Practice Labs - Ethical Hacker v10

Hacking Web Servers

Introduction

Webserver
Slowloris
HTTPrint
Directory Traversal
Brute-force
DirBuster
Metasploit Framework
WebDAV
Ethical Hacking

Welcome to the **Hacking Webservers** 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 - Exploiting the Webserver Vulnerabilities
- Exercise 2 - Preventing Webserver Exploitations

After completing this lab, you will be able to:

- Perform a Slowloris Attack on a Webserver
- Enumerate a Webserver using HTTPrint
- Perform Directory Traversal Attack
- Perform Web Application Brute Forcing Using DirBuster
- Use Skipfish to Perform Webserver Reconnaissance
- Find Files on a Webserver using Metasploit Framework
- Scan for Options on a Webserver using Metasploit Framework
- Find the Webserver Version using Metasploit Framework
- Check for WebDAV on a Webserver using Metasploit Framework
- Use Common Methods to Prevent Webserver Exploitation
- Disable HTTP TRACK and TRACE Verbs in Internet Information Services (IIS)

Exam Objectives

The following exam objectives are covered in this lab:

- **3.2** Information Security Attack Detection
- **3.3** Information Security Attack Prevention

> ***Note:*** *Our main focus is to cover the practical, hands-on aspects of the exam objectives. We recommend referring to course material or a search engine to research theoretical topics in more detail.*

Lab Duration

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

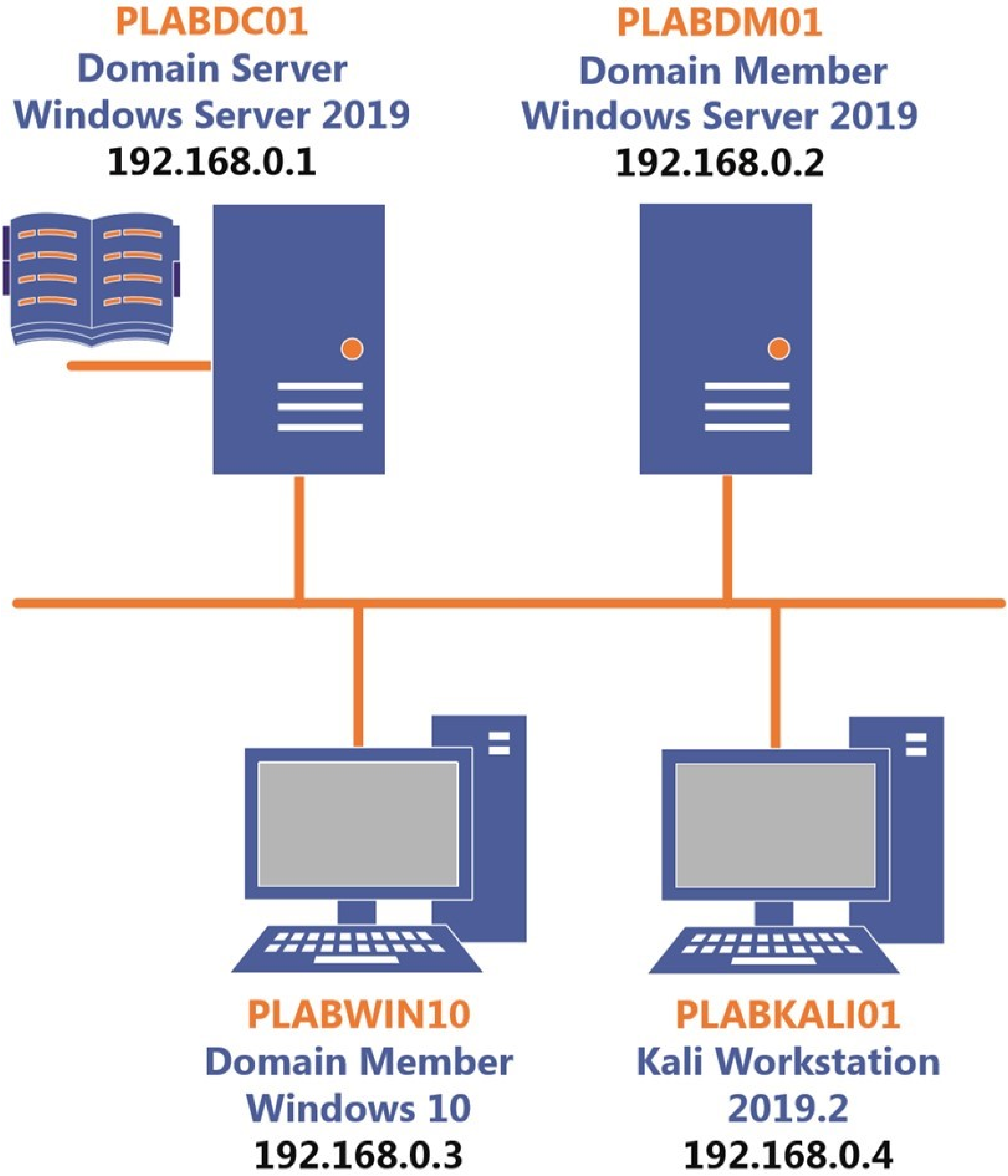
Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

> Click **Next** to view the Lab topology used in this module.

Lab Topology

During your session, you will have access to the following lab configuration.



Depending on the exercises, you may or may not use all of the devices, but they are shown here in the layout to get an overall understanding of the topology of the lab.

- **PLABDC01 -** (Windows Server 2019 - Domain Server)
- **PLABDM01 -** (Windows Server 2019 - Domain Controller)
- **PLABWIN10 -** (Windows 10 - Workstation)
- **PLABKALI01 -** (Kali 2019.2 - Linux Kali Workstation)

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

Exercise 1 - Exploiting the Webserver Vulnerabilities

A Webserver is designed to host Websites and Web applications. It uses HTTP as the base protocol for delivering the content to the users, who can either be on the intranet or the Internet. The security of a Webserver becomes critical because if it is compromised, then the hosted Website or Web application is also compromised. The attacker can gain access to the Webserver by exploiting one or more vulnerabilities.

The vulnerabilities can be inherent to the Webserver, which means that they are bugs or defects within the Webserver code. Other Webserver vulnerabilities can be external, such as:

- Insufficient permissions on files and directories
- Unnecessary services running
- Unnecessary ports open
- Default configuration being used

This is not an exhaustive list but provides an overview of the type of vulnerabilities that can be present in a Webserver.

An attacker, depending on the vulnerabilities found, can perform one or more attacks on the Webserver. Some of these attacks are:

- Denial-of-Service (DoS)
- Directory traversal
- DNS amplification

- DNS server hijacking
- Man-in-the-middle
- Sniffing
- Webserver misconfiguration

In this exercise, you will learn to exploit some of these vulnerabilities.

Learning Outcomes

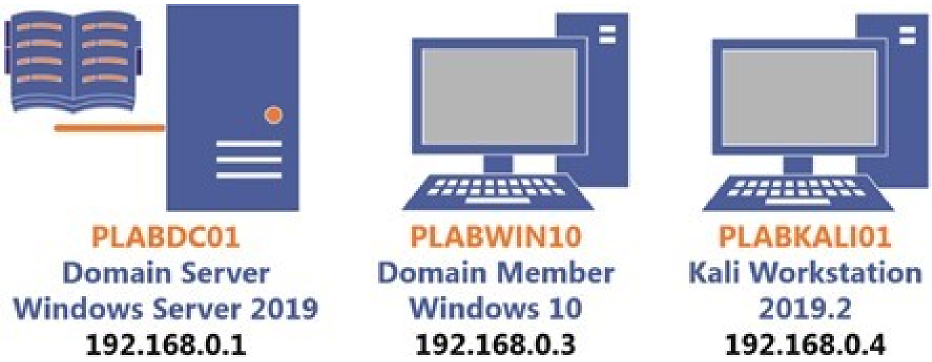
After completing this exercise, you will be able to:

- Perform a Slowloris Attack on a Web Server
- Enumerate a Webserver using HTTPrint
- Perform Directory Traversal Attack
- Perform Web Application Brute Forcing Using DirBuster
- Use Skipfish to Perform Webserver Reconnaissance
- Find Files on a Webserver using Metasploit Framework
- Scan for Options on a Webserver using Metasploit Framework
- Find the Webserver Version using Metasploit Framework
- Check for WebDAV on a Webserver using Metasploit Framework

Your Devices

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

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



Task 1 - Perform a Slowloris Attack on a Webserver

Slowloris is an effective Denial-of-Service attack tool that uses low bandwidth. It triggers and sends partial HTTP requests to a Webserver and continues sending to prevent sockets from being closed. The Webserver cannot close the sockets on its own and continues opening the sockets as the requests are received from Slowloris. Finally, the requests sent by Slowloris overwhelm the Webserver, and when the Webserver's maximum connection limit is reached, it starts to deny the legitimate requests. To prevent this attack, you can use some of the following methods:

- Use hardware-based load balancers that do not accept the partial http requests.
- Limit the connections to the Webserver in a firewall, such as Iptables
- Configure the timeout in the Webserver configuration

To perform the Slowloris attack on a Webserver, perform the following steps:

Step 1

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

Credentials are:

Username:

```
root
```

Password:

```
Passw0rd
```

The desktop of **PLABKALI01** is displayed.

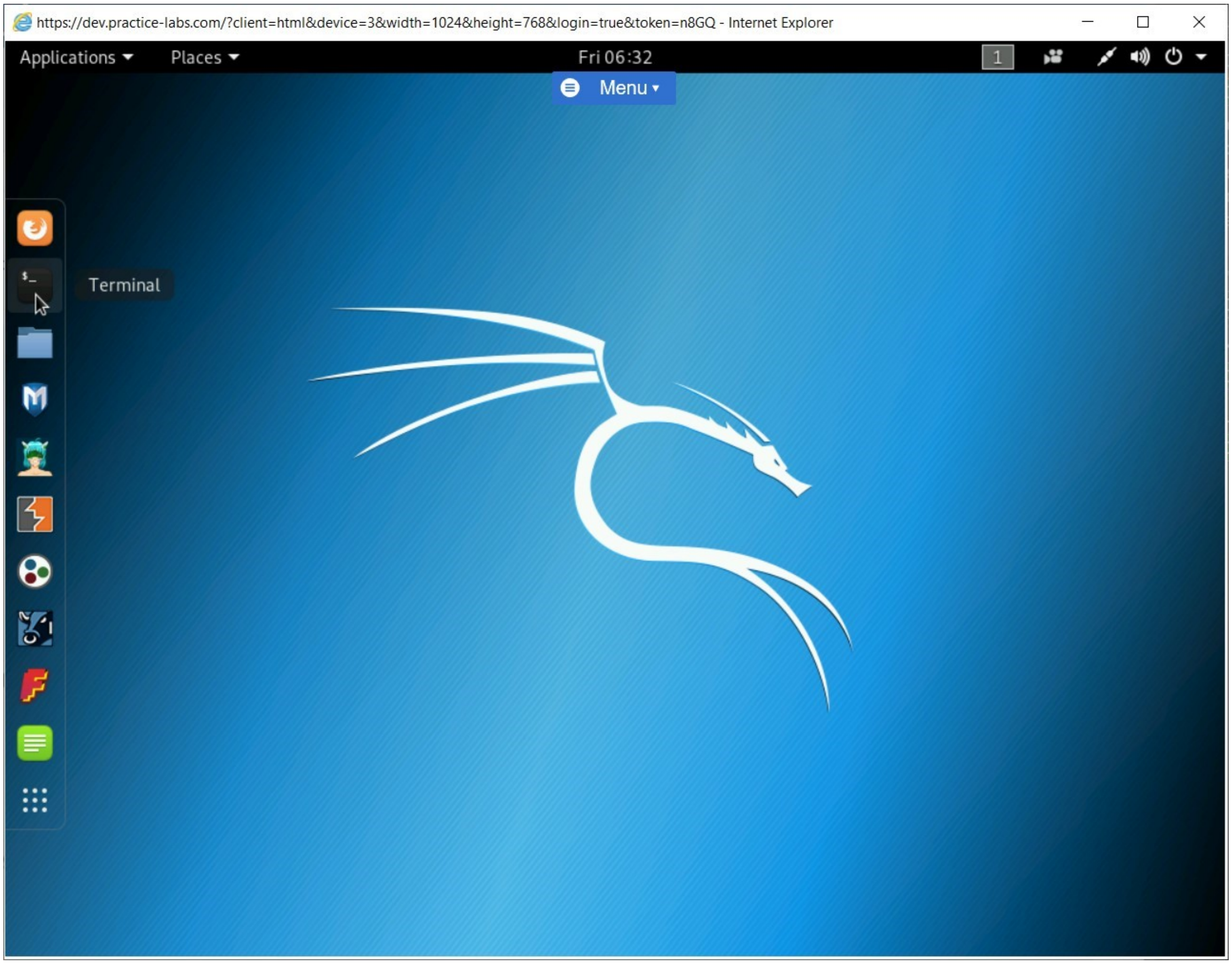

https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Fri 06:32
1
Menu
Terminal

Figure 1.1 Screenshot of PLABKALI01: Showing the desktop of PLABKALI01.

Step 2

On the desktop, in the left pane, click the **Terminal** icon.

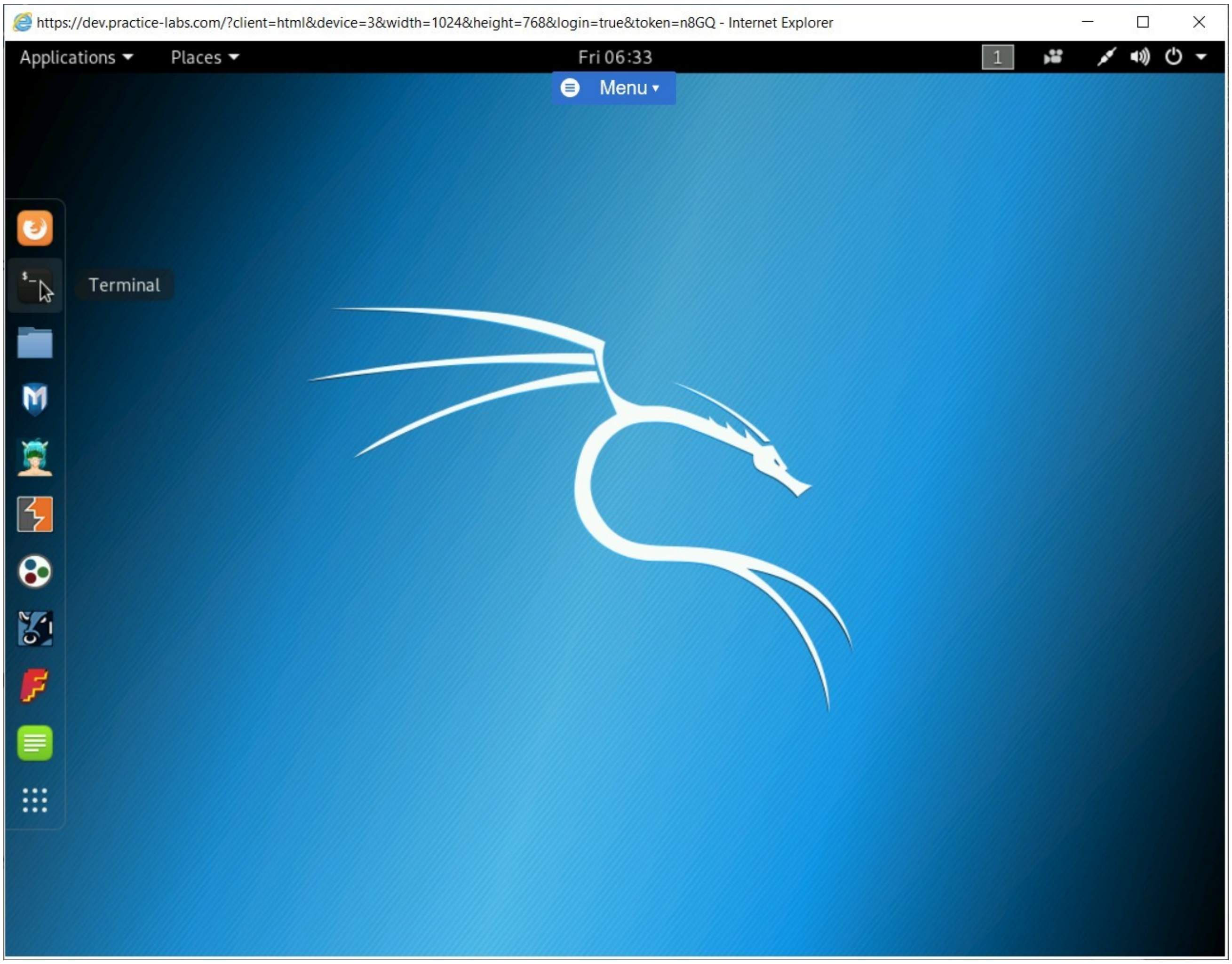

https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Fri 06:33
Menu
Terminal

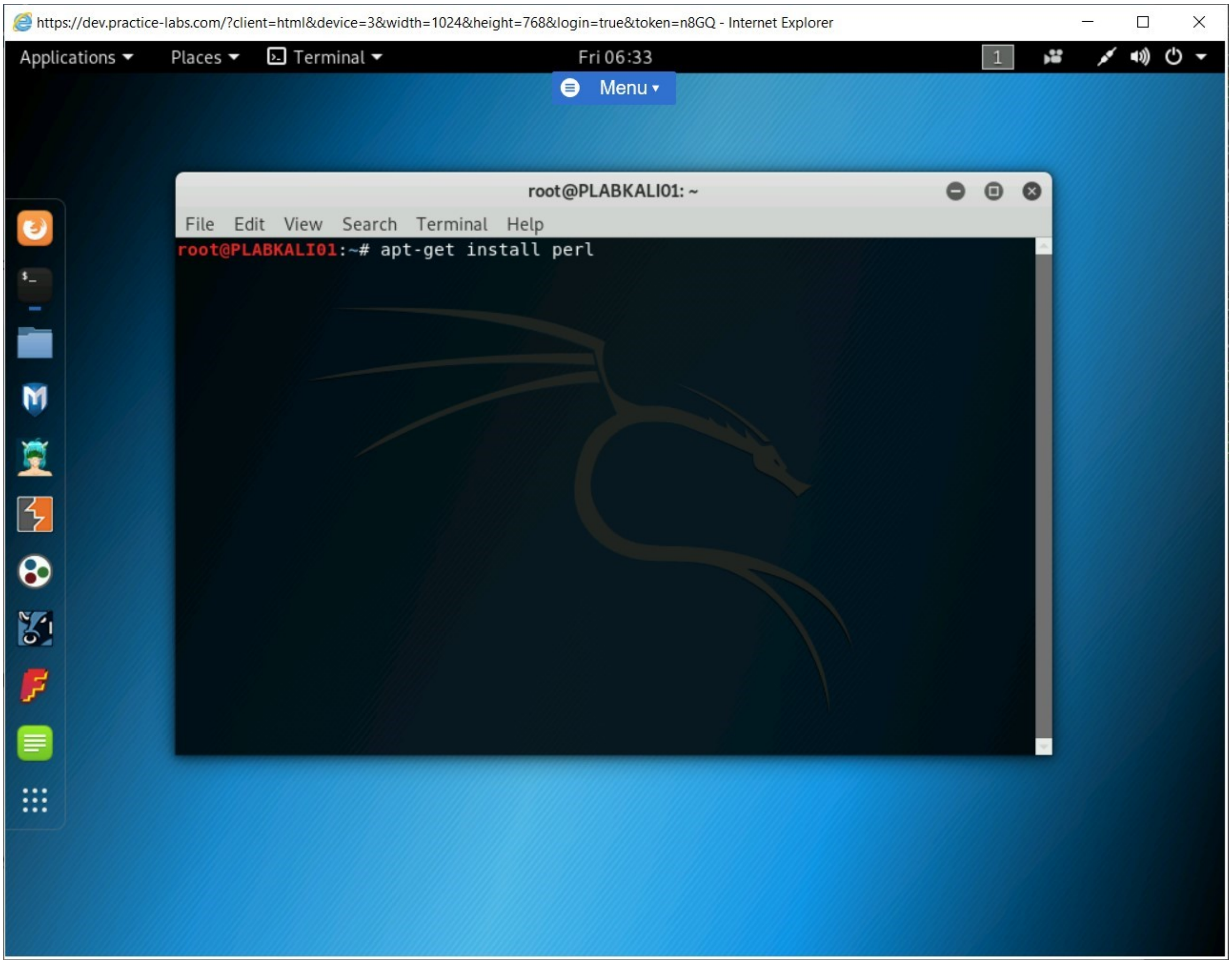
Figure 1.2 Screenshot of PLABKALI01: Clicking the Terminal icon in the left pane.

Step 3

Slowloris is a Perl-based tool. Therefore, you need to install **Perl** on Kali Linux. To do this, type the following command:

```
apt-get install perl
```

Press **Enter**.



https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 06:33
Menu
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# apt-get install perl
```

Figure 1.3 Screenshot of PLABKALI01: Entering the apt-get command to install perl.

Note: *The installation may take a couple of minutes to complete.*

Step 4

Clear the screen by entering the following command:

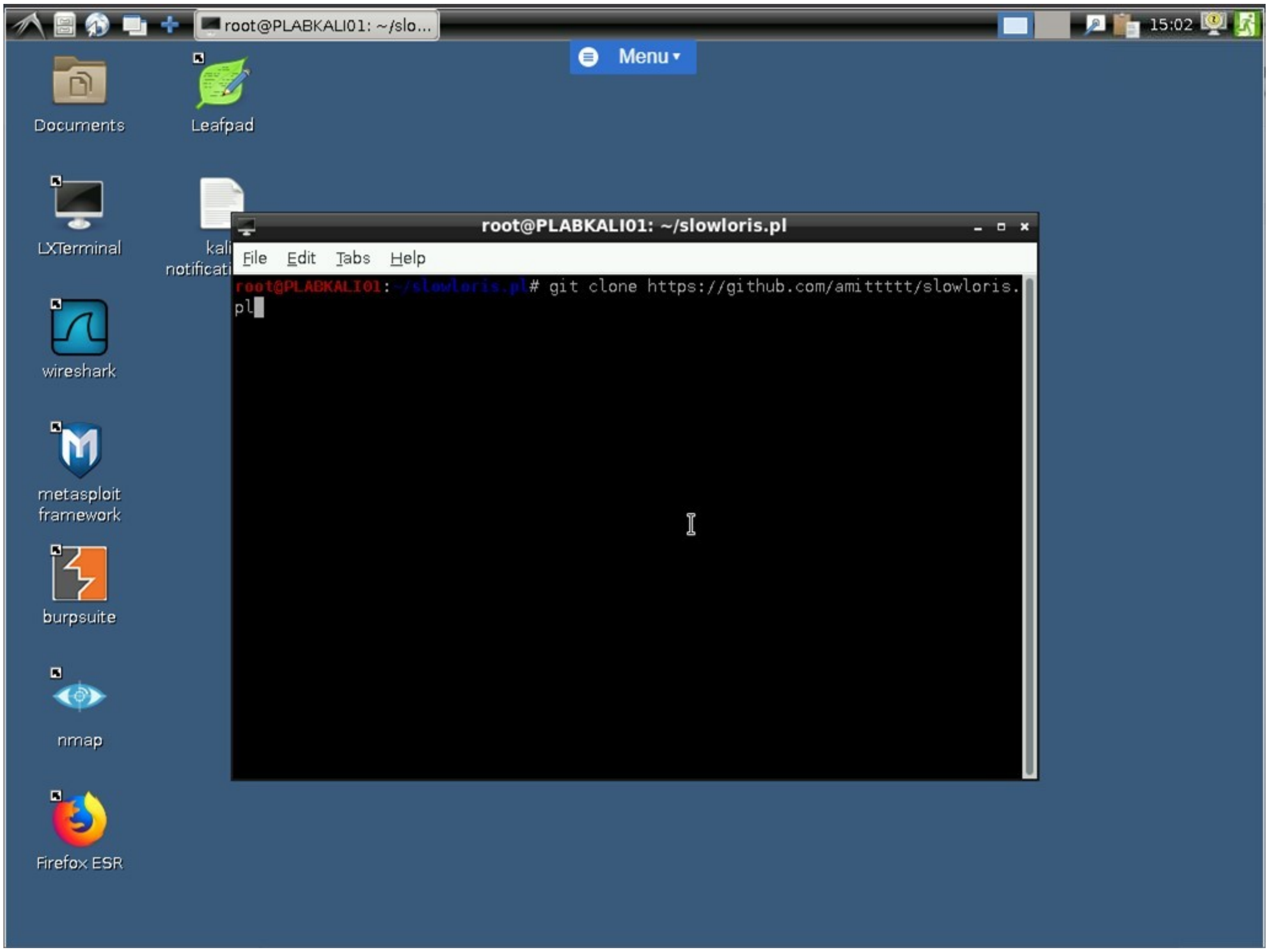
```
clear
```

Next, you need to install Slowloris. To do this, type the following command:

```
git clone https://github.com/amittttt/slowloris.pl
```

Press **Enter**.

Slowloris is now installed on Kali Linux.



```
root@PLABKALI01:~/slowloris.pl# git clone https://github.com/amittttt/slowloris.
pl
```

Figure 1.5 Screenshot of PLABKALI01: Showing the cloned Slowloris package from GitHub.

Step 5

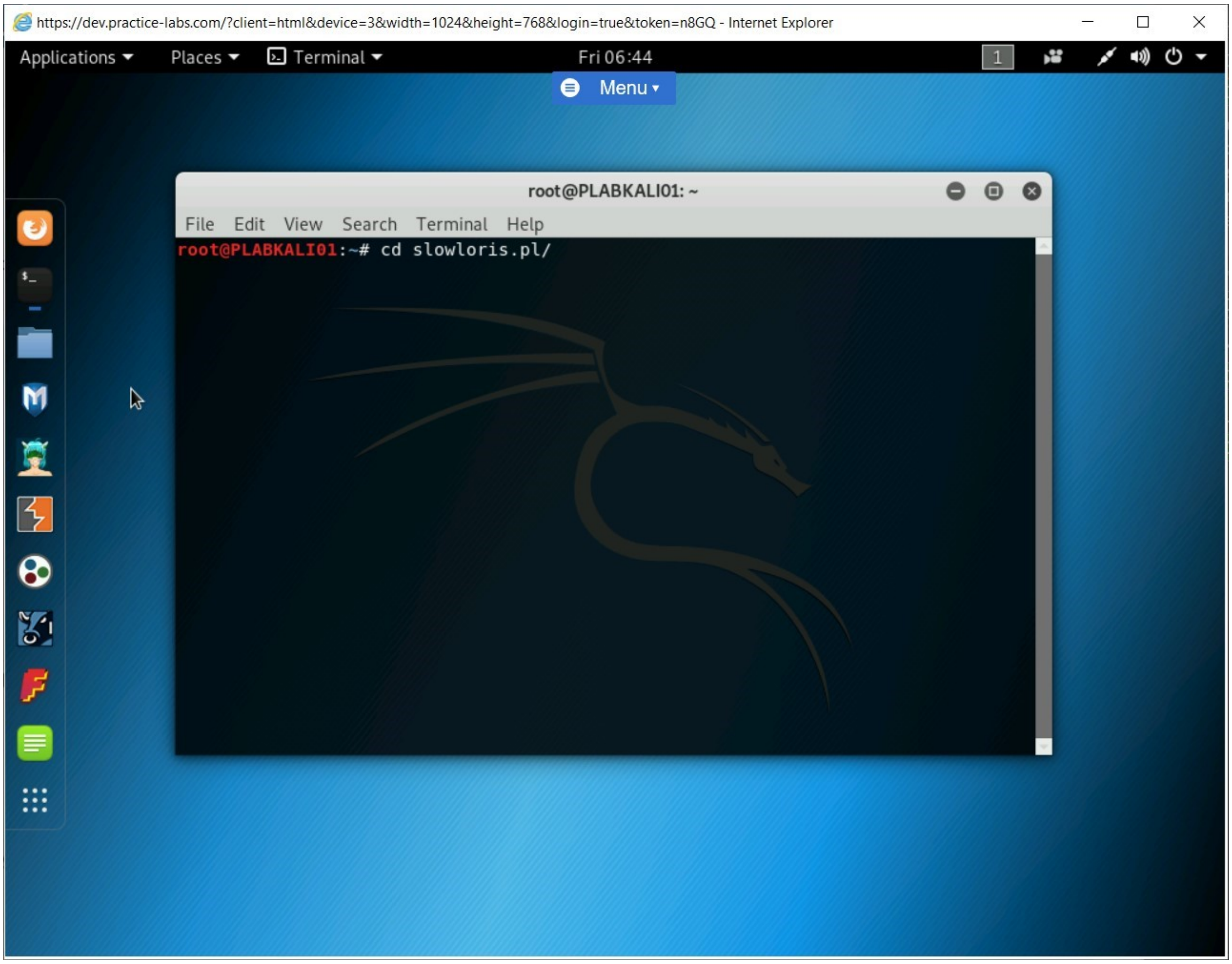
Clear the screen by entering the following command:

```
clear
```

To navigate to the slowloris directory, type the following command:

```
cd slowloris.pl
```

Press **Enter**.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 06:44
1
Menu
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# cd slowloris.pl/
```

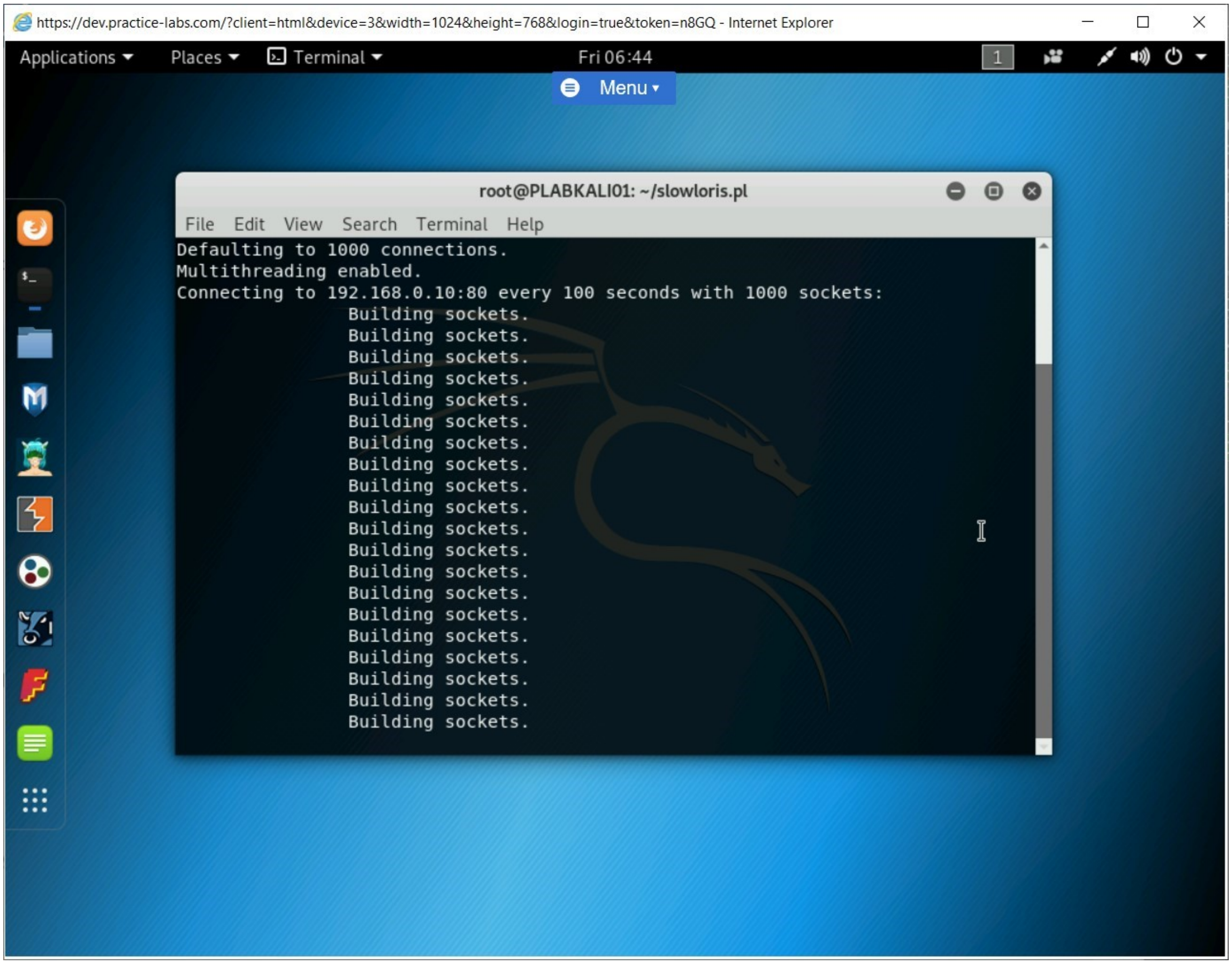
Figure 1.6 Screenshot of PLABKALI01: Navigating to the slowloris.pl directory.

Step 6

Now, you will execute the **slowris.perl** script. To do this, type the following command:

```
perl slowloris.pl -dns 192.168.0.10
```

Press **Enter**. Notice that **Slowloris** has started to consume sockets.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 06:44
Menu
root@PLABKALI01: ~/slowloris.pl
File Edit View Search Terminal Help

```
Defaulting to 1000 connections.
Multithreading enabled.
Connecting to 192.168.0.10:80 every 100 seconds with 1000 sockets:
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
```

Figure 1.7 Screenshot of PLABKALI01: Showing the slowloris command consuming sockets.

Step 7

Let’s connect to the Website running on **192.168.0.10**. Connect to **PLABWIN10**. The desktop of **PLABWIN10** is displayed.

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

```
Internet Explorer
```

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

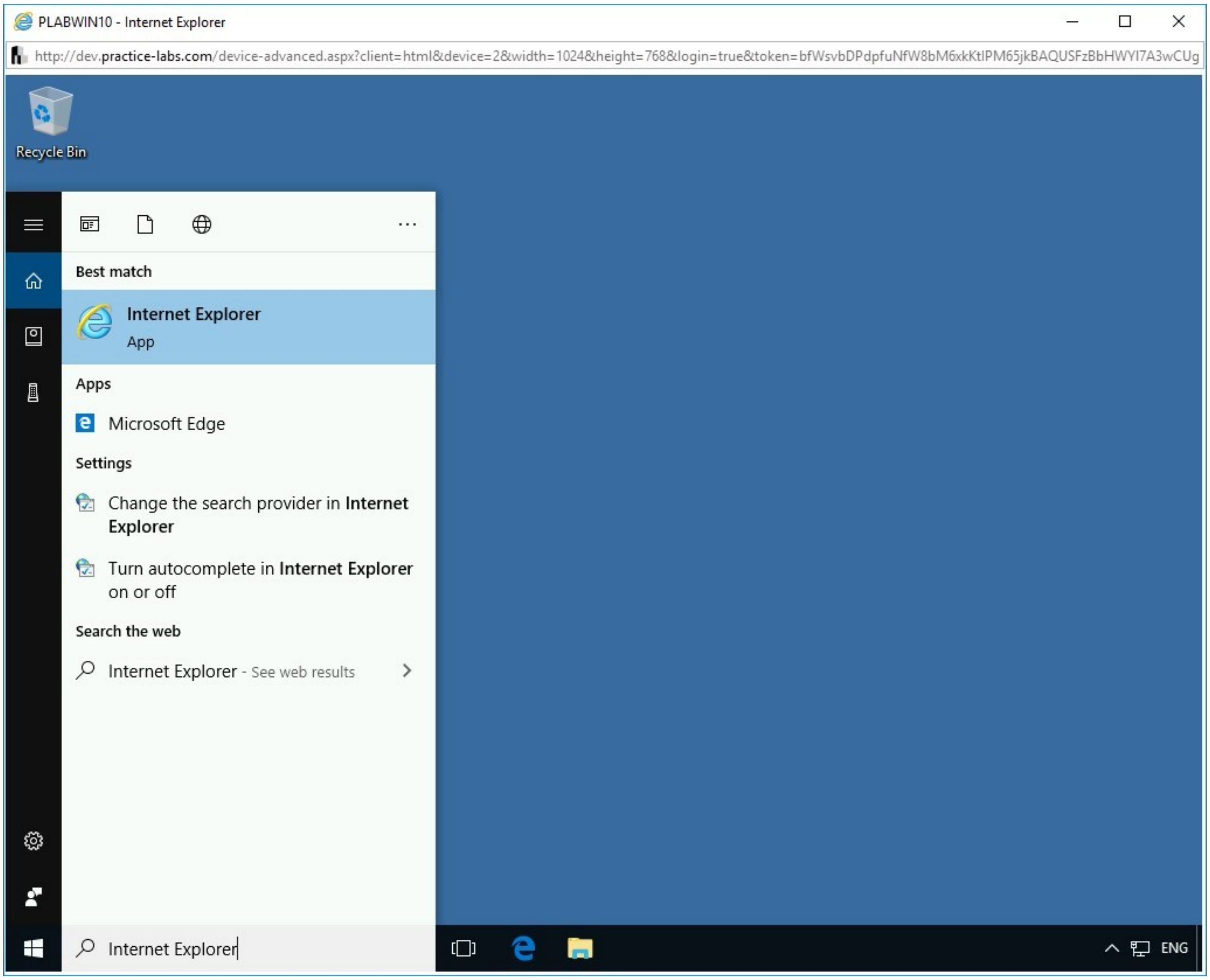

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bfWsvbDPdpfuNfW8bM6xkKtIPM65jkBAQUSFzBbHWYI7A3wCUg
Recycle Bin
Best match
Internet Explorer
App
Apps
Microsoft Edge
Settings
Change the search provider in Internet Explorer
Turn autocomplete in Internet Explorer on or off
Search the web
Internet Explorer - See web results
Internet Explorer
ENG

Figure 1.8 Screenshot of PLABWIN10: Selecting Internet Explorer from the search results.

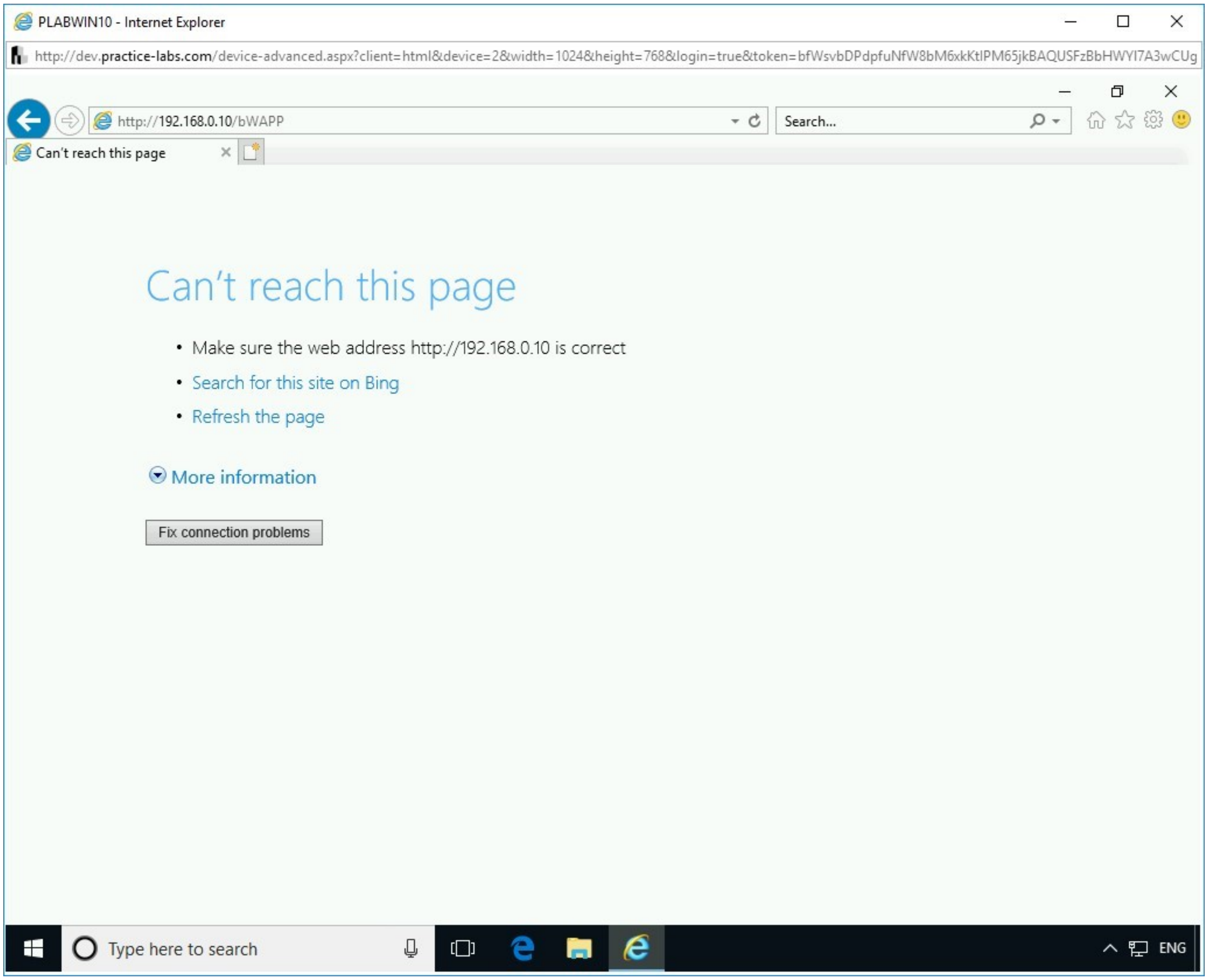
Step 8

The **Internet Explorer** window is displayed. In the address bar, type the following URL:

```
http://192.168.0.10/bWAPP
```

Press **Enter**. Notice the error. The Website fails to load.

> ***Note:*** *It may load in some cases, but it will eventually time out or become unresponsive.*



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bfWsvbDPdpfuNfW8bM6xkKtIPM65jkBAQUSFzBbHWYI7A3wCUg
http://192.168.0.10/bWAPP
Search...
Can't reach this page
Type here to search
ENG

Can't reach this page

- Make sure the web address http://192.168.0.10 is correct
- Search for this site on Bing
- Refresh the page

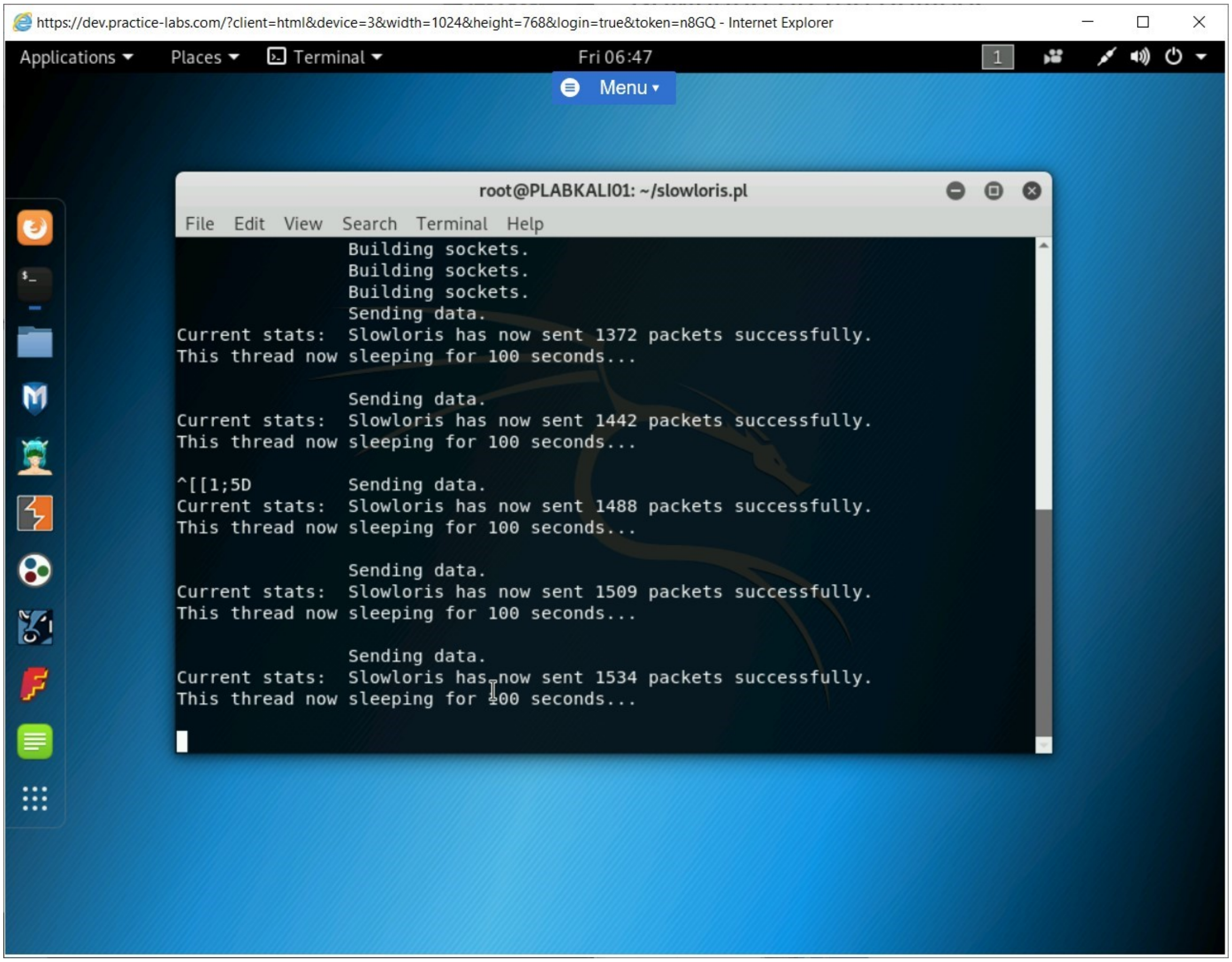
More information

Fix connection problems

Figure 1.9 Screenshot of PLABWIN10: Showing the error in loading the webpage.

Step 9

Switch back to **PLABKALI01**. Notice that **Slowloris** is consuming sockets continuously.

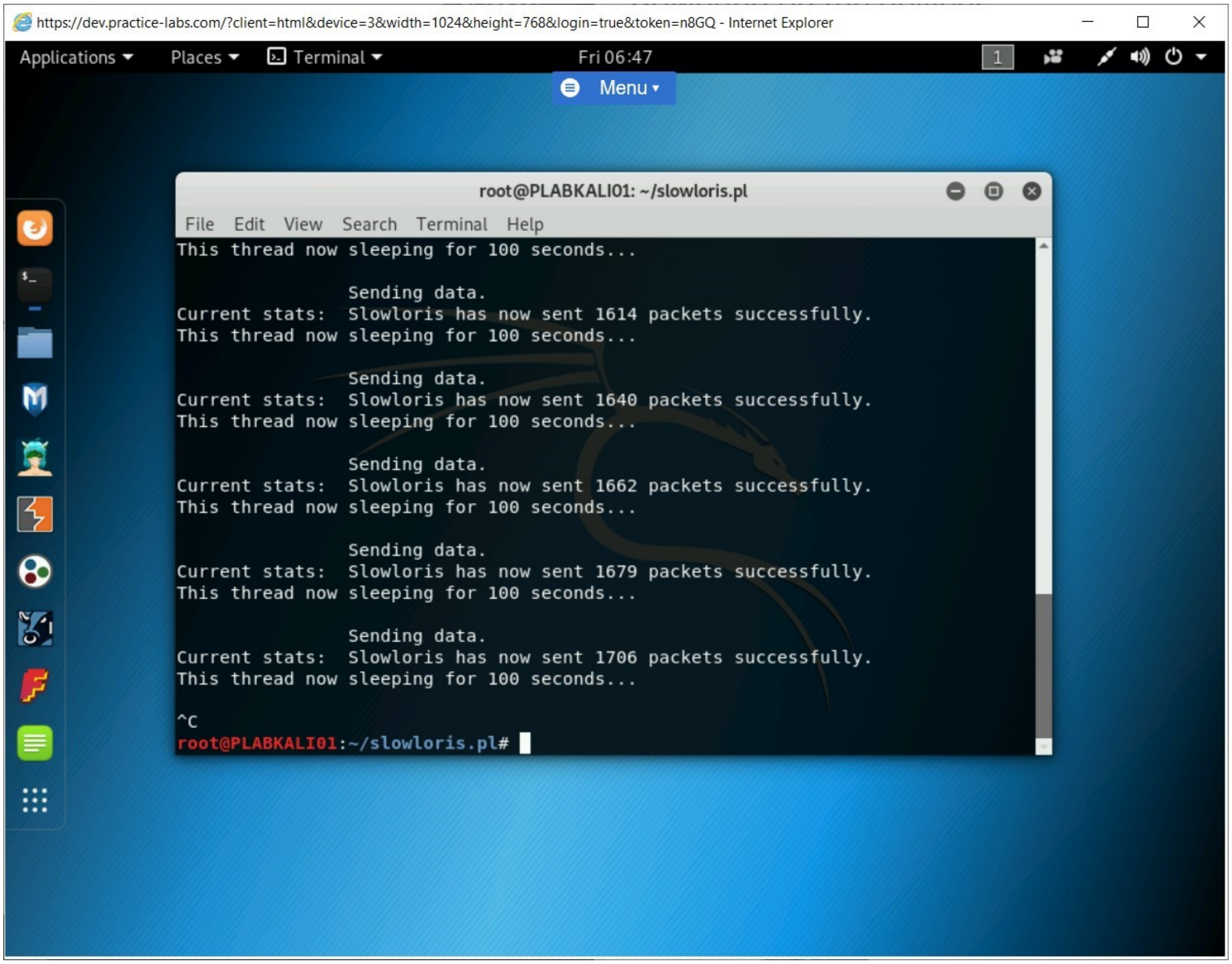

https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 06:47
Menu
root@PLABKALI01: ~/slowloris.pl
File Edit View Search Terminal Help

```
                Building sockets.
                Building sockets.
                Building sockets.
                Sending data.
Current stats:  Slowloris has now sent 1372 packets successfully.
This thread now sleeping for 100 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1442 packets successfully.
This thread now sleeping for 100 seconds...

^[[1;5D         Sending data.
Current stats:  Slowloris has now sent 1488 packets successfully.
This thread now sleeping for 100 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1509 packets successfully.
This thread now sleeping for 100 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1534 packets successfully.
This thread now sleeping for 100 seconds...
```

Figure 1.10 Screenshot of PLABKALI01: Showing the slowloris command consuming sockets.

Step 10

Press **Ctrl + C** to terminate the **slowloris** command.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 06:47
Menu
root@PLABKALI01: ~/slowloris.pl
File Edit View Search Terminal Help

```
This thread now sleeping for 100 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1614 packets successfully.
This thread now sleeping for 100 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1640 packets successfully.
This thread now sleeping for 100 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1662 packets successfully.
This thread now sleeping for 100 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1679 packets successfully.
This thread now sleeping for 100 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1706 packets successfully.
This thread now sleeping for 100 seconds...

^C
root@PLABKALI01:~/slowloris.pl#
```

Figure 1.11 Screenshot of PLABKALI01: Pressing the Ctrl + c keys to terminate the slowloris command.

Step 11

Switch back to **PLABWIN10**. You can now attempt to reload the website in **PLABWIN10**. You can press **F5** or **Fn + F5**.

Notice that the website now loads without any issue.

Close the **Internet Explorer** window on **PLABWIN10**. Exit from the terminal window on **PLABKALI01**.

