Using a Port Scanner

A port scanner is a software tool used for probing into local or remote systems to find out open TCP/UDP ports and collect system information such as operating system type installed on the computer. This is used by system administrators to validate the security policy of firewalls and by hackers to determine the open ports on a computer that can be possibly exploited.

You will see that a port scanner is much more than just a piece of software that pings many devices at once. It has many more capabilities, some of which you will experiment with here.

A wide array of port scanning software either free or subscription-based are available for public use. You can use a port scanning tool in a test lab environment. However, precaution must be observed when using this tool in a corporate network, as port scans normally trigger an alert when detected by firewall appliances.

Please refer to your course material or use your favorite search engine to research this topic in more detail.

Learning Outcomes

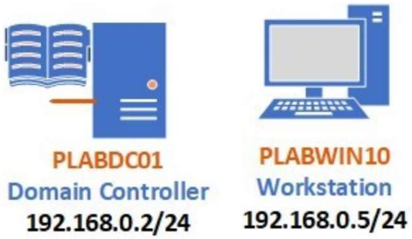
After completing this exercise, you will be able to:

- Use Advanced IP Scanner

Your Devices

You will be using the following devices in this lab. Please make sure these are powered on before proceeding.

- **PLABDC01** (Domain Controller)
- **PLABWIN10** (Workstation)



Task 1 - Use Advanced IP Scanner to scan the network

You can use the **Advanced IP Scanner** tool to list the devices available in the given IP address range. Moreover, this tool can also list the folders shared on the scanned network. In this task, you will use the **Advanced IP Scanner** to scan the lab environment, and then review the scan-results. Moreover, you will explore other functionalities of the **Advanced IP Scanner** tool.

To use the network scanner, perform the following steps:

Step 1

Connect to the **PLABWIN10** device.

Double click the Advanced IP Scanner icon on the desktop.

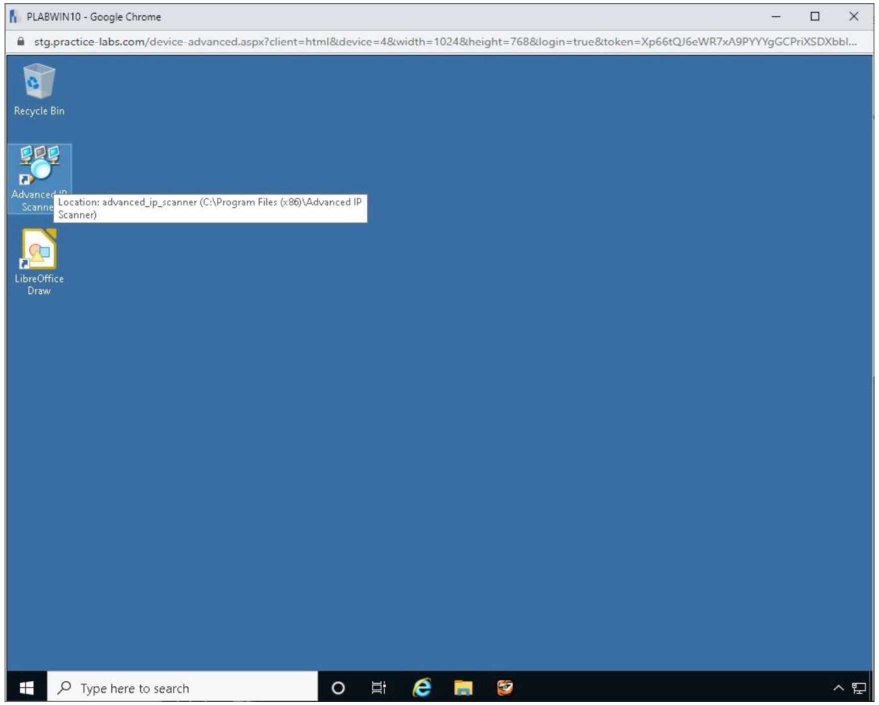

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=Xp66tQJ6eWR7xA9PYYYgGCPriXSDXbbl...
Recycle Bin
Advanced IP Scanner
Location: advanced_ip_scanner (C:\Program Files (x86)\Advanced IP Scanner)
LibreOffice Draw
Type here to search

Figure 4.1 Screenshot of the PLABWIN10 desktop: Advanced IP Scanner icon on the PLABWIN10 Windows desktop is highlighted.

