Practice Labs - Ethical Hacker v10

Scanning Networks

- **Introduction**
- **Lab Topology**
- **Exercise 1 - Using Microsoft Network Scanning Tools**
- **Exercise 2 - Using Linux Network Scanning Tools**
- **Review**

Introduction

Network Scanning
ID Serve
Nmap
Zenmap
CurrPorts
Netcat
Hping3
MyLanViewer
Netdiscover
Fping
Ethical Hacking

Welcome to the **Scanning Networks** 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 - Using Microsoft Network Scanning Tools
- Exercise 2 - Using Linux Network Scanning Tools

After completing this module, you will be able to:

- Banner Grab Using ID Serve
- Explore a Network Using Nmap
- Use CurrPorts to Monitor TCP/IP Connections
- Use MyLanViewer to Scan a Network
- Use Hping3 for Network Scanning
- Perform a TCP Scan Using Dmitry
- Use Netcat for Port Scan
- Use Netdiscover for Scanning the Network
- Perform Stealth Scanning Using Nmap
- Use fping for Network Scanning
- Use Msfconsole to Perform TCP Stealth on a Network

Exam Objectives

The following exam objective is 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.

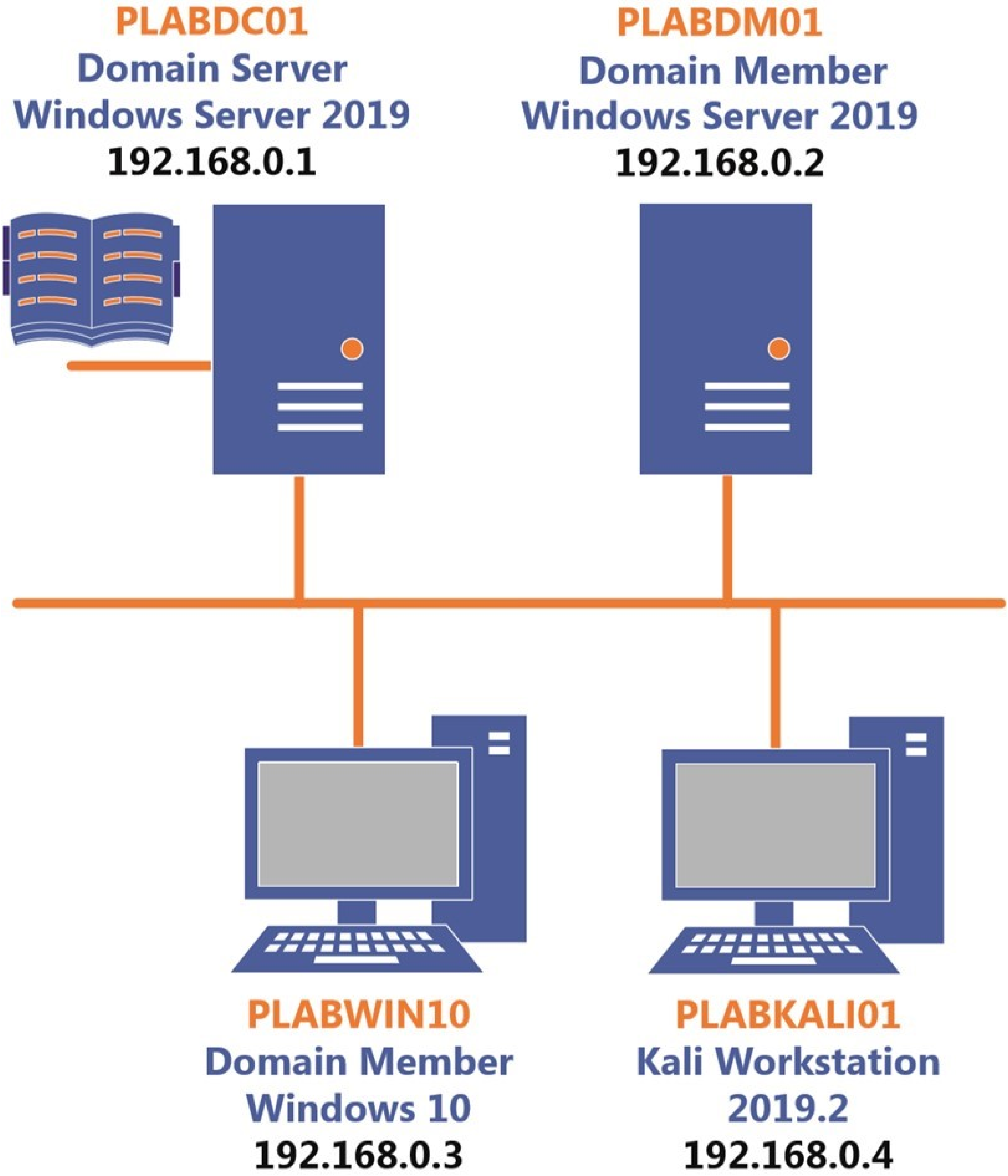
Help and Support

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 - Using Microsoft Network Scanning Tools

There are several Windows-based network scanning tools that are available. Some of the key tools are:

- ID Serve
- CurrPorts
- Nmap
- MyLanViewer
- NetView
- Amap
- Netscan Tools Pro
- LANSurveyor
- Friendly Pinger
- Global Network Inventory

It is important to understand that some of the tools will work in a similar fashion, such as discover live systems on a network. On the other hand, some tools, such as ID Serve, have a distinct function, such as a scan for a Webserver and extract its configuration information.

In this exercise, you will learn to use some of the key Windows-based tools for network scanning.

Learning Outcomes

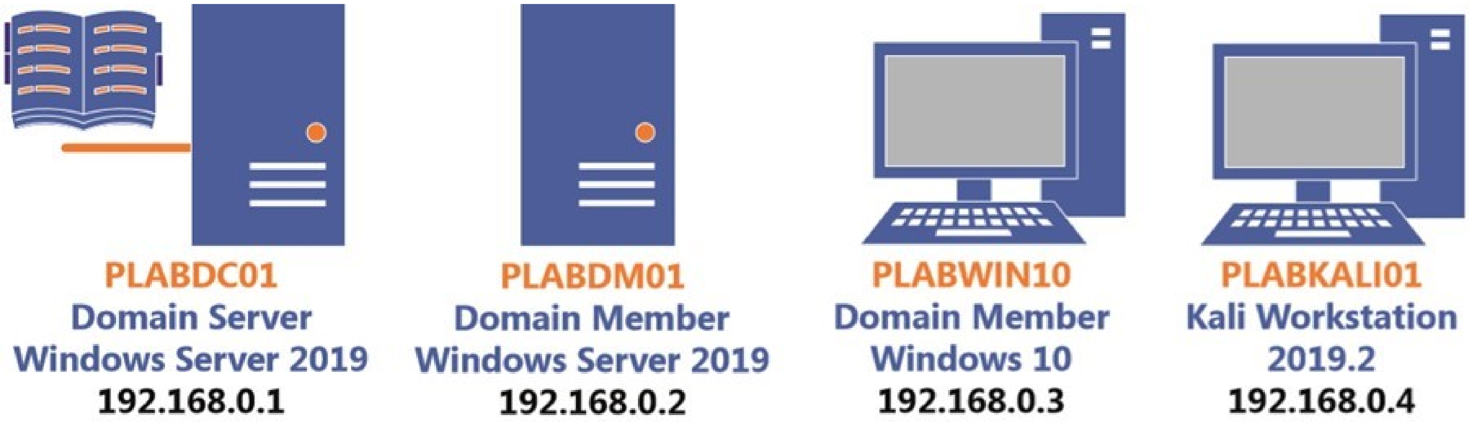
After completing this exercise, you will be able to:

- Banner Grab Using ID Serve
- Explore a Network Using Nmap
- Use CurrPorts to Monitor TCP/IP Connections
- Use MyLanViewer to Scan a Network

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 - Banner Grab Using ID Serve

As an ethical hacker, it is important to know banner grabbing methods. ID Serve is one of the key tools used in banner grabbing. ID Serve can connect any of the server ports on any:

- Domain
- IP address

ID Serve can be used to grab the server's greeting message (if any) along with the make and model. It can also grab the operating system's information.

In this task, you will perform banner grabbing using ID Serve. To do this, perform the following steps:

Step 1

Ensure you have powered on the required devices and connect to **PLABWIN10**.

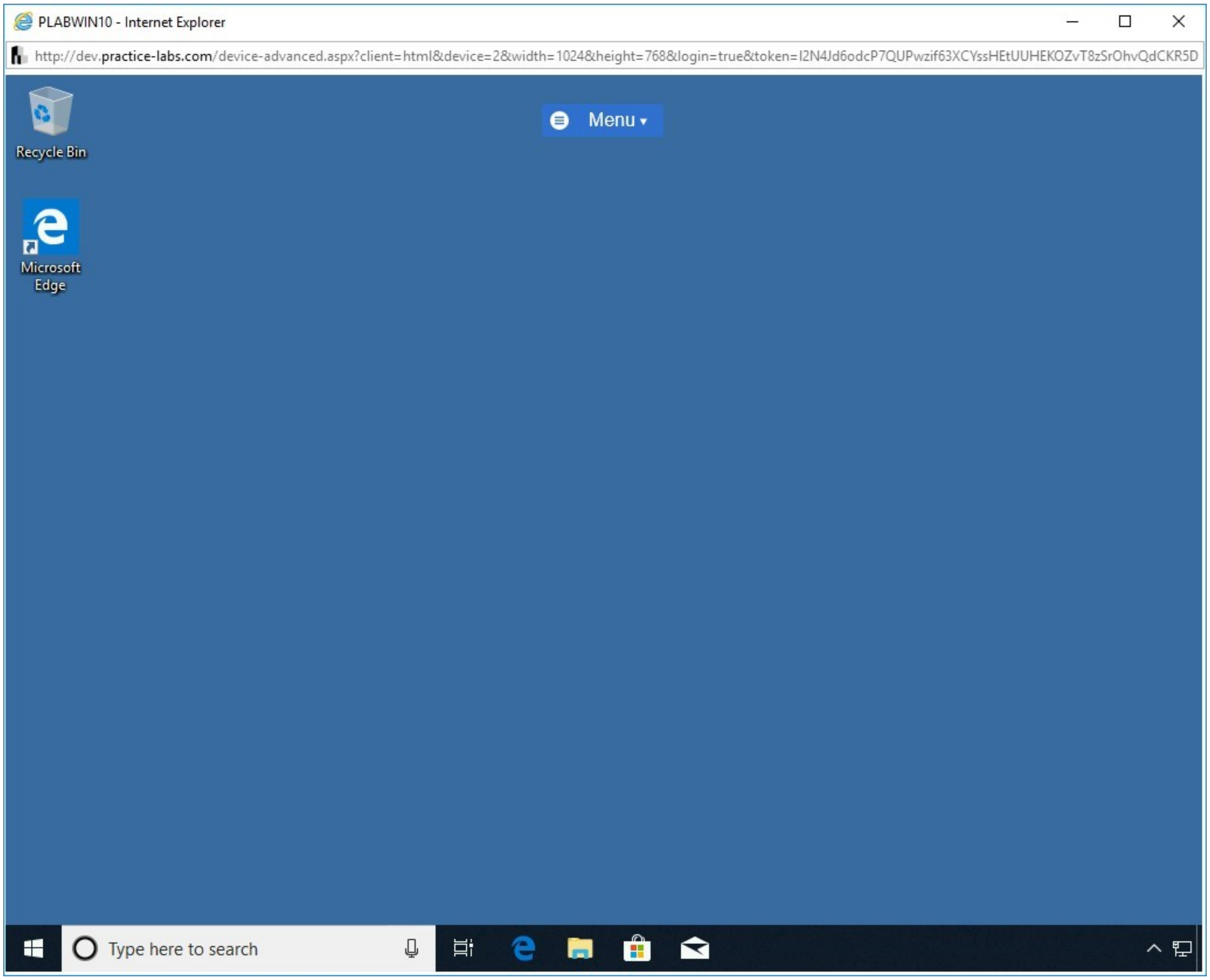

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=I2N4Jd6odcP7QUPwzif63XCYssHEtUUHEKOZvT8zSrOhvQdCKR5D
Menu ▾
Recycle Bin
Microsoft Edge
Type here to search

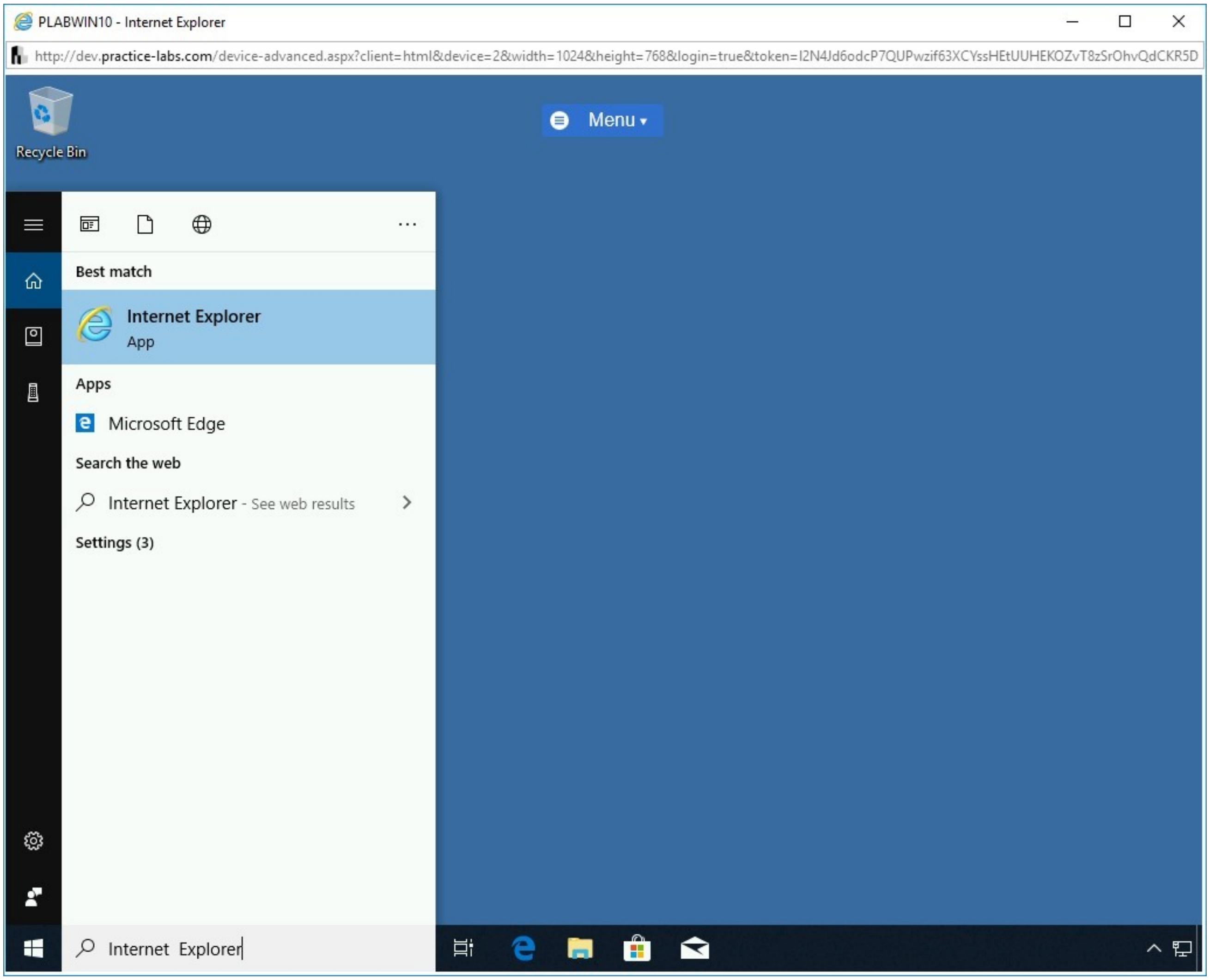
Figure 1.1 Screenshot of PLABWIN10: Showing the desktop of PLABWIN10.

Step 2

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

```
Internet Explorer
```

Press **Enter**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=I2N4Jd6odcP7QUPwzif63XCYssHEtUUHEKOZvT8zSrOhvQdCKR5D
Recycle Bin
Menu
Best match
Internet Explorer
App
Apps
Microsoft Edge
Search the web
Internet Explorer - See web results
Settings (3)

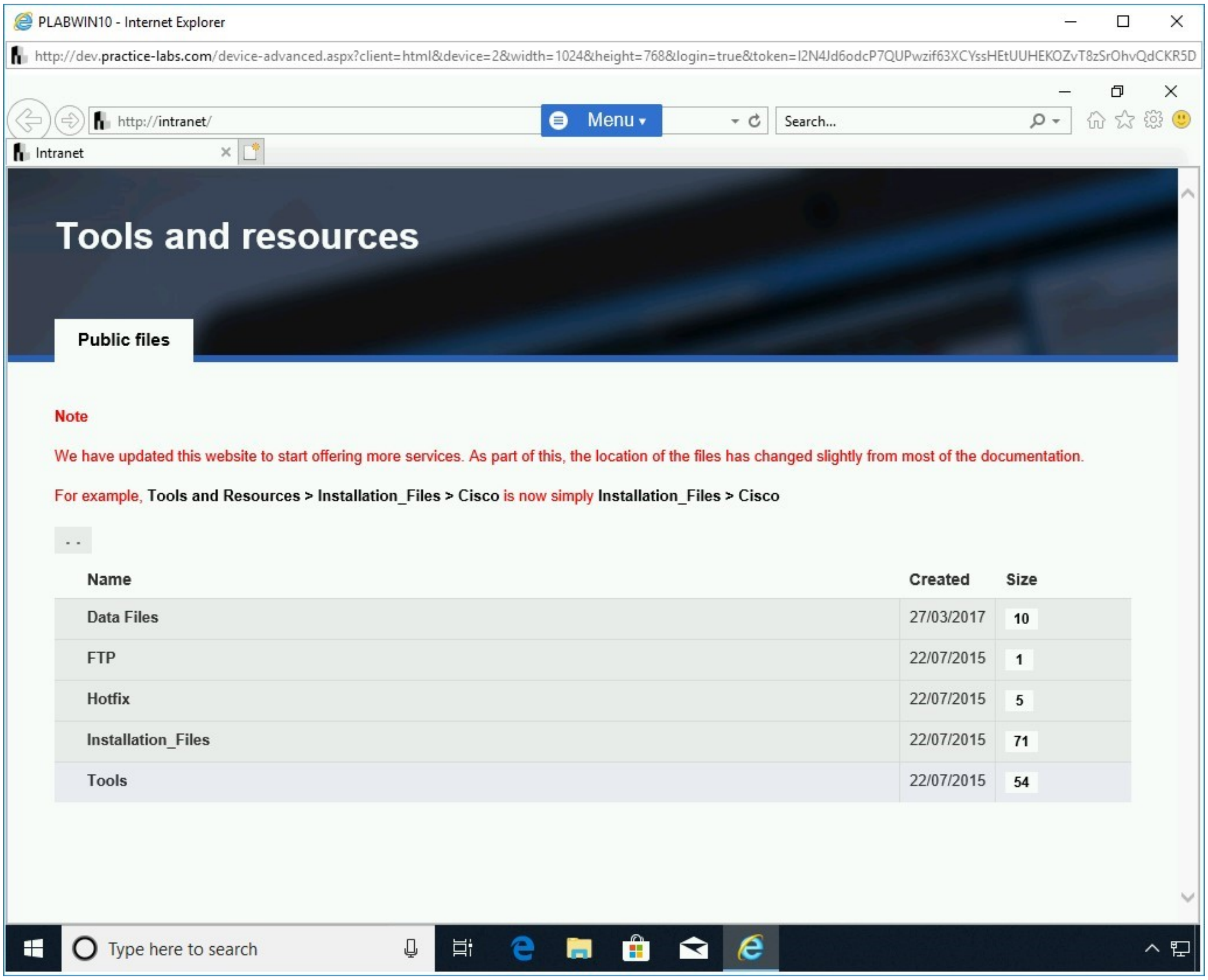
Internet Explorer

Figure 1.2 Screenshot of PLABWIN10: Searching for Internet Explorer and then selecting it from the search results.

Step 3

The **Intranet** website is displayed.

Click **Tools** from the list.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=I2N4Jd6odcP7QUPwzif63XCYssHEtUUHEKOZvT8zSrOhvQdCKR5D
http://intranet/
Menu
Search...
Intranet
Type here to search

Tools and resources

Public files

Note

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

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

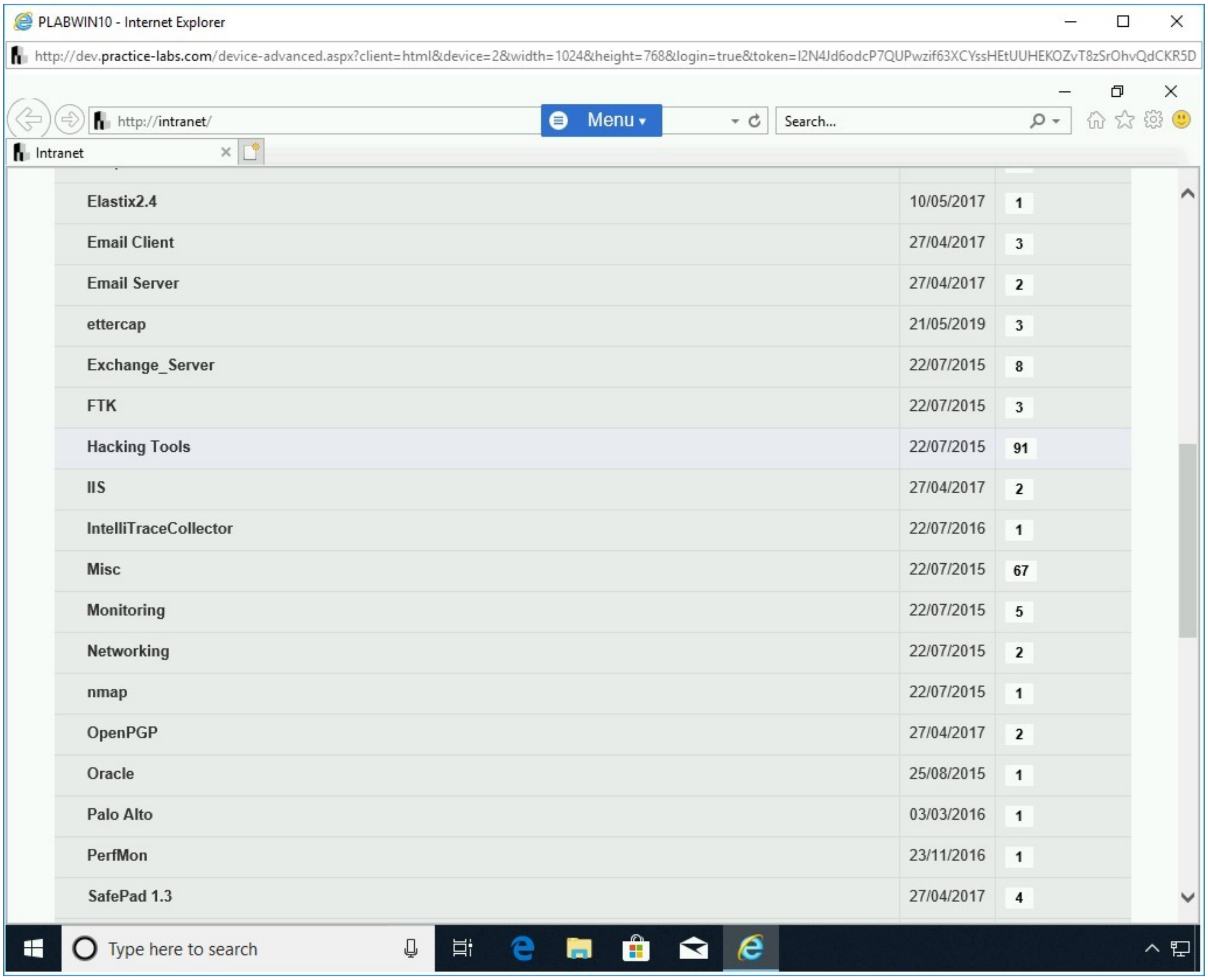
. .

Name	Created	Size
Data Files	27/03/2017	10
FTP	22/07/2015	1
Hotfix	22/07/2015	5
Installation_Files	22/07/2015	71
Tools	22/07/2015	54

Figure 1.3 Screenshot of PLABWIN10: Clicking the Tools folder on the Intranet website.

Step 4

Scroll down and click **Hacking Tools**.

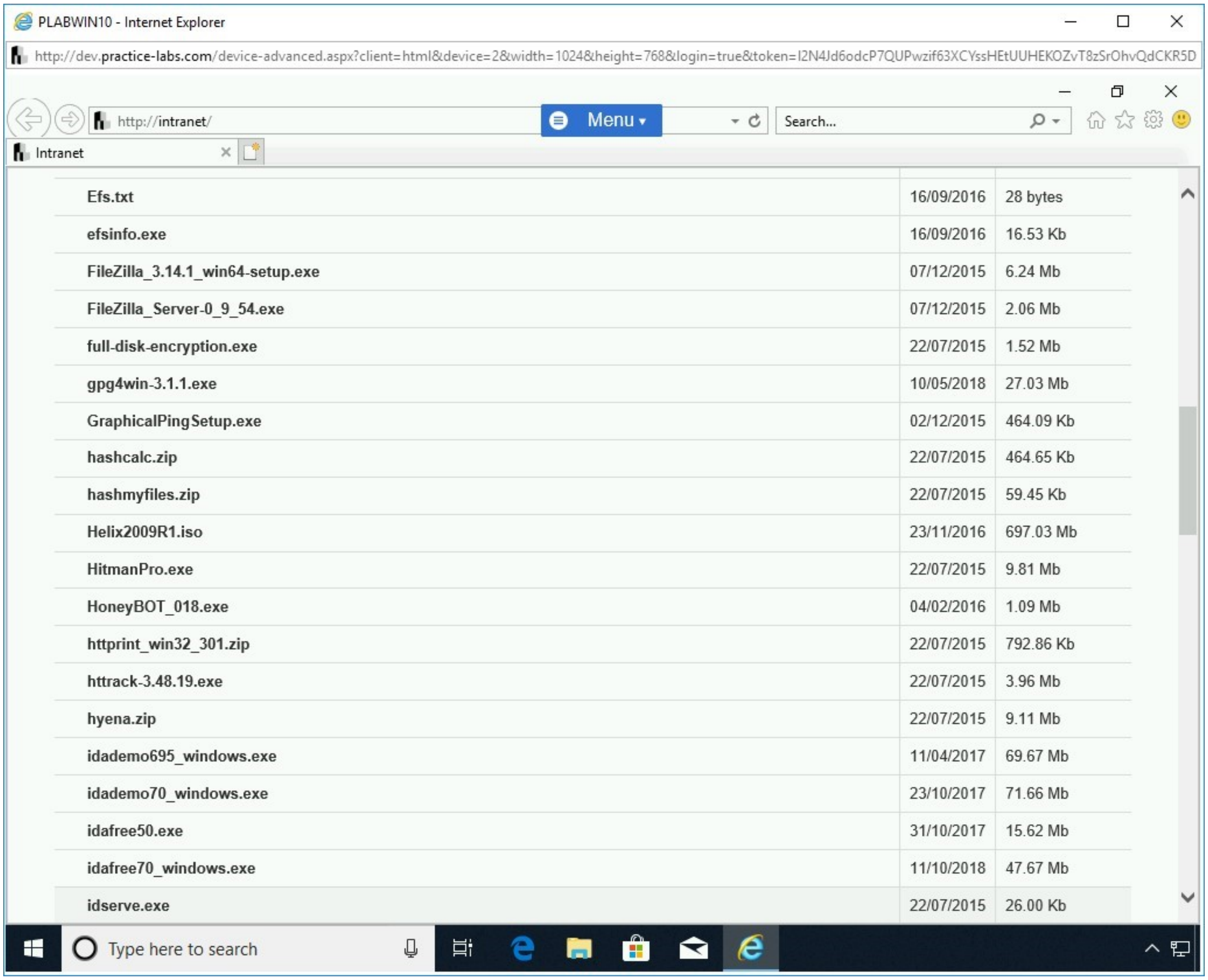

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=I2N4Jd6odcP7QUPwzif63XCYssHEtUUHEKOZvT8zSrOhvQdCKR5D
http://intranet/
Menu
Search...
Intranet
Type here to search

Elastix2.4	10/05/2017	1
Email Client	27/04/2017	3
Email Server	27/04/2017	2
ettercap	21/05/2019	3
Exchange_Server	22/07/2015	8
FTK	22/07/2015	3
Hacking Tools	22/07/2015	91
IIS	27/04/2017	2
IntelliTraceCollector	22/07/2016	1
Misc	22/07/2015	67
Monitoring	22/07/2015	5
Networking	22/07/2015	2
nmap	22/07/2015	1
OpenPGP	27/04/2017	2
Oracle	25/08/2015	1
Palo Alto	03/03/2016	1
PerfMon	23/11/2016	1
SafePad 1.3	27/04/2017	4

Figure 1.4 Screenshot of PLABWIN10: Clicking the Hacking Tools folder on the intranet Website.

Step 5

Scroll down and click **idserve.exe**.

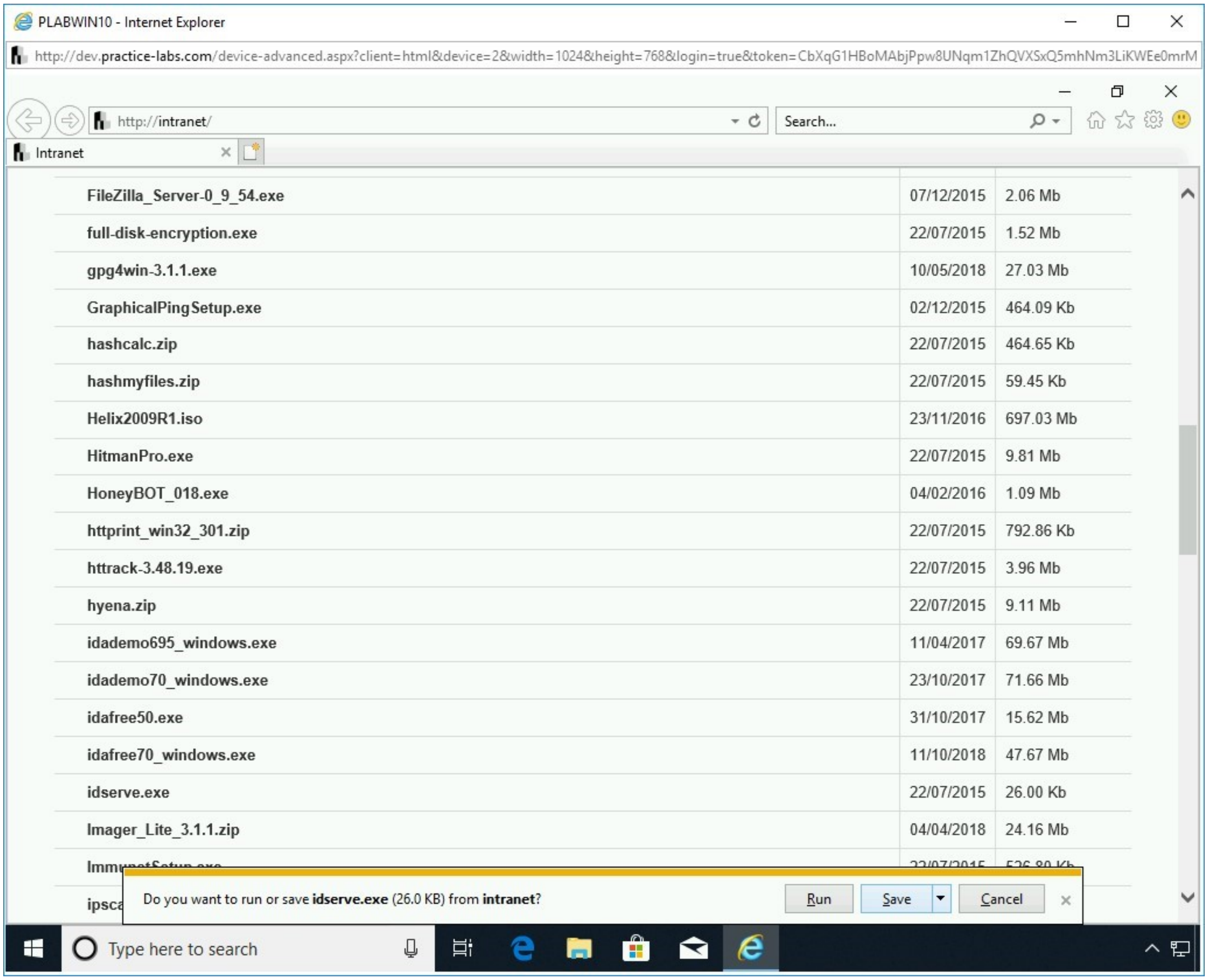

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=I2N4Jd6odcP7QUPwzif63XCYssHEtUUHEKOZvT8zSrOhvQdCKR5D
http://intranet/
Menu
Search...
Intranet
Type here to search

Efs.txt	16/09/2016	28 bytes
efsinfo.exe	16/09/2016	16.53 Kb
FileZilla_3.14.1_win64-setup.exe	07/12/2015	6.24 Mb
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4win-3.1.1.exe	10/05/2018	27.03 Mb
GraphicalPingSetup.exe	02/12/2015	464.09 Kb
hashcalc.zip	22/07/2015	464.65 Kb
hashmyfiles.zip	22/07/2015	59.45 Kb
Helix2009R1.iso	23/11/2016	697.03 Mb
HitmanPro.exe	22/07/2015	9.81 Mb
HoneyBOT_018.exe	04/02/2016	1.09 Mb
httprint_win32_301.zip	22/07/2015	792.86 Kb
httrack-3.48.19.exe	22/07/2015	3.96 Mb
hyena.zip	22/07/2015	9.11 Mb
idademo695_windows.exe	11/04/2017	69.67 Mb
idademo70_windows.exe	23/10/2017	71.66 Mb
idafree50.exe	31/10/2017	15.62 Mb
idafree70_windows.exe	11/10/2018	47.67 Mb
idserve.exe	22/07/2015	26.00 Kb

Figure 1.5 Screenshot of PLABWIN10: Clicking the idserve.exe tool.

Step 6

A notification bar appears at the bottom of Internet Explorer. Click **Save**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Type here to search

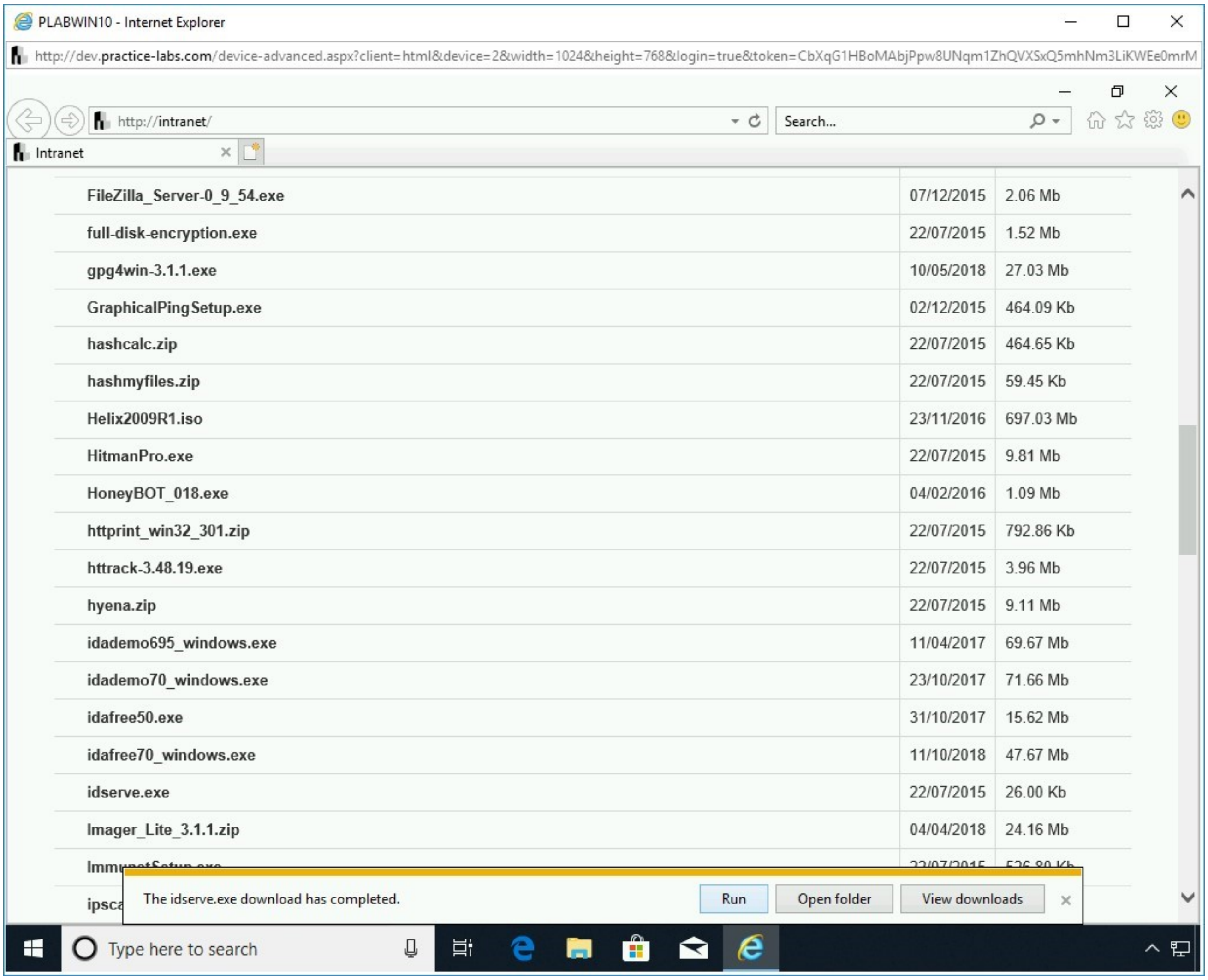
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4win-3.1.1.exe	10/05/2018	27.03 Mb
GraphicalPingSetup.exe	02/12/2015	464.09 Kb
hashcalc.zip	22/07/2015	464.65 Kb
hashmyfiles.zip	22/07/2015	59.45 Kb
Helix2009R1.iso	23/11/2016	697.03 Mb
HitmanPro.exe	22/07/2015	9.81 Mb
HoneyBOT_018.exe	04/02/2016	1.09 Mb
httprint_win32_301.zip	22/07/2015	792.86 Kb
httrack-3.48.19.exe	22/07/2015	3.96 Mb
hyena.zip	22/07/2015	9.11 Mb
idademo695_windows.exe	11/04/2017	69.67 Mb
idademo70_windows.exe	23/10/2017	71.66 Mb
idafree50.exe	31/10/2017	15.62 Mb
idafree70_windows.exe	11/10/2018	47.67 Mb
idserve.exe	22/07/2015	26.00 Kb
Imager_Lite_3.1.1.zip	04/04/2018	24.16 Mb
ImmunetSetup.exe	22/07/2015	526.80 Kb
ipsca		

Do you want to run or save **idserve.exe** (26.0 KB) from **intranet**?

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

Step 7

Click **Run** on the notification bar.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Type here to search

FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4win-3.1.1.exe	10/05/2018	27.03 Mb
GraphicalPingSetup.exe	02/12/2015	464.09 Kb
hashcalc.zip	22/07/2015	464.65 Kb
hashmyfiles.zip	22/07/2015	59.45 Kb
Helix2009R1.iso	23/11/2016	697.03 Mb
HitmanPro.exe	22/07/2015	9.81 Mb
HoneyBOT_018.exe	04/02/2016	1.09 Mb
httprint_win32_301.zip	22/07/2015	792.86 Kb
httrack-3.48.19.exe	22/07/2015	3.96 Mb
hyena.zip	22/07/2015	9.11 Mb
idademo695_windows.exe	11/04/2017	69.67 Mb
idademo70_windows.exe	23/10/2017	71.66 Mb
idafree50.exe	31/10/2017	15.62 Mb
idafree70_windows.exe	11/10/2018	47.67 Mb
idserve.exe	22/07/2015	26.00 Kb
Imager_Lite_3.1.1.zip	04/04/2018	24.16 Mb
ImmunetSetup.exe	22/07/2015	526.80 Kb
ipsca		

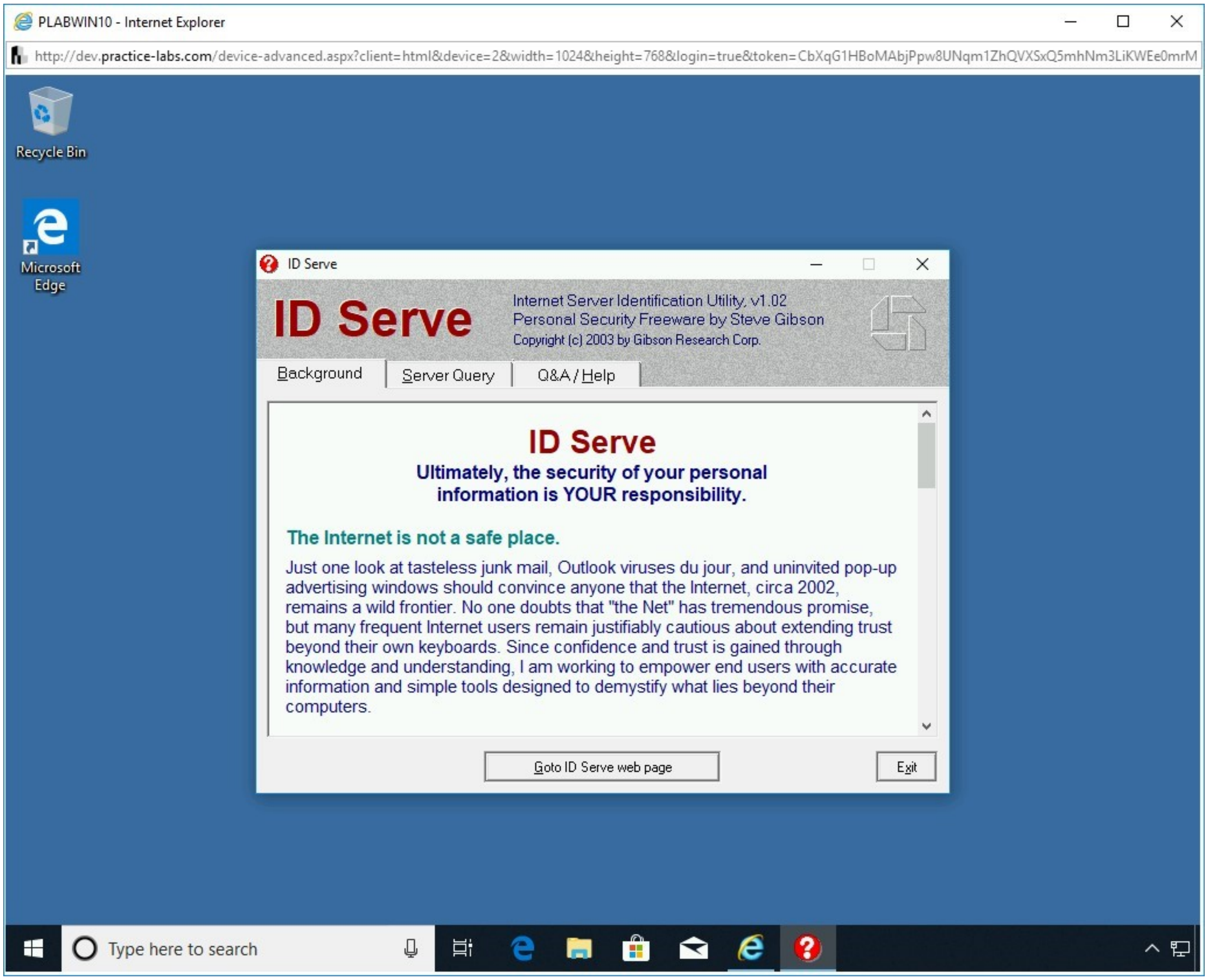
The idserve.exe download has completed.

Figure 1.7 Screenshot of PLABWIN10: Clicking Run in the notification bar.

Step 8

Minimize the **Internet Explorer** window.

On the **ID Serve** window, click the **Server Query** tab.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
Recycle Bin
Microsoft Edge
ID Serve
Background
Server Query
Q&A / Help
Goto ID Serve web page
Exit
Type here to search

ID Serve

Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.

ID Serve

Ultimately, the security of your personal information is YOUR responsibility.

The Internet is not a safe place.

Just one look at tasteless junk mail, Outlook viruses du jour, and uninvited pop-up advertising windows should convince anyone that the Internet, circa 2002, remains a wild frontier. No one doubts that "the Net" has tremendous promise, but many frequent Internet users remain justifiably cautious about extending trust beyond their own keyboards. Since confidence and trust is gained through knowledge and understanding, I am working to empower end users with accurate information and simple tools designed to demystify what lies beyond their computers.

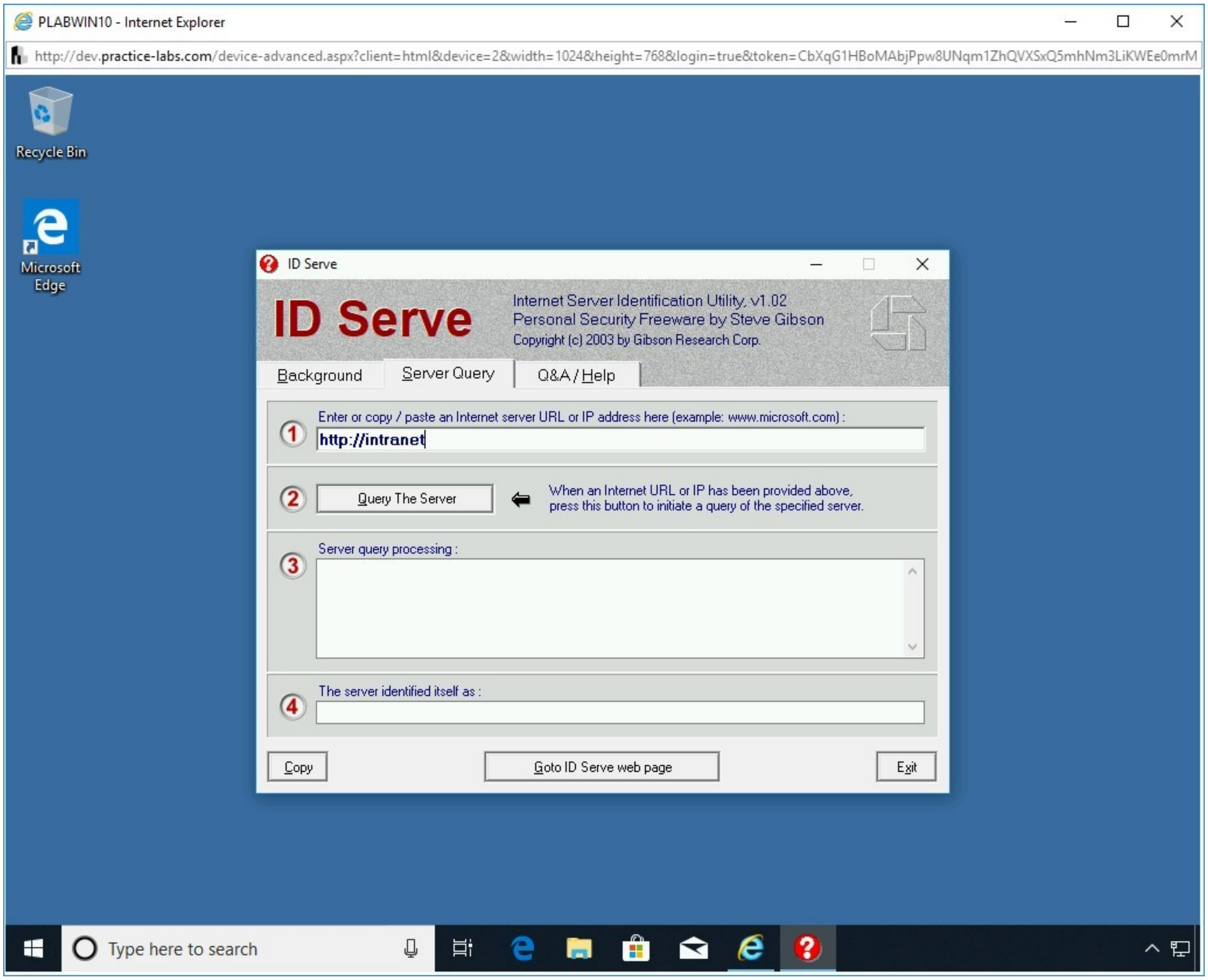
Figure 1.8 Screenshot of PLABWIN10: Clicking the Server Query tab in the ID Serve dialog box.

Step 9

On the **Server Query** tab, type the following URL in the **Enter or copy / paste an Internet server URL or IP address here** text box:

```
http://intranet
```

Click **Query The Server**.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM

ID Serve

Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.

1 Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com) :

http://intranet

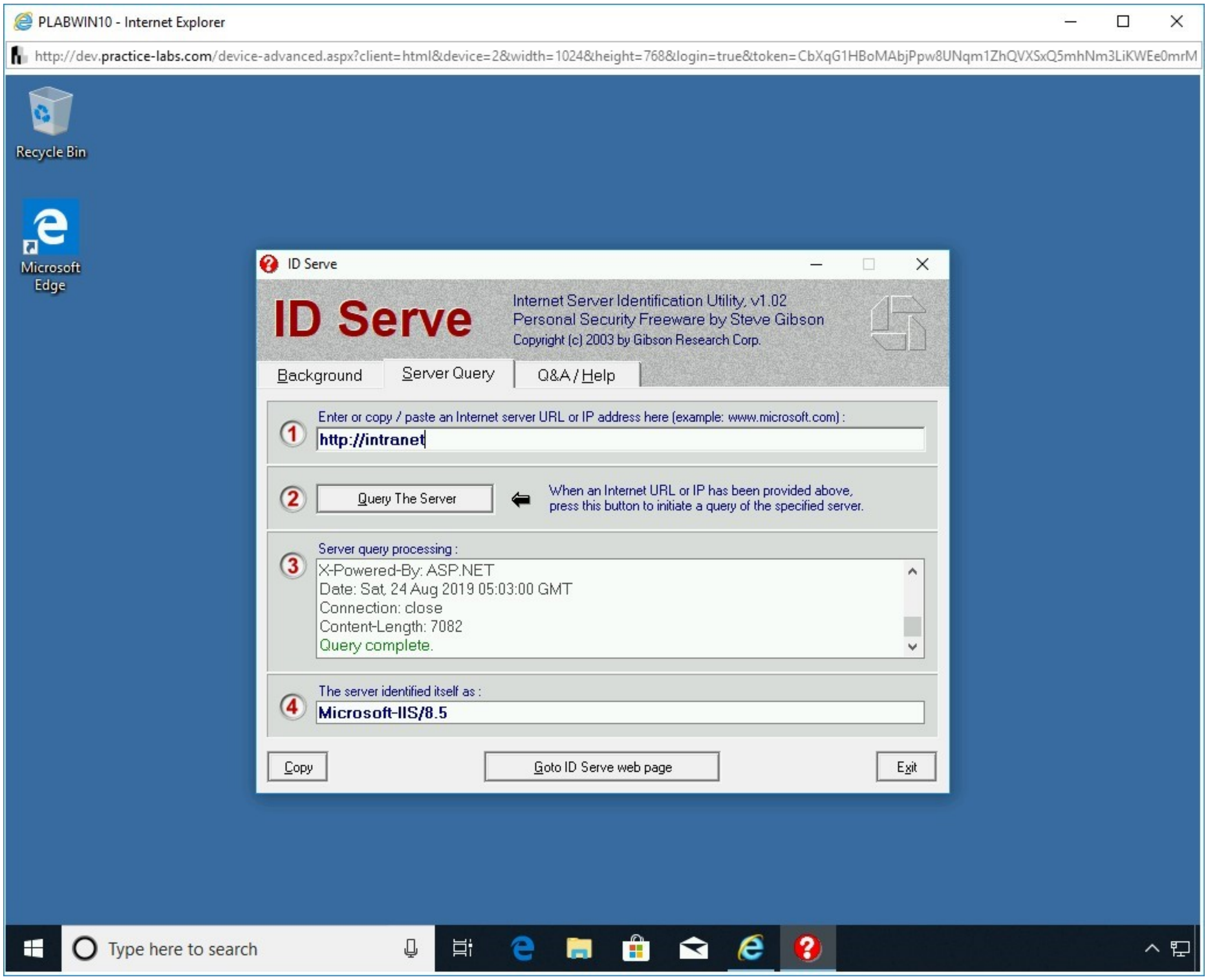
2 When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.

3 Server query processing :

4 The server identified itself as :

Figure 1.9 Screenshot of PLABWIN10: Typing the URL for the Intranet Website and clicking Query The Server.

A lot of Web server information is displayed.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM

Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.

Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com) :
http://intranet

When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.

Server query processing :

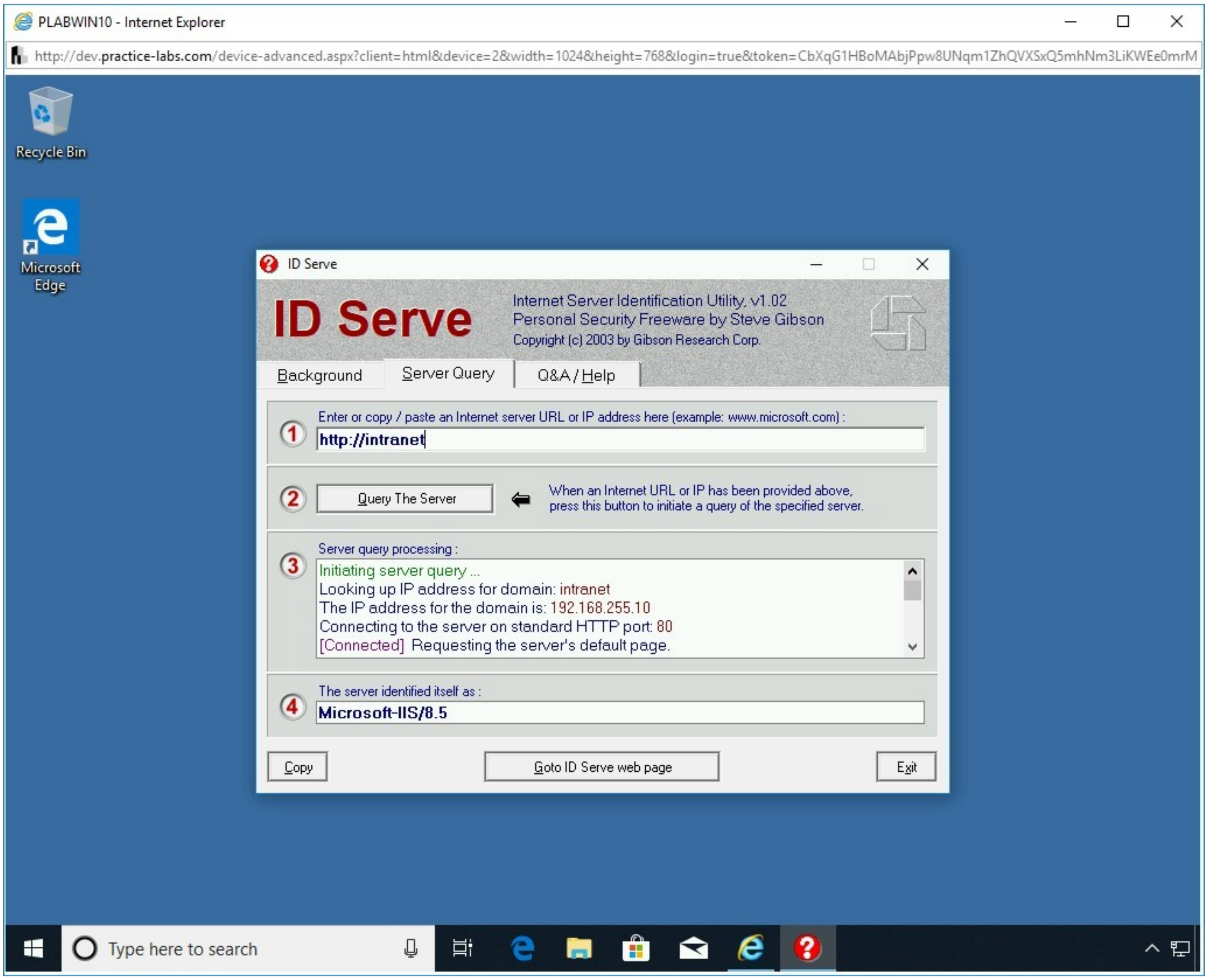
```
X-Powered-By: ASP.NET
Date: Sat, 24 Aug 2019 05:03:00 GMT
Connection: close
Content-Length: 7082
Query complete.
```

The server identified itself as :
Microsoft-IIS/8.5

Figure 1.10 Screenshot of PLABWIN10: Showing the configuration of the Intranet Webserver.

Step 10

You can scroll up and find the Webserver’s IP address.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
Recycle Bin
Microsoft Edge
ID Serve
ID Serve
Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.
Background
Server Query
Q&A / Help
1
2
Query The Server
When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.
3
4
Copy
Goto ID Serve web page
Exit
Type here to search

Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com) :
http://intranet

Server query processing :

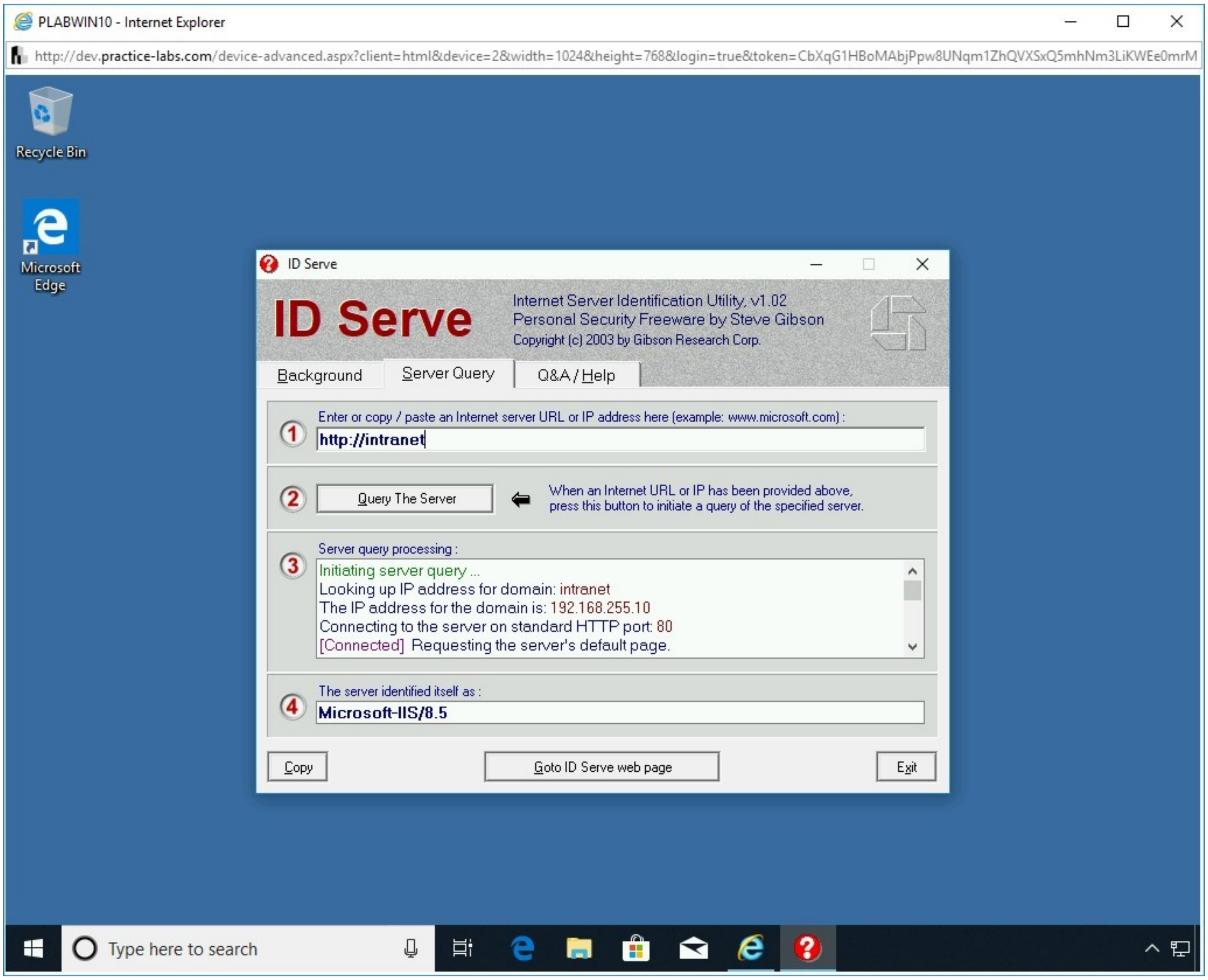
```
Initiating server query ...
Looking up IP address for domain: intranet
The IP address for the domain is: 192.168.255.10
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
```

The server identified itself as :
Microsoft-IIS/8.5

Figure 1.11 Screenshot of PLABWIN10: Showing the IP address of the Intranet Webserver.

