**Practice Labs - Ethical Hacker v10**

# Footprinting and Reconnaissance

- **Introduction**
- **Lab Topology**
- **Exercise 1 - Reconnaissance Tools and Techniques**
- **Exercise 2 - Conducting Active Reconnaissance in a Network**
- **Exercise 3 - Conducting Passive Reconnaissance in a Network**
- **Review**

## Introduction

Passive Reconnaissance
WHOis
Social Engineering
Maltego
Recon-ng
Metasploit
Active Reconnaissance
Nmap
Port
Service
Operating System
Ethical Hacking

Welcome to the **Footprinting and Reconnaissance** 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 - Reconnaissance Tools and Techniques
- Exercise 2 - Conducting Active Reconnaissance in a Network
- Exercise 3 - Conducting Passive Reconnaissance in a Network

After completing this lab, you will be able to:

- Know the Terminology
- Know Tools Used in Reconnaissance
- Know the Need for Reconnaissance or Footprinting
- Know Footprinting Countermeasures
- Identify Live Hosts on a Network
- Perform Discovery Scans
- Perform Port Scanning
- Fingerprint an Operating System
- Perform Service Probing
- Use the WHOis Website
- Perform Social Media Exploitation
- Use SHODAN
- Use Google Hacking Database
- Perform DNS Querying
- Use theHarvester
- Create a Temporary E-mail Account
- Use Maltego
- Use the AnyWho Website

# Exam Objectives

The following exam objectives are covered in this lab:

- **5.2** Information Security Assessment Methodologies

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

# Lab Duration

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

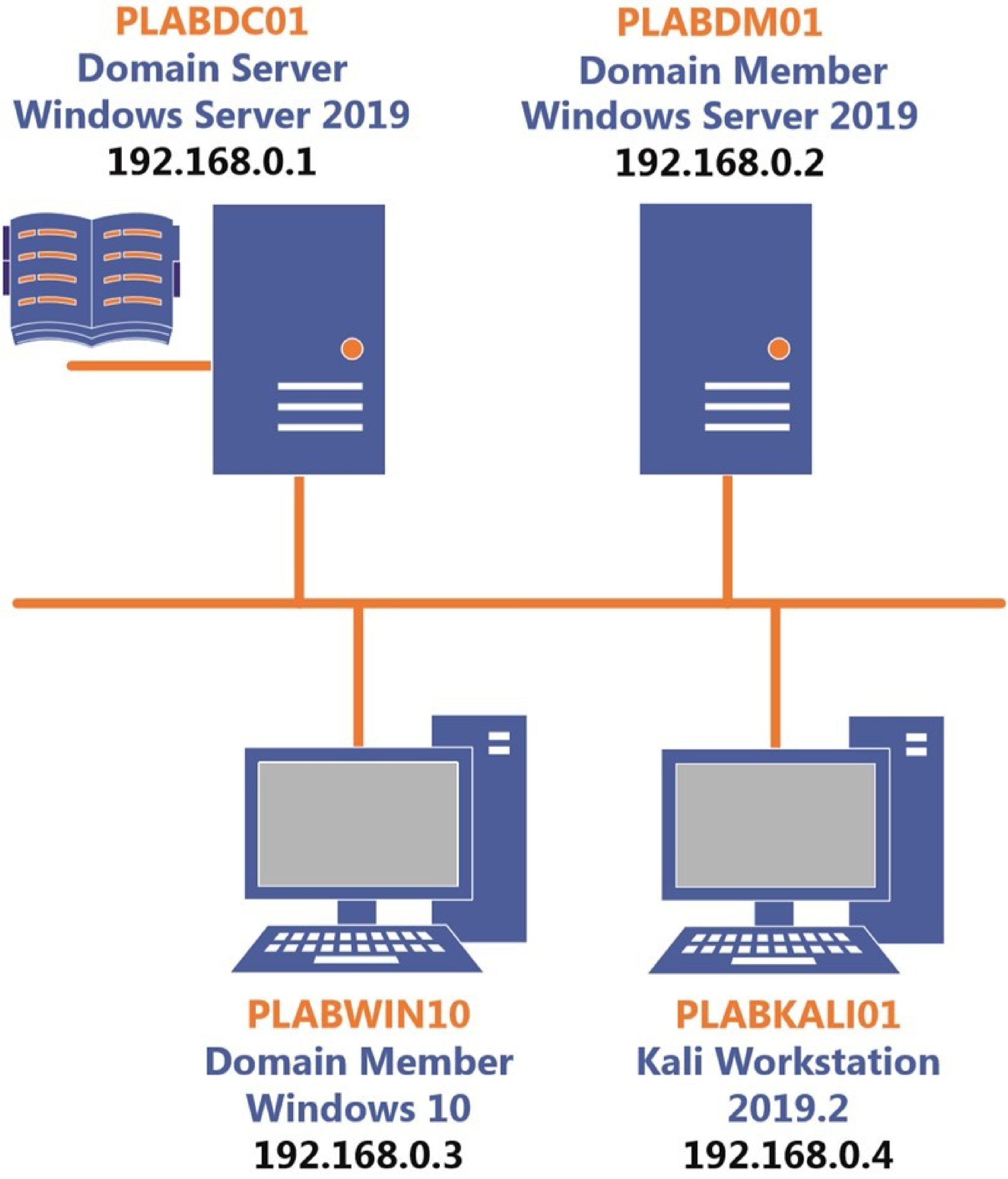
# Help and Support

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

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

# Lab Topology

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



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

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

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

## Exercise 1 - Reconnaissance Tools and Techniques

Reconnaissance, also known as Footprinting, is a method of collecting information about a target. It is the first phase and lays the foundation for the attack. With the discovered information, you can determine the attack surface of a target.

The following could be gathered about a target using reconnaissance:

- Basic information using Web searches
- Location of live systems on the network
- Network size
- Identification of open ports and running services
- Operating system version

Reconnaissance can be split into three parts:

1. **Footprinting**: Collecting information about an organization in a passive manner.
2. **Scanning**: Using active reconnaissance methods, such as nmap scanning, to extract information about networks and systems.
3. **Enumeration**: After footprinting and scanning have been completed, you can use the information to find the area that you want to attack. For example, if the attacker finds out that a specific version of Apache is being used, then the attacker can narrow down the attack to exploit its vulnerabilities.

In this exercise, you will learn about reconnaissance tools and techniques.

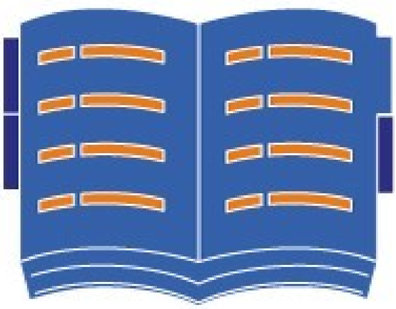
# Learning Outcomes

After completing this exercise, you will be able to:

- Know the Terminology
- Know Tools Used in Reconnaissance
- Know the Need for Reconnaissance or Footprinting
- Know Footprinting Countermeasures

# Your Devices

This exercise contains supporting materials for Reconnaissance Tools and Techniques.



### Task 1 - Know the Terminology

There is some basic terminology that an ethical hacker needs to know, including types of reconnaissance and footprinting.

There are five types of reconnaissance:

- Active
- Passive
- Pseudonymous
- Internet
- Anonymous

## *Active*

Using the active reconnaissance method, you directly interact with the system. For example, you can execute an nmap command to collect information about the open ports.

Active reconnaissance can include the following methods:

- IP or Port scanning
- Operating system scanning
- Footprinting of existing services in a system
- Zone transfer on an internal DNS server
- Spidering the public Webpages
- Fuzzing
- Social Engineering

## *Passive*

Passive reconnaissance is the opposite of active reconnaissance. You do not interact with the system. Instead, you use various methods, such as a Web search, to find information about a target.

Passive reconnaissance can use some of the following methods:

- Search the Whois database
- Browse through the target's Website
- Perform Social Network scraping
- Search Google or any search engine
- Extract the DNS information
- Review blogs, public forums, and Websites
- Search breach databases and DarkWeb about the target

## *Pseudonymous*

In this method, you collect information that is published by the target under a pseudo name. The target uses this name so that the information about him or her cannot be traced back to them.

## *Internet*

In this method, you would use the Internet to collect information about the target. For example, you can use Google hacking to find the information that otherwise is not visible in normal searches.

## *Anonymous*

In this method, you collect the information in an anonymous manner. You would use this method when you do not want someone to trace you.

### Task 2 - Tools Used in Reconnaissance

Various tools can be used in reconnaissance or footprinting. Some of the key tools are:

- Whois - Queries for domain names
- Nslookup - Queries DNS
- FOCA - Enumeration for users, files, folders, and OS information
- theHarvester - Information gathering for an E-mail address, subdomains, hostnames, banners
- Shodan - Information search engine using metadata
- Maltego - Information gathering
- Recon-ng - Web reconnaissance
- Censys - Search engine for information about devices on the Internet

Kali Linux also includes reconnaissance or footprinting tools under different categories, which are:

- DNS Analysis
- IDS/IPS Identification
- Live Host Identification
- Network & Port Scanners
- OSINT Analysis
- Route Analysis
- SMB Analysis

- SMTP Analysis
- SNMP Analysis
- SSL Analysis

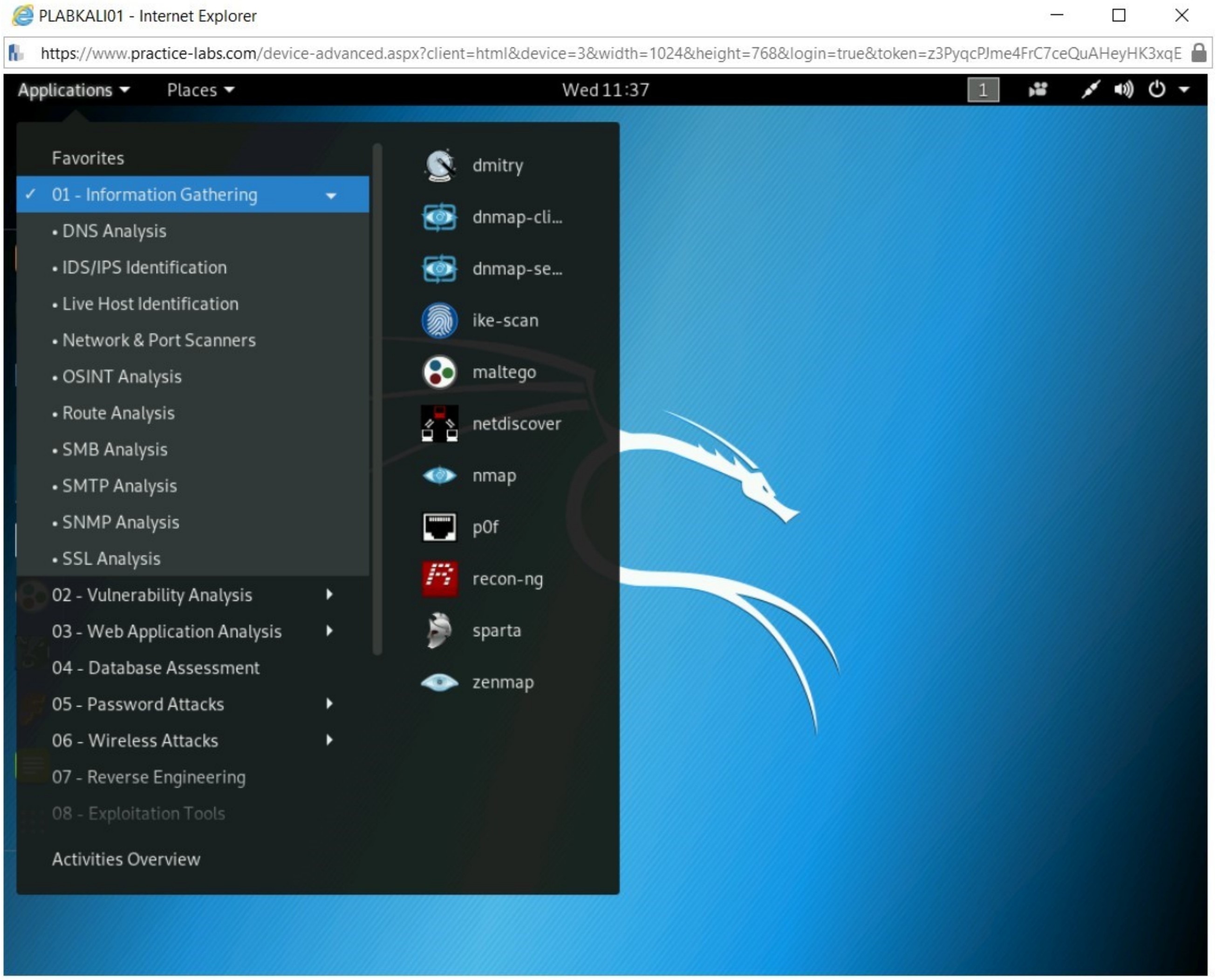


Figure 1.1 Screenshot of PLABKALI01: Displaying the categories of tools under 01- Information Gathering in the Applications menu.

The **DNS Analysis** category includes the following tools:

- dnsenum
- dnsmap
- dnsrecon
- dnstracer
- dnswalk
- fierce
- urlcrazy

The **IDS/IPS Identification** category includes the following tools:

- fragroute
- fragrouter
- ftest
- lbd
- wafw00f

The **Live Host Identification** category includes the following tools:

- arping
- cdpsnarf
- fping
- hping3
- masscan
- miranda
- ncat
- thcping6
- unicorscan
- wof-e
- xprobe2

The **Network & Port Scanners** category includes the following tools:

- masscan
- nmap
- unicorscan
- zenmap

The **OSINT Analysis** category includes the following tools:

- automater
- maltego
- theHarvester
- twofi
- urlcrazy

The **Route Analysis** category includes the following tools:

- 0trace
- intrace
- irpas-ass
- irpass-cdp
- netdiscover
- netmask

The **SMB Analysis** category includes the following tools:

- enum4linux
- nbtscan
- smbmap

The **SMTP Analysis** category includes the following tools:

- smtp-user-enum
- swaks

The **SNMP Analysis** category includes the following tools:

- braa
- onesixtyone
- snmp-check

The **SSL Analysis** category includes the following tools:

- sslaudit
- ssldump
- sslh
- sslscan
- sslyze
- tlssled

## Task 3 - Need for Reconnaissance or Footprinting

Without footprinting, it would be difficult for a hacker to break into a system or network. Therefore, hackers spend a significant amount of time gathering information about the system or the network of an organization. Based on the collected information, hackers build their hacking strategy and execute it. As an ethical hacker, you gain the following benefits when you perform footprinting:

## Understand the Security Posture

When you footprint an organization’s network, you can gain information on the security devices, the level of defense, and much more information about the security implementation. Based on the information that you collect, you build your attack accordingly. For example, you can understand if the organization has single-layered security, such as a firewall, or defense-in-depth, which contains multiple layers of security devices.

## Reduce Attack Area

The attack area is the target system or network that you want to exploit. It is always better to reduce the attack area so that you have a more controlled attack. Attacking a larger area is easier to trace, so the organization has more of a chance to stop the attack. You can reduce the attack area to a network subnet, a specific domain name, or an individual system that connects to the Internet directly.

## Collect Maximum Information

In the reconnaissance or footprinting phase, you may be able to gather a lot of information. Once identified and analysed, this information can help you generate your own database about the security weaknesses of a target system or network. Based on the weaknesses, you can prepare your attack to break into the security perimeter.

## Draw Network Diagram

Using the footprinting method, you can collect information and generate a network diagram, which can help you understand the network layout. For example, you can run the tracert tool to find the path from a system to a target system. A network diagram gives you clarity on how systems are placed on a network. For example, you can find whether the Internet-facing servers are placed on the same network or on a separate network, such as the demilitarized zone (DMZ).

### Task 4 - Footprinting Countermeasures

It is important to understand that footprinting and reconnaissance cannot be fully prevented. However, there are countermeasures that can be taken to minimize the impact. Some of the key countermeasures are:

- Perform footprinting to see what is visible to an external entity
- Disable unnecessary ports and services
- Configure a firewall to lockout ports that are not required
- Configure Webservers to use only required ports and disable the remaining ports
- Configure an intrusion detection system (IDS) to filter traffic and look for footprinting patterns
- Enforce security policies on the systems
- Educate users about security policies and various attacks, such as social engineering
- Disable directory listings on the Webservers
- Use separate internal and external DNS servers
- Use TCP/IP and IPsec filters
- Configure Webservers to disable banner

## Exercise 2 - Conducting Active Reconnaissance in a Network

Active reconnaissance is a hands-on method where you interact with the system directly to collect information.

In this exercise, you will learn about conducting active reconnaissance.

## Learning Outcomes

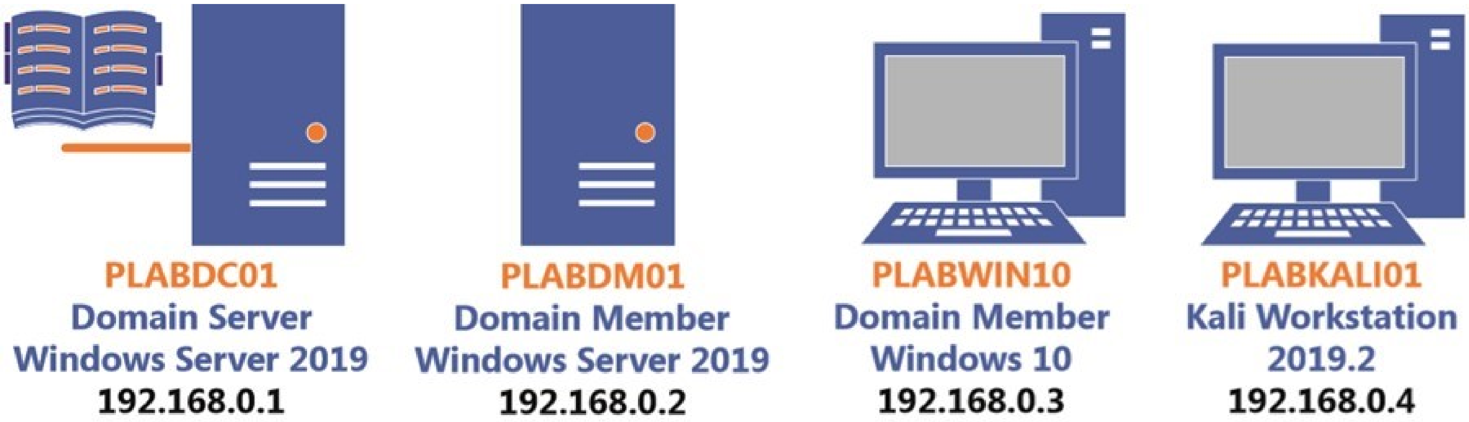
After completing this exercise, you will be able to:

- Identify Live Hosts on a Network
- Perform Discovery Scans
- Perform Port Scanning
- Fingerprint an Operating System
- Perform Service Probing

# 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 - Member)
- **PLABWIN10 -** (Windows 10 - Workstation)
- **PLABKALI01 -** (Kali 2019.2 - Linux Kali Workstation)



## Task 1 - Identify Live Hosts on a Network

Network Mapper, known as Nmap, is a network and host discovery tool. It is one of the most widely used tools for various activities, such as:

- Discovering hosts, services, and ports
- Fingerprinting operating systems
- Enumeration
- Discovering vulnerabilities on the local and remote host
- Finding the IP address of a remote system

Using Nmap, you can scan for targets by:

- Scanning for a single IP: nmap 192.168.0.1
- Scanning for a host by using its name: nmap host1.plab.com
- Scanning an entire subnet: nmap plab.com/24, nmap 192.168.0.0/24, nmap 192.168.0.*
- Scanning for a range of IP addresses: nmap 192.168.0.1-10
- Scanning for a range and a system outside the range: nmap 192.168.0.1, 1.10

In this task, you will use Nmap to identify the live systems on a network. To do this, perform the following steps:

## Step 1

Ensure that you have logged into **PLABKALI01**.

Crentials are:

```
Username: root Password: Passw0rd
```

## Step 2

On the desktop, click **Terminal**.

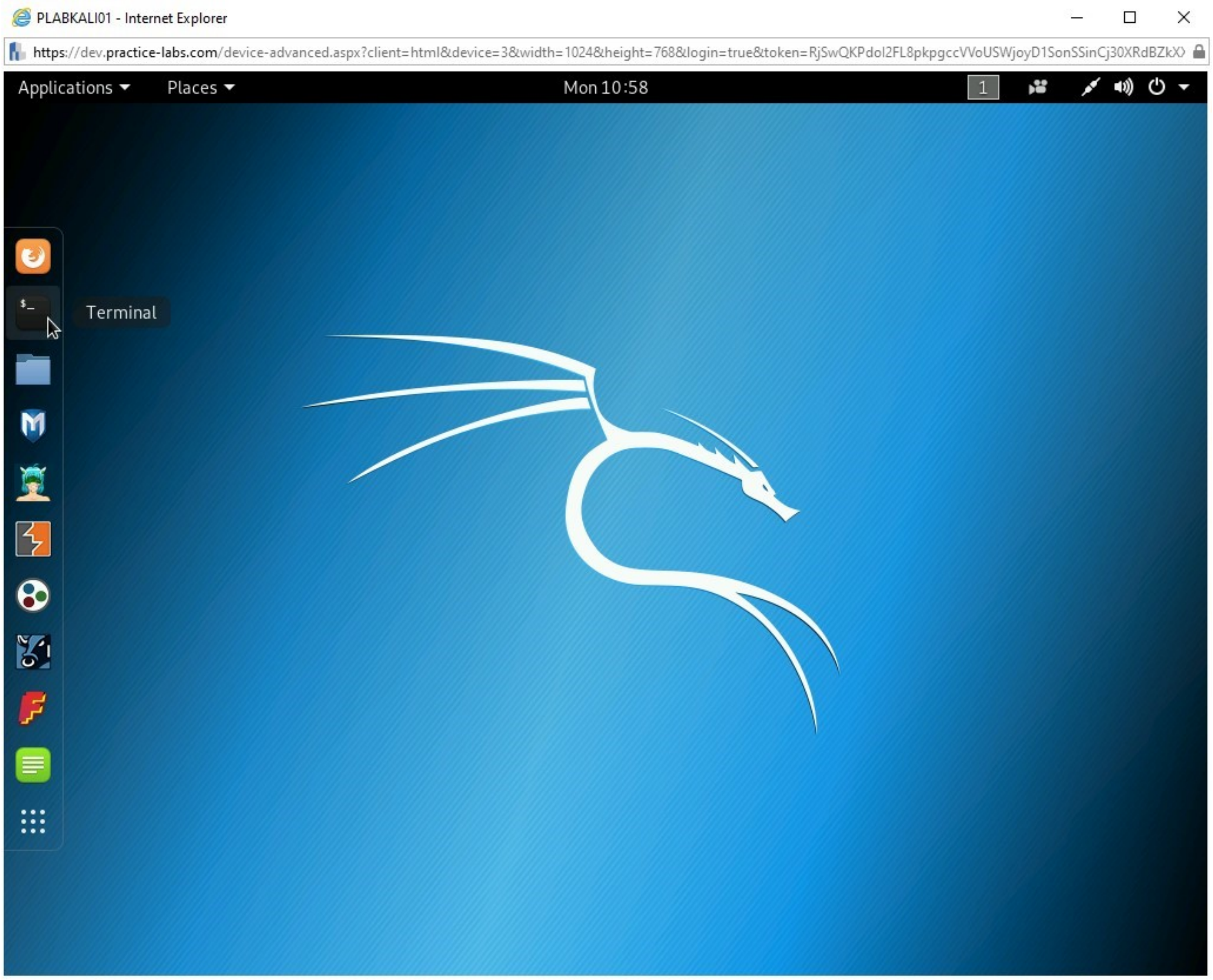

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Mon 10:58
1
Terminal

Figure 2.1 Screenshot of PLABKALI01: Clicking the Terminal icon in the left pane.

## Step 3

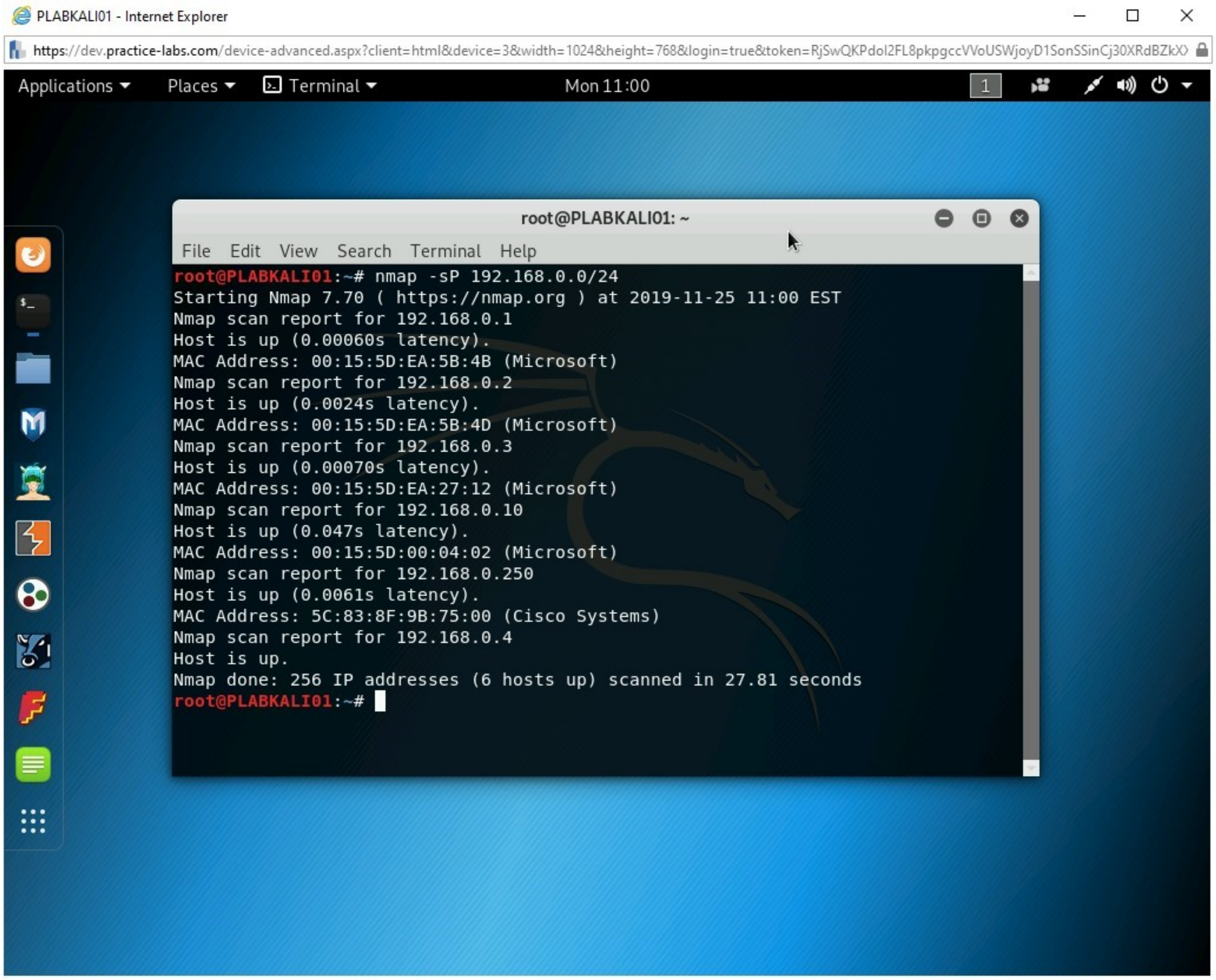
The terminal window is displayed. You will now perform a ping scan to discover the live hosts in a network. Type the following command:

```
nmap -sP 192.168.0.0/24
```

Press **Enter**.

***Note**: the -sP parameter is used for ping scanning. When you use CIDR /24, Nmap will scan all 256 IP addresses on the network.*

The output of the command is displayed. Notice that there were six hosts that were detected. It has found five systems in the lab environment, including Kali. Along with this, the gateway IP, 192.168.0.250, is also found.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:00
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# nmap -sP 192.168.0.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:00 EST
Nmap scan report for 192.168.0.1
Host is up (0.00060s latency).
MAC Address: 00:15:5D:EA:5B:4B (Microsoft)
Nmap scan report for 192.168.0.2
Host is up (0.0024s latency).
MAC Address: 00:15:5D:EA:5B:4D (Microsoft)
Nmap scan report for 192.168.0.3
Host is up (0.00070s latency).
MAC Address: 00:15:5D:EA:27:12 (Microsoft)
Nmap scan report for 192.168.0.10
Host is up (0.047s latency).
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Nmap scan report for 192.168.0.250
Host is up (0.0061s latency).
MAC Address: 5C:83:8F:9B:75:00 (Cisco Systems)
Nmap scan report for 192.168.0.4
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 27.81 seconds
root@PLABKALI01:~#
```

Figure 2.2 Screenshot of PLABKALI01: Showing the output of the nmap -sP command.

## Step 4

Clear the screen by entering the following command:

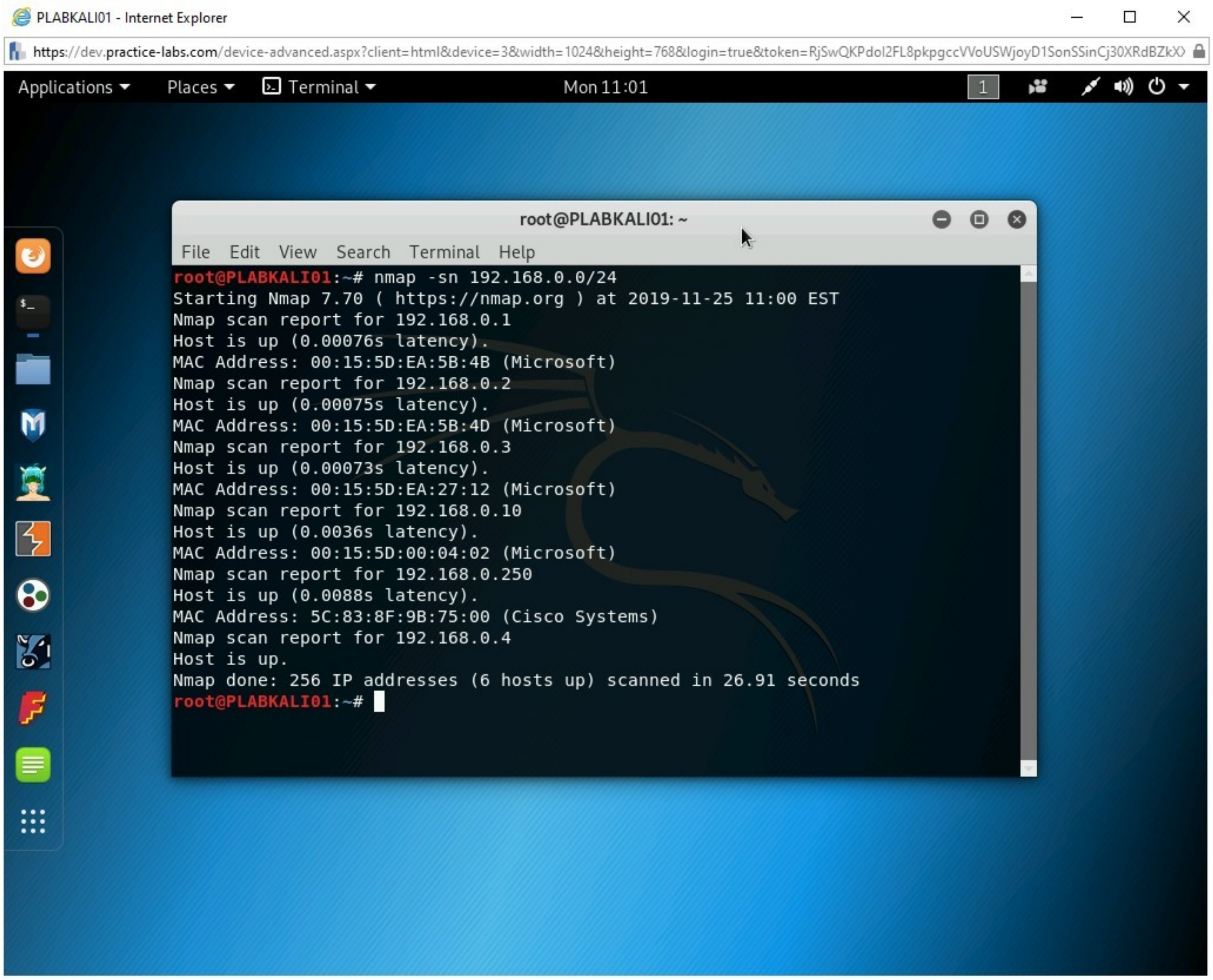
```
clear
```

You can also perform a scan without ping. To do this, type the following command:

```
nmap -sn 192.168.0.0/24
```

Press **Enter**.

The output of the command is displayed. Notice that without the ping scan, it has detected six systems on the network.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:01
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# nmap -sn 192.168.0.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:00 EST
Nmap scan report for 192.168.0.1
Host is up (0.00076s latency).
MAC Address: 00:15:5D:EA:5B:4B (Microsoft)
Nmap scan report for 192.168.0.2
Host is up (0.00075s latency).
MAC Address: 00:15:5D:EA:5B:4D (Microsoft)
Nmap scan report for 192.168.0.3
Host is up (0.00073s latency).
MAC Address: 00:15:5D:EA:27:12 (Microsoft)
Nmap scan report for 192.168.0.10
Host is up (0.0036s latency).
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Nmap scan report for 192.168.0.250
Host is up (0.0088s latency).
MAC Address: 5C:83:8F:9B:75:00 (Cisco Systems)
Nmap scan report for 192.168.0.4
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 26.91 seconds
root@PLABKALI01:~#
```

Figure 2.3 Screenshot of PLABKALI01: Showing the output of the nmap -sn command.

## Step 5

Clear the screen by entering the following command:

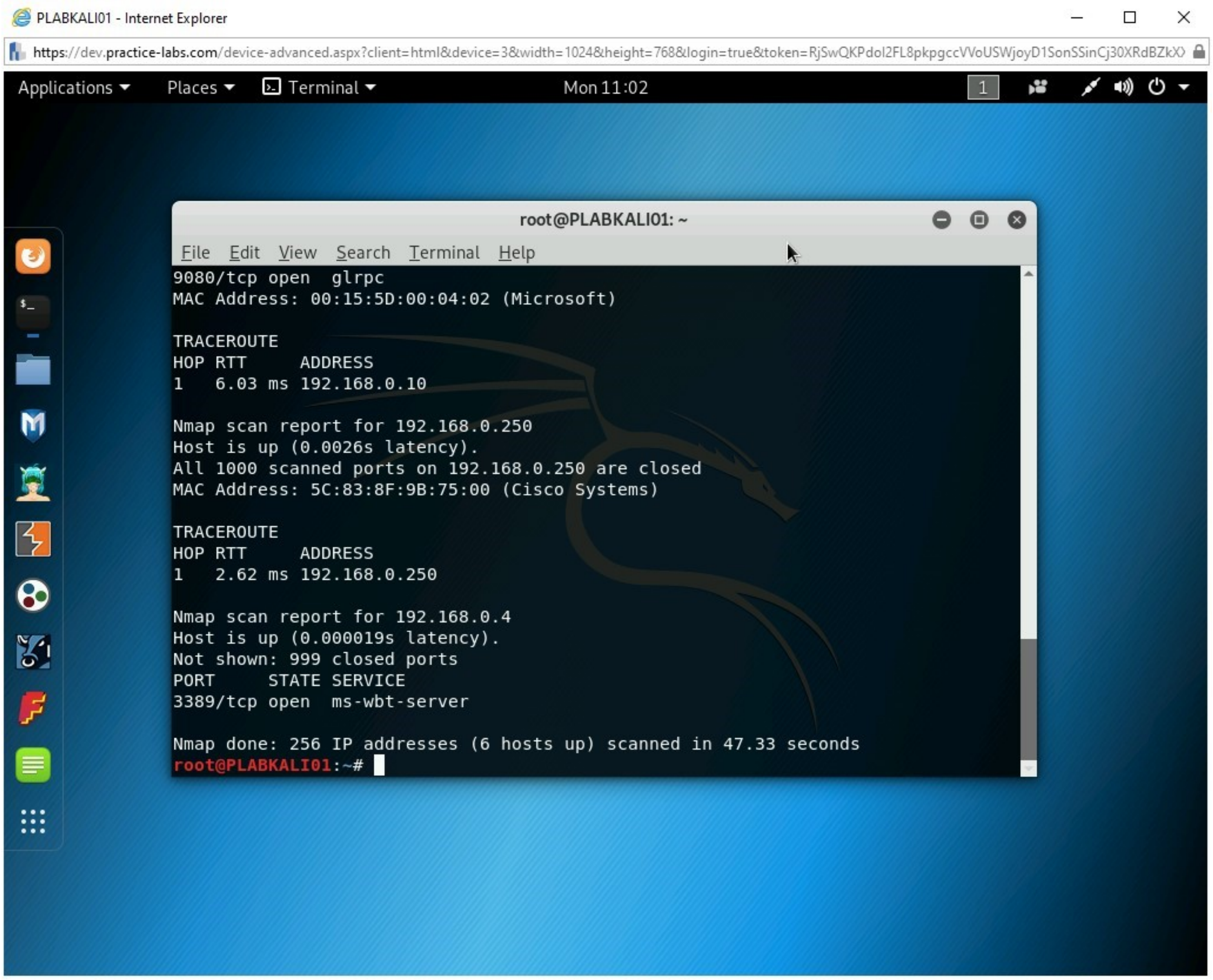
```
clear
```

You can also trace the path between your system and each of the hosts that is live on the network. To do this, type the following command:

```
nmap --traceroute 192.168.0.0/24
```

Press **Enter**.

Notice the output of the command. In the output, the hops from your system to the systems on the network are displayed. Since this is within the same IP subnet, there is a single hop. The output also displays open ports on each live system.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:02
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
9080/tcp open  glrpc
MAC Address: 00:15:5D:00:04:02 (Microsoft)

TRACEROUTE
HOP RTT     ADDRESS
1   6.03 ms 192.168.0.10

Nmap scan report for 192.168.0.250
Host is up (0.0026s latency).
All 1000 scanned ports on 192.168.0.250 are closed
MAC Address: 5C:83:8F:9B:75:00 (Cisco Systems)

TRACEROUTE
HOP RTT     ADDRESS
1   2.62 ms 192.168.0.250

Nmap scan report for 192.168.0.4
Host is up (0.000019s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap done: 256 IP addresses (6 hosts up) scanned in 47.33 seconds
root@PLABKALI01:~#
```

Figure 2.4 Screenshot of PLABKALI01: Showing the output of the nmap - - traceroute command.

## Step 6

Clear the screen by entering the following command:

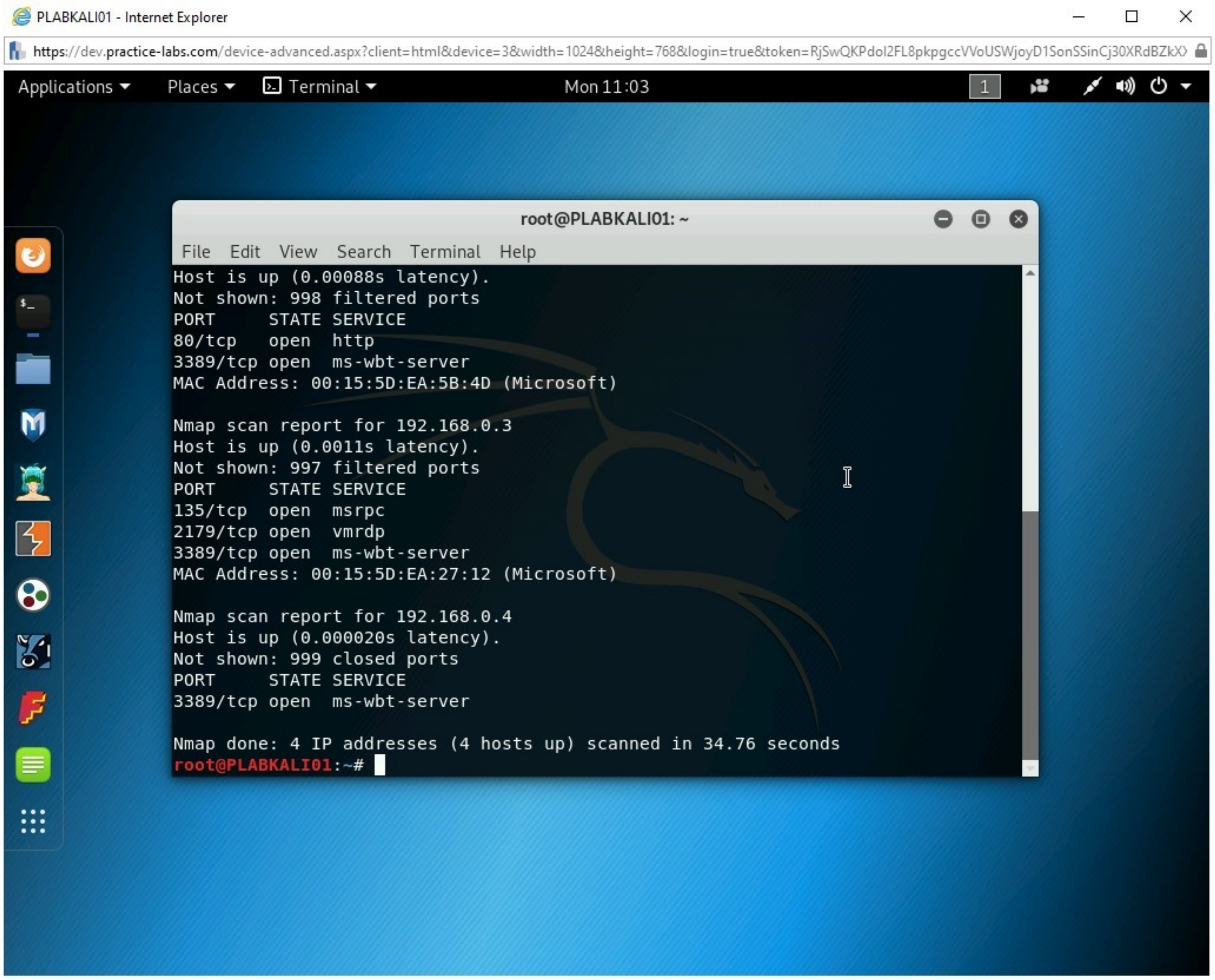
```
clear
```

You can also scan for live hosts on a network using an IP address range. To do this, type the following command:

```
nmap 192.168.0.1-4
```

Press **Enter**.

The output of the command is displayed. Notice that only four hosts are listed in the scan. Without any parameters, the nmap command scans for the live systems and open ports.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:03
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
Host is up (0.00088s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:EA:5B:4D (Microsoft)

Nmap scan report for 192.168.0.3
Host is up (0.0011s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:EA:27:12 (Microsoft)

Nmap scan report for 192.168.0.4
Host is up (0.000020s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap done: 4 IP addresses (4 hosts up) scanned in 34.76 seconds
root@PLABKALI01:~#
```

Figure 2.5 Screenshot of PLABKALI01: Showing the output of the nmap command with a series of IP addresses.

## Step 7

Clear the screen by entering the following command:

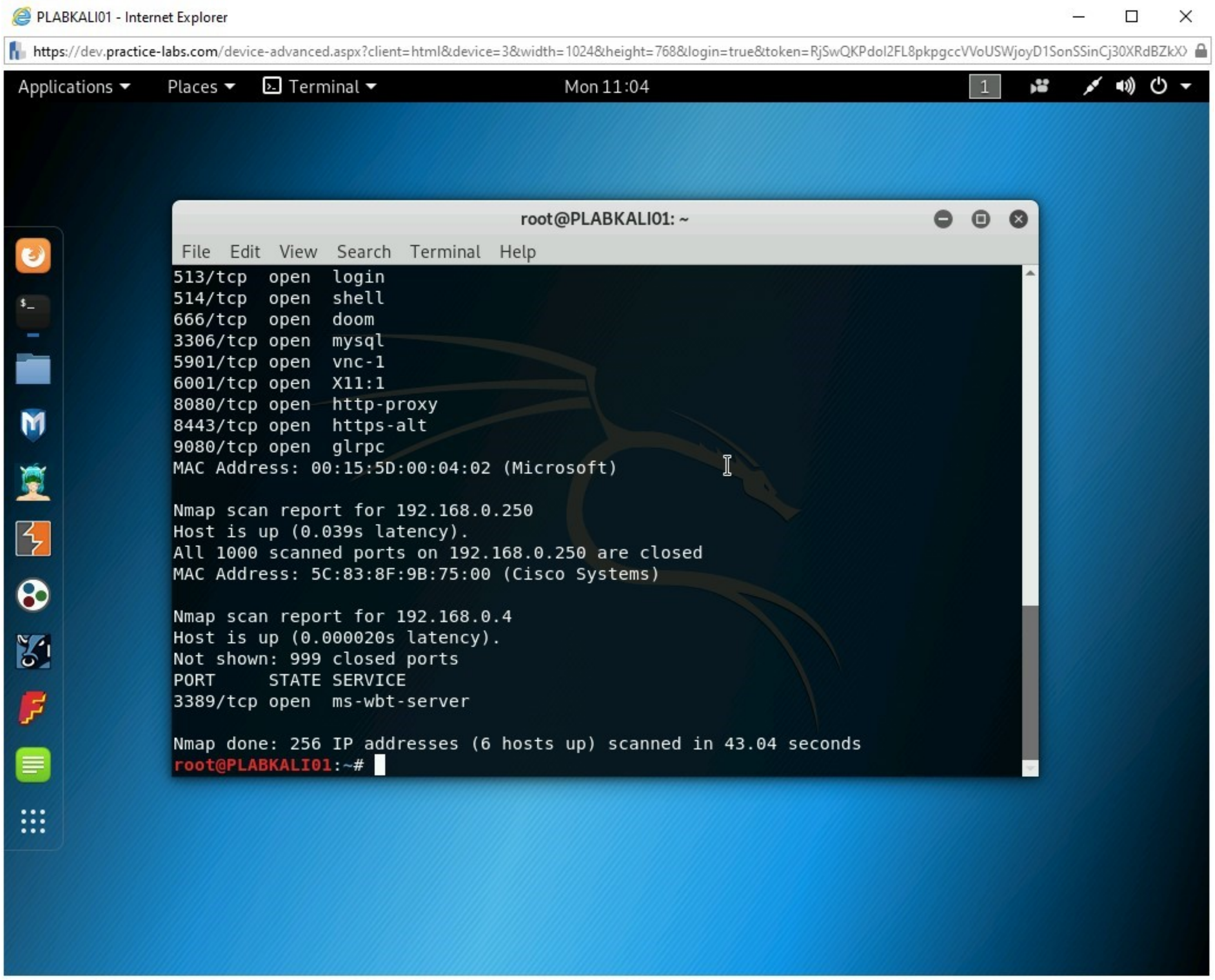
```
clear
```

You can also use a wildcard to scan an IP range. To do this, type the following command:

```
nmap 192.168.0.*
```

Press **Enter**.

Notice the output of the command. It has searched for all live systems in the subnet of 256 IP addresses.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:04
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
MAC Address: 00:15:5D:00:04:02 (Microsoft)

Nmap scan report for 192.168.0.250
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.0.250 are closed
MAC Address: 5C:83:8F:9B:75:00 (Cisco Systems)

Nmap scan report for 192.168.0.4
Host is up (0.000020s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap done: 256 IP addresses (6 hosts up) scanned in 43.04 seconds
root@PLABKALI01:~#
```

Figure 2.6 Screenshot of PLABKALI01: Showing the output of the nmap command with a wildcard.

**Alert**: Keep the terminal window open.

### Task 2 - Perform Discovery Scans

A discovery scan is used to locate live hosts on a network. There are various methods that can be used in discovery scans. Some of these are:

- Using ping scan
- Using ARP scan
- Using a port scan

In this task, you will learn to perform different types of discovery scans. To do this, perform the following steps:

## *Step 1*

Ensure that you are connected to **PLABKALI01**, and the terminal window is open.

Clear the screen by entering the following command:

```
clear
```

Using ping for discovering a host is a common method.

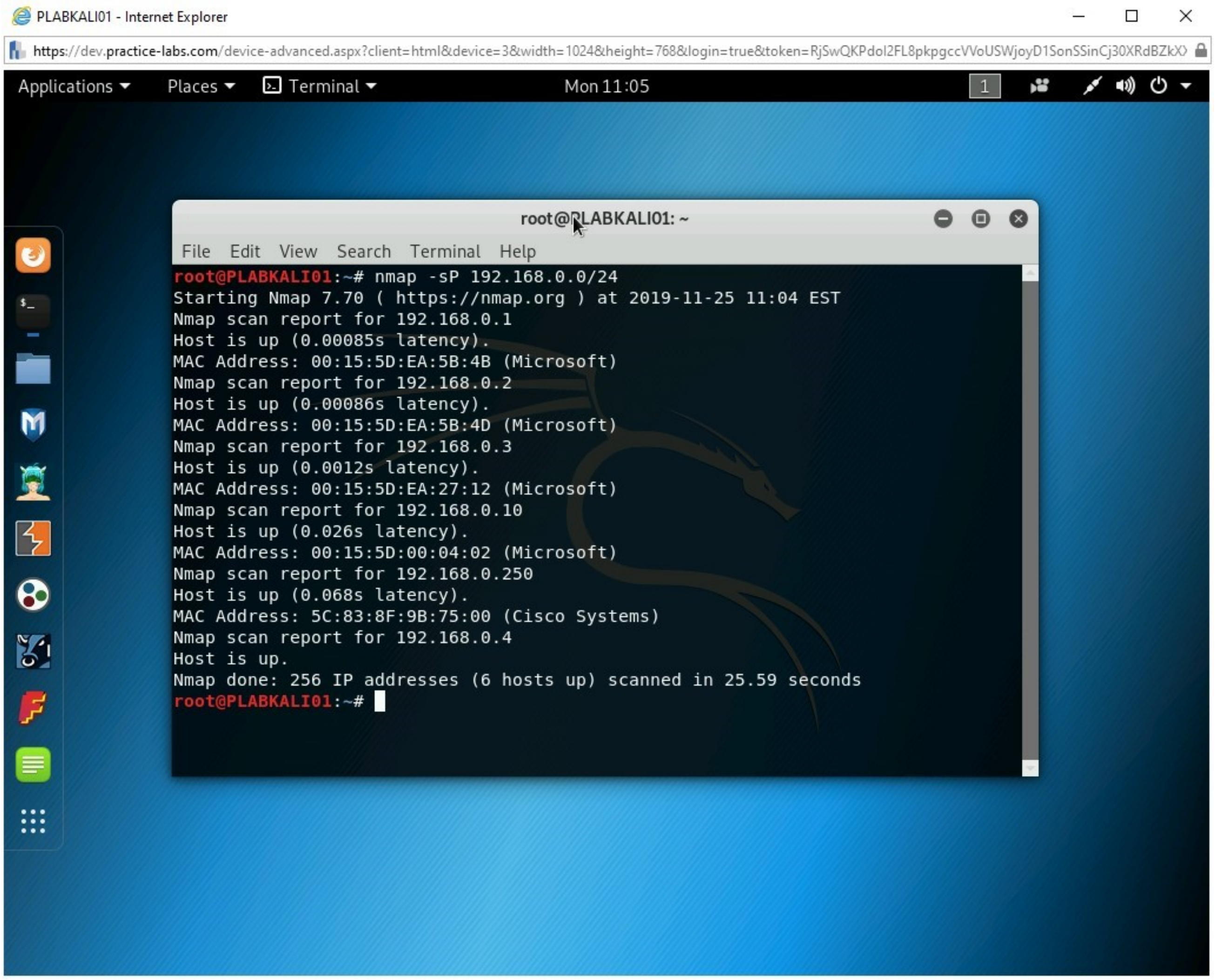
Type the following command:

```
nmap -sP 192.168.0.0/24
```

Press **Enter**.

> ***Note****: Several systems have firewalls running that block ping commands, and therefore, discovering a host using ping may not be successful.*

Notice the output of the command. When you execute this command, it sends an ICMP REQUEST message to every IP address. The hosts that respond to the ICMP REQUEST message are considered alive and are listed in the output. This command output does not list the hosts that do not respond.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:05
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# nmap -sP 192.168.0.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:04 EST
Nmap scan report for 192.168.0.1
Host is up (0.00085s latency).
MAC Address: 00:15:5D:EA:5B:4B (Microsoft)
Nmap scan report for 192.168.0.2
Host is up (0.00086s latency).
MAC Address: 00:15:5D:EA:5B:4D (Microsoft)
Nmap scan report for 192.168.0.3
Host is up (0.0012s latency).
MAC Address: 00:15:5D:EA:27:12 (Microsoft)
Nmap scan report for 192.168.0.10
Host is up (0.026s latency).
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Nmap scan report for 192.168.0.250
Host is up (0.068s latency).
MAC Address: 5C:83:8F:9B:75:00 (Cisco Systems)
Nmap scan report for 192.168.0.4
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 25.59 seconds
root@PLABKALI01:~#
```

Figure 2.7 Screenshot of PLABKALI01: Showing the output of the nmap -sP command.

## Step 2

Clear the screen by entering the following command:

```
clear
```

You can also send ARP requests to the hosts on a given subnet, and if the target system responds to these requests, then it means that it is alive. This method, unlike the Ping scan method, is not usually blocked by the firewall. Therefore, you are likely to get a better outcome.

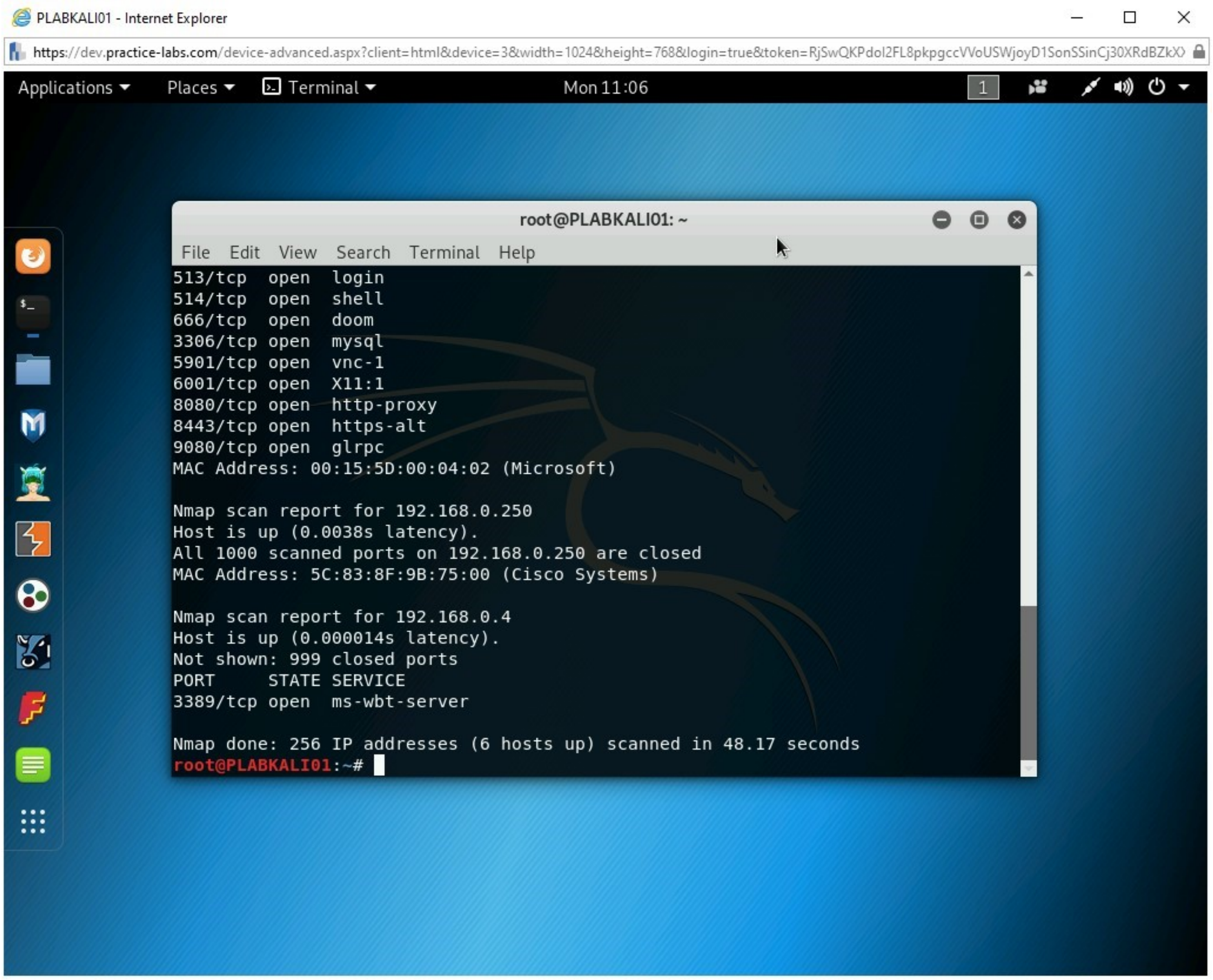
To send the ARP requests to the **192.168.0.0/24** subnet, type the following command:

```
nmap -PR 192.168.0.0/24
```

Press **Enter**.

Notice the outcome of this command. With the **-PR** parameter, the nmap command has scanned 256 IP addresses and found 6 hosts live. Open ports are also listed.

> ***Note****: You can scan for the live hosts without also detecting the open ports. To do this, you can use the following command:* ***nmap -sn 192.168.0.0/24****.*


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:06
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
MAC Address: 00:15:5D:00:04:02 (Microsoft)

Nmap scan report for 192.168.0.250
Host is up (0.0038s latency).
All 1000 scanned ports on 192.168.0.250 are closed
MAC Address: 5C:83:8F:9B:75:00 (Cisco Systems)

Nmap scan report for 192.168.0.4
Host is up (0.000014s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap done: 256 IP addresses (6 hosts up) scanned in 48.17 seconds
root@PLABKALI01:~#
```

Figure 2.8 Screenshot of PLABKALI01: Showing the output of the nmap -PR command.

## Step 3

Clear the screen by entering the following command:

```
clear
```

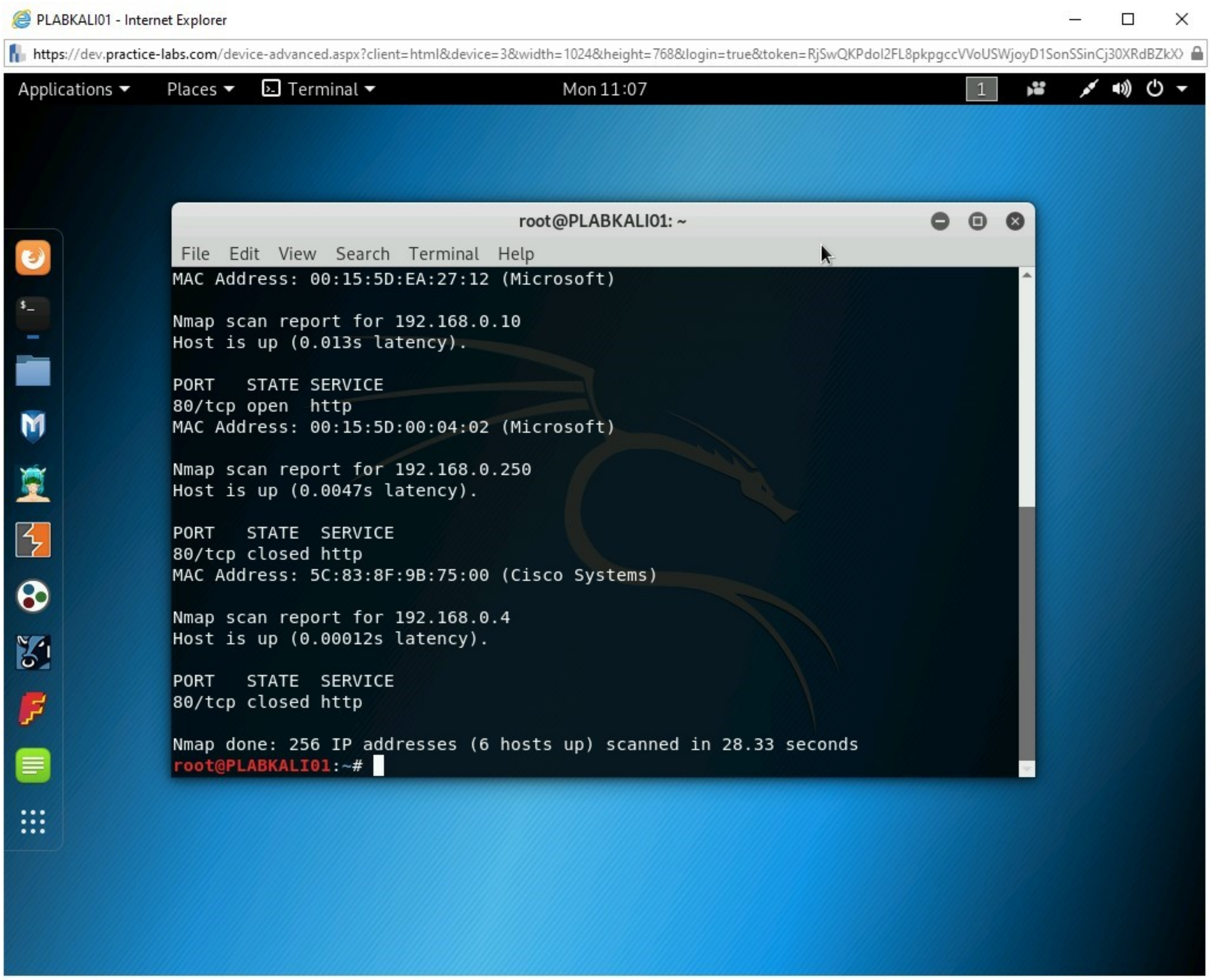
You can also scan for open ports to detect the system status. This could be useful when the systems have firewalls enabled, or the systems are in another subnet or network. When you attempt to detect the ports, the systems will respond to the request. Type the following command:

```
nmap -p 80 192.168.0.0/24
```

Press **Enter**.

The output of this command is displayed. Notice that seven hosts are scanned, but one host, **192.168.0.2**, is running a Web server.

> ***Note***: *With the -p parameter, you can scan for more than one port. For example, you can use the following command:* ***nmap -p 22, 23, 80, 139, 445, 3389 192.168.0.0/24****. Each port number needs to be separated by a comma.*


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:07
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
MAC Address: 00:15:5D:EA:27:12 (Microsoft)

Nmap scan report for 192.168.0.10
Host is up (0.013s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:15:5D:00:04:02 (Microsoft)

Nmap scan report for 192.168.0.250
Host is up (0.0047s latency).

PORT   STATE  SERVICE
80/tcp closed http
MAC Address: 5C:83:8F:9B:75:00 (Cisco Systems)

Nmap scan report for 192.168.0.4
Host is up (0.00012s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 256 IP addresses (6 hosts up) scanned in 28.33 seconds
root@PLABKALI01:~#
```

Figure 2.9 Screenshot of PLABKALI01: Showing the output of the nmap -p command.

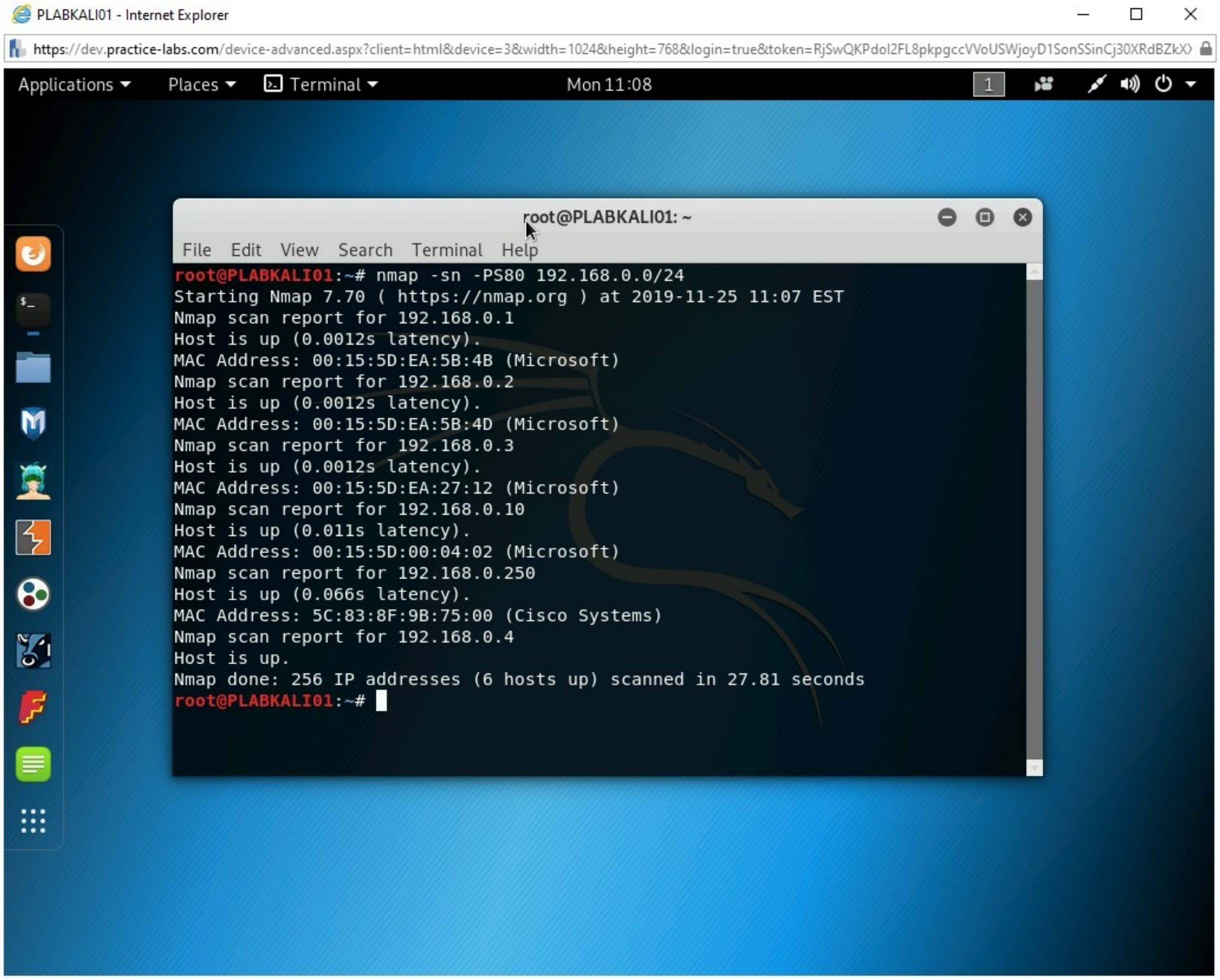
## Step 4

You can also send the **SYN** message to a specific port on a subnet to detect live systems. To do this, type the following command:

```
nmap -sn -PS80 192.168.0.0/24
```

Press **Enter**.