Step 2

The **Advanced IP Scanner** window is displayed. Maximize this window. Note that in the address range field, a default range of IP address is already defined.

From this range, remove the **169.254.0.1 - 169.254.255.254** network ID range.

The remaining network ID range is **192.168.0.1 - 254**.

Click **Scan**.

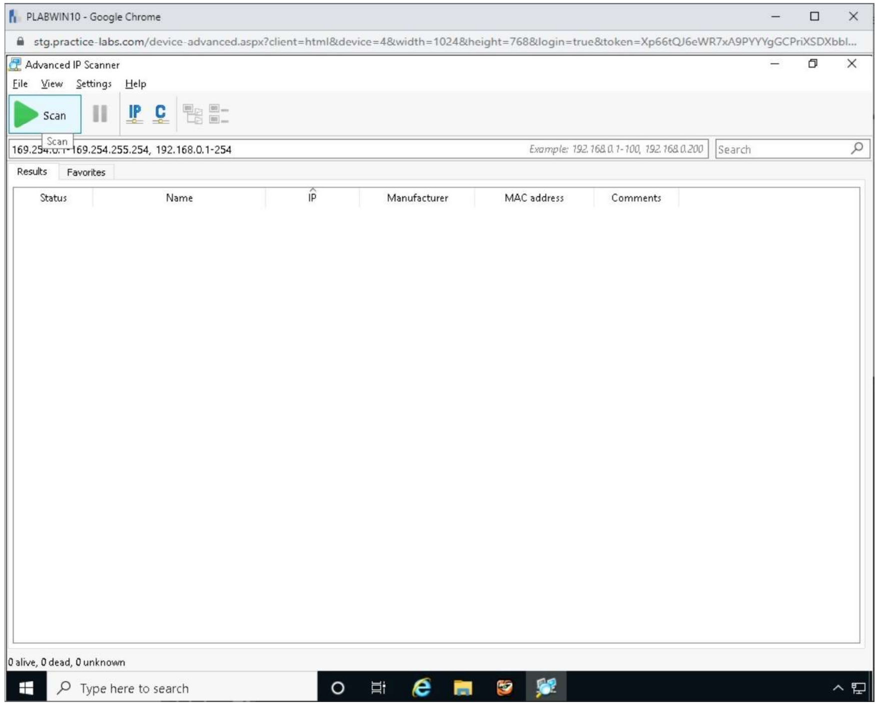

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=Xp66tQJ6eWR7xA9PYYYgGCPriXSDXbbl...
Advanced IP Scanner
File View Settings Help
Scan
IP C
169.254.0.1-169.254.255.254, 192.168.0.1-254
Example: 192.168.0.1-100, 192.168.0.200
Search
Results Favorites
Status Name IP Manufacturer MAC address Comments
0 alive, 0 dead, 0 unknown
Type here to search

Figure 4.2 Screenshot of the PLABWIN10 desktop: Advanced IP Scanner window is displayed showing the required settings performed, and the Scan button highlighted.