Step 11

Click **Exit** to close the **ID Serve** dialog box.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
Recycle Bin
Microsoft Edge
ID Serve
Background
Server Query
Q&A / Help
Query The Server
Copy
Goto ID Serve web page
Exit
Type here to search

ID Serve

Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.

1 Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com) :
http://intranet

2 When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.

3 Server query processing :

```
Initiating server query ...
Looking up IP address for domain: intranet
The IP address for the domain is: 192.168.255.10
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
```

4 The server identified itself as :
Microsoft-IIS/8.5

Figure 1.12 Screenshot of PLABWIN10: Clicking Exit to close the ID Server dialog box.

Task 2 - Explore a Network Using Nmap

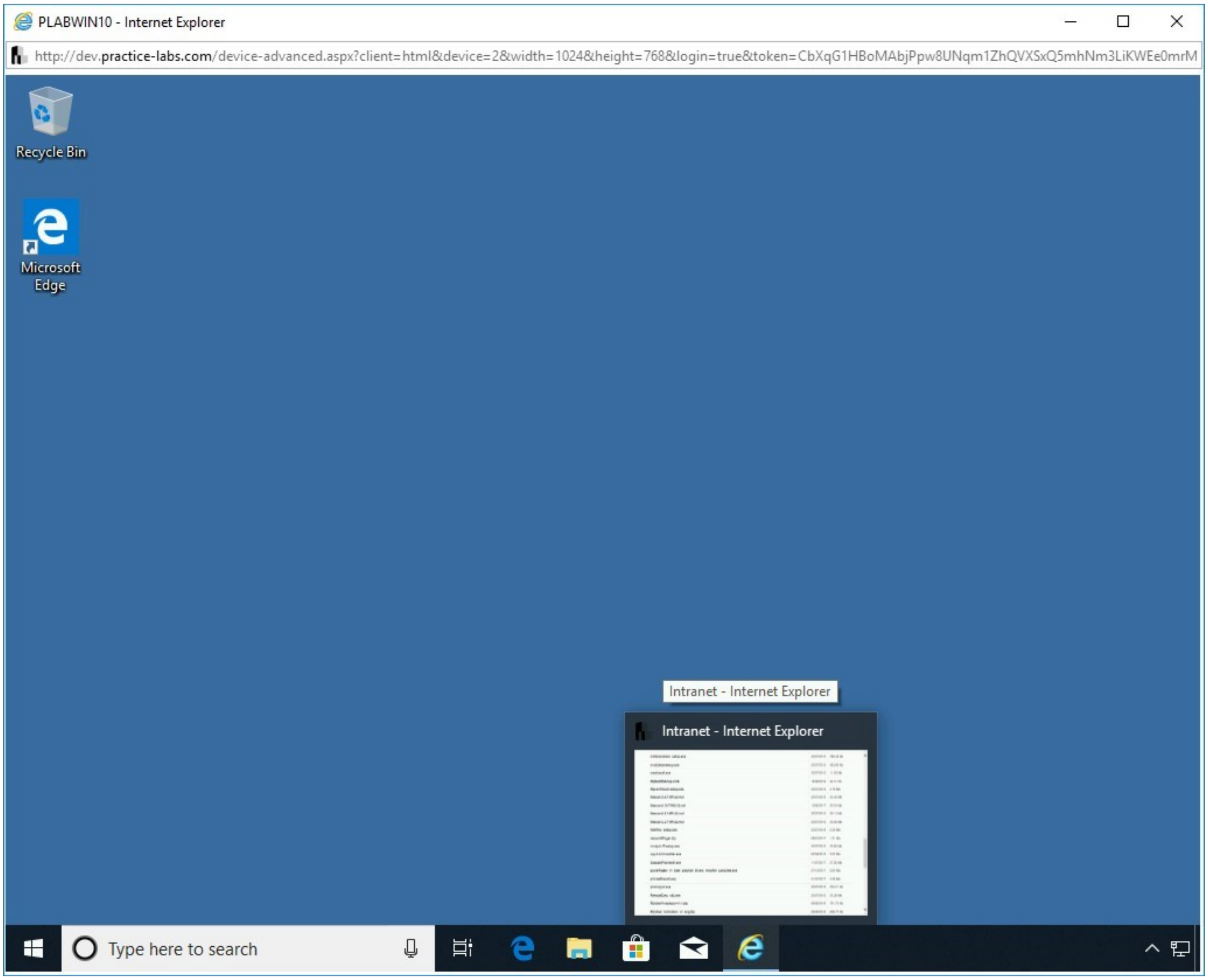
Nmap has a graphical user interface (GUI) with the name Zenmap. It has the same capabilities as Nmap. You can scan for ports, services, and so on.

In this task, you will explore a network using Nmap. To do this, perform the following steps:

Step 1

Ensure you have powered on the required devices and connect to **PLABWIN10**.

Restore the **Internet Explorer** window from the taskbar.



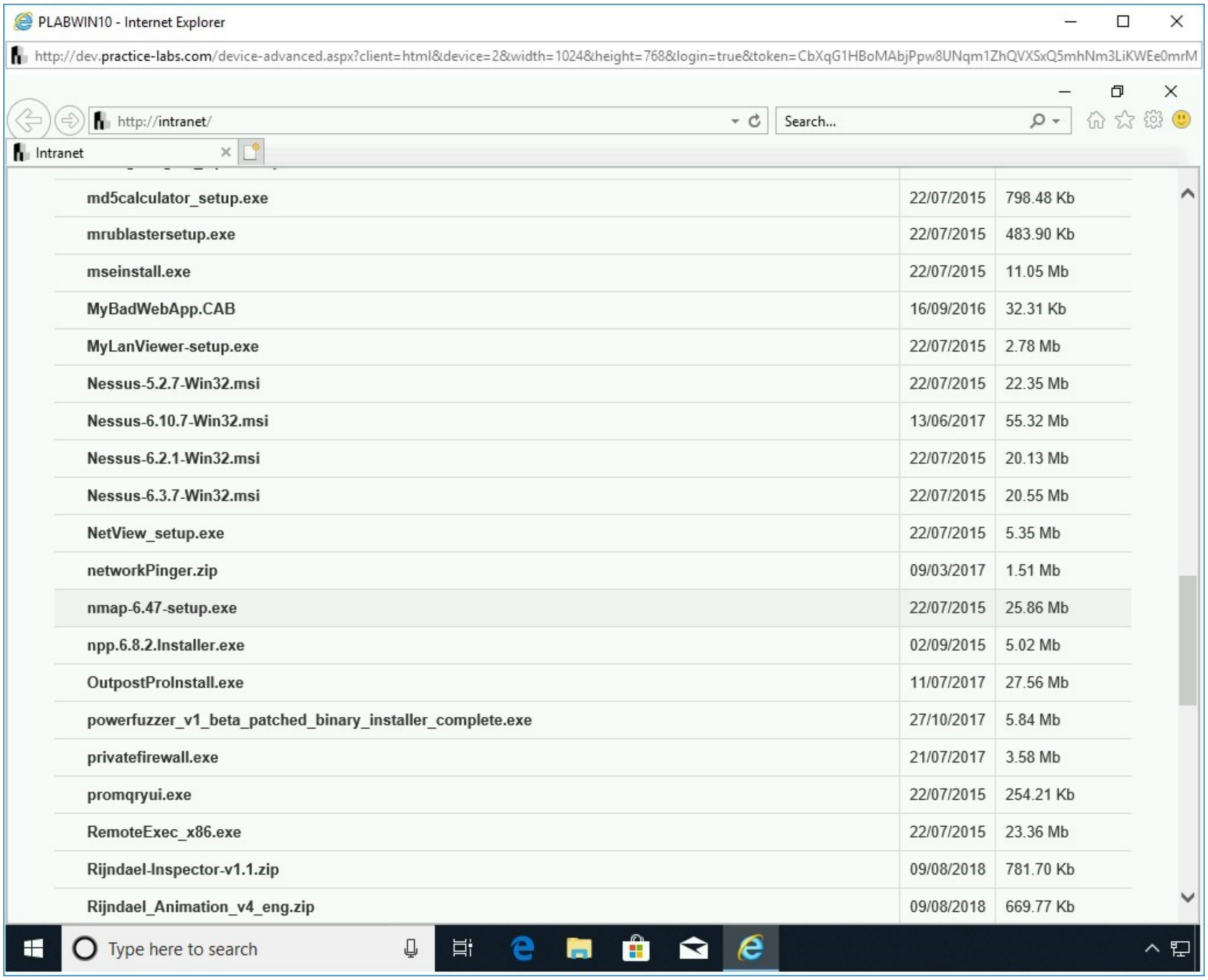
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM

PLABWIN10 - Internet Explorer
Recycle Bin
Microsoft Edge
Intranet - Internet Explorer
Intranet - Internet Explorer
Type here to search

Figure 1.13 Screenshot of PLABWIN10: Restoring Internet Explorer from the taskbar.

Step 2

Ensure that you are on the **Hacking Tools** page on the **Intranet** Website. Scroll down and click **nmap-6.47-setup.exe**.

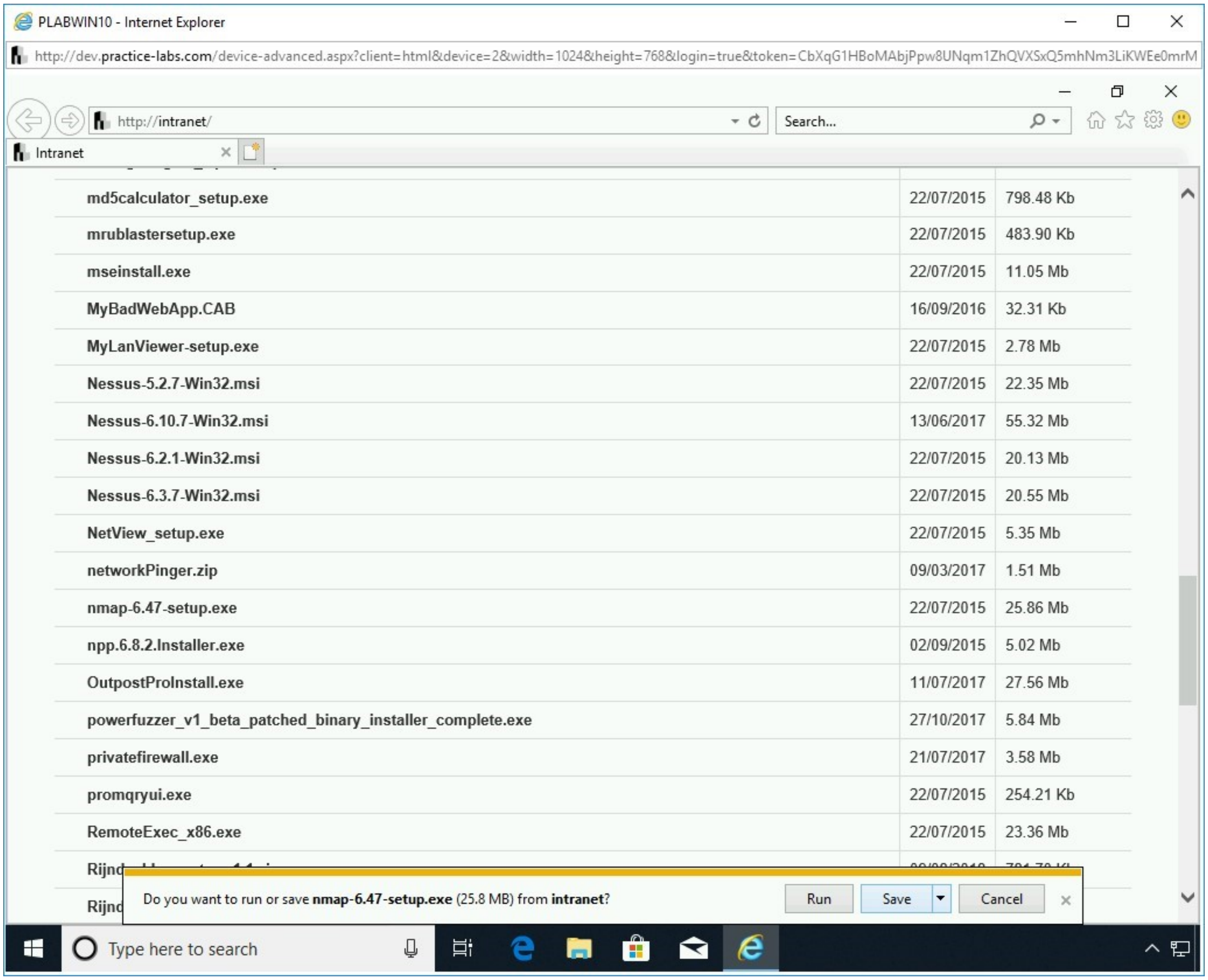

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Type here to search

md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb

Figure 1.14 Screenshot of PLABWIN10: Clicking the nmap executable from the Intranet Website.

Step 3

A notification bar appears. Click **Save**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Type here to search

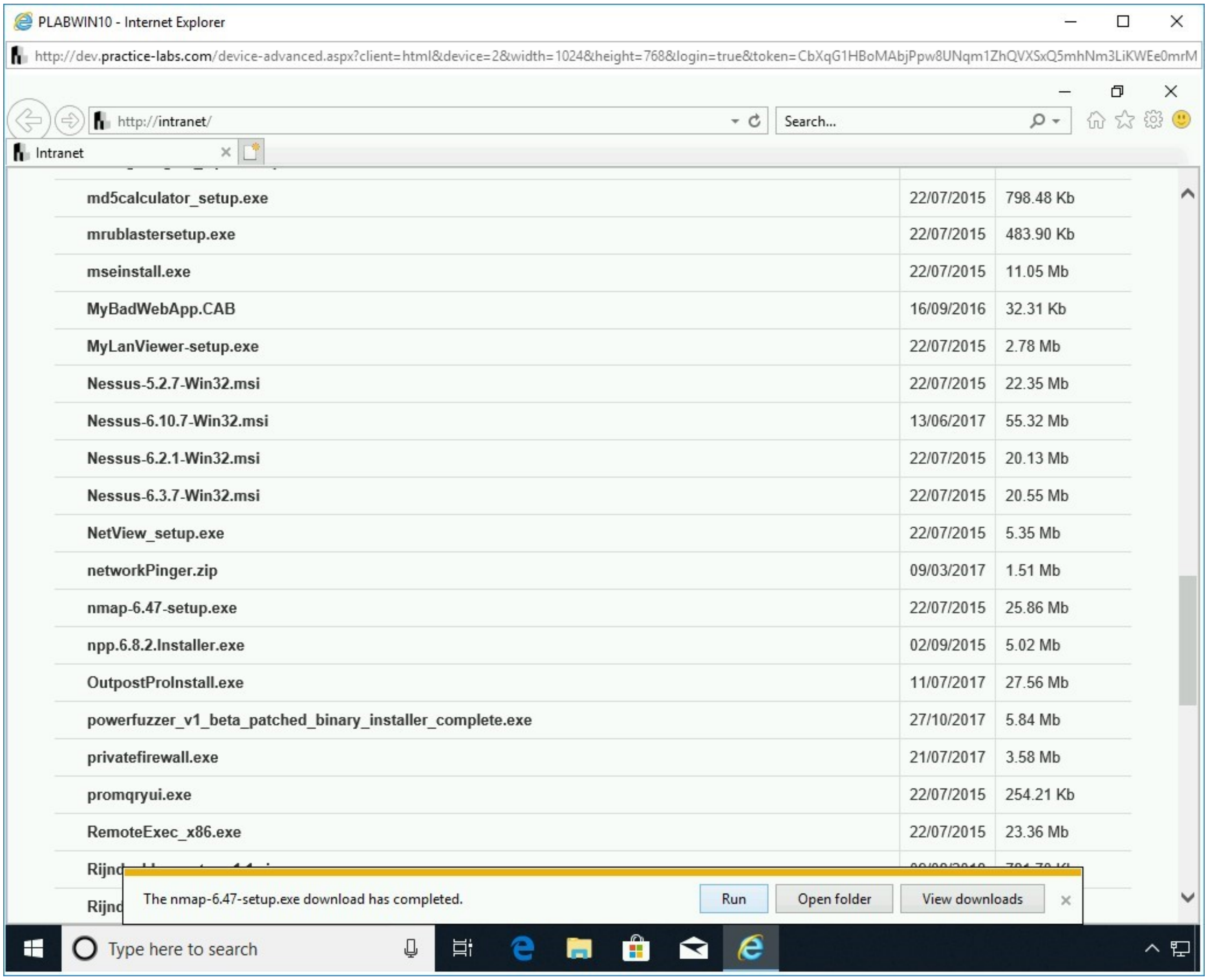
md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijnd		
Rijnd		

Do you want to run or save **nmap-6.47-setup.exe** (25.8 MB) from **intranet**?

Figure 1.15 Screenshot of PLABWIN10: Clicking Save in the notification bar.

Step 4

After the installer is downloaded, click **Run** in the notification bar.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Run
Open folder
View downloads
Type here to search

md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijnd		
Rijnd		

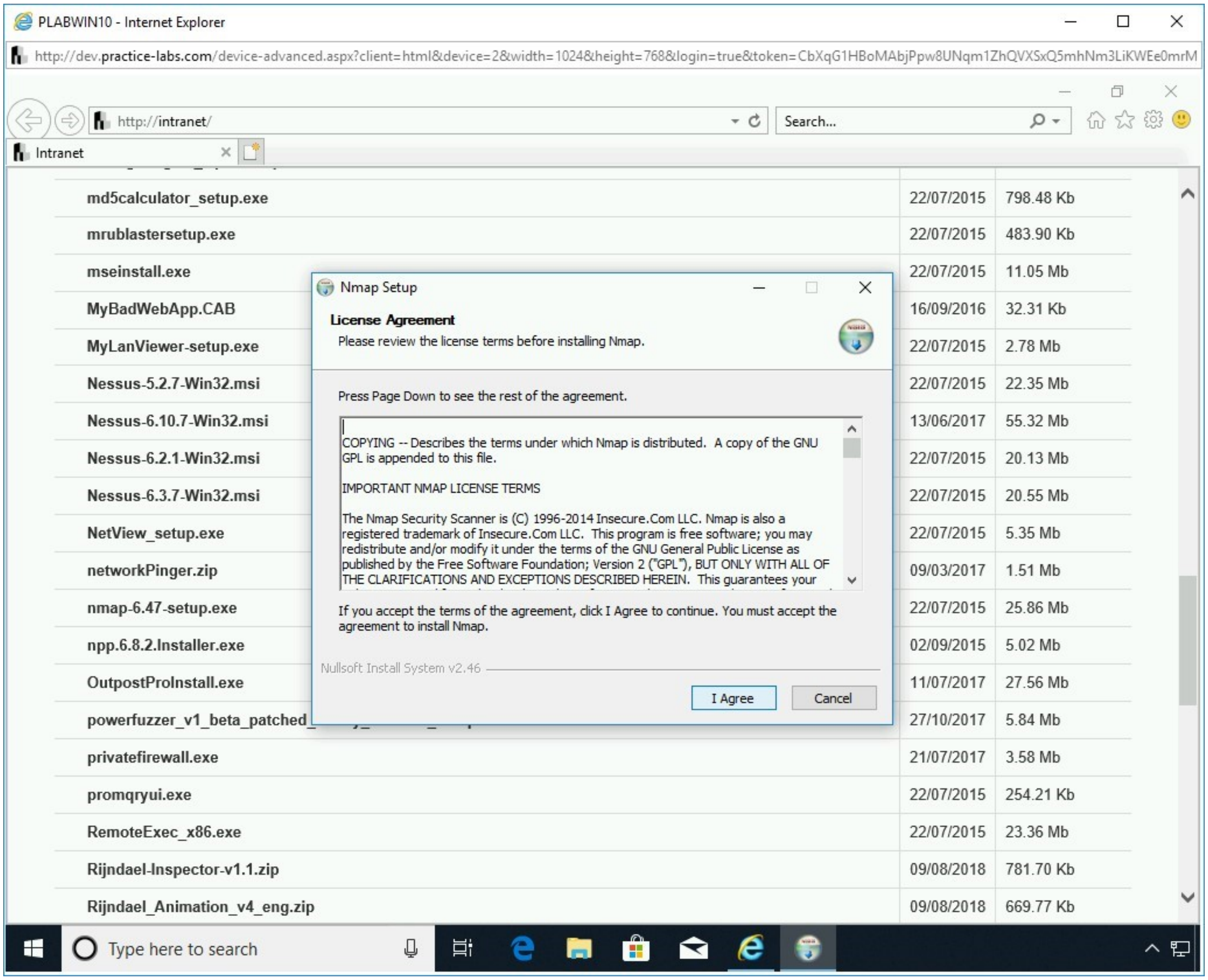
The nmap-6.47-setup.exe download has completed.

Figure 1.16 Screenshot of PLABWIN10: Clicking Run in the notification bar.

Step 5

The **Nmap Setup** dialog box is displayed.

On the **License Agreement** page, click **I Agree**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Type here to search

md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb

Nmap Setup

License Agreement

Please review the license terms before installing Nmap.

Press Page Down to see the rest of the agreement.

COPYING -- Describes the terms under which Nmap is distributed. A copy of the GNU GPL is appended to this file.

IMPORTANT NMAP LICENSE TERMS

The Nmap Security Scanner is (C) 1996-2014 Insecure.Com LLC. Nmap is also a registered trademark of Insecure.Com LLC. This program is free software; you may redistribute and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; Version 2 ("GPL"), BUT ONLY WITH ALL OF THE CLARIFICATIONS AND EXCEPTIONS DESCRIBED HEREIN. This guarantees your

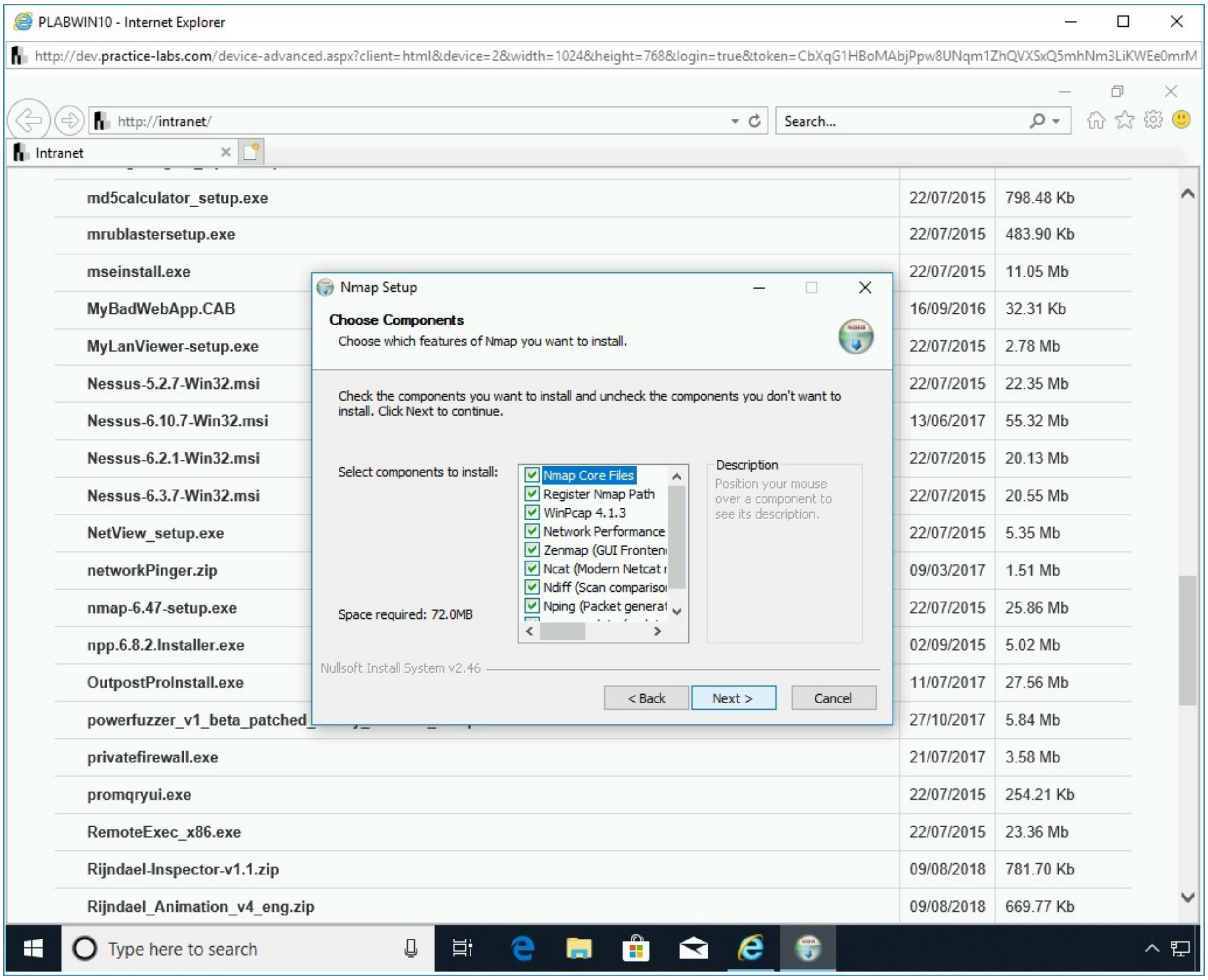
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Nmap.

Nullsoft Install System v2.46

Figure 1.17 Screenshot of PLABWIN10: Clicking I Agree on the License Agreement page.

Step 6

On the **Choose Components** page, keep the default selection and click **Next**.


PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM

http://intranet/

Intranet

md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb

Nmap Setup

Choose Components

Choose which features of Nmap you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

- ☑ Nmap Core Files
- ☑ Register Nmap Path
- ☑ WinPcap 4.1.3
- ☑ Network Performance
- ☑ Zenmap (GUI Fronten
- ☑ Ncat (Modern Netcat r
- ☑ Ndiff (Scan compariso
- ☑ Nping (Packet generat

Description

Position your mouse over a component to see its description.

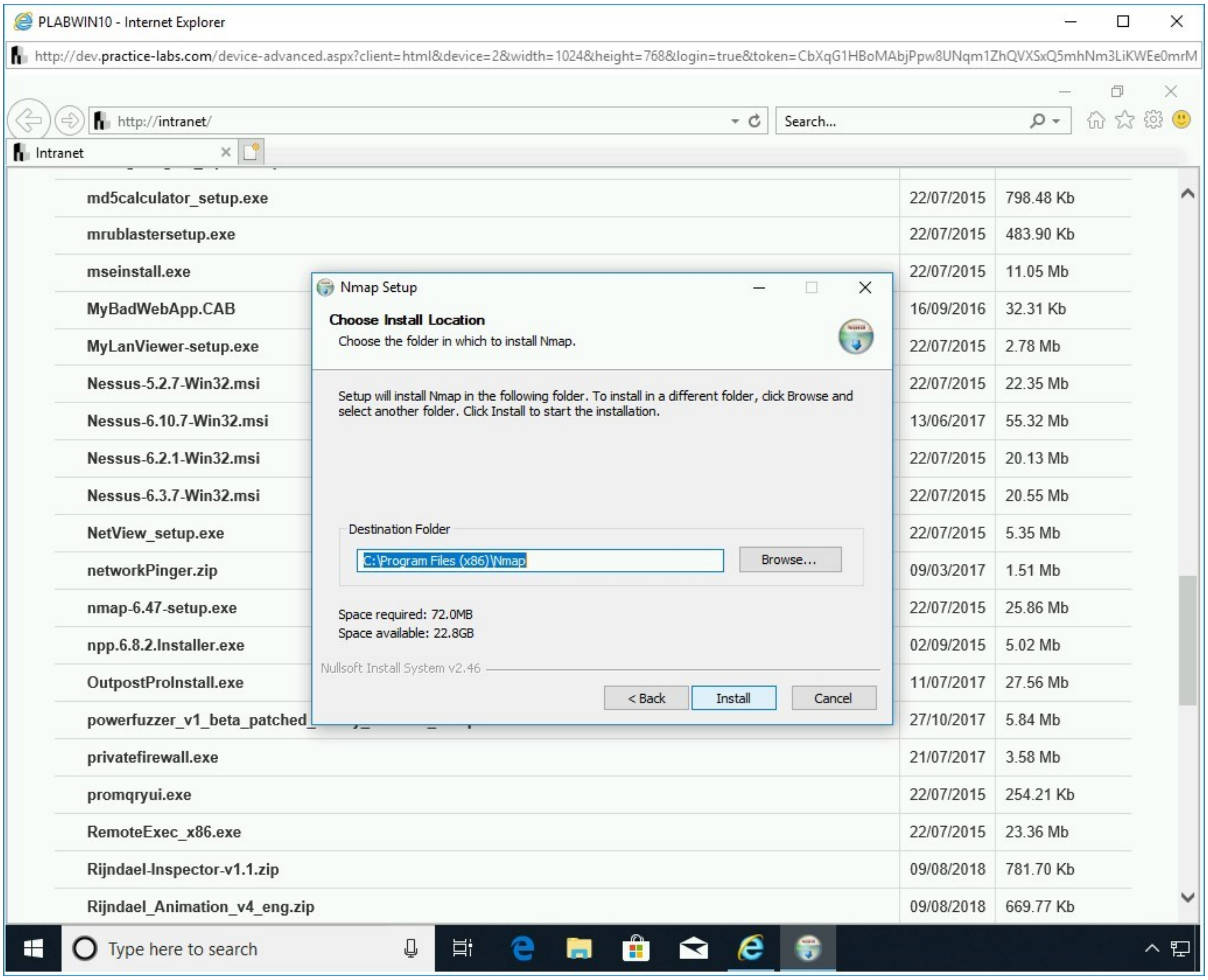
Space required: 72.0MB

Nullsoft Install System v2.46

Figure 1.18 Screenshot of PLABWIN10: Keeping the default selection and clicking Next on the Choose Components page.

Step 7

On the **Choose Install Location** page, keep the default Destination Folder path, and click **Install**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Type here to search

Nmap Setup

Choose Install Location

Choose the folder in which to install Nmap.

Setup will install Nmap in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder

C:\Program Files (x86)\Nmap

Space required: 72.0MB
Space available: 22.8GB

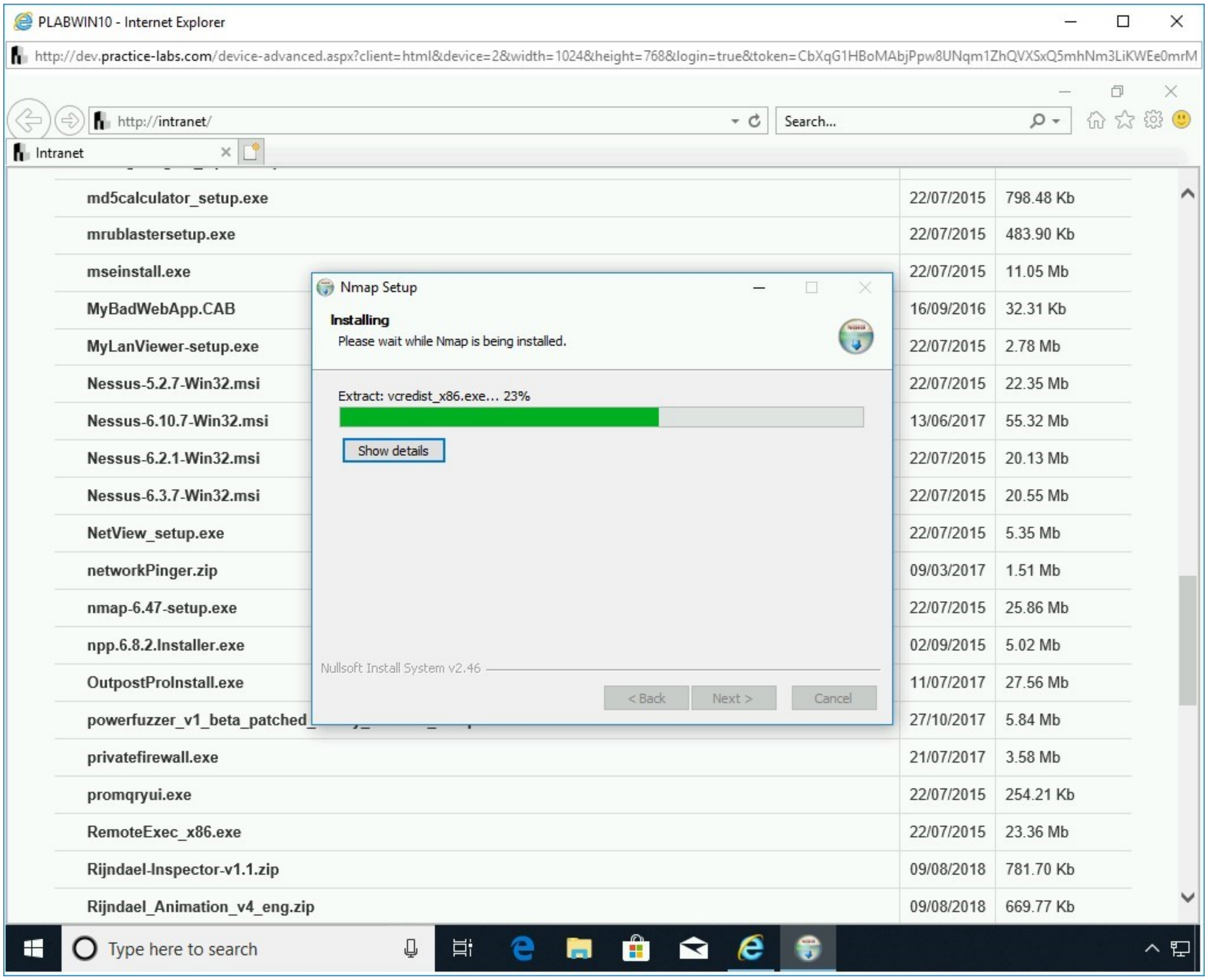
Nullsoft Install System v2.46

Browse...
< Back
Install
Cancel

md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb

Figure 1.19 Screenshot of PLABWIN10: Keeping the default location and clicking Install on the Choose Install Location.

The installation progress is displayed.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Nmap Setup
Show details
Nullsoft Install System v2.46
< Back
Next >
Cancel
Type here to search

Installing

Please wait while Nmap is being installed.

Extract: vcredist_x86.exe... 23%

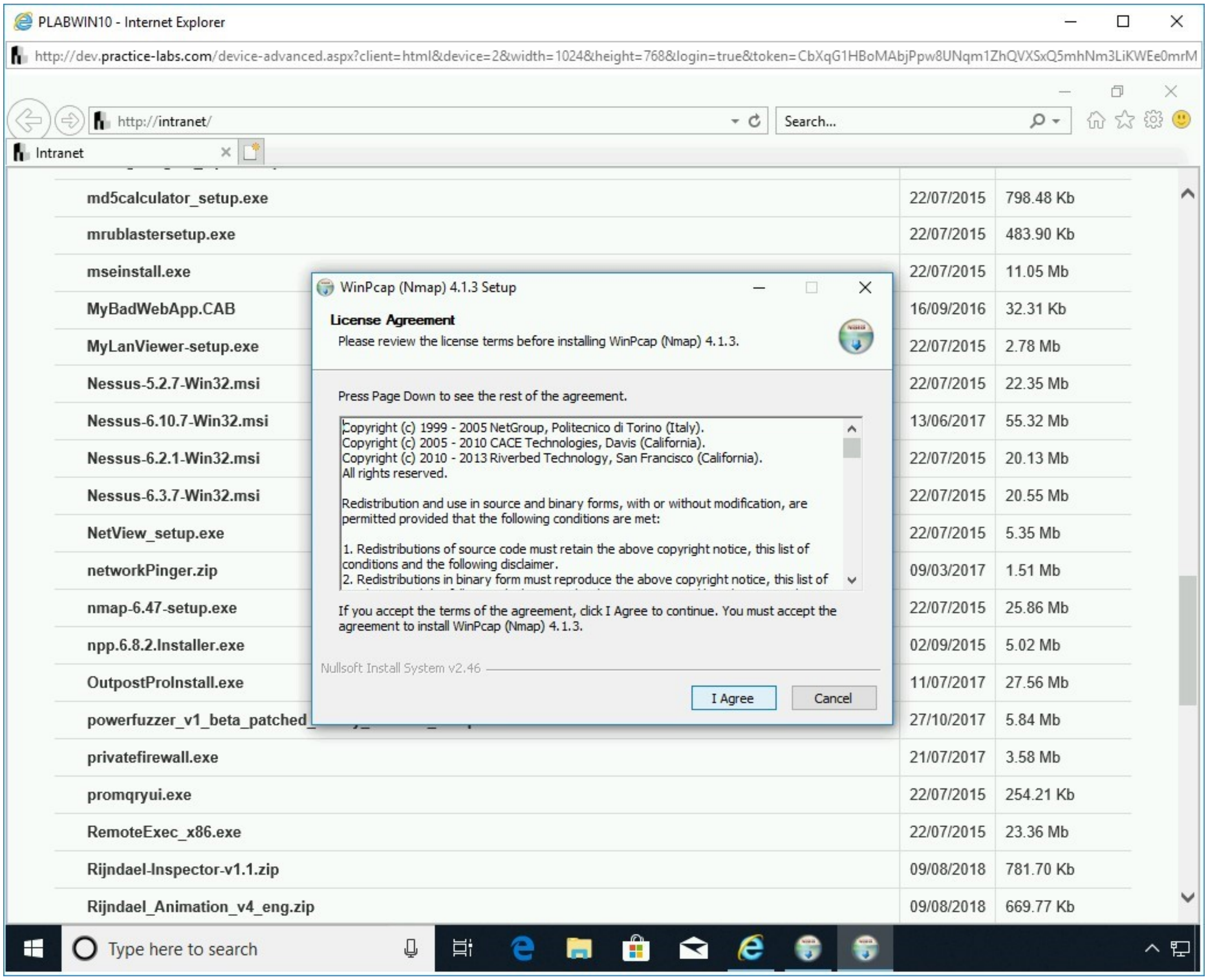
md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb

Figure 1.20 Screenshot of PLABWIN10: Showing the installation progress on the Installing page.

Step 8

Another dialog box named **WinPcap (Nmap) 4.1.3 Setup** is displayed.

On the **License Agreement** page, click **I Agree**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet

md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb

License Agreement

Please review the license terms before installing WinPcap (Nmap) 4.1.3.

Press Page Down to see the rest of the agreement.

Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
Copyright (c) 2010 - 2013 Riverbed Technology, San Francisco (California).
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of

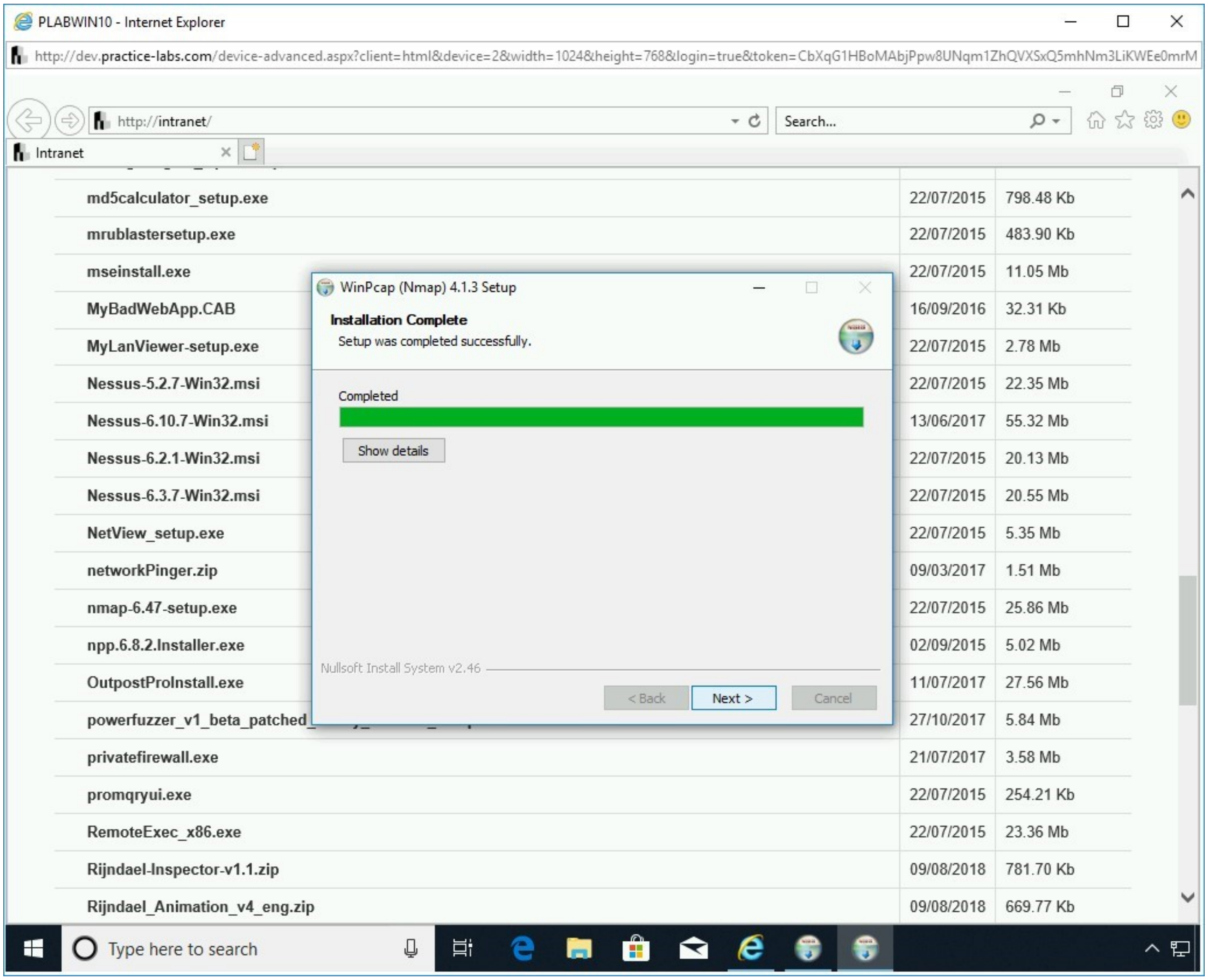
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinPcap (Nmap) 4.1.3.

Figure 1.21 Screenshot of PLABWIN10: Clicking I Agree on the License Agreement page.

Step 9

The installation progress for **WinPcap** is displayed.

Once complete, click **Next.**


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet

md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb

WinPcap (Nmap) 4.1.3 Setup

Installation Complete

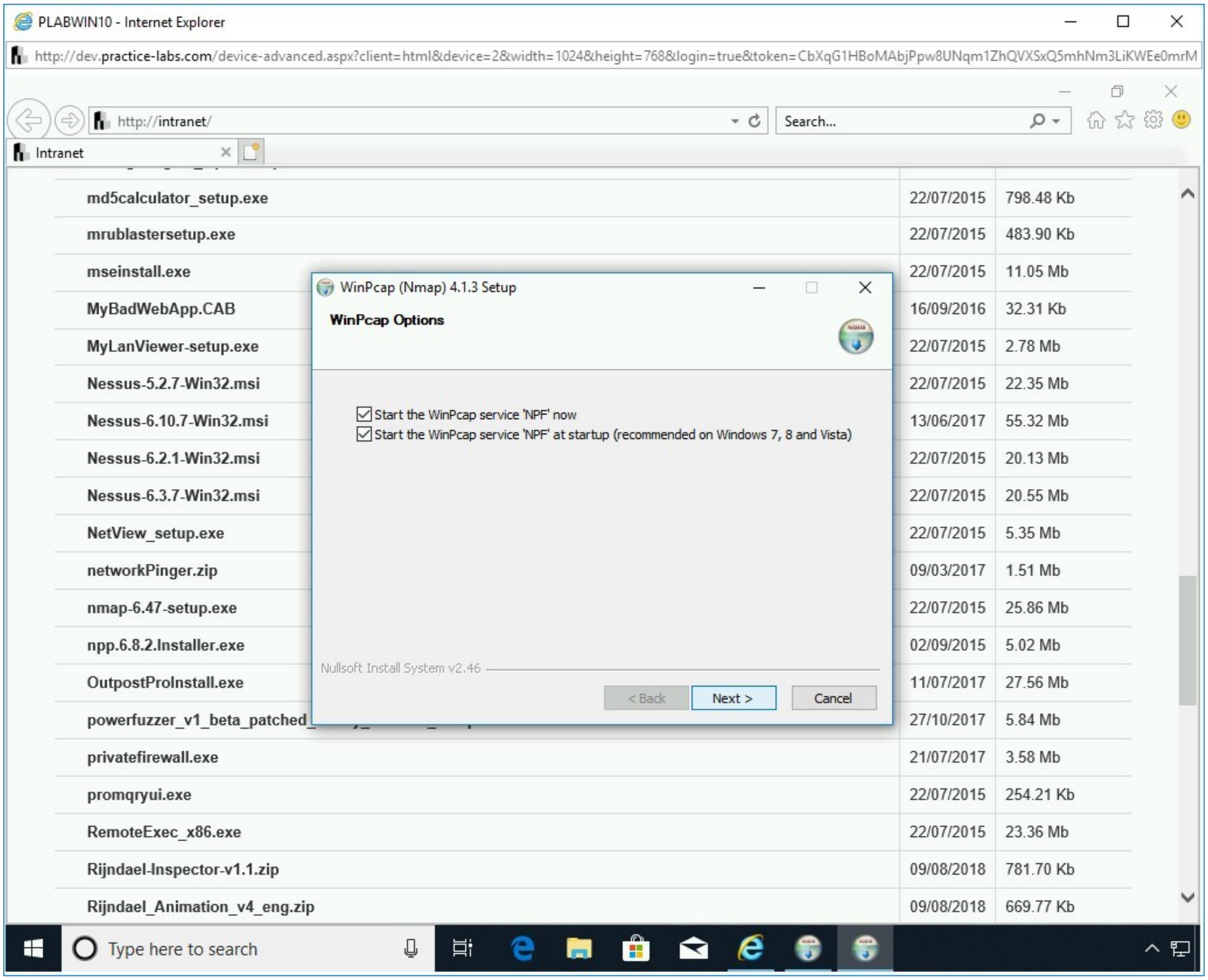
Setup was completed successfully.

Completed

Figure 1.22 Screenshot of PLABWIN10: Showing the installation completion and clicking Next.

Step 10

On the **WinPcap Options** page, keep the default selection and click **Next**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Type here to search

md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb

WinPcap (Nmap) 4.1.3 Setup

WinPcap Options

☑ Start the WinPcap service 'NPF' now

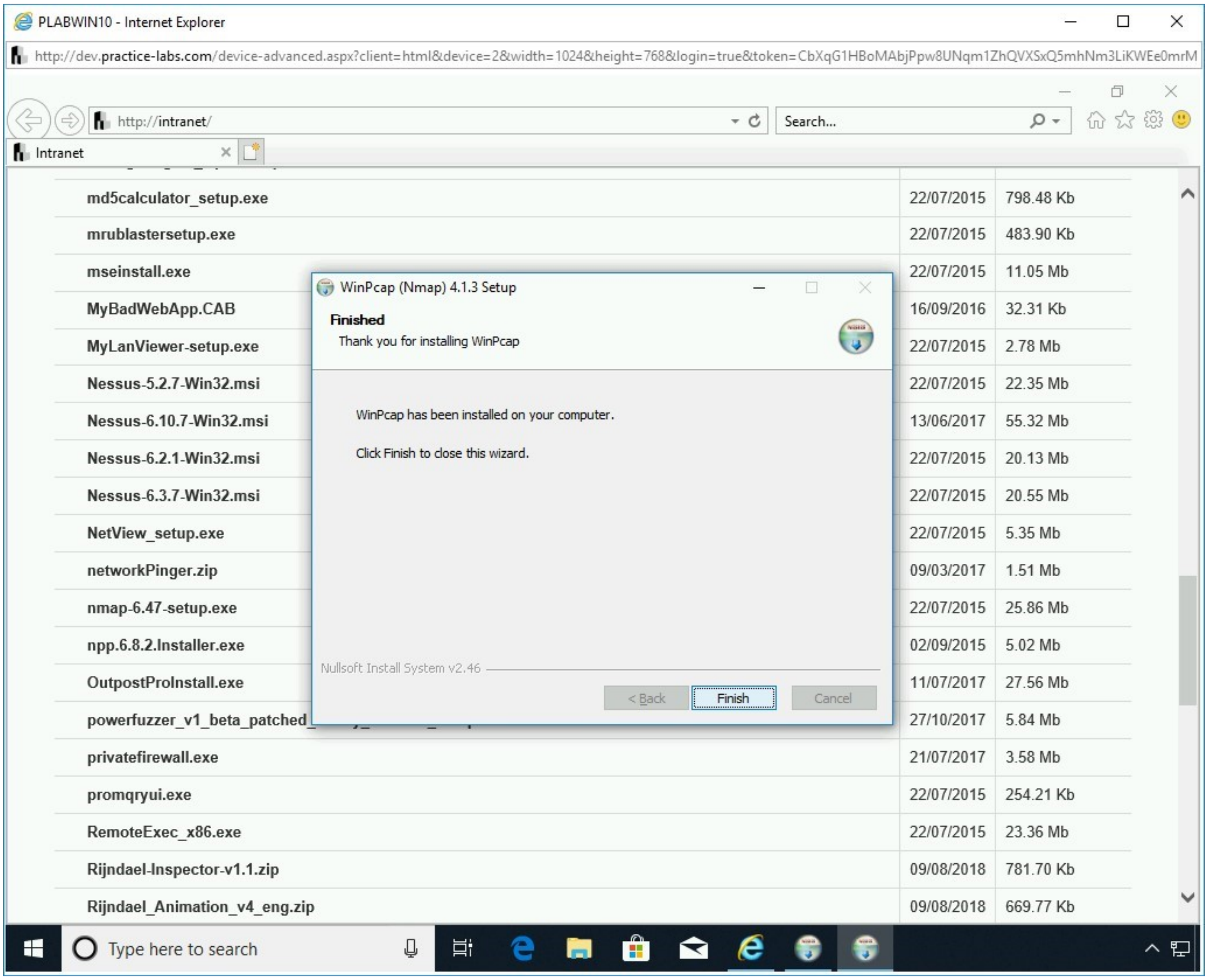
☑ Start the WinPcap service 'NPF' at startup (recommended on Windows 7, 8 and Vista)

Nullsoft Install System v2.46

Figure 1.23 Screenshot of PLABWIN10: Showing the options on the WinPcap Options and clicking Next.

Step 11

On the **Finished** page, click **Finish**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Type here to search

md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb

WinPcap (Nmap) 4.1.3 Setup

Finished

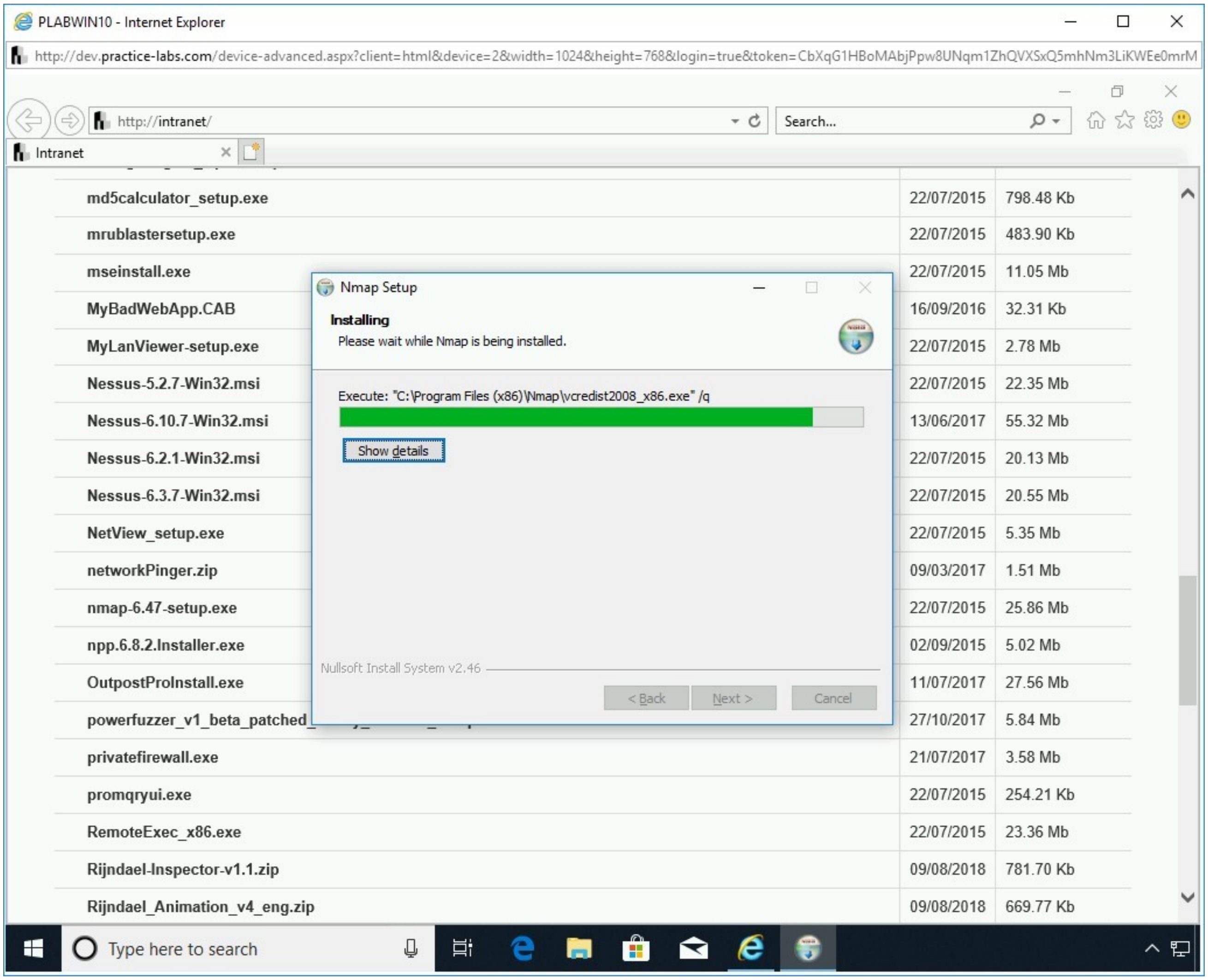
Thank you for installing WinPcap

WinPcap has been installed on your computer.

Click Finish to close this wizard.

Figure 1.24 Screenshot of PLABWIN10: Clicking Finish on the Finished page.

On the **Installing** page, the installation progress is displayed.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM

http://intranet/

Intranet

md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb

Nmap Setup

Installing

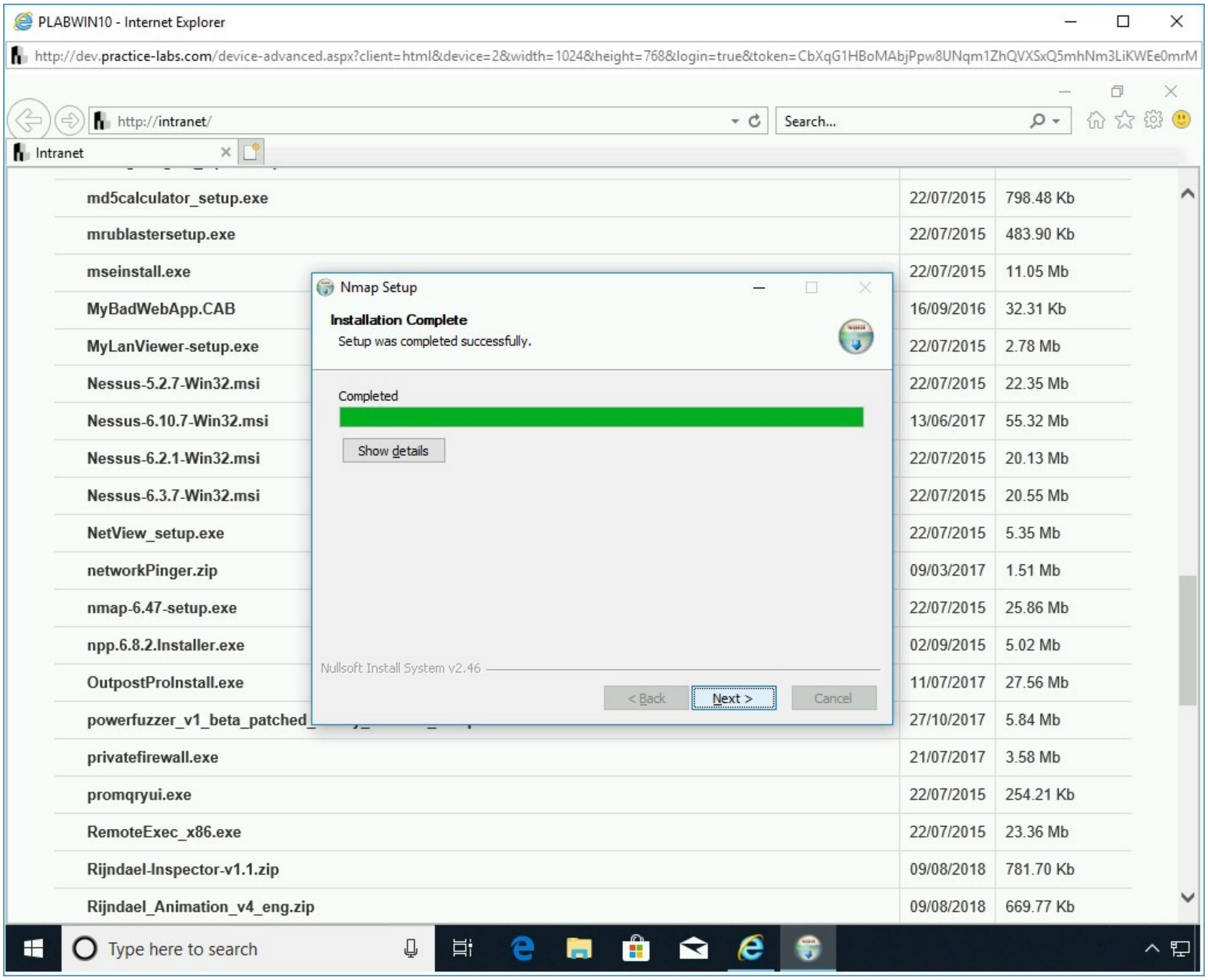
Please wait while Nmap is being installed.

Execute: "C:\Program Files (x86)\Nmap\vcredist2008_x86.exe" /q

Figure 1.25 Screenshot of PLABWIN10: Showing the installation progress on the Installing page.