The output of this command is displayed. Notice that six hosts were found to be live in this subnet.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:08
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# nmap -sn -PS80 192.168.0.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:07 EST
Nmap scan report for 192.168.0.1
Host is up (0.0012s latency).
MAC Address: 00:15:5D:EA:5B:4B (Microsoft)
Nmap scan report for 192.168.0.2
Host is up (0.0012s latency).
MAC Address: 00:15:5D:EA:5B:4D (Microsoft)
Nmap scan report for 192.168.0.3
Host is up (0.0012s latency).
MAC Address: 00:15:5D:EA:27:12 (Microsoft)
Nmap scan report for 192.168.0.10
Host is up (0.011s latency).
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Nmap scan report for 192.168.0.250
Host is up (0.066s latency).
MAC Address: 5C:83:8F:9B:75:00 (Cisco Systems)
Nmap scan report for 192.168.0.4
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 27.81 seconds
root@PLABKALI01:~#
```

Figure 2.10 Screenshot of PLABKALI01: Showing the output of the nmap -sn -PS80 command.

**Alert**: Keep the terminal window open.

## Task 3 - Perform Port Scanning

Using the port scan method, you can determine the TCP or UDP port that is being used. You can either scan for the entire range of ports, which are from 1 to 65535, or can scan for specific ports. When scanning for ports, you need to be aware that there can be different states of a port:

**Open**: An application is listening for connections on this port.

**Closed**: The messages were received, but no application is listening on the port.

**Filtered**: The messages were not received, and the state of the port could not be determined. This state occurs when some type of filtering is being used on the port.

**Unfiltered**: The messages are received, but the state of the port could not be determined.

**Open/Filtered**: The port was either filtered or open, but Nmap was not able to determine the state.

**Closed/Filtered**: The port was either filtered or closed, but Nmap was not able to determine the state.

To use port scanning, perform the following steps:

### *Step 1*

Ensure that you are connected to **PLABKALI01**, and the terminal window is open.

Clear the screen by entering the following command:

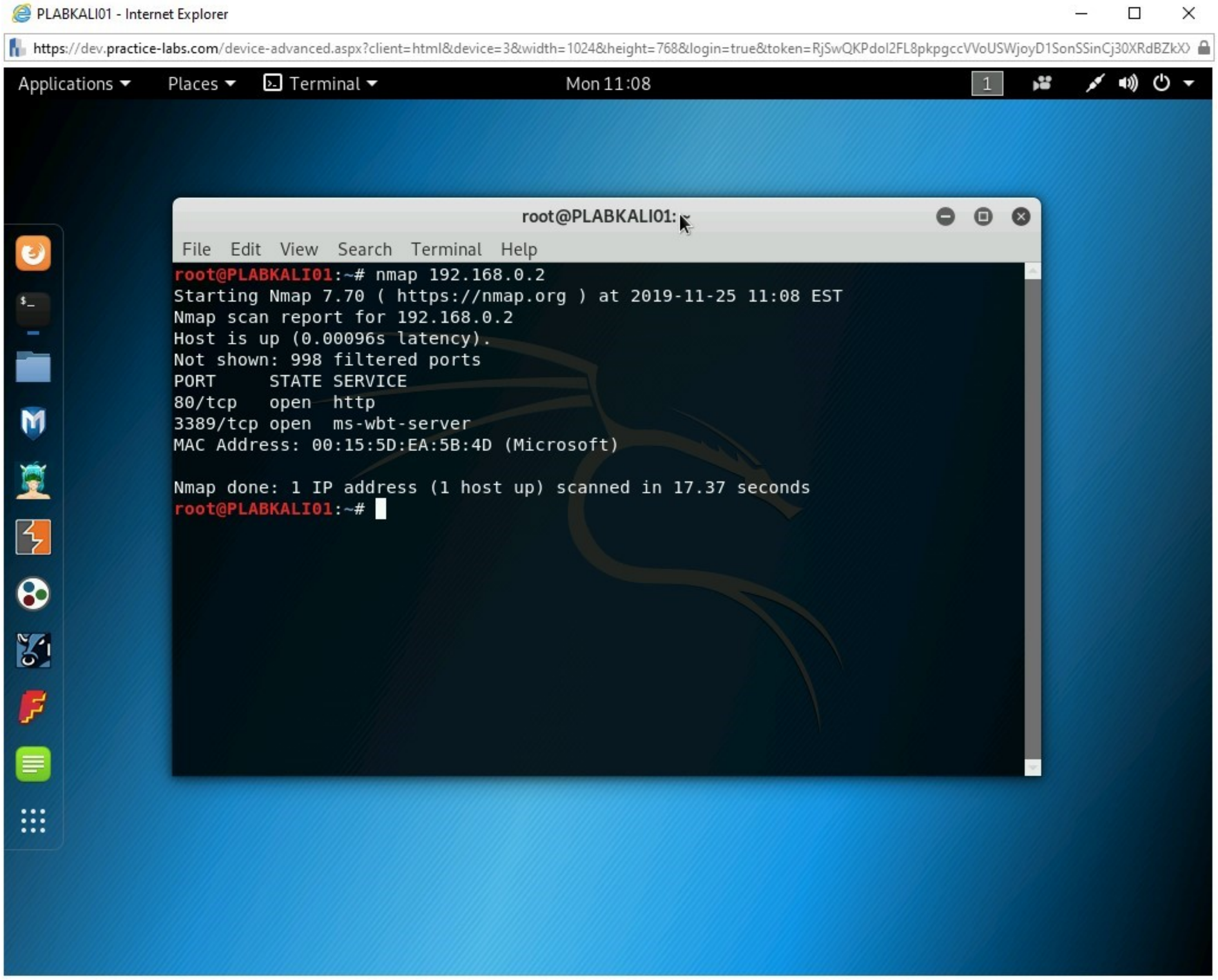
```
clear
```

One of the simplest methods is to target a system with the nmap command without using any parameters. To do this, type the following command:

```
nmap 192.168.0.2
```

Press **Enter**.

The output of this command is displayed. Notice that **192.168.0.2** has two ports open, which are **80** and **3389**.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:08
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# nmap 192.168.0.2
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:08 EST
Nmap scan report for 192.168.0.2
Host is up (0.00096s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:EA:5B:4D (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 17.37 seconds
root@PLABKALI01:~#
```

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

## *Step 2*

Clear the screen by entering the following command:

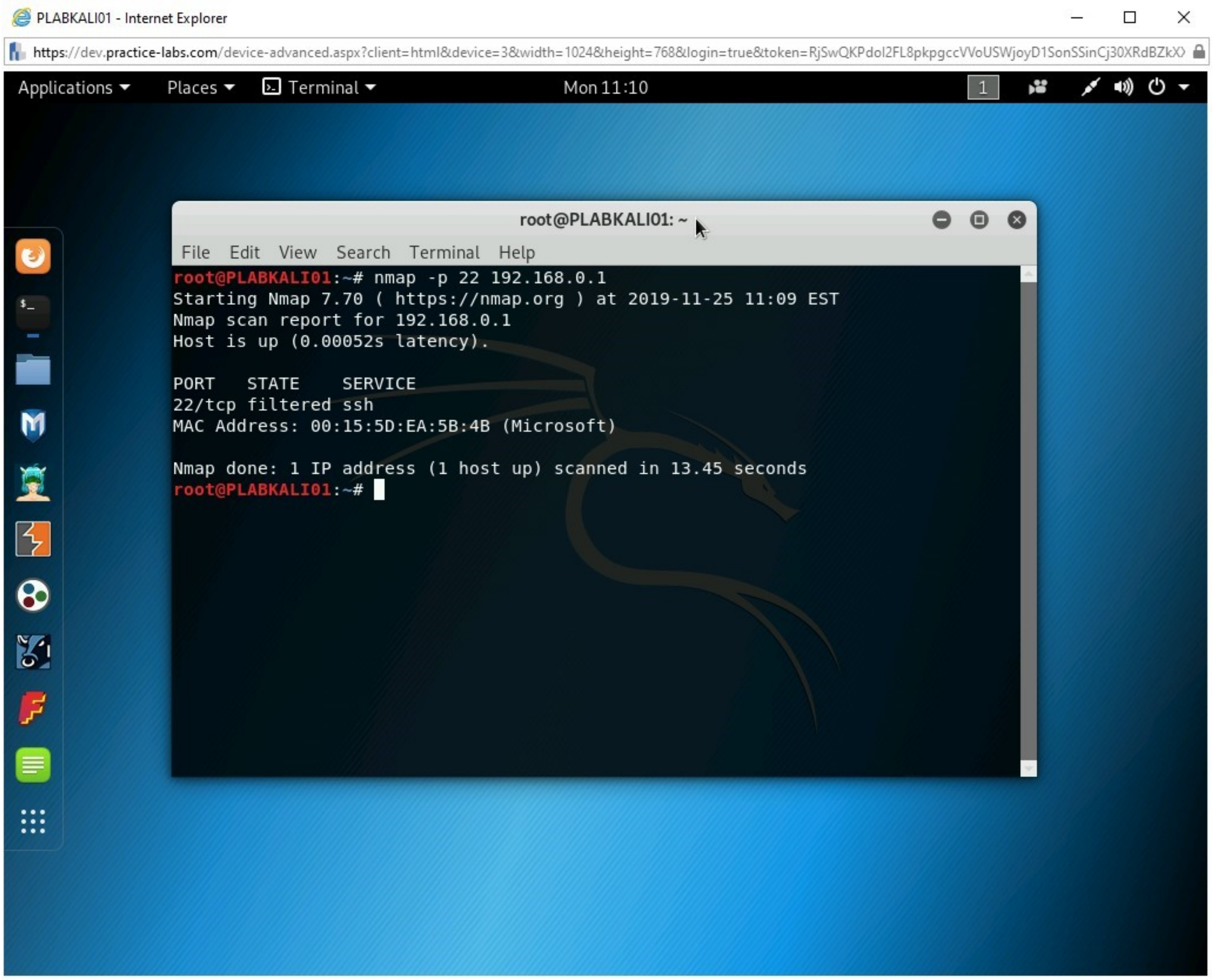
```
clear
```

You can scan for a single port on a host. To do this, type the following command:

```
nmap -p 22 192.168.0.1
```

Press **Enter**.

The output of this command is displayed. Notice that the state of the port is set to filtered.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:10
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# nmap -p 22 192.168.0.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:09 EST
Nmap scan report for 192.168.0.1
Host is up (0.00052s latency).

PORT   STATE    SERVICE
22/tcp filtered ssh
MAC Address: 00:15:5D:EA:5B:4B (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 13.45 seconds
root@PLABKALI01:~#
```

Figure 2.12 Screenshot of PLABKALI01: Showing the output of the nmap -p 22 command.

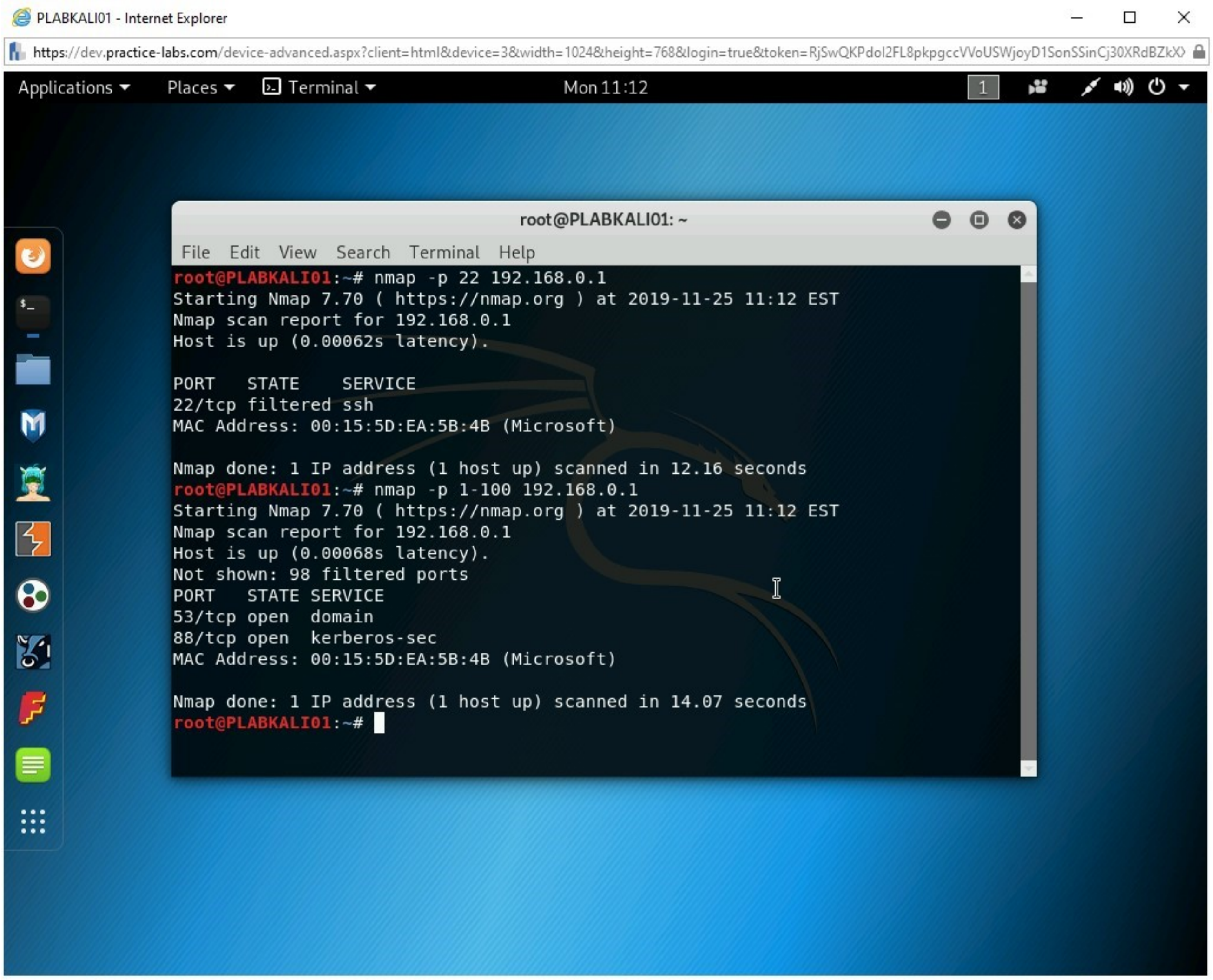
## *Step 3*

Let's try to scan for the range of ports on **192.168.0.1**, which is the domain controller. To do this, type the following command:

```
nmap -p 1-100 192.168.0.1
```

Press **Enter**.

Notice that the command has been executed successfully. The output displays that there are 98 filtered ports and two open ports, which are **53** and **88**.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:12
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# nmap -p 22 192.168.0.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:12 EST
Nmap scan report for 192.168.0.1
Host is up (0.00062s latency).

PORT   STATE    SERVICE
22/tcp filtered ssh
MAC Address: 00:15:5D:EA:5B:4B (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 12.16 seconds
root@PLABKALI01:~# nmap -p 1-100 192.168.0.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:12 EST
Nmap scan report for 192.168.0.1
Host is up (0.00068s latency).
Not shown: 98 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
88/tcp open  kerberos-sec
MAC Address: 00:15:5D:EA:5B:4B (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 14.07 seconds
root@PLABKALI01:~#
```

Figure 2.13 Screenshot of PLABKALI01: Showing the output of the nmap -p 1-100 command.

## *Step 4*

Clear the screen by entering the following command:

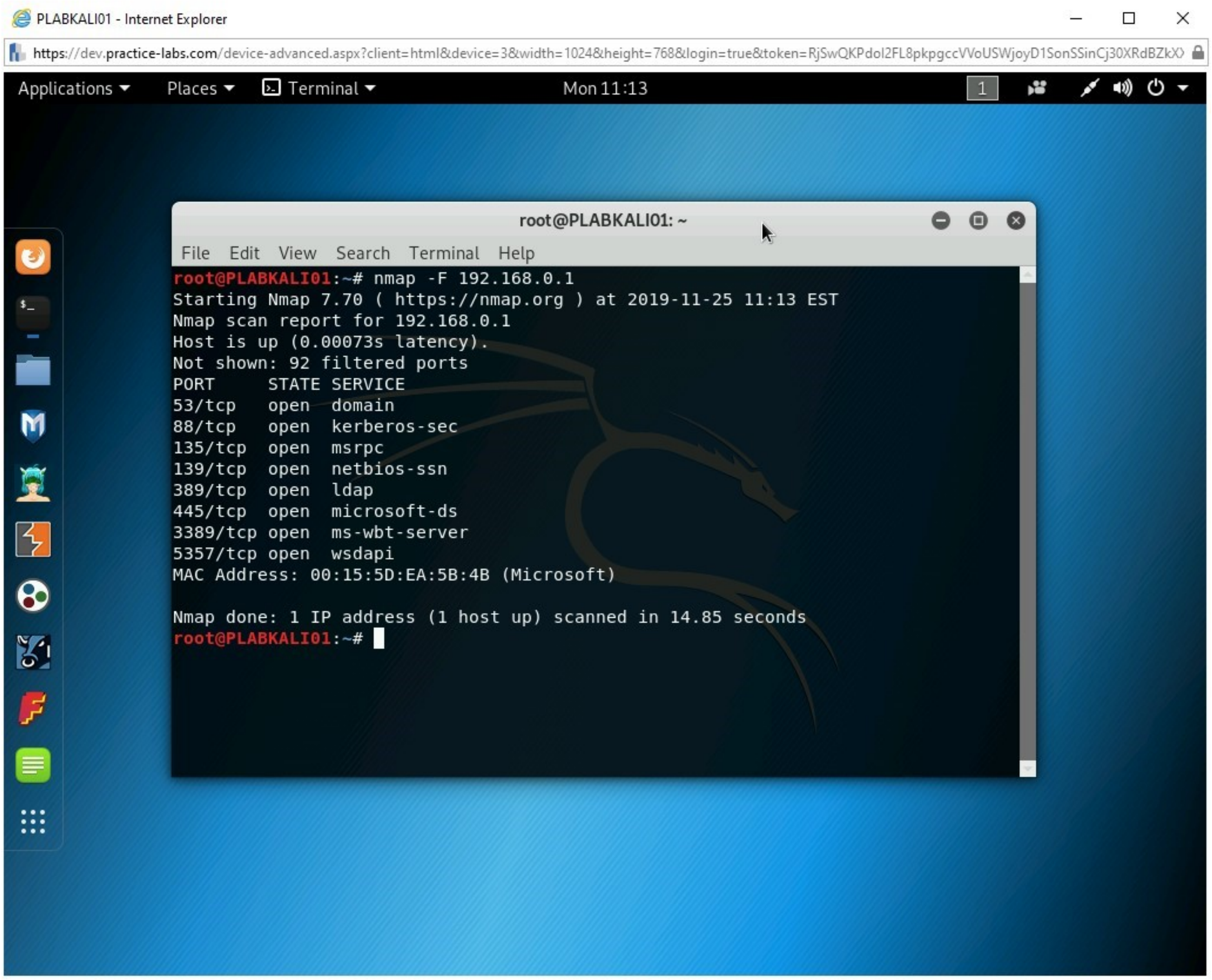
```
clear
```

A fast scan will scan for the 100 common ports on a given system. To do this, type the following command:

```
nmap -F 192.168.0.1
```

Press **Enter**.

The output of this command is displayed. Notice that the output of this command is different than the previous command. It shows 92 filtered ports and 8 open ports. The output is different because the fast scan uses the 100 most common ports.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:13
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# nmap -F 192.168.0.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:13 EST
Nmap scan report for 192.168.0.1
Host is up (0.00073s latency).
Not shown: 92 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 00:15:5D:EA:5B:4B (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 14.85 seconds
root@PLABKALI01:~# 
```

Figure 2.14 Screenshot of PLABKALI01: Showing the output of the nmap -F command.

## *Step 5*

Clear the screen by entering the following command:

```
clear
```

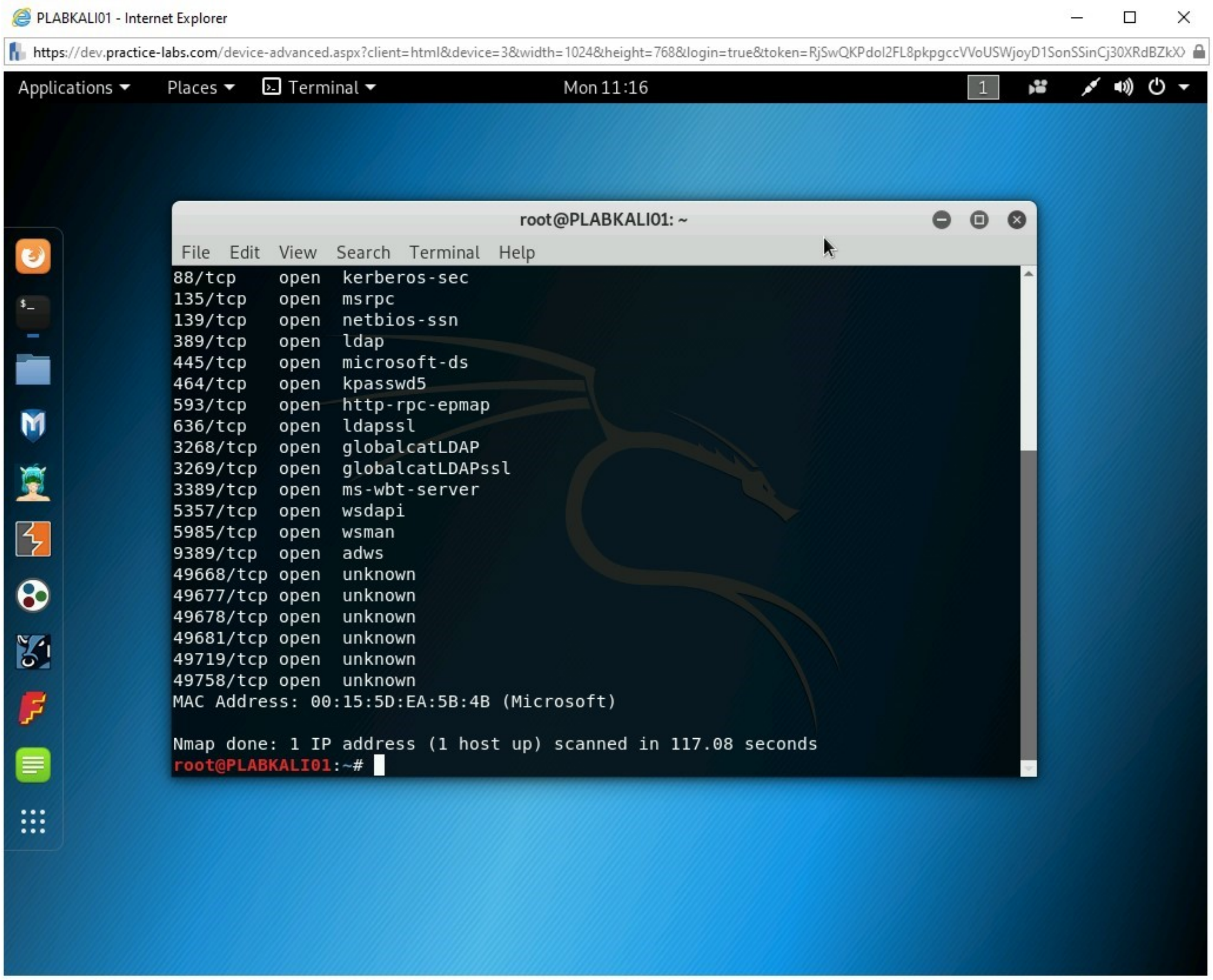
You will now scan for **65535** ports on a system. To do this, type the following command:

```
nmap -p- 192.168.0.1
```

Press **Enter**.

***Note**: This command will take a while to generate the output.*

The output of this command is displayed. Note that it took nearly two minutes to generate the output due to the number of ports being scanned. It found several ports open on the domain controller, which is 192.168.0.1.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:16
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
5985/tcp  open  wsman
9389/tcp  open  adws
49668/tcp open  unknown
49677/tcp open  unknown
49678/tcp open  unknown
49681/tcp open  unknown
49719/tcp open  unknown
49758/tcp open  unknown
MAC Address: 00:15:5D:EA:5B:4B (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 117.08 seconds
root@PLABKALI01:~#
```

Figure 2.15 Screenshot of PLABKALI01: Showing the output of the nmap -p- command.

## *Step 6*

Clear the screen by entering the following command:

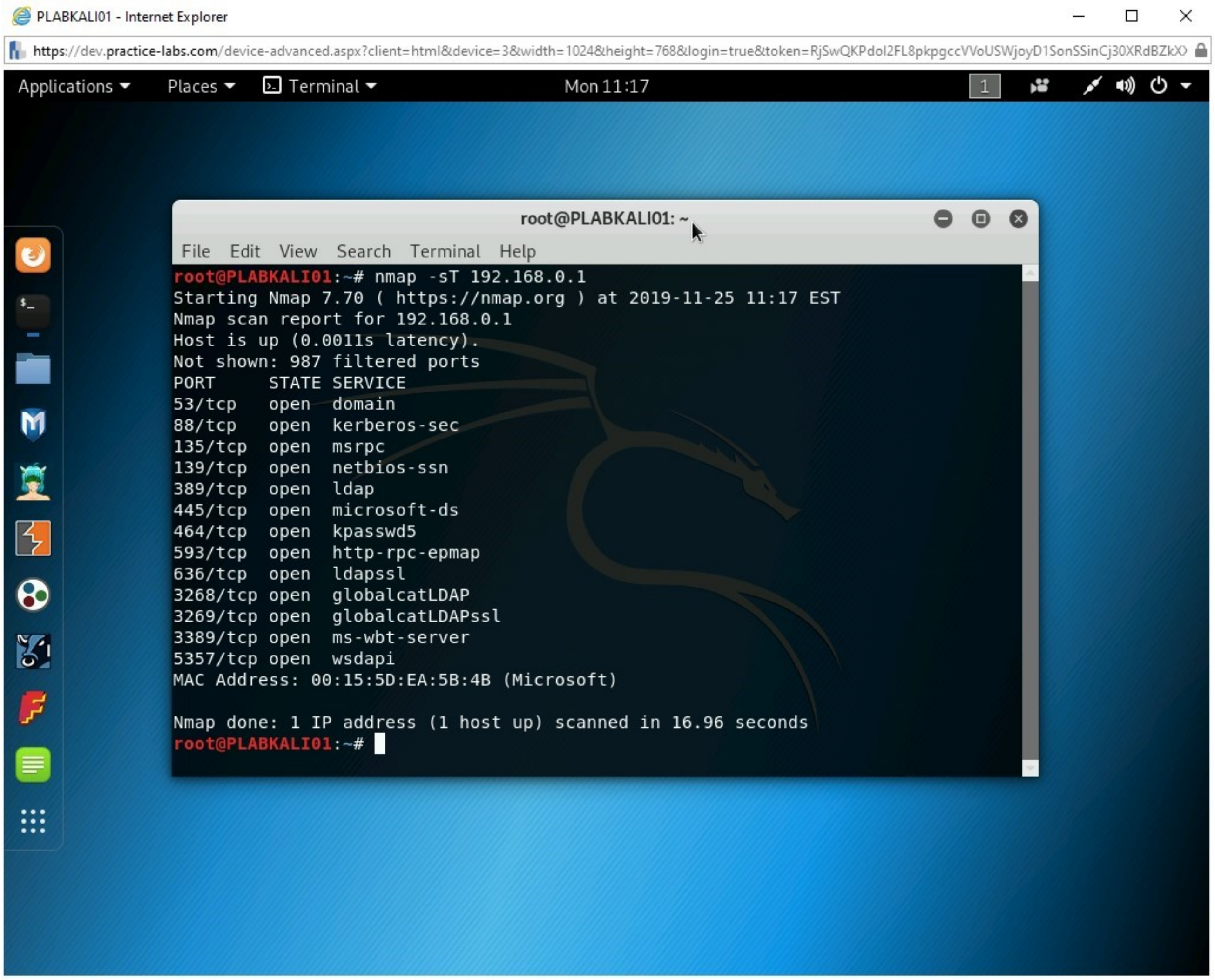
```
clear
```

Next, you will perform port scanning using **TCP** connect. Type the following command:

```
nmap -sT 192.168.0.1
```

Press **Enter**.

Notice the output. This command has scanned **1000** ports. There are **987** filtered and **13** open ports.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:17
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# nmap -sT 192.168.0.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:17 EST
Nmap scan report for 192.168.0.1
Host is up (0.0011s latency).
Not shown: 987 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 00:15:5D:EA:5B:4B (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 16.96 seconds
root@PLABKALI01:~#
```

Figure 2.16 Screenshot of PLABKALI01: Showing the output of the nmap -sT command.

## Step 7

Clear the screen by entering the following command:

```
clear
```

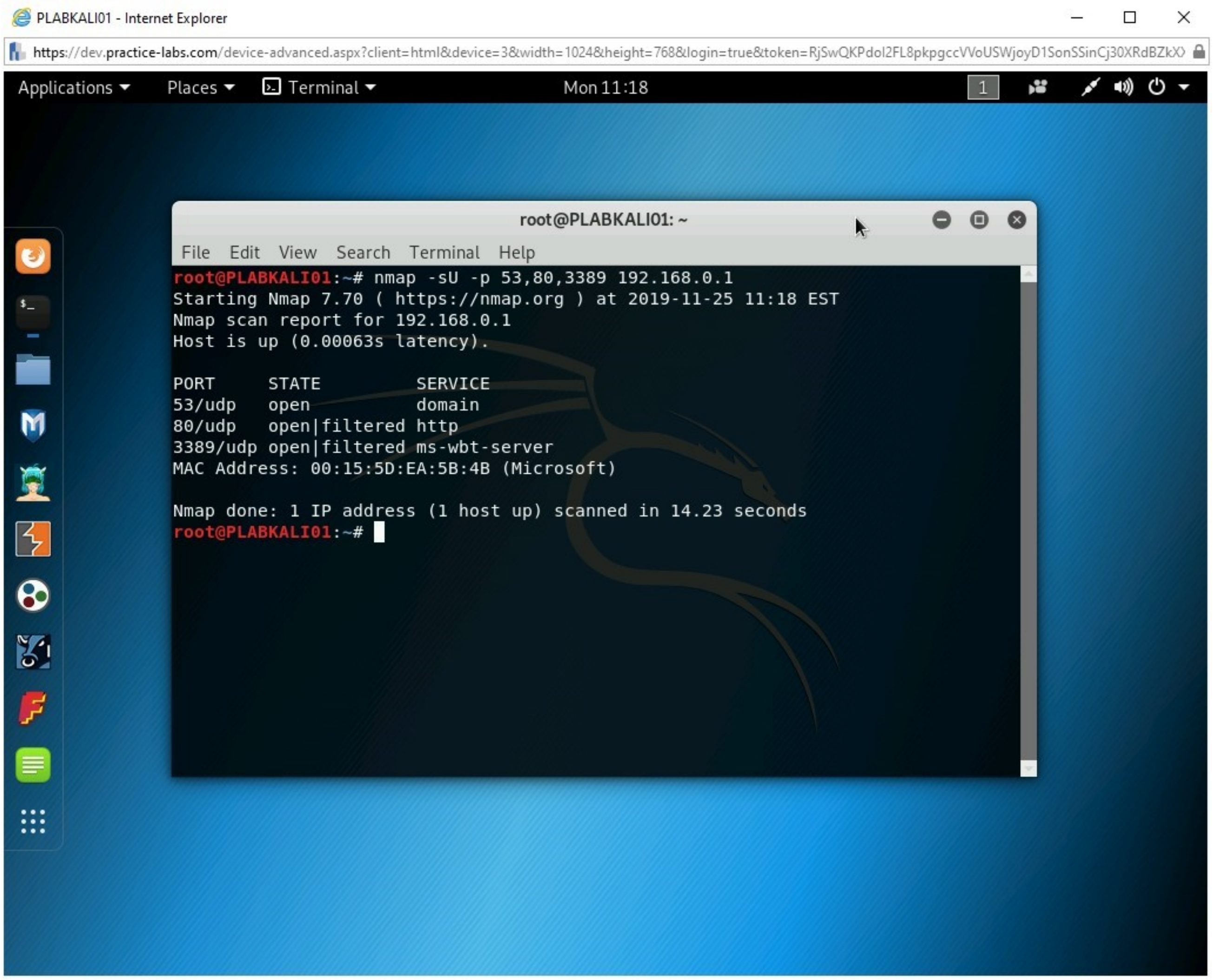
Let’s scan for the selective **UDP** ports only. Type the following command:

```
nmap -sU -p 53,80,3389 192.168.0.1
```

Press **Enter**.

> ***Note***: *Do not input a space after the comma when listing the ports. If you do, Nmap considers it to be the IP address and will attempt to find the route to the port number.*

The output of this command is displayed. Notice that only **NTP** port, **123**, is open. The remaining two ports are filtered.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:18
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# nmap -sU -p 53,80,3389 192.168.0.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:18 EST
Nmap scan report for 192.168.0.1
Host is up (0.00063s latency).

PORT     STATE         SERVICE
53/udp   open          domain
80/udp   open|filtered http
3389/udp open|filtered ms-wbt-server
MAC Address: 00:15:5D:EA:5B:4B (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 14.23 seconds
root@PLABKALI01:~#
```

Figure 2.17 Screenshot of PLABKALI01: Showing the output of the nmap -sU command.

## *Step 8*

Clear the screen by entering the following command:

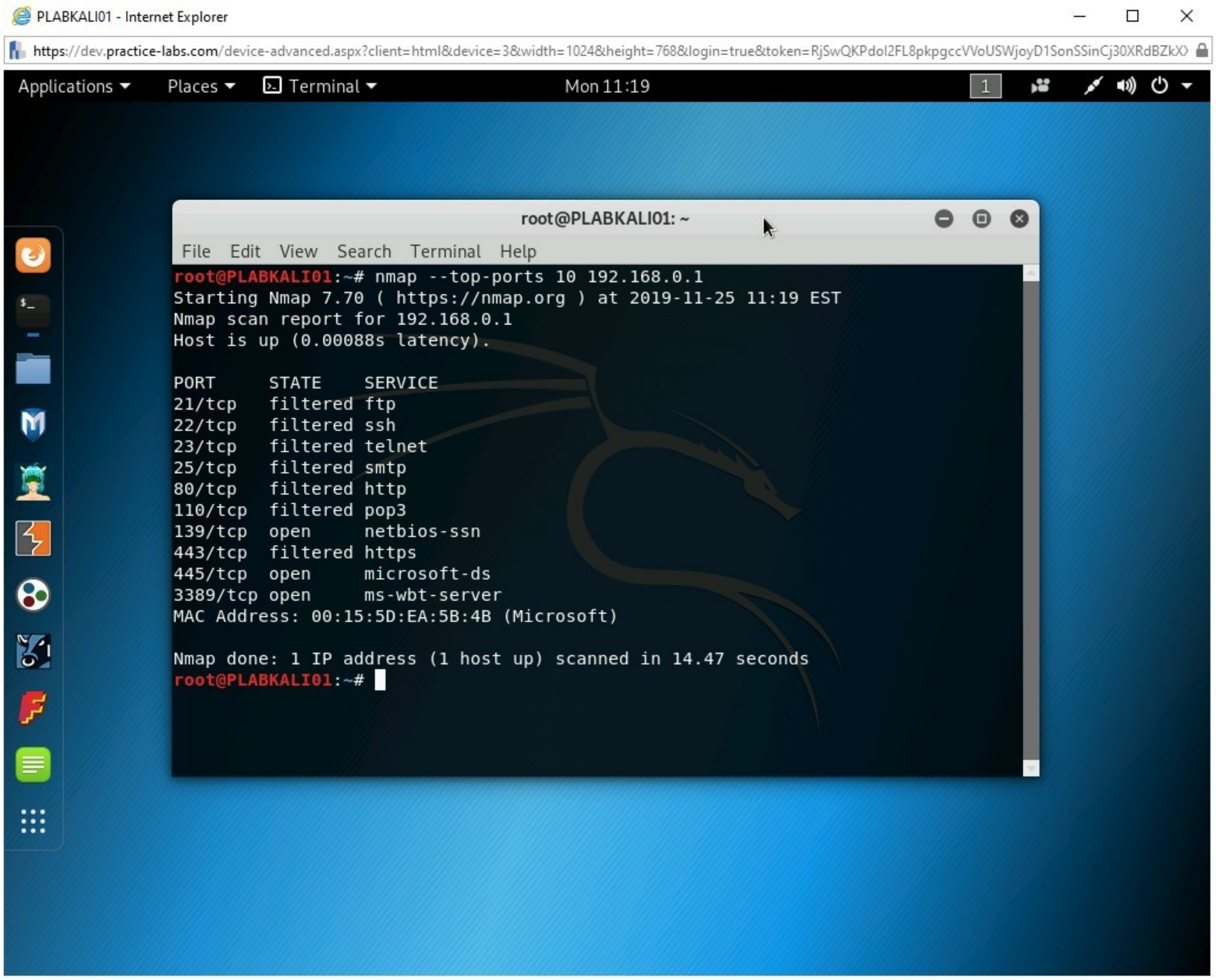
```
clear
```

You can also use the **--top-ports** parameter with a specified number to find ports. To do this, type the following command:

```
nmap --top-ports 10 192.168.0.1
```

Press **Enter**.

Notice that the top 10 used ports are listed as the output with their current state.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:19
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# nmap --top-ports 10 192.168.0.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:19 EST
Nmap scan report for 192.168.0.1
Host is up (0.00088s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   filtered http
110/tcp  filtered pop3
139/tcp  open     netbios-ssn
443/tcp  filtered https
445/tcp  open     microsoft-ds
3389/tcp open     ms-wbt-server
MAC Address: 00:15:5D:EA:5B:4B (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 14.47 seconds
root@PLABKALI01:~#
```

Figure 2.18 Screenshot of PLABKALI01: Showing the output of the nmap -top-ports command.

**Alert**: Keep the terminal window open.

## Task 4 - Fingerprint an Operating System

Operating system fingerprinting is also known as banner grabbing. With the help of fingerprinting, you can determine the type of operating system and its version on a remote system. There are primarily two types of fingerprinting:

**Active**

Nmap contains a list of operating systems. When you execute a command to determine the operating system of a remote host, packets are sent to the remote host, and the response is received, which is compared with the list of operating systems. Nmap then provides the closest match.

Here are some nmap commands for OS fingerprinting:

To fingerprint a remote system, type the following command:

```
nmap -O 192.168.0.3
```

The **-O** parameter provides more options for operating system detection. You can choose to skip the hosts that are not up and running and scan for the operating system only on the live hosts.

To do this, type the following command:

```
nmap -O --osscan-limit 192.168.0.0/24
```

You can also use **--osscan-guess** option with the **-O** parameter. It will attempt to detect the operating system. If it is not able to do so, then it will provide the closest signature possible. It performs an aggressive detection of the operating system.

To do this, type the following command:

```
nmap -O --osscan-guess 192.168.0.3
```

When you perform an operating system scan, Nmap, by default, attempts five times to detect the name and version. However, to speed up the process, you can limit the number of attempts.

To do this, type the following command:

```
nmap -O --max-os-tries 2 192.168.0.5
```

You can also use the **-A** parameter with the nmap command to perform fingerprinting.

To do this, type the following command:

```
nmap -A 192.168.0.6
```

**Passive**

Passive fingerprinting can be performed in different ways. For example, you can get a lot of details from the error messages, which can contain information, such as the type of operating system and server. Sniffing network traffic can also be helpful in determining the operating system.

To fingerprint a system, perform the following steps:

## *Step 1*

Ensure that you are connected to **PLABKALI01**, and the terminal window is open.

Clear the screen by entering the following command:

```
clear
```

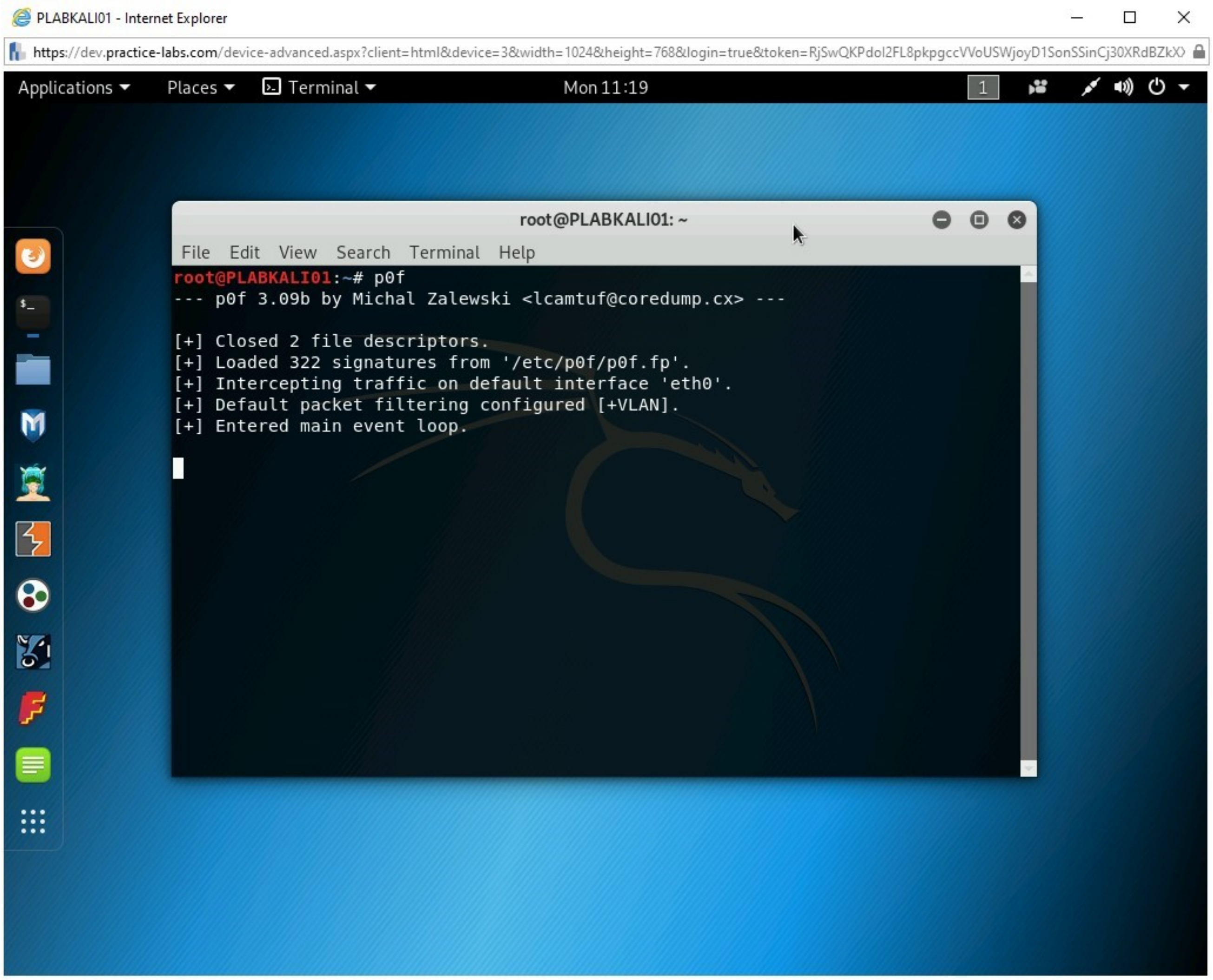
Other than Nmap, you can also use another tool named **p0f** for operating system fingerprinting. It is a good tool to find out the operating system of a Website. To use the p0f tool, type the following command:

```
p0f
```

Press **Enter**.

***Note***: *You can use the p0f command with the -i <interface_name> to use a specific interface on your system. For example, you can use eth0 -i eth0.*

Notice that the **p0f** tool has started but is not currently doing anything. It has 322 signatures that are kept in the **/etc/p0f/p0f.fp** file. It also mentions that it is using the eth0 interface.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:19
root@PLABKALI01: ~
File Edit View Search Terminal Help

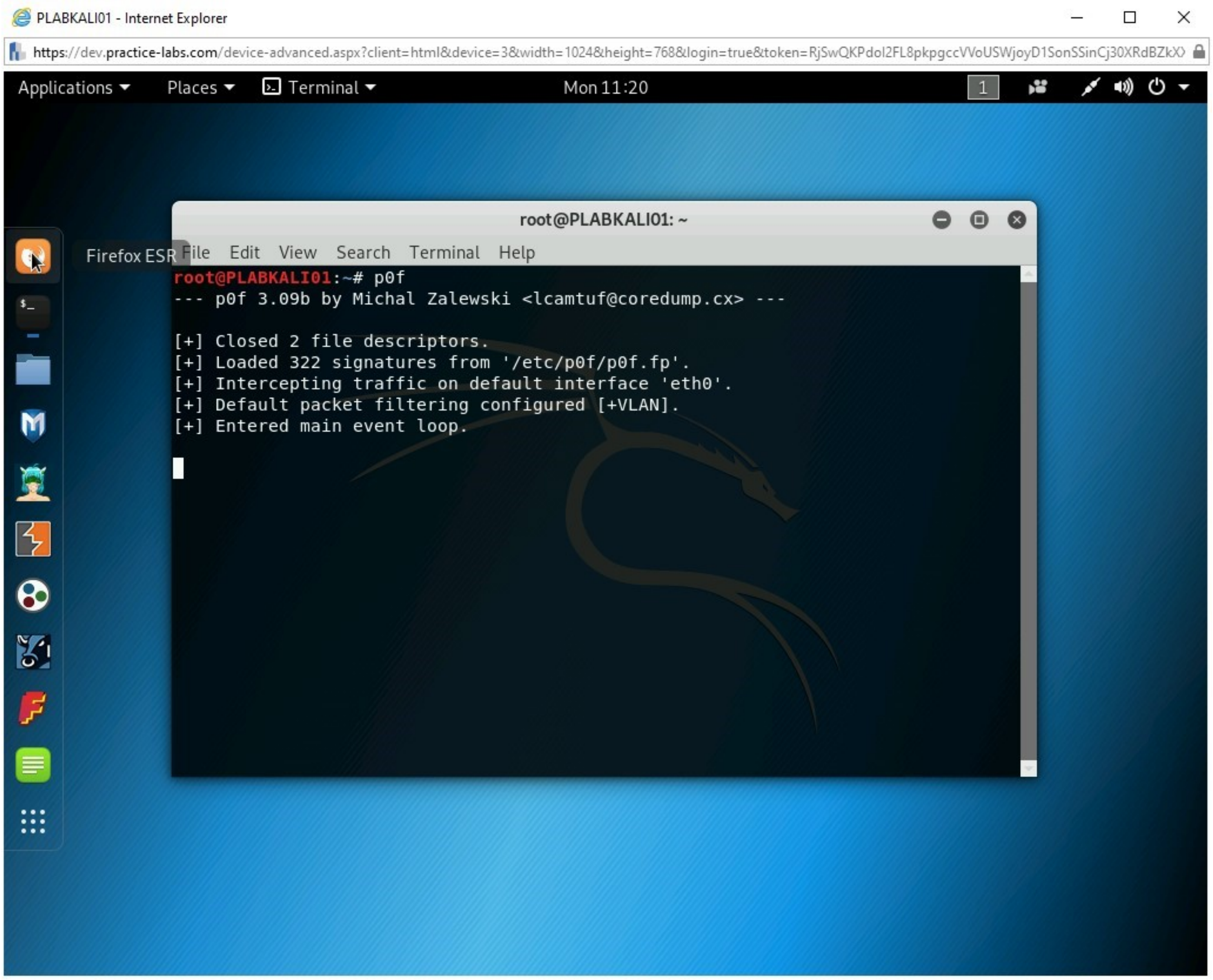
```
root@PLABKALI01:~# p0f
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 2 file descriptors.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on default interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Entered main event loop.
```

Figure 2.19 Screenshot of PLABKALI01: Showing the start of the p0f command.

## *Step 2*

Next, you need to open a Website. Let’s open Firefox from the left pane.

Click the **Firefox ESR** icon.

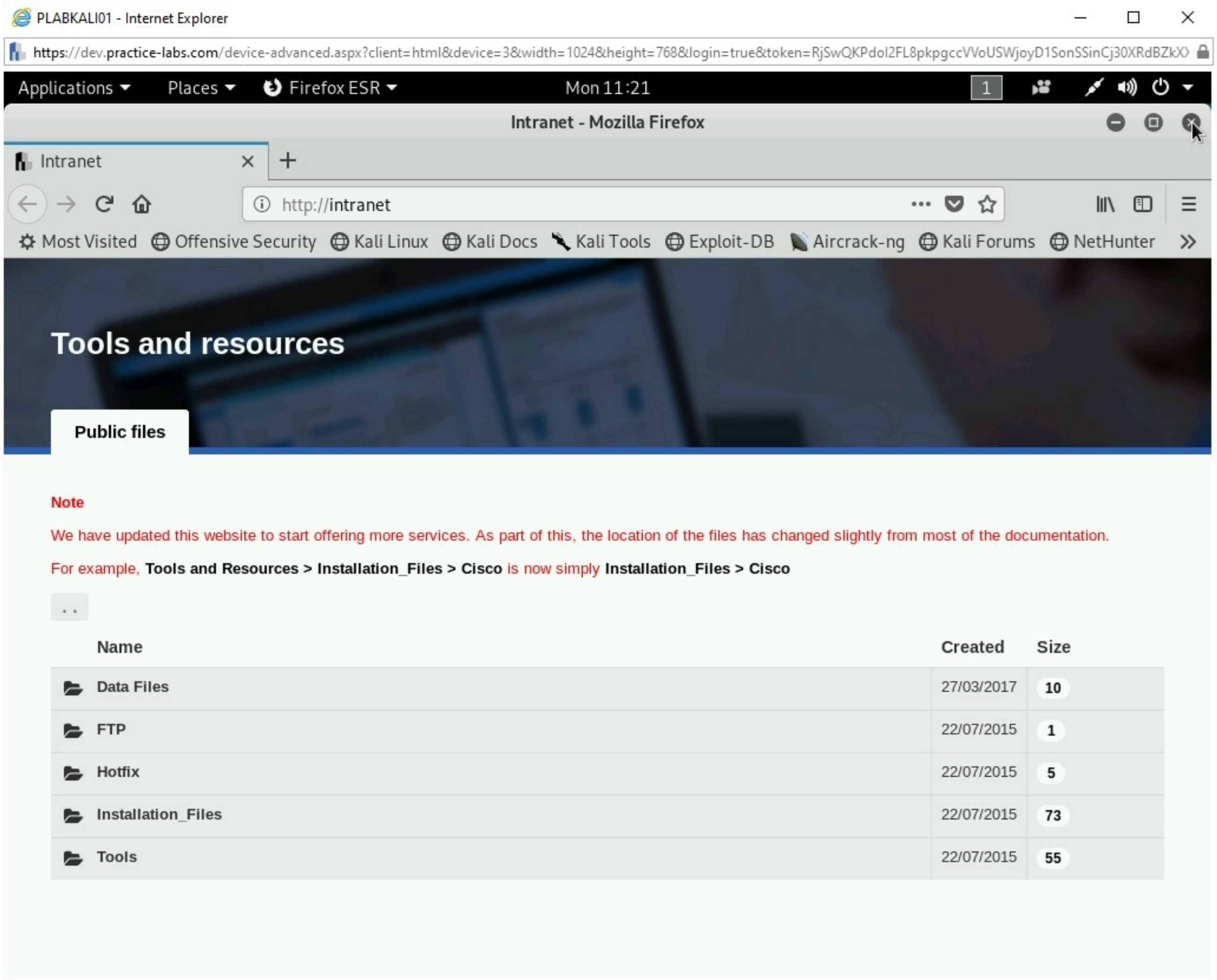

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:20
root@PLABKALI01: ~
Firefox ESR
File Edit View Search Terminal Help

```
root@PLABKALI01:~# p0f
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 2 file descriptors.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on default interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Entered main event loop.
```

Figure 2.20 Screenshot of PLABKALI01: Clicking the Firefox icon in the left pane on the desktop.

Notice that the default intranet Website is loaded.

Close the **Firefox** window.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Firefox ESR
Mon 11:21
Intranet - Mozilla Firefox
Intranet
http://intranet
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Tools and resources
Public files

Note

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

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

..

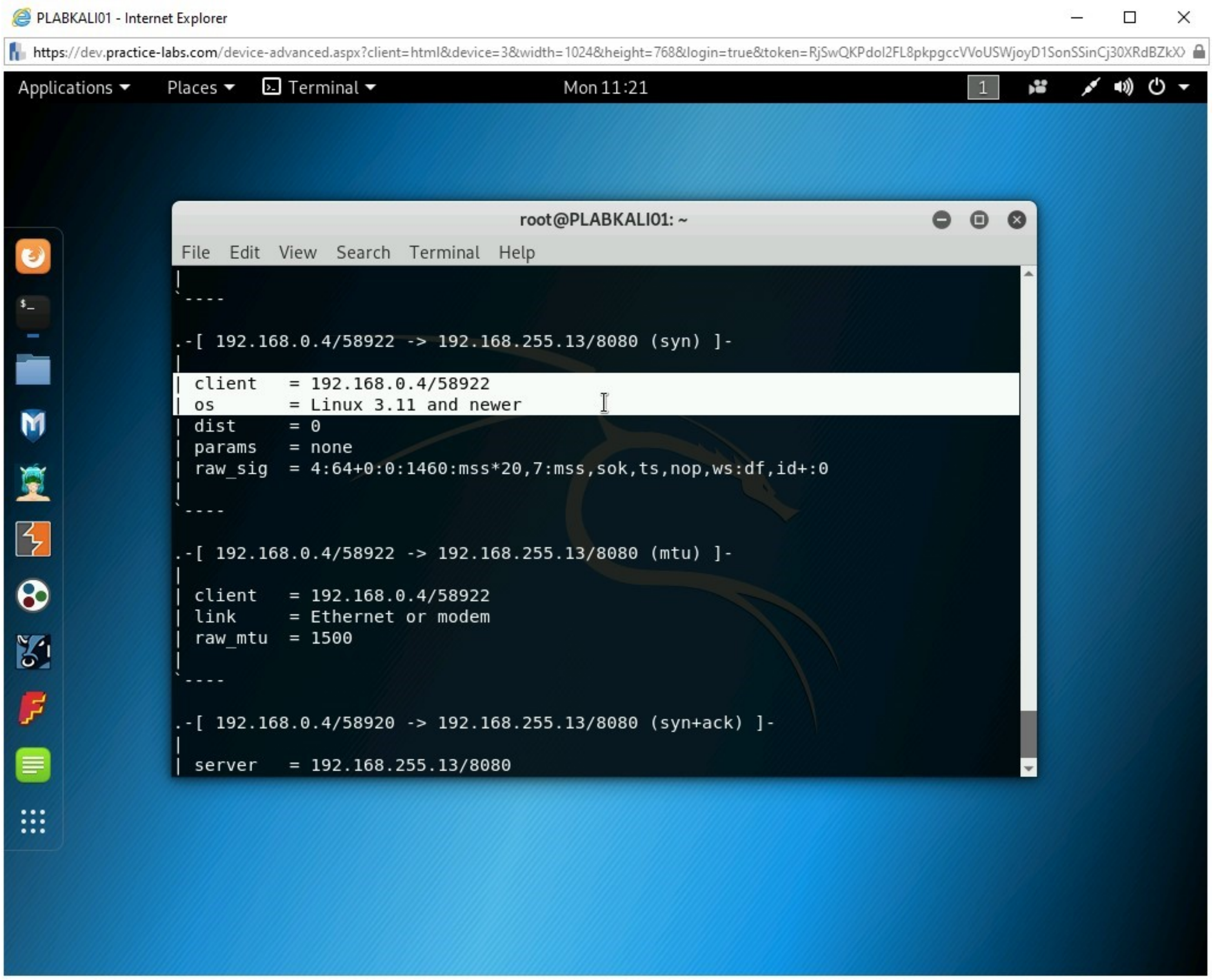
| Name | Created | Size |
|---|---|---|
| Data Files | 27/03/2017 | 10 |
| FTP | 22/07/2015 | 1 |
| Hotfix | 22/07/2015 | 5 |
| Installation_Files | 22/07/2015 | 73 |
| Tools | 22/07/2015 | 55 |

Figure 2.21 Screenshot of PLABKALI01: Showing the Intranet Webpage.

## *Step 3*

**p0f** has started to capture a lot of data. Press **Ctrl + C** to stop the p0f tool.

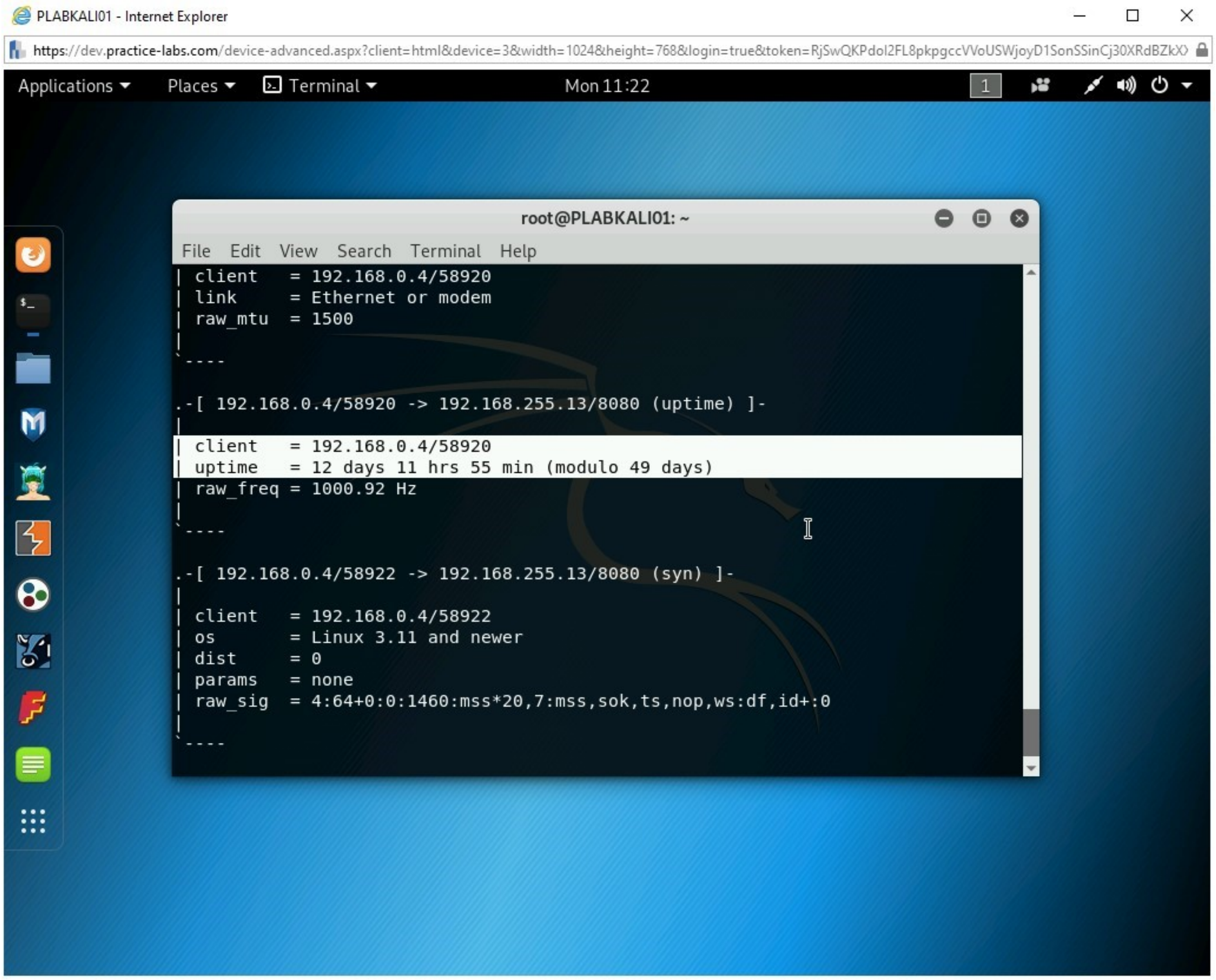
It has discovered that the operating system is Linux.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:21
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
|
`----

.-[ 192.168.0.4/58922 -> 192.168.255.13/8080 (syn) ]-
|
| client   = 192.168.0.4/58922
| os       = Linux 3.11 and newer
| dist     = 0
| params   = none
| raw_sig  = 4:64+0:0:1460:mss*20,7:mss,sok,ts,nop,ws:df,id+:0
|
`----

.-[ 192.168.0.4/58922 -> 192.168.255.13/8080 (mtu) ]-
|
| client   = 192.168.0.4/58922
| link     = Ethernet or modem
| raw_mtu  = 1500
|
`----

.-[ 192.168.0.4/58920 -> 192.168.255.13/8080 (syn+ack) ]-
|
| server   = 192.168.255.13/8080
```

Figure 2.22 Screenshot of PLABKALI01: Stopping the p0f command.

Scroll up and notice that it has also determined the uptime for the Webserver.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:22
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
| client   = 192.168.0.4/58920
| link     = Ethernet or modem
| raw_mtu  = 1500
|
`----

.-[ 192.168.0.4/58920 -> 192.168.255.13/8080 (uptime) ]-
|
| client   = 192.168.0.4/58920
| uptime   = 12 days 11 hrs 55 min (modulo 49 days)
| raw_freq = 1000.92 Hz
|
`----

.-[ 192.168.0.4/58922 -> 192.168.255.13/8080 (syn) ]-
|
| client   = 192.168.0.4/58922
| os       = Linux 3.11 and newer
| dist     = 0
| params   = none
| raw_sig  = 4:64+0:0:1460:mss*20,7:mss,sok,ts,nop,ws:df,id+:0
|
`----
```

Figure 2.23 Screenshot of PLABKALI01: Showing the captured output of the p0f command.

**Note**: Keep the terminal window open.

## Task 5 - Perform Service Probing

Using Nmap, you can find a lot of details about the running services and their version numbers. In this task, you will learn about service probing.

To do this, perform the following steps:

## *Step 1*

Ensure that you are connected to **PLABKALI01**, and the terminal window is open.

Clear the screen by entering the following command:

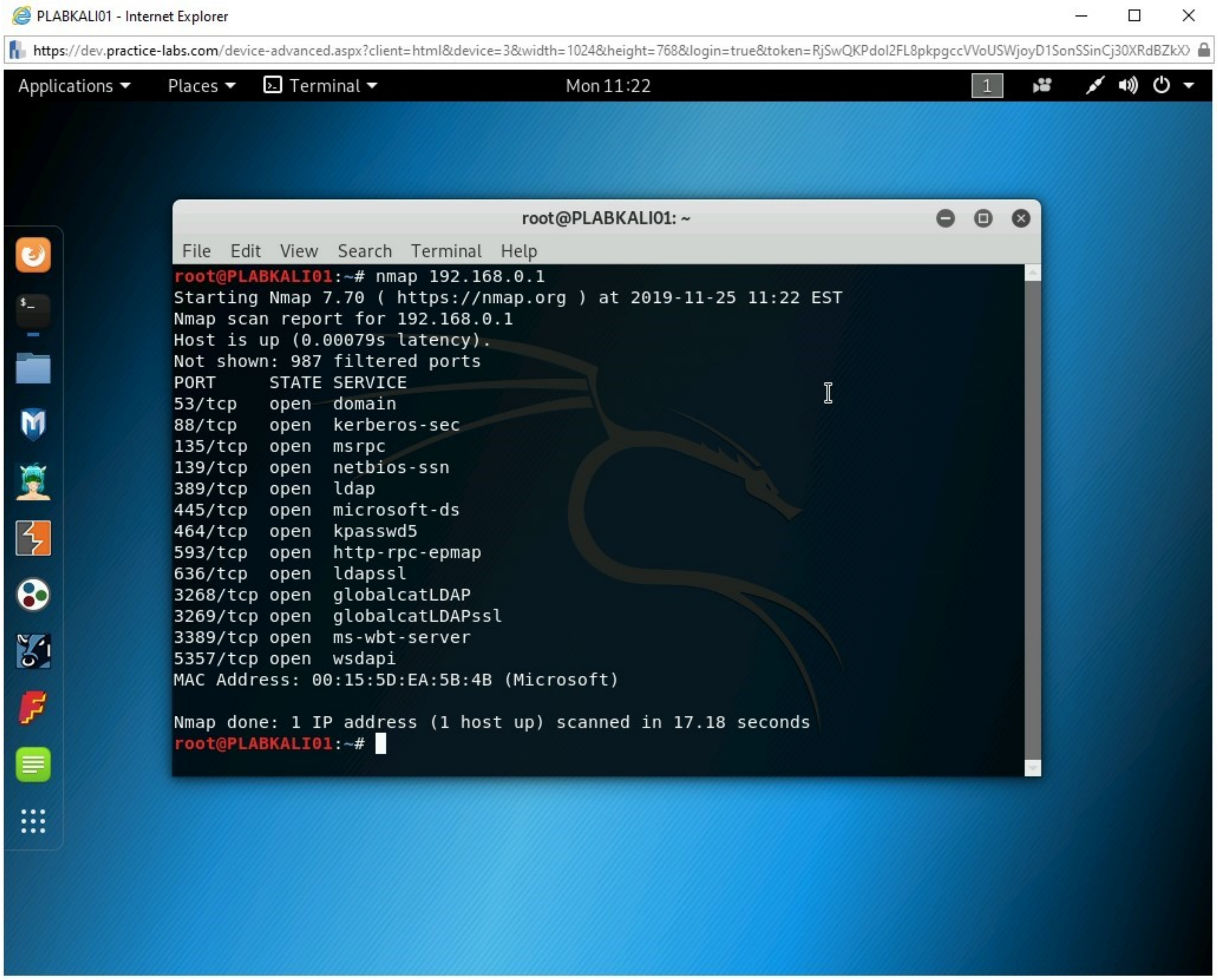
```
clear
```

To check the ports open on a system, enter the following command:

```
nmap 192.168.0.1
```

Press **Enter**.

Notice the output that displays several open ports on **192.168.0.1**.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:22
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# nmap 192.168.0.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:22 EST
Nmap scan report for 192.168.0.1
Host is up (0.00079s latency).
Not shown: 987 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 00:15:5D:EA:5B:4B (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 17.18 seconds
root@PLABKALI01:~# 
```

Figure 2.24 Screenshot of PLABKALI01: Showing the output of the nmap command.