Step 3

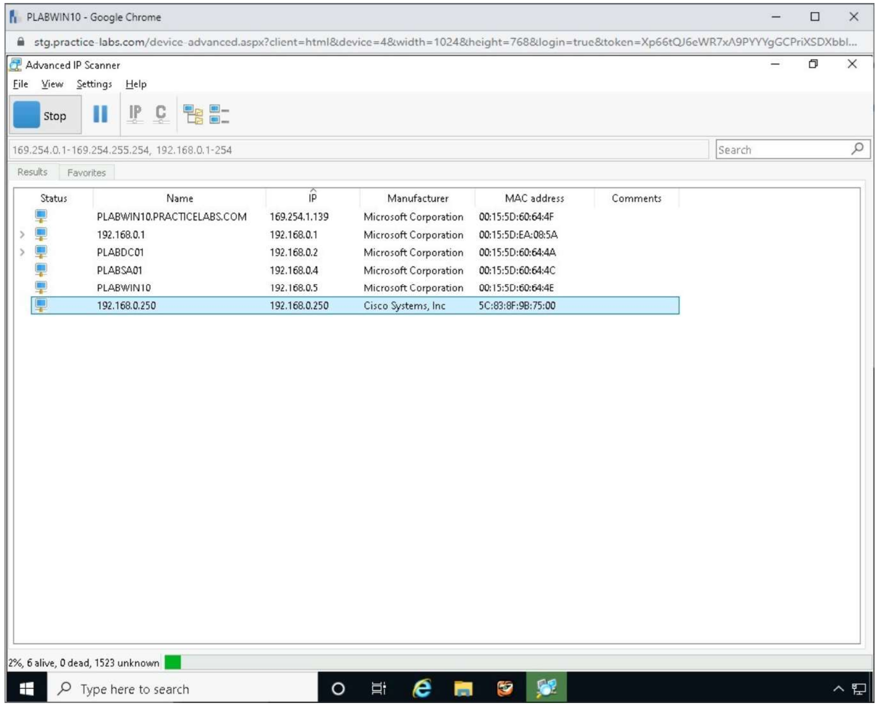
> *Note: As soon as the scan begins, it is tracked on the track bar displayed at the bottom of the scanner window.*

After a few seconds, the **Advanced IP Scanner** lists the devices within the range of **192.168.0.1 - 192.168.0.254** ip addresses discovered on the network.

Note the following about the result:

- The scan result identifies the IP address, the machine name, the manufacturer, and the MAC (media access control) address of each device.
- If you refer to the lab topology, you will see that all the network devices have been discovered including the **PLABWIN10** device itself - the device running the scan.

- There is also a device with an IP address of **192.168.0.250**. This is the default gateway for all devices to reach the Internet. This is a Cisco router - as the manufacturer column indicates.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=Xp66tQJ6eWR7xA9PYYYgGCPriXSDXbbl...
Advanced IP Scanner
File View Settings Help
Stop
IP C
Search
Results Favorites
Type here to search

169.254.0.1-169.254.255.254, 192.168.0.1-254

Status	Name	IP	Manufacturer	MAC address	Comments
	PLABWIN10.PRACTICELABS.COM	169.254.1.139	Microsoft Corporation	00:15:5D:60:64:4F	
	192.168.0.1	192.168.0.1	Microsoft Corporation	00:15:5D:EA:08:5A	
	PLABDC01	192.168.0.2	Microsoft Corporation	00:15:5D:60:64:4A	
	PLABSA01	192.168.0.4	Microsoft Corporation	00:15:5D:60:64:4C	
	PLABWIN10	192.168.0.5	Microsoft Corporation	00:15:5D:60:64:4E	
	192.168.0.250	192.168.0.250	Cisco Systems, Inc	5C:83:8F:9B:75:00	