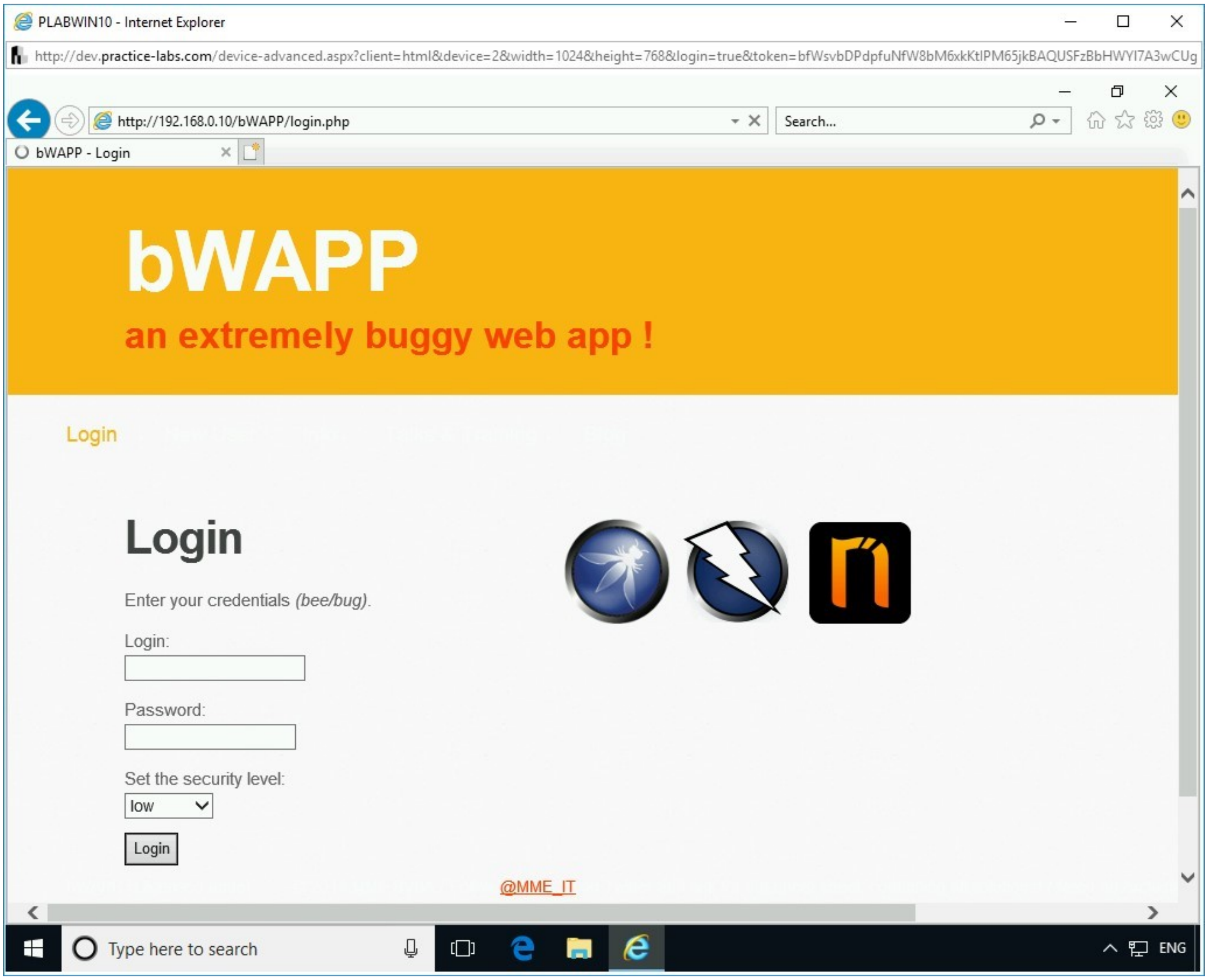

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bfWsvbDPdpfuNfW8bM6xkKtIPM65jkBAQUSFzBbHWYI7A3wCUg
http://192.168.0.10/bWAPP/login.php
Search...
bWAPP - Login
bWAPP
an extremely buggy web app !
Login
Login
Enter your credentials (bee/bug).
Login:
Password:
Set the security level:
low
Login
@MME_IT
Type here to search
ENG

Figure 1.12 Screenshot of PLABWIN10: Showing the Webpage loading without any error.

Task 2 - Enumerate a Web Server using HTTPrint

Other than using the command line tools, you can also use HTTPrint to enumerate a Webserver. In this task, you will learn to use HTTPrint to enumerate a Webserver.

> ***Note:*** *HTTPrint can be downloaded from www.net-square.com/httprint.html*

Step 1

Ensure you have powered the required devices. Connect to **PLABWIN10**.

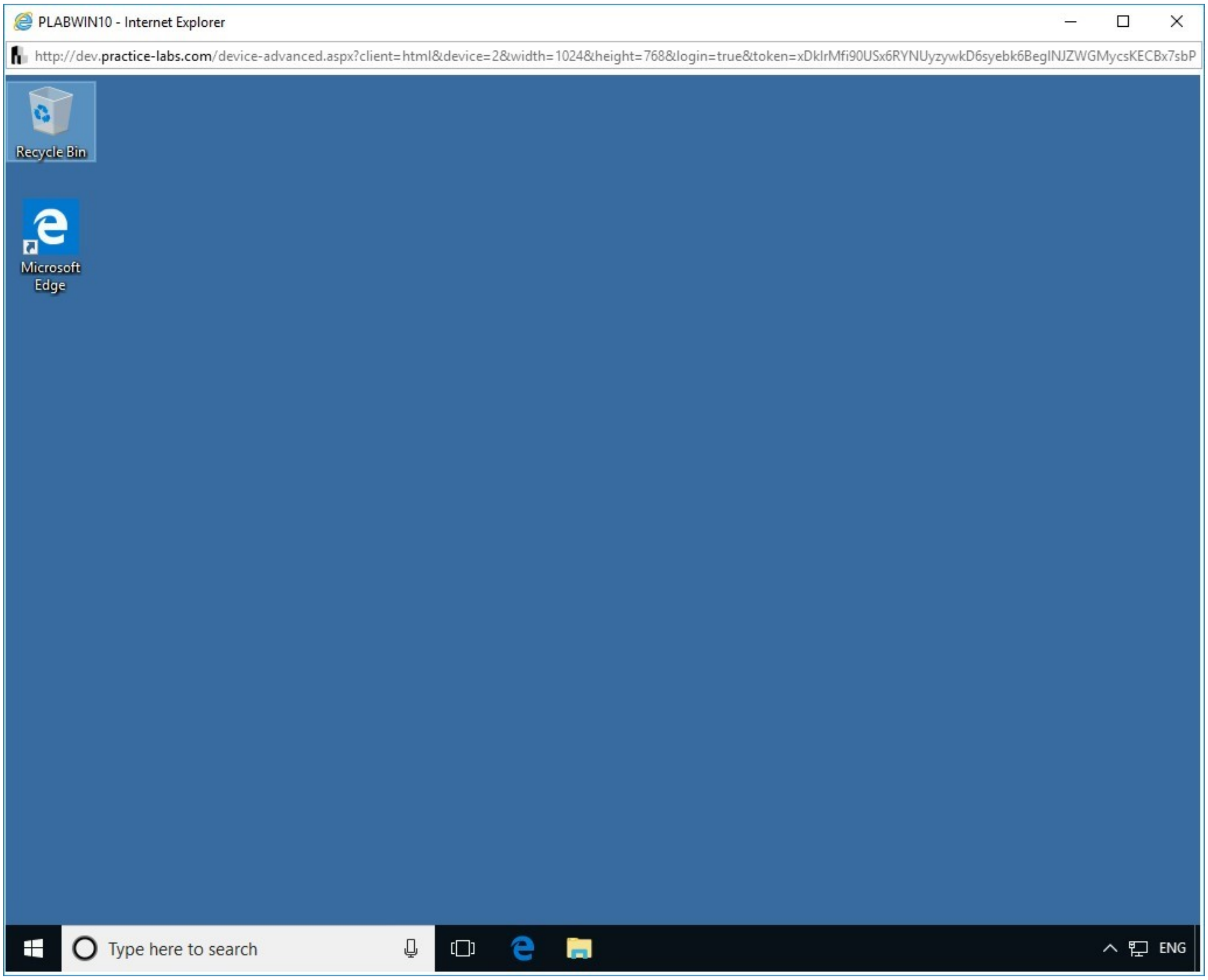

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDklrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP
Recycle Bin
Microsoft Edge
Type here to search
ENG

Figure 1.13 Screenshot of PLABWIN10: Showing the desktop of PLABWIN10.

Step 2

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

```
Internet Explorer
```

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

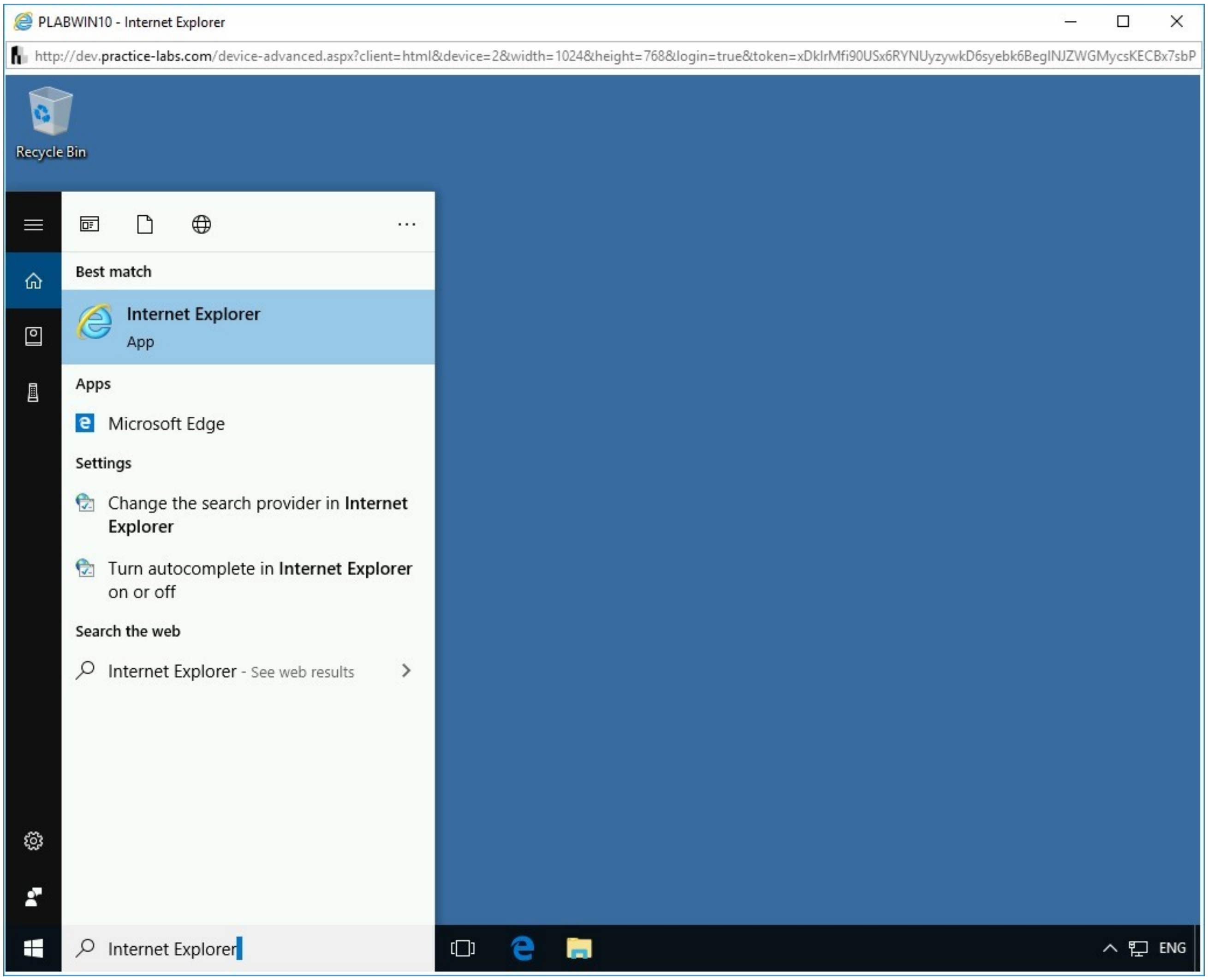
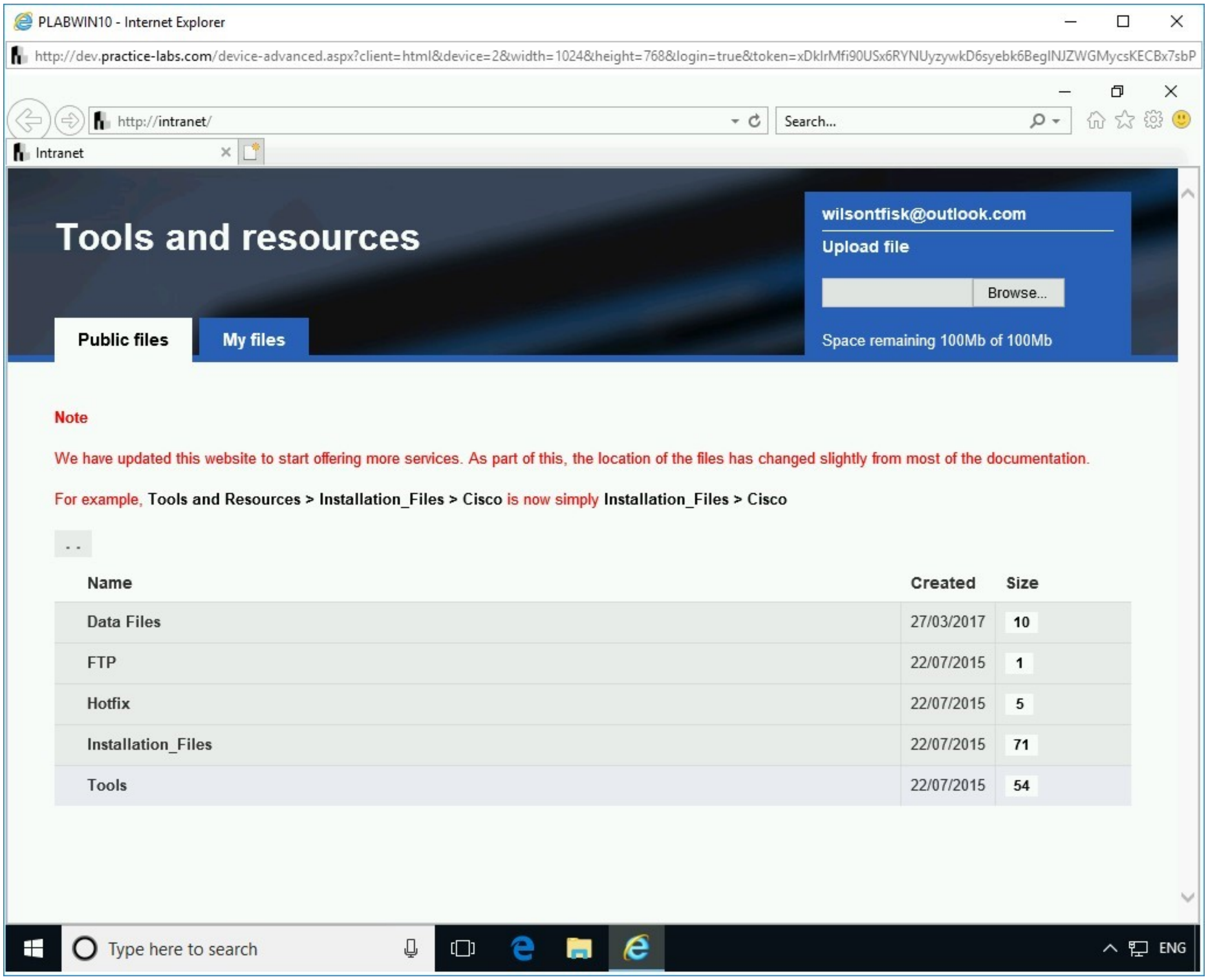

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDklrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP
Recycle Bin
Best match
Internet Explorer
App
Apps
Microsoft Edge
Settings
Change the search provider in Internet Explorer
Turn autocomplete in Internet Explorer on or off
Search the web
Internet Explorer - See web results
Internet Explorer
ENG

Figure 1.14 Screenshot of PLABWIN10: Selecting Internet Explorer from the search results.

Step 3

On the **Intranet** homepage, click **Tools**.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDkIrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP

http://intranet/

Note

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

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

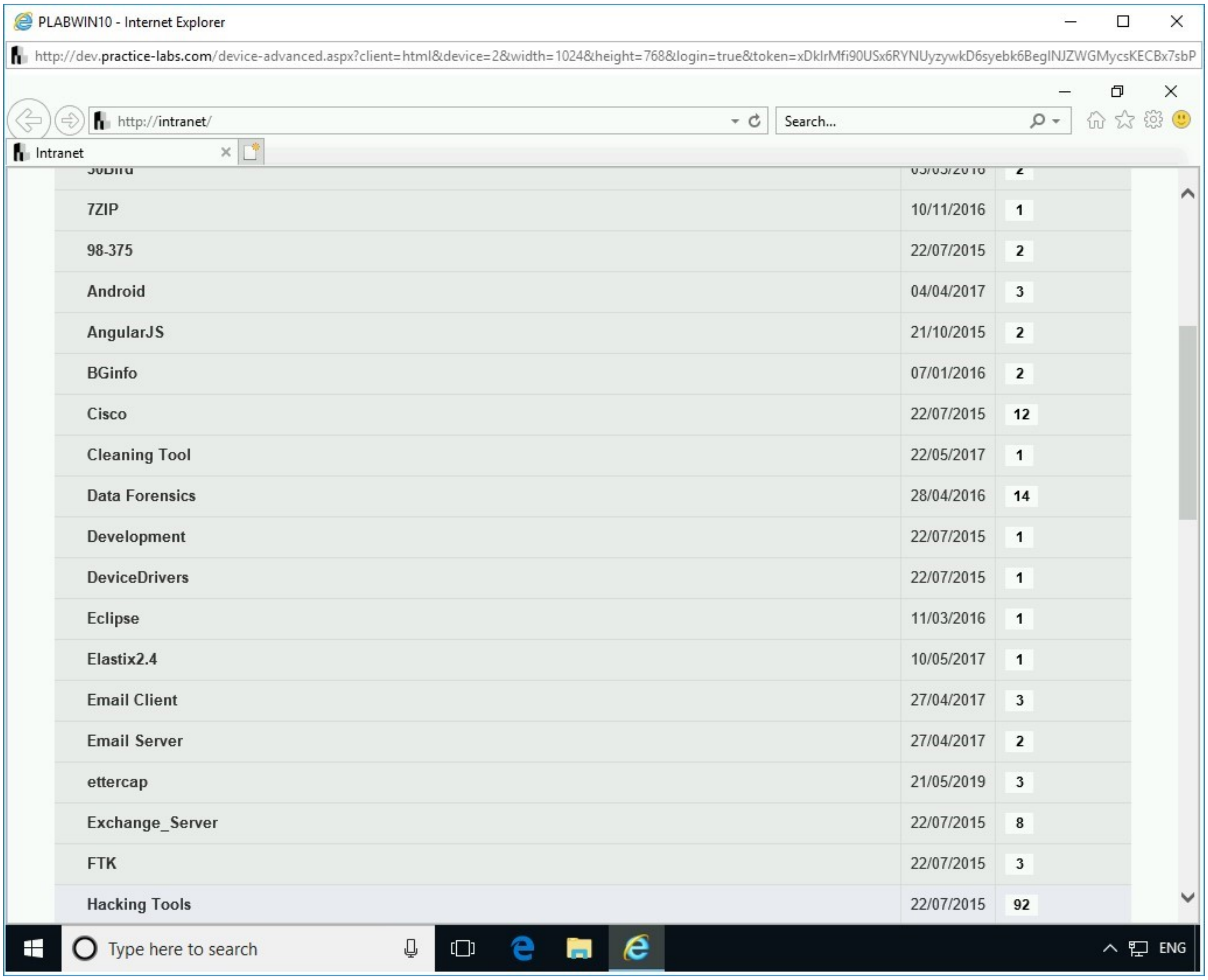
. .

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

Figure 1.15 Screenshot of PLABWIN10: Clicking Tools on the Intranet homepage.

Step 4

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



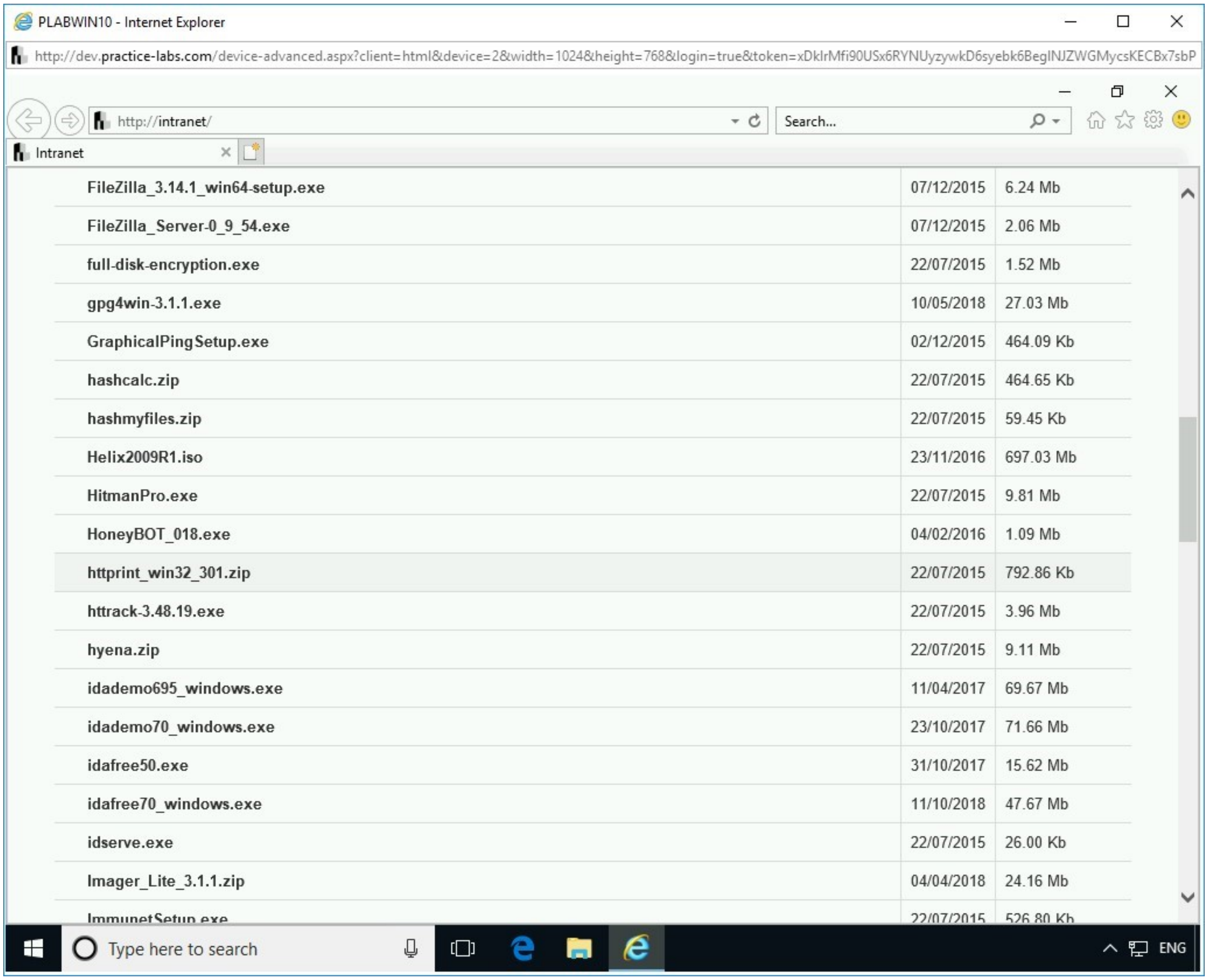
PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDkIrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP
http://intranet/
Search...
Intranet
Type here to search
ENG

3DBird	05/05/2016	2
7ZIP	10/11/2016	1
98-375	22/07/2015	2
Android	04/04/2017	3
AngularJS	21/10/2015	2
BGinfo	07/01/2016	2
Cisco	22/07/2015	12
Cleaning Tool	22/05/2017	1
Data Forensics	28/04/2016	14
Development	22/07/2015	1
DeviceDrivers	22/07/2015	1
Eclipse	11/03/2016	1
Elastix2.4	10/05/2017	1
Email Client	27/04/2017	3
Email Server	27/04/2017	2
ettercap	21/05/2019	3
Exchange_Server	22/07/2015	8
FTK	22/07/2015	3
Hacking Tools	22/07/2015	92

Figure 1.16 Screenshot of PLABWIN10: Clicking Tools on the Intranet homepage.

Step 5

Locate and click **httprint_win32_301.zip**.

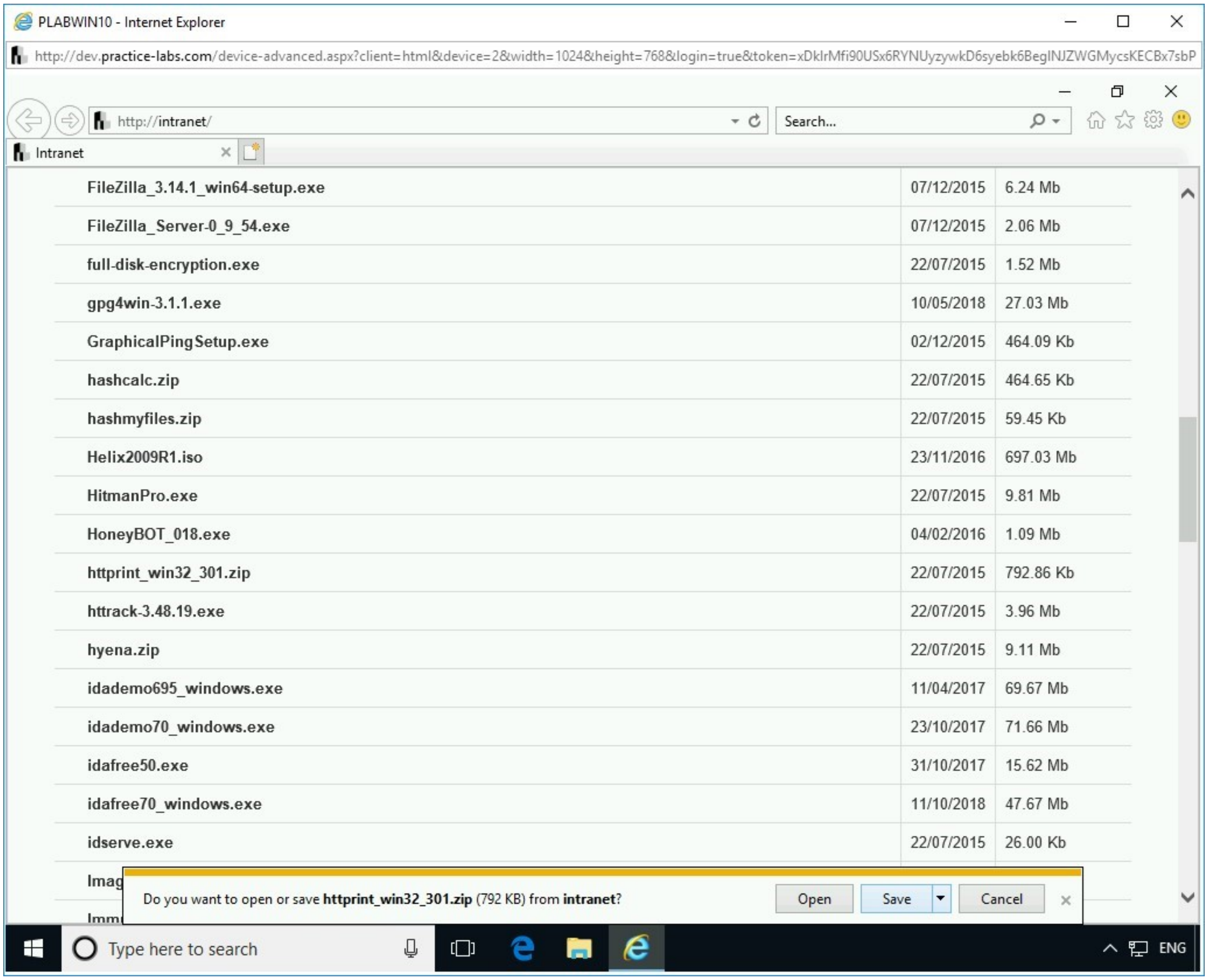

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDklrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP
http://intranet/
Search...
Intranet
Type here to search
ENG

FileZilla_3.14.1_win64-setup.exe	07/12/2015	6.24 Mb
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4win-3.1.1.exe	10/05/2018	27.03 Mb
GraphicalPingSetup.exe	02/12/2015	464.09 Kb
hashcalc.zip	22/07/2015	464.65 Kb
hashmyfiles.zip	22/07/2015	59.45 Kb
Helix2009R1.iso	23/11/2016	697.03 Mb
HitmanPro.exe	22/07/2015	9.81 Mb
HoneyBOT_018.exe	04/02/2016	1.09 Mb
httprint_win32_301.zip	22/07/2015	792.86 Kb
httrack-3.48.19.exe	22/07/2015	3.96 Mb
hyena.zip	22/07/2015	9.11 Mb
idademo695_windows.exe	11/04/2017	69.67 Mb
idademo70_windows.exe	23/10/2017	71.66 Mb
idafree50.exe	31/10/2017	15.62 Mb
idafree70_windows.exe	11/10/2018	47.67 Mb
idserve.exe	22/07/2015	26.00 Kb
Imager_Lite_3.1.1.zip	04/04/2018	24.16 Mb
ImmunetSetup.exe	22/07/2015	526.80 Kb

Figure 1.17 Screenshot of PLABWIN10: Clicking Tools on the Intranet homepage.

Step 6

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


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDklrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP
http://intranet/
Search...
Intranet
Open
Save
Cancel
Type here to search
ENG

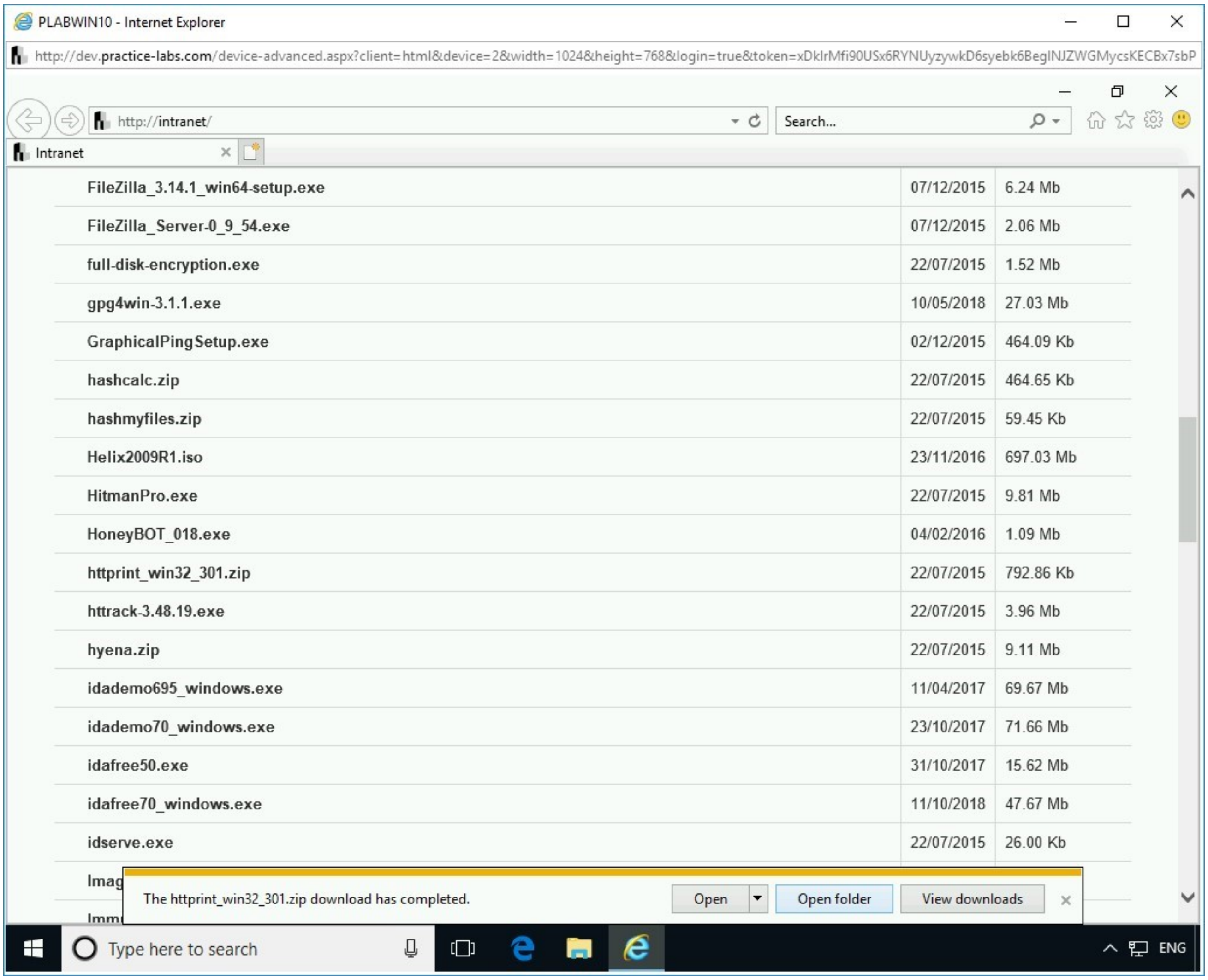
FileZilla_3.14.1_win64-setup.exe	07/12/2015	6.24 Mb
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4win-3.1.1.exe	10/05/2018	27.03 Mb
GraphicalPingSetup.exe	02/12/2015	464.09 Kb
hashcalc.zip	22/07/2015	464.65 Kb
hashmyfiles.zip	22/07/2015	59.45 Kb
Helix2009R1.iso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

Do you want to open or save **httprint_win32_301.zip** (792 KB) from **intranet**?

Figure 1.18 Screenshot of PLABWIN10: Clicking Tools on the Intranet homepage.

Step 7

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


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDkIrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP
http://intranet/
Search...
Intranet
Open
Open folder
View downloads
Type here to search
ENG

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

The httprint_win32_301.zip download has completed.

Figure 1.19 Screenshot of PLABWIN10: Clicking Tools on the Intranet homepage.

Step 8

The **File Explorer** window is now open. You will need to extract the files from the zip file.

Alert: If you run HTTPrint from the zip file, then it will not be able to load the signature file.

Right-click **httprint_win32_301** and select **Extract All**.

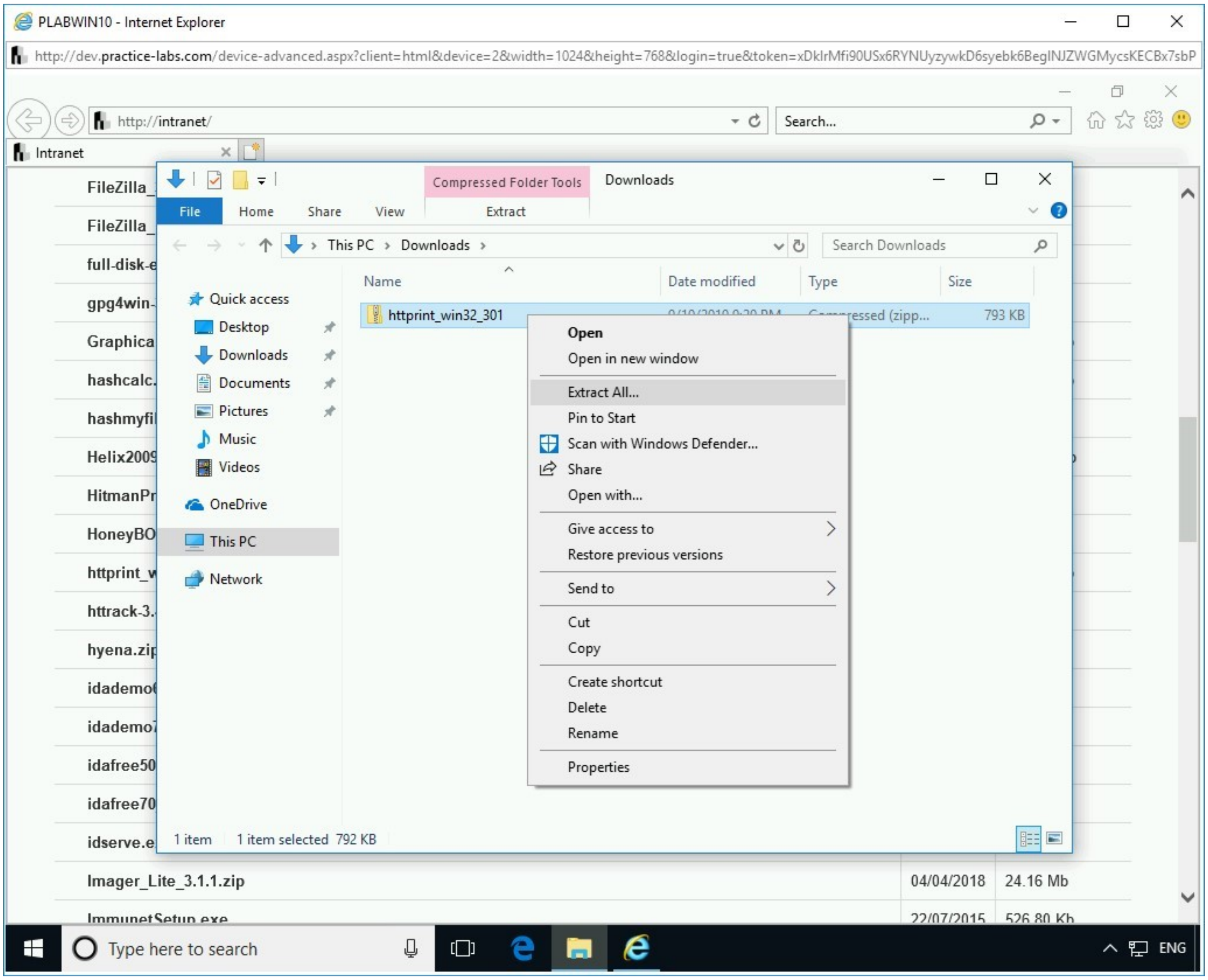
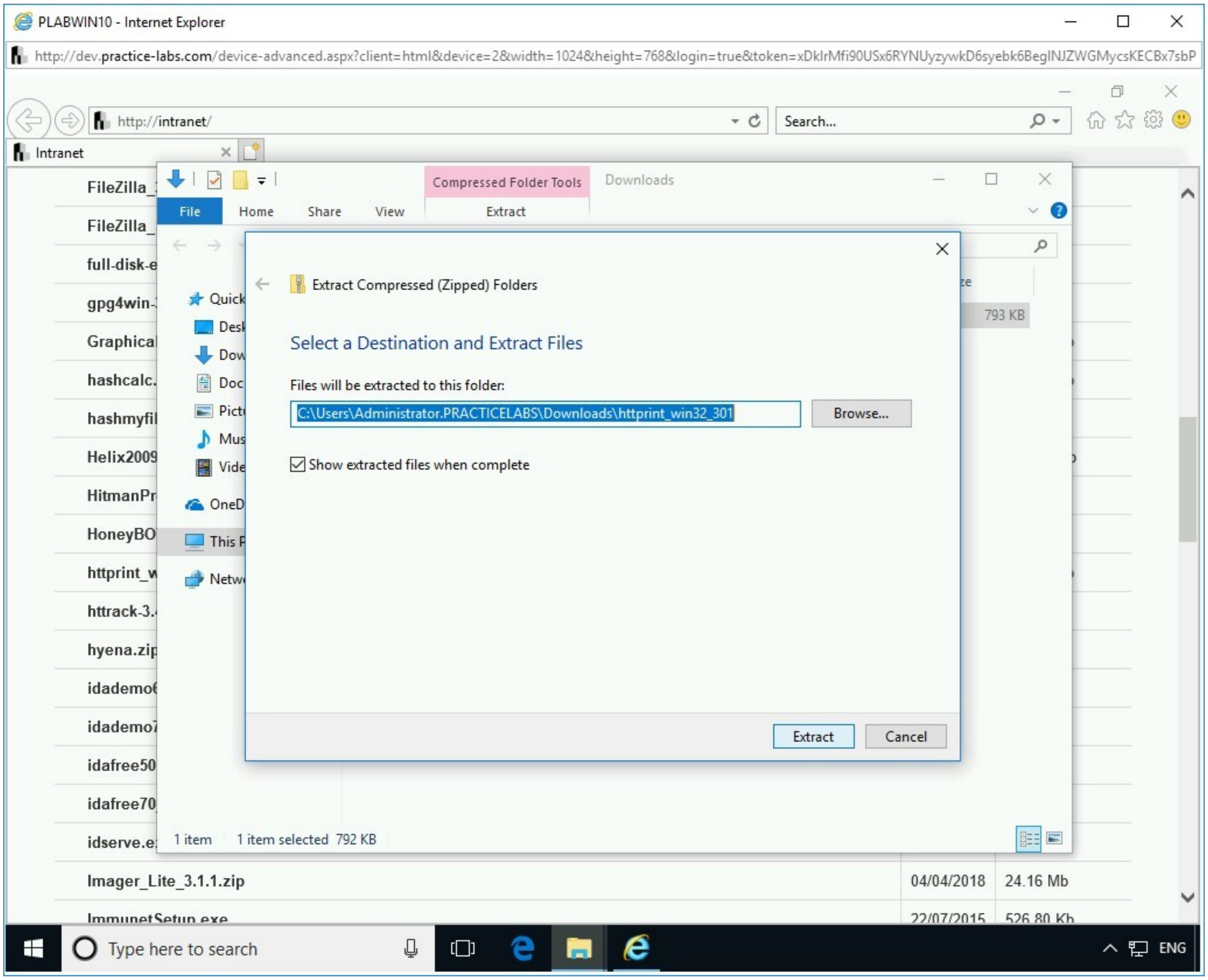


Figure 1.20 Screenshot of PLABWIN10: Selecting the Extract All option from the context menu.

Step 9

The **Extract Compressed (Zipped) Folders** dialog box is displayed. Keep the default path and click **Extract**.



Extract Compressed (Zipped) Folders

Select a Destination and Extract Files

Files will be extracted to this folder:

C:\Users\Administrator.PRACTICELABS\Downloads\httprint_win32_301

☑ Show extracted files when complete

Figure 1.21 Screenshot of PLABWIN10: Showing the Extract Compressed (Zipped) Folders dialog box and clicking the Extract button.

Step 10

Notice that a new **File Explorer** window is opened. Double-click the **httprint_301** folder.

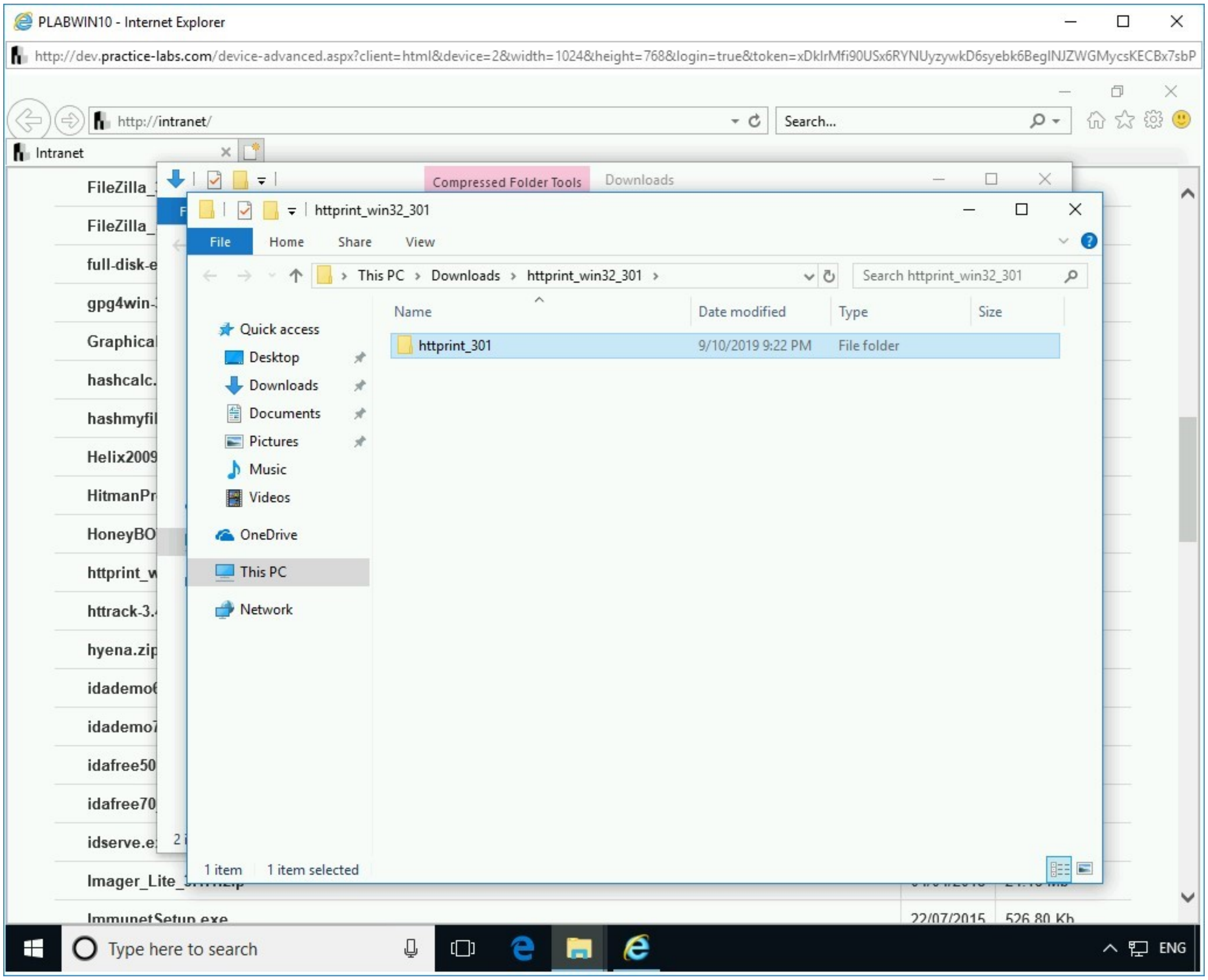
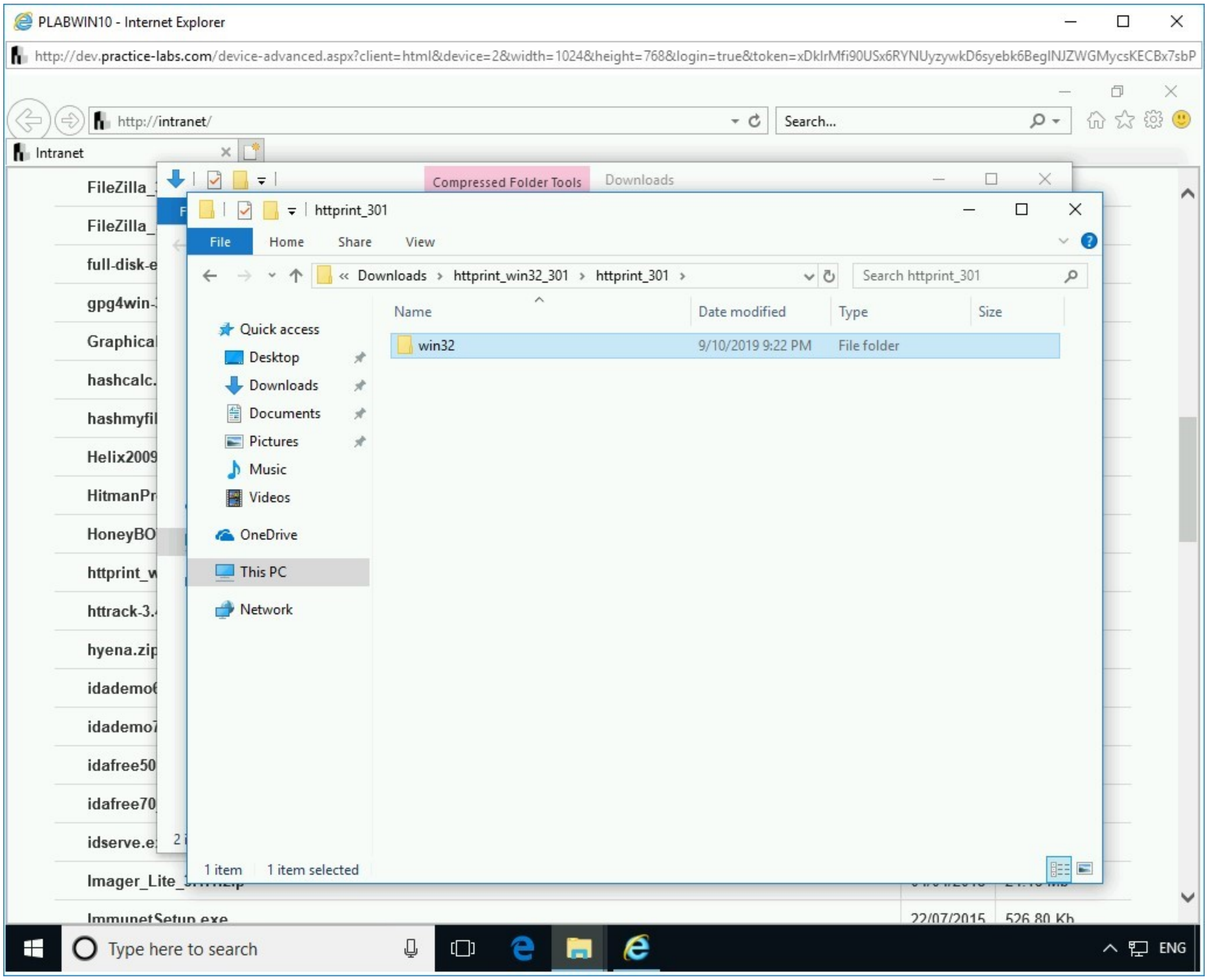


Figure 1.22 Screenshot of PLABWIN10: Double-clicking the httprint_301 folder.

Step 11

Double-click the **win32** folder.



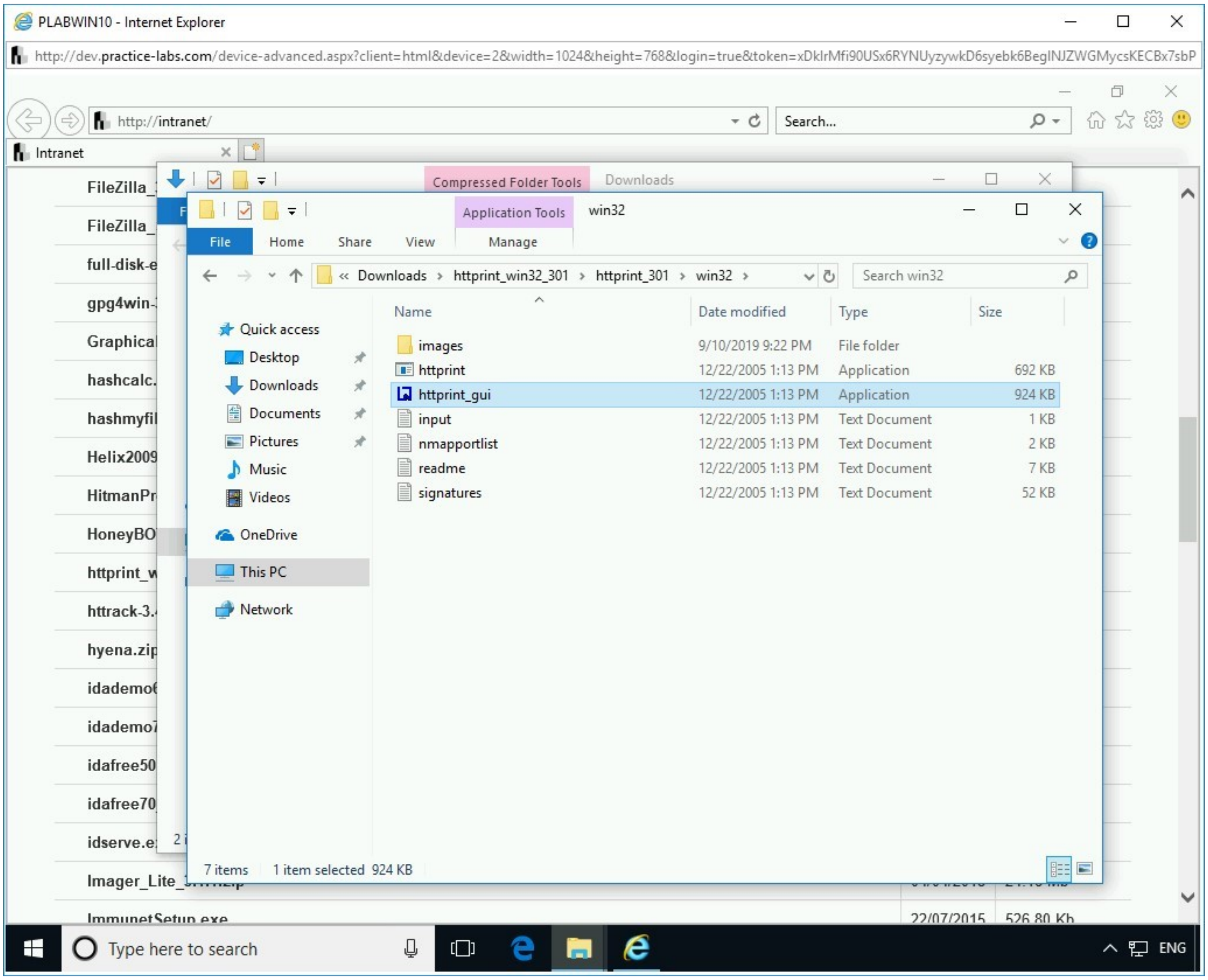
PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDklrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP
http://intranet/
Search...
Intranet
Compressed Folder Tools
Downloads
httprint_301
File
Home
Share
View
« Downloads › httprint_win32_301 › httprint_301 ›
Search httprint_301
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
1 item
1 item selected
Type here to search
ENG

Name	Date modified	Type	Size
win32	9/10/2019 9:22 PM	File folder	

Figure 1.23 Screenshot of PLABWIN10: Double-clicking the win32 folder.