Step 12

After the installation is completed, click **Next** on the **Installation Complete** page.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Type here to search

md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb

Nmap Setup

Installation Complete

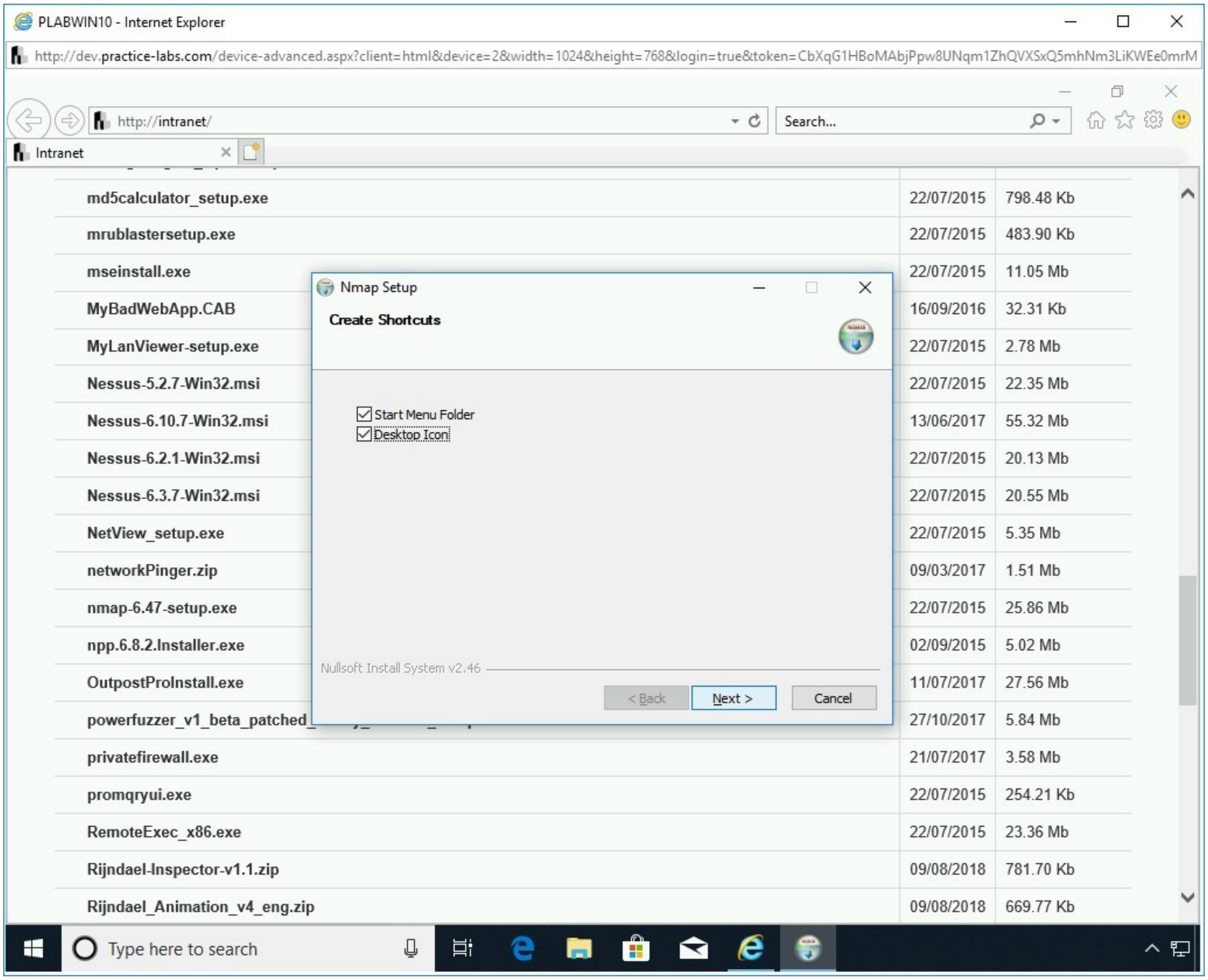
Setup was completed successfully.

Completed

Figure 1.26 Screenshot of PLABWIN10: Clicking Next on the Installation Complete page.

Step 13

On the **Create Shortcuts** page, keep the default selection and click **Next**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Nmap Setup
< Back
Next >
Cancel
Type here to search

md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb

Create Shortcuts

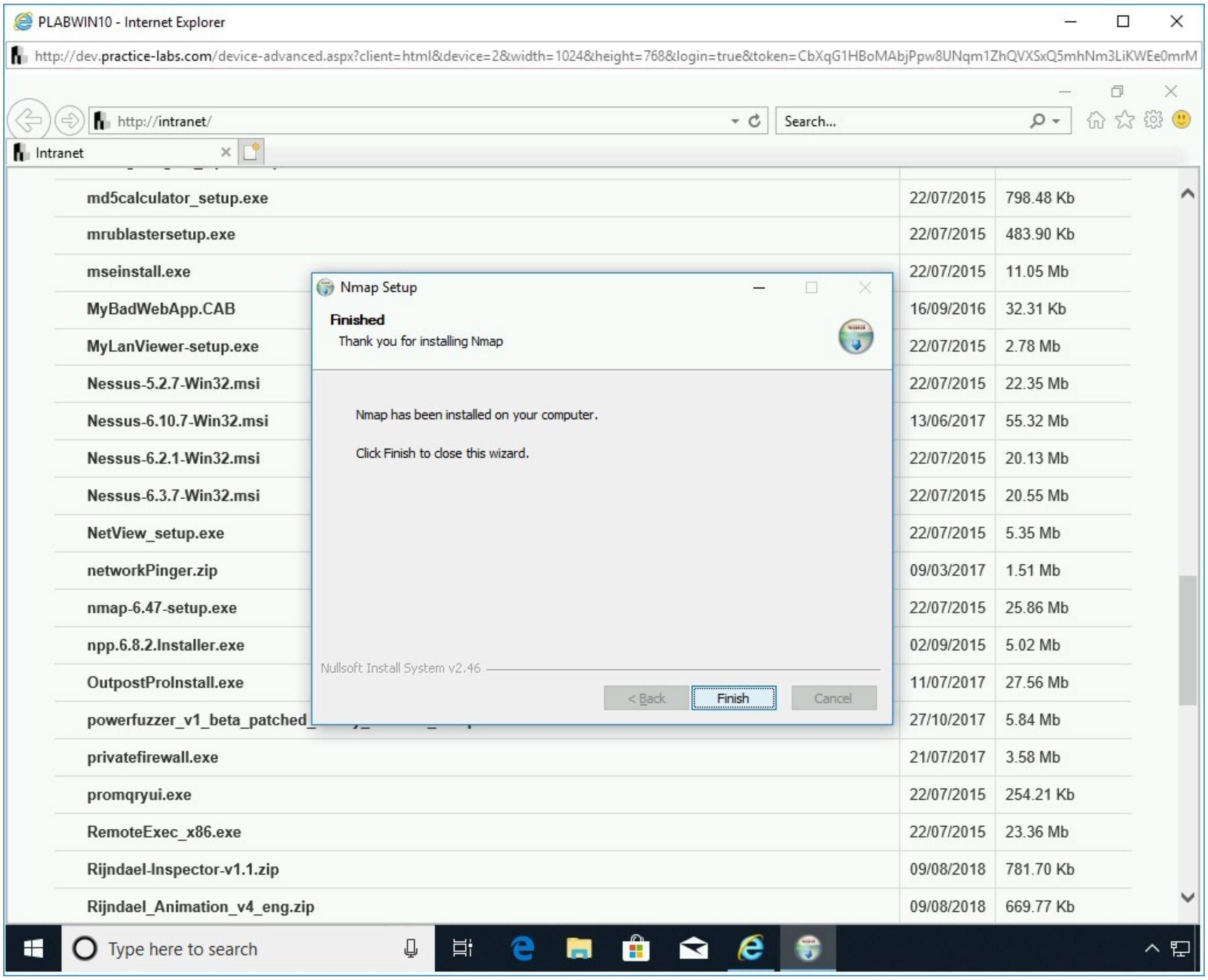
☑ Start Menu Folder
☑ Desktop Icon

Nullsoft Install System v2.46

Figure 1.27 Screenshot of PLABWIN10: Clicking Next on the Create Shortcuts page.

Step 14

On the **Finished** page, click **Finish**.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM

http://intranet/

md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb

Nmap Setup

Finished

Thank you for installing Nmap

Nmap has been installed on your computer.

Click Finish to close this wizard.

Nullsoft Install System v2.46

Figure 1.28 Screenshot of PLABWIN10: Clicking Finished on the Finish page.

Step 15

Minimize the **Internet Explorer** window.

On the desktop, double-click the **Nmap - Zenmap GUI** icon.

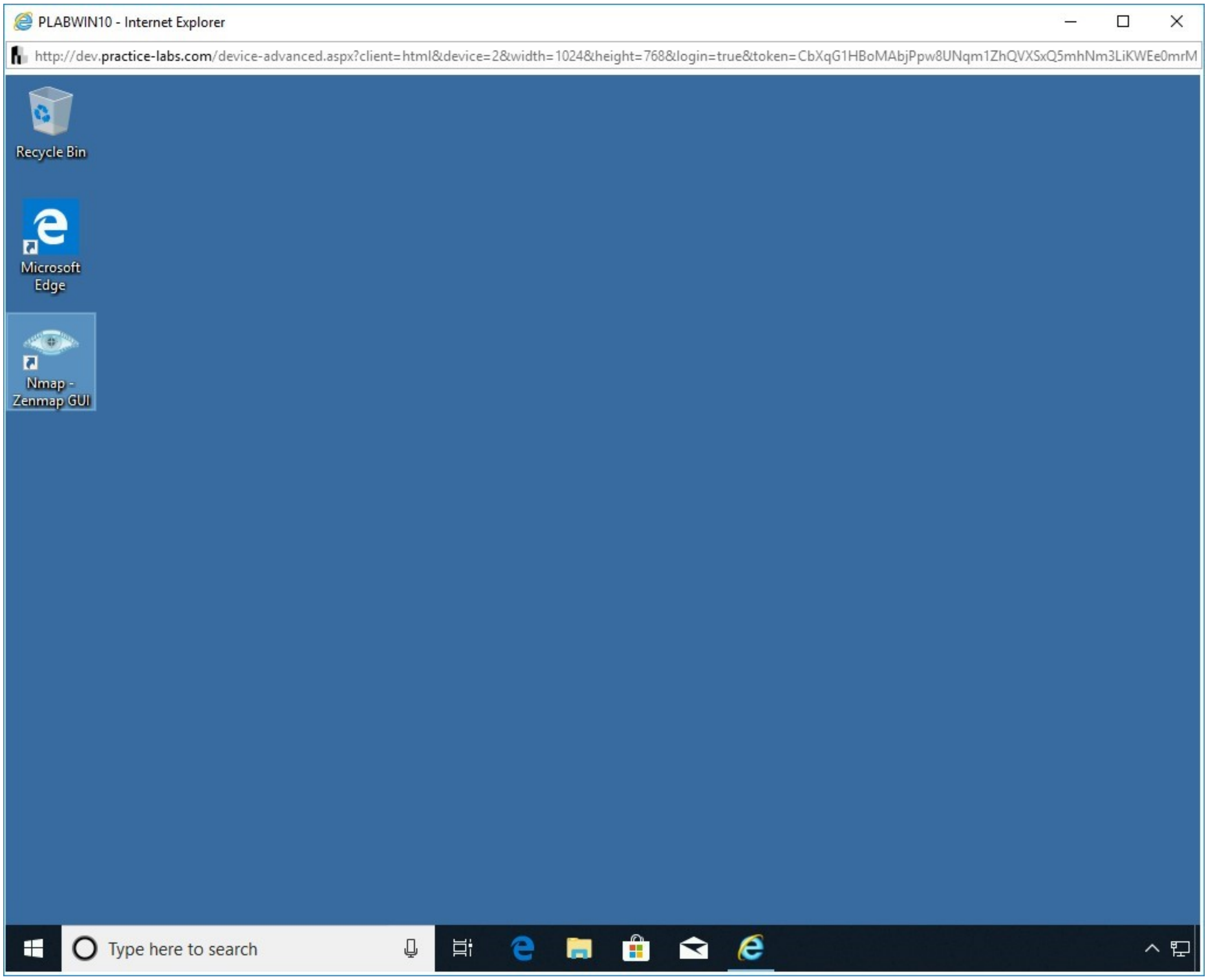

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
Recycle Bin
Microsoft Edge
Nmap - Zenmap GUI
Type here to search

Figure 1.29 Screenshot of PLABWIN10: Double-clicking the Nmap - Zenmap GUI icon on the desktop.

Step 16

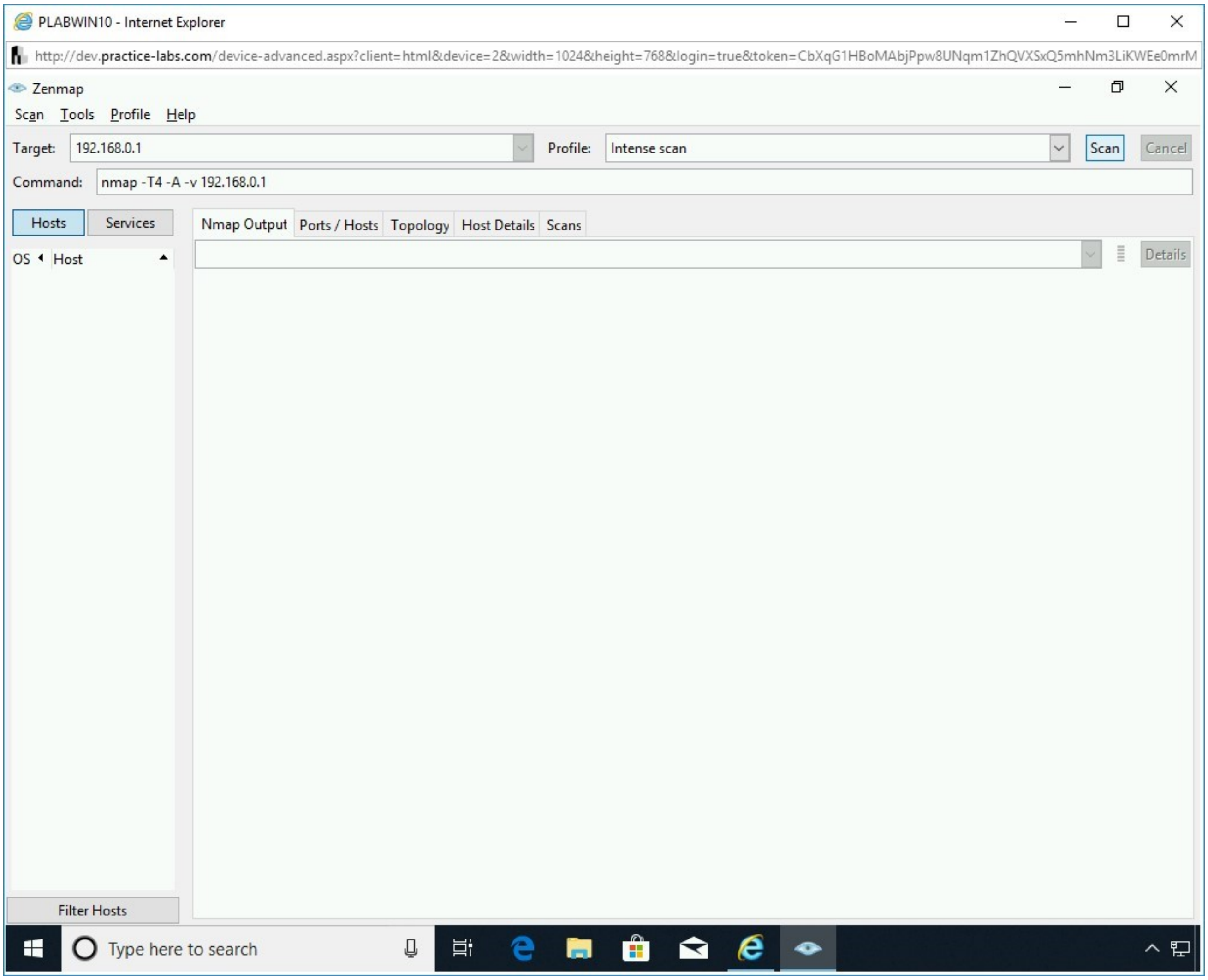
The **Zenmap** window is displayed. The top section has three key fields:

- **Target**: The system that you want to scan.
- **Profile**: A pre-defined scan method. The default method is Intense scan.
- **Command**: This is entered based on the profile selection. You can also choose to type a command manually.

In the **Target** text box, type the following IP address:

```
192.168.0.1
```

Click **Scan**.



Target: 192.168.0.1

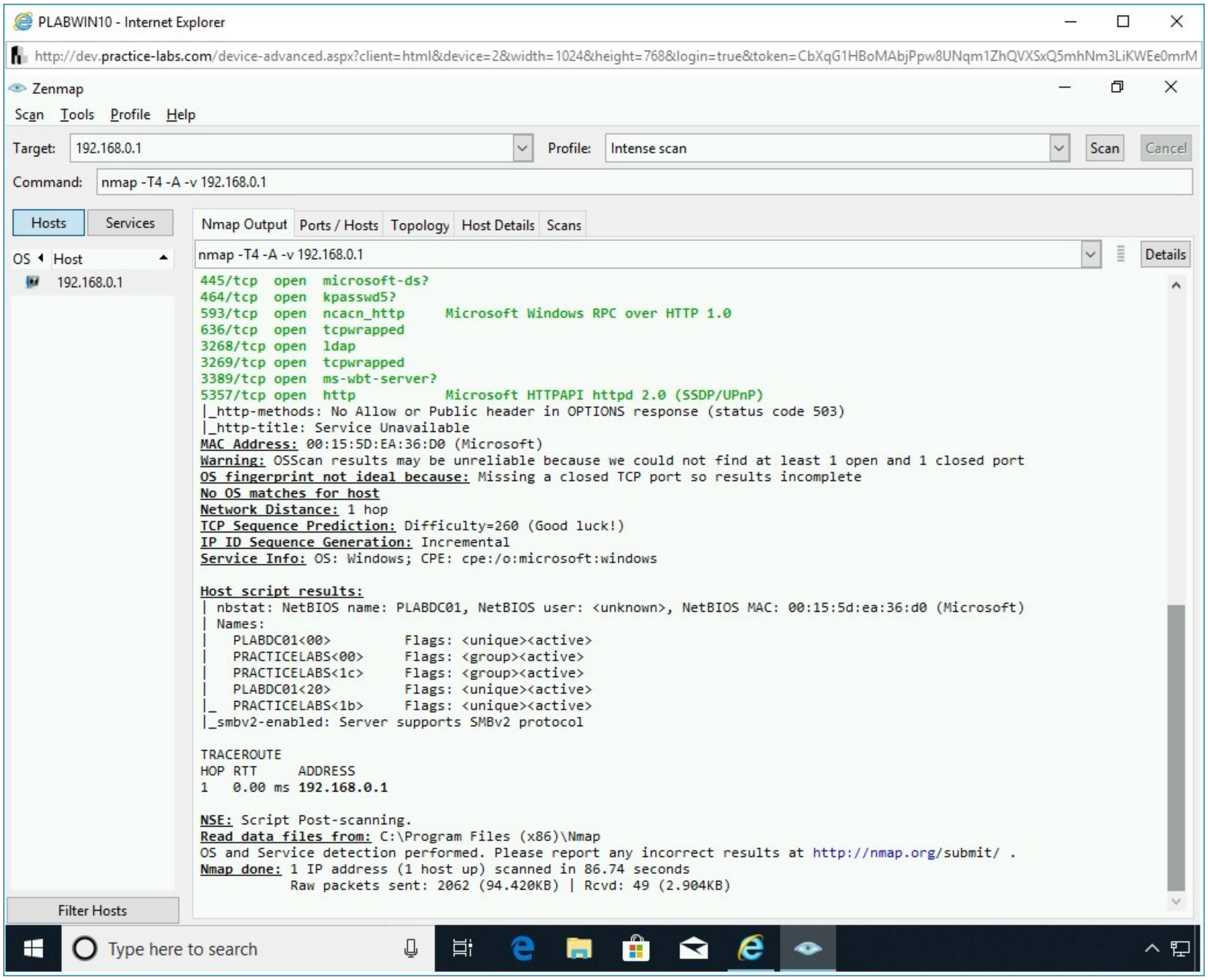
Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.1

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
Zenmap
Scan Tools Profile Help
Scan
Cancel
Hosts
Services
OS Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
Filter Hosts
Type here to search

Figure 1.30 Screenshot of PLABWIN10: Entering the IP address in the Target text box and clicking Scan.

The output is displayed on the **Nmap Output** tab in the right pane.

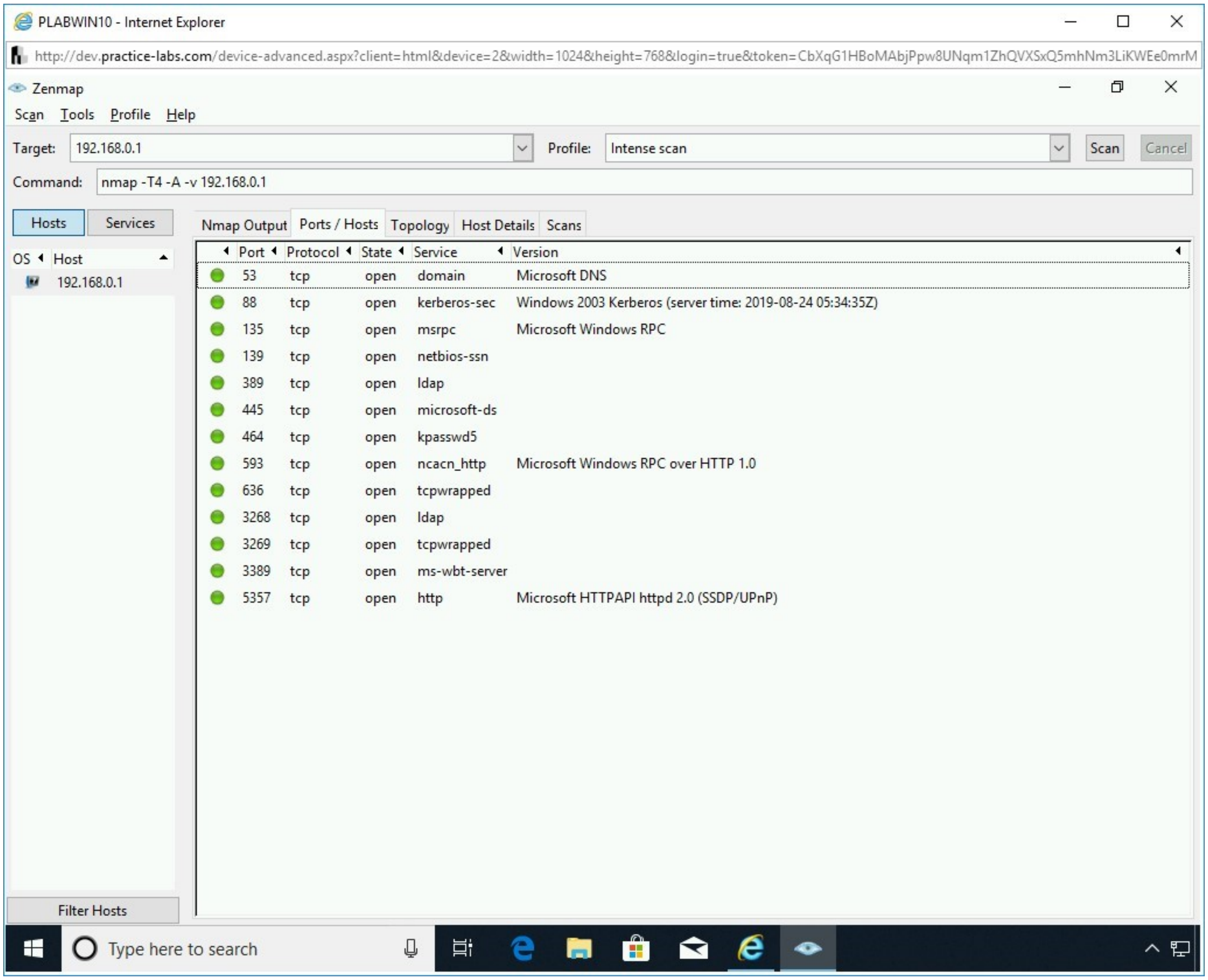

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
Zenmap
Scan Tools Profile Help
Target: 192.168.0.1
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.0.1
Hosts
Services
OS
Host
192.168.0.1
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.0.1
Details
Filter Hosts
Type here to search

```
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server?
5357/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
|_http-title: Service Unavailable
MAC Address: 00:15:5D:EA:36:D0 (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: PLABDC01, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:ea:36:d0 (Microsoft)
| Names:
|   PLABDC01<00>         Flags: <unique><active>
|   PRACTICELABS<00>     Flags: <group><active>
|   PRACTICELABS<1c>     Flags: <group><active>
|   PLABDC01<20>         Flags: <unique><active>
|_  PRACTICELABS<1b>     Flags: <unique><active>
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT     ADDRESS
1   0.00 ms 192.168.0.1

NSE: Script Post-scanning.
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.74 seconds
           Raw packets sent: 2062 (94.420KB) | Rcvd: 49 (2.904KB)
```

Figure 1.31 Screenshot of PLABWIN10: Showing the scan results on the Nmap Output tab.

Step 17

To view the ports information only, click the **Ports / Hosts** tab.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM

Target: 192.168.0.1

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.1

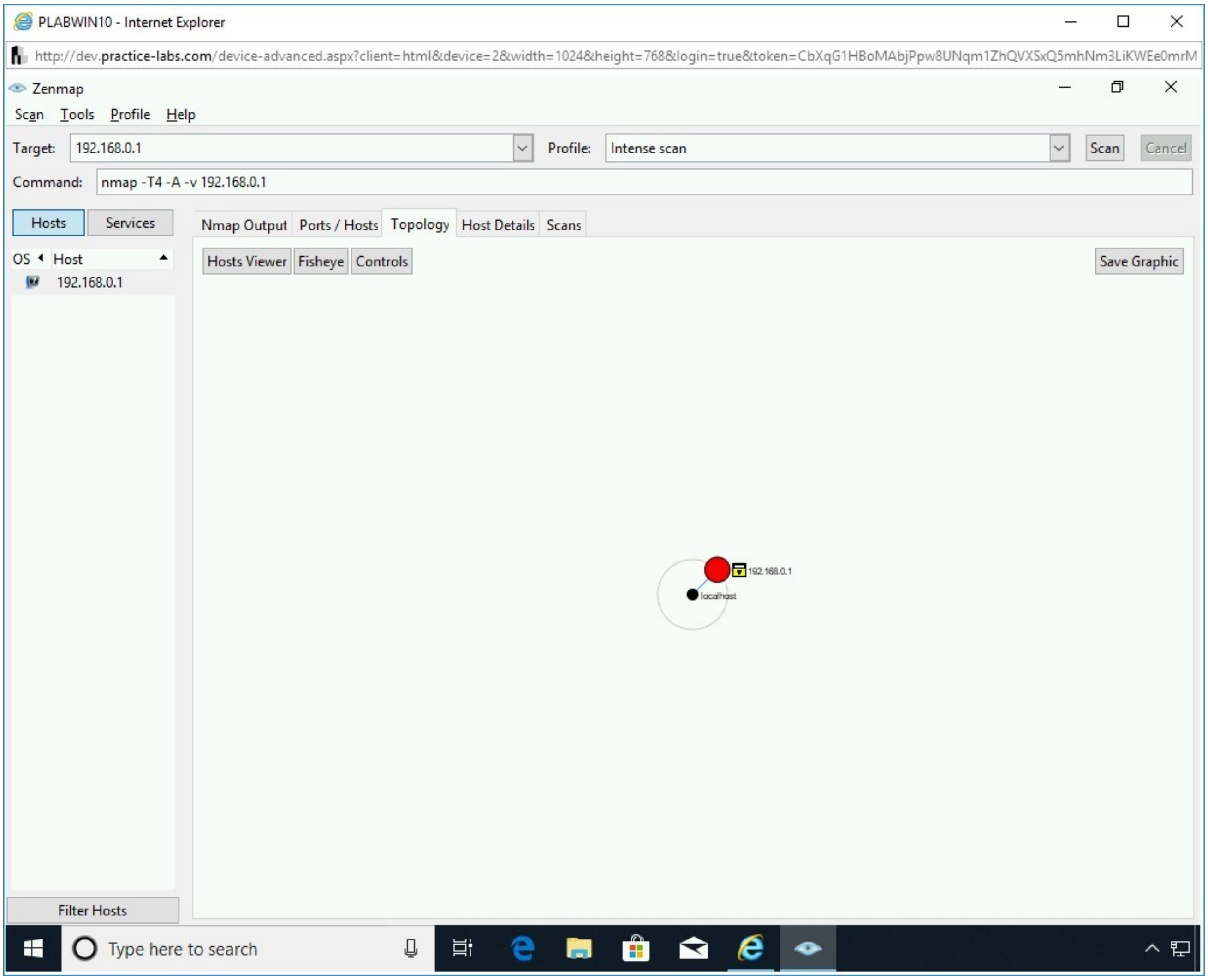
192.168.0.1

Port	Protocol	State	Service	Version
53	tcp	open	domain	Microsoft DNS
88	tcp	open	kerberos-sec	Windows 2003 Kerberos (server time: 2019-08-24 05:34:35Z)
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	
389	tcp	open	ldap	
445	tcp	open	microsoft-ds	
464	tcp	open	kpasswd5	
593	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	tcp	open	tcpwrapped	
3268	tcp	open	ldap	
3269	tcp	open	tcpwrapped	
3389	tcp	open	ms-wbt-server	
5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Figure 1.32 Screenshot of PLABWIN10: Showing the open ports on the Ports / Hosts tab.

Step 18

Click the **Topology** tab. The topology for **192.168.0.1** is displayed.



Target: 192.168.0.1

Profile: Intense scan

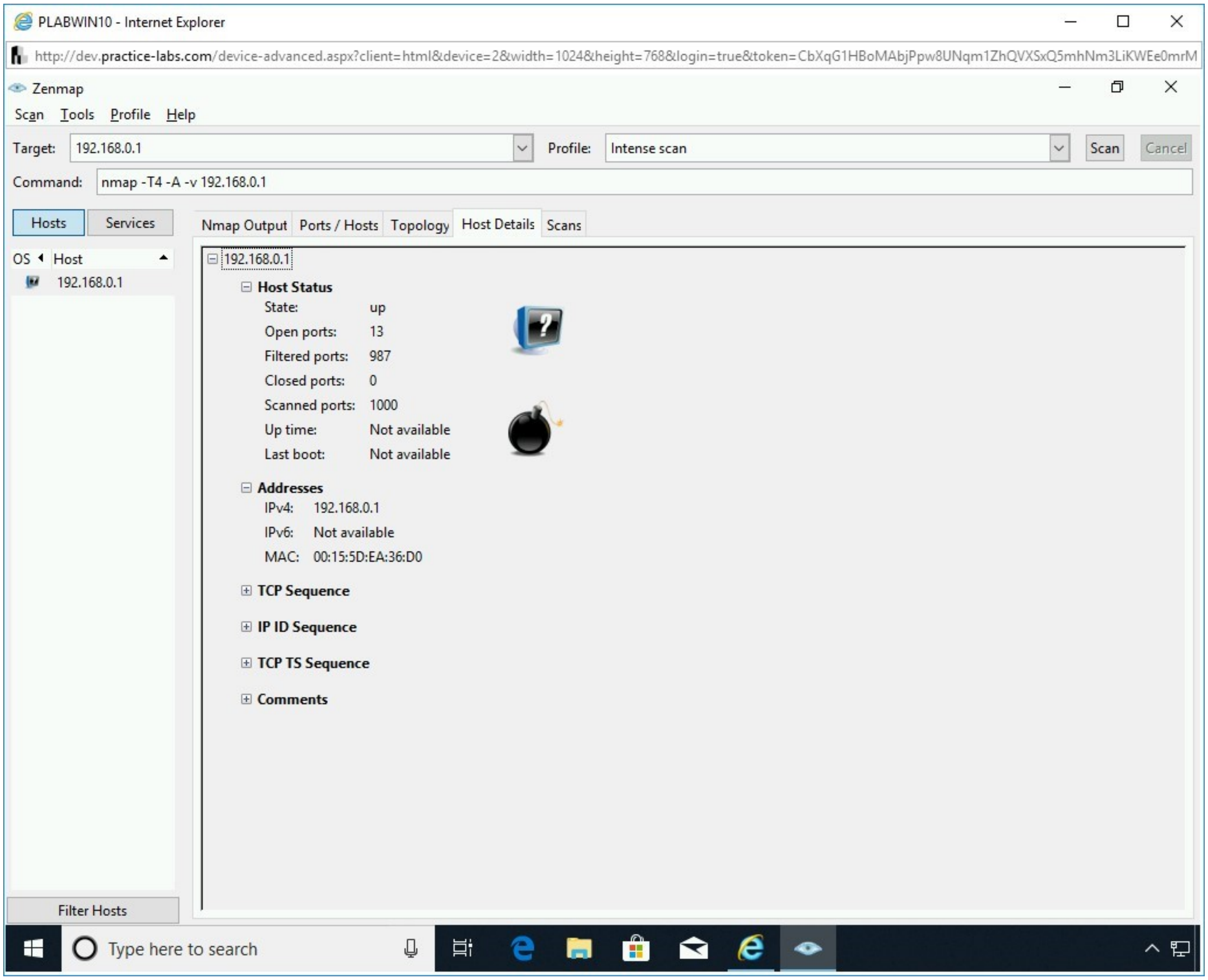
Command: nmap -T4 -A -v 192.168.0.1

Figure 1.33 Screenshot of PLABWIN10: Showing topology on the Topology tab.

Step 19

Click the **Host Details** tab.

Notice that it displays quite a bit of detail. You can find its state (which is up), open ports, filtered ports, and scanned ports.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM

Target: 192.168.0.1

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.1

```
192.168.0.1
  Host Status
    State:          up
    Open ports:     13
    Filtered ports: 987
    Closed ports:   0
    Scanned ports:  1000
    Up time:        Not available
    Last boot:      Not available
  Addresses
    IPv4:  192.168.0.1
    IPv6:  Not available
    MAC:   00:15:5D:EA:36:D0
  TCP Sequence
  IP ID Sequence
  TCP TS Sequence
  Comments
```

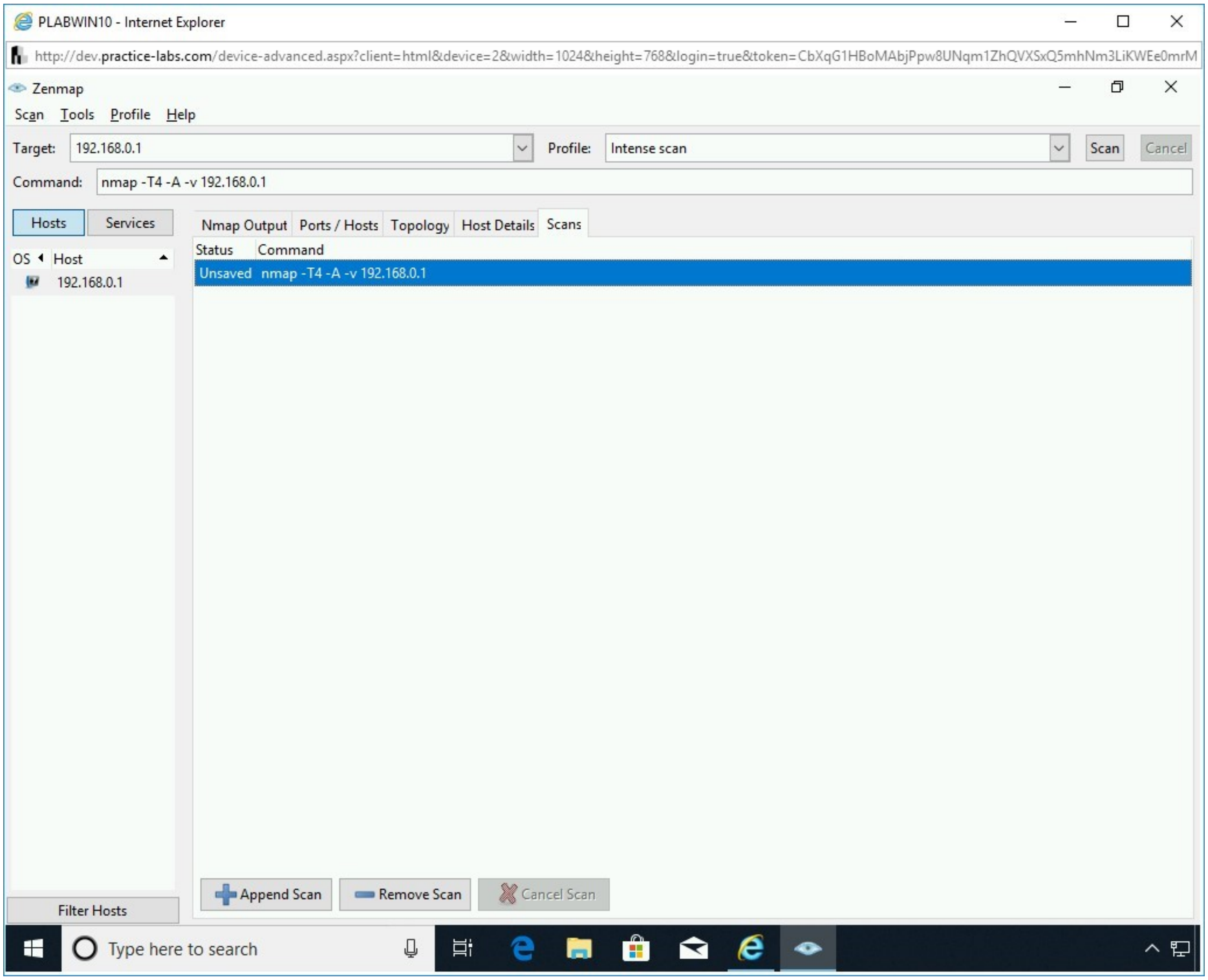
Figure 1.34 Screenshot of PLABWIN10: Showing the host information on the Host Details tab.

Step 20

Click the **Scans** tab.

Notice that it displays the command that has been executed to get the information about the target system.

> ***Note****: The current scan is in an unsaved state. You can use the Scan > Save Scan option (in the toolbar) to save the scan. Alternatively, you can press the Ctrl + s keys to save the scan.*



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
Zenmap
Scan Tools Profile Help
Scan
Cancel
Hosts
Services
OS Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Append Scan
Remove Scan
Cancel Scan
Filter Hosts
Type here to search

Target: 192.168.0.1

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.1

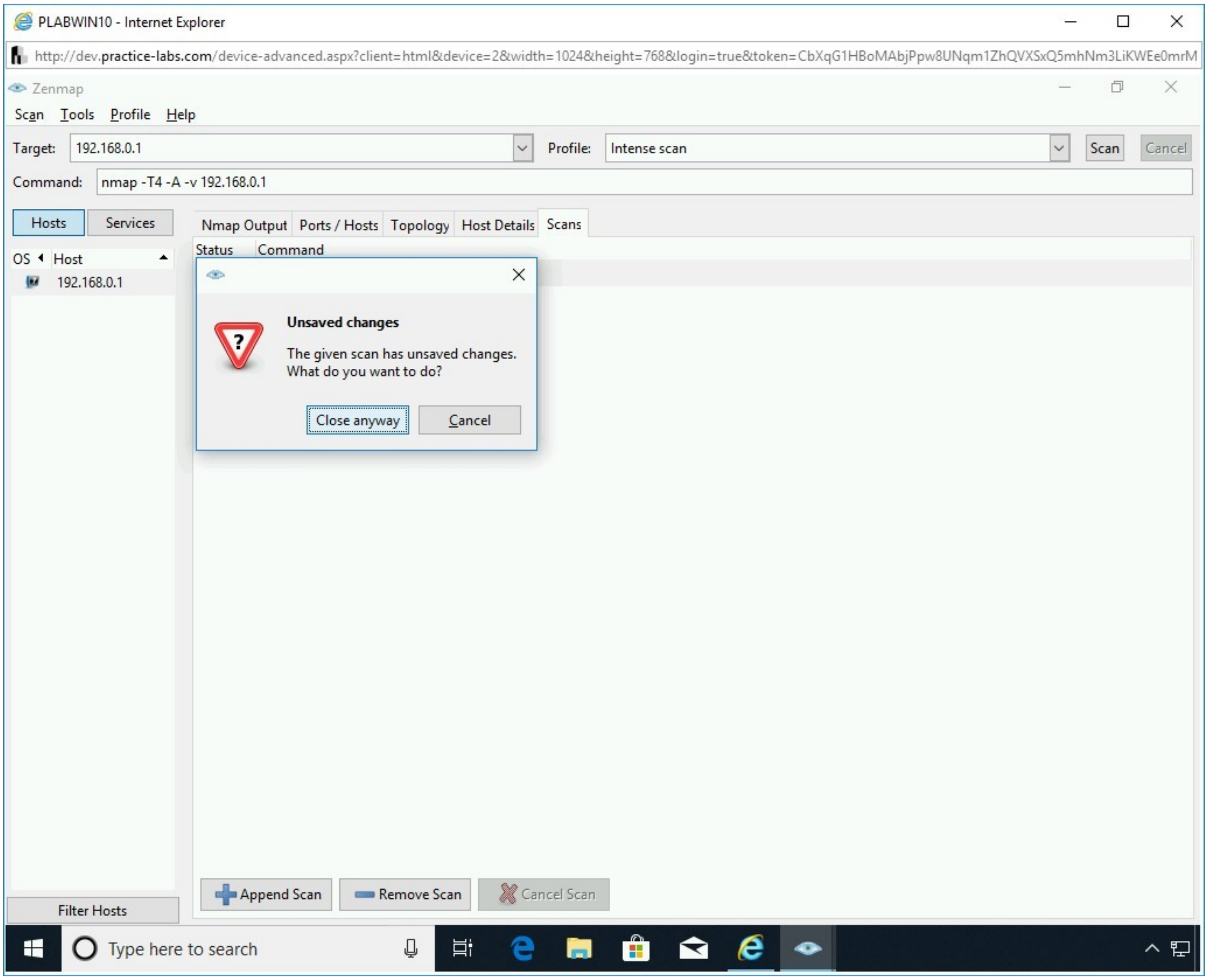
192.168.0.1

Status	Command
Unsaved	nmap -T4 -A -v 192.168.0.1

Figure 1.35 Screenshot of PLABWIN10: Showing the unsaved command on the Scans tab.

Step 21

Close the **Zenmap** window. When prompted to save changes, click **Close anyway**.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM

Target: 192.168.0.1

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.1

Unsaved changes

The given scan has unsaved changes.
What do you want to do?

Figure 1.36 Screenshot of PLABWIN10: Clicking Close anyway o the Unsaved changes dialog box.

Task 3 - Use CurrPorts to Monitor TCP/IP Connections

CurrPorts is a network monitoring tool. It can display the open TCP and UDP connections on a local system.

In this task, you will use CurrPorts to monitor TCP/IP connections. To do this, perform the following steps:

Step 1

Ensure you have powered on the required devices and connect to **PLABWIN10**.

Restore the **Internet Explorer** window from the taskbar.

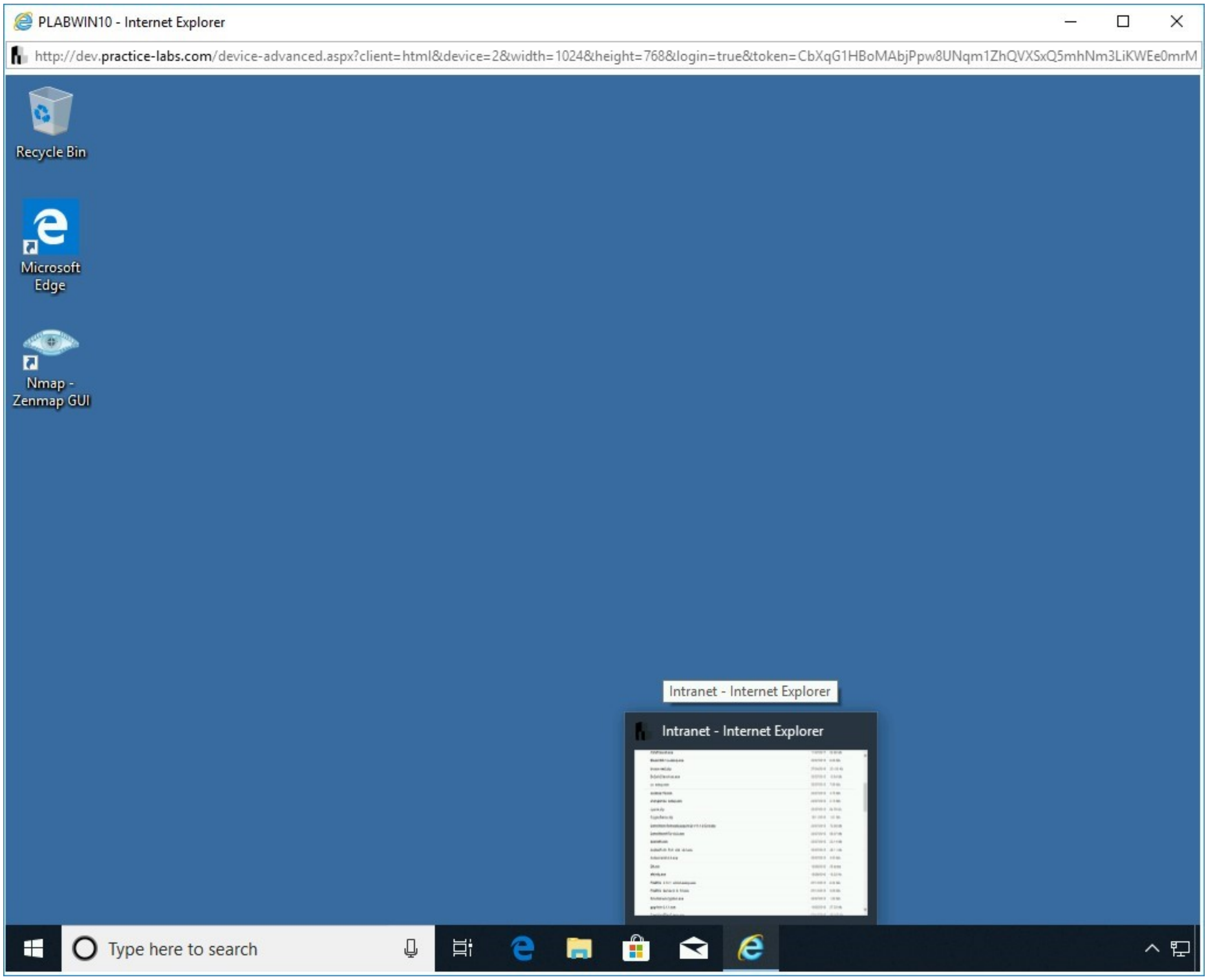
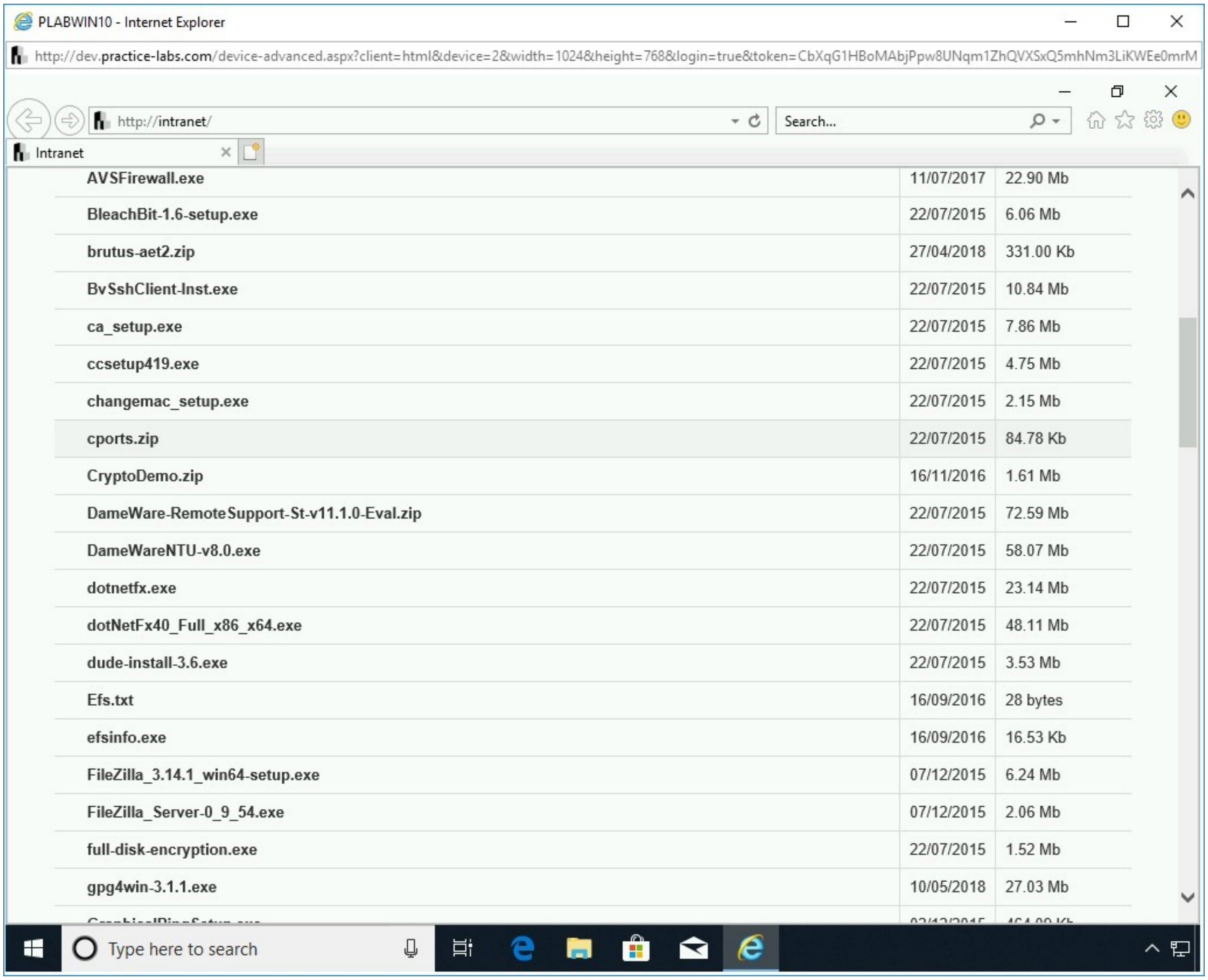

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
Recycle Bin
Microsoft Edge
Nmap - Zenmap GUI
Intranet - Internet Explorer
Intranet - Internet Explorer
Type here to search

Figure 1.37 Screenshot of PLABWIN10: Restoring the Internet Explorer window from the taskbar.

Step 2

Ensure that you are on the **Hacking Tools** page on the **Intranet** Website.

Scroll and click **cports.zip**.

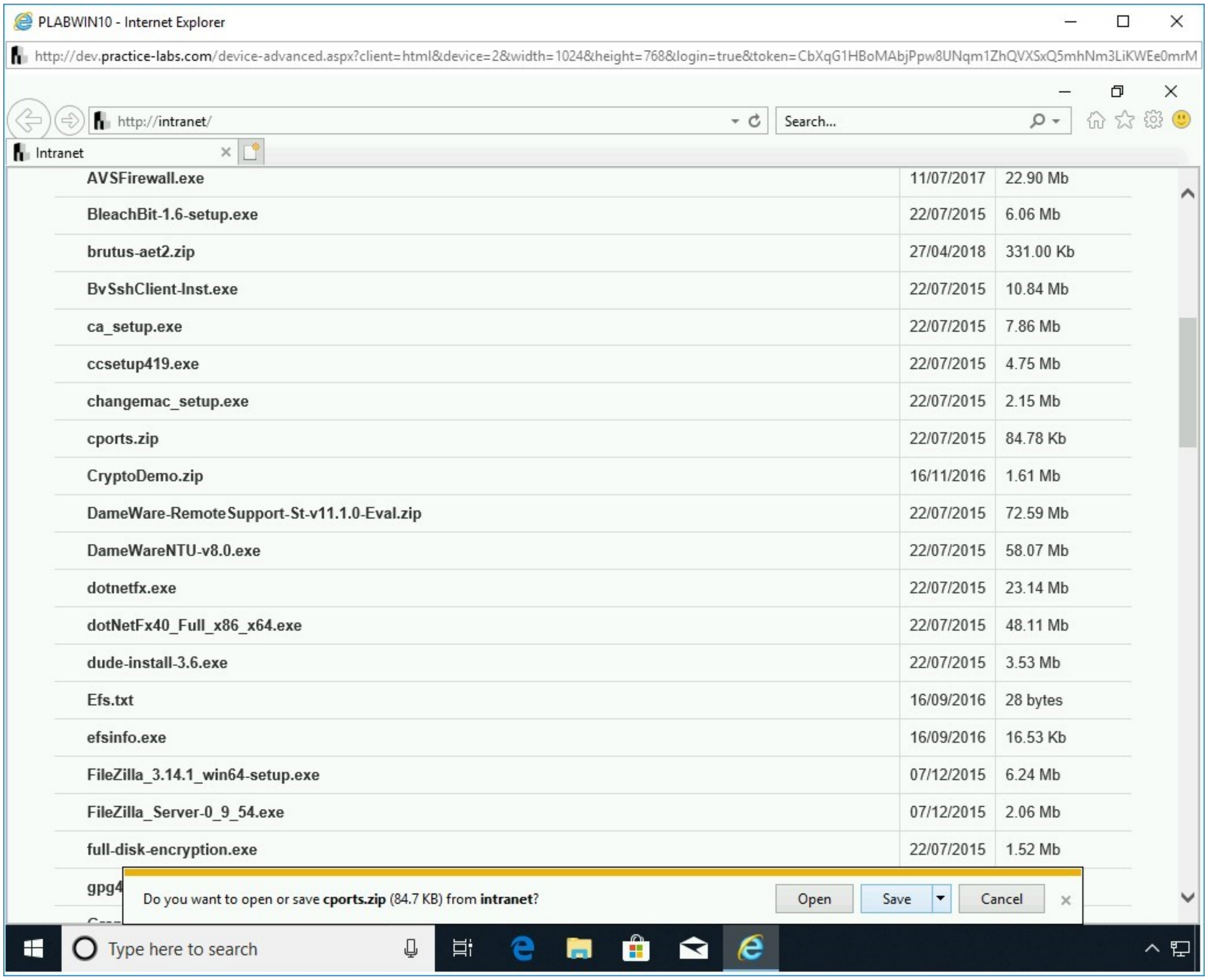

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Type here to search

AVSFirewall.exe	11/07/2017	22.90 Mb
BleachBit-1.6-setup.exe	22/07/2015	6.06 Mb
brutus-aet2.zip	27/04/2018	331.00 Kb
BvSshClient-Inst.exe	22/07/2015	10.84 Mb
ca_setup.exe	22/07/2015	7.86 Mb
ccsetup419.exe	22/07/2015	4.75 Mb
changemac_setup.exe	22/07/2015	2.15 Mb
cports.zip	22/07/2015	84.78 Kb
CryptoDemo.zip	16/11/2016	1.61 Mb
DameWare-RemoteSupport-St-v11.1.0-Eval.zip	22/07/2015	72.59 Mb
DameWareNTU-v8.0.exe	22/07/2015	58.07 Mb
dotnetfx.exe	22/07/2015	23.14 Mb
dotNetFx40_Full_x86_x64.exe	22/07/2015	48.11 Mb
dude-install-3.6.exe	22/07/2015	3.53 Mb
Efs.txt	16/09/2016	28 bytes
efsinfo.exe	16/09/2016	16.53 Kb
FileZilla_3.14.1_win64-setup.exe	07/12/2015	6.24 Mb
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4win-3.1.1.exe	10/05/2018	27.03 Mb

Figure 1.38 Screenshot of PLABWIN10: Clicking the cports.zip file on the Intranet Webpage.

Step 3

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


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Open
Save
Cancel
Type here to search

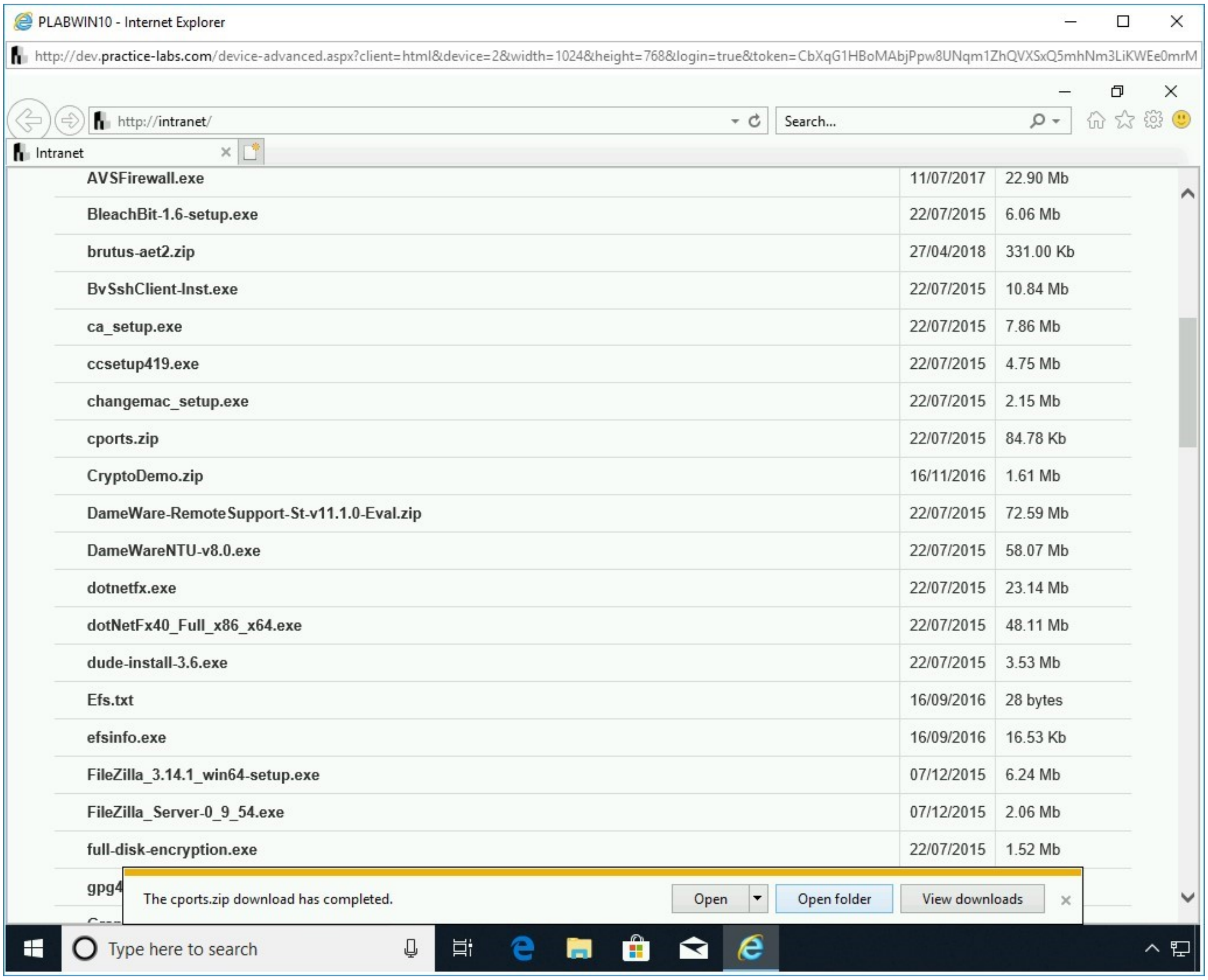
AVSFirewall.exe	11/07/2017	22.90 Mb
BleachBit-1.6-setup.exe	22/07/2015	6.06 Mb
brutus-aet2.zip	27/04/2018	331.00 Kb
BvSshClient-Inst.exe	22/07/2015	10.84 Mb
ca_setup.exe	22/07/2015	7.86 Mb
ccsetup419.exe	22/07/2015	4.75 Mb
changemac_setup.exe	22/07/2015	2.15 Mb
cports.zip	22/07/2015	84.78 Kb
CryptoDemo.zip	16/11/2016	1.61 Mb
DameWare-RemoteSupport-St-v11.1.0-Eval.zip	22/07/2015	72.59 Mb
DameWareNTU-v8.0.exe	22/07/2015	58.07 Mb
dotnetfx.exe	22/07/2015	23.14 Mb
dotNetFx40_Full_x86_x64.exe	22/07/2015	48.11 Mb
dude-install-3.6.exe	22/07/2015	3.53 Mb
Efs.txt	16/09/2016	28 bytes
efsinfo.exe	16/09/2016	16.53 Kb
FileZilla_3.14.1_win64-setup.exe	07/12/2015	6.24 Mb
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4		

Do you want to open or save **cports.zip** (84.7 KB) from **intranet**?