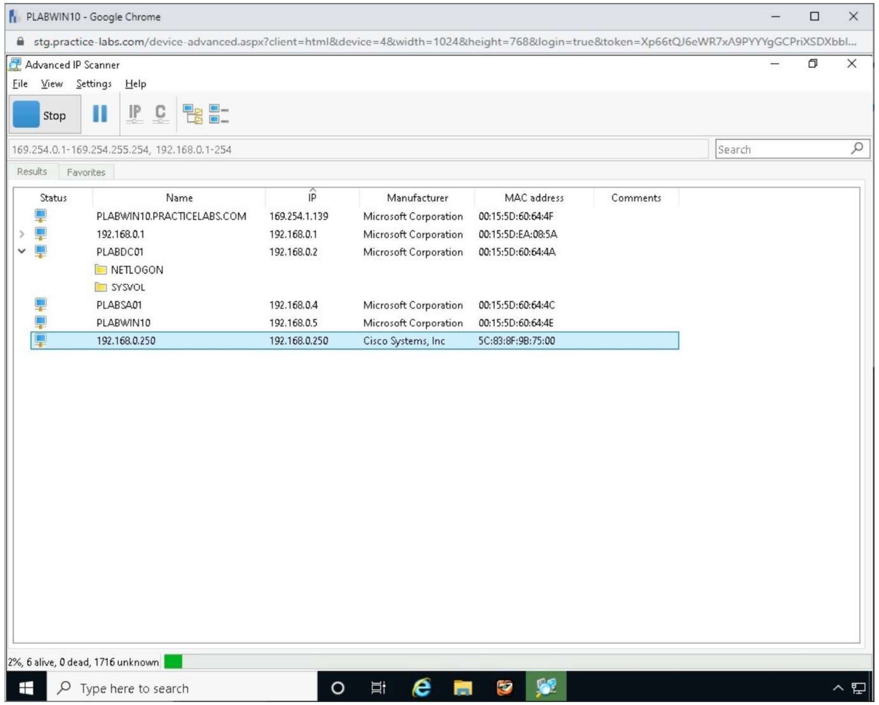
2%, 6 alive, 0 dead, 1523 unknown

Figure 4.3 Screenshot of the PLABWIN10 desktop: Advanced IP Scanner window is displayed listing results of scanning the specified IP address range.

Step 4

When the scan is successfully completed, expand the listed **PLABDC01** host.

Notice that the scanner has also discovered two shared folders on the device. The Advanced IP Scanner can detect shared folders on the network.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=Xp66tQJ6eWR7xA9PYYYgGCPriXSDXbbl...
Advanced IP Scanner
File View Settings Help
Stop
IP C
Search
Results Favorites
Type here to search

169.254.0.1-169.254.255.254, 192.168.0.1-254

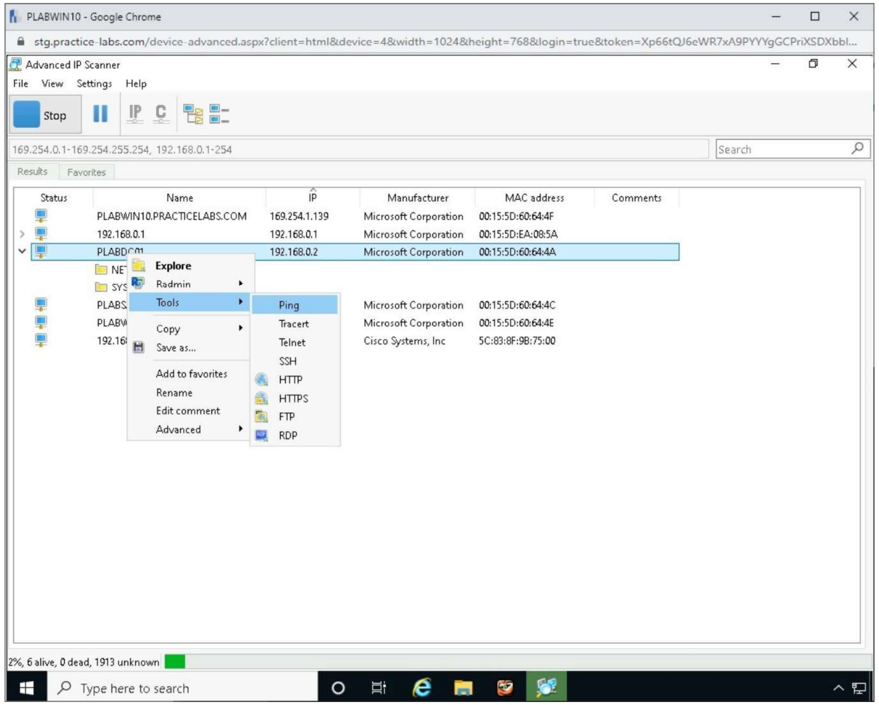
Status	Name	IP	Manufacturer	MAC address	Comments
	PLABWIN10.PRACTICELABS.COM	169.254.1.139	Microsoft Corporation	00:15:5D:60:64:4F	
	192.168.0.1	192.168.0.1	Microsoft Corporation	00:15:5D:EA:08:5A	
	PLABDC01	192.168.0.2	Microsoft Corporation	00:15:5D:60:64:4A	
	NETLOGON				
	SYSVOL				
	PLABSA01	192.168.0.4	Microsoft Corporation	00:15:5D:60:64:4C	
	PLABWIN10	192.168.0.5	Microsoft Corporation	00:15:5D:60:64:4E	
	192.168.0.250	192.168.0.250	Cisco Systems, Inc	5C:83:8F:9B:75:00	

2%, 6 alive, 0 dead, 1716 unknown

Figure 4.4 Screenshot of the PLABWIN10 desktop: Advanced IP Scanner window is displayed listing the shared folders discovered on the PLABDC01 device.