Step 12

You are now in the **httprint_301\win32** folder. Double-click **httprint_gui**.



Downloads › httprint_win32_301 › httprint_301 › win32

Name	Date modified	Type	Size
images	9/10/2019 9:22 PM	File folder	
httprint	12/22/2005 1:13 PM	Application	692 KB
httprint_gui	12/22/2005 1:13 PM	Application	924 KB
input	12/22/2005 1:13 PM	Text Document	1 KB
nmapportlist	12/22/2005 1:13 PM	Text Document	2 KB
readme	12/22/2005 1:13 PM	Text Document	7 KB
signatures	12/22/2005 1:13 PM	Text Document	52 KB

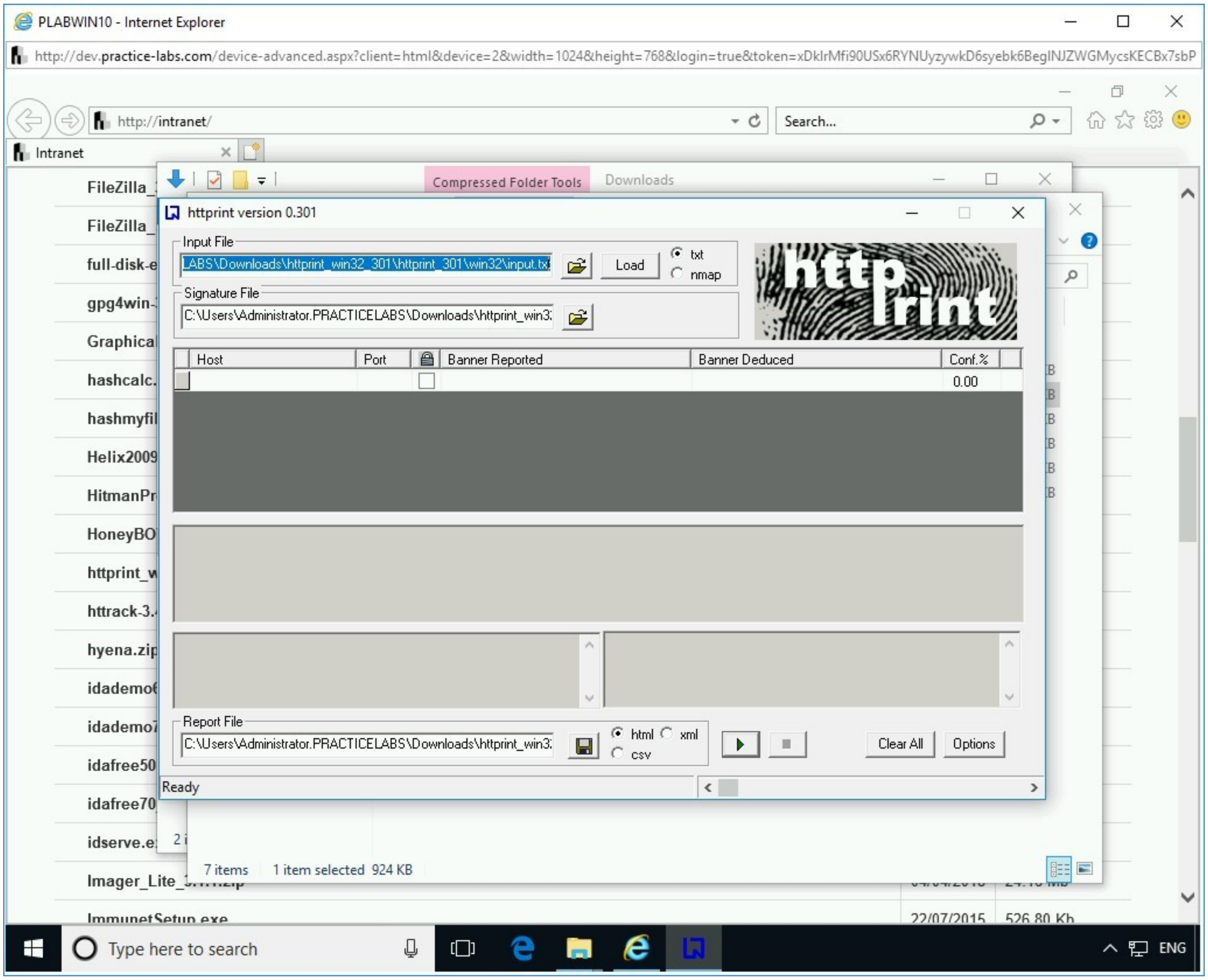
7 items   1 item selected 924 KB

Figure 1.24 Screenshot of PLABWIN10: Double-clicking httprint_gui..

Step 13

***Note:** If the Open File - Security Warning dialog box is displayed, click Run.*

The **httprint version 0.301** window is displayed.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDklrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP
http://intranet/
Search...
Intranet
Compressed Folder Tools
Downloads
httprint version 0.301
Load
Clear All
Options
7 items
1 item selected 924 KB
Type here to search
ENG

Input File: LABS\Downloads\httprint_win32_301\httprint_301\win32\input.txt ● txt ○ nmap

Signature File: C:\Users\Administrator.PRACTICELABS\Downloads\httprint_win3:

Host	Port		Banner Reported	Banner Deduced	Conf.%
		□			0.00

Report File: C:\Users\Administrator.PRACTICELABS\Downloads\httprint_win3: ● html ○ xml ○ csv

Ready

Figure 1.25 Screenshot of PLABWIN10: Showing the httprint version 0.301 window.

Step 14

Enter the following information:

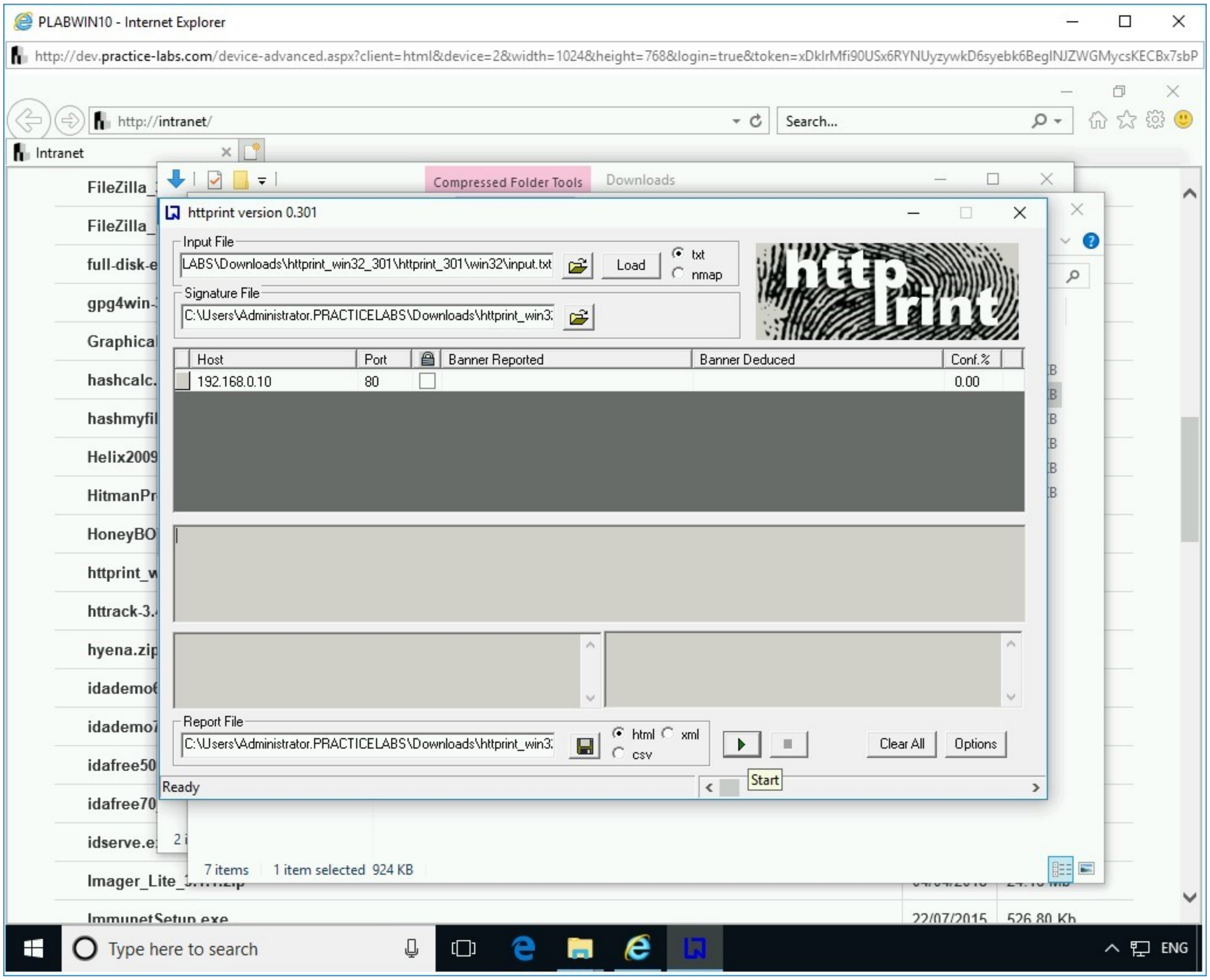
Host:

```
192.168.0.10
```

Port:

```
80
```

Click **Start**.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDkIrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP

httprint version 0.301

Input File: LABS\Downloads\httprint_win32_301\httprint_301\win32\input.txt

● txt ○ nmap

Signature File: C:\Users\Administrator.PRACTICELABS\Downloads\httprint_win3:

Host	Port	Banner Reported	Banner Deduced	Conf.%
192.168.0.10	80			0.00

Report File: C:\Users\Administrator.PRACTICELABS\Downloads\httprint_win3:

● html ○ xml ○ csv

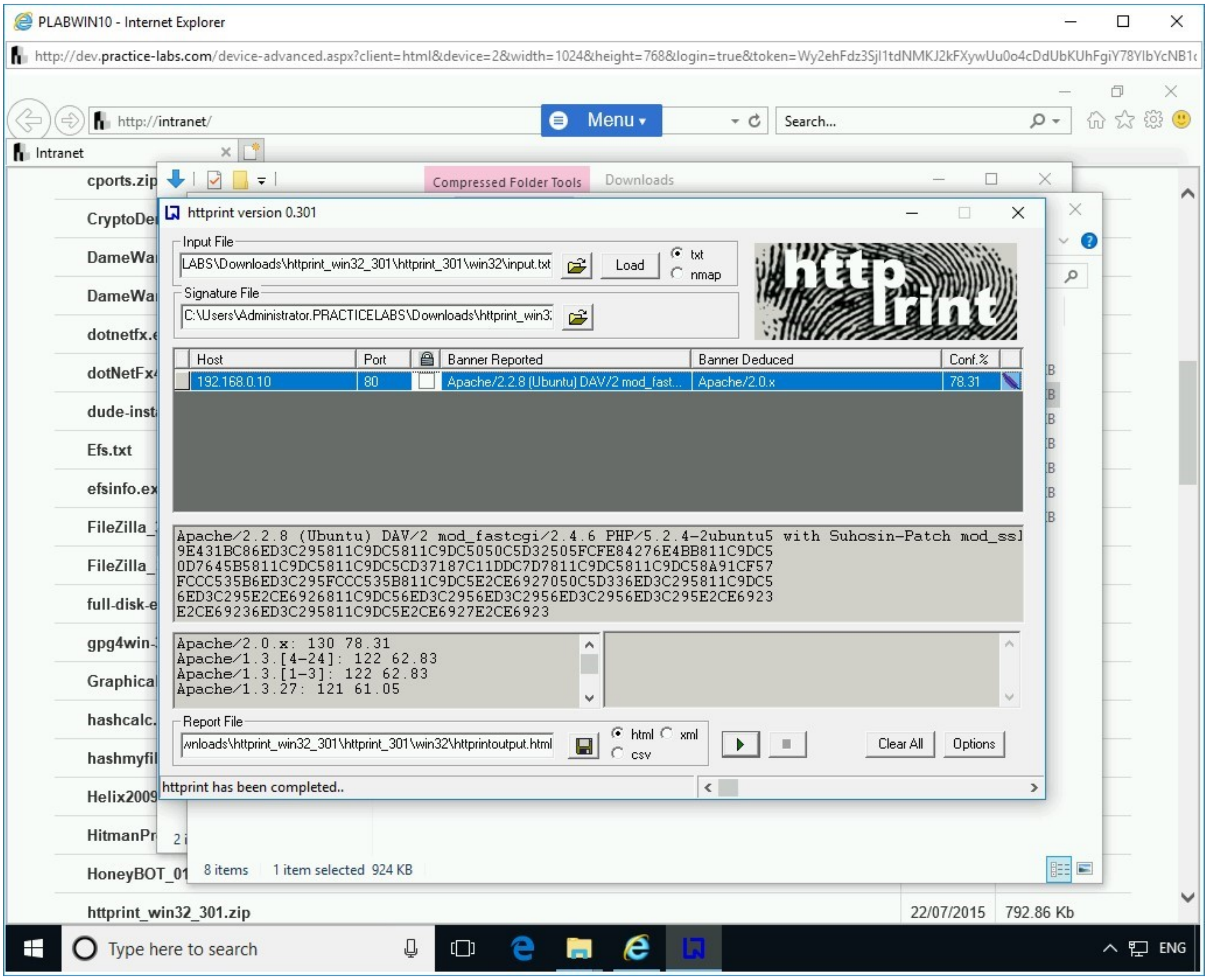
Ready

Figure 1.26 Screenshot of PLABWIN10: Entering the IP address in the Host column and clicking Start.

Step 15

The **httprint_gui** dialog box is displayed. It prompts with a message that **httprint** is now completed. Click **OK**.

Note that a set of parameters are displayed as a result.



Input File: LABS\Downloads\httprint_win32_301\httprint_301\win32\input.txt ● txt ○ nmap

Signature File: C:\Users\Administrator.PRACTICELABS\Downloads\httprint_win3:

Host	Port		Banner Reported	Banner Deduced	Conf.%
192.168.0.10	80	□	Apache/2.2.8 (Ubuntu) DAV/2 mod_fast...	Apache/2.0.x	78.31

```
Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl
9E431BC86ED3C295811C9DC5811C9DC5050C5D32505FCFE84276E4BB811C9DC5
0D7645B5811C9DC5811C9DC5CD37187C11DDC7D7811C9DC5811C9DC58A91CF57
FCCC535B6ED3C295FCCC535B811C9DC5E2CE6927050C5D336ED3C295811C9DC5
6ED3C295E2CE6926811C9DC56ED3C2956ED3C2956ED3C2956ED3C295E2CE6923
E2CE69236ED3C295811C9DC5E2CE6927E2CE6923
```

```
Apache/2.0.x: 130 78.31
Apache/1.3.[4-24]: 122 62.83
Apache/1.3.[1-3]: 122 62.83
Apache/1.3.27: 121 61.05
```

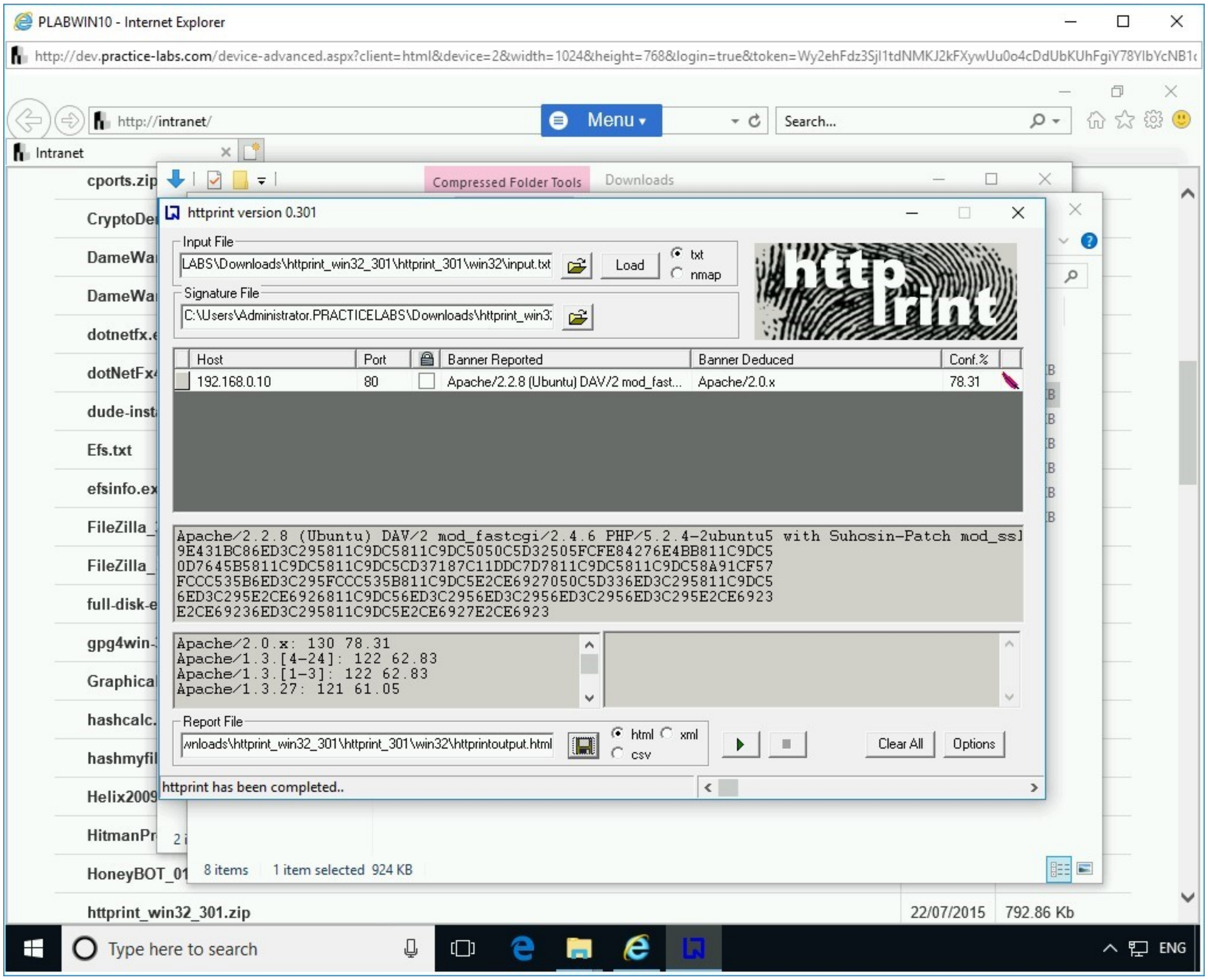
Report File: wnloads\httprint_win32_301\httprint_301\win32\httprintoutput.html ● html ○ xml ○ csv

httprint has been completed..

Figure 1.27 Screenshot of PLABWIN10: Showing the output with the Webserver information.

Step 16

Let’s save the file. Click the **floppy disk** icon.



Input File: LABS\Downloads\httprint_win32_301\httprint_301\win32\input.txt ● txt ○ nmap

Signature File: C:\Users\Administrator.PRACTICELABS\Downloads\httprint_win3:

Host	Port		Banner Reported	Banner Deduced	Conf.%
192.168.0.10	80	□	Apache/2.2.8 (Ubuntu) DAV/2 mod_fast...	Apache/2.0.x	78.31

```
Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl
9E431BC86ED3C295811C9DC5811C9DC5050C5D32505FCFE84276E4BB811C9DC5
0D7645B5811C9DC5811C9DC5CD37187C11DDC7D7811C9DC5811C9DC58A91CF57
FCCC535B6ED3C295FCCC535B811C9DC5E2CE6927050C5D336ED3C295811C9DC5
6ED3C295E2CE6926811C9DC56ED3C2956ED3C2956ED3C2956ED3C295E2CE6923
E2CE69236ED3C295811C9DC5E2CE6927E2CE6923
```

```
Apache/2.0.x: 130 78.31
Apache/1.3.[4-24]: 122 62.83
Apache/1.3.[1-3]: 122 62.83
Apache/1.3.27: 121 61.05
```

Report File: wnloads\httprint_win32_301\httprint_301\win32\httprintoutput.html ● html ○ xml ○ csv

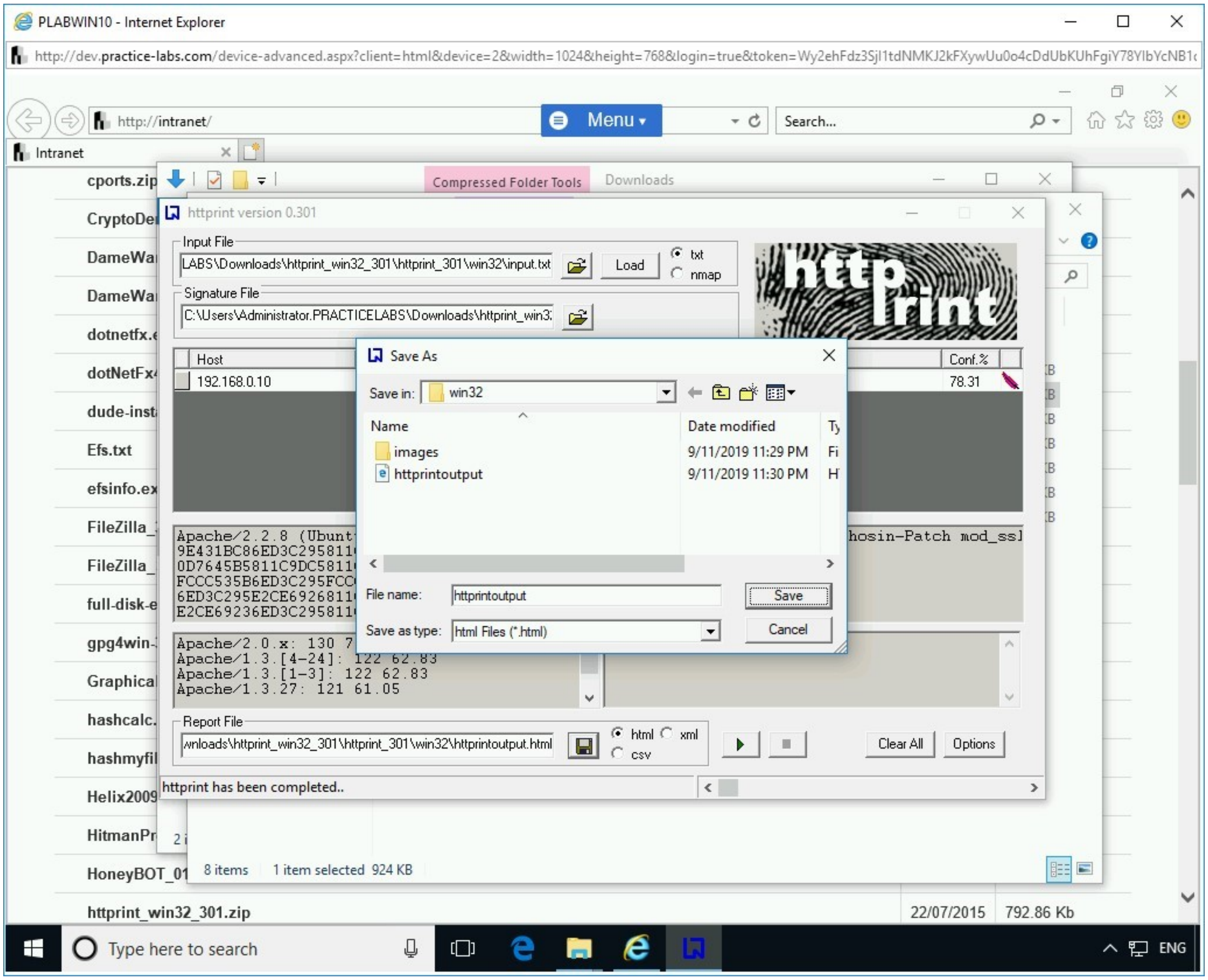
httprint has been completed..

Figure 1.28 Screenshot of PLABWIN10: Clicking the Floppy icon to save the file.

Step 17

The **Save As** dialog box is displayed. Keep the default name and click **Save**.

> **Note**: *Make sure you note the path where you are downloading the report. If prompted to overwrite an existing report, go ahead and overwrite it. Else, you can save the report with a new name.*


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=Wy2ehFdz3SjI1tdNMKJ2kFXywUu0o4cDdUbKUhFgiY78YlbYcNB1
http://intranet/
Menu
Search...
Intranet
Compressed Folder Tools
Downloads
httprint version 0.301
Save As
Clear All
Options
Type here to search
ENG

Input File: LABS\Downloads\httprint_win32_301\httprint_301\win32\input.txt
Load
● txt ○ nmap

Signature File: C:\Users\Administrator.PRACTICELABS\Downloads\httprint_win3:

Host	Conf.%
192.168.0.10	78.31

```
Apache/2.2.8 (Ubunt
9E431BC86ED3C295811
0D7645B5811C9DC5811
FCCC535B6ED3C295FCC
6ED3C295E2CE6926811
E2CE69236ED3C295811
```

```
hosin-Patch mod_ssl
```

```
Apache/2.0.x: 130 7
Apache/1.3.[4-24]: 122 62.83
Apache/1.3.[1-3]: 122 62.83
Apache/1.3.27: 121 61.05
```

Save in: win32

Name	Date modified	Ty
images	9/11/2019 11:29 PM	Fi
httprintoutput	9/11/2019 11:30 PM	H

File name: httprintoutput
Save as type: html Files (*.html)
Save
Cancel

Report File: wnloads\httprint_win32_301\httprint_301\win32\httprintoutput.html
● html ○ xml ○ csv

httprint has been completed..

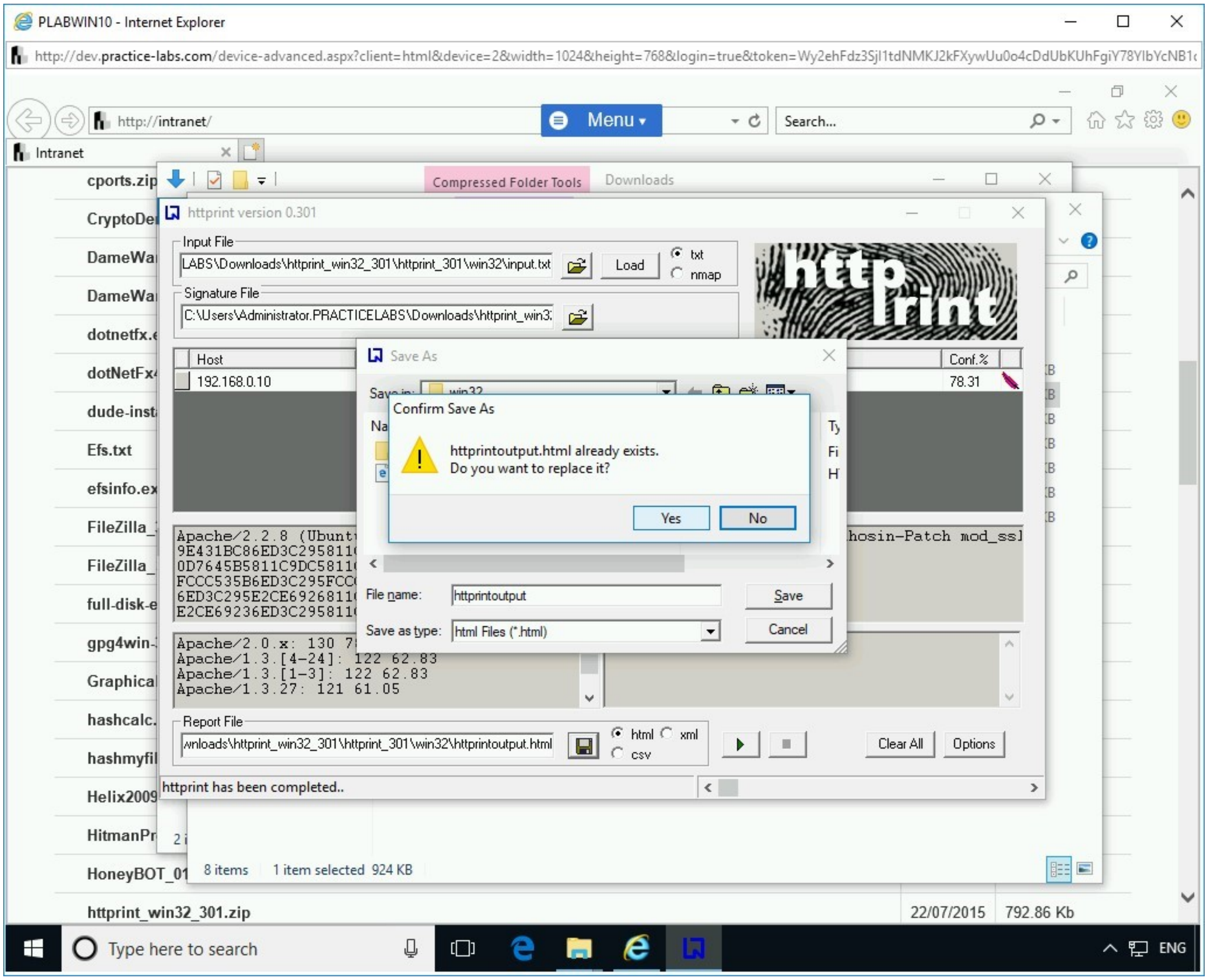
8 items 1 item selected 924 KB

cports.zip
CryptoDe
DameWa
DameWa
dotnetfx.
dotNetFx
dude-inst
Efs.txt
efsinfo.ex
FileZilla_
FileZilla_
full-disk-e
gpg4win-
Graphica
hashcalc.
hashmyfil
Helix2009
HitmanPr
HoneyBOT_01
httprint_win32_301.zip 22/07/2015 792.86 Kb

Figure 1.29 Screenshot of PLABWIN10: Saving the output in the Save As dialog box and clicking Save.

Step 18

When prompted to overwrite the existing file, click **Yes**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=Wy2ehFdz3SjI1tdNMKJ2kFXywUu0o4cDdUbKUhFgiY78YlbYcNB1
http://intranet/
Menu
Search...
Intranet
Compressed Folder Tools
Downloads
httprint version 0.301
Save As
Type here to search
ENG

Input File: LABS\Downloads\httprint_win32_301\httprint_301\win32\input.txt

Load ● txt ○ nmap

Signature File: C:\Users\Administrator.PRACTICELABS\Downloads\httprint_win3

Host	Conf.%
192.168.0.10	78.31

```
Apache/2.2.8 (Ubunt                                   hosin-Patch mod_ssl
9E431BC86ED3C295811
0D7645B5811C9DC5811
FCCC535B6ED3C295FCC
6ED3C295E2CE6926811
E2CE69236ED3C295811
```

```
Apache/2.0.x: 130 7
Apache/1.3.[4-24]: 122 62.83
Apache/1.3.[1-3]: 122 62.83
Apache/1.3.27: 121 61.05
```

Confirm Save As

httprintoutput.html already exists.
Do you want to replace it?

Yes | No

Save in: win32

File name: httprintoutput

Save as type: html Files (*.html)

Save | Cancel

Report File: wnloads\httprint_win32_301\httprint_301\win32\httprintoutput.html

● html ○ xml ○ csv

Clear All | Options

httprint has been completed..

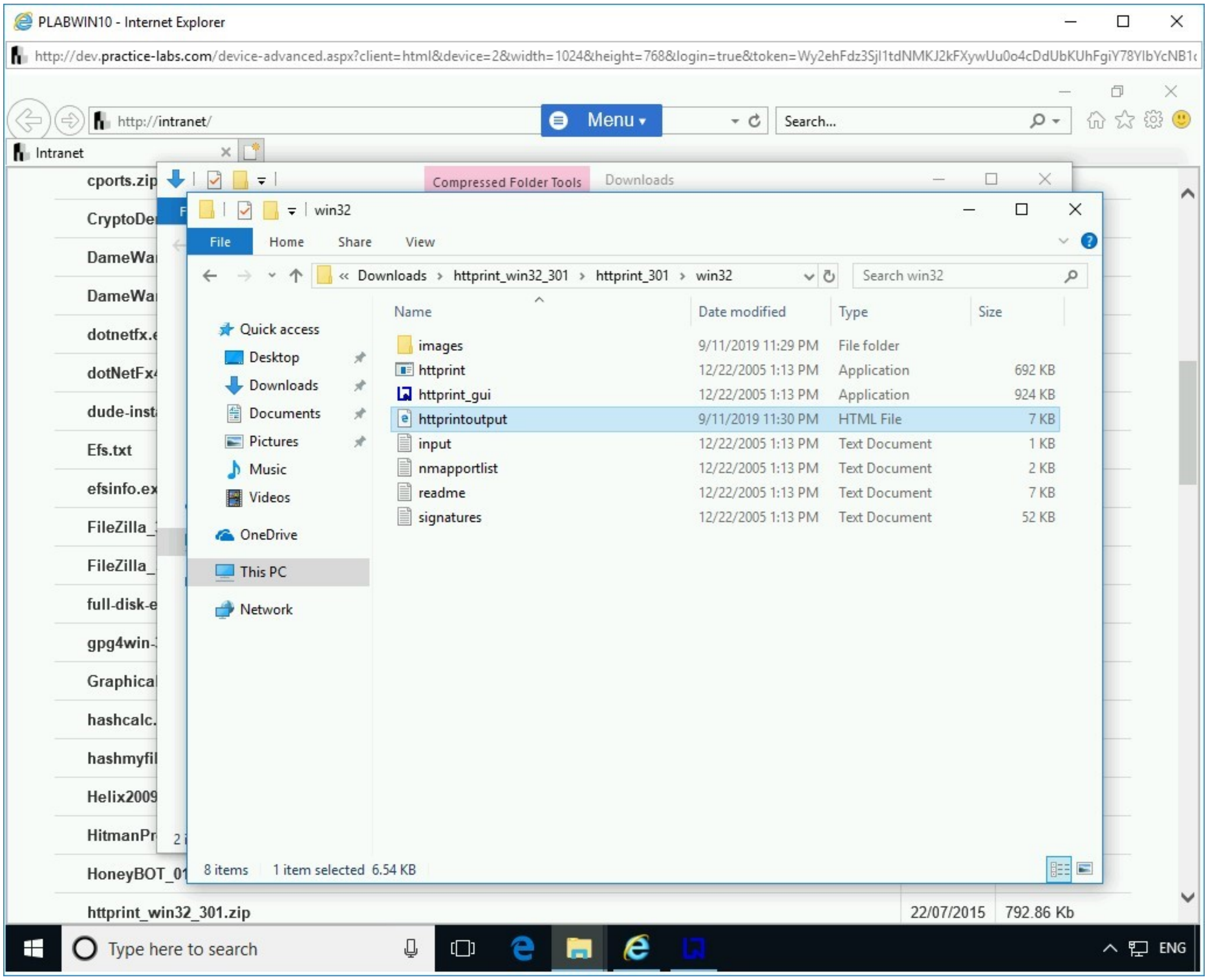
8 items   1 item selected 924 KB

cports.zip		
CryptoDe		
DameWa		
DameWa		
dotnetfx.		
dotNetFx		
dude-inst		
Efs.txt		
efsinfo.ex		
FileZilla_		
FileZilla_		
full-disk-e		
gpg4win-		
Graphica		
hashcalc.		
hashmyfil		
Helix2009		
HitmanPr		
HoneyBOT_01		
httprint_win32_301.zip	22/07/2015	792.86 Kb

Figure 1.30 Screenshot of PLABWIN10: Clicking Tools on the Intranet homepage.

Step 19

Minimize **HTTPrint** and navigate to the directory where you saved the report. Double-click the file to open it.



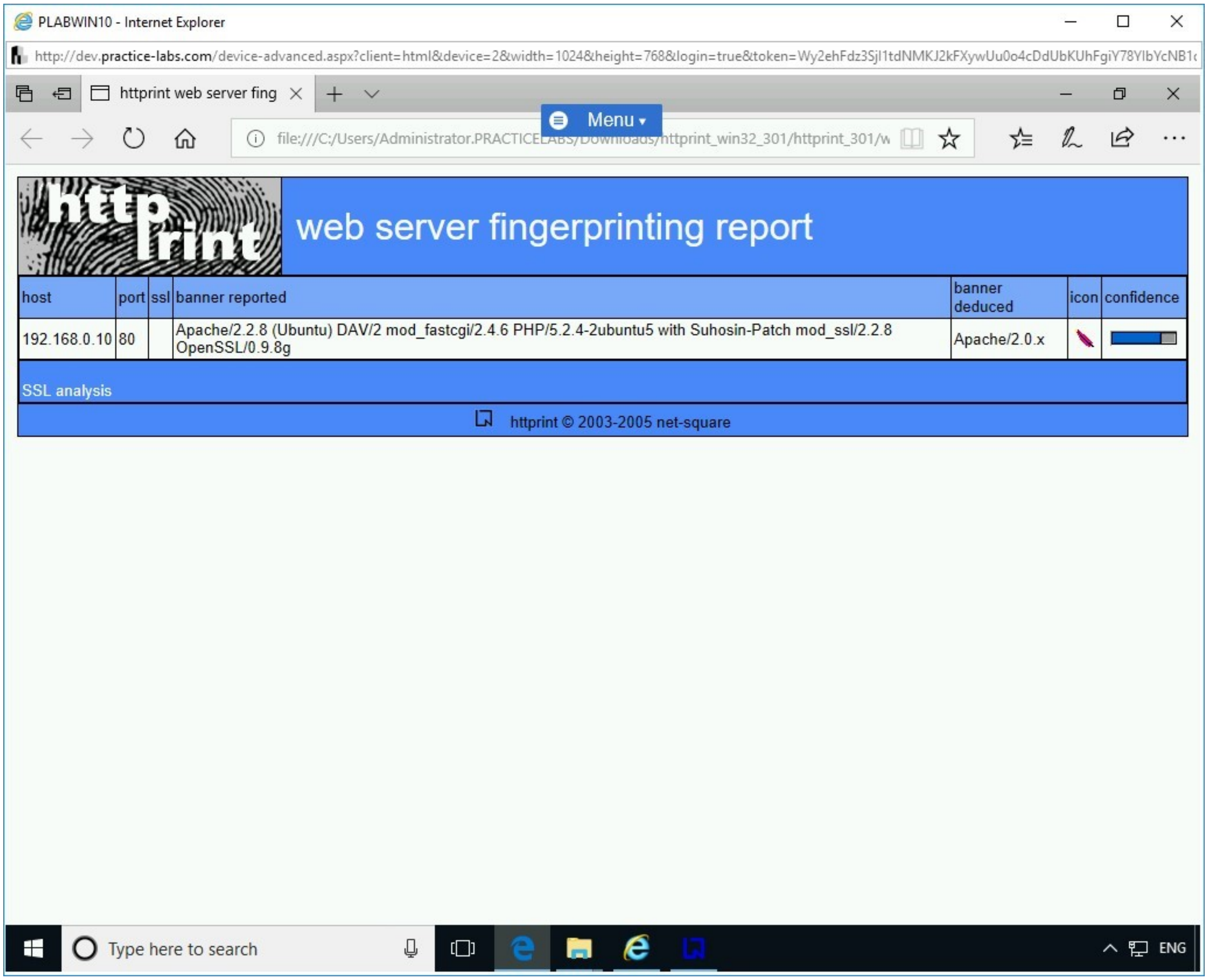
Name	Date modified	Type	Size
images	9/11/2019 11:29 PM	File folder	
httprint	12/22/2005 1:13 PM	Application	692 KB
httprint_gui	12/22/2005 1:13 PM	Application	924 KB
httprintoutput	9/11/2019 11:30 PM	HTML File	7 KB
input	12/22/2005 1:13 PM	Text Document	1 KB
nmapportlist	12/22/2005 1:13 PM	Text Document	2 KB
readme	12/22/2005 1:13 PM	Text Document	7 KB
signatures	12/22/2005 1:13 PM	Text Document	52 KB

Figure 1.31 Screenshot of PLABWIN10: Navigating to the win32 directory and double-clicking the HTML file.

Step 20

The **Internet Explorer** opens the report since it is in the **HTML** format.

It is the same information that you viewed within the **HTTPrint** tool. Close the **Edge** browser.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=Wy2ehFdz3SjI1tdNMKJ2kFXywUu0o4cDdUbKUhFgiY78YIbYcNB1
httprint web server fing
Menu
file:///C:/Users/Administrator.PRACTICELABS/Downloads/httprint_win32_301/httprint_301/w
httprint
Type here to search
ENG

web server fingerprinting report

host	port	ssl	banner reported	banner deduced	icon	confidence
192.168.0.10	80		Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g	Apache/2.0.x		

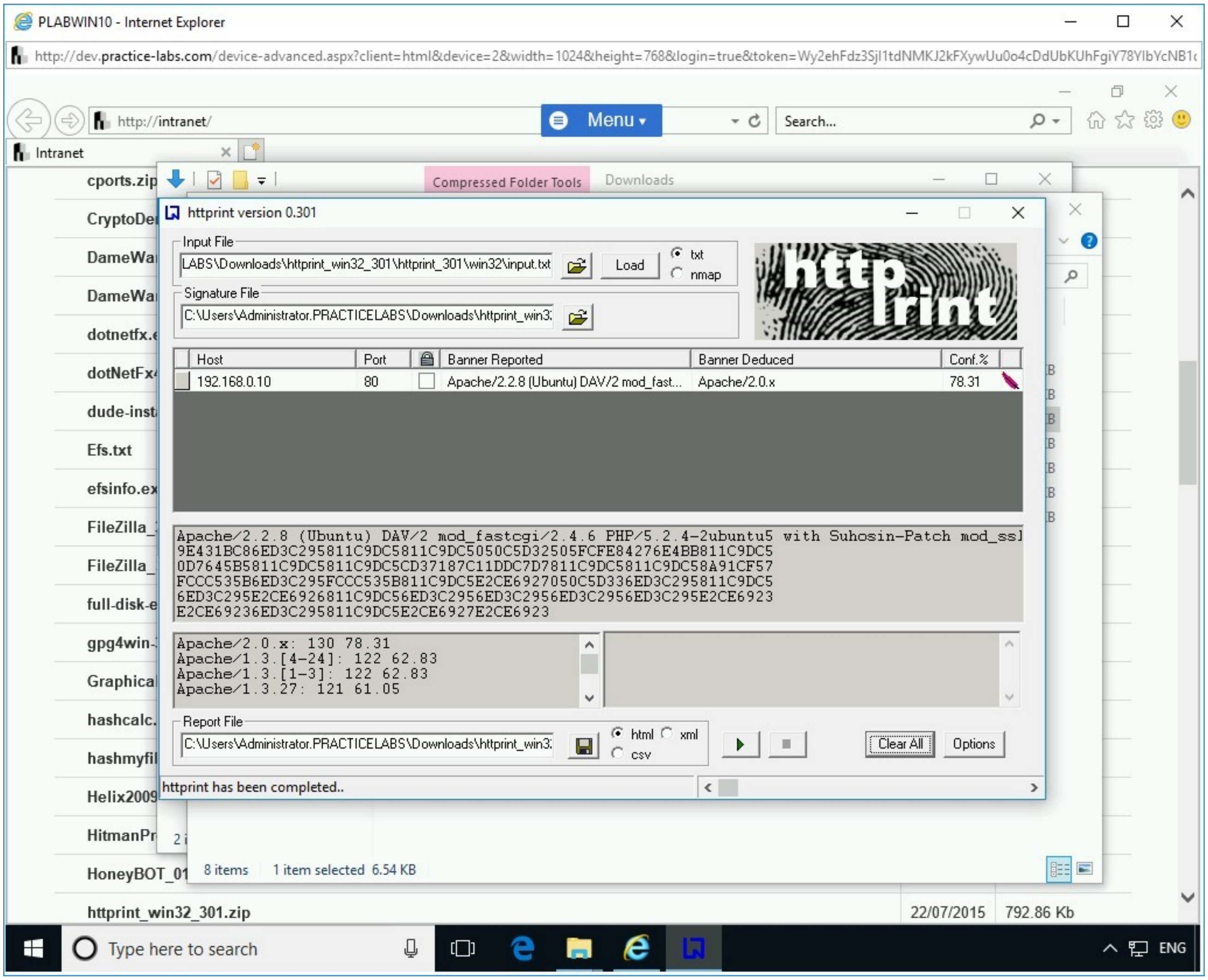
SSL analysis

httprint © 2003-2005 net-square

Figure 1.32 Screenshot of PLABWIN10: Showing the Webserver enumeration details in an HTML file.

Step 21

Switch back to the **HTTPrint** tool. Click **Clear All**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=Wy2ehFdz3Sjl1tdNMKJ2kFXywUu0o4cDdUbKUhFgiY78YlbYcNB1
http://intranet/
Menu
Search...
Intranet
Compressed Folder Tools
Downloads
httprint version 0.301
http print

Input File: LABS\Downloads\httprint_win32_301\httprint_301\win32\input.txt   Load   ● txt ○ nmap

Signature File: C:\Users\Administrator.PRACTICELABS\Downloads\httprint_win3:

Host	Port	🔒	Banner Reported	Banner Deduced	Conf.%
192.168.0.10	80	□	Apache/2.2.8 (Ubuntu) DAV/2 mod_fast...	Apache/2.0.x	78.31

```
Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl
9E431BC86ED3C295811C9DC5811C9DC5050C5D32505FCFE84276E4BB811C9DC5
0D7645B5811C9DC5811C9DC5CD37187C11DDC7D7811C9DC5811C9DC58A91CF57
FCCC535B6ED3C295FCCC535B811C9DC5E2CE6927050C5D336ED3C295811C9DC5
6ED3C295E2CE6926811C9DC56ED3C2956ED3C2956ED3C2956ED3C295E2CE6923
E2CE69236ED3C295811C9DC5E2CE6927E2CE6923
```

```
Apache/2.0.x: 130 78.31
Apache/1.3.[4-24]: 122 62.83
Apache/1.3.[1-3]: 122 62.83
Apache/1.3.27: 121 61.05
```

Report File: C:\Users\Administrator.PRACTICELABS\Downloads\httprint_win3:   ● html ○ xml ○ csv

httprint has been completed..

Figure 1.33 Screenshot of PLABWIN10: Clicking Tools on the Intranet homepage.

Step 22

Enter the following information:

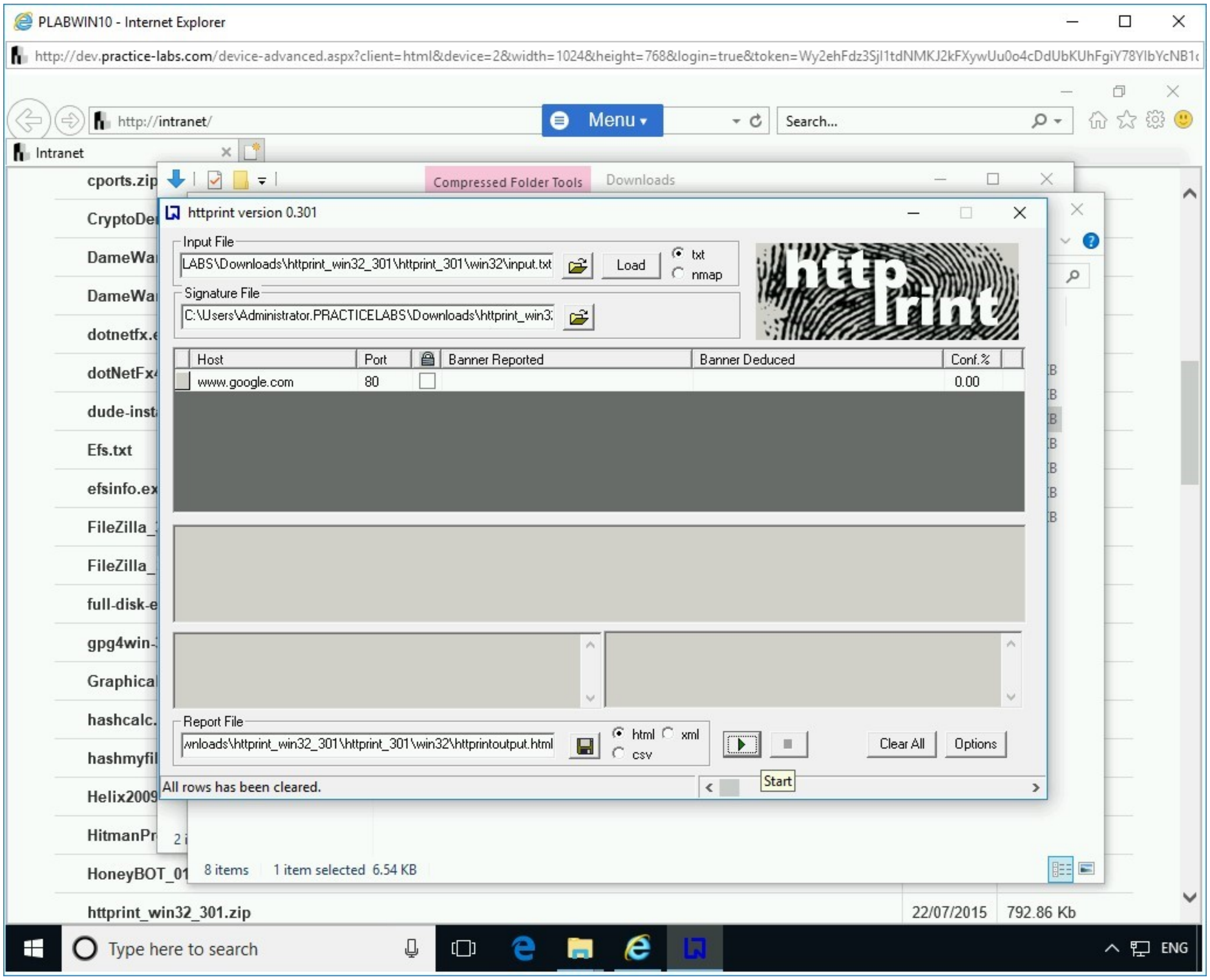
Host:

```
www.google.com
```

Port:

```
80
```

Click **Start**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=Wy2ehFdz3Sjl1tdNMKJ2kFXywUu0o4cDdUbKUhFgiY78YlbYcNB1
http://intranet/
Menu
Search...
Intranet
Compressed Folder Tools
Downloads
httprint version 0.301
Load
Clear All
Options
Start
8 items
1 item selected 6.54 KB
Type here to search
ENG

Input File: LABS\Downloads\httprint_win32_301\httprint_301\win32\input.txt ● txt ○ nmap

Signature File: C:\Users\Administrator.PRACTICELABS\Downloads\httprint_win3:

Host	Port		Banner Reported	Banner Deduced	Conf.%
www.google.com	80	□			0.00

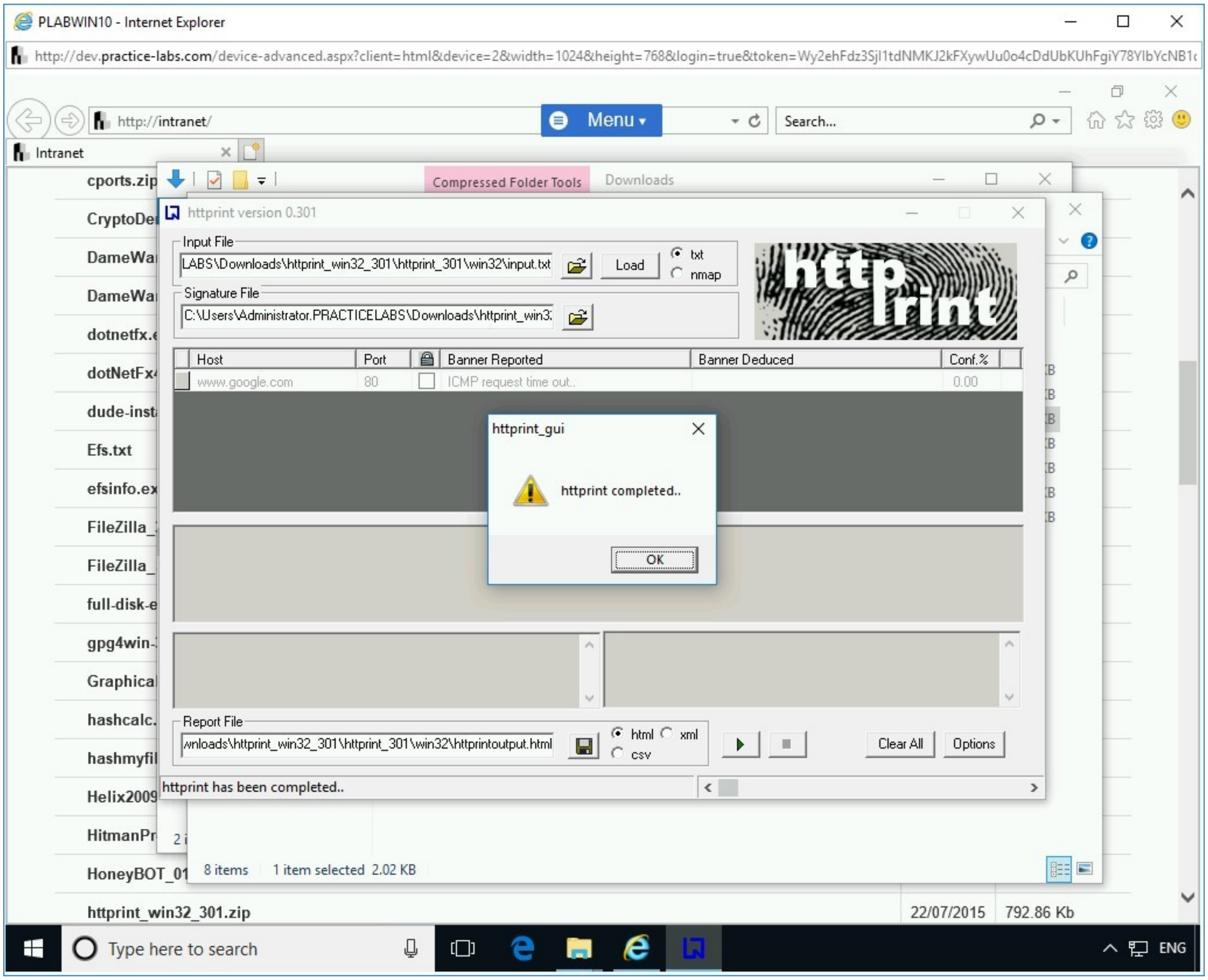
Report File: wnloads\httprint_win32_301\httprint_301\win32\httprintoutput.html ● html ○ xml ○ csv

All rows has been cleared.

