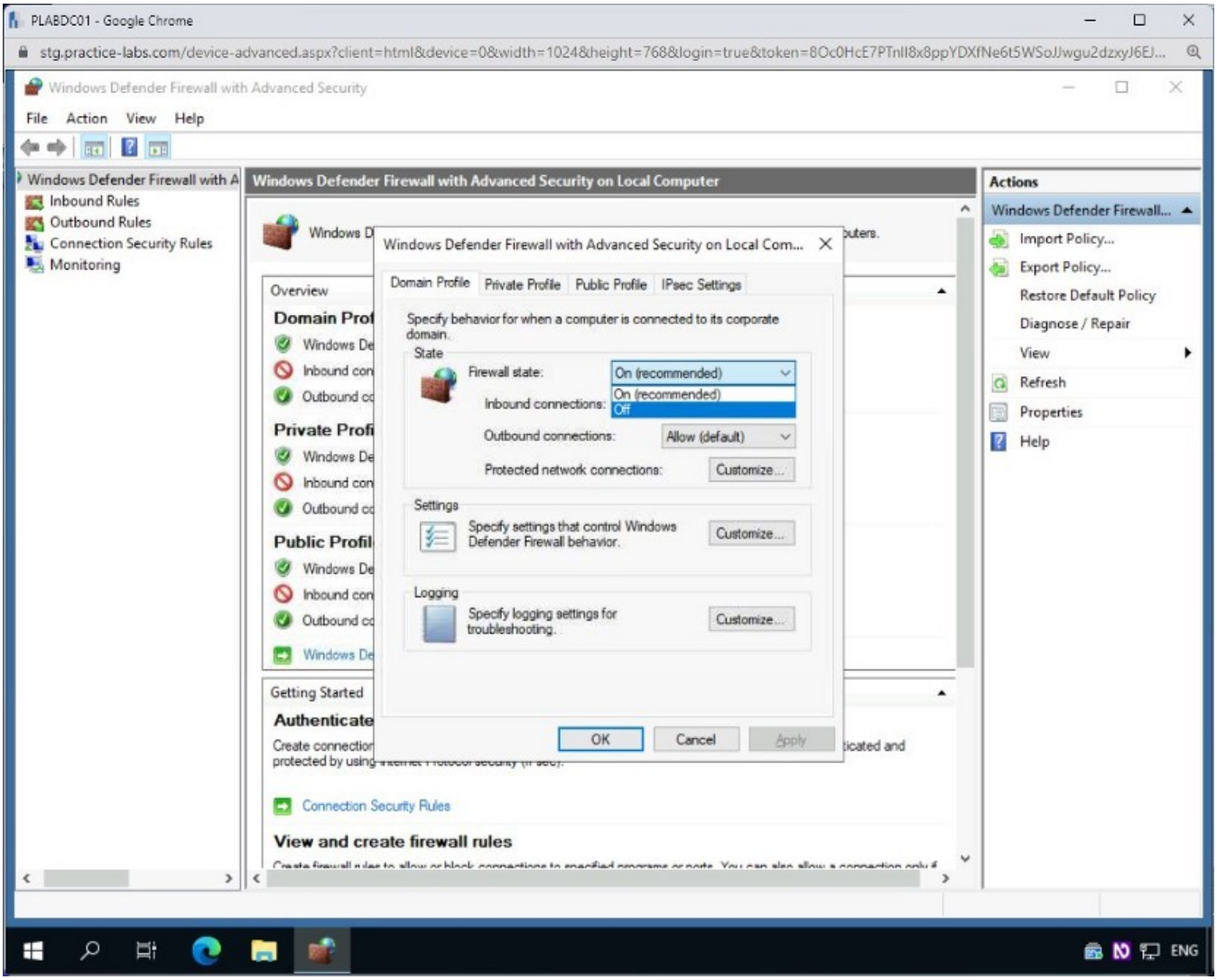


Step 5

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

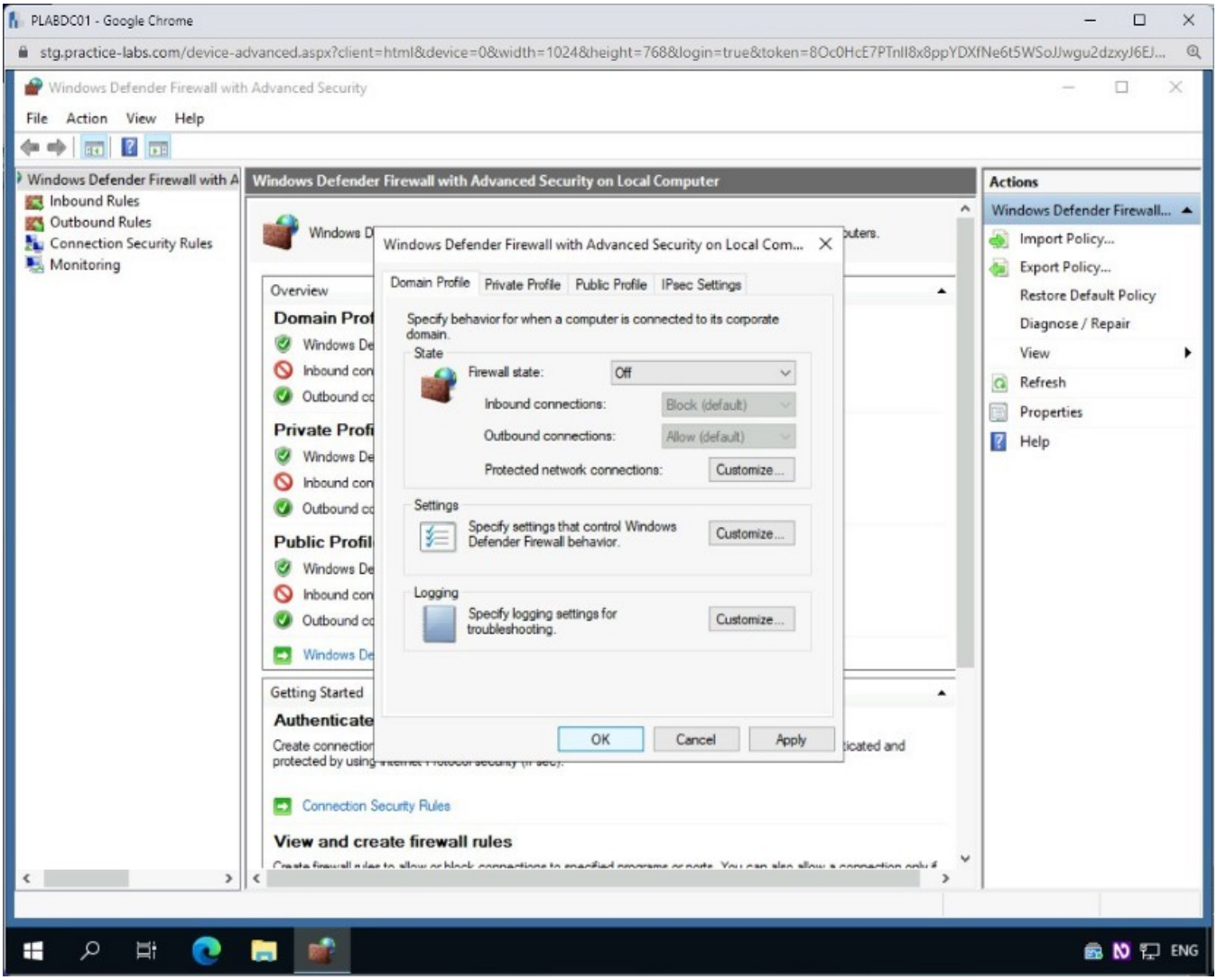
Click the **Firewall state** drop-down and select **Off**. You need to change the **Firewall** state to **Off**.

Alert: Repeat the same steps to turn off the firewall for **Private** and **Public** profiles.



Step 6

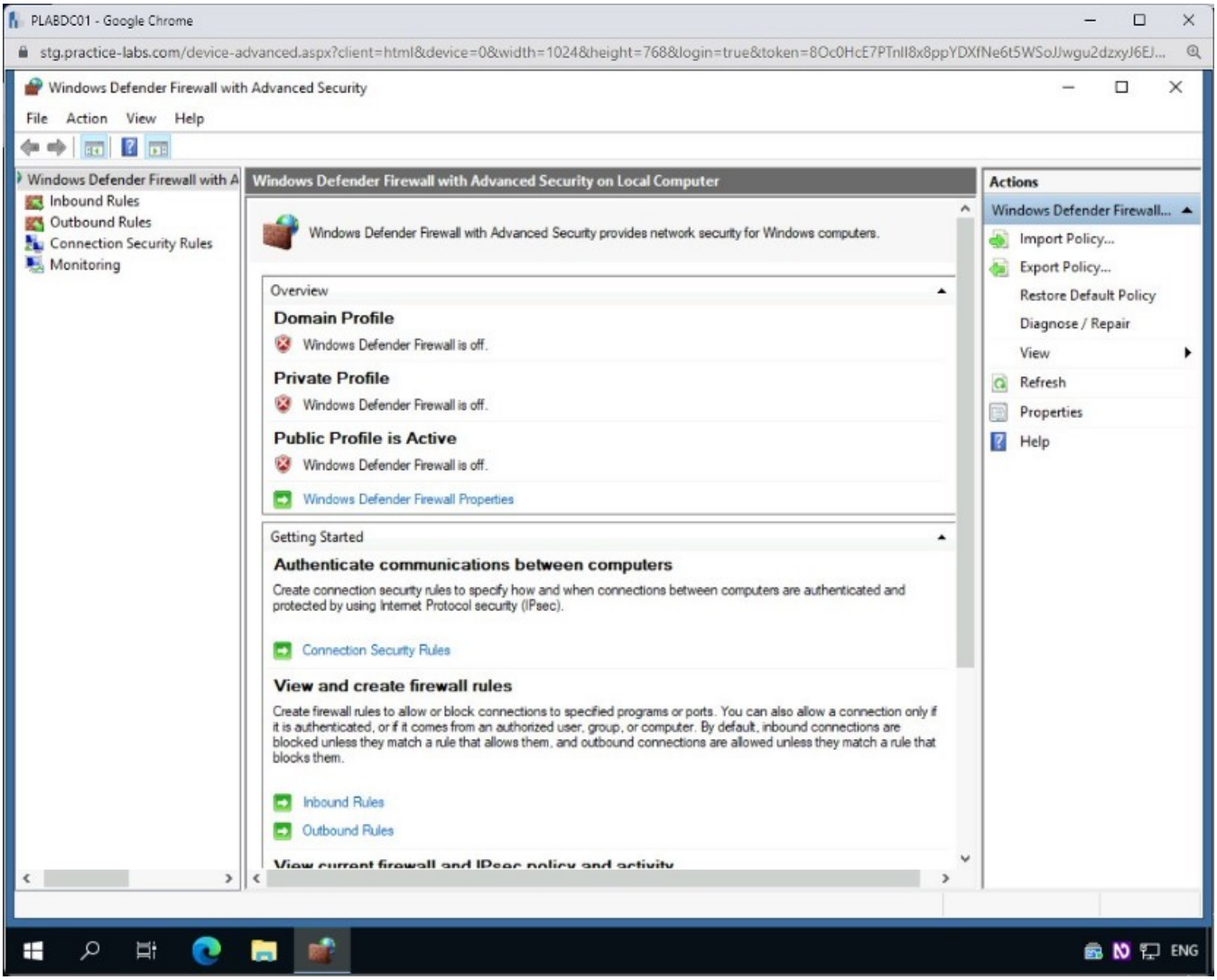
After the **Firewall** state is set to **Off**, click **OK**.



Step 7

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

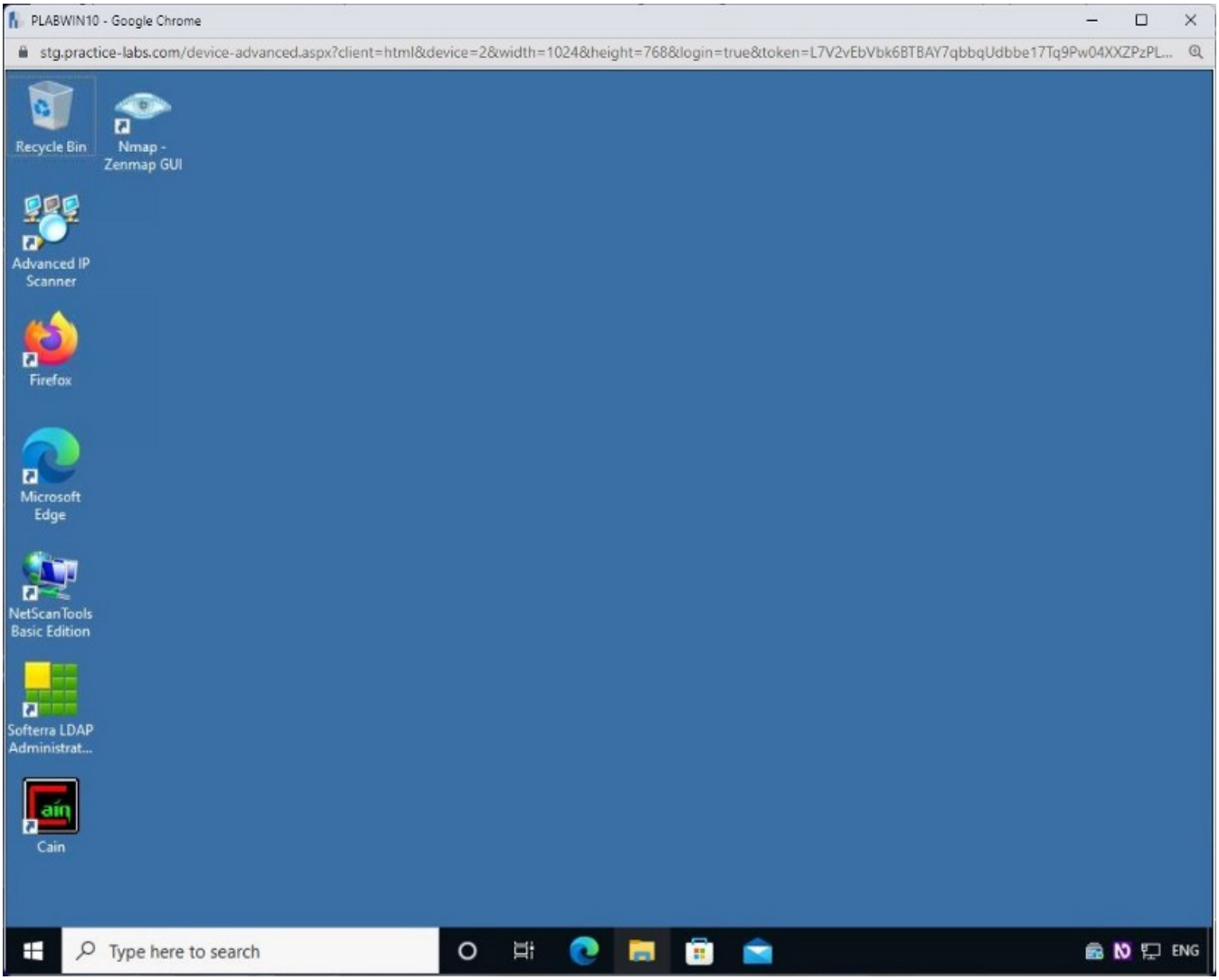
Alert: Repeat the above steps for all three profiles on both **PLABDM01** and **PLABDC01**.***Note****: You would not do this in a production environment as it exposes the device to several threats.*



Step 8

Switch to **PLABWIN10.**

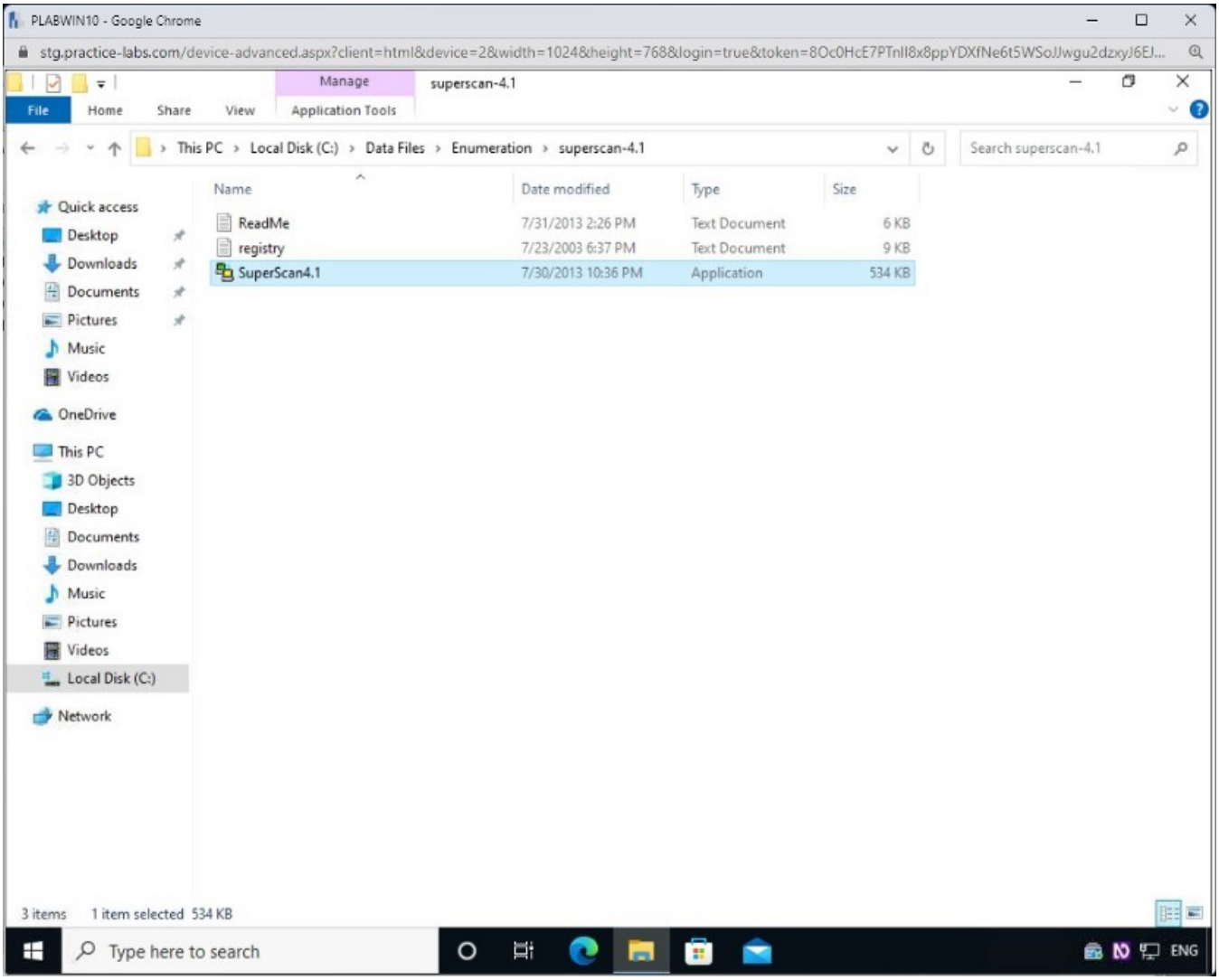
Click the **File Explorer** icon in the taskbar.



Step 9

The File Explorer window opens. Navigate to the **Local Disk** ©: > **Data Files** > **Enumeration** > **Superscan-4.1** folder.

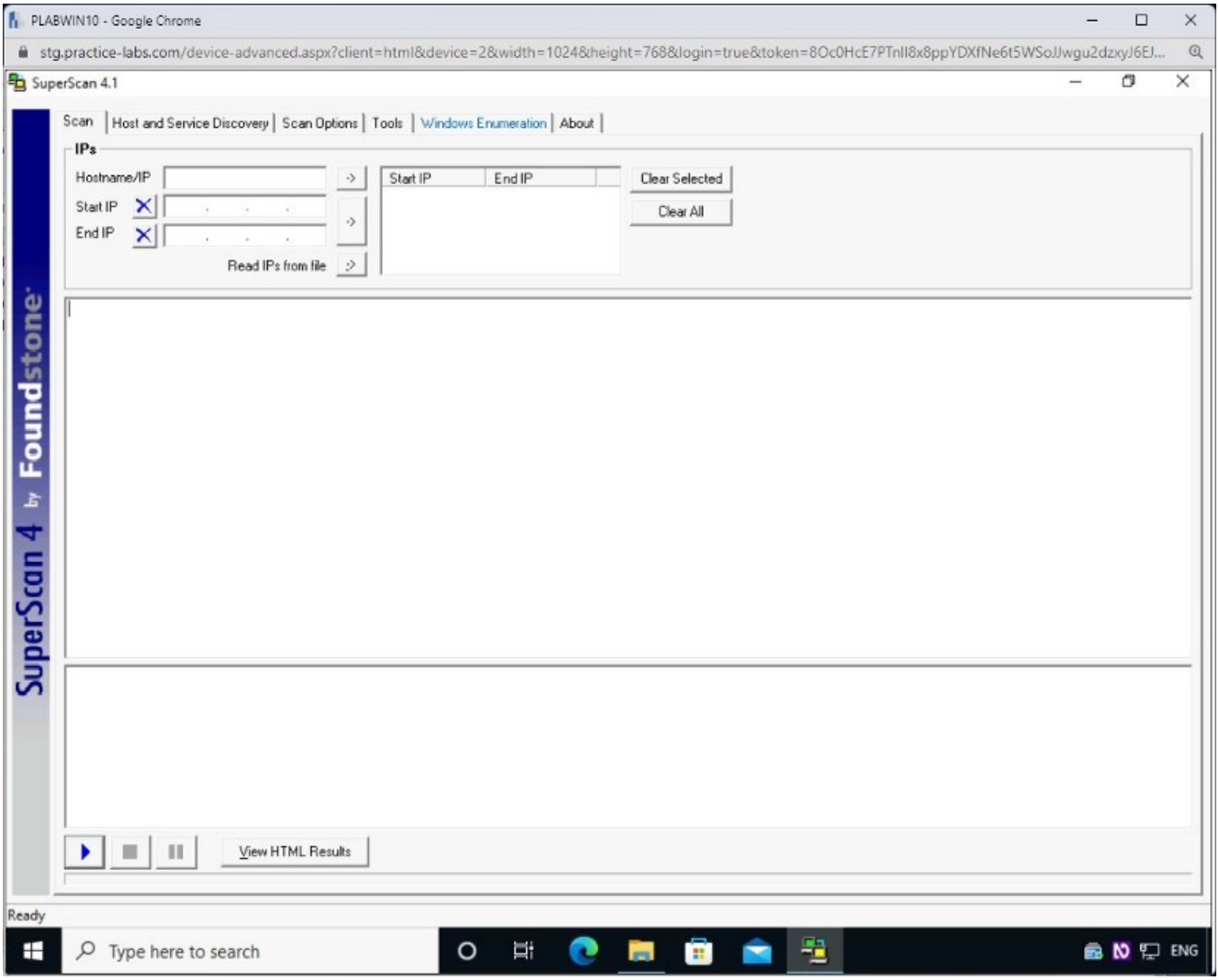
Double-click the **SuperScan4.1** application.



Step 10

The **SuperScan 4.1** window is displayed.

Click the **Windows Enumeration** tab.



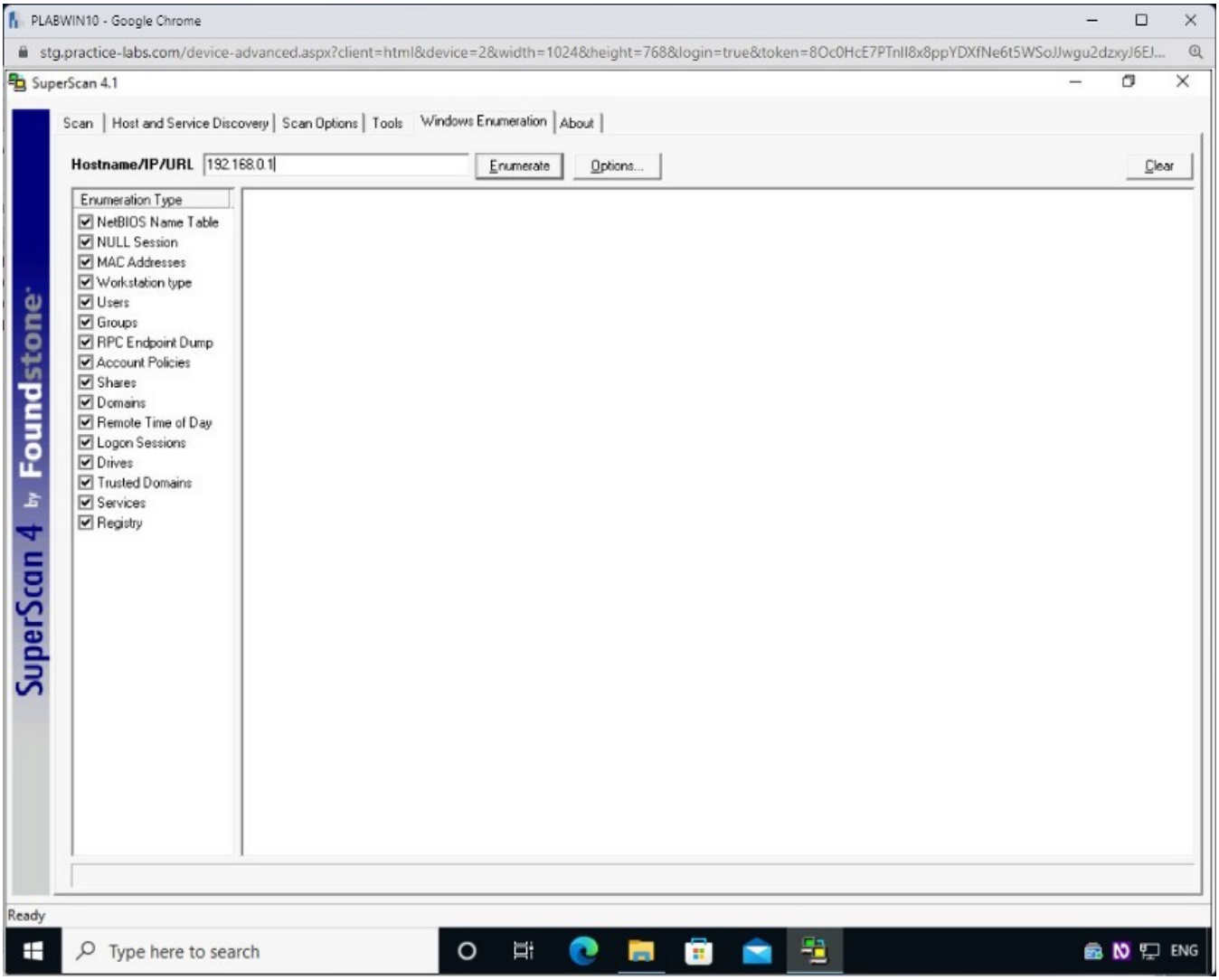
Step 11

There are two panes in the **Windows Enumeration** tab. The left pane contains the Enumeration types, and the right pane will display the enumeration result.

In the **Hostname/IP/URL** text box, type the following IP address:

```
192.168.0.1
```

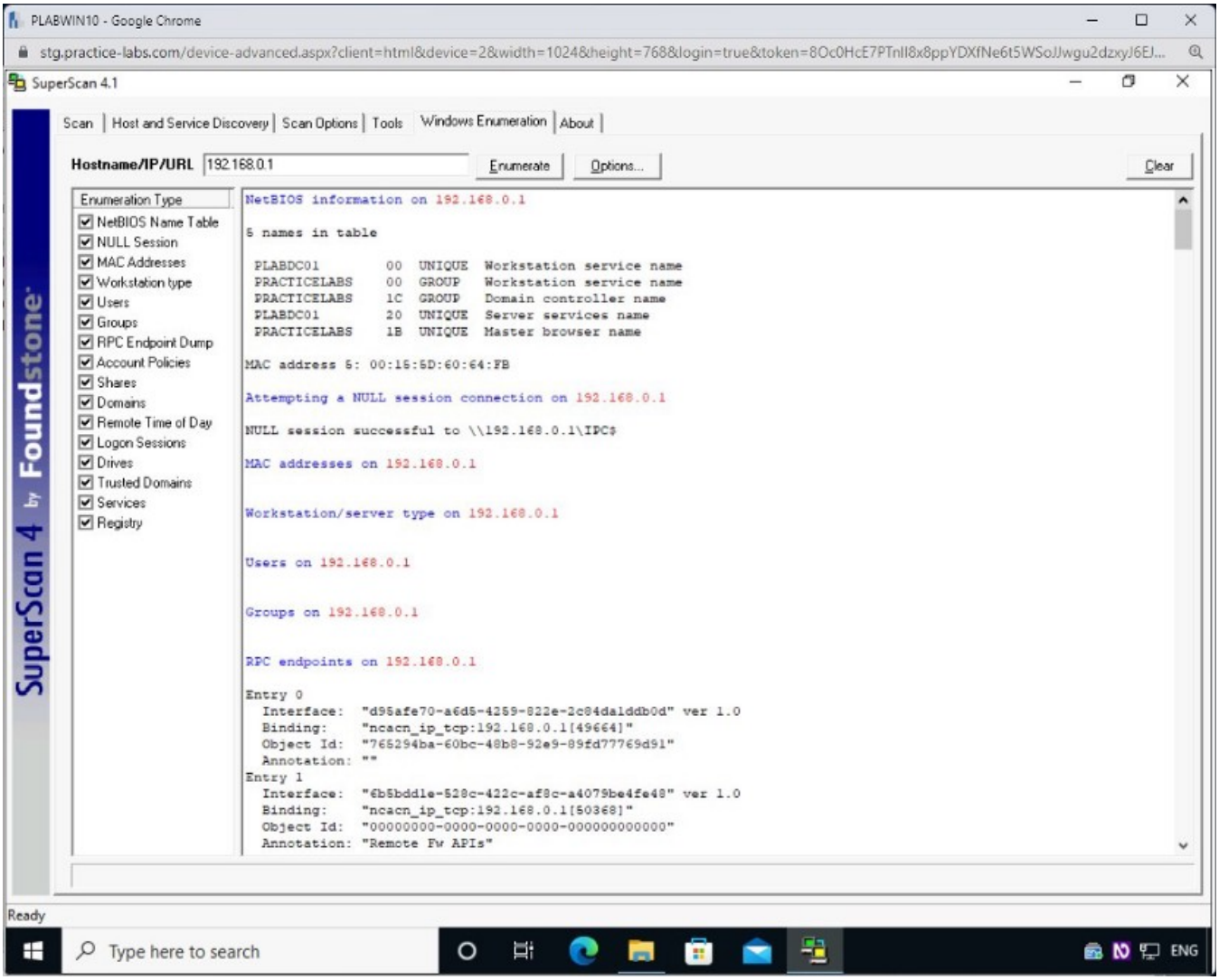
Click **Enumerate**.



Step 12

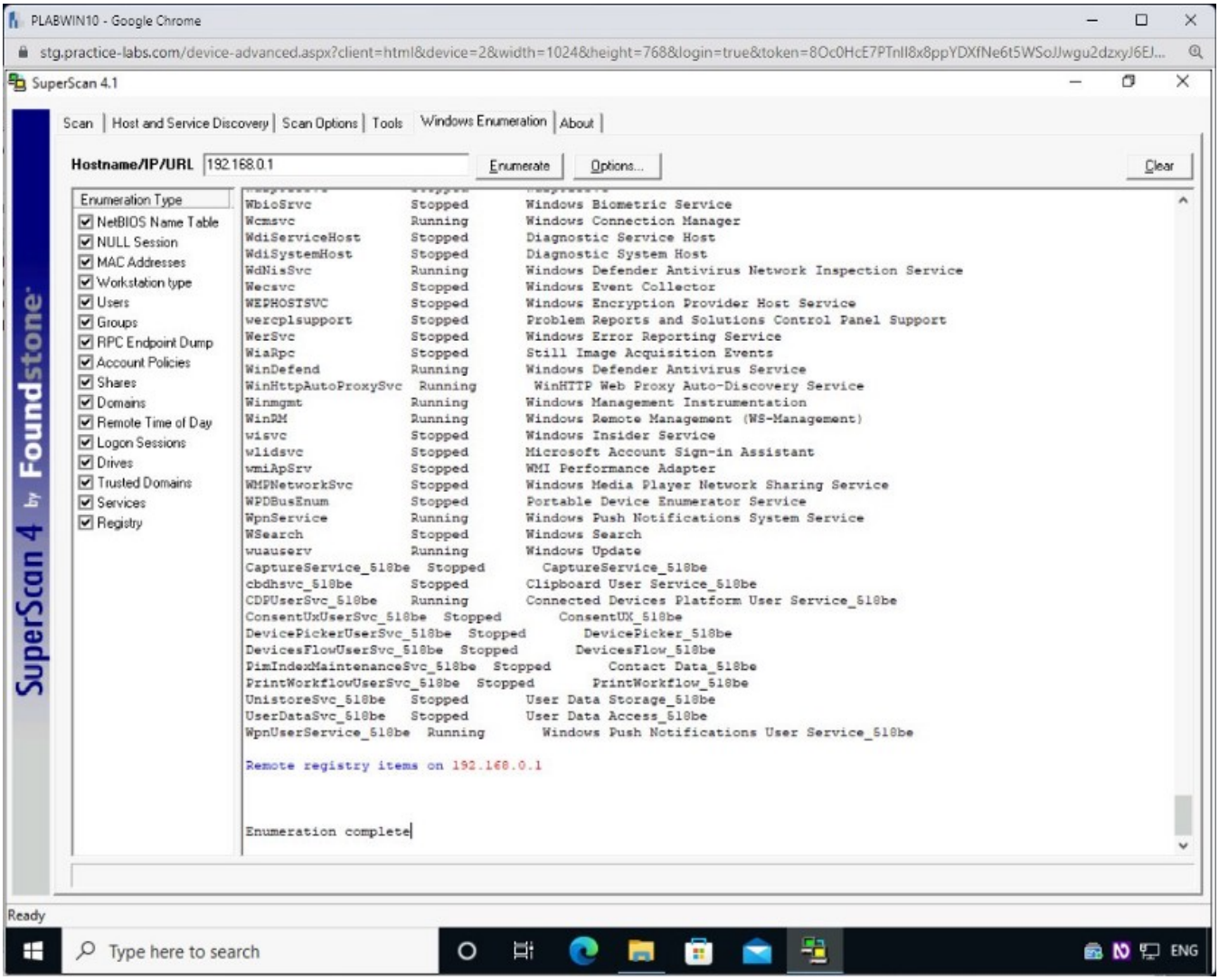
The results are displayed in the right pane.

Scroll up to view the results from the beginning.



Step 13

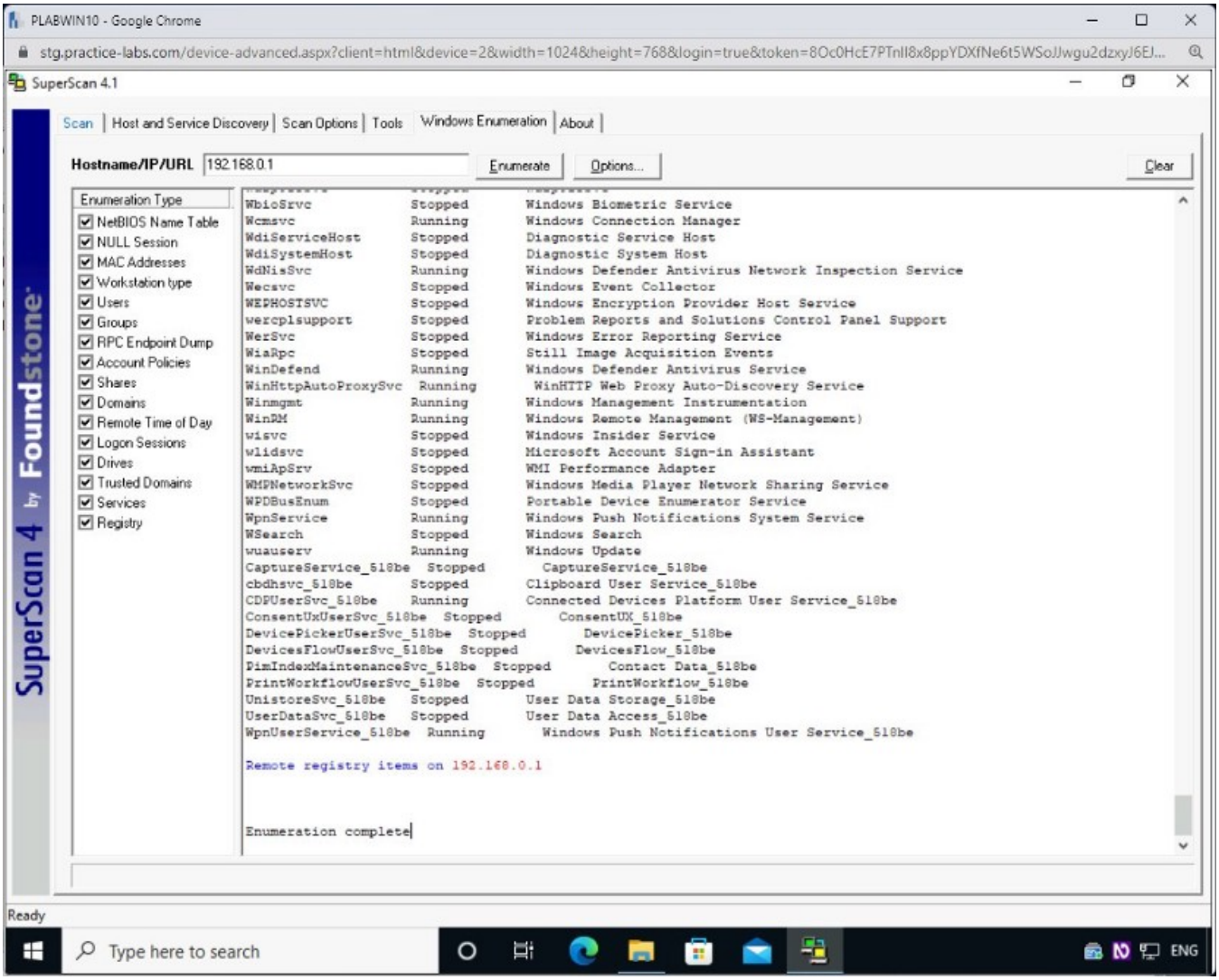
You can view the complete results by scrolling down.