Step 5

Right-click the listed **PLABDC01**, select **Tools** and then select **Ping**.



Status	Name	IP	Manufacturer	MAC address	Comments
	PLABWIN10.PRACTICELABS.COM	169.254.1.139	Microsoft Corporation	00:15:5D:60:64:4F	
	192.168.0.1	192.168.0.1	Microsoft Corporation	00:15:5D:EA:08:5A	
	PLABDC01	192.168.0.2	Microsoft Corporation	00:15:5D:60:64:4A	
	NE				
	SYS				
	PLABS		Microsoft Corporation	00:15:5D:60:64:4C	
	PLABW		Microsoft Corporation	00:15:5D:60:64:4E	
	192.16		Cisco Systems, Inc	5C:83:8F:9B:75:00	

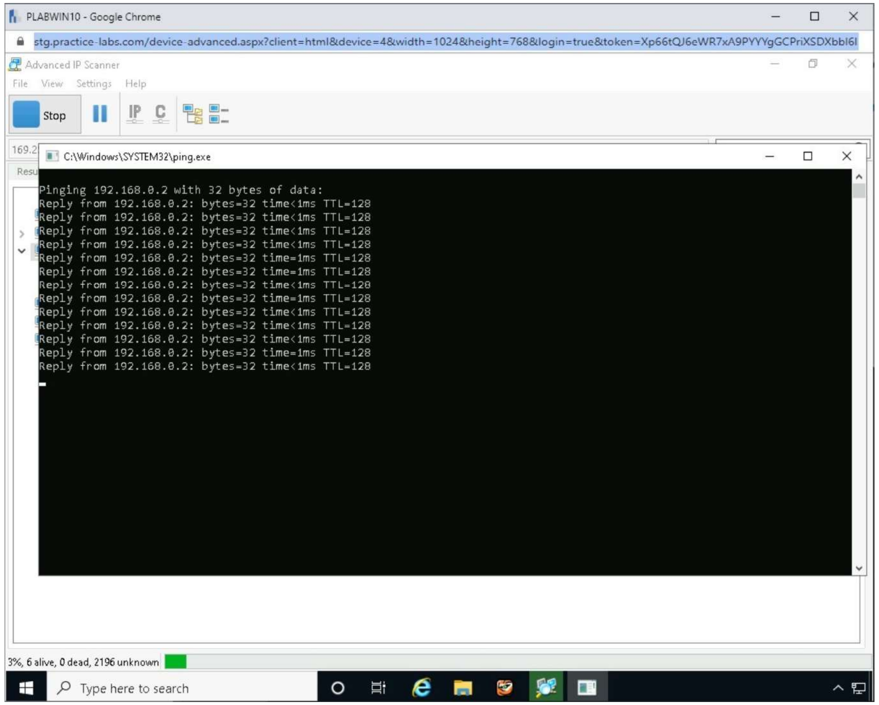
Figure 4.5 Screenshot of the PLABWIN10 desktop: Context menu (that appears on right-clicking the server-name node) > Tools > Ping menu-options are displayed on the Advanced IP Scanner window.

Step 6

This opens a command and prompt window, and sets up a ping session from **PLABWIN10** to **PLABDC01**.

Notice that the ping command is executed and replies from the pinged server (**PLABDC01**) are listed.

> *Note: The pings will continue until you either cancel them by using Ctrl+c or by closing the Command Prompt window.*