Figure 1.34 Screenshot of PLABWIN10: Entering www . google . com in the Host column and clicking Start.

Step 23

The **httprint_gui** dialog box is displayed. Click **OK** to close it.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=Wy2ehFdz3SjI1tdNMKJ2kFXywUu0o4cDdUbKUhFgiY78YlbYcNB1(

http://intranet/

httprint version 0.301

Input File: LABS\Downloads\httprint_win32_301\httprint_301\win32\input.txt ● txt ○ nmap

Signature File: C:\Users\Administrator.PRACTICELABS\Downloads\httprint_win3:

Host	Port		Banner Reported	Banner Deduced	Conf.%
www.google.com	80	□	ICMP request time out..		0.00

httprint_gui

httprint completed..

OK

Report File: wnloads\httprint_win32_301\httprint_301\win32\httprintoutput.html ● html ○ xml ○ csv

httprint has been completed..

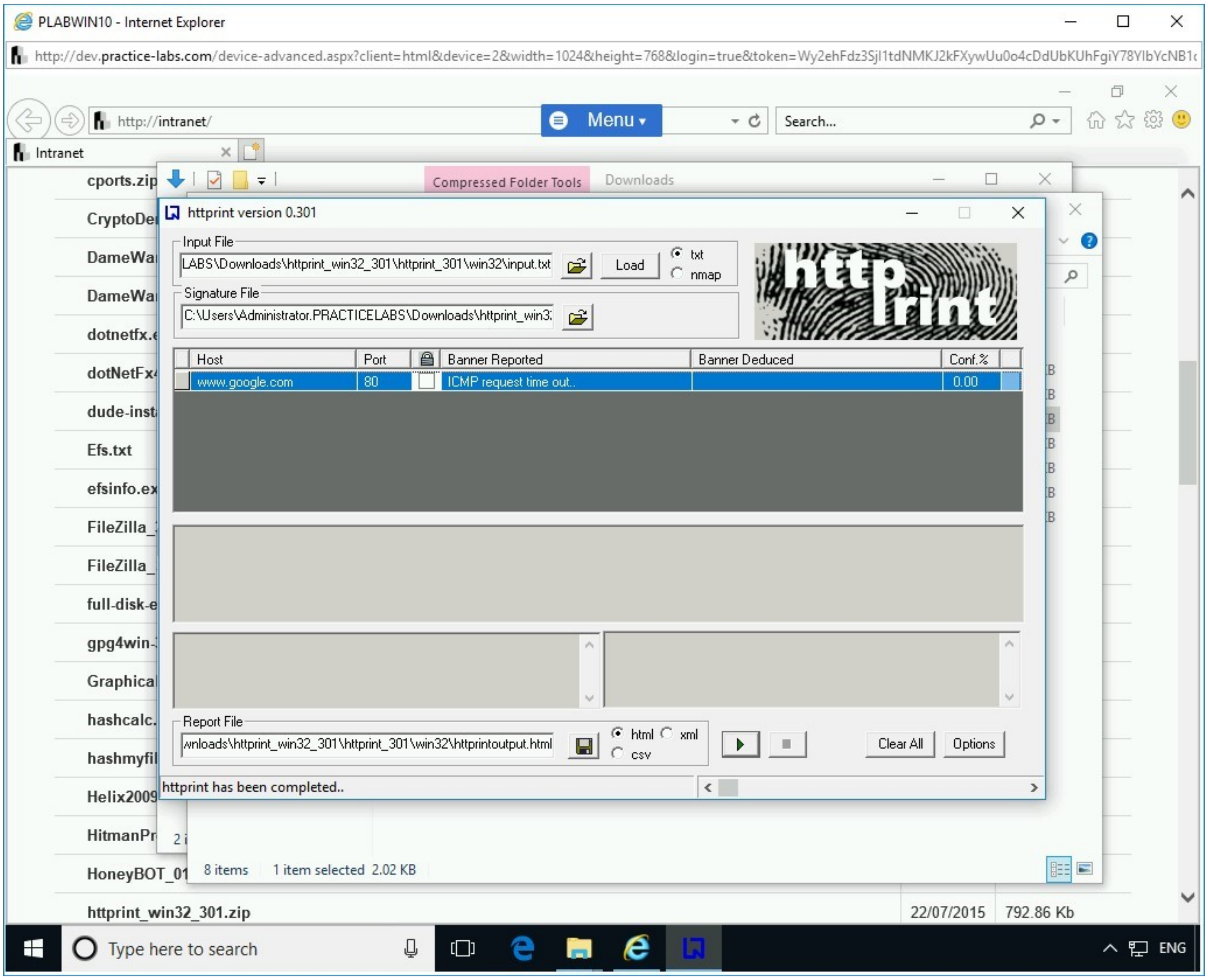
Figure 1.35 Screenshot of PLABWIN10: Showing the httprint_gui dialog box and clicking OK.

Note that the **Banner Reported** column shows **ICMP request time out**. This could be because of two reasons:

- Your network firewall is preventing the ICMP packets from going out.
- The target that you are trying to fingerprint prevents ICMP packets from coming into the network.

There could be a possibility that either both of the reasons are true or one of the reasons is true; you will get this error message.

Also, when you fingerprinted your internal Webserver, **192.168.0.10**, you did not get any error. The reason is that your system and Webserver are on the same network and same subnet.



Input File: LABS\Downloads\httprint_win32_301\httprint_301\win32\input.txt

● txt ○ nmap

Signature File: C:\Users\Administrator.PRACTICELABS\Downloads\httprint_win3:

Host	Port		Banner Reported	Banner Deduced	Conf.%
www.google.com	80	□	ICMP request time out..		0.00

Report File: wnloads\httprint_win32_301\httprint_301\win32\httprintoutput.html

● html ○ xml ○ csv

httprint has been completed..

Figure 1.36 Screenshot of PLABWIN10: Showing the output that has been blocked due to an ICMP error.

Close all open windows.

Task 3 - Perform Directory Traversal Attack

Directory traversal allows attackers to access restricted directories and file on a Webserver. It is most commonly known as the path traversal attack. Through the directory traversal attack, the attacker can bypass security implemented on the Webserver and access directories and files that are stored on the Webserver even though they are outside the root directory of the Webserver.

In most common scenarios, a Webserver administrator would restrict users to the Webserver's root directory, which holds the files for the Web application. The user will be restricted to navigate outside this directory. The Webserver administrator usually applies Access Control Lists (ACLs), which define the access rights and privileges for the users to view, modify, and execute files.

To perform a directory traversal attack, perform the following steps:

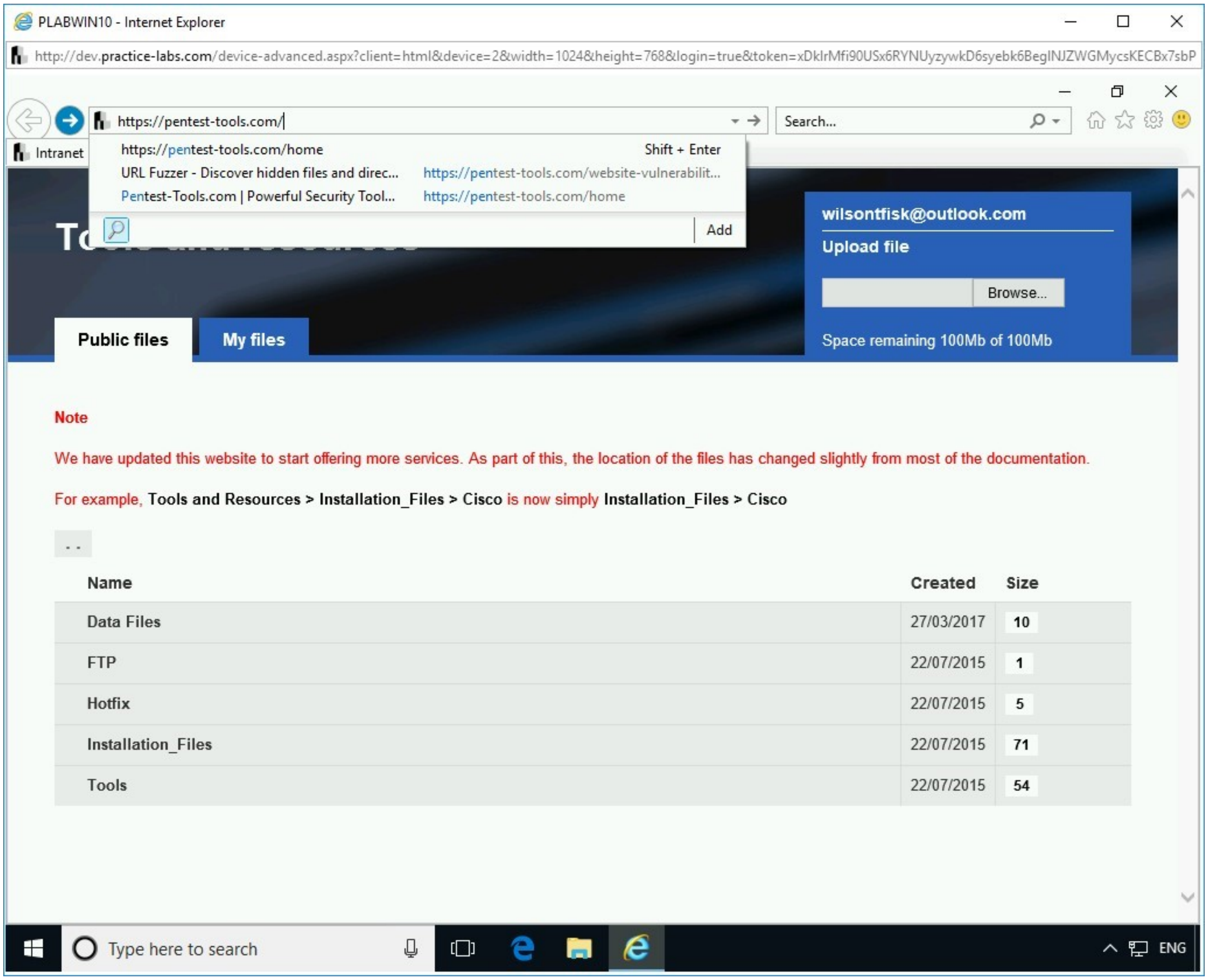
Step 1

Connect to **PLABWIN10**. Open **Internet Explorer**.

Type the following string in the address bar:

```
https://pentest-tools.com/home
```

Press **Enter**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDkIrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP
https://pentest-tools.com/
Search...
Intranet
https://pentest-tools.com/home
Shift + Enter
URL Fuzzer - Discover hidden files and direc...
https://pentest-tools.com/website-vulnerabilit...
Pentest-Tools.com | Powerful Security Tool...
https://pentest-tools.com/home
Add
wilsontfisk@outlook.com
Upload file
Browse...
Space remaining 100Mb of 100Mb
Public files
My files
Type here to search
ENG

Note

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

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

. .

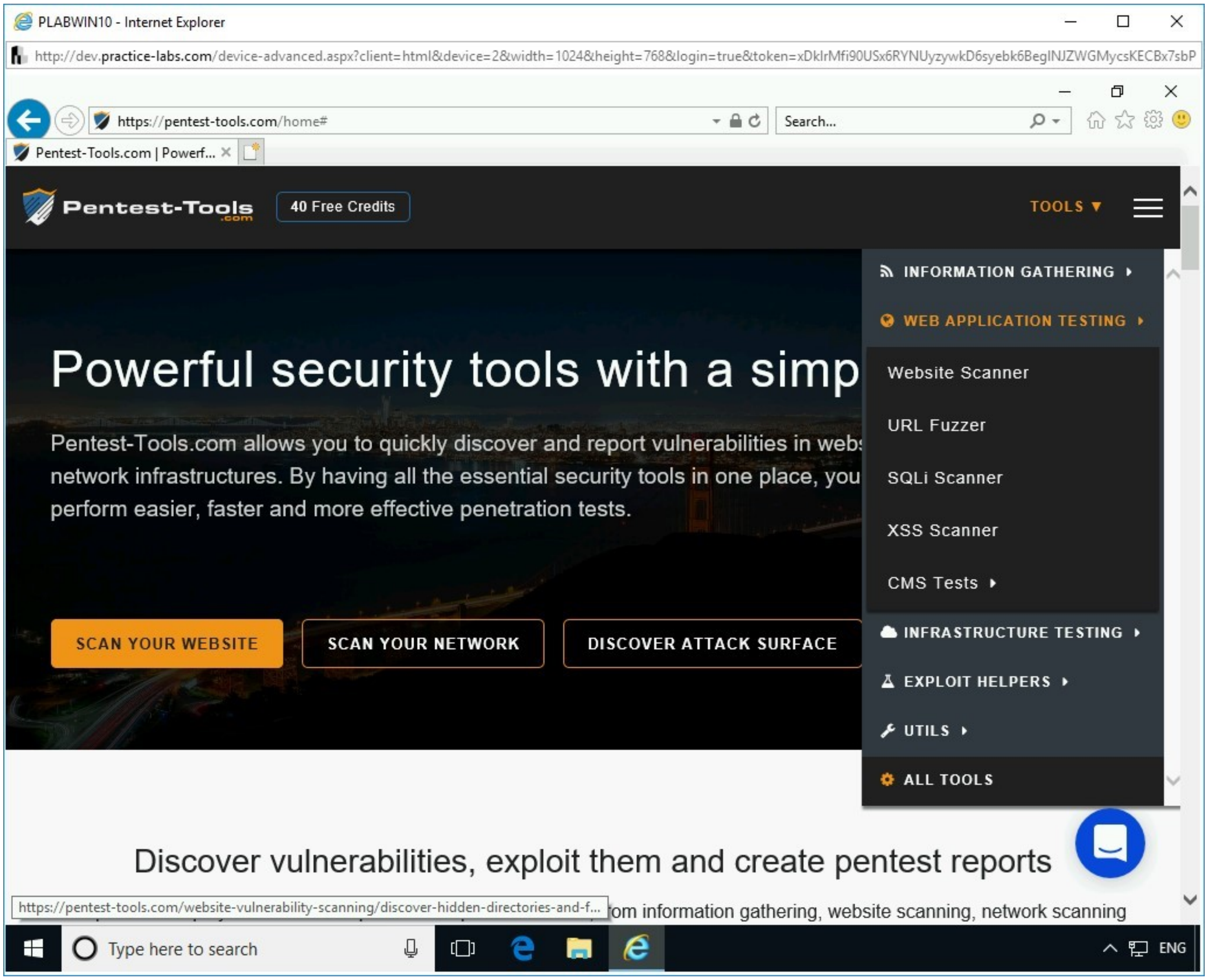
Name	Created	Size
Data Files	27/03/2017	10
FTP	22/07/2015	1
Hotfix	22/07/2015	5
Installation_Files	22/07/2015	71
Tools	22/07/2015	54

Figure 1.37 Screenshot of PLABWIN10: Entering a URL in the address bar.

Step 2

On the upper right-hand corner, click **Tools** and then select **URL Fuzzer** under the **WEB APPLICATION TESTING** category.

Note: If there is 0 free scans available, please complete this Task on your own PC outside of the Practice Labs environment.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDklrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP
https://pentest-tools.com/home#
Search...
Pentest-Tools.com | Powerf...
Pentest-Tools .com
40 Free Credits
TOOLS ▼
INFORMATION GATHERING ▸
WEB APPLICATION TESTING ▸
Website Scanner
URL Fuzzer
SQLi Scanner
XSS Scanner
CMS Tests ▸
INFRASTRUCTURE TESTING ▸
EXPLOIT HELPERS ▸
UTILS ▸
ALL TOOLS
SCAN YOUR WEBSITE
SCAN YOUR NETWORK
DISCOVER ATTACK SURFACE
https://pentest-tools.com/website-vulnerability-scanning/discover-hidden-directories-and-f...
Type here to search
ENG

Powerful security tools with a simp

Pentest-Tools.com allows you to quickly discover and report vulnerabilities in webs network infrastructures. By having all the essential security tools in one place, you perform easier, faster and more effective penetration tests.

Discover vulnerabilities, exploit them and create pentest reports

om information gathering, website scanning, network scanning

Figure 1.38 Screenshot of PLABWIN10: Clicking on the URL Fuzzer link on the Webpage.

Step 3

Close the small pop-up window.

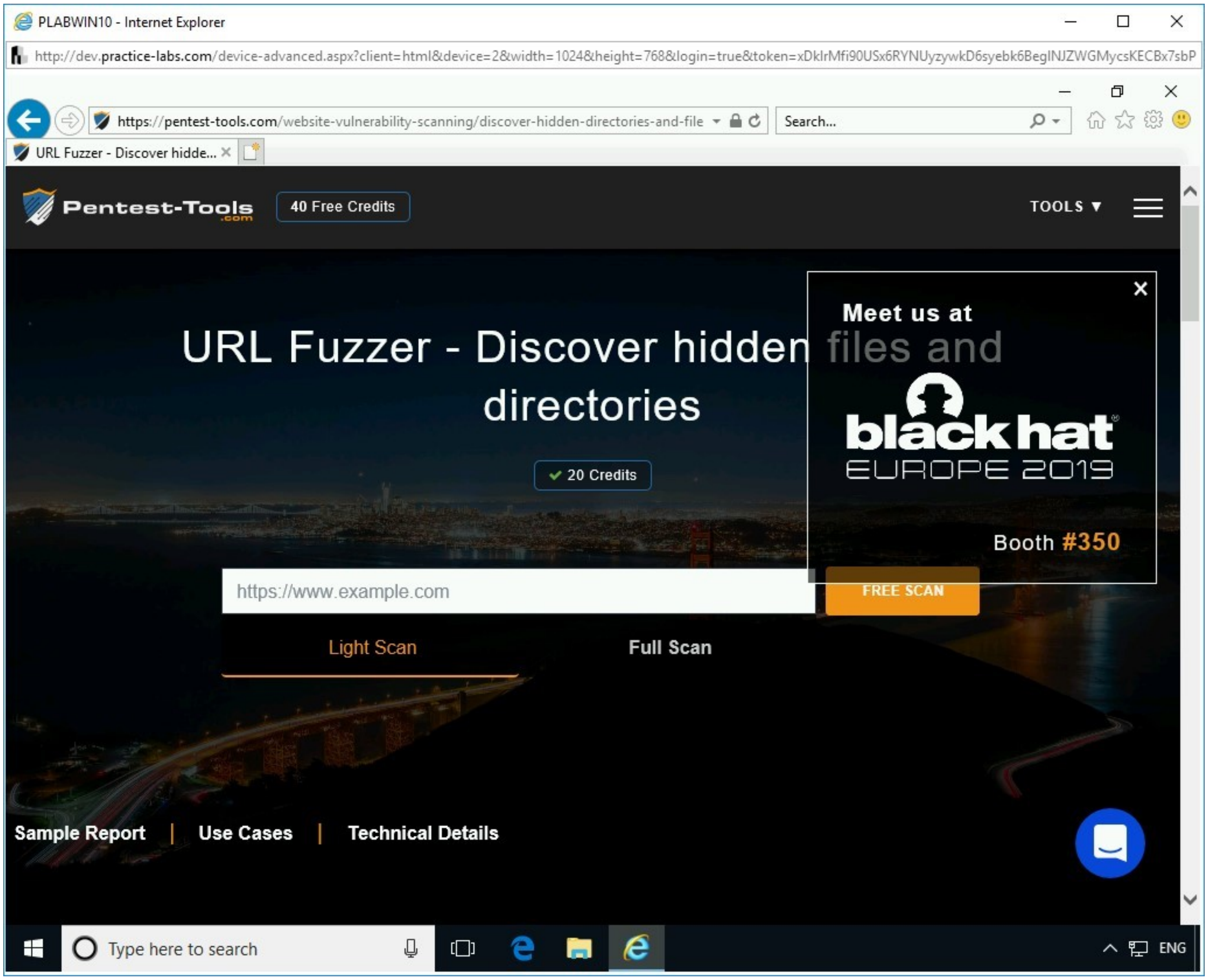

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDkIrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP
https://pentest-tools.com/website-vulnerability-scanning/discover-hidden-directories-and-file
Search...
URL Fuzzer - Discover hidde...
Pentest-Tools .com
40 Free Credits
TOOLS ▼
Meet us at
black hat
EUROPE 2019
Booth #350
URL Fuzzer - Discover hidden files and directories
✓ 20 Credits
https://www.example.com
FREE SCAN
Light Scan
Full Scan
Sample Report | Use Cases | Technical Details
Type here to search
ENG

Figure 1.39 Screenshot of PLABWIN10: Clicking Tools on the Intranet homepage.

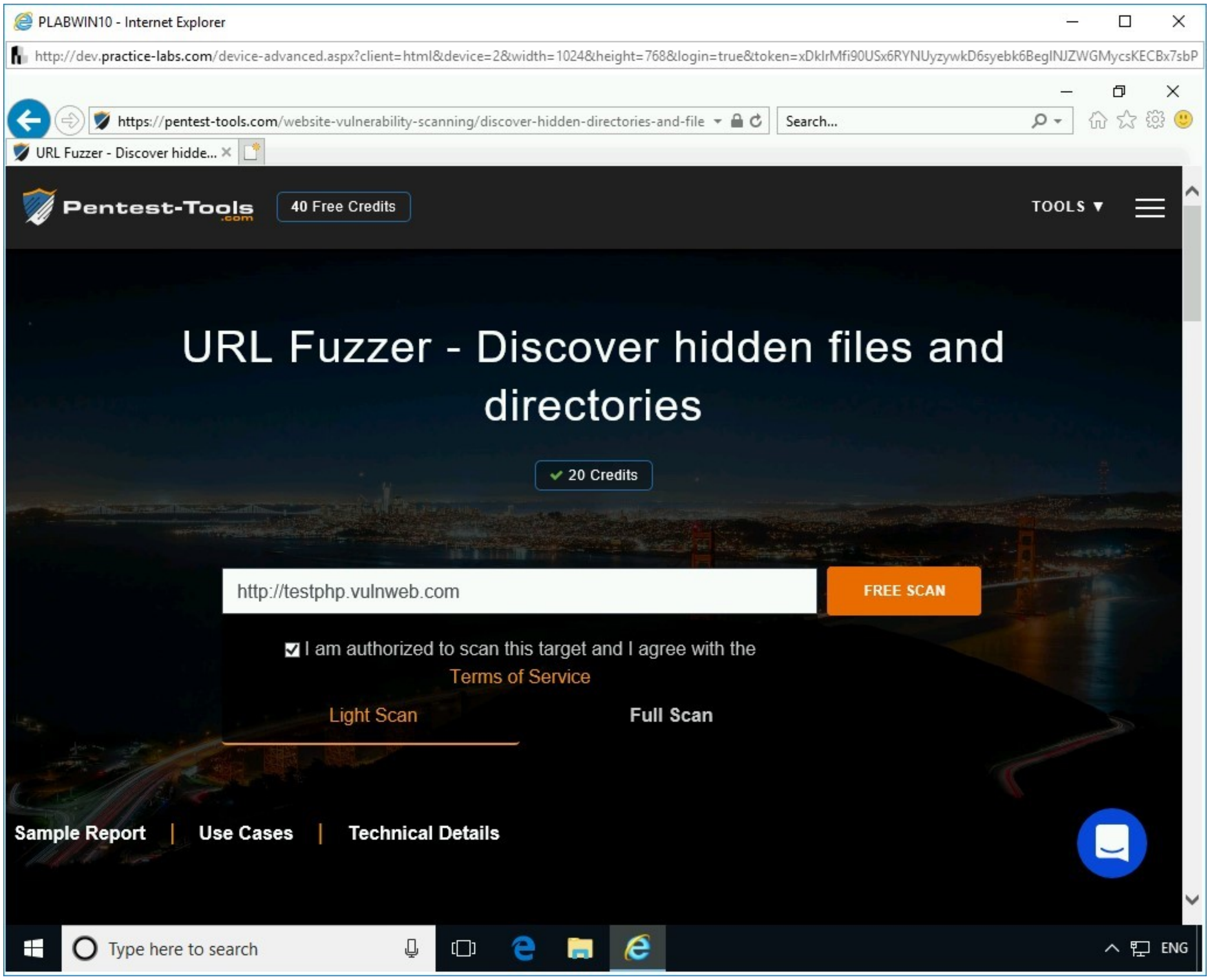
Step 4

The **URL Fuzzer** Webpage is now loaded. In the search textbox, type the following URL:

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

Select **I am authorized to scan this target, and I agree with the Terms of Service** click **FREE SCAN**.

Note: *The Light Scan option is selected by default and is free. Full Scan is a paid service.*



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDklrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP

https://pentest-tools.com/website-vulnerability-scanning/discover-hidden-directories-and-file

URL Fuzzer - Discover hidden files and directories

20 Credits

http://testphp.vulnweb.com

☑ I am authorized to scan this target and I agree with the Terms of Service

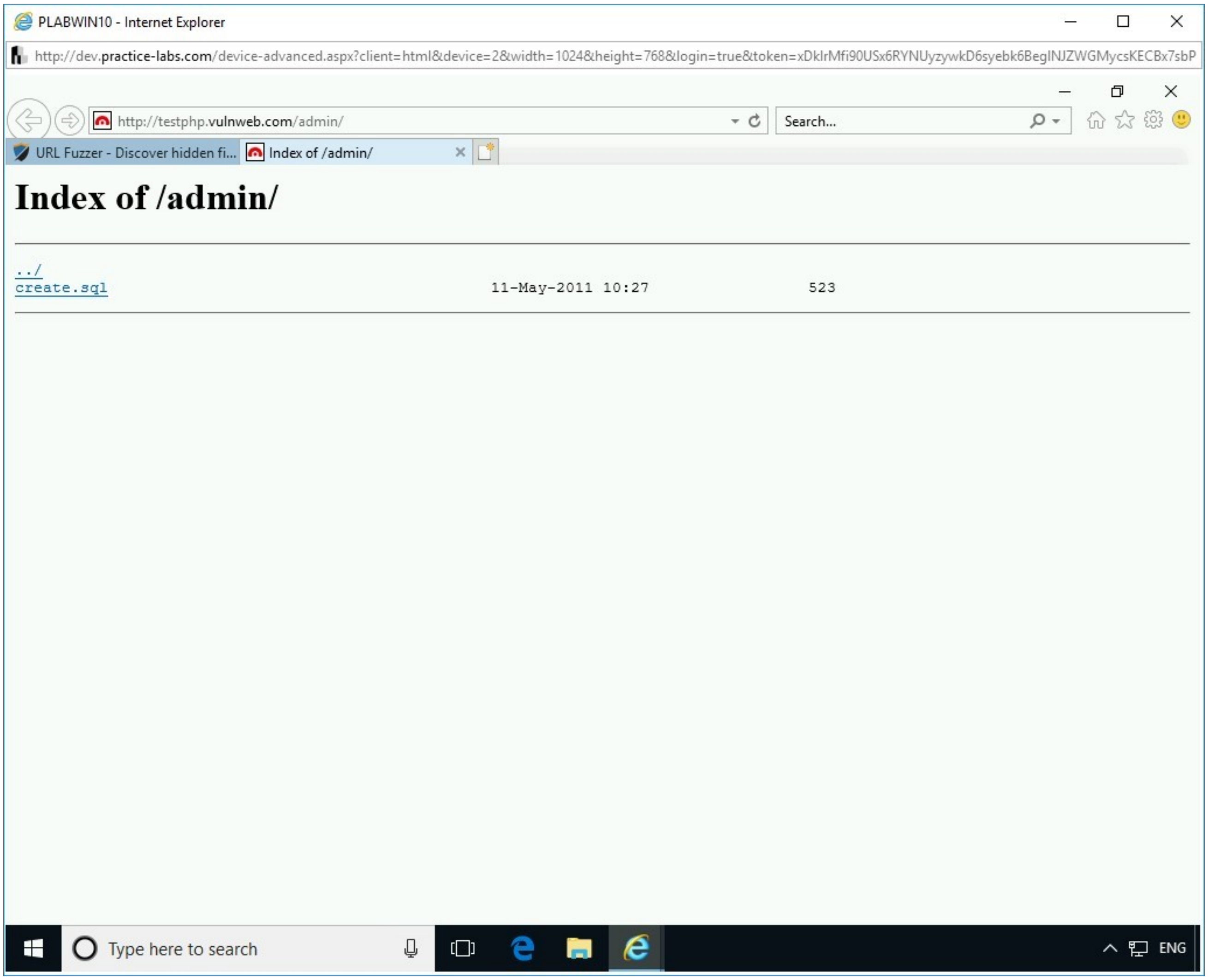
Figure 1.40 Screenshot of PLABWIN10: Entering the URL in the search bar and clicking FREE SCAN.

Step 5

The scanning starts.

After scanning is complete, you need to scroll down to view the list of directories. Click **/admin**/.

A new tab is opened. It displays a file named **create.sql**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDkIrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP
http://testphp.vulnweb.com/admin/
Search...
URL Fuzzer - Discover hidden fi...
Index of /admin/
Type here to search
ENG

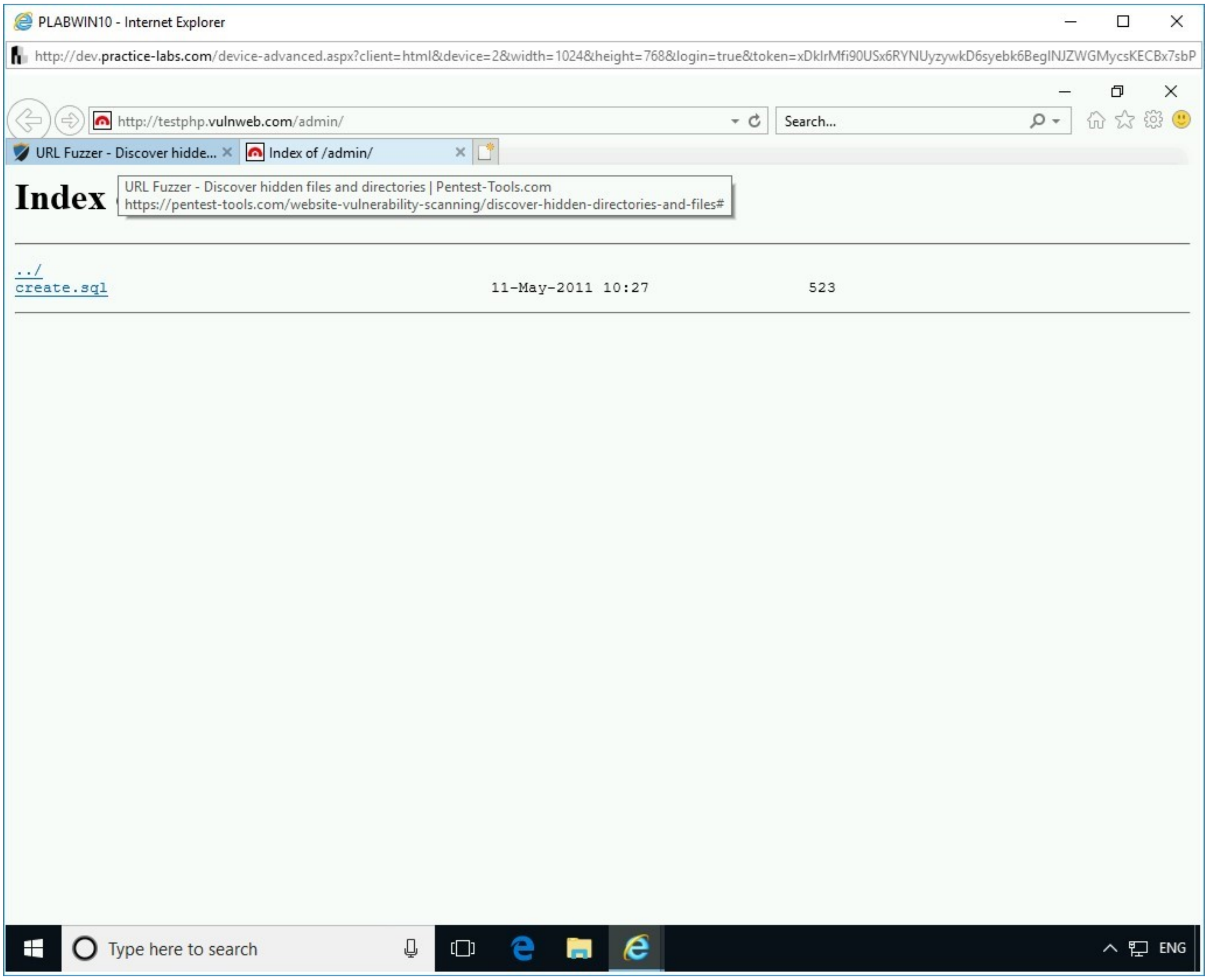
Index of /admin/

```
../
create.sql                                         11-May-2011 10:27                 523
```

Figure 1.41 Screenshot of PLABWIN10: Showing the create.sql file in the /admin/ directory.

Step 6

Click the **URL Fuzzer** tab.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDklrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP
http://testphp.vulnweb.com/admin/
Search...
URL Fuzzer - Discover hidde...
Index of /admin/
URL Fuzzer - Discover hidden files and directories | Pentest-Tools.com
https://pentest-tools.com/website-vulnerability-scanning/discover-hidden-directories-and-files#
Type here to search
ENG

Index

```
../
create.sql                                         11-May-2011 10:27                 523
```

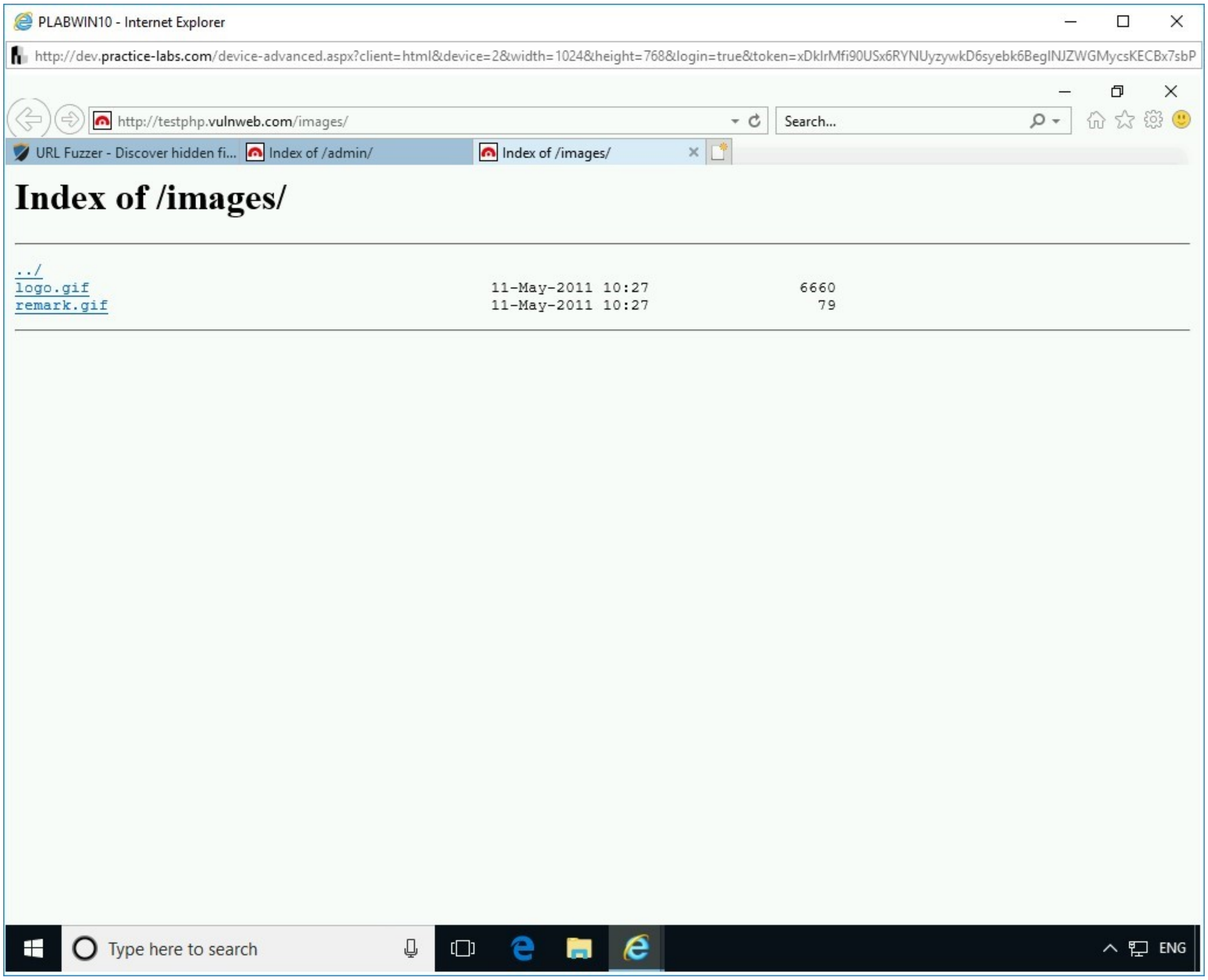
Figure 1.42 Screenshot of PLABWIN10: Clicking Tools on the Intranet homepage.

Step 7

Click the **/images/** folder.

A new tab is now opened. It displays two files, **logo.gif,** and **remark.gif** in the **/images/** folder.

Close the Internet Explorer window.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=xDkIrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP
http://testphp.vulnweb.com/images/
Search...
URL Fuzzer - Discover hidden fi...
Index of /admin/
Index of /images/
Type here to search
ENG

Index of /images/

```
../
logo.gif                                           11-May-2011 10:27                6660
remark.gif                                         11-May-2011 10:27                  79
```

Figure 1.43 Screenshot of PLABWIN10: Clicking Tools on the Intranet homepage.

Task 4 - Perform Web Application Brute Forcing Using DirBuster

There are several tools or Websites that you can use to traverse through a Website's directory structure. When you configure a Webserver with a Website, it is best to ensure that you have not enabled directory listing. If enabled, an attacker can exploit the Webserver and get the listing. In this task, you will learn to perform directory traversal using a multi-threaded tool named DirBuster, which can brute force the Web applications to find their directory structure.

To perform Web application brute force using DirBuster, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABKALI01**. Click the **Leafpad** icon in the left pane.

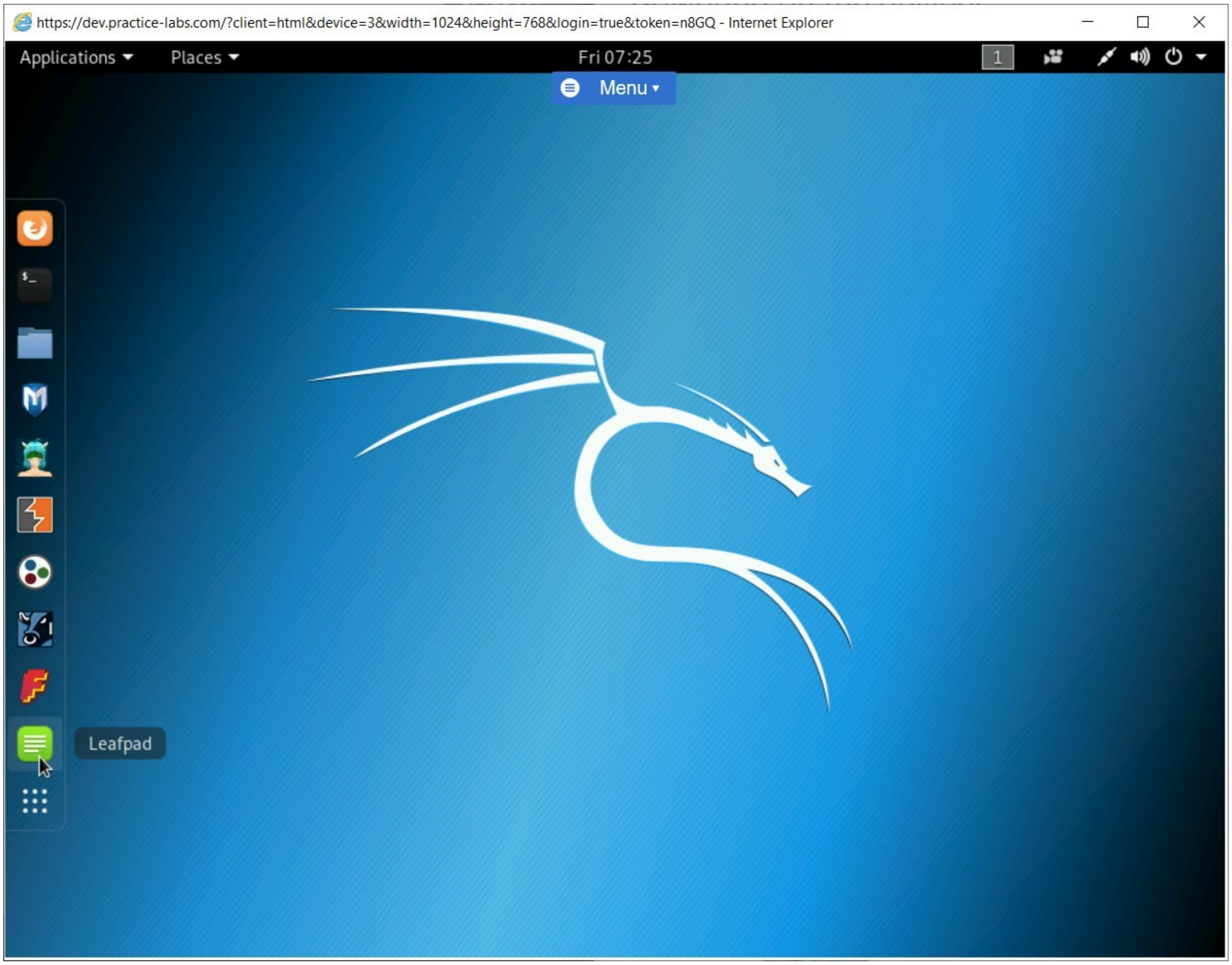

https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Fri 07:25
1
Menu
Leafpad

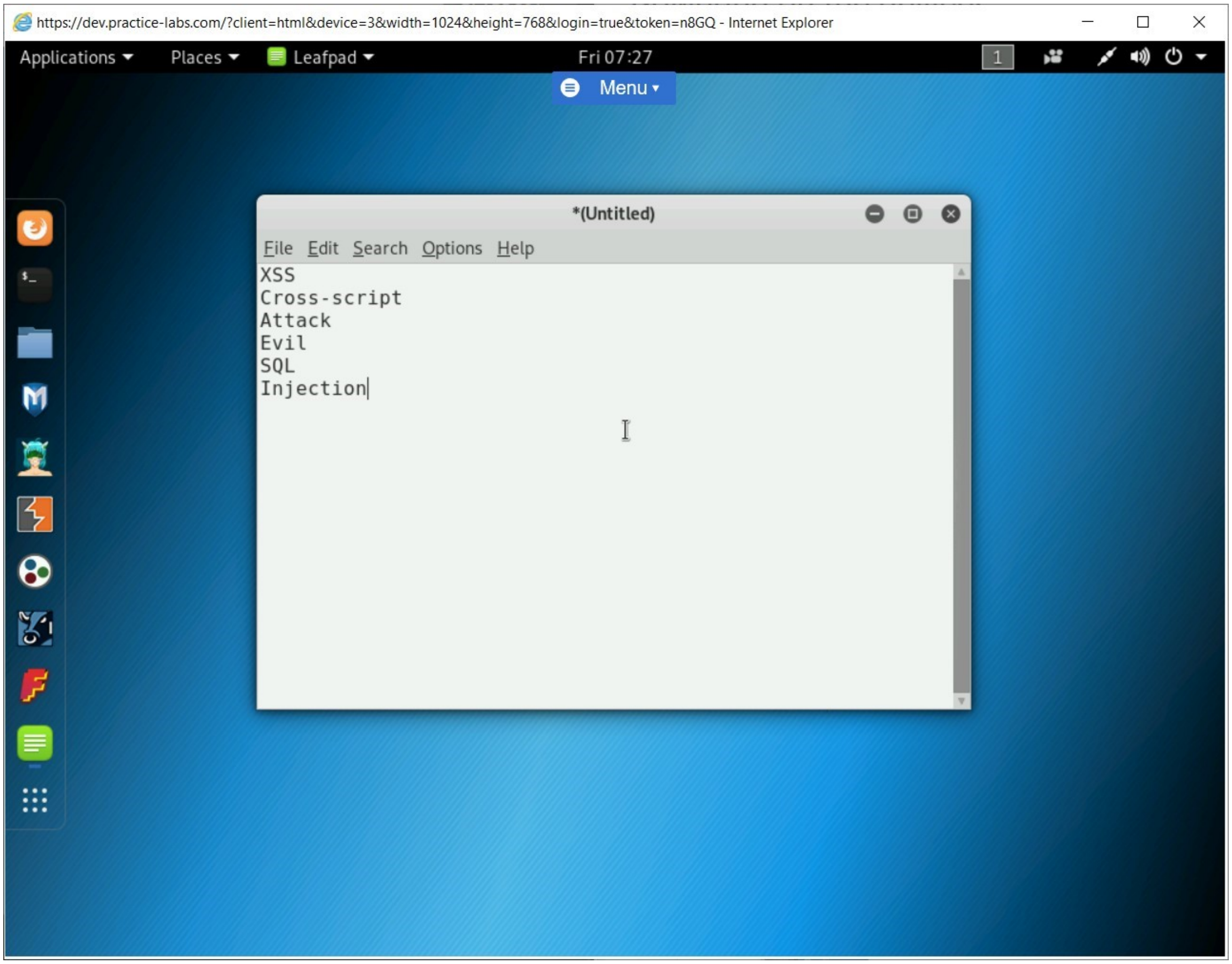
Figure 1.44 Screenshot of PLABKALI01: Showing the desktop of PLABKALI01 and clicking the Leafpad icon.

Step 2

The ***Untitled Document 1** window is opened. Type the following words:

```
XSS
Cross-script
Attack
```

```
Evil
SQL
Injection
```



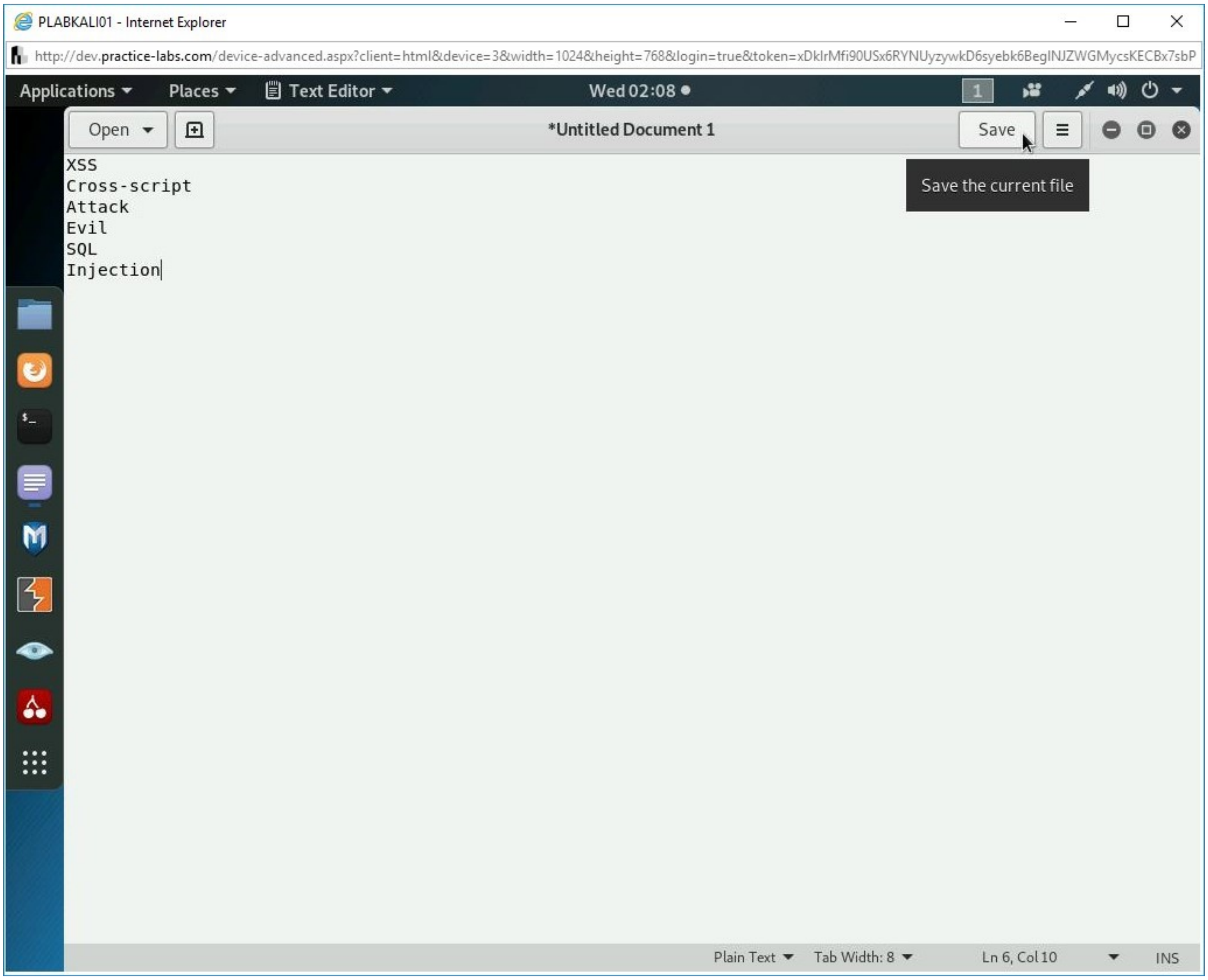
https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Leafpad
Fri 07:27
Menu
*(Untitled)
File
Edit
Search
Options
Help

```
XSS
Cross-script
Attack
Evil
SQL
Injection
```

Figure 1.45 Screenshot of PLABKALI01: Creating a file in Leadpad with some text.

Step 3

Click **File** and cklick **Save**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=xDklrMfi90USx6RYNUyzywkD6syebk6BegINJZWGMycsKECBx7sbP
Applications
Places
Text Editor
Wed 02:08
Open
*Untitled Document 1
Save
Save the current file
Plain Text
Tab Width: 8
Ln 6, Col 10
INS

```
XSS
Cross-script
Attack
Evil
SQL
Injection
```

Figure 1.46 Screenshot of PLABKALI01: Saving the file with the File (Save option.