Step 14

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

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



Step 15

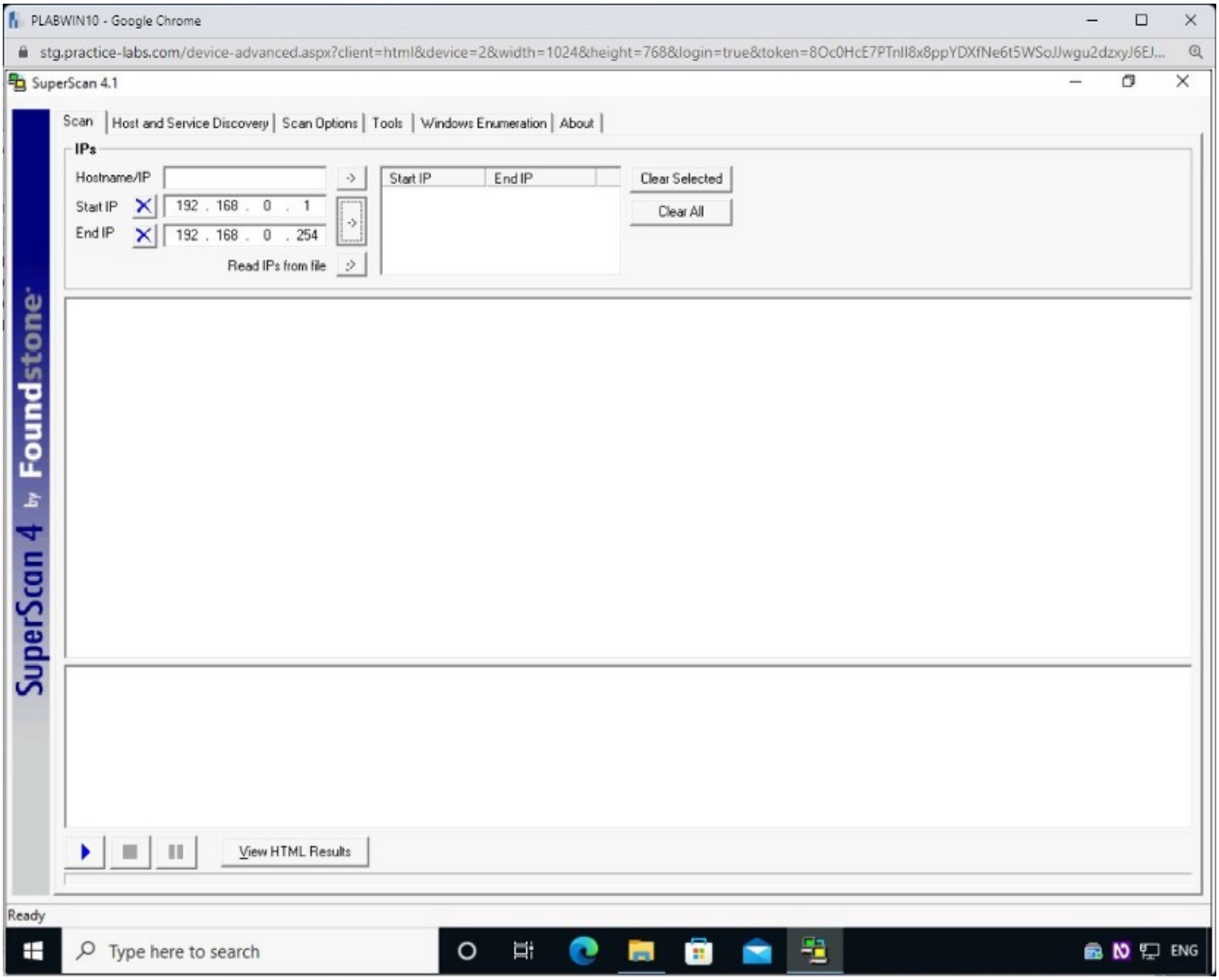
On the **Scan** tab, in the **Start IP** text box, type the following IP address:

```
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:

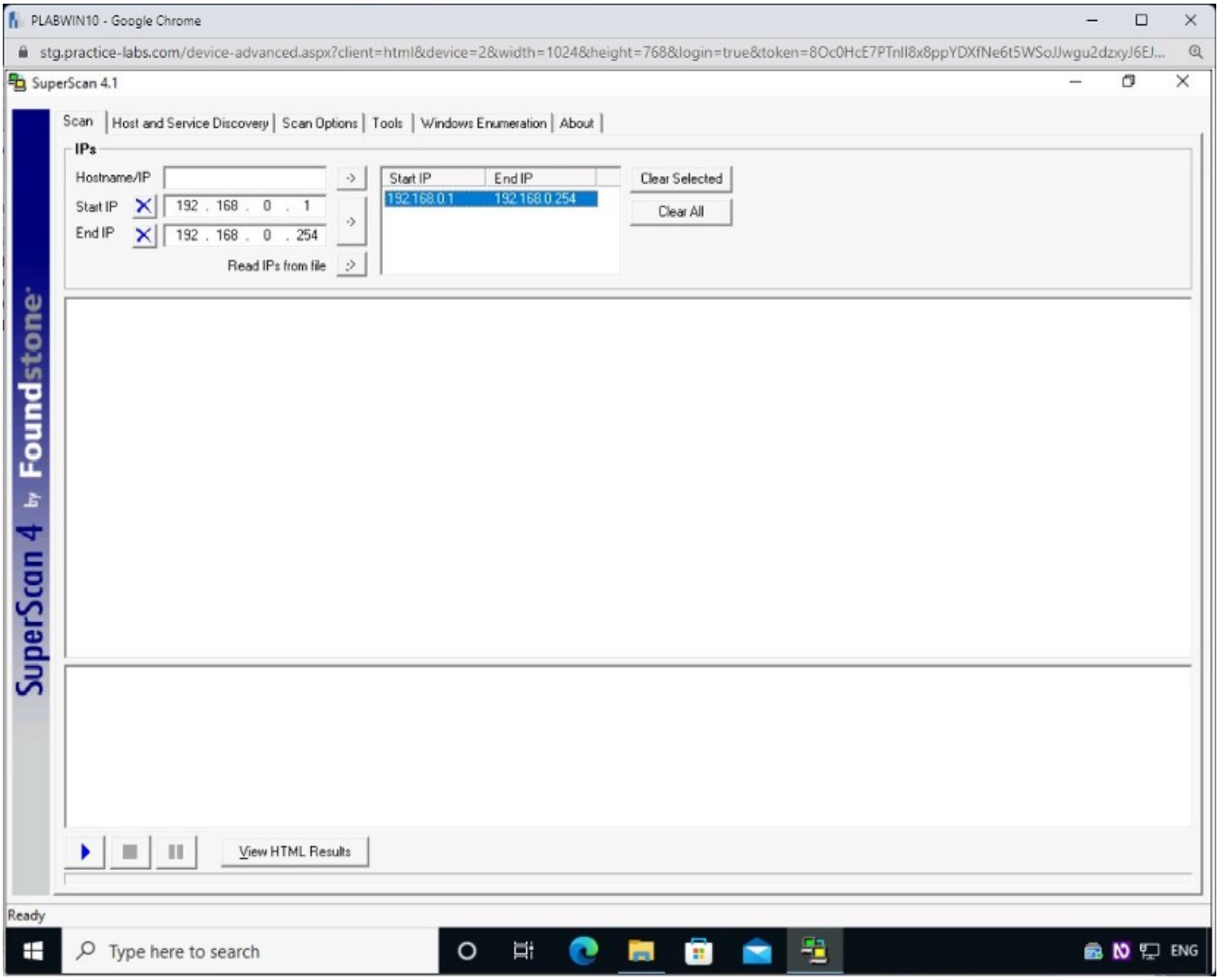
```
192.168.0.254
```

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



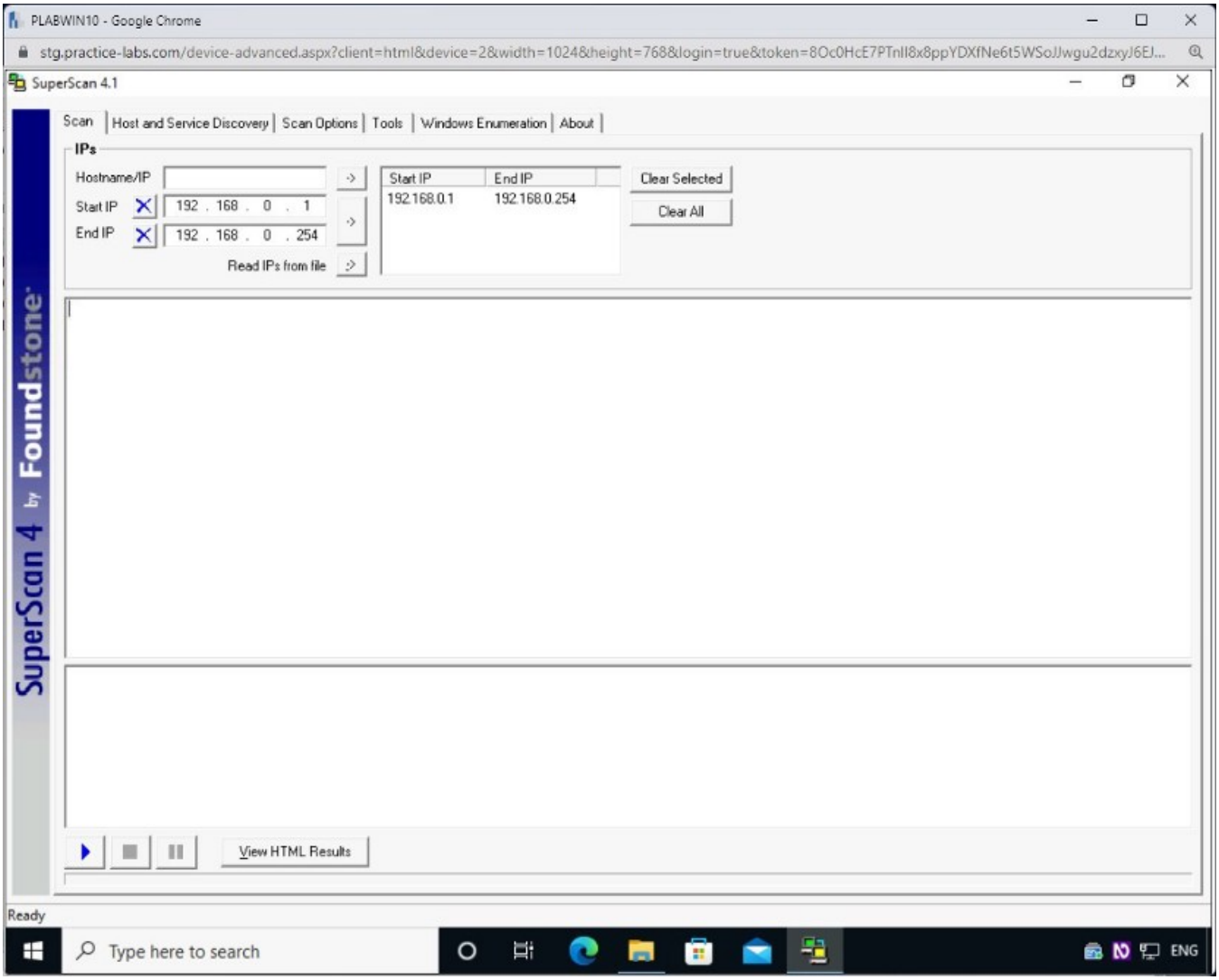
Step 16

The IP address range is now added to the **Start** and **End IP** text box.



Step 17

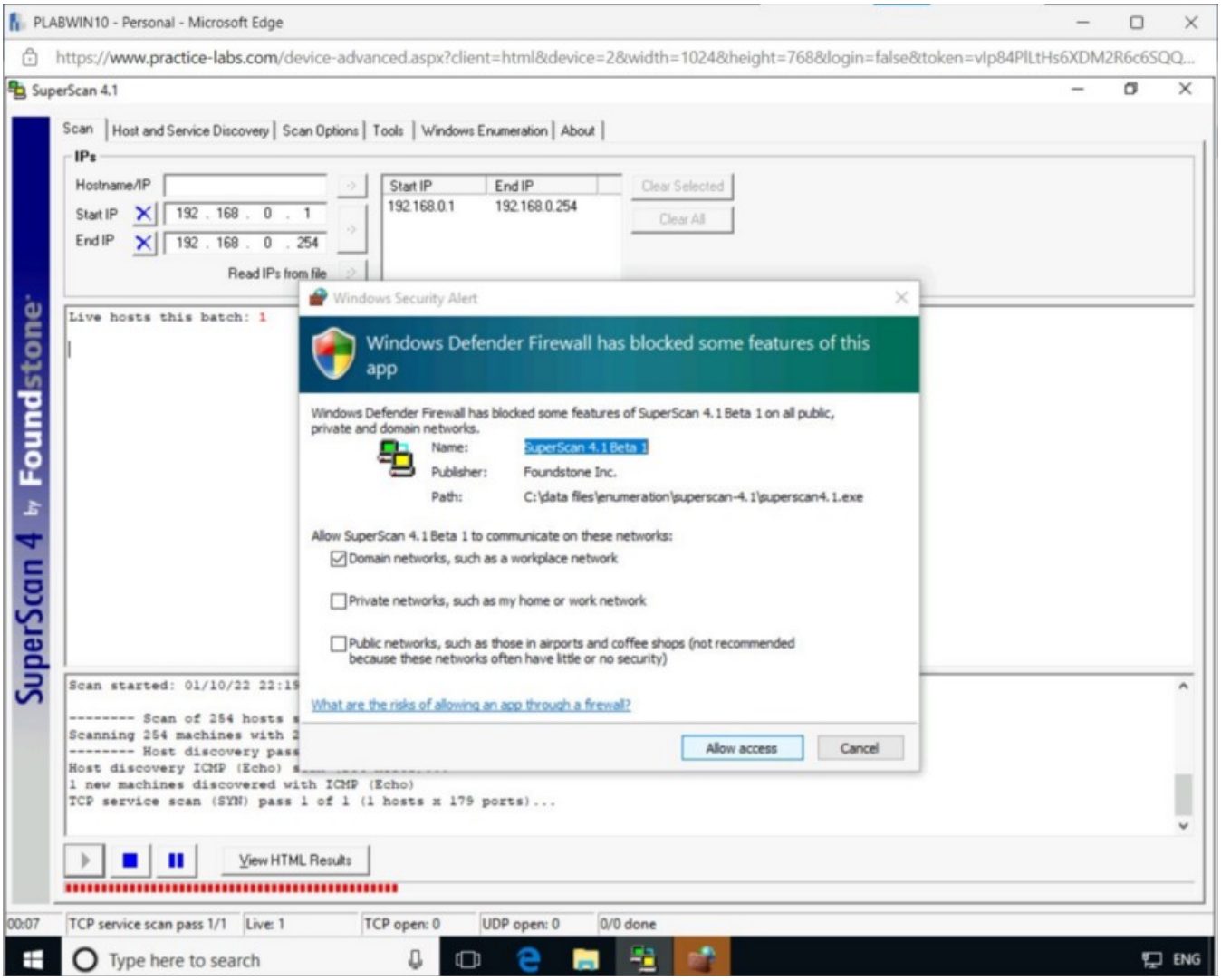
Click the **Play** button in the bottom left-hand corner.



Step 18

On the **Windows Security Alert** dialog box, click **Allow access**.

***Note**: This alert may not appear.*

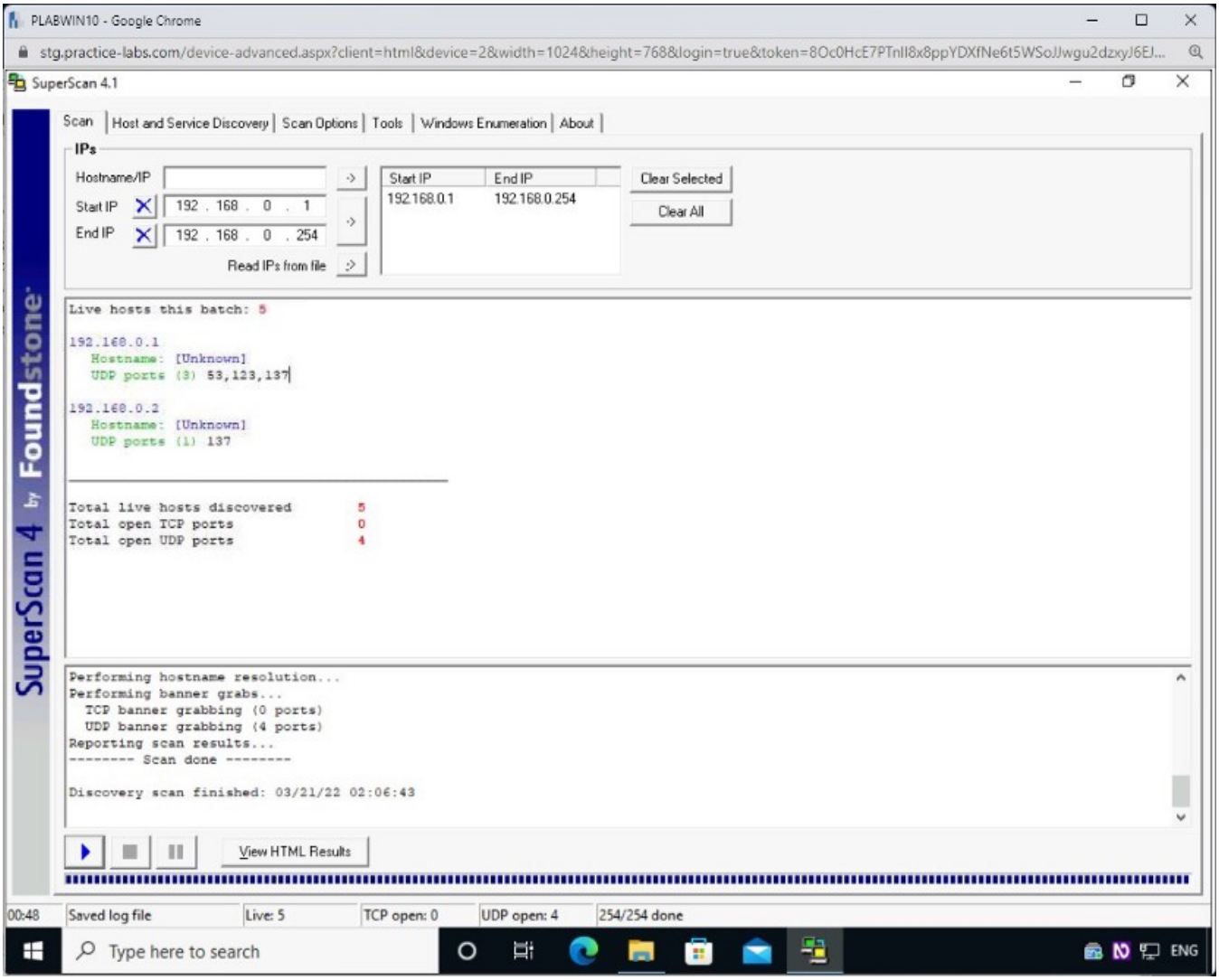


Step 19

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

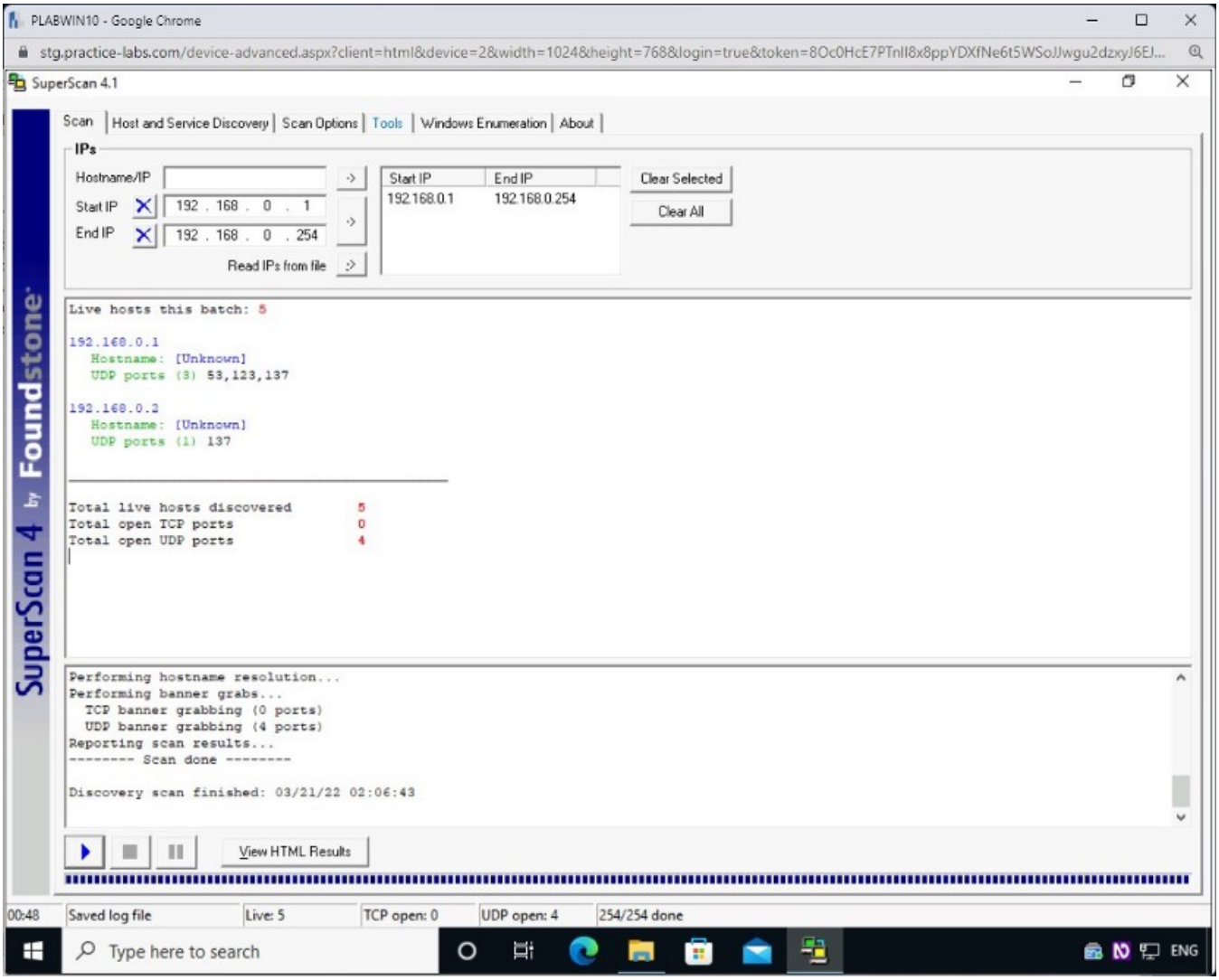
After the scan is completed, a detailed report is displayed when the progress bar has reached the end.

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



Step 20

Click the **Tools** tab.

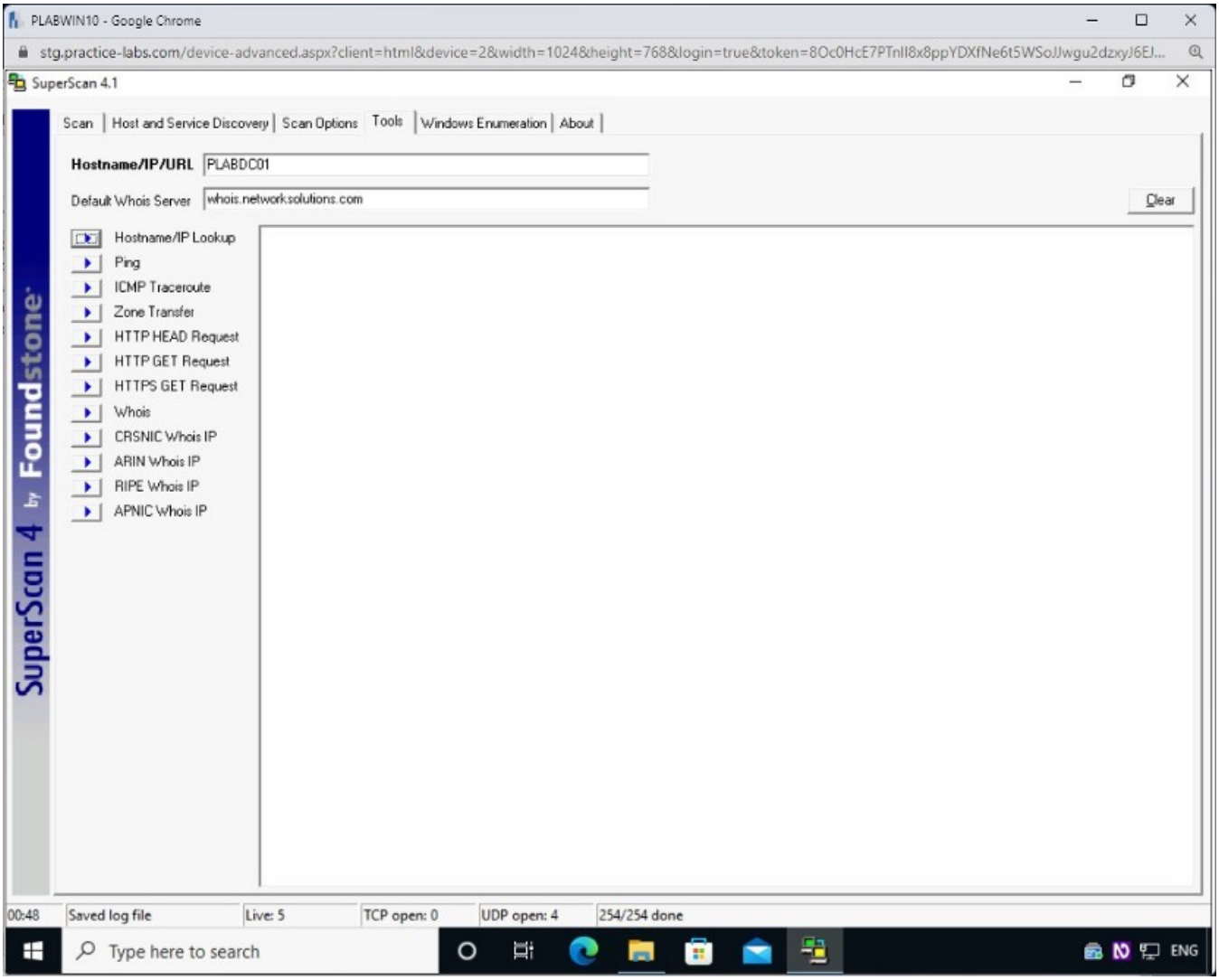


Step 21

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

```
PLABDC01
```

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

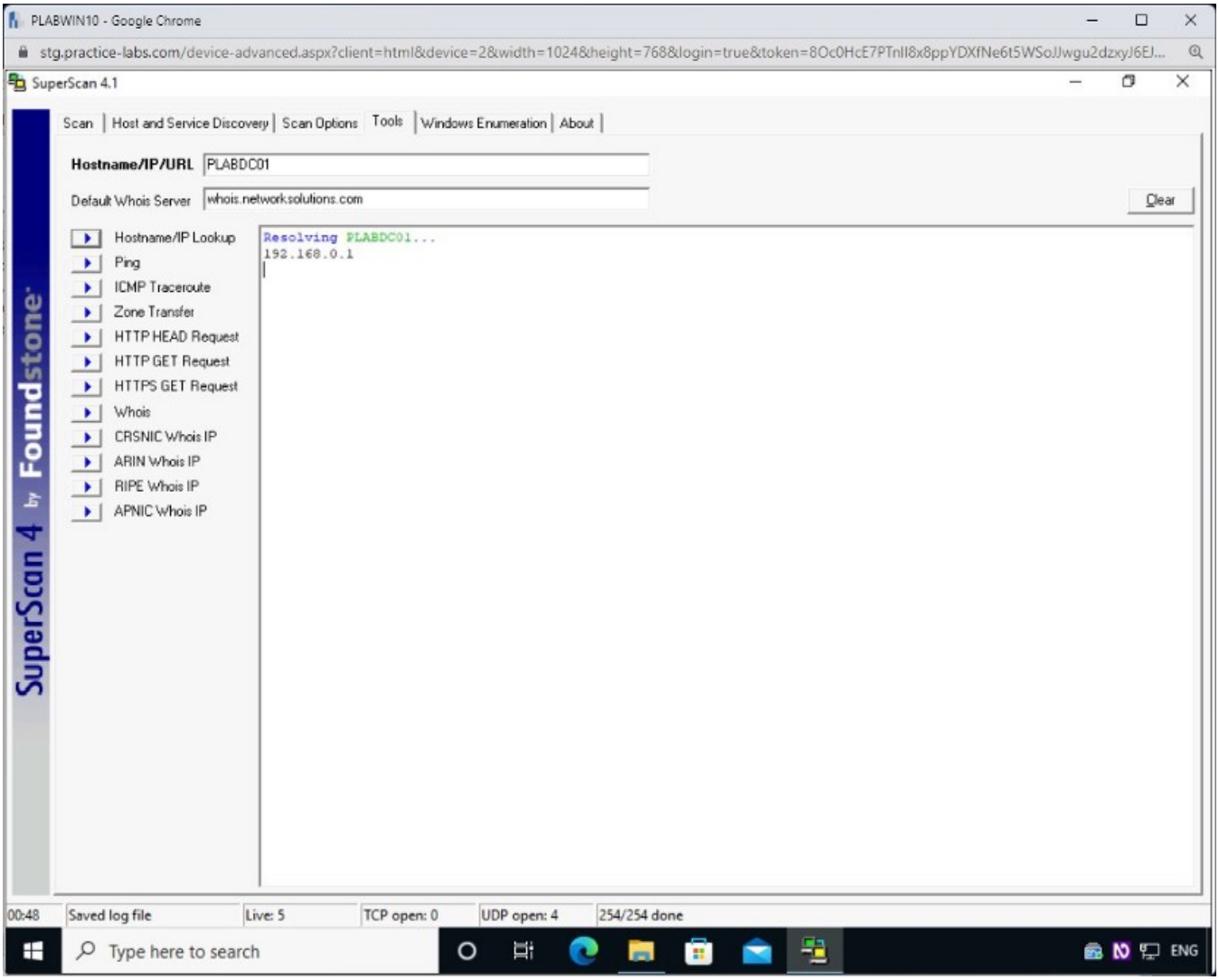


Step 22

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

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

Close the **SuperScan 4.1** window.



Close all open windows.

Task 2 — Perform NetBIOS Enumeration Using Nbtstat

In Windows, you have a utility named Nbtstat that helps you obtain NetBIOS information, such as NetBIOS name tables and NetBIOS name cache. It is a pretty easy-to-use utility with a few parameters.

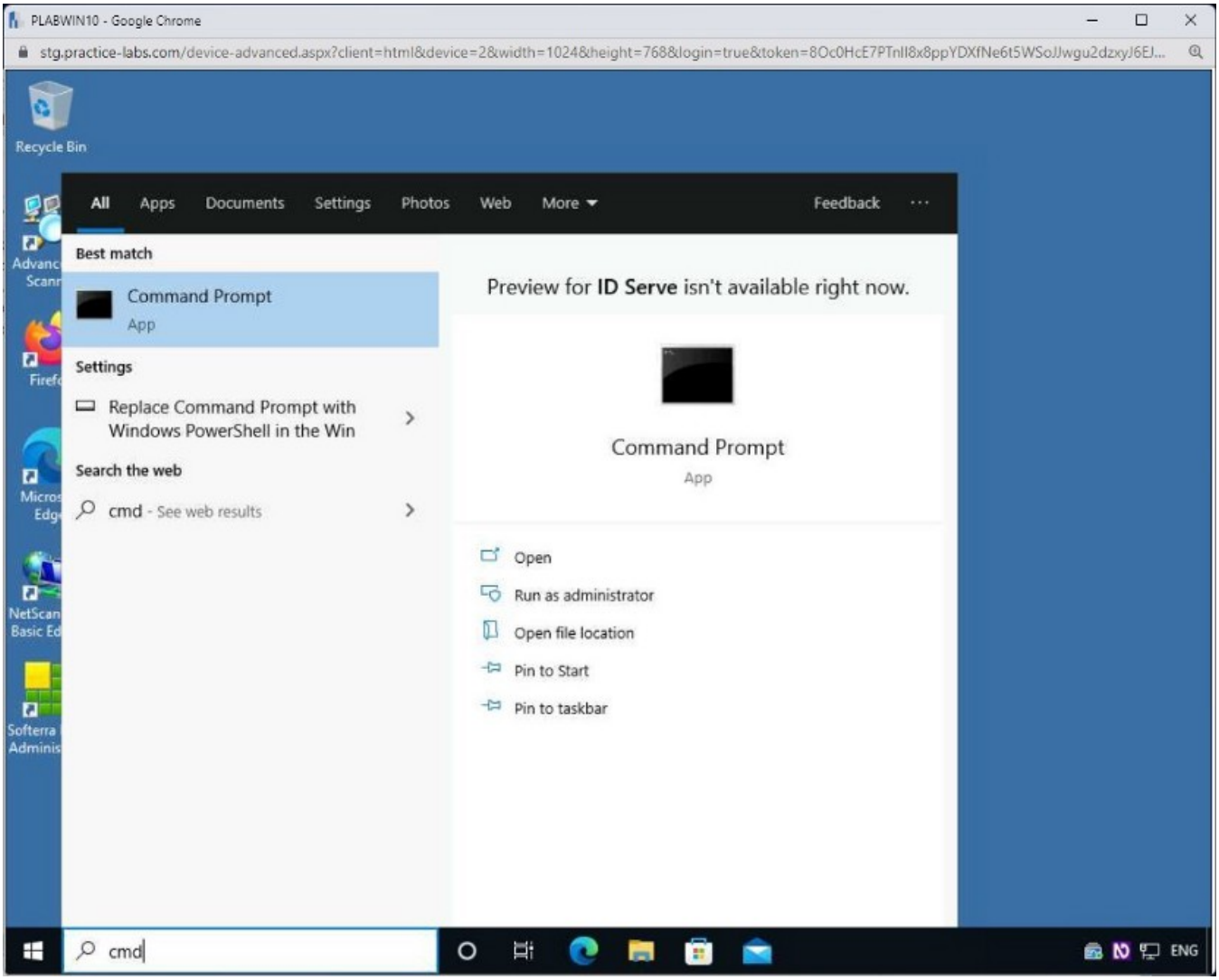
In this task, you will learn to perform NetBIOS enumeration using Nbtstat.

Step 1

Connect to **PLABWIN10**. In the Type here to search textbox, type the following command:

```
cmd
```

From the search results, click **Command Prompt**.

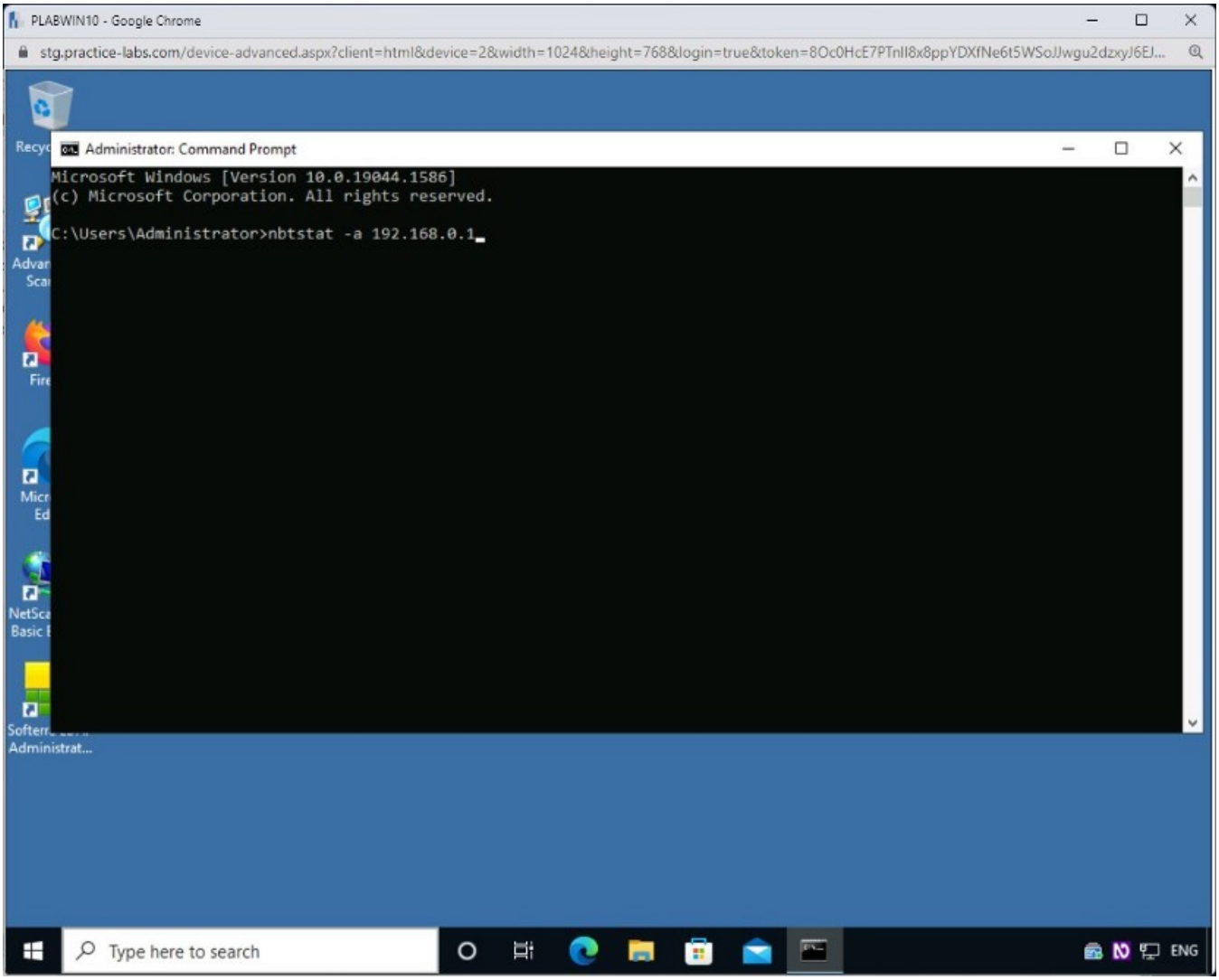


Step 2

In the command prompt window, type the following command:

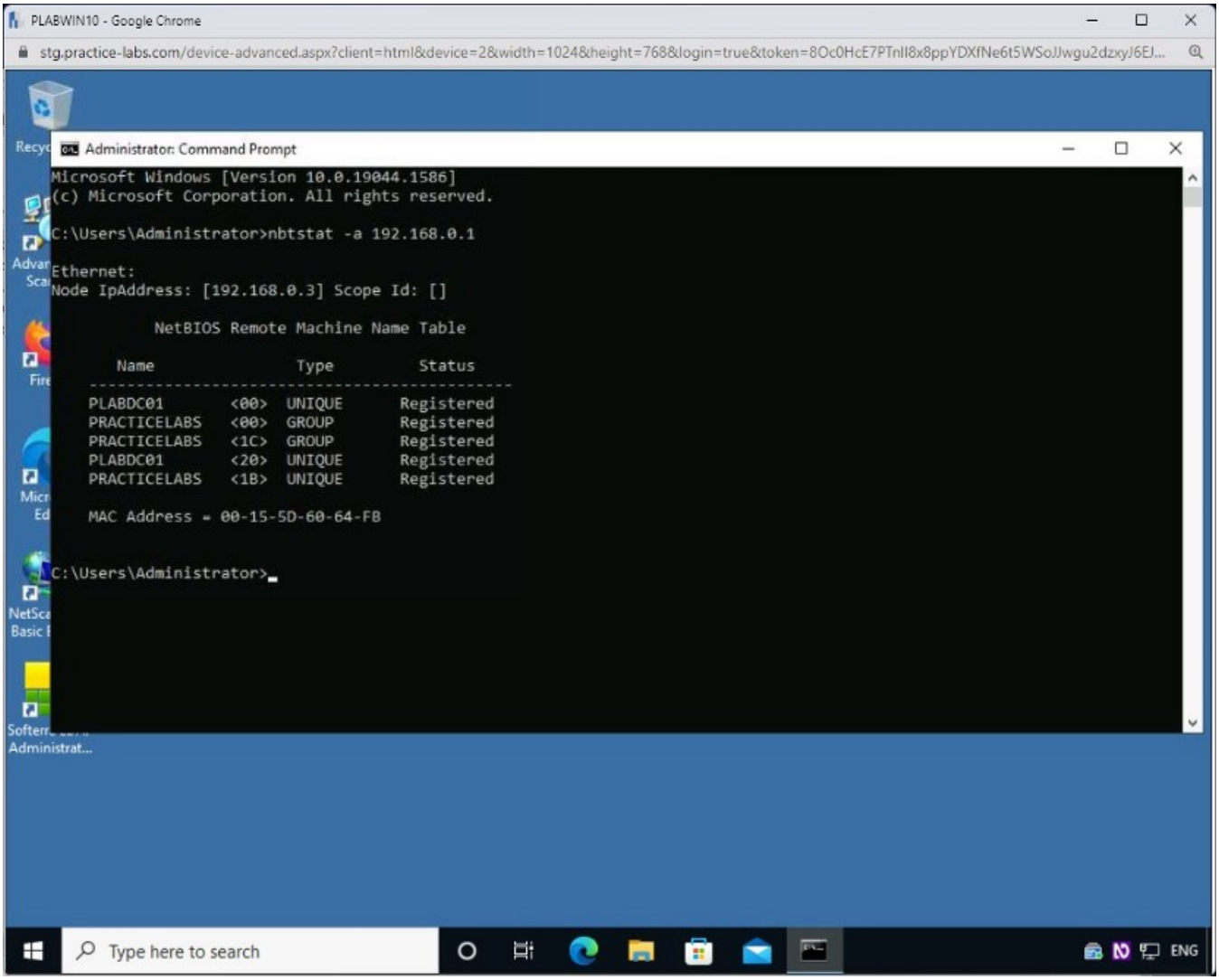
```
nbtstat -a 192.168.0.1
```

Press **Enter**. The **-a** parameter will display the NetBIOS name table from the system's IP address that you have specified.



Step 3

The **NetBIOS** name table from the remote system is displayed.



Step 4

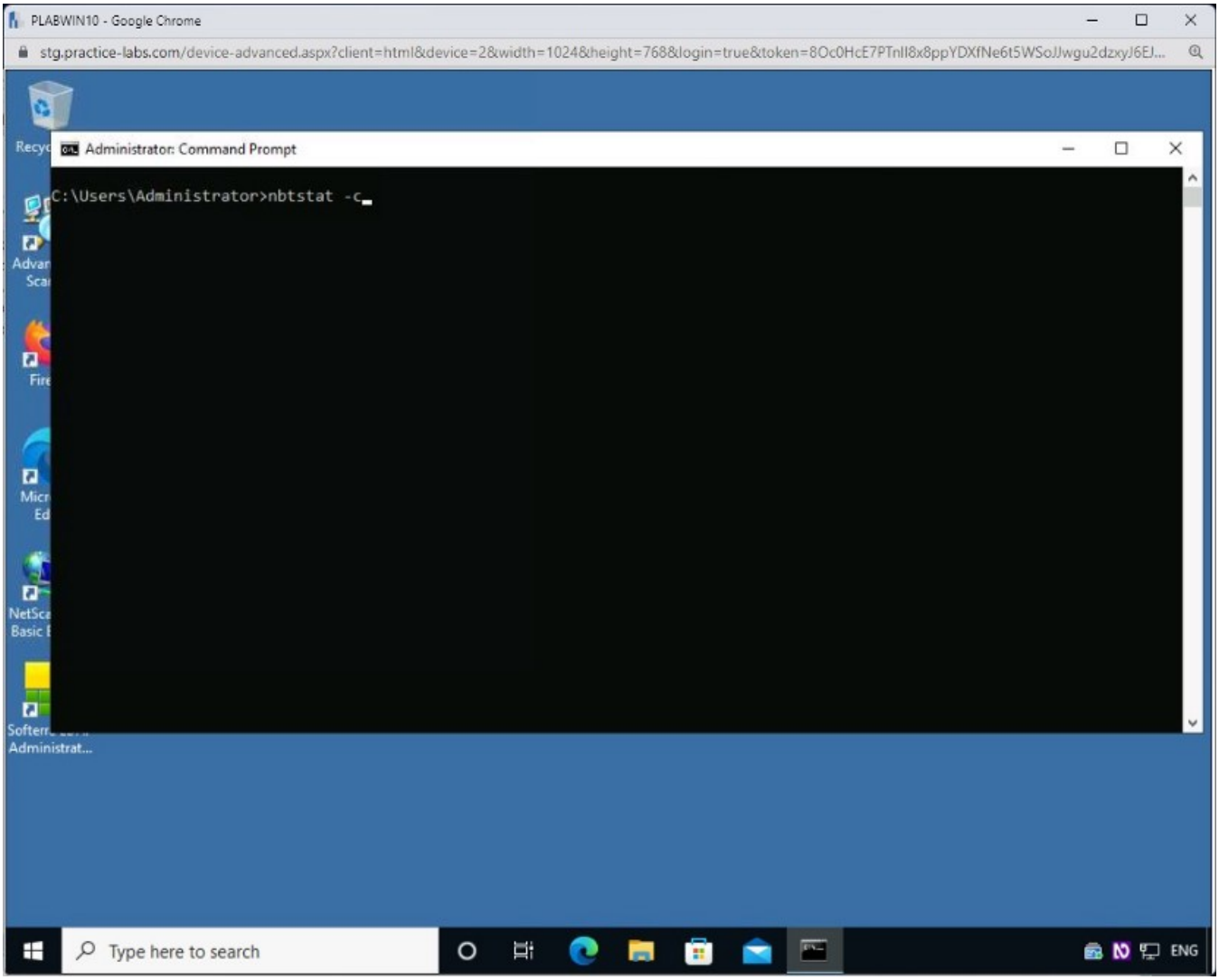
Clear the screen using the following command:

```
cls
```

You can also display the name cache along with the name table. To do this, type the following command:

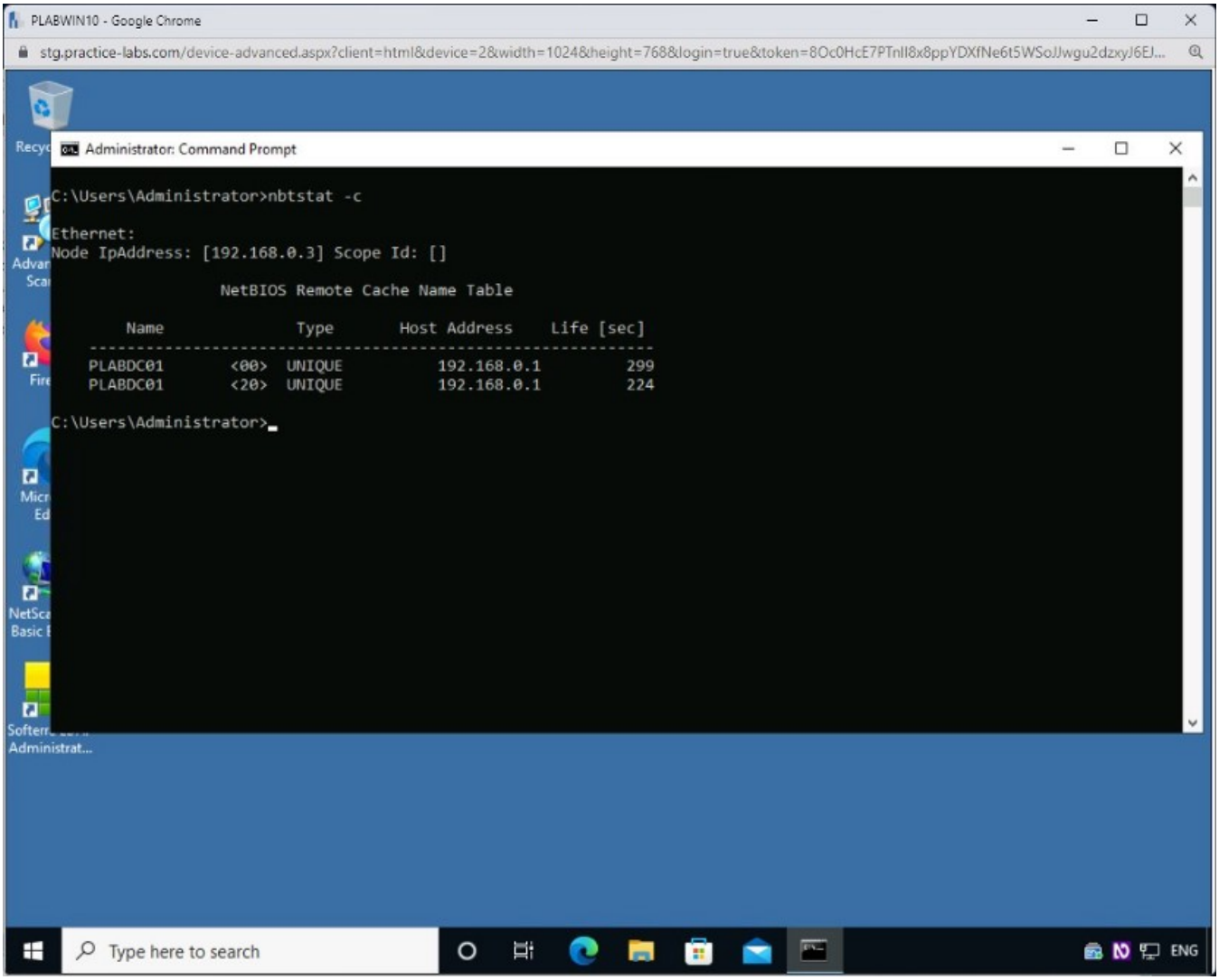
```
nbtstat -c
```

Press **Enter**. The **-c** parameter displays the name cache.



Step 5

The output displays the cache name table. It contains the name and IP address of the remote system, which is **PLABDC01**.



Close the command prompt window.

Task 3 — Perform NetBIOS Enumeration using Nmap

Nmap, other than the command, contains a Nmap Scripting Engine (NSE) used to execute ready-made scripts available within it. NSE also contains a script that helps you perform NetBIOS enumeration and can help you determine the NetBIOS names and MAC addresses.

In this task, you will learn to perform NetBIOS Enumeration using Nmap.

Step 1

Connect to **PLABKALI01**.

Log in using the following credentials:

Username:

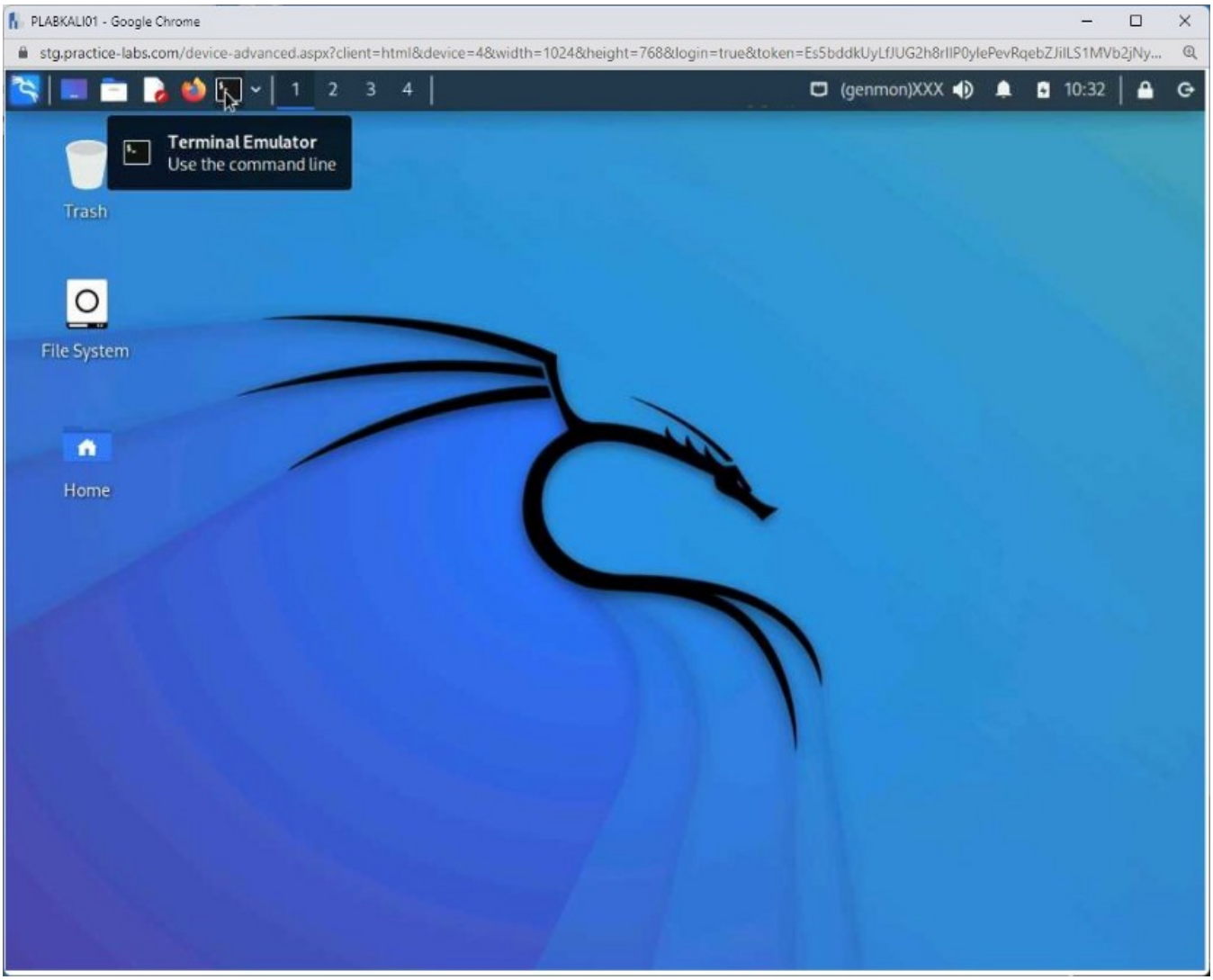
```
root
```

Password:

Password

The desktop of **PLABKALI01** is displayed.

Open a new terminal window by clicking the **Terminal Emulator** icon on the taskbar.



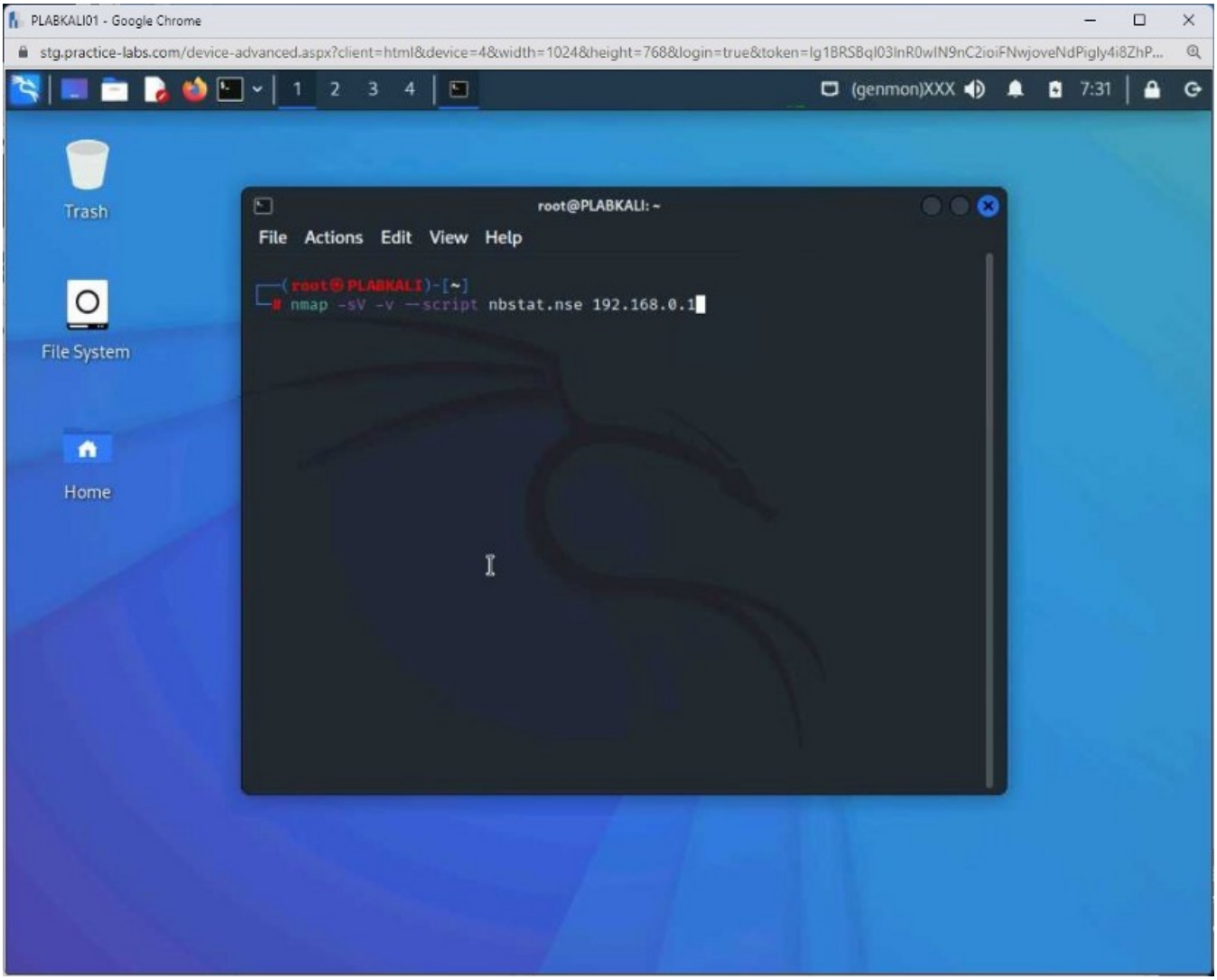
Step 2

You need to use the **nmap** tool and execute the following command:

```
nmap -sV -v --script nbstat.nse 192.168.0.1
```

Press **Enter**.

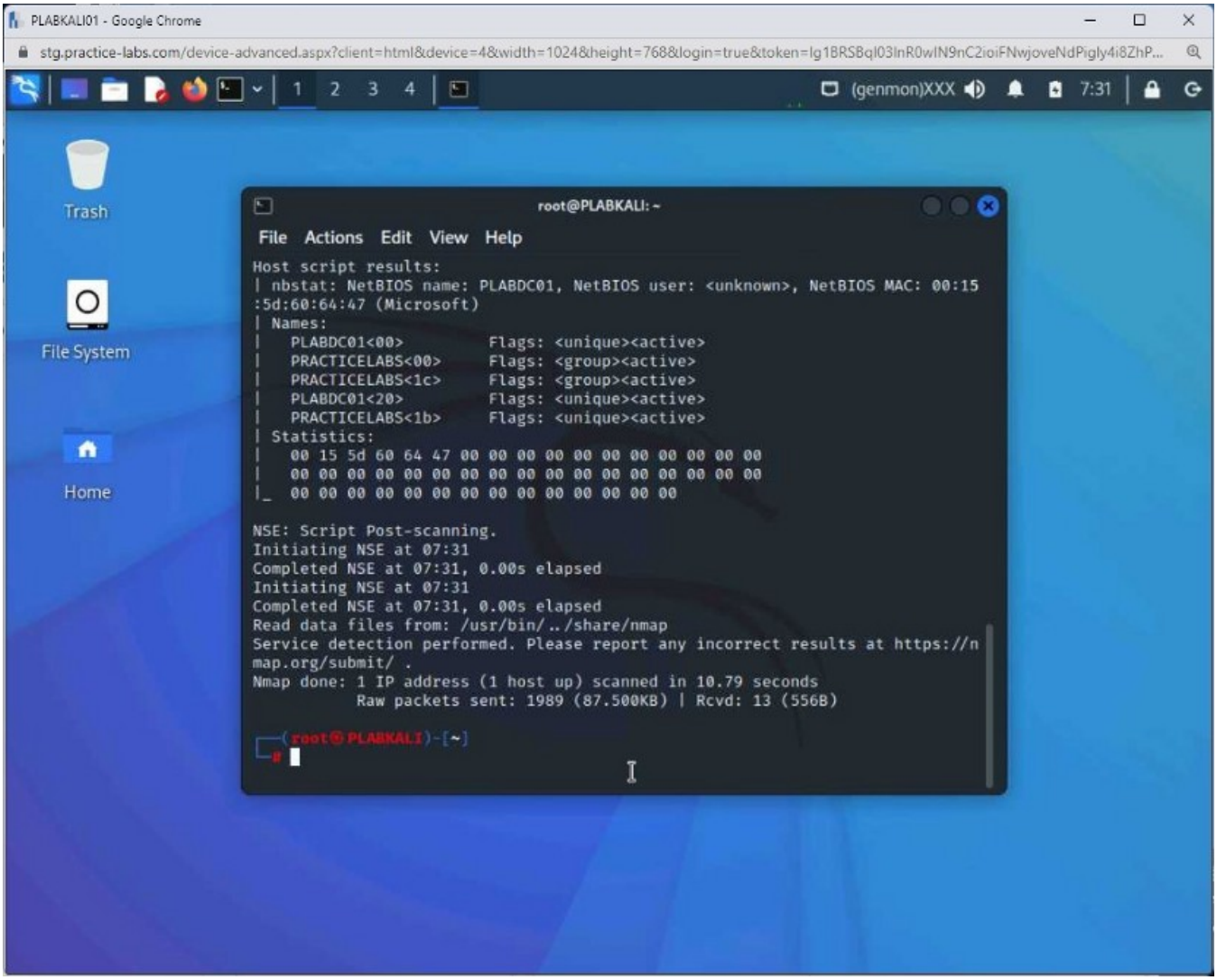
The **-sV** parameter helps you determine the service versions. The **-v** parameter increases the verbosity. The **— script** parameter enables you to use the mentioned script.



Step 3

The nmap script execution starts.

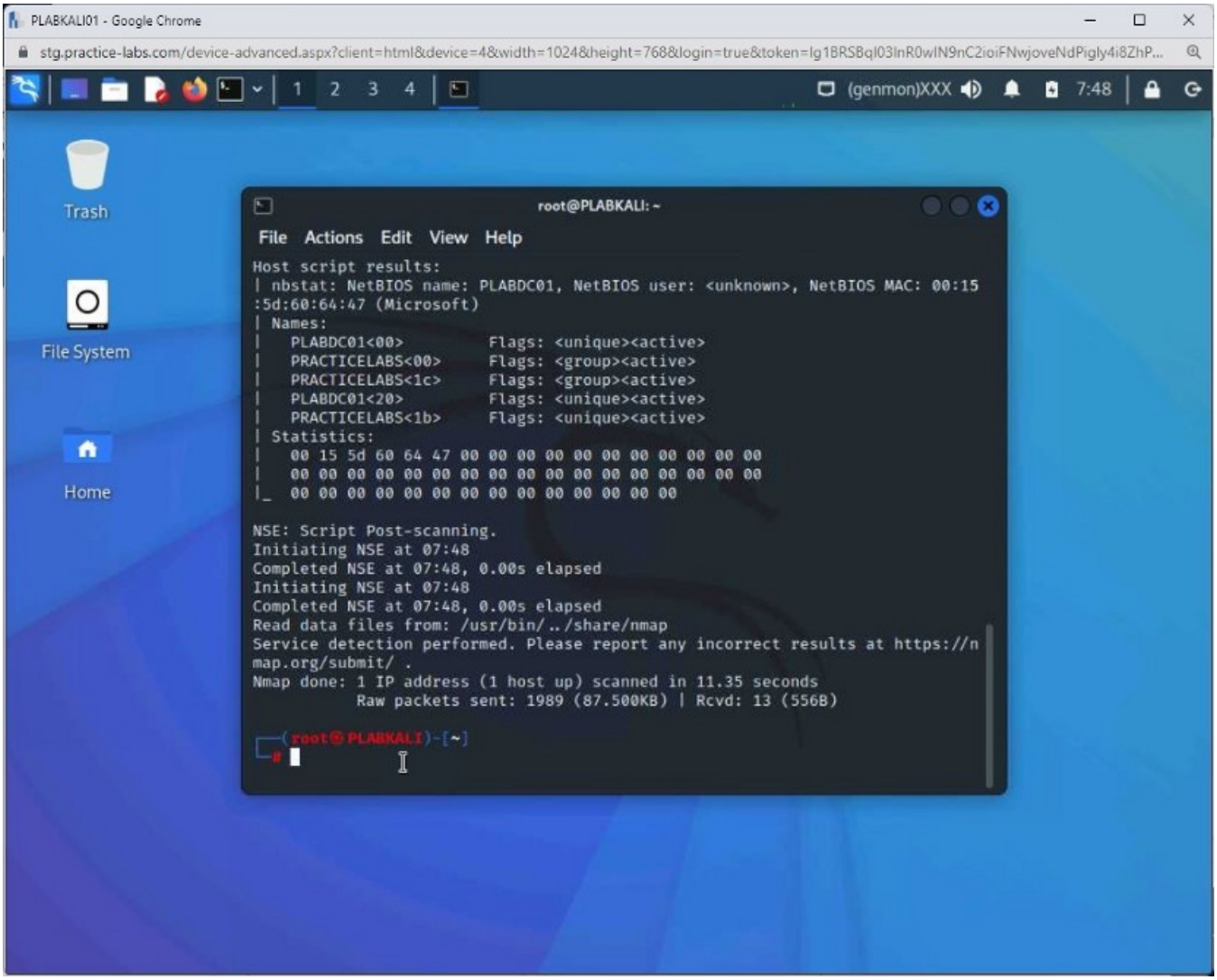
Notice that it has already determined the open ports and found **13** services running.



Step 4

The nmap script execution completes and provides a great deal of information. It was able to determine the following information:

- System name
- NetBIOS MAC address
- Domain name



Exercise 3 — SNMP Enumeration

Several devices are configured to use the Simple Network Management Protocol (SNMP), which helps an administrator manage them and get their current status.

An attacker can perform SNMP enumeration by using the default community string and extracting a lot of information from the device. The information can include ARP and routing tables.

In this exercise, you will learn to perform SNMP enumeration.

Learning Outcomes

After completing this exercise, you will be able to:

- Perform SNMP Enumeration Using IP Network Browser
- Perform SNMP Enumeration Using Snmp-check

Your Devices

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

PLABDC01Domain Controller192.168.0.1/24PLABWIN10Domain MemberWorkstation192.168.0.3/24PLABKALI01Domain MemberWorkstation192.168.0.5/24PLABDM01Domain Member Server192.168.0.2/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABDM01

Windows Server 2019 — Domain Member192.168.0.2/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

Task 1 — Installing SolarWinds Toolset Launch Pad

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

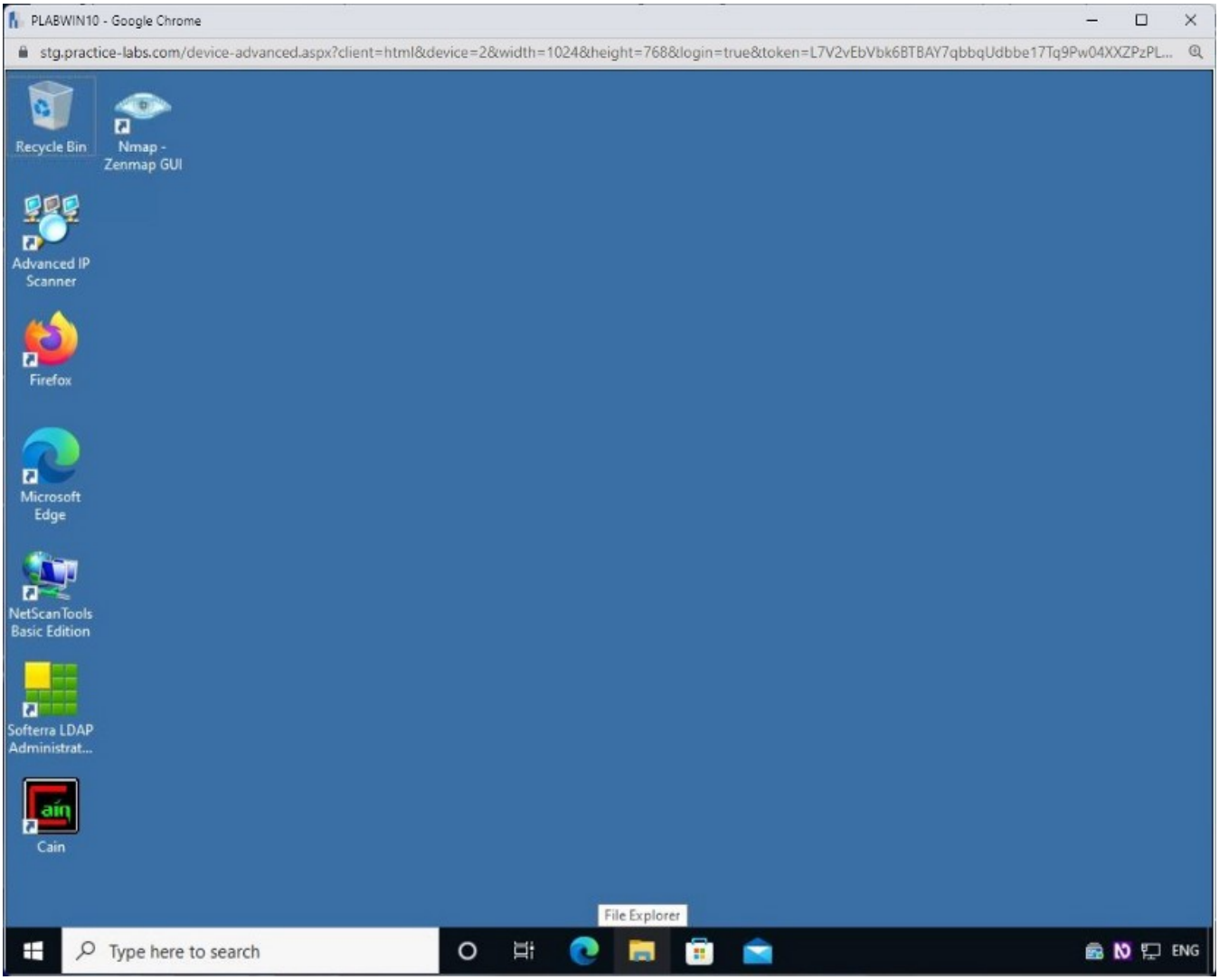
- SolarWind's Toolset Launch Pad / IP Network Browser
- ManageEngine OpUtils

SolarWinds Toolset is a network discovery tool using ICMP or SNMP. First, the trial version of this tool this needs to be installed. To do this, perform the following steps:

Step 1

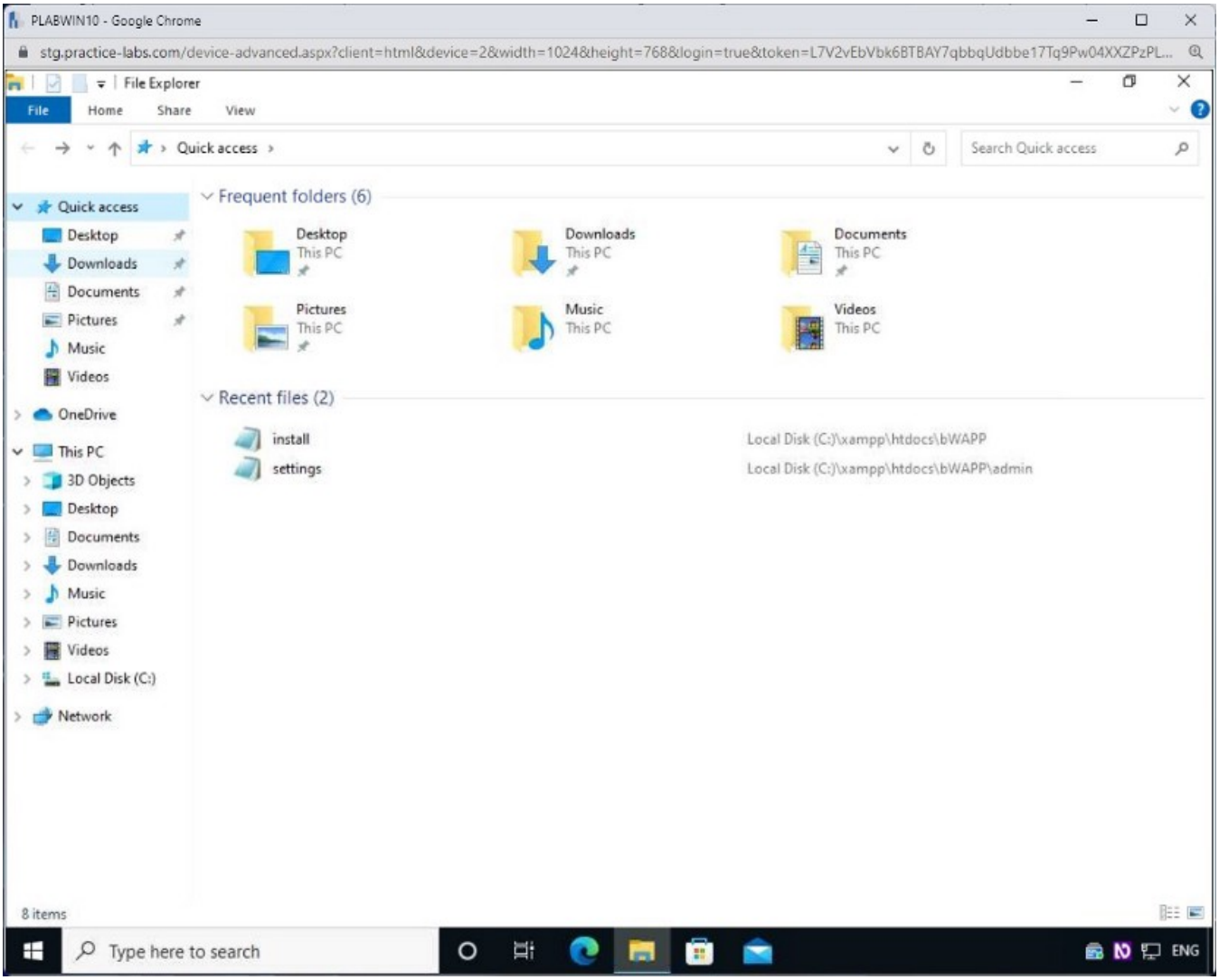
Ensure you have powered on all the devices listed in the introduction and connect to **PLABWIN10.**

Open **File Explorer** from the taskbar.



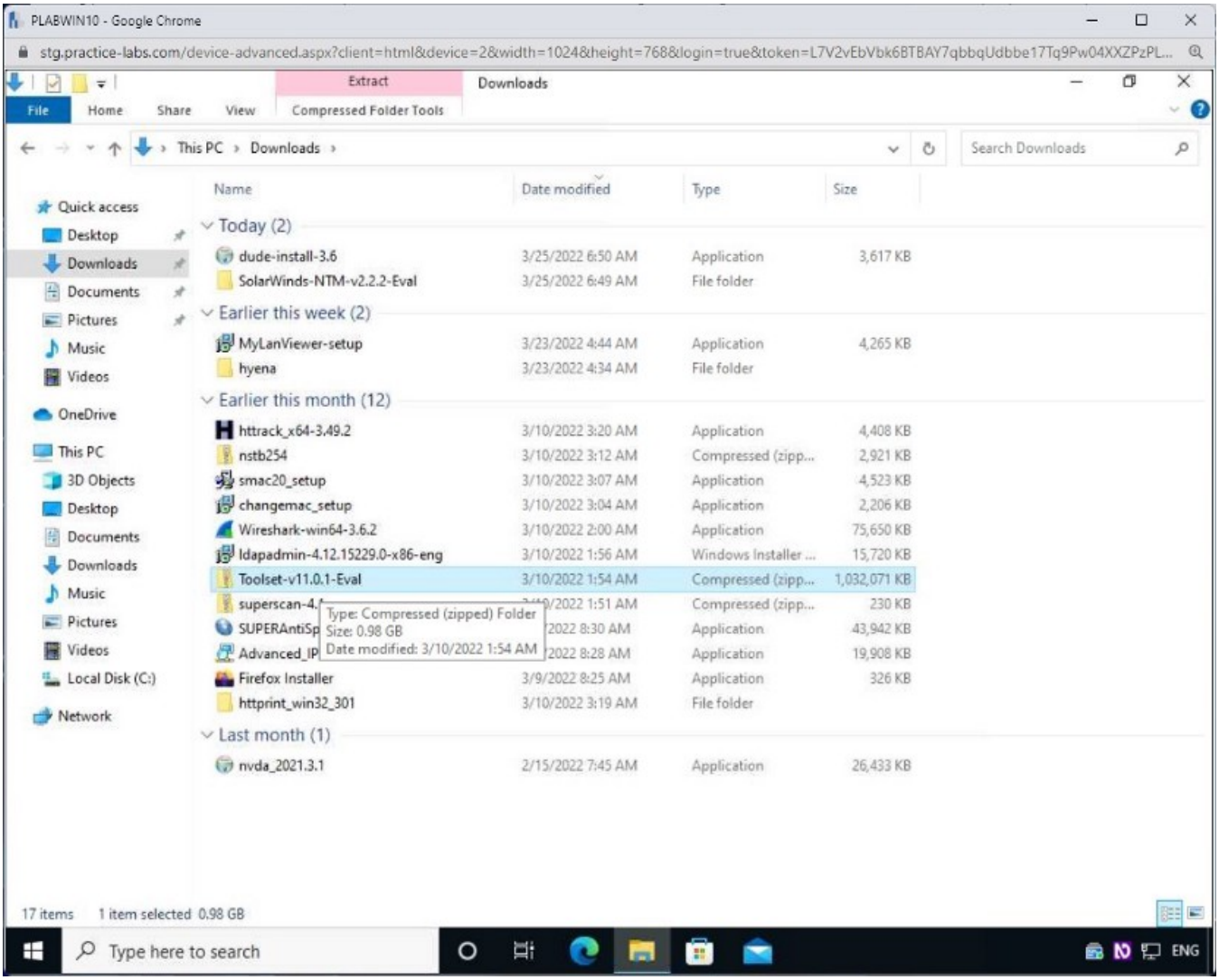
Step 2

Navigate to the **Downloads** folder.



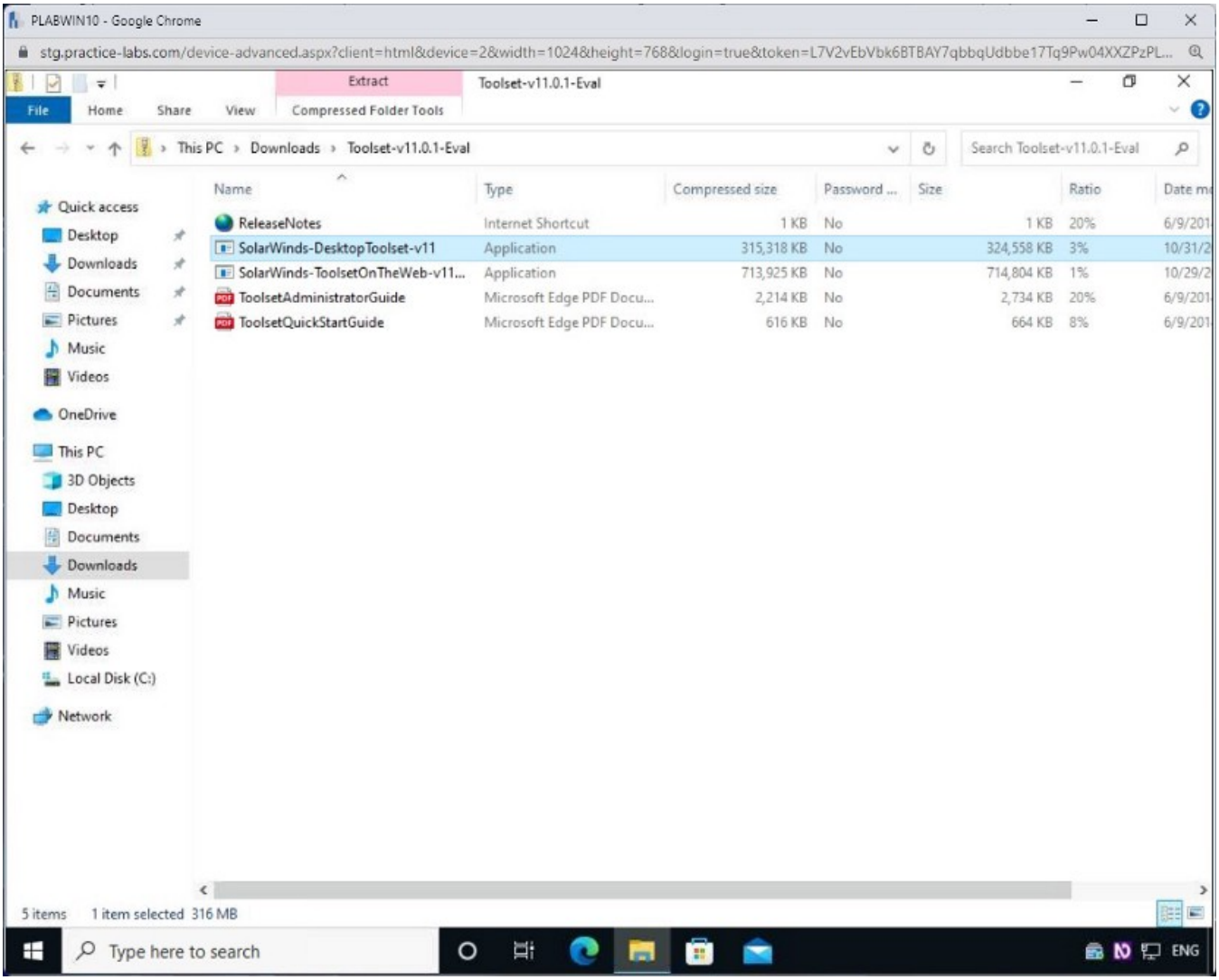
Step 3

Scroll down the list and double-click on the **Toolset-v11.01-Eval** folder.



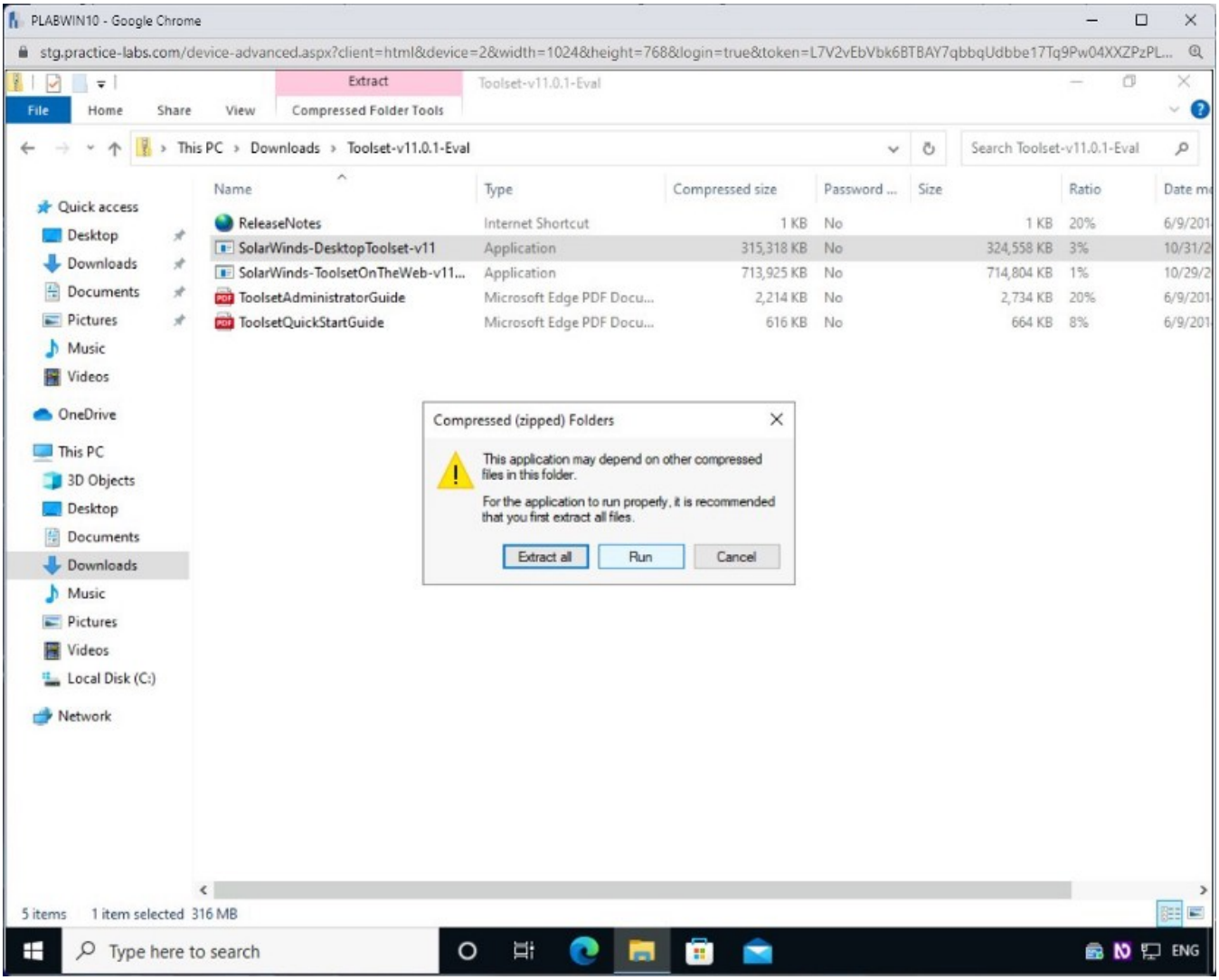
Step 4

Double click the **SolarWinds-DesktopToolset-v11** executable to begin installation of **Toolset Launch Pad**.



Step 5

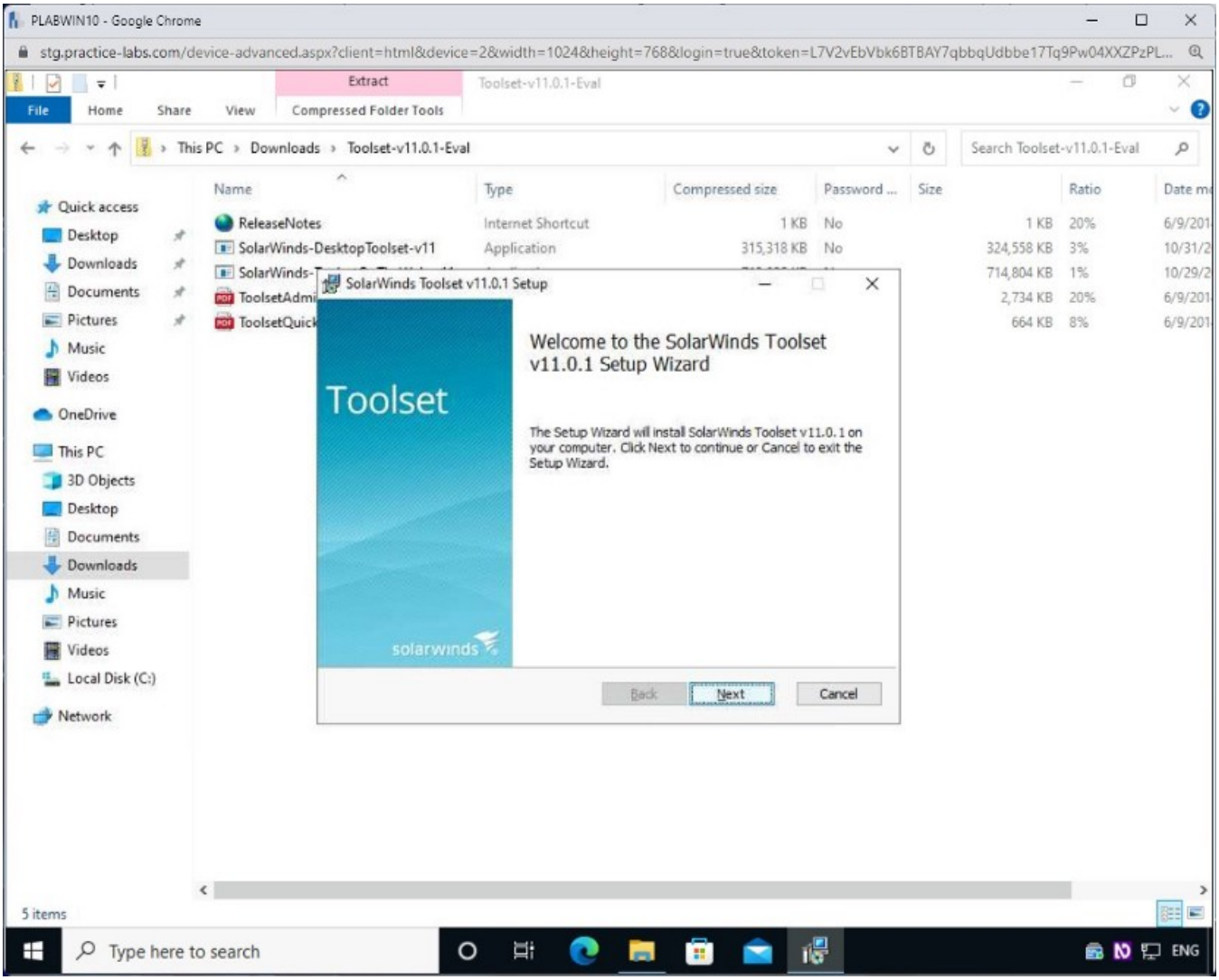
On the **Compressed (zipped) Folders** dialogue box, click **Run**.



Step 6

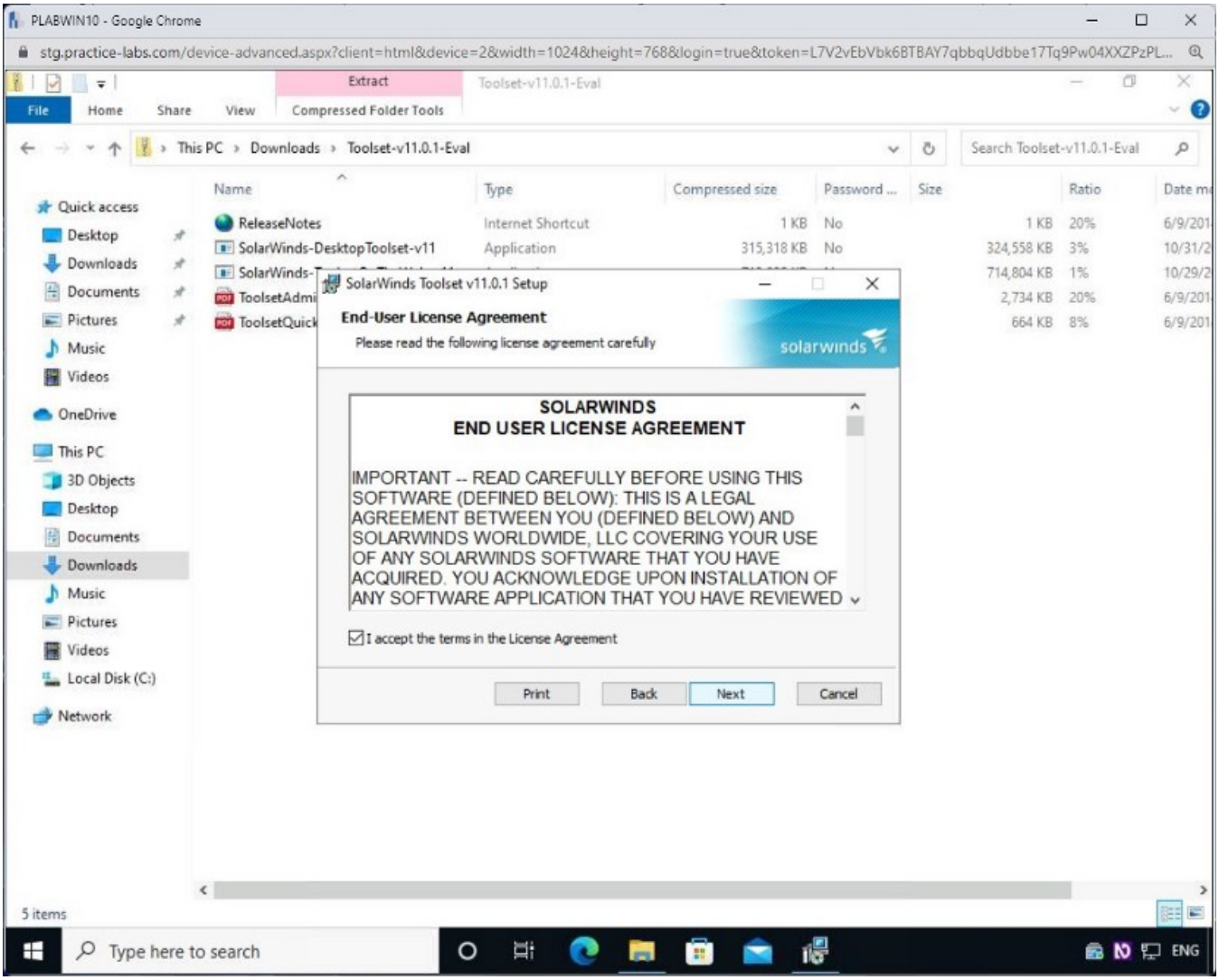
The **SolarWinds Toolset v11.0.1 Setup** window will display after a few moments.

Click **Next**.



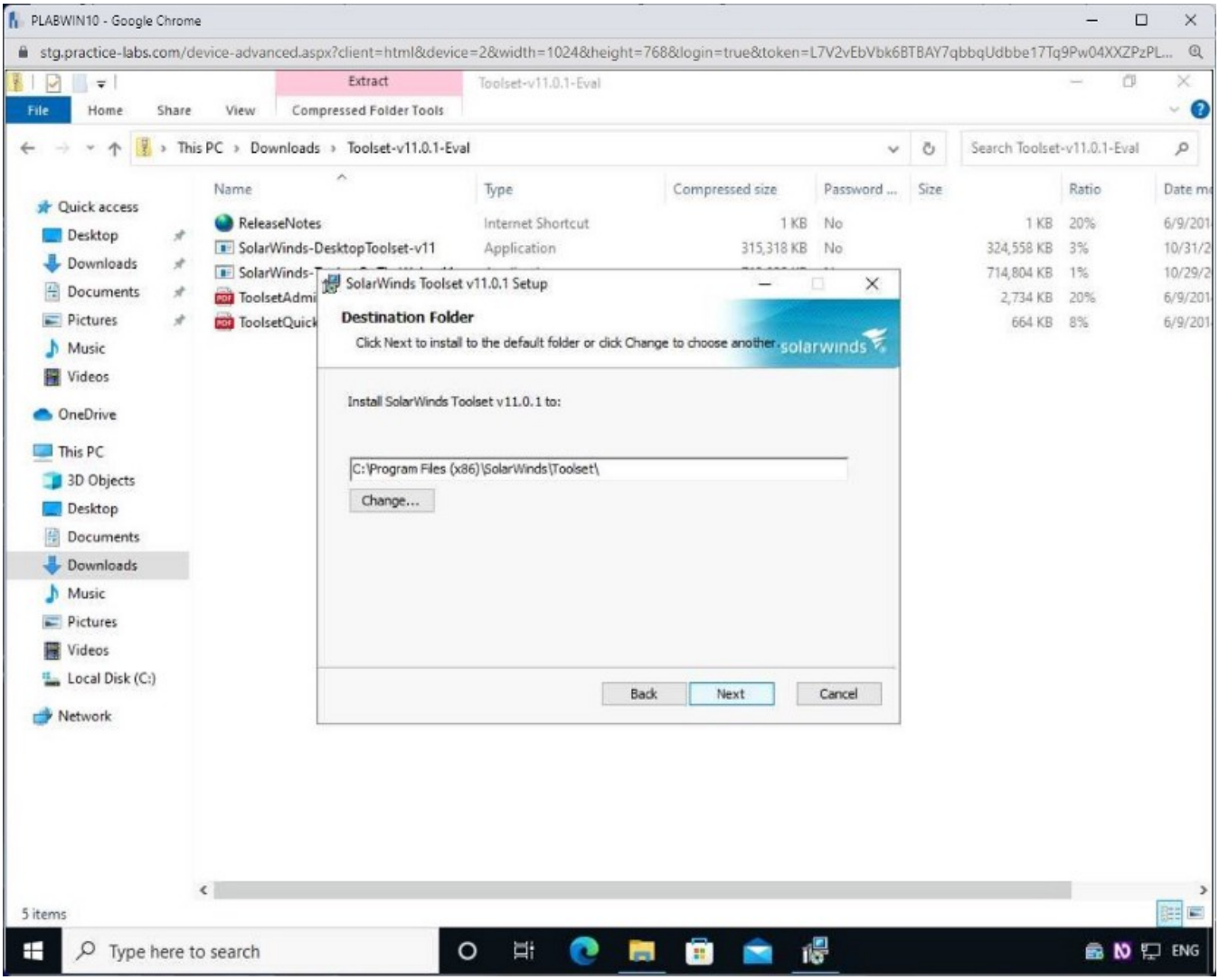
Step 7

On the **End-User Licence Agreement** page, check the **I accept the terms in the Licence Agreement** checkbox and then click **Next**.



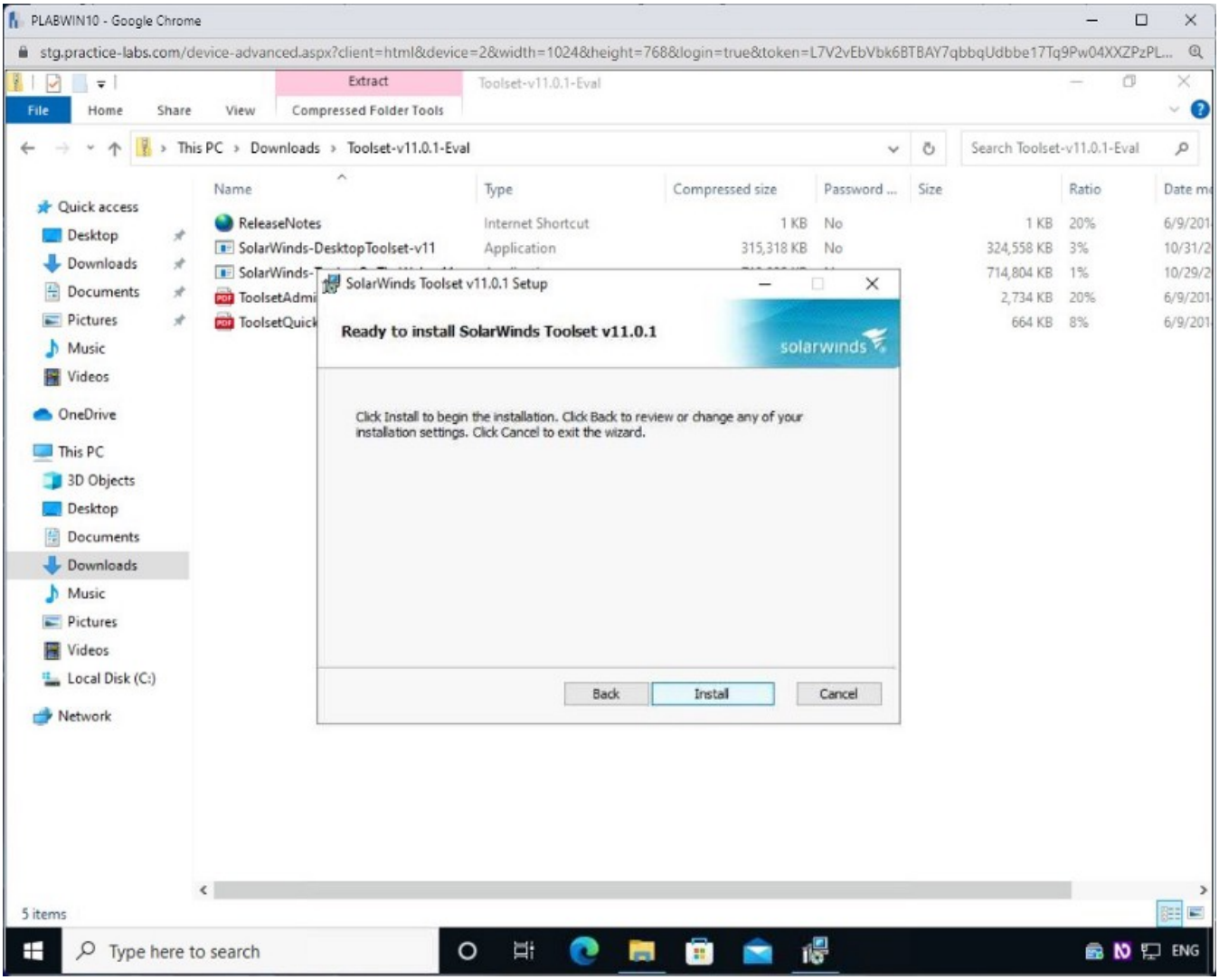
Step 8

On the **Destination Folder** page, leave the default option and click **Next**.



Step 9

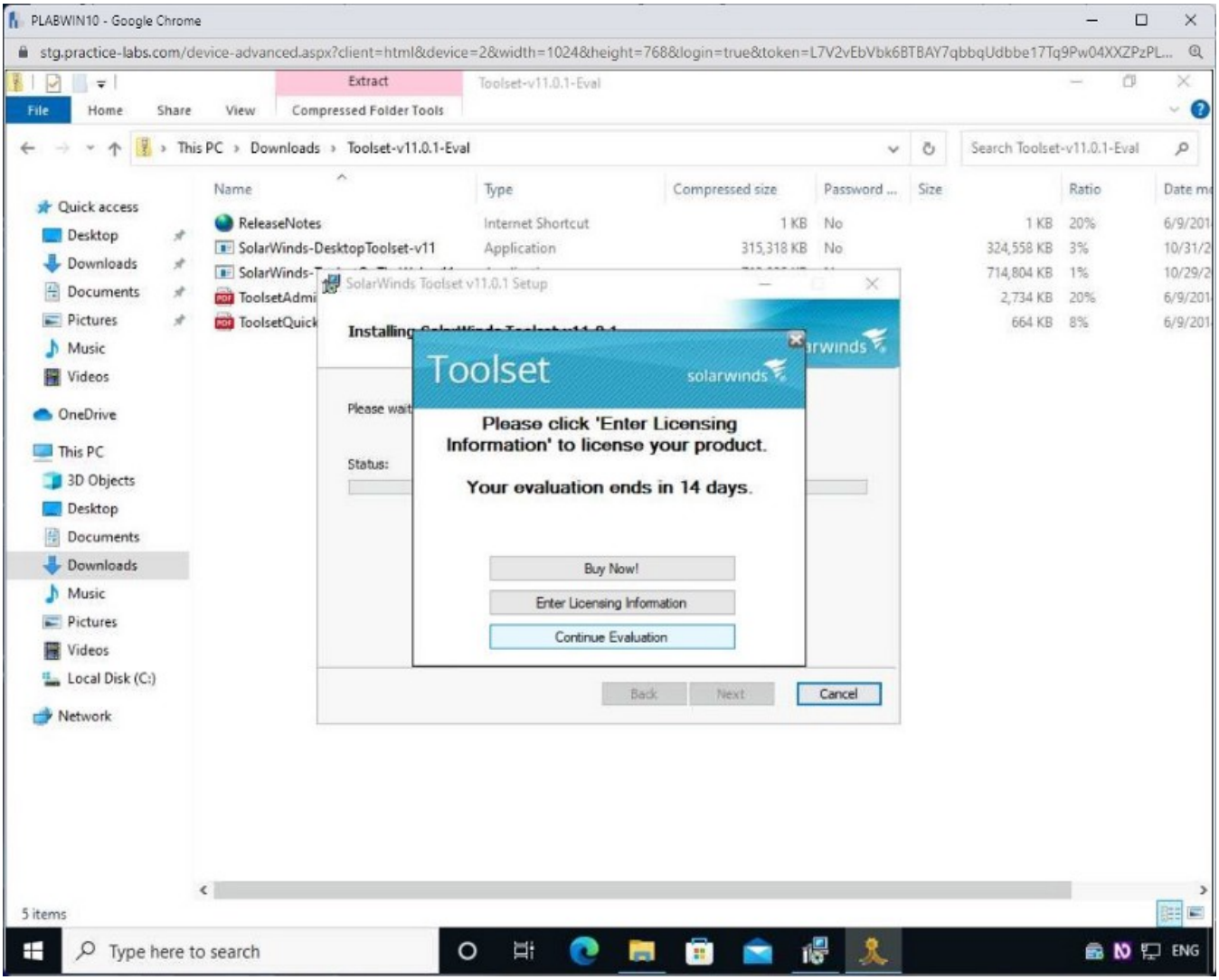
On the **Ready to Install SolarWinds Toolset v11.0.1** page, click **Install**.



Step 10

After a few minutes, the **Toolset licensing** window will appear.

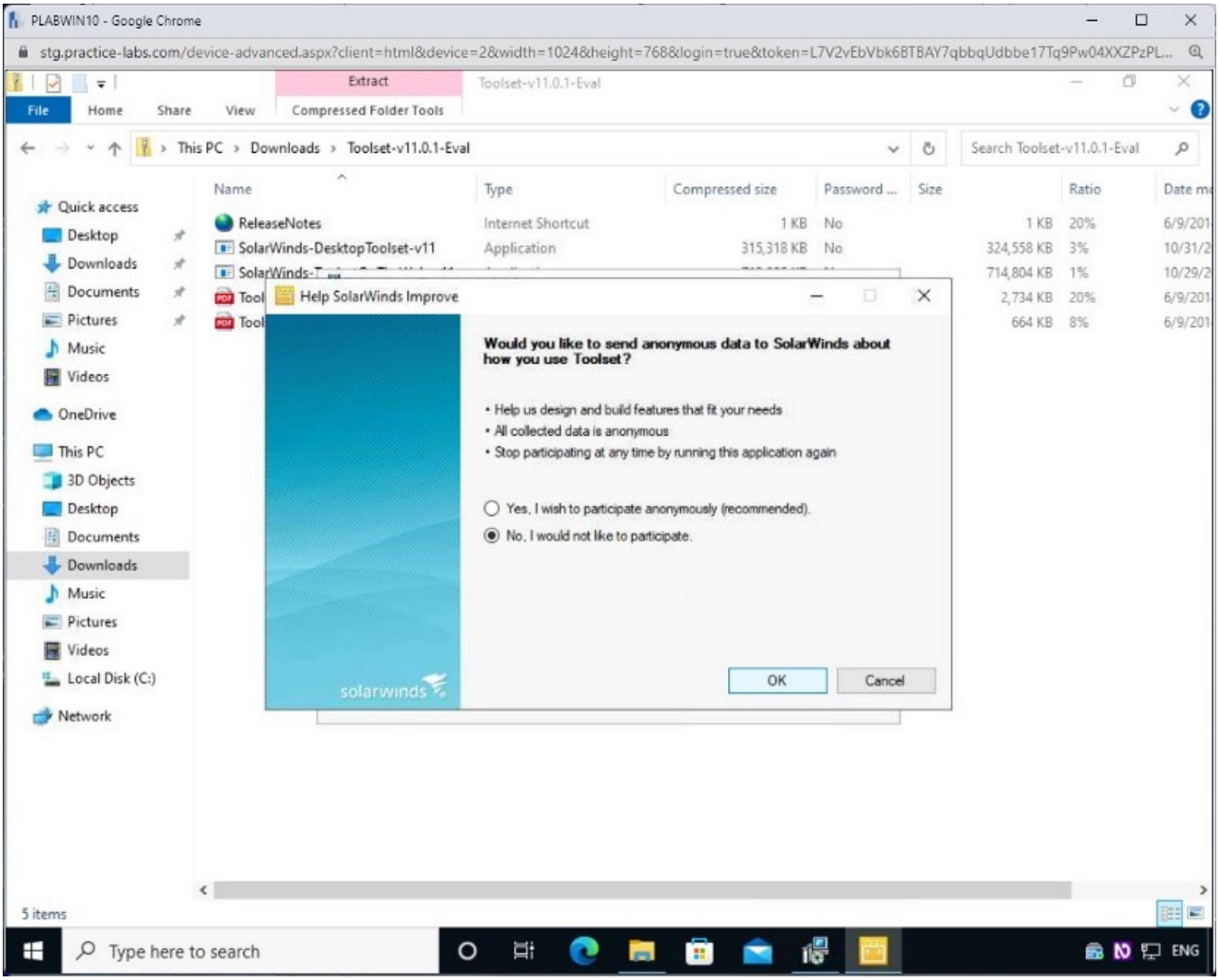
Click **Continue Evaluation**.



Step 11

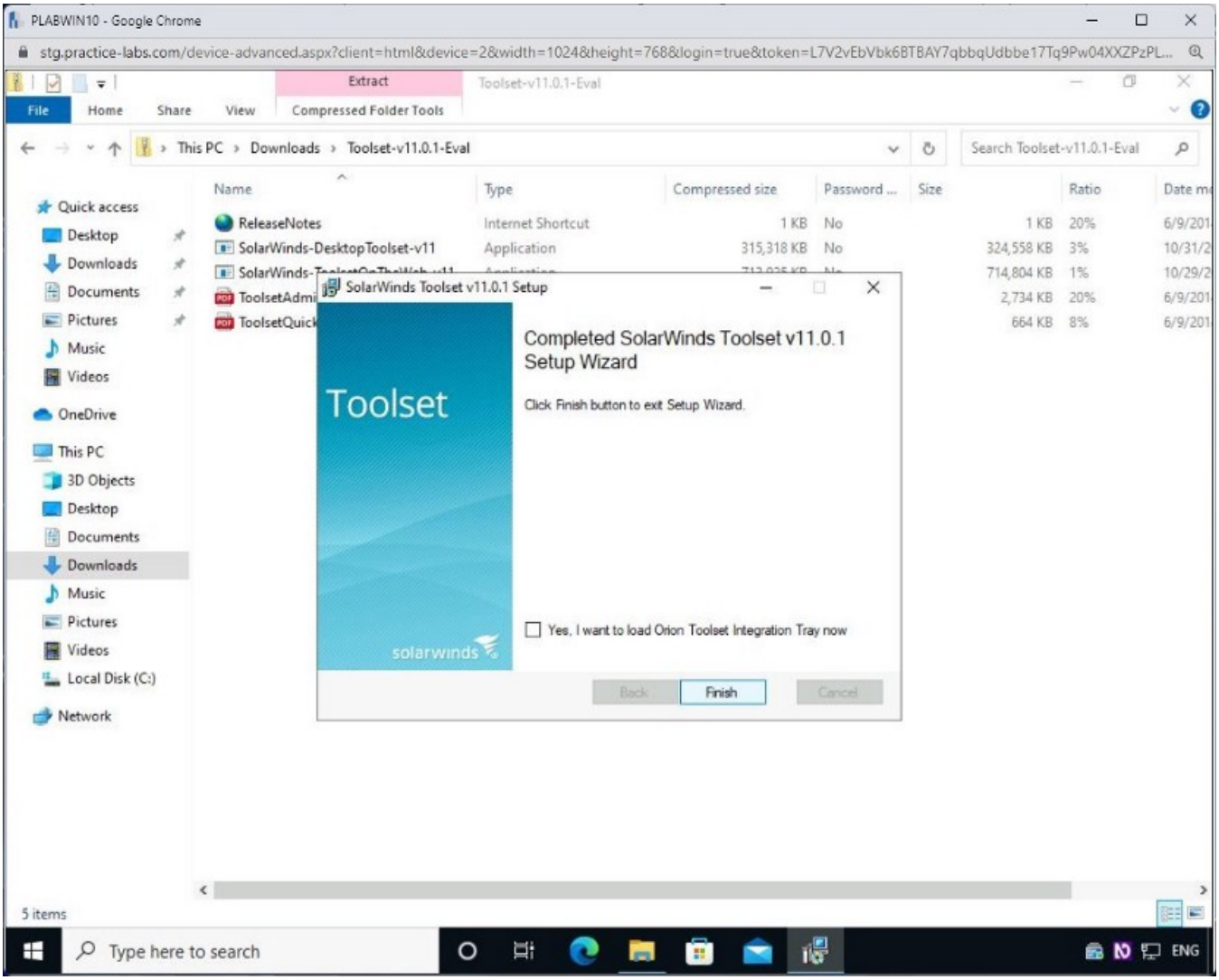
On the **Help SolarWinds Improve** page, select the **No, I would not like to participate** checkbox and click **OK**.

***Note**: A window may also appear to state that SolarWinds is installing free tools. Please allow this to complete.*



Step 12

Finally, on the **Completed SolarWinds Toolset v11.0.1 Setup Wizard** page, click **Finish**.



Close all open windows.

Task 2 — Perform SNMP Enumeration Using SolarWinds Toolset Launch Pad

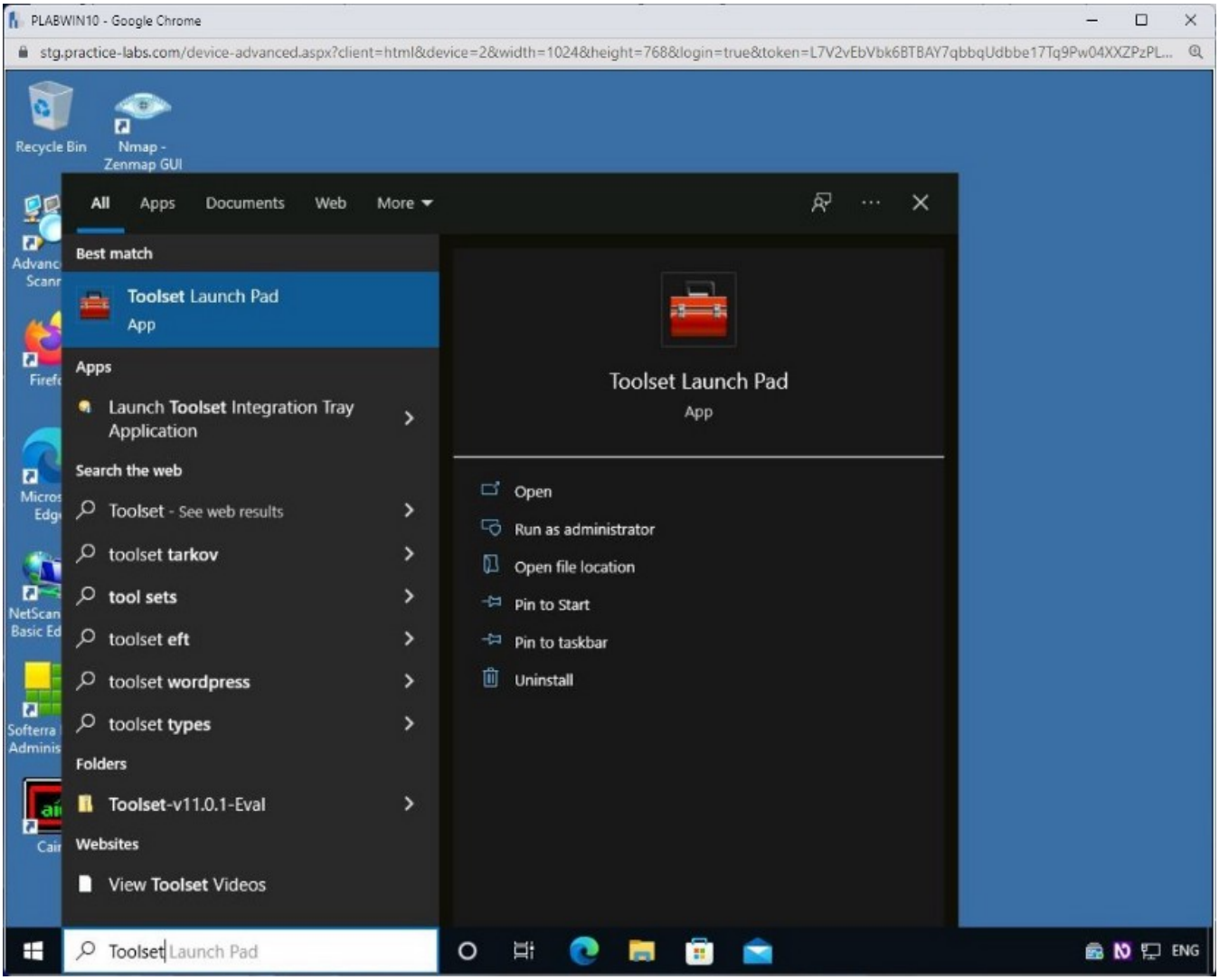
Now that SolarWinds Toolset Launch Pad has been installed, the tool can be used for SNMP enumeration. To do this, perform the following steps:

Step 1

In the **Type here to search** textbox, type the following:

```
Toolset
```

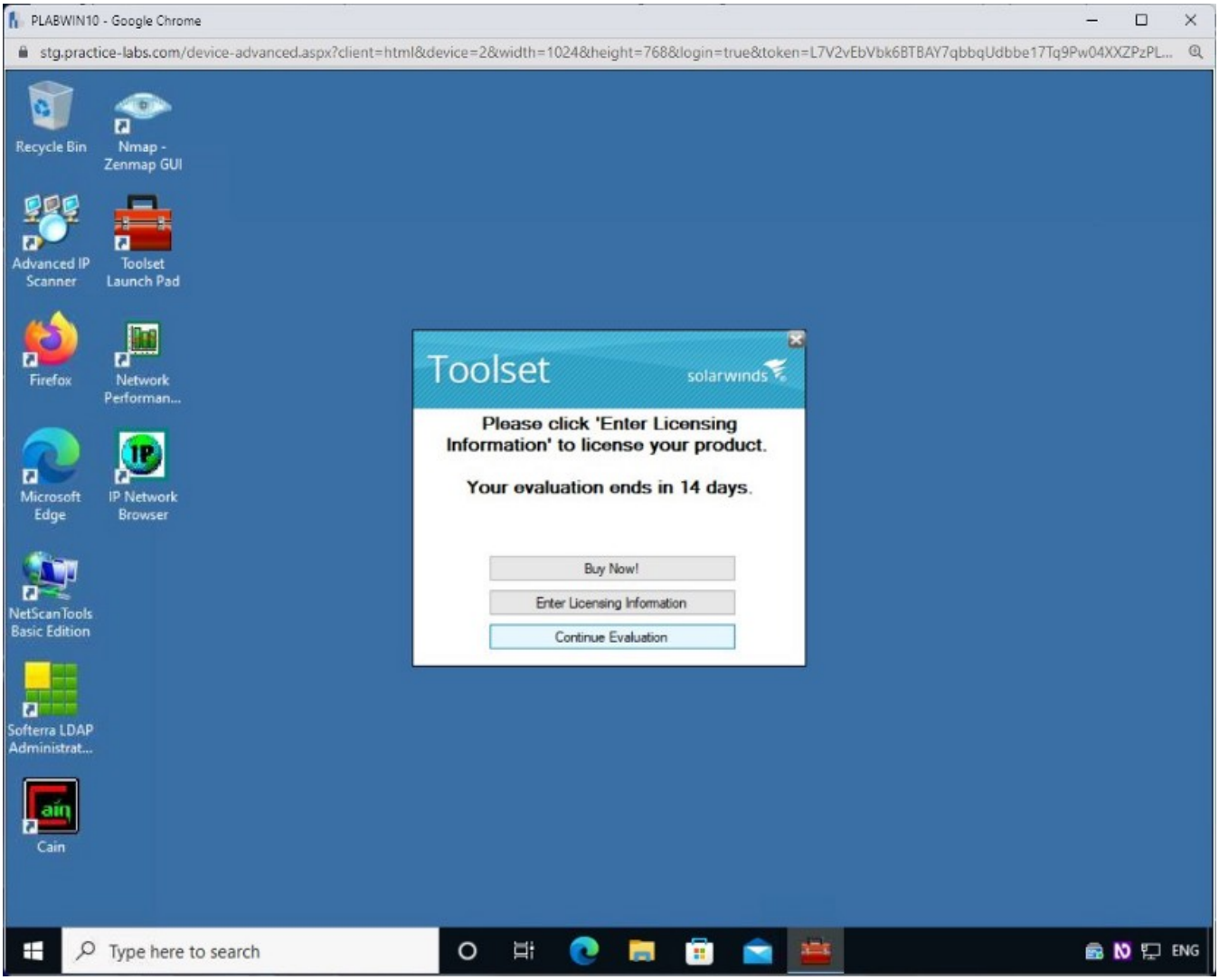
From the search results, click **Toolset Launch Pad**.



Step 2

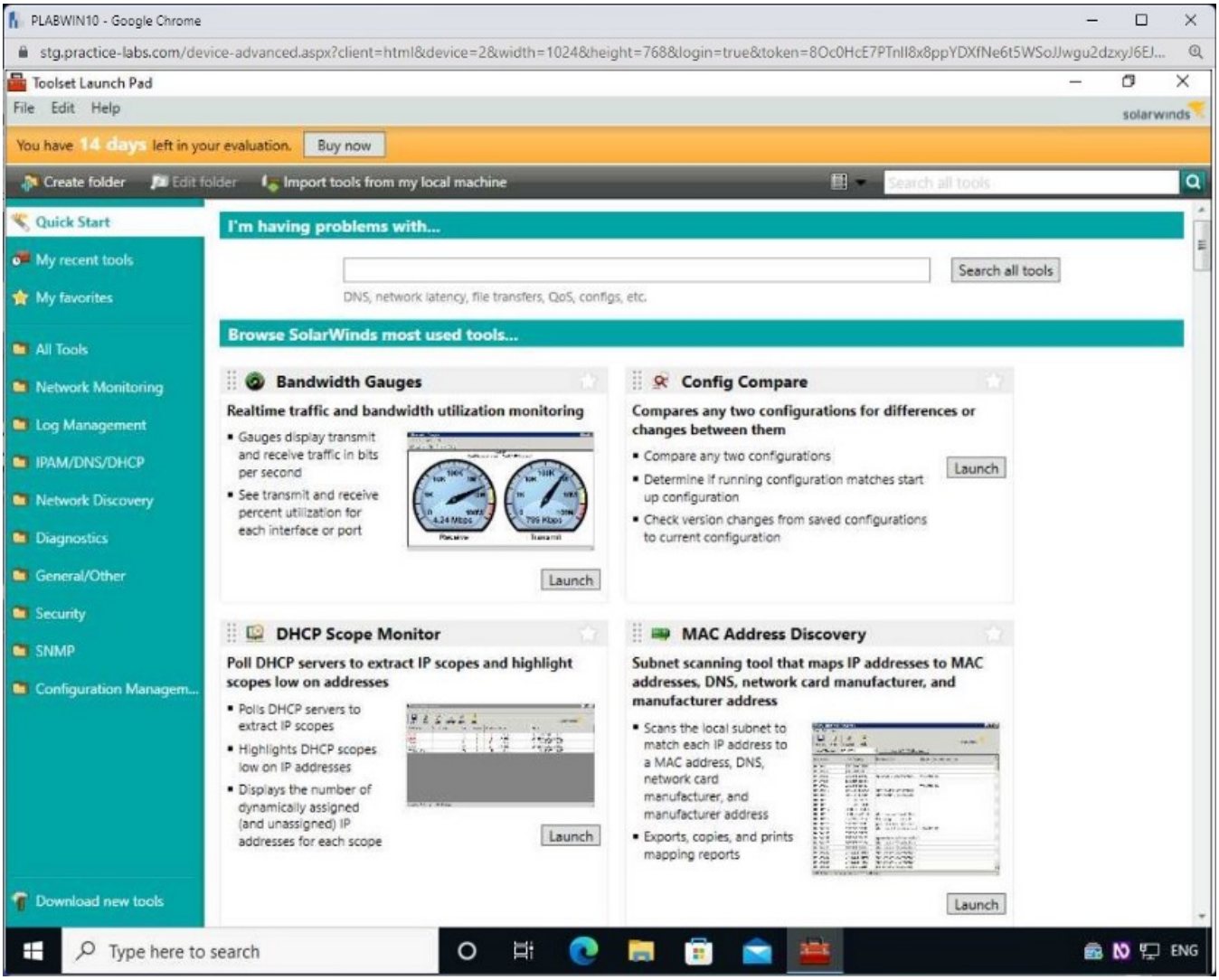
The **Toolset** dialog box is displayed.

Click **Continue Evaluation**.



Step 3

The **Toolset Launch pad** is displayed

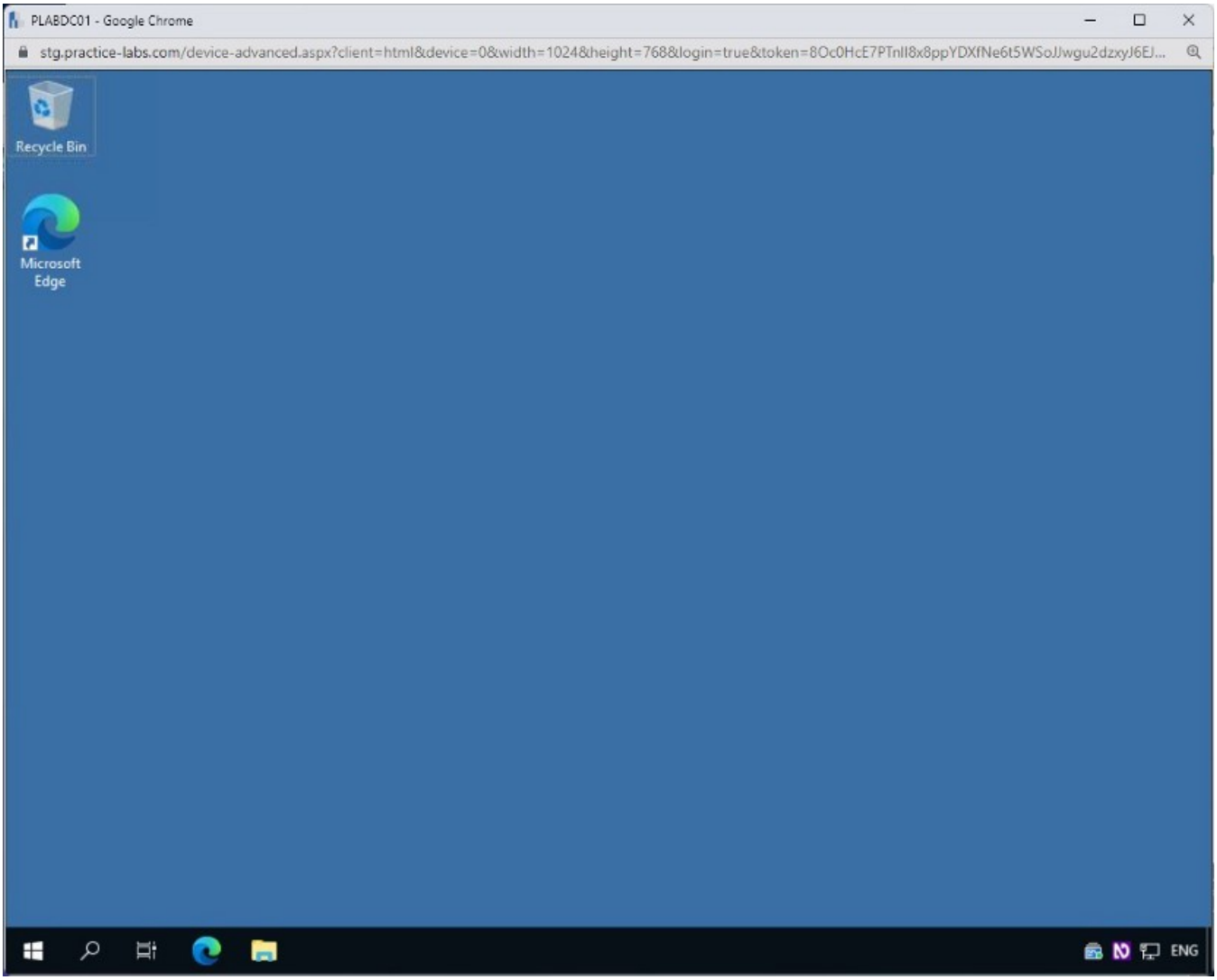


Step 4

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

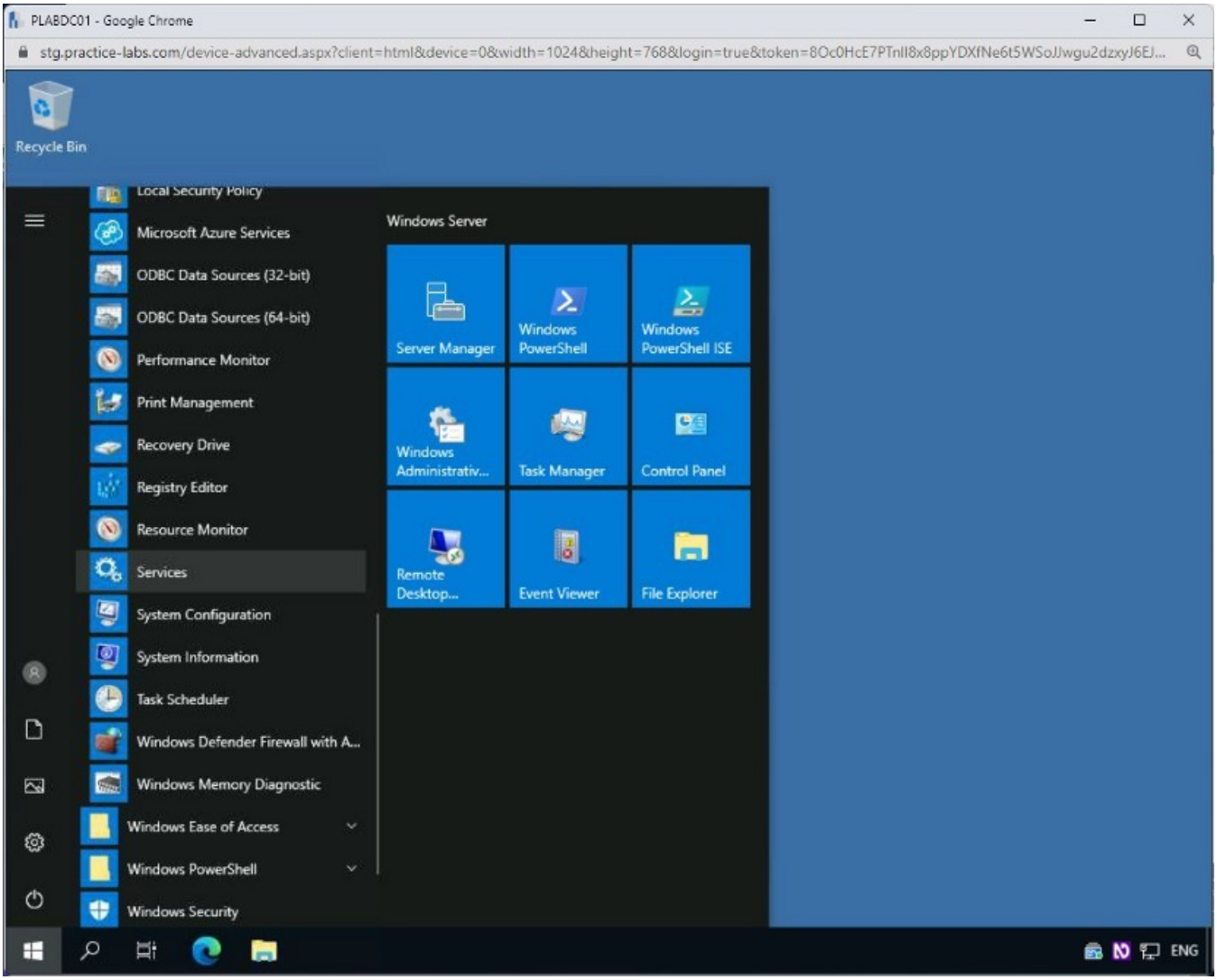
In this task, you will configure **PLABDC01** for accepting the requests.

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



Step 5

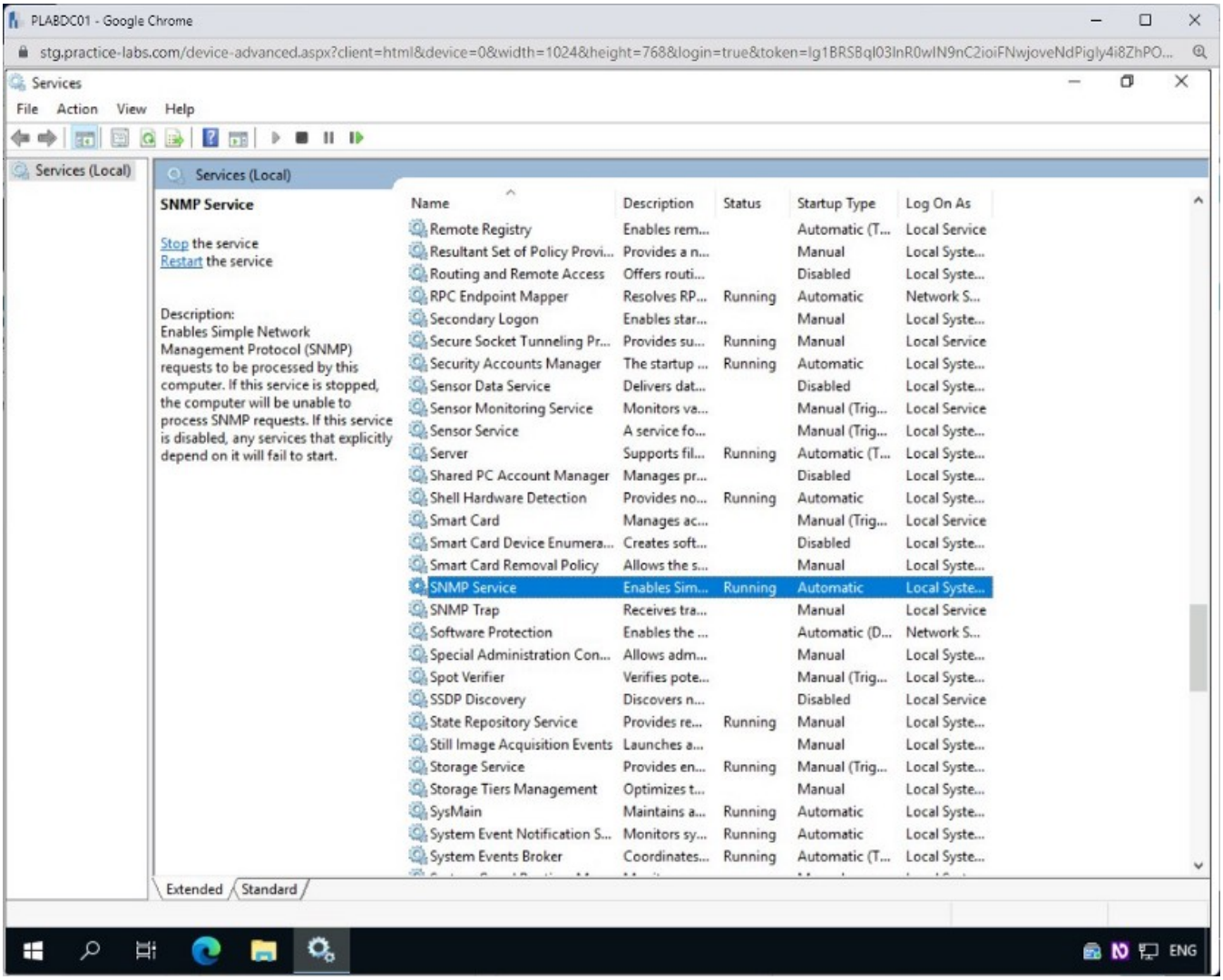
Click the **Start charm**, click **Windows Administrative Tools**, and select **Services**.



Step 6

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

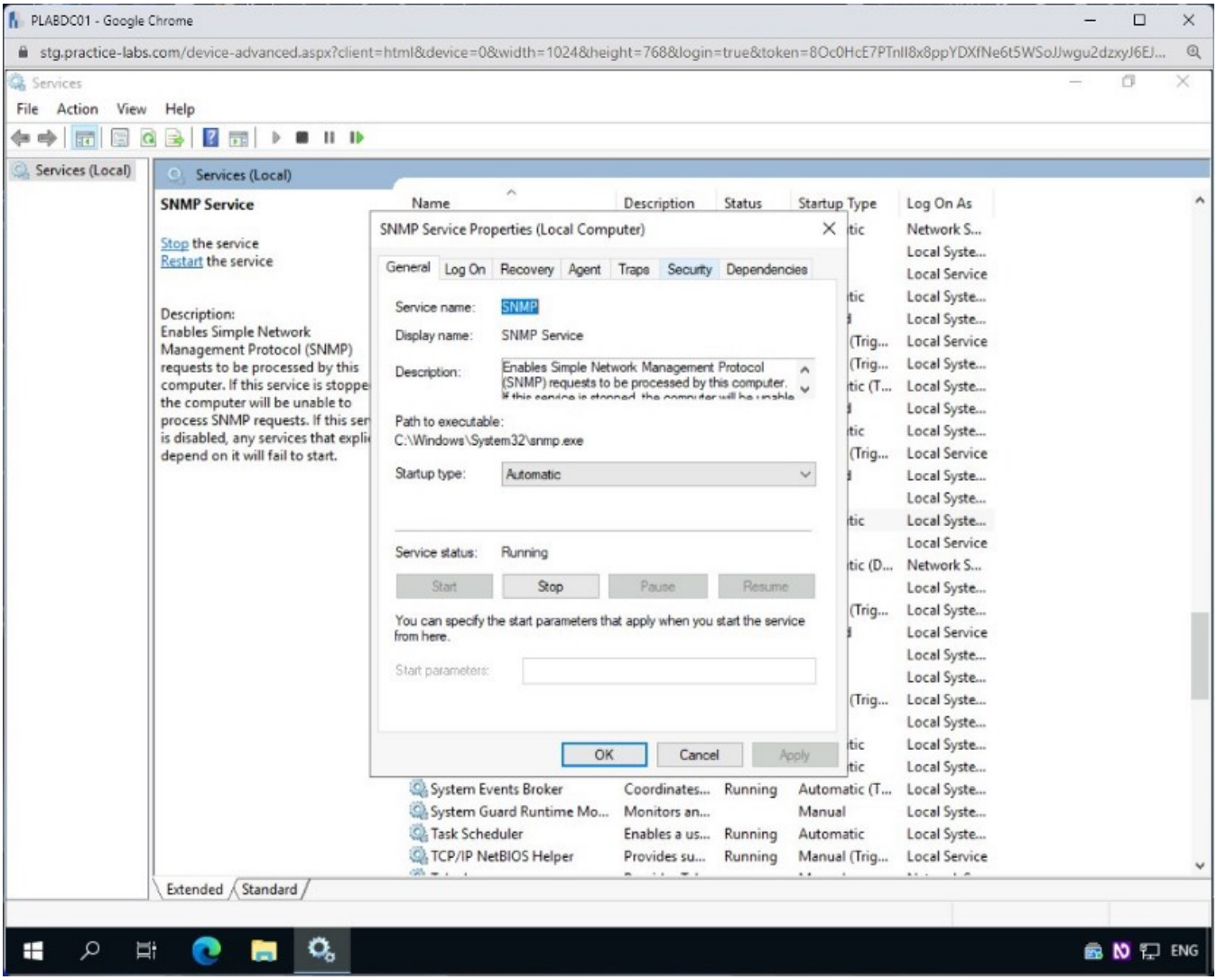
Scroll down and Double-click **SNMP Service**.



Step 7

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

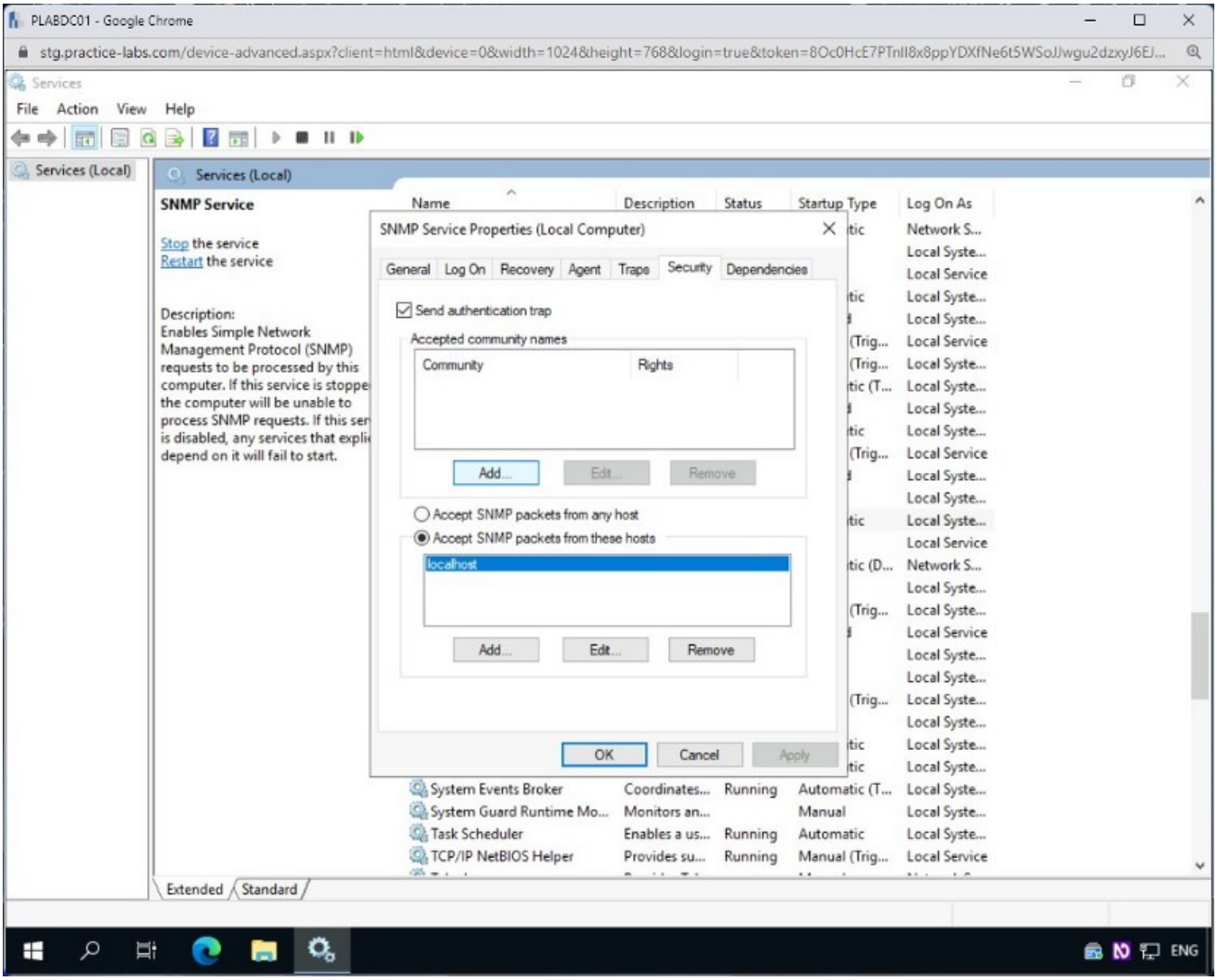
Click the **Security** tab.



Step 8

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.



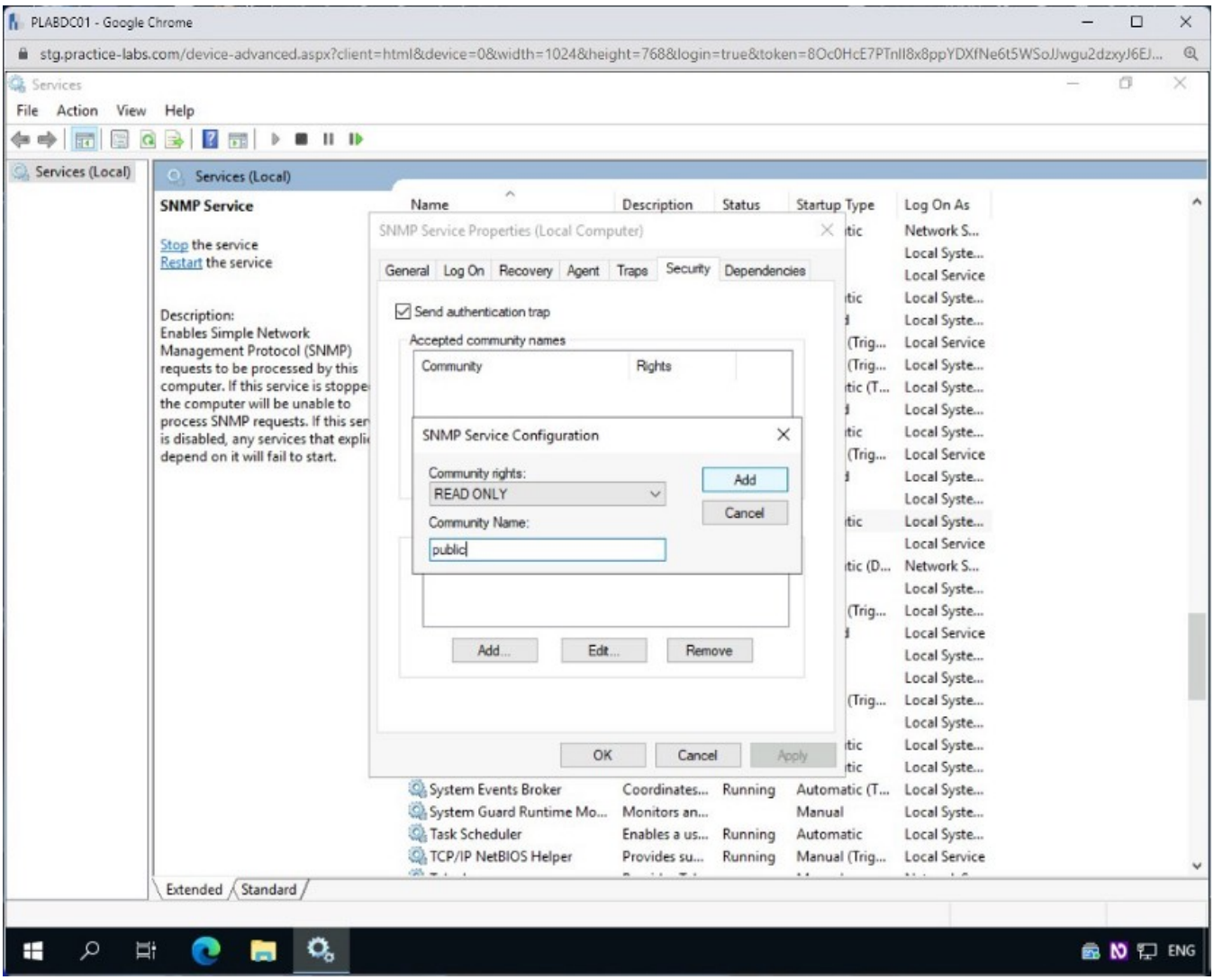
Step 9

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

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