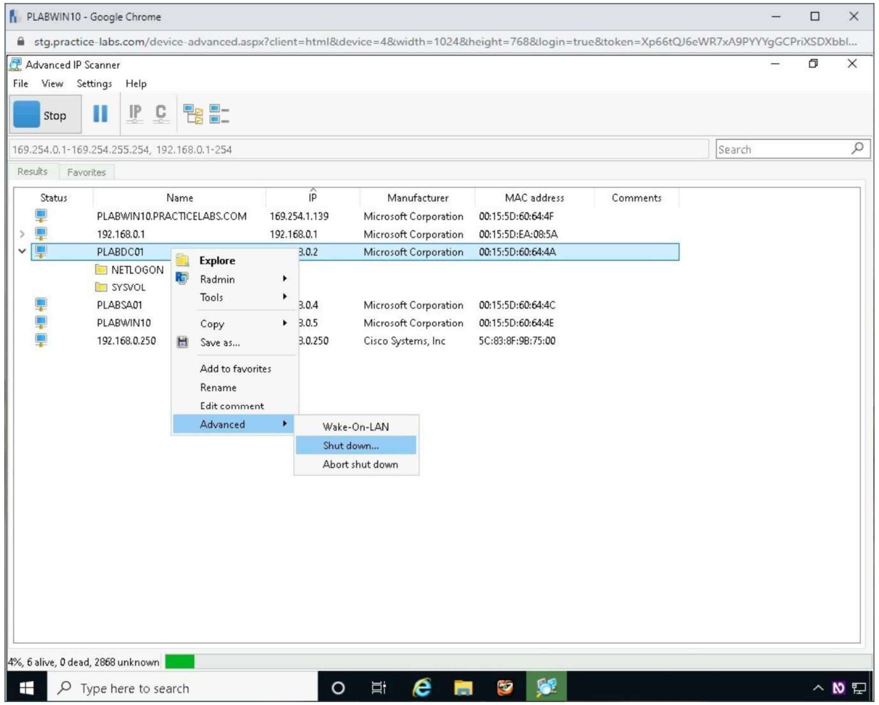
PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=Xp66tQJ6eWR7xA9PYYYgGCPriXSDXbbl6l
Advanced IP Scanner
File
View
Settings
Help
Stop
IP
C
169.2
Resu
C:\Windows\SYSTEM32\ping.exe
3%, 6 alive, 0 dead, 2196 unknown
Type here to search

```
Pinging 192.168.0.2 with 32 bytes of data:
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time=1ms TTL=128
Reply from 192.168.0.2: bytes=32 time=1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time=1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time=1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
```

Figure 4.6 Screenshot of the PLABWIN10 desktop: Command prompt window is displayed showing response of the pinged device.

Step 7

Right-click **PLABDC01** and select **Advanced** > **Shutdown**.



Status	Name	IP	Manufacturer	MAC address	Comments
	PLABWIN10.PRACTICELABS.COM	169.254.1.139	Microsoft Corporation	00:15:5D:60:64:4F	
	192.168.0.1	192.168.0.1	Microsoft Corporation	00:15:5D:EA:08:5A	
	PLABDC01	3.0.2	Microsoft Corporation	00:15:5D:60:64:4A	
	NETLOGON				
	SYSVOL				
	PLABSA01	3.0.4	Microsoft Corporation	00:15:5D:60:64:4C	
	PLABWIN10	3.0.5	Microsoft Corporation	00:15:5D:60:64:4E	
	192.168.0.250	3.0.250	Cisco Systems, Inc	5C:83:8F:9B:75:00	