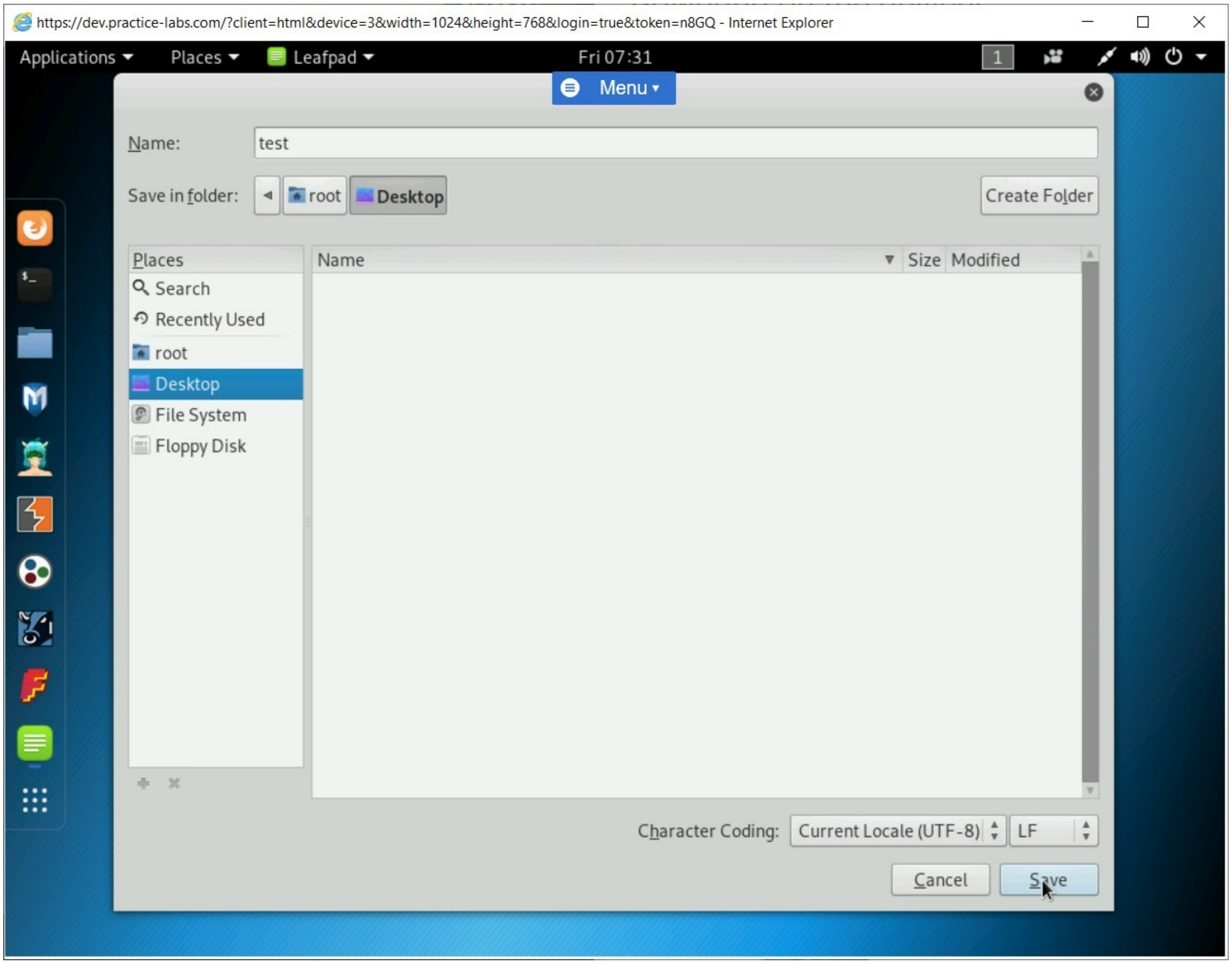
Step 4

The **Save As** dialog box is displayed.

From the left pane, select **Desktop**. In the **Name** text box, type the following name:

```
test
```

Click **Save**.



https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer

Name: test

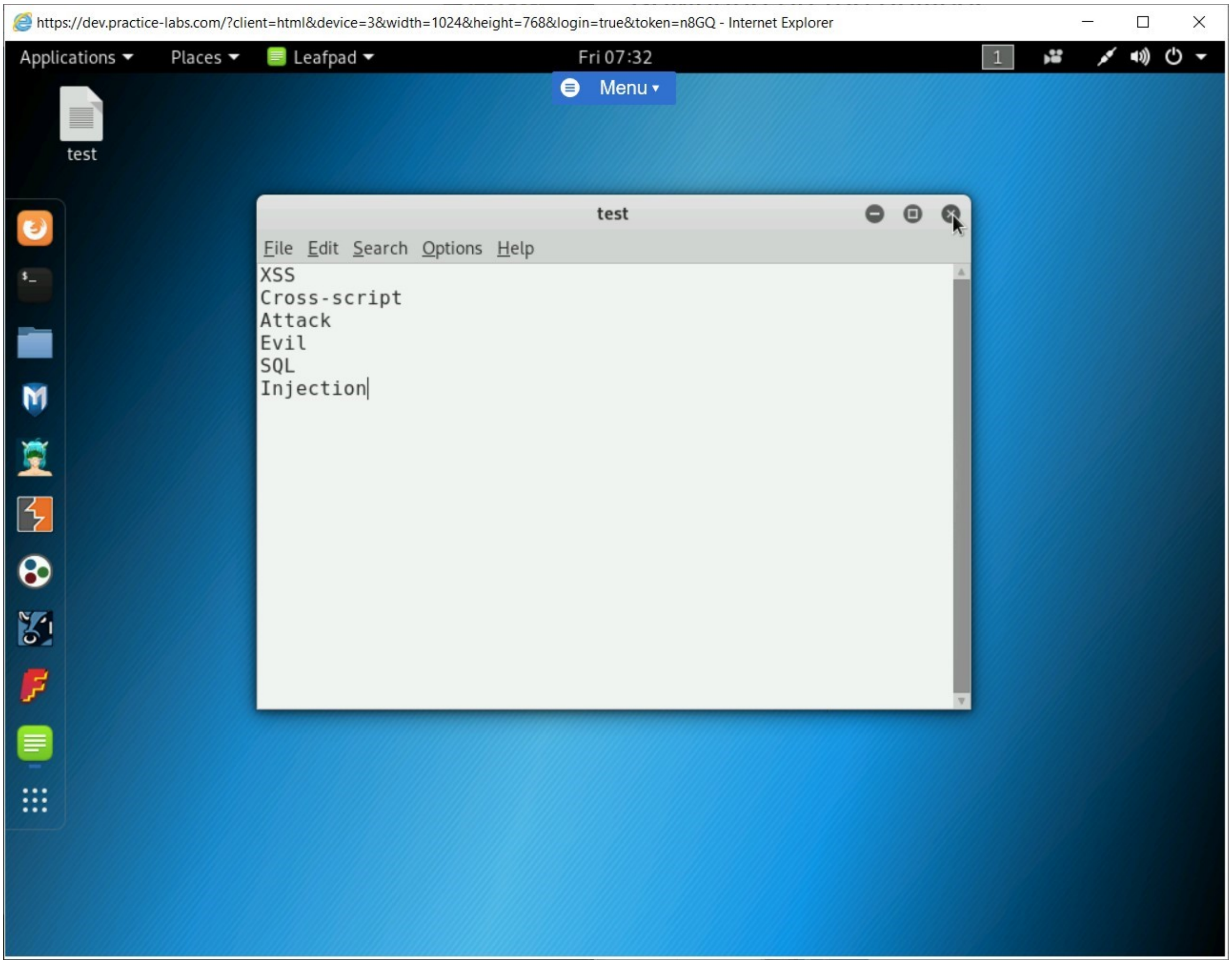
Save in folder: root / Desktop

Character Coding: Current Locale (UTF-8) LF

Figure 1.47 Screenshot of PLABKALI01: Naming the file as a test and saving on the Desktop.

Step 5

Notice that the file name is now changed to **test**. Close the **Text Editor** window.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Leafpad
Fri 07:32
1
Menu
test
test
File Edit Search Options Help

```
XSS
Cross-script
Attack
Evil
SQL
Injection
```

Figure 1.48 Screenshot of PLABKALI01: Showing the test file and closing it.

Step 6

Notice that the test file is now created on the desktop. Click the **Terminal** icon in the left pane.

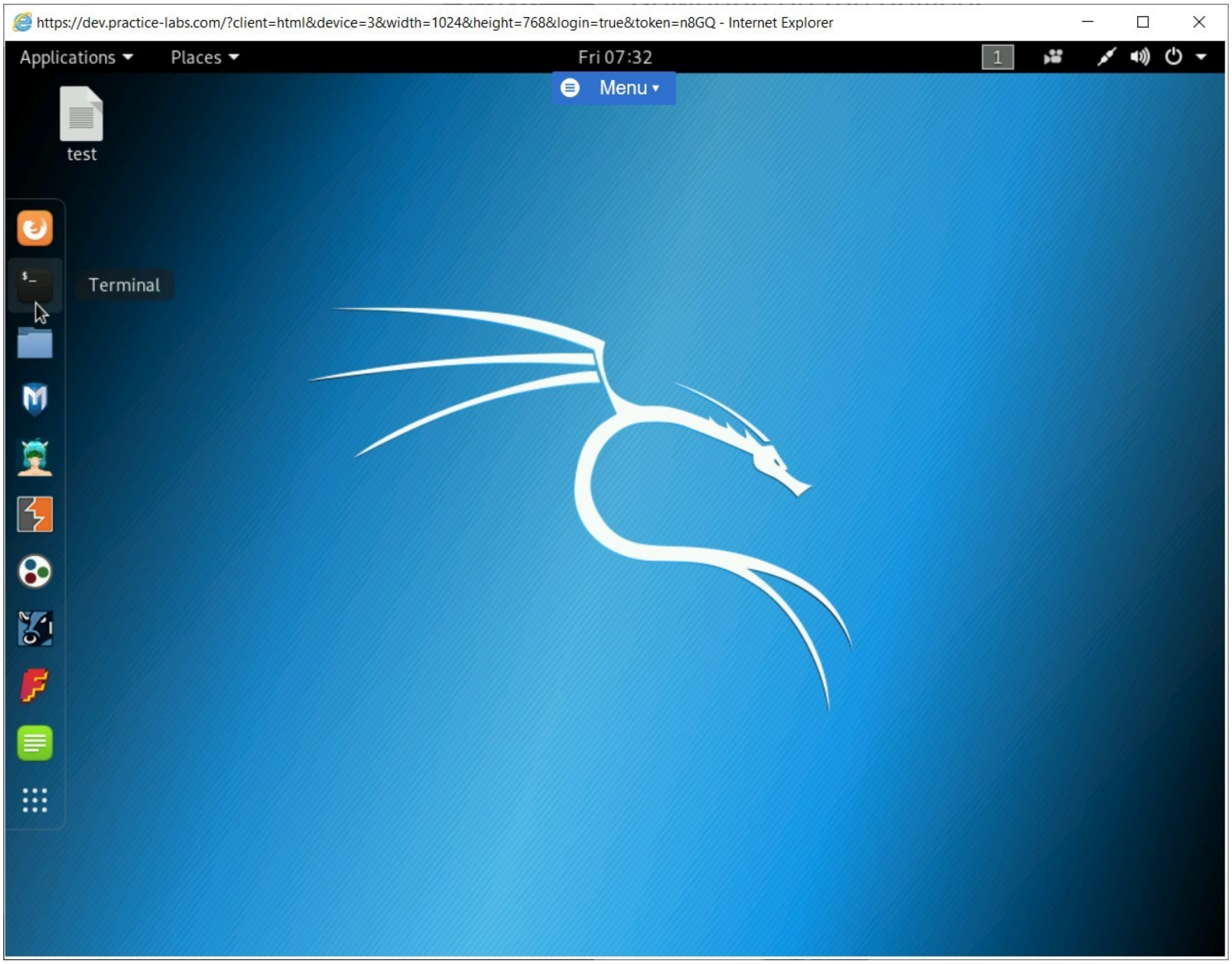

https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Fri 07:32
Menu
test
Terminal

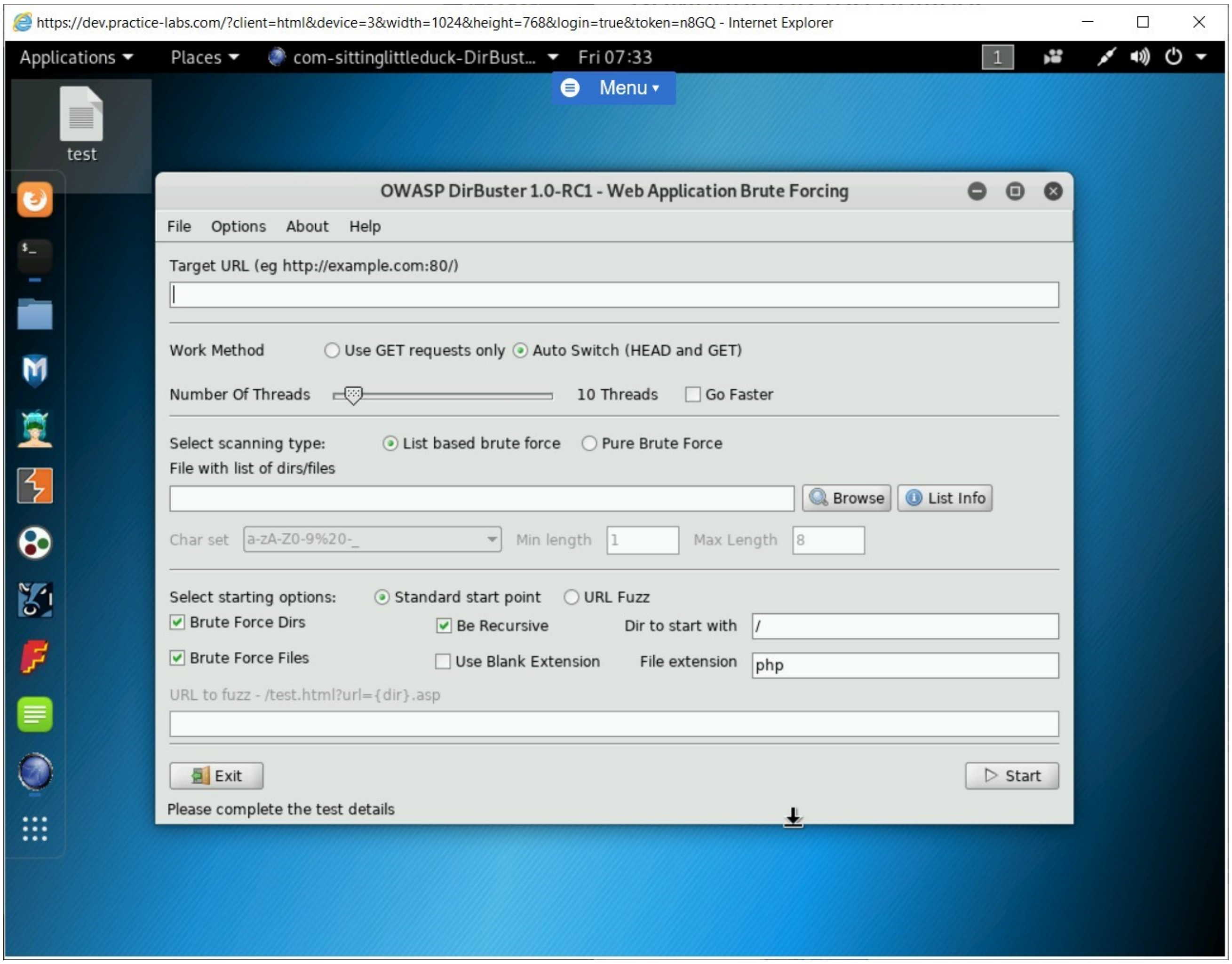
Figure 1.49 Screenshot of PLABKALI01: Clicking the Terminal icon from the left pane on the desktop.

Step 7

The terminal window is displayed. Type the following command:

```
dirbuster
```

Press **Enter**. The **OWASP DirBuster** window is displayed.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
com-sittinglittleduck-DirBust...
Fri 07:33
Menu
test
File
Options
About
Help
Browse
List Info
Exit
Start

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

Target URL (eg http://example.com:80/)

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details

Figure 1.50 Screenshot of PLABKALI01: Showing the OWASP DisBuster window.

Step 8

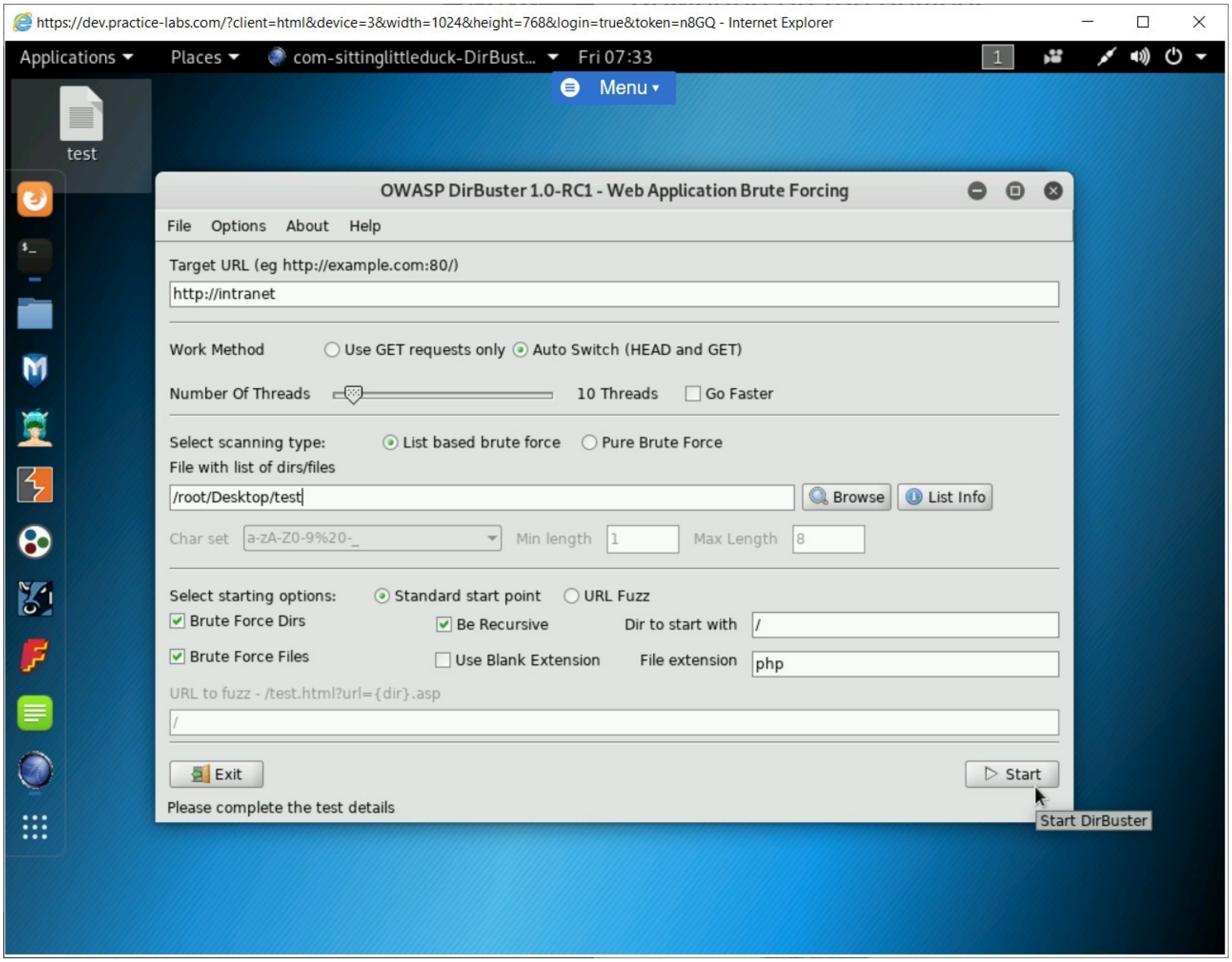
In the **Target URL** text box, type the following URL:

```
http://intranet
```

In the **File with the list of dirs/files** text box, type the following path:

```
/root/Desktop/test
```

Click **Start**.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
com-sittinglittleduck-DirBust...
Fri 07:33
Menu
test
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Browse
List Info
Exit
Start
Start DirBuster

Target URL (eg http://example.com:80/)
http://intranet

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files
/root/Desktop/test

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp
/

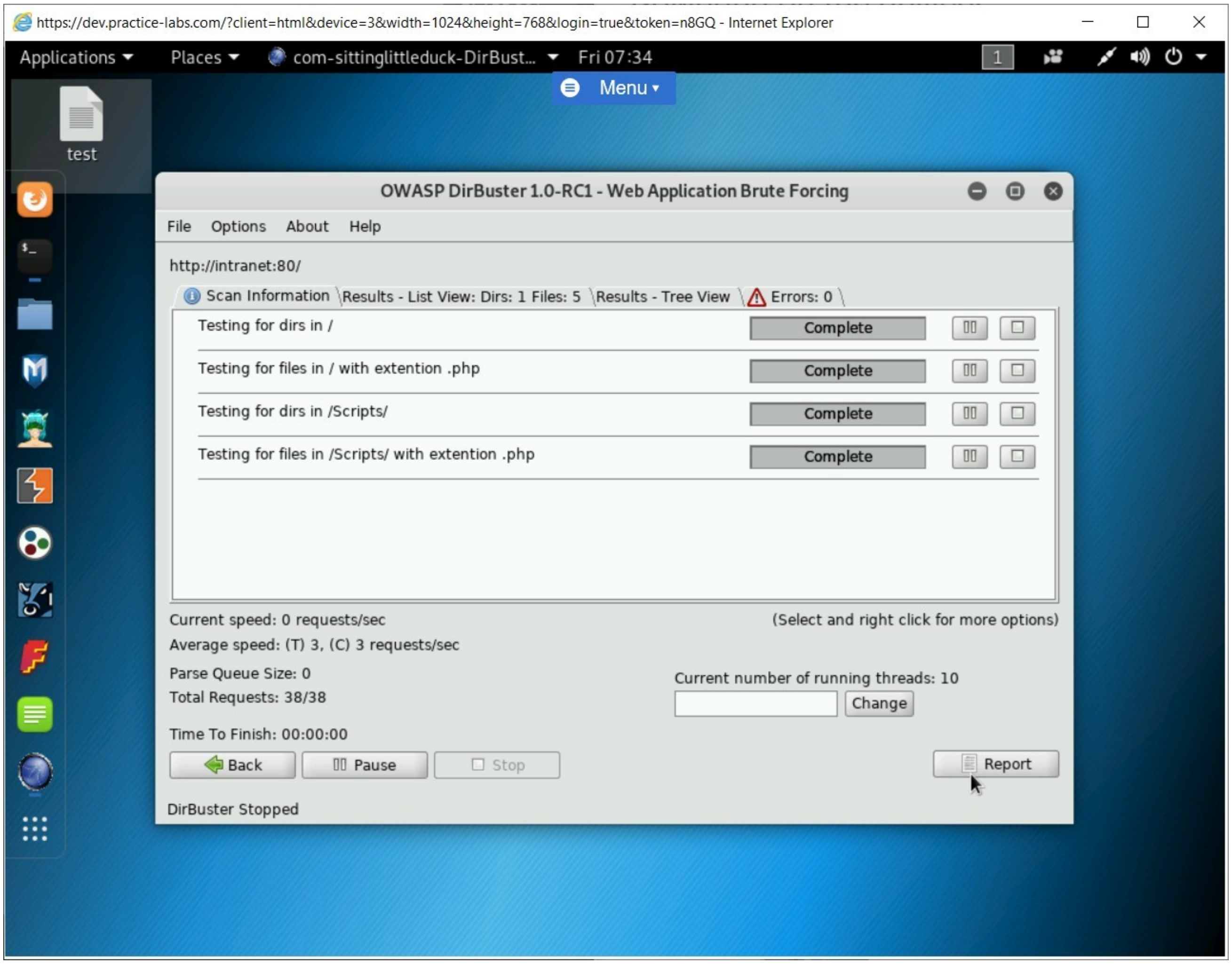
Please complete the test details

Figure 1.51 Screenshot of PLABKALI01: Entering the URL and the path for the test file and clicking Start.

Step 9

The scanning process starts.

After the scanning process is completed, click **Report**.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
com-sittinglittleduck-DirBust...
Fri 07:34
Menu
test
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 1 Files: 5
Results - Tree View
Errors: 0
Change
Back
Pause
Stop
Report

http://intranet:80/

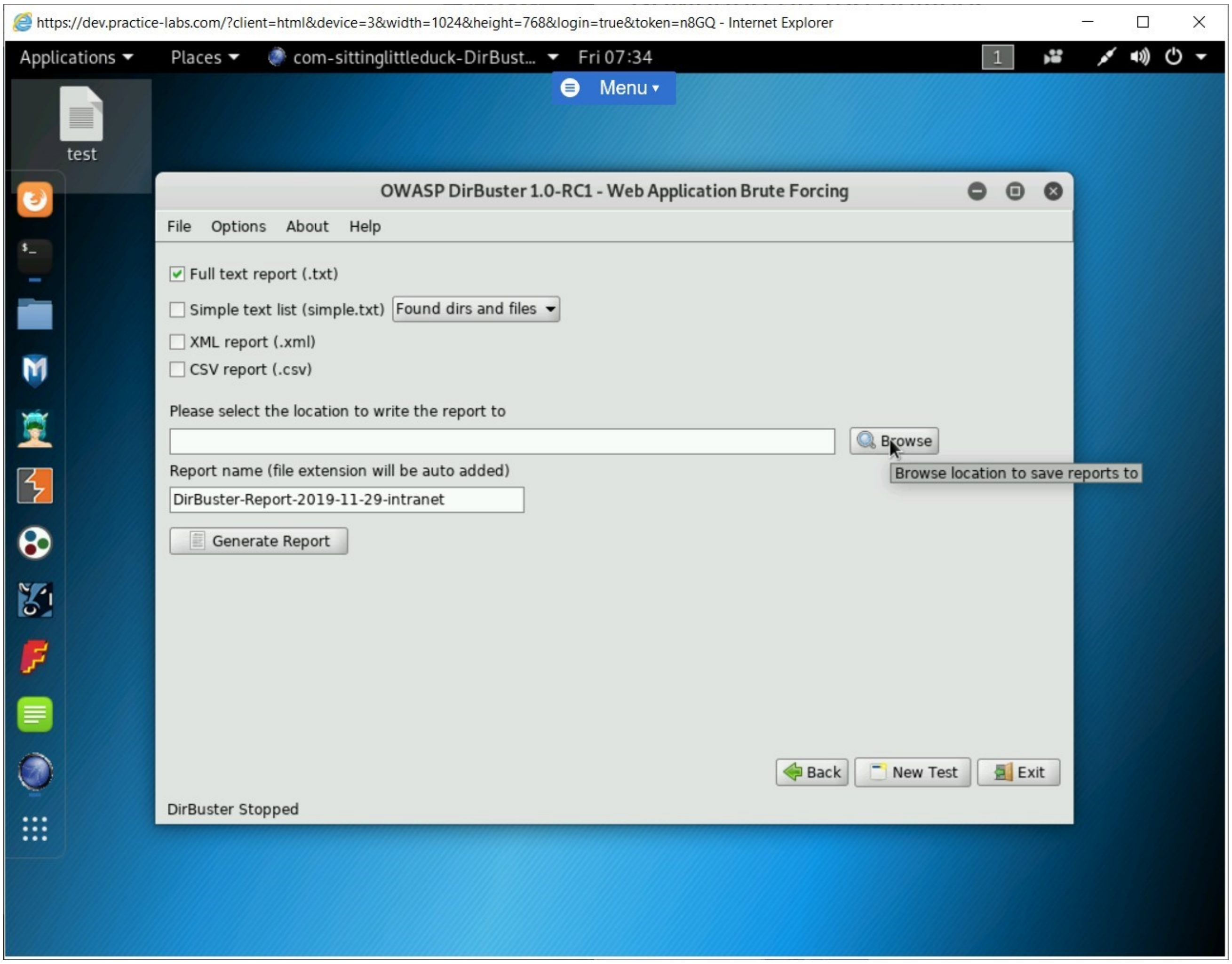
Testing for dirs in / Complete
Testing for files in / with extention .php Complete
Testing for dirs in /Scripts/ Complete
Testing for files in /Scripts/ with extention .php Complete

Current speed: 0 requests/sec
(Select and right click for more options)
Average speed: (T) 3, (C) 3 requests/sec
Parse Queue Size: 0
Total Requests: 38/38
Current number of running threads: 10
Time To Finish: 00:00:00
DirBuster Stopped

Figure 1.52 Screenshot of PLABKALI01: Clicking the Report button.

Step 10

Click **Browse**.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer

Applications
Places
com-sittinglittleduck-DirBust...
Fri 07:34
Menu
test

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

☑ Full text report (.txt)

□ Simple text list (simple.txt) Found dirs and files

□ XML report (.xml)

□ CSV report (.csv)

Please select the location to write the report to

Browse
Browse location to save reports to

Report name (file extension will be auto added)

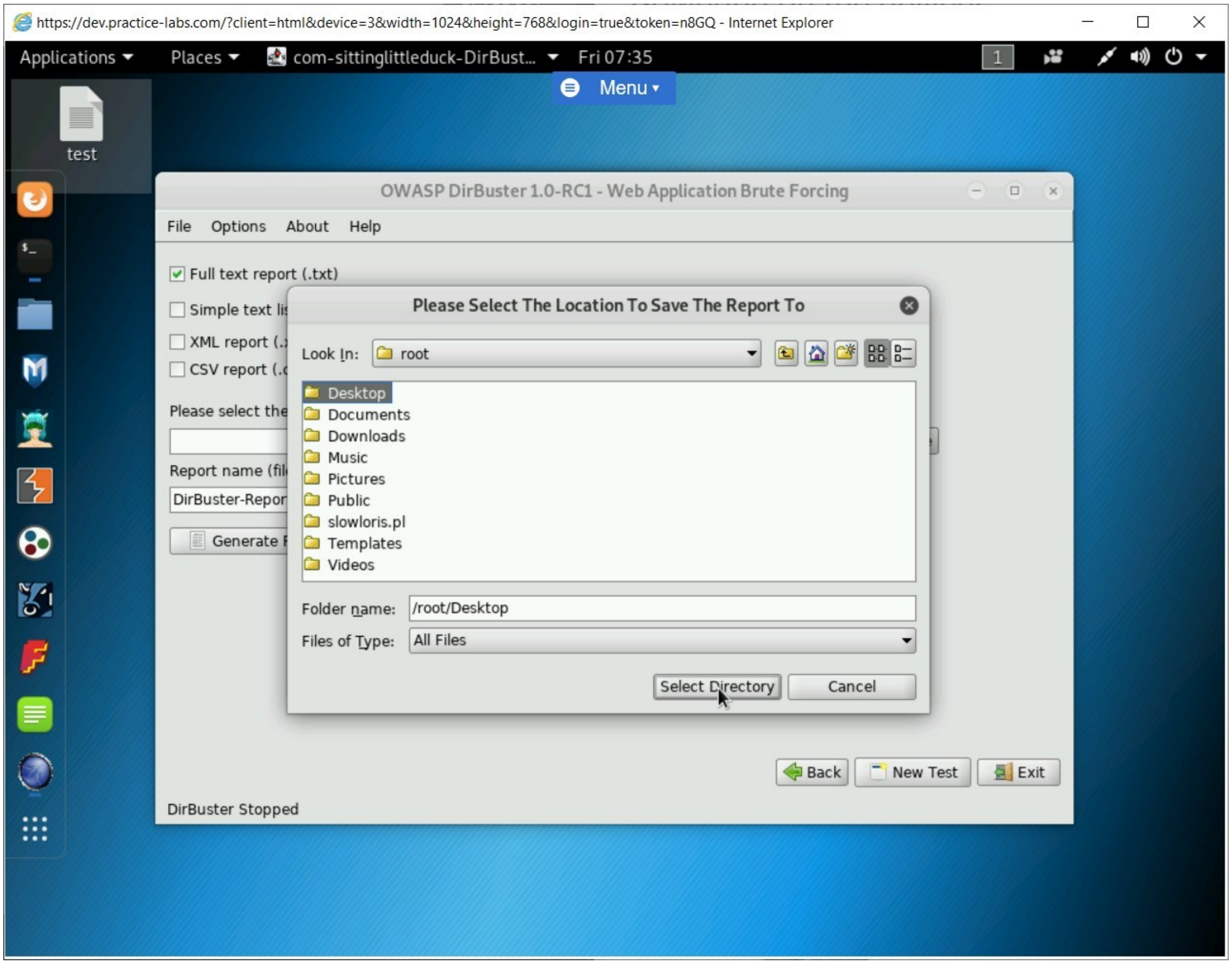
DirBuster-Report-2019-11-29-intranet

DirBuster Stopped

Figure 1.53 PLABKALI01: Clicking the Browse button.

Step 11

In the **Please Select The Location To Save The Report To** dialog box, select **Desktop** and click **Select Directory**.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
com-sittinglittleduck-DirBust...
Fri 07:35
Menu
test
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Generate F
Back
New Test
Exit
Select Directory
Cancel
Desktop
Documents
Downloads
Music
Pictures
Public
slowloris.pl
Templates
Videos

☑ Full text report (.txt)

□ Simple text li

□ XML report (.

□ CSV report (.

Please select the

Report name (fil

DirBuster-Repor

Please Select The Location To Save The Report To

Look In: root

Folder name: /root/Desktop

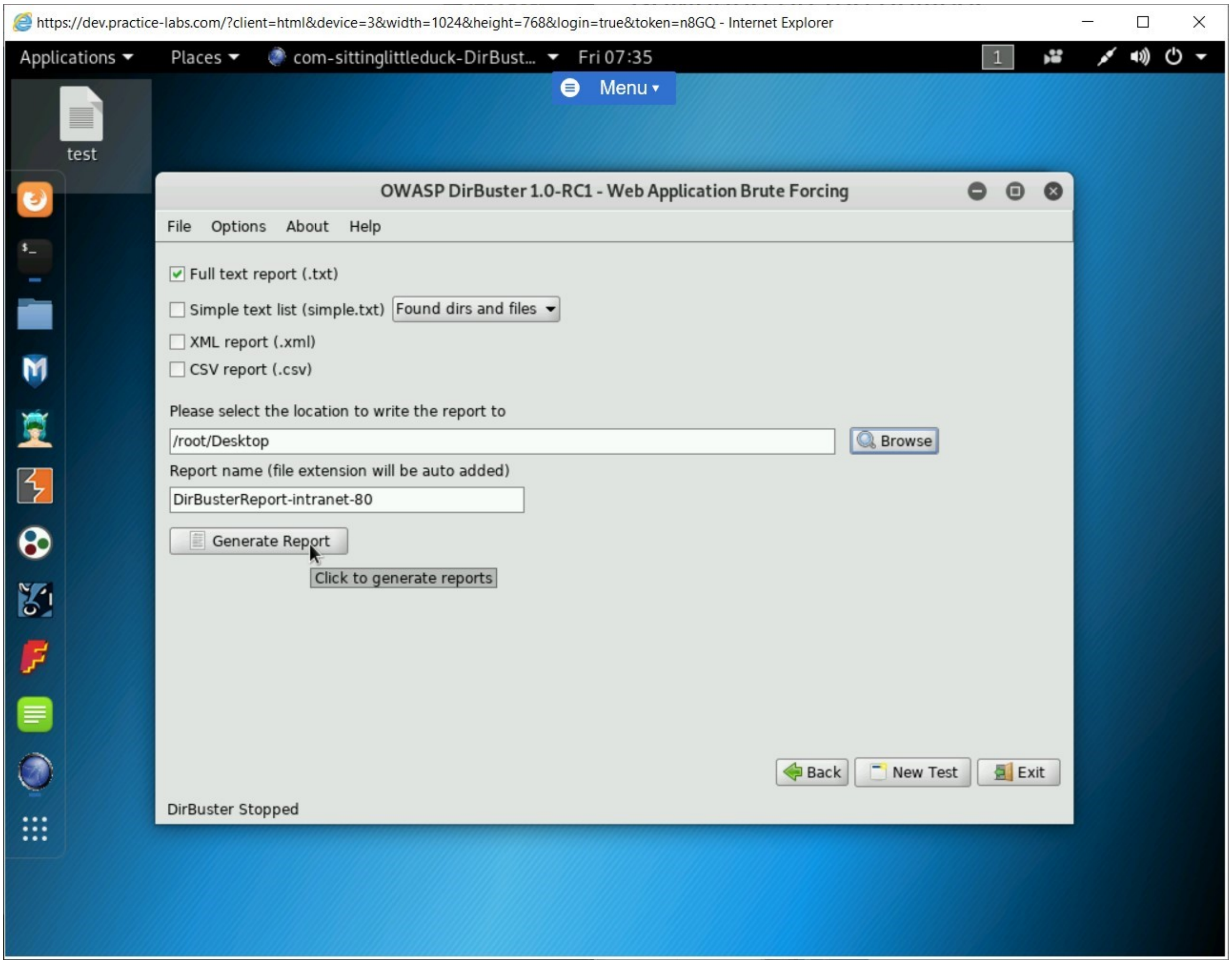
Files of Type: All Files

DirBuster Stopped

Figure 1.54 Screenshot of PLABKALI01: Setting the path to save the report.

Step 12

Click **Generate Report**.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
com-sittinglittleduck-DirBust...
Fri 07:35
Menu
test
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Browse
Generate Report
Click to generate reports
Back
New Test
Exit

☑ Full text report (.txt)

☐ Simple text list (simple.txt) Found dirs and files

☐ XML report (.xml)

☐ CSV report (.csv)

Please select the location to write the report to

/root/Desktop

Report name (file extension will be auto added)

DirBusterReport-intranet-80

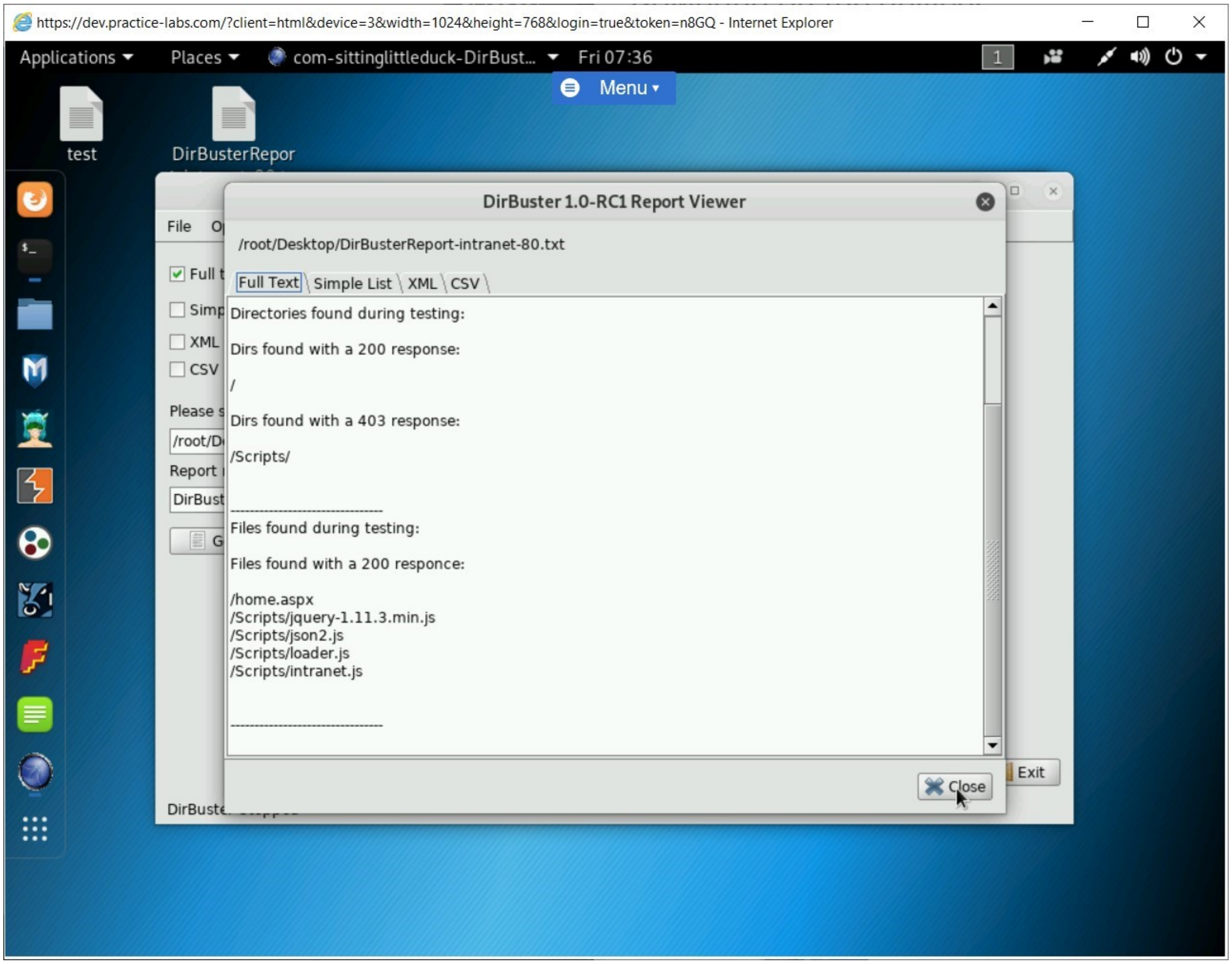
DirBuster Stopped

Figure 1.55 Screenshot of PLABKALI01: Clicking the Generate Report button.

Step 13

The **DirBuster 1.0-RC1 Report Viewer** dialog box is displayed. Notice the list of all files and directories that have been discovered.

Click **Close**.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
com-sittinglittleduck-DirBust...
Fri 07:36
Menu
test
DirBusterRepor
DirBuster 1.0-RC1 Report Viewer
File
Full Text
Simple List
XML
CSV
Close
Exit

/root/Desktop/DirBusterReport-intranet-80.txt

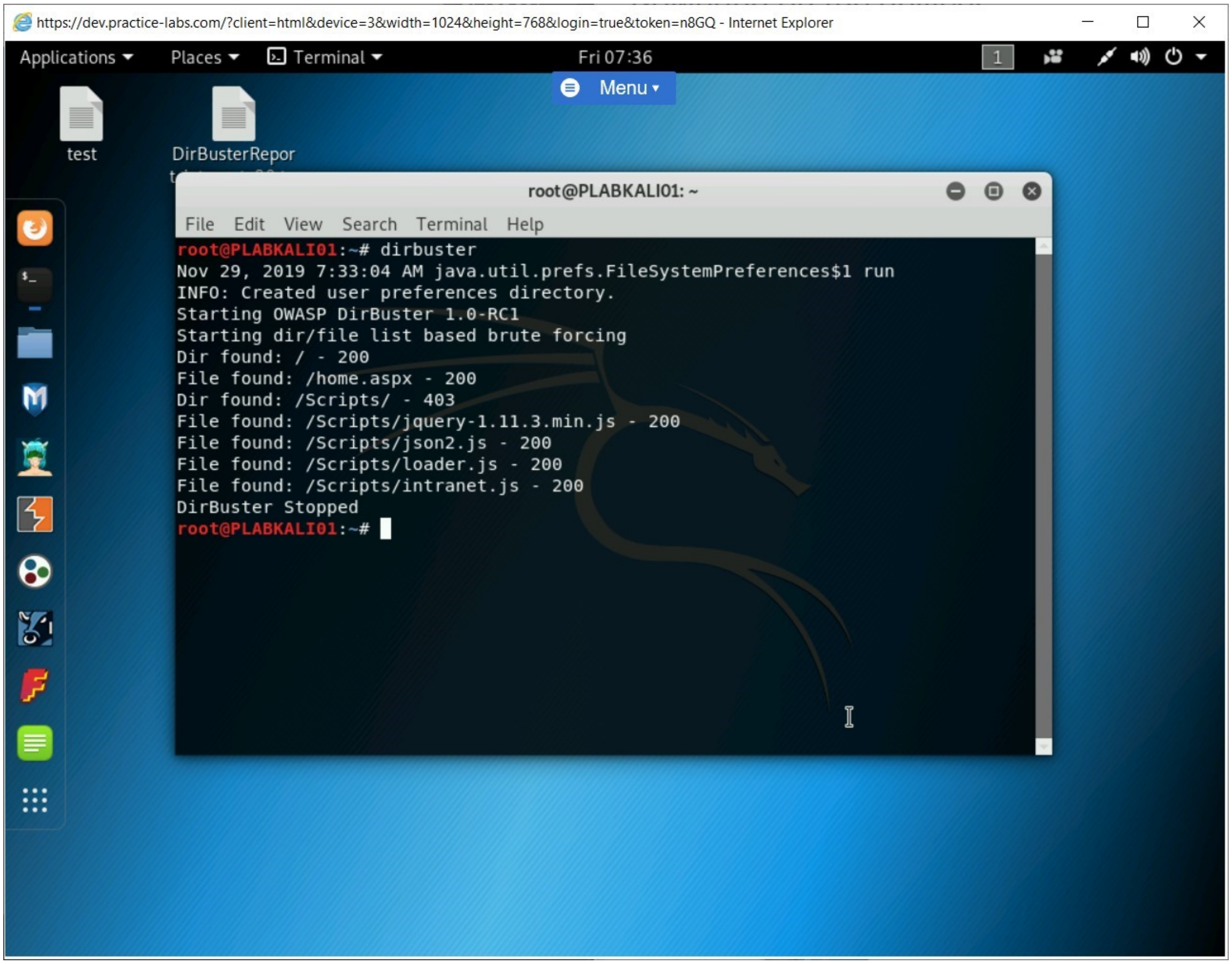
```
Directories found during testing:

Dirs found with a 200 response:

/

Dirs found with a 403 response:

/Scripts/


--------------------------------
Files found during testing:

Files found with a 200 responce:

/home.aspx
/Scripts/jquery-1.11.3.min.js
/Scripts/json2.js
/Scripts/loader.js
/Scripts/intranet.js


--------------------------------
```

Figure 1.56 Screenshot of PLABKALI01: Showing the discovered files and directories.

Step 14

Click **Exit** to close the **DirBuster** window.