Figure 1.39 Screenshot of PLABWIN10: Clicking Save in the notification bar.

Step 4

In the notification bar, click **Open folder**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Open
Open folder
View downloads
Type here to search

AVSFirewall.exe	11/07/2017	22.90 Mb
BleachBit-1.6-setup.exe	22/07/2015	6.06 Mb
brutus-aet2.zip	27/04/2018	331.00 Kb
BvSshClient-Inst.exe	22/07/2015	10.84 Mb
ca_setup.exe	22/07/2015	7.86 Mb
ccsetup419.exe	22/07/2015	4.75 Mb
changemac_setup.exe	22/07/2015	2.15 Mb
cports.zip	22/07/2015	84.78 Kb
CryptoDemo.zip	16/11/2016	1.61 Mb
DameWare-RemoteSupport-St-v11.1.0-Eval.zip	22/07/2015	72.59 Mb
DameWareNTU-v8.0.exe	22/07/2015	58.07 Mb
dotnetfx.exe	22/07/2015	23.14 Mb
dotNetFx40_Full_x86_x64.exe	22/07/2015	48.11 Mb
dude-install-3.6.exe	22/07/2015	3.53 Mb
Efs.txt	16/09/2016	28 bytes
efsinfo.exe	16/09/2016	16.53 Kb
FileZilla_3.14.1_win64-setup.exe	07/12/2015	6.24 Mb
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4		

The cports.zip download has completed.

Figure 1.40 Screenshot of PLABWIN10: Clicking Open folder on the notification bar.

Step 5

The **File Explorer** window displays the **Downloads** folder.

Right-click **cports** and select **Extract All...**

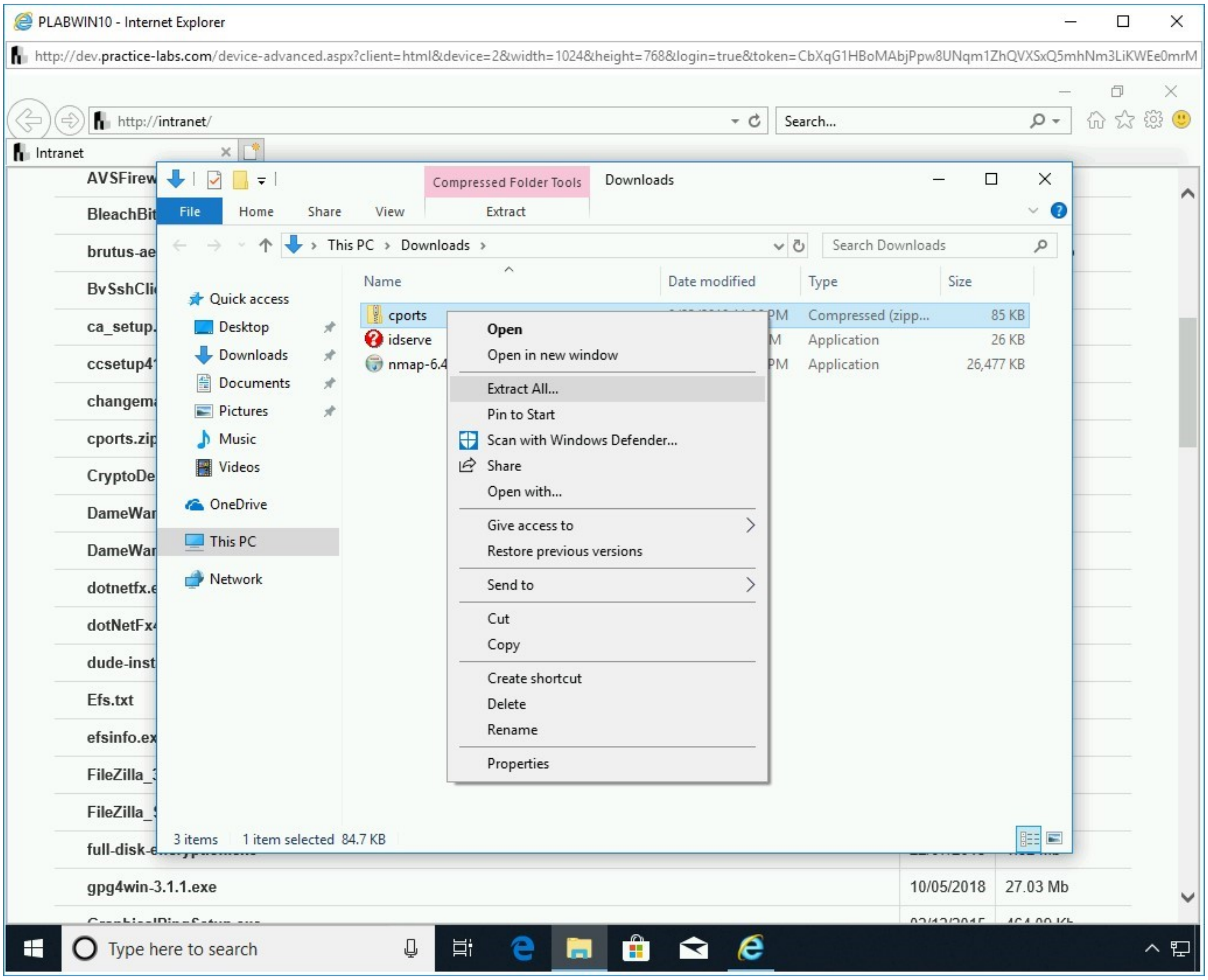
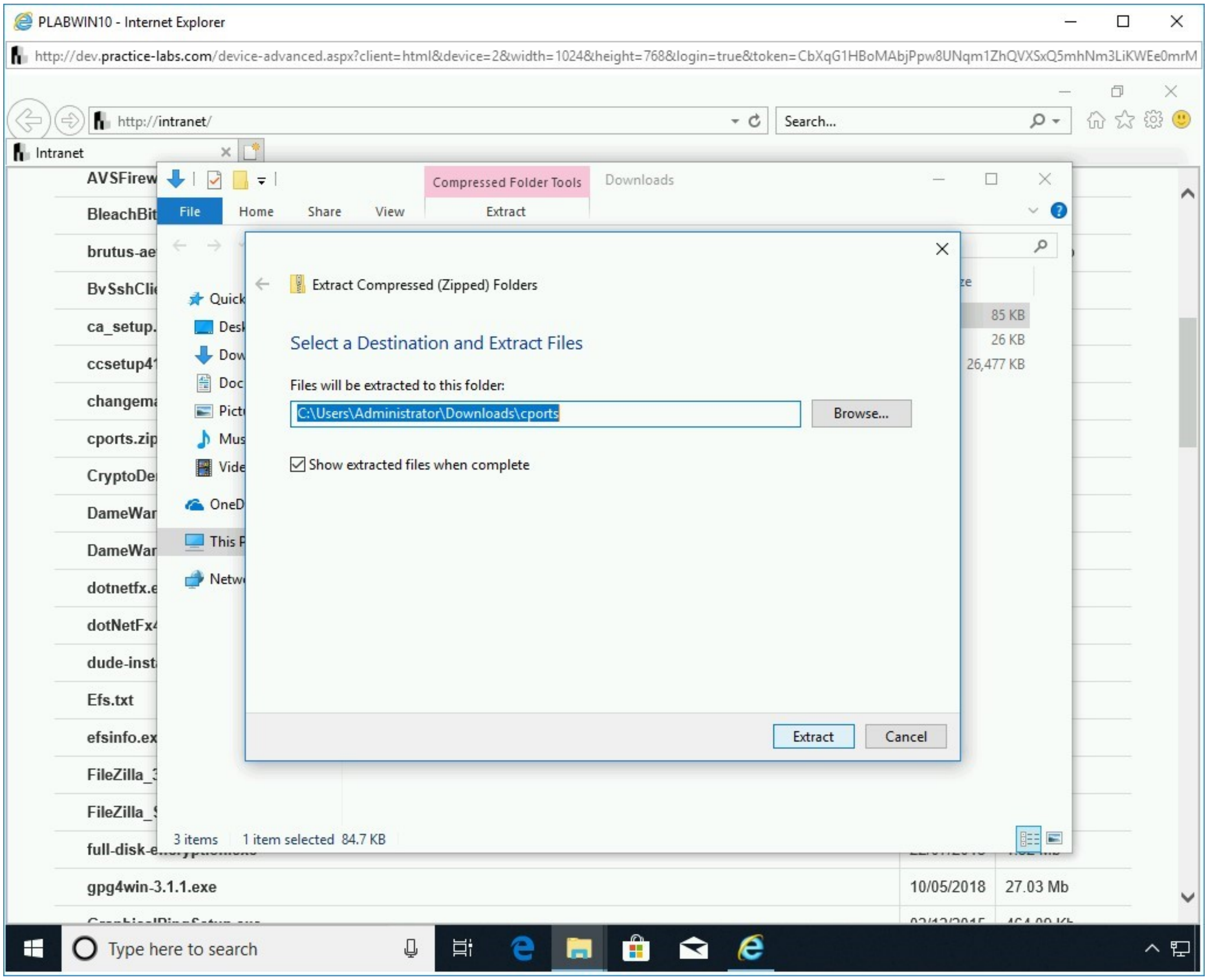


Figure 1.41 Screenshot of PLABWIN10: Selecting the Extract all option from the context menu.

Step 6

The **Extract Compressed (Zipped) Folders** dialog box is displayed.

Keep the default path and settings, then click **Extract**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
http://intranet/
Search...
Intranet
Compressed Folder Tools
Downloads
File
Home
Share
View
Extract
3 items
1 item selected 84.7 KB
Type here to search
Browse...
Extract
Cancel

Extract Compressed (Zipped) Folders

Select a Destination and Extract Files

Files will be extracted to this folder:

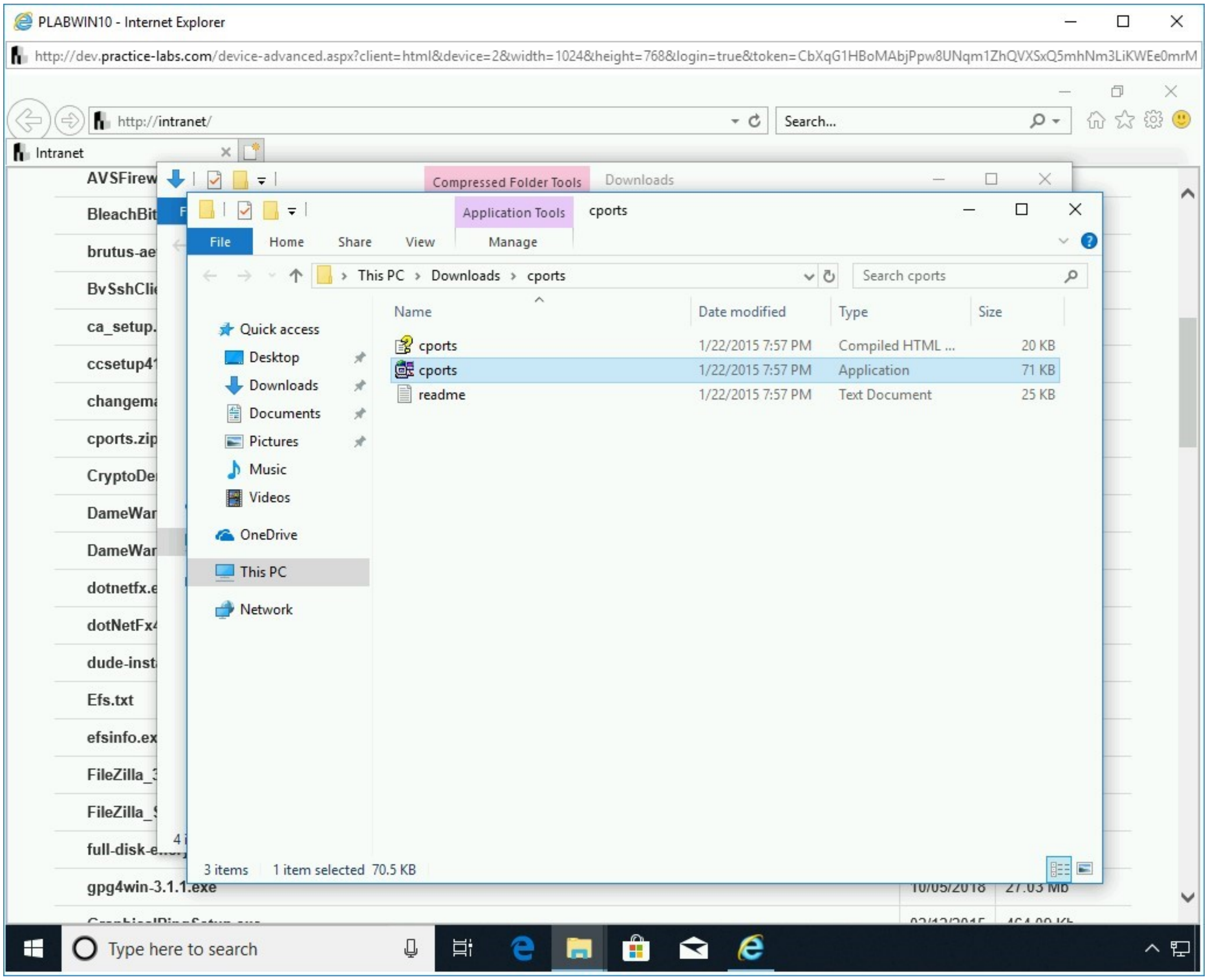
C:\Users\Administrator\Downloads\cports

☑ Show extracted files when complete

Figure 1.42 Screenshot of PLABWIN10: Showing the folder for extracting the files and clicking Extract.

Step 7

A new **File Explorer** window is displayed with the **cports** folder. Double-click the **cports** application file.



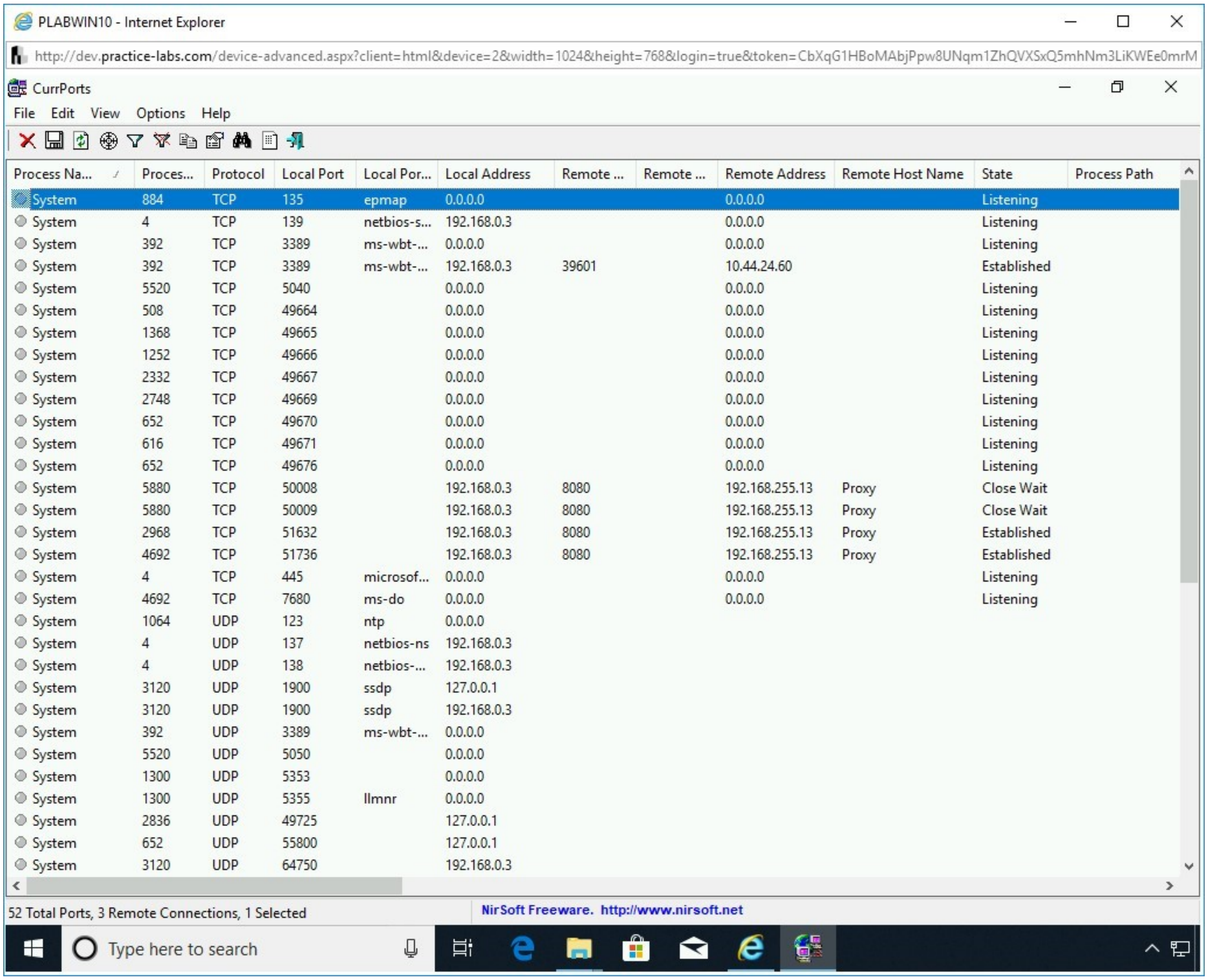
Name	Date modified	Type	Size
cports	1/22/2015 7:57 PM	Compiled HTML ...	20 KB
cports	1/22/2015 7:57 PM	Application	71 KB
readme	1/22/2015 7:57 PM	Text Document	25 KB

Figure 1.43 Screenshot of PLABWIN10: Showing the new File Explorer window and double-clicking the cports executable.

The **CurrPorts** window is displayed. Notice that it displays the open **TCP** and **UDP** connections.

The following information is displayed:

- Process Name
- Process ID
- Protocol
- Local Port
- Local and Remote Addresses
- State


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
CurrPorts
File Edit View Options Help

Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...	Remote Address	Remote Host Name	State	Process Path
System	884	TCP	135	epmap	0.0.0.0			0.0.0.0		Listening	
System	4	TCP	139	netbios-s...	192.168.0.3			0.0.0.0		Listening	
System	392	TCP	3389	ms-wbt-...	0.0.0.0			0.0.0.0		Listening	
System	392	TCP	3389	ms-wbt-...	192.168.0.3	39601		10.44.24.60		Established	
System	5520	TCP	5040		0.0.0.0			0.0.0.0		Listening	
System	508	TCP	49664		0.0.0.0			0.0.0.0		Listening	
System	1368	TCP	49665		0.0.0.0			0.0.0.0		Listening	
System	1252	TCP	49666		0.0.0.0			0.0.0.0		Listening	
System	2332	TCP	49667		0.0.0.0			0.0.0.0		Listening	
System	2748	TCP	49669		0.0.0.0			0.0.0.0		Listening	
System	652	TCP	49670		0.0.0.0			0.0.0.0		Listening	
System	616	TCP	49671		0.0.0.0			0.0.0.0		Listening	
System	652	TCP	49676		0.0.0.0			0.0.0.0		Listening	
System	5880	TCP	50008		192.168.0.3	8080		192.168.255.13	Proxy	Close Wait	
System	5880	TCP	50009		192.168.0.3	8080		192.168.255.13	Proxy	Close Wait	
System	2968	TCP	51632		192.168.0.3	8080		192.168.255.13	Proxy	Established	
System	4692	TCP	51736		192.168.0.3	8080		192.168.255.13	Proxy	Established	
System	4	TCP	445	microsof...	0.0.0.0			0.0.0.0		Listening	
System	4692	TCP	7680	ms-do	0.0.0.0			0.0.0.0		Listening	
System	1064	UDP	123	ntp	0.0.0.0						
System	4	UDP	137	netbios-ns	192.168.0.3						
System	4	UDP	138	netbios-...	192.168.0.3						
System	3120	UDP	1900	ssdp	127.0.0.1						
System	3120	UDP	1900	ssdp	192.168.0.3						
System	392	UDP	3389	ms-wbt-...	0.0.0.0						
System	5520	UDP	5050		0.0.0.0						
System	1300	UDP	5353		0.0.0.0						
System	1300	UDP	5355	llmnr	0.0.0.0						
System	2836	UDP	49725		127.0.0.1						
System	652	UDP	55800		127.0.0.1						
System	3120	UDP	64750		192.168.0.3						

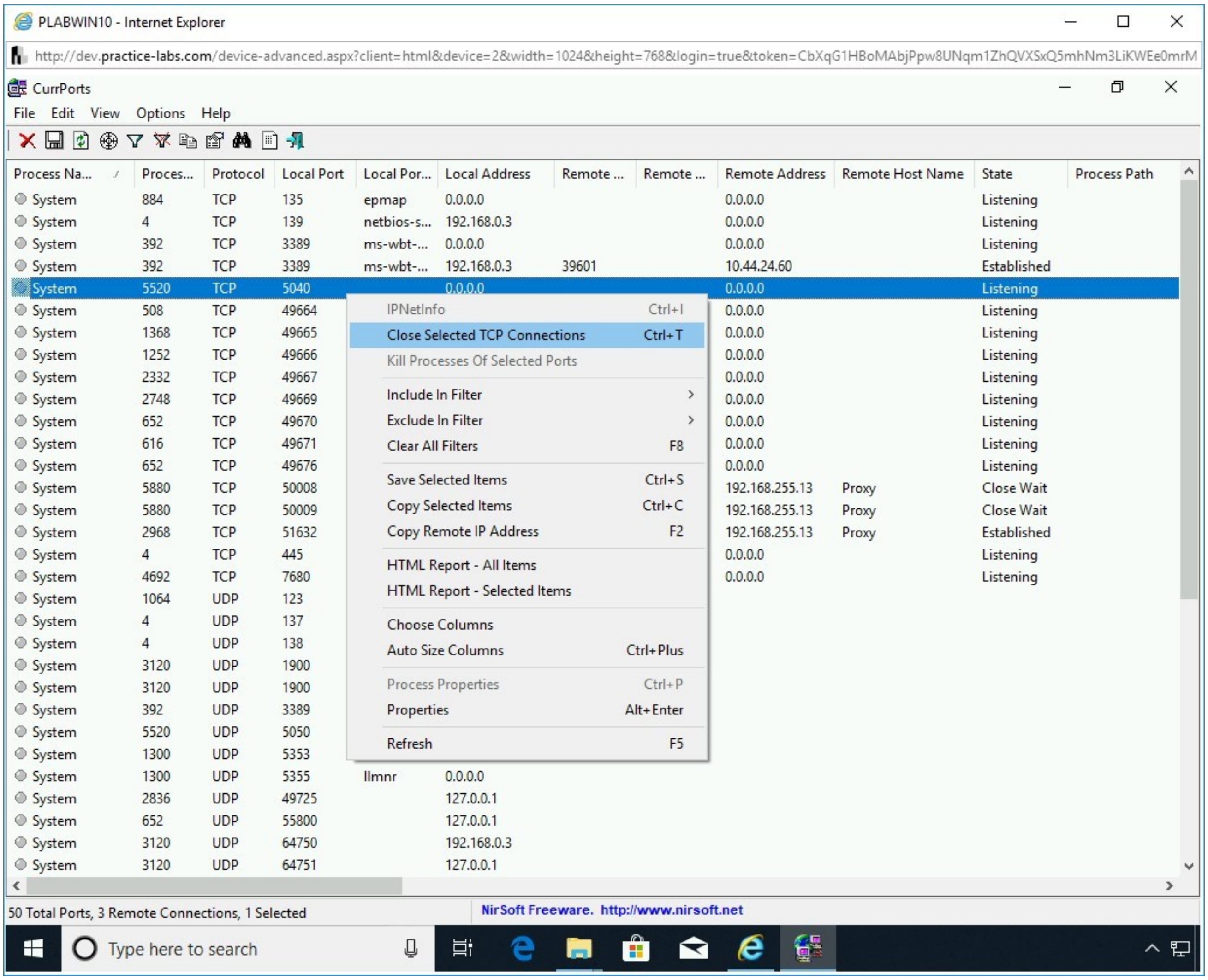
52 Total Ports, 3 Remote Connections, 1 Selected

Figure 1.44 Screenshot of PLABWIN10: Showing TCP and UDP connections.

Step 8

Let's attempt to close a **TCP** connection.

Select a **TCP** connection, right-click and select **Close Selected TCP Connections**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
CurrPorts
File
Edit
View
Options
Help
IPNetInfo Ctrl+I
Close Selected TCP Connections Ctrl+T
Kill Processes Of Selected Ports
Include In Filter
Exclude In Filter
Clear All Filters F8
Save Selected Items Ctrl+S
Copy Selected Items Ctrl+C
Copy Remote IP Address F2
HTML Report - All Items
HTML Report - Selected Items
Choose Columns
Auto Size Columns Ctrl+Plus
Process Properties Ctrl+P
Properties Alt+Enter
Refresh F5
NirSoft Freeware. http://www.nirsoft.net
Type here to search

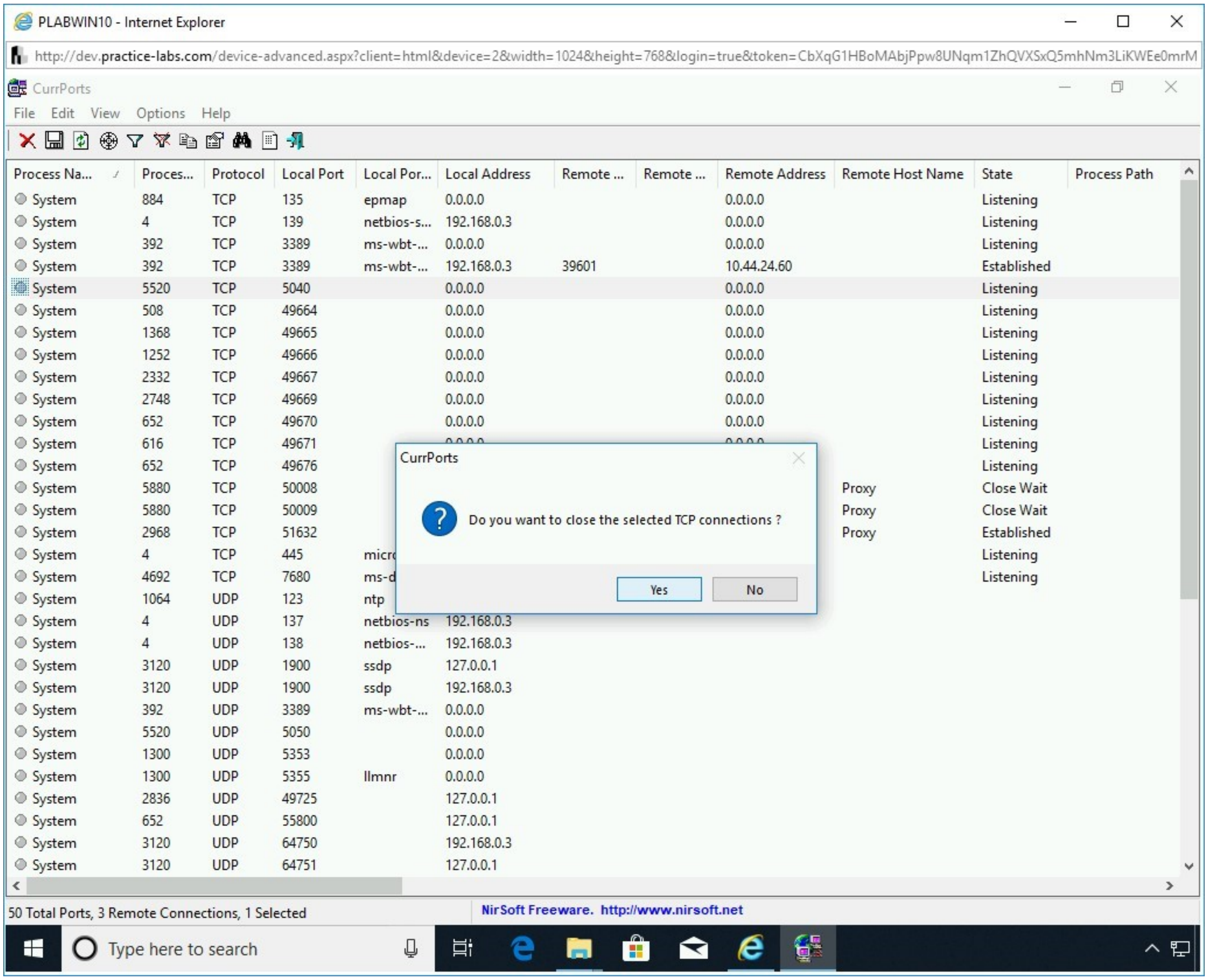
Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...	Remote Address	Remote Host Name	State	Process Path
System	884	TCP	135	epmap	0.0.0.0			0.0.0.0		Listening	
System	4	TCP	139	netbios-s...	192.168.0.3			0.0.0.0		Listening	
System	392	TCP	3389	ms-wbt-...	0.0.0.0			0.0.0.0		Listening	
System	392	TCP	3389	ms-wbt-...	192.168.0.3	39601		10.44.24.60		Established	
System	5520	TCP	5040		0.0.0.0			0.0.0.0		Listening	
System	508	TCP	49664					0.0.0.0		Listening	
System	1368	TCP	49665					0.0.0.0		Listening	
System	1252	TCP	49666					0.0.0.0		Listening	
System	2332	TCP	49667					0.0.0.0		Listening	
System	2748	TCP	49669					0.0.0.0		Listening	
System	652	TCP	49670					0.0.0.0		Listening	
System	616	TCP	49671					0.0.0.0		Listening	
System	652	TCP	49676					0.0.0.0		Listening	
System	5880	TCP	50008					192.168.255.13	Proxy	Close Wait	
System	5880	TCP	50009					192.168.255.13	Proxy	Close Wait	
System	2968	TCP	51632					192.168.255.13	Proxy	Established	
System	4	TCP	445					0.0.0.0		Listening	
System	4692	TCP	7680					0.0.0.0		Listening	
System	1064	UDP	123								
System	4	UDP	137								
System	4	UDP	138								
System	3120	UDP	1900								
System	3120	UDP	1900								
System	392	UDP	3389								
System	5520	UDP	5050								
System	1300	UDP	5353								
System	1300	UDP	5355	llmnr	0.0.0.0						
System	2836	UDP	49725		127.0.0.1						
System	652	UDP	55800		127.0.0.1						
System	3120	UDP	64750		192.168.0.3						
System	3120	UDP	64751		127.0.0.1						

50 Total Ports, 3 Remote Connections, 1 Selected

Figure 1.45 Screenshot of PLABWIN10: Selecting Close Selected TCP Connections from the context menu.

Step 9

The **CurrPorts** dialog box is displayed. It prompts to confirm the closure of the selected TCP connection. Click **Yes**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
CurrPorts
File Edit View Options Help

Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...	Remote Address	Remote Host Name	State	Process Path
System	884	TCP	135	epmap	0.0.0.0			0.0.0.0		Listening	
System	4	TCP	139	netbios-s...	192.168.0.3			0.0.0.0		Listening	
System	392	TCP	3389	ms-wbt-...	0.0.0.0			0.0.0.0		Listening	
System	392	TCP	3389	ms-wbt-...	192.168.0.3	39601		10.44.24.60		Established	
System	5520	TCP	5040		0.0.0.0			0.0.0.0		Listening	
System	508	TCP	49664		0.0.0.0			0.0.0.0		Listening	
System	1368	TCP	49665		0.0.0.0			0.0.0.0		Listening	
System	1252	TCP	49666		0.0.0.0			0.0.0.0		Listening	
System	2332	TCP	49667		0.0.0.0			0.0.0.0		Listening	
System	2748	TCP	49669		0.0.0.0			0.0.0.0		Listening	
System	652	TCP	49670		0.0.0.0			0.0.0.0		Listening	
System	616	TCP	49671		0.0.0.0			0.0.0.0		Listening	
System	652	TCP	49676							Listening	
System	5880	TCP	50008						Proxy	Close Wait	
System	5880	TCP	50009						Proxy	Close Wait	
System	2968	TCP	51632						Proxy	Established	
System	4	TCP	445	micrc						Listening	
System	4692	TCP	7680	ms-d						Listening	
System	1064	UDP	123	ntp							
System	4	UDP	137	netbios-ns	192.168.0.3						
System	4	UDP	138	netbios-...	192.168.0.3						
System	3120	UDP	1900	ssdp	127.0.0.1						
System	3120	UDP	1900	ssdp	192.168.0.3						
System	392	UDP	3389	ms-wbt-...	0.0.0.0						
System	5520	UDP	5050		0.0.0.0						
System	1300	UDP	5353		0.0.0.0						
System	1300	UDP	5355	llmnr	0.0.0.0						
System	2836	UDP	49725		127.0.0.1						
System	652	UDP	55800		127.0.0.1						
System	3120	UDP	64750		192.168.0.3						
System	3120	UDP	64751		127.0.0.1						

CurrPorts

Do you want to close the selected TCP connections ?

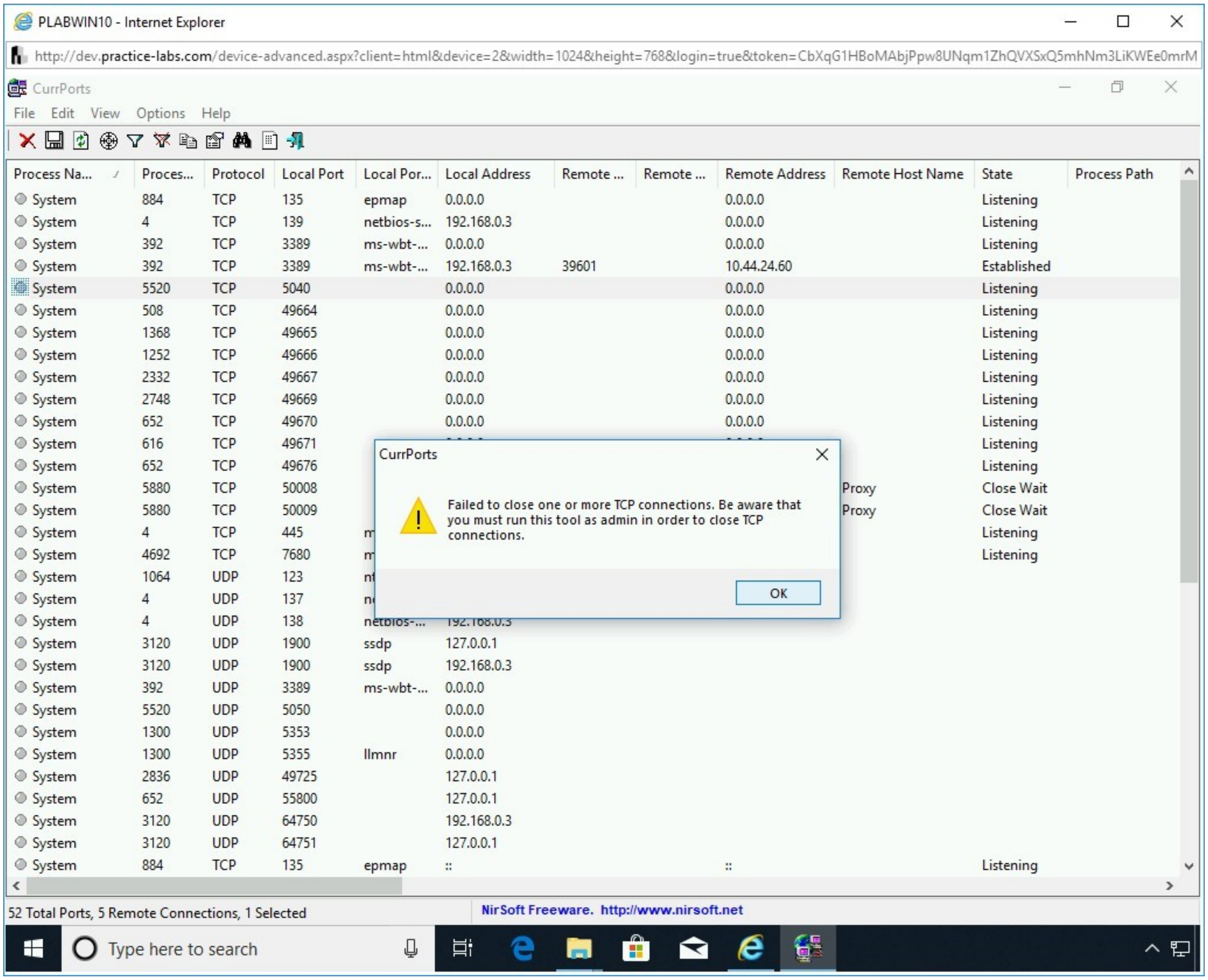
50 Total Ports, 3 Remote Connections, 1 Selected

Figure 1.46 Screenshot of PLABWIN10: Clicking Yes on the CurrPorts dialog box.

Step 10

The **CurrPorts** dialog box displays an error message. You must start the **CurrPorts** tool with admin privileges to close a TCP connection.

Click **OK**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
CurrPorts
File Edit View Options Help

Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...	Remote Address	Remote Host Name	State	Process Path
System	884	TCP	135	epmap	0.0.0.0			0.0.0.0		Listening	
System	4	TCP	139	netbios-s...	192.168.0.3			0.0.0.0		Listening	
System	392	TCP	3389	ms-wbt-...	0.0.0.0			0.0.0.0		Listening	
System	392	TCP	3389	ms-wbt-...	192.168.0.3	39601		10.44.24.60		Established	
System	5520	TCP	5040		0.0.0.0			0.0.0.0		Listening	
System	508	TCP	49664		0.0.0.0			0.0.0.0		Listening	
System	1368	TCP	49665		0.0.0.0			0.0.0.0		Listening	
System	1252	TCP	49666		0.0.0.0			0.0.0.0		Listening	
System	2332	TCP	49667		0.0.0.0			0.0.0.0		Listening	
System	2748	TCP	49669		0.0.0.0			0.0.0.0		Listening	
System	652	TCP	49670		0.0.0.0			0.0.0.0		Listening	
System	616	TCP	49671							Listening	
System	652	TCP	49676							Listening	
System	5880	TCP	50008						Proxy	Close Wait	
System	5880	TCP	50009						Proxy	Close Wait	
System	4	TCP	445	m						Listening	
System	4692	TCP	7680	m						Listening	
System	1064	UDP	123	nt							
System	4	UDP	137	n							
System	4	UDP	138	netbios-...	192.168.0.3						
System	3120	UDP	1900	ssdp	127.0.0.1						
System	3120	UDP	1900	ssdp	192.168.0.3						
System	392	UDP	3389	ms-wbt-...	0.0.0.0						
System	5520	UDP	5050		0.0.0.0						
System	1300	UDP	5353		0.0.0.0						
System	1300	UDP	5355	llmnr	0.0.0.0						
System	2836	UDP	49725		127.0.0.1						
System	652	UDP	55800		127.0.0.1						
System	3120	UDP	64750		192.168.0.3						
System	3120	UDP	64751		127.0.0.1						
System	884	TCP	135	epmap	::			::		Listening	

CurrPorts

Failed to close one or more TCP connections. Be aware that you must run this tool as admin in order to close TCP connections.

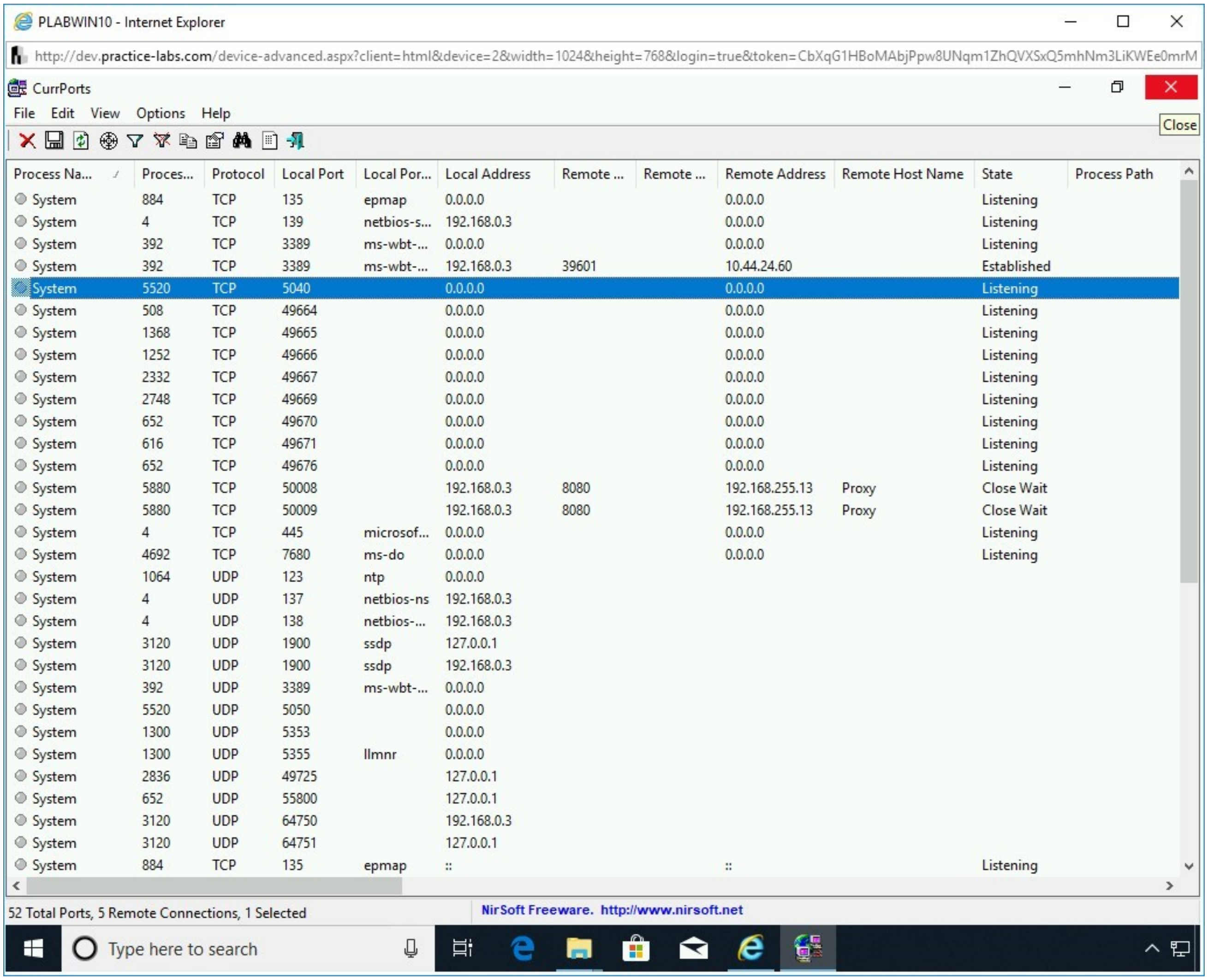
52 Total Ports, 5 Remote Connections, 1 Selected

NirSoft Freeware. http://www.nirsoft.net

Figure 1.47 Screenshot of PLABWIN10: Showing the error of elevated privileges required in the CurrPorts dialog box.

Step 11

Click **Close** to close the **CurrPorts** application.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
CurrPorts
File Edit View Options Help
Close

Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...	Remote Address	Remote Host Name	State	Process Path
System	884	TCP	135	epmap	0.0.0.0			0.0.0.0		Listening	
System	4	TCP	139	netbios-s...	192.168.0.3			0.0.0.0		Listening	
System	392	TCP	3389	ms-wbt-...	0.0.0.0			0.0.0.0		Listening	
System	392	TCP	3389	ms-wbt-...	192.168.0.3	39601		10.44.24.60		Established	
System	5520	TCP	5040		0.0.0.0			0.0.0.0		Listening	
System	508	TCP	49664		0.0.0.0			0.0.0.0		Listening	
System	1368	TCP	49665		0.0.0.0			0.0.0.0		Listening	
System	1252	TCP	49666		0.0.0.0			0.0.0.0		Listening	
System	2332	TCP	49667		0.0.0.0			0.0.0.0		Listening	
System	2748	TCP	49669		0.0.0.0			0.0.0.0		Listening	
System	652	TCP	49670		0.0.0.0			0.0.0.0		Listening	
System	616	TCP	49671		0.0.0.0			0.0.0.0		Listening	
System	652	TCP	49676		0.0.0.0			0.0.0.0		Listening	
System	5880	TCP	50008		192.168.0.3	8080		192.168.255.13	Proxy	Close Wait	
System	5880	TCP	50009		192.168.0.3	8080		192.168.255.13	Proxy	Close Wait	
System	4	TCP	445	microsof...	0.0.0.0			0.0.0.0		Listening	
System	4692	TCP	7680	ms-do	0.0.0.0			0.0.0.0		Listening	
System	1064	UDP	123	ntp	0.0.0.0						
System	4	UDP	137	netbios-ns	192.168.0.3						
System	4	UDP	138	netbios-...	192.168.0.3						
System	3120	UDP	1900	ssdp	127.0.0.1						
System	3120	UDP	1900	ssdp	192.168.0.3						
System	392	UDP	3389	ms-wbt-...	0.0.0.0						
System	5520	UDP	5050		0.0.0.0						
System	1300	UDP	5353		0.0.0.0						
System	1300	UDP	5355	llmnr	0.0.0.0						
System	2836	UDP	49725		127.0.0.1						
System	652	UDP	55800		127.0.0.1						
System	3120	UDP	64750		192.168.0.3						
System	3120	UDP	64751		127.0.0.1						
System	884	TCP	135	epmap	::			::		Listening	

52 Total Ports, 5 Remote Connections, 1 Selected

NirSoft Freeware. http://www.nirsoft.net

Figure 1.48 Screenshot of PLABWIN10: Closing the CurrPorts window.

Close the **File Explorer** windows.

Keep the **Internet Explorer** window open.

Task 4 - Use MyLanViewer to Scan a Network

MyLanViewer is a network and IP Scanner. It is also a tool that can search the WHOis database. You can use it for multiple purposes, such as:

- Traceroute
- Remote shutdown
- Wake On LAN (WOL) manager
- Wireless network scanner and monitor

In this task, you will use MyLanViewer to scan the network. To use MyLanViewer, perform the following steps:

Step 1

Ensure you have powered on the required devices and connect to **PLABWIN10**.

Restore the **Internet Explorer** window from the taskbar if it is minimized.

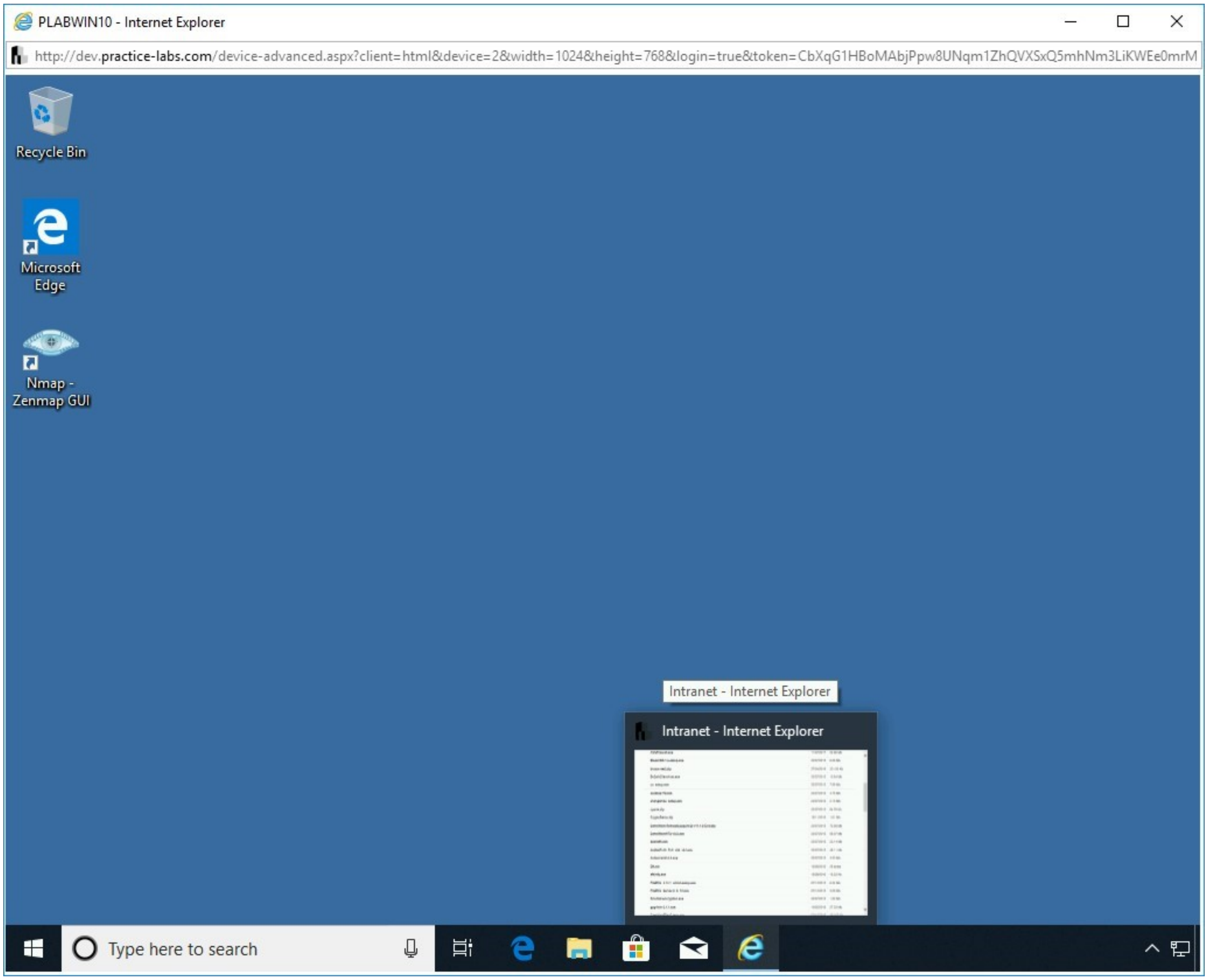
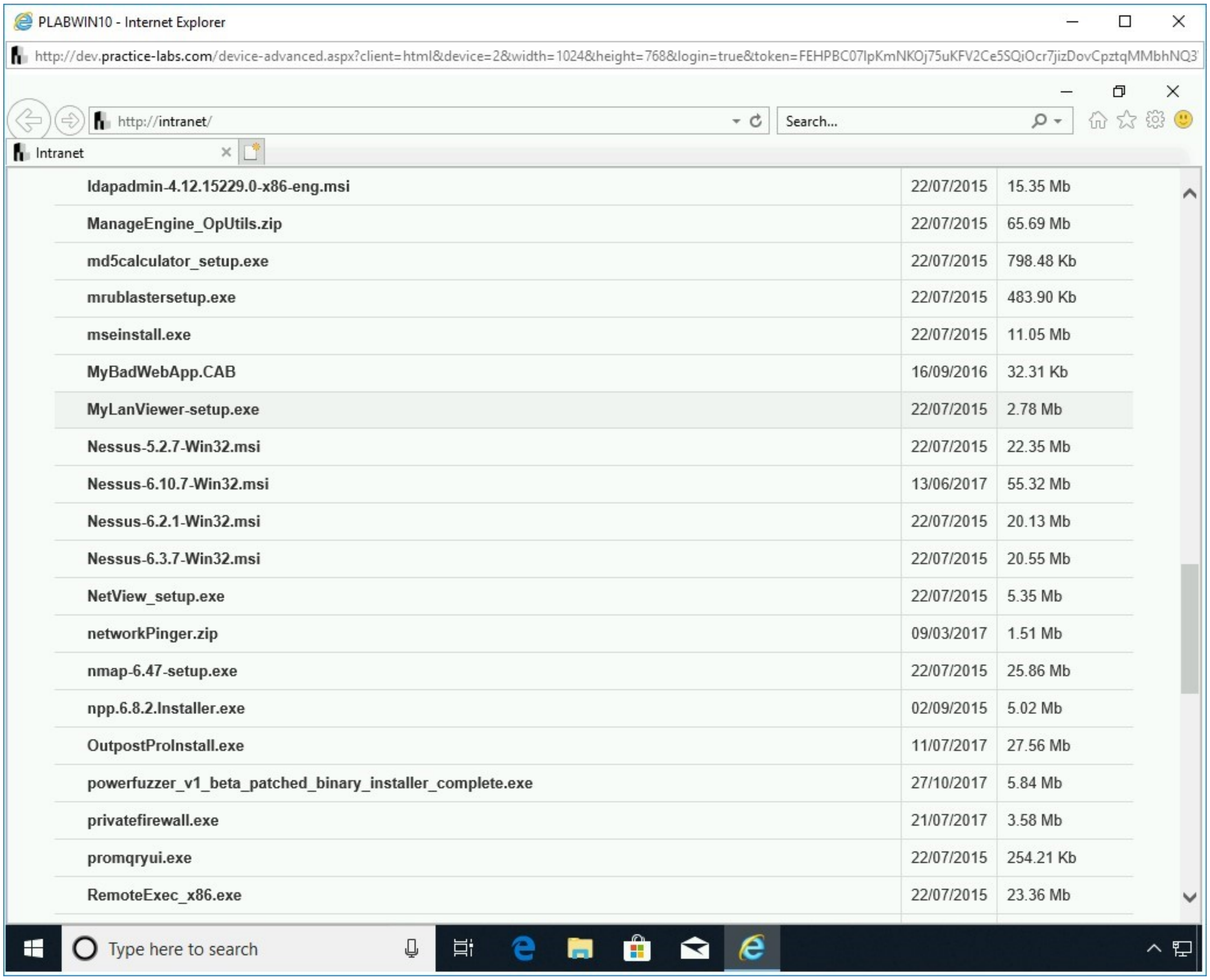

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=CbXqG1HBoMAbjPpw8UNqm1ZhQVXSxQ5mhNm3LiKWEe0mrM
Recycle Bin
Microsoft Edge
Nmap - Zenmap GUI
Intranet - Internet Explorer
Intranet - Internet Explorer
Type here to search

Figure 1.49 Screenshot of PLABWIN10: Restoring the Internet Explorer window from the taskbar.

Step 2

Ensure that you are on the **Hacking Tools** page on the **Intranet** Website.

Scroll down and click **MyLanViewer-setup.exe**.

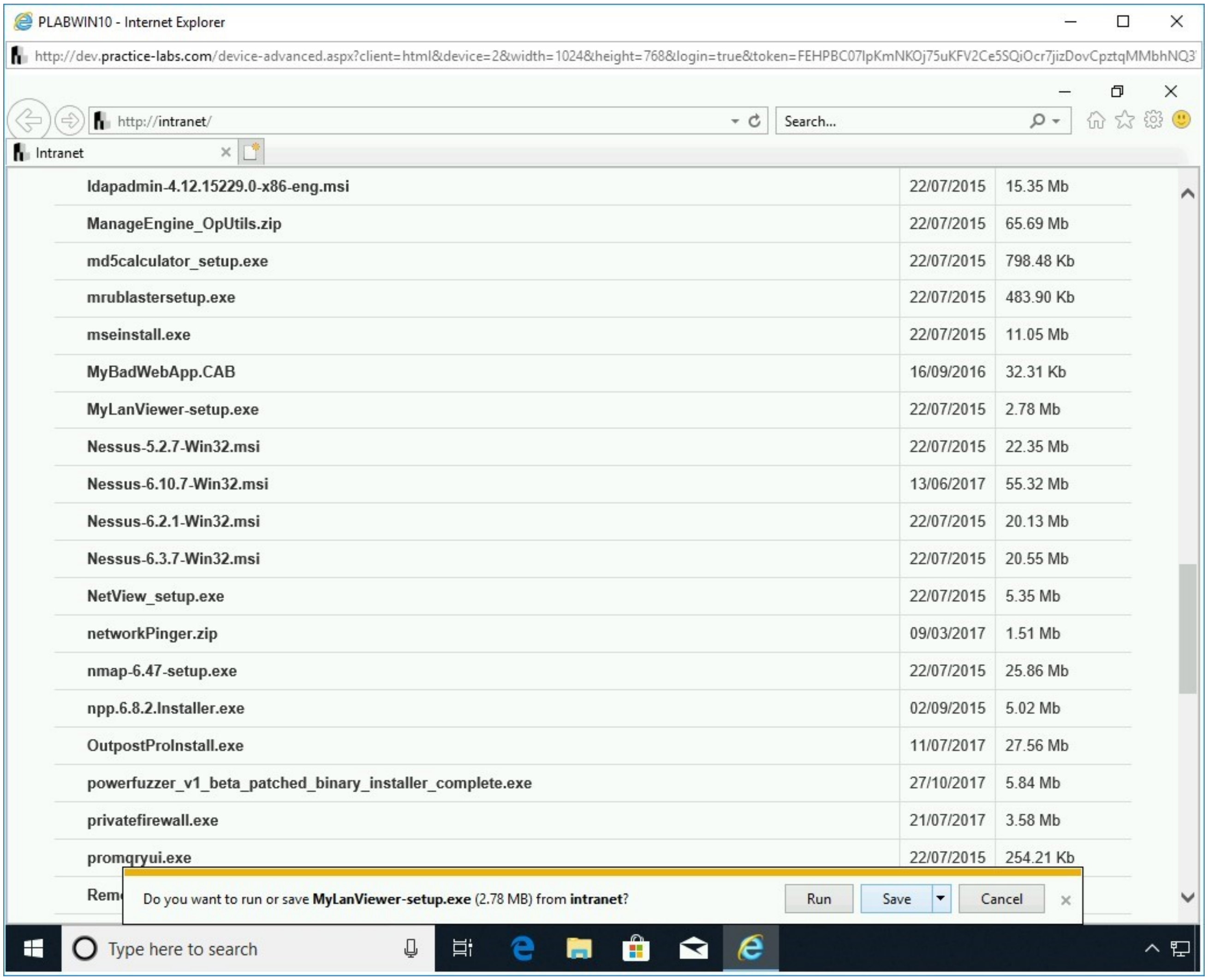

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
http://intranet/
Search...
Intranet
Type here to search

ldapadmin-4.12.15229.0-x86-eng.msi	22/07/2015	15.35 Mb
ManageEngine_OpUtils.zip	22/07/2015	65.69 Mb
md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb

Figure 1.50 Screenshot of PLABWIN10: Double-clicking the MyLanViewer-setup.exe file from the Intranet Webpage.