```
public
```

Click **Add**.

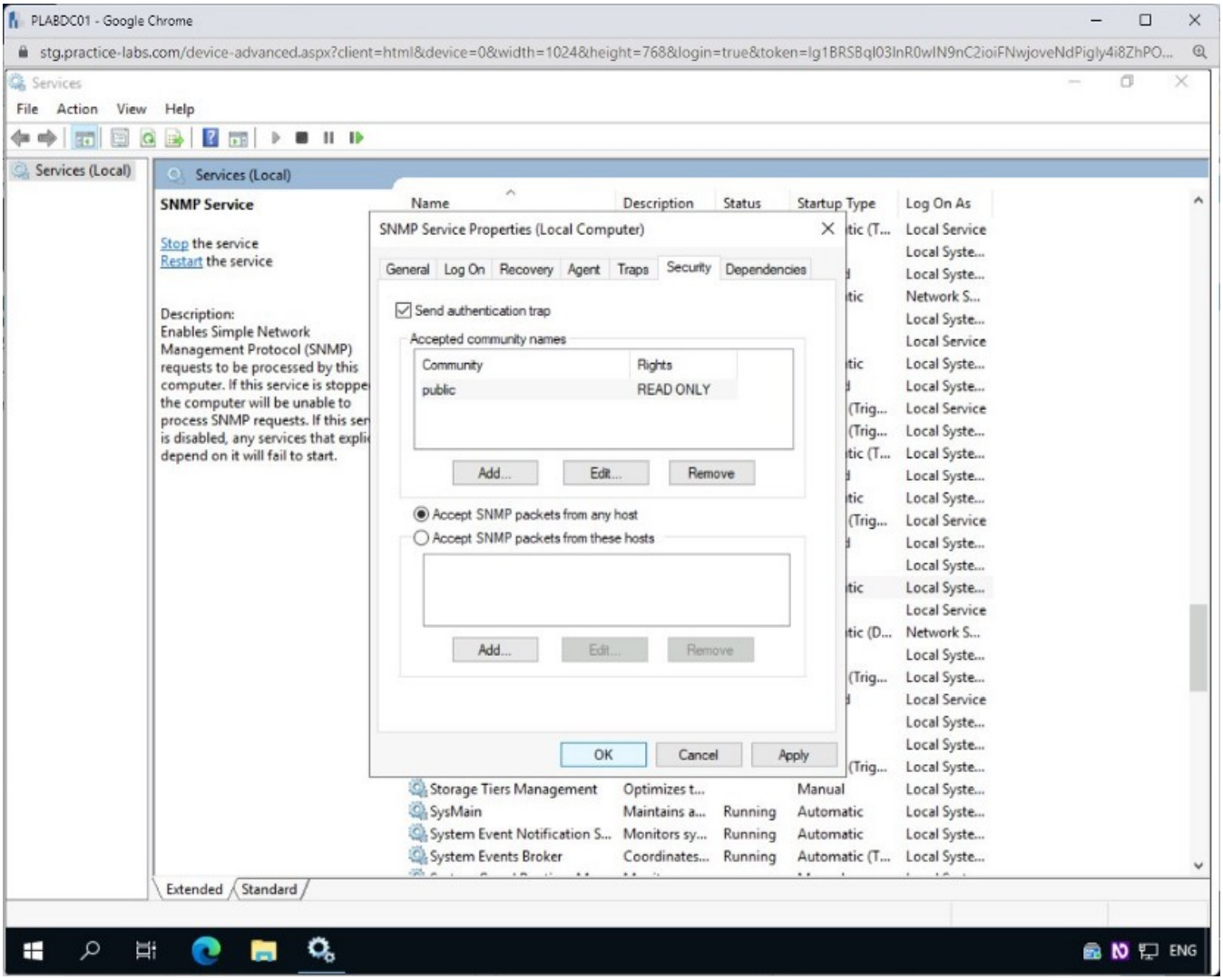


Step 10

Notice that the community public appears in the **Accepted community names** section.

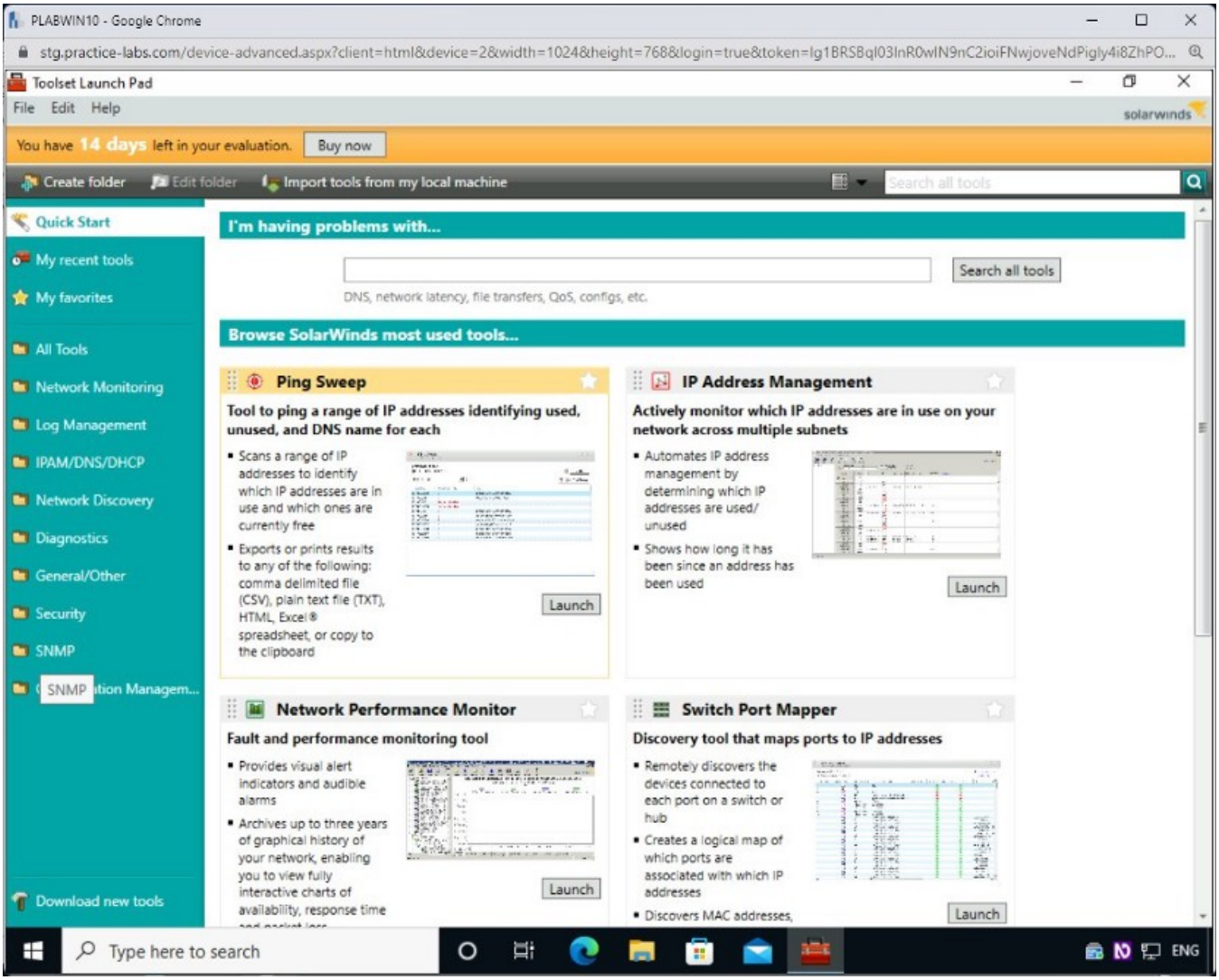
Select **Accept SNMP packets from any host** and click **OK**.

Close the **Services** window.



Step 11

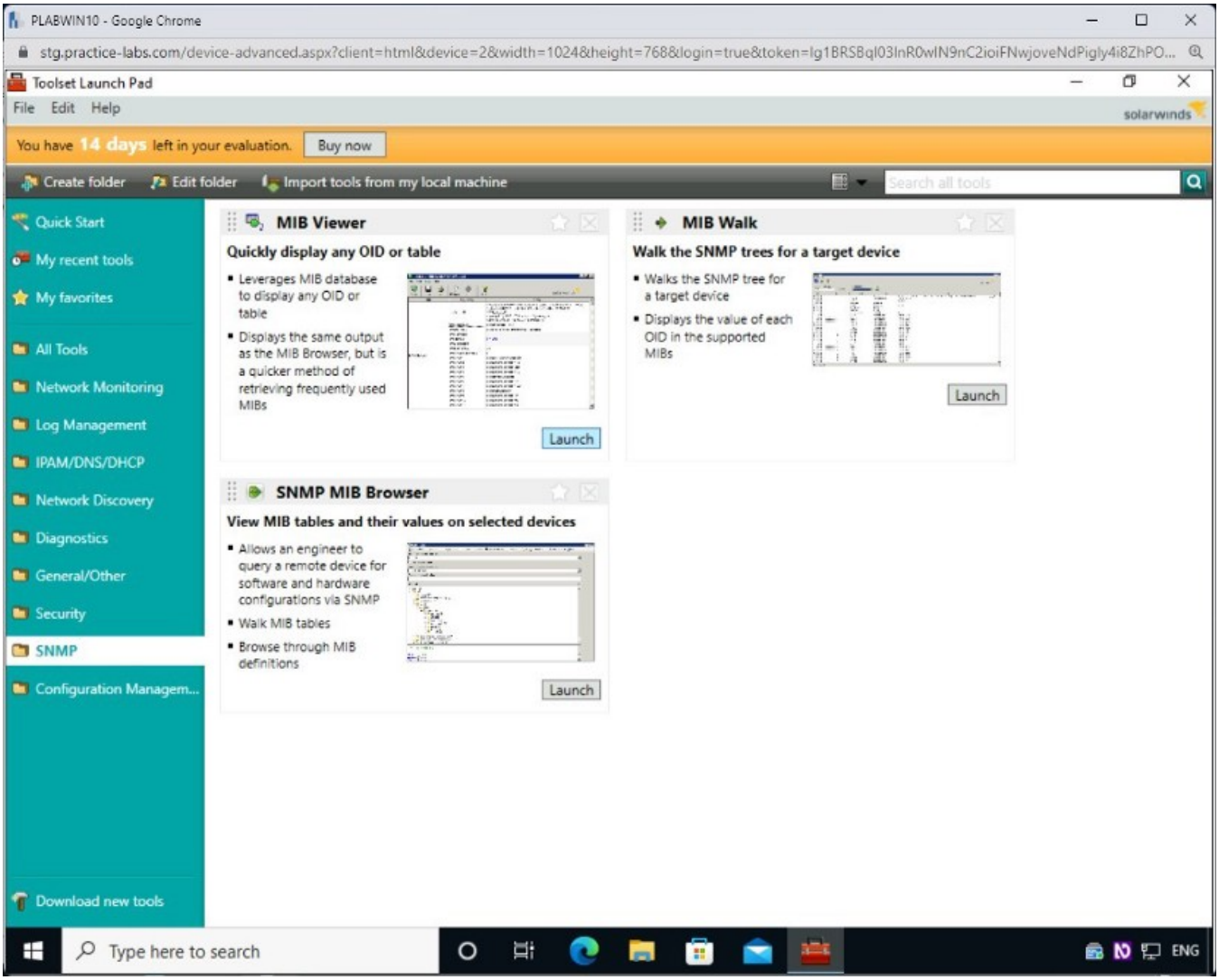
Connect to **PLABWIN10** and click **SNMP** in the left pane.



Step 12

The right pane lists several SNMP-related tools.

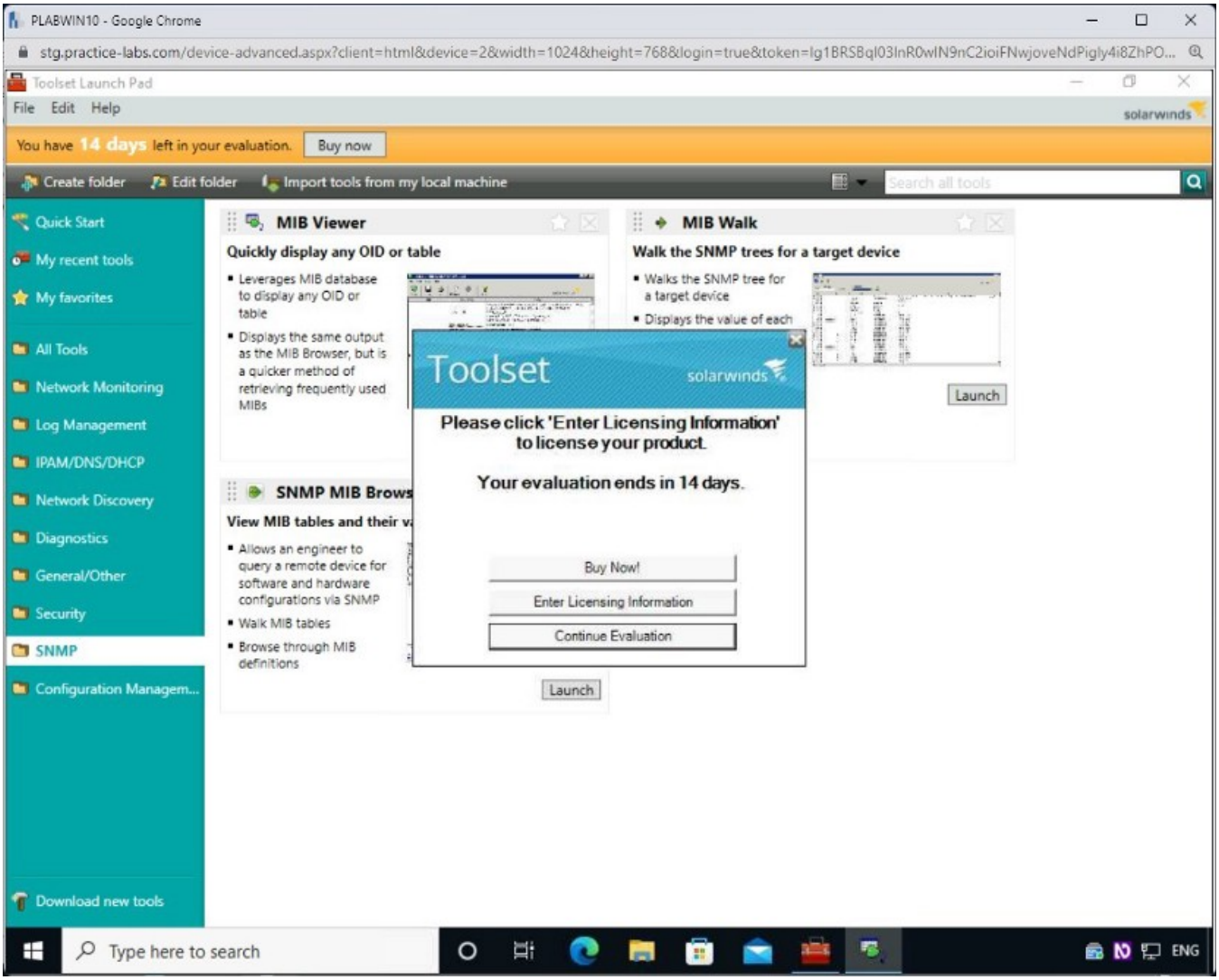
Click **Launch** under **MIB Viewer**.



Step 13

The **Toolset** dialog box is displayed.

Click **Continue Evaluation**.



Step 14

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

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

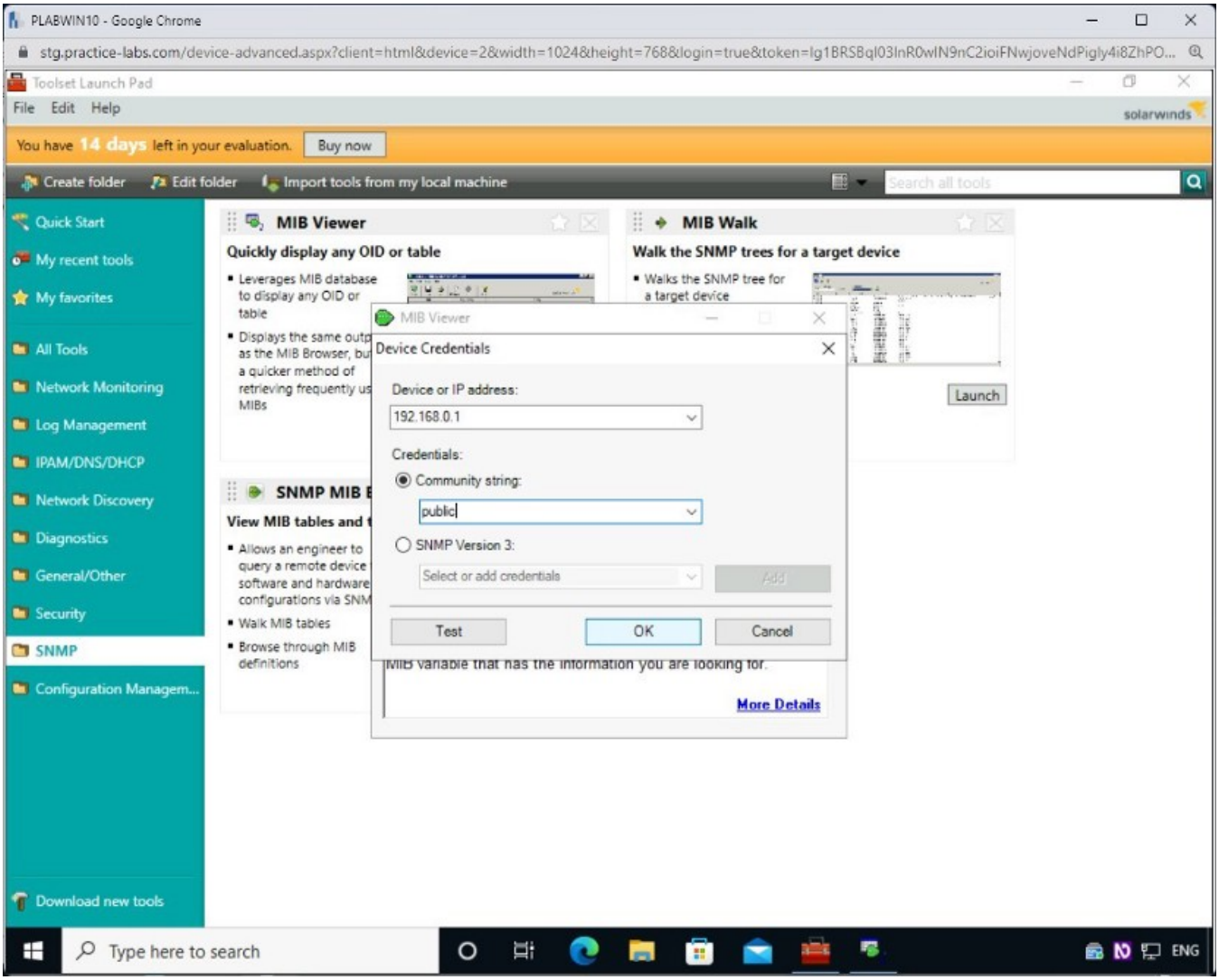
The **Device Credentials** dialog box is displayed. in the **Device or IP address** drop-down, enter:

```
192.168.0.1
```

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

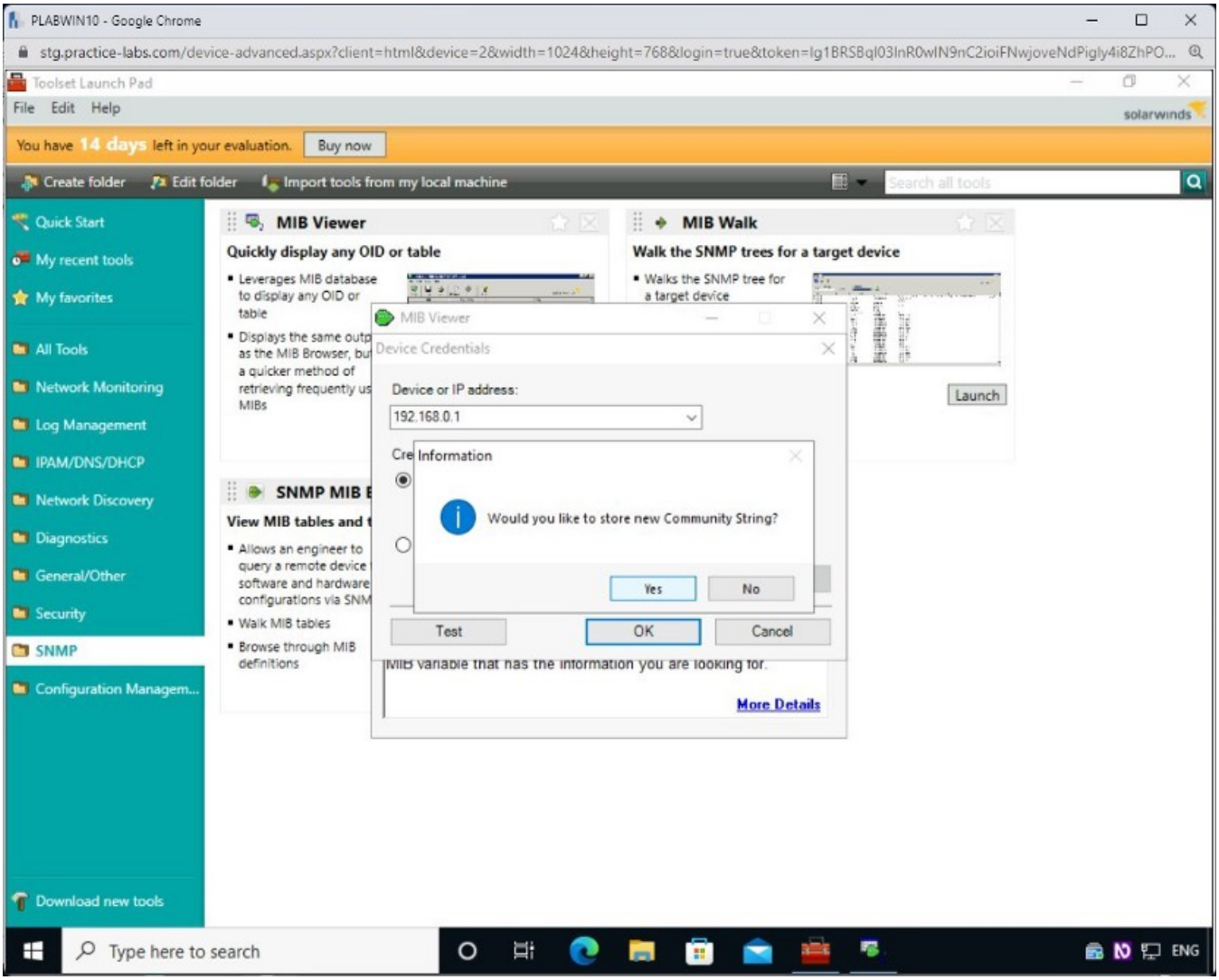
```
public
```

Click **OK**.



Step 15

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

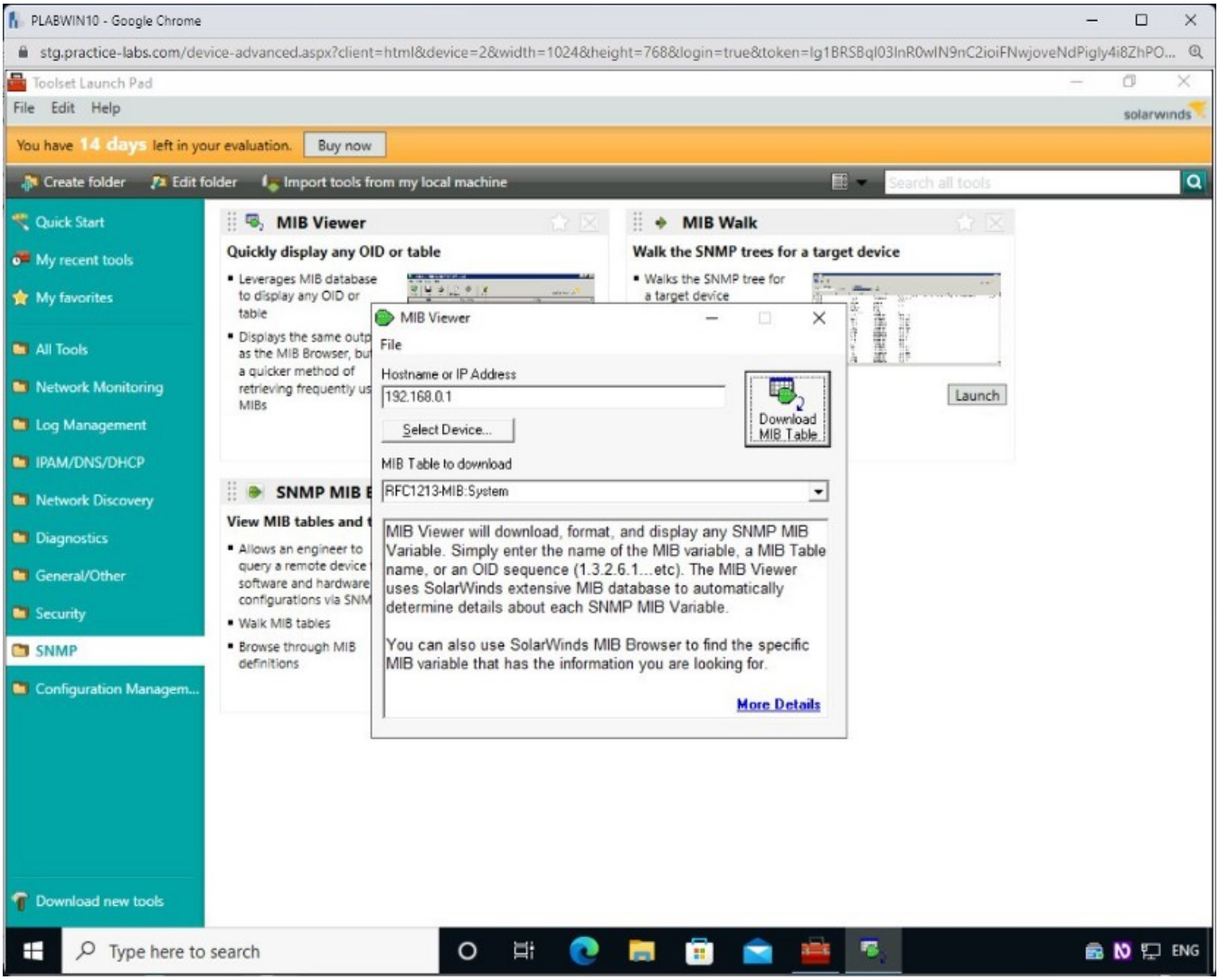


Step 16

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

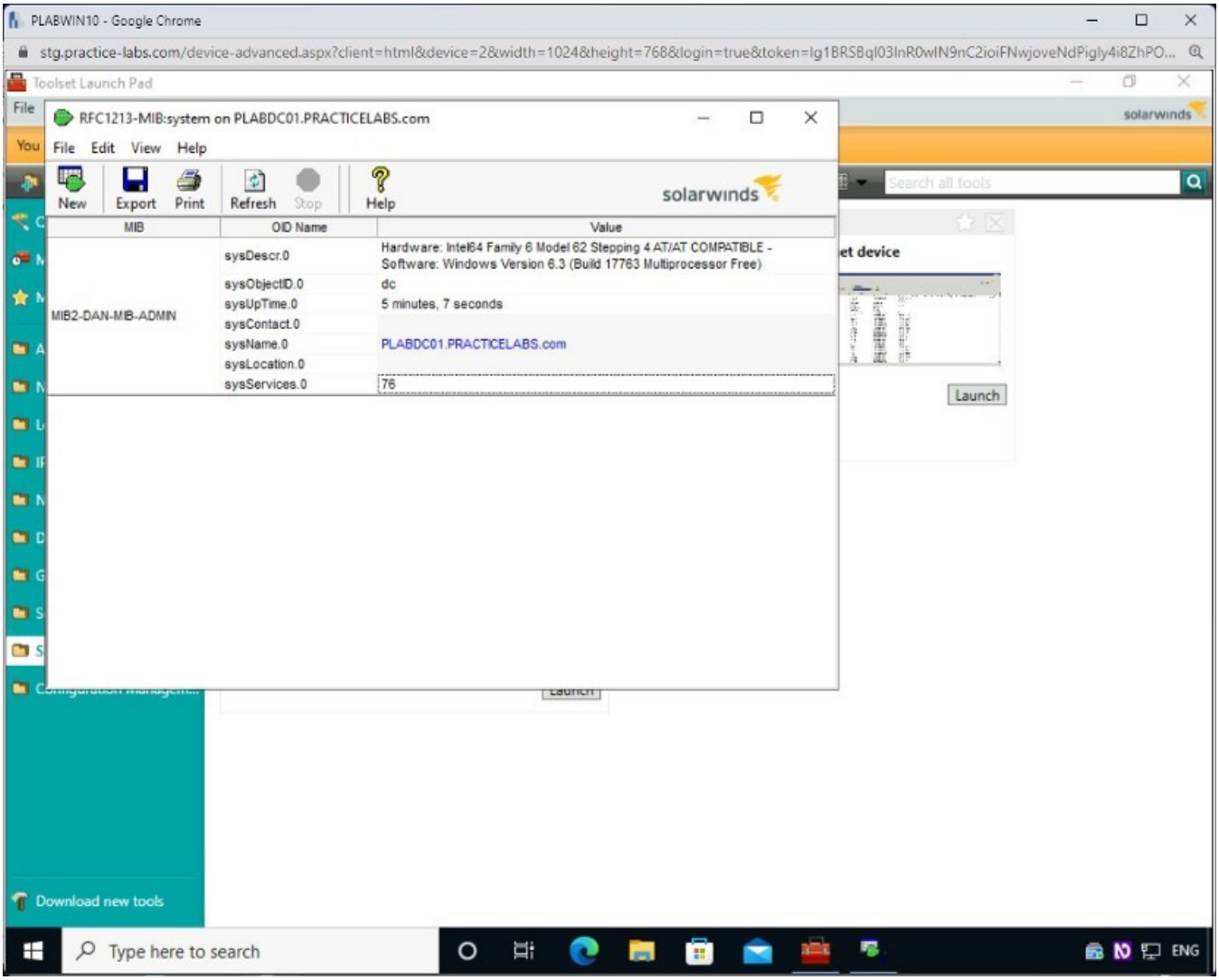
From the **MIB Table to download** drop-down, select any of the given **MIB** Table names.

Click **Download MIB Table**.



Step 17

The **RFC1213-MIB:system** dialog box is displayed, which displays information on the scanned network.



Close all open windows.

Task 3 — Perform SNMP Enumeration Using Snmp-check

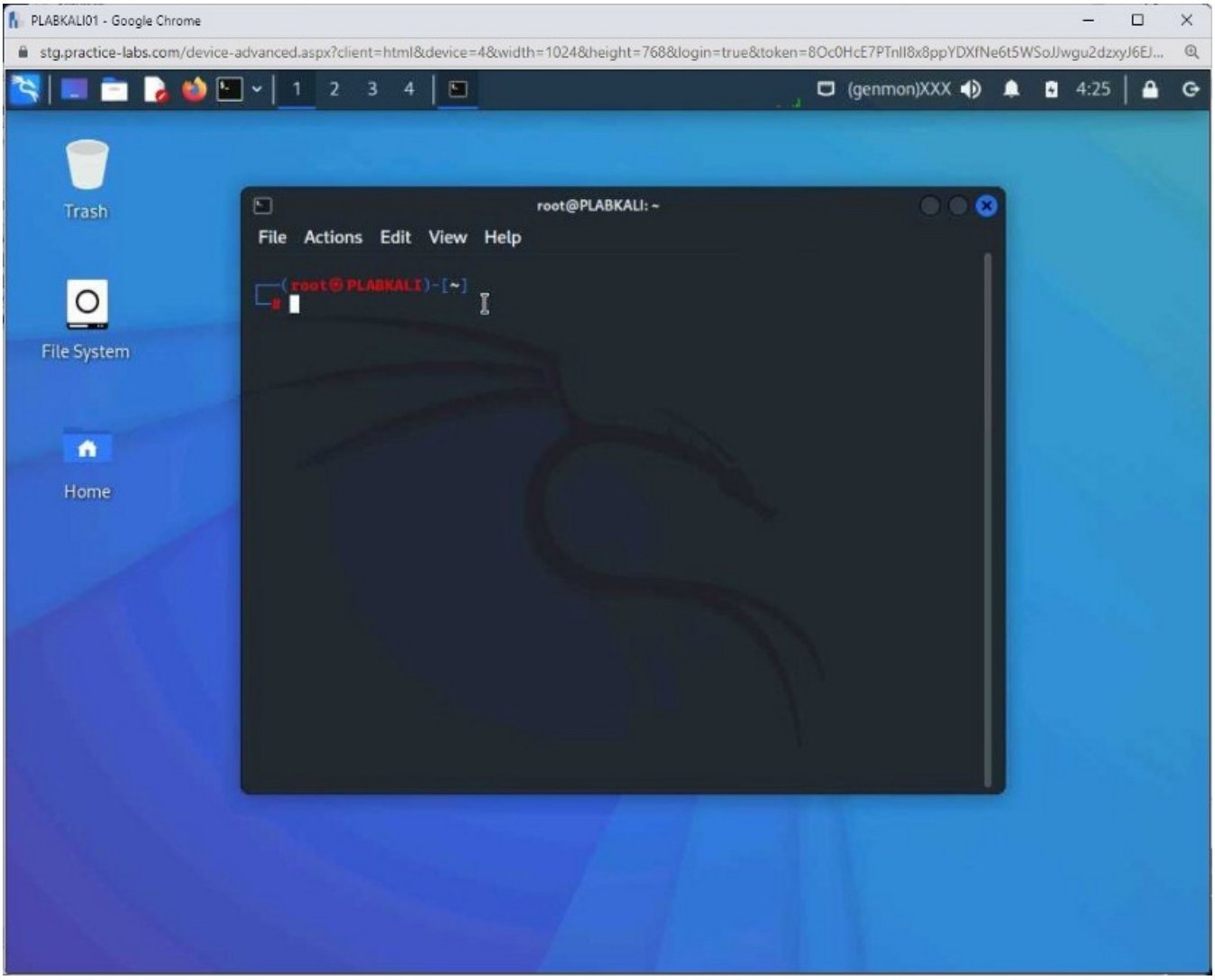
Snmp-check is a tool that is readily available in Kali Linux. Snmp-check is designed to enumerate the devices and systems running the SNMP service. It can collect a great deal of information in a readable format. Some of the key information it can collect is:

- System information including name, IP address, hardware details, uptime, and domain name
- User accounts
- Network information, such as IP forwarding enabled or not, TCP segments sent and received, and default TTL
- Network interfaces

In this task, you will learn to perform SNMP enumeration using snmp-check.

Step 1

Connect to **PLABKALI01** and open a new terminal window.



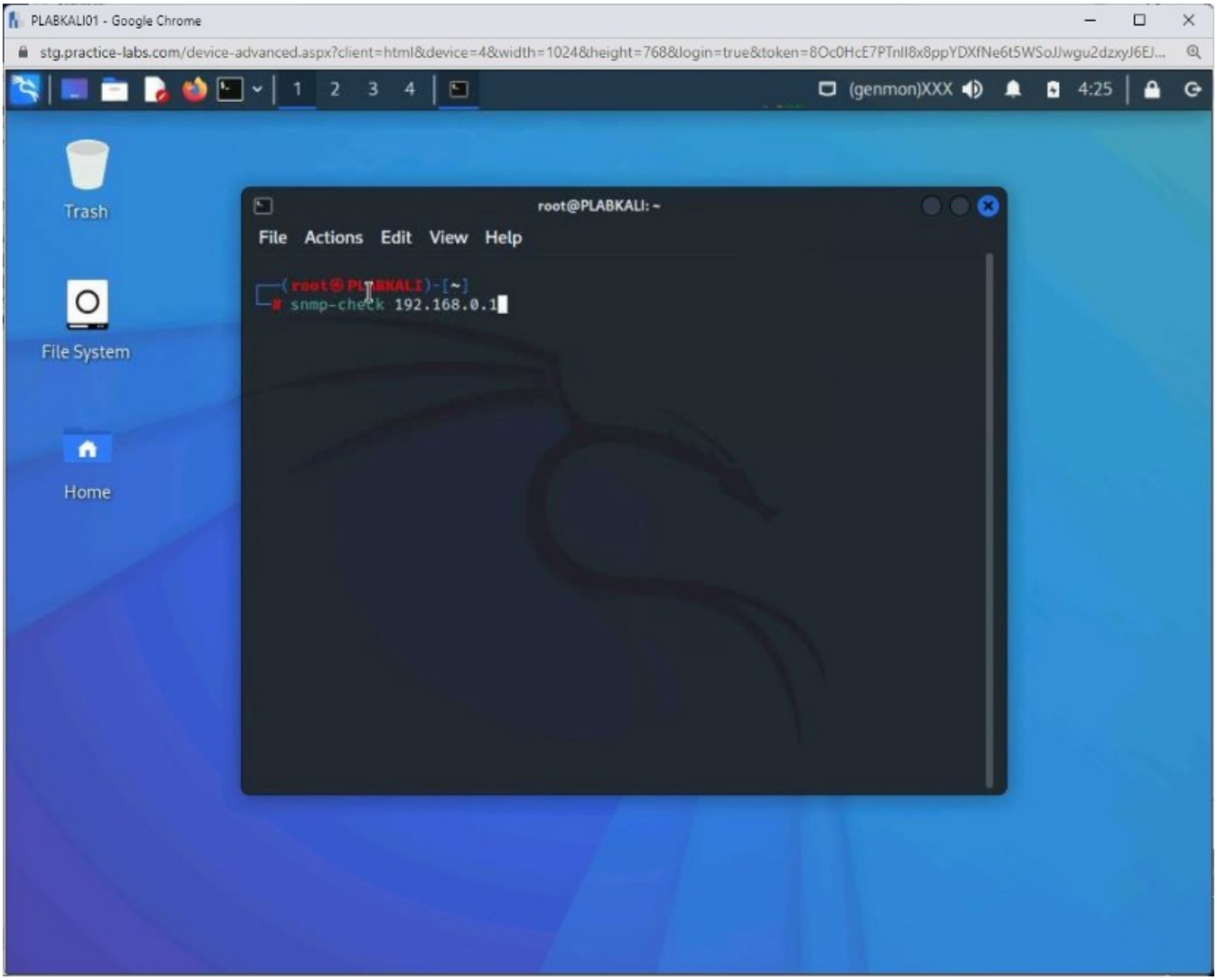
Step 2

The **snmp-check** command is simple. You have to provide the remote system name on which you want to perform SNMP enumeration.

Type the following command:

```
snmp-check 192.168.0.1
```

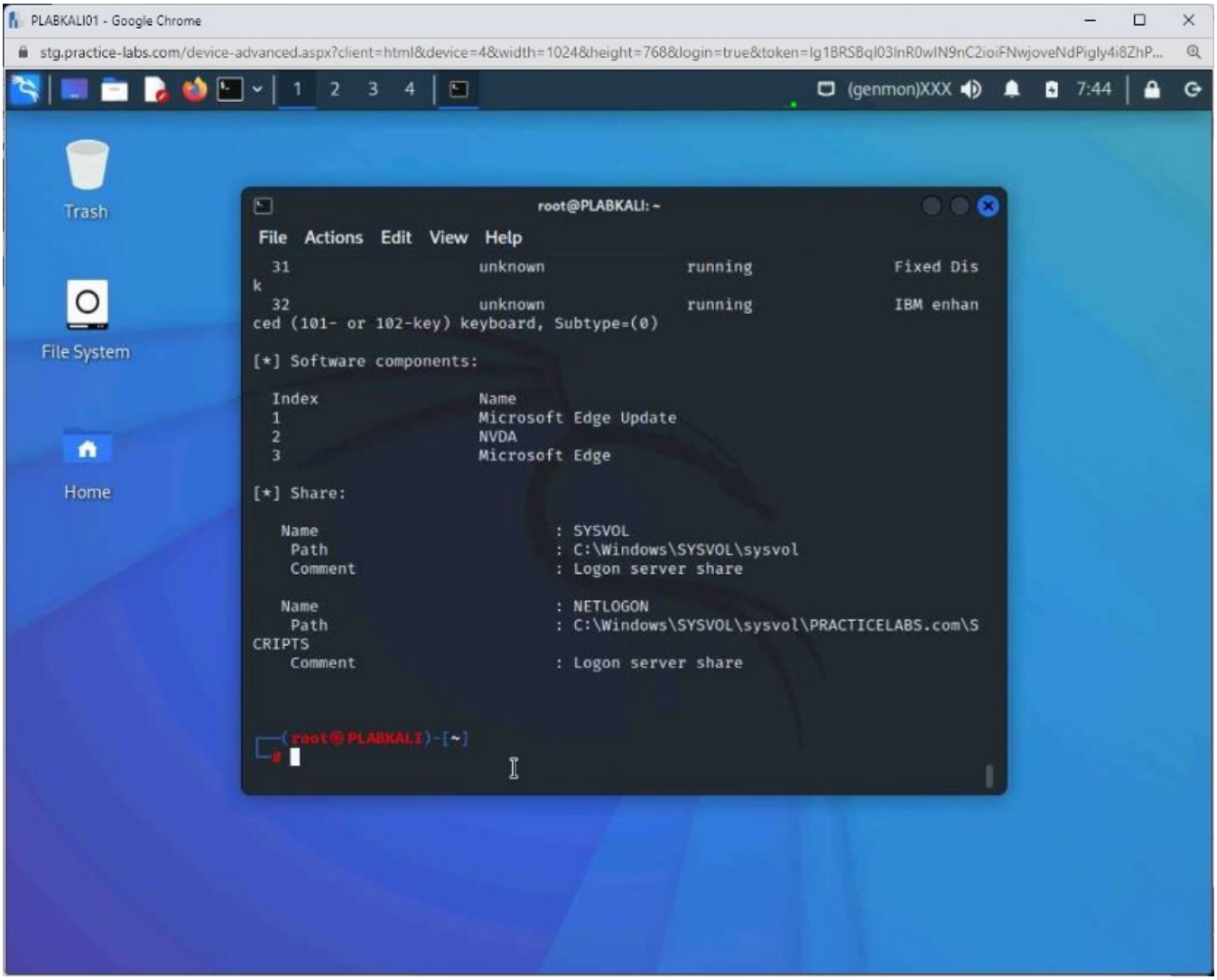
Press **Enter**.



Step 3

The command executes, and output is displayed.

Notice that the last section is **Share** that contains the shares on **PLABDC01**.



Step 4

Scroll up, and you will find several sections, such as:

- Network Services
- Processes
- Storage Information
- File system information
- Device information

Exercise 4 — LDAP Enumeration

The Lightweight Directory Access Protocol (LDAP) is used for accessing the directory services. LDAP accesses the Active Directory within the Windows environment to provide the directory listing. An attacker can enumerate LDAP and gain access to the information within it. Active Directory contains information about users, computers,

groups, and organizational units. The attacker can get access to this information by using querying the database.

In this exercise, you will learn to perform LDAP enumeration.

Learning Outcomes

After completing this exercise, you will be able to:

- Perform LDAP Enumeration Using Softerra LDAP Administrator

Your Devices

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

PLABDC01Domain Controller192.168.0.1/24PLABWIN10Domain MemberWorkstation192.168.0.3/24PLABKALI01Domain MemberWorkstation192.168.0.5/24PLABDM01Domain Member Server192.168.0.2/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABDM01

Windows Server 2019 — Domain Member192.168.0.2/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

Task 1 — Perform LDAP Enumeration Using Softerra LDAP Administrator

Softerra LDAP Administrator is a tool you can use for various LDAP directories. It works well with Active Directory and can also be used with Novell Directory Services. Even though it is an LDAP management tool, attackers can use it for user enumeration.

In this task, you will perform LDAP enumeration using Softerra LDAP Administrator. To do this, perform the following steps:

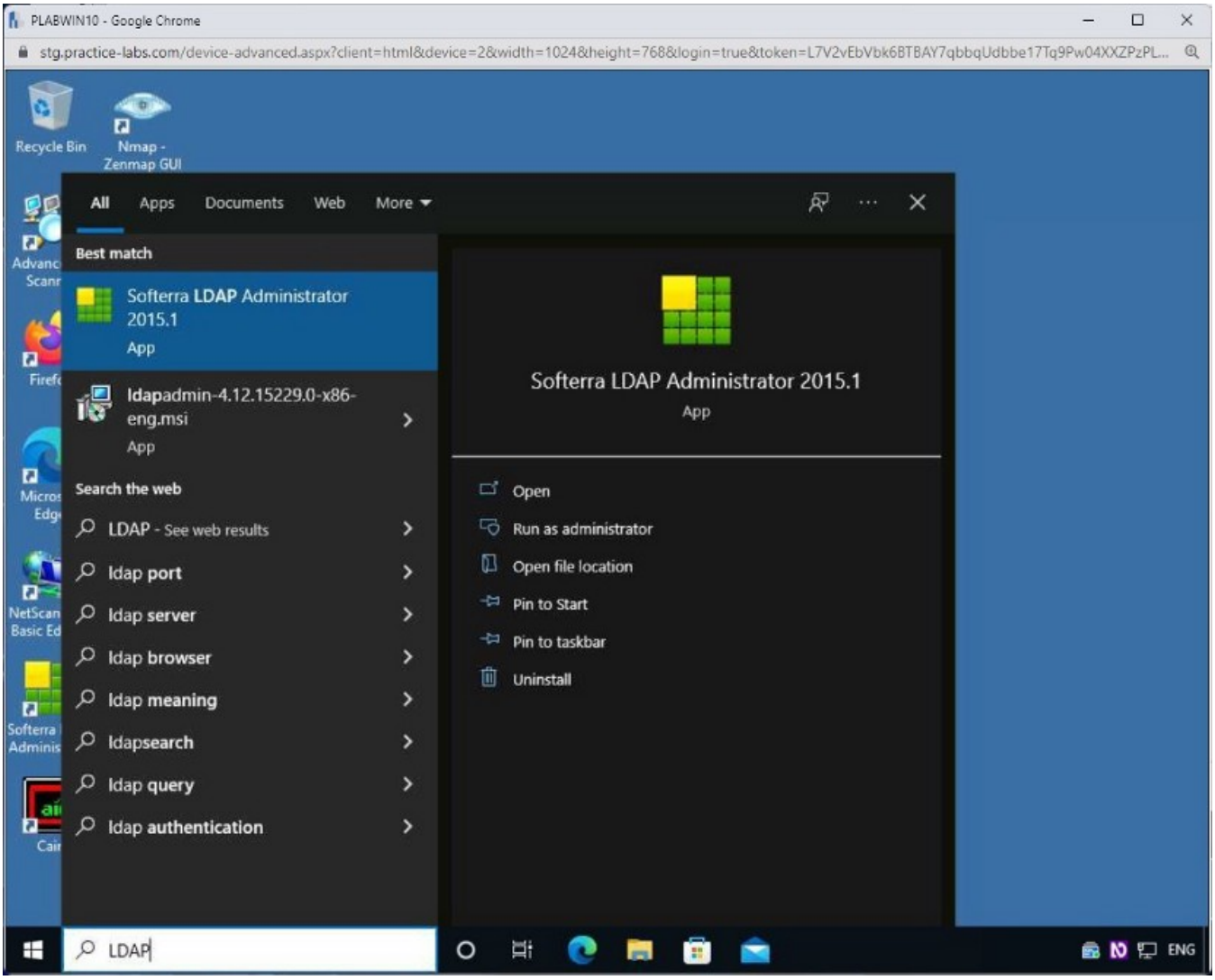
Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABWIN10.**

In the **Type here to search** textbox, type the following:

```
LDAP
```

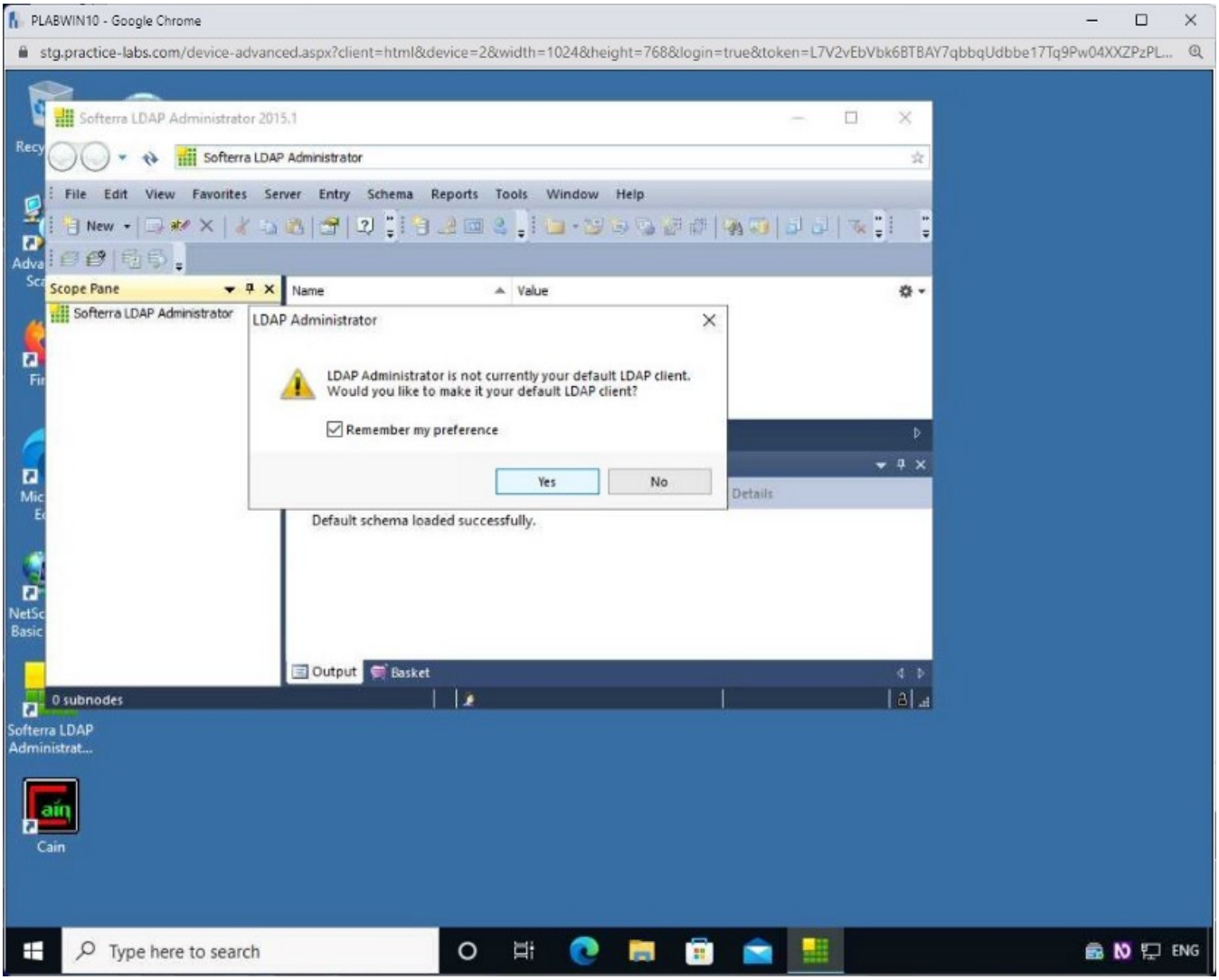
From the search results, click **Softerra LDAP Administrator 2015.1**.



Step 2

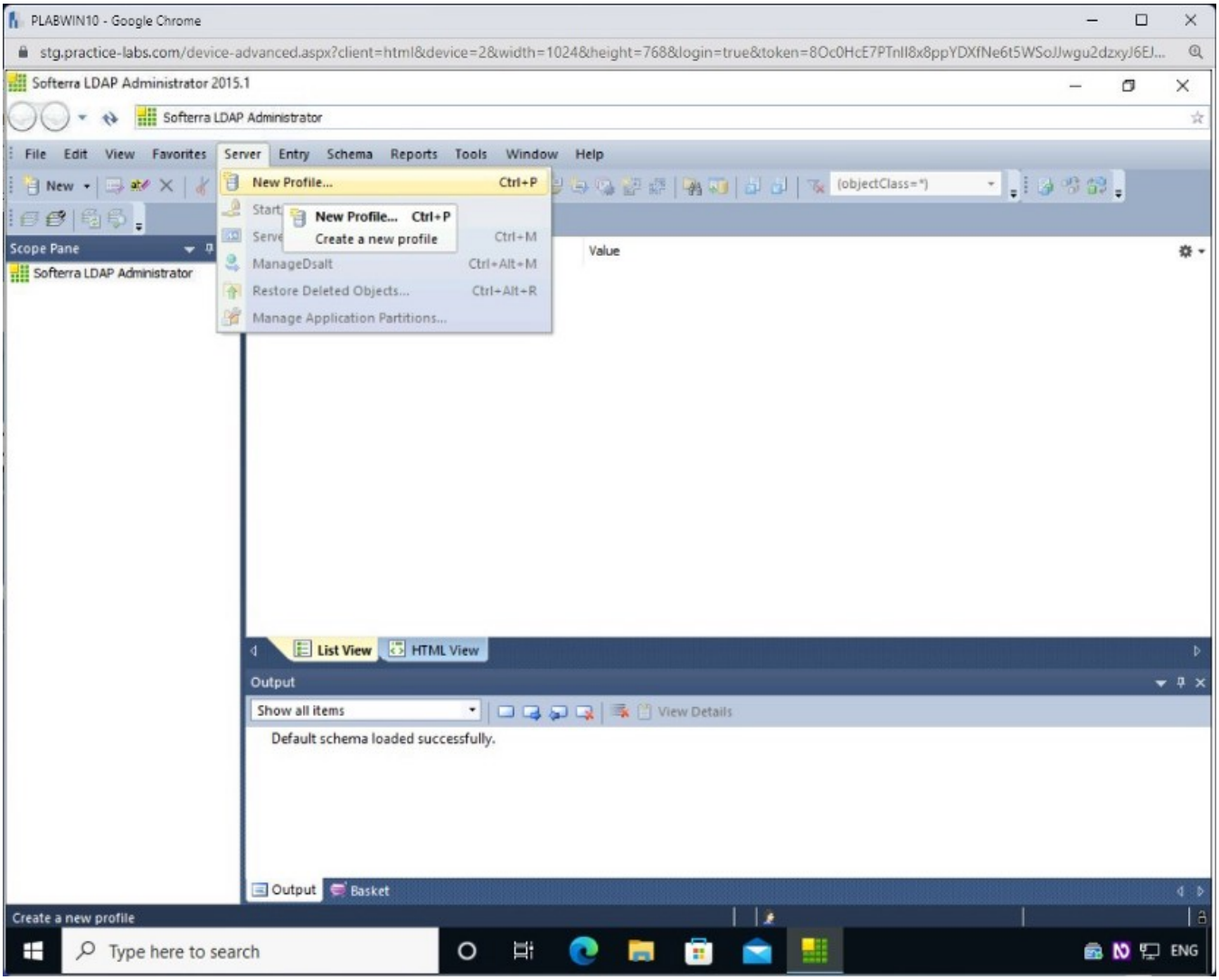
The **Softerra LDAP Administrator 2015.1** window is displayed.

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



Step 3

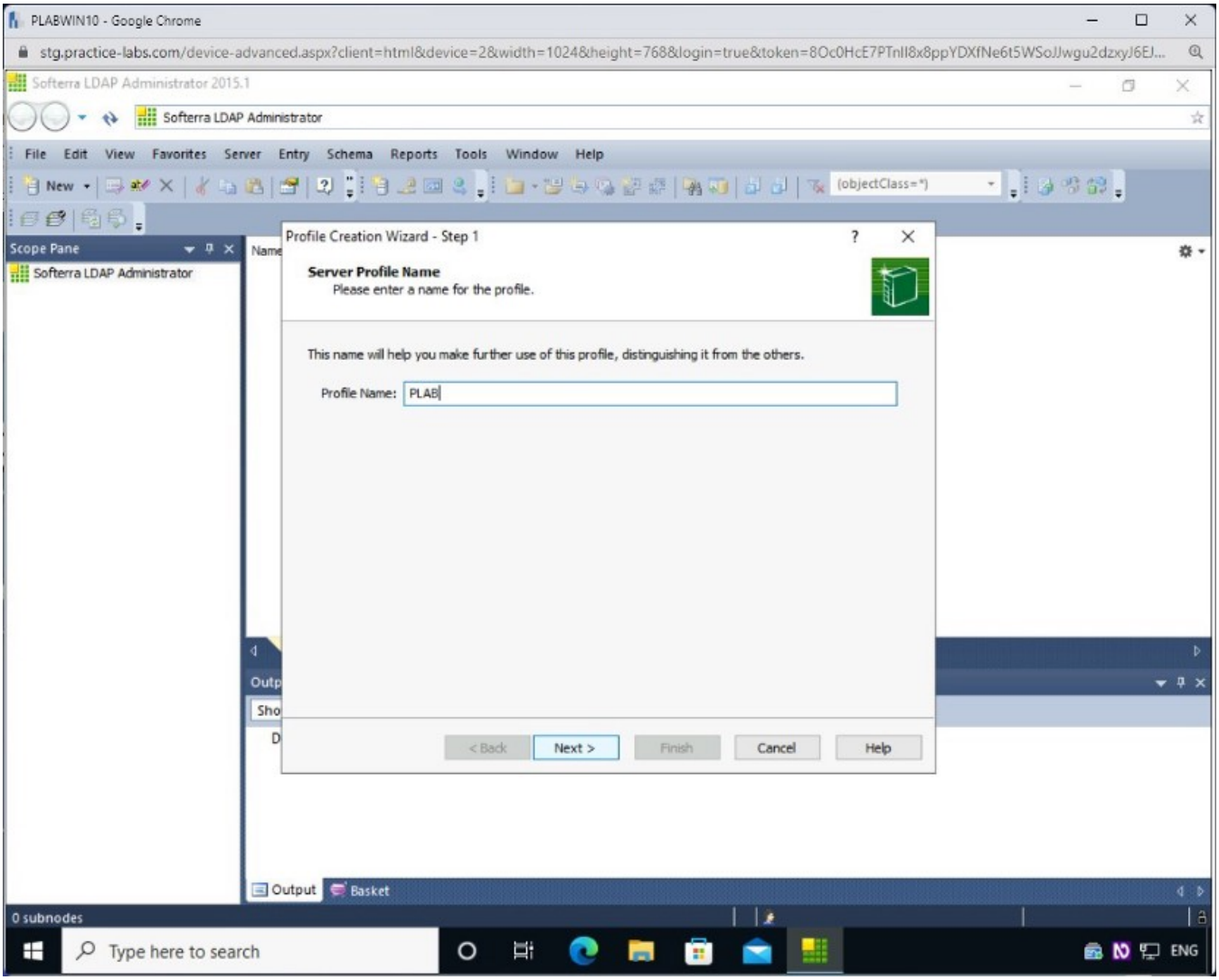
From the top menu bar, click **Server** and select **New Profile**.



Step 4

The **Profile Creation Wizard — Step 1** wizard is displayed.

Enter **PLAB** in the **Profile Name** textbox on the **Server Profile Name** page and click **Next**.

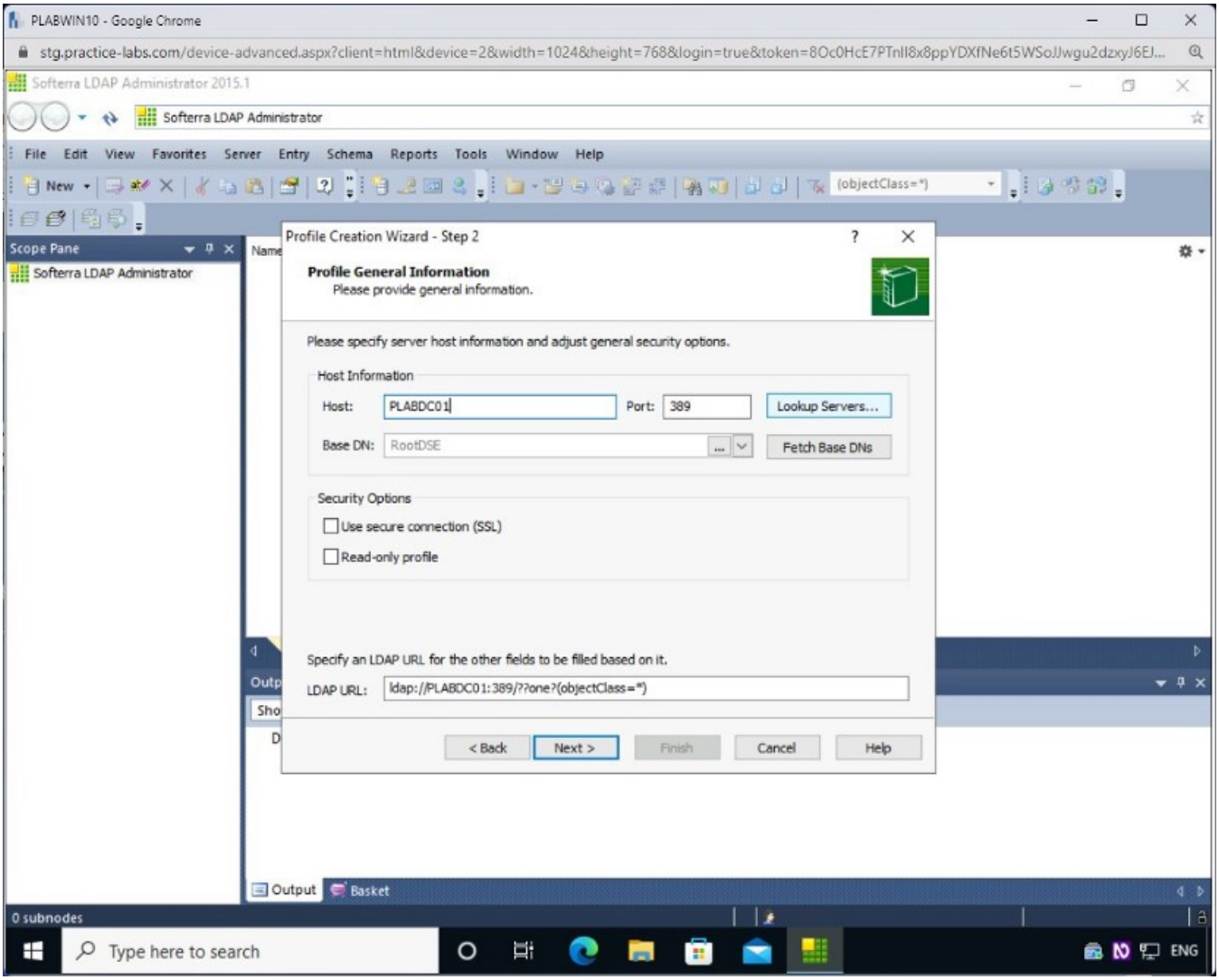


Step 5

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