You are back on the terminal window. Notice that a brief about the files and directories are also displayed.



https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 07:36
Menu
test
DirBusterRepor
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# dirbuster
Nov 29, 2019 7:33:04 AM java.util.prefs.FileSystemPreferences$1 run
INFO: Created user preferences directory.
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
File found: /home.aspx - 200
Dir found: /Scripts/ - 403
File found: /Scripts/jquery-1.11.3.min.js - 200
File found: /Scripts/json2.js - 200
File found: /Scripts/loader.js - 200
File found: /Scripts/intranet.js - 200
DirBuster Stopped
root@PLABKALI01:~# 
```

Figure 1.57 Screenshot of PLABKALI01: Showing the brief about files and directories.

Task 5 - Use Skipfish to Perform Webserver Reconnaissance

Skipfish is a tool that is available in Kali Linux. The sole purpose of Skipfish is to perform a deep reconnaissance of the Webserver and the deployed Web applications. Using Skipfish, you can collect a great deal of information, which will help you detect the vulnerabilities in the Webserver. You can then close the vulnerabilities to ensure optimal protection for the Webserver. You will be able to locate Webserver and Web application vulnerabilities when you use a vulnerability scan. This is the first task that you should perform after deploying a Webserver.

In this task, you will learn to use Skipfish. To use Skipfish, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABKALI01**. The terminal window should be open.

Clear the screen by entering the following command:

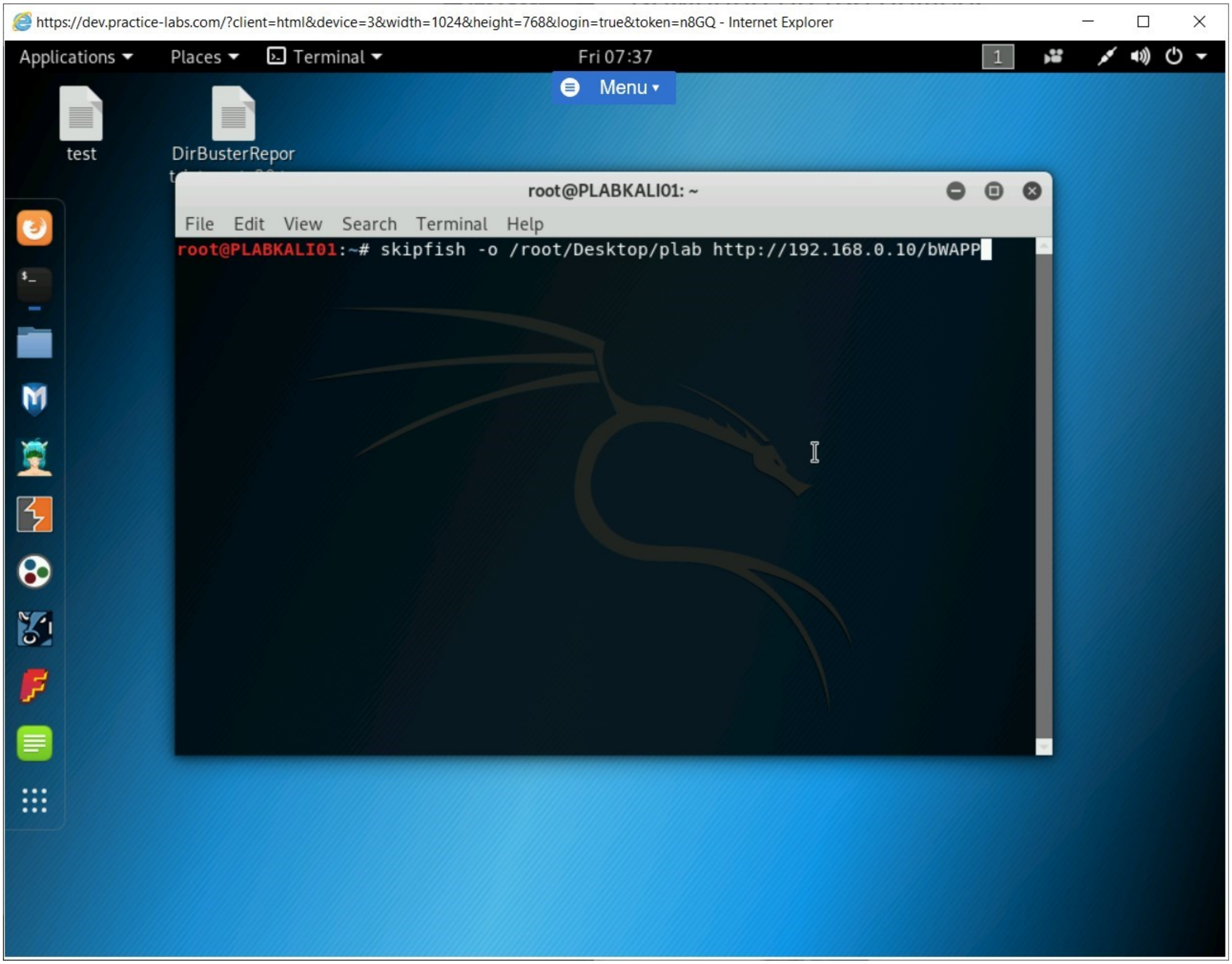
```
clear
```

To use Skipfish, type the following command:

> ***Note:*** *The -o parameter defines the directory in which a scan report will be saved.*

```
skipfish -o /root/Desktop/plab http://192.168.0.10/bWAPP
```

Press **Enter**.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 07:37
Menu
test
DirBusterRepor
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

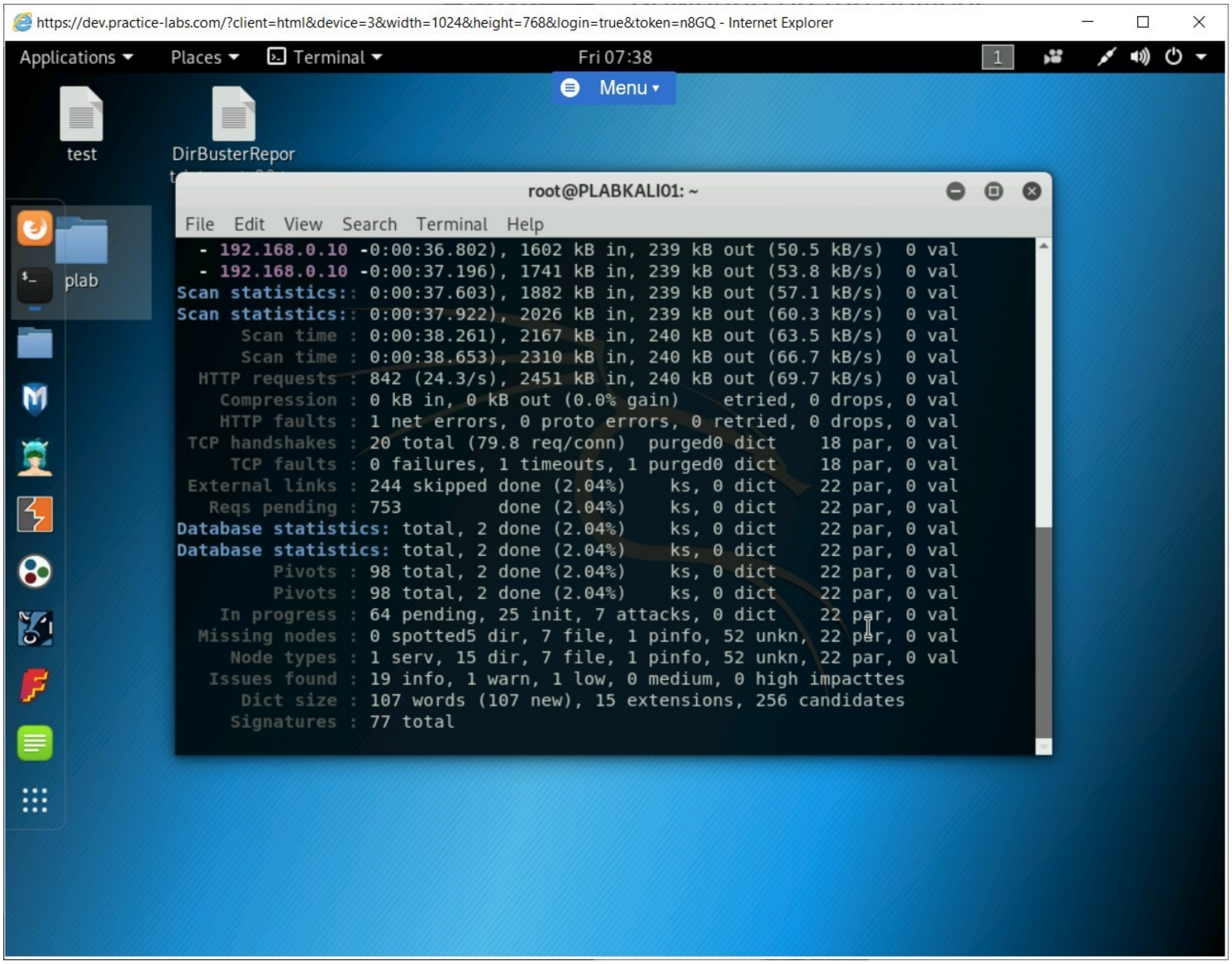
```
root@PLABKALI01:~# skipfish -o /root/Desktop/plab http://192.168.0.10/bWAPP
```

Step 2

You need to press **Enter** to start the scanning process.

Notice that the **plab** directory is now created on the desktop.

The scanning process is initiated. The scanning process duration depends on the size of the Web application. In the lab environment, it may take up to **30 minutes**.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 07:38
Menu
test
DirBusterRepor
plab
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

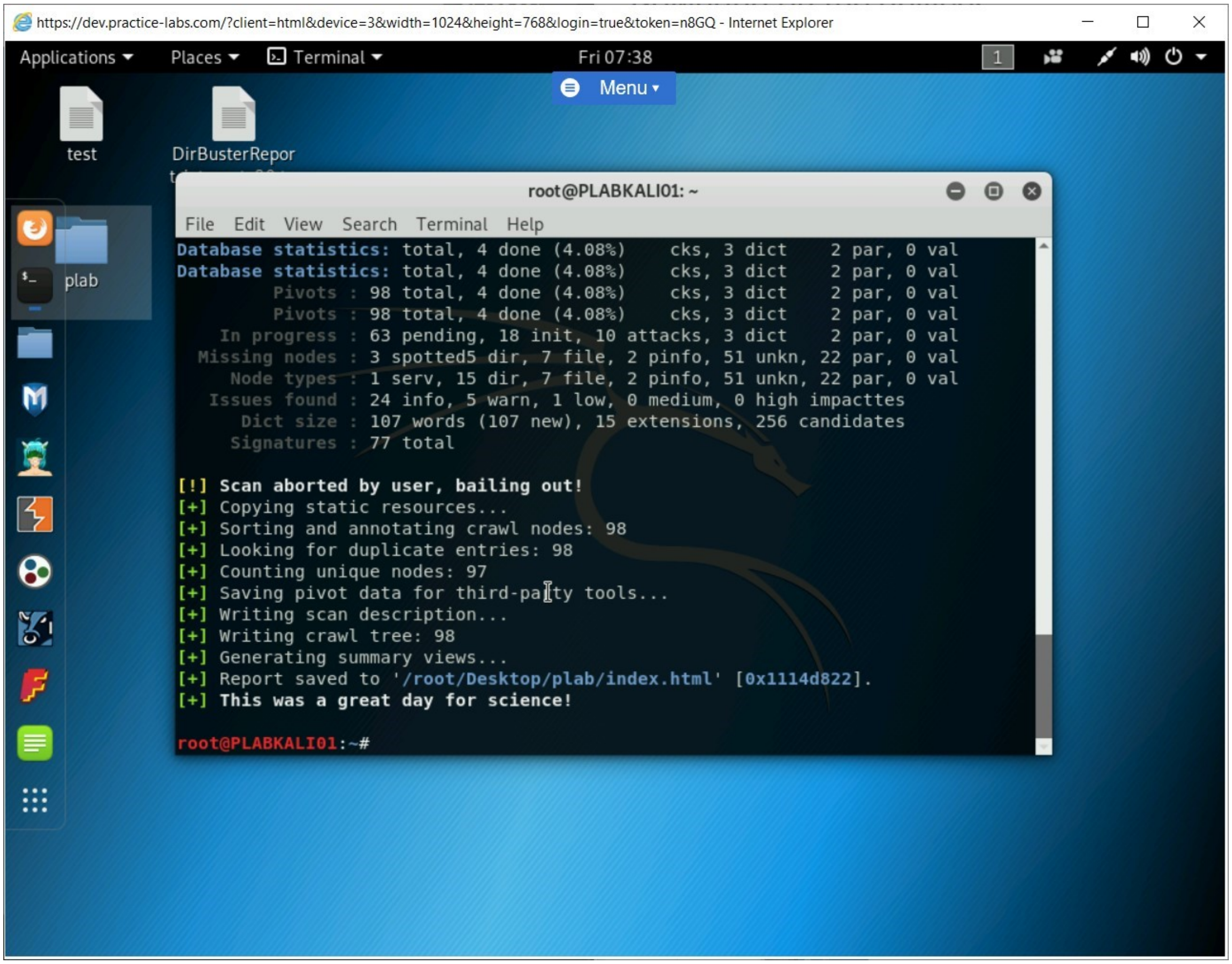
```
  - 192.168.0.10 -0:00:36.802), 1602 kB in, 239 kB out (50.5 kB/s)  0 val
  - 192.168.0.10 -0:00:37.196), 1741 kB in, 239 kB out (53.8 kB/s)  0 val
Scan statistics:: 0:00:37.603), 1882 kB in, 239 kB out (57.1 kB/s)  0 val
Scan statistics:: 0:00:37.922), 2026 kB in, 239 kB out (60.3 kB/s)  0 val
      Scan time : 0:00:38.261), 2167 kB in, 240 kB out (63.5 kB/s)  0 val
      Scan time : 0:00:38.653), 2310 kB in, 240 kB out (66.7 kB/s)  0 val
  HTTP requests : 842 (24.3/s), 2451 kB in, 240 kB out (69.7 kB/s)  0 val
    Compression : 0 kB in, 0 kB out (0.0% gain)    etried, 0 drops, 0 val
    HTTP faults : 1 net errors, 0 proto errors, 0 retried, 0 drops, 0 val
 TCP handshakes : 20 total (79.8 req/conn)  purged0 dict    18 par, 0 val
     TCP faults : 0 failures, 1 timeouts, 1 purged0 dict    18 par, 0 val
 External links : 244 skipped done (2.04%)    ks, 0 dict    22 par, 0 val
   Reqs pending : 753          done (2.04%)    ks, 0 dict    22 par, 0 val
Database statistics: total, 2 done (2.04%)    ks, 0 dict    22 par, 0 val
Database statistics: total, 2 done (2.04%)    ks, 0 dict    22 par, 0 val
         Pivots : 98 total, 2 done (2.04%)    ks, 0 dict    22 par, 0 val
         Pivots : 98 total, 2 done (2.04%)    ks, 0 dict    22 par, 0 val
    In progress : 64 pending, 25 init, 7 attacks, 0 dict    22 par, 0 val
  Missing nodes : 0 spotted5 dir, 7 file, 1 pinfo, 52 unkn, 22 par, 0 val
     Node types : 1 serv, 15 dir, 7 file, 1 pinfo, 52 unkn, 22 par, 0 val
   Issues found : 19 info, 1 warn, 1 low, 0 medium, 0 high impacttes
      Dict size : 107 words (107 new), 15 extensions, 256 candidates
     Signatures : 77 total
```

Figure 1.59 Screenshot of PLABKALI01: Showing process of discovering information from the Webserver.

Step 3

Since in the lab environment, you have limited time, you can stop the scanning process by pressing the **Ctrl + c** keys. However, in the real environment, you must let the process complete to get an overall security posture of the Webserver.

A brief summary of the scanning results is displayed. A detailed report is saved with the name **index.html** in the **/root/Desktop/plab** directory.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 07:38
Menu
test
DirBusterRepor
plab
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
Database statistics: total, 4 done (4.08%)    cks, 3 dict    2 par, 0 val
Database statistics: total, 4 done (4.08%)    cks, 3 dict    2 par, 0 val
         Pivots : 98 total, 4 done (4.08%)    cks, 3 dict    2 par, 0 val
         Pivots : 98 total, 4 done (4.08%)    cks, 3 dict    2 par, 0 val
    In progress : 63 pending, 18 init, 10 attacks, 3 dict    2 par, 0 val
  Missing nodes : 3 spotted5 dir, 7 file, 2 pinfo, 51 unkn, 22 par, 0 val
     Node types : 1 serv, 15 dir, 7 file, 2 pinfo, 51 unkn, 22 par, 0 val
   Issues found : 24 info, 5 warn, 1 low, 0 medium, 0 high impacttes
      Dict size : 107 words (107 new), 15 extensions, 256 candidates
     Signatures : 77 total

[!] Scan aborted by user, bailing out!
[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 98
[+] Looking for duplicate entries: 98
[+] Counting unique nodes: 97
[+] Saving pivot data for third-party tools...
[+] Writing scan description...
[+] Writing crawl tree: 98
[+] Generating summary views...
[+] Report saved to '/root/Desktop/plab/index.html' [0x1114d822].
[+] This was a great day for science!

root@PLABKALI01:~#
```

Figure 1.60 Screenshot of PLABKALI01: Showing the output of the skipfish command.

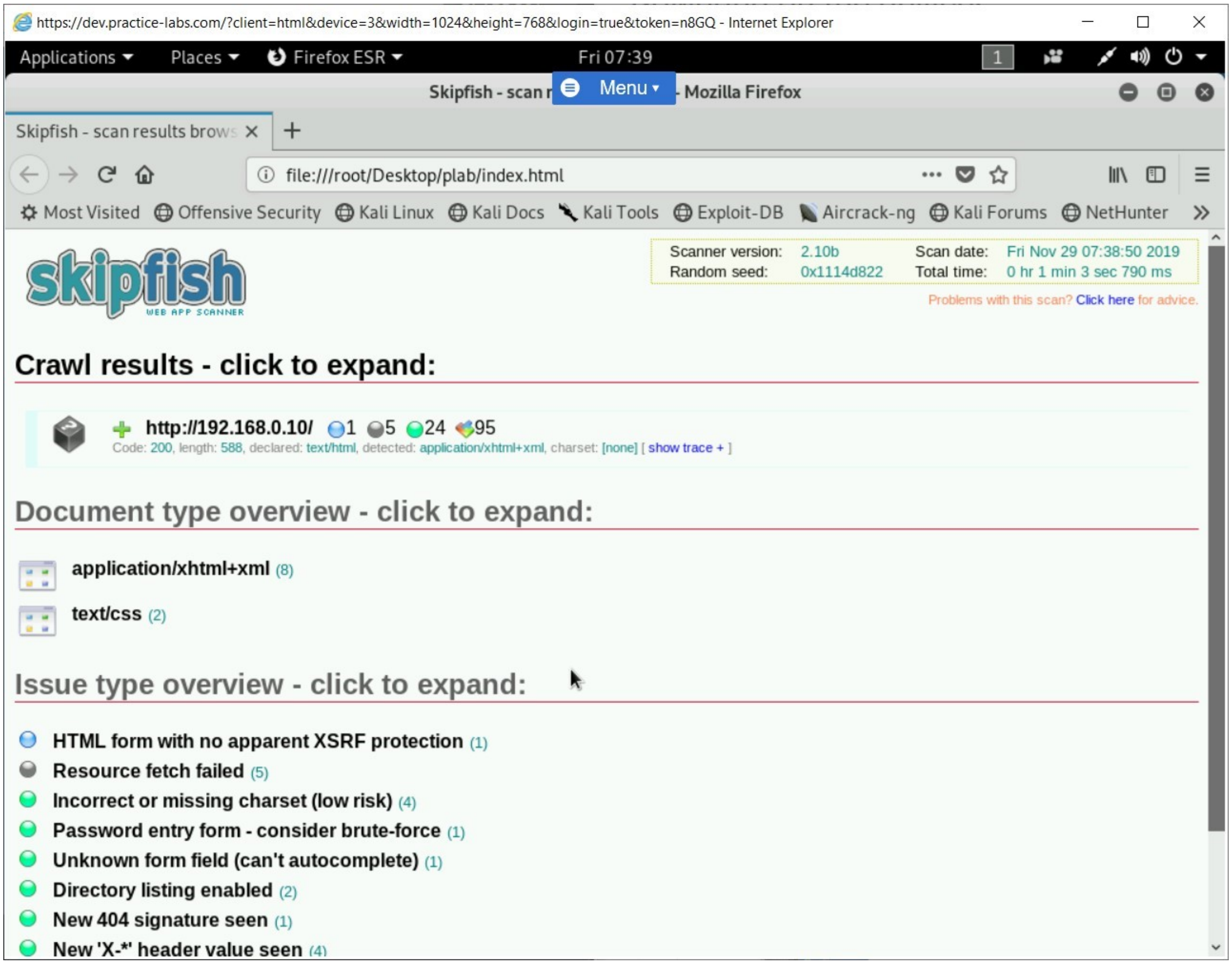
Step 4

To view the scan report, type the following command:

```
firefox /root/Desktop/plab/index.html
```

Press **Enter**.

The **Firefox** window opens and displays the **index.html** file.



Scanner version: 2.10b Scan date: Fri Nov 29 07:38:50 2019
Random seed: 0x1114d822 Total time: 0 hr 1 min 3 sec 790 ms

Problems with this scan? Click here for advice.

Crawl results - click to expand:

http://192.168.0.10/ 1 5 24 95
Code: 200, length: 588, declared: text/html, detected: application/xhtml+xml, charset: [none] [show trace +]

Document type overview - click to expand:

application/xhtml+xml (8)
text/css (2)

Issue type overview - click to expand:

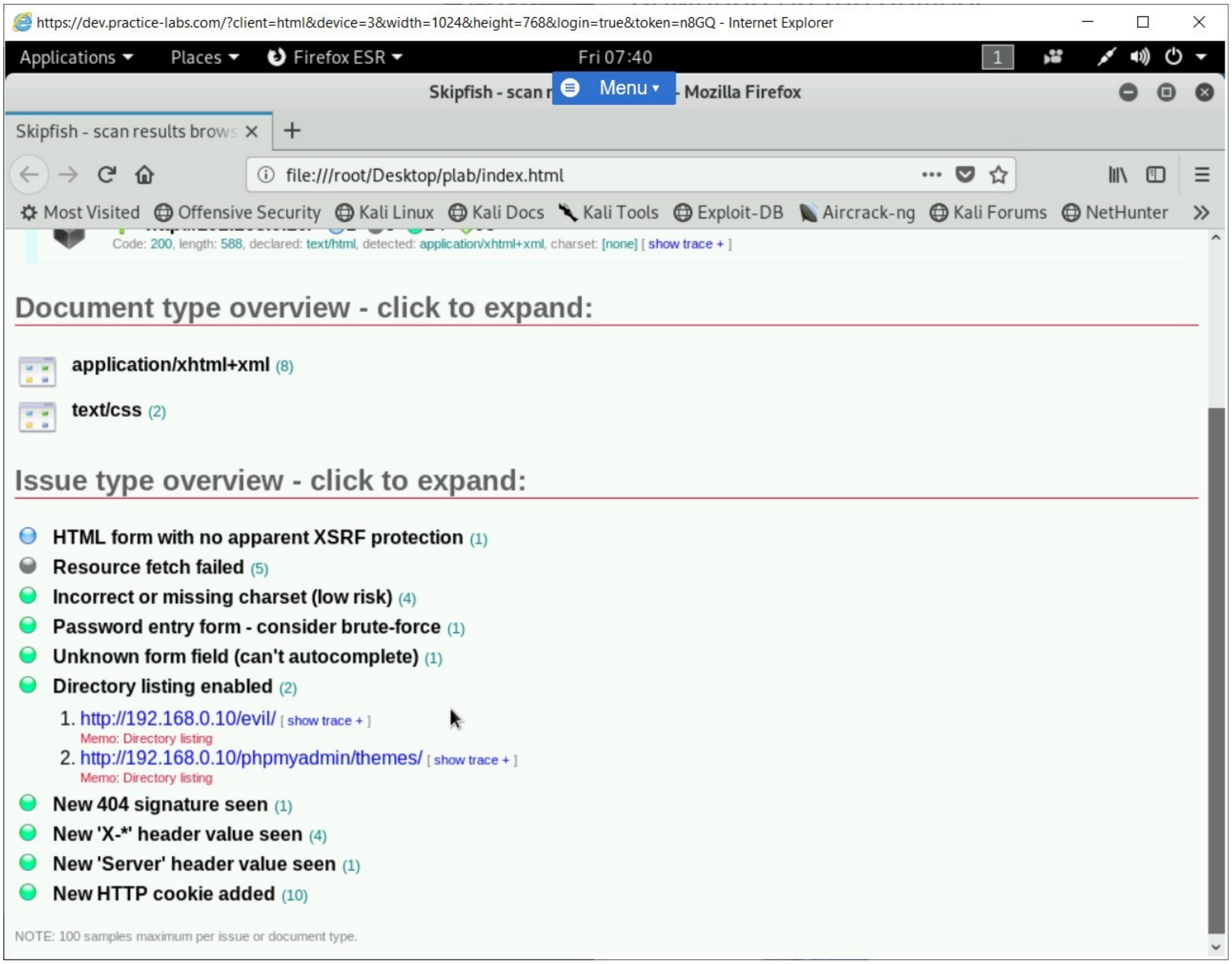
- HTML form with no apparent XSRF protection (1)
- Resource fetch failed (5)
- Incorrect or missing charset (low risk) (4)
- Password entry form - consider brute-force (1)
- Unknown form field (can't autocomplete) (1)
- Directory listing enabled (2)
- New 404 signature seen (1)
- New 'X-*' header value seen (4)

Figure 1.61 Screenshot of PLABKALI01: Showing the discovered issues on the Webserver.

Step 5

Click on **Directory listing enabled** in the **Issue type overview** section.Two different paths are shown that have directory listing enabled.

If time permits, you can go through the other issues that have been located on the Webserver.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Firefox ESR
Fri 07:40
Skipfish - scan r
Menu
- Mozilla Firefox
Skipfish - scan results brows
file:///root/Desktop/plab/index.html
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter

Code: 200, length: 588, declared: text/html, detected: application/xhtml+xml, charset: [none] [show trace +]

Document type overview - click to expand:

application/xhtml+xml (8)

text/css (2)

Issue type overview - click to expand:

- ● HTML form with no apparent XSRF protection (1)
- ● Resource fetch failed (5)
- ● Incorrect or missing charset (low risk) (4)
- ● Password entry form - consider brute-force (1)
- ● Unknown form field (can't autocomplete) (1)
- ● Directory listing enabled (2)
  1. http://192.168.0.10/evil/ [show trace +]
     Memo: Directory listing
  2. http://192.168.0.10/phpmyadmin/themes/ [show trace +]
     Memo: Directory listing
- ● New 404 signature seen (1)
- ● New 'X-*' header value seen (4)
- ● New 'Server' header value seen (1)
- ● New HTTP cookie added (10)

NOTE: 100 samples maximum per issue or document type.

Figure 1.62 Screenshot of PLABKALI01: Showing the URLs with the directory listing enabled.

Task 6 - Find Files on a Webserver using Metasploit Framework

Metasploit framework is the most widely used tool in exploiting vulnerabilities. A free edition is available in Kali Linux. Metasploit has a modular and flexible architecture that helps you develop new exploits as more and more vulnerabilities are discovered. On the other hand, it is also used in penetration testing.

You can use the Metasploit framework with or without a database. If you configure it with the database, then Metasploit will be able to track what you do within the framework.

You can use the Metasploit Framework for various reasons - starting with finding files to penetrating a system or a network. In this task, you will learn to find files on a

Webserver using the Metasploit Framework.

Step 1

Ensure that you have logged into the Kali Linux system.

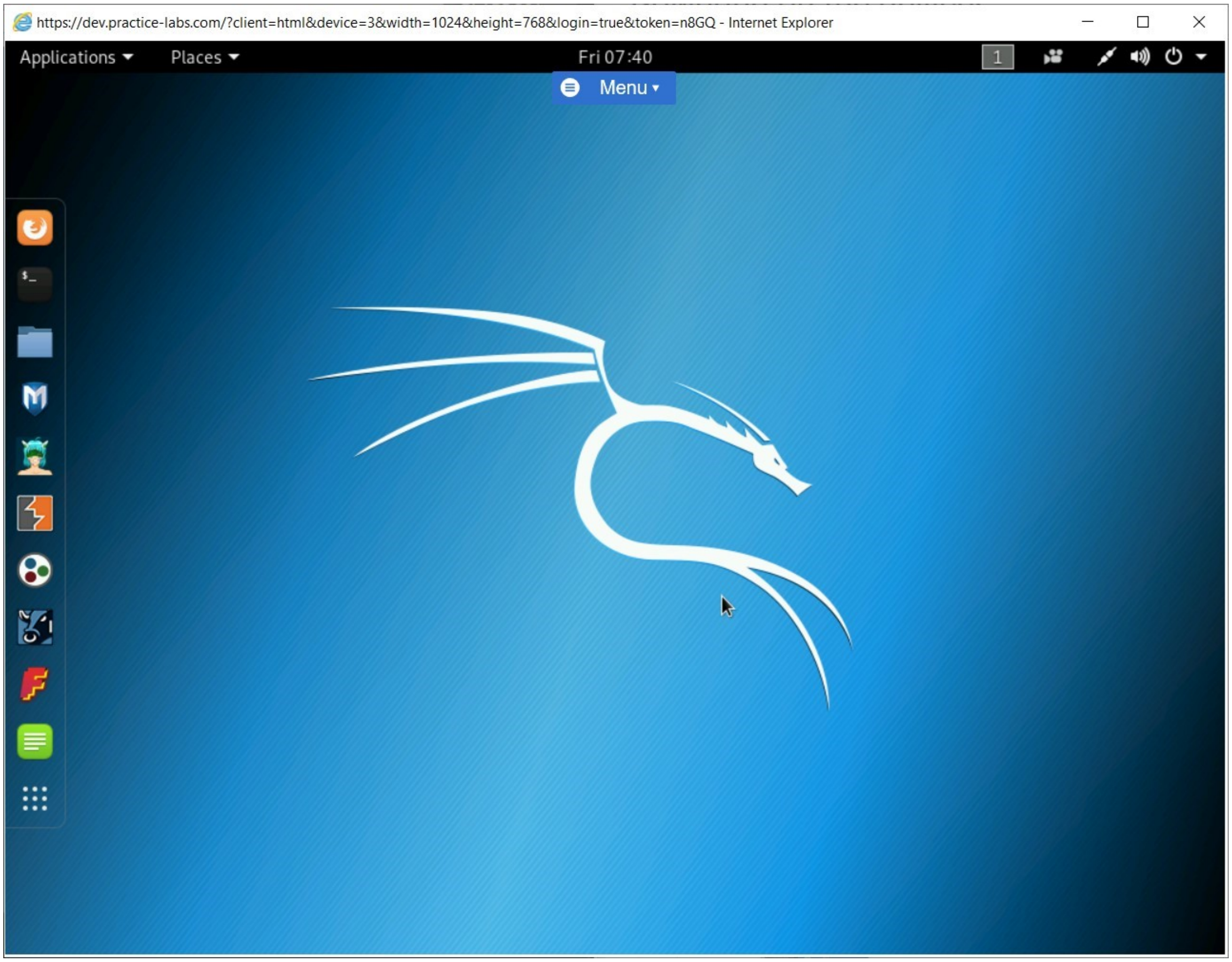

https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Fri 07:40
1
Menu

Figure 1.63 Screenshot of PLABKALI01: Showing the desktop of PLABKALI01.

Step 2

On the desktop, in the left pane, click the **Metasploit framework** icon

Note: Please be aware that a shell may appear but may default to a terminal layout. In order to acess Metasploit framework, use the following command:
Root@PLABKALI01:~# msfconsole -q

If this command is successful you should see the terimal default to:
Msf5>
You may proceed to step 3

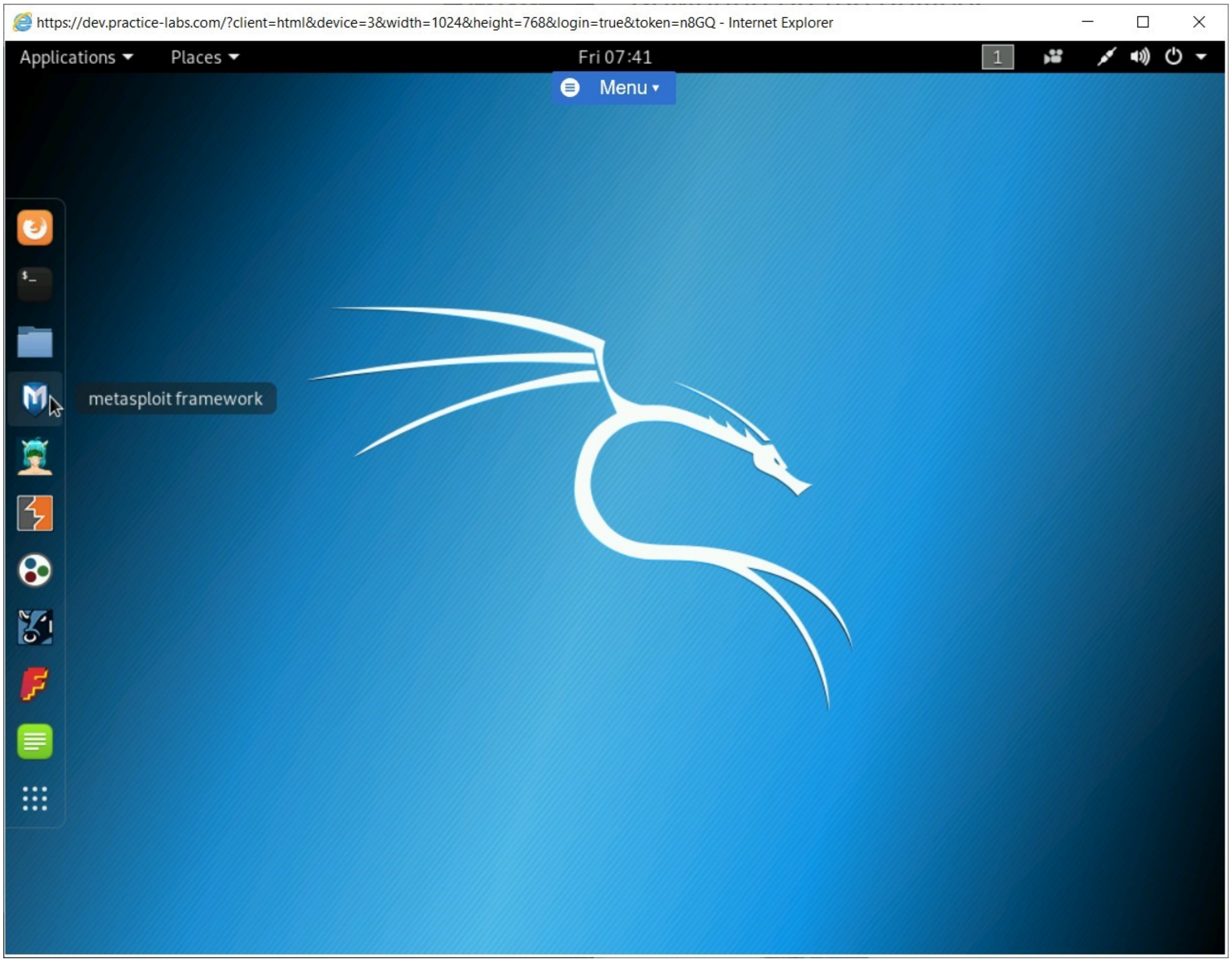

https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Fri 07:41
1
Menu
metasploit framework

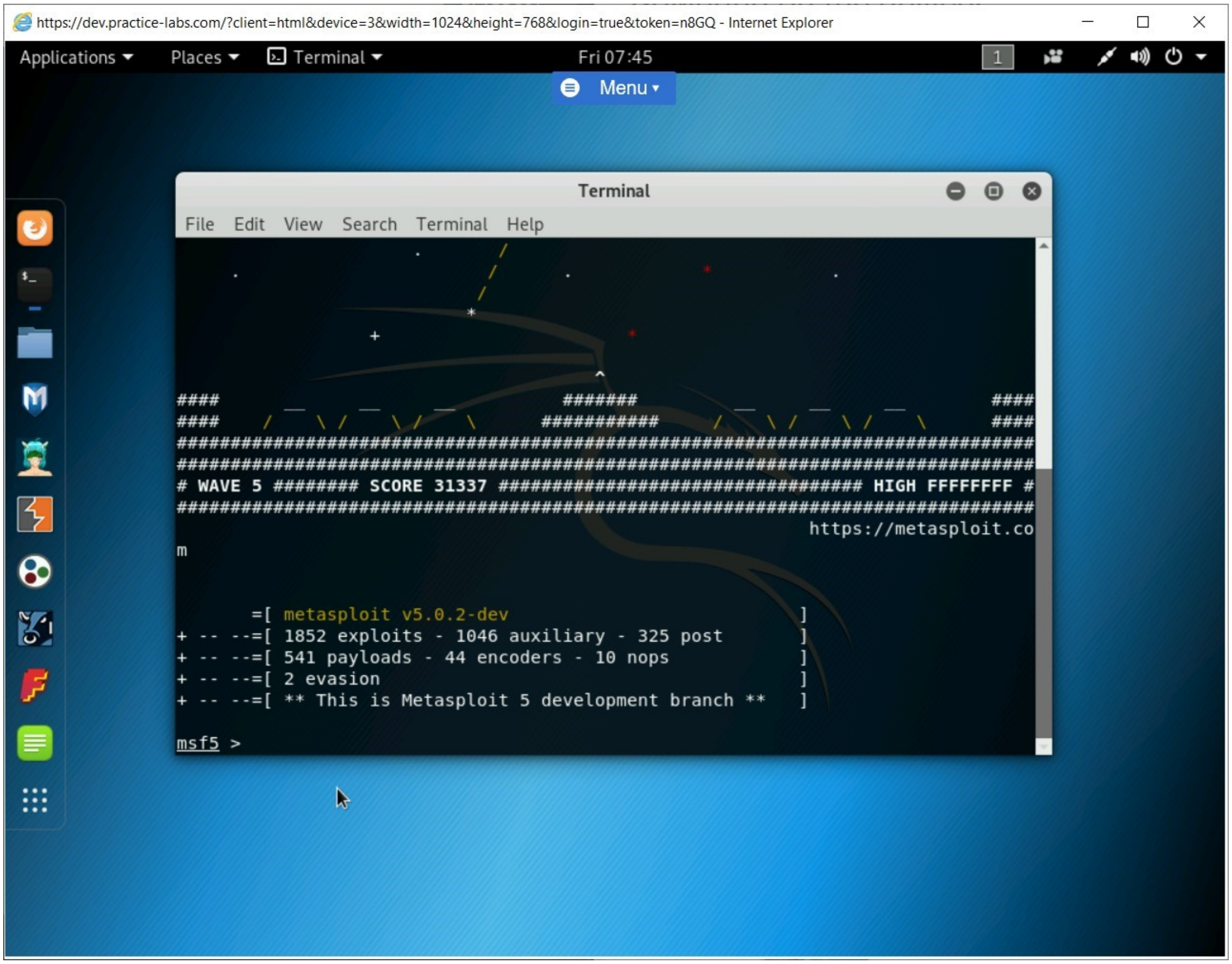
Figure 1.64 Screenshot of PLABKALI01: Clicking the Metasploit framework icon in the left pane.

Step 3

The terminal window is displayed. It displays a database and its user creation. Then, it proceeds to create the database schema.

The **metasploit framework** has started now.

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


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 07:45
Menu
Terminal
File
Edit
View
Search
Terminal
Help

```
                      .          /
     .                          /         .              *              .
                               /
                              *
                  +                            *

                                       ^
####      __     __     __          #######          __     __     __       ####
####    /    \ /    \ /    \      ###########      /    \ /    \ /    \     ####
################################################################################
################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################
                                                           https://metasploit.co
m


       =[ metasploit v5.0.2-dev                           ]
+ -- --=[ 1852 exploits - 1046 auxiliary - 325 post       ]
+ -- --=[ 541 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]
+ -- --=[ ** This is Metasploit 5 development branch **   ]

msf5 >
```

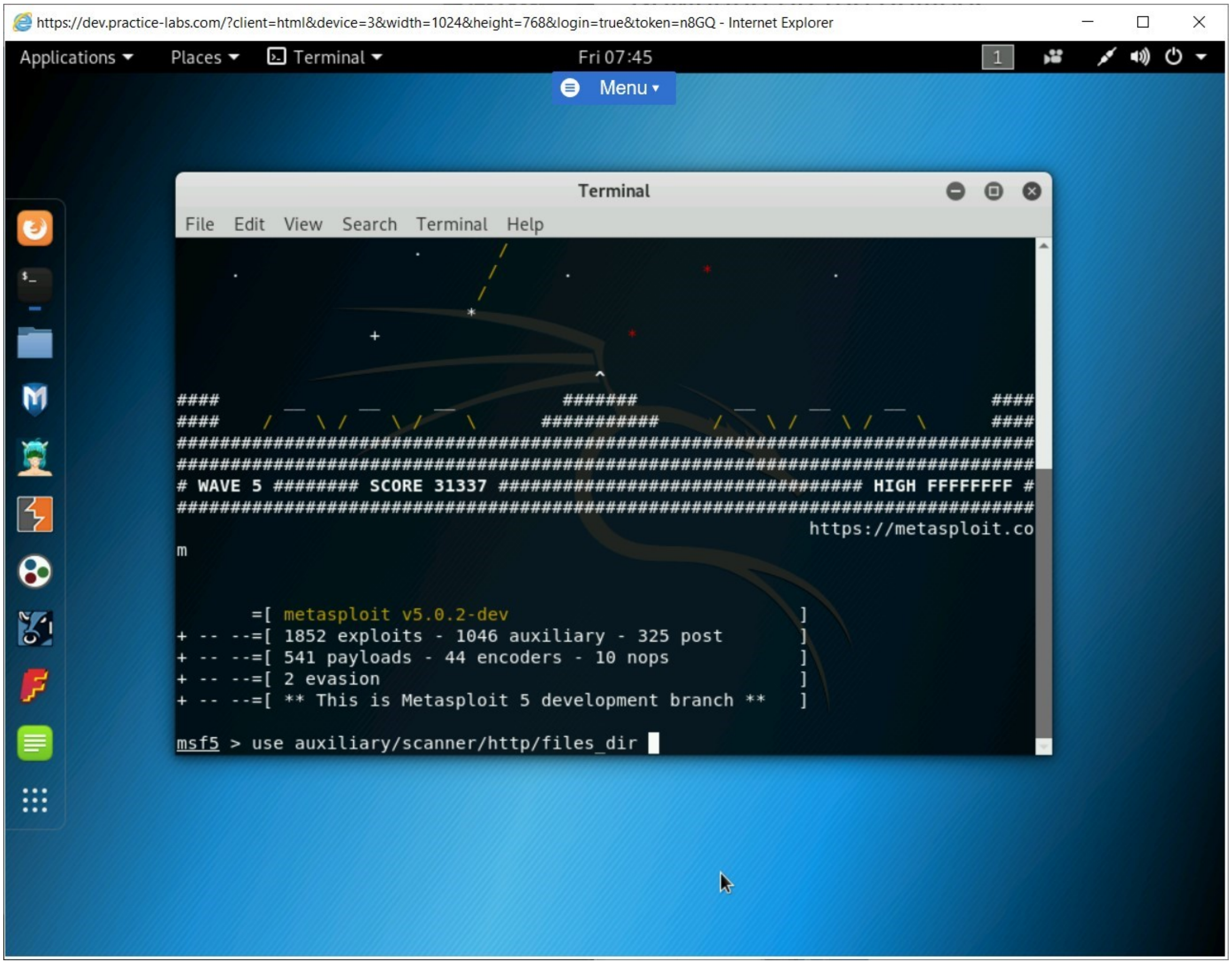
Figure 1.65 Screenshot of PLABKALI01: Showing the msf5 prompt after the Metasploit framework starts.

Step 4

You will now use the **files_dir** module to find files on the target system. The **files_dir** module uses a wordlist to find these files. To do this, type the following command:

```
use auxiliary/scanner/http/files_dir
```

Press **Enter**.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 07:45
Menu
Terminal
File Edit View Search Terminal Help

```
####                                #######                                ####
####    /  \ /  \ /  \            ###########            /  \ /  \ /  \        ####
################################################################################
################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################
                                                           https://metasploit.co
m


       =[ metasploit v5.0.2-dev                          ]
+ -- --=[ 1852 exploits - 1046 auxiliary - 325 post       ]
+ -- --=[ 541 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]
+ -- --=[ ** This is Metasploit 5 development branch **   ]

msf5 > use auxiliary/scanner/http/files_dir
```

Figure 1.66 Screenshot of PLABKALI01 Entering the command to use the files_dir module.

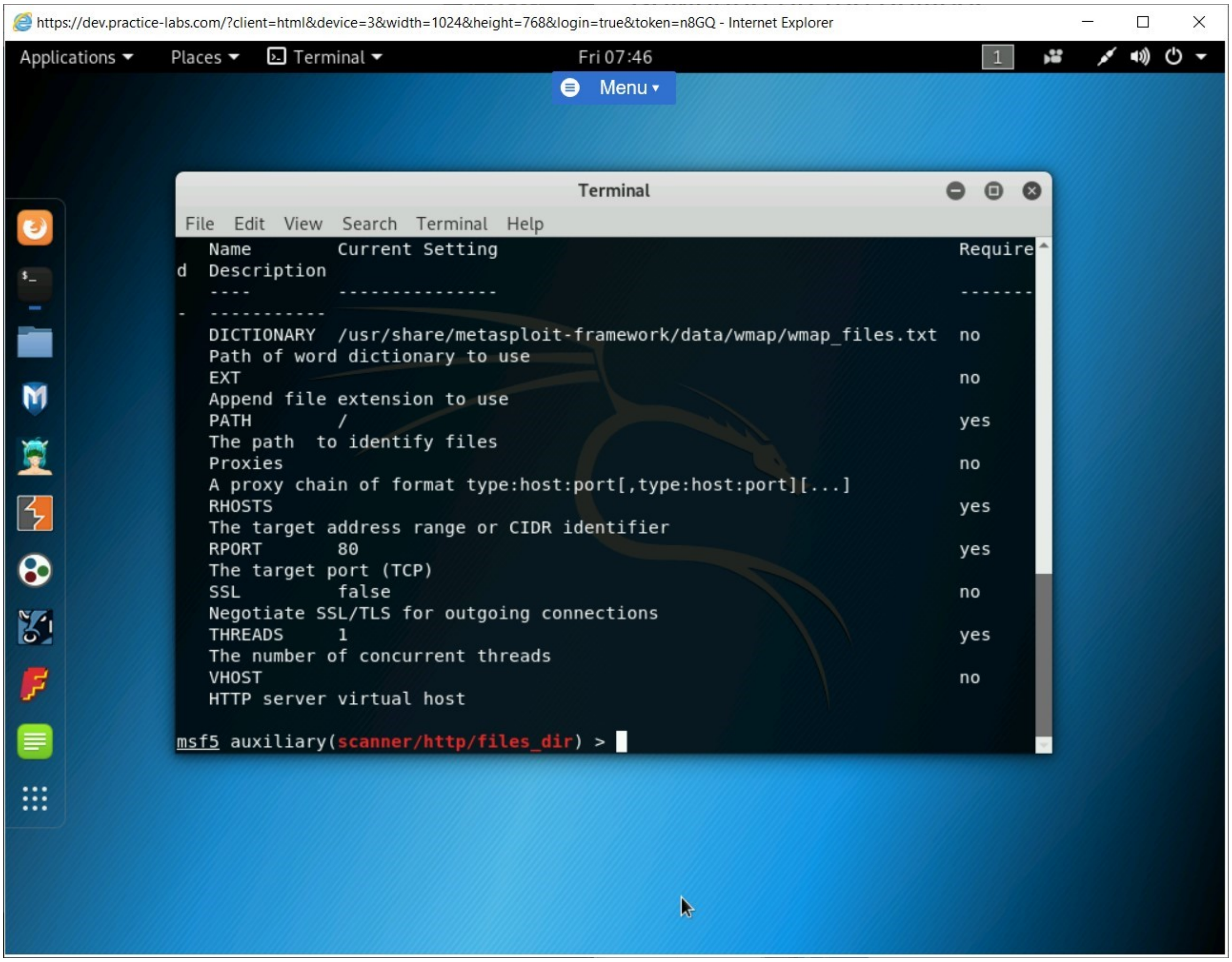
Step 5

The **files_dir** module is now loaded. Let's check the configuration options for the **files_dir** module. Type the following command:

```
show options
```

Press **Enter**.

Various options are displayed. Some of these are configured by default, and some you need to configure. Notice that the **DICTIONARY** option is already configured with a built-in dictionary that contains the keywords for searching on the target system.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 07:46
Menu
Terminal
File Edit View Search Terminal Help

```
   Name        Current Setting                                           Require
d  Description
   ----        ---------------                                           -------
-  -----------
   DICTIONARY  /usr/share/metasploit-framework/data/wmap/wmap_files.txt  no
   Path of word dictionary to use
   EXT                                                                   no
   Append file extension to use
   PATH        /                                                         yes
   The path  to identify files
   Proxies                                                               no
   A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                                                                yes
   The target address range or CIDR identifier
   RPORT       80                                                        yes
   The target port (TCP)
   SSL         false                                                     no
   Negotiate SSL/TLS for outgoing connections
   THREADS     1                                                         yes
   The number of concurrent threads
   VHOST                                                                 no
   HTTP server virtual host

msf5 auxiliary(scanner/http/files_dir) >
```

Figure 1.67 Screenshot of PLABKALI01: Showing the discovered files and directories.

Step 6

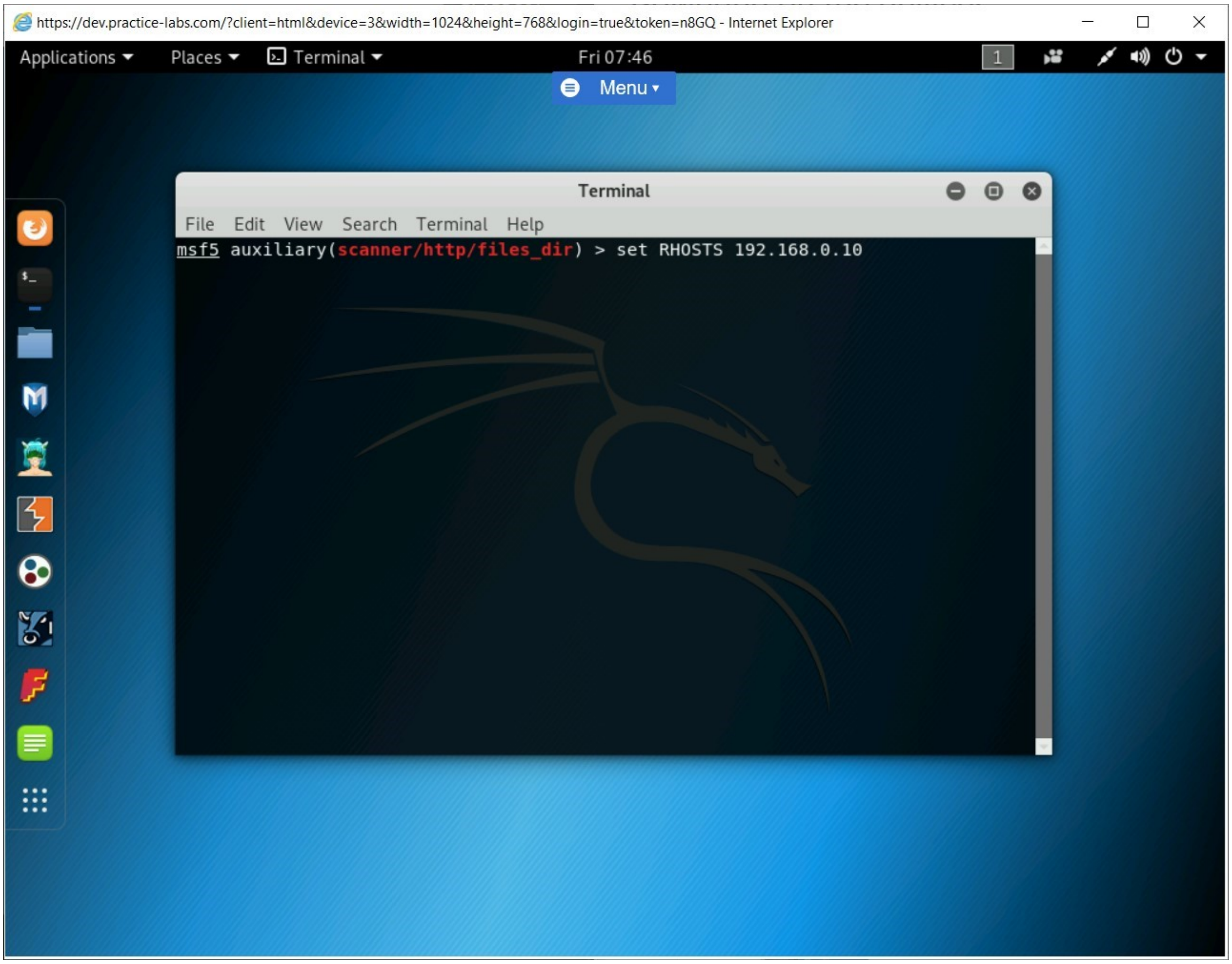
Clear the screen by entering the following command:

```
clear
```

You need to set now the target system that you want to exploit. To do this, type the following command:

```
set RHOSTS 192.168.0.10
```

Press **Enter**.



https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 07:46
Menu
Terminal
File Edit View Search Terminal Help

```
msf5 auxiliary(scanner/http/files_dir) > set RHOSTS 192.168.0.10
```

Figure 1.68 Screenshot of PLABKALI01: Showing the discovered files and directories.

Step 7

After you set the IP address of the target host, type the following command:

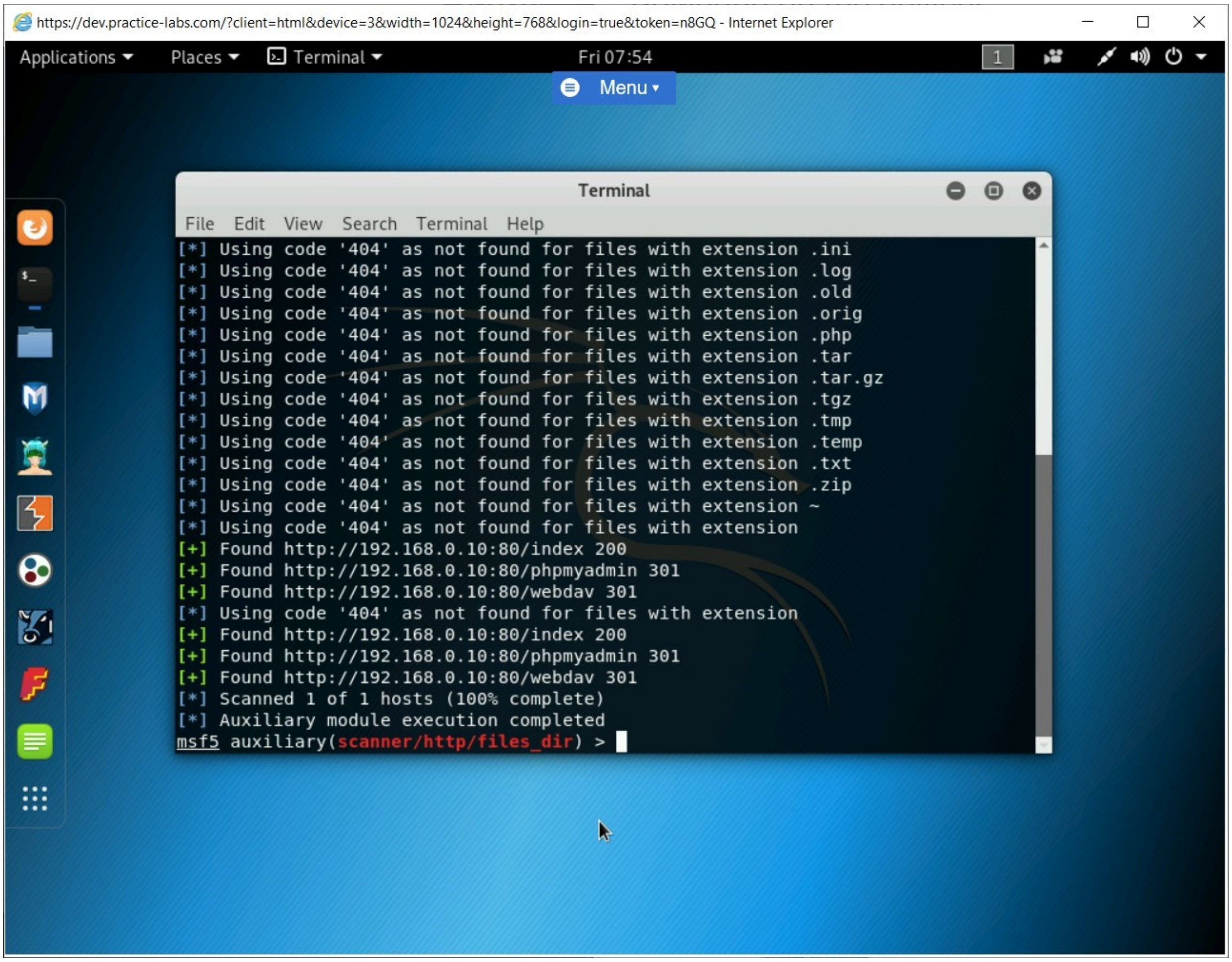
```
run
```

Press **Enter**.

The payload is now executed on the target host. It is now attempting to find files of specific types.

> ***Note:*** *The process of finding files of a specific type will run for a few minutes.*

After the process has completed, several files that can be useful to an attacker are found. Keep the terminal window open.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 07:54
Menu
Terminal
File Edit View Search Terminal Help

```
[*] Using code '404' as not found for files with extension .ini
[*] Using code '404' as not found for files with extension .log
[*] Using code '404' as not found for files with extension .old
[*] Using code '404' as not found for files with extension .orig
[*] Using code '404' as not found for files with extension .php
[*] Using code '404' as not found for files with extension .tar
[*] Using code '404' as not found for files with extension .tar.gz
[*] Using code '404' as not found for files with extension .tgz
[*] Using code '404' as not found for files with extension .tmp
[*] Using code '404' as not found for files with extension .temp
[*] Using code '404' as not found for files with extension .txt
[*] Using code '404' as not found for files with extension .zip
[*] Using code '404' as not found for files with extension ~
[*] Using code '404' as not found for files with extension
[+] Found http://192.168.0.10:80/index 200
[+] Found http://192.168.0.10:80/phpmyadmin 301
[+] Found http://192.168.0.10:80/webdav 301
[*] Using code '404' as not found for files with extension
[+] Found http://192.168.0.10:80/index 200
[+] Found http://192.168.0.10:80/phpmyadmin 301
[+] Found http://192.168.0.10:80/webdav 301
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/files_dir) >
```

Figure 1.69 Screenshot of PLABKALI01: Showing the discovered files and directories.