Step 3

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


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
http://intranet/
Search...
Intranet

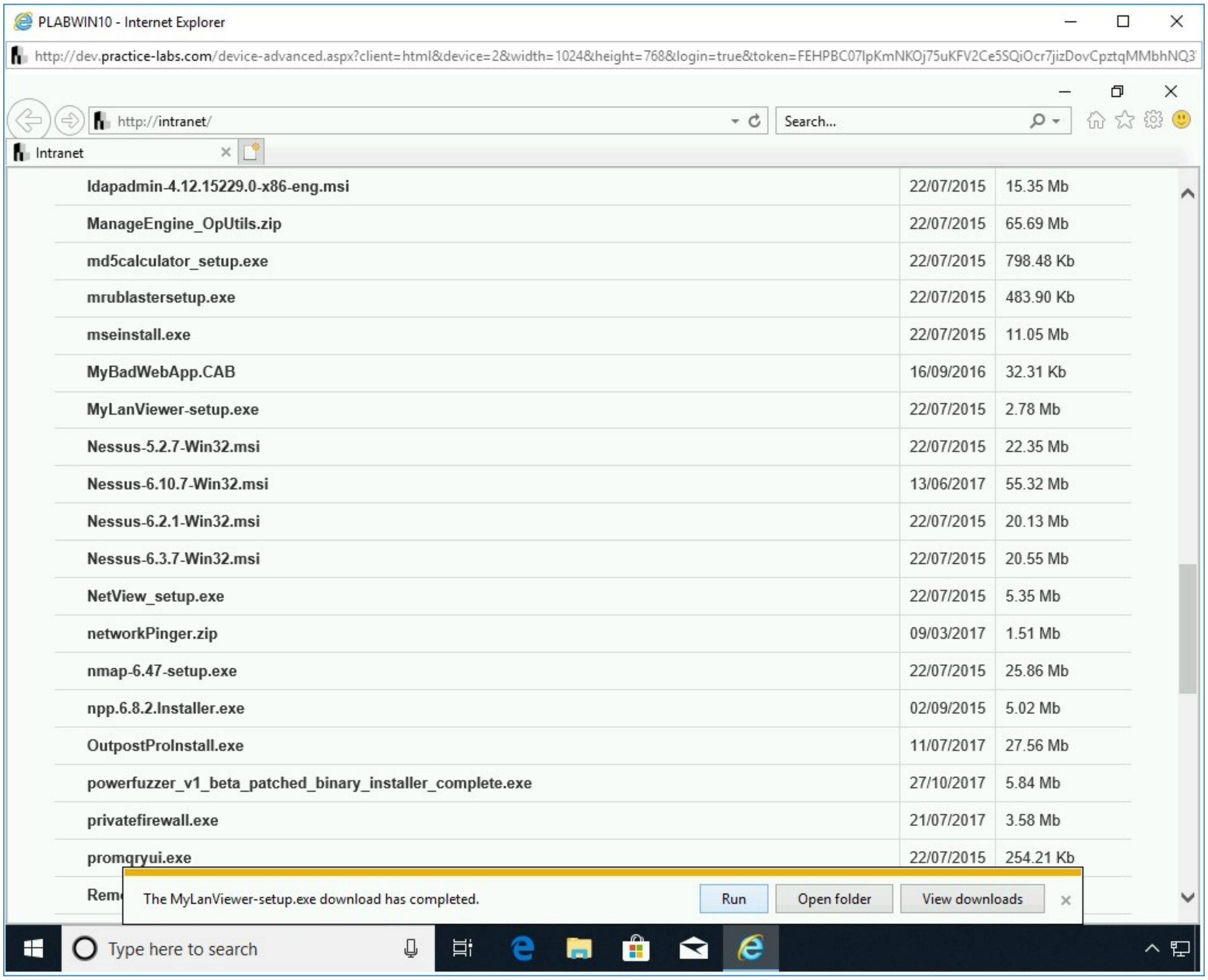
ldapadmin-4.12.15229.0-x86-eng.msi	22/07/2015	15.35 Mb
ManageEngine_OpUtils.zip	22/07/2015	65.69 Mb
md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
Rem		

Do you want to run or save **MyLanViewer-setup.exe** (2.78 MB) from **intranet**?

Figure 1.51 Screenshot of PLABWIN10: Clicking Save in the notification bar.

Step 4

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


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
http://intranet/
Search...
Intranet
Run
Open folder
View downloads
Type here to search

ldapadmin-4.12.15229.0-x86-eng.msi	22/07/2015	15.35 Mb
ManageEngine_OpUtils.zip	22/07/2015	65.69 Mb
md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
Rem		

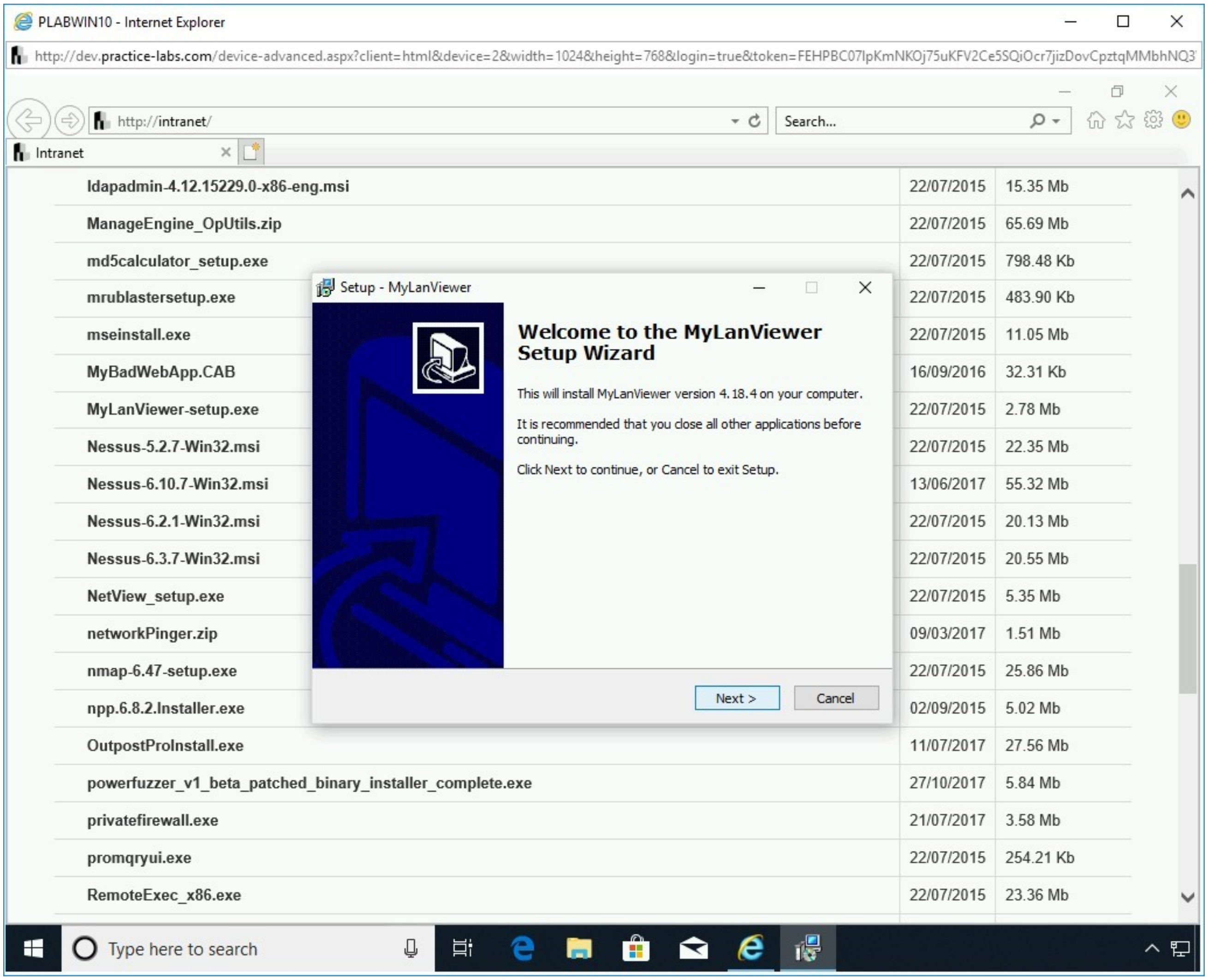
The MyLanViewer-setup.exe download has completed.

Figure 1.52 Screenshot of PLABWIN10: Clicking Run in the notification bar.

Step 5

The **Setup - MyLanViewer** wizard is displayed.

On the **Welcome to the MyLanViewer Setup Wizard** page, click **Next**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
http://intranet/
Search...
Intranet
Setup - MyLanViewer
Next >
Cancel
Type here to search

ldapadmin-4.12.15229.0-x86-eng.msi	22/07/2015	15.35 Mb
ManageEngine_OpUtils.zip	22/07/2015	65.69 Mb
md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb

Welcome to the MyLanViewer Setup Wizard

This will install MyLanViewer version 4.18.4 on your computer.

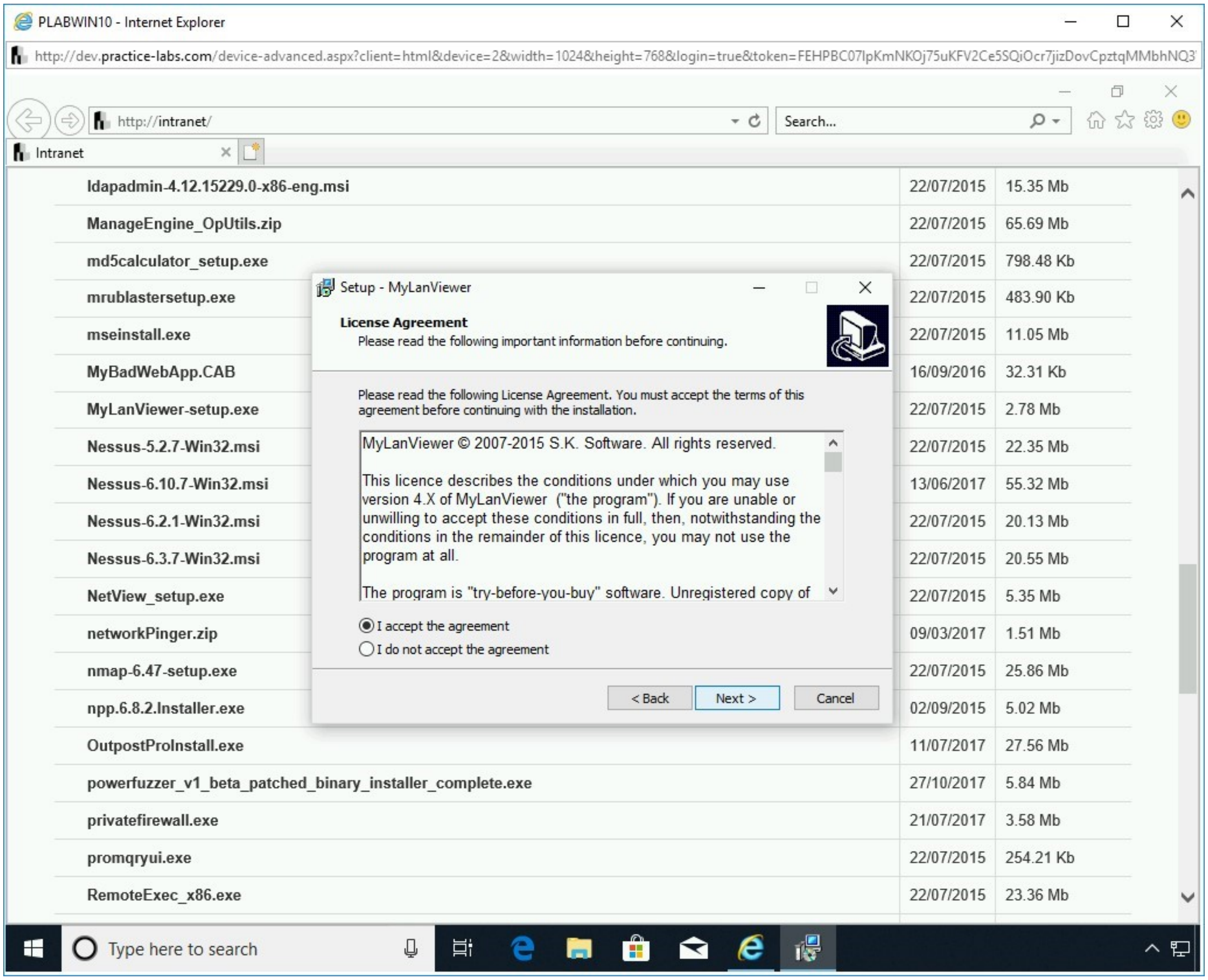
It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Figure 1.53 Screenshot of PLABWIN10: Clicking Next on the Welcome to the MyLANViwer Setup Wizard page.

Step 6

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



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
http://intranet/
Search...
Intranet
Type here to search

ldapadmin-4.12.15229.0-x86-eng.msi	22/07/2015	15.35 Mb
ManageEngine_OpUtils.zip	22/07/2015	65.69 Mb
md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb

Setup - MyLanViewer

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

MyLanViewer © 2007-2015 S.K. Software. All rights reserved.

This licence describes the conditions under which you may use version 4.X of MyLanViewer ("the program"). If you are unable or unwilling to accept these conditions in full, then, notwithstanding the conditions in the remainder of this licence, you may not use the program at all.

The program is "try-before-you-buy" software. Unregistered copy of

● I accept the agreement

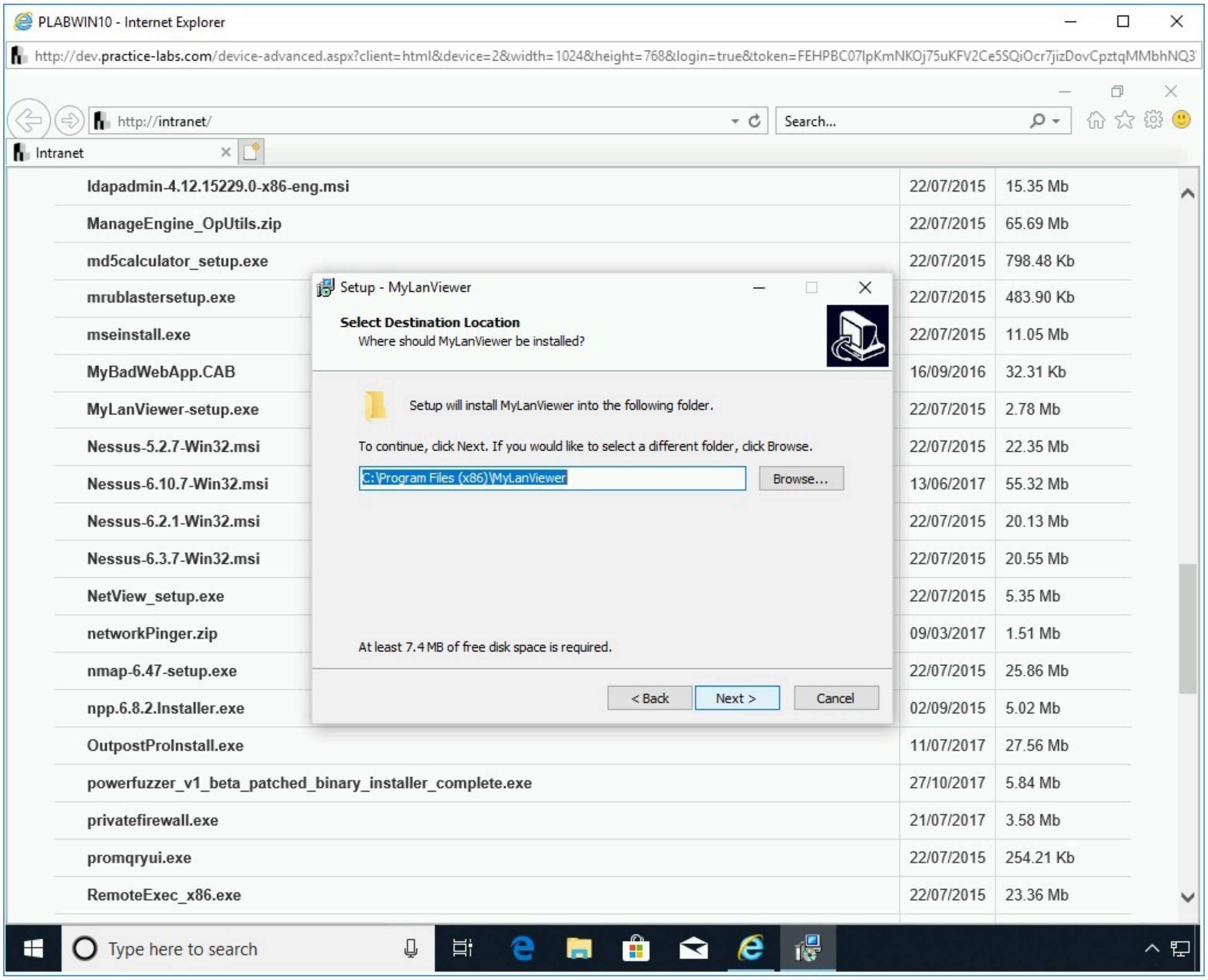
○ I do not accept the agreement

< Back | Next > | Cancel

Figure 1.54 Screenshot of PLABWIN10: Accepting the license agreement and clicking Next.

Step 7

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


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07lpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
http://intranet/
Search...
Intranet
Type here to search

ldapadmin-4.12.15229.0-x86-eng.msi	22/07/2015	15.35 Mb
ManageEngine_OpUtils.zip	22/07/2015	65.69 Mb
md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb

Setup - MyLanViewer

Select Destination Location

Where should MyLanViewer be installed?

Setup will install MyLanViewer into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

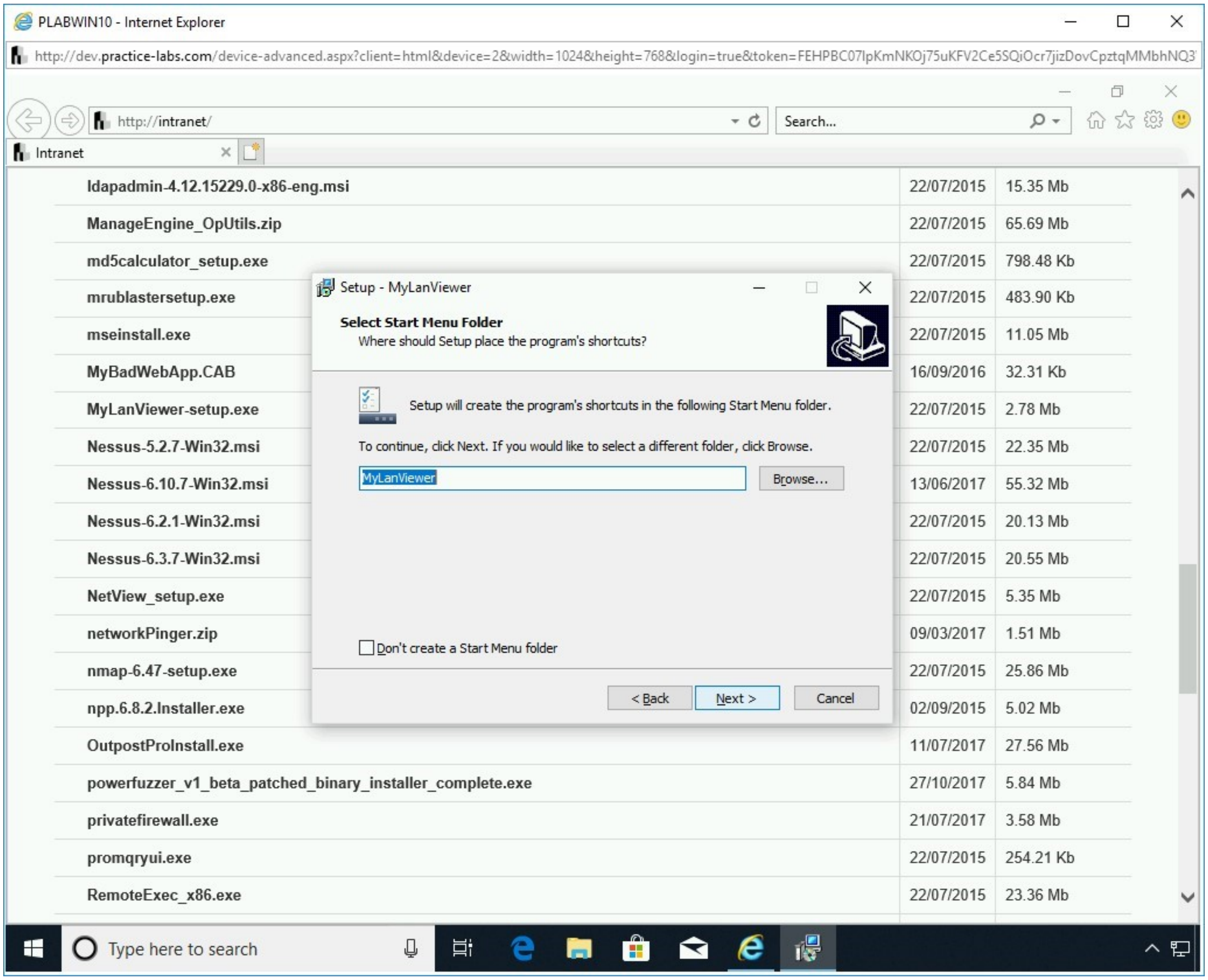
C:\Program Files (x86)\MyLanViewer

At least 7.4 MB of free disk space is required.

Figure 1.55 Screenshot of PLABWIN10: Clicking Next on the Select Destination Location page to accept the default location.

Step 8

On the **Select Start Menu Folder** page, keep the default name for the Start Menu and click **Next**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07lpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
http://intranet/
Search...
Intranet
Type here to search

ldapadmin-4.12.15229.0-x86-eng.msi	22/07/2015	15.35 Mb
ManageEngine_OpUtils.zip	22/07/2015	65.69 Mb
md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb

Setup - MyLanViewer

Select Start Menu Folder

Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

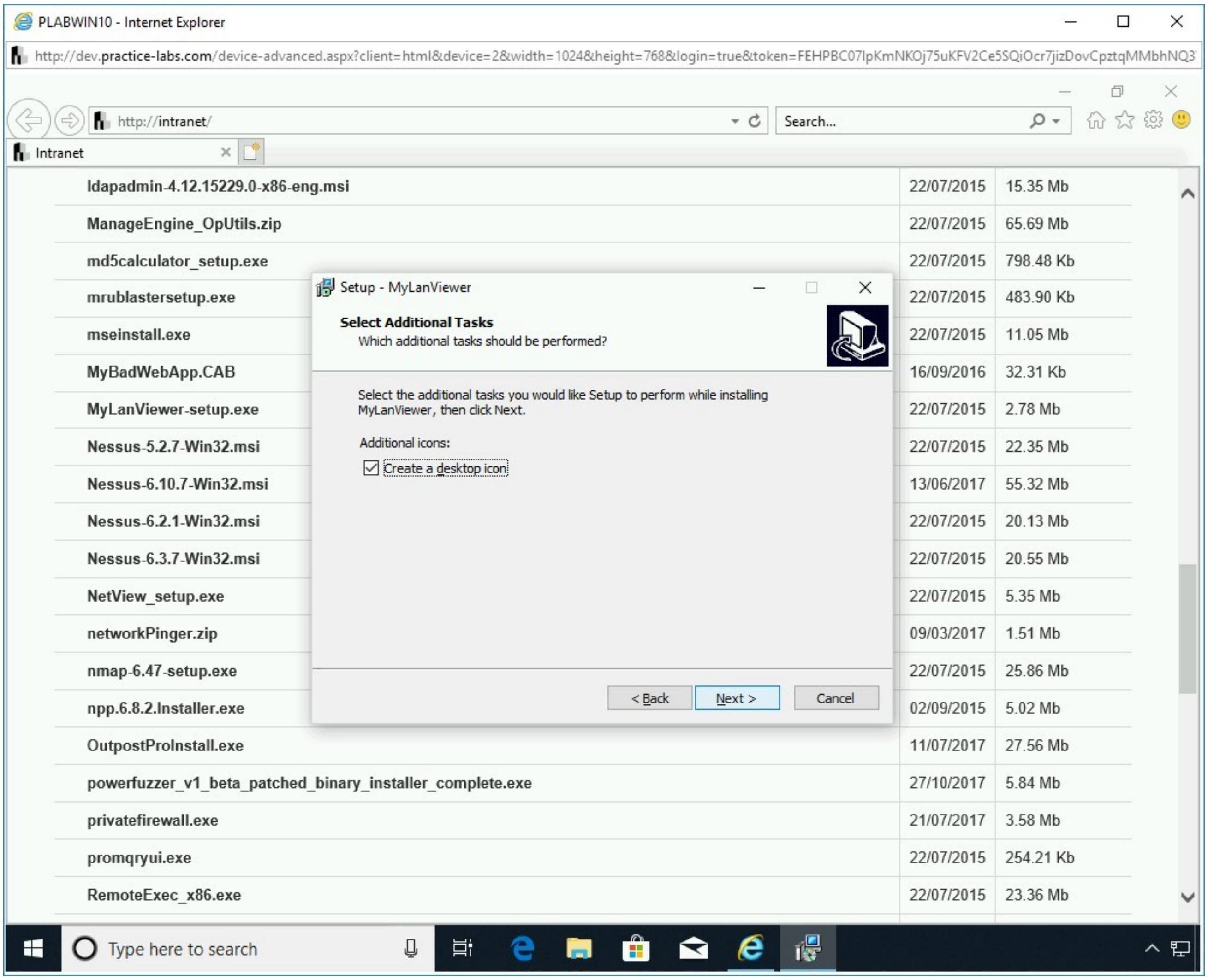
MyLanViewer

☐ Don't create a Start Menu folder

Figure 1.56 Screenshot of PLABWIN10: Clicking Next on the Select Start Menu Folder page.

Step 9

On the **Select Additional Tasks** page, keep the default selection and click **Next**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
http://intranet/
Search...
Intranet
Type here to search

ldapadmin-4.12.15229.0-x86-eng.msi	22/07/2015	15.35 Mb
ManageEngine_OpUtils.zip	22/07/2015	65.69 Mb
md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb

Setup - MyLanViewer

Select Additional Tasks

Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing MyLanViewer, then click Next.

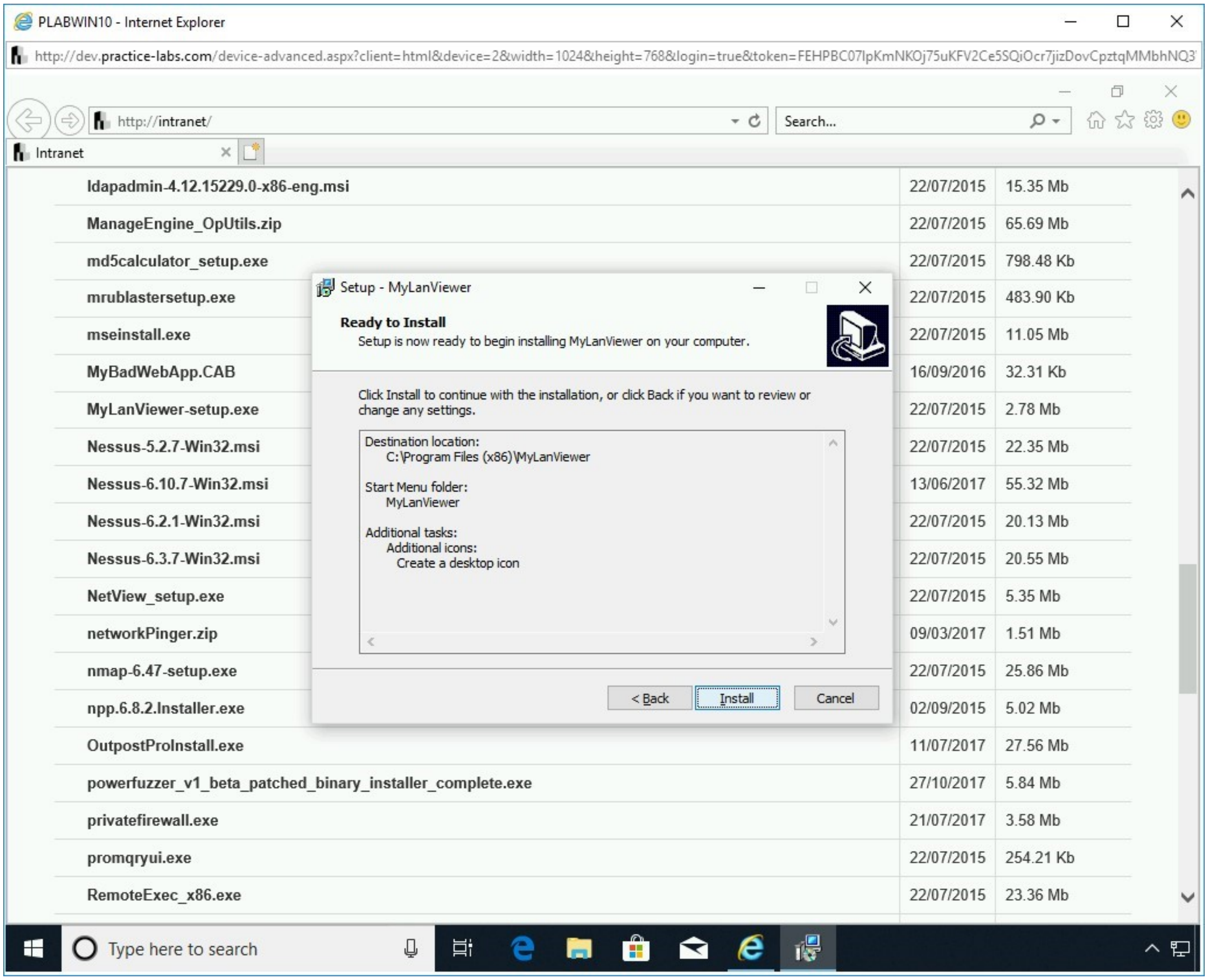
Additional icons:

☑ Create a desktop icon

Figure 1.57 Screenshot of PLABWIN10: Clicking Next on the Select Additional Tasks page.

Step 10

On the **Ready to Install** page, review the installation configuration, and click **Install**.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3

http://intranet/

ldapadmin-4.12.15229.0-x86-eng.msi	22/07/2015	15.35 Mb
ManageEngine_OpUtils.zip	22/07/2015	65.69 Mb
md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb

Setup - MyLanViewer

Ready to Install

Setup is now ready to begin installing MyLanViewer on your computer.

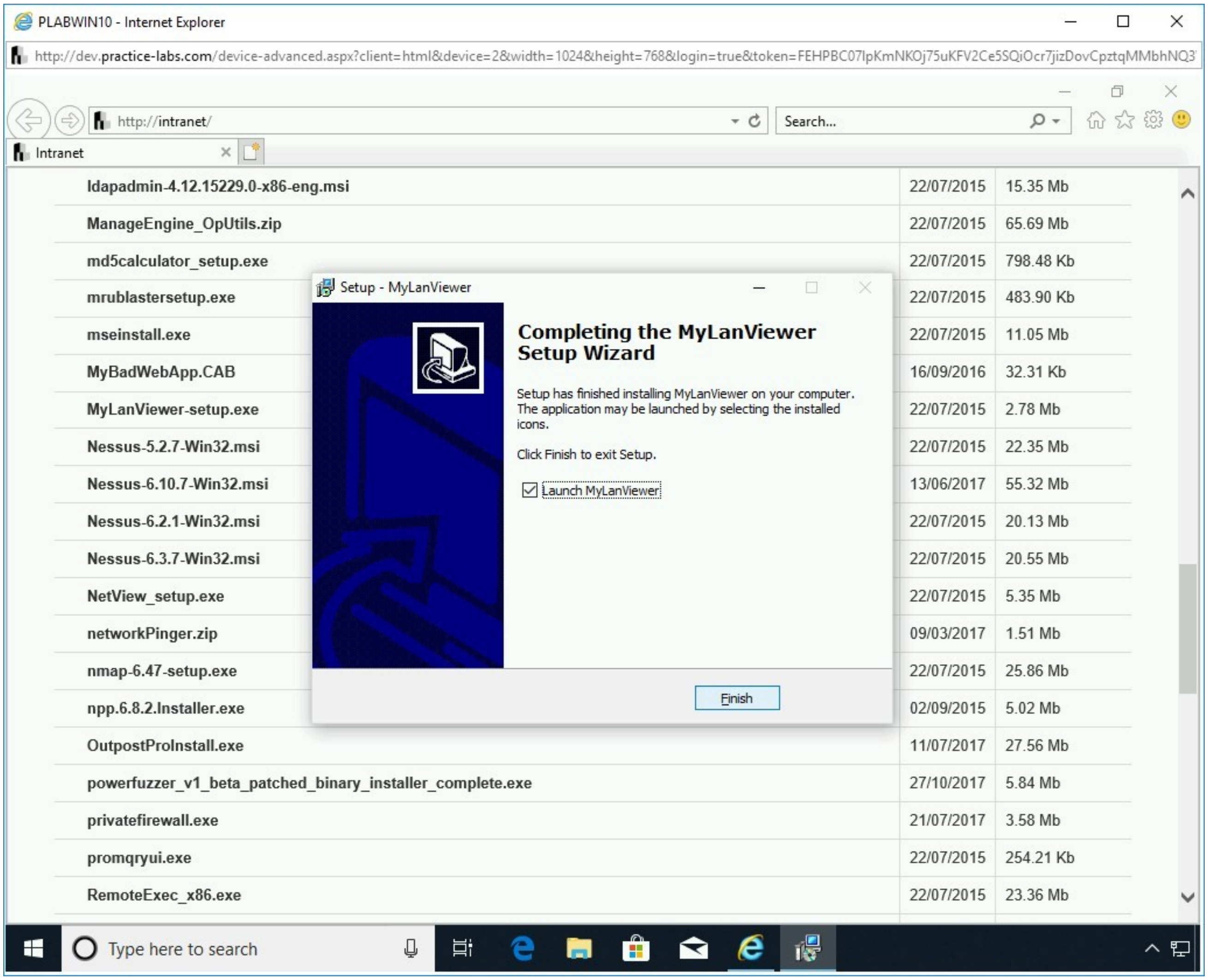
Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
    C:\Program Files (x86)\MyLanViewer

Start Menu folder:
    MyLanViewer

Additional tasks:
    Additional icons:
      Create a desktop icon
```

Figure 1.58 Screenshot of PLABWIN10: Clicking Install on the Ready to Install page.

Step 11

On the **Completing the MyLanViewer Setup Wizard** page, keep the default selection and click **Finish**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
http://intranet/
Search...
Intranet
Setup - MyLanViewer
Finish
Type here to search

ldapadmin-4.12.15229.0-x86-eng.msi	22/07/2015	15.35 Mb
ManageEngine_OpUtils.zip	22/07/2015	65.69 Mb
md5calculator_setup.exe	22/07/2015	798.48 Kb
mrublastersetup.exe	22/07/2015	483.90 Kb
mseinstall.exe	22/07/2015	11.05 Mb
MyBadWebApp.CAB	16/09/2016	32.31 Kb
MyLanViewer-setup.exe	22/07/2015	2.78 Mb
Nessus-5.2.7-Win32.msi	22/07/2015	22.35 Mb
Nessus-6.10.7-Win32.msi	13/06/2017	55.32 Mb
Nessus-6.2.1-Win32.msi	22/07/2015	20.13 Mb
Nessus-6.3.7-Win32.msi	22/07/2015	20.55 Mb
NetView_setup.exe	22/07/2015	5.35 Mb
networkPinger.zip	09/03/2017	1.51 Mb
nmap-6.47-setup.exe	22/07/2015	25.86 Mb
npp.6.8.2.Installer.exe	02/09/2015	5.02 Mb
OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb

Completing the MyLanViewer Setup Wizard

Setup has finished installing MyLanViewer on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

☑ Launch MyLanViewer

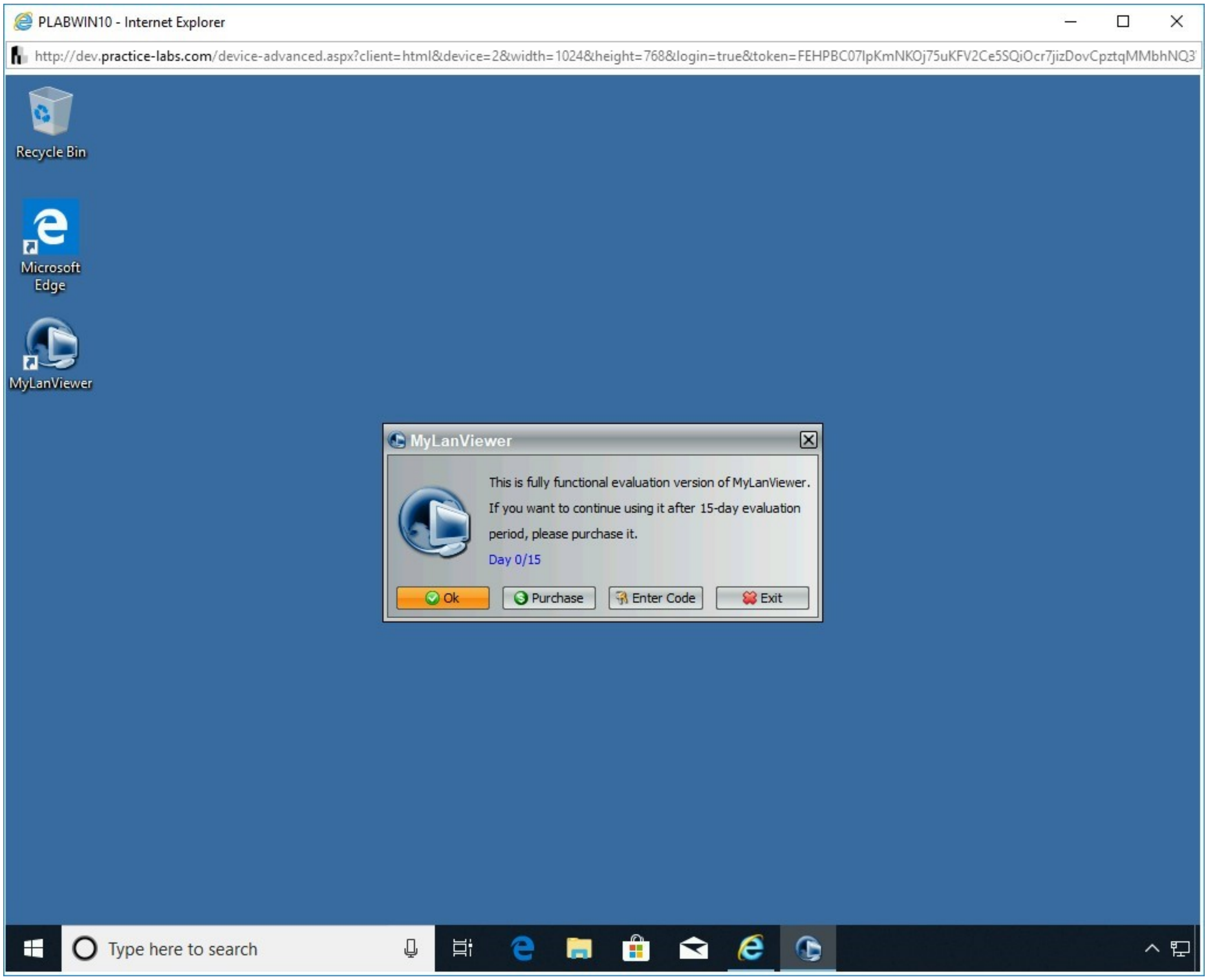
Figure 1.59 Screenshot of PLABWIN10: Clicking Finish on the Launch MyLanViewer page.

Minimize the **Internet Explorer** window.

Step 12

The **MyLanViewer** dialog box is displayed, informing that this is a trial version that will work as a fully functional product for **15** days.

Click **OK**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
Recycle Bin
Microsoft Edge
MyLanViewer
MyLanViewer
Ok
Purchase
Enter Code
Exit
Type here to search

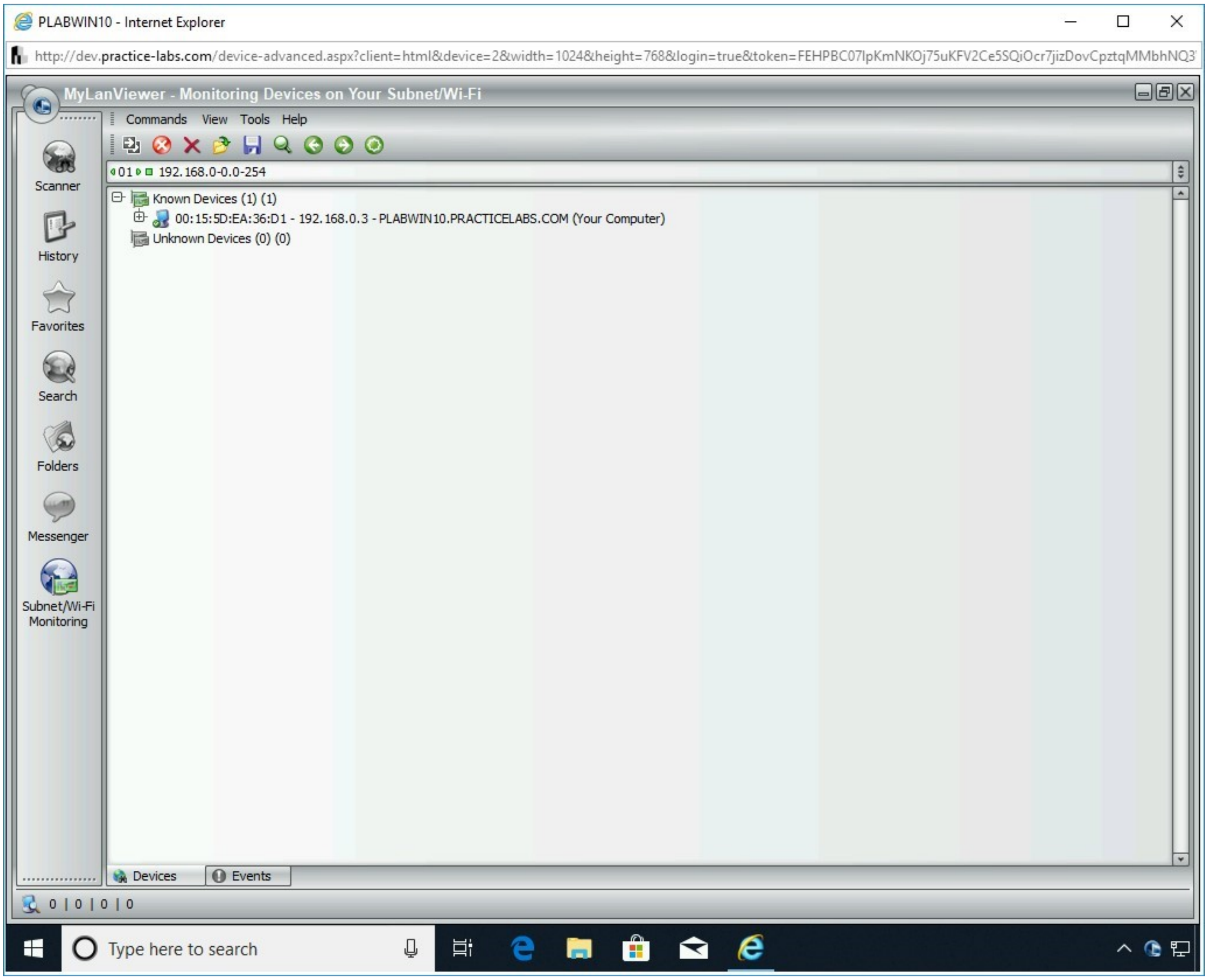
This is fully functional evaluation version of MyLanViewer. If you want to continue using it after 15-day evaluation period, please purchase it.

Day 0/15

Figure 1.60 Screenshot of PLABWIN10: Clicking OK on the MyLanViewer dialog box.

The **MyLanViewer - Monitoring Devices on Your Subnet/Wi-Fi** window is displayed.

MyLanViewer will now start to scan the subnet or Wi-Fi network depending on your system’s connectivity.



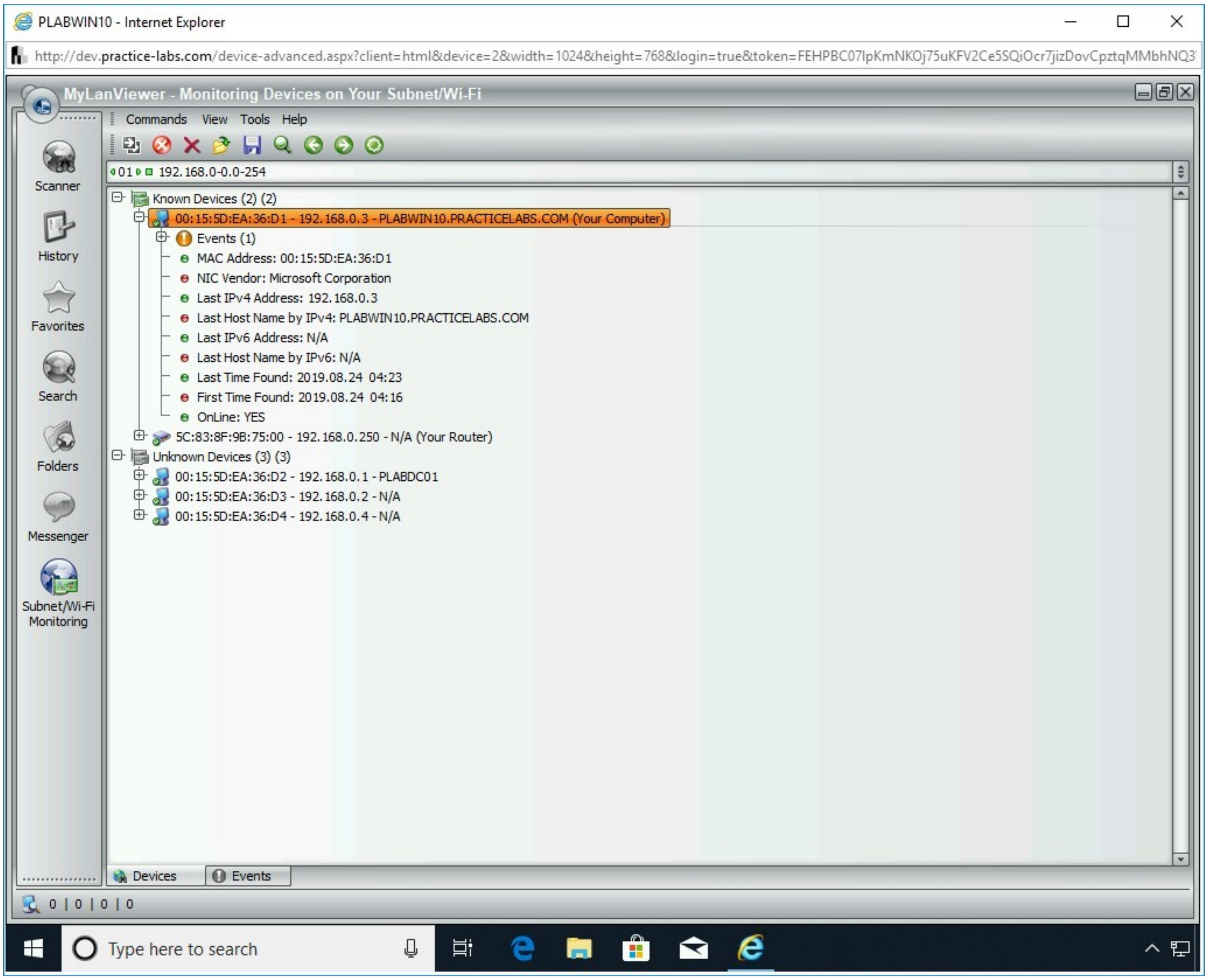
PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
MyLanViewer - Monitoring Devices on Your Subnet/Wi-Fi
Commands View Tools Help
01 192.168.0-0.0-254
Known Devices (1) (1)
00:15:5D:EA:36:D1 - 192.168.0.3 - PLABWIN10.PRACTICELABS.COM (Your Computer)
Unknown Devices (0) (0)
Scanner
History
Favorites
Search
Folders
Messenger
Subnet/Wi-Fi Monitoring
Devices
Events
0 | 0 | 0 | 0
Type here to search

Figure 1.61 Screenshot of PLABWIN10: Showing the scanning in the MyLanViewer - Monitoring Devices on Your Subnet/Wi-Fi window.

Step 13

After a few minutes, it is able to scan for the live systems on the subnet. Expand **PLABWIN10.PRACTICELABS.COM (Your Computer)**.

Notice that it has captured a lot of system-related information. For example, you can find its MAC address, IP address, and online status.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
MyLanViewer - Monitoring Devices on Your Subnet/Wi-Fi
Commands
View
Tools
Help
Scanner
History
Favorites
Search
Folders
Messenger
Subnet/Wi-Fi Monitoring
Devices
Events
0 | 0 | 0 | 0
Type here to search

01 192.168.0-0.0-254

Known Devices (2) (2)
- 00:15:5D:EA:36:D1 - 192.168.0.3 - PLABWIN10.PRACTICELABS.COM (Your Computer)
  - Events (1)
  - MAC Address: 00:15:5D:EA:36:D1
  - NIC Vendor: Microsoft Corporation
  - Last IPv4 Address: 192.168.0.3
  - Last Host Name by IPv4: PLABWIN10.PRACTICELABS.COM
  - Last IPv6 Address: N/A
  - Last Host Name by IPv6: N/A
  - Last Time Found: 2019.08.24 04:23
  - First Time Found: 2019.08.24 04:16
  - OnLine: YES
- 5C:83:8F:9B:75:00 - 192.168.0.250 - N/A (Your Router)

Unknown Devices (3) (3)
- 00:15:5D:EA:36:D2 - 192.168.0.1 - PLABDC01
- 00:15:5D:EA:36:D3 - 192.168.0.2 - N/A
- 00:15:5D:EA:36:D4 - 192.168.0.4 - N/A

Figure 1.62 Screenshot of PLABWIN10: Expanding PLABWIN10.PRACTICELABS.COM (Your Computer).

Step 14

Click **Tools** in the toolbar and select **Ping / Traceroute To Host**...

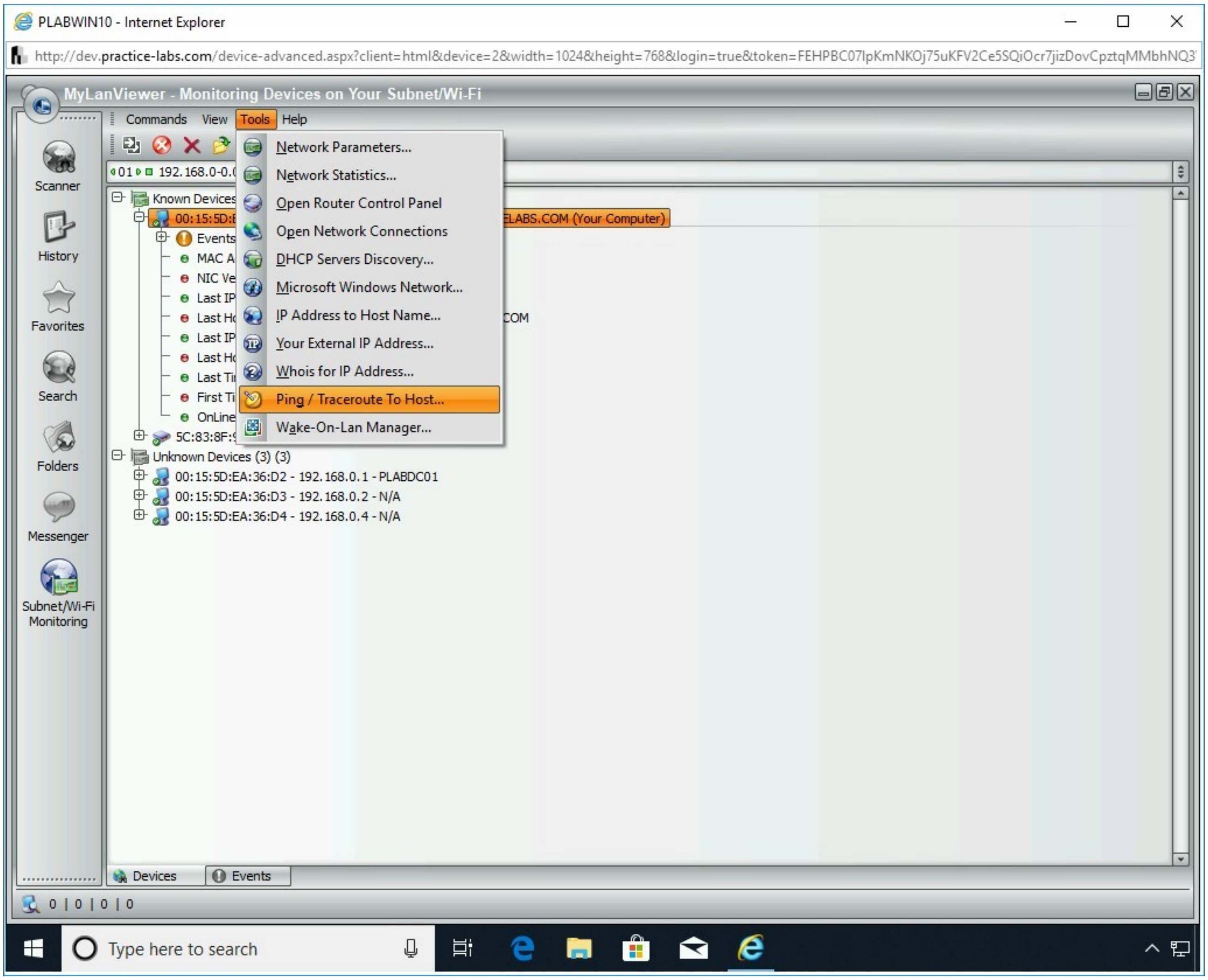

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
MyLanViewer - Monitoring Devices on Your Subnet/Wi-Fi
Commands
View
Tools
Help
Network Parameters...
Network Statistics...
Open Router Control Panel
Open Network Connections
DHCP Servers Discovery...
Microsoft Windows Network...
IP Address to Host Name...
Your External IP Address...
Whois for IP Address...
Ping / Traceroute To Host...
Wake-On-Lan Manager...
Scanner
History
Favorites
Search
Folders
Messenger
Subnet/Wi-Fi Monitoring
01 192.168.0-0.
Known Devices
00:15:5D:
LABS.COM (Your Computer)
Events
MAC A
NIC Ve
Last IP
Last Ho
Last IP
Last Ho
Last Ti
First Ti
OnLine
COM
5C:83:8F:
Unknown Devices (3) (3)
00:15:5D:EA:36:D2 - 192.168.0.1 - PLABDC01
00:15:5D:EA:36:D3 - 192.168.0.2 - N/A
00:15:5D:EA:36:D4 - 192.168.0.4 - N/A
Devices
Events
0 | 0 | 0 | 0
Type here to search

Figure 1.63 Screenshot of PLABWIN10: Clicking Tools and selecting Ping / Traceroute To Host option.

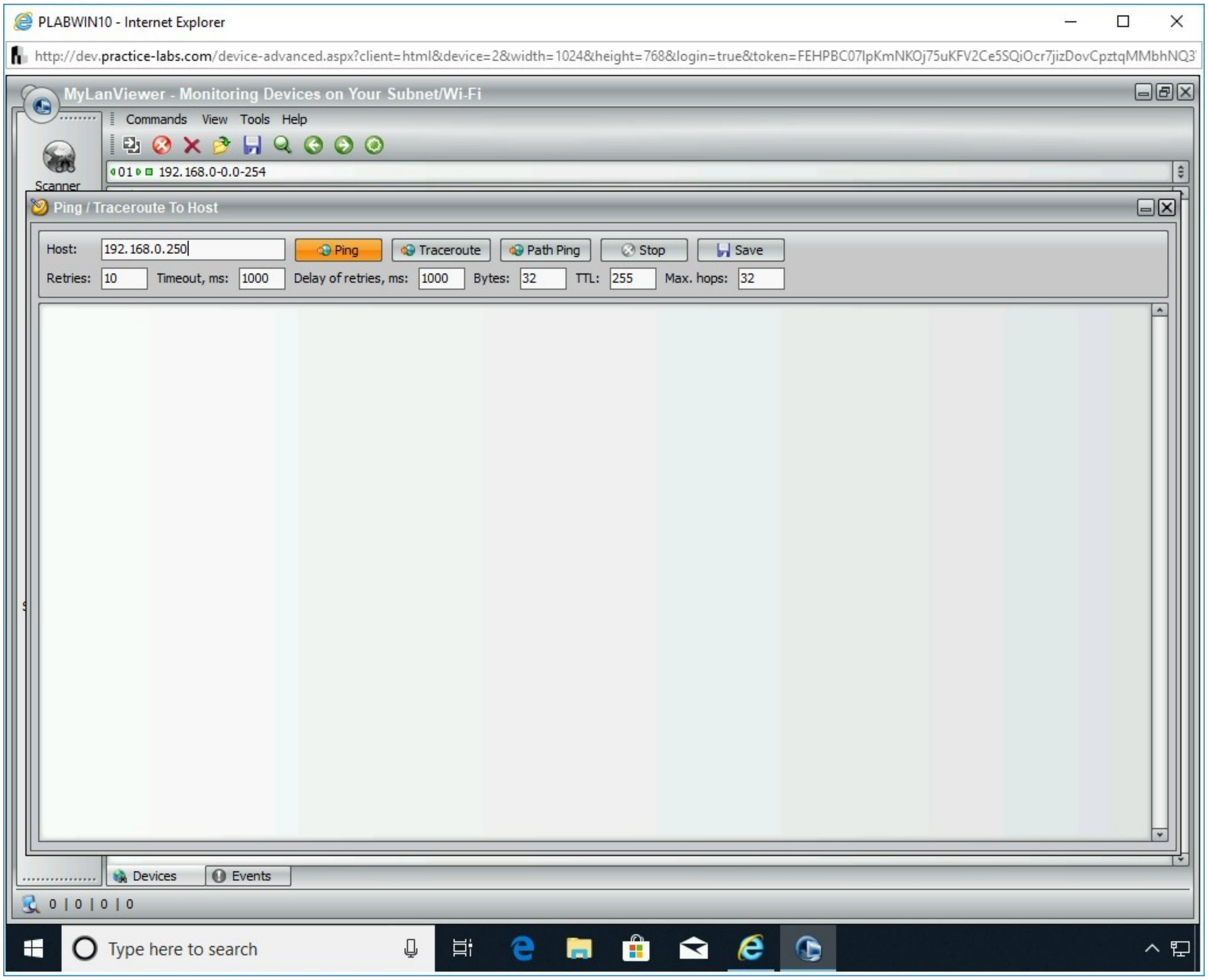
Step 15

The **Ping / Traceroute To Host** dialog box is displayed.

In the **Host** text box, type the following IP address:

```
192.168.0.250
```

Click **Ping**.



PLABWIN10 - Internet Explorer

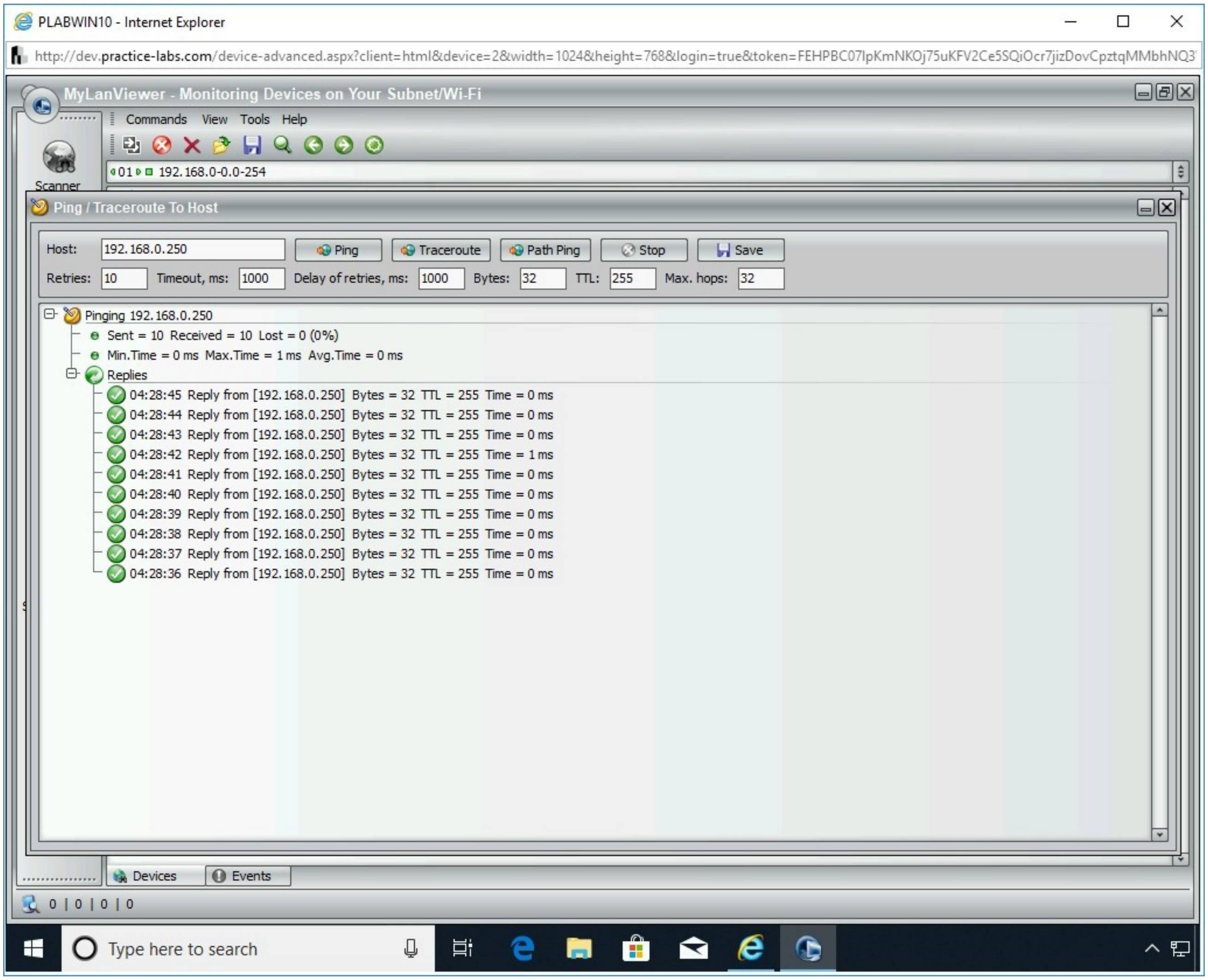
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3

Host: 192.168.0.250

Retries: 10 Timeout, ms: 1000 Delay of retries, ms: 1000 Bytes: 32 TTL: 255 Max. hops: 32

Figure 1.64 Screenshot of PLABWIN10: Entering the IP address in the Host textbox and clicking Ping.

The replies are received from the target, **192.168.0.250**.

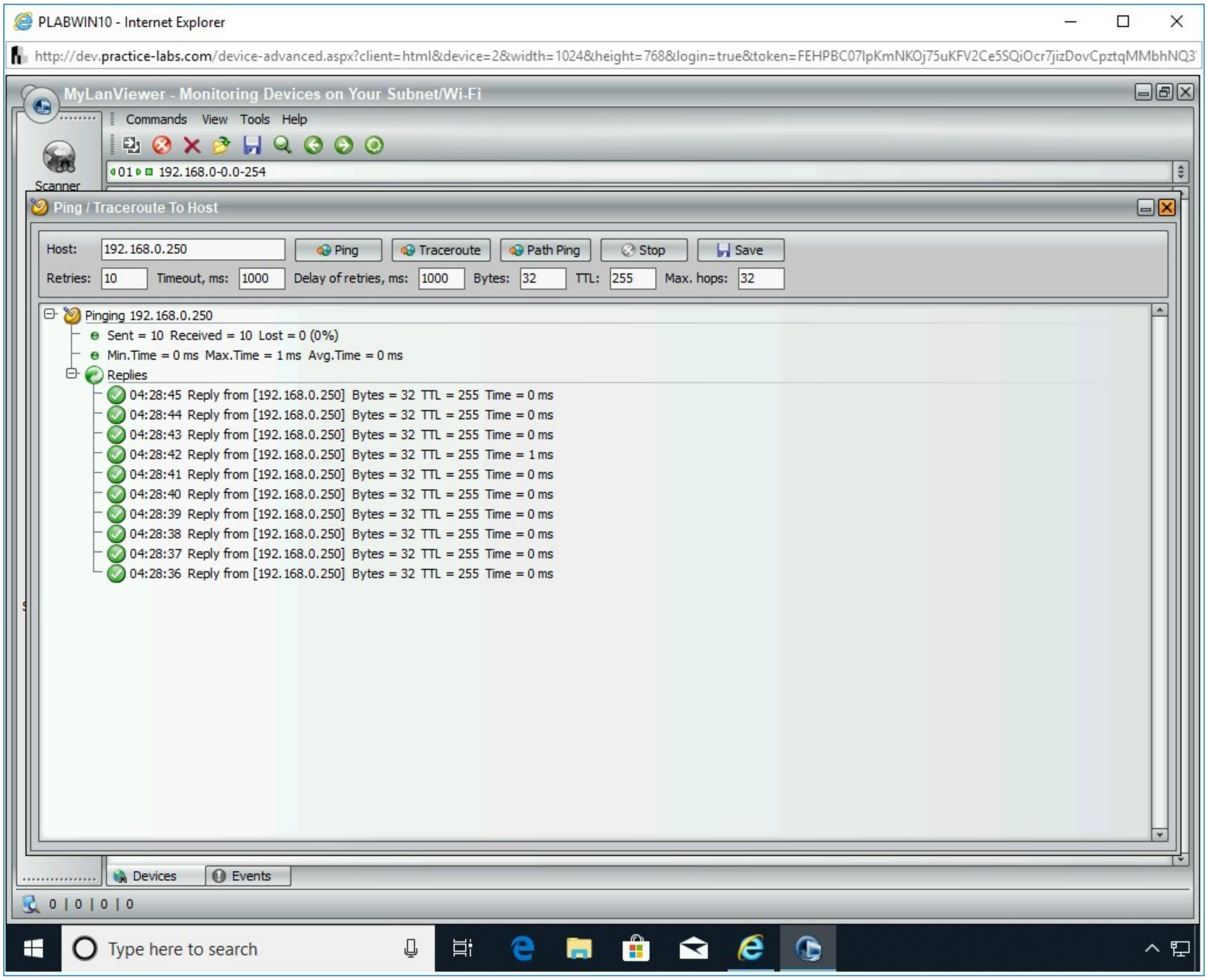

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
MyLanViewer - Monitoring Devices on Your Subnet/Wi-Fi
Commands
View
Tools
Help
Scanner
01
192.168.0-0.0-254
Ping / Traceroute To Host
Ping
Traceroute
Path Ping
Stop
Save
Devices
Events
0 | 0 | 0 | 0
Type here to search

```
Host: 192.168.0.250
Retries: 10   Timeout, ms: 1000   Delay of retries, ms: 1000   Bytes: 32   TTL: 255   Max. hops: 32

Pinging 192.168.0.250
  Sent = 10  Received = 10  Lost = 0 (0%)
  Min.Time = 0 ms  Max.Time = 1 ms  Avg.Time = 0 ms
  Replies
    04:28:45  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
    04:28:44  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
    04:28:43  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
    04:28:42  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 1 ms
    04:28:41  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
    04:28:40  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
    04:28:39  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
    04:28:38  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
    04:28:37  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
    04:28:36  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
```

Figure 1.65 Screenshot of PLABWIN10: Showing the received replies from the target system.

Step 16

Close the **Ping / Traceroute To Host** dialog box.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
MyLanViewer - Monitoring Devices on Your Subnet/Wi-Fi
Commands
View
Tools
Help
Scanner
01
192.168.0-0.0-254
Ping / Traceroute To Host
Ping
Traceroute
Path Ping
Stop
Save
Devices
Events
0 | 0 | 0 | 0
Type here to search

Host: 192.168.0.250

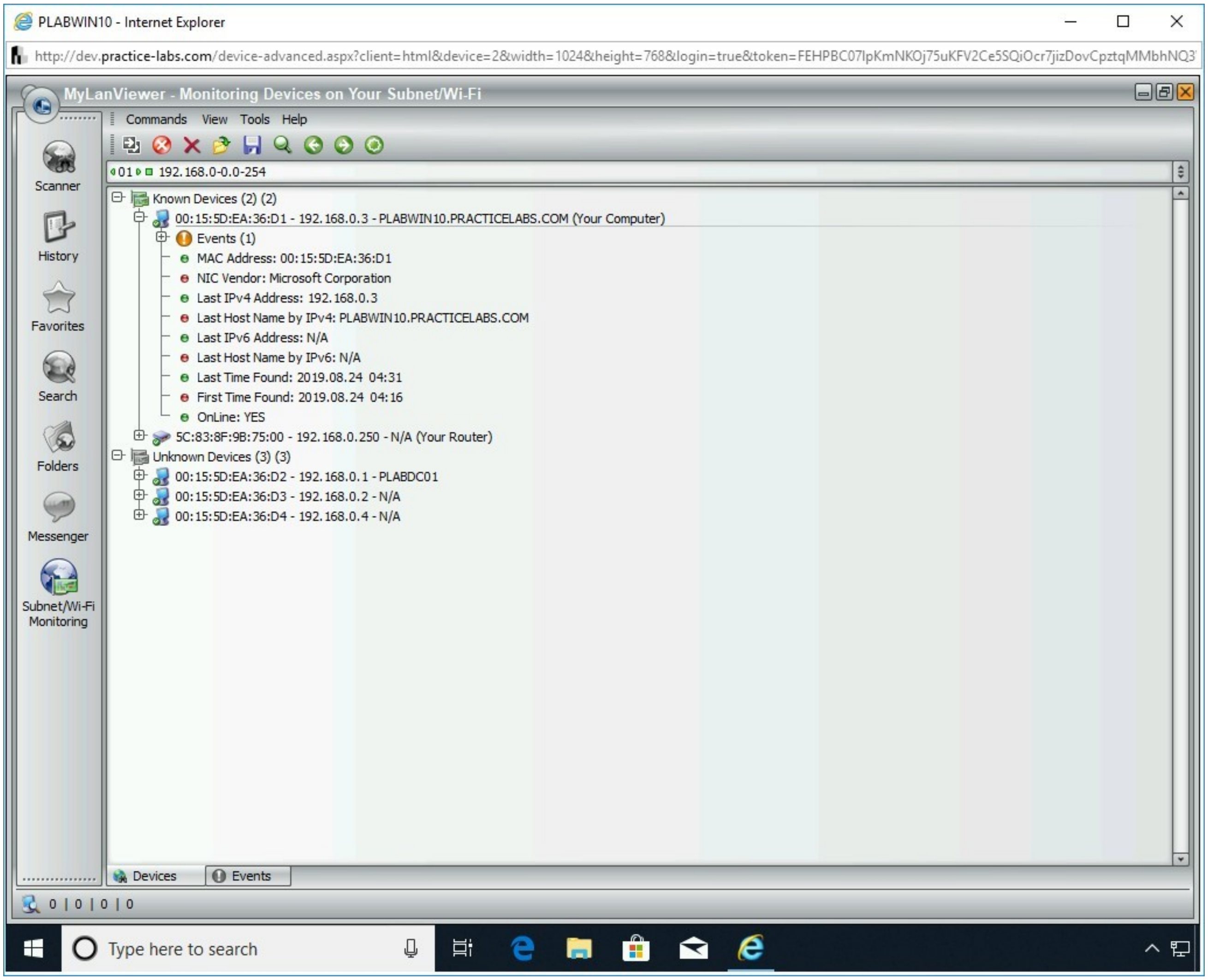
Retries: 10 Timeout, ms: 1000 Delay of retries, ms: 1000 Bytes: 32 TTL: 255 Max. hops: 32

```
Pinging 192.168.0.250
    Sent = 10  Received = 10  Lost = 0 (0%)
    Min.Time = 0 ms  Max.Time = 1 ms  Avg.Time = 0 ms
    Replies
        04:28:45  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
        04:28:44  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
        04:28:43  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
        04:28:42  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 1 ms
        04:28:41  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
        04:28:40  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
        04:28:39  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
        04:28:38  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
        04:28:37  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
        04:28:36  Reply from [192.168.0.250]  Bytes = 32  TTL = 255  Time = 0 ms
```

Figure 1.66 Screenshot of PLABWIN10: Closing the Ping / Traceroute To Host dialog box.

Step 17

Close the **MyLanViewer - Monitoring Devices on Your Subnet/Wi-Fi** window.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=FEHPBC07IpKmNKOj75uKFV2Ce5SQiOcr7jizDovCpztqMMbhNQ3
MyLanViewer - Monitoring Devices on Your Subnet/Wi-Fi
Commands
View
Tools
Help
Scanner
History
Favorites
Search
Folders
Messenger
Subnet/Wi-Fi Monitoring
Devices
Events
Type here to search

```
01 192.168.0-0.0-254
Known Devices (2) (2)
  00:15:5D:EA:36:D1 - 192.168.0.3 - PLABWIN10.PRACTICELABS.COM (Your Computer)
    Events (1)
    MAC Address: 00:15:5D:EA:36:D1
    NIC Vendor: Microsoft Corporation
    Last IPv4 Address: 192.168.0.3
    Last Host Name by IPv4: PLABWIN10.PRACTICELABS.COM
    Last IPv6 Address: N/A
    Last Host Name by IPv6: N/A
    Last Time Found: 2019.08.24 04:31
    First Time Found: 2019.08.24 04:16
    OnLine: YES
  5C:83:8F:9B:75:00 - 192.168.0.250 - N/A (Your Router)
Unknown Devices (3) (3)
  00:15:5D:EA:36:D2 - 192.168.0.1 - PLABDC01
  00:15:5D:EA:36:D3 - 192.168.0.2 - N/A
  00:15:5D:EA:36:D4 - 192.168.0.4 - N/A
0 | 0 | 0 | 0
```

Figure 1.67 Screenshot of PLABWIN10: Closing the MyLanViewer - Monitoring Devices on Your Subnet/Wi-Fi window.

Exercise 2 - Using Linux Network Scanning Tools

Kali Linux contains various tools that can be used for network scanning. These tools are:

- Hping3
- Dmitry
- Netcat
- Netdiscover
- Nmap

- Fping
- Msfconsole

Most of these tools are meant for network scanning. However, some of the tools are primarily for a different function. For example, Msfconsole if primarily a penetration testing and exploit creation tool, but it also provides the capability of scanning a network.

In this exercise, you will learn to use various Linux-based tools for network scanning.

Learning Outcomes

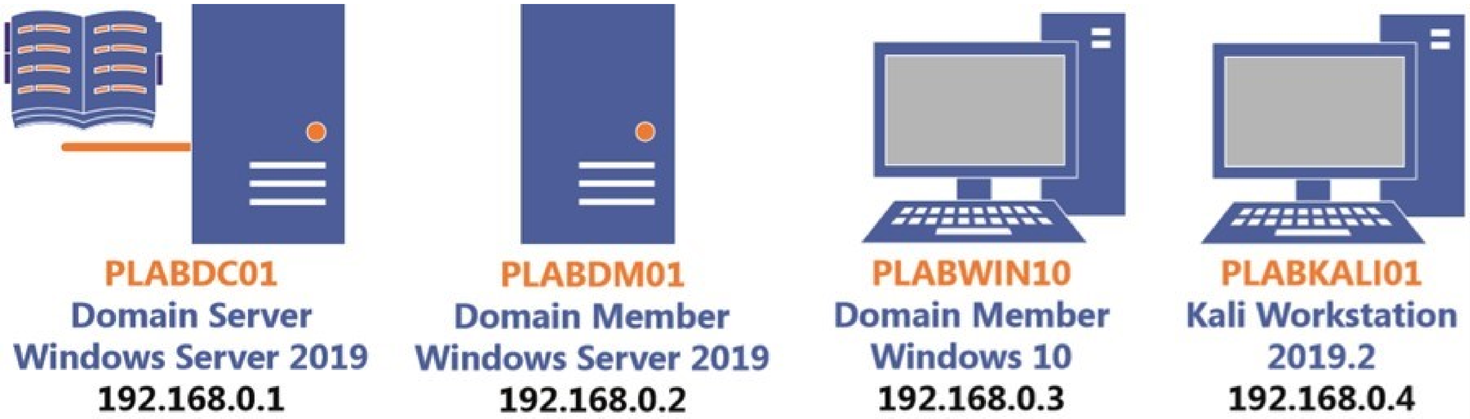
After completing this exercise, you will be able to:

- Use Hping3 for Network Scanning
- Perform a TCP Scan Using Dmitry
- Use Netcat for Port Scan
- Use Netdiscover for Scanning the Network
- Perform Stealth Scanning Using Nmap
- Use fping for Network Scanning
- Use Msfconsole to Perform TCP Stealth on a Network

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 Hping3 for Network Scanning

Hping3 is a powerful tool that can be used for various types of scanning in a network. It can perform Layer 3 and Layer 4 scanning.

In this task, you will use the hping3 tool to perform various types of network scanning. To do this, perform the following steps:

Step 1

Ensure you have powered on the required devices and connect to **PLABKALI01**.

Credentials are:

Username:

```
root
```

Password:

```
Passw0rd
```

Click the **Terminal** icon in the left pane.

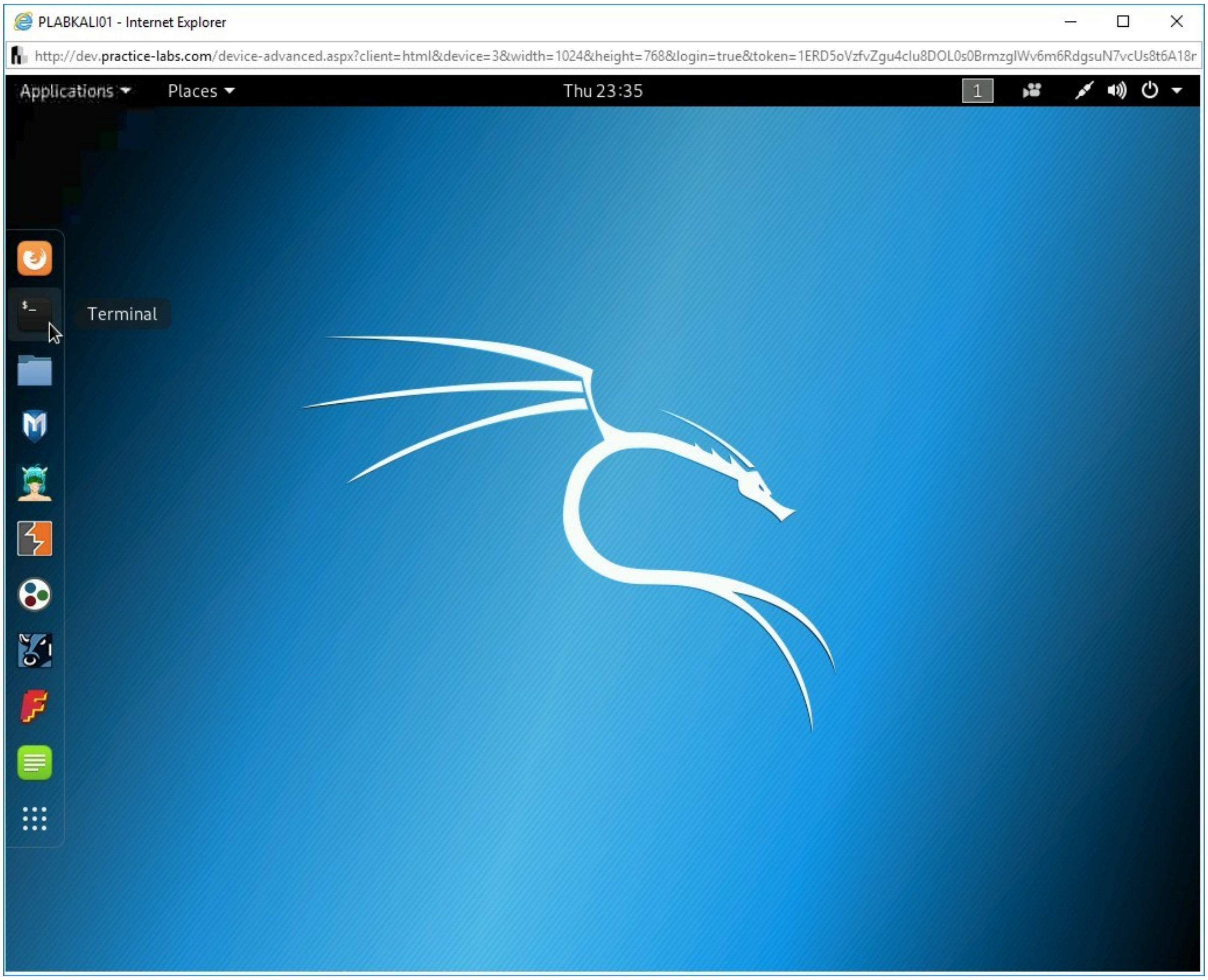

PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Thu 23:35
1
Terminal

Figure 2.1 Screenshot of PLABKALI01: Showing the desktop of PLABWIN10 and clicking the Terminal icon in the left pane.

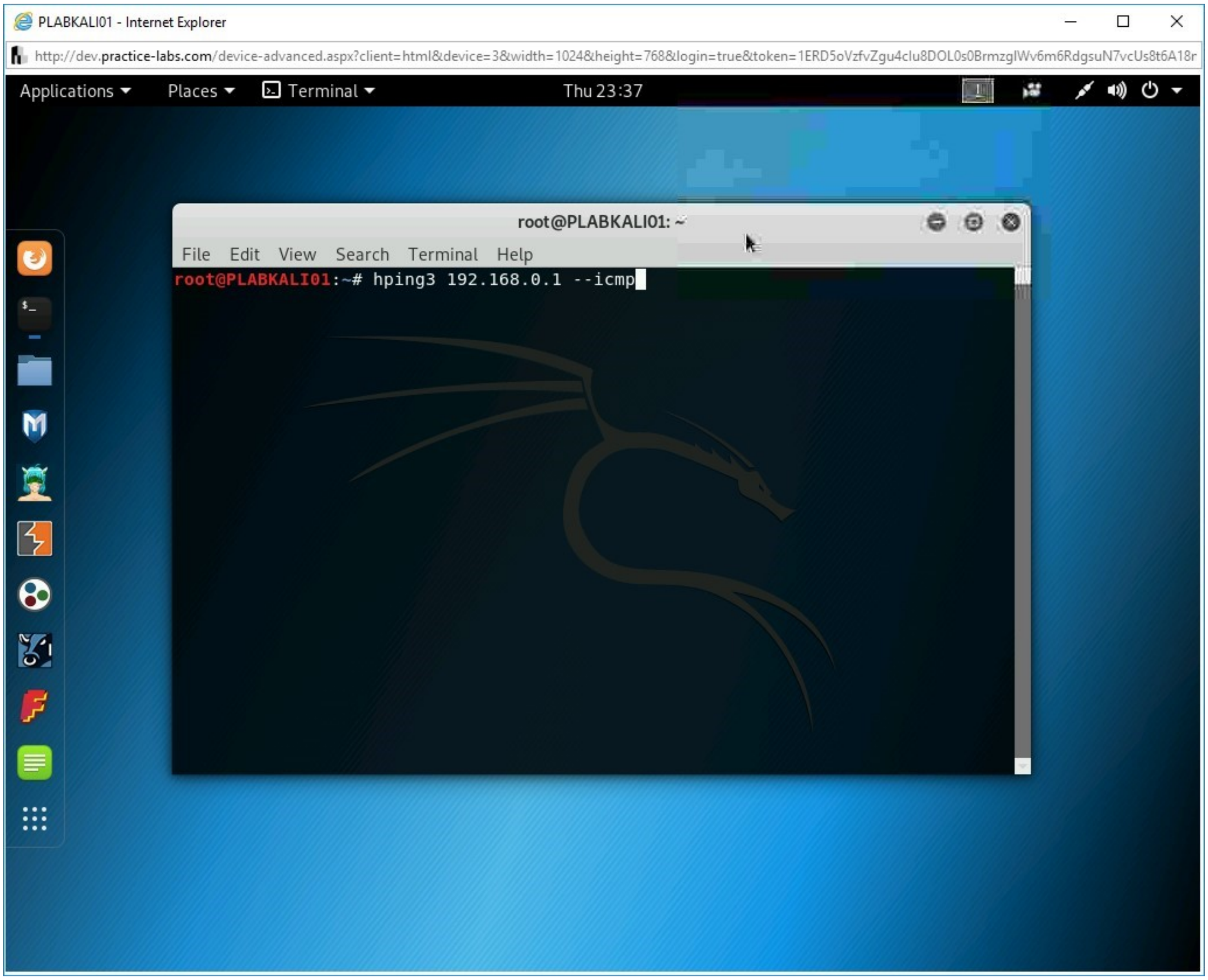
Step 2

The terminal window is displayed. You can perform an ICMP discovery of a single host using hping3.

Type the following command:

```
hping3 192.168.0.1 --icmp
```

Press **Enter**.



PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Terminal
Thu 23:37
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

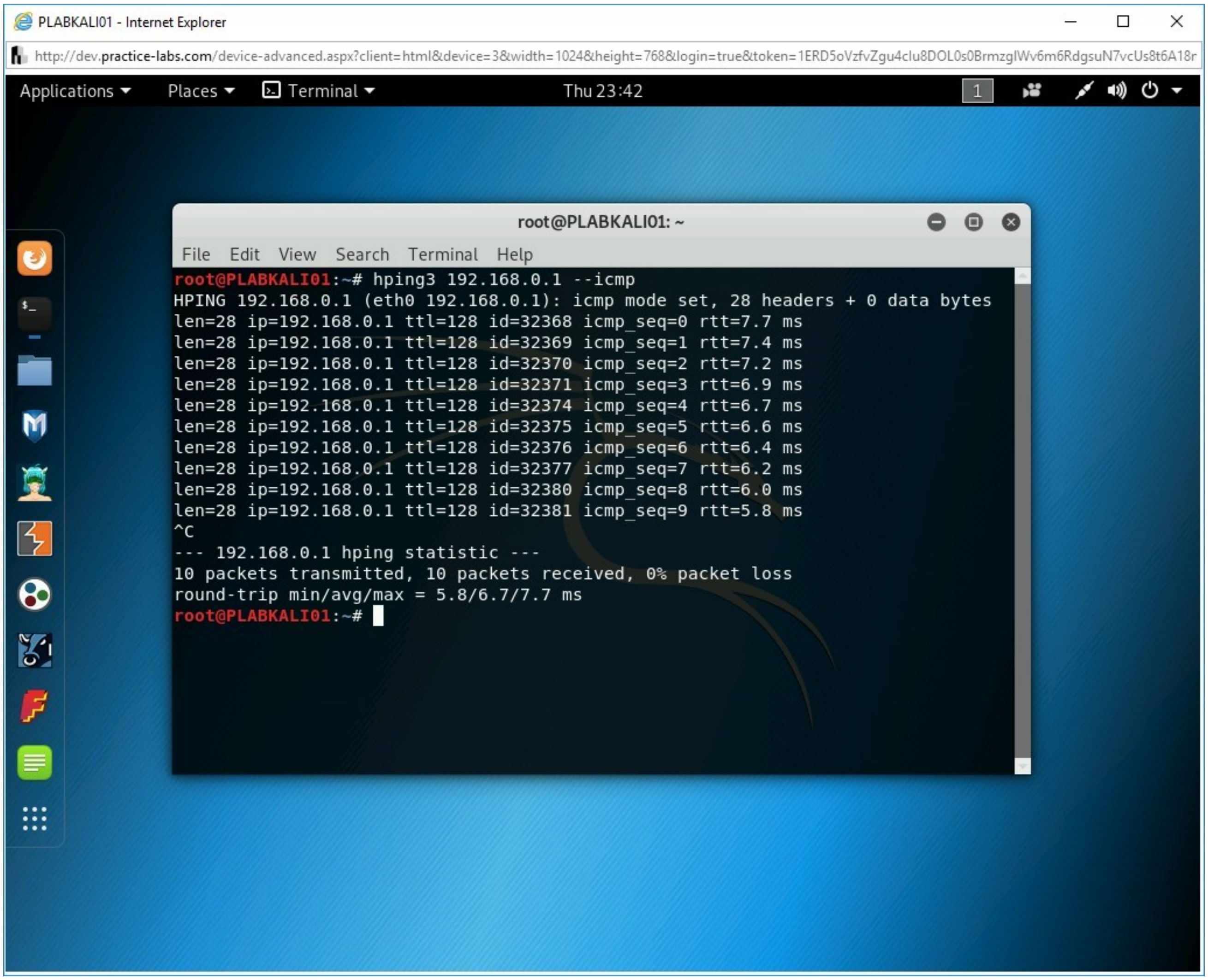
```
root@PLABKALI01:~# hping3 192.168.0.1 --icmp
```

Figure 2.2 Screenshot of PLABKALI01: Entering the command to perform ICMP discovery of a single host.

Step 3

The output of the command is displayed.

The **hping3** command will continue for an indefinite time unless you stop it. To do this, press the **Ctrl + C** keys.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Terminal
Thu 23:42
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# hping3 192.168.0.1 --icmp
HPING 192.168.0.1 (eth0 192.168.0.1): icmp mode set, 28 headers + 0 data bytes
len=28 ip=192.168.0.1 ttl=128 id=32368 icmp_seq=0 rtt=7.7 ms
len=28 ip=192.168.0.1 ttl=128 id=32369 icmp_seq=1 rtt=7.4 ms
len=28 ip=192.168.0.1 ttl=128 id=32370 icmp_seq=2 rtt=7.2 ms
len=28 ip=192.168.0.1 ttl=128 id=32371 icmp_seq=3 rtt=6.9 ms
len=28 ip=192.168.0.1 ttl=128 id=32374 icmp_seq=4 rtt=6.7 ms
len=28 ip=192.168.0.1 ttl=128 id=32375 icmp_seq=5 rtt=6.6 ms
len=28 ip=192.168.0.1 ttl=128 id=32376 icmp_seq=6 rtt=6.4 ms
len=28 ip=192.168.0.1 ttl=128 id=32377 icmp_seq=7 rtt=6.2 ms
len=28 ip=192.168.0.1 ttl=128 id=32380 icmp_seq=8 rtt=6.0 ms
len=28 ip=192.168.0.1 ttl=128 id=32381 icmp_seq=9 rtt=5.8 ms
^C
--- 192.168.0.1 hping statistic ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 5.8/6.7/7.7 ms
root@PLABKALI01:~#
```

Figure 2.3 Screenshot of PLABKALI01: Showing the response from the target system.

Step 4

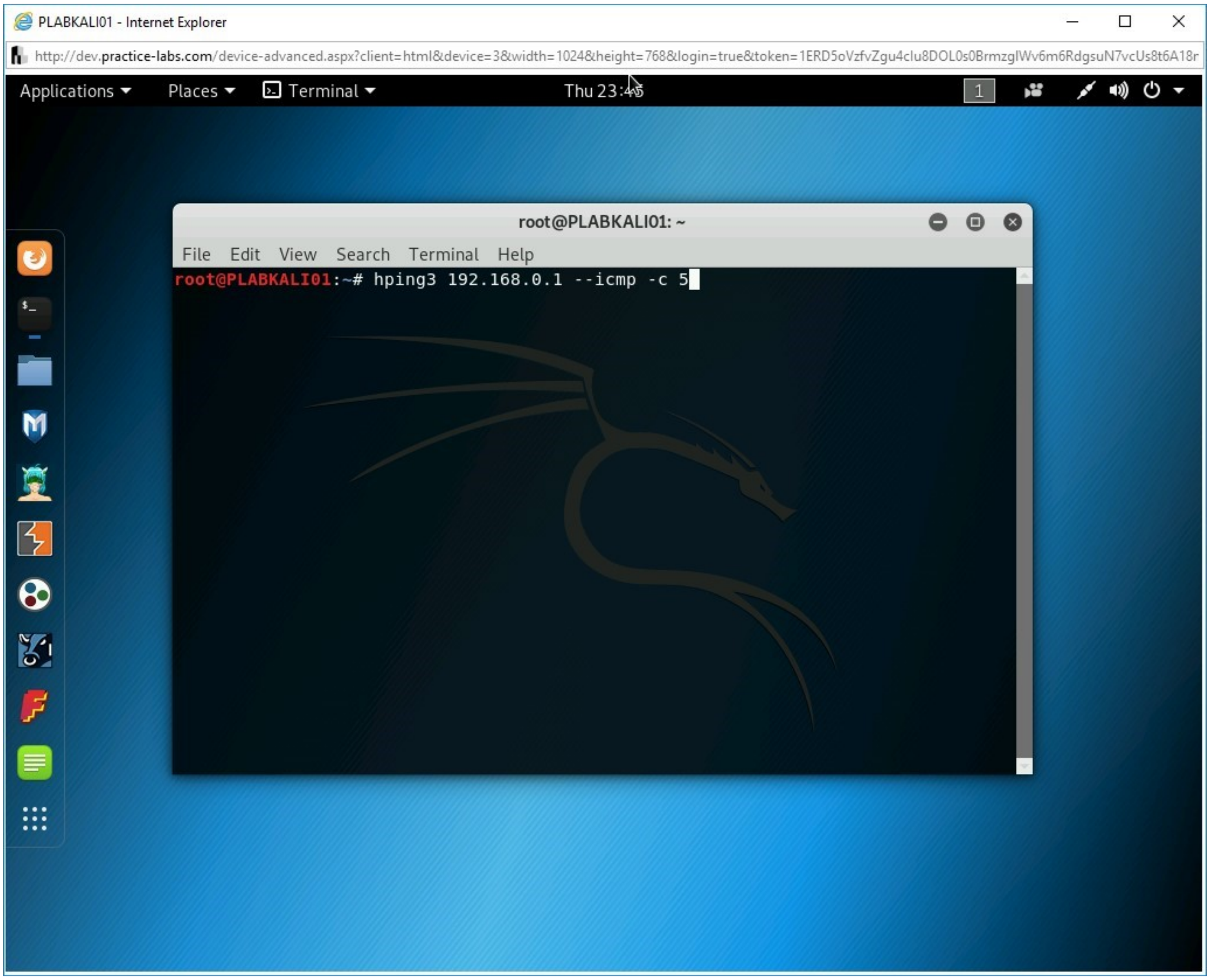
Clear the screen by entering the following command:

```
clear
```

You can also limit the command to perform ICMP discovery for a limited number. To do this, type the following command:

```
hping3 192.168.0.1 --icmp -c 5
```

Press **Enter**.



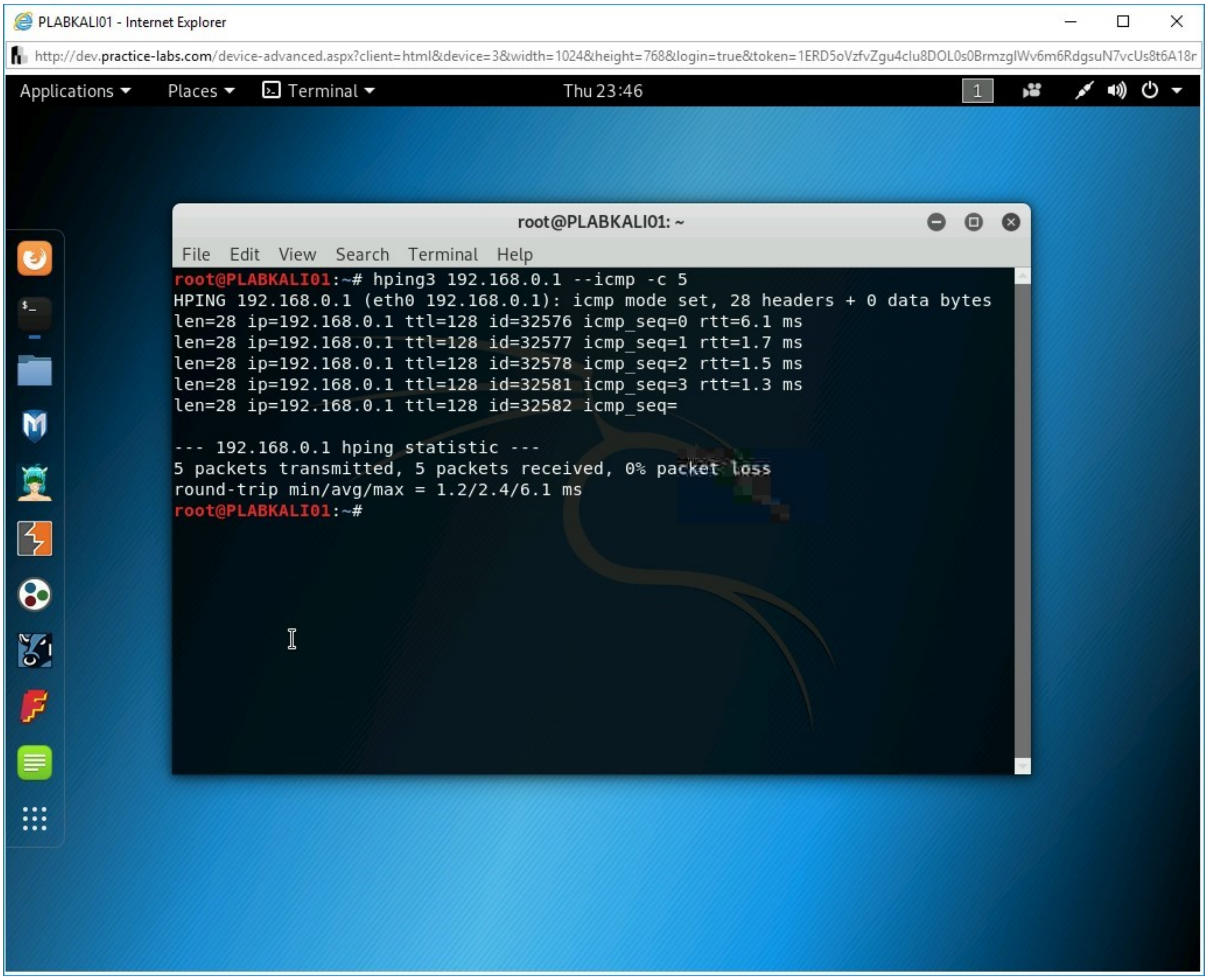
PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Terminal
Thu 23:45
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# hping3 192.168.0.1 --icmp -c 5
```

Figure 2.4 Screenshot of PLABKALI01: Entering the hping3 command to perform ICMP discovery for a limited number.

> ***Note**: The -S parameter sets the SYN flag.*

The output of the **hping3** command will be limited to five times.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Terminal
Thu 23:46
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# hping3 192.168.0.1 --icmp -c 5
HPING 192.168.0.1 (eth0 192.168.0.1): icmp mode set, 28 headers + 0 data bytes
len=28 ip=192.168.0.1 ttl=128 id=32576 icmp_seq=0 rtt=6.1 ms
len=28 ip=192.168.0.1 ttl=128 id=32577 icmp_seq=1 rtt=1.7 ms
len=28 ip=192.168.0.1 ttl=128 id=32578 icmp_seq=2 rtt=1.5 ms
len=28 ip=192.168.0.1 ttl=128 id=32581 icmp_seq=3 rtt=1.3 ms
len=28 ip=192.168.0.1 ttl=128 id=32582 icmp_seq=

--- 192.168.0.1 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.2/2.4/6.1 ms
root@PLABKALI01:~#
```

Figure 2.5 Screenshot of PLABKALI01: Showing the output of the hping3 command.

Step 5

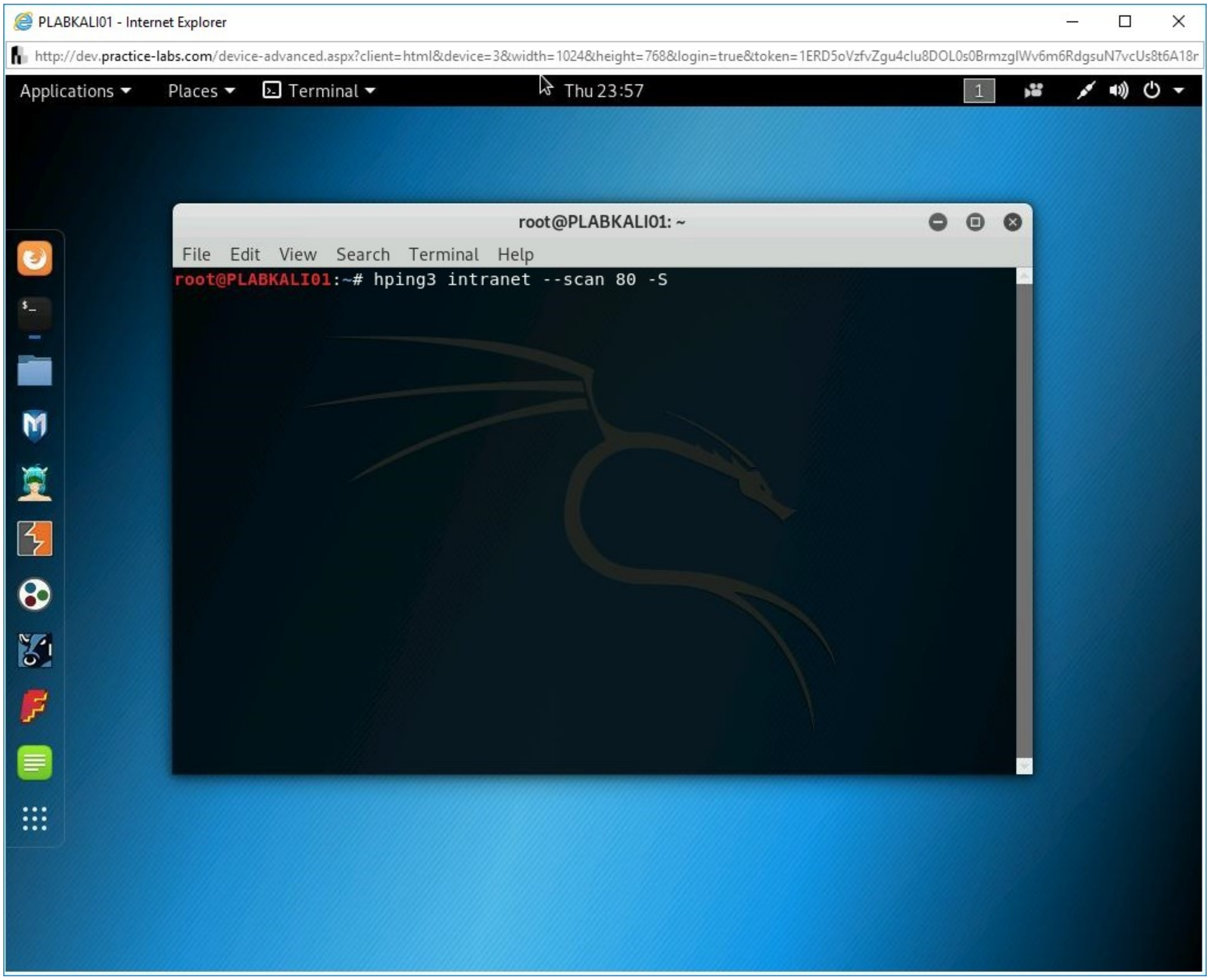
Clear the screen by entering the following command:

```
clear
```

You can also use the **hping3** command to scan for a specific TCP port. You need to specify the port number with the **- - scan** parameter. Type the following command:

```
hping3 intranet --scan 80 -S
```

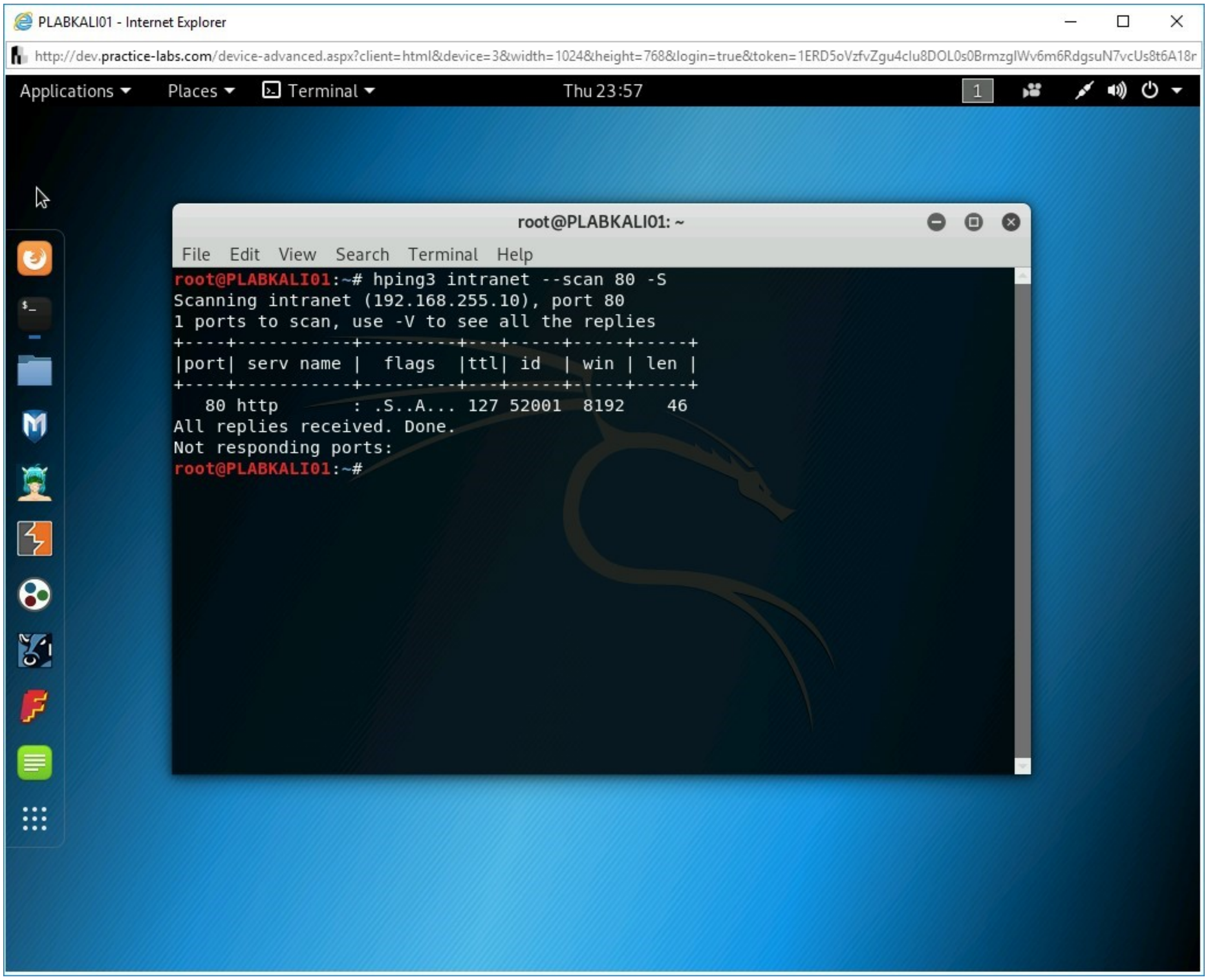
Press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Terminal
Thu 23:57
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# hping3 intranet --scan 80 -S
```

Figure 2.6 Screenshot of PLABKALI01: Entering the hping3 command to scan for a specific TCP port.

Notice that in the **flags** column, **S** and **A** are mentioned. This means that the **SYN+ACK** response was received from the target system.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Terminal
Thu 23:57
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# hping3 intranet --scan 80 -S
Scanning intranet (192.168.255.10), port 80
1 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   80 http       : .S..A... 127 52001  8192    46
All replies received. Done.
Not responding ports:
root@PLABKALI01:~#
```

Figure 2.7 Screenshot of PLABKALI01: Showing the output of the hping3 command.

SYN+ACK is part of the TCP 3-way handshake process between two systems, which has the following steps:

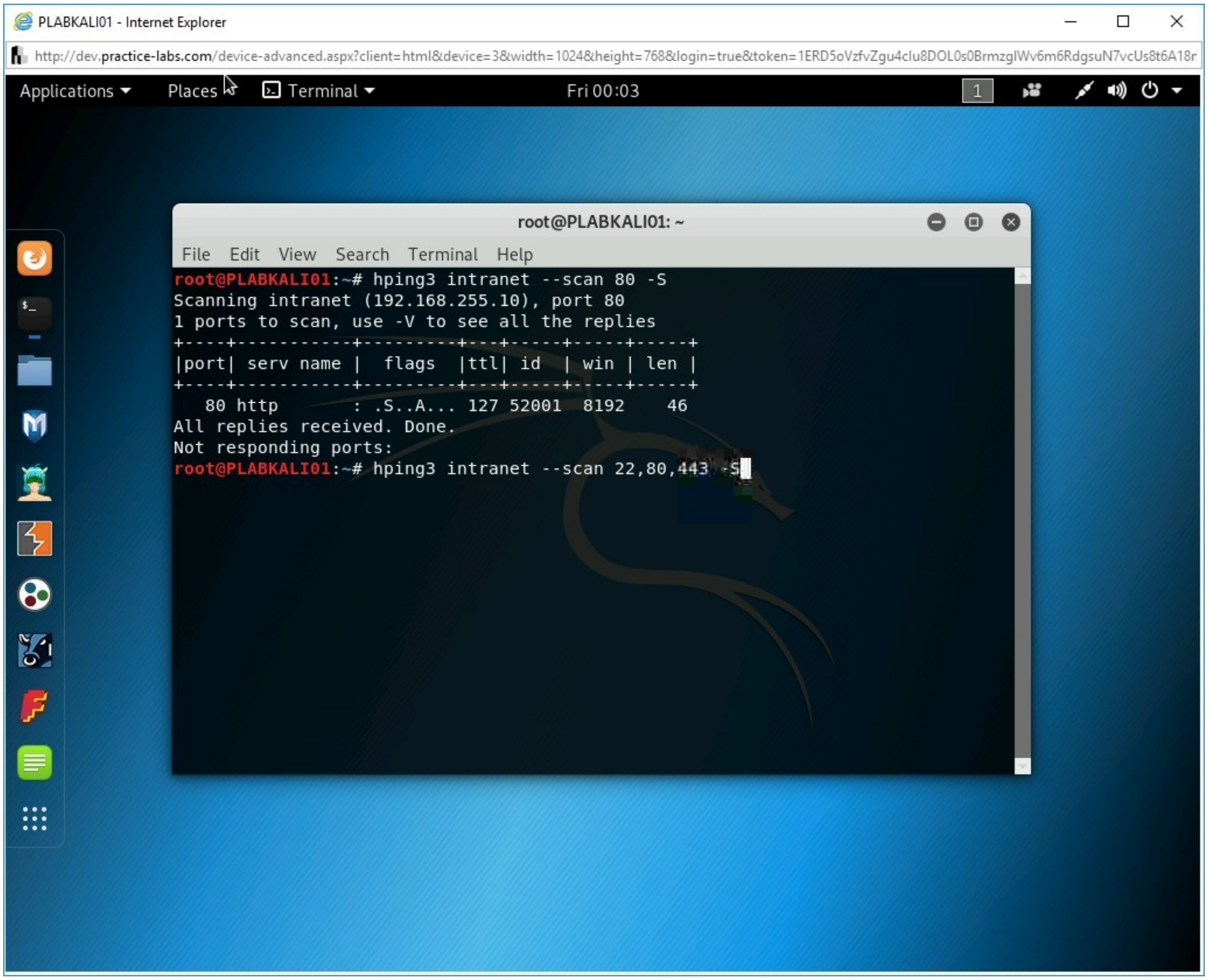
- Host1 sends a TCP SYN (synchronize) packet to Host2
- Host2 receives Host1's SYN (synchronize) packet
- Host2 sends a SYN (synchronize) -ACK (Acknowledgement).
- Host1 receives Host2's SYN+ACK
- Host1 sends ACK (Acknowledgement)
- Host2 receives ACK (Acknowledgement).

Step 6

You can also scan for multiple ports using the **hping3** command. To do this, type the following command:

```
hping3 intranet --scan 22,80,443 -S
```

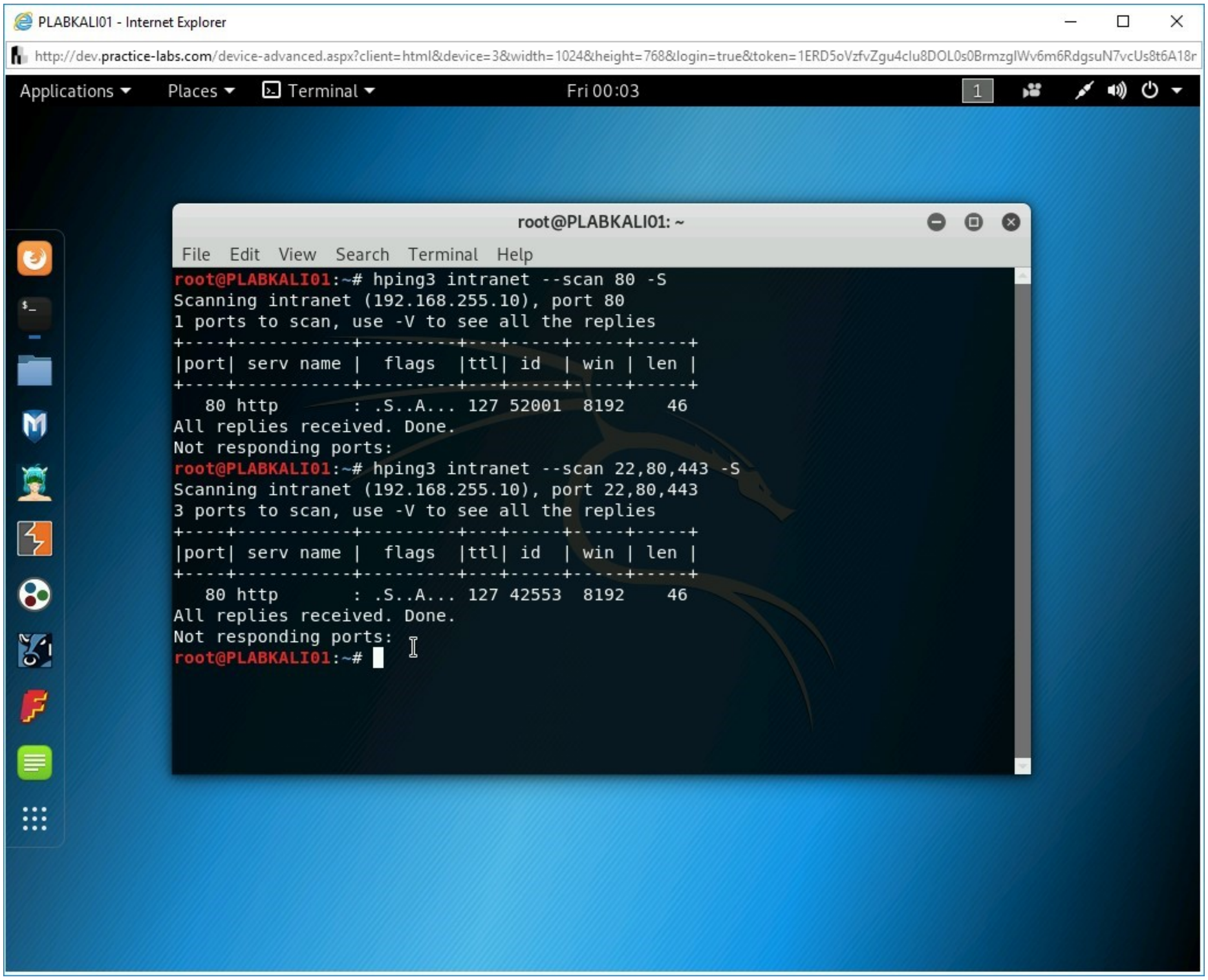
Press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Terminal
Fri 00:03
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# hping3 intranet --scan 80 -S
Scanning intranet (192.168.255.10), port 80
1 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   80 http       : .S..A... 127 52001  8192    46
All replies received. Done.
Not responding ports:
root@PLABKALI01:~# hping3 intranet --scan 22,80,443 -S
```

Figure 2.8 Screenshot of PLABKALI01: Entering the command to scan for multiple ports using the hping3 command.

Notice the output. Only port **80** has responded. The output only displays the ports if the **SYN+ACK** response is received.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Terminal
Fri 00:03
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# hping3 intranet --scan 80 -S
Scanning intranet (192.168.255.10), port 80
1 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   80 http       : .S..A... 127 52001  8192    46
All replies received. Done.
Not responding ports:
root@PLABKALI01:~# hping3 intranet --scan 22,80,443 -S
Scanning intranet (192.168.255.10), port 22,80,443
3 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   80 http       : .S..A... 127 42553  8192    46
All replies received. Done.
Not responding ports:
root@PLABKALI01:~#
```

Figure 2.9 Screenshot of PLABKALI01: Showing the output of the hping3 command.

Step 7

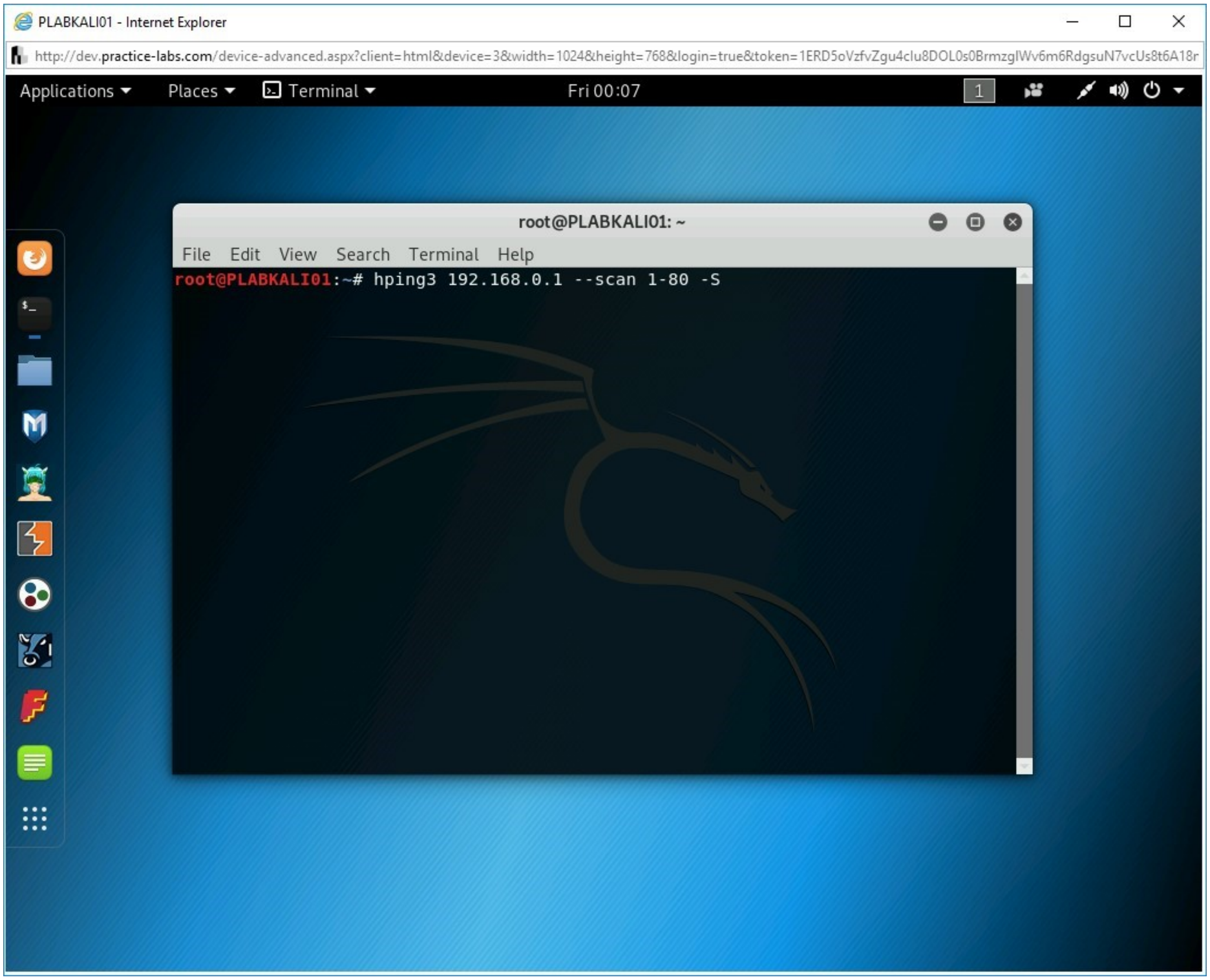
Clear the screen by entering the following command:

```
clear
```

You can also scan for a range of ports. To do this, you need to specify the first and the last port. Type the following command:

```
hping3 192.168.0.1 --scan 1-80 -S
```

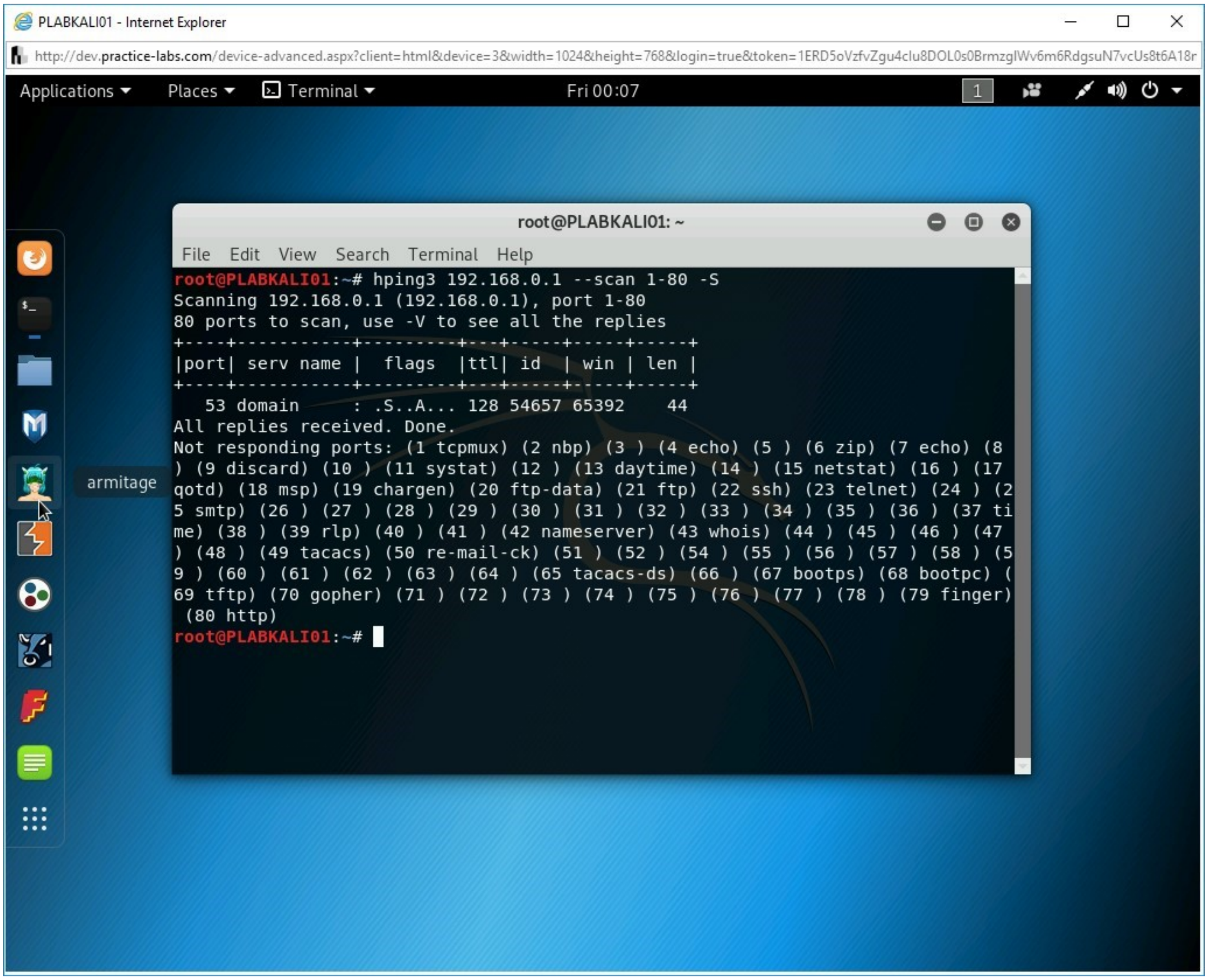
Press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Terminal
Fri 00:07
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# hping3 192.168.0.1 --scan 1-80 -S
```

Figure 2.10 Screenshot of PLABKALI01: Entering the hping3 command to scan for a range of ports.

Notice the output. Only port **53** is open.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Terminal
Fri 00:07
armitage
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# hping3 192.168.0.1 --scan 1-80 -S
Scanning 192.168.0.1 (192.168.0.1), port 1-80
80 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   53 domain     : .S..A... 128 54657 65392    44
All replies received. Done.
Not responding ports: (1 tcpmux) (2 nbp) (3 ) (4 echo) (5 ) (6 zip) (7 echo) (8
) (9 discard) (10 ) (11 systat) (12 ) (13 daytime) (14 ) (15 netstat) (16 ) (17
qotd) (18 msp) (19 chargen) (20 ftp-data) (21 ftp) (22 ssh) (23 telnet) (24 ) (2
5 smtp) (26 ) (27 ) (28 ) (29 ) (30 ) (31 ) (32 ) (33 ) (34 ) (35 ) (36 ) (37 ti
me) (38 ) (39 rlp) (40 ) (41 ) (42 nameserver) (43 whois) (44 ) (45 ) (46 ) (47
) (48 ) (49 tacacs) (50 re-mail-ck) (51 ) (52 ) (54 ) (55 ) (56 ) (57 ) (58 ) (5
9 ) (60 ) (61 ) (62 ) (63 ) (64 ) (65 tacacs-ds) (66 ) (67 bootps) (68 bootpc) (
69 tftp) (70 gopher) (71 ) (72 ) (73 ) (74 ) (75 ) (76 ) (77 ) (78 ) (79 finger)
 (80 http)
root@PLABKALI01:~#
```

Figure 2.11 Screenshot of PLABKALI01: Showing the output of the hping3 command.