## Step 2

Clear the screen by entering the following command:

```
clear
```

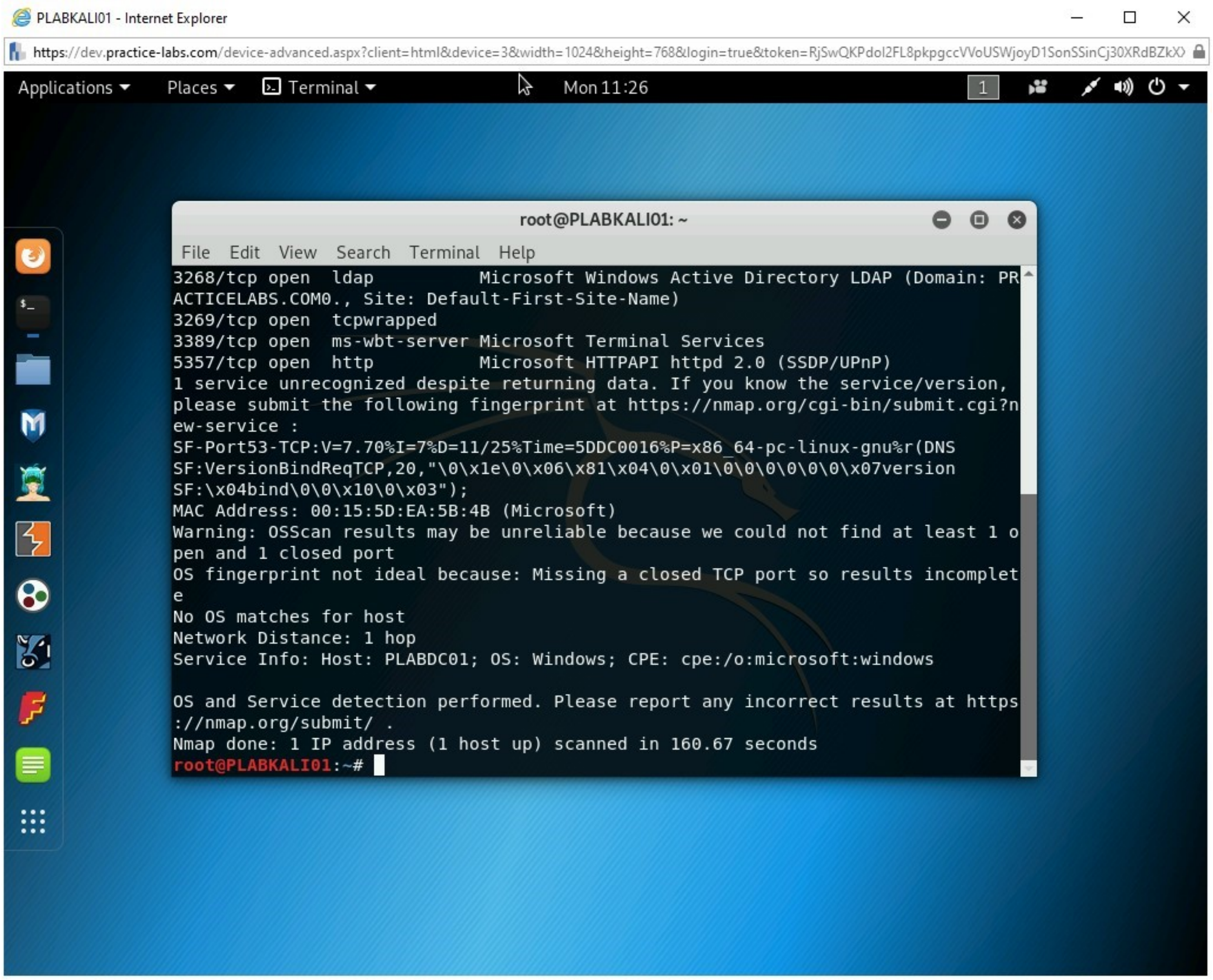
Next, let’s check the version of the services on the open ports on **192.168.0.1**.

Type the following command:

```
nmap -sV -O 192.168.0.1
```

Press **Enter**.

The output displays the version number of most of the services.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:26
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: PR
ACTICELABS.COM0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port53-TCP:V=7.70%I=7%D=11/25%Time=5DDC0016%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version
SF:\x04bind\0\0\x10\0\x03");
MAC Address: 00:15:5D:EA:5B:4B (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplet
e
No OS matches for host
Network Distance: 1 hop
Service Info: Host: PLABDC01; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 160.67 seconds
root@PLABKALI01:~#
```

Figure 2.25 Screenshot of PLABKALI01: Showing the output of the nmap -V command.

Close the **terminal** window.

# Exercise 3 - Conducting Passive Reconnaissance in a Network

Information gathering is critical in ethical hacking. Without gathering information, the attackers may not know exactly what to target and what strategies to use.

The attackers normally use open-source intelligence (OSINT) to obtain information that is available publicly.

Various places may contain useful information:

- Whois database
- Target's Website
- Perform Social Network scraping
- Google search results
- DNS information
- Review blogs, public forums, and Websites
- Search breach databases about the target
- Search DarkWeb about the target

A tool, such as Maltego, helps you with detailed footprinting information about a Website.

In this exercise, you will learn about passive reconnaissance for vulnerabilities in a network.

# Learning Outcomes

After completing this exercise, you will be able to:

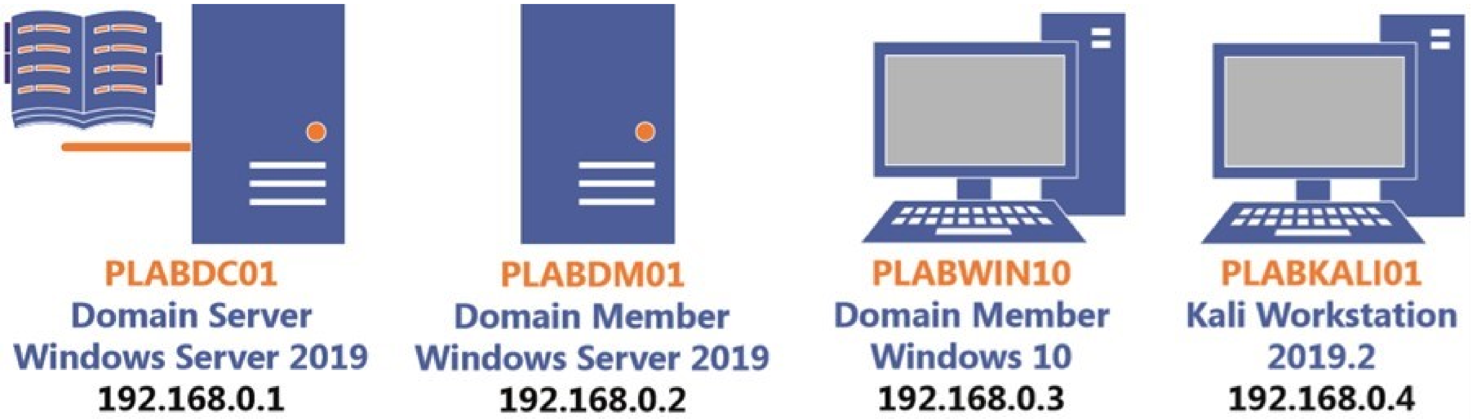
- Use the WHOis Website
- Perform Social Media Exploitation
- Use SHODAN
- Use Google Hacking Database
- Perform DNS Querying
- Use theHarvester
- Create a Temporary E-mail Account
- Use Maltego
- Use the AnyWho Website

# Your Devices

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

- **PLABDC01 -** (Windows Server 2019 - Domain Server)
- **PLABDM01 -** (Windows Server 2019 - Domain Member

- **PLABWIN10 -** (Windows 10 - Workstation)
- **PLABKALI01 -** (Kali 2019.2 - Linux Kali Workstation)



## Task 1 - Use the WHOis Website

The WHOis Website returns information about a domain name. For example, if you enter a domain name, such as practice-labs.com, WHOis will return the name and address of the domain's owner, which in this case, is Practice Labs. You can also use the whois command in Kali Linux.

Using this command, you can find out information about a domain, such as:

- Registrar
- Server name
- WHOis Server
- Referral URL
- IP address range

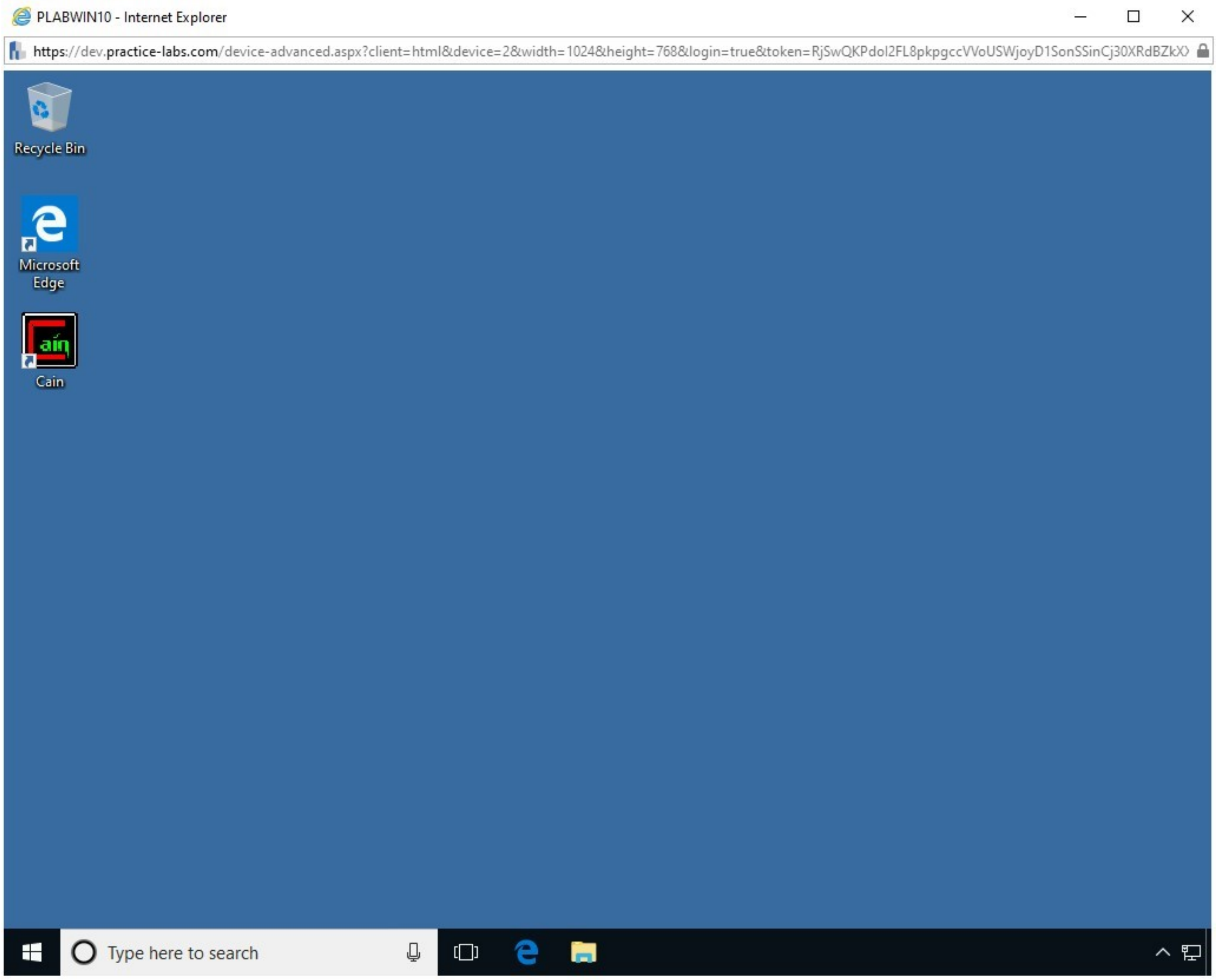
You can find out a lot of information about a particular domain. This information can be further used in attacking a particular domain or a server.

> ***Important:*** *This is a live Website. Therefore, the search results may vary.*

To use the WHOis Website, perform the following steps:

## *Step 1*

Ensure you have powered on all the devices listed in the introduction and connect to **PLABWIN10**.


PLABWIN10 - Internet Explorer

https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX

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

## *Step 2*

From the taskbar, click the **Microsoft Edge** icon.

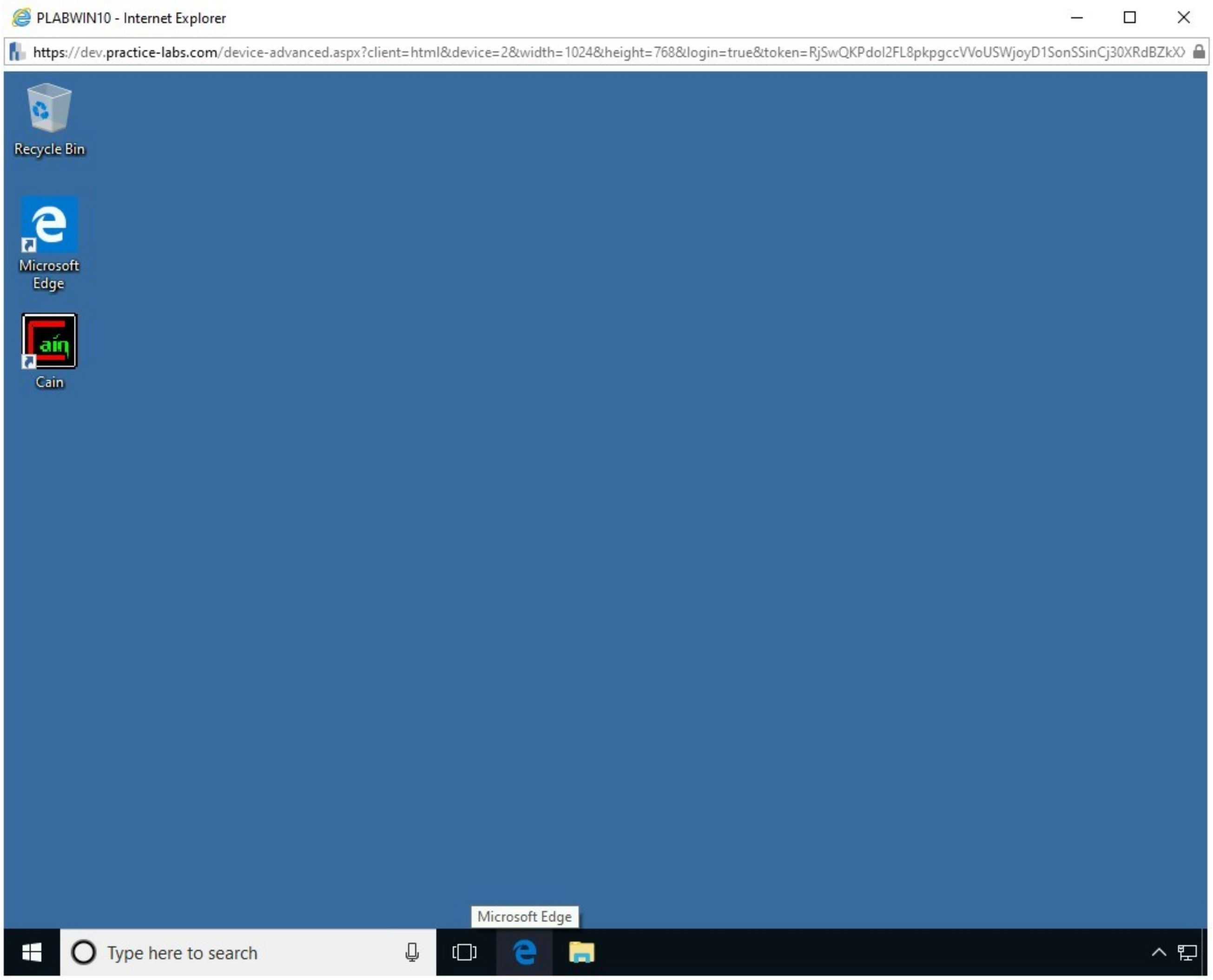
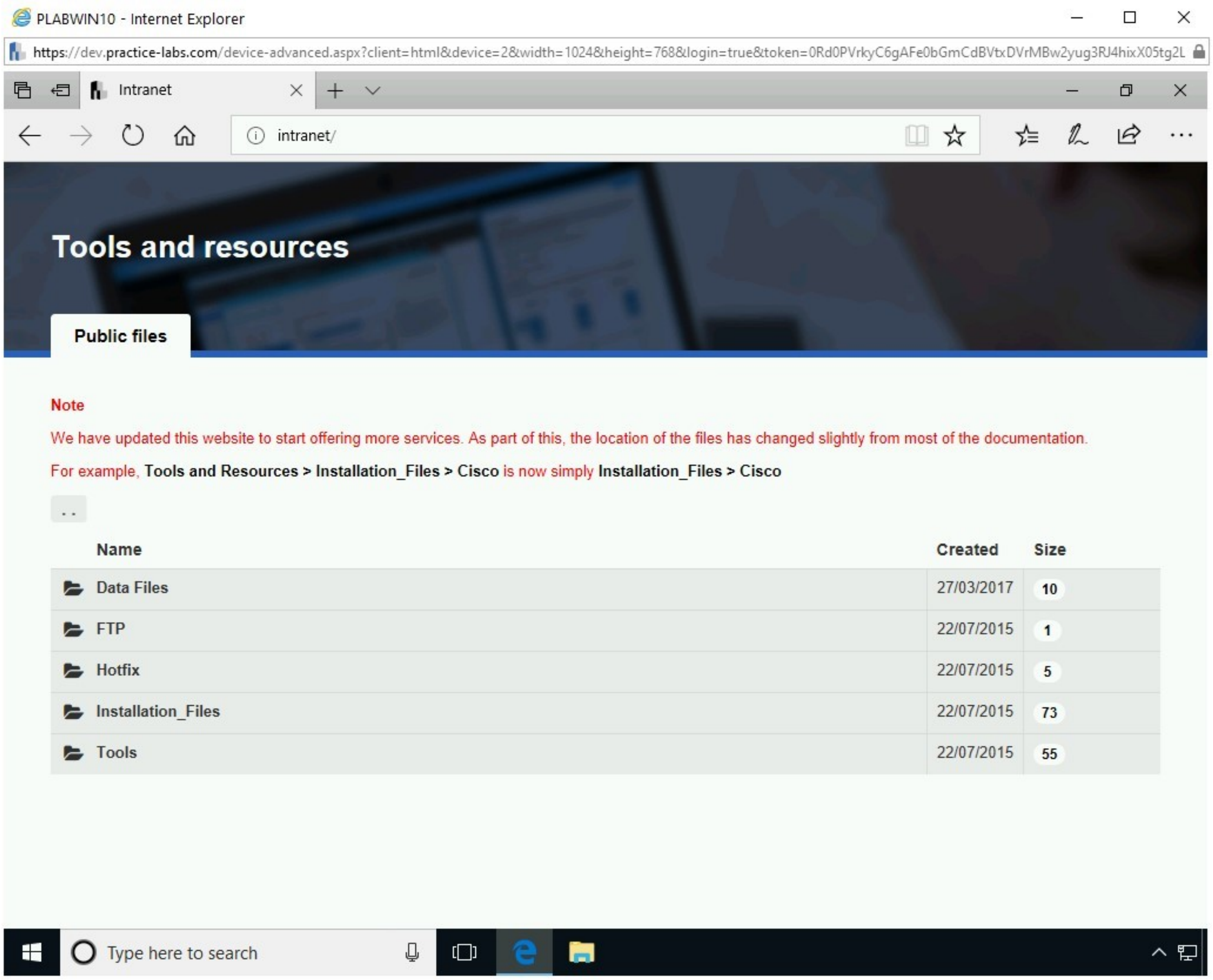

PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX)
Recycle Bin
Microsoft Edge
Cain
Microsoft Edge
Type here to search

Figure 3.2 Screenshot of PLABWIN10: Opening Microsoft Edge from the Taskbar.

## *Step 3*

The **Microsoft Edge** window is displayed. In the **Microsoft Edge** window, the default homepage, which is the **Practice Labs Intranet**, is displayed.


PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=0Rd0PVrkyC6gAFe0bGmCdBVtxDVrMBw2yug3RJ4hixX05tg2L
Intranet
intranet/
Tools and resources
Public files
Type here to search

Note

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

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

. .

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

Figure 3.3 Screenshot of PLABWIN10: Showing the default home page of the intranet Website.

## *Step 4*

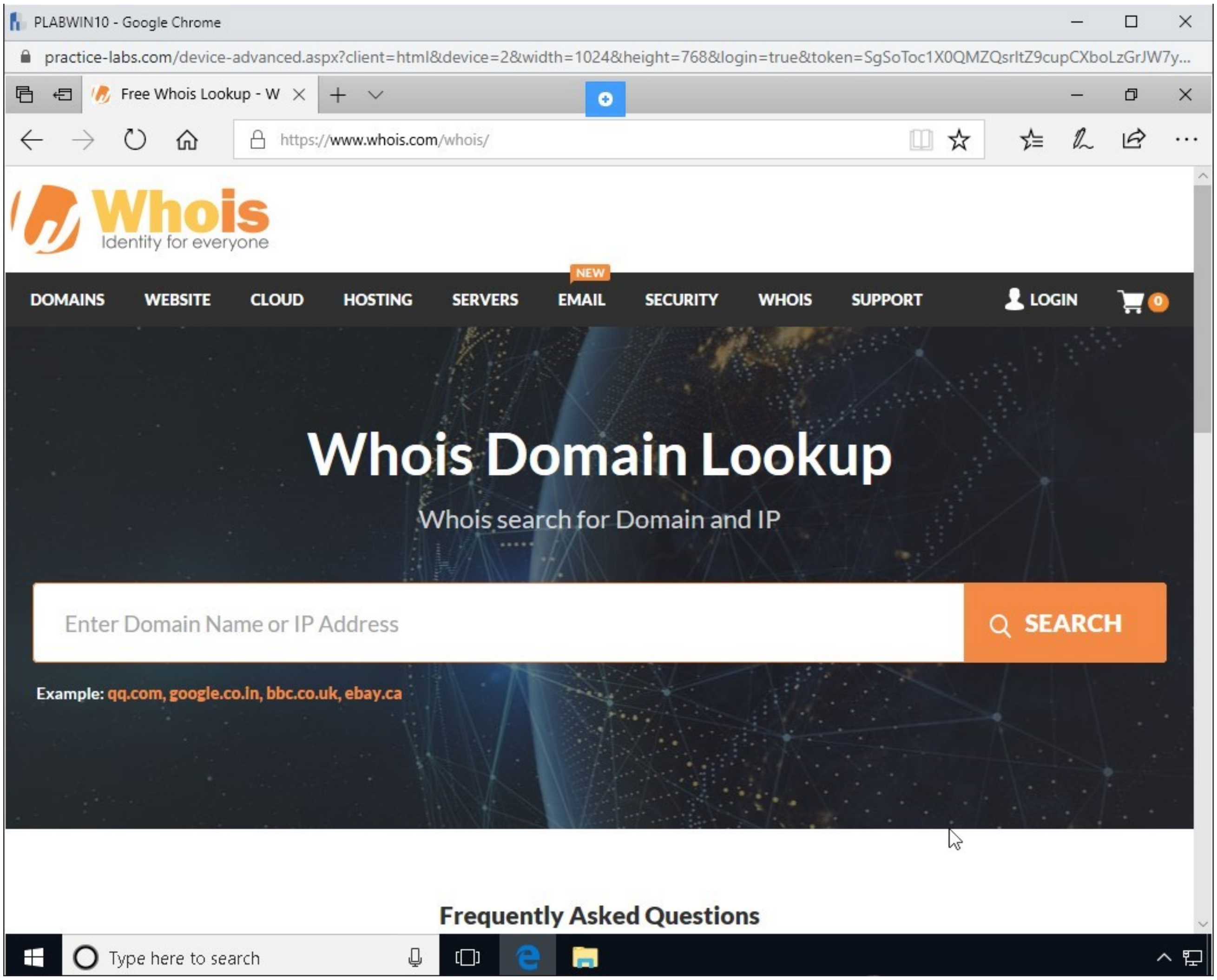
In the address bar, type the following URL:

```
https://whois.com/whois/
```

Press **Enter**.

The **Whois.com** Website is displayed.

***Note:*** *Even if you enter http, it will automatically convert to https. Also, you can also get the domain information from the https://whois.icann.org/en Website.*



PLABWIN10 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=SgSoToc1X0QMZQsrltZ9cupCXboLzGrJW7y...
Free Whois Lookup - W
https://www.whois.com/whois/
Whois
Identity for everyone
DOMAINS
WEBSITE
CLOUD
HOSTING
SERVERS
NEW
EMAIL
SECURITY
WHOIS
SUPPORT
LOGIN
0
Whois Domain Lookup
Whois search for Domain and IP
Enter Domain Name or IP Address
SEARCH
Example: qq.com, google.co.in, bbc.co.uk, ebay.ca
Frequently Asked Questions
Type here to search

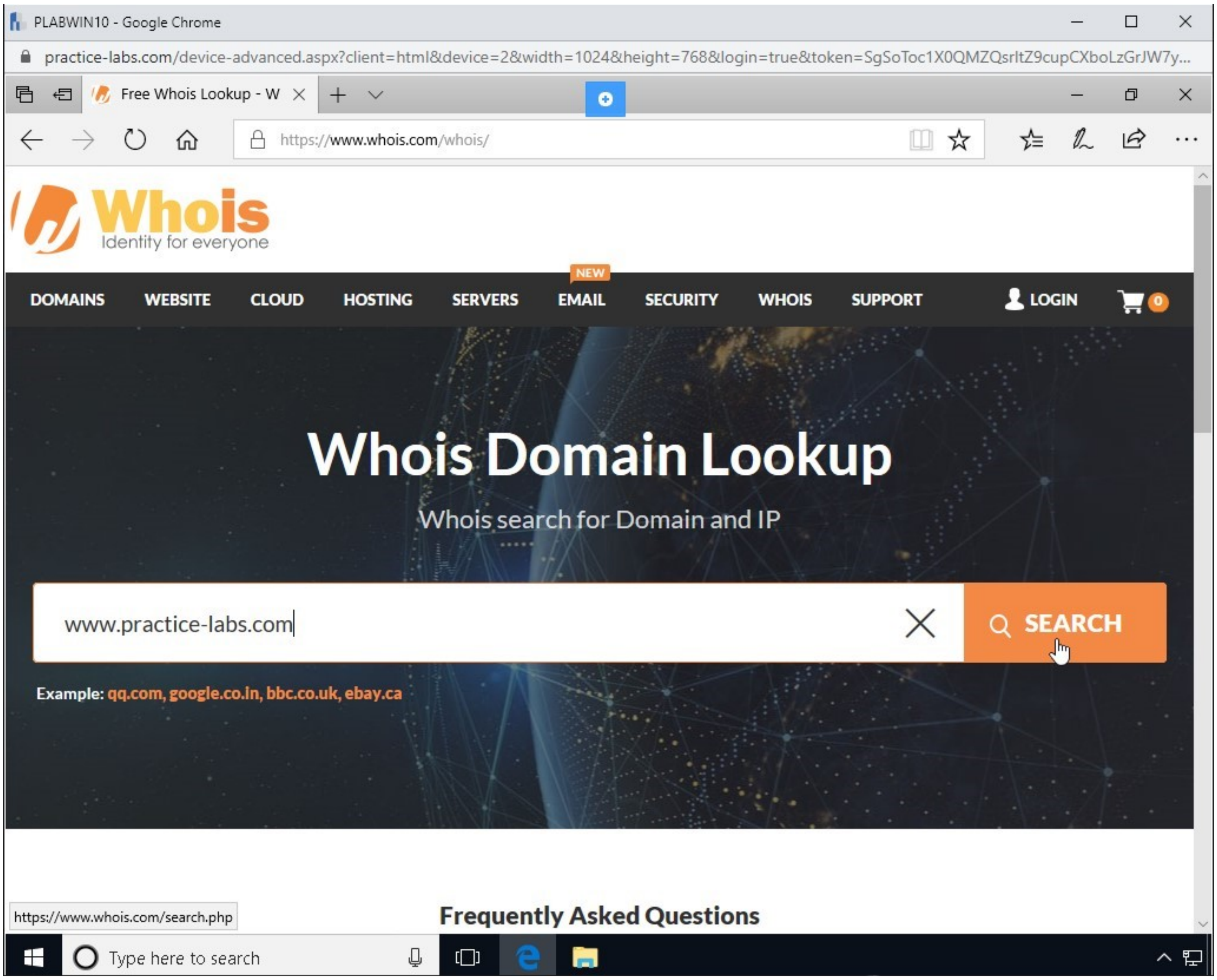
Figure 3.4 Screenshot of PLABWIN10: Showing the loaded Website, whois.com.

## Step 5

In the search bar, type the following URL:

```
www.practice-labs.com
```

Press **Enter** or click on the magnifying glass icon.


PLABWIN10 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=SgSoToc1X0QMZQsrltZ9cupCXboLzGrJW7y...
Free Whois Lookup - W
https://www.whois.com/whois/
Whois
Identity for everyone
DOMAINS
WEBSITE
CLOUD
HOSTING
SERVERS
NEW
EMAIL
SECURITY
WHOIS
SUPPORT
LOGIN
0
Whois Domain Lookup
Whois search for Domain and IP
SEARCH
Example: qq.com, google.co.in, bbc.co.uk, ebay.ca
https://www.whois.com/search.php
Frequently Asked Questions
Type here to search

www.practice-labs.com

Figure 3.5 Screenshot of PLABWIN10: Typing the domain name in the search text box and press Enter.

## *Step 6*

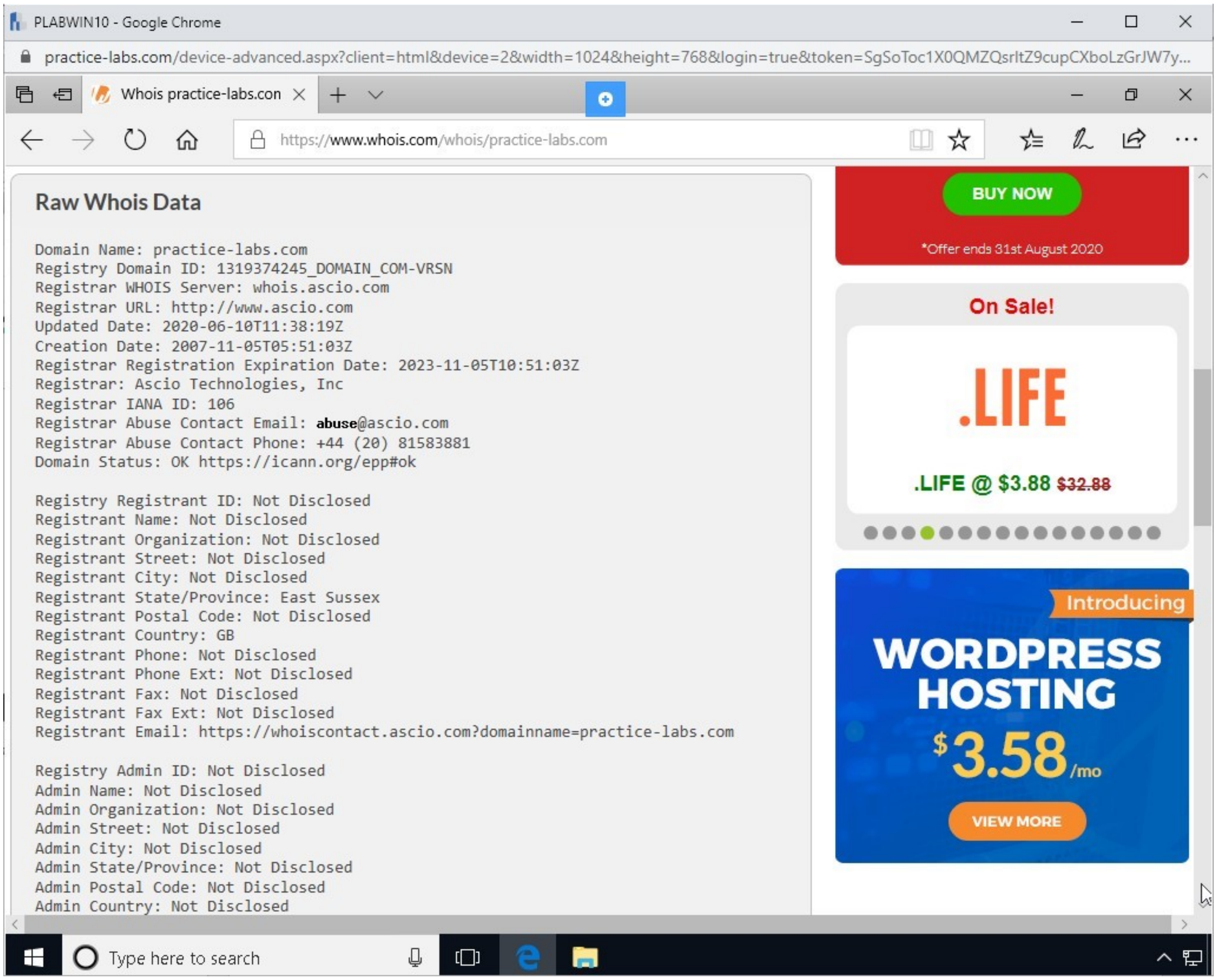
The results are displayed.

Scroll down to the **Raw Whois Data.**

Notice in the results throughout the entire page, several key points about the Website are displayed. Some of the key ones are:

- Domain name
- Registrar
- Whois server

- Referral URL
- Creation, Updated, and Expiration Date


PLABWIN10 - Google Chrome
practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=SgSoToc1X0QMZQsrltZ9cupCXboLzGrJW7y...
Whois practice-labs.con
https://www.whois.com/whois/practice-labs.com
BUY NOW
*Offer ends 31st August 2020
On Sale!
.LIFE
.LIFE @ $3.88 $32.88
Introducing
WORDPRESS HOSTING
$3.58/mo
VIEW MORE
Type here to search

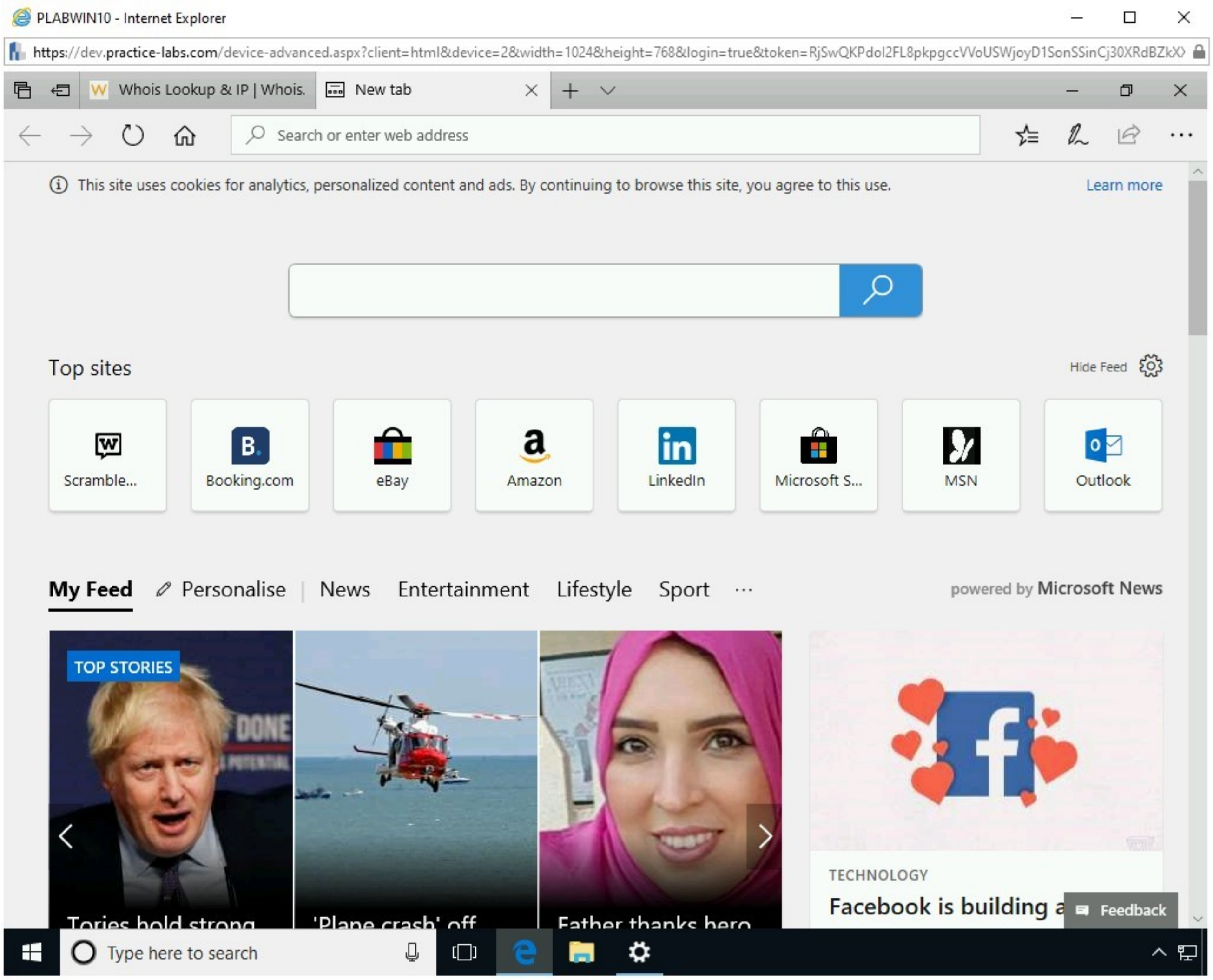
Raw Whois Data

```
Domain Name: practice-labs.com
Registry Domain ID: 1319374245_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.ascio.com
Registrar URL: http://www.ascio.com
Updated Date: 2020-06-10T11:38:19Z
Creation Date: 2007-11-05T05:51:03Z
Registrar Registration Expiration Date: 2023-11-05T10:51:03Z
Registrar: Ascio Technologies, Inc
Registrar IANA ID: 106
Registrar Abuse Contact Email: abuse@ascio.com
Registrar Abuse Contact Phone: +44 (20) 81583881
Domain Status: OK https://icann.org/epp#ok

Registry Registrant ID: Not Disclosed
Registrant Name: Not Disclosed
Registrant Organization: Not Disclosed
Registrant Street: Not Disclosed
Registrant City: Not Disclosed
Registrant State/Province: East Sussex
Registrant Postal Code: Not Disclosed
Registrant Country: GB
Registrant Phone: Not Disclosed
Registrant Phone Ext: Not Disclosed
Registrant Fax: Not Disclosed
Registrant Fax Ext: Not Disclosed
Registrant Email: https://whoiscontact.ascio.com?domainname=practice-labs.com

Registry Admin ID: Not Disclosed
Admin Name: Not Disclosed
Admin Organization: Not Disclosed
Admin Street: Not Disclosed
Admin City: Not Disclosed
Admin State/Province: Not Disclosed
Admin Postal Code: Not Disclosed
Admin Country: Not Disclosed
```

Figure 3.6 Screenshot of PLABWIN10: Showing the information regarding the Website that was searched.

## Step 7

Open another tab in **Microsoft Edge**.



This site uses cookies for analytics, personalized content and ads. By continuing to browse this site, you agree to this use.

Figure 3.7 Screenshot of PLABWIN10: Opening a new tab in Microsoft Edge.

## *Step 8*

In the new tab, type of the following URL in the address bar:

```
whois.domaintools.com
```

Press **Enter**.

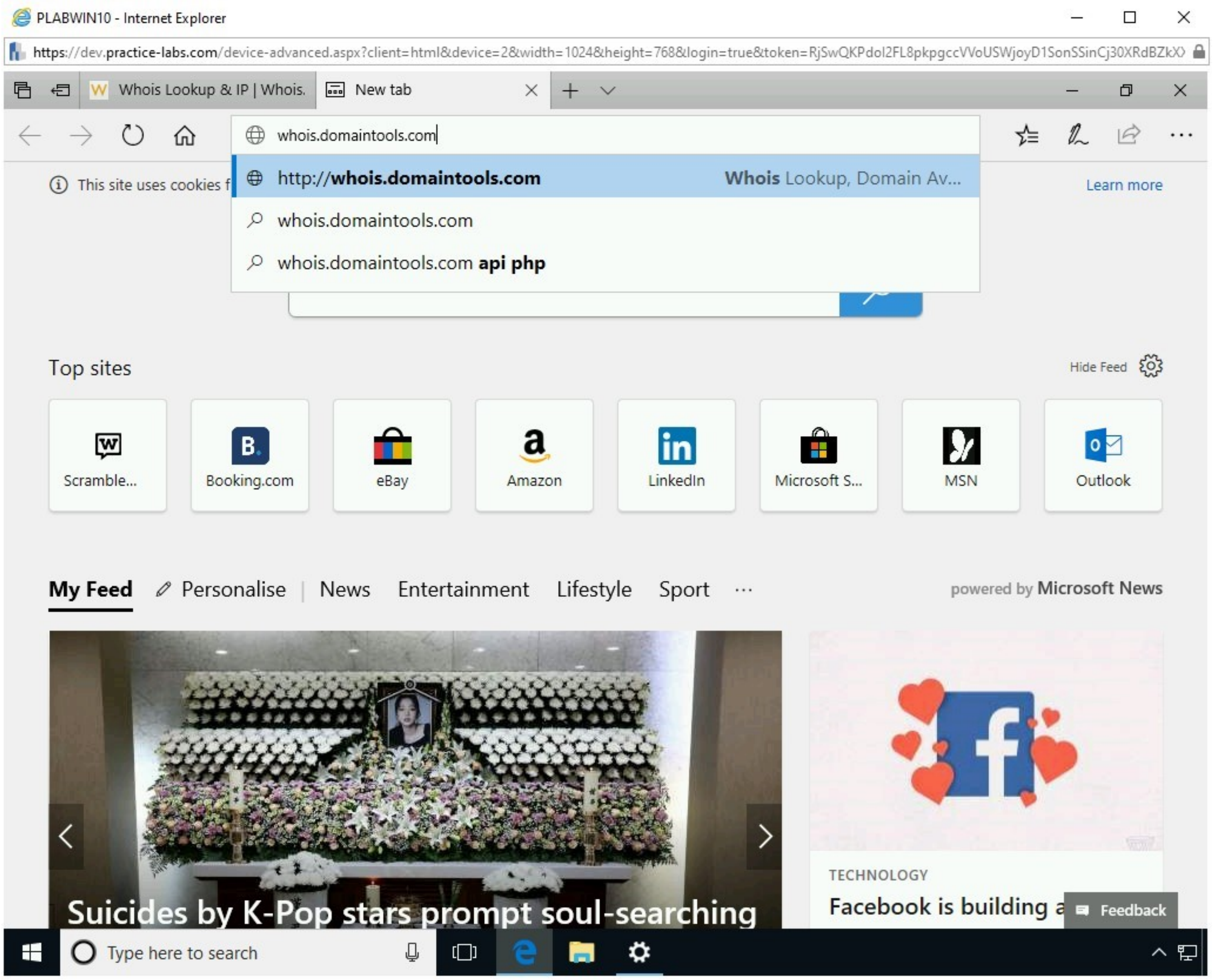

PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Whois Lookup & IP | Whois.
New tab
whois.domaintools.com
http://whois.domaintools.com
Whois Lookup, Domain Av...
whois.domaintools.com
whois.domaintools.com api php
This site uses cookies f
Learn more
Top sites
Hide Feed
Scramble...
Booking.com
eBay
Amazon
LinkedIn
Microsoft S...
MSN
Outlook
My Feed
Personalise
News
Entertainment
Lifestyle
Sport
powered by Microsoft News
Suicides by K-Pop stars prompt soul-searching
TECHNOLOGY
Facebook is building a
Feedback
Type here to search

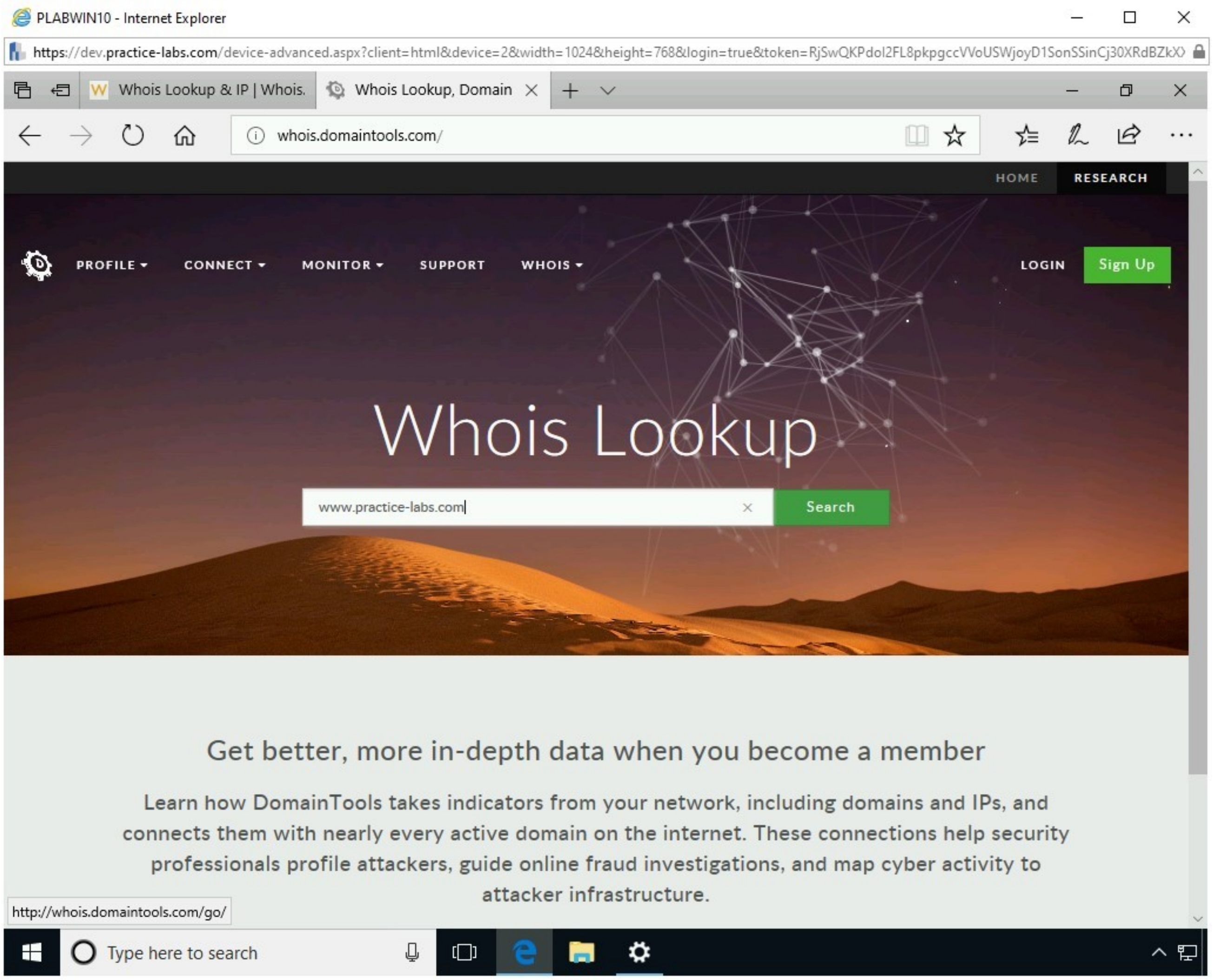
Figure 3.8 Screenshot of PLABWIN10: Typing the whois.domaintools.com URL in the address bar and press Enter.

## Step 9

The **Whois Lookup** Webpage is loaded. In the search text box, type the following URL:

```
www.practice-labs.com
```

Press **Enter**. Alternatively, click **Search**.



https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX

whois.domaintools.com/

Whois Lookup

www.practice-labs.com

Get better, more in-depth data when you become a member

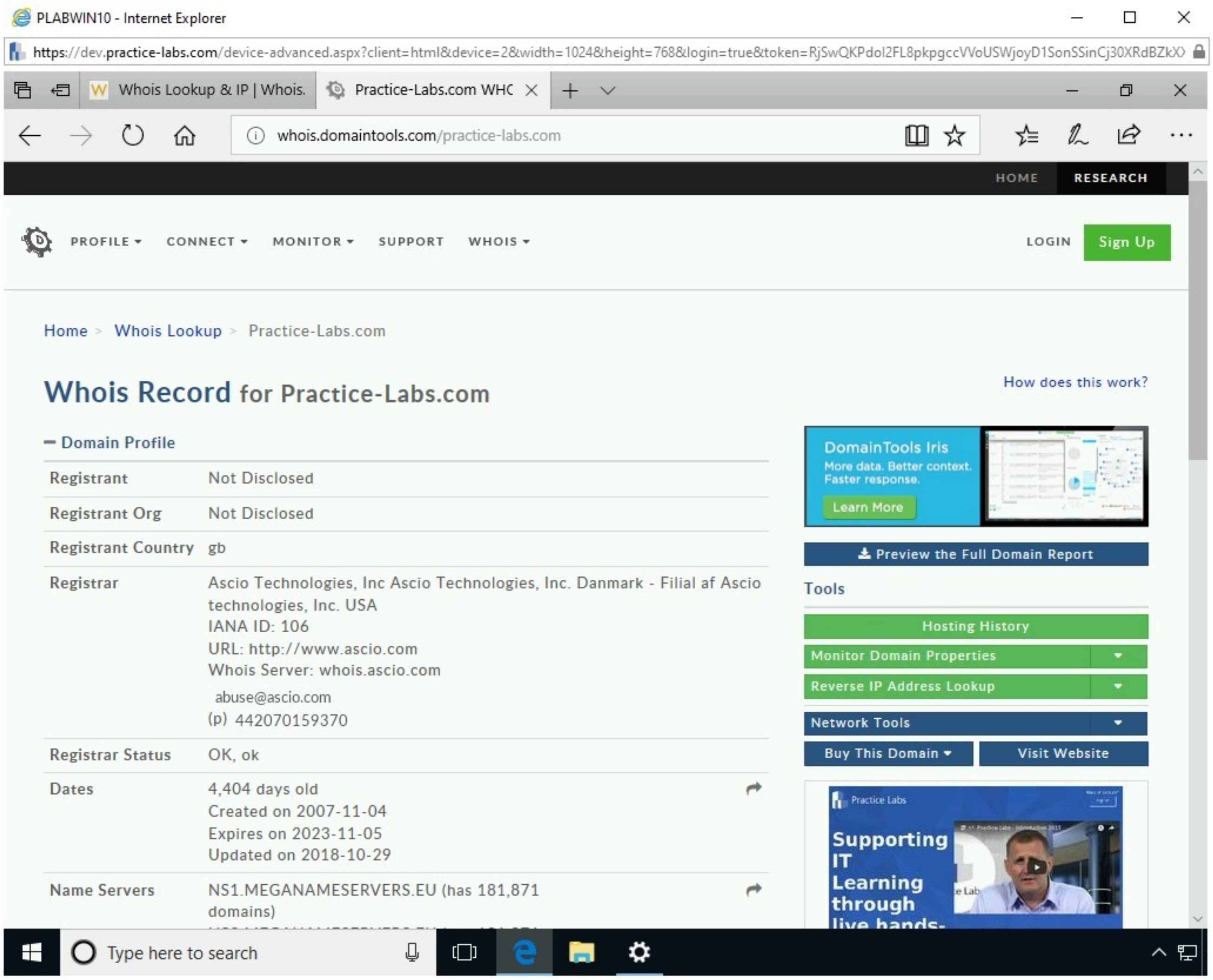
Learn how DomainTools takes indicators from your network, including domains and IPs, and connects them with nearly every active domain on the internet. These connections help security professionals profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure.

http://whois.domaintools.com/go/

Figure 3.9 Screenshot of PLABWIN10: Showing the whois.domaintools.com Webpage and searching for the domain name.

## *Step 10*

The **Whois Record** Webpage is loaded.



PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Whois Lookup & IP | Whois.
Practice-Labs.com WHC
whois.domaintools.com/practice-labs.com
HOME
RESEARCH
PROFILE
CONNECT
MONITOR
SUPPORT
WHOIS
LOGIN
Sign Up
Home > Whois Lookup > Practice-Labs.com
How does this work?
DomainTools Iris
More data. Better context. Faster response.
Learn More
Preview the Full Domain Report
Tools
Hosting History
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools
Buy This Domain
Visit Website
Practice Labs
Supporting IT Learning through live hands-
Type here to search

**Whois Record** for Practice-Labs.com

– Domain Profile

| | |
|---|---|
| Registrant | Not Disclosed |
| Registrant Org | Not Disclosed |
| Registrant Country | gb |
| Registrar | Ascio Technologies, Inc Ascio Technologies, Inc. Danmark - Filial af Ascio technologies, Inc. USA<br>IANA ID: 106<br>URL: http://www.ascio.com<br>Whois Server: whois.ascio.com<br>abuse@ascio.com<br>(p) 442070159370 |
| Registrar Status | OK, ok |
| Dates | 4,404 days old<br>Created on 2007-11-04<br>Expires on 2023-11-05<br>Updated on 2018-10-29 |
| Name Servers | NS1.MEGANAMESERVERS.EU (has 181,871 domains) |

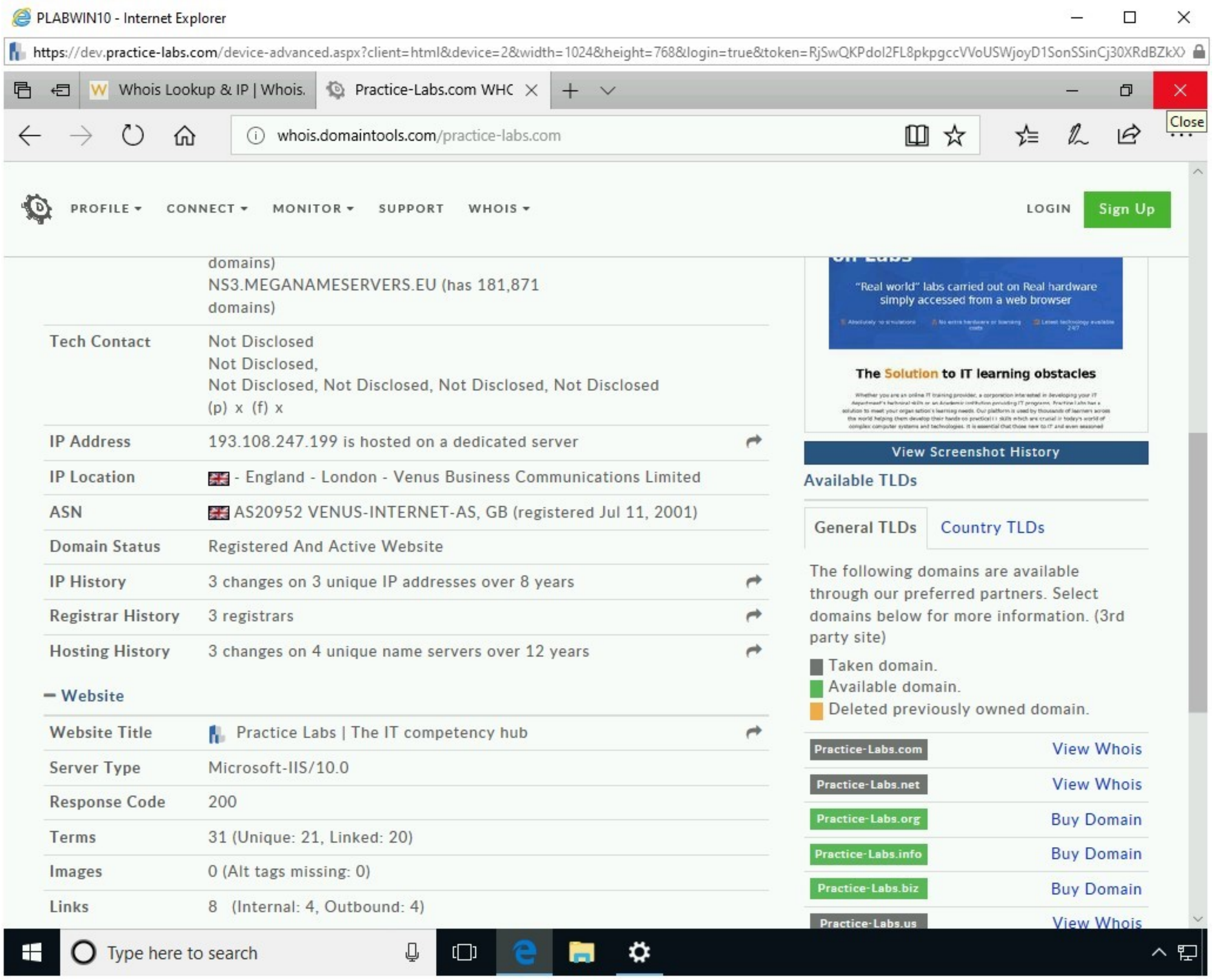
Figure 3.10 Screenshot of PLABWIN10: Showing the information about the searched domain name.

## Step 11

You can scroll down to read more about the searched Website. Notice that this Webpage displays a lot more information than the **WHOis** Website.

Scroll down to view some of the following information:

- Server type
- IP address
- IP location
- IP history
- Registrar history


PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Whois Lookup & IP | Whois.
Practice-Labs.com WHC
Close
whois.domaintools.com/practice-labs.com
PROFILE
CONNECT
MONITOR
SUPPORT
WHOIS
LOGIN
Sign Up
"Real world" labs carried out on Real hardware simply accessed from a web browser
The Solution to IT learning obstacles
View Screenshot History
Type here to search

| | |
|---|---|
| | domains)<br>NS3.MEGANAMESERVERS.EU (has 181,871 domains) |
| Tech Contact | Not Disclosed<br>Not Disclosed,<br>Not Disclosed, Not Disclosed, Not Disclosed, Not Disclosed<br>(p) x (f) x |
| IP Address | 193.108.247.199 is hosted on a dedicated server |
| IP Location | - England - London - Venus Business Communications Limited |
| ASN | AS20952 VENUS-INTERNET-AS, GB (registered Jul 11, 2001) |
| Domain Status | Registered And Active Website |
| IP History | 3 changes on 3 unique IP addresses over 8 years |
| Registrar History | 3 registrars |
| Hosting History | 3 changes on 4 unique name servers over 12 years |

− Website

| | |
|---|---|
| Website Title | Practice Labs \| The IT competency hub |
| Server Type | Microsoft-IIS/10.0 |
| Response Code | 200 |
| Terms | 31 (Unique: 21, Linked: 20) |
| Images | 0 (Alt tags missing: 0) |
| Links | 8 (Internal: 4, Outbound: 4) |

Available TLDs

General TLDs Country TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

▇ Taken domain.
🟩 Available domain.
🟧 Deleted previously owned domain.

| | |
|---|---|
| Practice-Labs.com | View Whois |
| Practice-Labs.net | View Whois |
| Practice-Labs.org | Buy Domain |
| Practice-Labs.info | Buy Domain |
| Practice-Labs.biz | Buy Domain |
| Practice-Labs.us | View Whois |

Figure 3.11 Screenshot of PLABWIN10: Showing information about the searched Website.

Close **Microsoft Edge**.

## Task 2 - Perform Social Media Exploitation

Social media Websites hold personal and organizational information. Organizations create their profiles to promote and market their products and services. At the same time, the employees of these organizations use social media Websites for their personal profiles.

There are several popular social media Websites that are used by organizations and people. These include:

- Twitter
- Facebook

- LinkedIn
- Instagram

Organizations and individuals create their profiles, generally with information such as their E-mail address, and phone number. Such information can be useful to the attacker. For example, an attacker can use information, such as an E-mail address, for phishing or a social engineering attack.

There are various tools available that can help you extract information about the organizations and their employees.

In this task, you will use **https://hunter.io** to extract information from a Website. To do this, perform the following steps:

## *Step 1*

Ensure you have powered on all the devices listed in the introduction and are connected to **PLABKALI01**

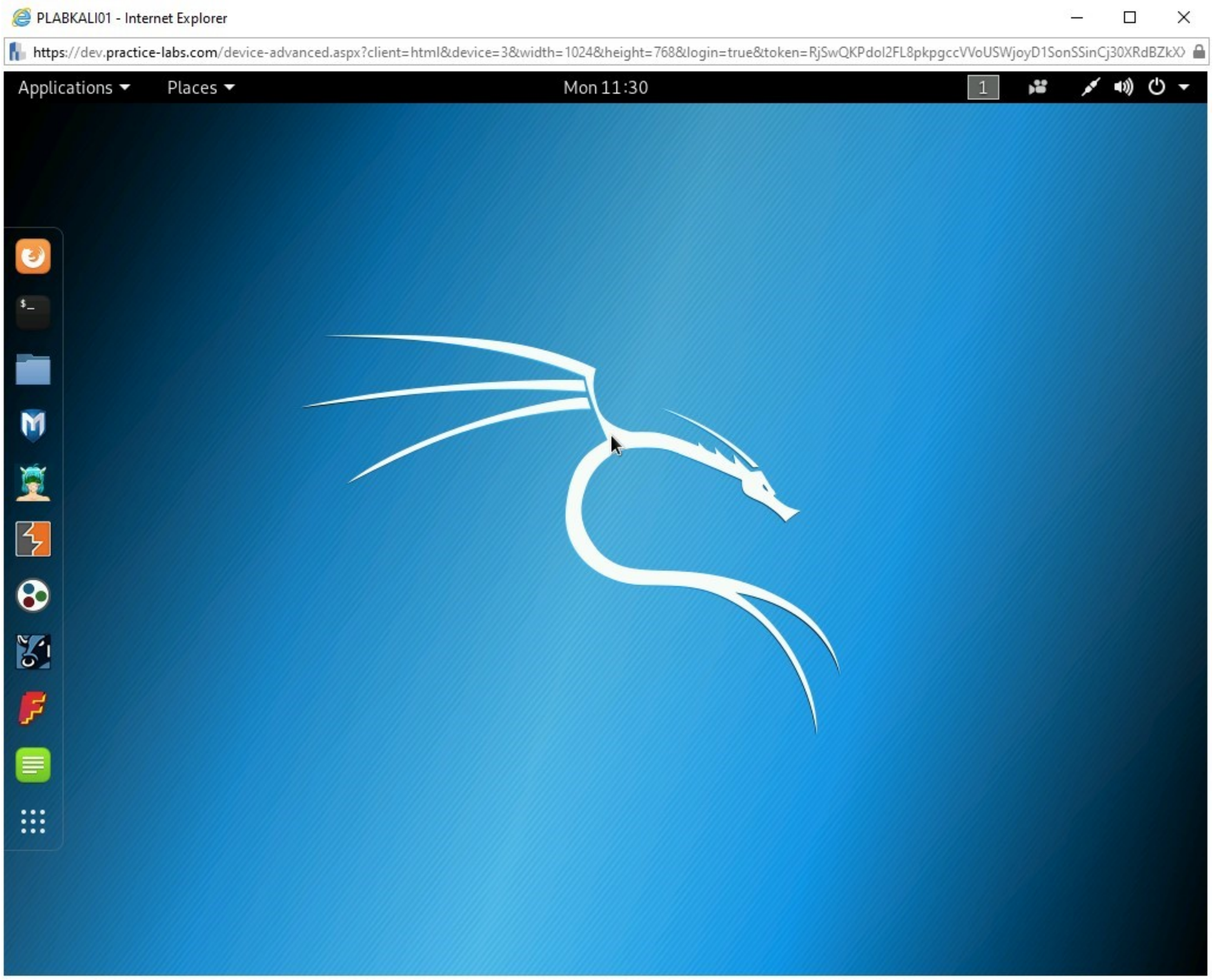

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Mon 11:30
1

Figure 3.12 Screenshot of PLABKALI01: Showing the PLABKALI01 desktop.

## *Step 2*

In the left pane, click the **Firefox ESR** icon.

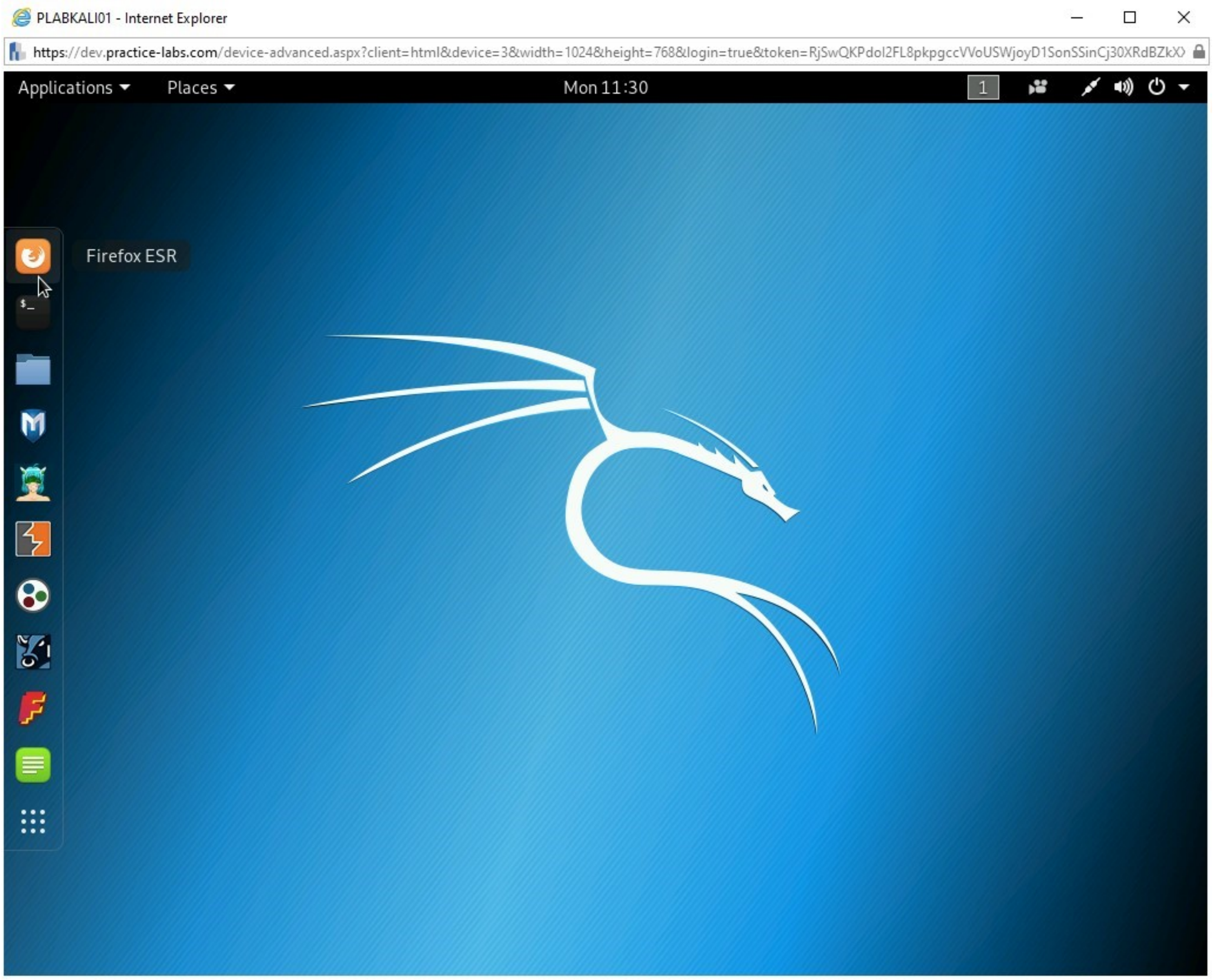

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Mon 11:30
1
Firefox ESR

Figure 3.13 Screenshot of PLABKALI01: Clicking the Firefox ESR icon in the left pane.

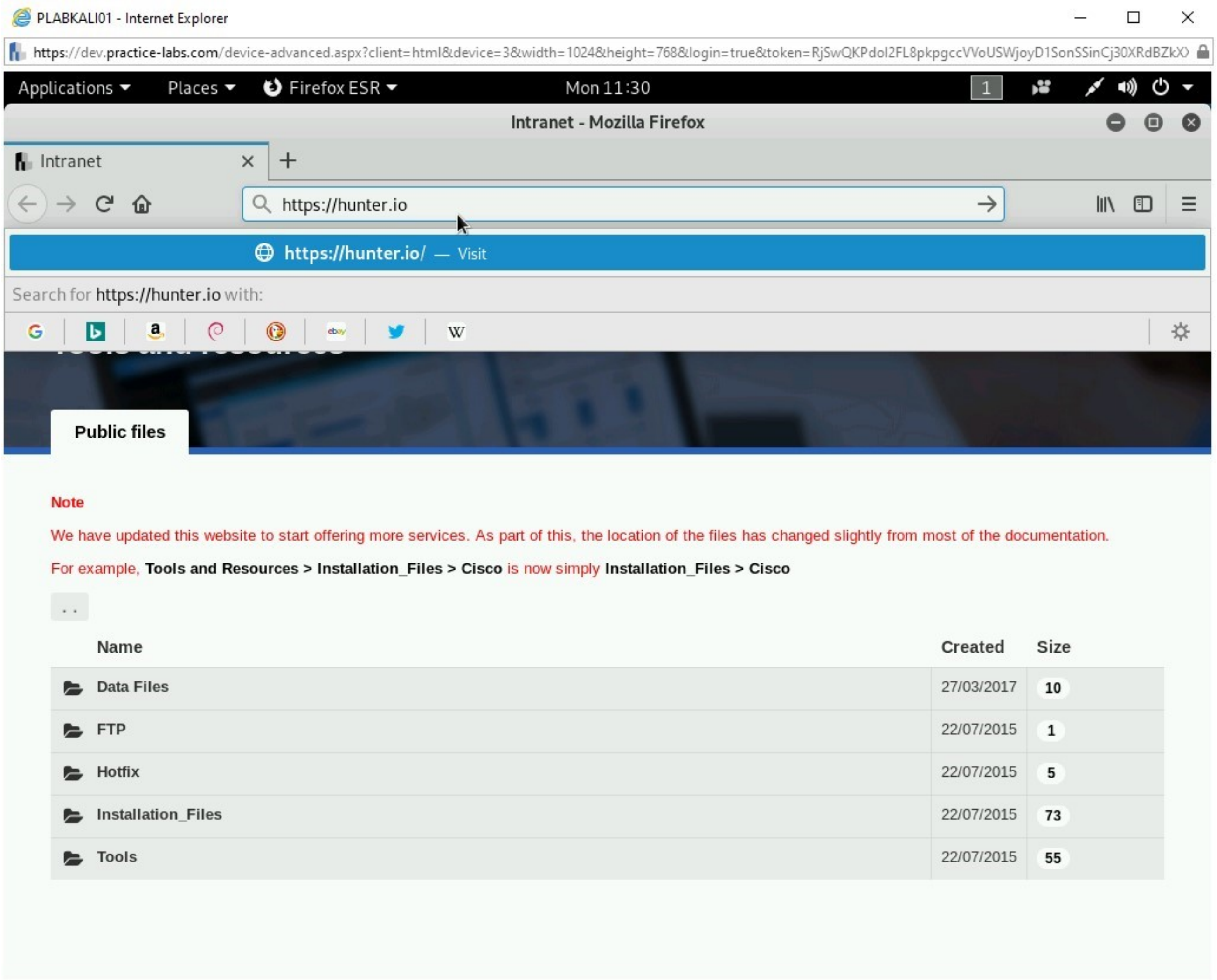
## *Step 3*

The **Firefox** window is displayed.

In the address bar, type the following URL:

```
https://hunter.io
```

Press **Enter**.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Firefox ESR
Mon 11:30
Intranet - Mozilla Firefox
Intranet
https://hunter.io
https://hunter.io/ — Visit
Search for https://hunter.io with:
Public files

Note

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

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

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

Figure 3.14 Screenshot of PLABKALI01: Entering the https://hunter.io URL in the address bar.

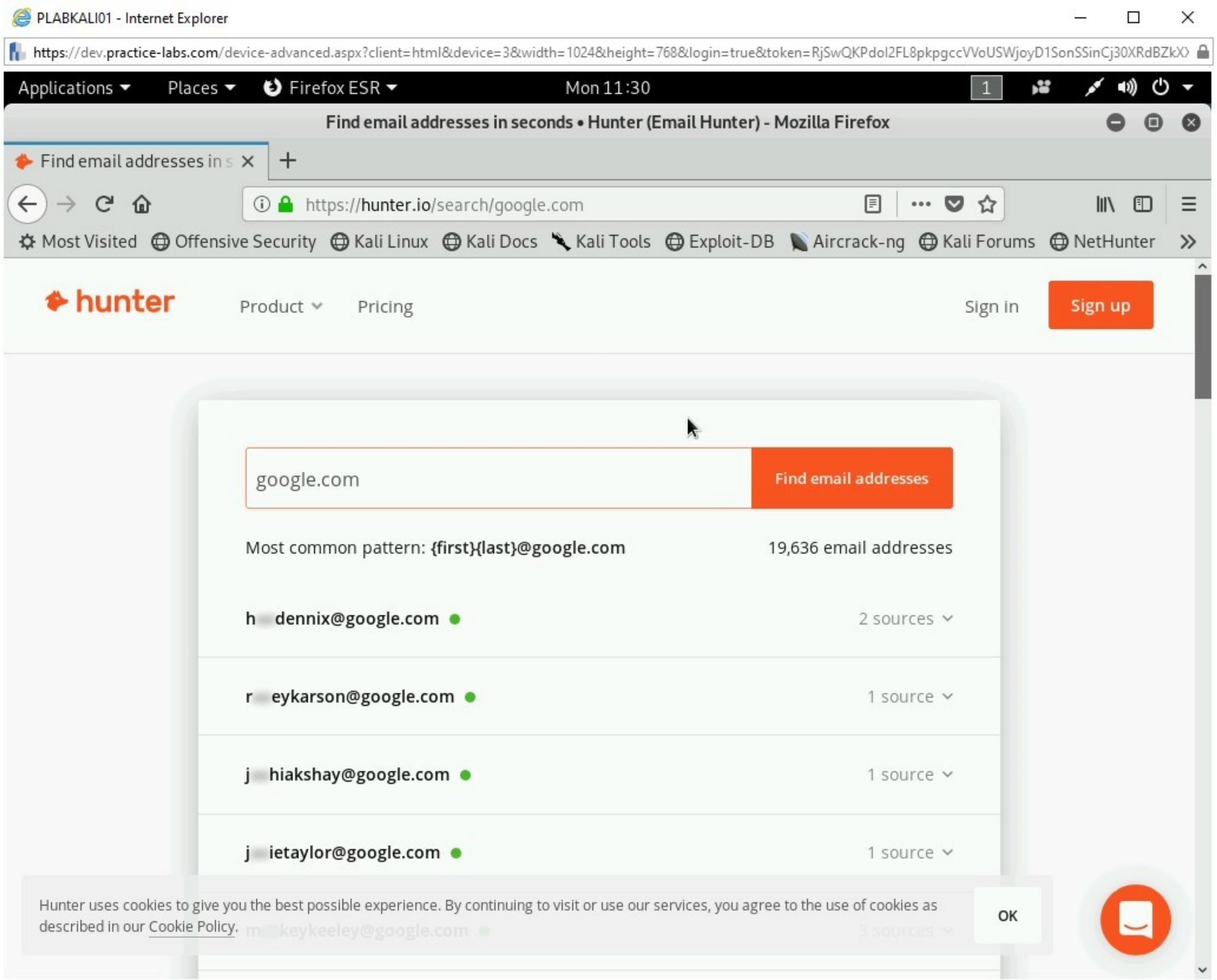
## *Step 4*

The **https://hunter.io** Website is displayed.

In the **Search** text box, type the following:

```
google.com
```

Press **Enter** or click **Find email addresses**.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Firefox ESR
Mon 11:30
Find email addresses in seconds • Hunter (Email Hunter) - Mozilla Firefox
Find email addresses in s
https://hunter.io/search/google.com
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
hunter
Product
Pricing
Sign in
Sign up
Find email addresses
OK

google.com

Most common pattern: {first}{last}@google.com 19,636 email addresses

h[redacted]dennix@google.com ● 2 sources

r[redacted]eykarson@google.com ● 1 source

j[redacted]hiakshay@google.com ● 1 source

j[redacted]ietaylor@google.com ● 1 source

m[redacted]keykeeley@google.com ● 3 sources

Hunter uses cookies to give you the best possible experience. By continuing to visit or use our services, you agree to the use of cookies as described in our Cookie Policy.

Figure 3.15 Screenshot of PLABKALI01: Showing the search results with masked E-mail addresses.

You get limited results when you perform a free search. However, below the results, the output states how many more results are available. For example, for google.com, it states that there are **19,636** more E-mail addresses available.

> ***Note**: You may have to sign up to use this service, if you do not wish to create an account, please move onto the next step.*

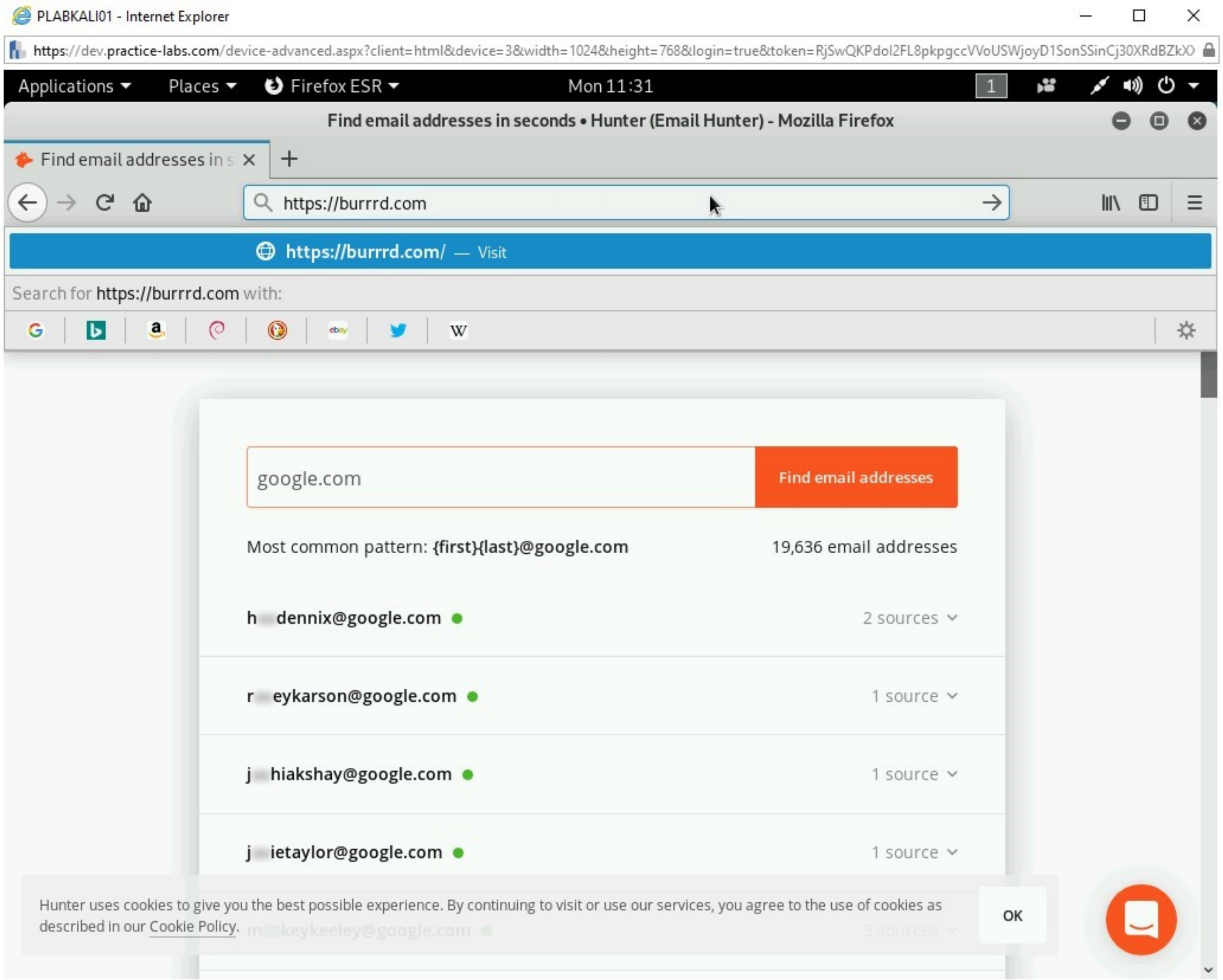
## Step 5

You can also gather information from **Twitter**.

In the **Firefox address bar**, type the following URL:

```
https://burrrd.com
```

Press **Enter**.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Firefox ESR
Mon 11:31
Find email addresses in seconds • Hunter (Email Hunter) - Mozilla Firefox
Find email addresses in s
https://burrrd.com
https://burrrd.com/ — Visit
Search for https://burrrd.com with:
Find email addresses
OK

google.com

Most common pattern: {first}{last}@google.com

19,636 email addresses

h[redacted]dennix@google.com ● 2 sources

r[redacted]eykarson@google.com ● 1 source

j[redacted]hiakshay@google.com ● 1 source

j[redacted]ietaylor@google.com ● 1 source

m[redacted]keykeeley@google.com ● 3 sources

Hunter uses cookies to give you the best possible experience. By continuing to visit or use our services, you agree to the use of cookies as described in our Cookie Policy.

Figure 3.16 Screenshot of PLABKALI01: Entering the https://burrrd.com URL in the address bar.

## Step 6

The **https://burrrd.com** Website is now loaded. It allows you to analyze a Twitter account. For example, you can enter any valid Twitter handle, and it will provide the statistics of that account.

In the **Username** textbox, type the following:

```
microsoft
```

Press **Enter** or click **ANALYZE**.

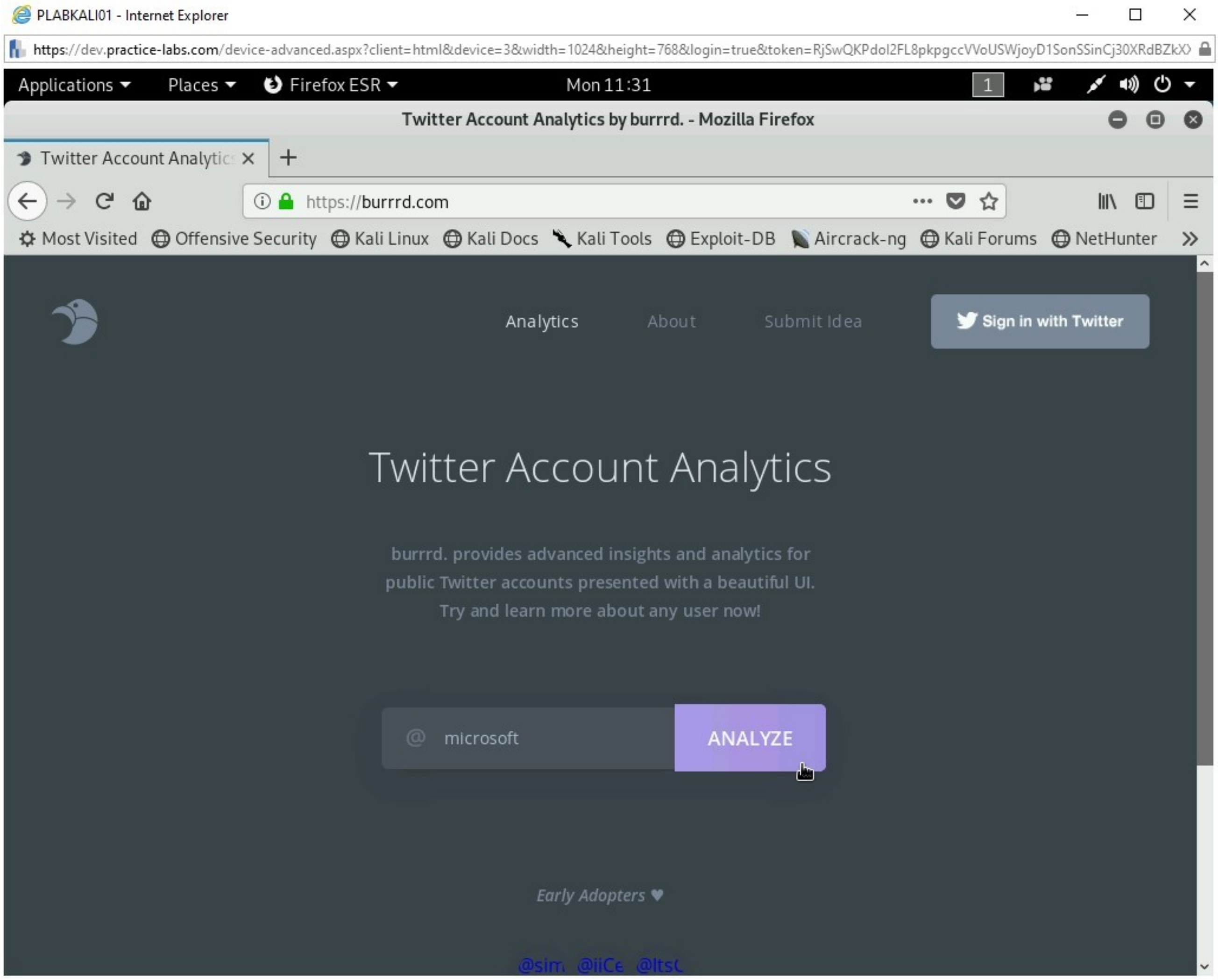
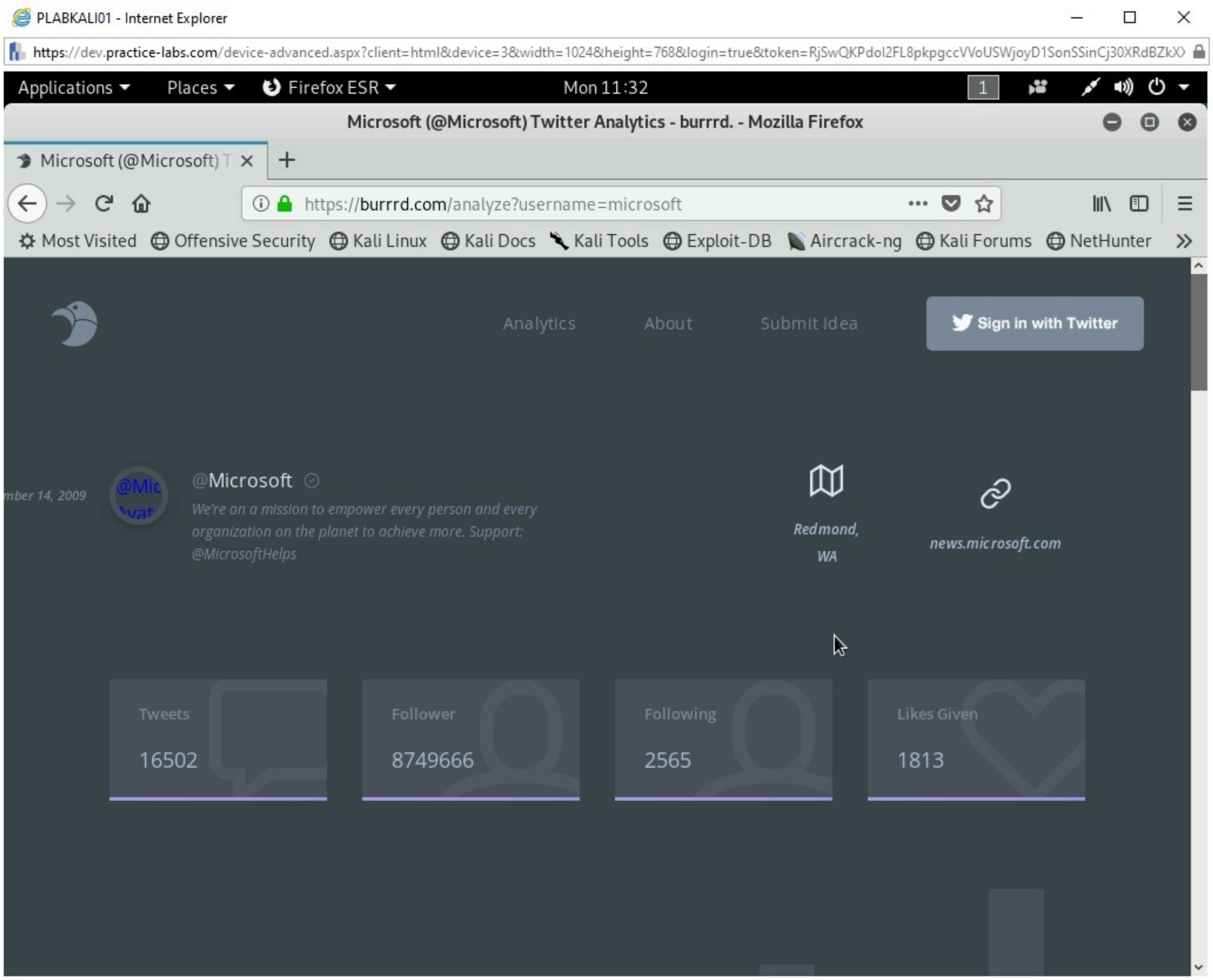

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Firefox ESR
Mon 11:31
Twitter Account Analytics by burrrd. - Mozilla Firefox
Twitter Account Analytic
https://burrrd.com
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Analytics
About
Submit Idea
Sign in with Twitter
Twitter Account Analytics
burrrd. provides advanced insights and analytics for public Twitter accounts presented with a beautiful UI. Try and learn more about any user now!
@ microsoft
ANALYZE
Early Adopters ♥

Figure 3.17 Screenshot of PLABKALI01: Entering Microsoft in the search text box.

## Step 7

The search results are displayed.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Firefox ESR
Mon 11:32
Microsoft (@Microsoft) Twitter Analytics - burrrd. - Mozilla Firefox
Microsoft (@Microsoft) T
https://burrrd.com/analyze?username=microsoft
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Analytics
About
Submit Idea
Sign in with Twitter

mber 14, 2009

@Microsoft

We're on a mission to empower every person and every organization on the planet to achieve more. Support: @MicrosoftHelps

Redmond, WA

news.microsoft.com

Tweets 16502

Follower 8749666

Following 2565

Likes Given 1813

Figure 3.18 Screenshot of PLABKALI01: Showing the search results.

Remember that only public information is being displayed. **Blurrrd.com** only collates that publicly available information.

> ***Note**: You will need to sign in to get information about tweets, followers, following, and likes given.*

## Step 8

You can scroll down to view more statistics about Microsoft, including Connected Users, Top 20 Words, and Top 20 Hashtags.

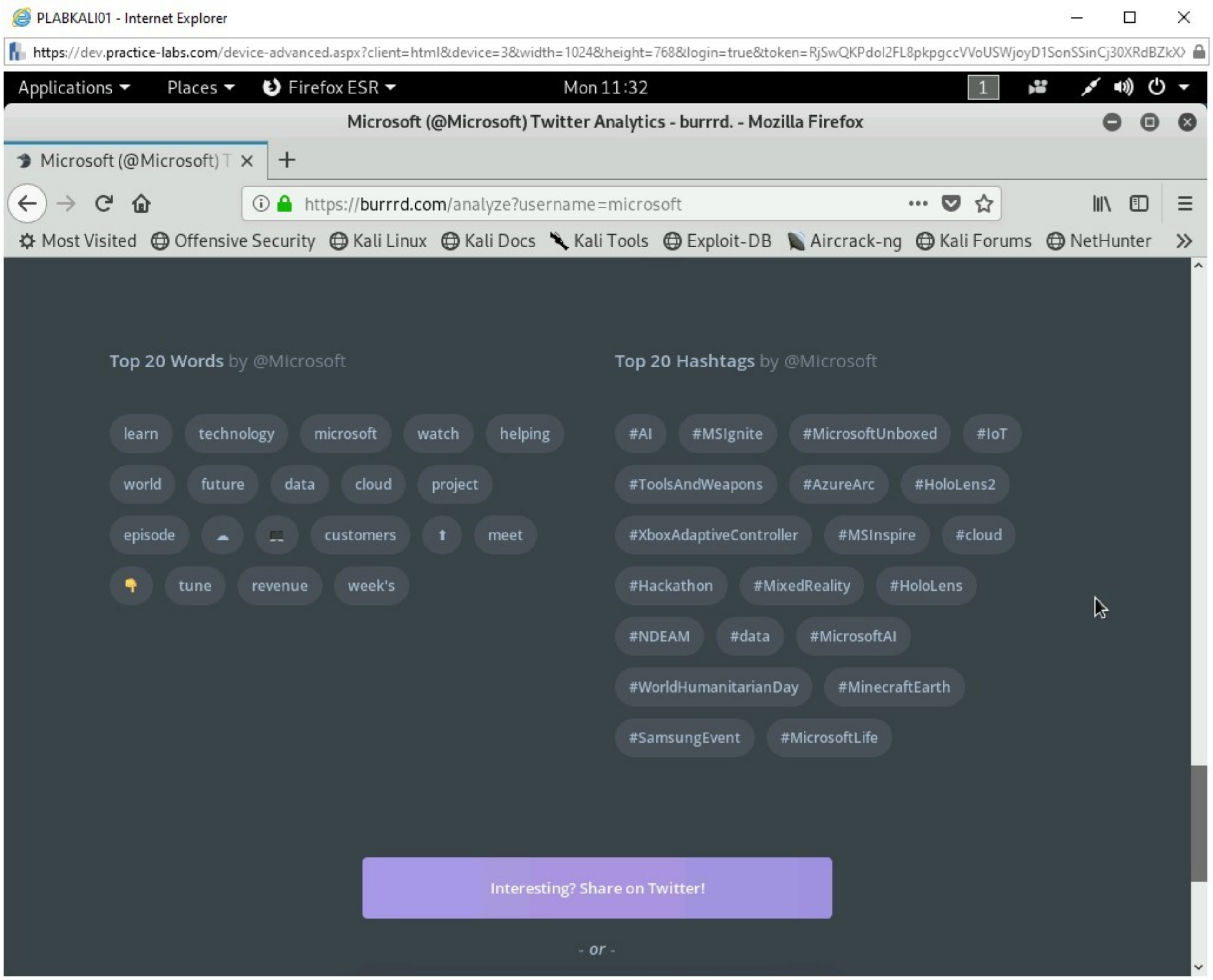


Figure 3.19 Screenshot of PLABKALI01: Showing the keywords and hashtags in the search results.

Keep the **Firefox** window open.

## Task 3 - Use SHODAN

SHODAN is a Website that helps you track the vulnerabilities of online systems and devices. Several online systems and devices, such as webcams and routers, remain configured with the default password. Shodan indexes such devices and provides complete details with the username and password. These usernames and passwords can be misused by anyone who can locate them on Shodan. For example, if a Webcam is IP-enabled, the attacker can use the default username and password to monitor the live feed of the Webcam.

Some of the systems and devices that Shodan can track are:

- Servers
- Routers
- Firewall devices
- Devices, such as Webcam and wireless routers
- IoT devices
- Industrial control systems (ICS)

> ***Note****: To be able to use Shodan, you need to create a user account on the https://shodan.io Website. After logging into the Website, you can simply perform a search and get the results.*

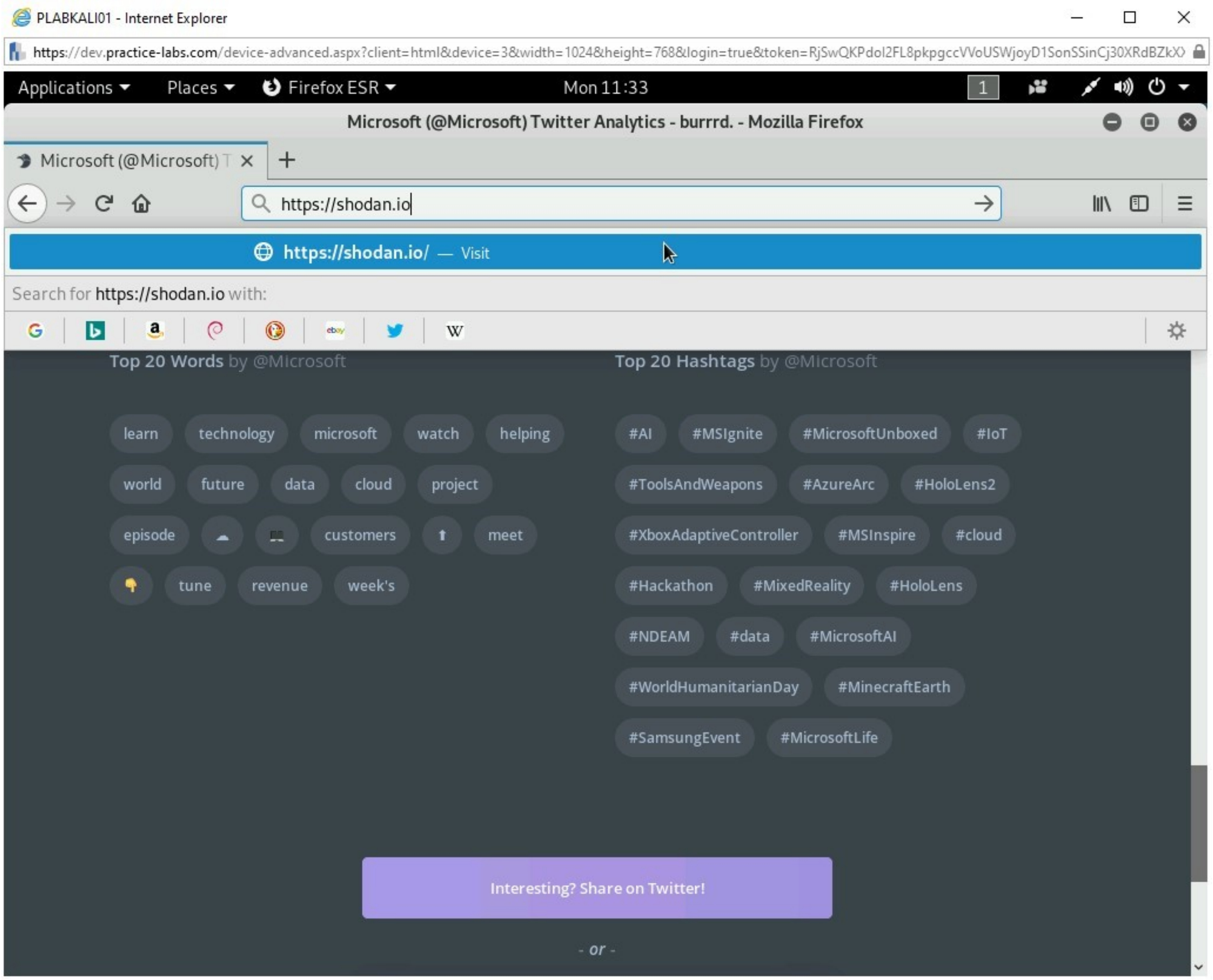
## Step 1

Ensure you have powered on all the devices listed in the introduction and are connected to **PLABKALI01**. Ensure that the **Firefox** window is open.

In the address bar, type the following URL:

```
https://shodan.io
```

Press **Enter**.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Firefox ESR
Mon 11:33
Microsoft (@Microsoft) Twitter Analytics - burrrd. - Mozilla Firefox
Microsoft (@Microsoft) T
https://shodan.io/ — Visit
Search for https://shodan.io with:
Top 20 Words by @Microsoft
learn
technology
microsoft
watch
helping
world
future
data
cloud
project
episode
customers
meet
tune
revenue
week's
Top 20 Hashtags by @Microsoft
#AI
#MSIgnite
#MicrosoftUnboxed
#IoT
#ToolsAndWeapons
#AzureArc
#HoloLens2
#XboxAdaptiveController
#MSInspire
#cloud
#Hackathon
#MixedReality
#HoloLens
#NDEAM
#data
#MicrosoftAI
#WorldHumanitarianDay
#MinecraftEarth
#SamsungEvent
#MicrosoftLife
Interesting? Share on Twitter!
- or -

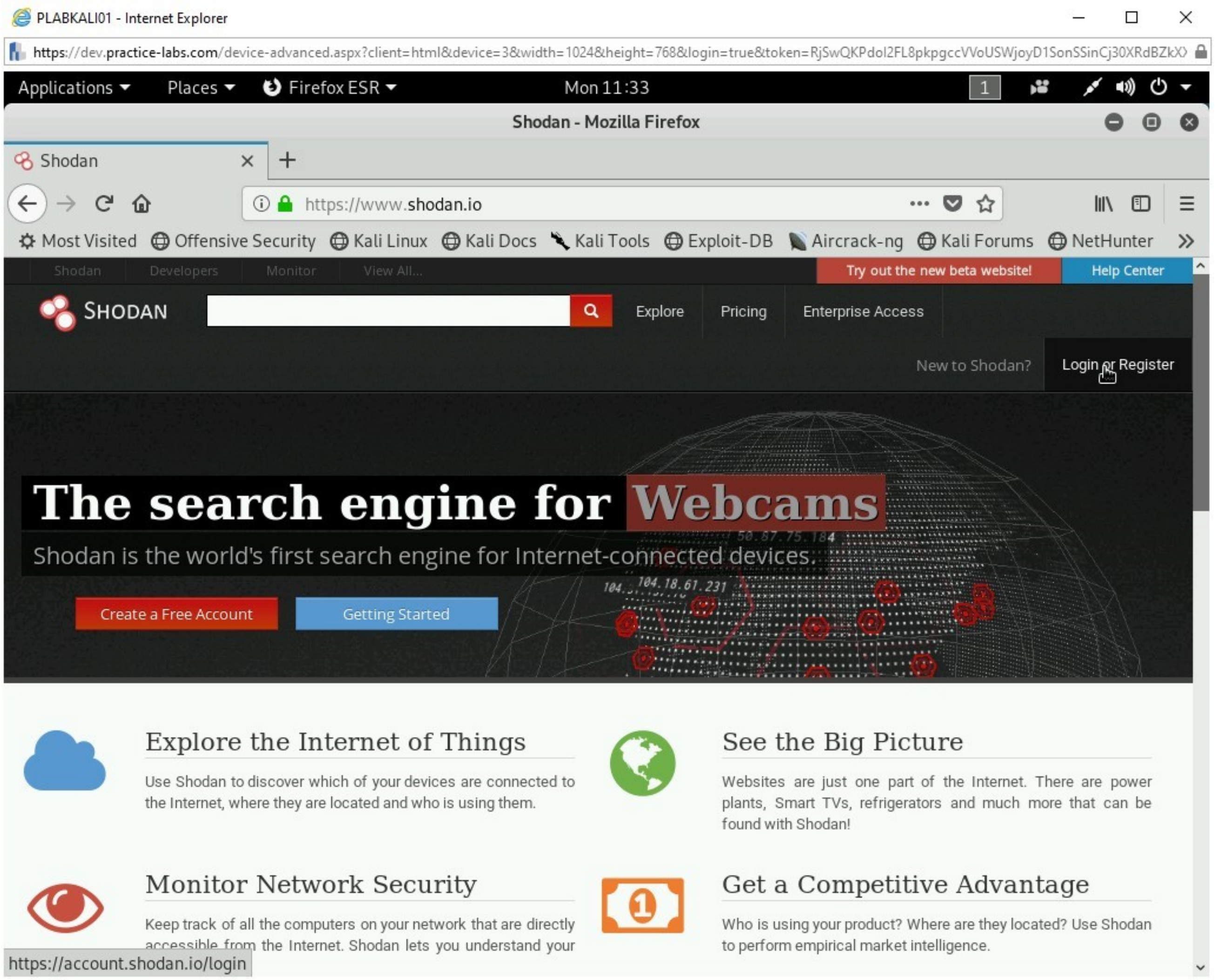
https://shodan.io

Figure 3.20 Screenshot of PLABKALI01: Entering the https://shodan.io URL in the address bar.

## Step 2

The **https://shodan.io** Website loads. You need to first log in to the Website to explore various things like open Webcams.

Click **Login or Register**.



The search engine for Webcams

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your

Get a Competitive Advantage

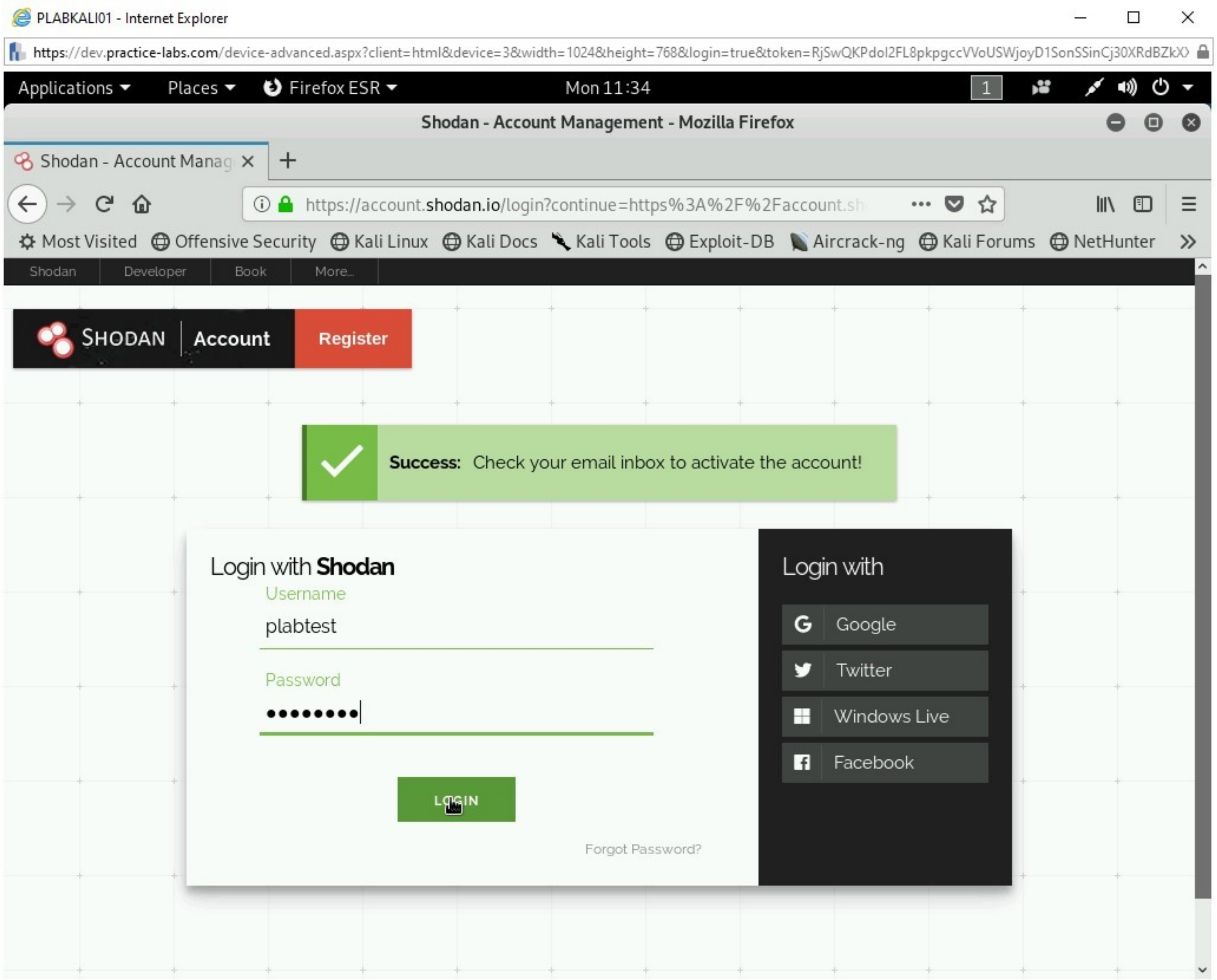
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Figure 3.21 Screenshot of PLABKALI01: Clicking the Login or Register option on the Shodan homepage.

## Step 3

Enter your login credentials and click **LOGIN**.

> ***Note**: When prompted to save user credentials, click Don’t Save.*


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Firefox ESR
Mon 11:34
Shodan - Account Management - Mozilla Firefox
Shodan - Account Manag
https://account.shodan.io/login?continue=https%3A%2F%2Faccount.sh
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Shodan
Developer
Book
More...
SHODAN
Account
Register
Login with
Google
Twitter
Windows Live
Facebook
LOGIN
Forgot Password?

**Success:** Check your email inbox to activate the account!

Login with **Shodan**

Username
plabtest

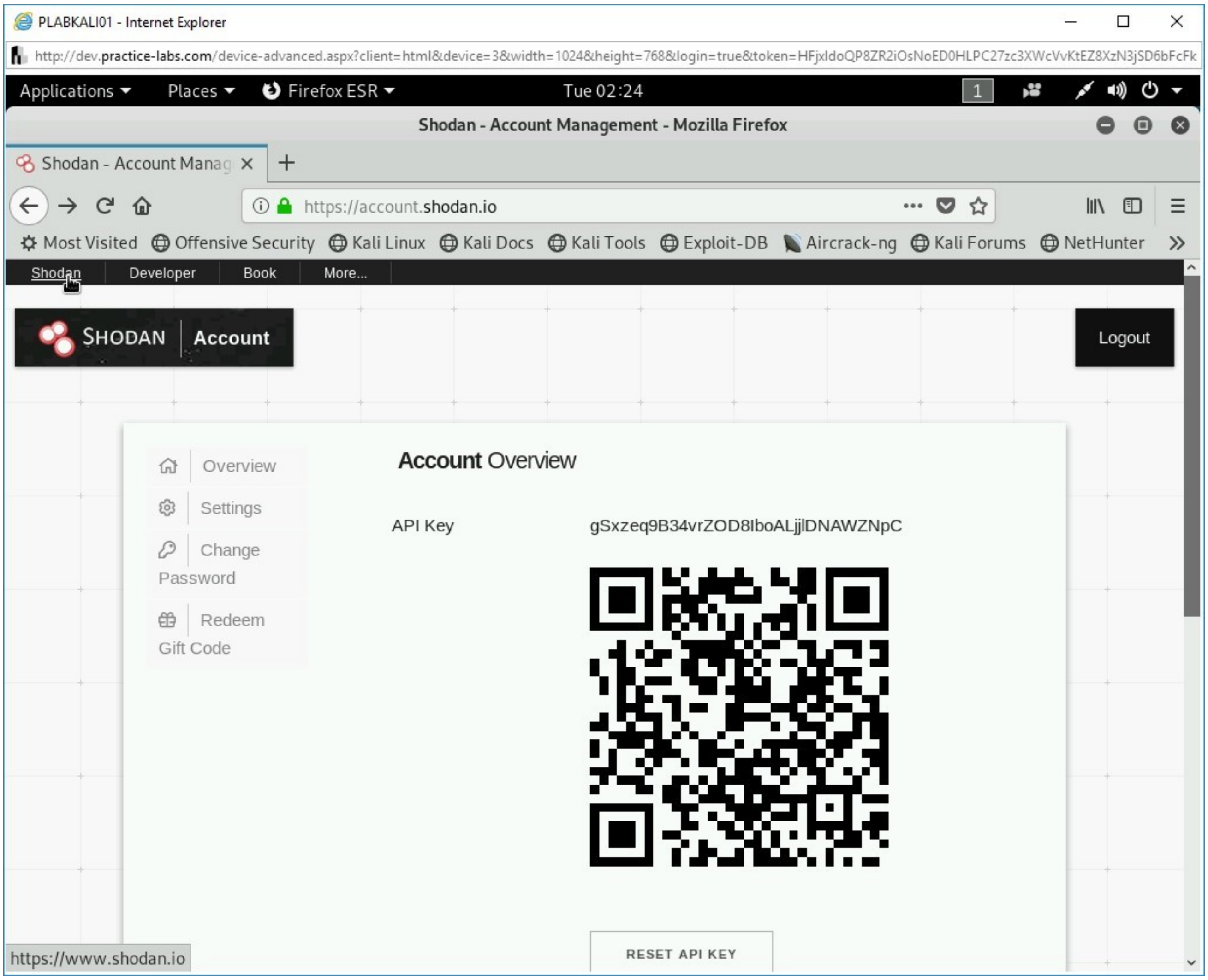
Password
•••••••••

Figure 3.22 Screenshot of PLABKALI01: Entering the login credentials on the Login with Shodan Webpage.

## *Step 4*

You are navigated to the profile page.

Click **Shodan** in the upper left corner.



Account Overview

API Key gSxzeq9B34vrZOD8IboALjjlDNAWZNpC

Figure 3.23 Screenshot of PLABKALI01: Clicking the Shodan link in the upper left corner.

## Step 5

You will now be on the home page.

In the search bar at the top of the Webpage, type the following:

```
VNC
```

Press **Enter**.

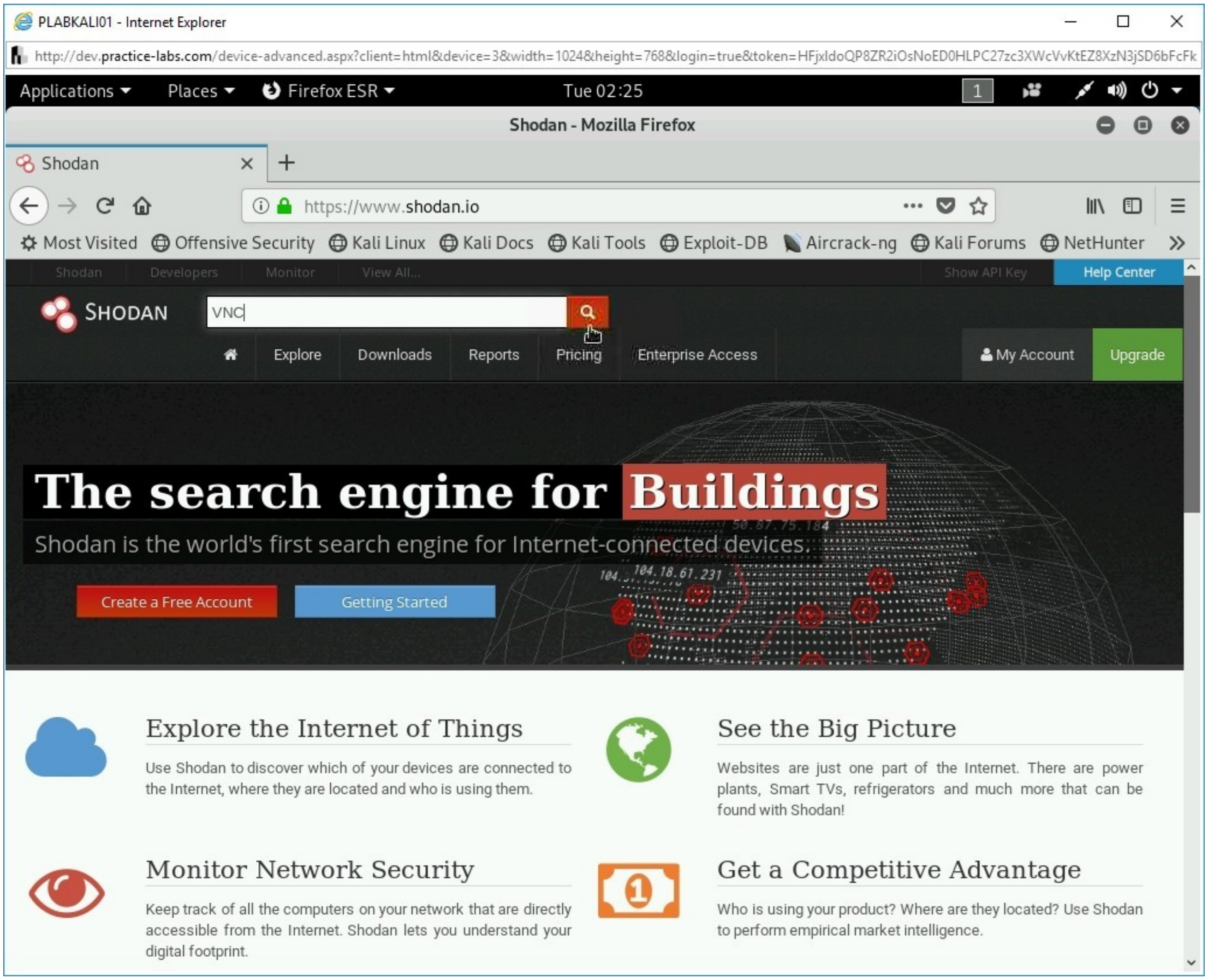
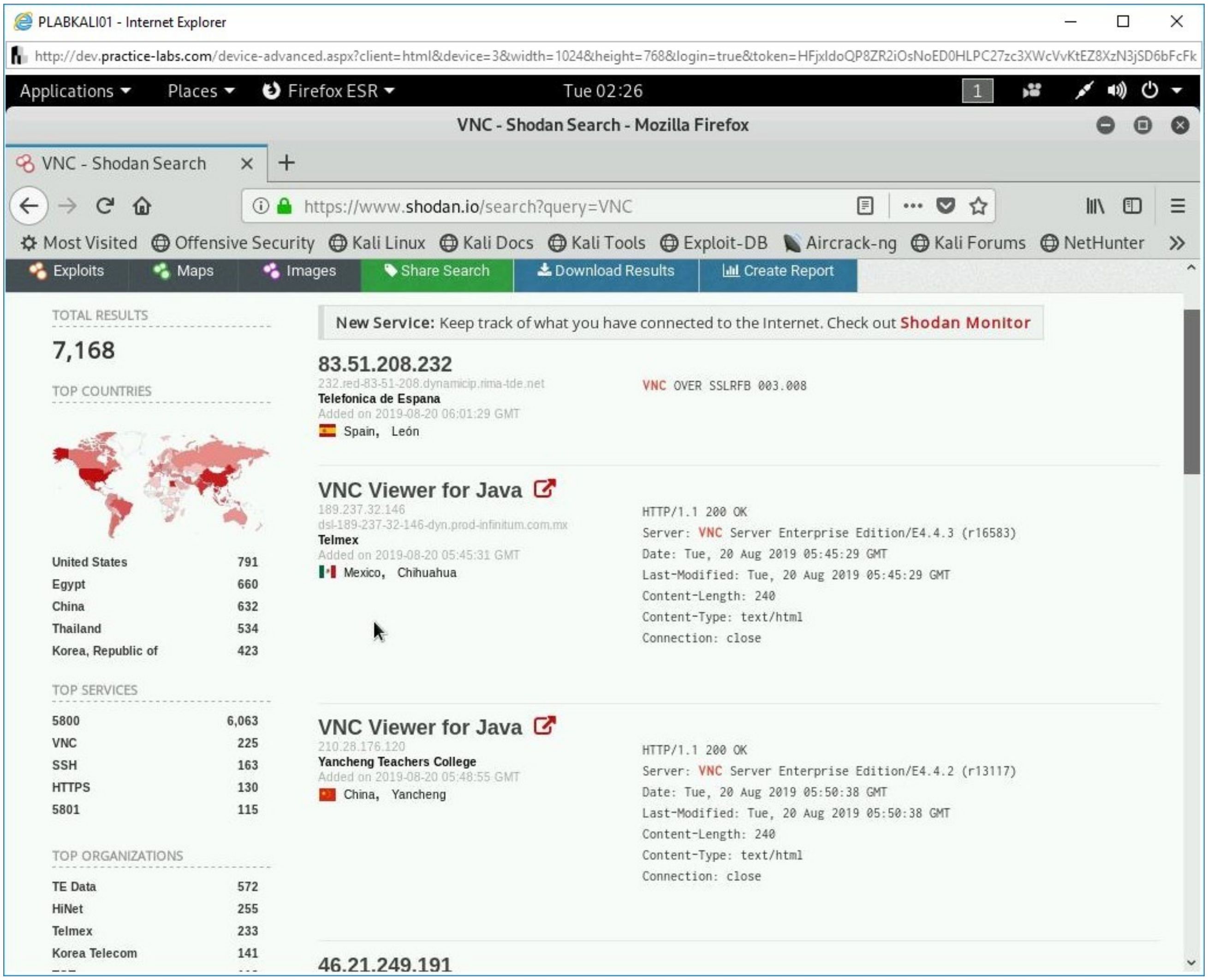

PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=HFjxIdoQP8ZR2iOsNoED0HLPC27zc3XWcVvKtEZ8XzN3jSD6bFcFk
Applications
Places
Firefox ESR
Tue 02:25
Shodan - Mozilla Firefox
Shodan
https://www.shodan.io
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Shodan
Developers
Monitor
View All...
Show API Key
Help Center
SHODAN
VNC
Explore
Downloads
Reports
Pricing
Enterprise Access
My Account
Upgrade
The search engine for Buildings
Shodan is the world's first search engine for Internet-connected devices.
Create a Free Account
Getting Started
Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.
See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!
Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.
Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Figure 3.24 Screenshot of PLABKALI01: Entering VNC in the search text box.

The search results are displayed. The left pane displays a lot of information, such as:

- TOP COUNTRIES
- TOP SERVICES
- TOP ORGANIZATIONS
- TOP OPERATING SYSTEMS
- TOP PRODUCTS

***Note***: *Scroll down to view all the items listed in the bullets. The results are likely to vary in your lab environment.*


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=HFjxldoQP8ZR2iOsNoED0HLPC27zc3XWcVvKtEZ8XzN3jSD6bFcFk
Applications
Places
Firefox ESR
Tue 02:26
VNC - Shodan Search - Mozilla Firefox
VNC - Shodan Search
https://www.shodan.io/search?query=VNC
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Exploits
Maps
Images
Share Search
Download Results
Create Report

TOTAL RESULTS

7,168

TOP COUNTRIES

| | |
|---|---|
| United States | 791 |
| Egypt | 660 |
| China | 632 |
| Thailand | 534 |
| Korea, Republic of | 423 |

TOP SERVICES

| | |
|---|---|
| 5800 | 6,063 |
| VNC | 225 |
| SSH | 163 |
| HTTPS | 130 |
| 5801 | 115 |

TOP ORGANIZATIONS

| | |
|---|---|
| TE Data | 572 |
| HiNet | 255 |
| Telmex | 233 |
| Korea Telecom | 141 |

**New Service:** Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

83.51.208.232
232.red-83-51-208.dynamicip.rima-tde.net
Telefonica de Espana
Added on 2019-08-20 06:01:29 GMT
Spain, León

```
VNC OVER SSLRFB 003.008
```

VNC Viewer for Java
189.237.32.146
dsl-189-237-32-146-dyn.prod-infinitum.com.mx
Telmex
Added on 2019-08-20 05:45:31 GMT
Mexico, Chihuahua

```
HTTP/1.1 200 OK
Server: VNC Server Enterprise Edition/E4.4.3 (r16583)
Date: Tue, 20 Aug 2019 05:45:29 GMT
Last-Modified: Tue, 20 Aug 2019 05:45:29 GMT
Content-Length: 240
Content-Type: text/html
Connection: close
```

VNC Viewer for Java
210.28.176.120
Yancheng Teachers College
Added on 2019-08-20 05:48:55 GMT
China, Yancheng

```
HTTP/1.1 200 OK
Server: VNC Server Enterprise Edition/E4.4.2 (r13117)
Date: Tue, 20 Aug 2019 05:50:38 GMT
Last-Modified: Tue, 20 Aug 2019 05:50:38 GMT
Content-Length: 240
Content-Type: text/html
Connection: close
```

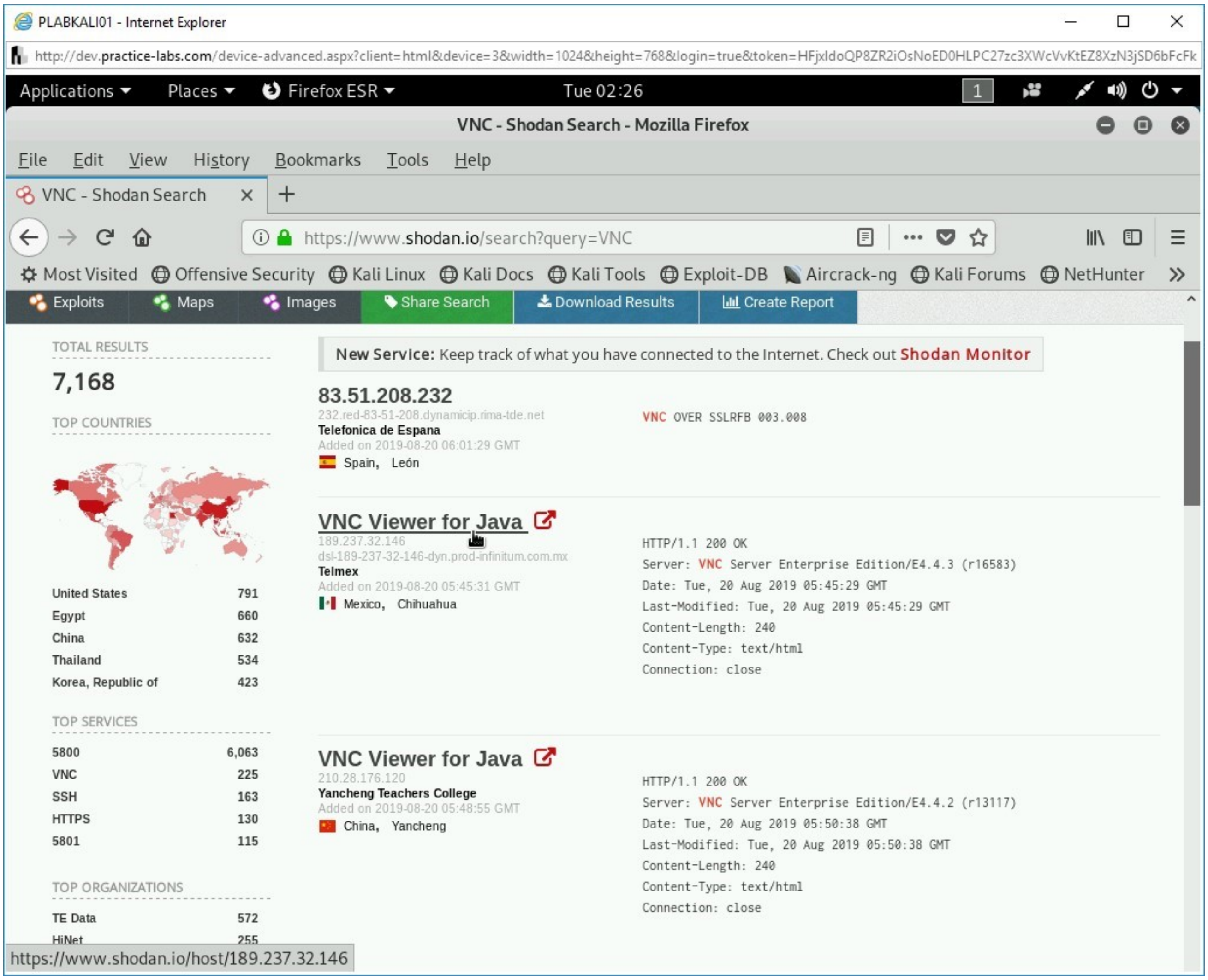
46.21.249.191

Figure 3.25 Screenshot of PLABKALI01: Showing the search results of the VNC keyword.

## Step 6

Click **VNC Viewer for Java** from the search results.

> ***Note***: *If this result is not visible in your search, you can select any other search item.*


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=HFjxldoQP8ZR2iOsNoED0HLPC27zc3XWcVvKtEZ8XzN3jSD6bFcFk
Applications
Places
Firefox ESR
Tue 02:26
VNC - Shodan Search - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
VNC - Shodan Search
https://www.shodan.io/search?query=VNC
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Exploits
Maps
Images
Share Search
Download Results
Create Report
https://www.shodan.io/host/189.237.32.146

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

TOTAL RESULTS

7,168

TOP COUNTRIES

| | |
|---|---|
| United States | 791 |
| Egypt | 660 |
| China | 632 |
| Thailand | 534 |
| Korea, Republic of | 423 |

TOP SERVICES

| | |
|---|---|
| 5800 | 6,063 |
| VNC | 225 |
| SSH | 163 |
| HTTPS | 130 |
| 5801 | 115 |

TOP ORGANIZATIONS

| | |
|---|---|
| TE Data | 572 |
| HiNet | 255 |

83.51.208.232
232.red-83-51-208.dynamicip.rima-tde.net
Telefonica de Espana
Added on 2019-08-20 06:01:29 GMT
Spain, León

```
VNC OVER SSLRFB 003.008
```

VNC Viewer for Java
189.237.32.146
dsl-189-237-32-146-dyn.prod-infinitum.com.mx
Telmex
Added on 2019-08-20 05:45:31 GMT
Mexico, Chihuahua

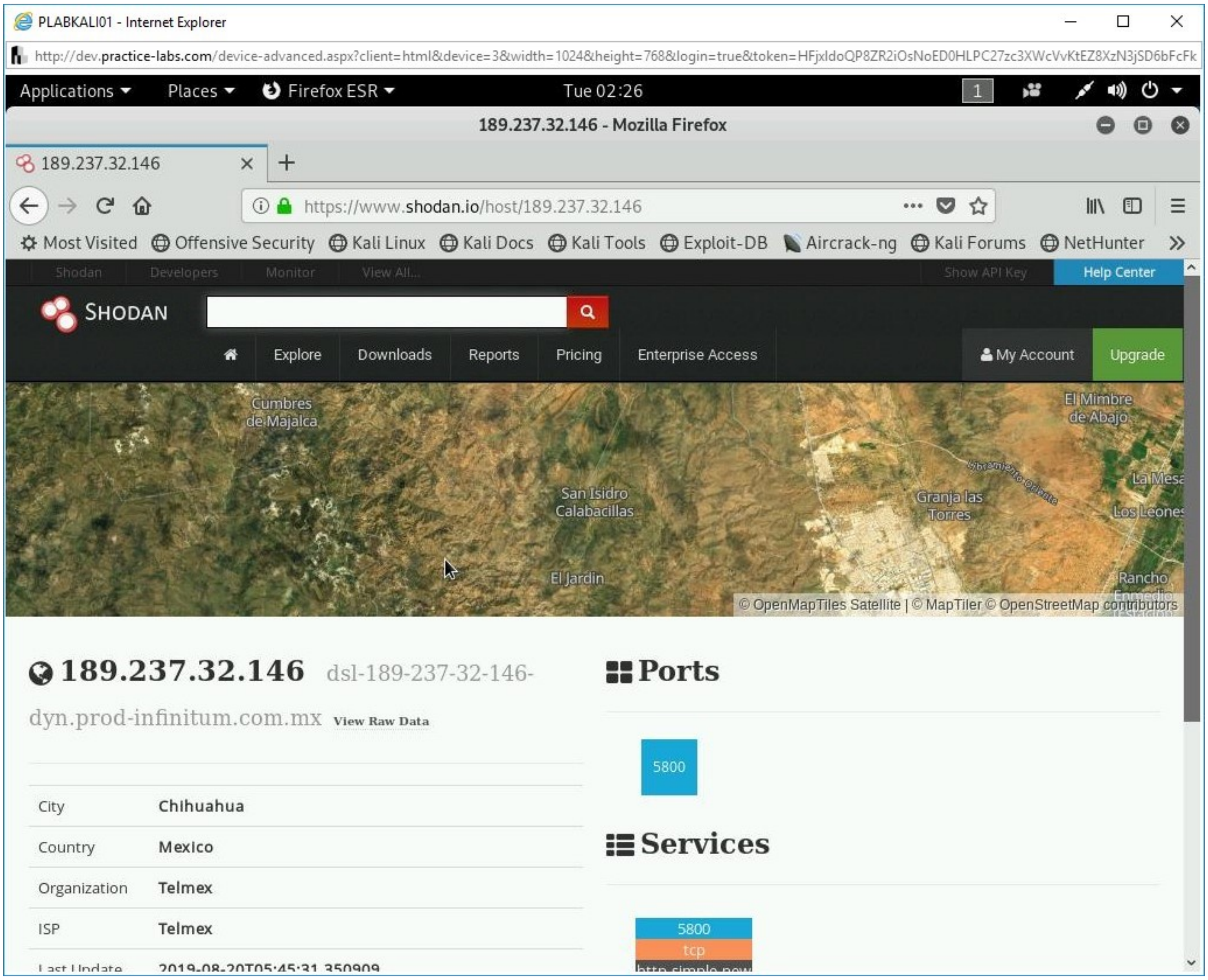
```
HTTP/1.1 200 OK
Server: VNC Server Enterprise Edition/E4.4.3 (r16583)
Date: Tue, 20 Aug 2019 05:45:29 GMT
Last-Modified: Tue, 20 Aug 2019 05:45:29 GMT
Content-Length: 240
Content-Type: text/html
Connection: close
```

VNC Viewer for Java
210.28.176.120
Yancheng Teachers College
Added on 2019-08-20 05:48:55 GMT
China, Yancheng