Task 7 - Scan for Options on a Webserver using Metasploit Framework

A Webserver can be configured with various options, such as TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, and so on. Using the Options module, you can search for these options.

In this task, you will search for various options available on a Webserver. To do this, perform the following steps:

Step 1

Ensure that you have logged into the Kali Linux system. Ensure that you are on the metasploit framework terminal.

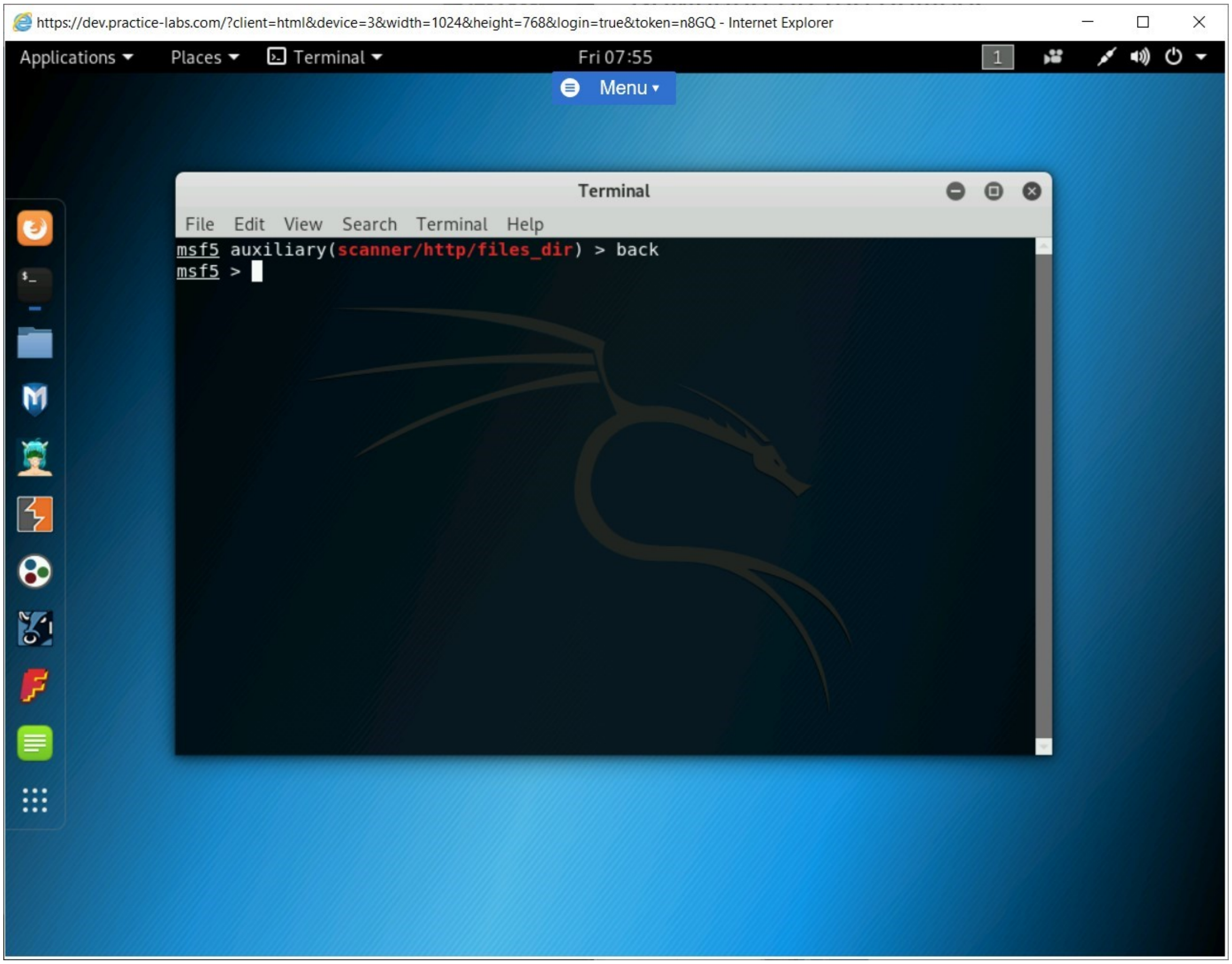
Clear the screen by entering the following command:

```
clear
```

You need to move out of the **files_dir** module. To do this, type the following command:

```
back
```

Press **Enter**.



https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 07:55
Menu
Terminal
File
Edit
View
Search
Terminal
Help

```
msf5 auxiliary(scanner/http/files_dir) > back
msf5 >
```

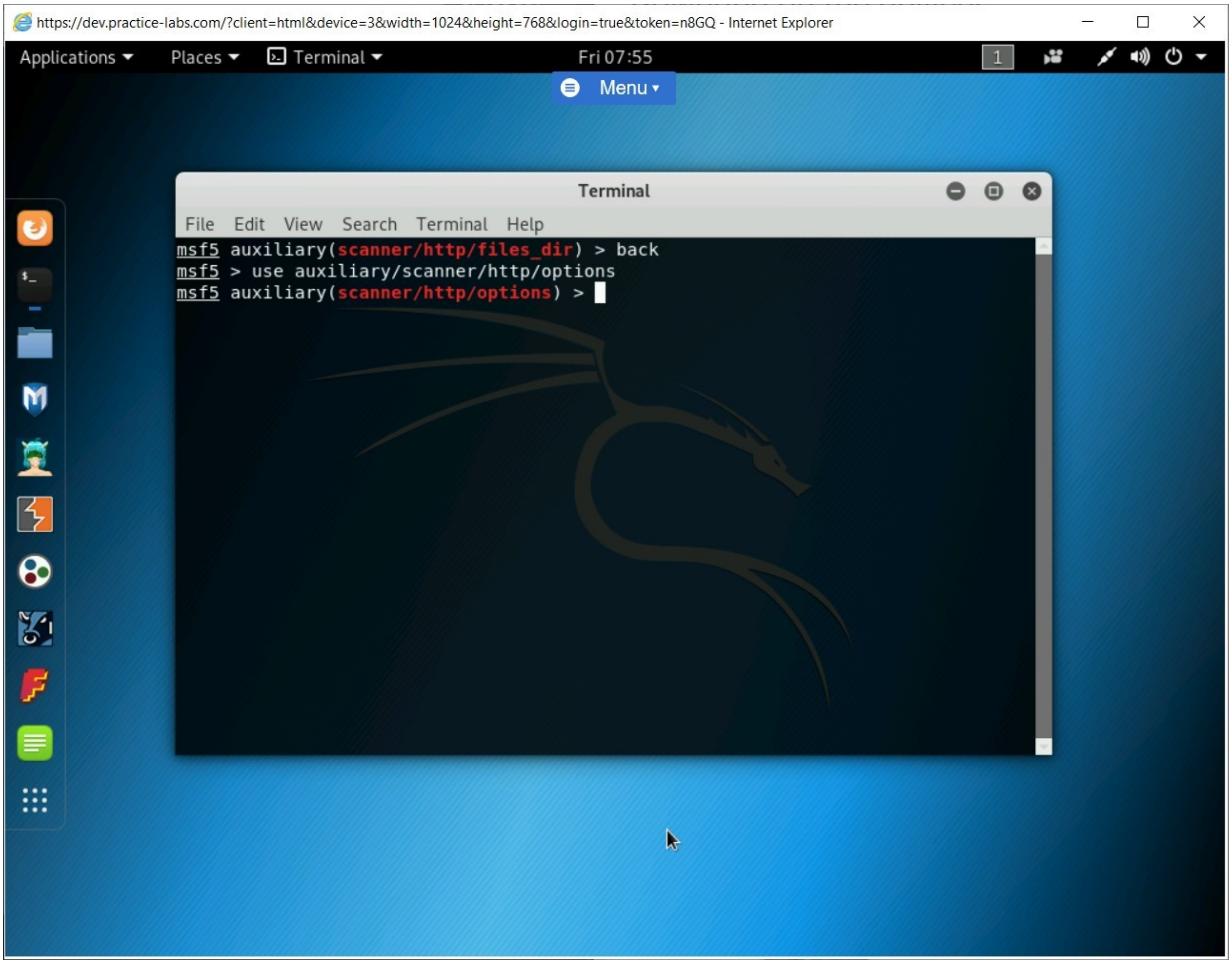
Figure 1.70 Screenshot of PLABKALI01: Entering the back command to go back to the Metasploit Framework prompt.

Step 2

You are back on the Metasploit Framework prompt. Now, you need to load the Options module. To do this, type the following command:

```
use auxiliary/scanner/http/options
```

Press **Enter**.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 07:55
Menu
Terminal
File Edit View Search Terminal Help

```
msf5 auxiliary(scanner/http/files_dir) > back
msf5 > use auxiliary/scanner/http/options
msf5 auxiliary(scanner/http/options) >
```

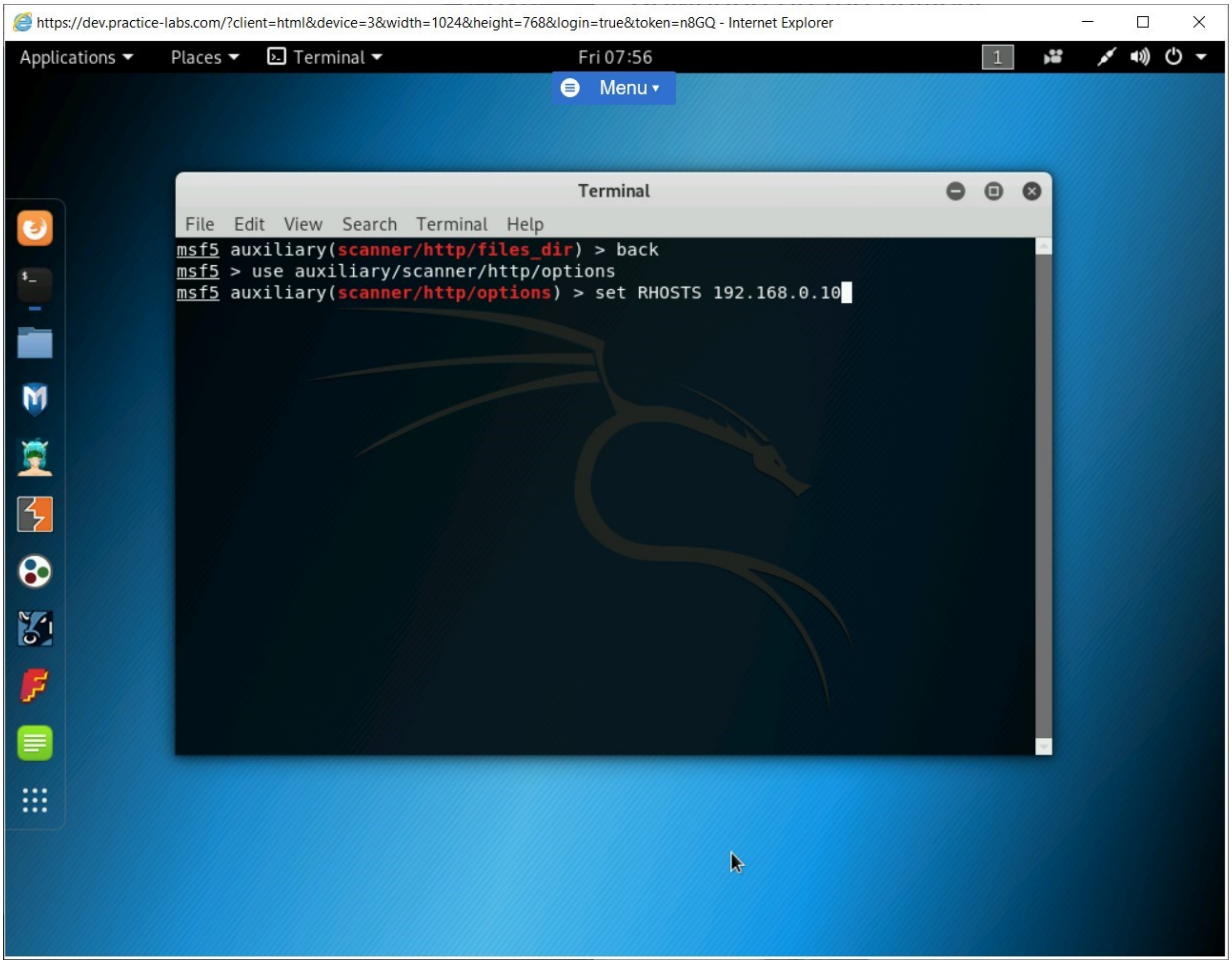
Figure 1.71 Screenshot of PLABKALI01: Entering the command to use the options module.

Step 3

You need to configure the target system now. To do this, type the following command:

```
set RHOSTS 192.168.0.10
```

Press **Enter**.



https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 07:56
Menu
Terminal
File Edit View Search Terminal Help

```
msf5 auxiliary(scanner/http/files_dir) > back
msf5 > use auxiliary/scanner/http/options
msf5 auxiliary(scanner/http/options) > set RHOSTS 192.168.0.10
```

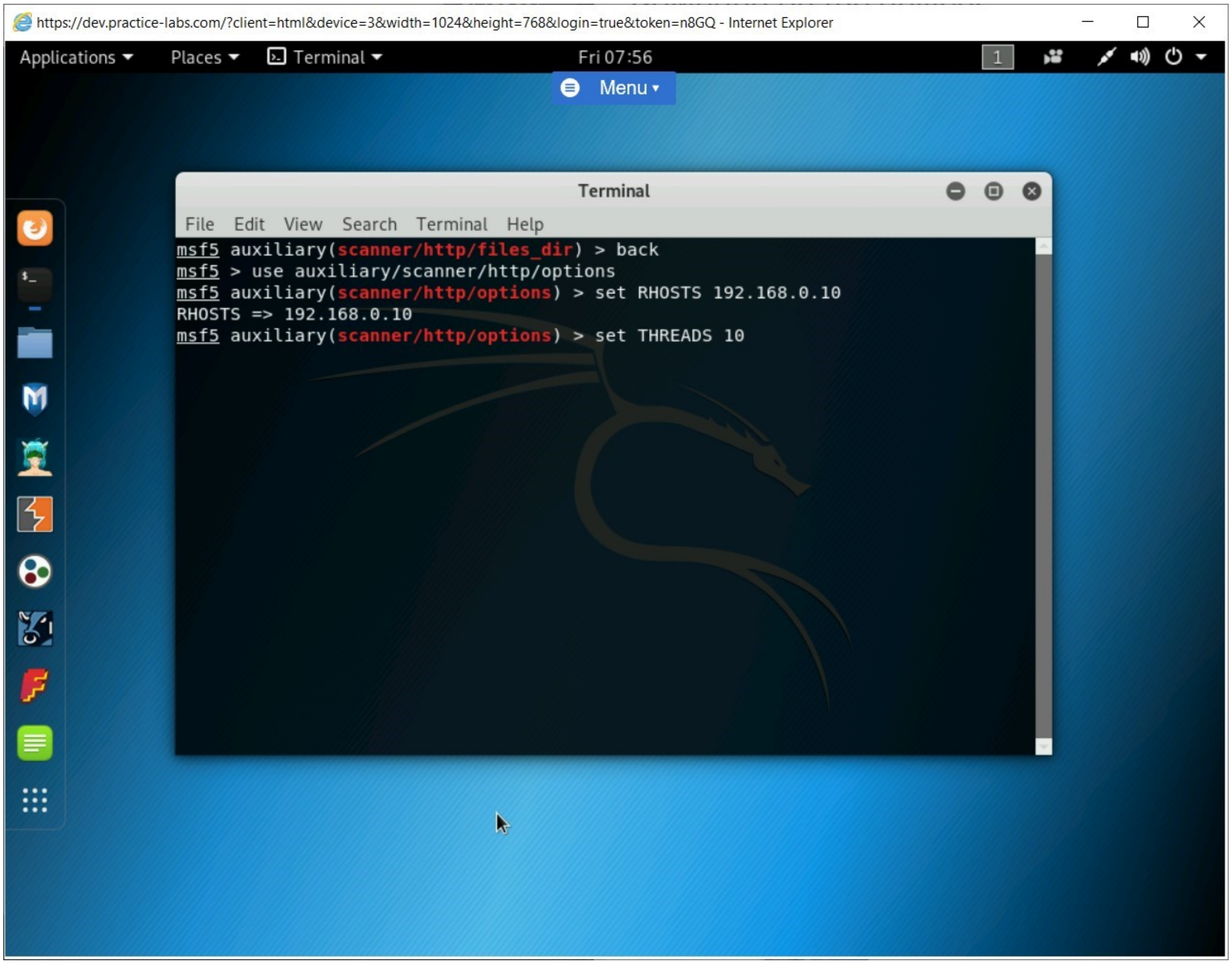
Figure 1.72 Screenshot of PLABKALI01: Entering the command to set the target system.

Step 4

Next, set the number of threads. To do this, type the following command:

```
set THREADS 10
```

Press **Enter**.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 07:56
Menu
Terminal
File Edit View Search Terminal Help

```
msf5 auxiliary(scanner/http/files_dir) > back
msf5 > use auxiliary/scanner/http/options
msf5 auxiliary(scanner/http/options) > set RHOSTS 192.168.0.10
RHOSTS => 192.168.0.10
msf5 auxiliary(scanner/http/options) > set THREADS 10
```

Figure 1.73 Screenshot of PLABKALI01: Entering the command to set the number of threads.

Step 5

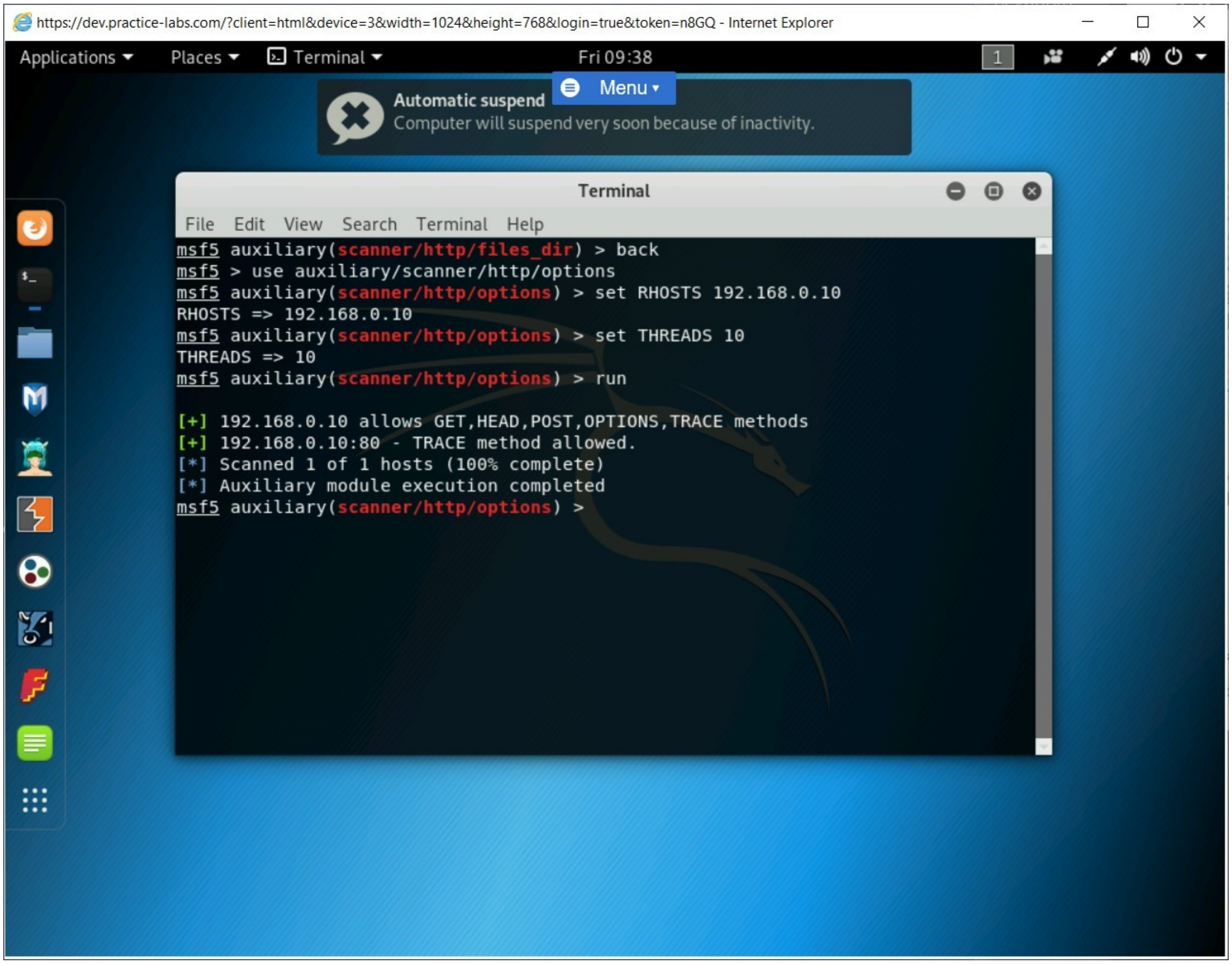
Now, type the following command to execute the payload:

```
run
```

Press **Enter**.

Notice that the output lists the options configured on the Webserver.

Keep the terminal window open.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 09:38
Automatic suspend
Computer will suspend very soon because of inactivity.
Menu
Terminal
File Edit View Search Terminal Help

```
msf5 auxiliary(scanner/http/files_dir) > back
msf5 > use auxiliary/scanner/http/options
msf5 auxiliary(scanner/http/options) > set RHOSTS 192.168.0.10
RHOSTS => 192.168.0.10
msf5 auxiliary(scanner/http/options) > set THREADS 10
THREADS => 10
msf5 auxiliary(scanner/http/options) > run

[+] 192.168.0.10 allows GET,HEAD,POST,OPTIONS,TRACE methods
[+] 192.168.0.10:80 - TRACE method allowed.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/options) >
```

Figure 1.74 Screenshot of PLABKALI01: Listing the output with the number of options configured on the Webserver.

Task 8 - Find the Webserver Version using the Metasploit Framework

Using Metasploit Framework, you can find the Webserver version that is running on a system. Metasploit Framework provides a module named http_version that is used for this purpose.

In this task, you will find the Webserver version using the Metasploit Framework. To do this, perform the following steps:

Step 1

Ensure that you have logged into the Kali Linux system. Ensure that you are on the metasploit framework terminal.

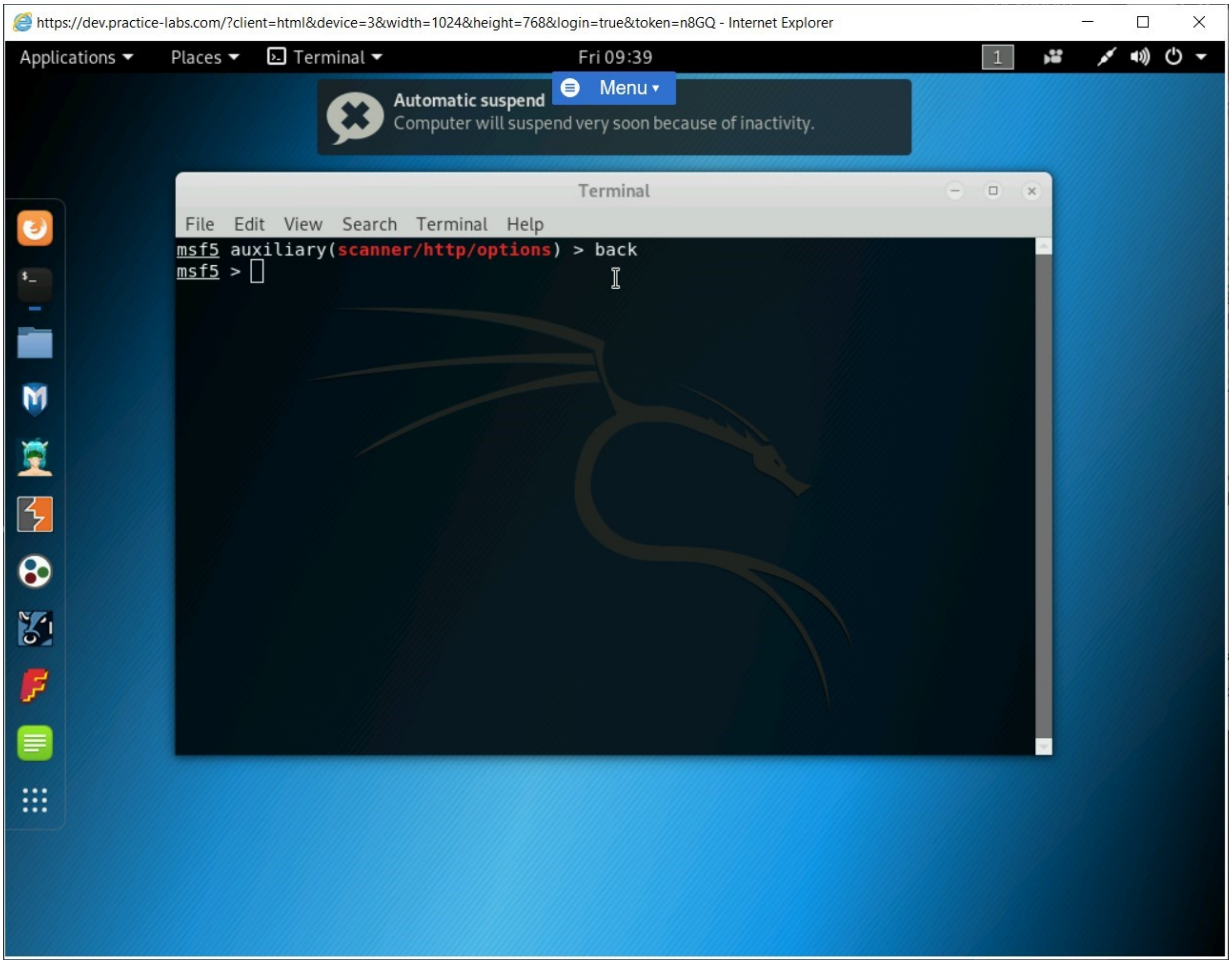
Clear the screen by entering the following command:

```
clear
```

You need to move out of the **Options** module. To do this, type the following command:

```
back
```

Press **Enter**.



https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 09:39
Menu
Terminal
File Edit View Search Terminal Help

Automatic suspend
Computer will suspend very soon because of inactivity.

```
msf5 auxiliary(scanner/http/options) > back
msf5 >
```

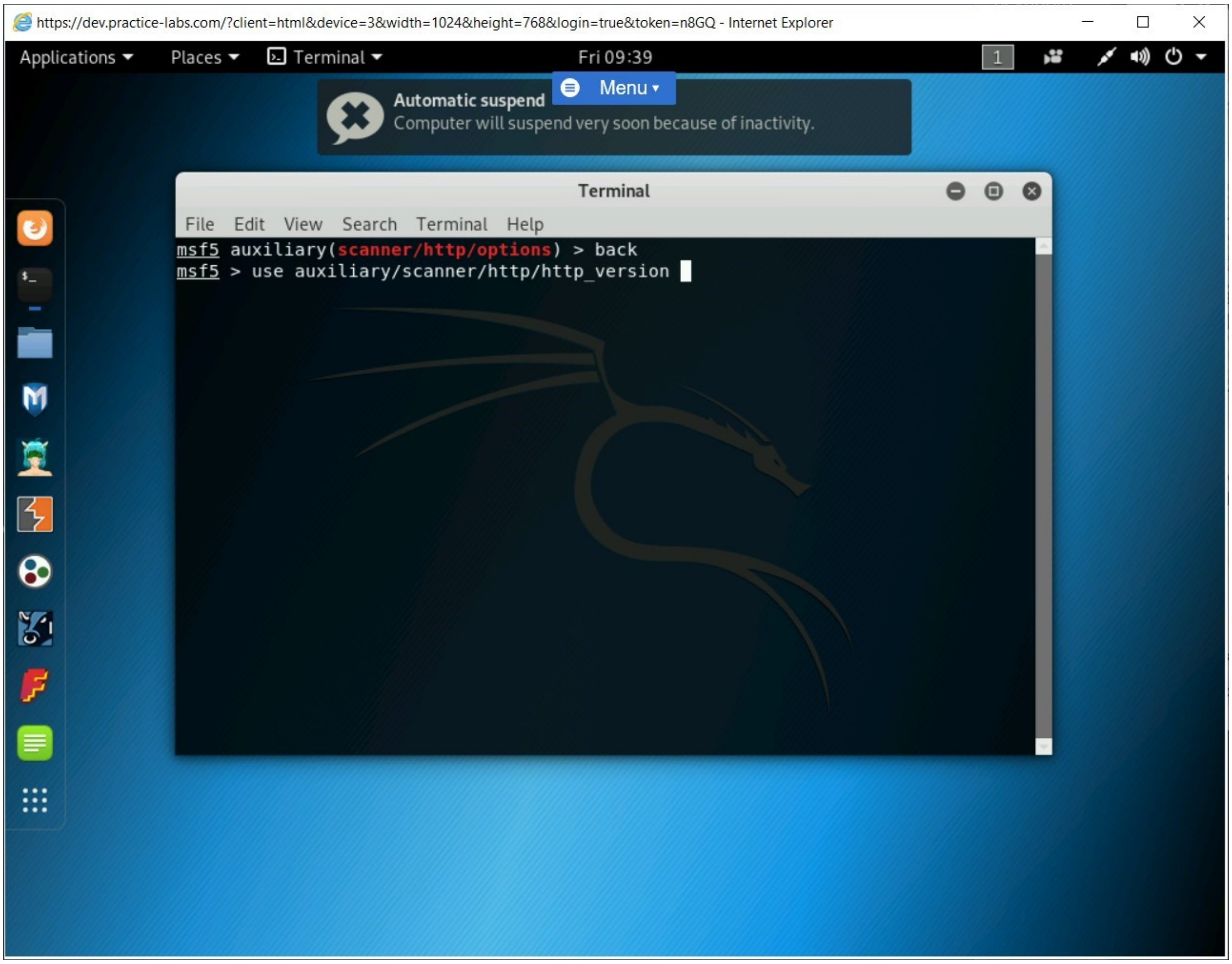
Figure 1.75 Screenshot of PLABKALI01: Entering the back command to go back to the Metasploit Framework prompt.

Step 2

You are back on the Metasploit Framework prompt. To find the Webserver version, you need to load the **http_version** module. To do this, type the following command:

```
use auxiliary/scanner/http/http_version
```

Press **Enter**.



https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 09:39
Menu
Automatic suspend
Computer will suspend very soon because of inactivity.
Terminal
File Edit View Search Terminal Help

```
msf5 auxiliary(scanner/http/options) > back
msf5 > use auxiliary/scanner/http/http_version
```

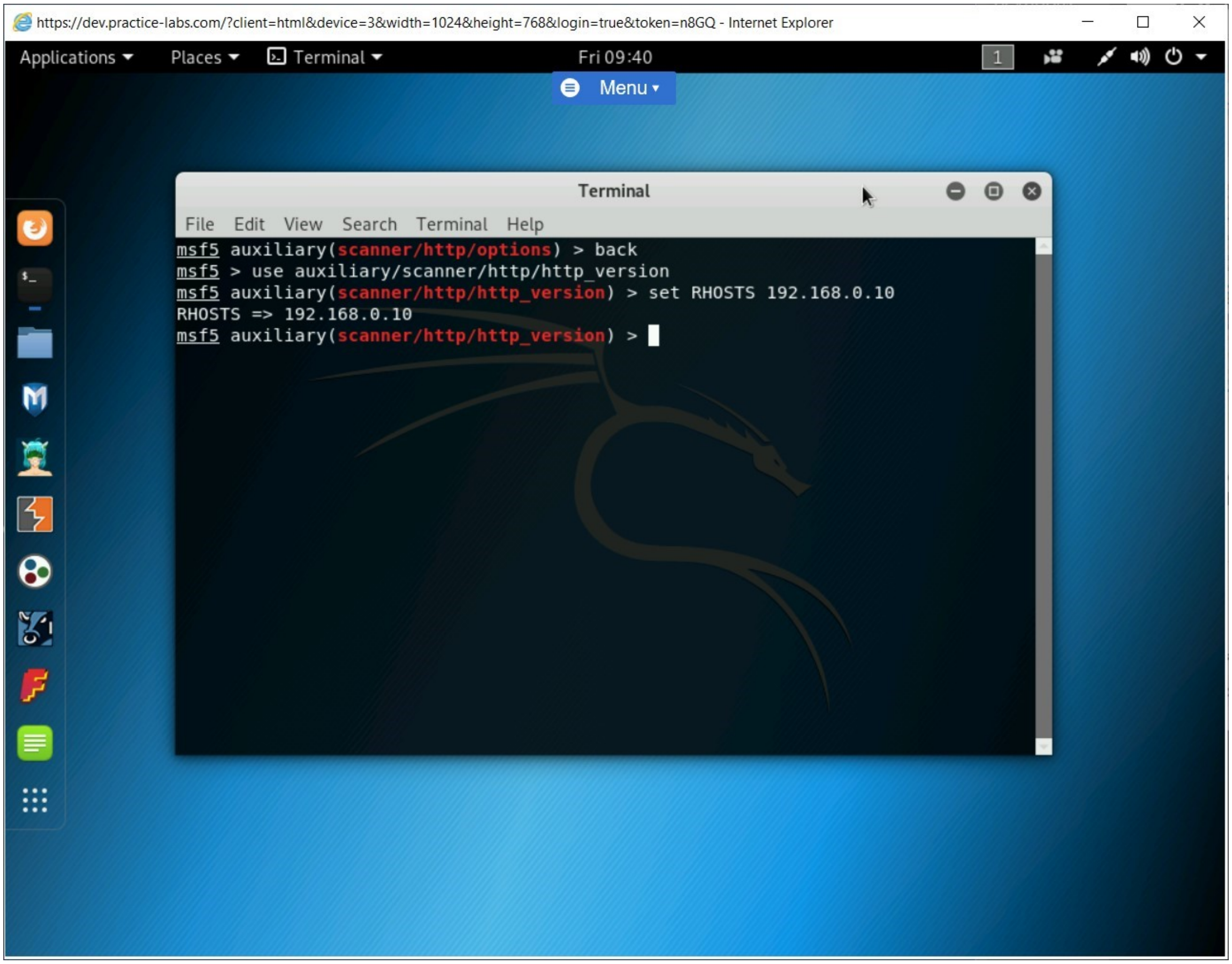
Figure 1.76 Screenshot of PLABKALI01: Entering the command to use the http_version module.

Step 3

Next, you need to set the target system. To do this, type the following command:

```
set RHOSTS 192.168.0.10
```

Press **Enter**.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 09:40
Menu
Terminal
File Edit View Search Terminal Help

```
msf5 auxiliary(scanner/http/options) > back
msf5 > use auxiliary/scanner/http/http_version
msf5 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.0.10
RHOSTS => 192.168.0.10
msf5 auxiliary(scanner/http/http_version) >
```

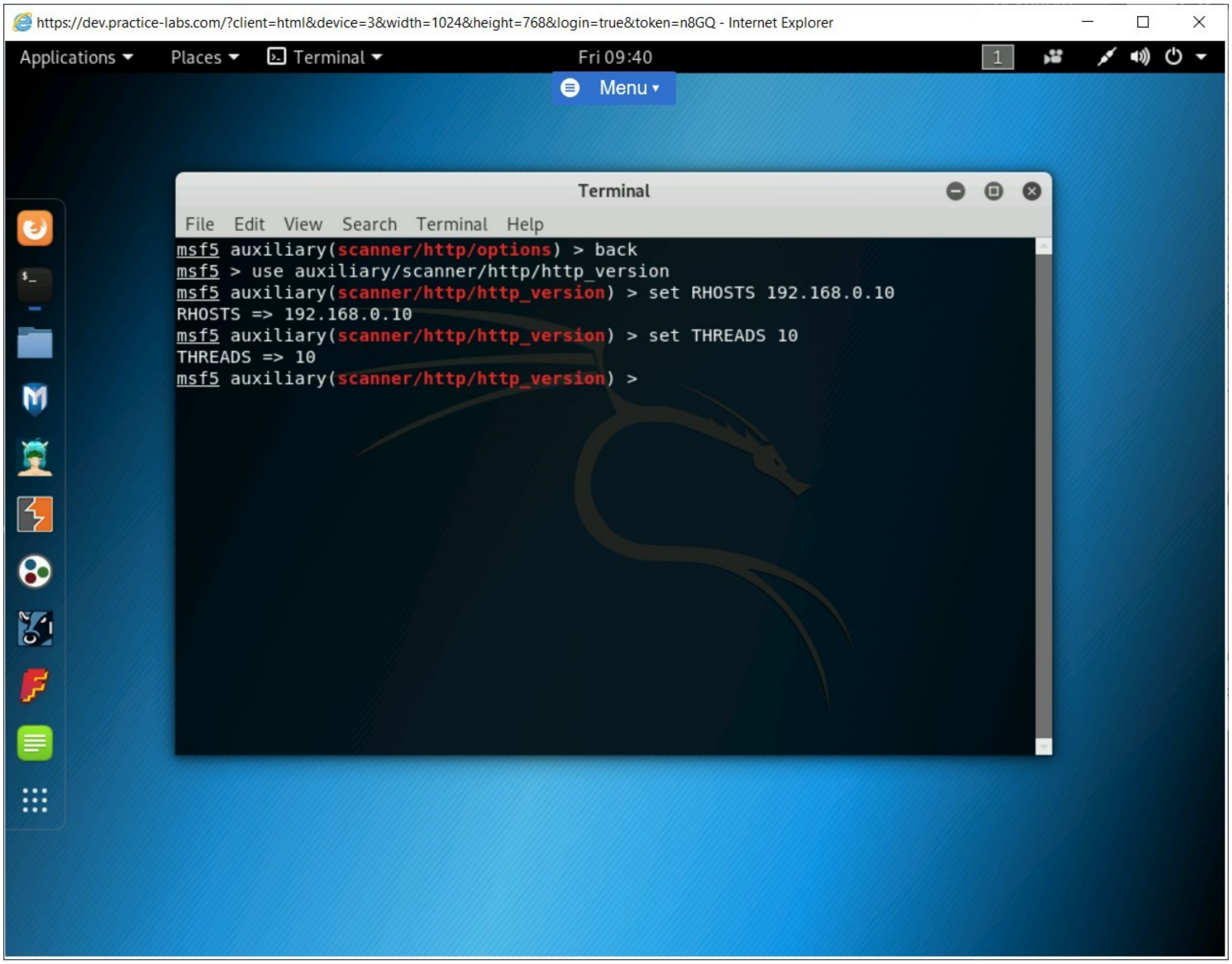
Figure 1.77 Screenshot of PLABKALI01: Entering the command to set the target system.

Step 4

Next, set the number of threads. To do this, type the following command:

```
set THREADS 10
```

Press **Enter**.



https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 09:40
Menu
Terminal
File Edit View Search Terminal Help

```
msf5 auxiliary(scanner/http/options) > back
msf5 > use auxiliary/scanner/http/http_version
msf5 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.0.10
RHOSTS => 192.168.0.10
msf5 auxiliary(scanner/http/http_version) > set THREADS 10
THREADS => 10
msf5 auxiliary(scanner/http/http_version) >
```

Figure 1.78 Screenshot of PLABKALI01: Entering the command to set the number of threads.

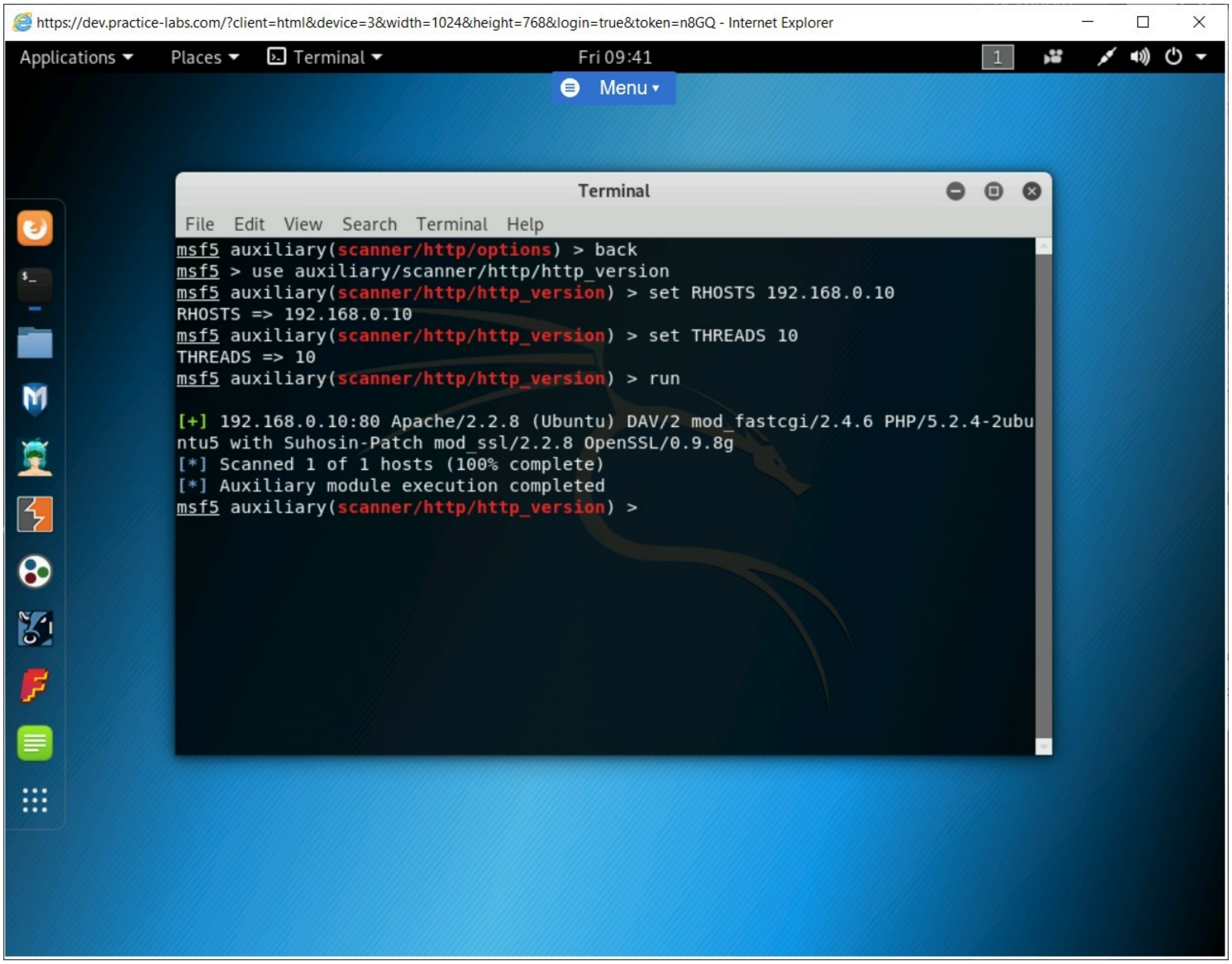
Step 5

Now, type the following command to execute the payload:

```
run
```

Press **Enter**.

The details of the Webserver are now displayed. Keep the terminal window open.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 09:41
Menu
Terminal
File Edit View Search Terminal Help

```
msf5 auxiliary(scanner/http/options) > back
msf5 > use auxiliary/scanner/http/http_version
msf5 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.0.10
RHOSTS => 192.168.0.10
msf5 auxiliary(scanner/http/http_version) > set THREADS 10
THREADS => 10
msf5 auxiliary(scanner/http/http_version) > run

[+] 192.168.0.10:80 Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubu
ntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/http_version) >
```

Figure 1.79 Screenshot of PLABKALI01: Showing the Webserver version.

Task 9 - Check for WebDAV on a Webserver using Metasploit Framework

Metasploit Framework provides a module named webdav_scanner that you can use to verify if WebDAV is enabled. If it is enabled, the attacker can plan for the attack accordingly.

In this task, you will check for WebDAV on a Webserver using Metasploit Framework. To do this, perform the following steps:

Step 1

Ensure that you have logged into the Kali Linux system. Ensure that you are on the metasploit framework terminal.

Clear the screen by entering the following command:

```
clear
```

You need to move out of the **Options** module. To do this, type the following command:

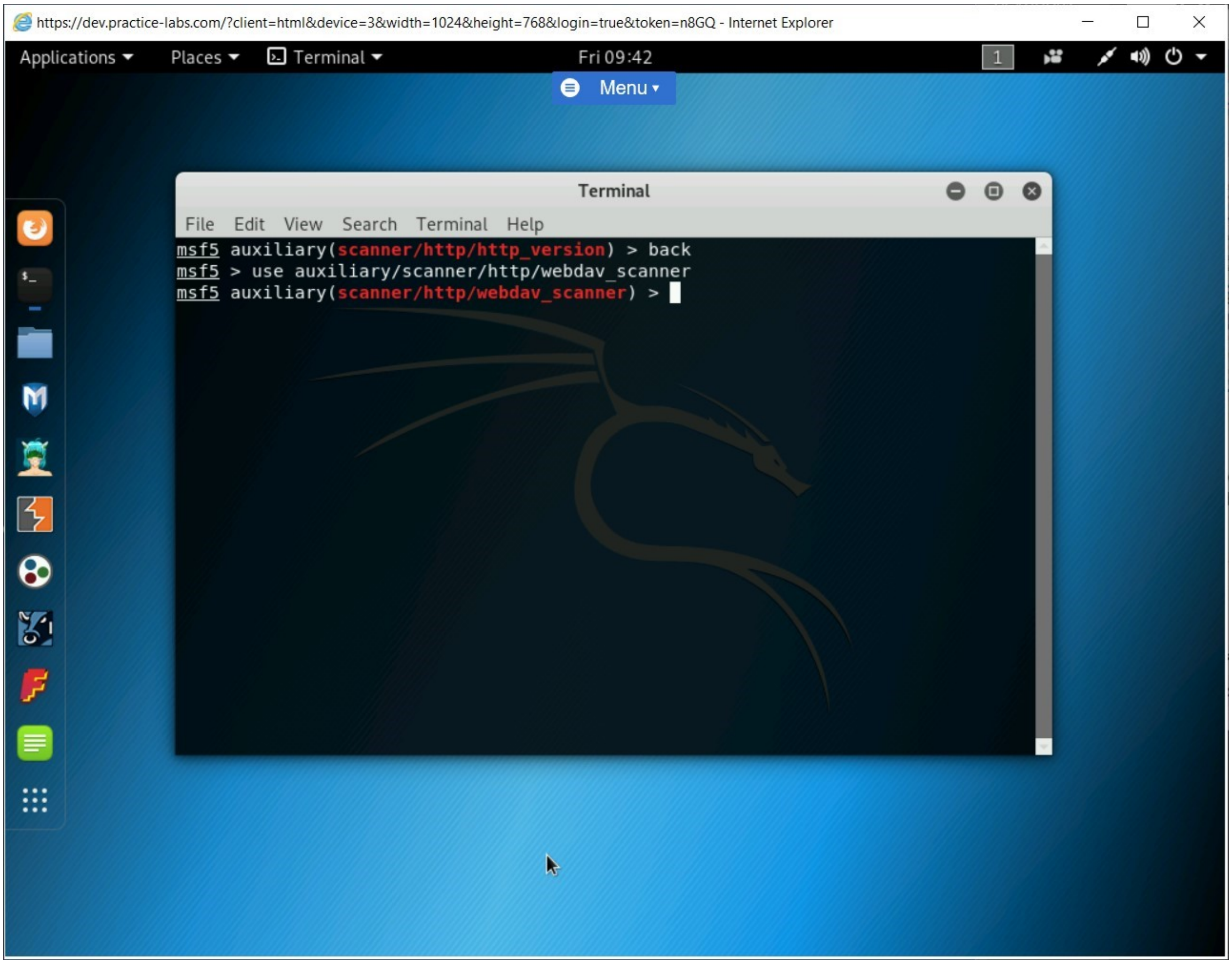
```
back
```

Press **Enter**.

You are back on the Metasploit Framework prompt. You need to enable the **webdav_scanner** module first. To do this, type the following command:

```
use auxiliary/scanner/http/webdav_scanner
```

Press **Enter**.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 09:42
Menu
Terminal
File Edit View Search Terminal Help

```
msf5 auxiliary(scanner/http/http_version) > back
msf5 > use auxiliary/scanner/http/webdav_scanner
msf5 auxiliary(scanner/http/webdav_scanner) > 
```

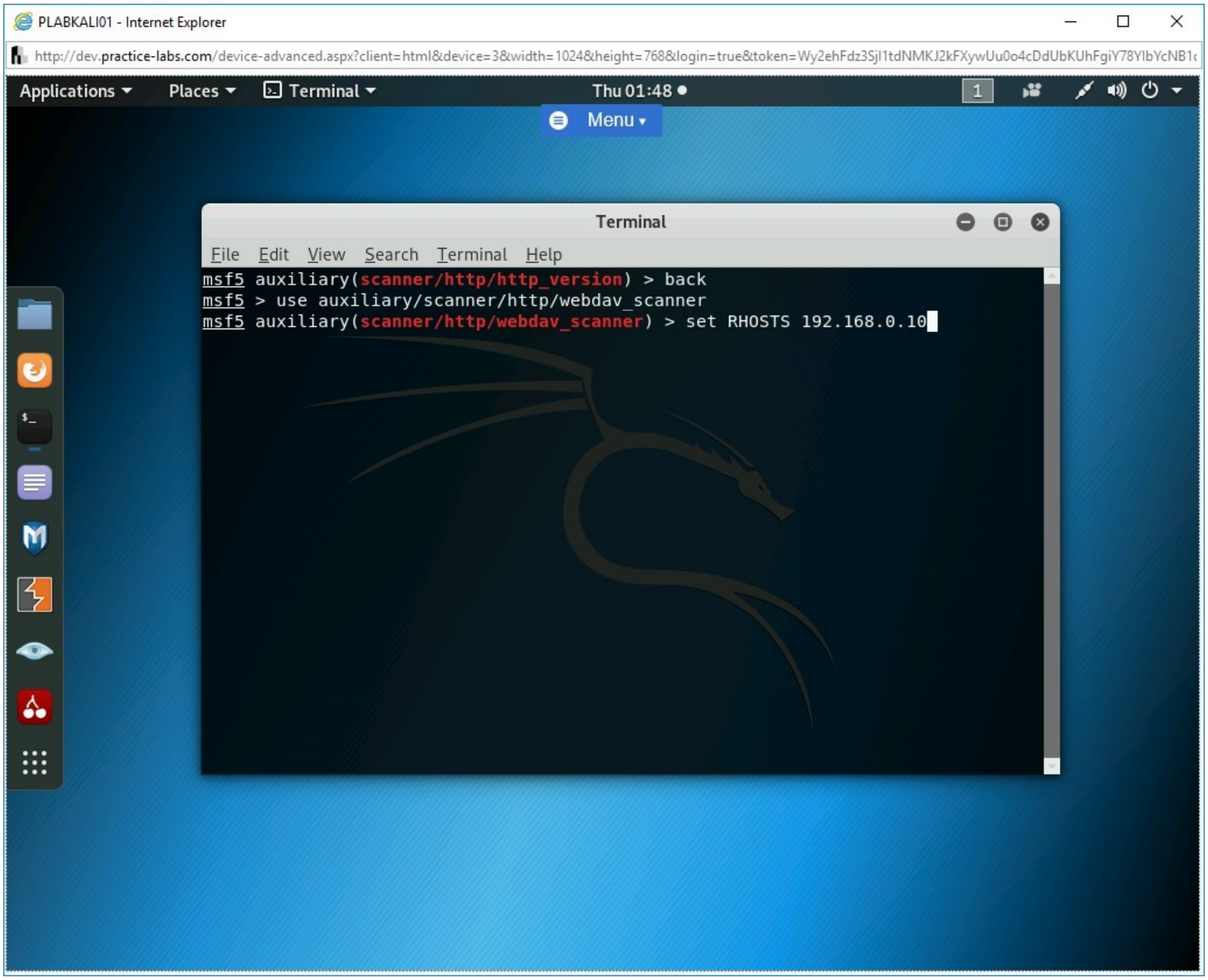
Figure 1.80 Screenshot of PLABKALI01: Entering the command to use the webdav_scanner module.