Step 8

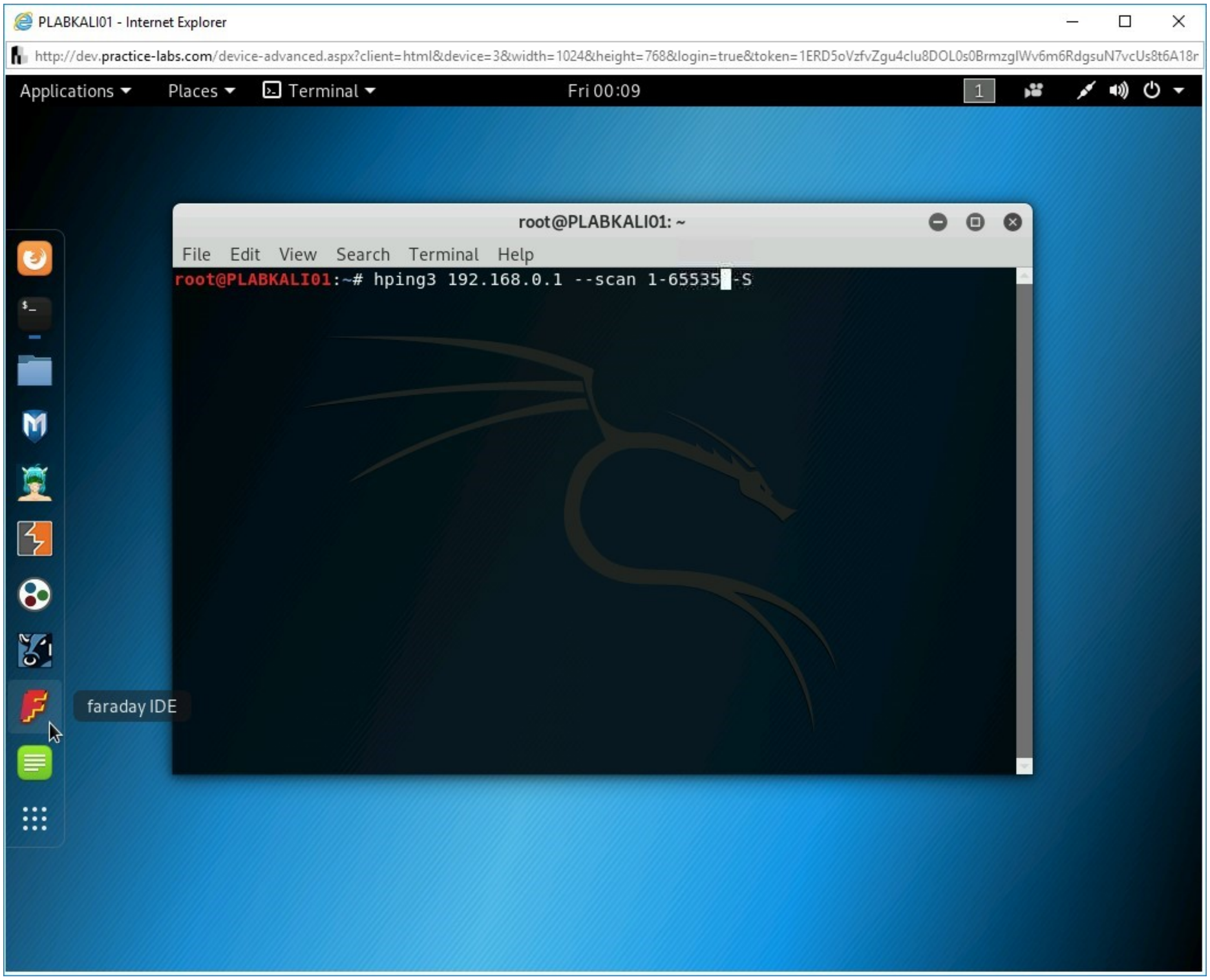
Clear the screen by entering the following command:

```
clear
```

To scan the entire TCP port range, type the following command:

```
hping3 192.168.0.1 --scan 1-65535 -S
```

Press **Enter**.

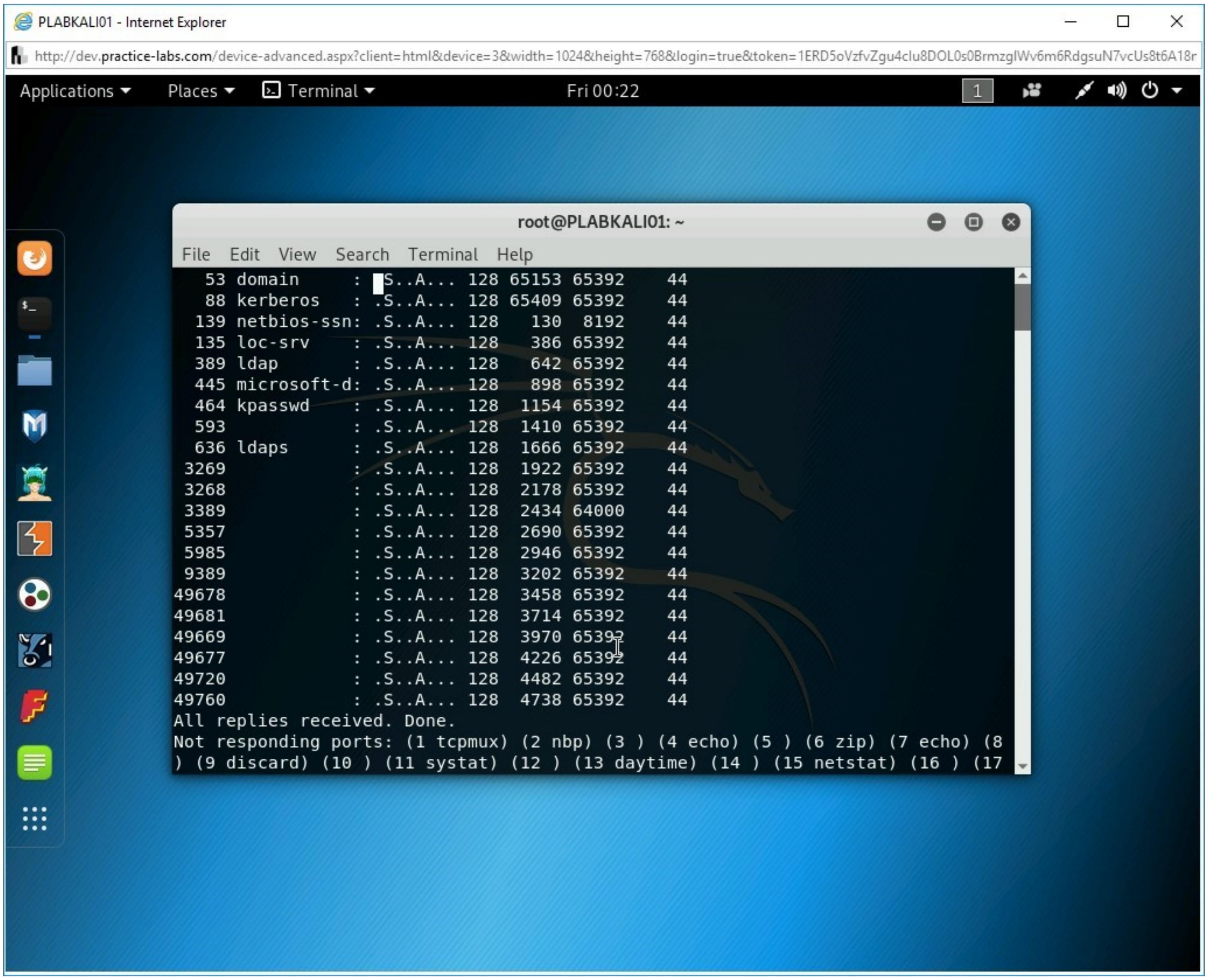


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Terminal
Fri 00:09
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help
faraday IDE

```
root@PLABKALI01:~# hping3 192.168.0.1 --scan 1-65535 -S
```

Figure 2.12 Screenshot of PLABKALI01: Entering the hping3 command to scan the entire TCP port range.

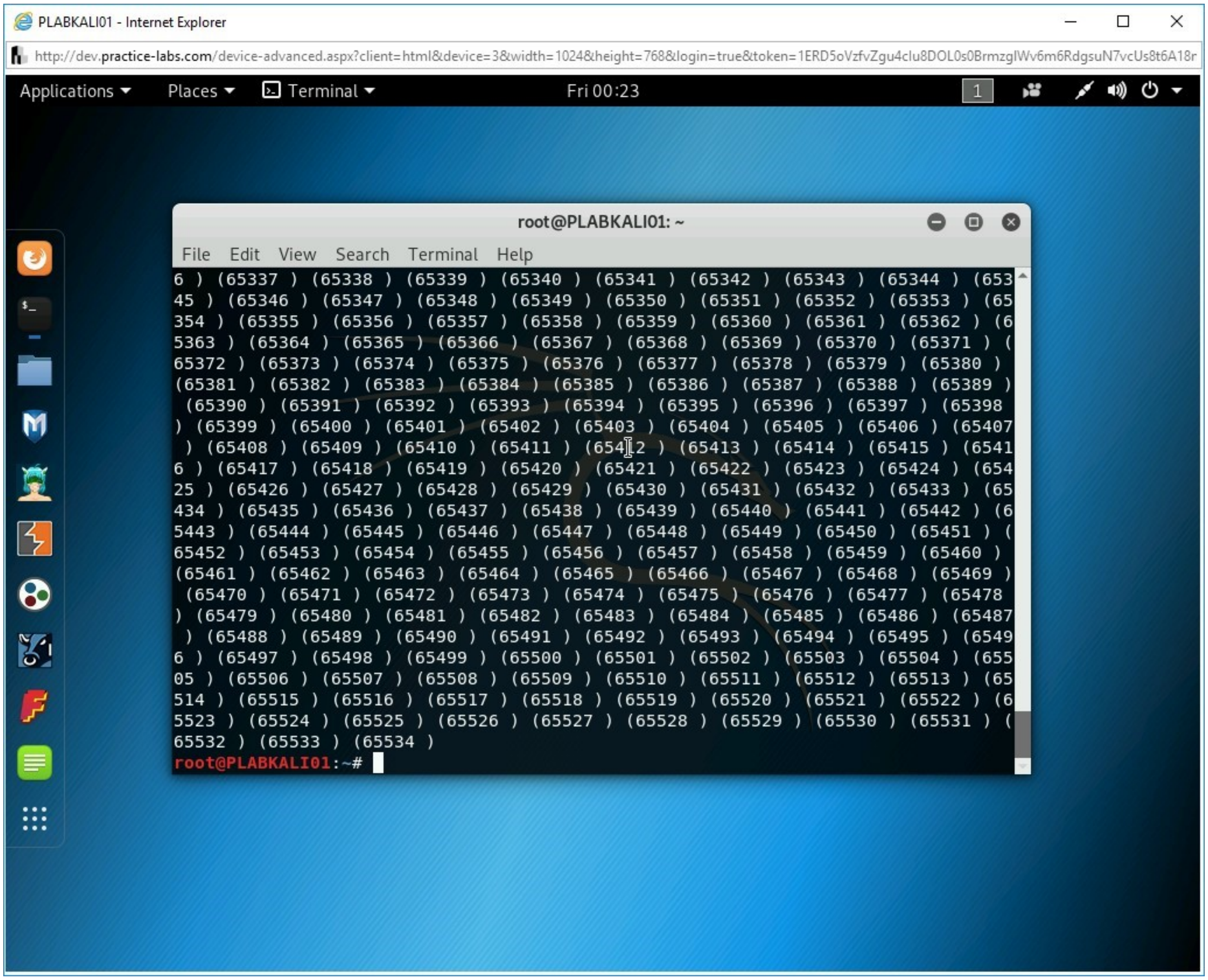
Scroll up to see the output mentioning open ports.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Terminal
Fri 00:22
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
   53 domain     : .S..A... 128 65153 65392    44
   88 kerberos   : .S..A... 128 65409 65392    44
  139 netbios-ssn: .S..A... 128   130  8192    44
  135 loc-srv    : .S..A... 128   386 65392    44
  389 ldap       : .S..A... 128   642 65392    44
  445 microsoft-d: .S..A... 128   898 65392    44
  464 kpasswd    : .S..A... 128  1154 65392    44
  593            : .S..A... 128  1410 65392    44
  636 ldaps      : .S..A... 128  1666 65392    44
 3269            : .S..A... 128  1922 65392    44
 3268            : .S..A... 128  2178 65392    44
 3389            : .S..A... 128  2434 64000    44
 5357            : .S..A... 128  2690 65392    44
 5985            : .S..A... 128  2946 65392    44
 9389            : .S..A... 128  3202 65392    44
49678            : .S..A... 128  3458 65392    44
49681            : .S..A... 128  3714 65392    44
49669            : .S..A... 128  3970 65392    44
49677            : .S..A... 128  4226 65392    44
49720            : .S..A... 128  4482 65392    44
49760            : .S..A... 128  4738 65392    44
All replies received. Done.
Not responding ports: (1 tcpmux) (2 nbp) (3 ) (4 echo) (5 ) (6 zip) (7 echo) (8
) (9 discard) (10 ) (11 systat) (12 ) (13 daytime) (14 ) (15 netstat) (16 ) (17
```

Figure 2.13 Screenshot of PLABKALI01: Showing the partial output of the hping3 command.

Scroll down to the command prompt. Notice that all closed ports are mentioned.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Terminal
Fri 00:23
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
6 ) (65337 ) (65338 ) (65339 ) (65340 ) (65341 ) (65342 ) (65343 ) (65344 ) (653
45 ) (65346 ) (65347 ) (65348 ) (65349 ) (65350 ) (65351 ) (65352 ) (65353 ) (65
354 ) (65355 ) (65356 ) (65357 ) (65358 ) (65359 ) (65360 ) (65361 ) (65362 ) (6
5363 ) (65364 ) (65365 ) (65366 ) (65367 ) (65368 ) (65369 ) (65370 ) (65371 ) (
65372 ) (65373 ) (65374 ) (65375 ) (65376 ) (65377 ) (65378 ) (65379 ) (65380 )
(65381 ) (65382 ) (65383 ) (65384 ) (65385 ) (65386 ) (65387 ) (65388 ) (65389 )
 (65390 ) (65391 ) (65392 ) (65393 ) (65394 ) (65395 ) (65396 ) (65397 ) (65398
) (65399 ) (65400 ) (65401 ) (65402 ) (65403 ) (65404 ) (65405 ) (65406 ) (65407
 ) (65408 ) (65409 ) (65410 ) (65411 ) (65412 ) (65413 ) (65414 ) (65415 ) (6541
6 ) (65417 ) (65418 ) (65419 ) (65420 ) (65421 ) (65422 ) (65423 ) (65424 ) (654
25 ) (65426 ) (65427 ) (65428 ) (65429 ) (65430 ) (65431 ) (65432 ) (65433 ) (65
434 ) (65435 ) (65436 ) (65437 ) (65438 ) (65439 ) (65440 ) (65441 ) (65442 ) (6
5443 ) (65444 ) (65445 ) (65446 ) (65447 ) (65448 ) (65449 ) (65450 ) (65451 ) (
65452 ) (65453 ) (65454 ) (65455 ) (65456 ) (65457 ) (65458 ) (65459 ) (65460 )
(65461 ) (65462 ) (65463 ) (65464 ) (65465 ) (65466 ) (65467 ) (65468 ) (65469 )
 (65470 ) (65471 ) (65472 ) (65473 ) (65474 ) (65475 ) (65476 ) (65477 ) (65478
) (65479 ) (65480 ) (65481 ) (65482 ) (65483 ) (65484 ) (65485 ) (65486 ) (65487
 ) (65488 ) (65489 ) (65490 ) (65491 ) (65492 ) (65493 ) (65494 ) (65495 ) (6549
6 ) (65497 ) (65498 ) (65499 ) (65500 ) (65501 ) (65502 ) (65503 ) (65504 ) (655
05 ) (65506 ) (65507 ) (65508 ) (65509 ) (65510 ) (65511 ) (65512 ) (65513 ) (65
514 ) (65515 ) (65516 ) (65517 ) (65518 ) (65519 ) (65520 ) (65521 ) (65522 ) (6
5523 ) (65524 ) (65525 ) (65526 ) (65527 ) (65528 ) (65529 ) (65530 ) (65531 ) (
65532 ) (65533 ) (65534 )
root@PLABKALI01:~#
```

Figure 2.14 Screenshot of PLABKALI01: Showing the output of the hping3 command.

Step 9

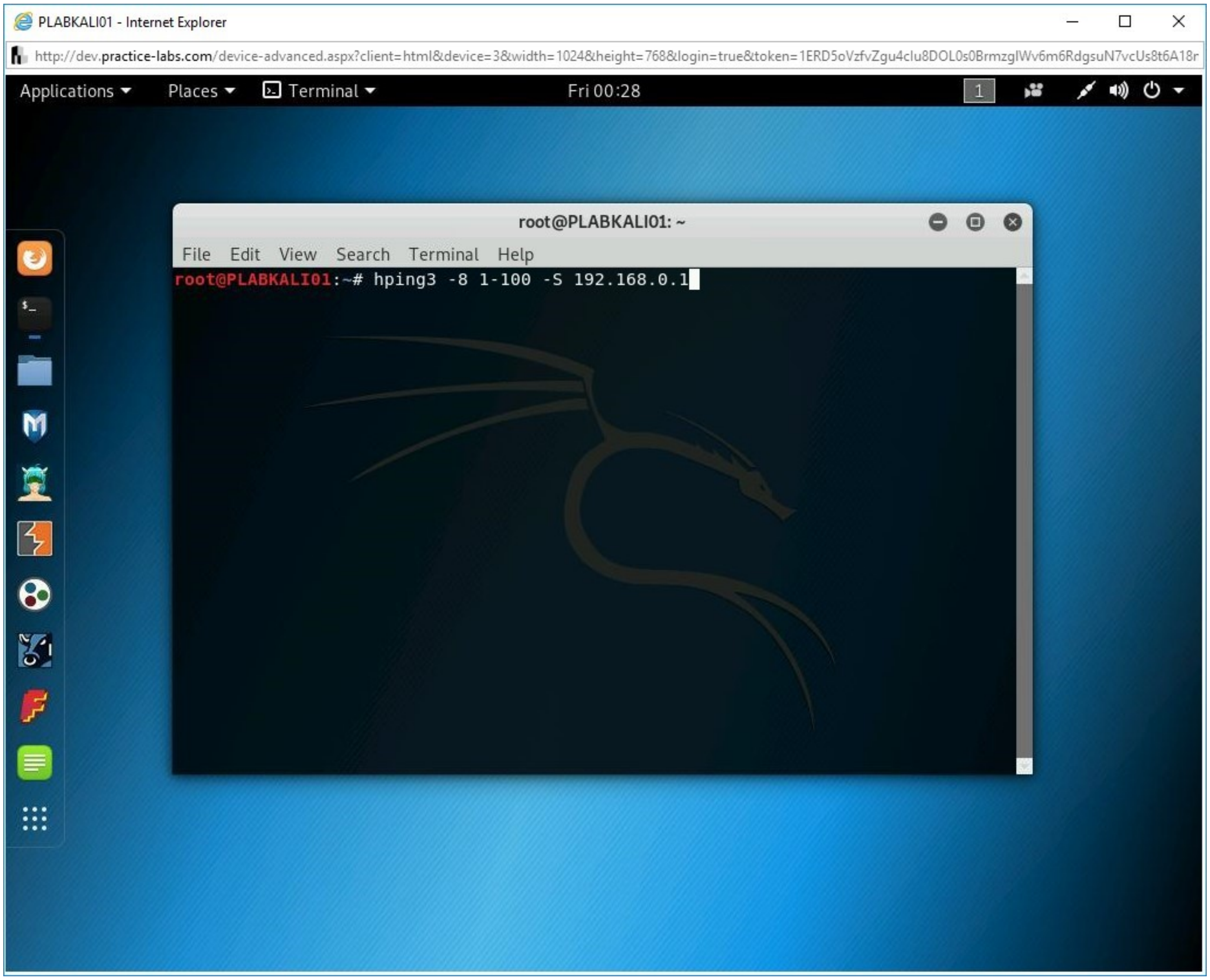
Clear the screen by entering the following command:

```
clear
```

You can use **hping3** to determine open ports on a target. To identify open ports on **192.168.0.1**, type the following command:

```
hping3 -8 0-100 -S 192.168.0.1
```

Press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Terminal
Fri 00:28
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# hping3 -8 1-100 -S 192.168.0.1
```

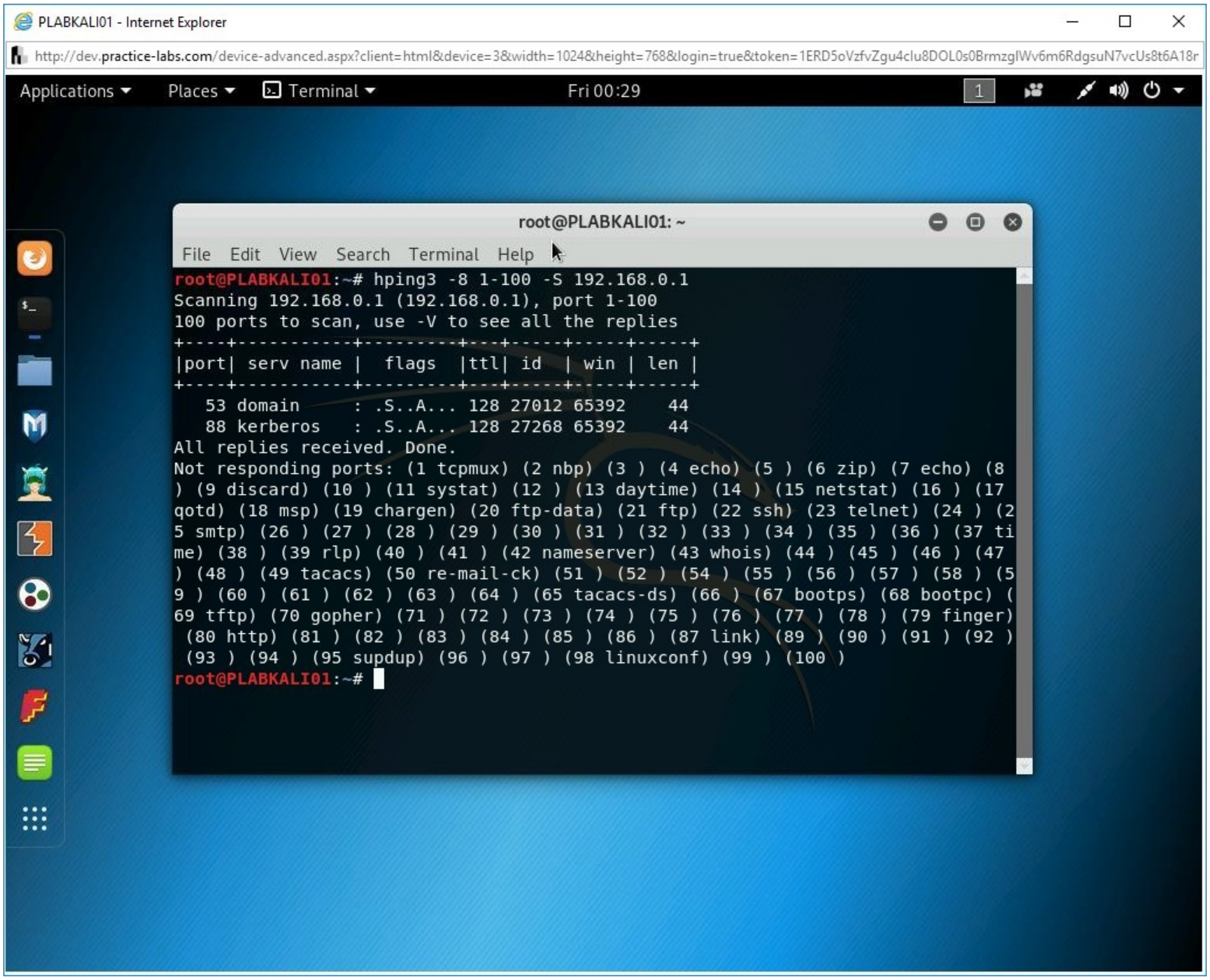
Figure 2.15 Screenshot of PLABKALI01: Entering the hping3 command to determine open ports on a target.

The given command specifies the following switches:

- -8 = Enable SCAN mode.
- 0-100 = Range of ports to scan.
- -S = set SYN flag.

The output displays the list of open ports and the services that use them. The output also displays the list of ports that do not respond to the scan.

Note: *Notice the given command sent the SYN flag and received the SYN ACK flag from each open port on PLABDC01.*


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=1ERD5oVzfvZgu4clu8DOL0s0BrmzglWv6m6RdgsuN7vcUs8t6A18r
Applications
Places
Terminal
Fri 00:29
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# hping3 -8 1-100 -S 192.168.0.1
Scanning 192.168.0.1 (192.168.0.1), port 1-100
100 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   53 domain     : .S..A... 128 27012 65392    44
   88 kerberos   : .S..A... 128 27268 65392    44
All replies received. Done.
Not responding ports: (1 tcpmux) (2 nbp) (3 ) (4 echo) (5 ) (6 zip) (7 echo) (8
) (9 discard) (10 ) (11 systat) (12 ) (13 daytime) (14 ) (15 netstat) (16 ) (17
qotd) (18 msp) (19 chargen) (20 ftp-data) (21 ftp) (22 ssh) (23 telnet) (24 ) (2
5 smtp) (26 ) (27 ) (28 ) (29 ) (30 ) (31 ) (32 ) (33 ) (34 ) (35 ) (36 ) (37 ti
me) (38 ) (39 rlp) (40 ) (41 ) (42 nameserver) (43 whois) (44 ) (45 ) (46 ) (47
) (48 ) (49 tacacs) (50 re-mail-ck) (51 ) (52 ) (54 ) (55 ) (56 ) (57 ) (58 ) (5
9 ) (60 ) (61 ) (62 ) (63 ) (64 ) (65 tacacs-ds) (66 ) (67 bootps) (68 bootpc) (
69 tftp) (70 gopher) (71 ) (72 ) (73 ) (74 ) (75 ) (76 ) (77 ) (78 ) (79 finger)
 (80 http) (81 ) (82 ) (83 ) (84 ) (85 ) (86 ) (87 link) (89 ) (90 ) (91 ) (92 )
 (93 ) (94 ) (95 supdup) (96 ) (97 ) (98 linuxconf) (99 ) (100 )
root@PLABKALI01:~#
```

Figure 2.16 Screenshot of PLABKALI01: Showing the output of the hping3 command with the output of the list of open ports and the services that use them.

Keep the terminal window open.

Task 2 - Perform a TCP Scan Using Dmitry

Dmitry is an information gathering tool. It has the capability to gather the following types of information:

- Subdomains

- E-mail addresses
- Uptime information
- TCP port scan
- WHOis lookups

In this task, you will use Dmitry to perform a TCP scan. To do this, perform the following steps:

Step 1

Ensure you have powered on the required devices and connect to **PLABKALI01**.

If you are continuing from the previous task, the terminal window should be open. If not, then open a new terminal window.

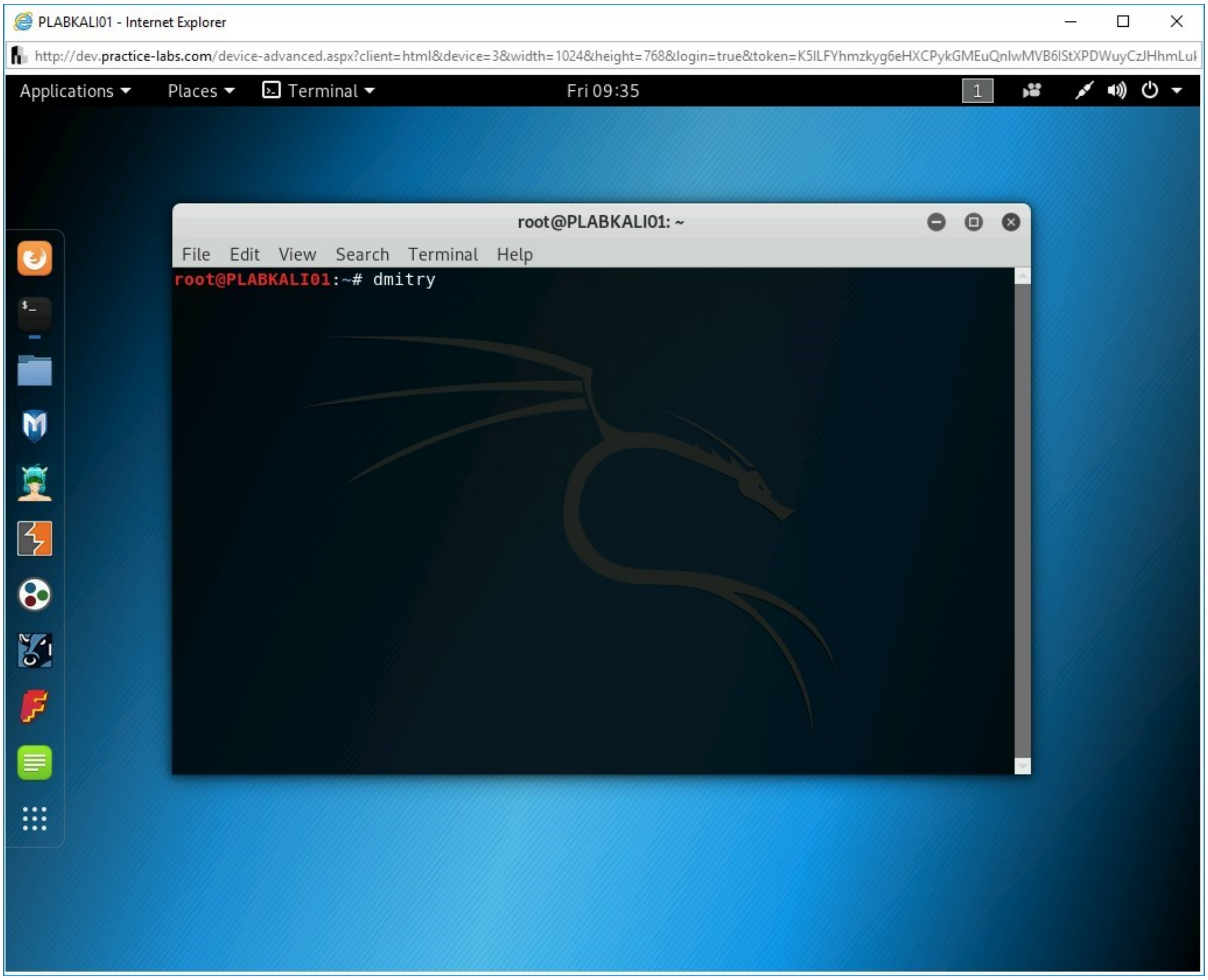
If continuing from the previous task, then clear the screen by entering the following command:

```
clear
```

To view the parameters of the dmitry command, type the following:

```
dmitry
```

Press **Enter**.

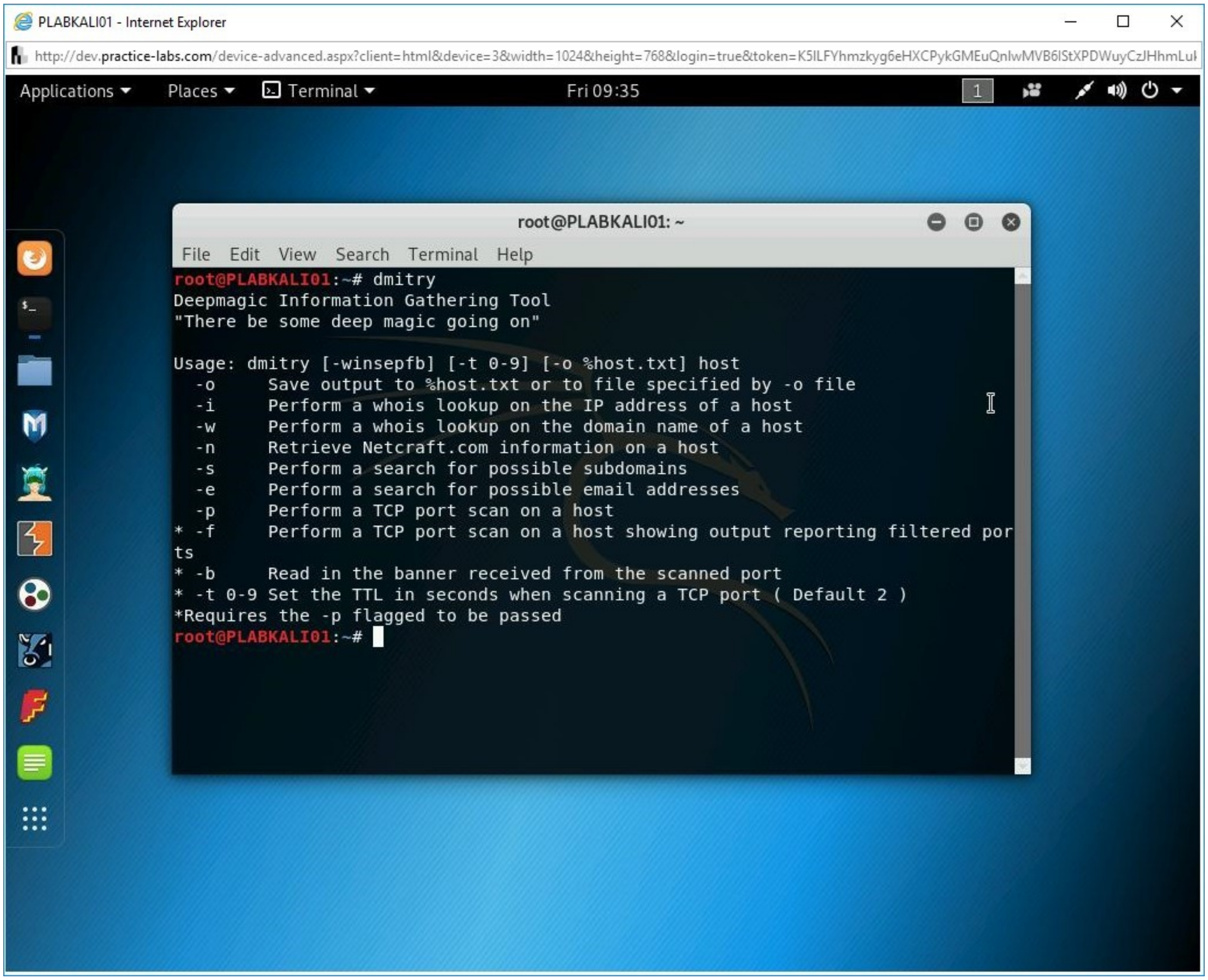


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=K5ILFYhmzkyg6eHXCPykGMEuQnlwMVB6lStXPDWuyCzJHhmLuk
Applications
Places
Terminal
Fri 09:35
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# dmitry
```

Figure 2.17 Screenshot of PLABKALI01: Entering the dmitry command.

The output displays the list of parameters.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=K5ILFYhmzkyg6eHXCPykGMEuQnlwMVB6lStXPDWuyCzJHhmLuł
Applications
Places
Terminal
Fri 09:35
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# dmitry
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o     Save output to %host.txt or to file specified by -o file
  -i     Perform a whois lookup on the IP address of a host
  -w     Perform a whois lookup on the domain name of a host
  -n     Retrieve Netcraft.com information on a host
  -s     Perform a search for possible subdomains
  -e     Perform a search for possible email addresses
  -p     Perform a TCP port scan on a host
* -f     Perform a TCP port scan on a host showing output reporting filtered por
ts
* -b     Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
root@PLABKALI01:~#
```

Figure 2.18 Screenshot of PLABKALI01: Showing the output of the dmitry command with various parameters.

Step 2

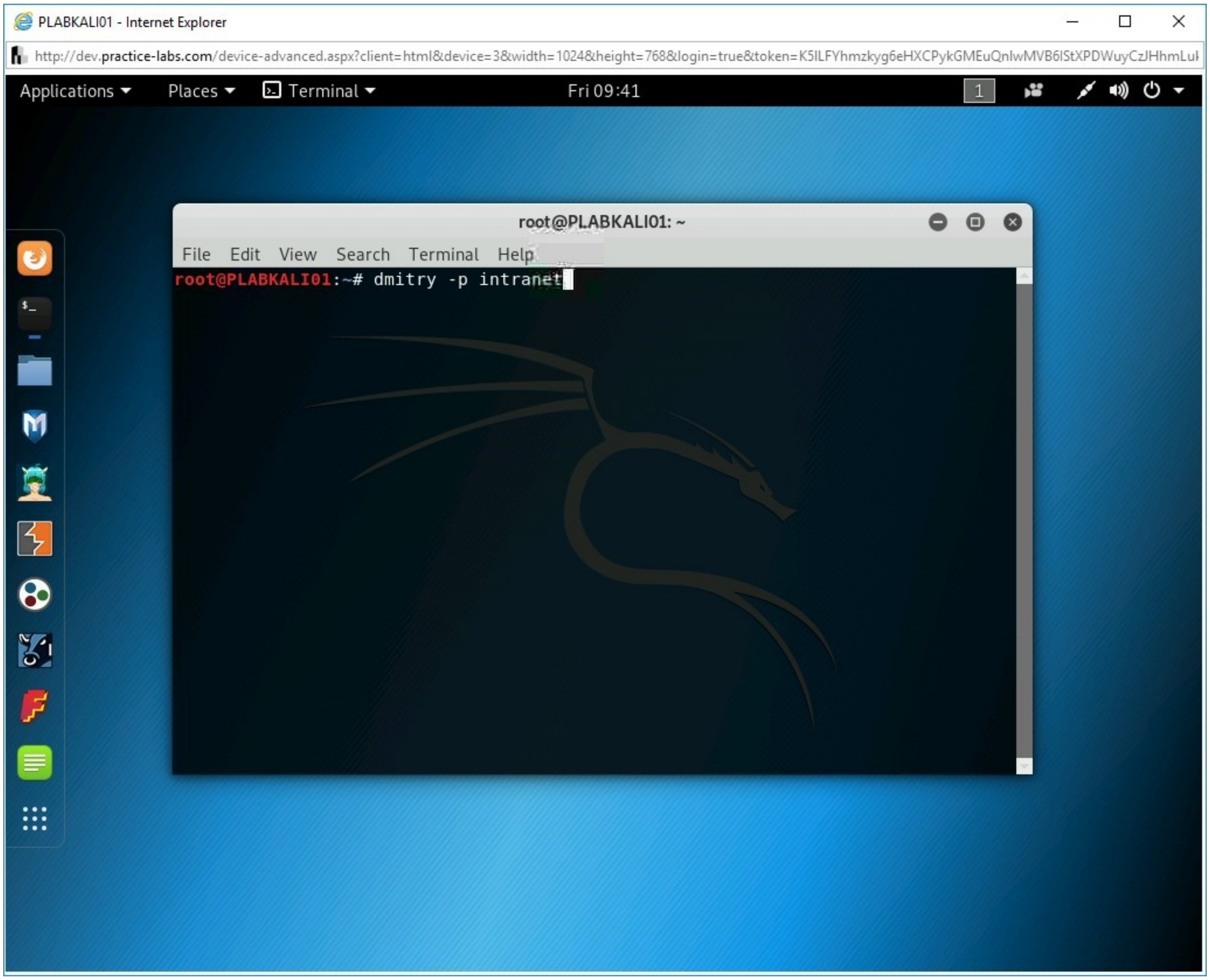
Clear the screen by entering the following command:

```
clear
```

You will now use the **-p** parameter along with the **dmitry** command to perform a **TCP scan**. Type the following command:

```
dmitry -p intranet
```

Press **Enter**.

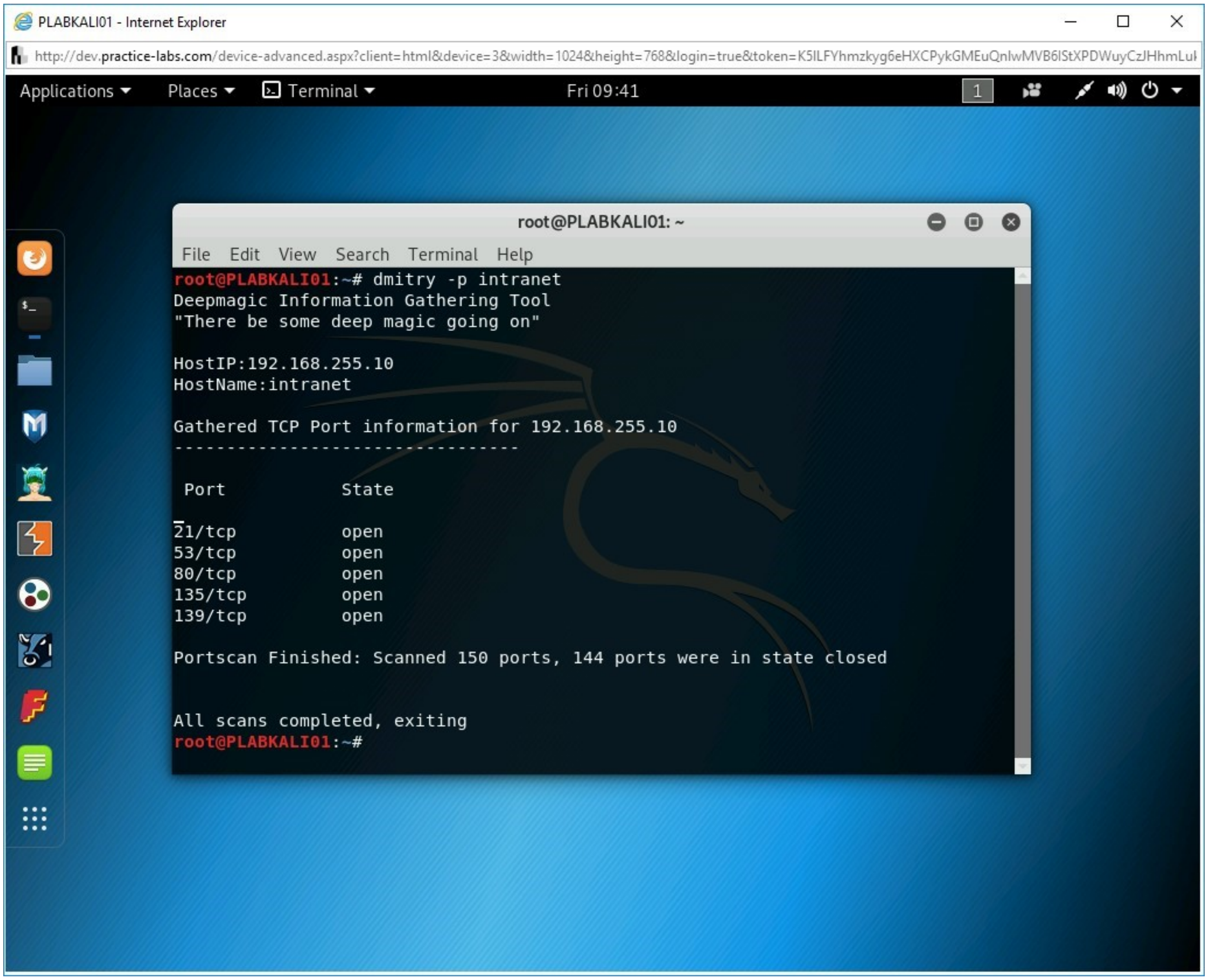


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=K5ILFYhmzkyg6eHXCPykGMEuQnlwMVB6IStXPDWuyCzJHhmLuk
Applications
Places
Terminal
Fri 09:41
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# dmitry -p intranet
```

Figure 2.19 Screenshot of PLABKALI01: Entering the dmitry command to perform a TCP scan.

The output displays the list of open ports. It also shows the target's IP address.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=K5ILFYhmzkyg6eHXCPykGMEuQnlwMVB6lStXPDWuyCzJHhmLul
Applications
Places
Terminal
Fri 09:41
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# dmitry -p intranet
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:192.168.255.10
HostName:intranet

Gathered TCP Port information for 192.168.255.10
---------------------------------

 Port           State

21/tcp          open
53/tcp          open
80/tcp          open
135/tcp         open
139/tcp         open

Portscan Finished: Scanned 150 ports, 144 ports were in state closed


All scans completed, exiting
root@PLABKALI01:~#
```

Figure 2.20 Screenshot of PLABKALI01: Showing the output of the dmitry command.

Step 3

Clear the screen by entering the following command:

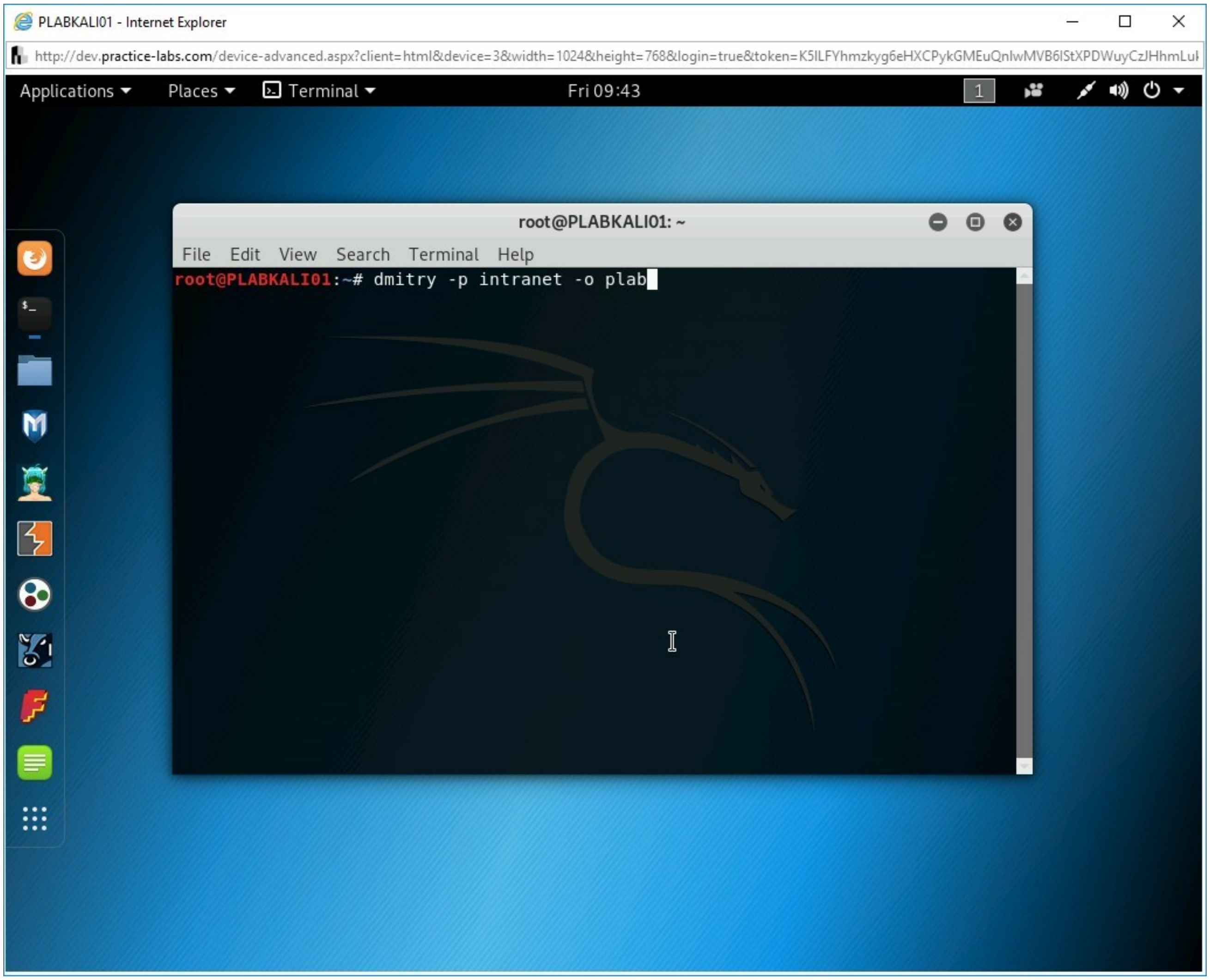
```
clear
```

You can also send the **dmitry** output to a text file. In this step, you will send the output to a text file named **plab**.

To do this, type the following command:

```
dmitry -p intranet -o plab
```

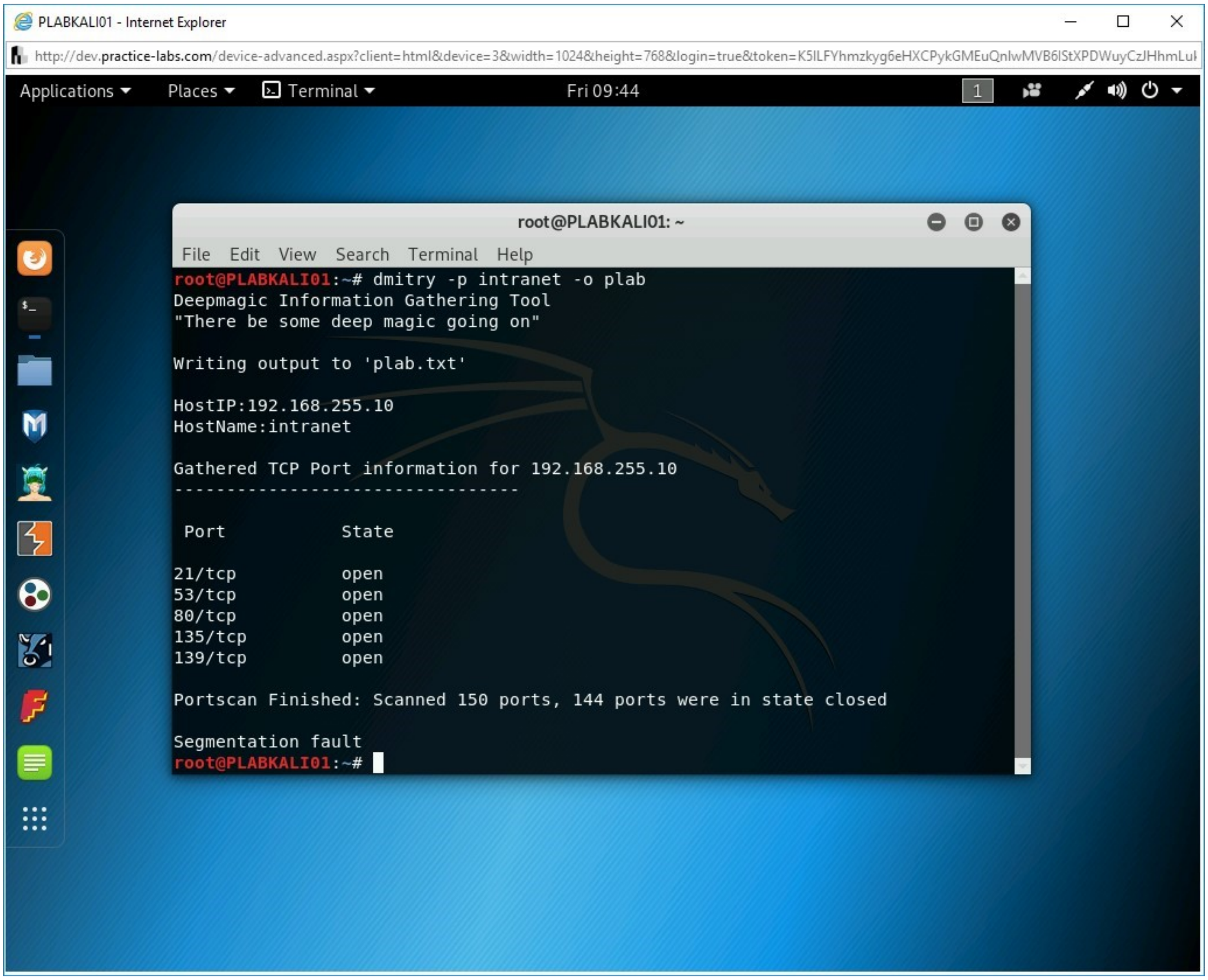
Press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=K5ILFYhmzkyg6eHXCPykGMEuQnlwMVB6IStXPDWuyCzJHhmLuł
Applications
Places
Terminal
Fri 09:43
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# dmitry -p intranet -o plab
```

Figure 2.21 Screenshot of PLABKALI01: Entering the dmitry command to send the output to a text file.

Notice that the output mentions writing output to **plab.txt**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=K5ILFYhmzkyg6eHXCPykGMEuQnlwMVB6lStXPDWuyCzJHhmLuk
Applications
Places
Terminal
Fri 09:44
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# dmitry -p intranet -o plab
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Writing output to 'plab.txt'

HostIP:192.168.255.10
HostName:intranet

Gathered TCP Port information for 192.168.255.10
---------------------------------

 Port           State

21/tcp          open
53/tcp          open
80/tcp          open
135/tcp         open
139/tcp         open

Portscan Finished: Scanned 150 ports, 144 ports were in state closed

Segmentation fault
root@PLABKALI01:~#
```

Figure 2.22 Screenshot of PLABKALI01: Showing the output of the dmitry command with the generated output file.

Step 4

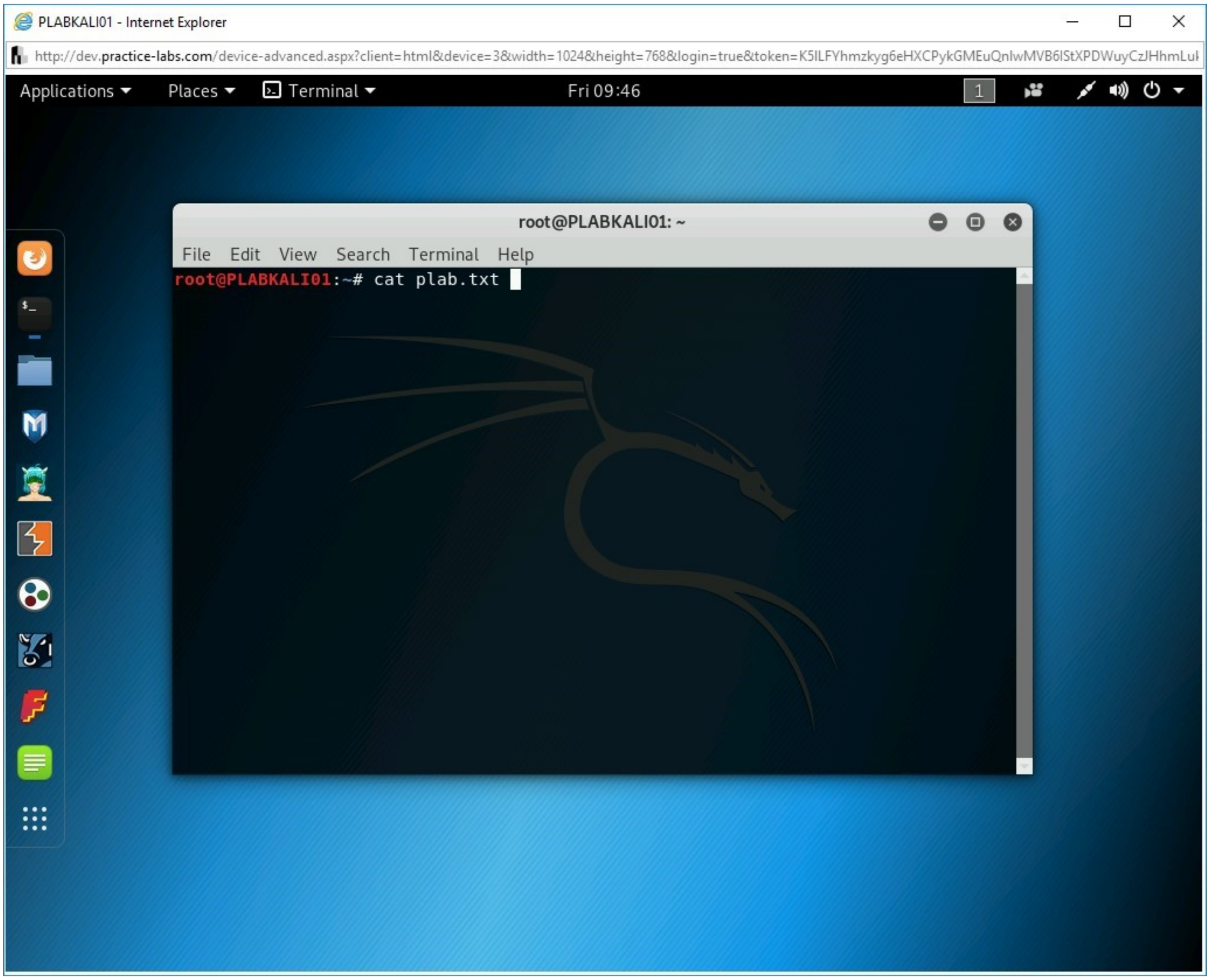
Clear the screen by entering the following command:

```
clear
```

To view the **plab.txt** file type the following command:

```
cat plab.txt
```

Press **Enter**.



PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=K5ILFYhmzkyg6eHXCPykGMEuQnlwMVB6lStXPDWuyCzJHhmLuł
Applications
Places
Terminal
Fri 09:46
root@PLABKALI01: ~
File Edit View Search Terminal Help

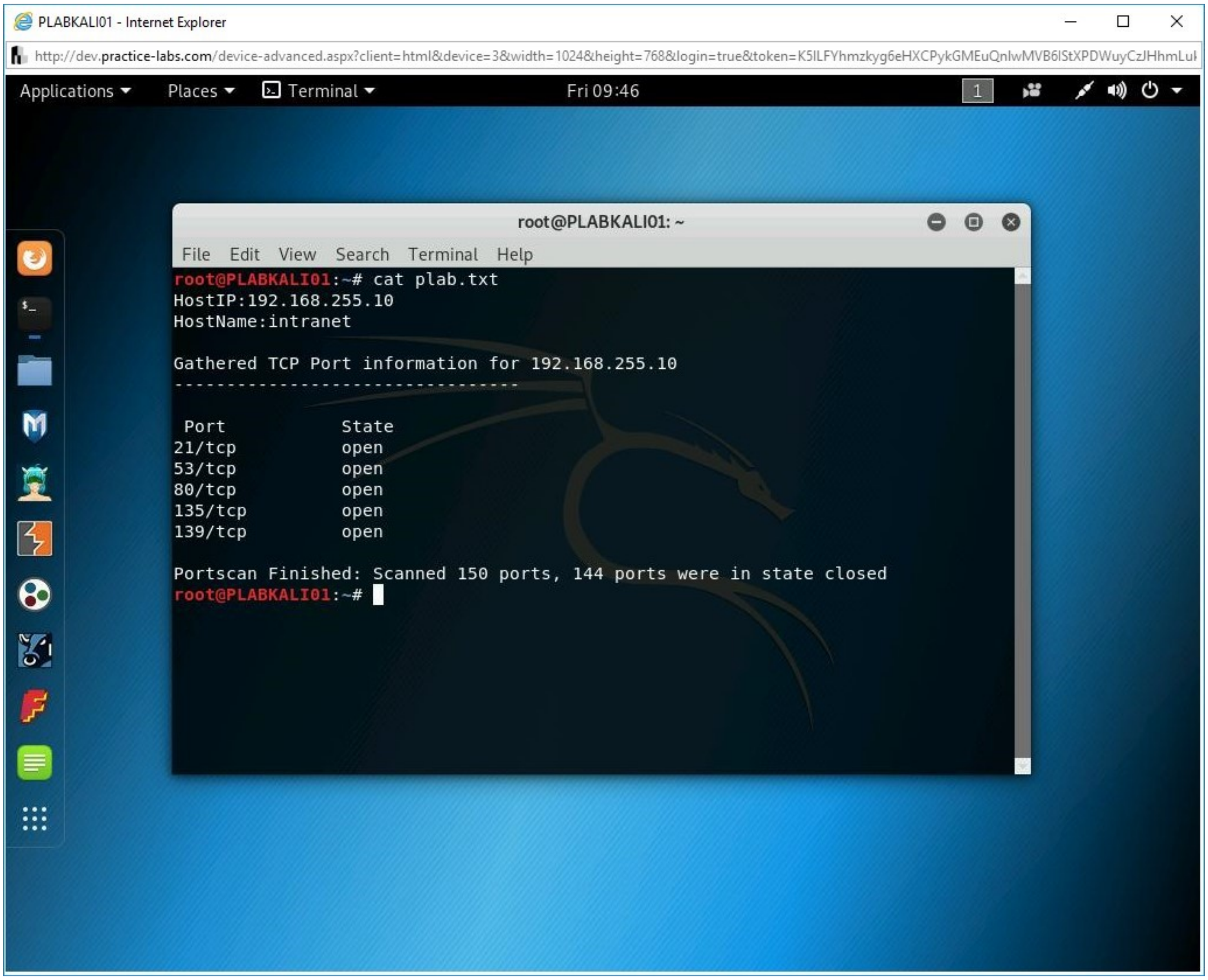
```
root@PLABKALI01:~# cat plab.txt
```

Figure 2.23 Screenshot of PLABKALI01: Entering the cat command to view the plab.txt file.

Notice that the output is the same as the output for the following command:

```
dmitry -p intranet
```

The plab.txt file contains the same output as the above-mentioned command.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=K5ILFYhmzkyg6eHXCPykGMEuQnlwMVB6lStXPDWuyCzJHhmLul
Applications
Places
Terminal
Fri 09:46
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# cat plab.txt
HostIP:192.168.255.10
HostName:intranet

Gathered TCP Port information for 192.168.255.10
--------------------------------

 Port           State
21/tcp          open
53/tcp          open
80/tcp          open
135/tcp         open
139/tcp         open

Portscan Finished: Scanned 150 ports, 144 ports were in state closed
root@PLABKALI01:~#
```

Figure 2.24 Screenshot of PLABKALI01: Showing the contents of the plab.txt file.

Keep the terminal window open.

Task 3 - Use Netcat for Port Scan

Netcat, or nc, is a tool that is used for monitoring network connections and can also be used for port scanning.

In this task, you will use nc for port scanning. To do this, perform the following steps:

Step 1

Ensure you have powered on the required devices and connect to **PLABKALI01**.

If you are continuing from the previous task, the terminal window should be open. If not, then open a new terminal window.

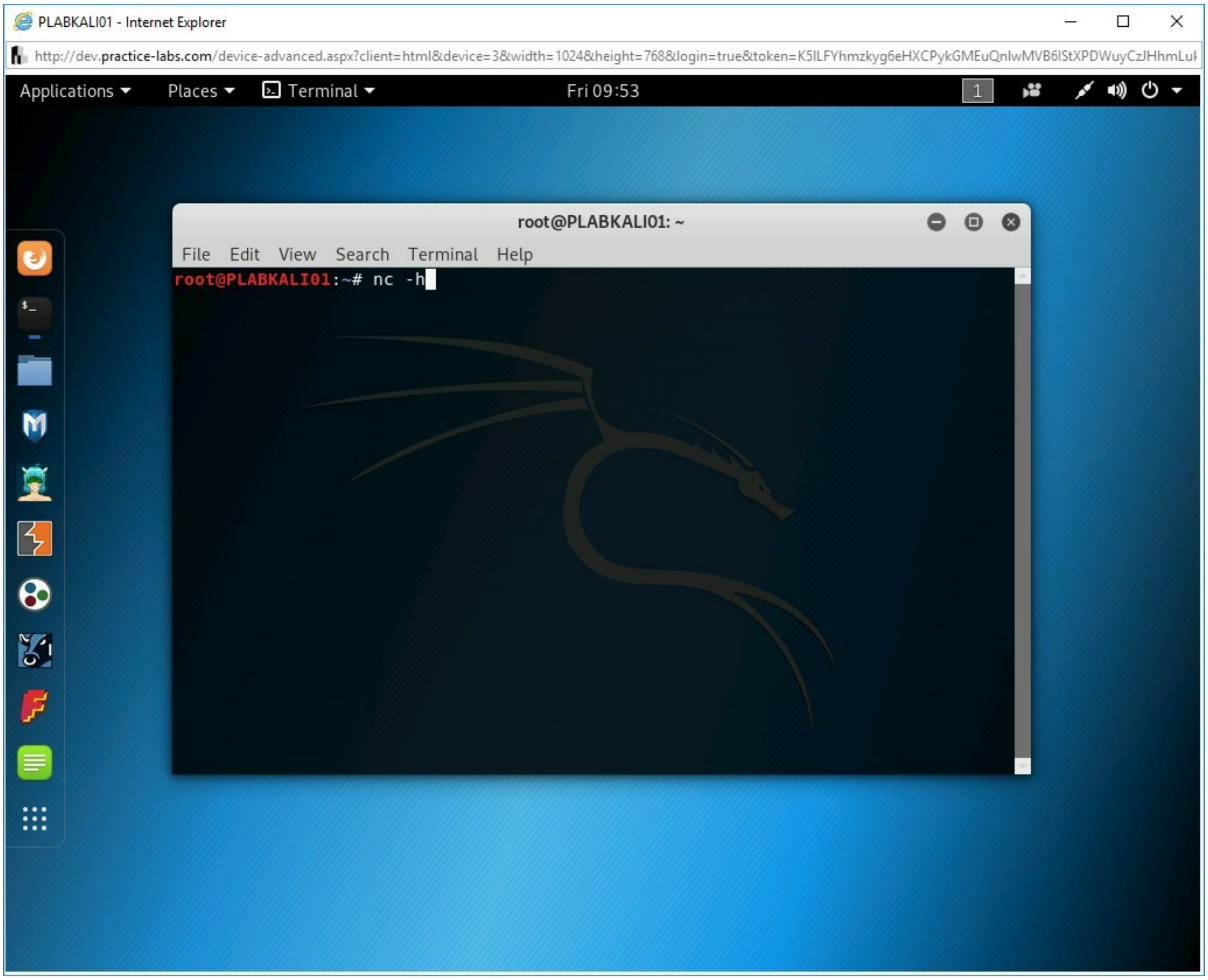
If continuing from the previous task, then clear the screen by entering the following command:

```
clear
```

To view the list of parameters of **nc** command, type the following:

```
nc -h
```

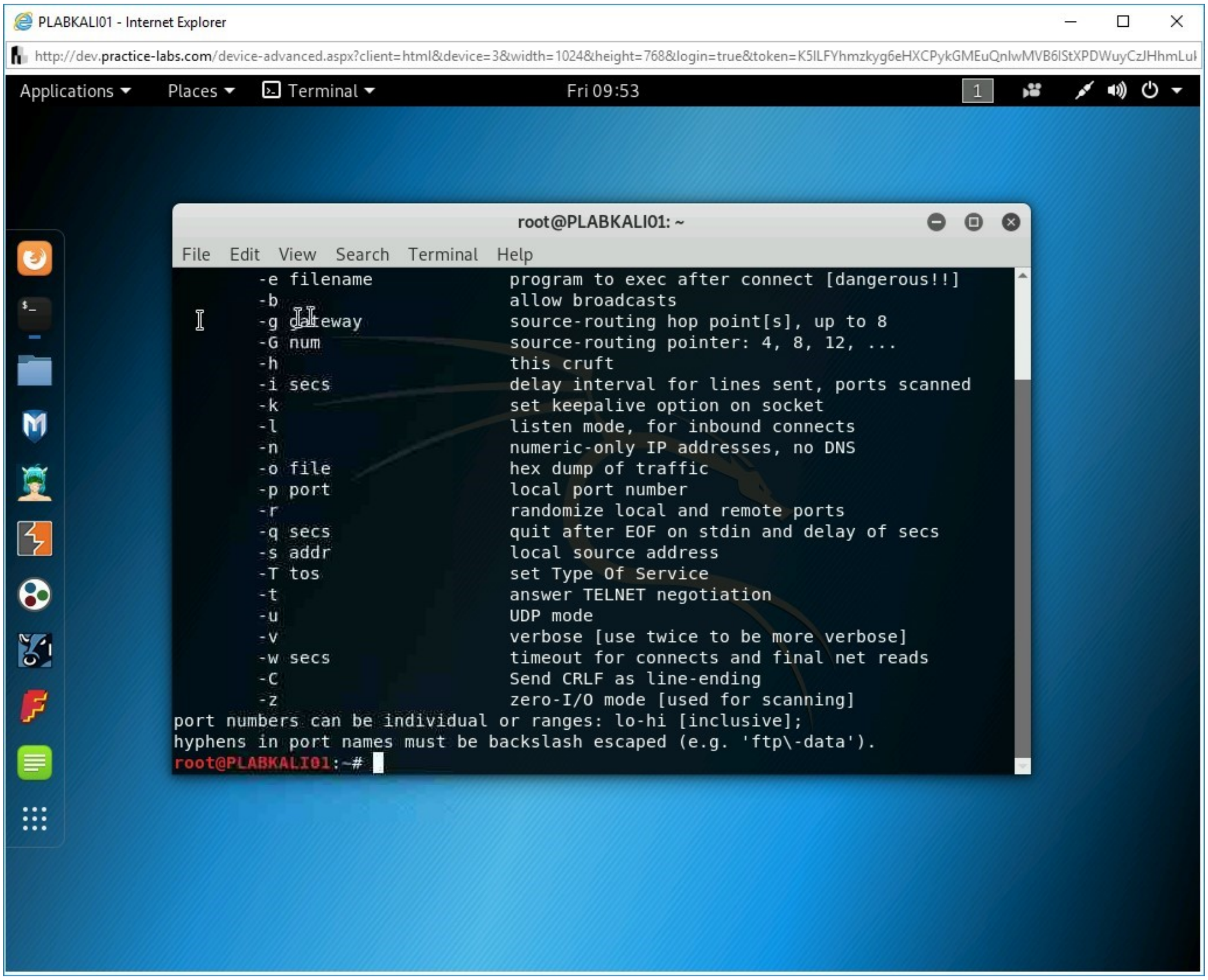
Press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=K5ILFYhmzkyg6eHXCPykGMEuQnlwMVB6lStXPDWuyCzJHhmLul
Applications
Places
Terminal
Fri 09:53
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# nc -h
```

Figure 2.25 Screenshot of PLABKALI01: Entering the nc command to view its list of parameters.

The output of the **nc -h** command is displayed.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=K5ILFYhmzkyg6eHXCPykGMEuQnlwMVB6lStXPDWuyCzJHhmLul
Applications
Places
Terminal
Fri 09:53
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
        -e filename             program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -C                      Send CRLF as line-ending
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').
root@PLABKALI01:~#
```

Figure 2.26 Screenshot of PLABKALI01: Showing the output of the nc -h command.

Step 2

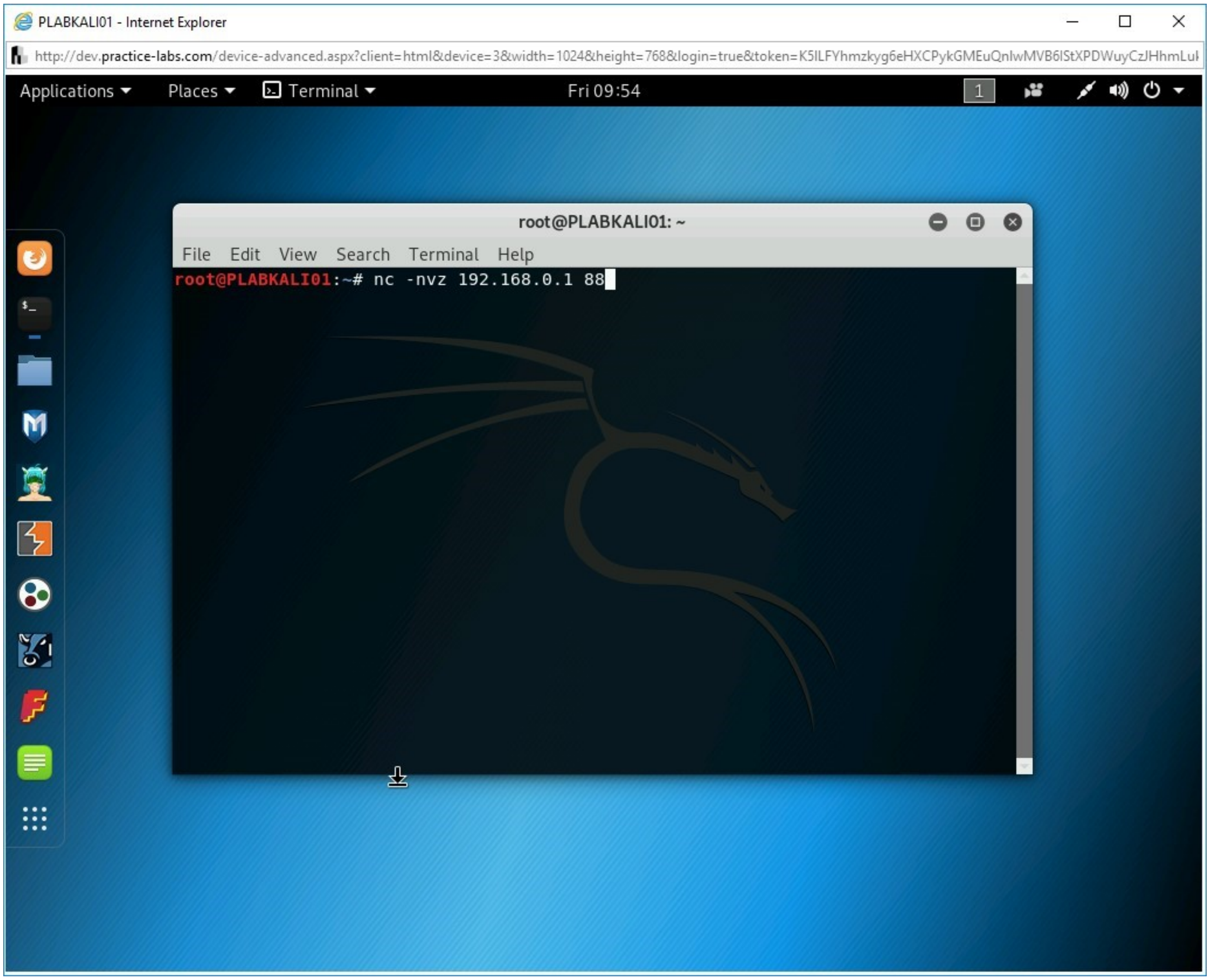
Clear the screen by entering the following command:

```
clear
```

To scan for a specific port, type the following command:

```
nc -nvz 192.168.0.1 88
```

Press **Enter**.

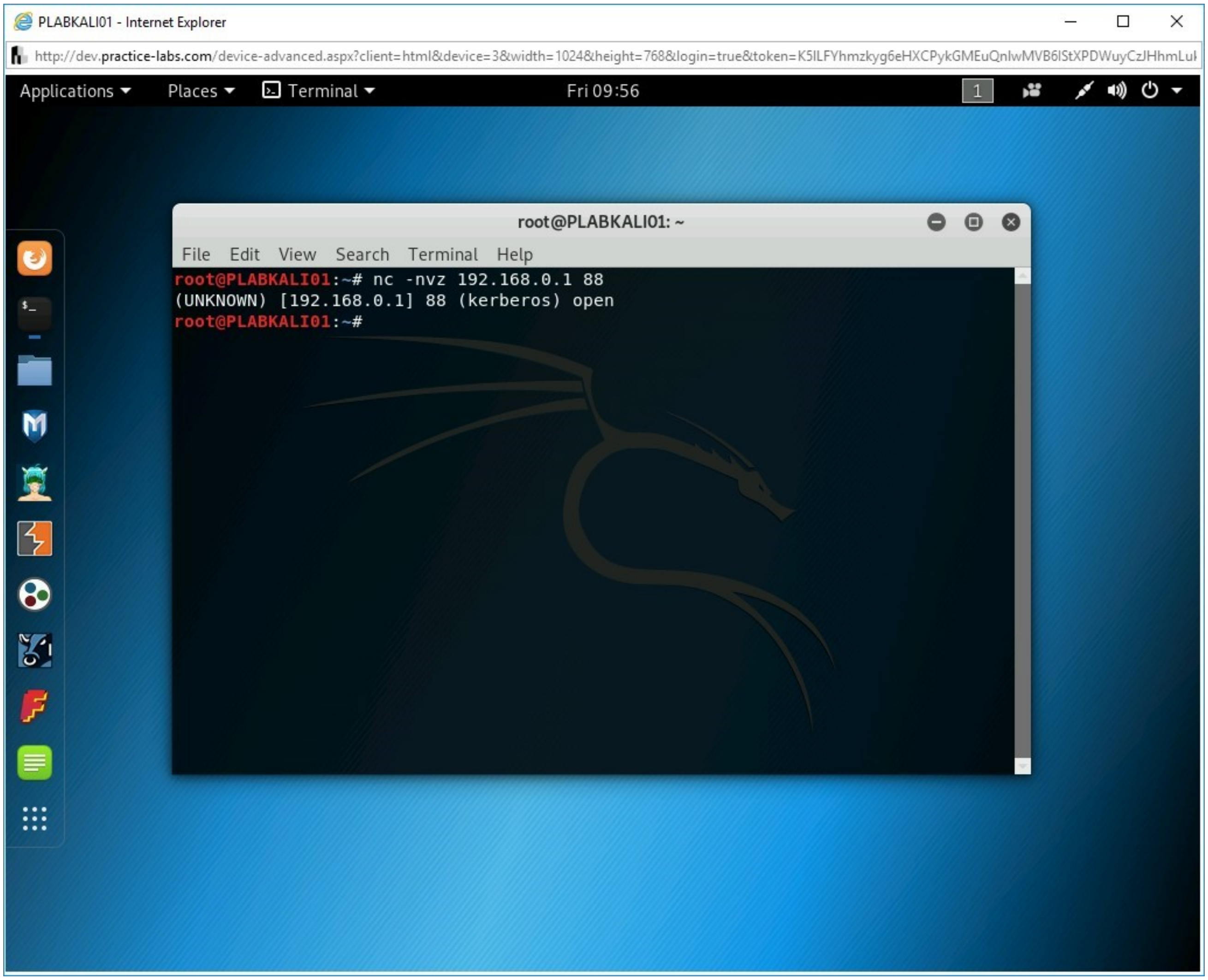

PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=K5ILFYhmzkyg6eHXCPykGMEuQnlwMVB6lStXPDWuyCzJHhmLuI
Applications
Places
Terminal
Fri 09:54
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# nc -nvz 192.168.0.1 88
```

Figure 2.27 Screenshot of PLABKALI01: Entering the nc command to view the specific port on a system.

***Note**: The -n parameter states that an IP address will be used. The -z parameter is used for scanning. The -v parameter is used for verbose output.*

The output of the **nc** command is displayed. It confirms that the port **88**, which is used by Kerberos, is open. You can test out various ports and find out if they are open.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=K5ILFYhmzkyg6eHXCPykGMEuQnlwMVB6lStXPDWuyCzJHhmLuk
Applications
Places
Terminal
Fri 09:56
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# nc -nvz 192.168.0.1 88
(UNKNOWN) [192.168.0.1] 88 (kerberos) open
root@PLABKALI01:~#
```

Figure 2.28 Screenshot of PLABKALI01: Showing the output of the nc command.

Keep the terminal window open.

Task 4 - Use Netdiscover for Scanning the Network

Netdiscover is a tool that can perform Layer 2 discovery. You can pass the range of IP address in the CIDR notation, and Netdiscover can scan the entire range.

In this task, you will learn to scan the network using Netdiscover. To do this, type the following command:

Step 1

Ensure you have powered on the required devices and connect to **PLABKALI01**.

If you are continuing from the previous task, the terminal window should be open. If not, then open a new terminal window.

If continuing from the previous task, then clear the screen by entering the following command:

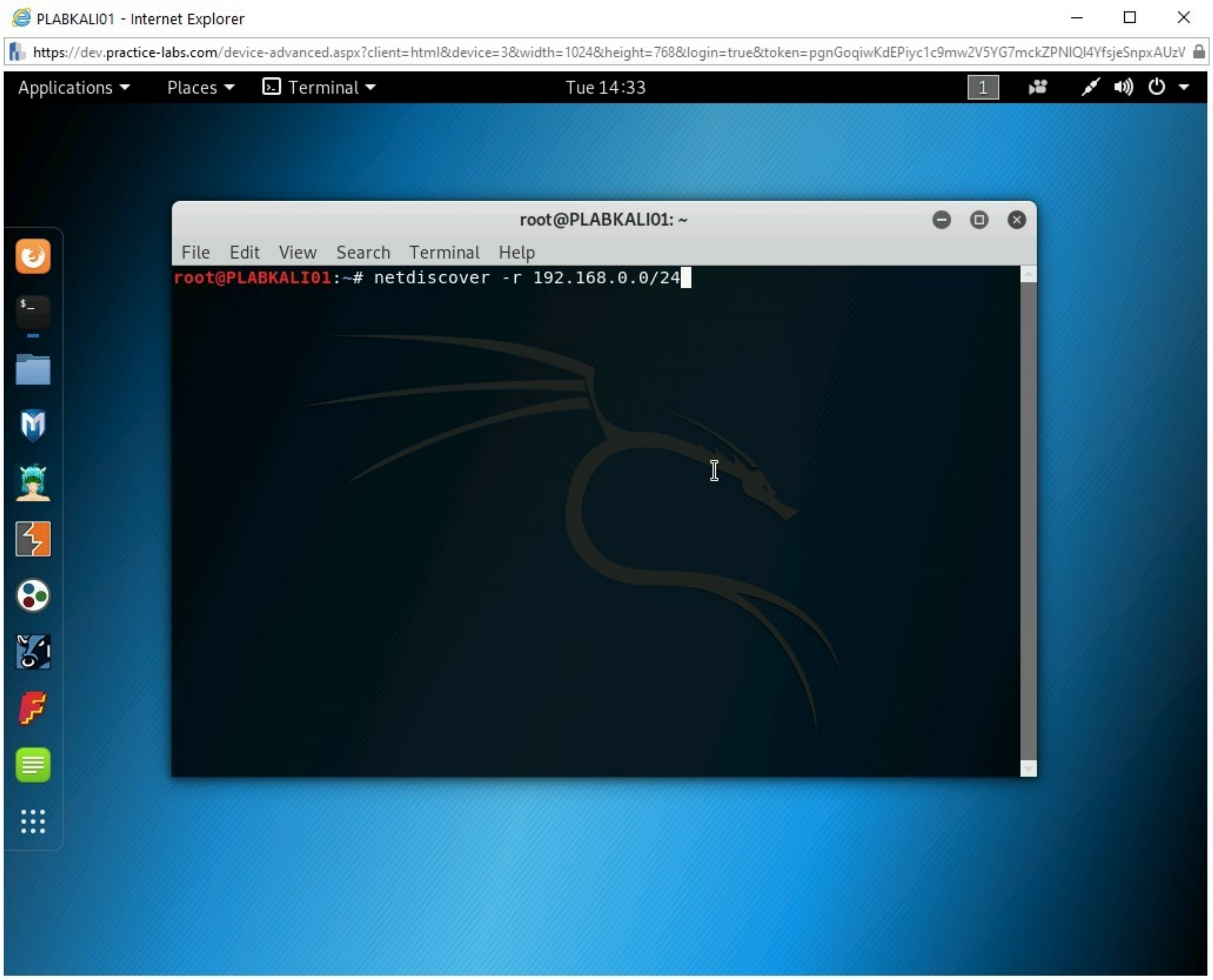
```
clear
```

To view the list of parameters of the **netdiscover** command, type the following:

```
netdiscover -r 192.168.0.0/24
```

Press **Enter**.

> ***Note****: The -r parameter is used for defining the CIDR notation.*

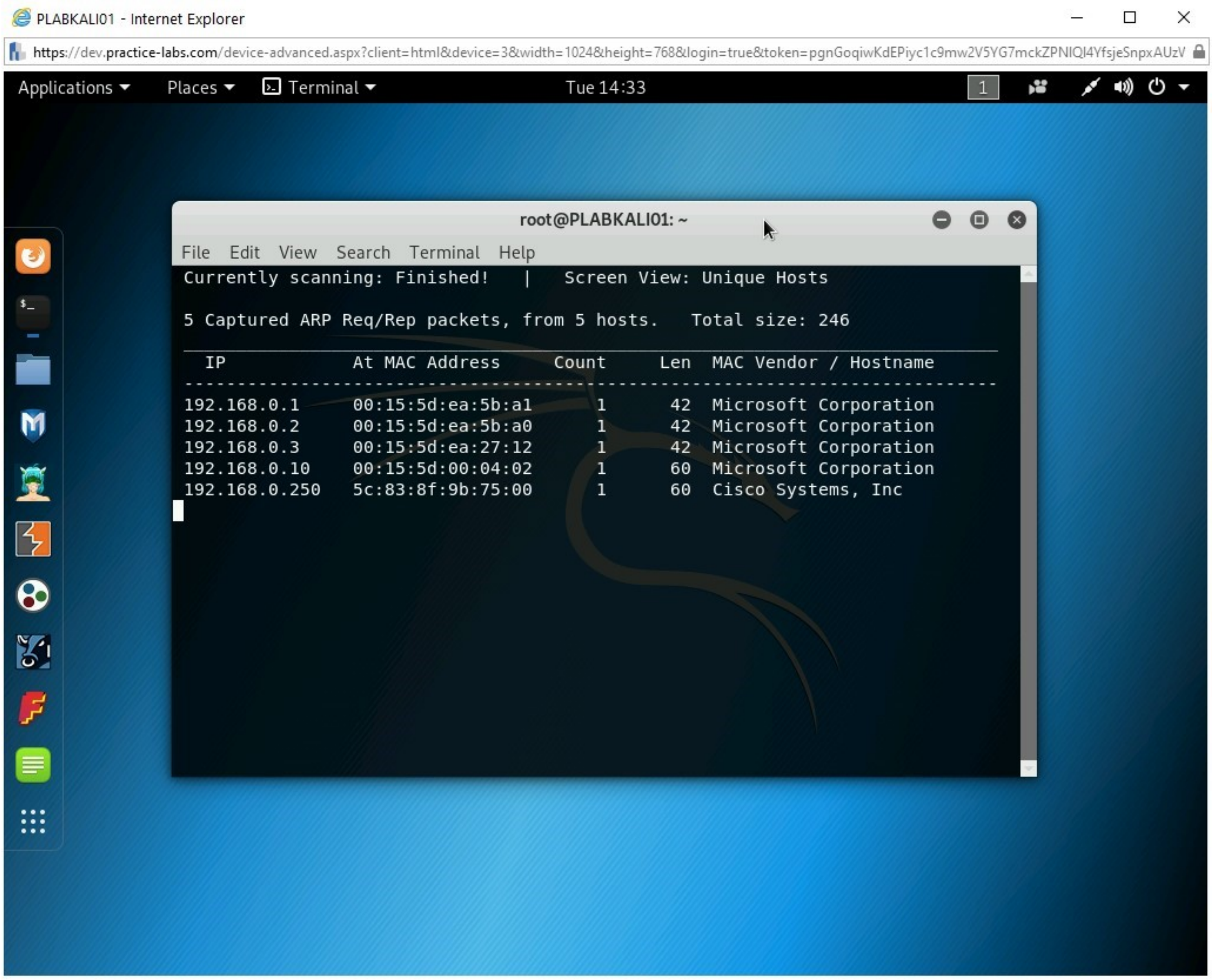

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=pgnGoqiwKdEPiyc1c9mw2V5YG7mckZPNIQI4YfsjeSnpxAUzV
Applications
Places
Terminal
Tue 14:33
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# netdiscover -r 192.168.0.0/24
```

Figure 2.29 Screenshot of PLABKALI01: Showing the desktop of PLABWIN10.

Notice the output of the **netdiscover** command. It has detected **five** systems on the network.

> ***Note***: *The fifth system is the Kali Linux system. Since you are executing the command from sixth system, it does not mention it in the list.*


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=pgnGoqiwKdEPiyc1c9mw2V5YG7mckZPNIQl4YfsjeSnpxAUzV
Applications
Places
Terminal
Tue 14:33
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 246
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.0.1     00:15:5d:ea:5b:a1      1      42  Microsoft Corporation
192.168.0.2     00:15:5d:ea:5b:a0      1      42  Microsoft Corporation
192.168.0.3     00:15:5d:ea:27:12      1      42  Microsoft Corporation
192.168.0.10    00:15:5d:00:04:02      1      60  Microsoft Corporation
192.168.0.250   5c:83:8f:9b:75:00      1      60  Cisco Systems, Inc
```

Figure 2.30 Screenshot of PLABKALI01: Showing the output of the netdiscover command.

Step 2

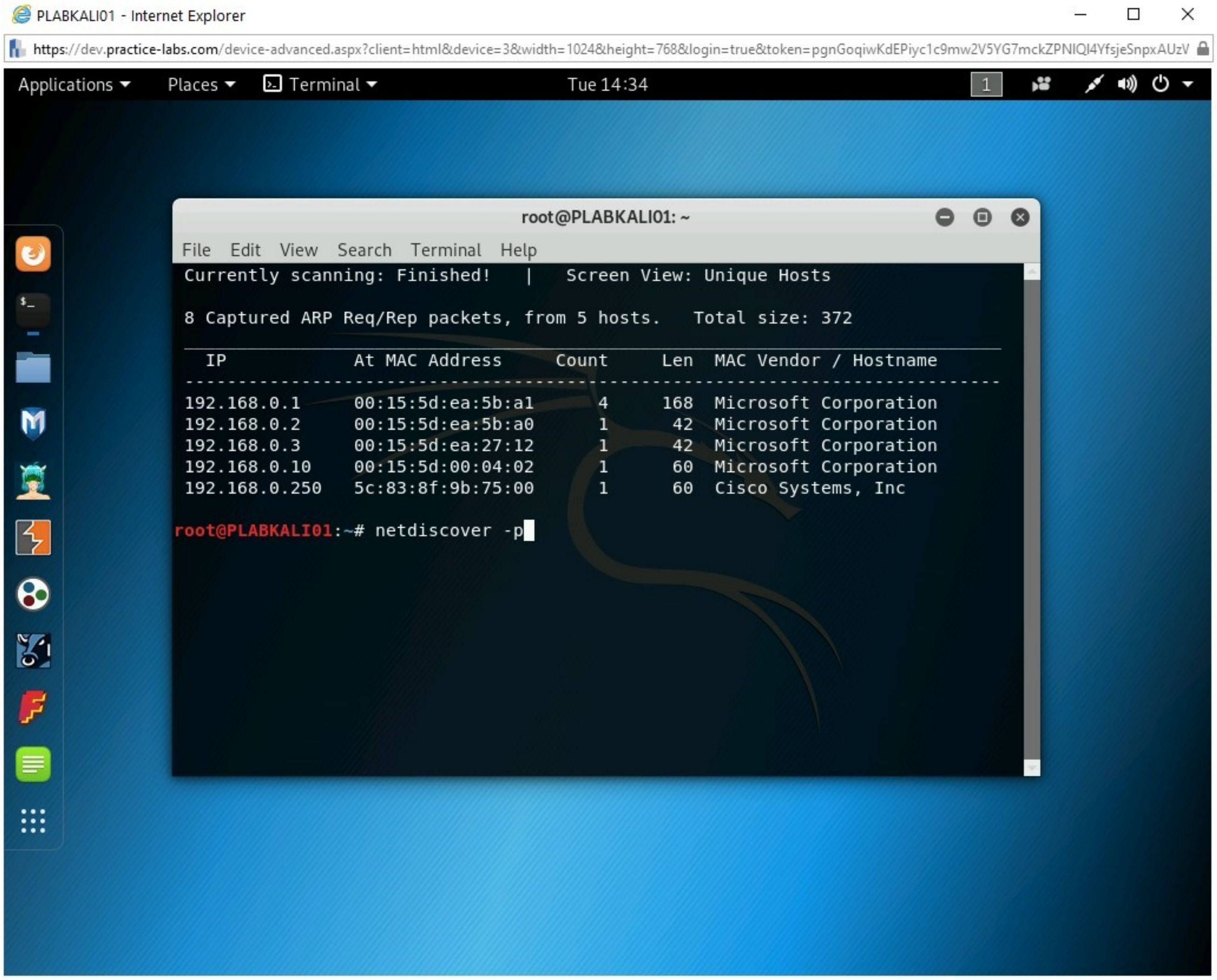
Press **Ctrl** + **C** to break the command.

If you are scanning an entire system, it can alert an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS). This is because ARP requests are broadcasted all over the subnet, which can alert an IDS or IPS. You can run the netdiscover command in stealth mode using the **-p** parameter.

Type the following command:

```
netdiscover -p
```

Press **Enter**.

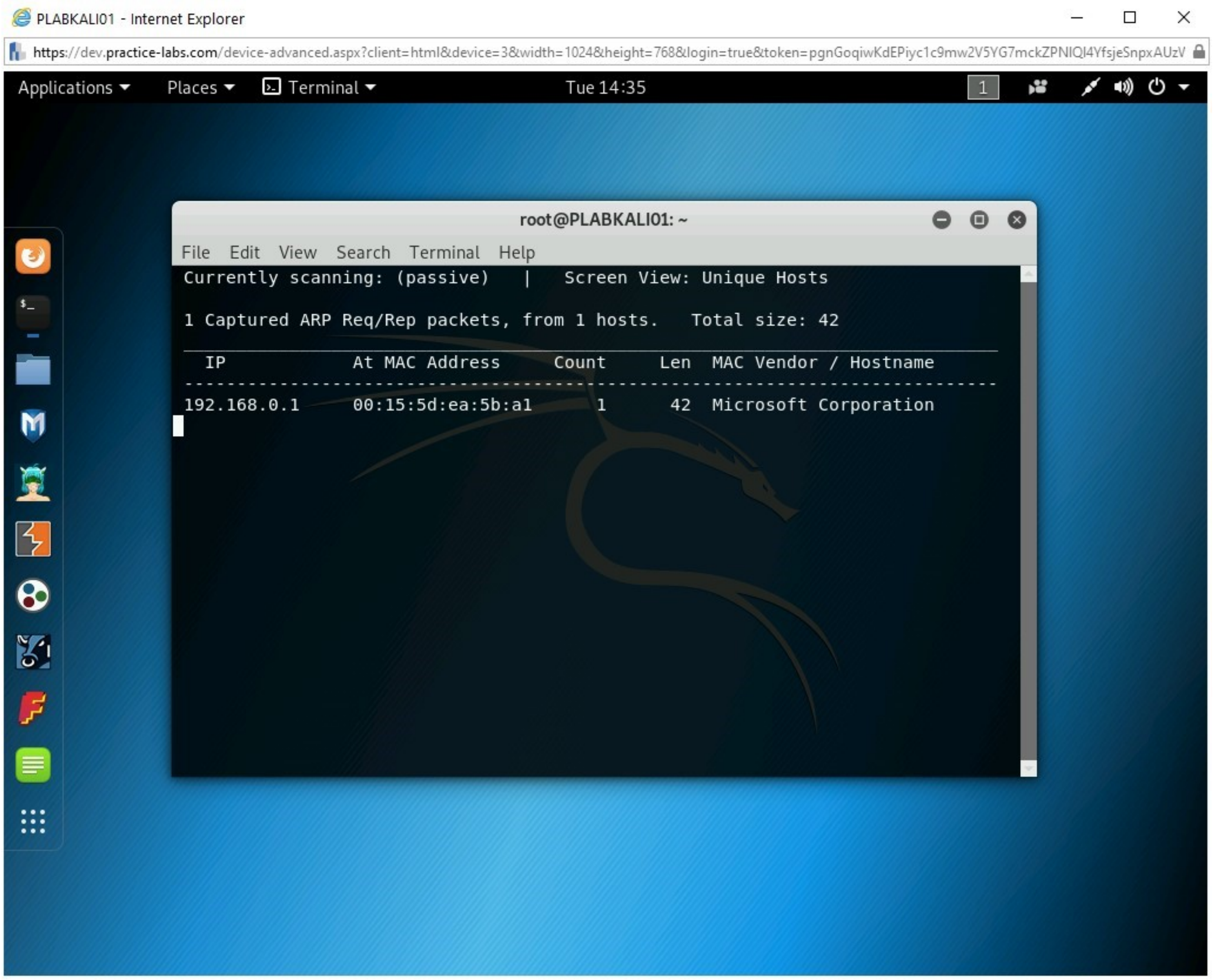

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=pgnGoqiwKdEPiyc1c9mw2V5YG7mckZPNIQl4YfsjeSnpxAUzV
Applications ▾
Places ▾
Terminal ▾
Tue 14:34
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

8 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 372
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.0.1     00:15:5d:ea:5b:a1      4     168  Microsoft Corporation
192.168.0.2     00:15:5d:ea:5b:a0      1      42  Microsoft Corporation
192.168.0.3     00:15:5d:ea:27:12      1      42  Microsoft Corporation
192.168.0.10    00:15:5d:00:04:02      1      60  Microsoft Corporation
192.168.0.250   5c:83:8f:9b:75:00      1      60  Cisco Systems, Inc

root@PLABKALI01:~# netdiscover -p
```

Figure 2.31 Screenshot of PLABKALI01: Executing the netdiscover command in the stealth mode.

Notice that the command executes in the passive mode, which is stealth mode.

***Note**: If may take a few minutes to scan for systems on a network.*

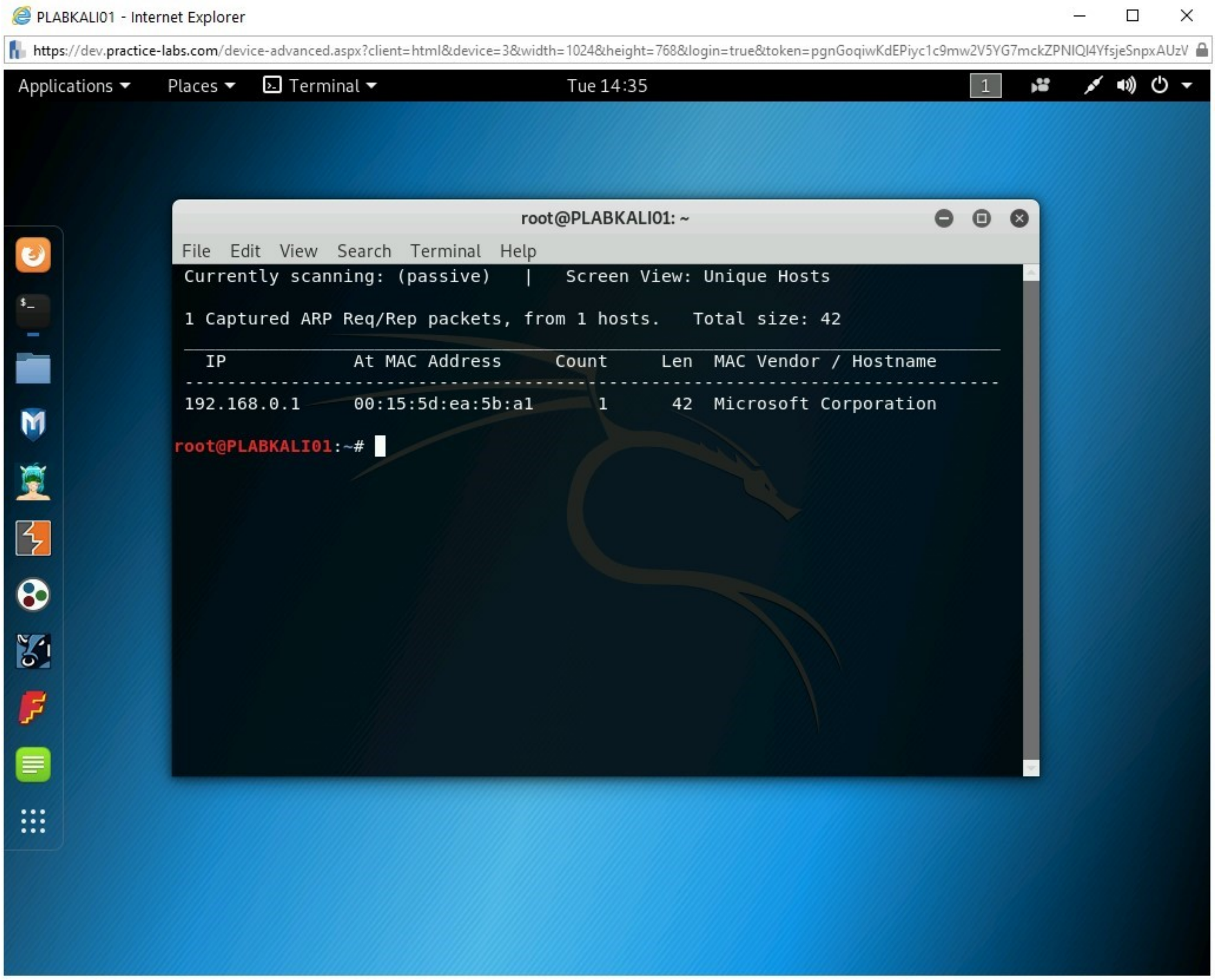

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=pgnGoqiwKdEPiyc1c9mw2V5YG7mckZPNIQI4YfsjeSnpxAUzV
Applications
Places
Terminal
Tue 14:35
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
Currently scanning: (passive)   |   Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 42
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.0.1     00:15:5d:ea:5b:a1      1      42  Microsoft Corporation
```

Figure 2.32 Screenshot of PLABKALI01: Showing the progress of the netdiscover command in stealth mode.

Step 3

If this command takes a long time to run, you can break the command by pressing **Ctrl** + **C** keys.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=pgnGoqiwKdEPiyc1c9mw2V5YG7mckZPNIQl4YfsjeSnpxAUzV
Applications
Places
Terminal
Tue 14:35
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
Currently scanning: (passive)   |   Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 42
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.0.1     00:15:5d:ea:5b:a1      1      42  Microsoft Corporation

root@PLABKALI01:~# 
```

Figure 2.33 Screenshot of PLABKALI01: Breaking the netdiscover command.

Task 5 - Perform Stealth Scanning Using Nmap

In a stealth scan, the attacker does not complete the three-way handshake with the victim's system and, therefore, goes undetected. Nmap has different options for conducting stealth scans, which you will perform in this task. To conduct stealth scanning, perform the following steps:

Step 1

Ensure that you are connected to Kali Linux and the terminal window is open.

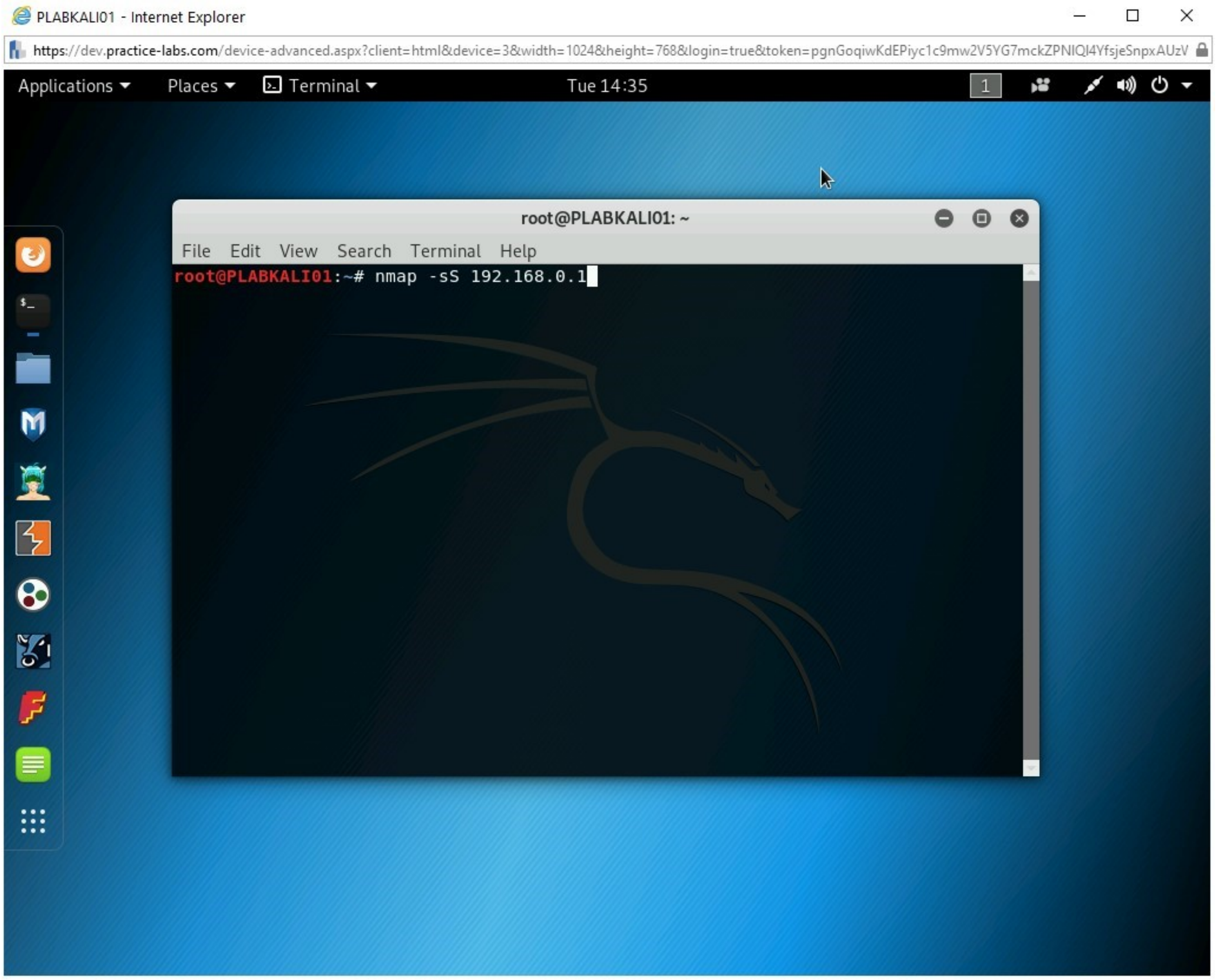
If not already, clear the screen by entering the following command:

```
clear
```

You will now scan for the ports using a **TCP SYN** scan, which is known to be a stealth scan. Type the following command:

```
nmap -sS 192.168.0.1
```

Press **Enter**.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=pgnGoqiwKdEPiyc1c9mw2V5YG7mckZPNIQl4YfsjeSnpxAUzV
Applications
Places
Terminal
Tue 14:35
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# nmap -sS 192.168.0.1
```

Figure 2.34 Screenshot of PLABKALI01: Typing the nmap -sS command in the terminal window.

> ***Note:*** *If no port range is specified, the command ‘nmap -sS <target>’ performs an SYN scan on well-known 1,000 TCP ports on the host <target>. Nmap scans can be specifically crafted as desired. Detailed information about all the switches supported by Nmap can be found in the help section of the tool.*

The output lists the open ports on 192.168.0.1.

Figure 2.35 Screenshot of PLABKALI01: Showing the output of the -sS command.

Step 2

Clear the screen by entering the following command:

```
clear
```

ACK scan cannot be used for scanning ports. This type of scan will never show ports in the "open" state, and hence it should be used in conjunction with other scan types to gain more information about firewalls or packet filters between your source machine and the target machine.

If used for port scanning, ACK scan will only provide a meaningful result if the target OS type is Solaris.

ACK scanning is mainly used to discover the rules of a filter. It can help to determine if a firewall is stateless (that blocks incoming SYN packets) or stateful (that tracks connections and also blocks unsolicited ACK packets).

As the name indicates, the ACK scan sends ACK packets to the target host. If the target responds with an RST packet, then the port is classified as "unfiltered" (the port is allowed to send its RST packet through the firewall that is in place). If no packets are received, the port is said to be "filtered" (the firewall prevented the RST packet sent from the port).

To perform a **TCP ACK** scan, type the following command:

```
nmap -sA 192.168.0.0/24
```

Press **Enter**.

The following are the switches used in the given command:

- -sA : ACK Scan
- -p : Specific port number to scan (port range can also be specified)

The output of this command is displayed. The output does not contain the **open** or **closed** ports but **filtered** or **unfiltered** ports. For example, all **1000** ports on **192.168.0.2** are filtered whereas, on **192.168.0.250**, they are unfiltered.

Figure 2.37 Screenshot of PLABKALI01: Showing the output of the nmap -sA command.

Step 3

Clear the screen by entering the following command:

```
clear
```

You can also perform a stealth scan to avoid being detected by the non-stateful firewalls. This is known as **Null** scan. In this type of scan, the **TCP** segment does not carry a flag. In the usual state, there would be at least the **ACK** flag that is raised.

To perform this, type the following command:

```
nmap -sN 192.168.0.1-4
```

Press **Enter**.

Figure 2.38 Screenshot of PLABKALI01: Typing the nmap -sN command in the terminal window.

The output of this command is displayed. It lists the open and filtered ports on various target systems.

Figure 2.39 Screenshot of PLABKALI01: Showing the output of the nmap -sN command.

Step 4

Clear the screen by entering the following command:

```
clear
```

Another type of stealth scan is a **FIN** scan, which sends a **TCP FIN** message. To conduct a **FIN** scan, type the following command:

```
nmap -sF 192.168.0.1-4
```

Press **Enter**.

Figure 2.40 Screenshot of PLABKALI01: Typing the nmap -sF command in the terminal window.

The output of this command is displayed.

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

Step 5

Clear the screen by entering the following command:

```
clear
```

The next type of stealth scan is **Xmas** scan, which sends the **TCP** segment with **three flags** raised. These flags are **FIN**, **PSH**, and **URG**.

> ***Note***: *The Null, FIN, and Xmas scans are used to avoid being detected by the non-stateful firewall.*

To perform the **Xmas** scan, type the following command:

```
nmap -sX 192.168.0.1-3
```

Press **Enter**.

Figure 2.42 Screenshot of PLABKALI01: Typing the nmap -sX command in the terminal window.

Notice the outcome of this command.

Figure 2.43 Screenshot of PLABKALI01: Showing the output of the nmap -sX command.

Step 6

Clear the screen by entering the following command:

```
clear
```

You can also choose the speed of your stealth scan. For example, you choose **paranoid** (T0), **sneaky** (T1), **polite** (T2), **normal** (T3), **aggressive** (T4), and **insane** (T5). **T0** is the slowest scan, and **T5** is the fastest scan.

To perform a T5 scan on a system, type the following command:

```
nmap 192.168.0.2 -T 5
```

Press **Enter**.

Figure 2.44 Screenshot of PLABKALI01: Typing the nmap command with the -T5 parameter in the terminal window.

Notice the speed of the scan.

> ***Note**: You can attempt to perform a T1 or T2 scan and notice the time difference.*

Figure 2.45 Screenshot of PLABKALI01: Showing the output of the nmap command with the -T parameter.

Keep the terminal window open.

Task 6 - Use fping for Network Scanning

The fping tool is similar to the ping tool but has additional features. One of the additional features is that it can be used as a scanning tool.

To use fping as a scanning tool, perform the following steps:

Step 1

Ensure that you are connected to Kali Linux and the terminal window is open.

Clear the screen by entering the following command:

```
clear
```

You can simply pass the IP address to the fping command as a parameter to check if a system is alive on the network.

Type the following command:

```
fping 192.168.0.1
```

Press **Enter**.

Figure 2.46 Screenshot of PLABKALI01: Entering the fping command to check if a host is alive.

The output shows that the mentioned system is alive on the network.

Figure 2.47 Screenshot of PLABKALI01: Showing the output of the fping command.

Step 2

Using the **-g** parameter, you can scan for more than one system on the network.

To do this, type the following command:

```
fping -g 192.168.0.1 192.168.0.2
```

Press **Enter**.

Figure 2.48 Screenshot of PLABKALI01: Entering the fping command to check for more than one system.

Notice that output displays the status of each of the systems.

Figure 2.49 Screenshot of PLABKALI01: Showing the output of the fping -g command.

Step 3

Using the **-g** parameter, you can scan an entire subnet using the **CIDR** notation.

To do this, type the following command:

```
fping -g 192.168.0.0/24
```

Press **Enter**.

Figure 2.50 Screenshot of PLABKALI01: Entering the fping command to scan an entire subnet using the CIDR notation.

Notice the output scans for the live systems on the entire subnet and lists the status of each IP address.

Note: *You can scroll to see the status of the systems.*

Figure 2.51 Screenshot of PLABKALI01: Showing the output of the fping command.

Close the **terminal** window.

Task 7 - Use Msfconsole to Perform TCP Stealth on a Network

Metasploit framework is the most widely used tool in exploiting vulnerabilities. A free edition is available in Kali Linux. Metasploit has a modular and flexible architecture that helps you develop new exploits as more vulnerabilities are discovered. On the other hand, it is also used in penetration testing. Other than the modules for penetration testing, Metasploit Framework also contains modules that can be used for various types of scans, such as:

- UDP scan
- TCP stealth scan
- Full connect scan

In this task, you will perform a TCP stealth scan. To do this, perform the following steps:

Step 1

Ensure you have powered on the required devices and connect to **PLABKALI01**.

Click the **metasploit framework** icon in the left pane.

Figure 2.52 Screenshot of PLABKALI01: Showing the desktop of PLABKALI01 and clicking on the metasploit framework icon.

Step 2

The terminal window is displayed.

Type **msfconsole**

Press **Enter**

Figure 2.53 Screenshot of PLABKALI01: Showing the msf5 prompt after the Metasploit framework starts.

The **metasploit framework** has started now.

> ***Note****: The number of exploits and payloads will change from time to time.*

Step 3

Next, you will load the module with the **use** command. To do this, type the following command:

```
use auxiliary/scanner/portscan/syn
```

Press **Enter**.

Figure 2.54 Screenshot of PLABKALI01: Using the use command for a module.

Step 4

You will now need to set the remote host on which you want to perform **the TCP stealth scan**. Type the following command:

```
set RHOSTS 192.168.0.1
```

Press **Enter**.

Figure 2.55 Screenshot of PLABKALI01: Setting the RHOSTS value.

Step 5

Notice that the **RHOSTS** value is now set. You will now set the number of concurrent tasks to be performed in the background. This is done by setting the **THREADS** value. Type the following command:

```
set THREADS 25
```

Press **Enter**.

Figure 2.56 Screenshot of PLABKALI01: Setting the THREADS value.

Step 6

Notice that the **THREADS** value is now set. You will need to set the port. This is done by setting the **PORTS** value. Type the following command:

```
set PORTS 53
```

Press **Enter**.

Figure 2.57 Screenshot of PLABKALI01: Setting the PORTS value.

Step 7

Notice that the **PORTS** value is now set. You can now execute the module.

To do this, type the following command:

```
run
```

Press **Enter**.

Figure 2.58 Screenshot of PLABKALI01: Using the run command to execute the module.

Notice the output. It has found the **port 53** to be open.

Figure 2.59 Screenshot of PLABKALI01: Showing the output of the run command.

Step 8

Let's now scan against a range of ports. To do this, you need to reset the **PORTS** value. Type the following command:

```
set PORTS 1-100
```

Press **Enter**.

Notice that the value of **PORTS** has been reset to **1-100**. This means ports **1** to **100** will be scanned.

Figure 2.60 Screenshot of PLABKALI01: Entering the command to reset the PORTS value.

Step 9

You can now execute the module. To do this, type the following command:

```
run
```

Press **Enter**.

Figure 2.61 Screenshot of PLABKALI01: Using the run command to execute the module.

Notice that in the range of **1** to **100**, two ports, **53** and **88**, are found open.

Figure 2.62 Screenshot of PLABKALI01: Showing the open ports.

Step 10

You have performed a **TCP stealth scan** against a single host. You can reset the **RHOSTS** value to perform this scan against multiple hosts in one go. To do this, type the following command:

```
set RHOSTS 192.168.0.1-3
```

Press **Enter**. Notice that the value of **RHOSTS** has been reset to **192.168.0.1-3**.

Figure 2.63 Screenshot of PLABKALI01: Resetting the RHOSTS value.

Step 11

You can now execute the module. To do this, type the following command:

```
run
```

Press **Enter**.

Figure 2.64 Screenshot of PLABKALI01: Using the run command to execute the module.

Notice the output. Port **53** and **88** are open on **192.168.0.1**. Port **80** is open on **192.168.0.2**.

Figure 2.65 Screenshot of PLABKALI01: Showing the open ports.

Review

Well done, you have completed the **Scanning Networks** Practice Lab.

Summary

You completed the following exercises:

- Exercise 1 - Using Microsoft Network Scanning Tools
- Exercise 2 - Using Linux Network Scanning Tools

You should now be able to:

- Banner Grab Using ID Serve
- Explore a Network Using Nmap
- Use CurrPorts to Monitor TCP/IP Connections
- Use MyLanViewer to Scan a Network
- Use Hping3 for Network Scanning
- Perform a TCP Scan Using Dmitry
- Use Netcat for Port Scan
- Use Netdiscover for Scanning the Network
- Perform Stealth Scanning Using Nmap
- Use fping for Network Scanning
- Use Msfconsole to Perform TCP Stealth on a Network

Feedback

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