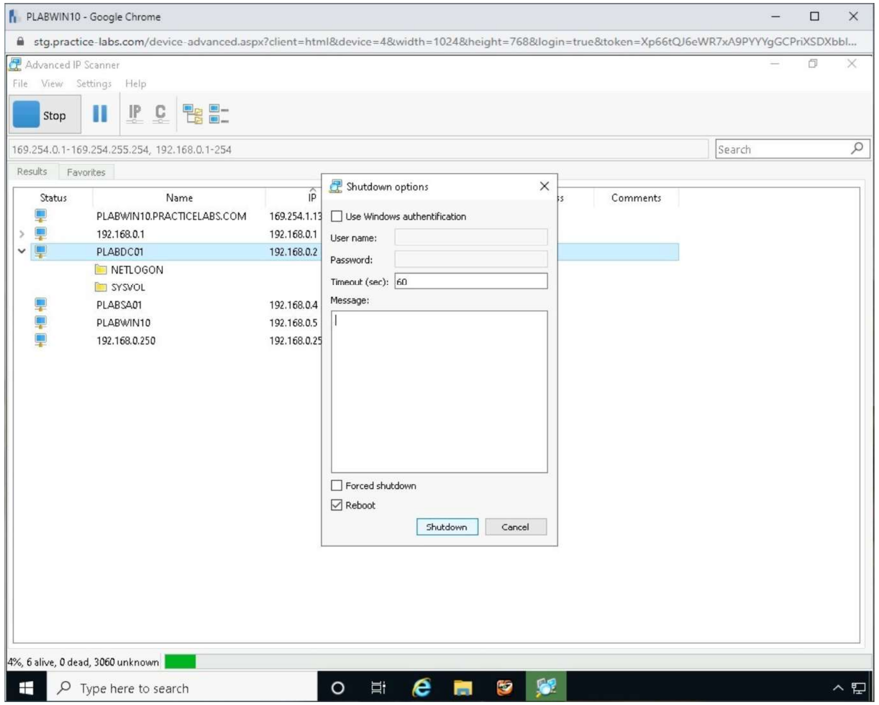
4%, 6 alive, 0 dead, 2868 unknown

Figure 4.7 Screenshot of the PLABWIN10 desktop: Context menu (that appears on right-clicking the server-name node) > Advanced > Shut down menu-options are displayed on the Advanced IP Scanner window.

Step 8

On the **Shutdown options** dialog box, select the **Reboot** checkbox.

Click **Shutdown**.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=Xp66tQJ6eWR7xA9PYYYgGCPriXSDXbbl...
Advanced IP Scanner
File View Settings Help
Stop
169.254.0.1-169.254.255.254, 192.168.0.1-254
Search
Results Favorites
Shutdown options
Shutdown
Cancel
Type here to search

Status	Name	IP
	PLABWIN10.PRACTICELABS.COM	169.254.1.13
	192.168.0.1	192.168.0.1
	PLABDC01	192.168.0.2
	NETLOGON	
	SYSVOL	
	PLABSA01	192.168.0.4
	PLABWIN10	192.168.0.5
	192.168.0.250	192.168.0.25

☐ Use Windows authentification
User name:
Password:
Timeout (sec): 60
Message:
☐ Forced shutdown
☑ Reboot

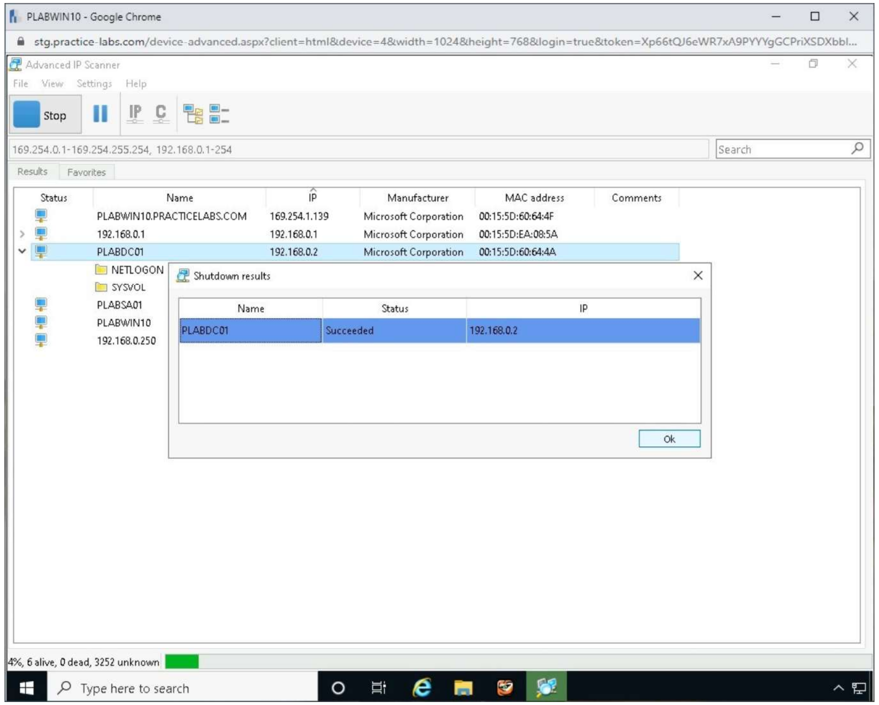
4%, 6 alive, 0 dead, 3060 unknown

Figure 4.8 Screenshot of the PLABWIN10 desktop: Shutdown options dialog box is displayed showing the required settings performed, and the Shutdown button highlighted.