```
HTTP/1.1 200 OK
Server: VNC Server Enterprise Edition/E4.4.2 (r13117)
Date: Tue, 20 Aug 2019 05:50:38 GMT
Last-Modified: Tue, 20 Aug 2019 05:50:38 GMT
Content-Length: 240
Content-Type: text/html
Connection: close
```

Figure 3.26 Screenshot of PLABKALI01: Clicking the VNC Viewer for Java result.

The information about the selected result is displayed. Notice the right pane displays the ports and services available on this IP address. You can scroll down to view detailed information.



**189.237.32.146** dsl-189-237-32-146-dyn.prod-infinitum.com.mx View Raw Data

| | |
|---|---|
| City | Chihuahua |
| Country | Mexico |
| Organization | Telmex |
| ISP | Telmex |
| Last Update | 2019-08-20T05:45:31.350909 |

**Ports**

5800

**Services**

5800
tcp
http-simple-new

Figure 3.27 Screenshot of PLABKALI01: Showing the details of the selected search result.

## *Step 7*

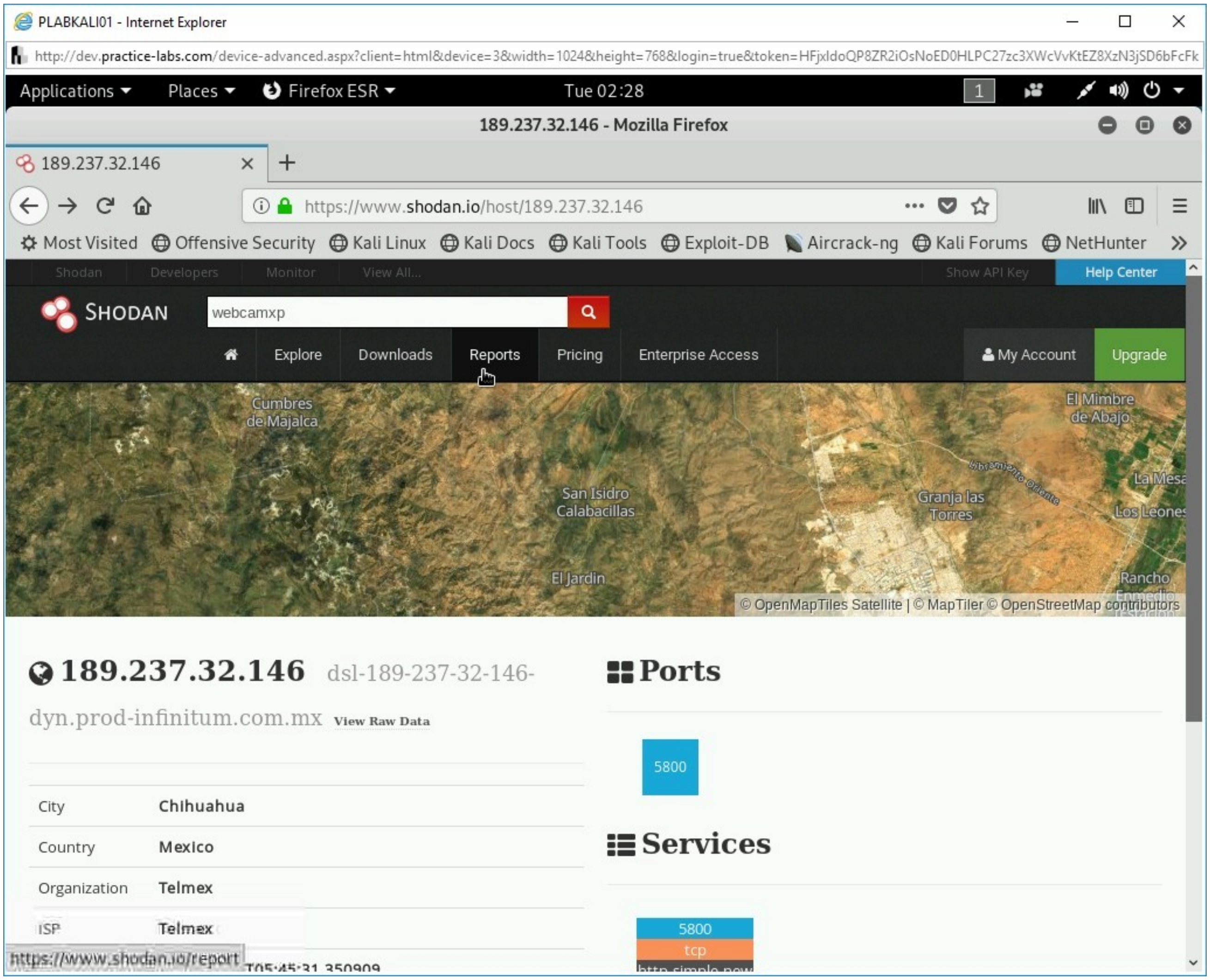
You can also search for live webcams on Shodan. For example, you can search for **webcamxp**. The search result will provide a list of live webcams from around the world.

> ***Note****: The shodan.io Website is regularly updated, and therefore, you are likely to see a different set of hosts on this Webpage.*

In the **search** box, type the following:

```
webcamxp
```

Press **Enter**.



Search: webcamxp

189.237.32.146 dsl-189-237-32-146-dyn.prod-infinitum.com.mx

| | |
|---|---|
| City | Chihuahua |
| Country | Mexico |
| Organization | Telmex |
| ISP | Telmex |

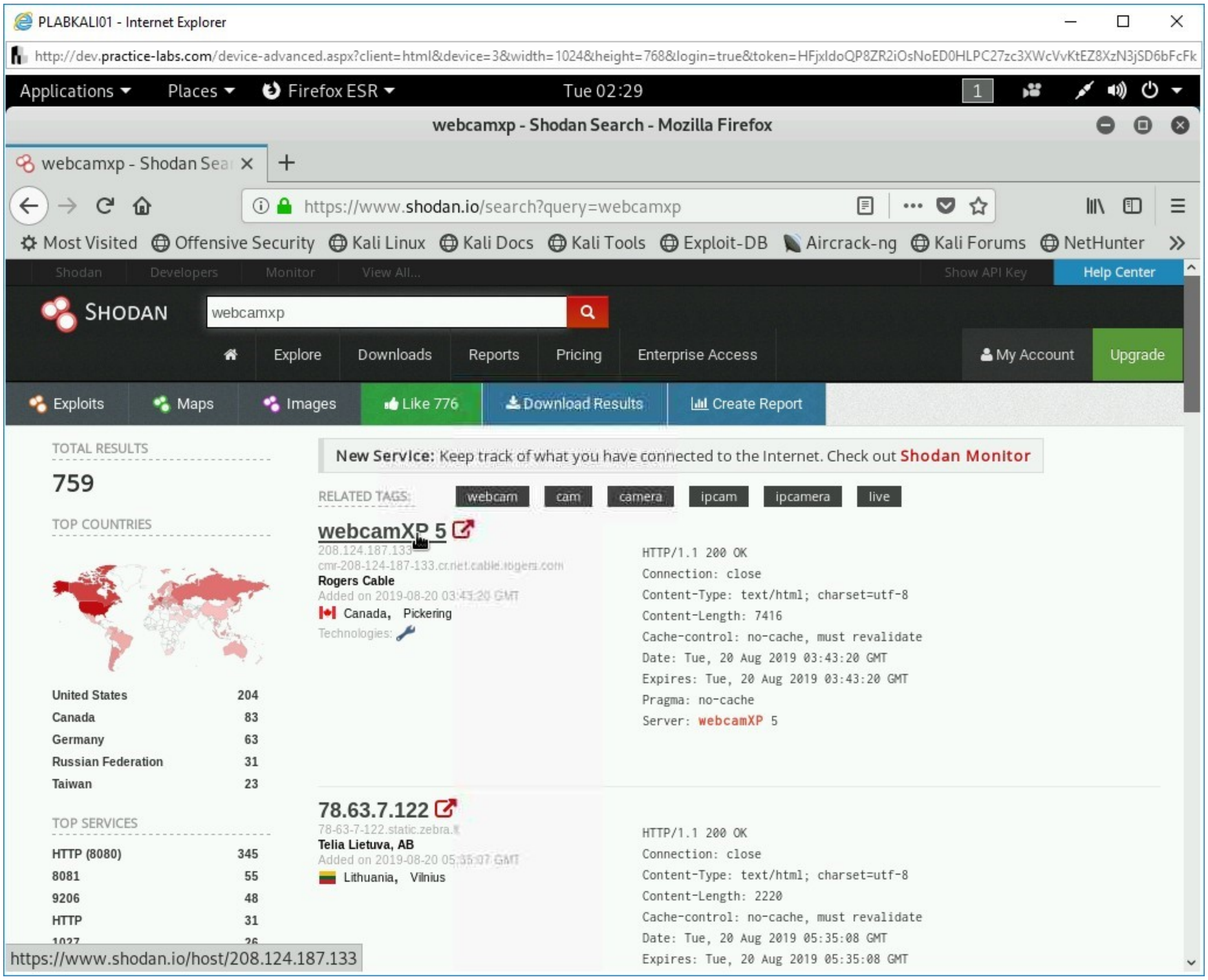
Ports: 5800

Services: 5800 tcp

Figure 3.28 Screenshot of PLABKALI01: Entering webcamxp in the search text box.

## Step 8

Select any of the search results.



**New Service:** Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

TOTAL RESULTS

759

TOP COUNTRIES

| | |
|---|---|
| United States | 204 |
| Canada | 83 |
| Germany | 63 |
| Russian Federation | 31 |
| Taiwan | 23 |

TOP SERVICES

| | |
|---|---|
| HTTP (8080) | 345 |
| 8081 | 55 |
| 9206 | 48 |
| HTTP | 31 |
| 1027 | 26 |

**webcamXP 5**
208.124.187.133
cmr-208-124-187-133.cr.net.cable.rogers.com
**Rogers Cable**
Added on 2019-08-20 03:43:20 GMT
Canada, Pickering
Technologies:

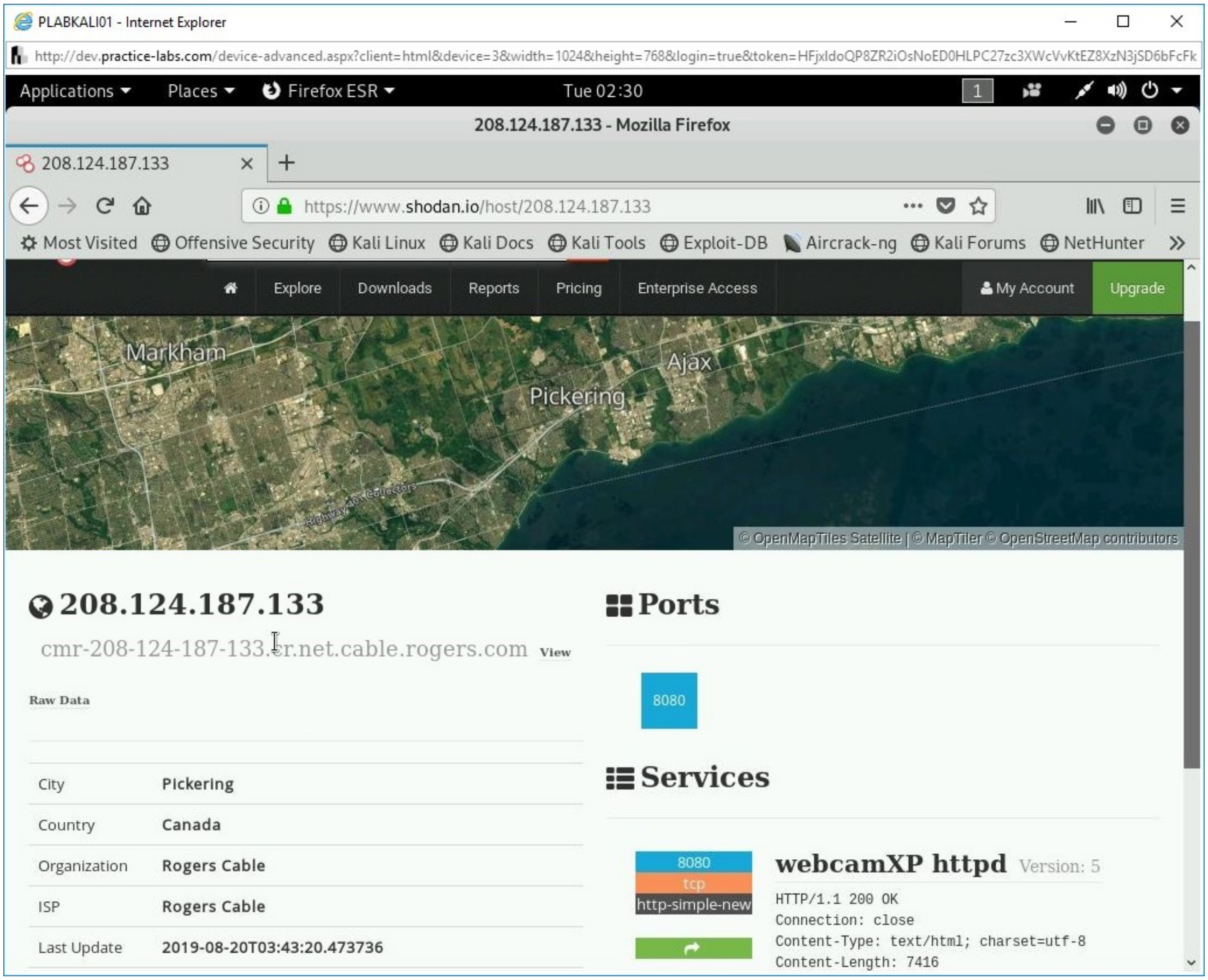
```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 7416
Cache-control: no-cache, must revalidate
Date: Tue, 20 Aug 2019 03:43:20 GMT
Expires: Tue, 20 Aug 2019 03:43:20 GMT
Pragma: no-cache
Server: webcamXP 5
```

**78.63.7.122**
78-63-7-122.static.zebra.lt
**Telia Lietuva, AB**
Added on 2019-08-20 05:35:07 GMT
Lithuania, Vilnius

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 2220
Cache-control: no-cache, must revalidate
Date: Tue, 20 Aug 2019 05:35:08 GMT
Expires: Tue, 20 Aug 2019 05:35:08 GMT
```

Figure 3.29 Screenshot of PLABKALI01: Showing the search results for the keyword webcamxp.

Notice that the detailed information about the search result is displayed. The right pane displays that there is one port open.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=HFjxldoQP8ZR2iOsNoED0HLPC27zc3XWcVvKtEZ8XzN3jSD6bFcFk
Applications
Places
Firefox ESR
Tue 02:30
208.124.187.133 - Mozilla Firefox
208.124.187.133
https://www.shodan.io/host/208.124.187.133
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Explore
Downloads
Reports
Pricing
Enterprise Access
My Account
Upgrade
Markham
Ajax
Pickering
© OpenMapTiles Satellite | © MapTiler © OpenStreetMap contributors
208.124.187.133
cmr-208-124-187-133.cr.net.cable.rogers.com
View
Raw Data
Ports
8080
Services
8080
tcp
http-simple-new
webcamXP httpd
Version: 5

| | |
|---|---|
| City | Pickering |
| Country | Canada |
| Organization | Rogers Cable |
| ISP | Rogers Cable |
| Last Update | 2019-08-20T03:43:20.473736 |

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 7416
```

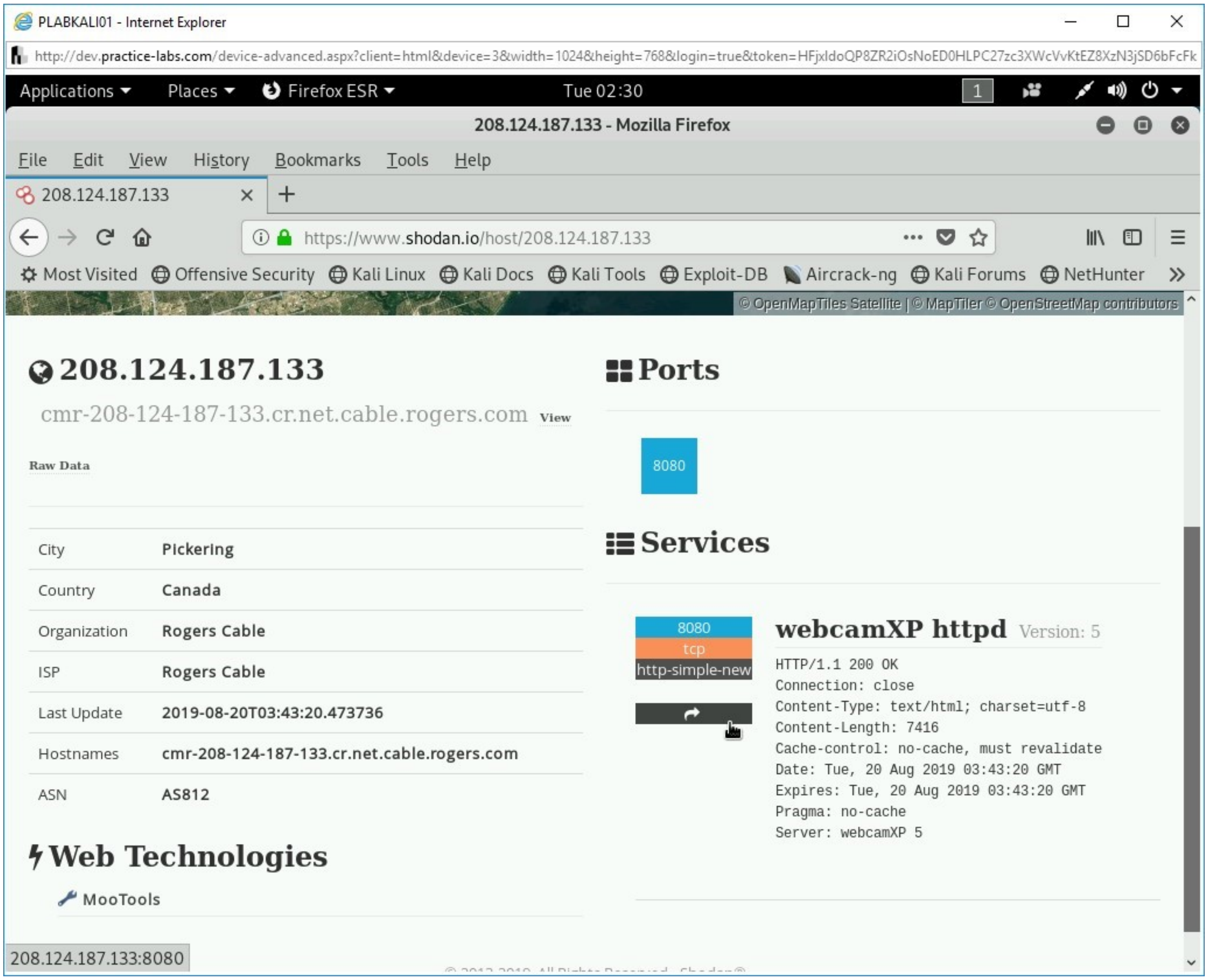
Figure 3.30 Screenshot of PLABKALI01: Showing the details of the search result.

## *Step 9*

Scroll down to the **webcamXP httpd** section in the right pane.

You will now navigate to a Webpage that will display the live feed of this webcam.

To the left of the **webcamXP httpd** section, click the rectangular **arrow button**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=HFjxldoQP8ZR2iOsNoED0HLPC27zc3XWcVvKtEZ8XzN3jSD6bFcFk
Applications
Places
Firefox ESR
Tue 02:30
1
208.124.187.133 - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
208.124.187.133
https://www.shodan.io/host/208.124.187.133
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
© OpenMapTiles Satellite | © MapTiler © OpenStreetMap contributors
208.124.187.133:8080

## 208.124.187.133

cmr-208-124-187-133.cr.net.cable.rogers.com View

Raw Data

| | |
|---|---|
| City | Pickering |
| Country | Canada |
| Organization | Rogers Cable |
| ISP | Rogers Cable |
| Last Update | 2019-08-20T03:43:20.473736 |
| Hostnames | cmr-208-124-187-133.cr.net.cable.rogers.com |
| ASN | AS812 |

## Web Technologies

MooTools

## Ports

8080

## Services

8080
tcp
http-simple-new

### webcamXP httpd Version: 5

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 7416
Cache-control: no-cache, must revalidate
Date: Tue, 20 Aug 2019 03:43:20 GMT
Expires: Tue, 20 Aug 2019 03:43:20 GMT
Pragma: no-cache
Server: webcamXP 5
```

Figure 3.31 Screenshot of PLABKALI01: Clicking the green rectangle with the white arrow in the webcamXP httpd section in the right pane.

A new tab opens. A live feed of the webcam is now being displayed.

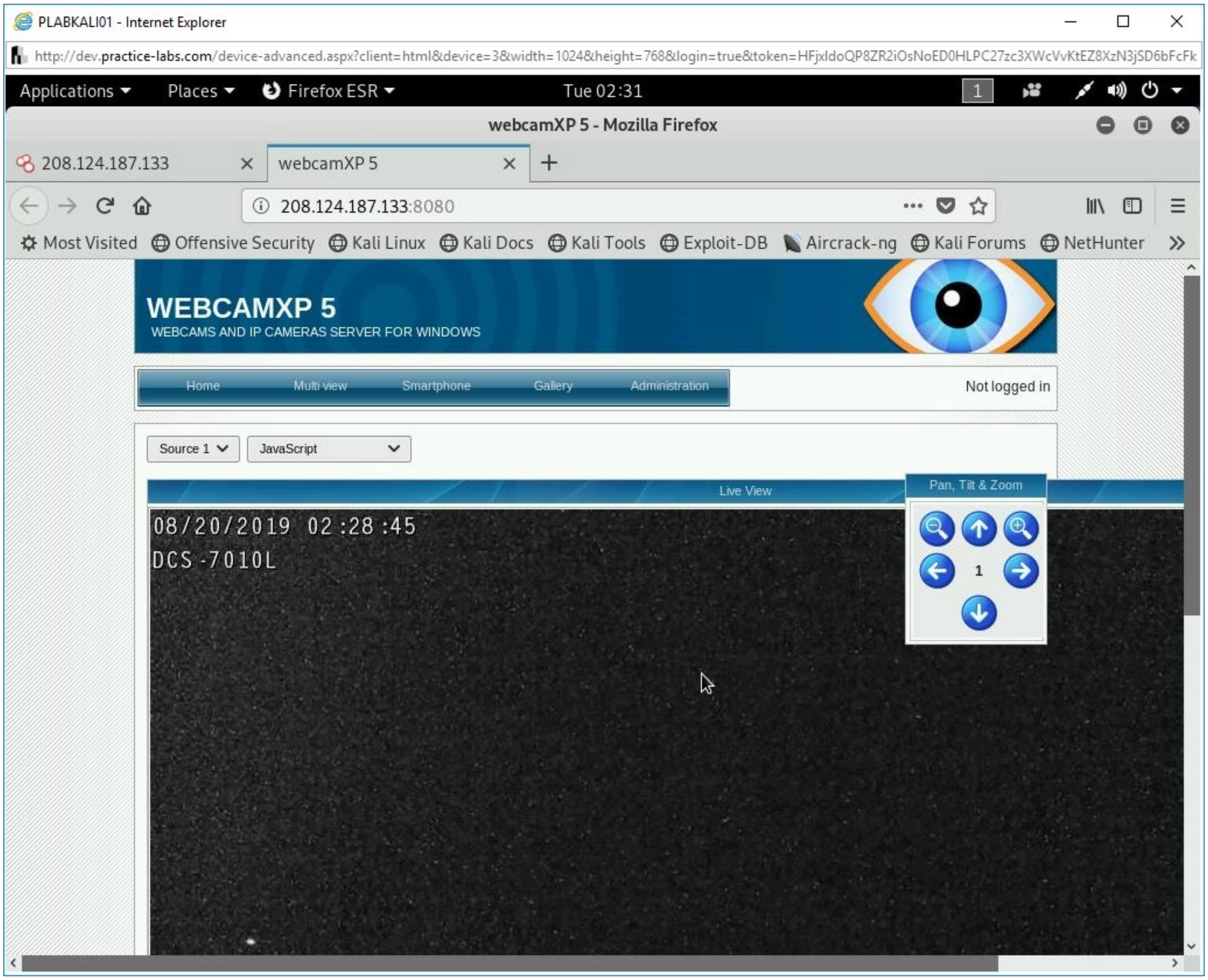


Figure 3.32 Screenshot of PLABKALI01: Showing the live feed on a new tab in Firefox.

Close the **Firefox** window.

## Task 4 - Use the Google Hacking Database

The Google Hacking Database (GHDB) is a database of queries that you can use to identify sensitive data.

GHDB provides some of the following information:

- Advisories
- Server vulnerabilities
- Error messages
- Files containing passwords
- Sensitive directories

- Pages containing login portals and network or vulnerability data

To use GHDB, perform the following steps:

## Step 1

Ensure you have powered the required devices specified in the introduction, then connect to **PLABWIN10**.

The desktop is displayed.

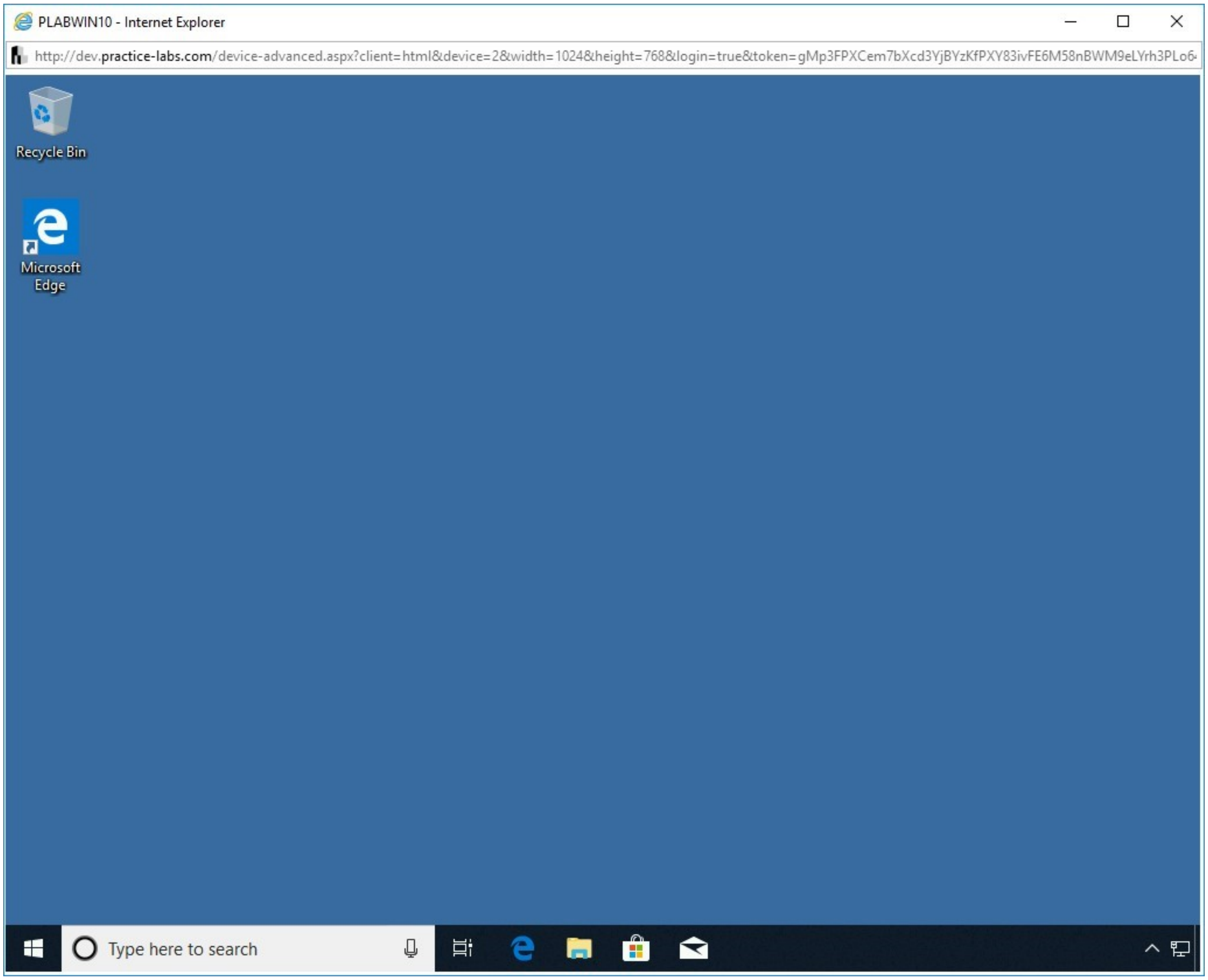
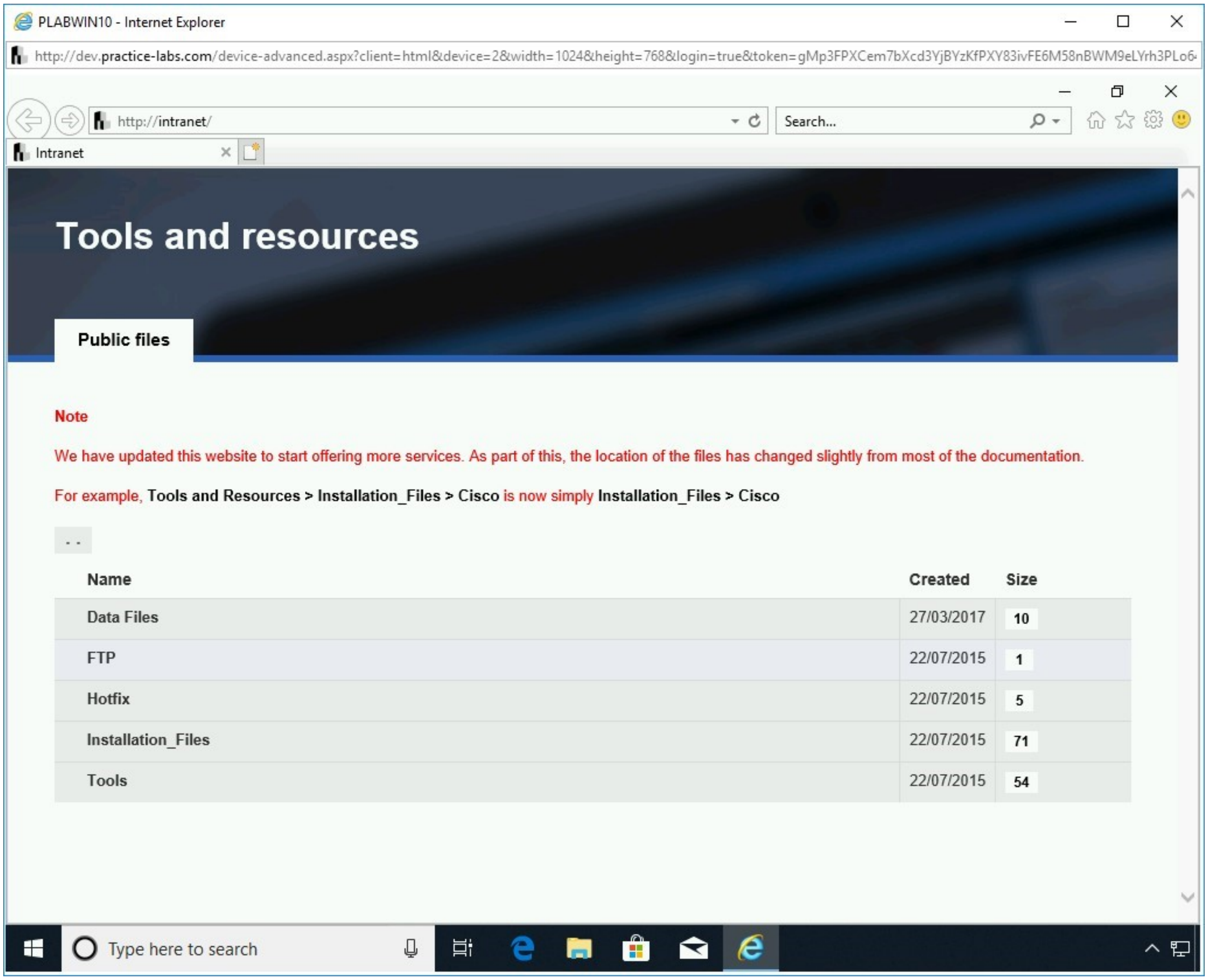

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=gMp3FPXCem7bXcd3YjBYzKfPXY83ivFE6M58nBWM9eLYrh3PLo6
Recycle Bin
Microsoft Edge
Type here to search

Figure 3.33 Screenshot of PLABWIN10: Showing the desktop with multiple icons.

## Step 2

Open **Internet Explorer**.

In the **Internet Explorer** window, the default homepage, which is the **Practice Labs Intranet**, is displayed.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=gMp3FPXCem7bXcd3YjBYzKfPXY83ivFE6M58nBWM9eLYrh3PLo6

http://intranet/

Tools and resources

Public files

Note

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

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

. .

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

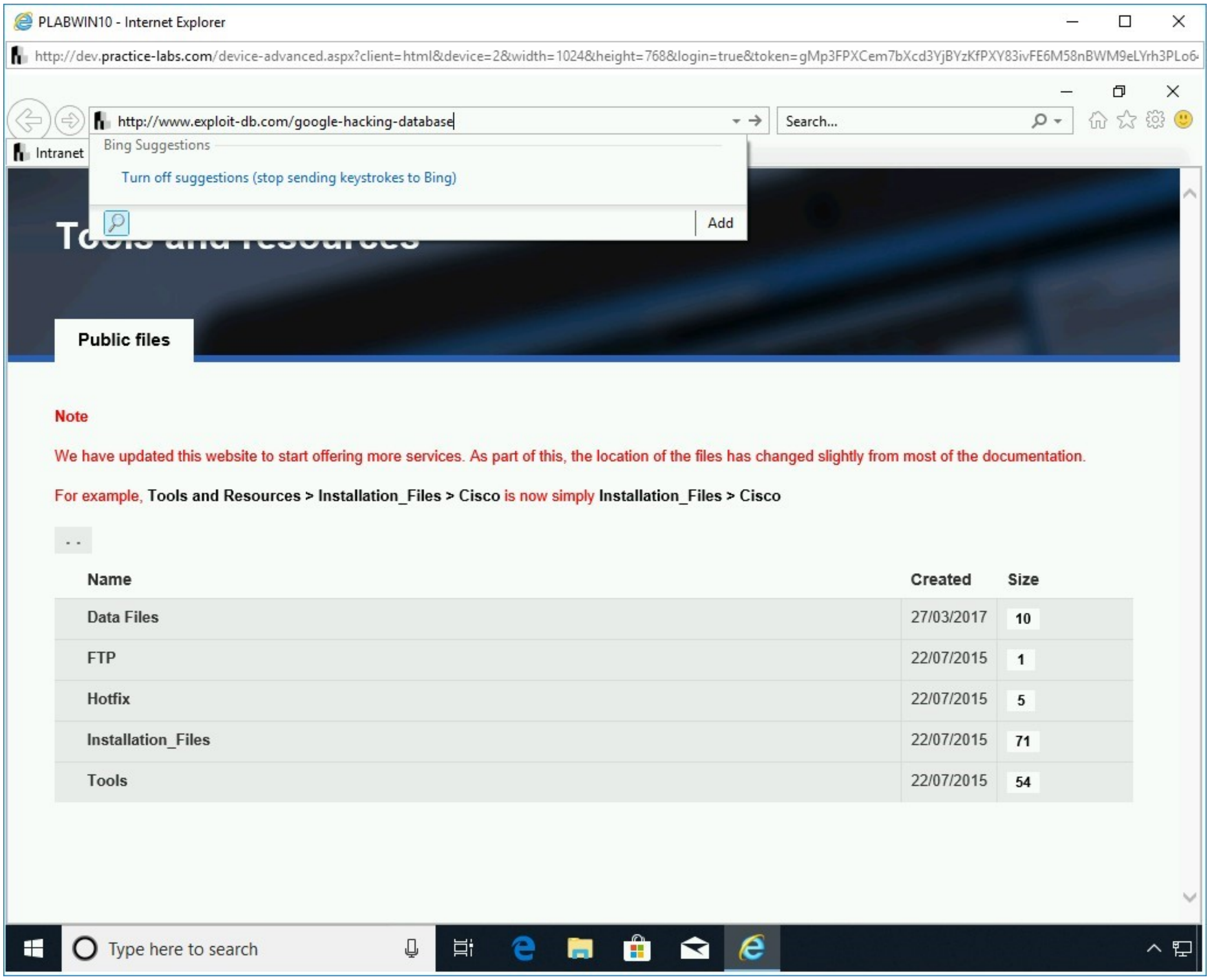
Figure 3.34 Screenshot of PLABWIN10: Showing the default home page of the intranet Website.

## *Step 3*

In the address bar, type the following URL:

```
http://www.exploit-db.com/google-hacking-database
```

Press **Enter**.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=gMp3FPXCem7bXcd3YjBYzKfPXY83ivFE6M58nBWM9eLYrh3PLo6

http://www.exploit-db.com/google-hacking-database

**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

. .

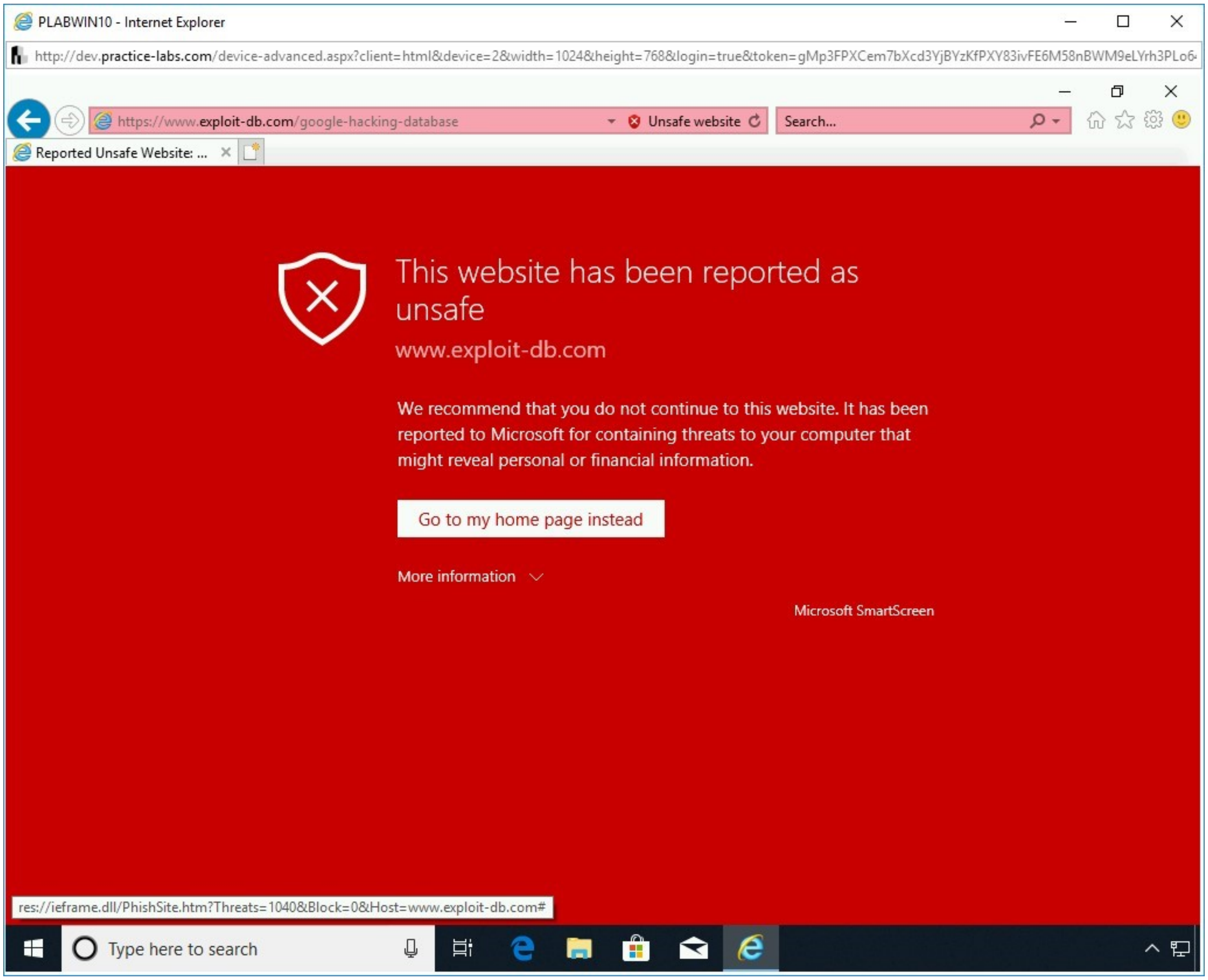
| Name | Created | Size |
|---|---|---|
| Data Files | 27/03/2017 | 10 |
| FTP | 22/07/2015 | 1 |
| Hotfix | 22/07/2015 | 5 |
| Installation_Files | 22/07/2015 | 71 |
| Tools | 22/07/2015 | 54 |

Figure 3.35 Screenshot of PLABWIN10: Typing the GHDB URL in the address bar.

## *Step 4*

You will be prompted with a **SmartScreen** warning.

Click the **More information** drop-down.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=gMp3FPXCem7bXcd3YjBYzKfPXY83ivFE6M58nBWM9eLYrh3PLo6
https://www.exploit-db.com/google-hacking-database
Unsafe website
Search...
Reported Unsafe Website: ...

This website has been reported as unsafe

www.exploit-db.com

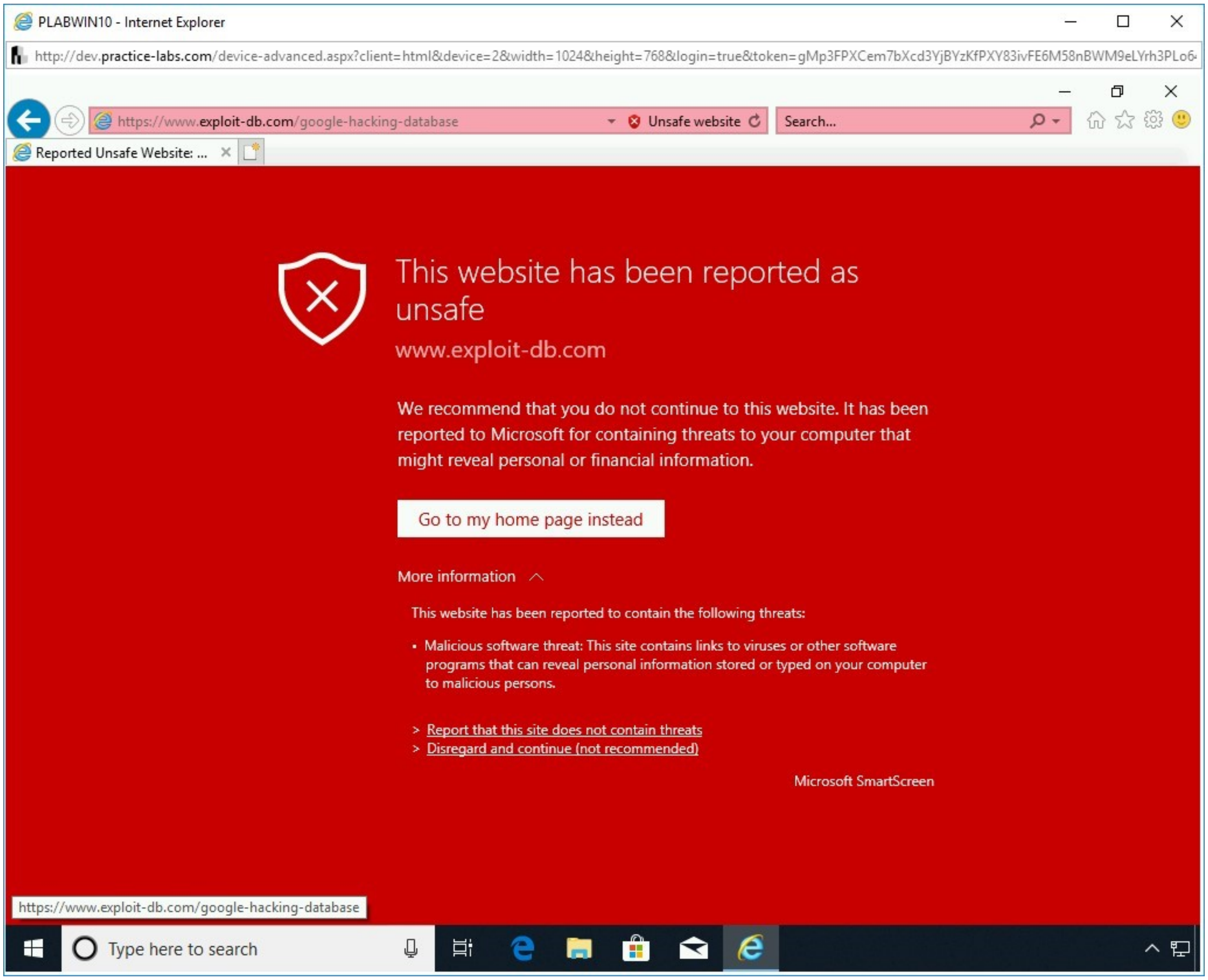
We recommend that you do not continue to this website. It has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.

Go to my home page instead
More information
Microsoft SmartScreen
res://ieframe.dll/PhishSite.htm?Threats=1040&Block=0&Host=www.exploit-db.com#
Type here to search

Figure 3.36 Screenshot of PLABWIN10: Showing the SmartScreen error screen.

## Step 5

Click **Disregard and continue (not recommended)**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=gMp3FPXCem7bXcd3YjBYzKfPXY83ivFE6M58nBWM9eLYrh3PLo6
https://www.exploit-db.com/google-hacking-database
Unsafe website
Search...
Reported Unsafe Website: ...
Go to my home page instead
https://www.exploit-db.com/google-hacking-database
Type here to search

This website has been reported as unsafe

www.exploit-db.com

We recommend that you do not continue to this website. It has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.

More information

This website has been reported to contain the following threats:

- Malicious software threat: This site contains links to viruses or other software programs that can reveal personal information stored or typed on your computer to malicious persons.

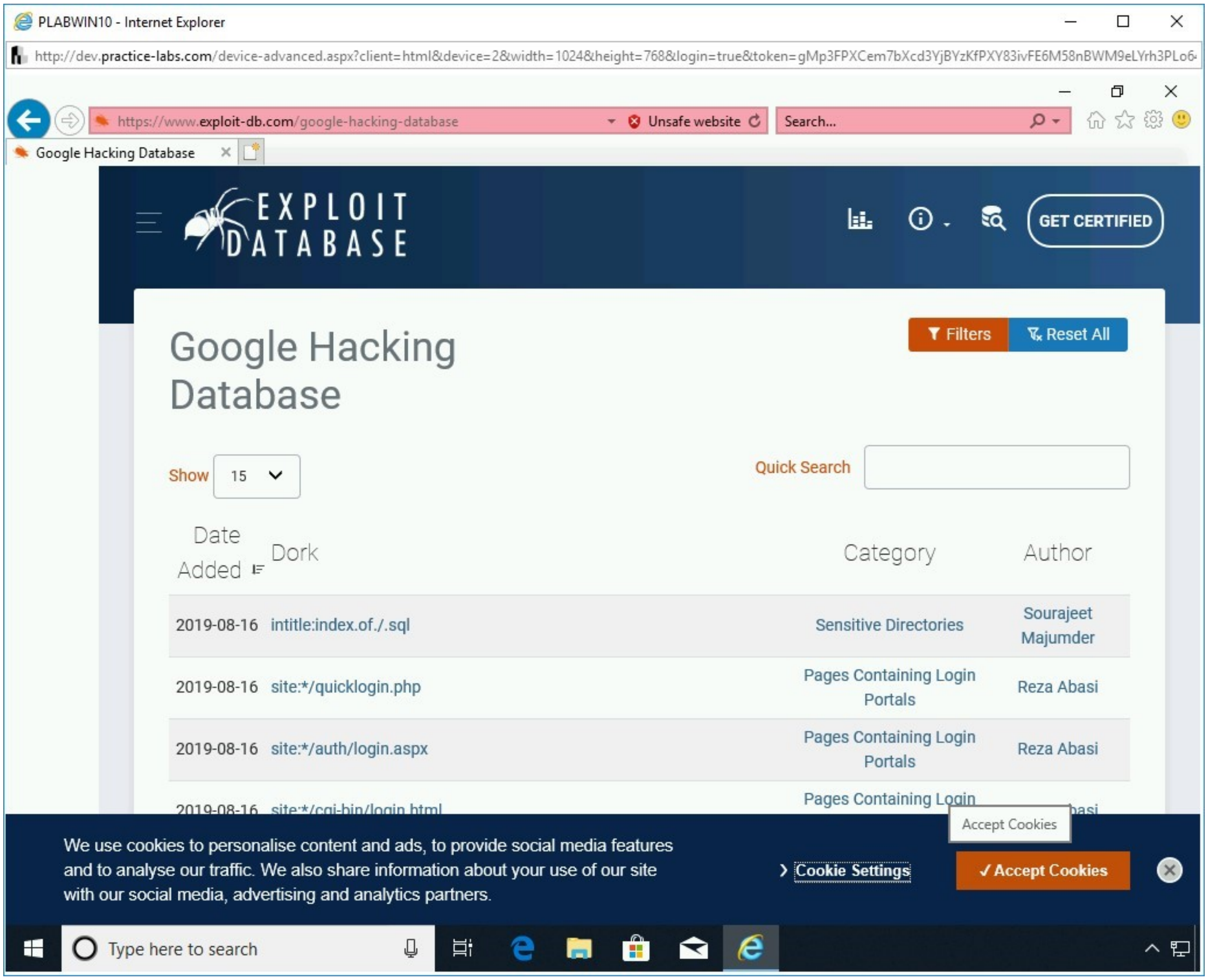
> Report that this site does not contain threats
> Disregard and continue (not recommended)

Microsoft SmartScreen

Figure 3.37 Screenshot of PLABWIN10: Clicking the Disregard and continue (not recommended) option.

## Step 6

When prompted with cookies notification, click **Accept Cookies**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=gMp3FPXCem7bXcd3YjBYzKfPXY83ivFE6M58nBWM9eLYrh3PLo6
https://www.exploit-db.com/google-hacking-database
Unsafe website
Search...
Google Hacking Database
EXPLOIT DATABASE
GET CERTIFIED
Filters
Reset All
Google Hacking Database
Show
15
Quick Search
Accept Cookies
Cookie Settings
✓Accept Cookies
Type here to search

| Date Added | Dork | Category | Author |
|---|---|---|---|
| 2019-08-16 | intitle:index.of./.sql | Sensitive Directories | Sourajeet Majumder |
| 2019-08-16 | site:*/quicklogin.php | Pages Containing Login Portals | Reza Abasi |
| 2019-08-16 | site:*/auth/login.aspx | Pages Containing Login Portals | Reza Abasi |
| 2019-08-16 | site:*/cgi-bin/login.html | Pages Containing Login | asi |

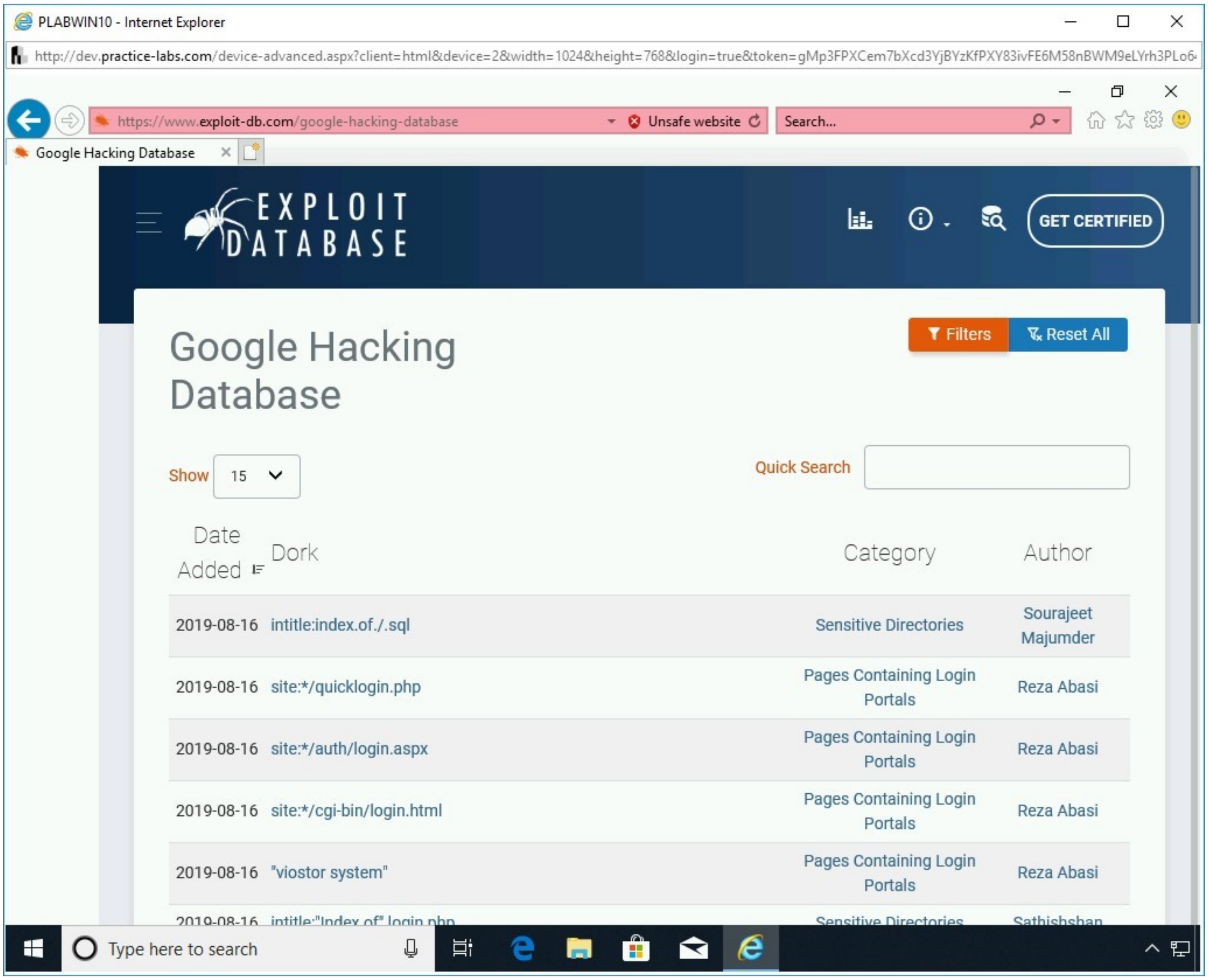
We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners.

Figure 3.38 Screenshot of PLABWIN10: Clicking Accept Cookies on the notification bar.

## *Step 7*

The **Google Hacking Database** Website is displayed.

Click the **Filters** button.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=gMp3FPXCem7bXcd3YjBYzKfPXY83ivFE6M58nBWM9eLYrh3PLo6
https://www.exploit-db.com/google-hacking-database
Unsafe website
Search...
Google Hacking Database
EXPLOIT DATABASE
GET CERTIFIED
Filters
Reset All
Type here to search

Google Hacking Database

Show 15

Quick Search

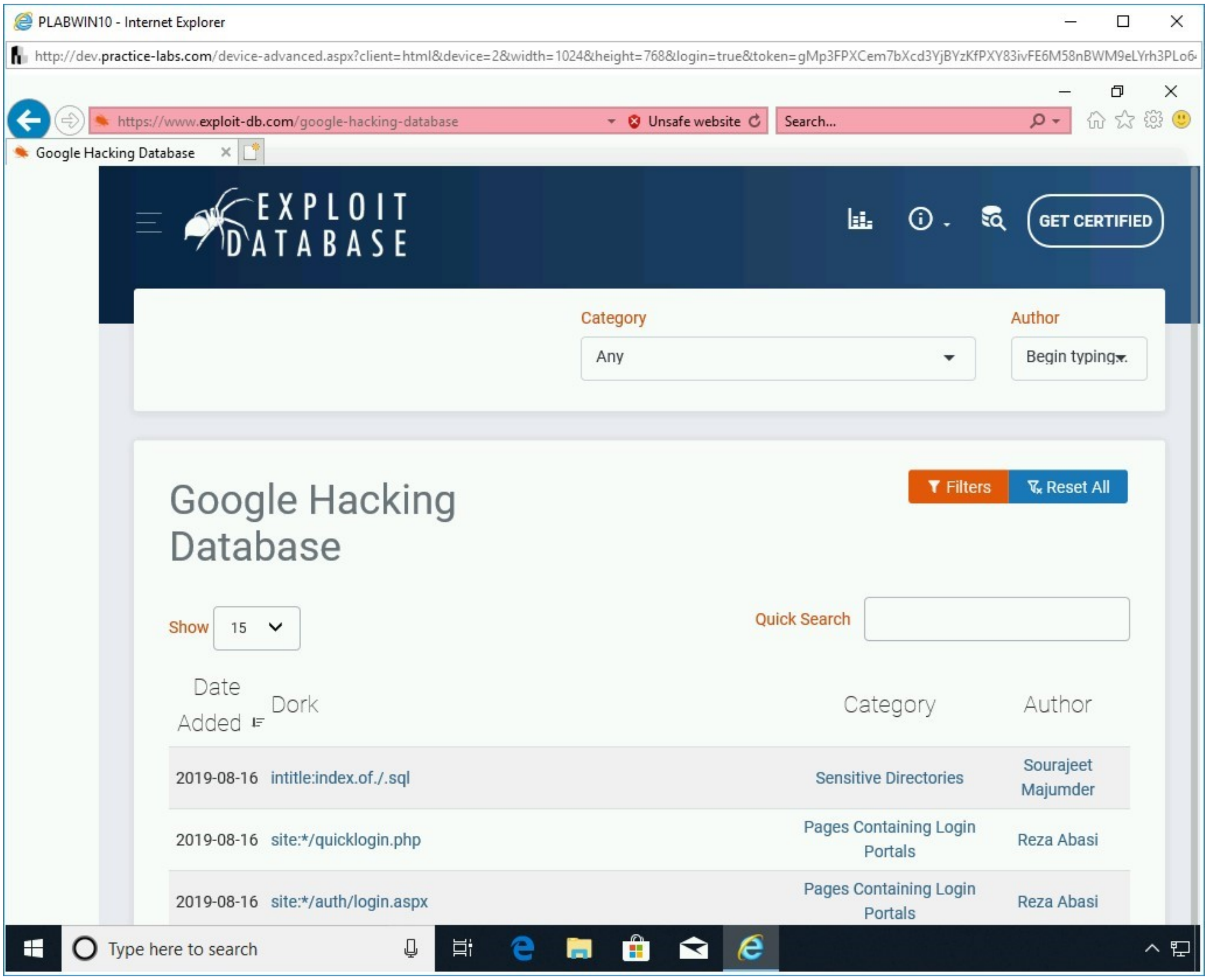
| Date Added | Dork | Category | Author |
|---|---|---|---|
| 2019-08-16 | intitle:index.of./.sql | Sensitive Directories | Sourajeet Majumder |
| 2019-08-16 | site:*/quicklogin.php | Pages Containing Login Portals | Reza Abasi |
| 2019-08-16 | site:*/auth/login.aspx | Pages Containing Login Portals | Reza Abasi |
| 2019-08-16 | site:*/cgi-bin/login.html | Pages Containing Login Portals | Reza Abasi |
| 2019-08-16 | "viostor system" | Pages Containing Login Portals | Reza Abasi |
| 2019-08-16 | intitle:"Index of" login.php | Sensitive Directories | Sathishshan |

Figure 3.39 Screenshot of PLABWIN10: Clicking Filters on the home page of the GHDB Website.

## *Step 8*

The **Category** and **Author** drop-down lists appear at the top of the Webpage.

Click the drop-down arrow in the **Category** drop-down box.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=gMp3FPXCem7bXcd3YjBYzKfPXY83ivFE6M58nBWM9eLYrh3PLo6
https://www.exploit-db.com/google-hacking-database
Unsafe website
Search...
Google Hacking Database
EXPLOIT DATABASE
GET CERTIFIED
Filters
Reset All
Type here to search

Google Hacking Database

Category: Any

Author: Begin typing...

Show 15

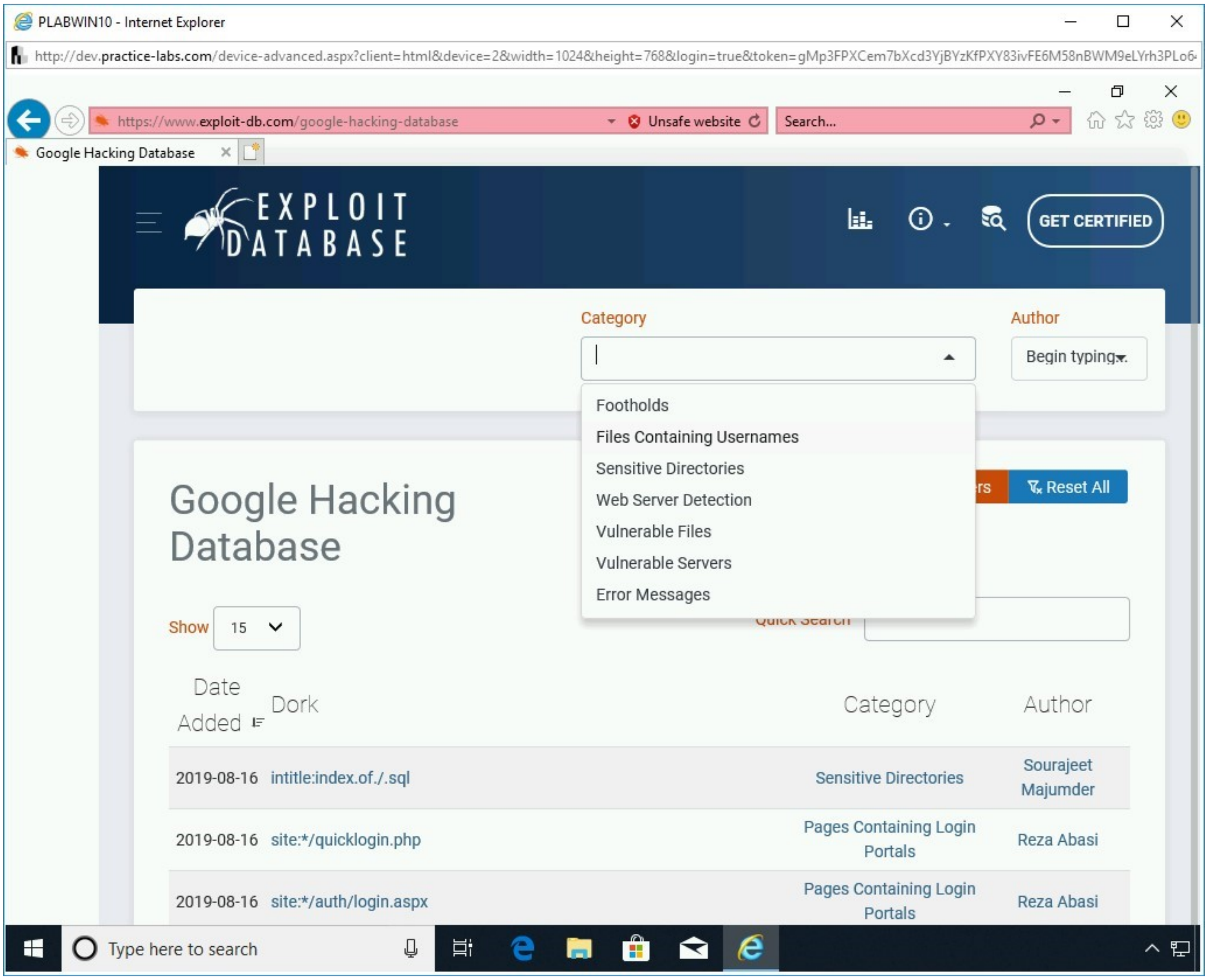
Quick Search

| Date Added | Dork | Category | Author |
|---|---|---|---|
| 2019-08-16 | intitle:index.of./.sql | Sensitive Directories | Sourajeet Majumder |
| 2019-08-16 | site:*/quicklogin.php | Pages Containing Login Portals | Reza Abasi |
| 2019-08-16 | site:*/auth/login.aspx | Pages Containing Login Portals | Reza Abasi |

Figure 3.40 Screenshot of PLABWIN10: Clicking the drop-down arrow on the Category drop-down box.

## Step 9

From the drop-down list, select **Files Containing Usernames**.



| Date Added | Dork | Category | Author |
|---|---|---|---|
| 2019-08-16 | intitle:index.of./.sql | Sensitive Directories | Sourajeet Majumder |
| 2019-08-16 | site:*/quicklogin.php | Pages Containing Login Portals | Reza Abasi |
| 2019-08-16 | site:*/auth/login.aspx | Pages Containing Login Portals | Reza Abasi |

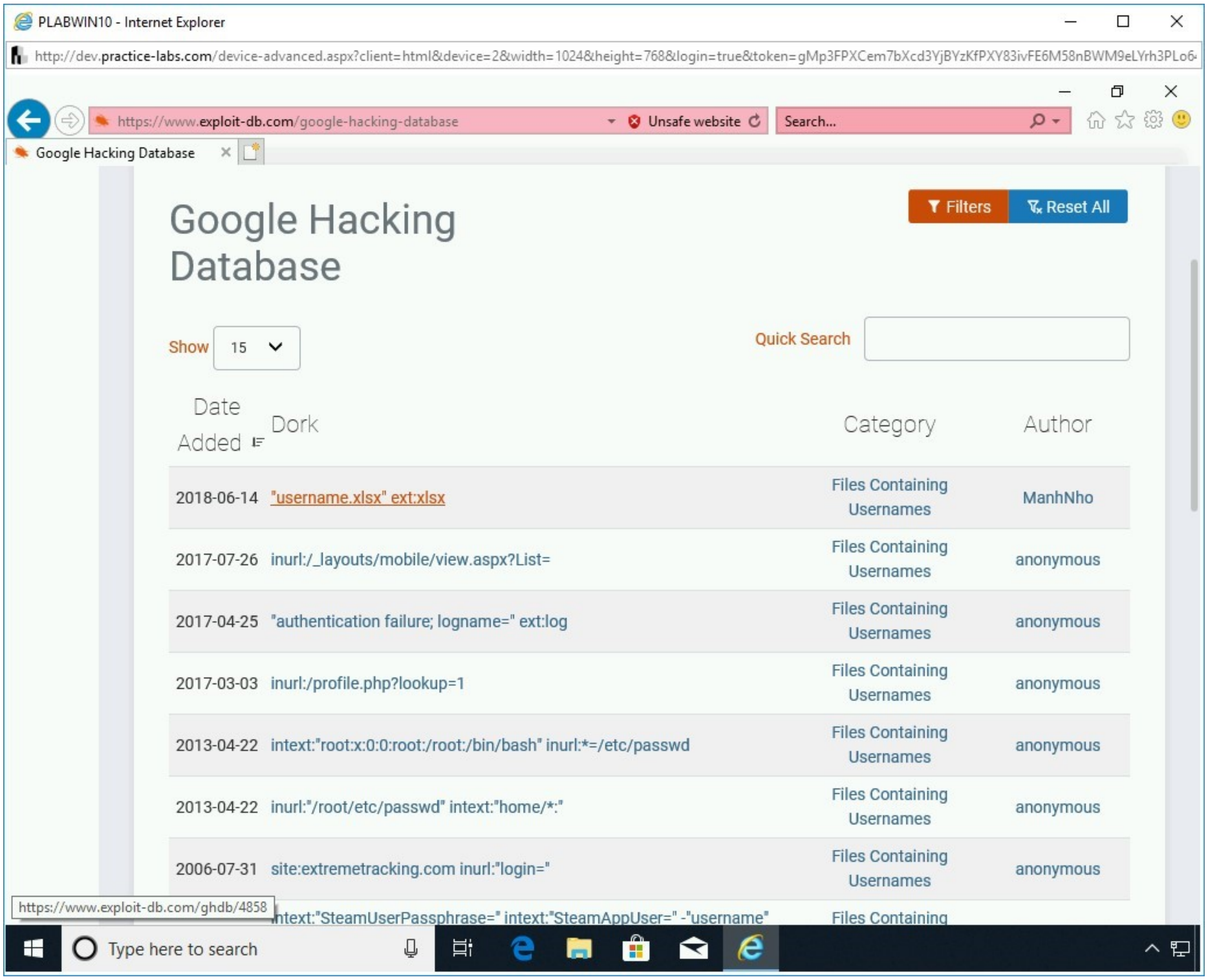
Figure 3.41 Screenshot of PLABWIN10: Selecting Files Containing Usernames from the Category drop-down list.