```
PLABDC01
```

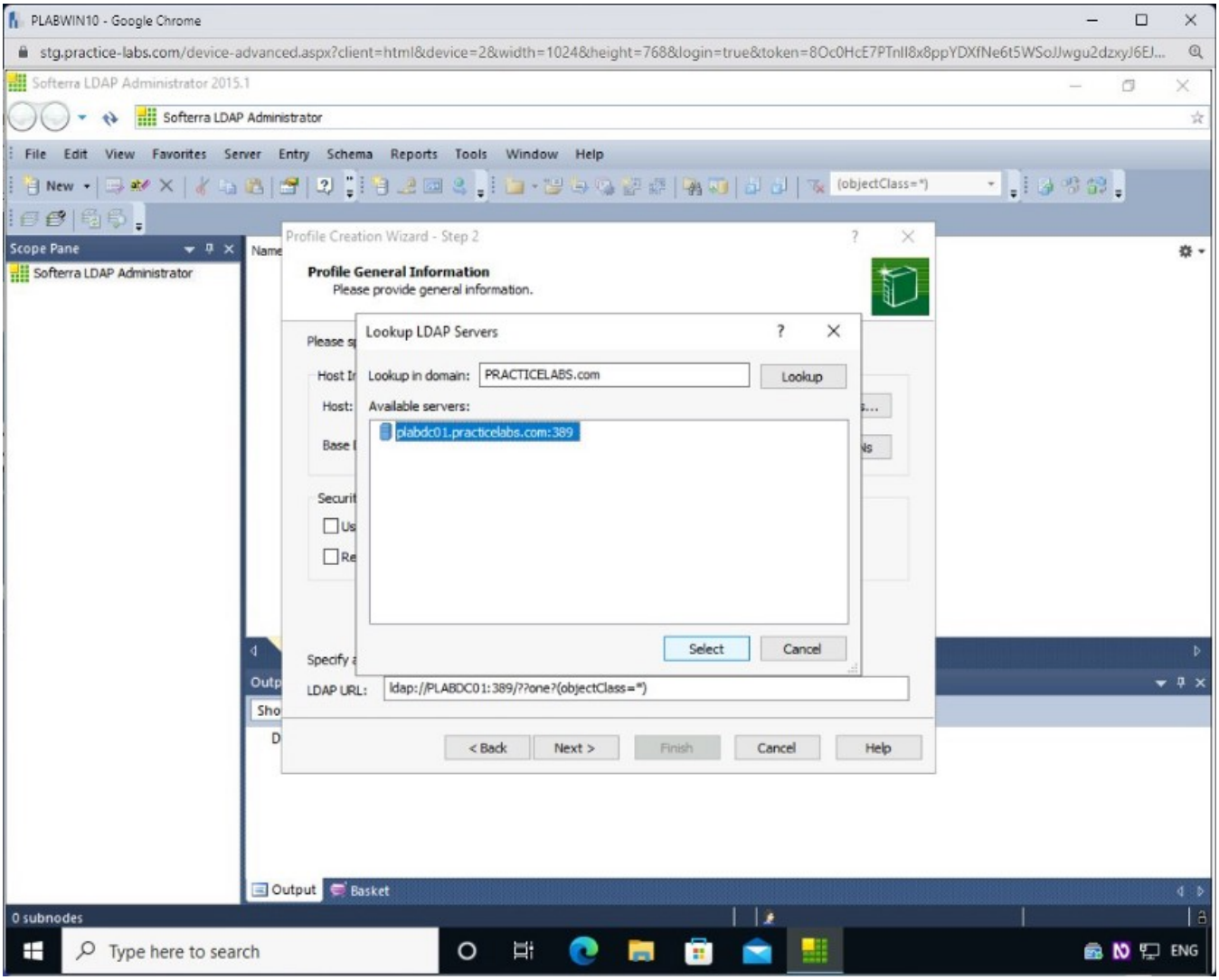
Click **Lookup Servers**.



Step 6

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

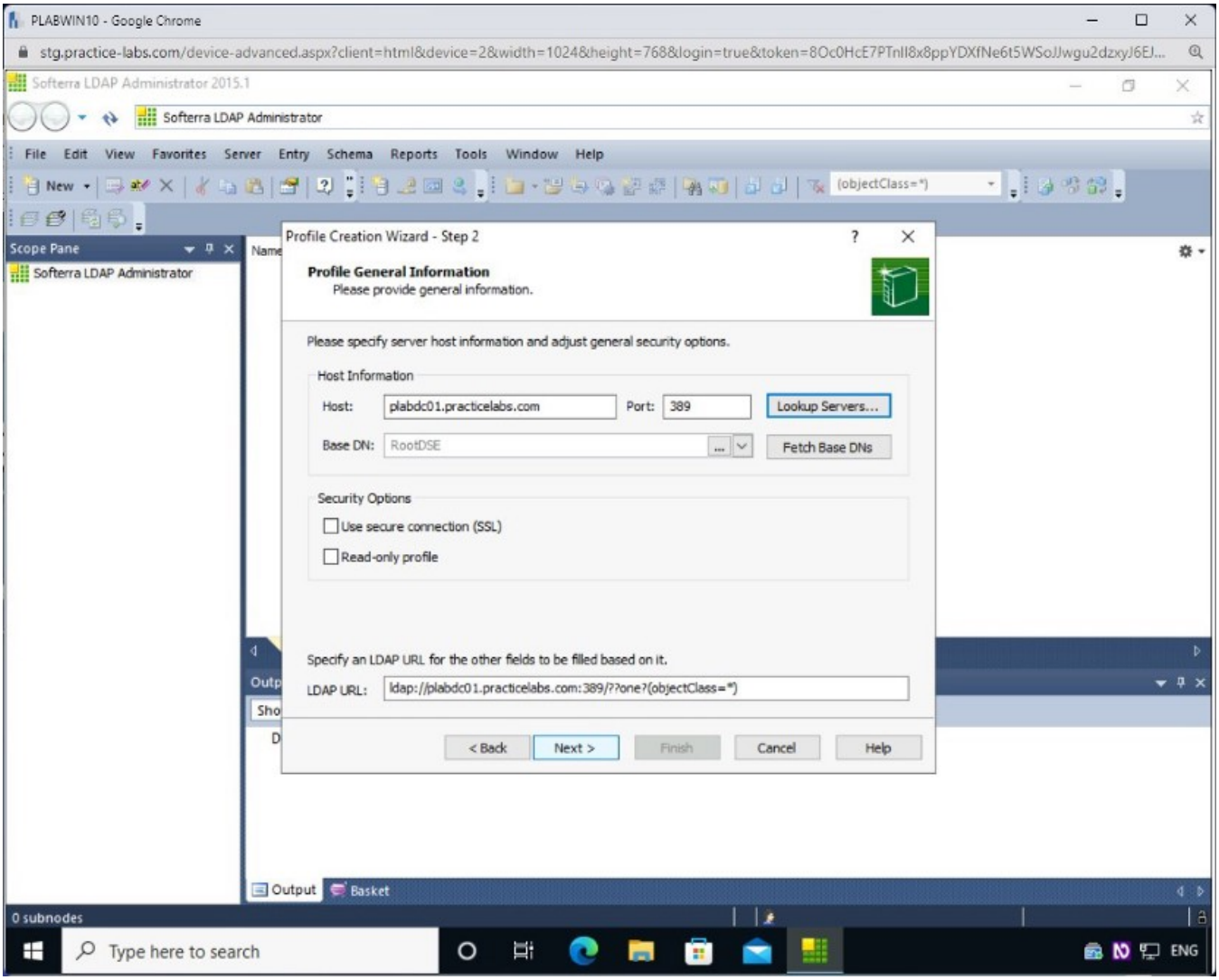
The **Available servers** textbox displays **plabdc01.practicelabs.com:389**.
Select **plabdc01.practicelabs.com:389** and click **Select**.



Step 7

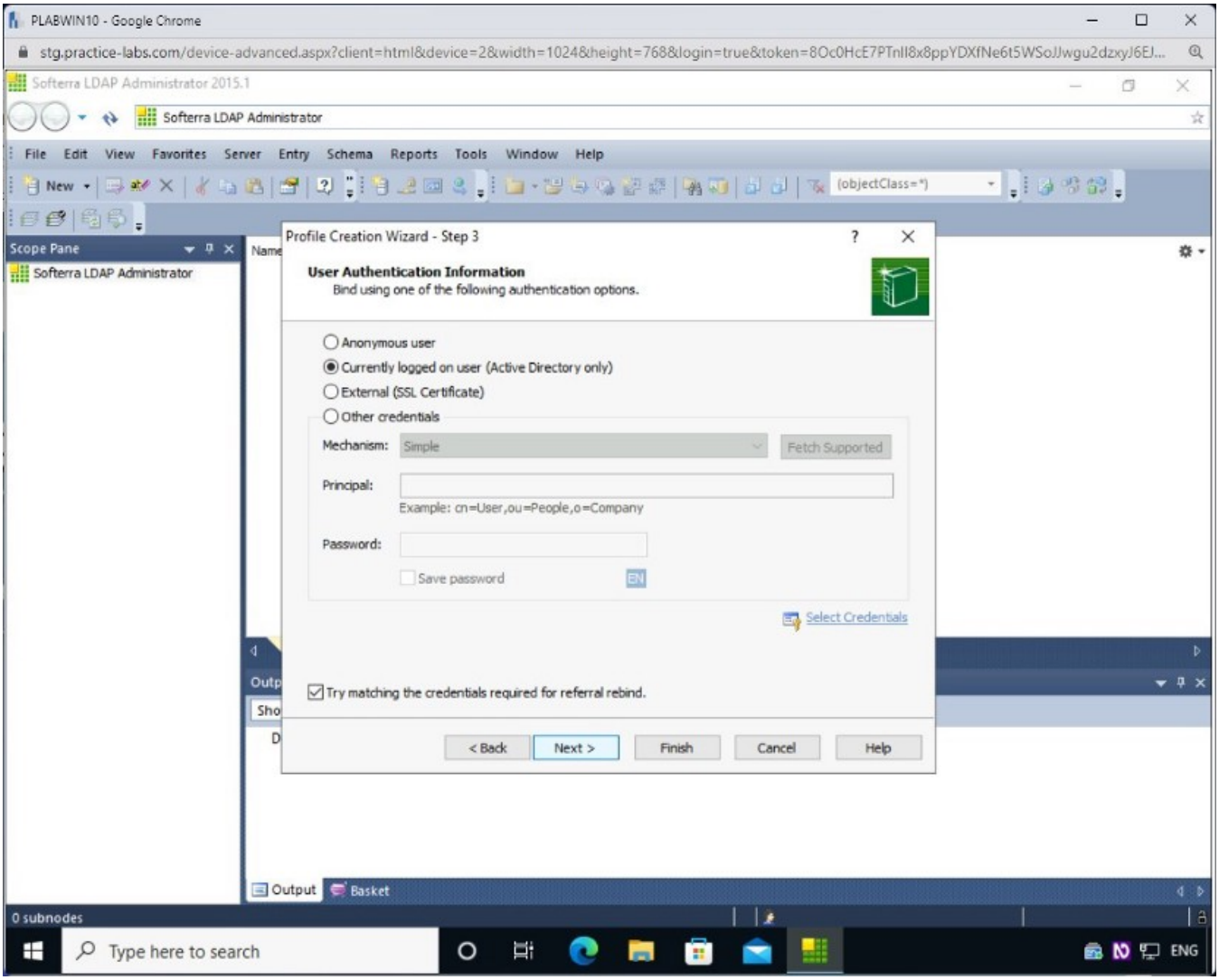
You are back on the **Profile Creation Wizard**. Note that all the information is now populated.

Click **Next**.



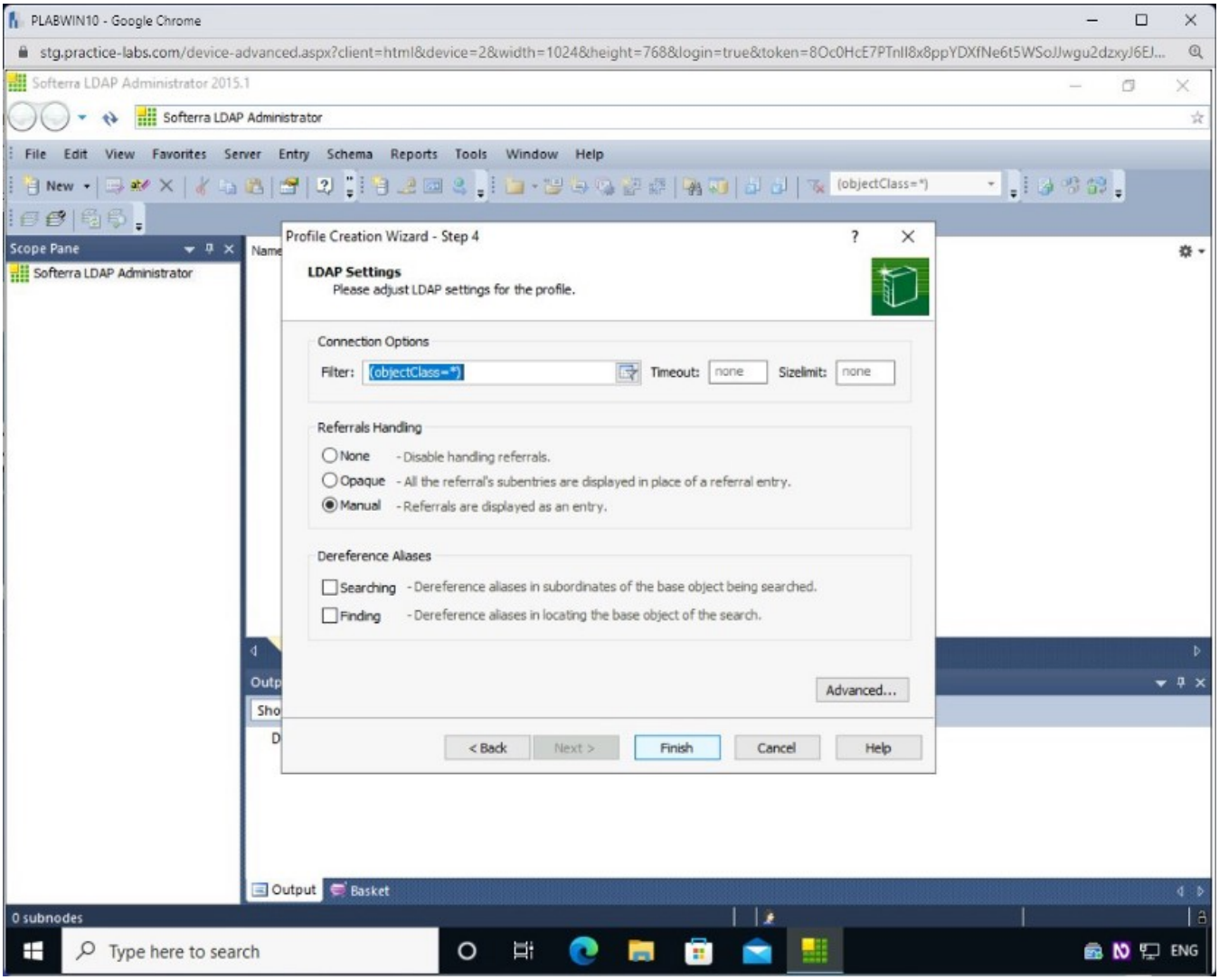
Step 8

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



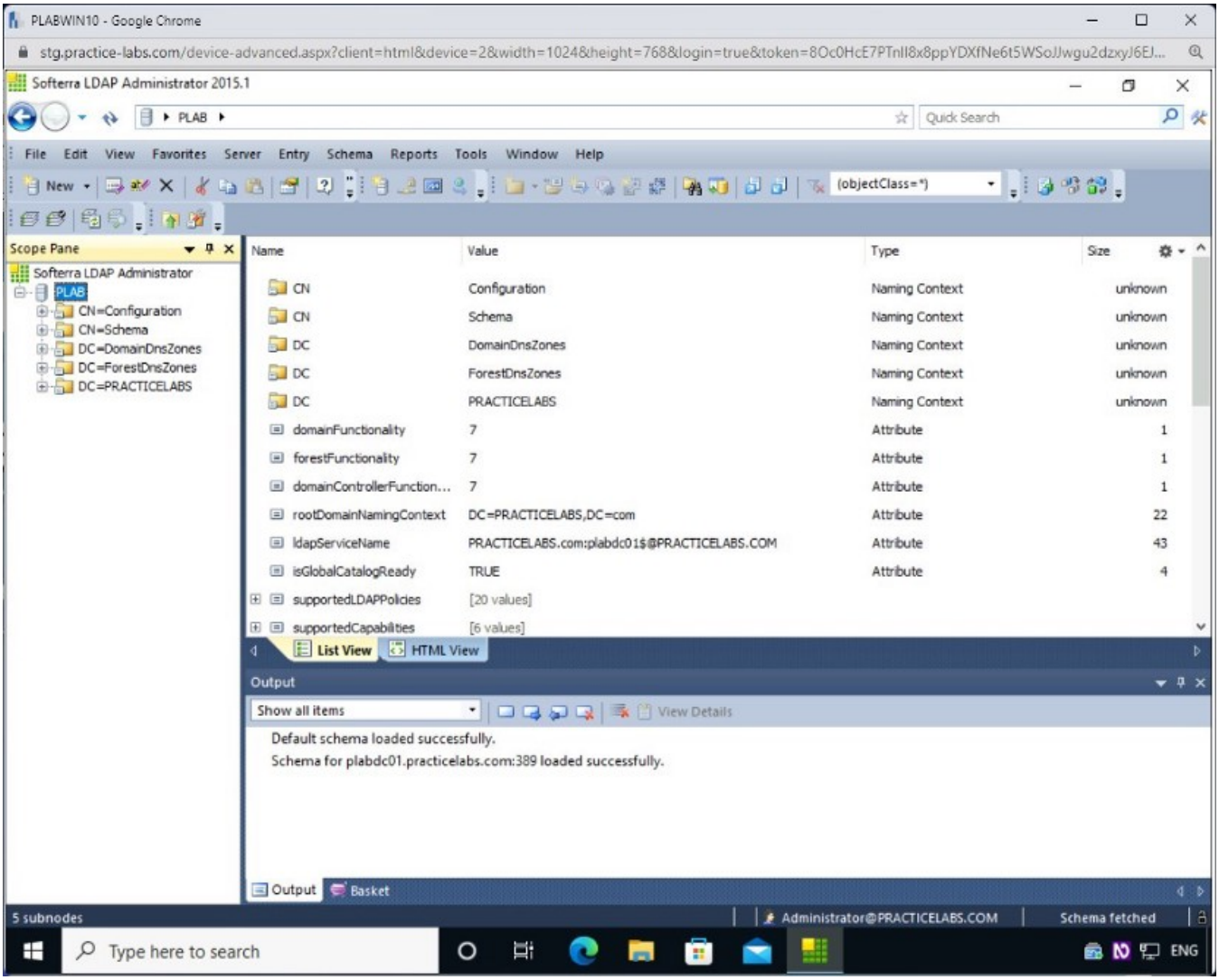
Step 9

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



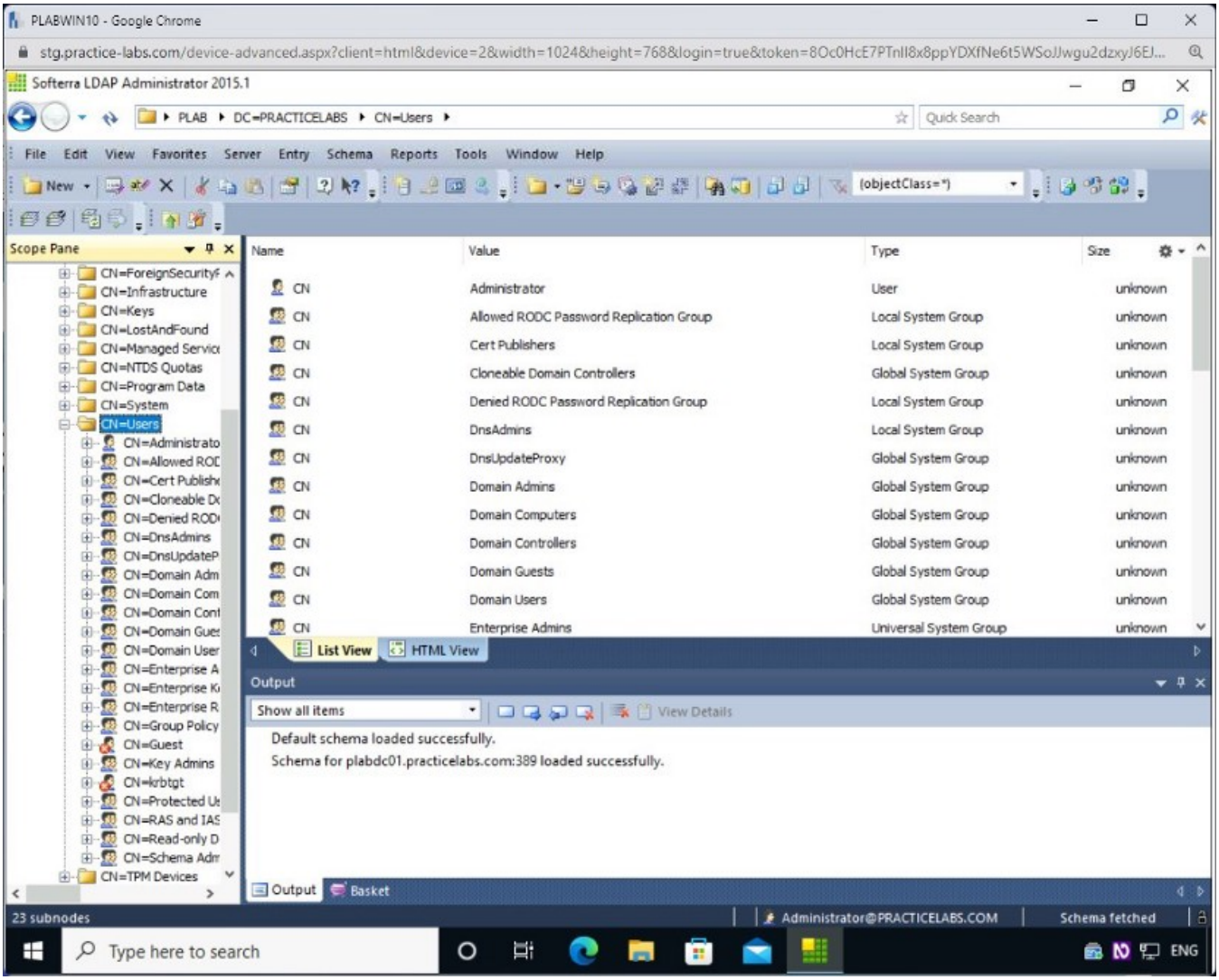
Step 10

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



Step 11

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

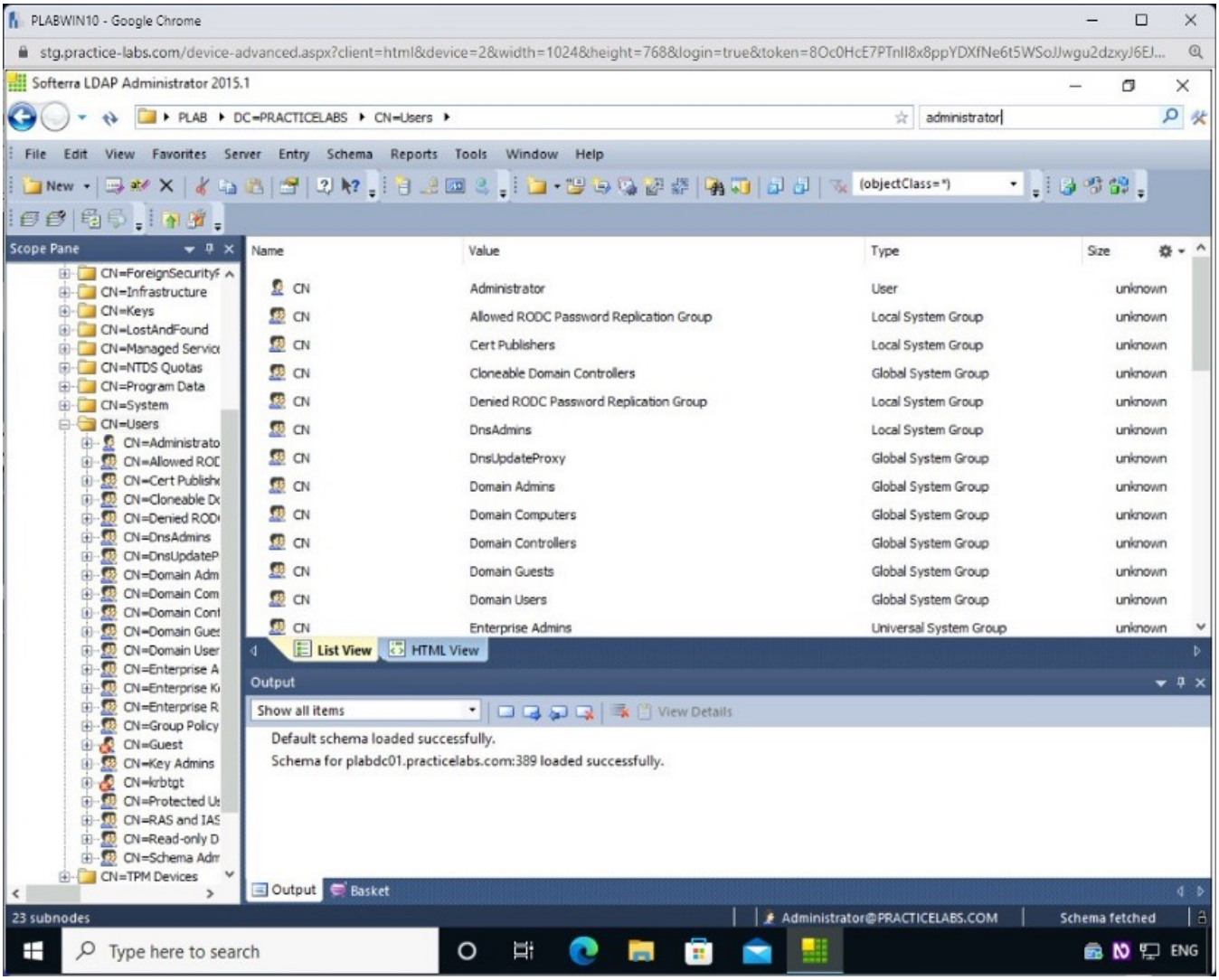


Step 12

The quickest method to locate information in **LDAP Administrator** is by searching it.

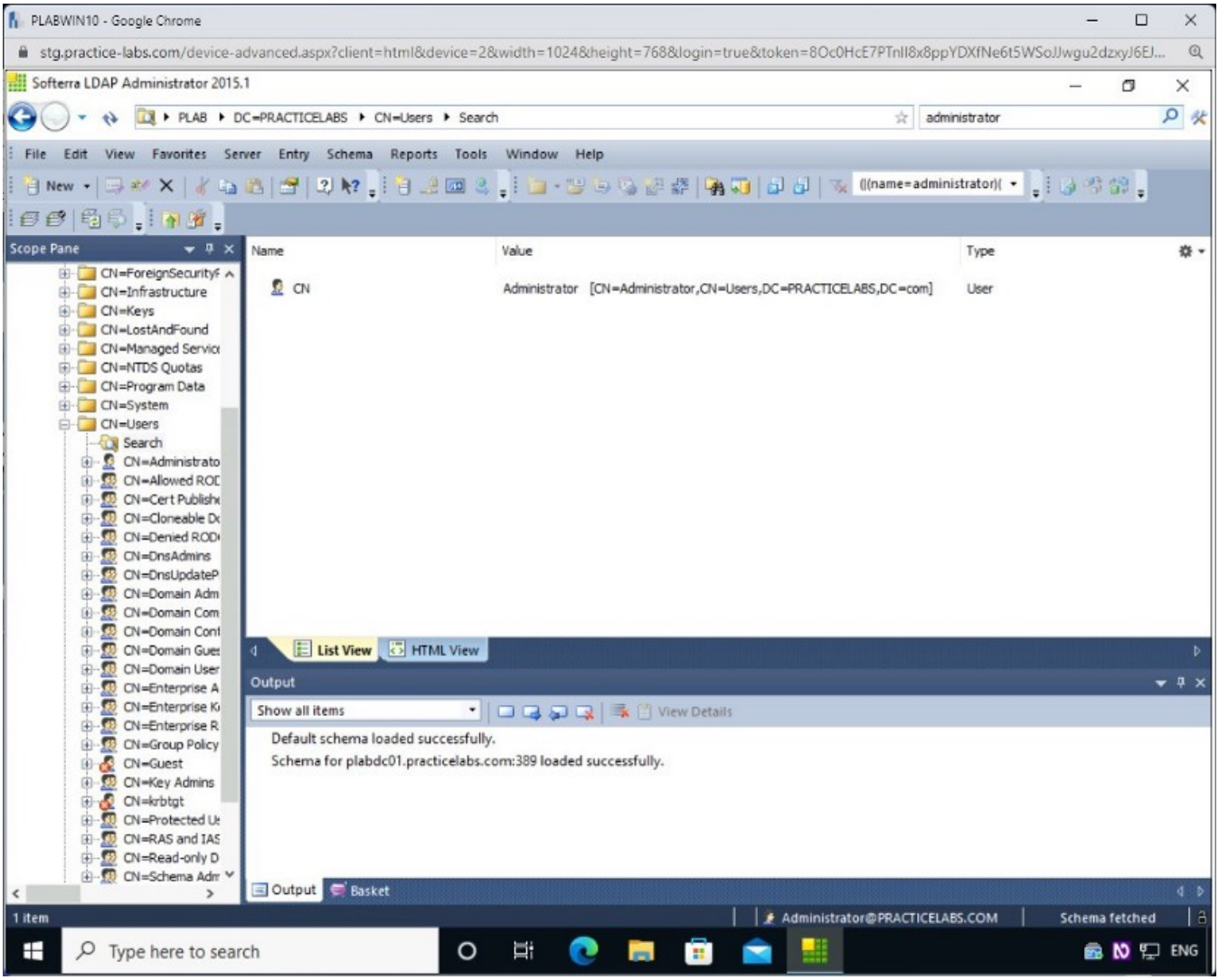
You can use **Quick Search**, located on the right side above the menu bar, to find the required information.

Click on **PLAB** at the top of the **Scope** pane and enter **administrator** in **Quick Search**. Once entered, click the search button adjacent to the search box.



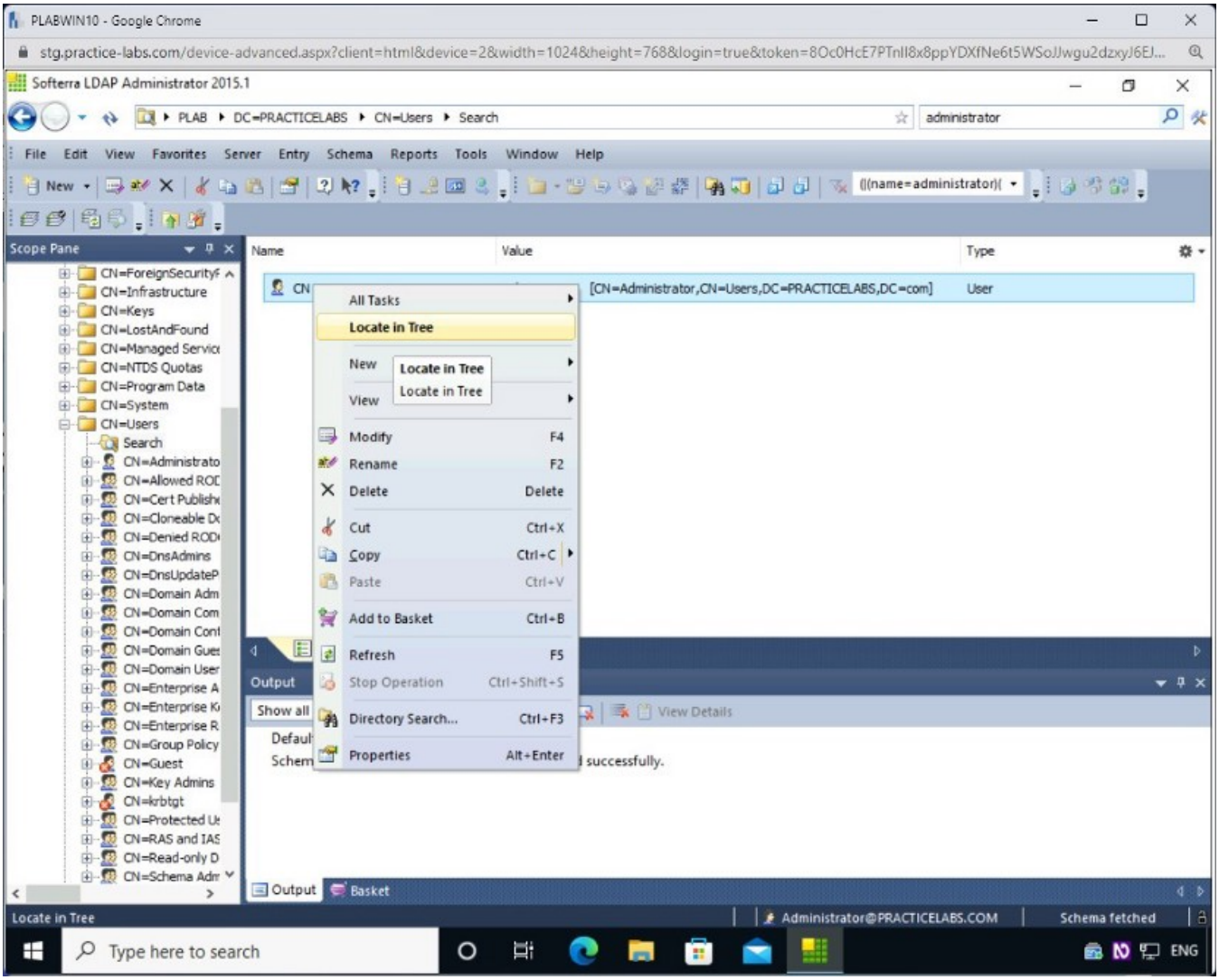
Step 13

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



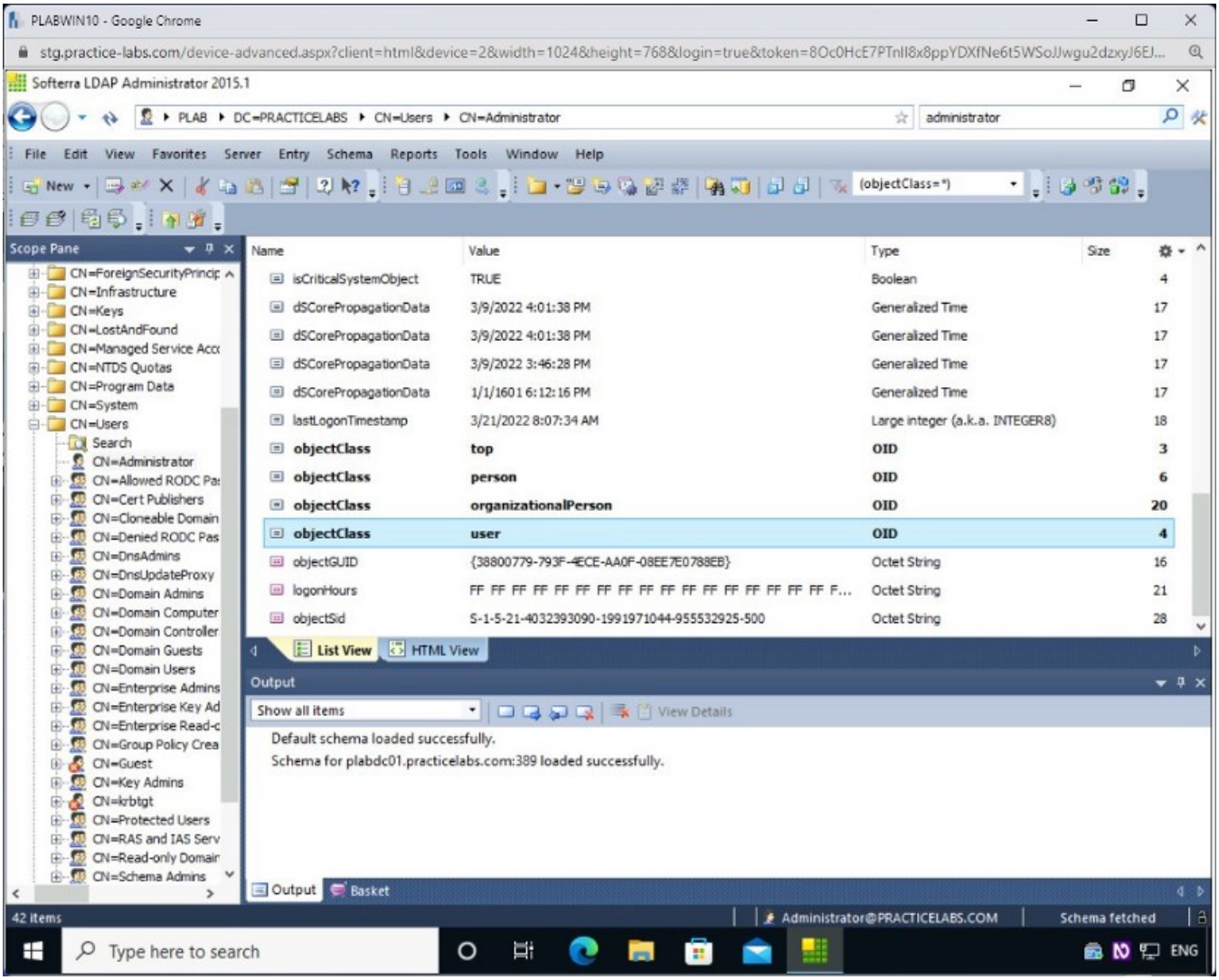
Step 14

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



Step 15

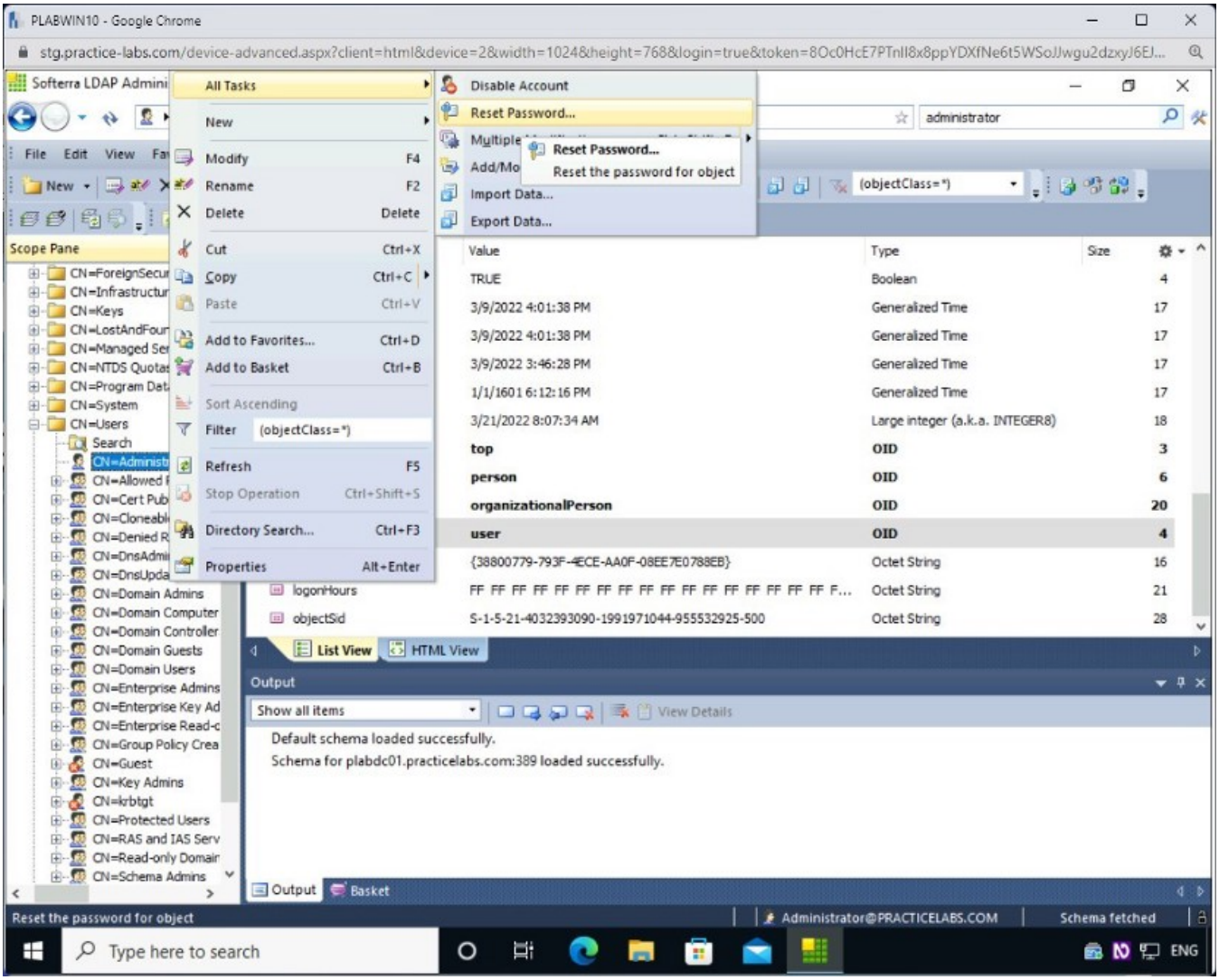
Note that the nodes in the left pane are automatically expanded, and the **administrator** is highlighted.



Step 16

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

Right-click **CN=Administrator** in the left-hand pane, select **All Tasks**, and select **Reset Password**.



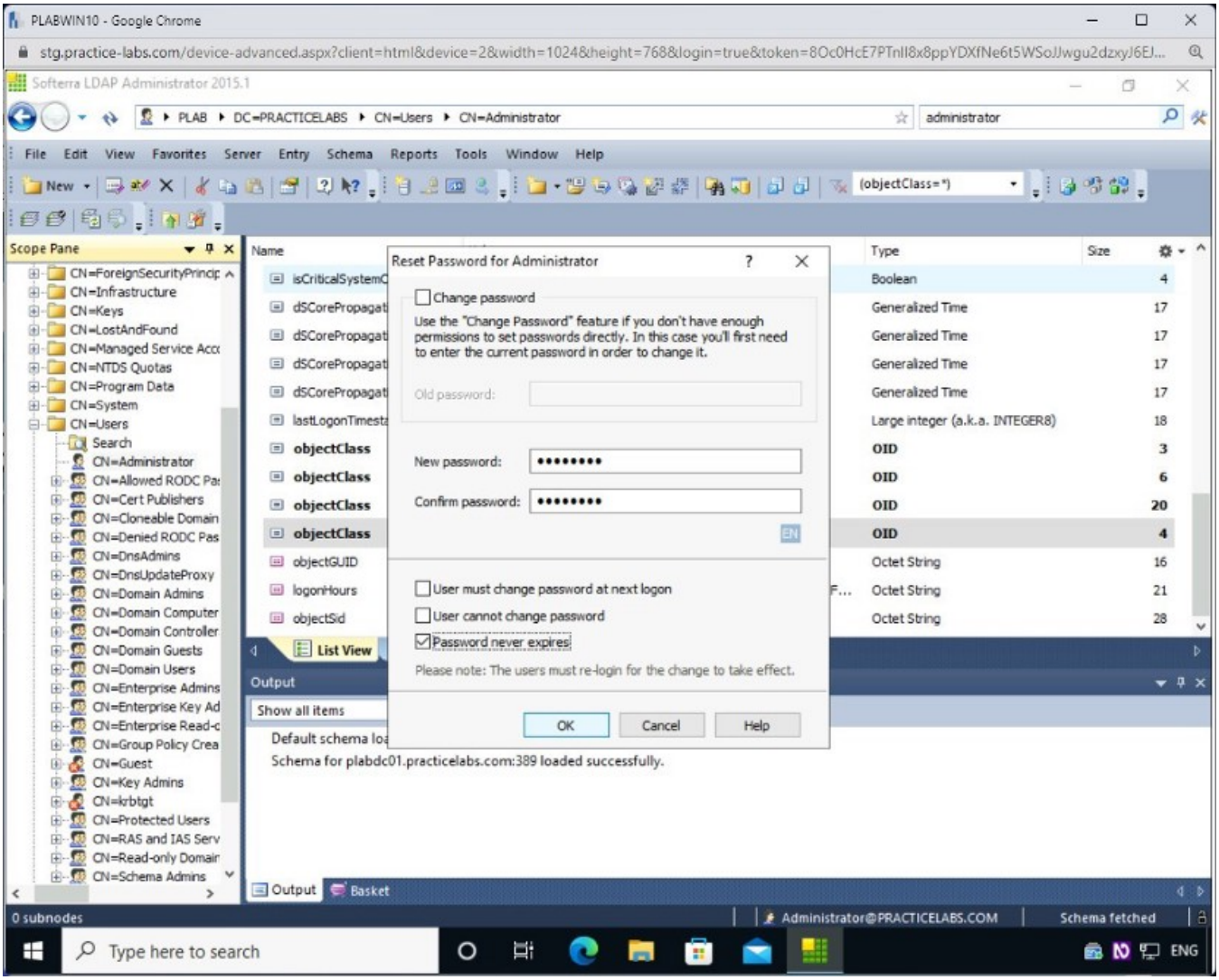
Step 17

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

In the **New password** and **Confirm password** text boxes, type the following:

Password

Click **OK**.



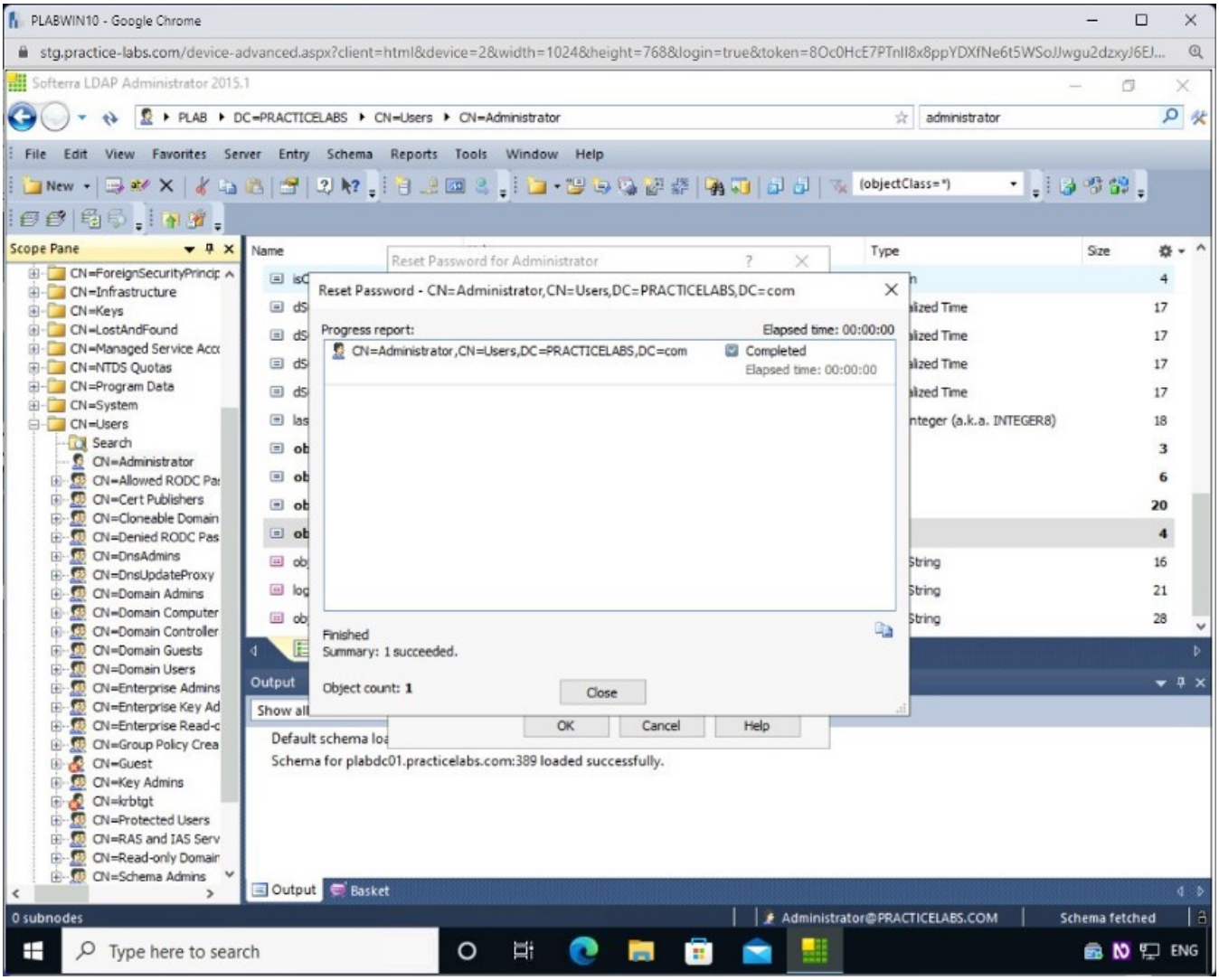
Step 18

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: *If time permits, you can spend more time exploring this tool as it has far more capabilities than the ones demonstrated in the lab environment.*

Close the **Softerra LDAP Administrator** window.



Methods of Prevention

In the above exercises, you learned that you could perform Enumeration using different methods. Let's investigate how to prevent these methods from being performed.

Preventing SNMP Enumeration

To prevent SNMP enumeration, you need to stop the SNMP service. An alternate method is to restrict it to the localhost.

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:

- Shut down SNMP service if not required
- Never use the default public community string
- Upgrade to SNMPv3

- Use the Additional restrictions for anonymous connections policy in Group Policy
- 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
- Restrict access to null session pipes and shares, and IPSec filtering
- Do not configure read-write authorization on the SNMP service

Preventing LDAP Enumeration

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

- Always use SSL to encrypt LDAP communication
- Use Kerberos to restrict the access only to known users
- Enable account lockout policy
- Use NTLM to limit access only to the authenticated users