Step 2

Next, you need to set the target system. To do this, type the following command:

```
set RHOSTS 192.168.0.10
```

Press **Enter**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=Wy2ehFdz3Sjl1tdNMKJ2kFXywUu0o4cDdUbKUhFgiY78YlbYcNB1
Applications
Places
Terminal
Thu 01:48 ●
Menu
Terminal
File
Edit
View
Search
Terminal
Help

```
msf5 auxiliary(scanner/http/http_version) > back
msf5 > use auxiliary/scanner/http/webdav_scanner
msf5 auxiliary(scanner/http/webdav_scanner) > set RHOSTS 192.168.0.10
```

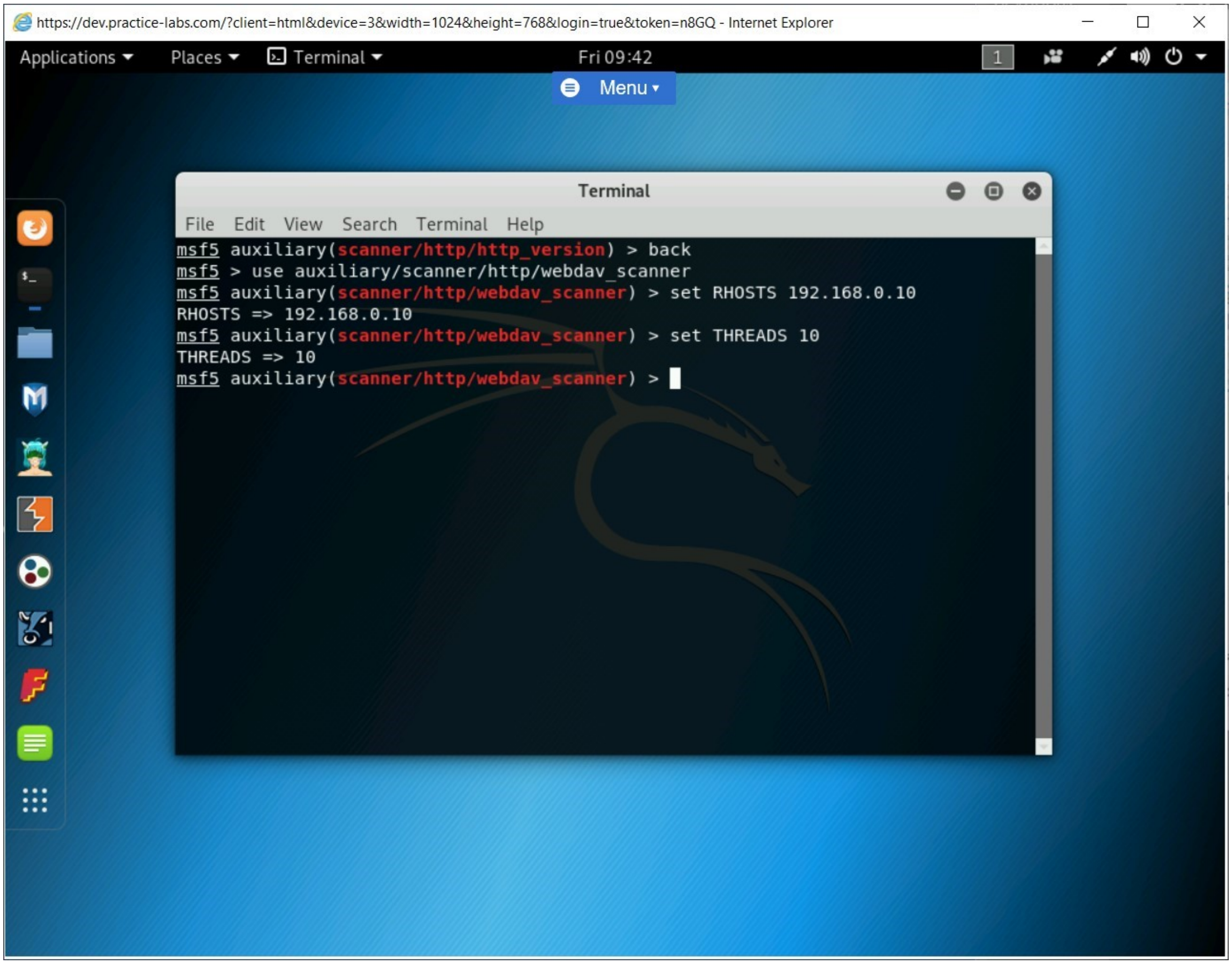
Figure 1.81 Screenshot of PLABKALI01: Entering the command to set the target host.

Step 3

Next, set the number of threads. To do this, type the following command:

```
set THREADS 10
```

Press **Enter**.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 09:42
Menu
Terminal
File
Edit
View
Search
Terminal
Help

```
msf5 auxiliary(scanner/http/http_version) > back
msf5 > use auxiliary/scanner/http/webdav_scanner
msf5 auxiliary(scanner/http/webdav_scanner) > set RHOSTS 192.168.0.10
RHOSTS => 192.168.0.10
msf5 auxiliary(scanner/http/webdav_scanner) > set THREADS 10
THREADS => 10
msf5 auxiliary(scanner/http/webdav_scanner) > 
```

Figure 1.82 Screenshot of PLABKALI01: Entering the command to set a number of threads.

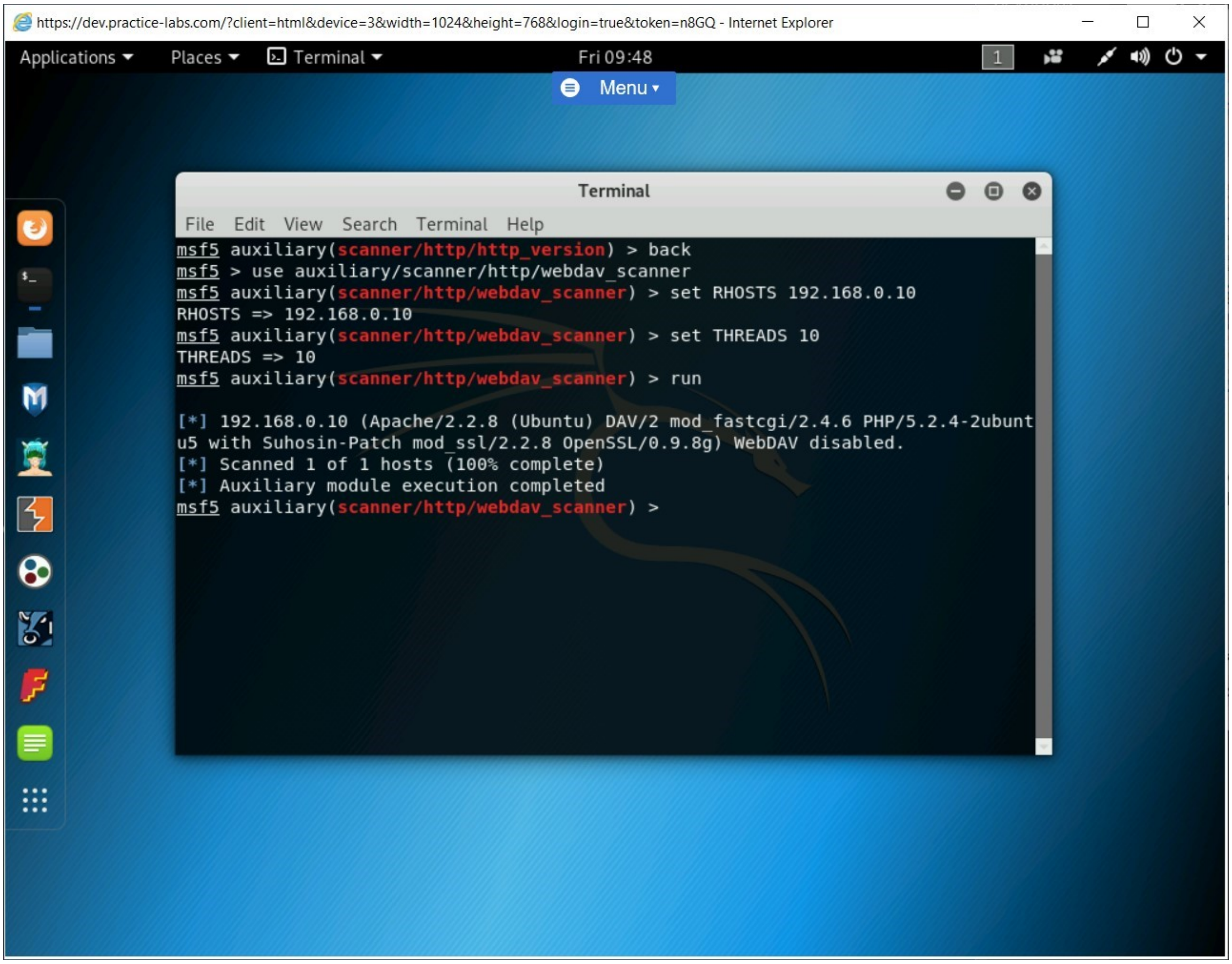
Step 4

Now, type the following command to execute the payload:

```
run
```

Press **Enter**.

Notice the output states that **WebDAV** is disabled.


https://dev.practice-labs.com/?client=html&device=3&width=1024&height=768&login=true&token=n8GQ - Internet Explorer
Applications
Places
Terminal
Fri 09:48
Menu
Terminal
File Edit View Search Terminal Help

```
msf5 auxiliary(scanner/http/http_version) > back
msf5 > use auxiliary/scanner/http/webdav_scanner
msf5 auxiliary(scanner/http/webdav_scanner) > set RHOSTS 192.168.0.10
RHOSTS => 192.168.0.10
msf5 auxiliary(scanner/http/webdav_scanner) > set THREADS 10
THREADS => 10
msf5 auxiliary(scanner/http/webdav_scanner) > run

[*] 192.168.0.10 (Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubunt
u5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g) WebDAV disabled.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/webdav_scanner) >
```

Figure 1.83 Screenshot of PLABKALI01: Showing the Webserver version along with WebDAV status.

Exercise 2 - Preventing Webserver Exploitations

A Webserver hosting one or more web applications must be prevented from being exploited. In the previous exercise, you learned about different types of exploitations that can take place against a Webserver. Therefore, there are several countermeasures that you can take to prevent webserver exploitation.

In this exercise, you will learn about several methods to prevent webserver exploitation.

Learning Outcomes

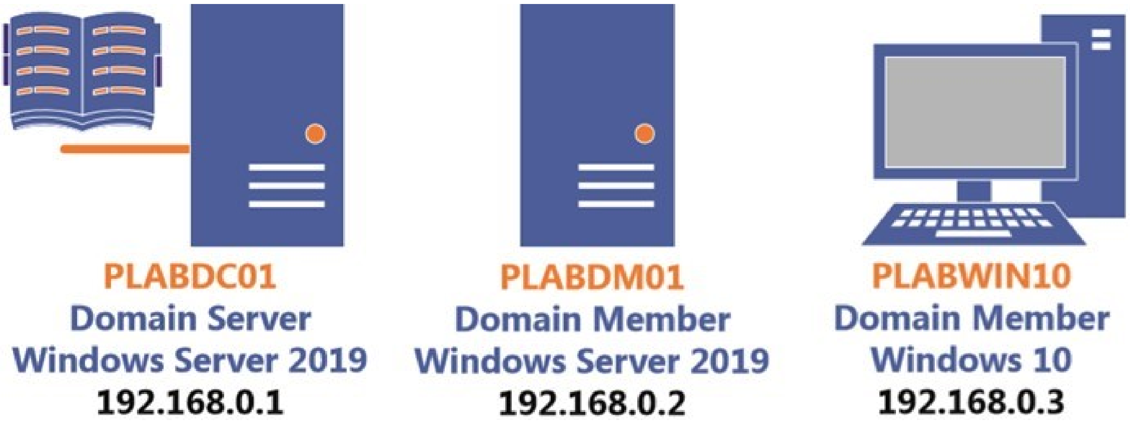
After completing this exercise, you will be able to:

- Use common methods to prevent Webserver Exploitation
- Disable HTTP TRACK and TRACE Verbs in Internet Information Services (IIS)

Your Devices

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

- **PLABDC01 -** (Windows Server 2019 - Domain Server)
- **PLABDM01 -** (Windows Server 2019 - Domain Controller)
- **PLABKALI01 -** (Kali 2019.2 - Linux Kali Workstation)



Task 1 - Use Common Methods to Prevent Webserver Exploitation

A Webserver can be prone to different types of vulnerabilities. You need to be aware of some of the prevention methods that you can apply on the Webserver to protect its data. Some of the most common methods to prevent Webserver exploitation are:

- Placing the Webserver in a secure zone, preferably where the firewall and other security appliances or applications, such as Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) are placed
- Placing the Webserver in a DMZ, which is protected with a firewall. Such placement will protect the Webserver from external attacks
- Filtering the incoming traffic to the Webserver
- Deploying a Web application change detection method, which can detect any malicious executable attempting to change the Web application functionality

- Implementing hashing to track the changes made to the Webserver and the Web application files
- Disabling unnecessary open ports and running services
- Using a server certificate on the Webserver
- Encrypting the outgoing traffic to prevent Man-In-the-Middle (MITM) attacks
- Disabling the debug compilers on the Webserver
- Disabling tracking on the Webserver
- Using HTTPS instead of HTTP
- Enabling auditing to track failed logins
- Disabling the default accounts on the Webserver
- Performing regular patch updates on the Webserver and the Web application
- Using complex password policy
- Removing unused modules and extensions from the Webserver
- Using the least privilege principle for the database accounts

Task 2 - Disable HTTP TRACK and TRACE verbs in Internet Information Services (IIS)

Webservers usually return the full request in their responses to the client, which originally made the request. TRACK is a verb, which is used in IIS, and returns the full request in the response to the client. TRACK is similar to TRACE, but it is Microsoft's implementation. When a security scanning tool scans the Webserver, it might find the HTTP TRACK to be enabled. Same is the case if TRACE is also enabled. If either one or both are enabled, they are considered to be vulnerabilities. When these are enabled, they can lead to a cross-site scripting attack. A hacker may use a Webpage with XMLHTTP and force the client to issue a TRACK request from the Webserver. When the response is returned, the hacker can then capture the client cookies.

To disable HTTP TRACK and TRACE verbs in IIS, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABDM01**. The **Server Manager** window is displayed by default. Click **Close**.

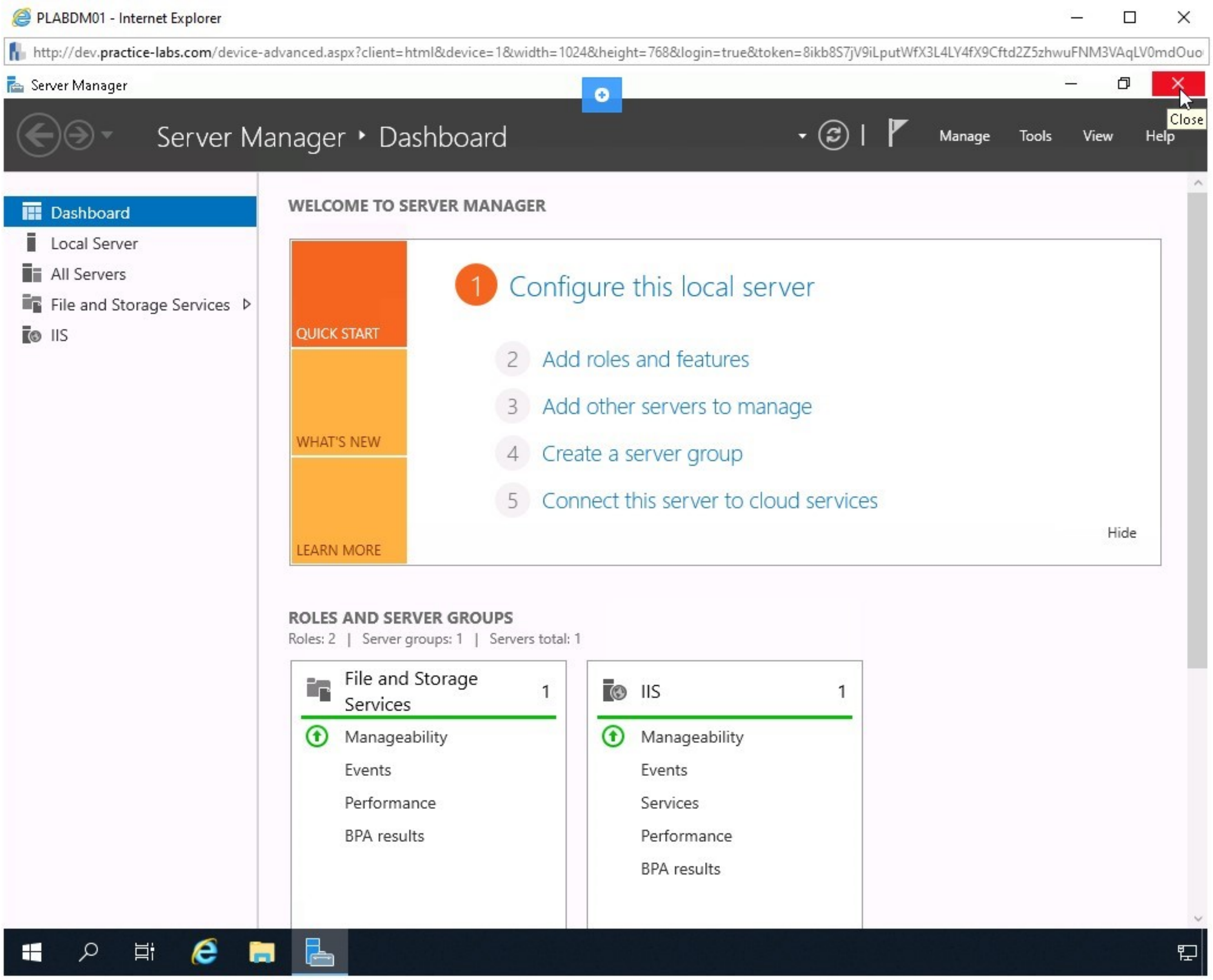

PLABDM01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=1&width=1024&height=768&login=true&token=8ikb8S7jV9iLputWfX3L4LY4fX9Cftd2Z5zhwuFNM3VAqLV0mdOuo
Server Manager
Close
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
BPA results
IIS 1
Manageability
Events
Services
Performance
BPA results

Figure 2.1 Screenshot of PLABDM01: Showing the Server Manager window.

Step 2

Click the Windows charm, select **Windows Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.

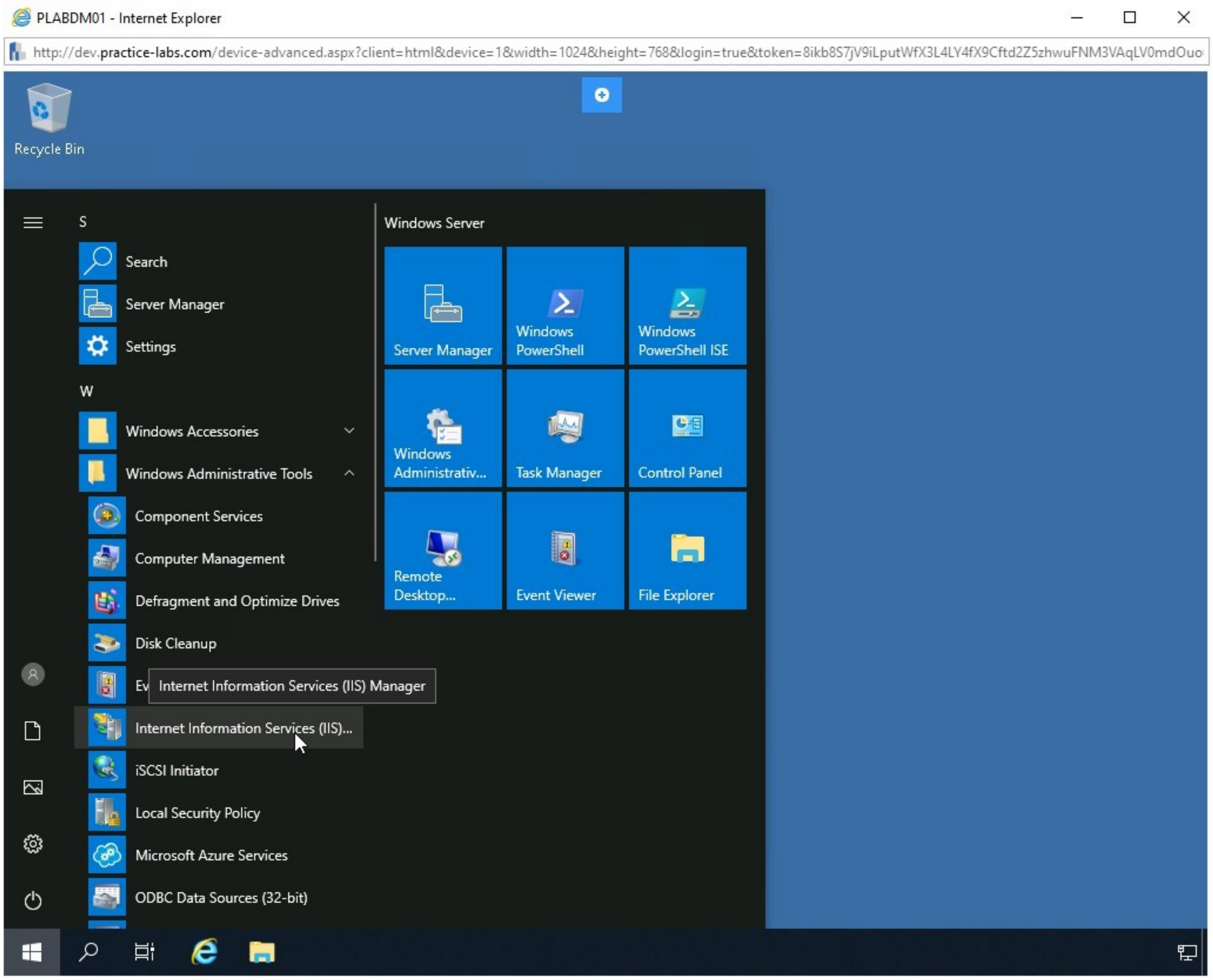

PLABDM01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=1&width=1024&height=768&login=true&token=8ikb8S7jV9iLputWfX3L4LY4fX9Cftd2Z5zhwuFNM3VAqLV0mdOuo
Recycle Bin
S
Search
Server Manager
Settings
W
Windows Accessories
Windows Administrative Tools
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
Ev
Internet Information Services (IIS) Manager
Internet Information Services (IIS)...
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer

Figure 2.2 Screenshot of PLABDM01: Selecting Windows Administrative Tools, and then selecting Internet Information Services (IIS) Manager.

Step 3

In the left pane, select PLABDM01 and then double-click **Request Filtering** in the right pane.

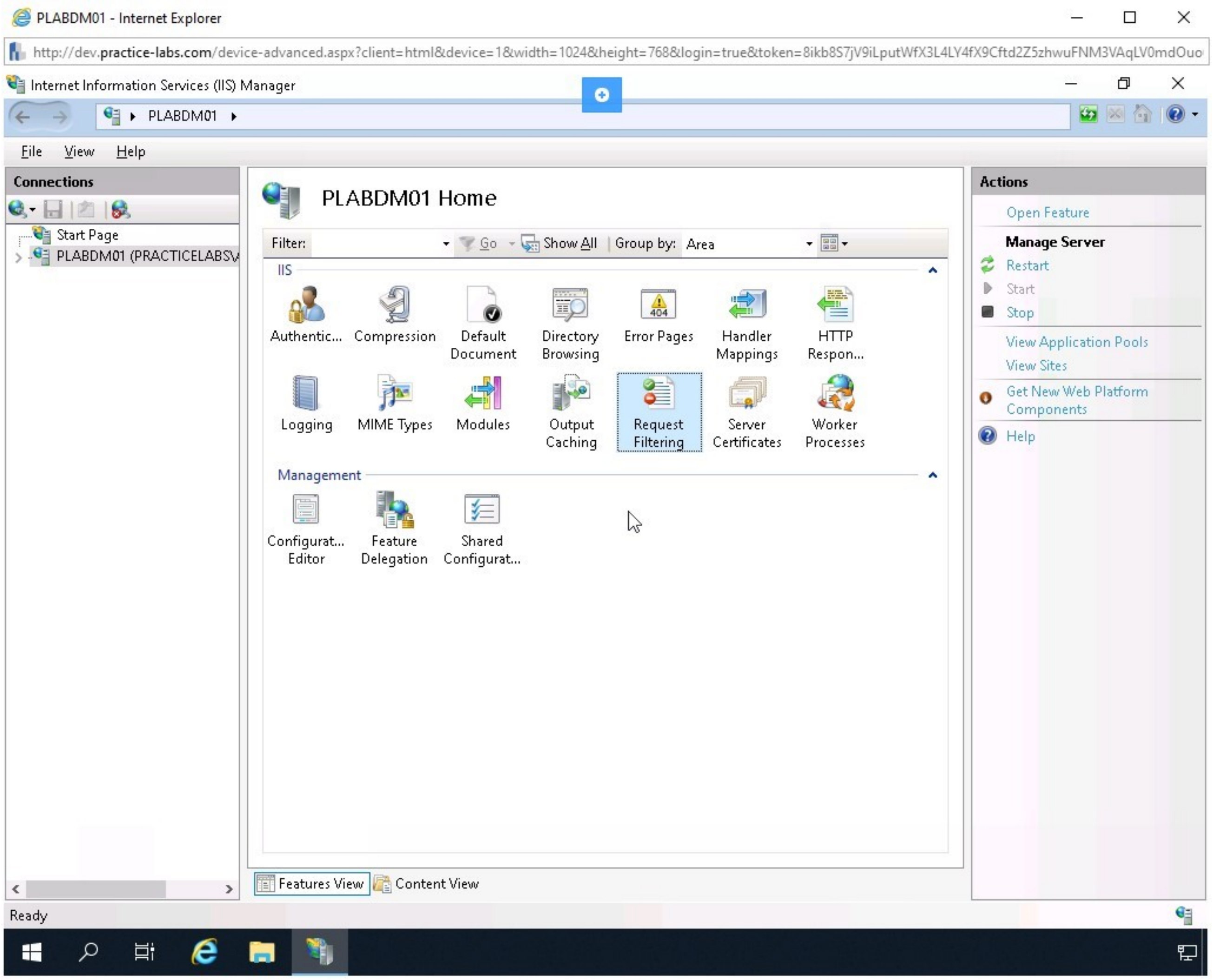
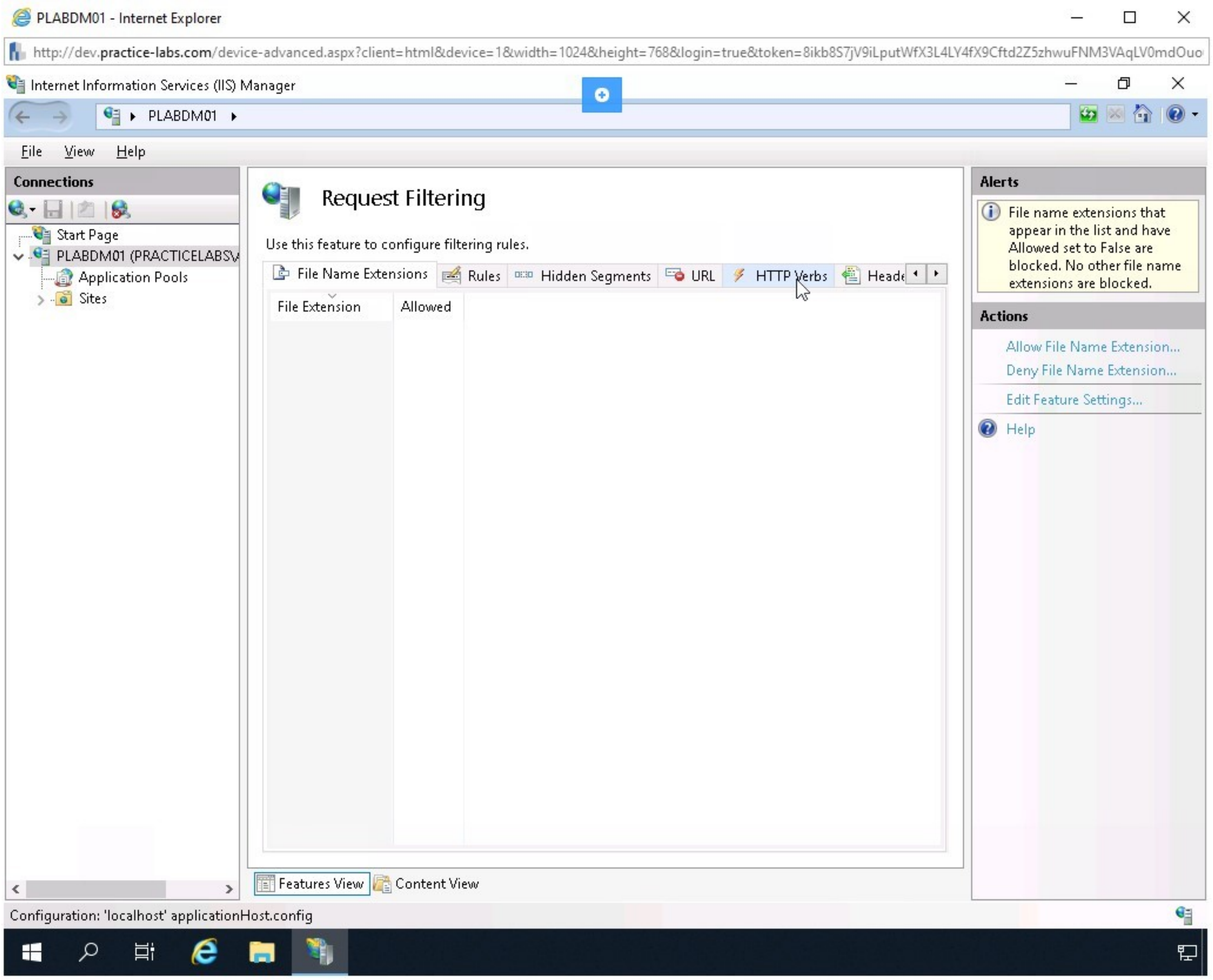


Figure 2.3 Screenshot of PLABDM01: Selecting PLABDM01 in the left pane and then double-clicking Request Filtering in the middle pane.

Step 4

The middle pane displays the **Request Filtering** page. Click the **HTTP Verbs** tab.


PLABDM01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=1&width=1024&height=768&login=true&token=8ikb8S7jV9iLputWfX3L4LY4fX9Cftd2Z5zhwuFNM3VAqLV0mdOuo
Internet Information Services (IIS) Manager
PLABDM01
File
View
Help
Connections
Start Page
PLABDM01 (PRACTICELABS\
Application Pools
Sites
Request Filtering
File Name Extensions
Rules
Hidden Segments
URL
HTTP Verbs
Heade
File Extension
Allowed
Features View
Content View
Alerts
Actions
Allow File Name Extension...
Deny File Name Extension...
Edit Feature Settings...
Help

Use this feature to configure filtering rules.

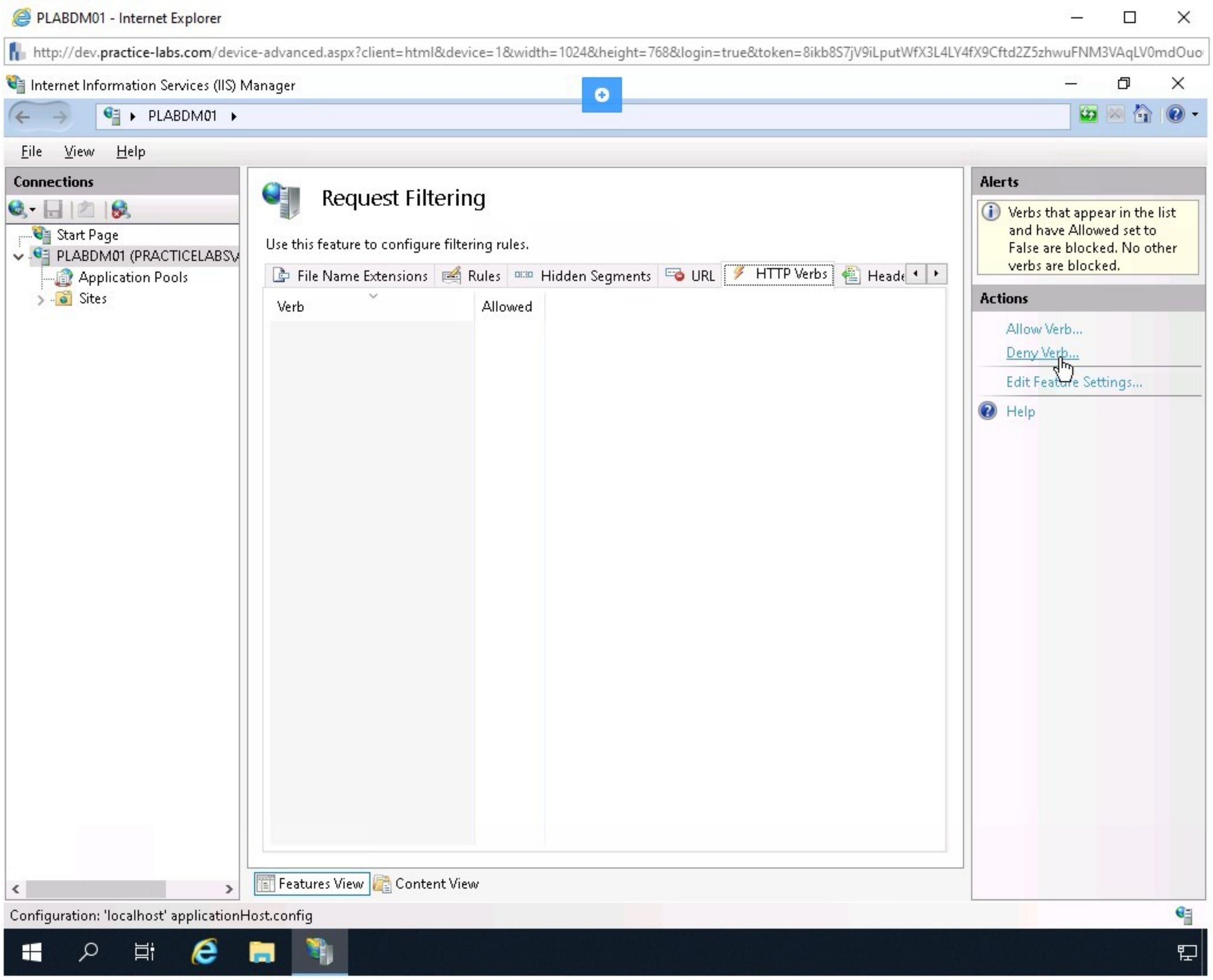
File name extensions that appear in the list and have Allowed set to False are blocked. No other file name extensions are blocked.

Configuration: 'localhost' applicationHost.config

Figure 2.4 Screenshot of PLABDM01: Clicking the HTTP Verbs tab in the middle pane, which is named Request Filtering.

Step 5

The **HTTP Verbs** tab is displayed. In the right pane, click **Deny Verb**.



Use this feature to configure filtering rules.

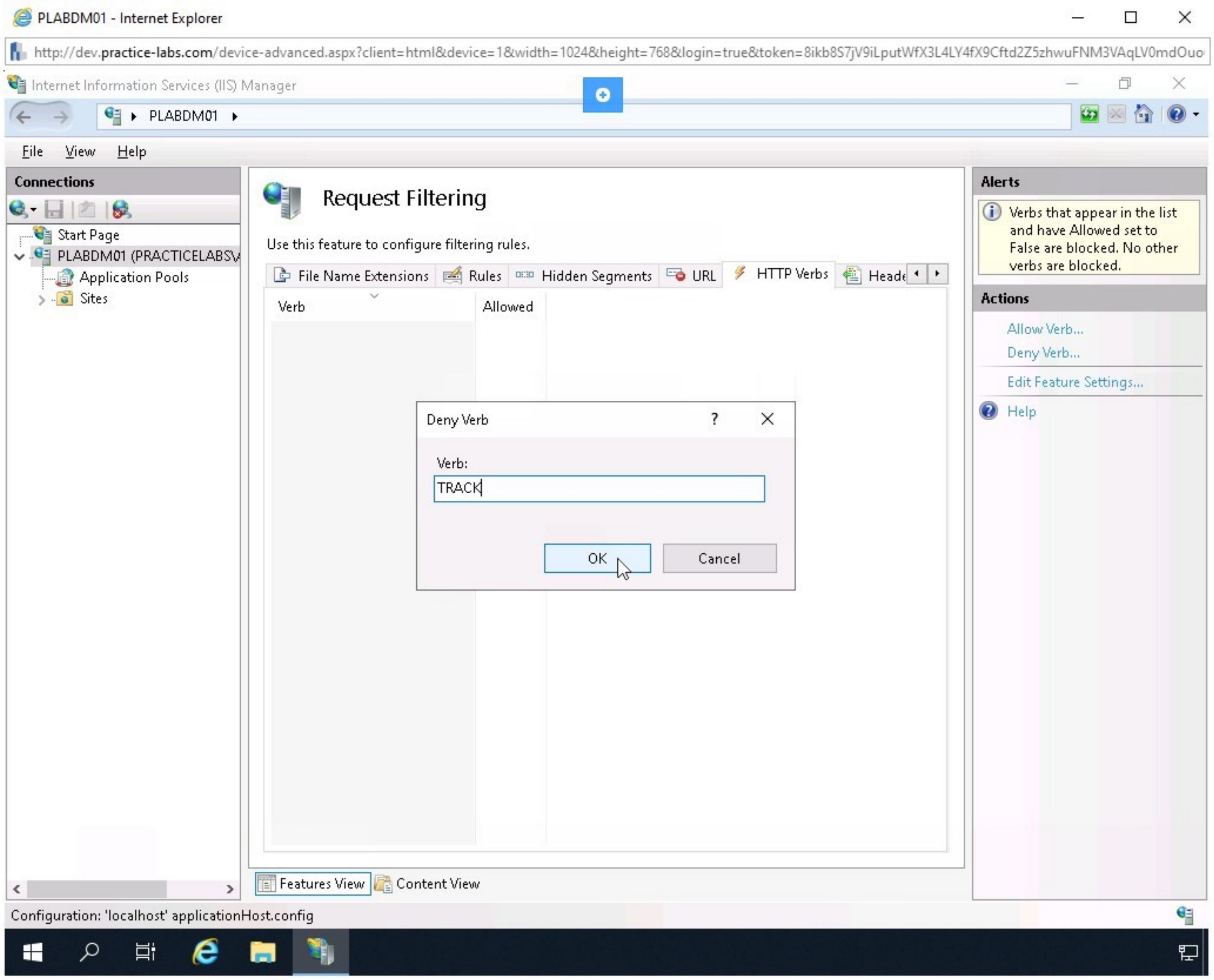
Verbs that appear in the list and have Allowed set to False are blocked. No other verbs are blocked.

Configuration: 'localhost' applicationHost.config

Figure 2.5 Screenshot of PLABDM01: Clicking Deny Verb in the right pane.

Step 6

The **Deny Verb** dialog box is displayed. In the **Verb** textbox, type **TRACK** and click **OK**.



Use this feature to configure filtering rules.

Verb: TRACK

Verbs that appear in the list and have Allowed set to False are blocked. No other verbs are blocked.

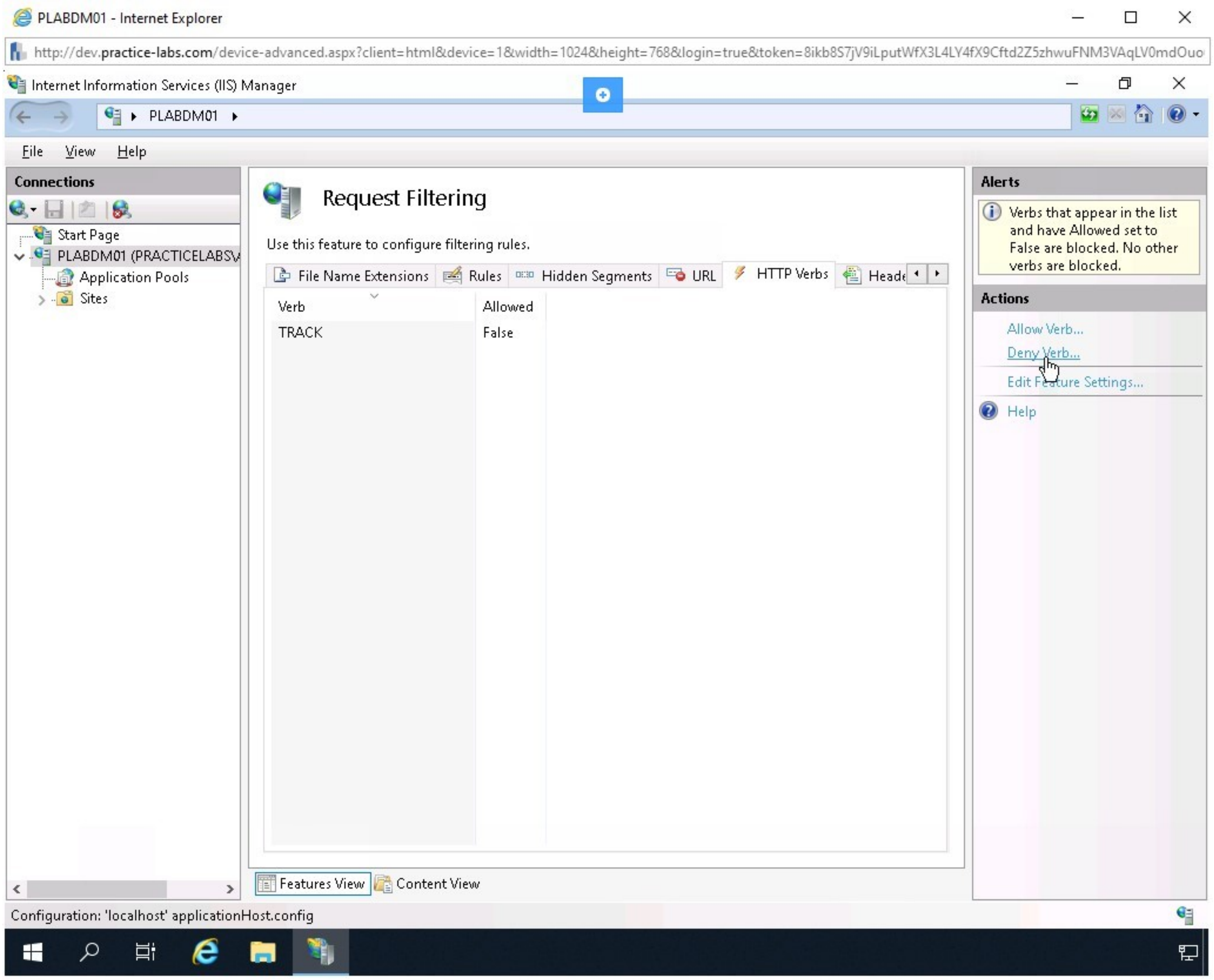
Configuration: 'localhost' applicationHost.config

Figure 2.6 Screenshot of PLABDM01: Adding the TRACK verb in the Deny Verb dialog box and clicking OK.

Step 7

Notice that the **TRACK** verb appears in the middle pane. You will now need to add **TRACE** verb to be denied.

Click **Deny Verb** in the right pane.



Use this feature to configure filtering rules.

Verb	Allowed
TRACK	False

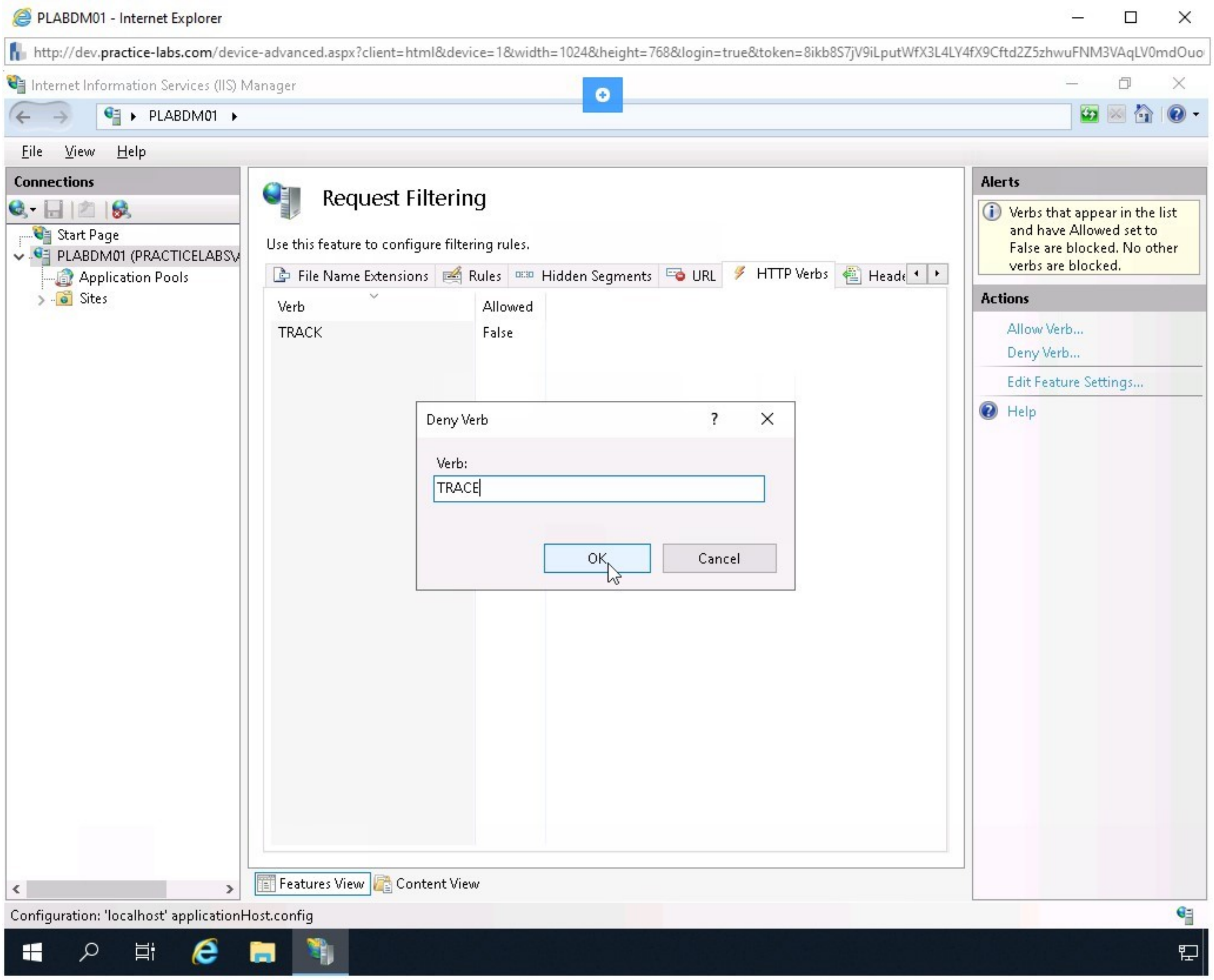
Verbs that appear in the list and have Allowed set to False are blocked. No other verbs are blocked.

Configuration: 'localhost' applicationHost.config

Figure 2.7 Screenshot of PLABDM01: Showing the TRACK verb in the middle pane and then clicking Deny Verb in the right pane.

Step 8

The **Deny Verb** dialog box is displayed. In the **Verb** textbox, type **TRACE** and click **OK**.



Use this feature to configure filtering rules.

Verb	Allowed
TRACK	False

Verbs that appear in the list and have Allowed set to False are blocked. No other verbs are blocked.

Deny Verb

Verb: TRACE

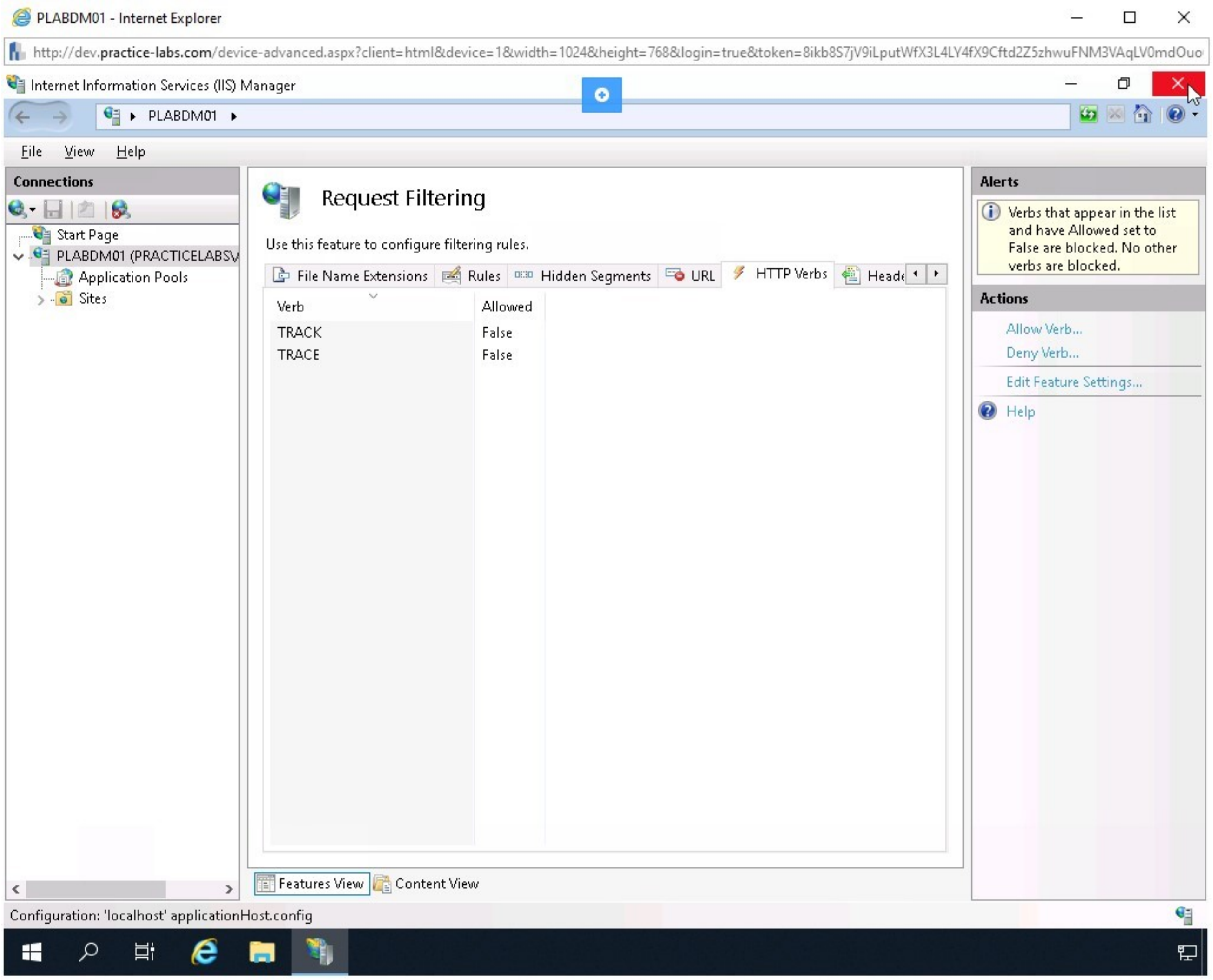
Configuration: 'localhost' applicationHost.config

Figure 2.8 Screenshot of PLABDM01: Adding the TRACE verb in the Deny Verb dialog box and clicking OK.

Step 9

Notice that **TRACK** and **TRACE** verbs are now added in the middle pane.

Click Close to close the **Internet Information Services (IIS) Manager**.



Use this feature to configure filtering rules.

Verb	Allowed
TRACK	False
TRACE	False

Verbs that appear in the list and have Allowed set to False are blocked. No other verbs are blocked.

Configuration: 'localhost' applicationHost.config

Figure 2.9 Screenshot of PLABDM01: Showing the TRACK and TRACE verbs added in the middle pane.

Review

Well done, you have completed the **Hacking Webservers** Practice Lab.

Summary

You completed the following exercises:

- Exercise 1 - Exploiting the Webserver Vulnerabilities
- Exercise 2 - Preventing Webserver Exploitations

You should now be able to:

- Perform a Slowloris Attack on a Webserver
- Enumerate a Webserver using HTTPrint
- Perform Directory Traversal Attack
- Perform Web Application Brute Forcing Using DirBuster
- Use Skipfish to Perform Webserver Reconnaissance
- Find Files on a Webserver using Metasploit Framework
- Scan for Options on a Webserver using Metasploit Framework
- Find the Webserver Version using Metasploit Framework
- Check for WebDAV on a Webserver using Metasploit Framework
- Use Common Methods to Prevent Webserver Exploitation
- Disable HTTP TRACK and TRACE Verbs in Internet Information Services (IIS)

Feedback

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