Step 9

The **Shutdown results** window is displayed. It indicates that the shutdown initiation has **Succeeded.**

Click **OK**.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=Xp66tQJ6eWR7xA9PYYYgGCPriXSDXbbl...
Advanced IP Scanner
File
View
Settings
Help
Stop
Search
Results
Favorites
Type here to search

169.254.0.1-169.254.255.254, 192.168.0.1-254

Status	Name	IP	Manufacturer	MAC address	Comments
	PLABWIN10.PRACTICELABS.COM	169.254.1.139	Microsoft Corporation	00:15:5D:60:64:4F	
	192.168.0.1	192.168.0.1	Microsoft Corporation	00:15:5D:EA:08:5A	
	PLABDC01	192.168.0.2	Microsoft Corporation	00:15:5D:60:64:4A	
	NETLOGON				
	SYSVOL				
	PLABSA01				
	PLABWIN10				
	192.168.0.250				

Shutdown results

Name	Status	IP
PLABDC01	Succeeded	192.168.0.2

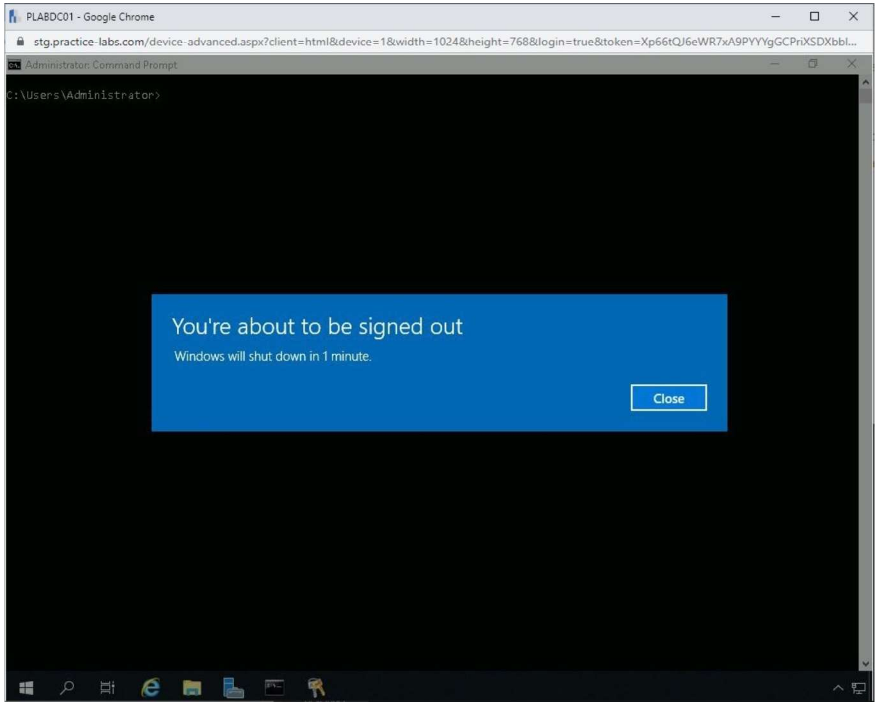
Ok

4%, 6 alive, 0 dead, 3252 unknown

Figure 4.9 Screenshot of the PLABWIN10 desktop: Shutdown results window is displayed showing status of the initiated shutdown and the OK button highlighted.

Step 10

If you look at the desktop of the **PLABDC01** device within a minute of sending the shutdown request, you will see a message informing you that you are about to be signed out. If you leave it long enough (about a minute), it will log you out, and it will reboot the device.


PLABDC01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=1&width=1024&height=768&login=true&token=Xp66tQJ6eWR7xA9PYYYgGCPriXSDXbbl...
Administrator: Command Prompt
Close

```
C:\Users\Administrator>
```

You're about to be signed out

Windows will shut down in 1 minute.

Figure 4.10 Screenshot of the PLABDC01 desktop: You're about to be signed out information box is displayed and the Close button highlighted.

Keep all devices that you have powered on in their current state and proceed to the next exercise.