## *Step 10*

The search results are displayed.

Click any result that contains the filetype **xlsx**.

> ***Note**: The results shown below are likely to vary in your search results. You may have to scroll to the next pages to find such a result.*


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=gMp3FPXCem7bXcd3YjBYzKfPXY83ivFE6M58nBWM9eLYrh3PLo6
https://www.exploit-db.com/google-hacking-database
Unsafe website
Search...
Google Hacking Database
Filters
Reset All
Quick Search
Show 15
https://www.exploit-db.com/ghdb/4858
Type here to search

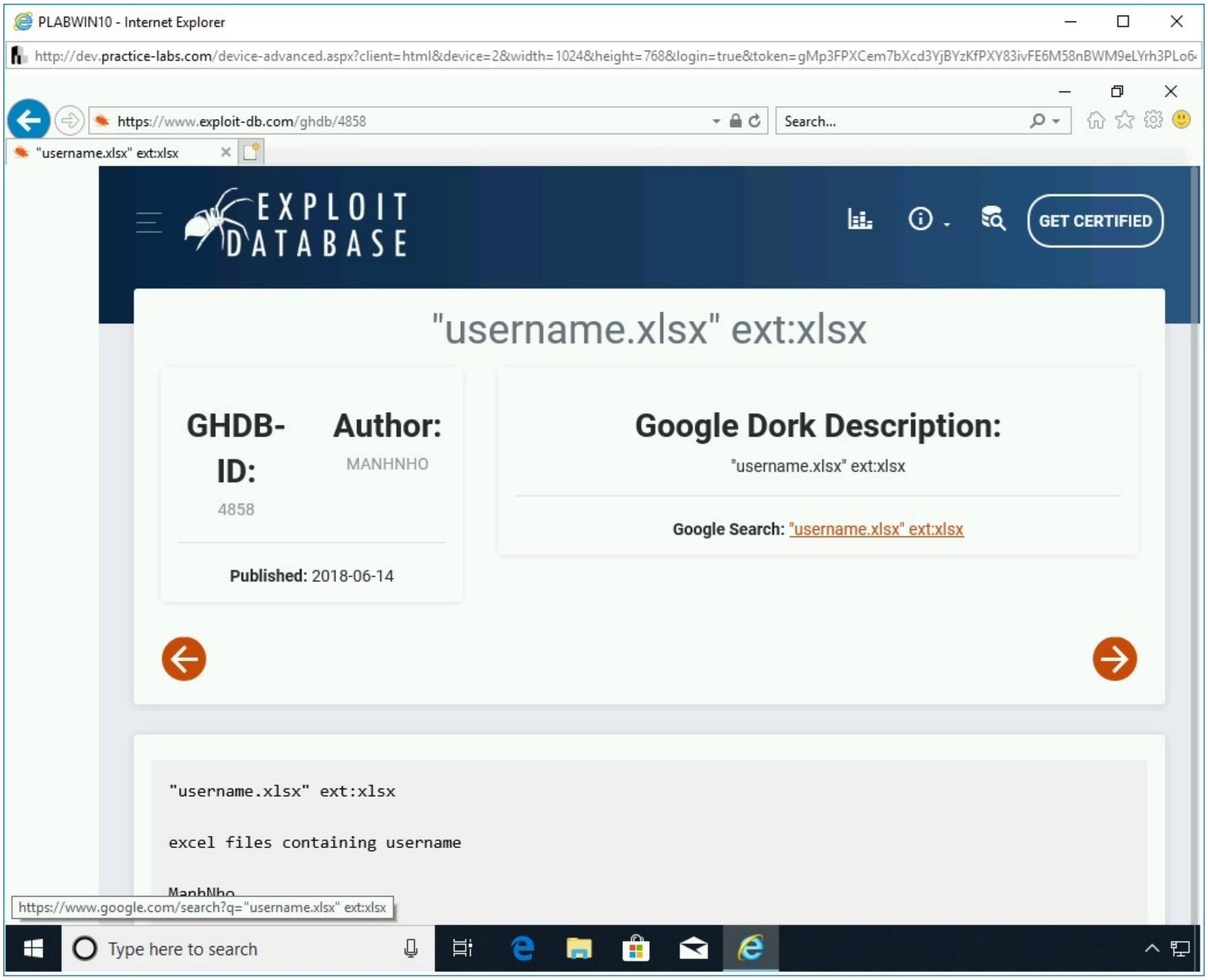
Google Hacking Database

| Date Added | Dork | Category | Author |
|---|---|---|---|
| 2018-06-14 | "username.xlsx" ext:xlsx | Files Containing Usernames | ManhNho |
| 2017-07-26 | inurl:/_layouts/mobile/view.aspx?List= | Files Containing Usernames | anonymous |
| 2017-04-25 | "authentication failure; logname=" ext:log | Files Containing Usernames | anonymous |
| 2017-03-03 | inurl:/profile.php?lookup=1 | Files Containing Usernames | anonymous |
| 2013-04-22 | intext:"root:x:0:0:root:/root:/bin/bash" inurl:*=/etc/passwd | Files Containing Usernames | anonymous |
| 2013-04-22 | inurl:"/root/etc/passwd" intext:"home/*:" | Files Containing Usernames | anonymous |
| 2006-07-31 | site:extremetracking.com inurl:"login=" | Files Containing Usernames | anonymous |
| | ntext:"SteamUserPassphrase=" intext:"SteamAppUser=" -"username" | Files Containing | |

Figure 3.42 Screenshot of PLABWIN10: Clicking the search result.

## Step 11

The result's information is displayed. Click on the link provided in the **Google Search** field.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=gMp3FPXCem7bXcd3YjBYzKfPXY83ivFE6M58nBWM9eLYrh3PLo6
https://www.exploit-db.com/ghdb/4858
Search...
"username.xlsx" ext:xlsx
EXPLOIT DATABASE
GET CERTIFIED

"username.xlsx" ext:xlsx

GHDB-ID: 4858

Author: MANHNHO

Published: 2018-06-14

Google Dork Description: "username.xlsx" ext:xlsx

Google Search: "username.xlsx" ext:xlsx

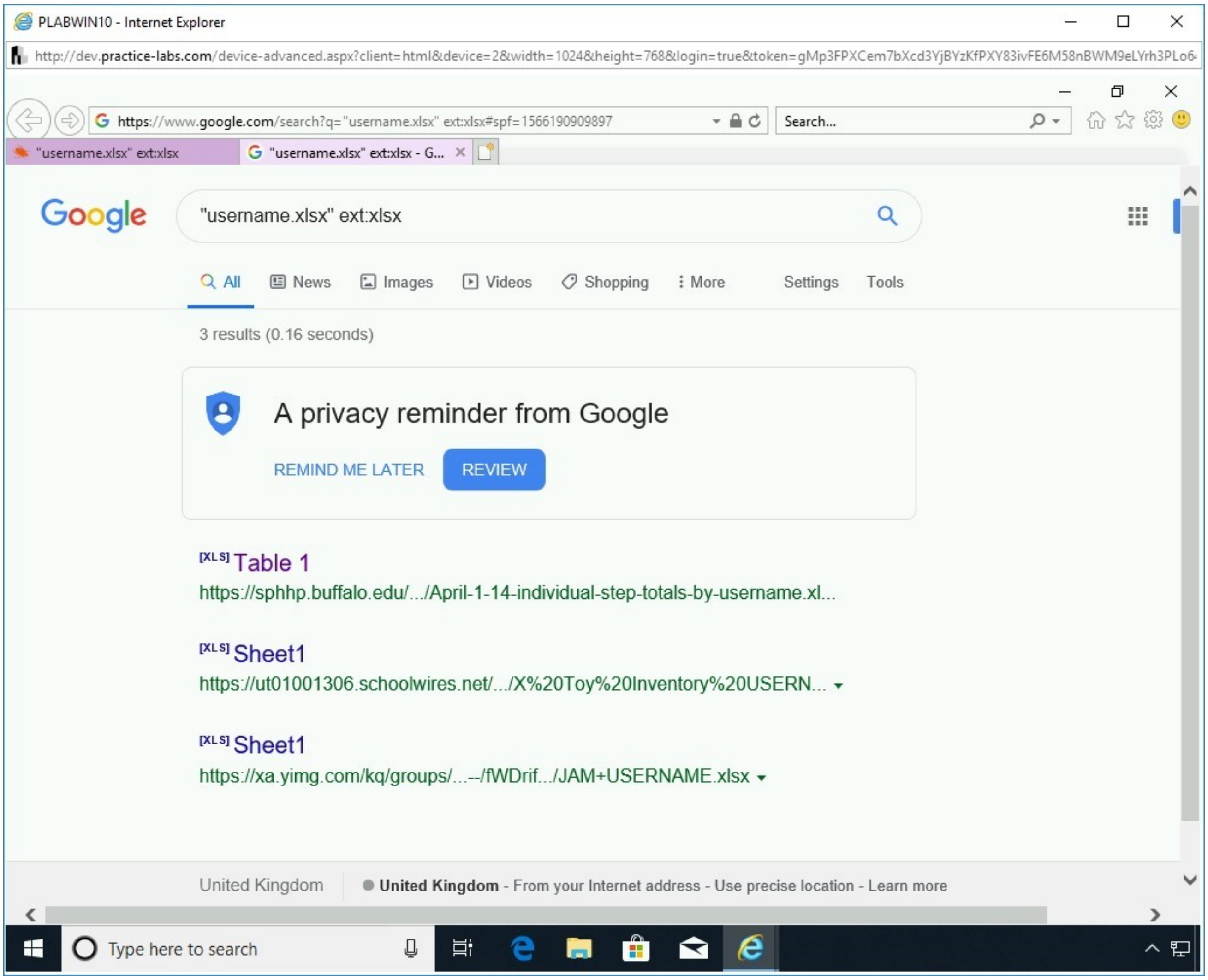
```
"username.xlsx" ext:xlsx

excel files containing username

ManhNho
```

https://www.google.com/search?q="username.xlsx" ext:xlsx
Type here to search

Figure 3.43 Screenshot of PLABWIN10: Clicking the link provided in the Google Search field.

A new tab is opened with a list of Websites that contain a file with the .xlsx extension. Each file contains a list of the user information.

You can download and read any of the .xlsx files.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=gMp3FPXCem7bXcd3YjBYzKfPXY83ivFE6M58nBWM9eLYrh3PLo6
https://www.google.com/search?q="username.xlsx" ext:xlsx#spf=1566190909897
Search...
"username.xlsx" ext:xlsx
"username.xlsx" ext:xlsx - G...
Google
All
News
Images
Videos
Shopping
More
Settings
Tools
REMIND ME LATER
REVIEW
United Kingdom
United Kingdom - From your Internet address - Use precise location - Learn more
Type here to search

"username.xlsx" ext:xlsx

3 results (0.16 seconds)

A privacy reminder from Google

[XLS] Table 1
https://sphhp.buffalo.edu/.../April-1-14-individual-step-totals-by-username.xl...

[XLS] Sheet1
https://ut01001306.schoolwires.net/.../X%20Toy%20Inventory%20USERN...

[XLS] Sheet1
https://xa.yimg.com/kq/groups/...-/fWDrif.../JAM+USERNAME.xlsx

Figure 3.44 Screenshot of PLABWIN10: Showing the results of the search of the username files.

## Task 5 - Perform DNS Querying

nslookup is a network administration command-line tool that is primarily used to query the Domain Name System (DNS). Using this tool, you can obtain the domain name or IP address mapping.

To use nslookup, perform the following steps:

### *Step 1*

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

On the desktop, click **Terminal**.

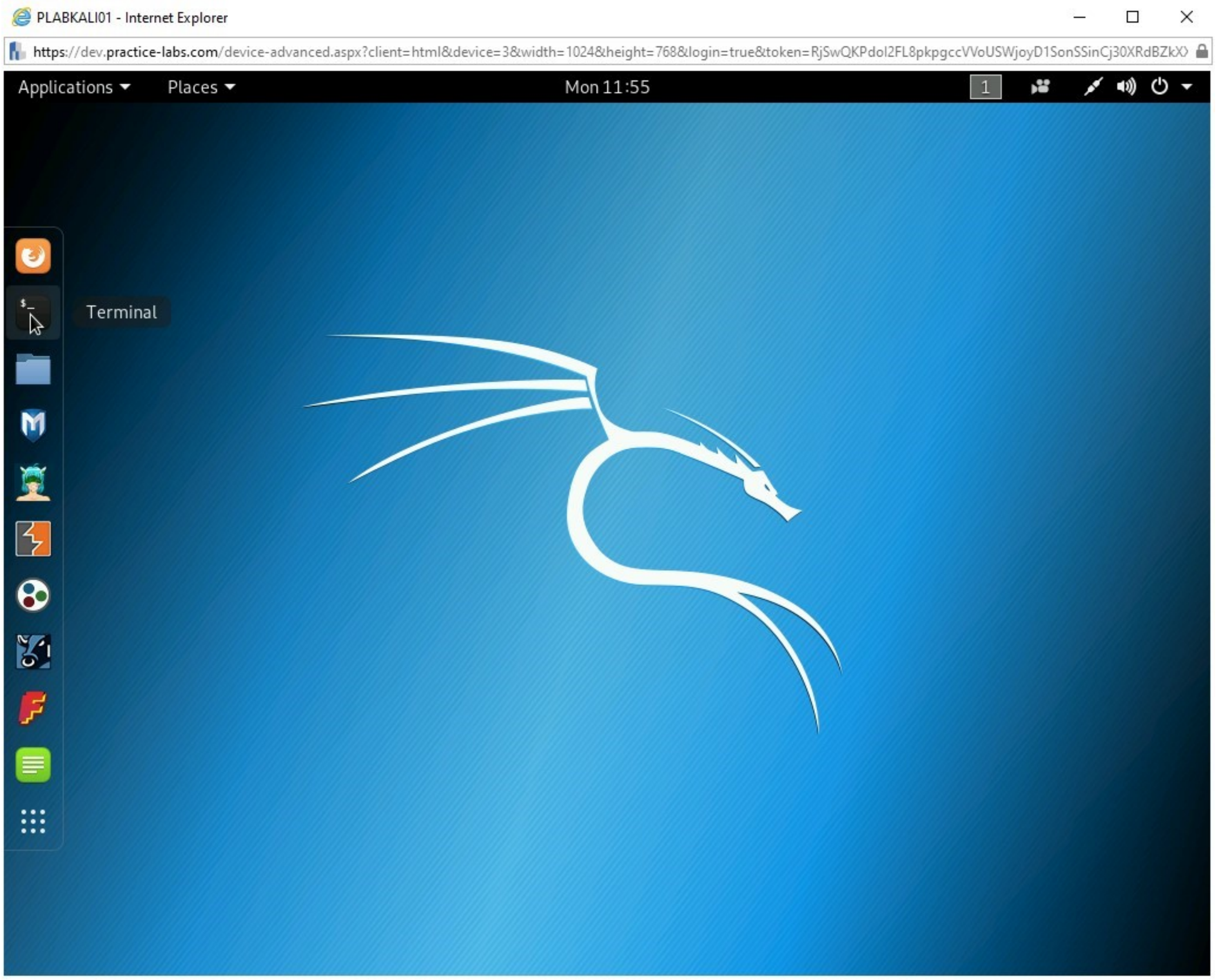

PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Mon 11:55
1
Terminal

Figure 3.45 Screenshot of PLABKALI01: Clicking the Terminal icon in the left toolbar.

## Step 2

The terminal window is displayed. Enter the following command:

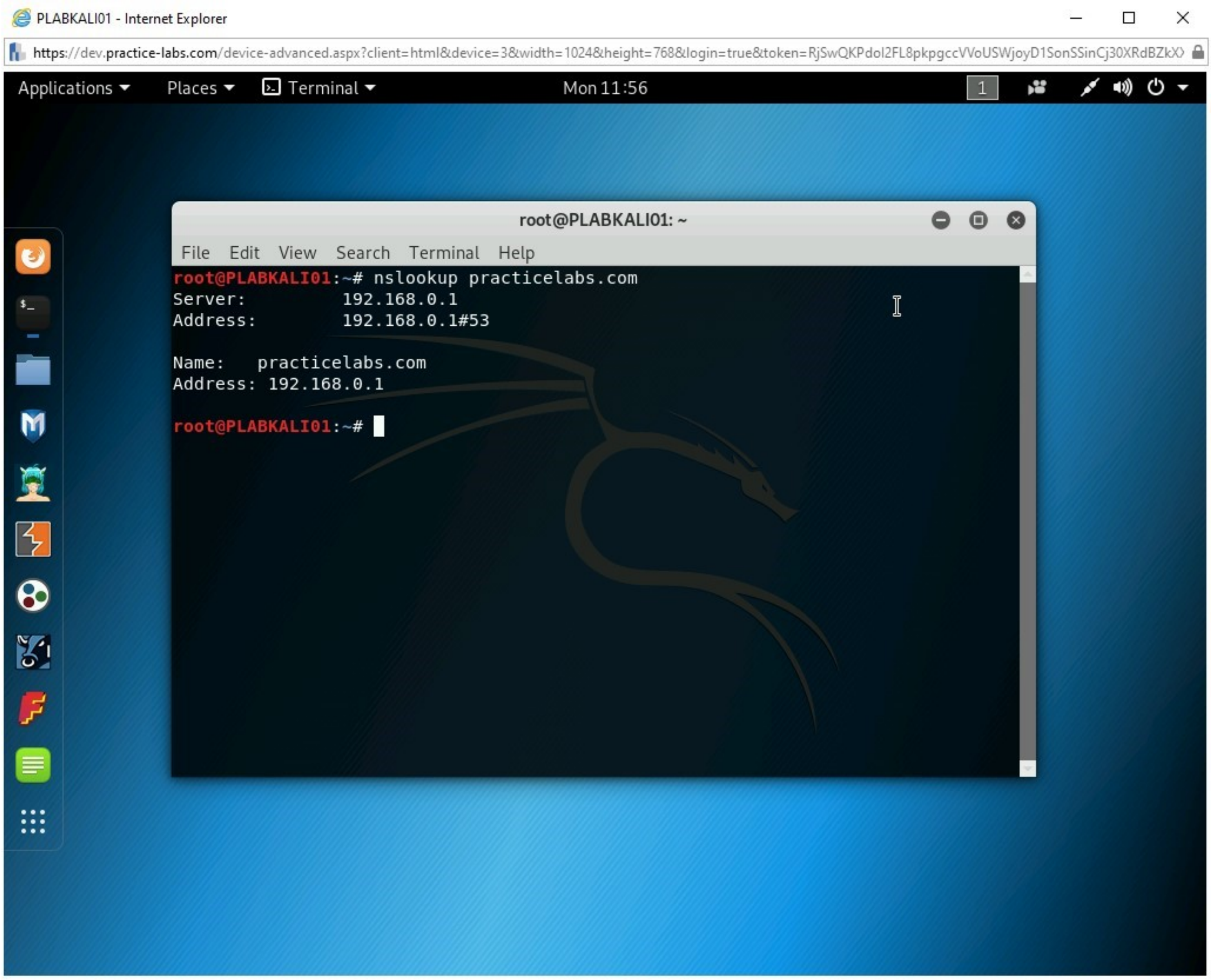
```
nslookup practicelabs.com
```

Press **Enter**.

Note that the IP address for the domain, practicelabs.com, is displayed. The first two lines of output specify the server to which the request was directed. This is the default server for DNS name resolution. The second section provides the name of the record and its corresponding IP address.

In this example, the DNS server is **192.168.0.1**. The record for **practicelabs.com** is also mapped to the same IP address, **192.168.0.1**.

In a real-world scenario, you are likely to find that both results have different IP addresses.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:56
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# nslookup practicelabs.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Name:   practicelabs.com
Address: 192.168.0.1

root@PLABKALI01:~# 
```

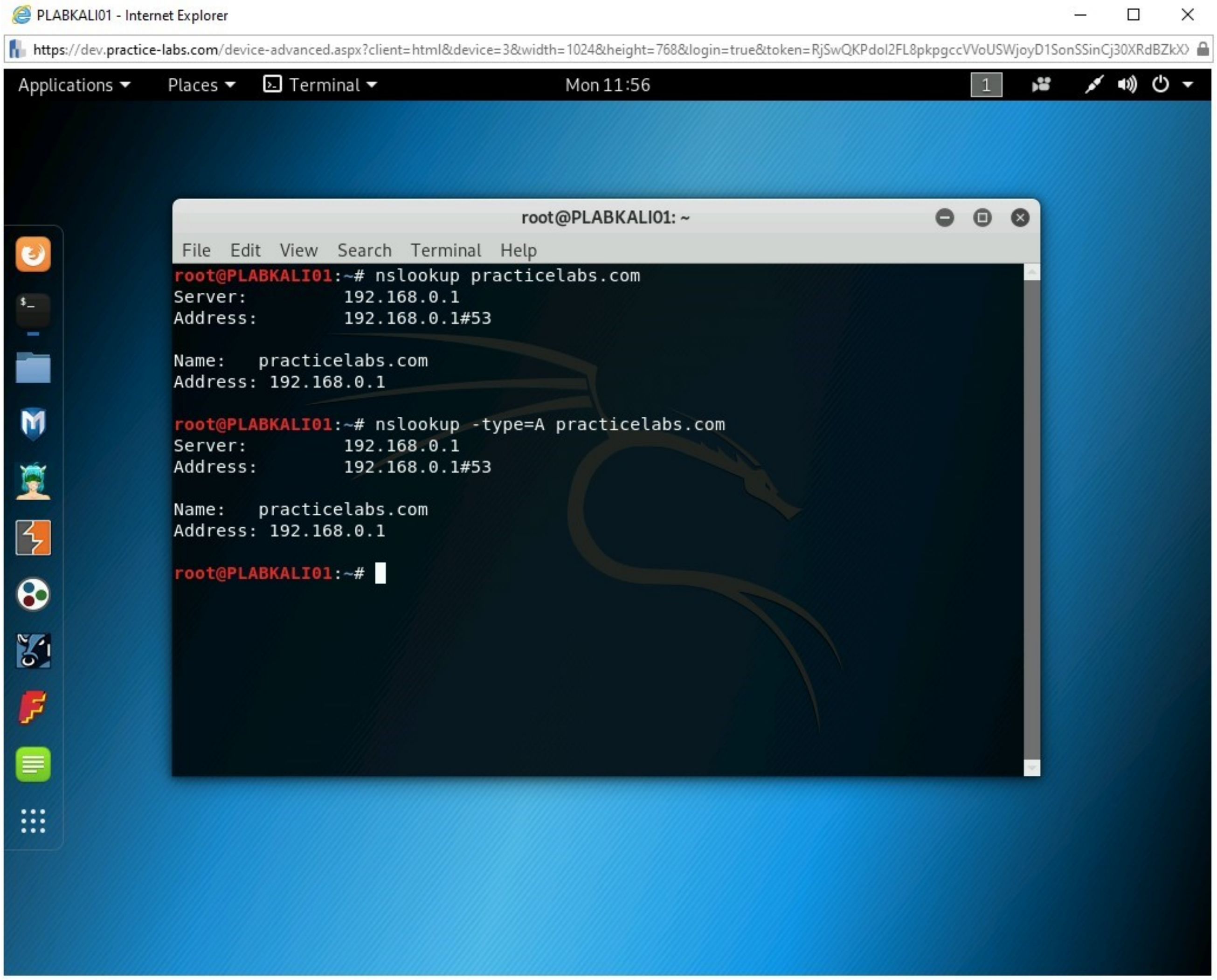
Figure 3.46 Screenshot of PLABKALI01: Showing the results of the nslookup command.

## *Step 3*

You can also check for a specific record. For example, to check for any **A** (Address) records for **practicelabs.com**, type the following command:

```
nslookup -type=A practicelabs.com
```

Press **Enter**.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:56
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# nslookup practicelabs.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Name:   practicelabs.com
Address: 192.168.0.1

root@PLABKALI01:~# nslookup -type=A practicelabs.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Name:   practicelabs.com
Address: 192.168.0.1

root@PLABKALI01:~# 
```

Figure 3.47 Screenshot of PLABKALI01: Showing the result of the nslookup command for the A records of the specified domain.

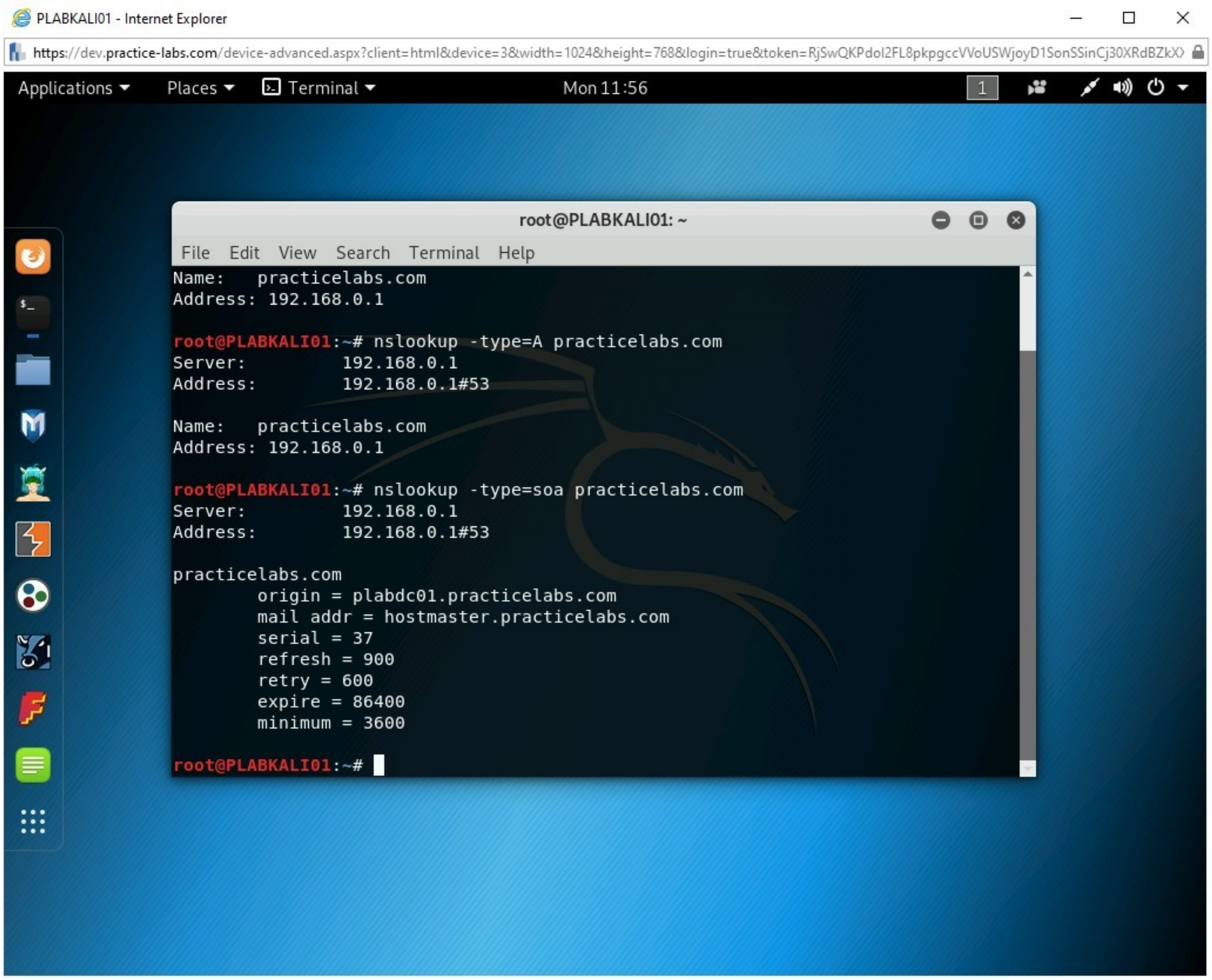
## Step 4

You can use the **-type=soa** option to tell **nslookup** to display the authoritative (primary) name server.

Type the following command:

```
nslookup -type=soa practicelabs.com
```

Press **Enter**.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=RjSwQKPdol2FL8pkpgccVVoUSWjoyD1SonSSinCj30XRdBZkX
Applications
Places
Terminal
Mon 11:56
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
Name:   practicelabs.com
Address: 192.168.0.1

root@PLABKALI01:~# nslookup -type=A practicelabs.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Name:   practicelabs.com
Address: 192.168.0.1

root@PLABKALI01:~# nslookup -type=soa practicelabs.com
Server:         192.168.0.1
Address:        192.168.0.1#53

practicelabs.com
        origin = plabdc01.practicelabs.com
        mail addr = hostmaster.practicelabs.com
        serial = 37
        refresh = 900
        retry = 600
        expire = 86400
        minimum = 3600

root@PLABKALI01:~#
```

Figure 3.48 Screenshot of PLABKALI01: Showing the result of the nslookup -type=soa command.

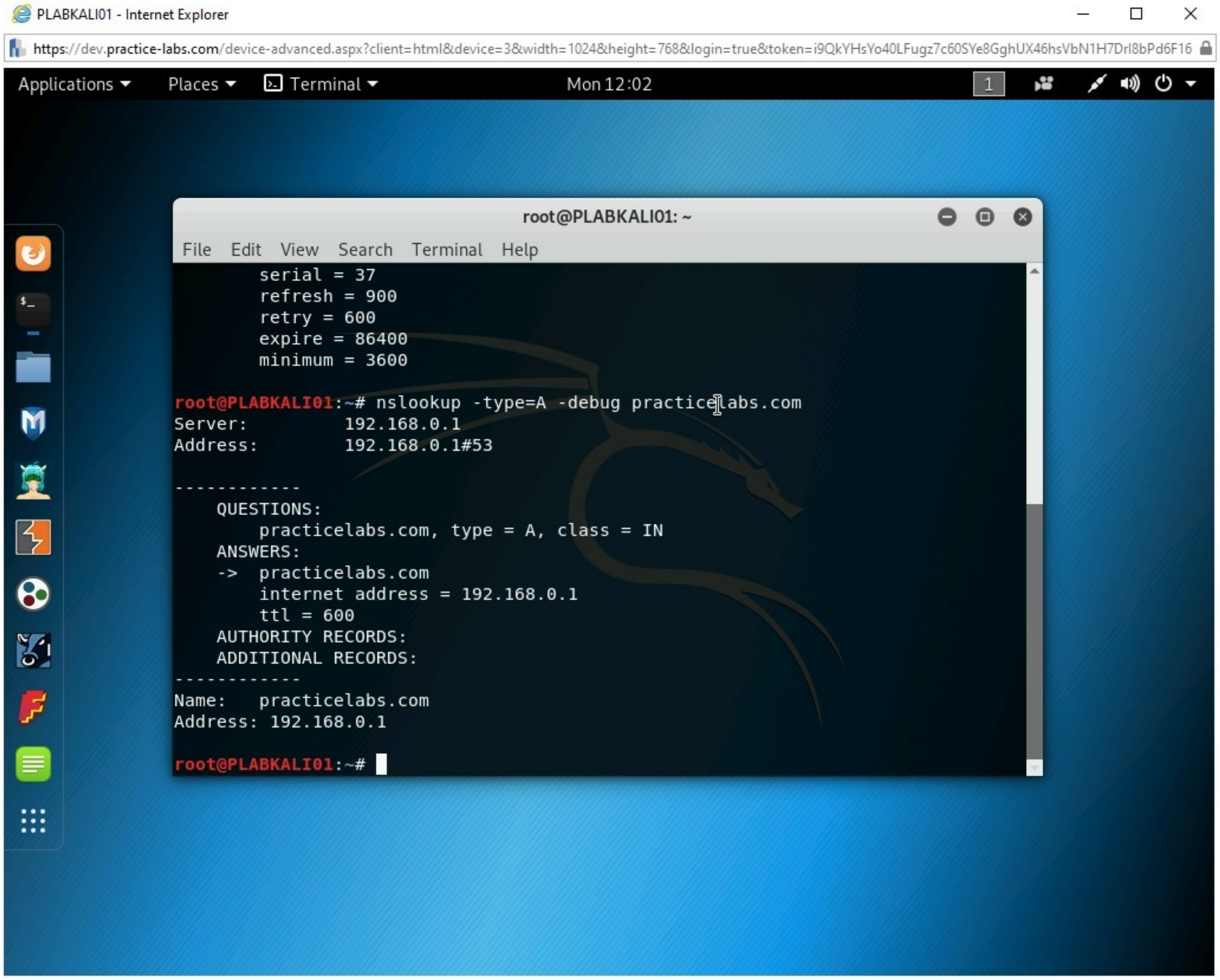
## Step 5

You can also verify how long a record is cached using the debug parameter.

Type the following command:

```
nslookup -type=A -debug practicelabs.com
```

Press **Enter**.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=i9QkYHsYo40LFugz7c60SYe8GghUX46hsVbN1H7Drl8bPd6F16
Applications
Places
Terminal
Mon 12:02
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
        serial = 37
        refresh = 900
        retry = 600
        expire = 86400
        minimum = 3600

root@PLABKALI01:~# nslookup -type=A -debug practicelabs.com
Server:         192.168.0.1
Address:        192.168.0.1#53

------------
    QUESTIONS:
        practicelabs.com, type = A, class = IN
    ANSWERS:
    ->  practicelabs.com
        internet address = 192.168.0.1
        ttl = 600
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Name:   practicelabs.com
Address: 192.168.0.1

root@PLABKALI01:~#
```

Figure 3.49 Screenshot of PLABKALI01: Showing the result of the nslookup -type=A command with the debug parameter.

Note that there is no indication of when the records are going to expire. However, if you attempt to execute this command on a live server on the Internet, you will get that information. The internal server does not provide complete details.

## *Step 6*

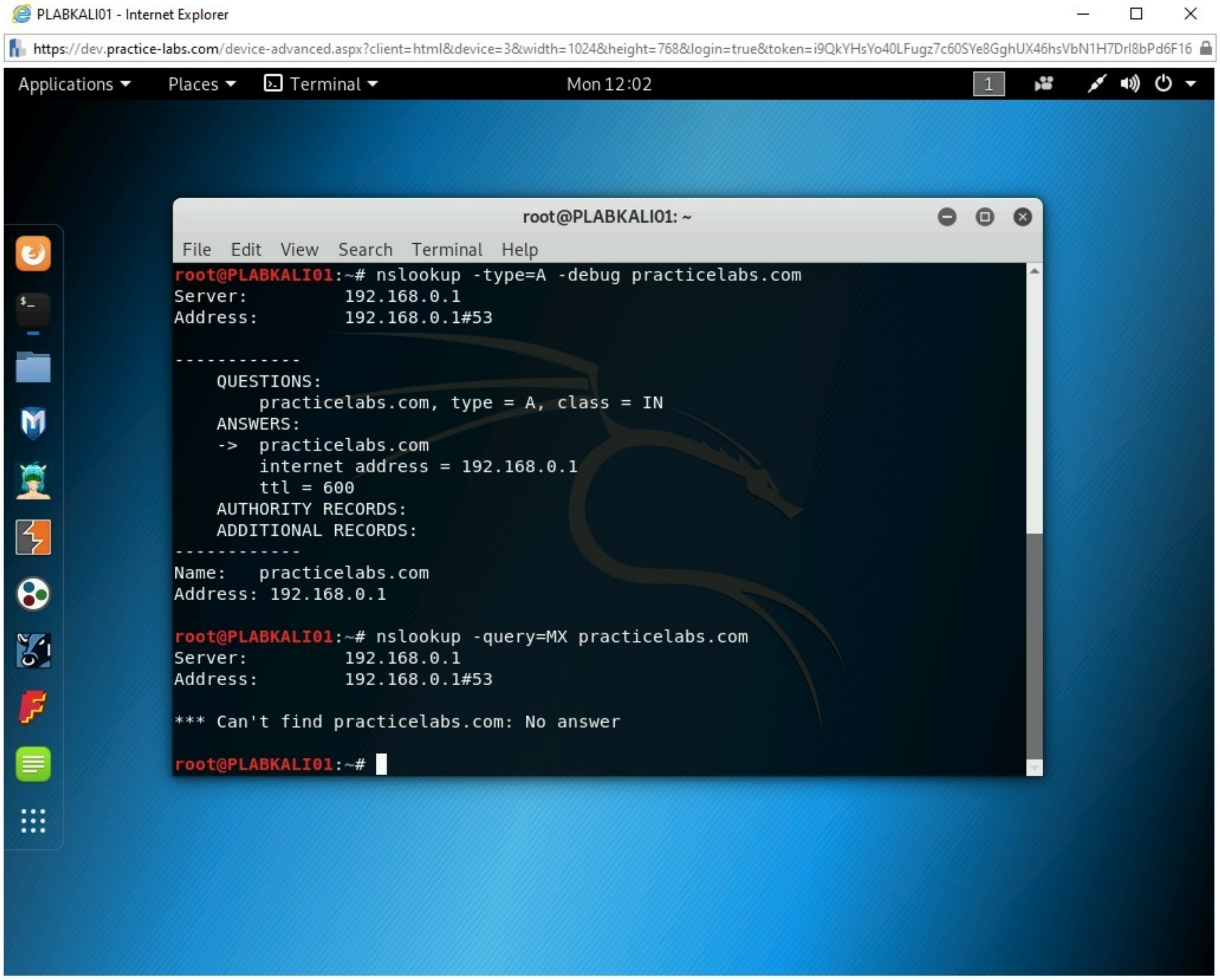
You can also use the **MX** record to map a domain name to a list of mail exchange servers for that domain. For example, the **MX** record provides the details of the mail server to which all the E-mails are sent for the **practicelabs.com** domain.

Type the following command:

```
nslookup -query=MX practicelabs.com
```

Press **Enter**.

Since there is no mail server for this domain, notice that this command fails.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=i9QkYHsYo40LFugz7c60SYe8GghUX46hsVbN1H7Drl8bPd6F16
Applications
Places
Terminal
Mon 12:02
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# nslookup -type=A -debug practicelabs.com
Server:         192.168.0.1
Address:        192.168.0.1#53

------------
    QUESTIONS:
        practicelabs.com, type = A, class = IN
    ANSWERS:
    ->  practicelabs.com
        internet address = 192.168.0.1
        ttl = 600
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Name:   practicelabs.com
Address: 192.168.0.1

root@PLABKALI01:~# nslookup -query=MX practicelabs.com
Server:         192.168.0.1
Address:        192.168.0.1#53

*** Can't find practicelabs.com: No answer

root@PLABKALI01:~# 
```

Figure 3.50 Screenshot of PLABKALI01: Showing the result of the nslookup -query=MX command.

## *Step 7*

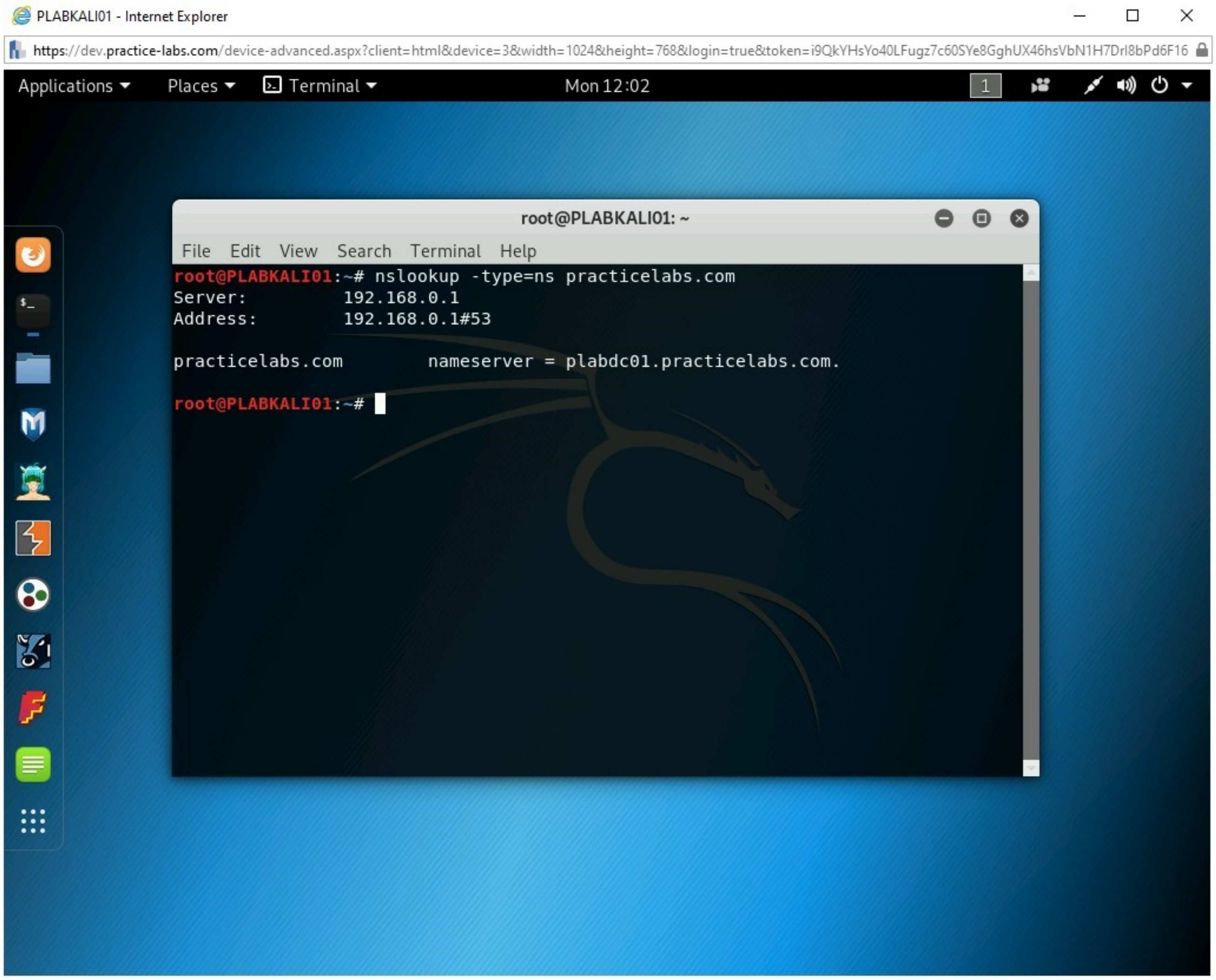
Clear the screen by entering the following command:

```
clear
```

The **NS** record maps a domain name to a list of the DNS servers that are authoritative for this domain. Type the following command:

```
nslookup -type=ns practicelabs.com
```

Press **Enter**.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=i9QkYHsYo40LFugz7c60SYe8GghUX46hsVbN1H7Drl8bPd6F16
Applications
Places
Terminal
Mon 12:02
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# nslookup -type=ns practicelabs.com
Server:         192.168.0.1
Address:        192.168.0.1#53

practicelabs.com        nameserver = plabdc01.practicelabs.com.

root@PLABKALI01:~# 
```

Figure 3.51 Screenshot of PLABKALI01: Showing the result of the nslookup -type=ns command.

Since there is only one DNS server, it is listed as the response to the command.

## *Step 8*

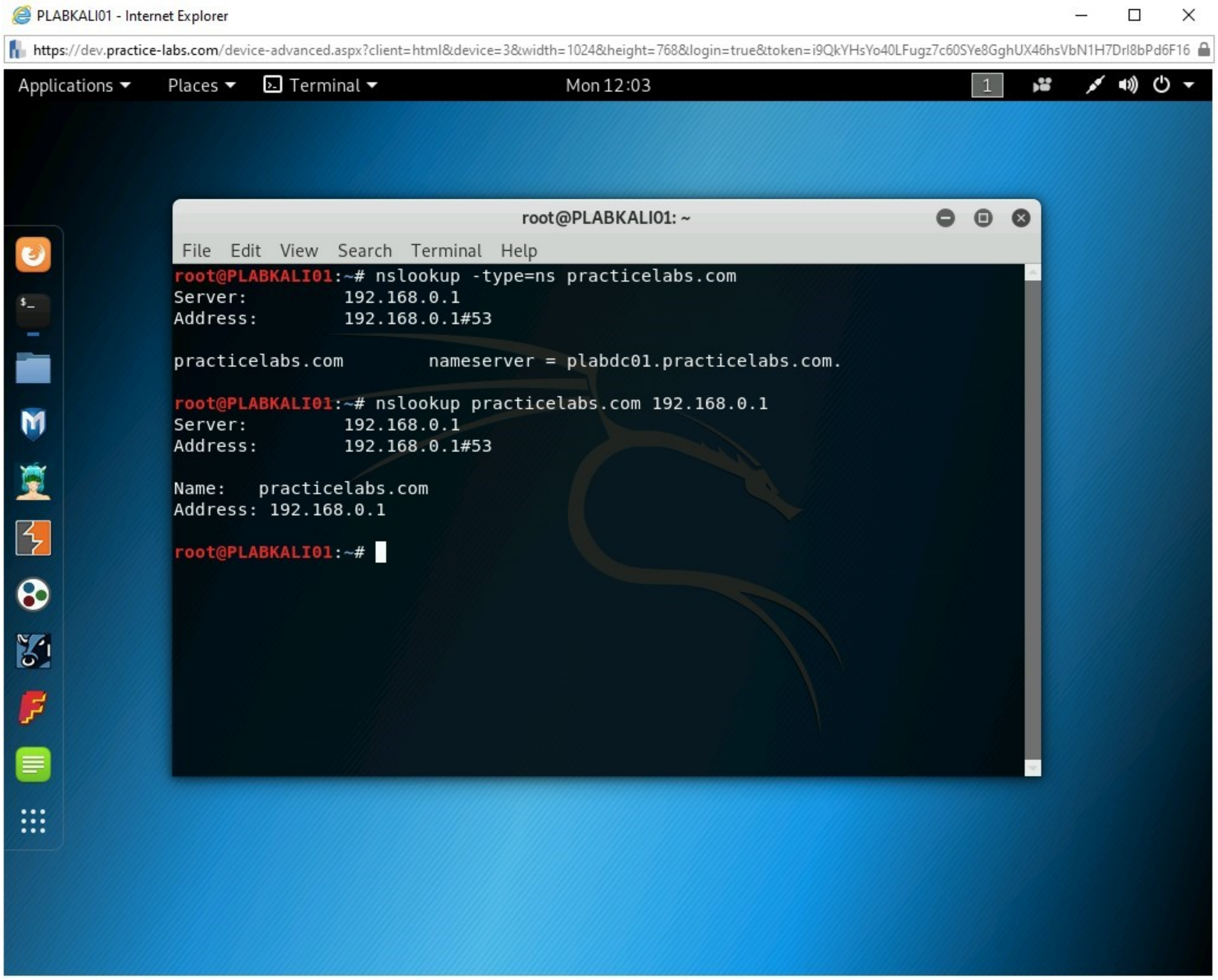
You can perform domain name resolution using a specific DNS server.

Type the following command:

```
nslookup practicelabs.com 192.168.0.1
```

Press **Enter**.

Notice the listed details as the output of this command.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=i9QkYHsYo40LFugz7c60SYe8GghUX46hsVbN1H7Drl8bPd6F16
Applications
Places
Terminal
Mon 12:03
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# nslookup -type=ns practicelabs.com
Server:         192.168.0.1
Address:        192.168.0.1#53

practicelabs.com        nameserver = plabdc01.practicelabs.com.

root@PLABKALI01:~# nslookup practicelabs.com 192.168.0.1
Server:         192.168.0.1
Address:        192.168.0.1#53

Name:   practicelabs.com
Address: 192.168.0.1

root@PLABKALI01:~# 
```

Figure 3.52 Screenshot of PLABKALI01: Showing the result of the nslookup command.

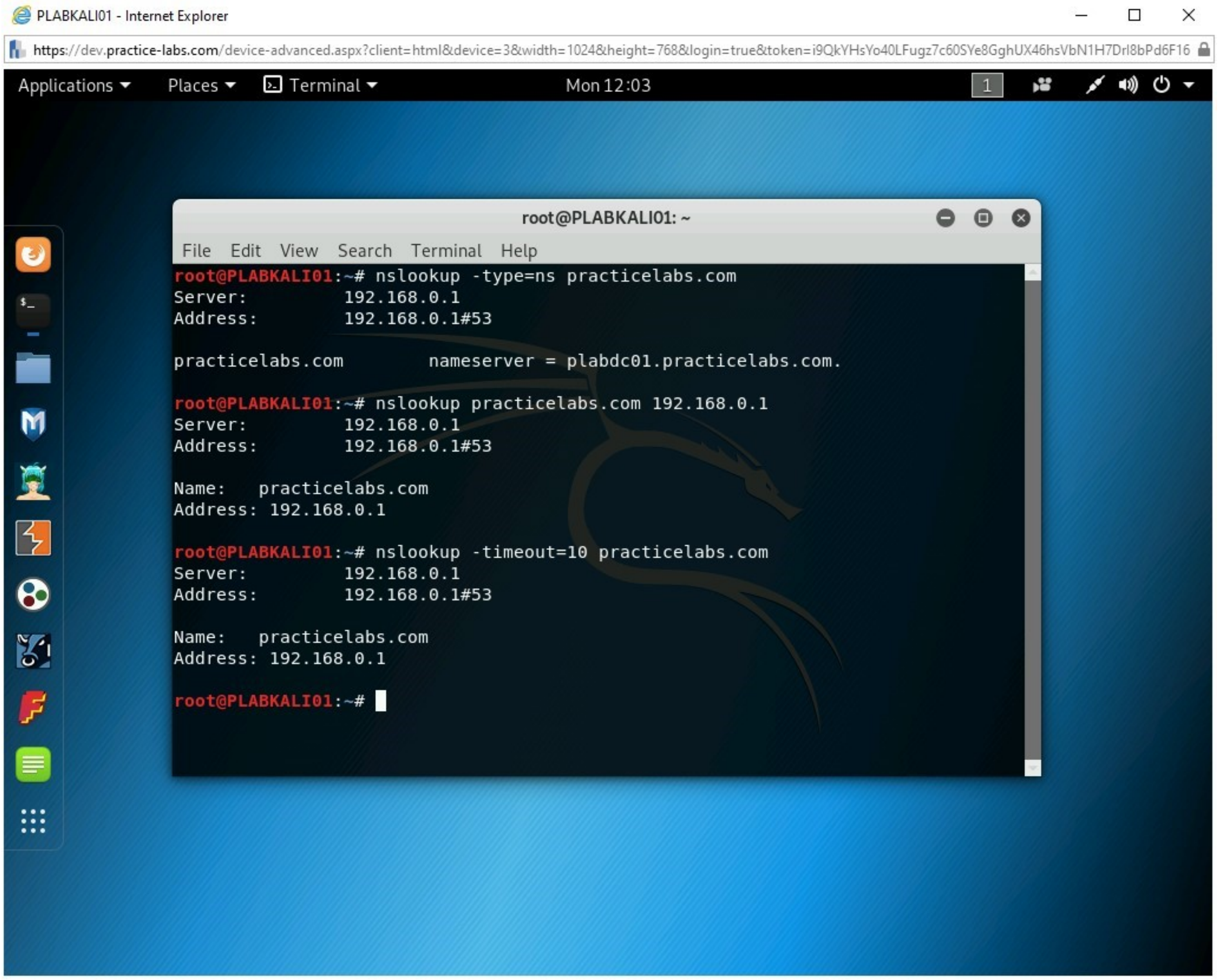
## *Step 9*

You can also change the default timeout to wait for a reply using the **-timeout** option. Type the following command:

```
nslookup -timeout=10 practicelabs.com
```

Press **Enter**.

Observe the output of the command.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=i9QkYHsYo40LFugz7c60SYe8GghUX46hsVbN1H7Drl8bPd6F16
Applications
Places
Terminal
Mon 12:03
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# nslookup -type=ns practicelabs.com
Server:         192.168.0.1
Address:        192.168.0.1#53

practicelabs.com        nameserver = plabdc01.practicelabs.com.

root@PLABKALI01:~# nslookup practicelabs.com 192.168.0.1
Server:         192.168.0.1
Address:        192.168.0.1#53

Name:   practicelabs.com
Address: 192.168.0.1

root@PLABKALI01:~# nslookup -timeout=10 practicelabs.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Name:   practicelabs.com
Address: 192.168.0.1

root@PLABKALI01:~#
```

Figure 3.53 Screenshot of PLABKALI01: Showing the result of the nslookup -timeout command.

## Step 10

Clear the screen by entering the following command:

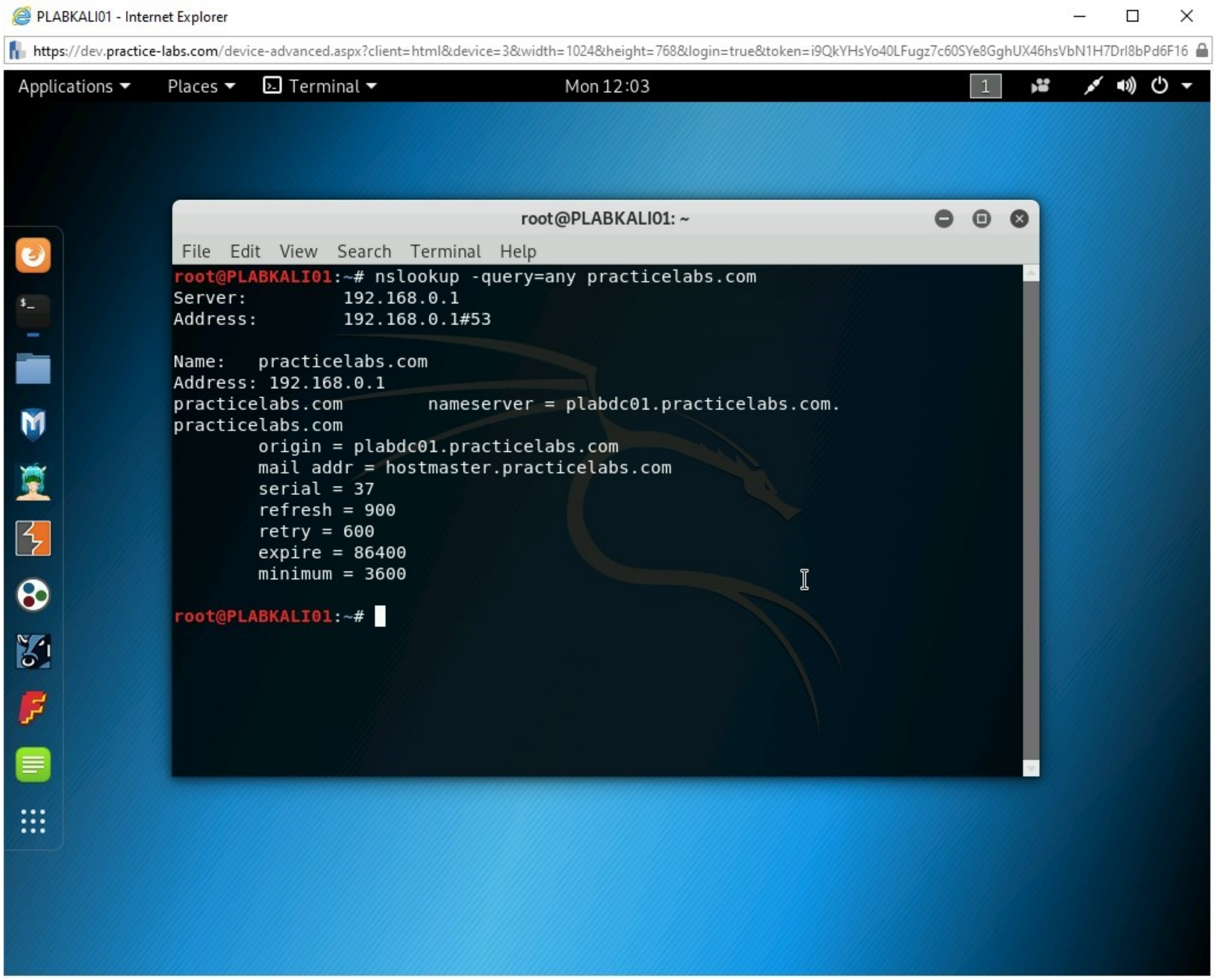
```
clear
```

You can view all the available DNS records using the **-query=any** option. Type the following command:

```
nslookup -query=any practicelabs.com
```

Press **Enter**.

Notice the listed details as the output of this command.



PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=i9QkYHsYo40LFugz7c60SYe8GghUX46hsVbN1H7Drl8bPd6F16
Applications
Places
Terminal
Mon 12:03
1
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
root@PLABKALI01:~# nslookup -query=any practicelabs.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Name:   practicelabs.com
Address: 192.168.0.1
practicelabs.com        nameserver = plabdc01.practicelabs.com.
practicelabs.com
        origin = plabdc01.practicelabs.com
        mail addr = hostmaster.practicelabs.com
        serial = 37
        refresh = 900
        retry = 600
        expire = 86400
        minimum = 3600

root@PLABKALI01:~# 
```

Figure 3.54 Screenshot of PLABKALI01: Showing the nslookup -query=any command.

Keep the terminal window open.

## Task 6 - Use theHarvester

The theHarvester tool is primarily used for information gathering. By providing a domain name and a search engine name, you can search for the following information:

- E-mail accounts
- Usernames
- Hostnames
- Subdomains
- Banners

To use theHarvester, perform the following steps:

## Step 1

Ensure you have powered on the devices listed in the introduction and are connected to **PLABKALI01**.

On the desktop, click **Terminal** if already not opened.

> ***Note****: Clear the screen with the clear command if the terminal window was already opened.*

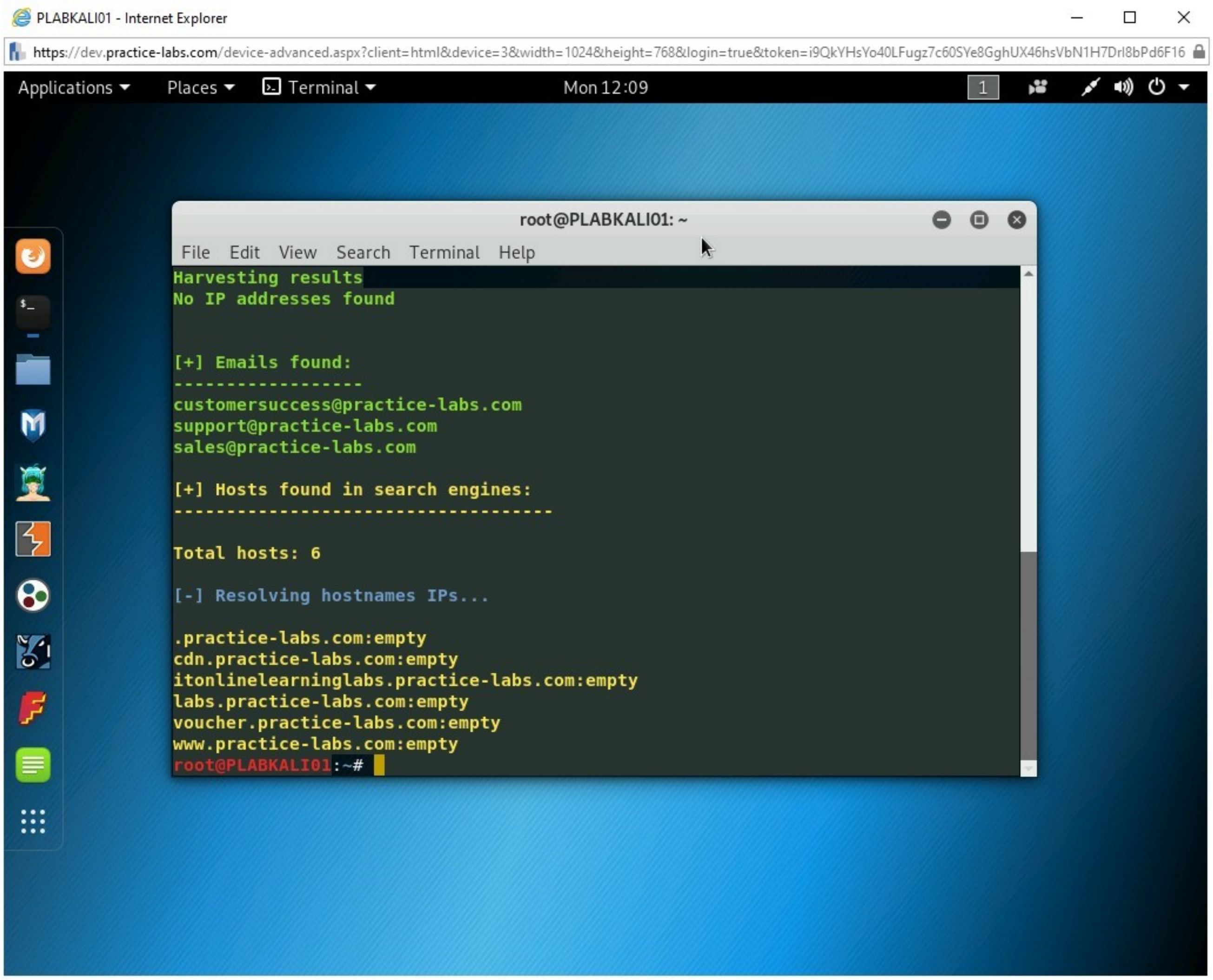
Type the following command:

```
theHarvester -d practice-labs.com -l 500 -b google
```

Press **Enter**.

The -d parameter is used for the domain name. The -l parameter is used for the number of results. The -b parameter is used for the source of information, which is a search engine.

The command is now executed. It can locate the E-mail addresses and the number of hosts. Note that the results do not provide IP addresses.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=i9QkYHsYo40LFugz7c60SYe8GghUX46hsVbN1H7Drl8bPd6F16
Applications
Places
Terminal
Mon 12:09
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
Harvesting results
No IP addresses found


[+] Emails found:
------------------
customersuccess@practice-labs.com
support@practice-labs.com
sales@practice-labs.com

[+] Hosts found in search engines:
------------------------------------

Total hosts: 6

[-] Resolving hostnames IPs...

.practice-labs.com:empty
cdn.practice-labs.com:empty
itonlinelearninglabs.practice-labs.com:empty
labs.practice-labs.com:empty
voucher.practice-labs.com:empty
www.practice-labs.com:empty
root@PLABKALI01:~#
```

Figure 3.55 Screenshot of PLABKALI01: Showing the output of the theharvester command with the -d and -l parameter.

***Note**: The hostnames are not resolved because of the firewall restrictions in the lab environment. In a real-world scenario, you would be able to get the IP addresses.*

## Step 2

Clear the screen by entering the following command:

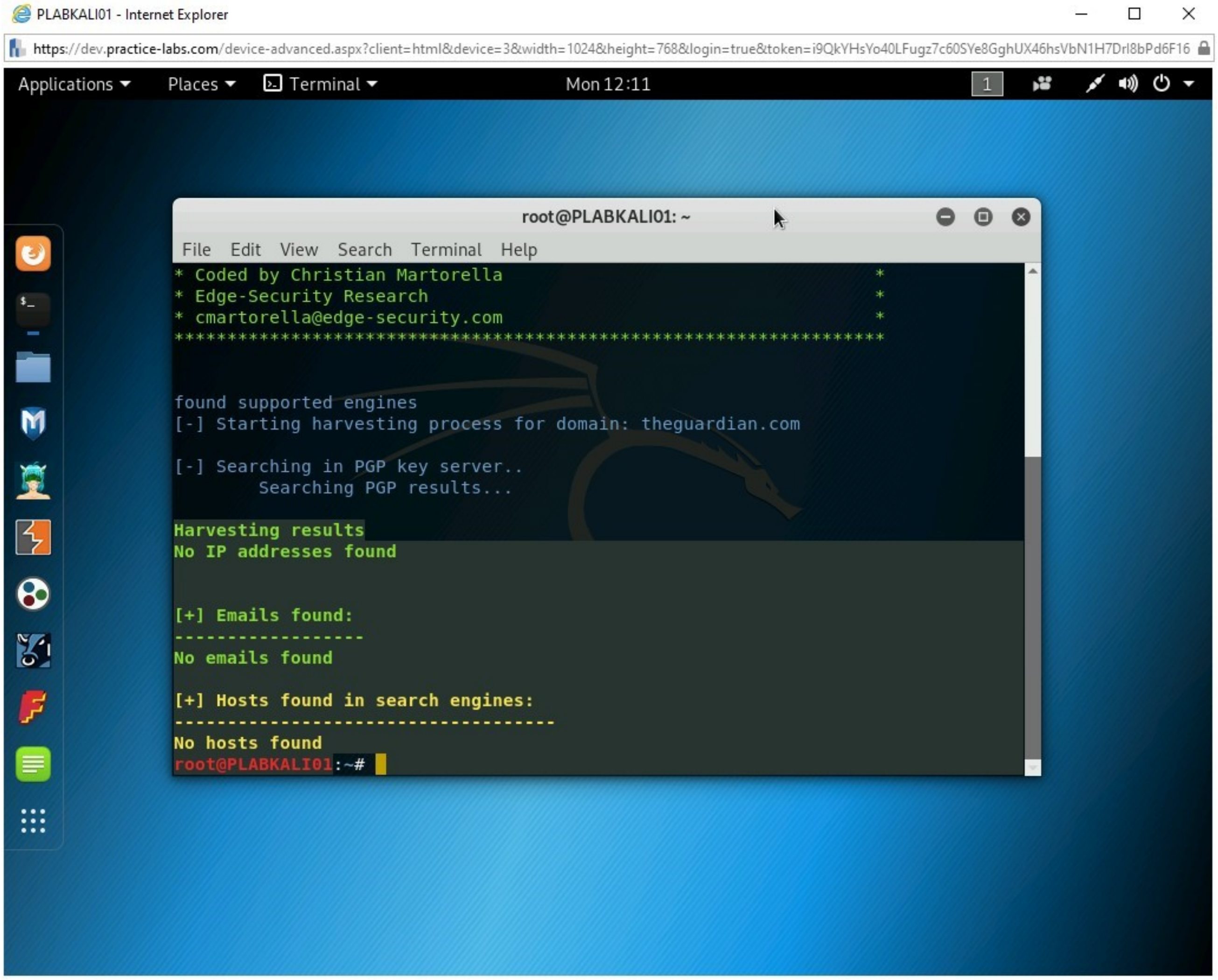
```
clear
```

To get E-mail addresses from **theguardian.com**, type the following command:

```
theHarvester -d theguardian.com -b bing
```

Press **Enter**.

The output of this command may take a few minutes to display.


PLABKALI01 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=i9QkYHsYo40LFugz7c60SYe8GghUX46hsVbN1H7Drl8bPd6F16
Applications
Places
Terminal
Mon 12:11
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
* Coded by Christian Martorella                                *
* Edge-Security Research                                       *
* cmartorella@edge-security.com                                *
*******************************************************************


found supported engines
[-] Starting harvesting process for domain: theguardian.com

[-] Searching in PGP key server..
        Searching PGP results...

Harvesting results
No IP addresses found


[+] Emails found:
------------------
No emails found

[+] Hosts found in search engines:
------------------------------------
No hosts found
root@PLABKALI01:~#
```

Figure 3.56 Screenshot of PLABKALI01: Showing the fetched E-mail addresses from the theguardian.com Website.

> ***Note**: The above output used the "-b pgp" source which is now deprecated. To see a list of sources enter the command **theHarvester -help** at the command line.*

Keep the terminal windows open.

## Task 7 - Create a Temporary E-mail Account

There will be numerous occasions when you are asked to provide your E-mail account for registration on a Website. Using your own E-mail ID can lead to SPAM and various other threats. Therefore, in these situations, you can use a temporary E-mail account for registration.

In this task, you will create a temporary E-mail account. To do this, perform the following steps:

### *Step 1*

Ensure you have powered on all the devices listed in the introduction, and connect to **PLABWIN10**.

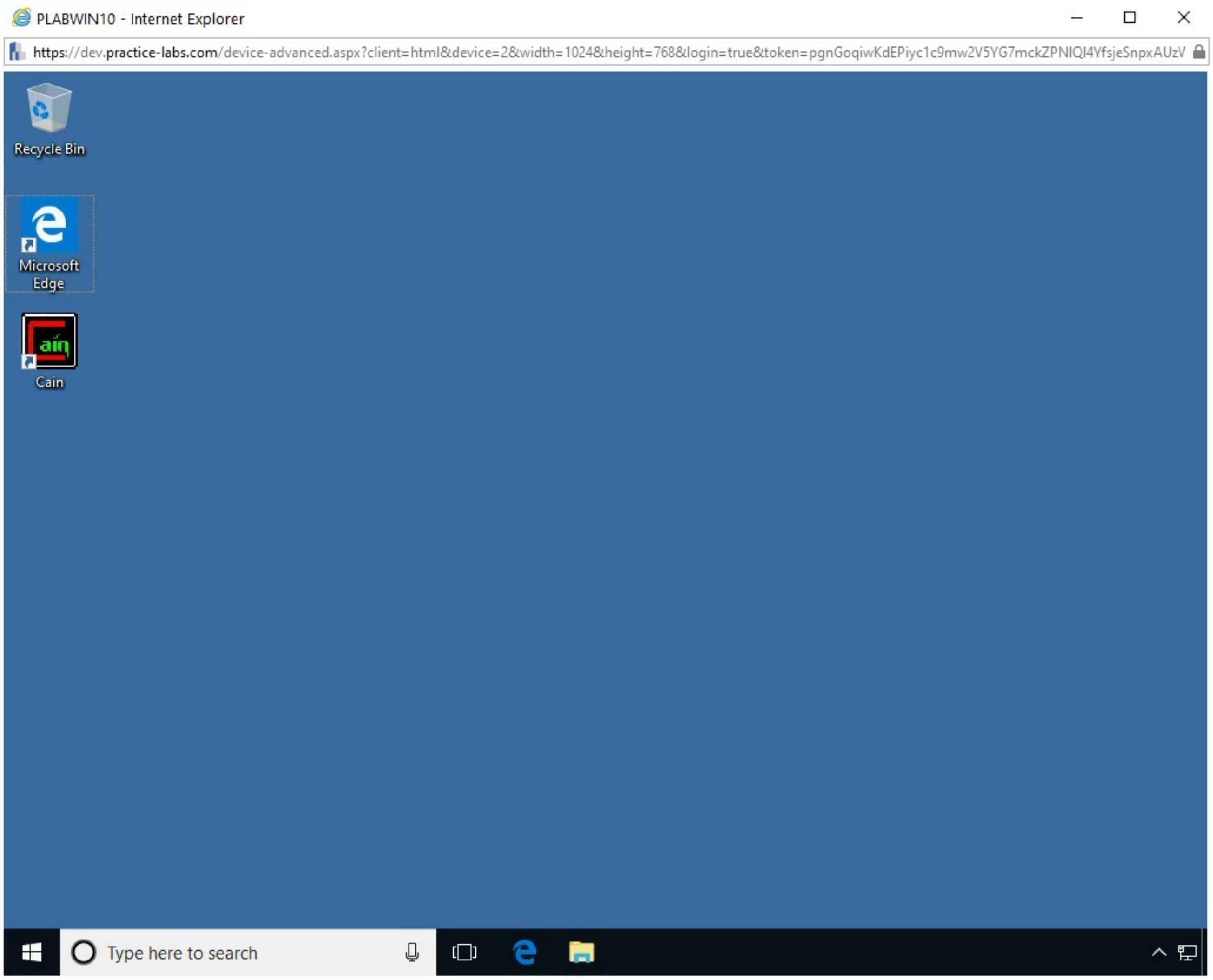
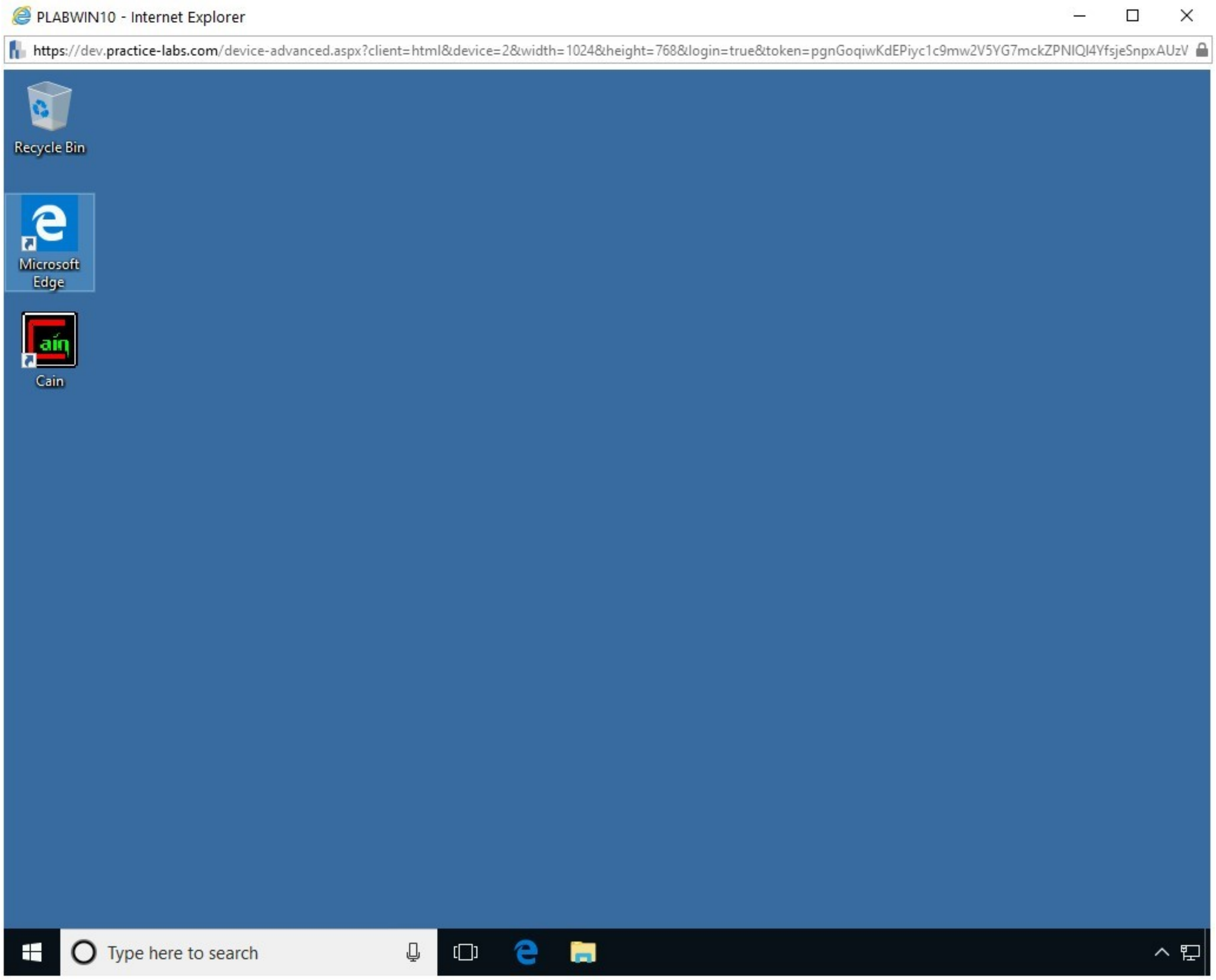

PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=pgnGoqiwKdEPiyc1c9mw2V5YG7mckZPNIQl4YfsjeSnpxAUzV
Recycle Bin
Microsoft Edge
Cain
Type here to search

Figure 3.57 Screenshot of PLABWIN10: The desktop screen.

## *Step 2*

Double click on **Microsoft Edge** on the desktop



PLABWIN10 - Internet Explorer

https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=pgnGoqiwKdEPiyc1c9mw2V5YG7mckZPNIQI4YfsjeSnpxAUzV

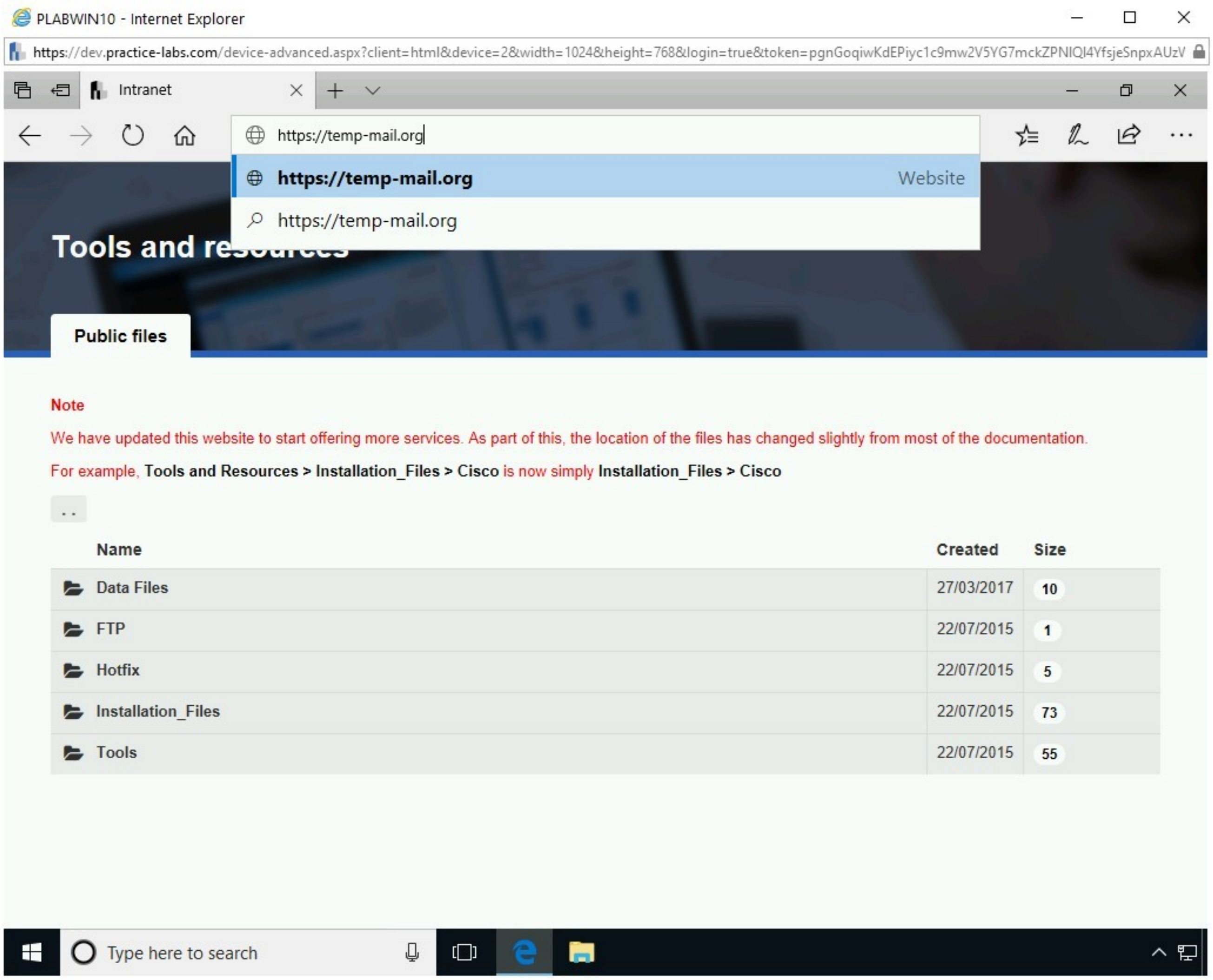
Figure 3.58 Screenshot of PLABWIN10: Selecting Internet Explorer from the search results.

## Step 3

The the Microsoft Edge window is displayed. In the address bar, type the following URL:

```
https://temp-mail.org
```

Press **Enter**.



PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=pgnGoqiwKdEPiyc1c9mw2V5YG7mckZPNIQI4YfsjeSnpxAUzV
Intranet
https://temp-mail.org
https://temp-mail.org
Website
https://temp-mail.org
Tools and resources
Public files
Type here to search

Note

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

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

. .

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

Figure 3.59 Screenshot of PLABWIN10: Entering the URL in the address bar of Internet Explorer.

The **Your Temporary Email Address** Webpage is displayed. Notice that there is a default E-mail address displayed.

> ***Note***: *In the next task,* ***Use Maltego****, you can use the temporary or your own personal E-mail address.*

Scroll down to view the remaining Webpage. If you need to copy this E-mail address, you can click the **Green** icon.

If you do not like the E-mail address, you can click **Change**. You can also click **Delete** to delete the above-shown E-mail address and its content.

***Note**: Every time you open this Webpage, you will see a new and unique E-mail address. The E-mail address shown in the screenshot will not match the one you will see.*

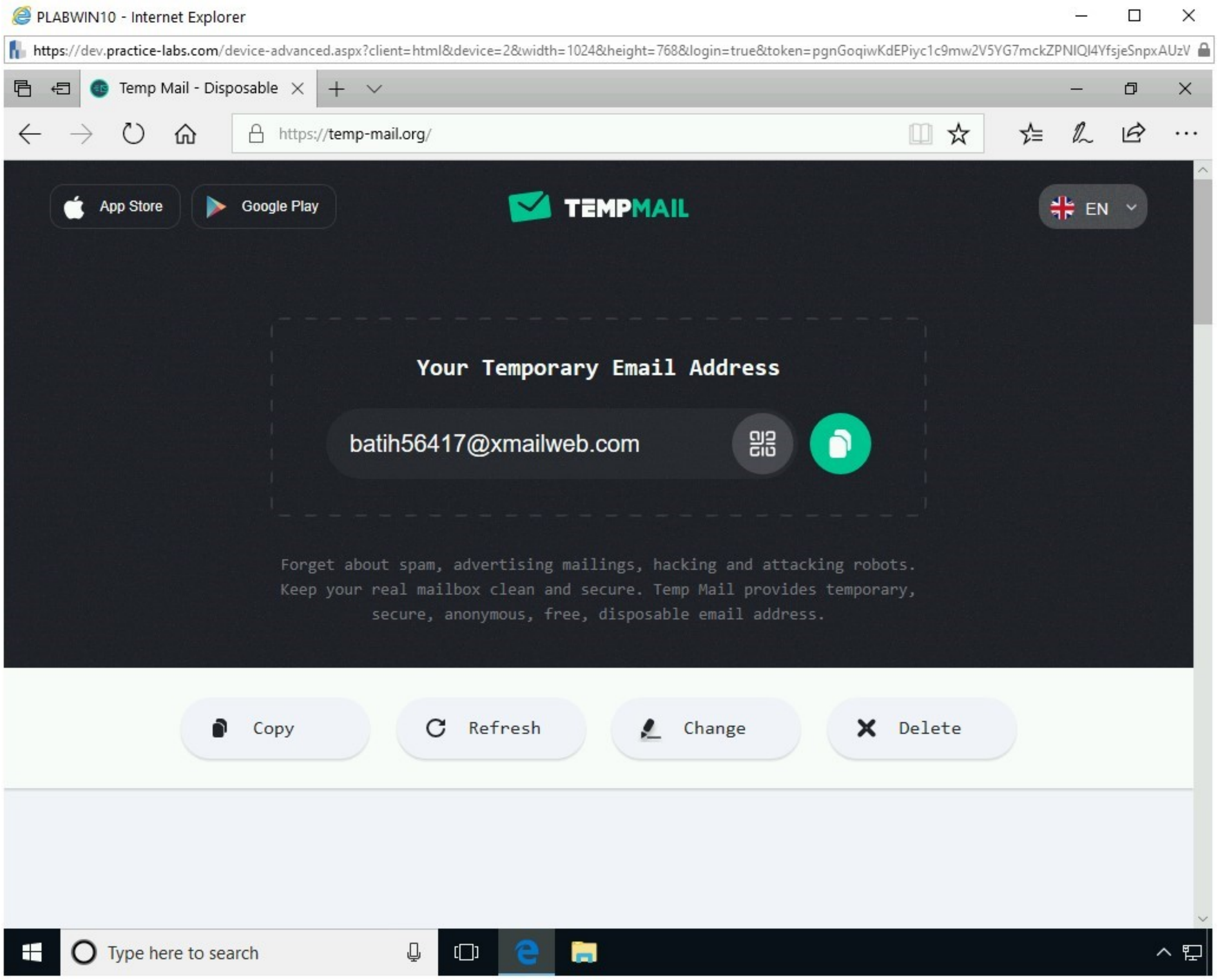
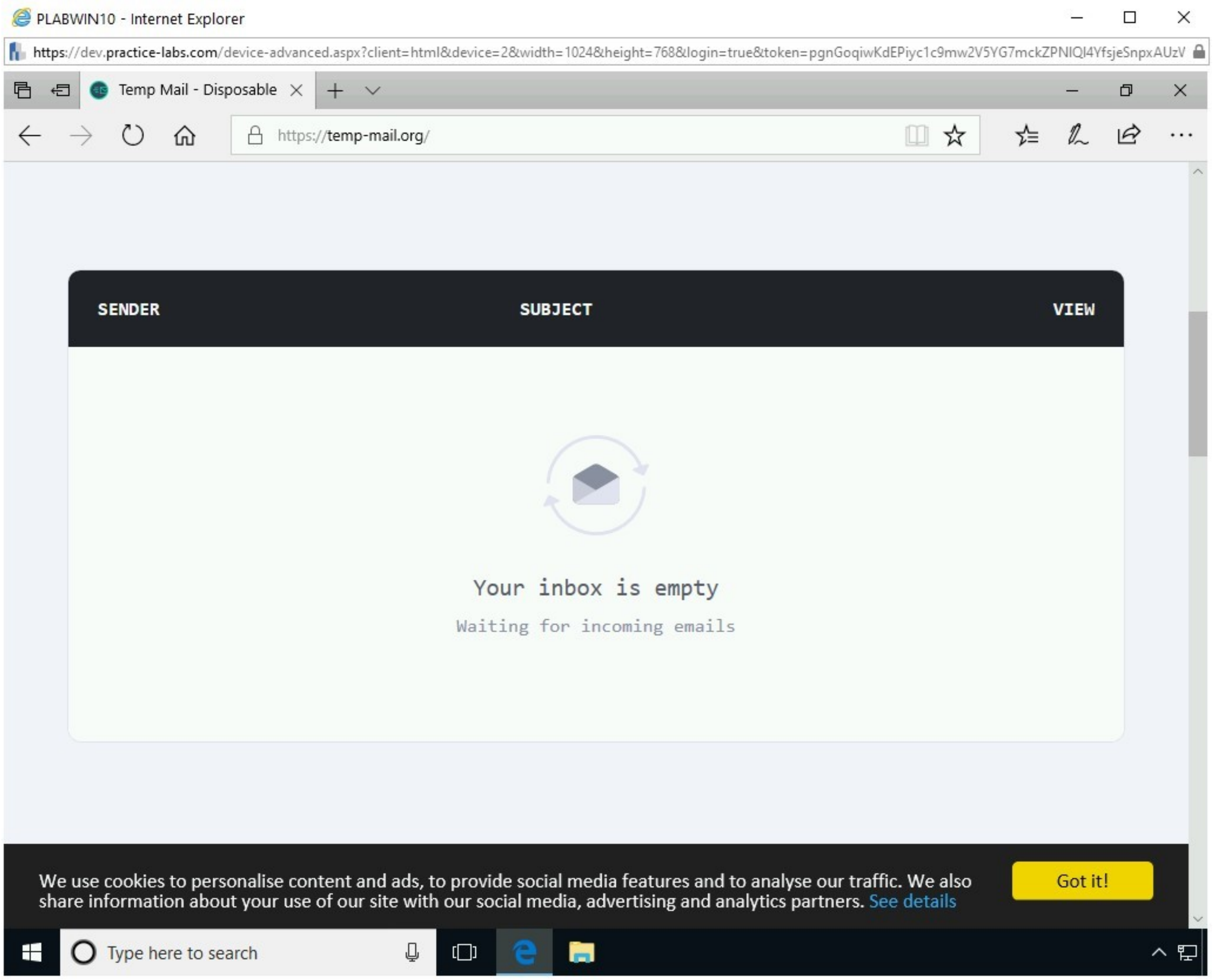

PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=pgnGoqiwKdEPiyc1c9mw2V5YG7mckZPNIQl4YfsjeSnpxAUzV
Temp Mail - Disposable
https://temp-mail.org/
App Store
Google Play
TEMPMAIL
EN
Your Temporary Email Address
batih56417@xmailweb.com
Forget about spam, advertising mailings, hacking and attacking robots. Keep your real mailbox clean and secure. Temp Mail provides temporary, secure, anonymous, free, disposable email address.
Copy
Refresh
Change
Delete
Type here to search

Figure 3.60 Screenshot of PLABWIN10: Showing the homepage of the temp-mail.org Website along with the temporary E-mail address.

The bottom section of the Webpage displays the inbox. Any E-mails sent to you will be stored here.



PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=pgnGoqiwKdEPiyc1c9mw2V5YG7mckZPNIQl4YfsjeSnpxAUzV
Temp Mail - Disposable
https://temp-mail.org/
SENDER
SUBJECT
VIEW
Your inbox is empty
Waiting for incoming emails
We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. See details
Got it!
Type here to search

Figure 3.61 Screenshot of PLABWIN10: Showing the empty inbox of an E-mail address.

## Task 8 - Use Maltego

Maltego is a tool used for open-source intelligence gathering and forensics. Maltego can discover and collect data in graphical format for analysis. Maltego is available as a free and commercial product.

> ***Note:*** *It is important to understand that the capabilities of a tool, such as Maltego, is shown in a limited capacity in this task. You may want to explore it further.*

You can use a free license for learning purposes, but to perform ethical hacking, you would need to use the commercial product as it offers more functionality. Maltego does not intrude into any network and provides information that is available publicly.

**Alert**: Maltego requires you to register before you can use it. You should first create the account on the Maltego Website outside the lab environment and use it within the task. You can either use your own E-mail ID or use the one that you created in the previous task. You can register via the following URL: **https://www.paterva.com/community/community.php**

To use Maltego, perform the following steps:

## *Step 1*

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

To start **Maltego**, click the left-most icon in the status bar, select **01 - Information Gathering**, and then select **maltego**.

***Note****: There are two alternate methods to start maltego. You can click the maltego icon in the icon bar on the desktop. You can also start it with the maltego command in the terminal window.*

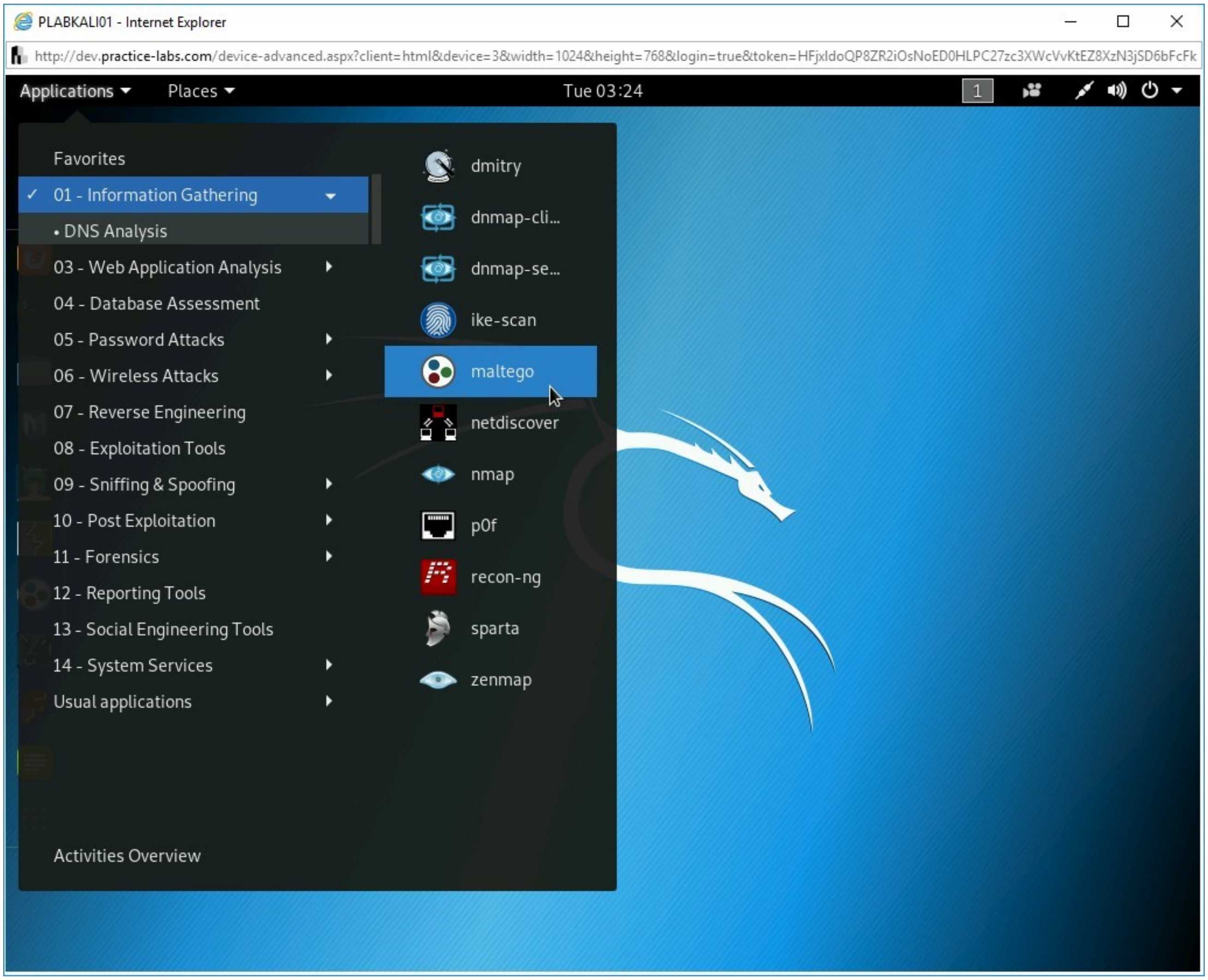


Figure 3.62 Screenshot of PLABKALI01: Showing the selection of the maltego option from the menu.

## Step 2

The application starts. You may have to wait for a few minutes while it loads.

***Note:*** *The application may minimize by itself. If it does, invoke the window to start working.*

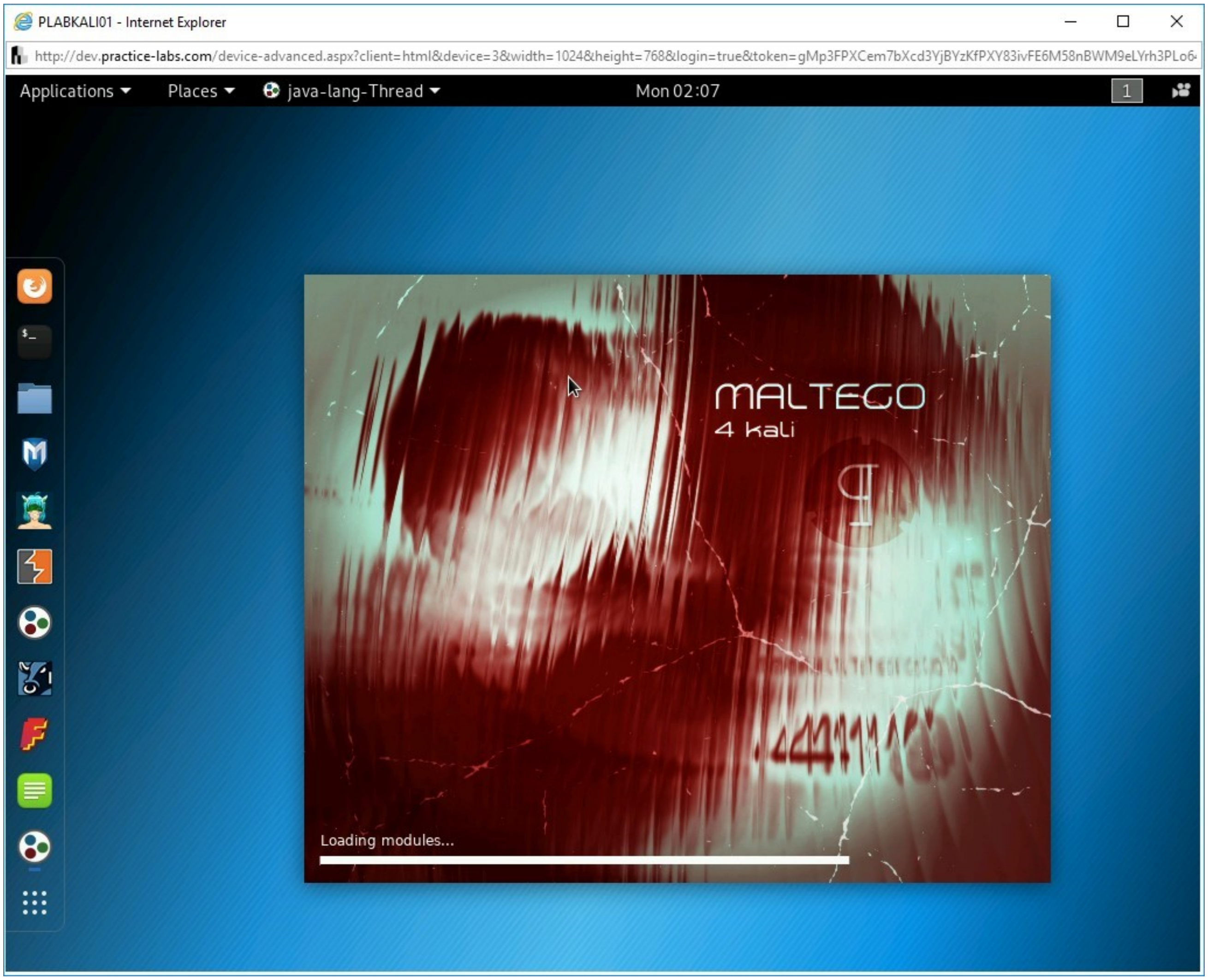
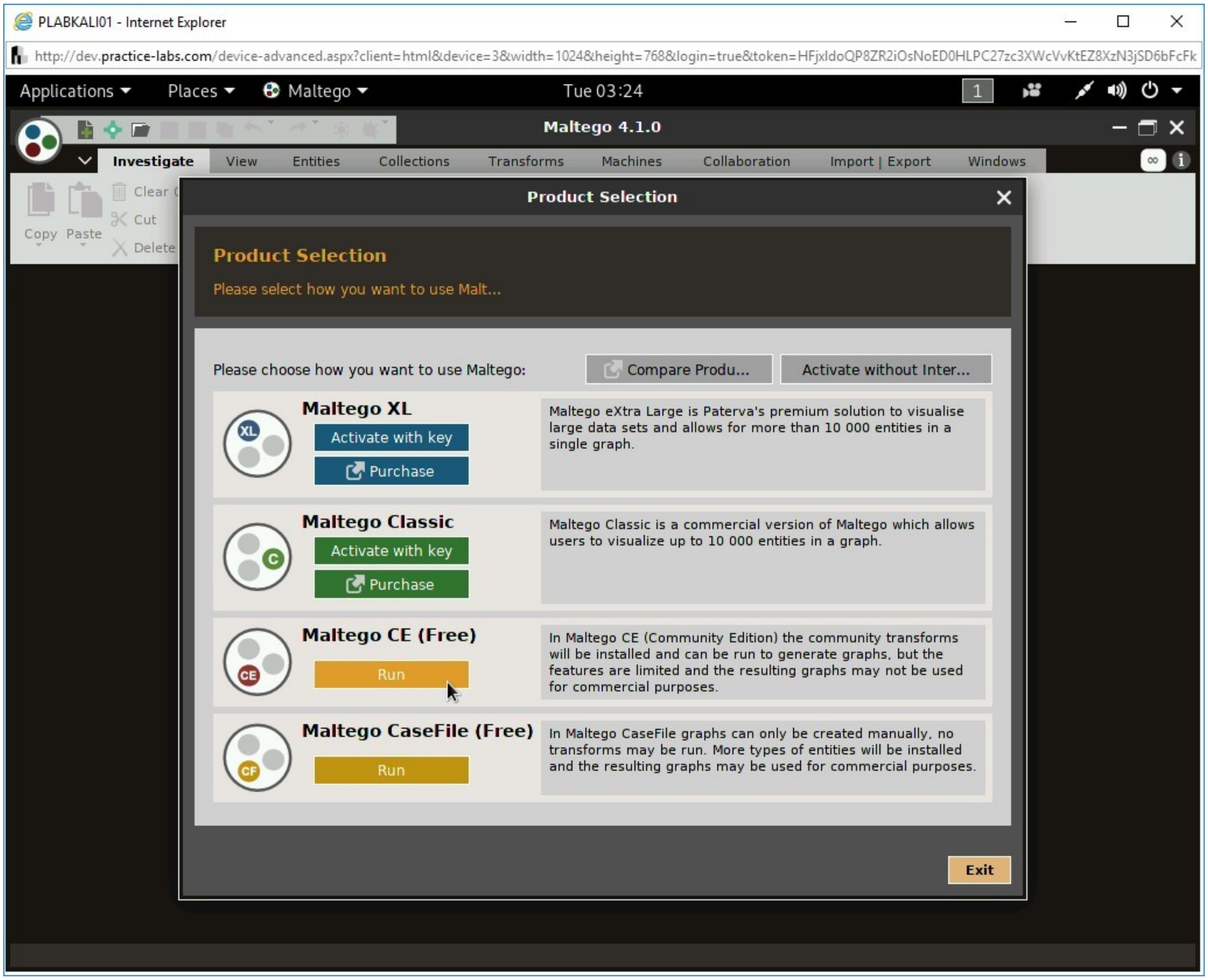

PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=gMp3FPXCem7bXcd3YjBYzKfPXY83ivFE6M58nBWM9eLYrh3PLo6
Applications
Places
java-lang-Thread
Mon 02:07
1
MALTEGO
4 kali
Loading modules...

Figure 3.63 Screenshot of PLABKALI01: Showing the splash screen of Maltego.

## Step 3

After Maltego starts, you need to select the product that you want to use. Click the **Run** button below the **Maltego CE (Free)** section.



Maltego eXtra Large is Paterva's premium solution to visualise large data sets and allows for more than 10 000 entities in a single graph.

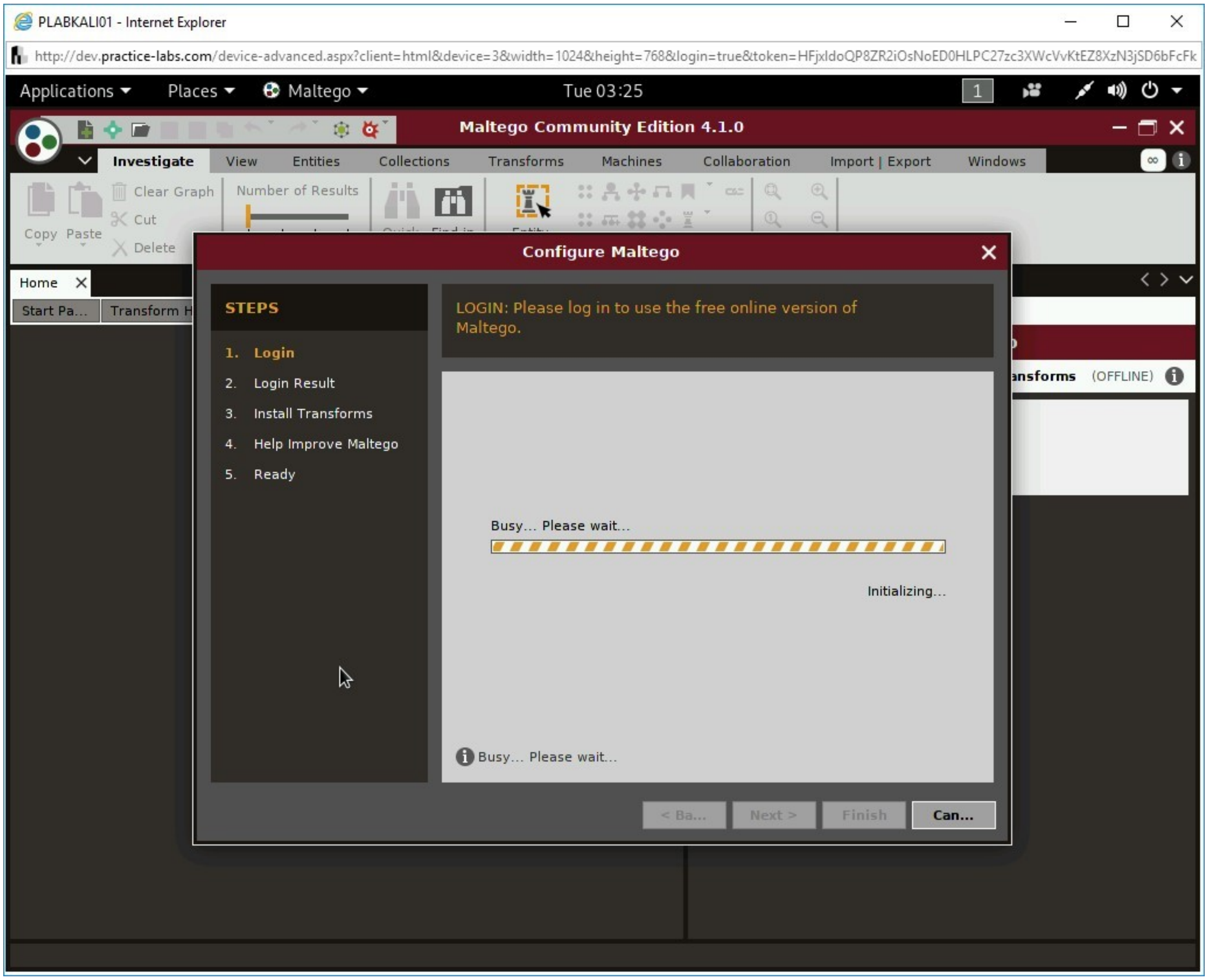
Maltego Classic is a commercial version of Maltego which allows users to visualize up to 10 000 entities in a graph.

In Maltego CE (Community Edition) the community transforms will be installed and can be run to generate graphs, but the features are limited and the resulting graphs may not be used for commercial purposes.

In Maltego CaseFile graphs can only be created manually, no transforms may be run. More types of entities will be installed and the resulting graphs may be used for commercial purposes.

Figure 3.64 Screenshot of PLABKALI01: Selecting Run from the Product Selection dialog box.

The **Configure Maltego** dialog box is displayed. It begins to initialize the product.



LOGIN: Please log in to use the free online version of Maltego.

Busy… Please wait…

Initializing…

Busy… Please wait…

Figure 3.65 Screenshot of PLABKALI01: Showing the initialization of the product.

## Step 4

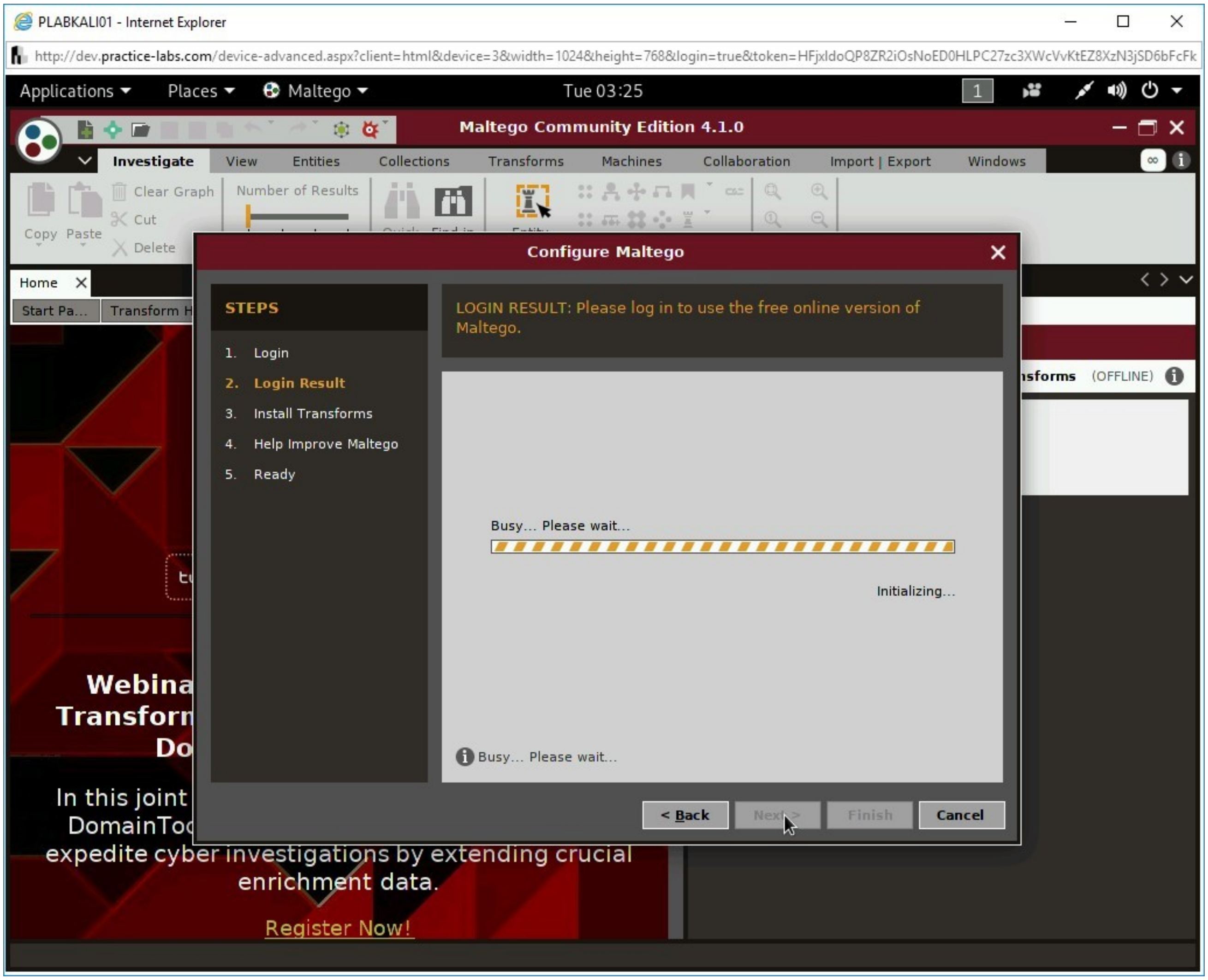
*Note: If you see the 'Login server could not be contacted' message, click* ***Back****, and then on the previous page, click* ***Next****. You should now see the refreshed LOGIN page.*

Enter your email address in the **Email Address** textbox and enter the password in the **Password** textbox.

Then, you also need to enter the displayed **CAPTCHA**, which will be different every time you log in.

Click **Next**.

The login details are now being validated.



LOGIN RESULT: Please log in to use the free online version of Maltego.

Busy... Please wait...

Initializing...

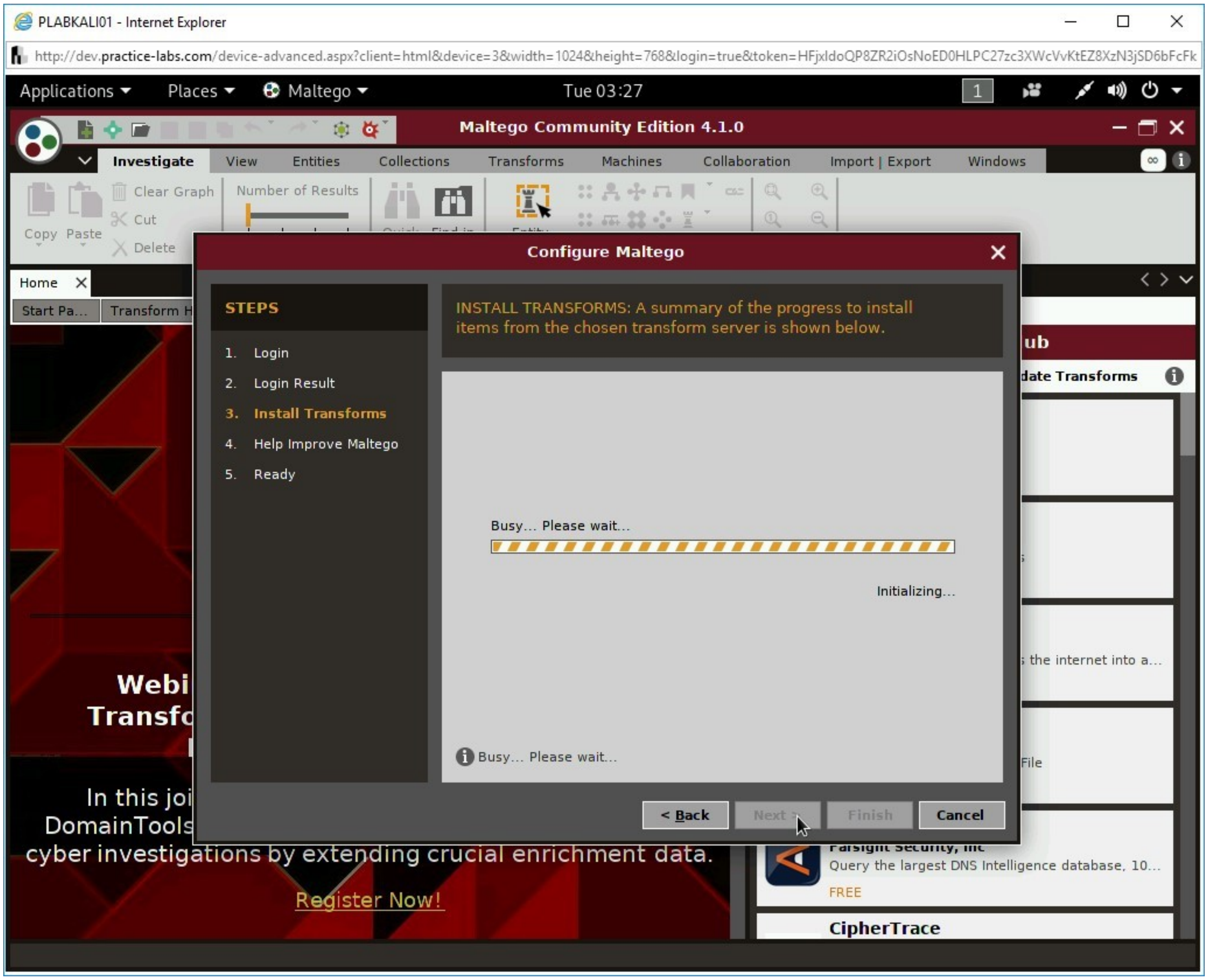
Busy... Please wait...

Figure 3.66 Screenshot of PLABKALI01: Showing the validation of the login credentials.

## Step 5

After the login is successful, you will be displayed with your login details. Click **Next**.

Maltego starts to install transforms.



STEPS

1. Login
2. Login Result
3. Install Transforms
4. Help Improve Maltego
5. Ready

INSTALL TRANSFORMS: A summary of the progress to install items from the chosen transform server is shown below.

Busy... Please wait...

Initializing...

Busy... Please wait...

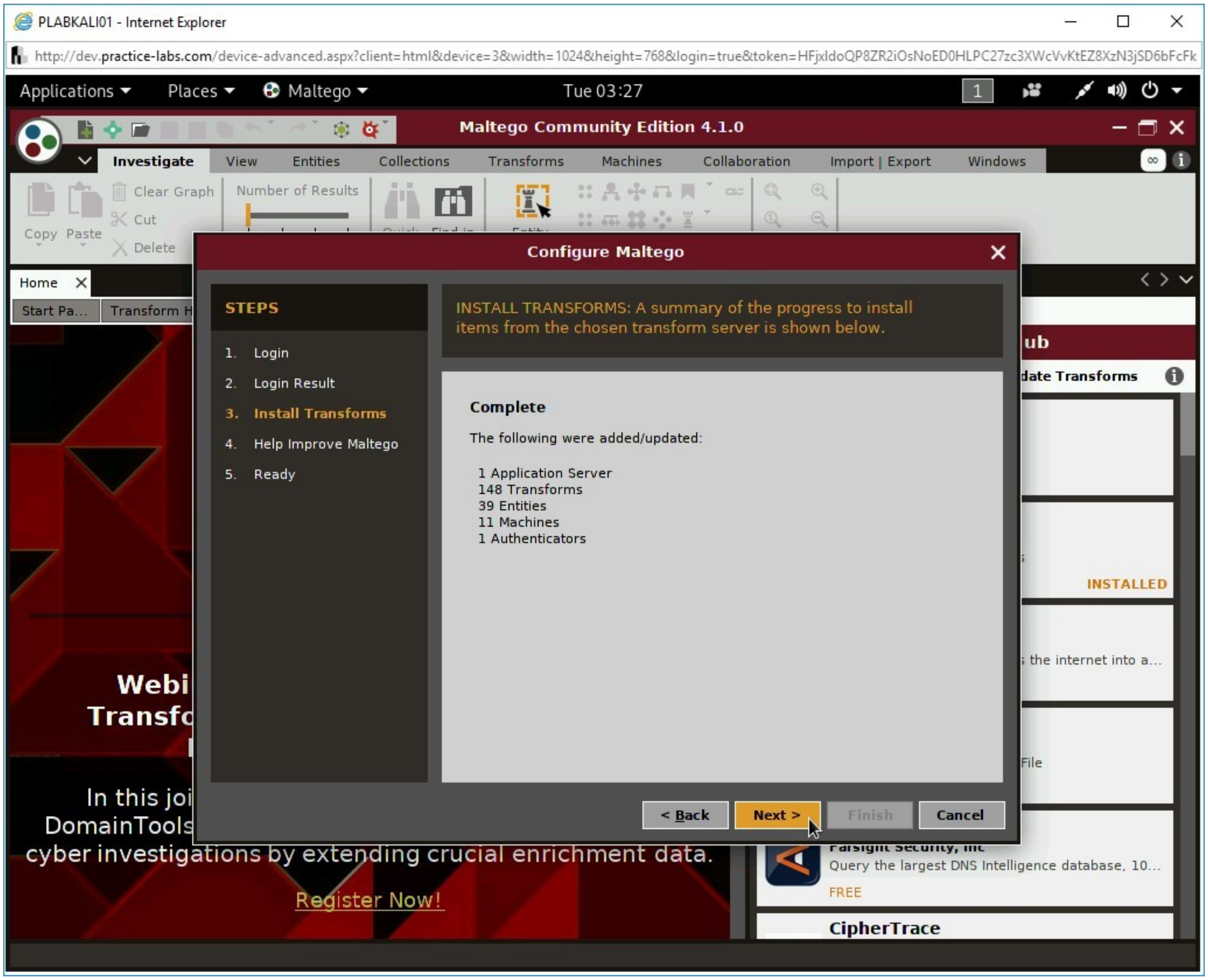
Farsight Security, Inc
Query the largest DNS Intelligence database, 10...

In this joi
DomainTools
cyber investigations by extending crucial enrichment data.

Figure 3.67 Screenshot of PLABKALI01: Showing the installation of transforms.

## *Step 6*

On the **Complete** screen, click **Next**.



INSTALL TRANSFORMS: A summary of the progress to install items from the chosen transform server is shown below.

Complete

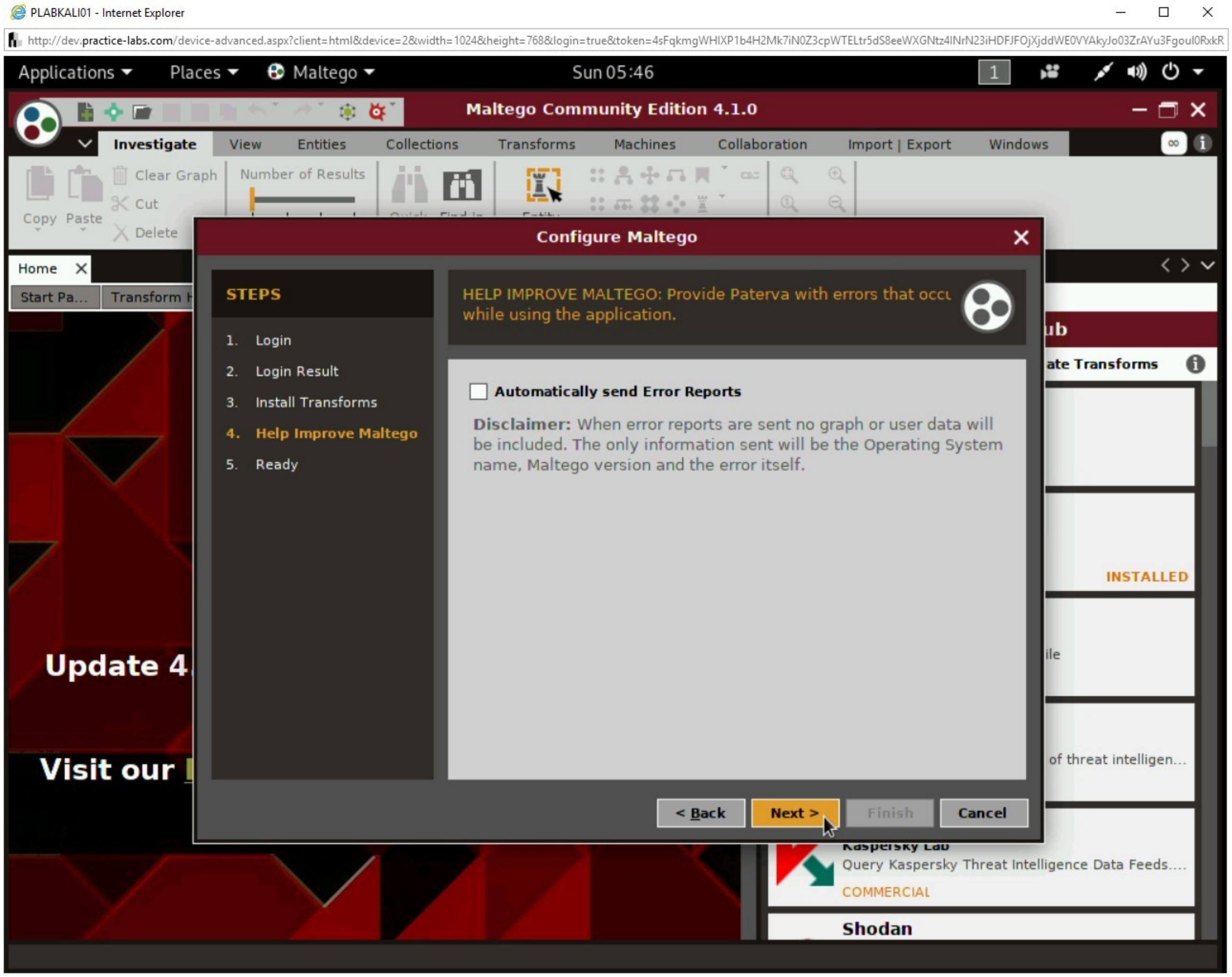
The following were added/updated:

1 Application Server
148 Transforms
39 Entities
11 Machines
1 Authenticators

Figure 3.68 Screenshot of PLABKALI01: Showing the complete installation screen.

## *Step 7*

On the next page, keep the default settings and click **Next**.



Configure Maltego

STEPS

1. Login
2. Login Result
3. Install Transforms
4. **Help Improve Maltego**
5. Ready

HELP IMPROVE MALTEGO: Provide Paterva with errors that occu while using the application.

□ **Automatically send Error Reports**

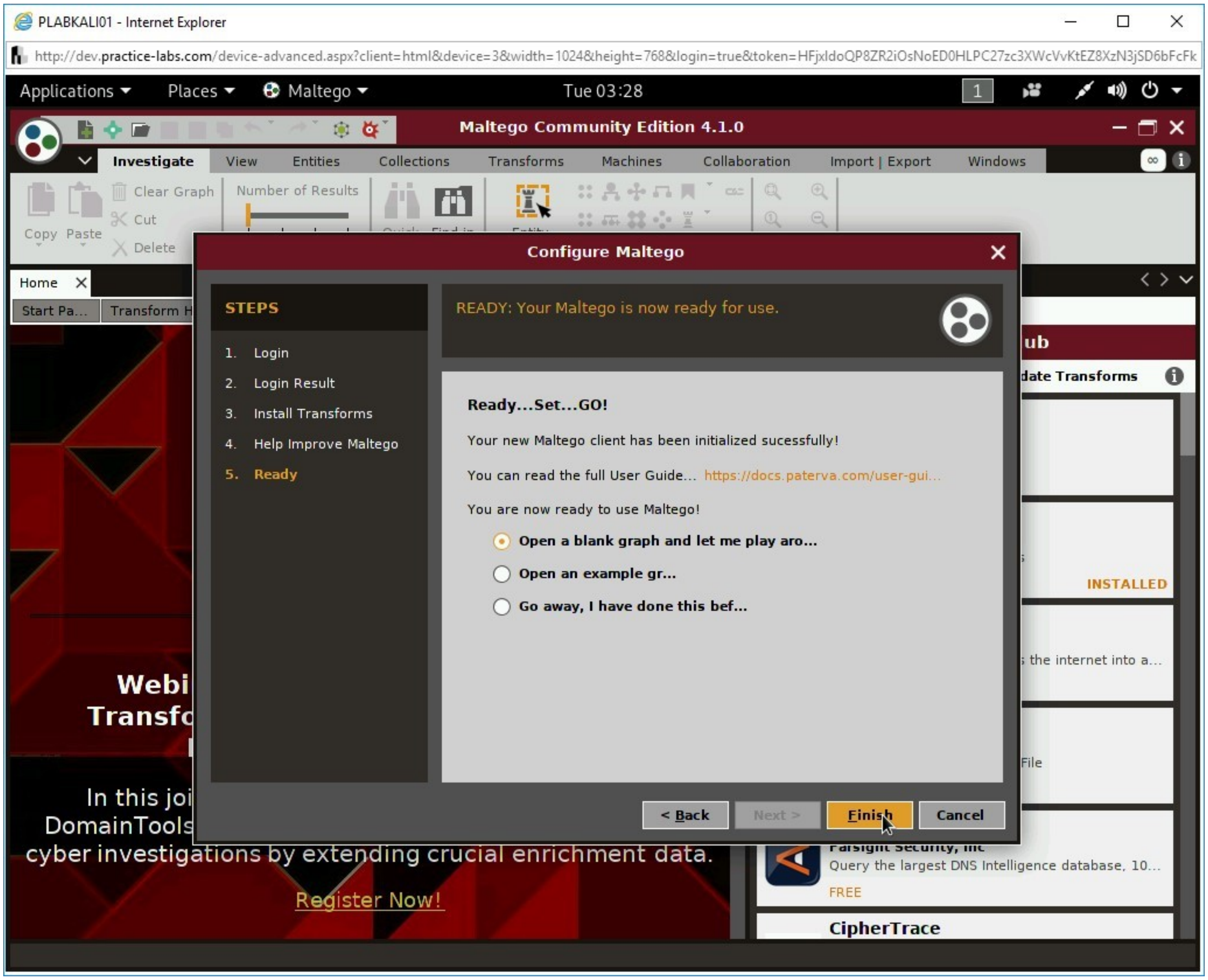
**Disclaimer:** When error reports are sent no graph or user data will be included. The only information sent will be the Operating System name, Maltego version and the error itself.

< Back | Next > | Finish | Cancel

Figure 3.69 Screenshot of PLABKALI01: Clicking Next on the HELP IMPROVE MALTEGO page.

## *Step 8*

On the **Ready…Set…GO!** page, select **Open a blank graph and let me play aro…** and click **Finish**.


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=HFjxldoQP8ZR2iOsNoED0HLPC27zc3XWcVvKtEZ8XzN3jSD6bFcFk
Applications
Places
Maltego
Tue 03:28
Maltego Community Edition 4.1.0
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Copy
Paste
Clear Graph
Cut
Delete
Number of Results
Home
Start Pa...
Transform H
INSTALLED
Query the largest DNS Intelligence database, 10...
FREE
CipherTrace
Register Now!

Configure Maltego

STEPS

1. Login
2. Login Result
3. Install Transforms
4. Help Improve Maltego
5. Ready

READY: Your Maltego is now ready for use.

**Ready...Set...GO!**

Your new Maltego client has been initialized sucessfully!

You can read the full User Guide... https://docs.paterva.com/user-gui...

You are now ready to use Maltego!

- ● Open a blank graph and let me play aro...
- ○ Open an example gr...
- ○ Go away, I have done this bef...

< Back | Next > | Finish | Cancel

Figure 3.70 Screenshot of PLABKALI01: Selecting the blank graph to start working in Maltego.

A new blank graph is added.

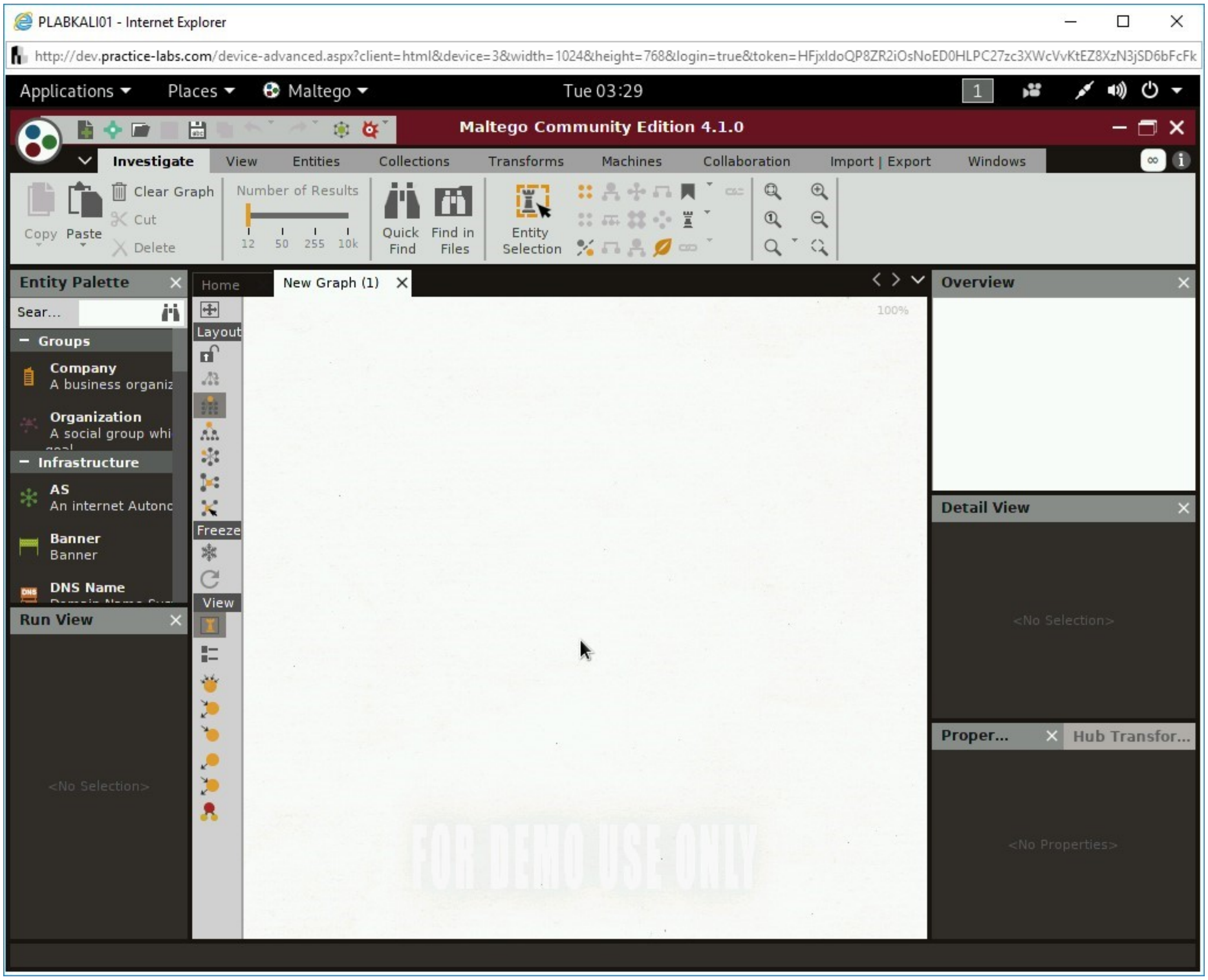
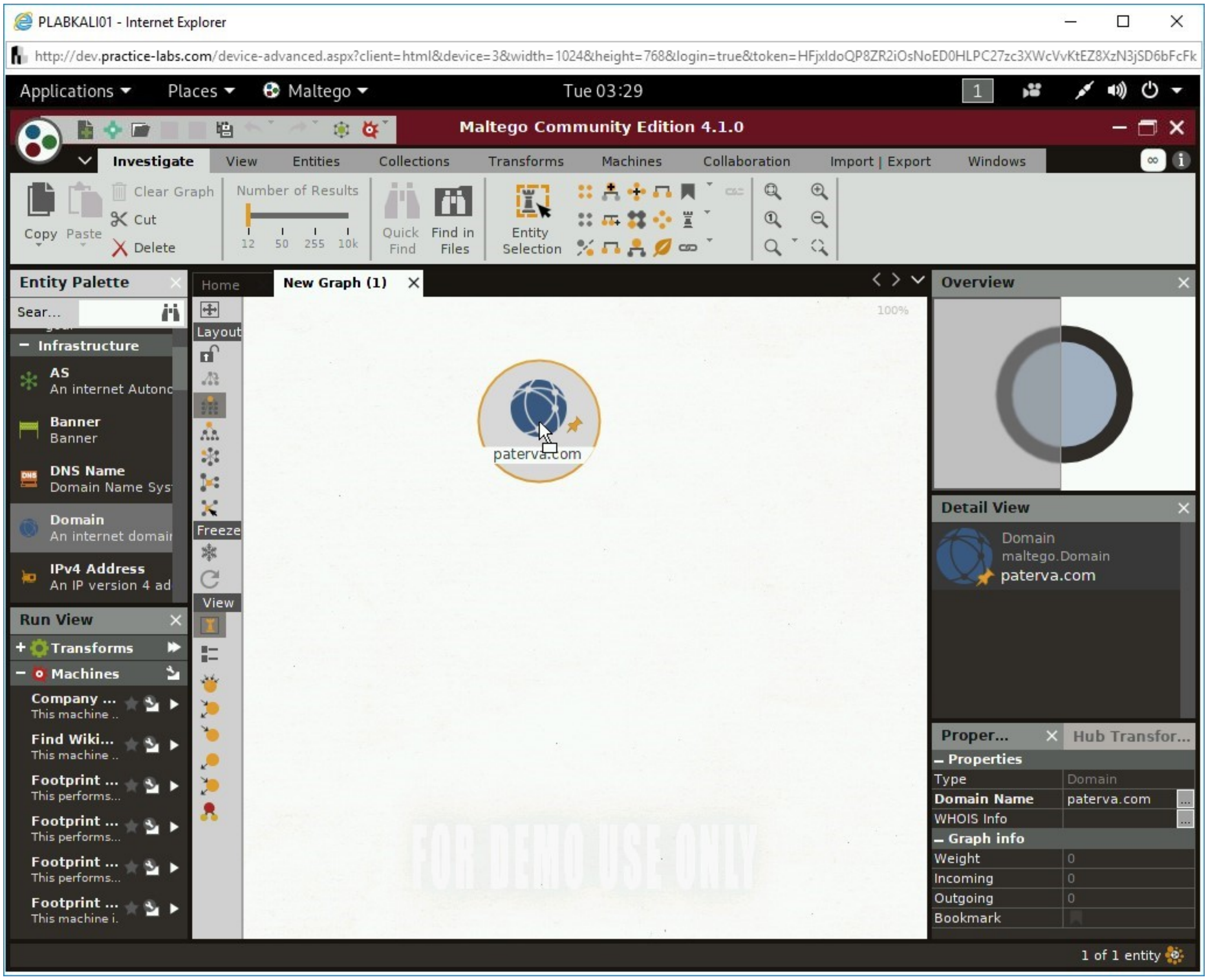


Figure 3.71 Screenshot of PLABKALI01: Showing a new blank graph in Maltego.

## Step 9

From the left pane, drag and drop the **Domain** icon onto the graph.

***Note**: You may have to scroll down to find Domain.*



| Properties | |
|---|---|
| Type | Domain |
| Domain Name | paterva.com |
| WHOIS Info | |
| **Graph info** | |
| Weight | 0 |
| Incoming | 0 |
| Outgoing | 0 |
| Bookmark | |

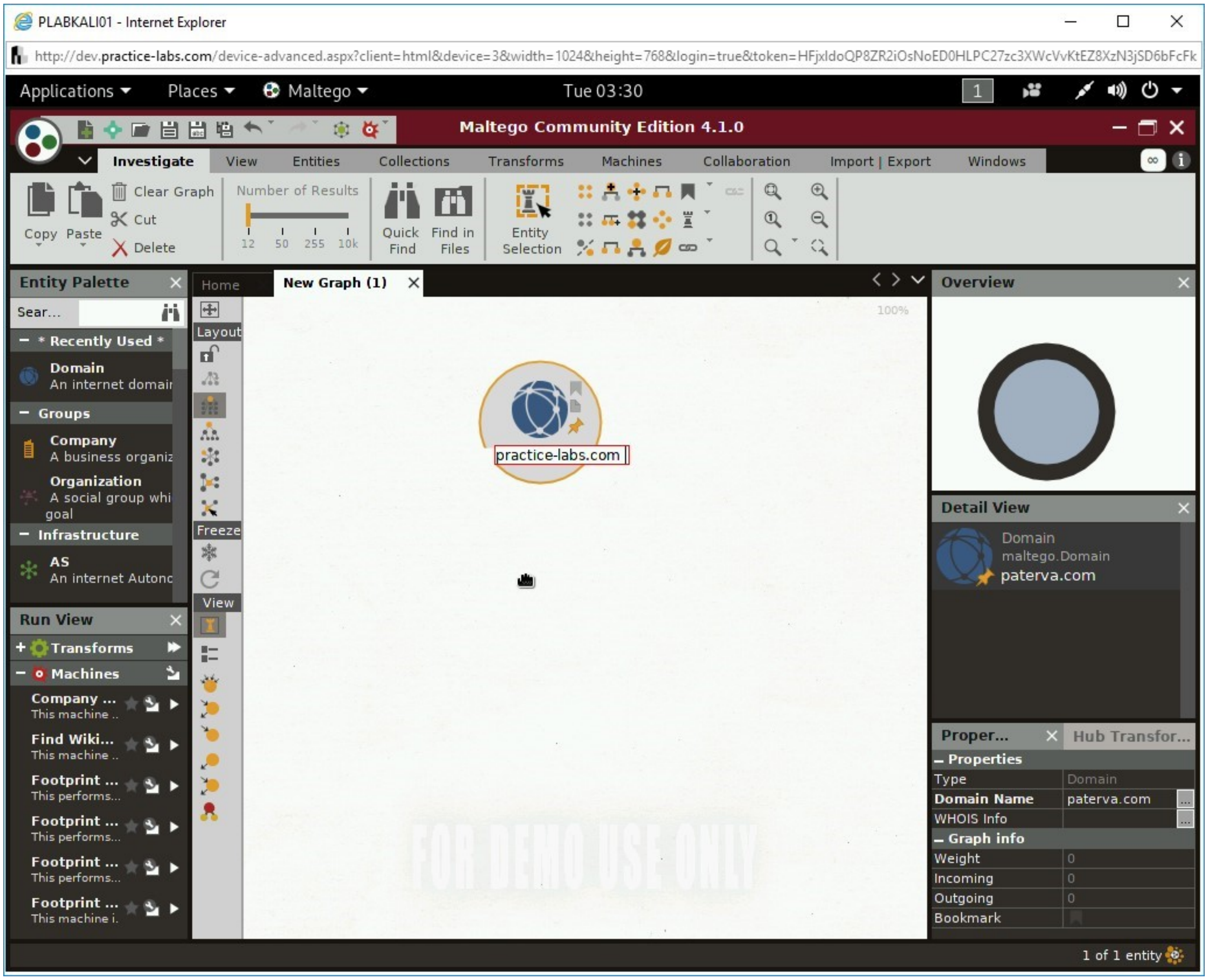
Figure 3.72 Screenshot of PLABKALI01: Dragging the Domain icon onto the graph.

## Step 10

Notice that **paterva.com** is the default name assigned to the domain. To change the domain name, double-click on the text and overwrite with the following text:

```
practice-labs.com
```

Press **Enter** or click anywhere on the graph.



| Properties | |
|---|---|
| Type | Domain |
| Domain Name | paterva.com |
| WHOIS Info | |
| Graph info | |
| Weight | 0 |
| Incoming | 0 |
| Outgoing | 0 |
| Bookmark | |

Figure 3.73 Screenshot of PLABKALI01: Changing the name of the domain to practice-labs.com.

## Step 11

Right-click **practice-labs.com** and select **All Transforms** from the **Run Transform...** dialog box.

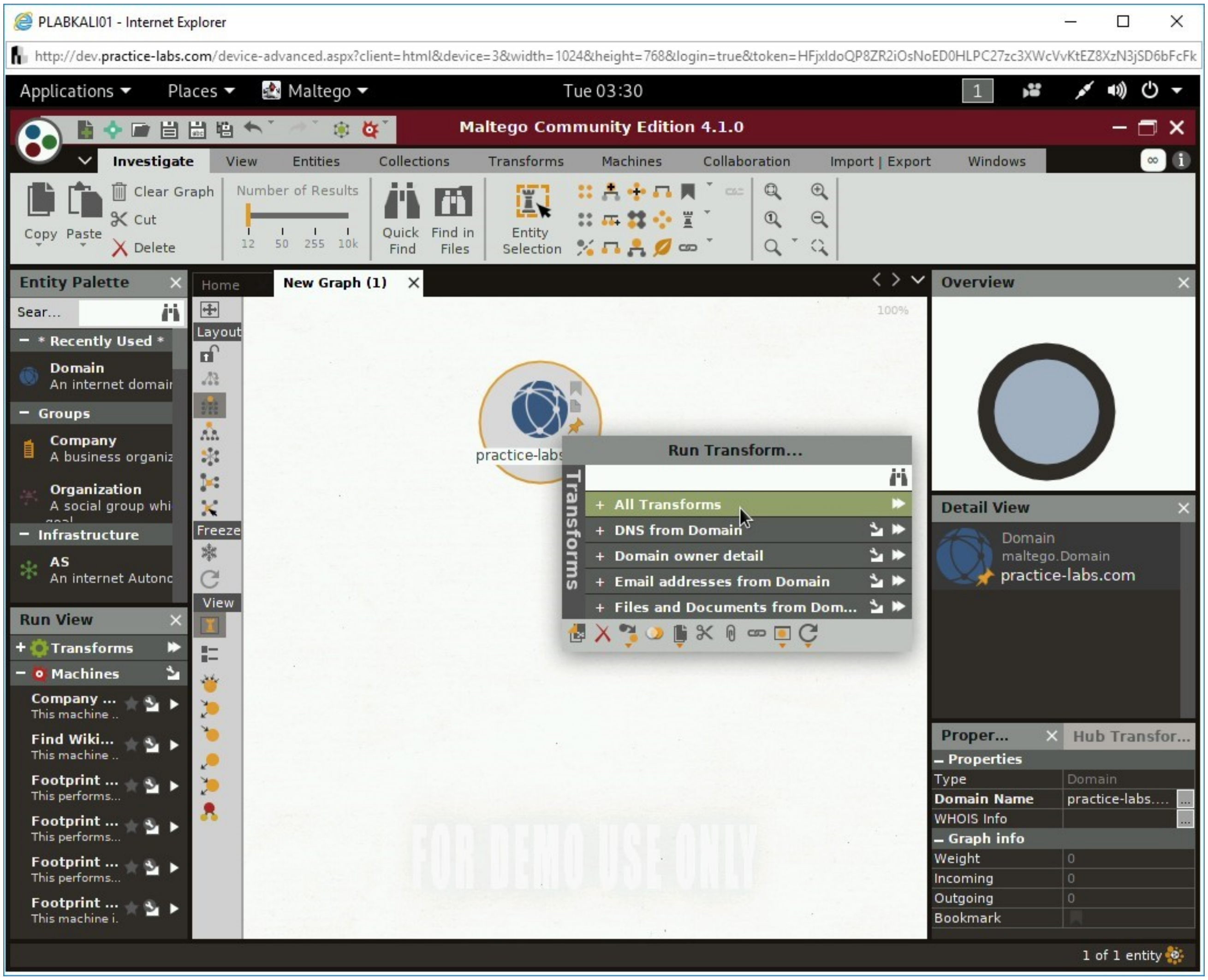
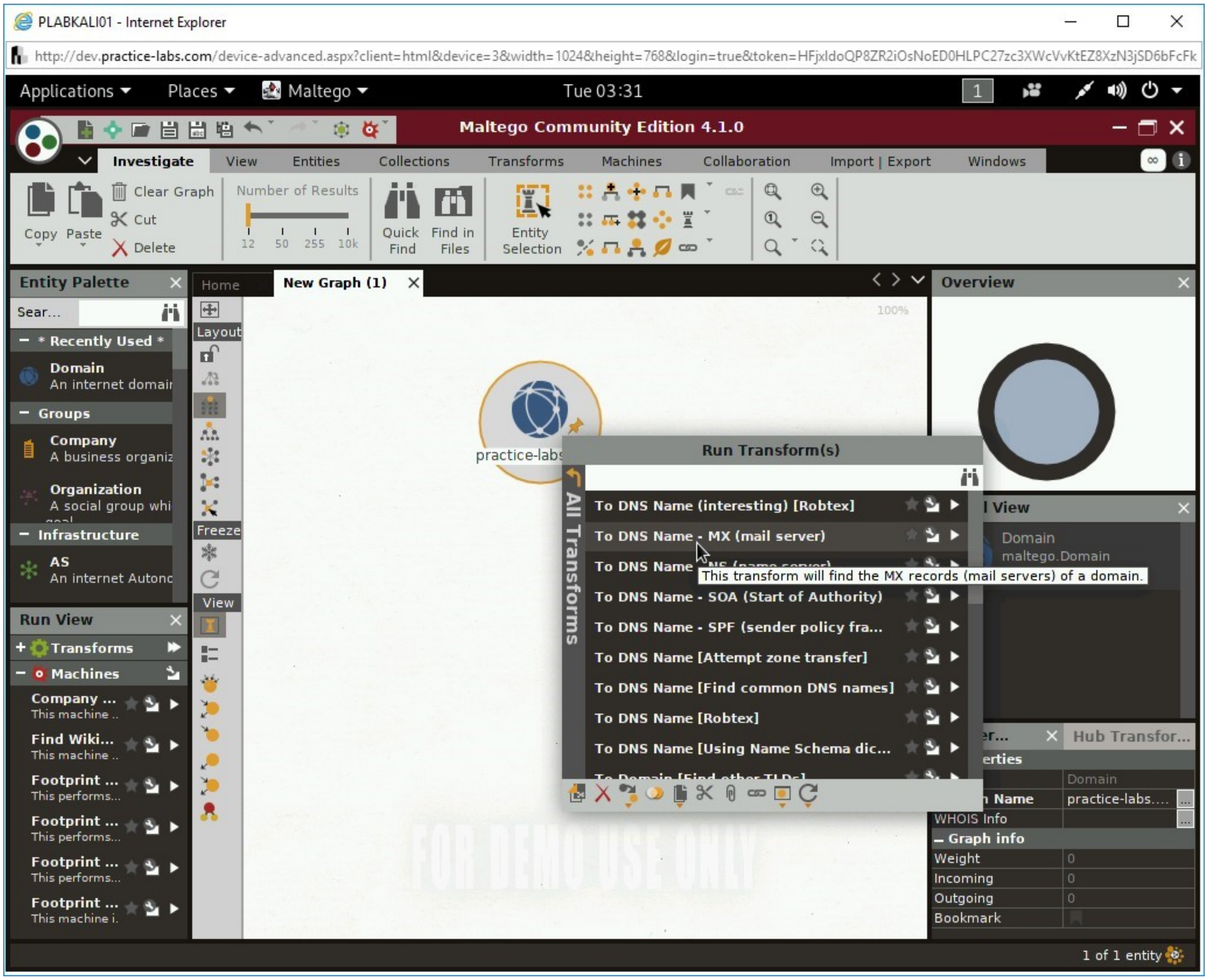


Figure 3.74 Screenshot of PLABKALI01: Selecting All Transforms in the Run Transform dialog box.

## Step 12

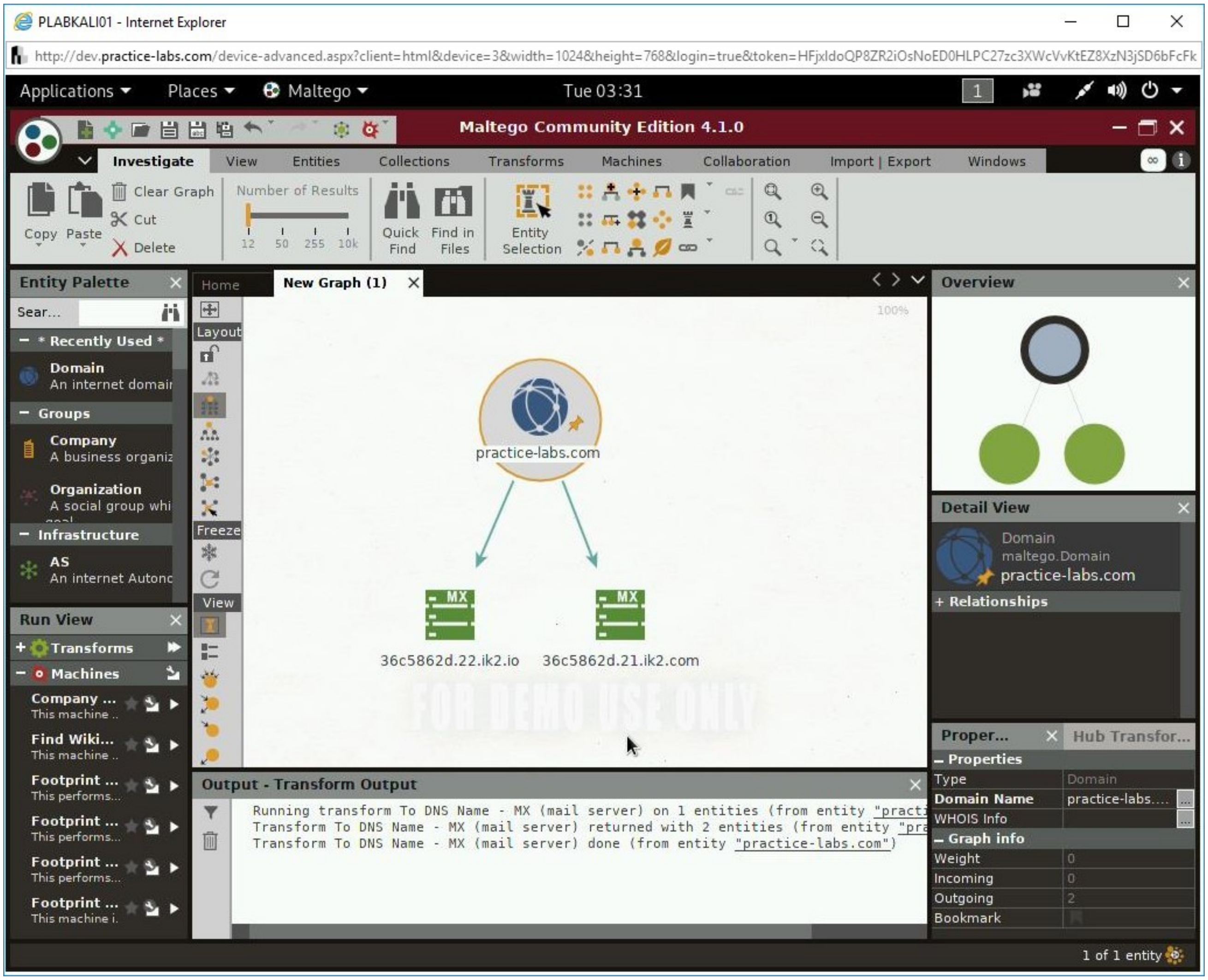
The **Run Transform(s)** dialog box is displayed. To find the mail servers for the **practice-labs.com** domain, select **To DNS Name - MX (mail server)**.



This transform will find the MX records (mail servers) of a domain.

Figure 3.75 Screenshot of PLABKALI01: Selecting the To DNS Name - MX (mail server) option from the Run Transform(s) dialog box.

Notice that it has found two mail servers.



```
Running transform To DNS Name - MX (mail server) on 1 entities (from entity "practi
Transform To DNS Name - MX (mail server) returned with 2 entities (from entity "pra
Transform To DNS Name - MX (mail server) done (from entity "practice-labs.com")
```

– Properties

| | |
|---|---|
| Type | Domain |
| Domain Name | practice-labs.... |
| WHOIS Info | |

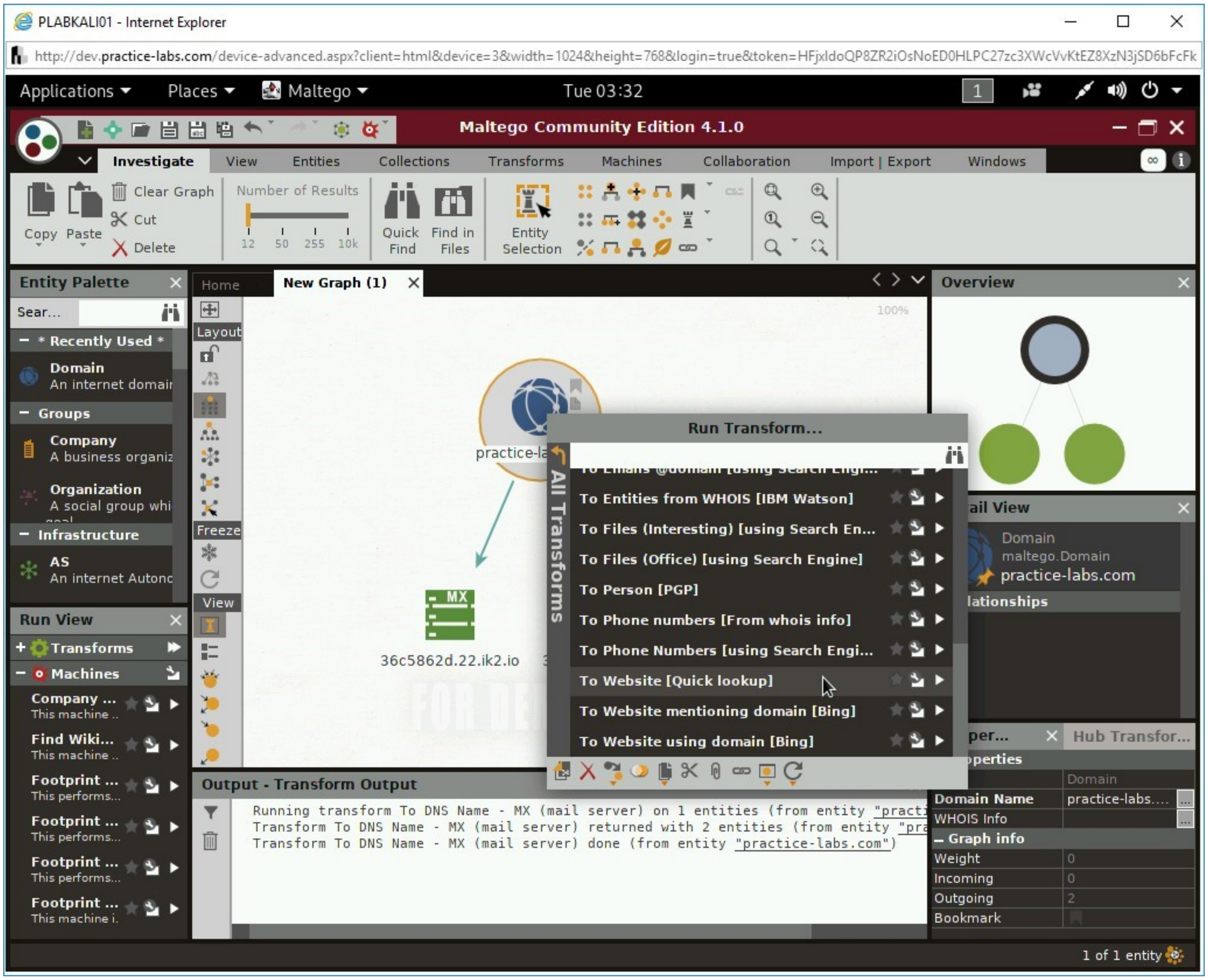
– Graph info

| | |
|---|---|
| Weight | 0 |
| Incoming | 0 |
| Outgoing | 2 |
| Bookmark | |

Figure 3.76 Screenshot of PLABKALI01: Showing the result of running the selected transform.

## *Step 13*

Right-click the domain name and select **To Website [Quick lookup]**.



Output - Transform Output

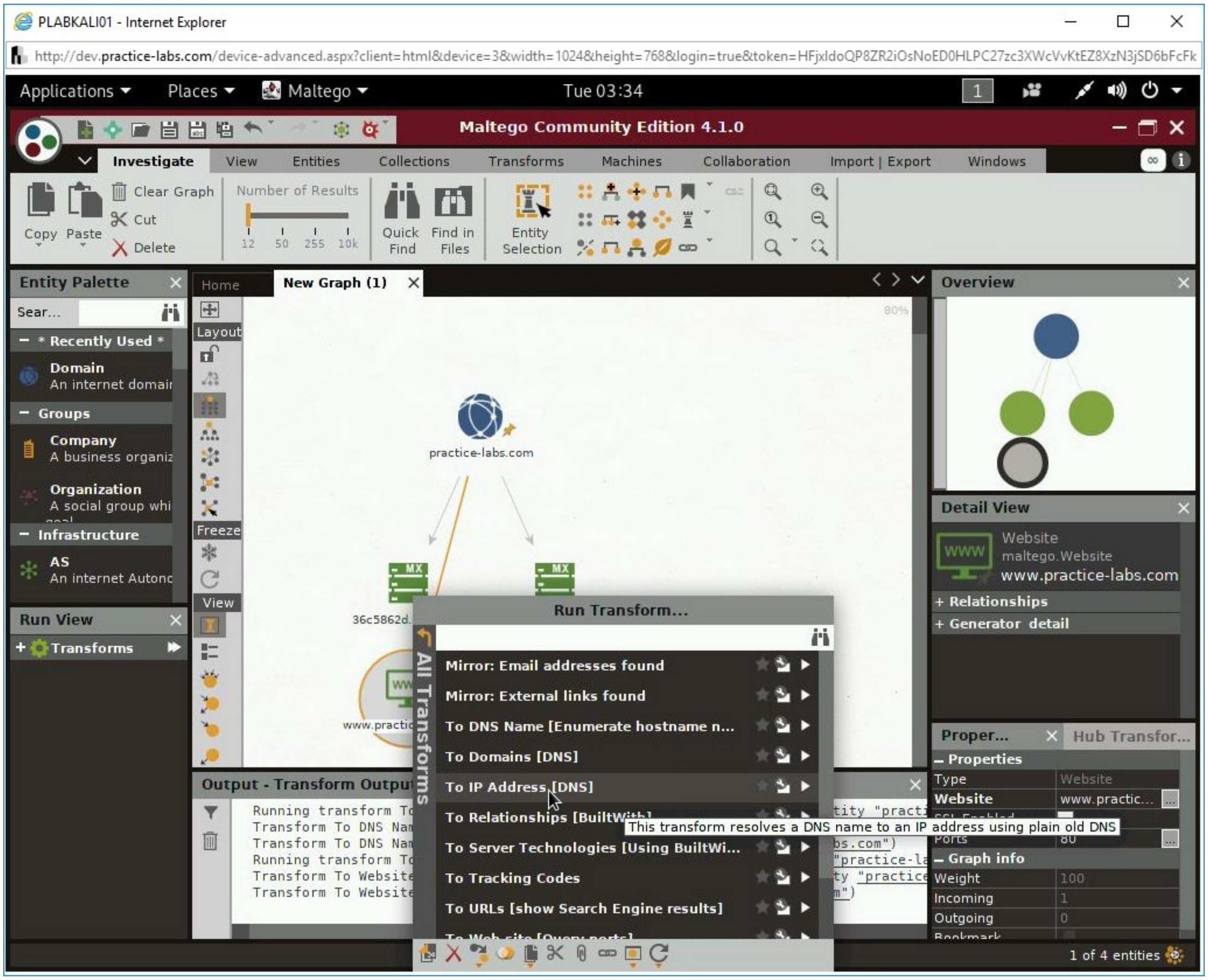
```
Running transform To DNS Name - MX (mail server) on 1 entities (from entity "practi
Transform To DNS Name - MX (mail server) returned with 2 entities (from entity "pra
Transform To DNS Name - MX (mail server) done (from entity "practice-labs.com")
```

Figure 3.77 Screenshot of PLABKALI01: Selecting the To Website [Quick lookup] transform.

## Step 14

A Website has been found.

Right-click the Website icon and select **To IP Address [DNS]**.



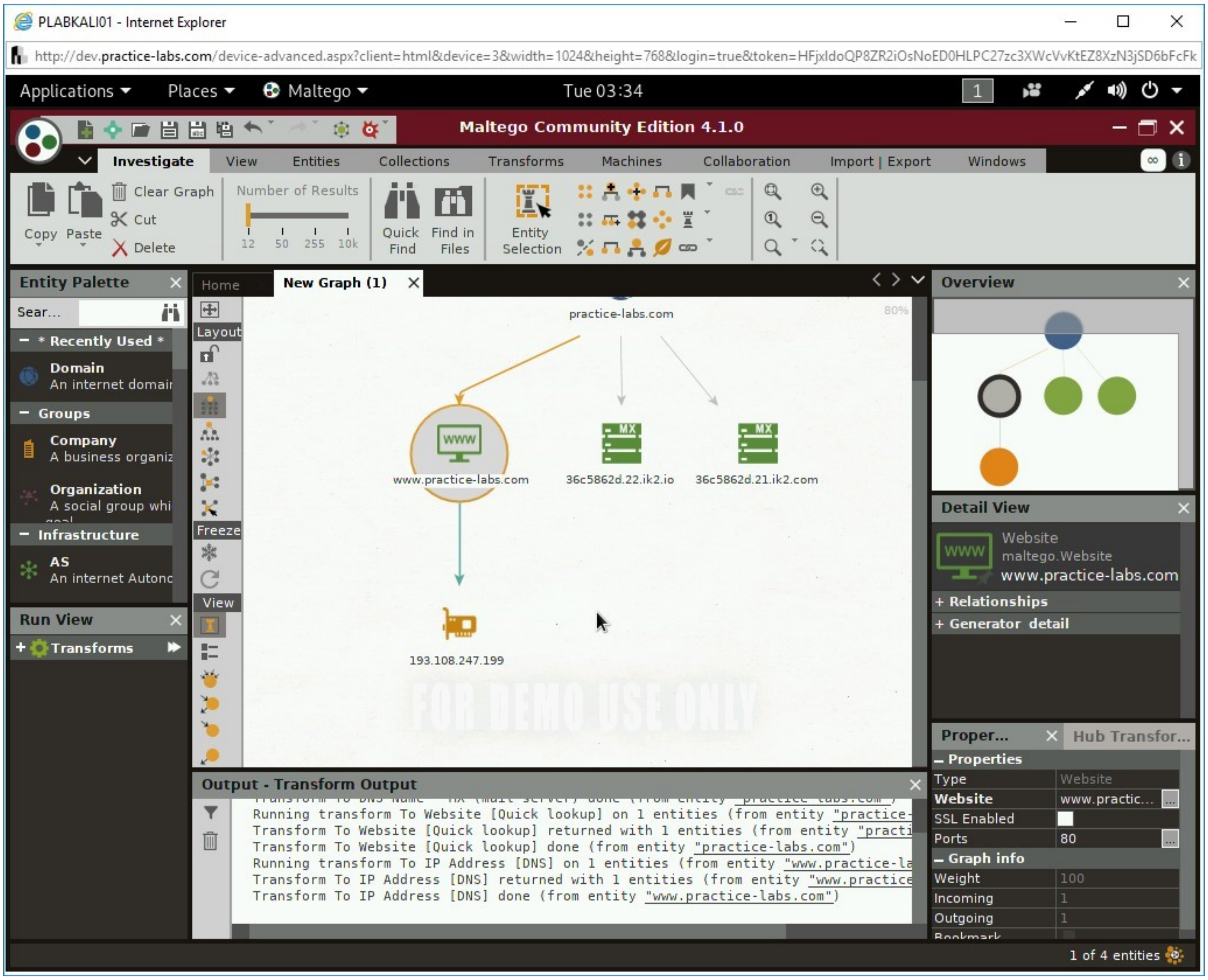
```
Running transform To
Transform To DNS Nam
Transform To DNS Nam
Running transform To
Transform To Website
Transform To Website
```

This transform resolves a DNS name to an IP address using plain old DNS

| | |
|---|---|
| Type | Website |
| Website | www.practic... |
| SSL Enabled | |
| Ports | 80 |
| Weight | 100 |
| Incoming | 1 |
| Outgoing | 0 |

Figure 3.78 Screenshot of PLABKALI01: Selecting the To IP Address [DNS] transform on the selected Website.

Notice that it has translated the DNS name of the Website to an IP address.



Output - Transform Output

```
Running transform To Website [Quick lookup] on 1 entities (from entity "practice-
Transform To Website [Quick lookup] returned with 1 entities (from entity "practi
Transform To Website [Quick lookup] done (from entity "practice-labs.com")
Running transform To IP Address [DNS] on 1 entities (from entity "www.practice-la
Transform To IP Address [DNS] returned with 1 entities (from entity "www.practice
Transform To IP Address [DNS] done (from entity "www.practice-labs.com")
```

– Properties

| | |
|---|---|
| Type | Website |
| **Website** | www.practic... |
| SSL Enabled | □ |
| Ports | 80 |

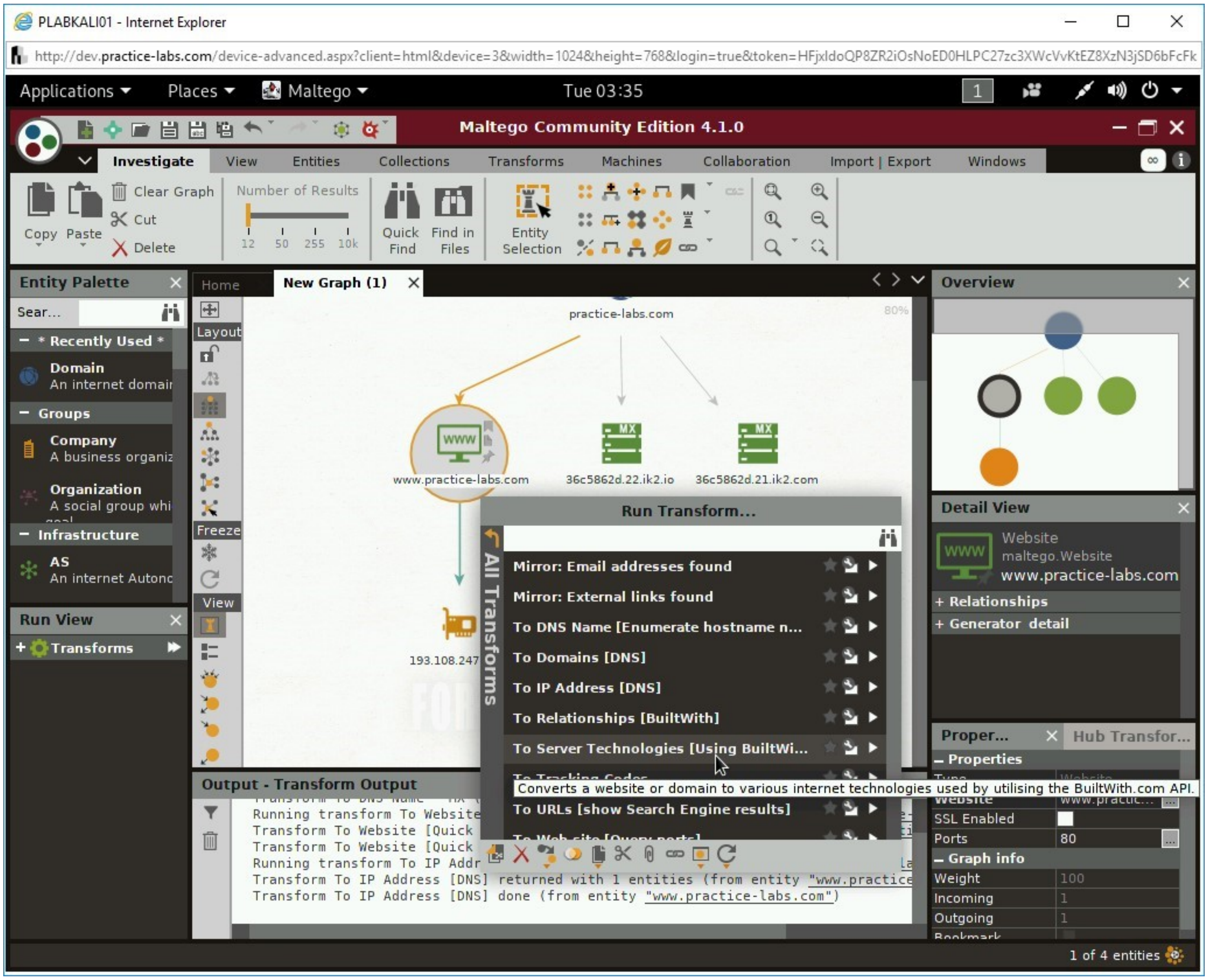
– Graph info

| | |
|---|---|
| Weight | 100 |
| Incoming | 1 |
| Outgoing | 1 |

Figure 3.79 Screenshot of PLABKALI01: Showing the IP address of the Website.

## *Step 15*

Again, right-click the Website icon and select **To Server Technologies [Using BuiltWi...**

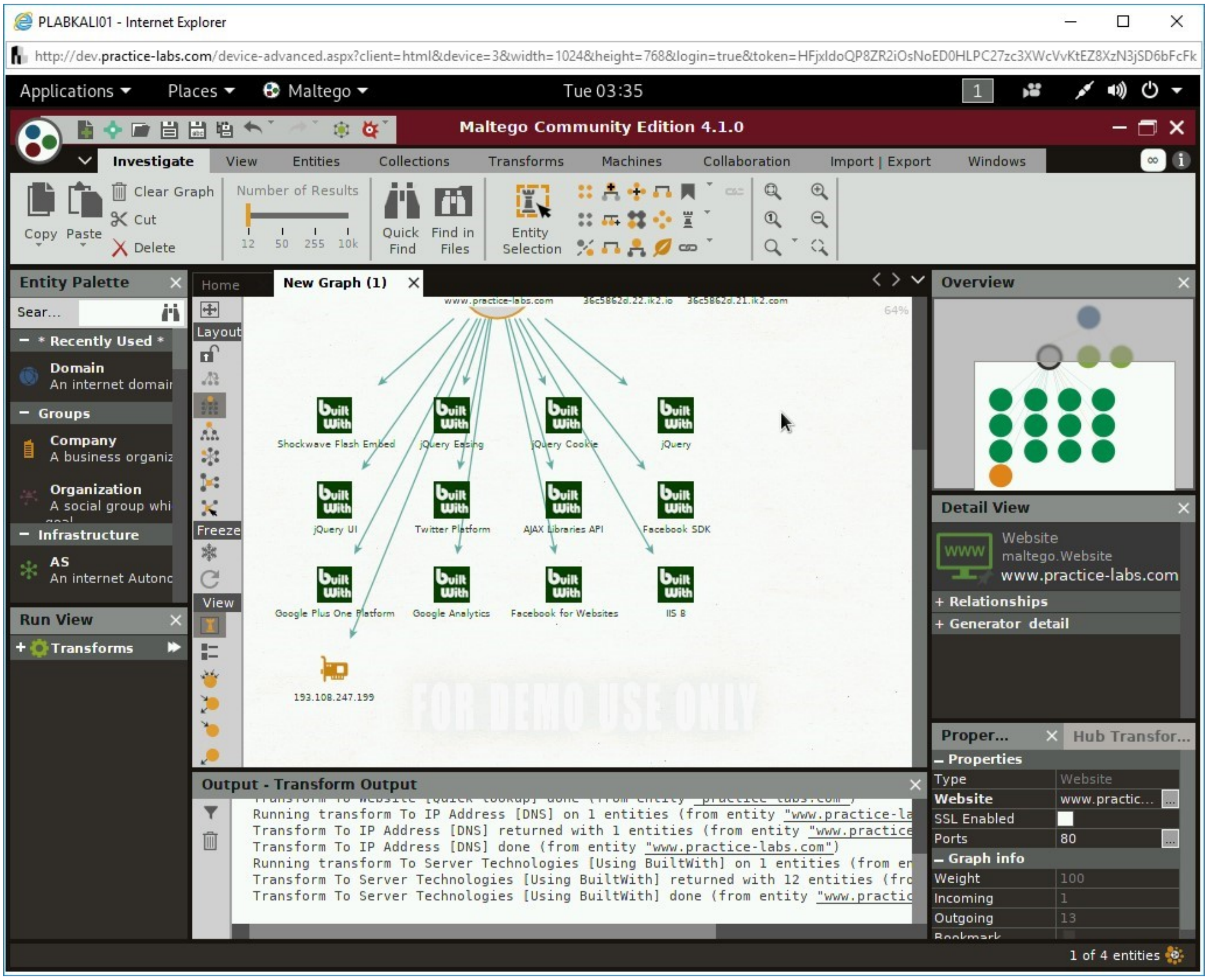


Converts a website or domain to various internet technologies used by utilising the BuiltWith.com API.

```
Transform To DNS Name - MX (
Running transform To Website
Transform To Website [Quick
Transform To Website [Quick
Running transform To IP Addr
Transform To IP Address [DNS] returned with 1 entities (from entity "www.practice
Transform To IP Address [DNS] done (from entity "www.practice-labs.com")
```

Figure 3.80 Screenshot of PLABKALI01: Selecting the To Server Technologies [Using BuiltWi... transform.

The technologies used in the Website are now listed. Notice that it has displayed **IIS 8**, which can help you in deciding the next course of action in ethical hacking.



```
Running transform To IP Address [DNS] on 1 entities (from entity "www.practice-la
Transform To IP Address [DNS] returned with 1 entities (from entity "www.practice
Transform To IP Address [DNS] done (from entity "www.practice-labs.com")
Running transform To Server Technologies [Using BuiltWith] on 1 entities (from en
Transform To Server Technologies [Using BuiltWith] returned with 12 entities (fro
Transform To Server Technologies [Using BuiltWith] done (from entity "www.practic
```

| | |
|---|---|
| – Properties | |
| Type | Website |
| Website | www.practic... |
| SSL Enabled | □ |
| Ports | 80 |
| – Graph info | |
| Weight | 100 |
| Incoming | 1 |
| Outgoing | 13 |

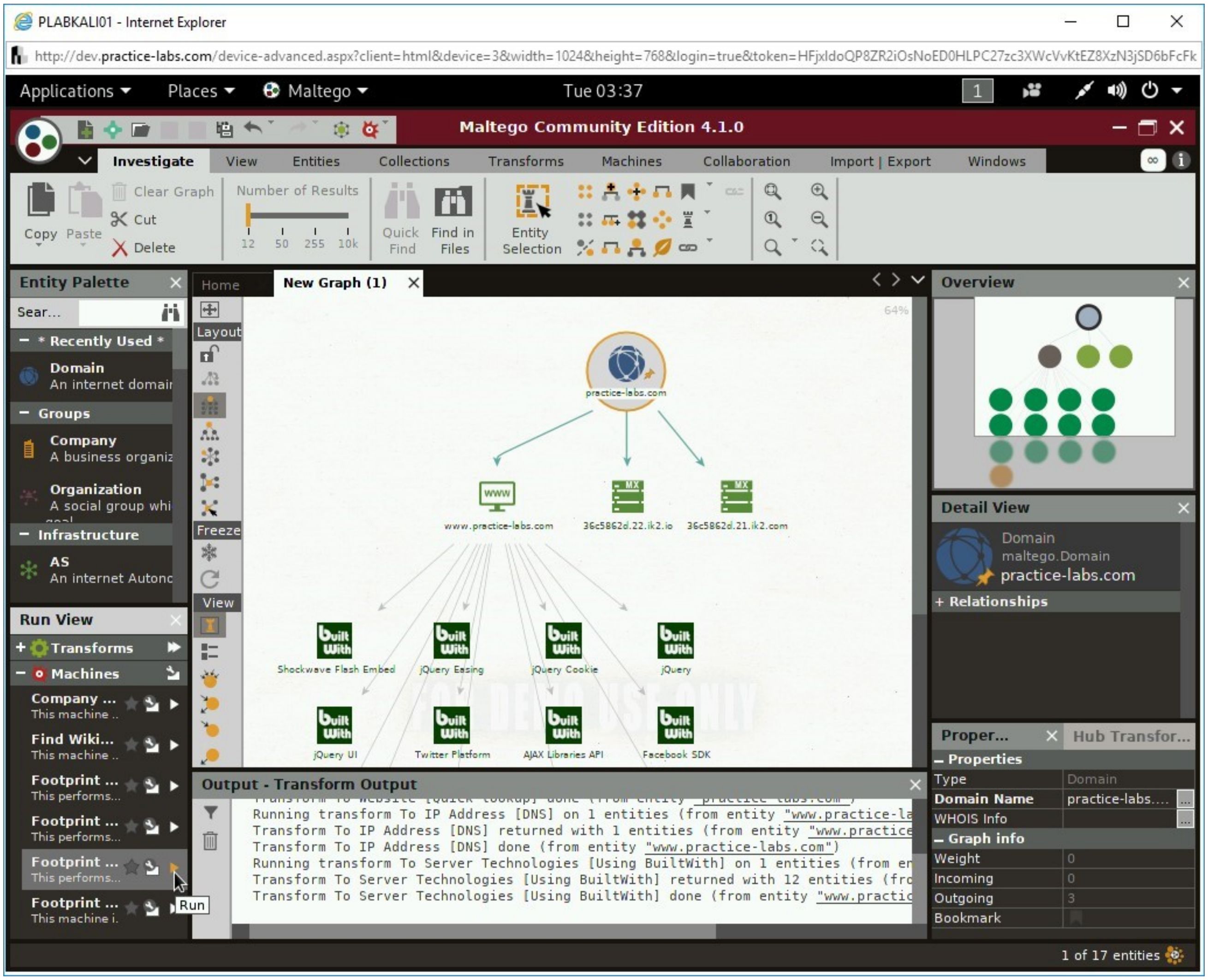
Figure 3.81 Screenshot of PLABKALI01: Showing the technologies used in the Website.

## Step 16

Let's do footprinting on the domain.

Select the domain icon and then in the **Machines** section in the left pane, select **Footprint**, which is the third Footprint... option. Click **Run** next to it.

> ***Note:*** *If the left pane is not showing the Run View with the Machines section, please select the Windows tab at the top, far most right and then select Run View.*



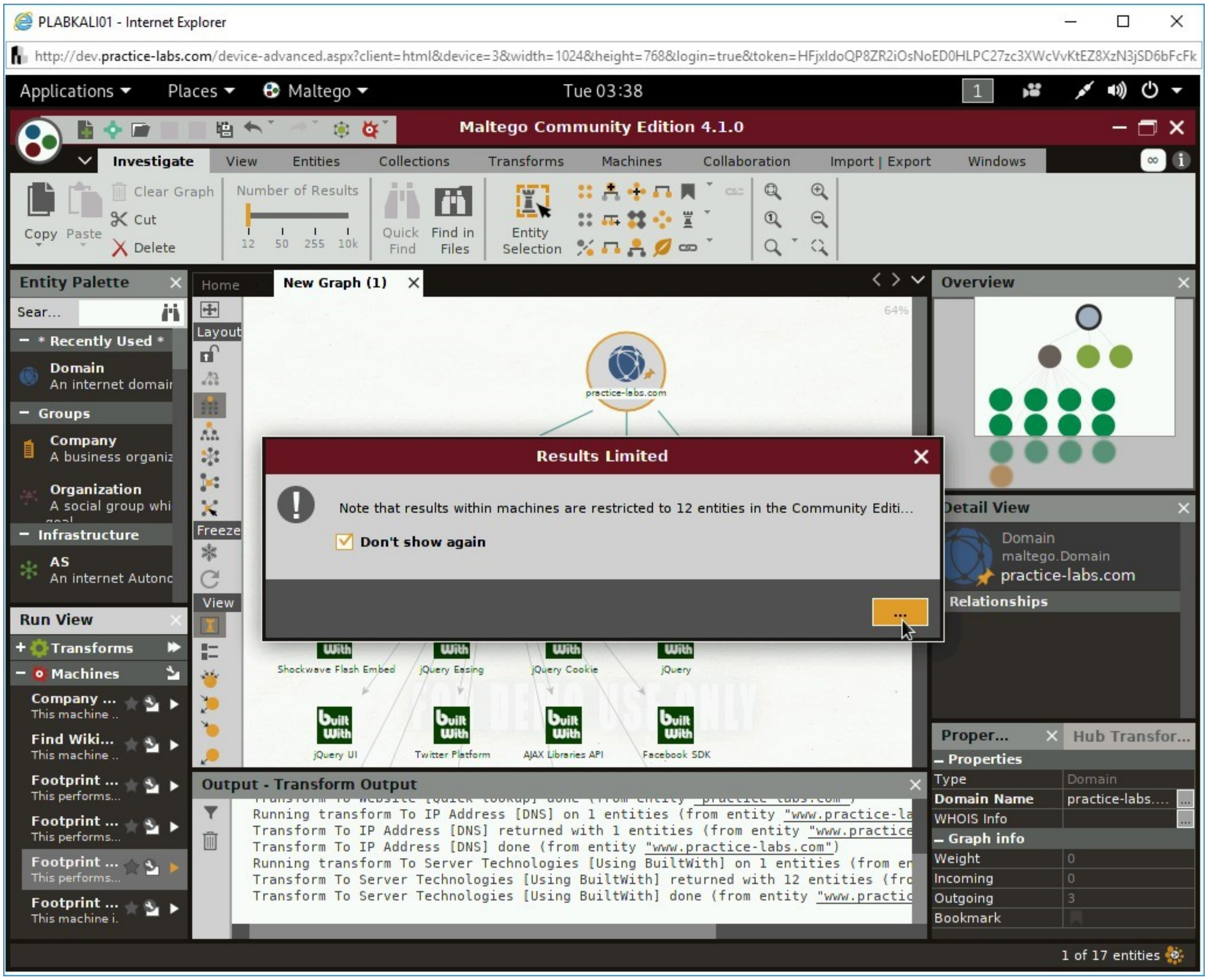
Output - Transform Output

```
Transform To Website [Quick lookup] done (from entity "practice-labs.com")
Running transform To IP Address [DNS] on 1 entities (from entity "www.practice-la
Transform To IP Address [DNS] returned with 1 entities (from entity "www.practice
Transform To IP Address [DNS] done (from entity "www.practice-labs.com")
Running transform To Server Technologies [Using BuiltWith] on 1 entities (from en
Transform To Server Technologies [Using BuiltWith] returned with 12 entities (fro
Transform To Server Technologies [Using BuiltWith] done (from entity "www.practic
```

Figure 3.82 Screenshot of PLABKALI01: Selecting the Footprint option from the Machines section.

## Step 17

Because you are using a **Community** version, you are prompted with a message that only **12 entities** will be displayed. Select **Don’t show again** and click ….



**Results Limited**

Note that results within machines are restricted to 12 entities in the Community Editi...

☑ Don't show again

...

Output - Transform Output

```
Running transform To IP Address [DNS] on 1 entities (from entity "www.practice-la
Transform To IP Address [DNS] returned with 1 entities (from entity "www.practice
Transform To IP Address [DNS] done (from entity "www.practice-labs.com")
Running transform To Server Technologies [Using BuiltWith] on 1 entities (from en
Transform To Server Technologies [Using BuiltWith] returned with 12 entities (fro
Transform To Server Technologies [Using BuiltWith] done (from entity "www.practic
```

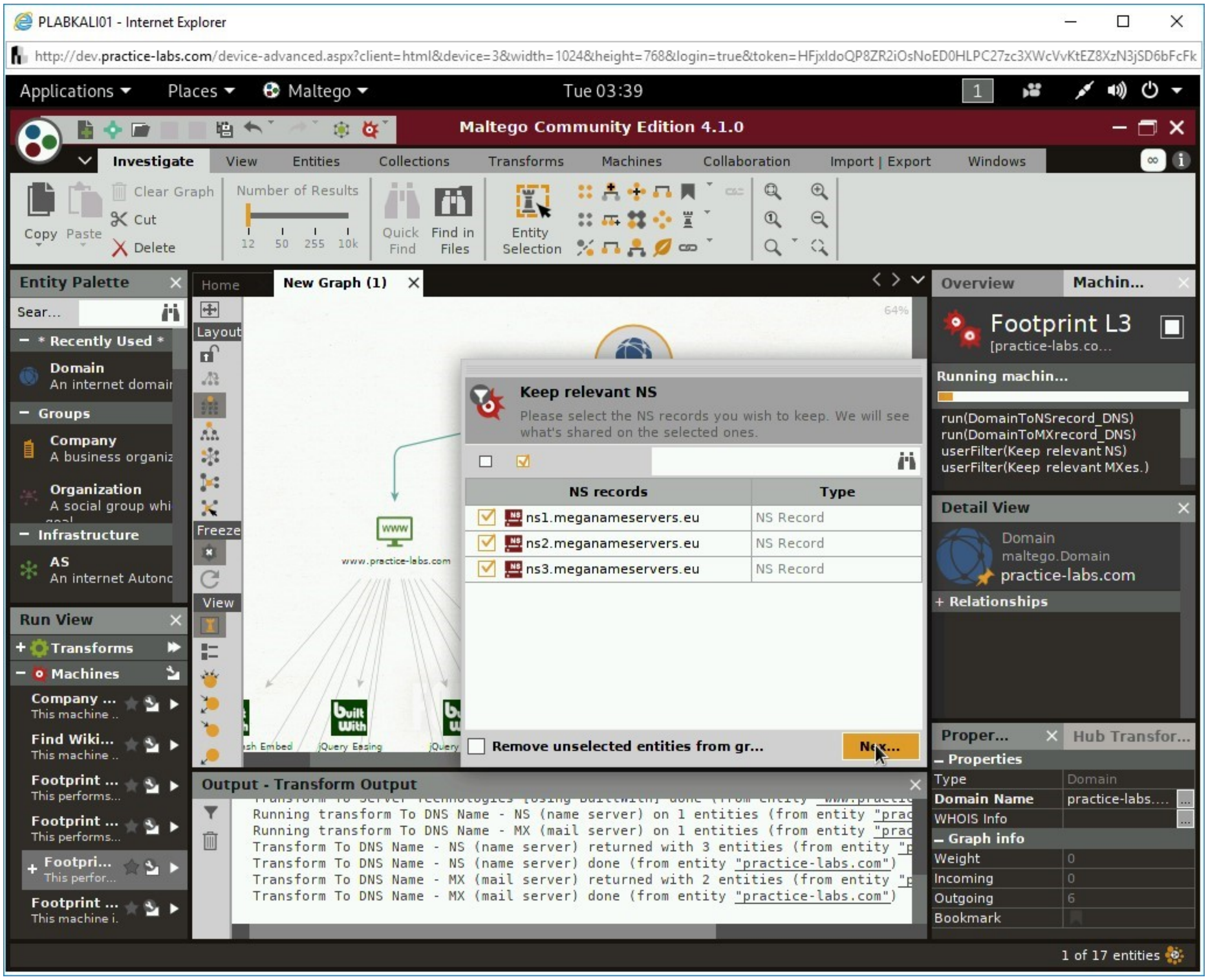
| Properties |  |
|---|---|
| Type | Domain |
| Domain Name | practice-labs.... |
| WHOIS Info |  |

| Graph info |  |
|---|---|
| Weight | 0 |
| Incoming | 0 |
| Outgoing | 3 |
| Bookmark |  |

Figure 3.83 Screenshot of PLABKALI01: Displaying the warning of the limitation of the results.

## Step 18

The **Keep relevant NS** dialog box is displayed. Click **Nex...**



PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=HFjxldoQP8ZR2iOsNoED0HLPC27zc3XWcVvKtEZ8XzN3jSD6bFcFk
Applications Places Maltego Tue 03:39
Maltego Community Edition 4.1.0
Investigate View Entities Collections Transforms Machines Collaboration Import | Export Windows
Copy Paste Clear Graph Cut Delete Number of Results 12 50 255 10k Quick Find Find in Files Entity Selection
Entity Palette
Recently Used
Groups
Infrastructure
Run View
Transforms
Machines
Home New Graph (1)
www.practice-labs.com
Overview Machin...
Detail View
Proper... Hub Transfor...
Output - Transform Output
1 of 17 entities

**Keep relevant NS**

Please select the NS records you wish to keep. We will see what's shared on the selected ones.

| NS records | Type |
|---|---|
| ☑ ns1.meganameservers.eu | NS Record |
| ☑ ns2.meganameservers.eu | NS Record |
| ☑ ns3.meganameservers.eu | NS Record |

□ Remove unselected entities from gr... Nex...

Footprint L3
[practice-labs.co...
Running machin...

```
run(DomainToNSrecord_DNS)
run(DomainToMXrecord_DNS)
userFilter(Keep relevant NS)
userFilter(Keep relevant MXes.)
```

Domain
maltego.Domain
practice-labs.com

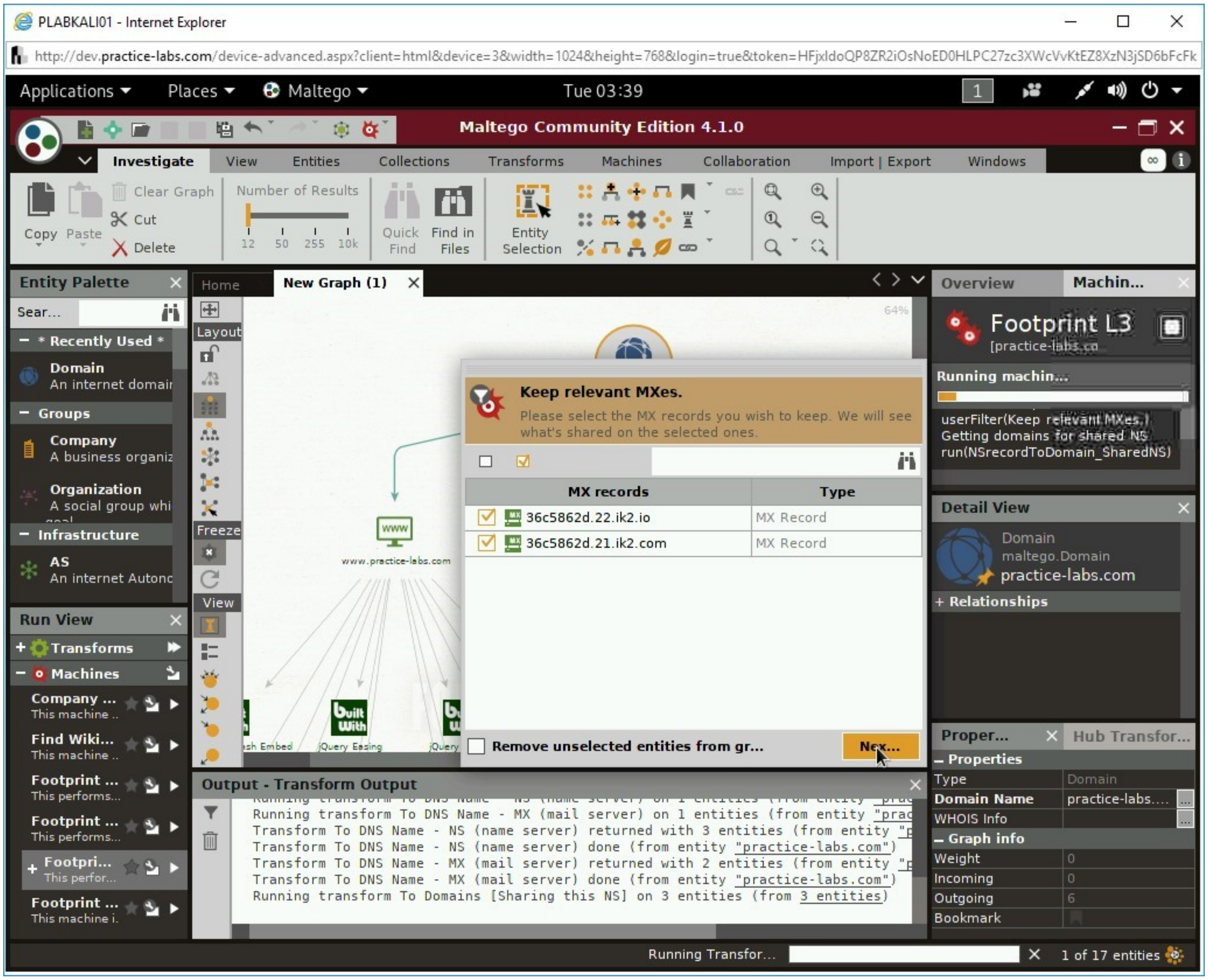
| | |
|---|---|
| Properties | |
| Type | Domain |
| Domain Name | practice-labs.... |
| WHOIS Info | |
| Graph info | |
| Weight | 0 |
| Incoming | 0 |
| Outgoing | 6 |
| Bookmark | |

```
Running transform To DNS Name - NS (name server) on 1 entities (from entity "prac
Running transform To DNS Name - MX (mail server) on 1 entities (from entity "prac
Transform To DNS Name - NS (name server) returned with 3 entities (from entity "p
Transform To DNS Name - NS (name server) done (from entity "practice-labs.com")
Transform To DNS Name - MX (mail server) returned with 2 entities (from entity "p
Transform To DNS Name - MX (mail server) done (from entity "practice-labs.com")
```

Figure 3.84 Screenshot of PLABKALI01: Showing the existing NS records.

## Step 19

The **Keep relevant MXes**. dialog box is displayed. Click **Nex...**



**Keep relevant MXes.**

Please select the MX records you wish to keep. We will see what's shared on the selected ones.

| | MX records | Type |
|---|---|---|
| ☑ | 36c5862d.22.ik2.io | MX Record |
| ☑ | 36c5862d.21.ik2.com | MX Record |

☐ Remove unselected entities from gr...

Nex...

userFilter(Keep relevant MXes.)
Getting domains for shared NS
run(NSrecordToDomain_SharedNS)

Domain
maltego.Domain
practice-labs.com

| Properties | |
|---|---|
| Type | Domain |
| Domain Name | practice-labs.... |
| WHOIS Info | |

| Graph info | |
|---|---|
| Weight | 0 |
| Incoming | 0 |
| Outgoing | 6 |
| Bookmark | |

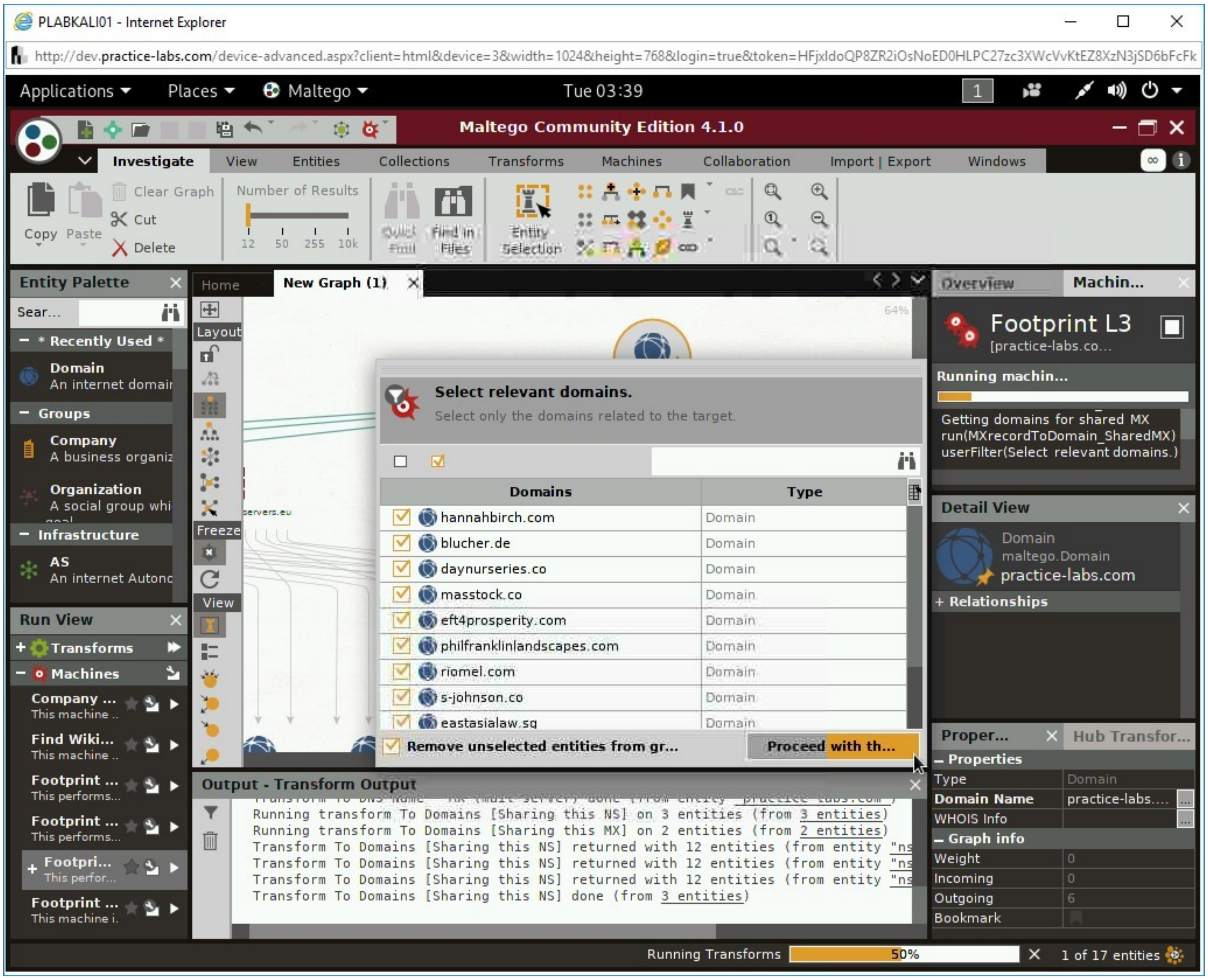
Output - Transform Output

```
Running transform To DNS Name - MX (mail server) on 1 entities (from entity "prac
Transform To DNS Name - NS (name server) returned with 3 entities (from entity "p
Transform To DNS Name - NS (name server) done (from entity "practice-labs.com")
Transform To DNS Name - MX (mail server) returned with 2 entities (from entity "p
Transform To DNS Name - MX (mail server) done (from entity "practice-labs.com")
Running transform To Domains [Sharing this NS] on 3 entities (from 3 entities)
```

Figure 3.85 Screenshot of PLABKALI01: Showing the existing MX records.

## Step 20

On the **Select relevant domains.** dialog box, deselect all domain names and click **Proceed with th...**


PLABKALI01 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=HFjxldoQP8ZR2iOsNoED0HLPC27zc3XWcVvKtEZ8XzN3jSD6bFcFk
Applications
Places
Maltego
Tue 03:39
Maltego Community Edition 4.1.0
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Entity Palette
Run View
Overview
Machin...
Detail View
Proper...
Hub Transfor...

Footprint L3
[practice-labs.co...
Running machin...

Getting domains for shared MX
run(MXrecordToDomain_SharedMX)
userFilter(Select relevant domains.)

**Select relevant domains.**

Select only the domains related to the target.

| Domains | Type |
|---|---|
| ☑ hannahbirch.com | Domain |
| ☑ blucher.de | Domain |
| ☑ daynurseries.co | Domain |
| ☑ masstock.co | Domain |
| ☑ eft4prosperity.com | Domain |
| ☑ philfranklinlandscapes.com | Domain |
| ☑ riomel.com | Domain |
| ☑ s-johnson.co | Domain |
| ☑ eastasialaw.sg | Domain |

☑ Remove unselected entities from gr...

Proceed with th...

Output - Transform Output

```
Running transform To Domains [Sharing this NS] on 3 entities (from 3 entities)
Running transform To Domains [Sharing this MX] on 2 entities (from 2 entities)
Transform To Domains [Sharing this NS] returned with 12 entities (from entity "ns
Transform To Domains [Sharing this NS] returned with 12 entities (from entity "ns
Transform To Domains [Sharing this NS] returned with 12 entities (from entity "ns
Transform To Domains [Sharing this NS] done (from 3 entities)
```

| Properties | |
|---|---|
| Type | Domain |
| Domain Name | practice-labs.... |
| WHOIS Info | |
| Graph info | |
| Weight | 0 |
| Incoming | 0 |
| Outgoing | 6 |
| Bookmark | |

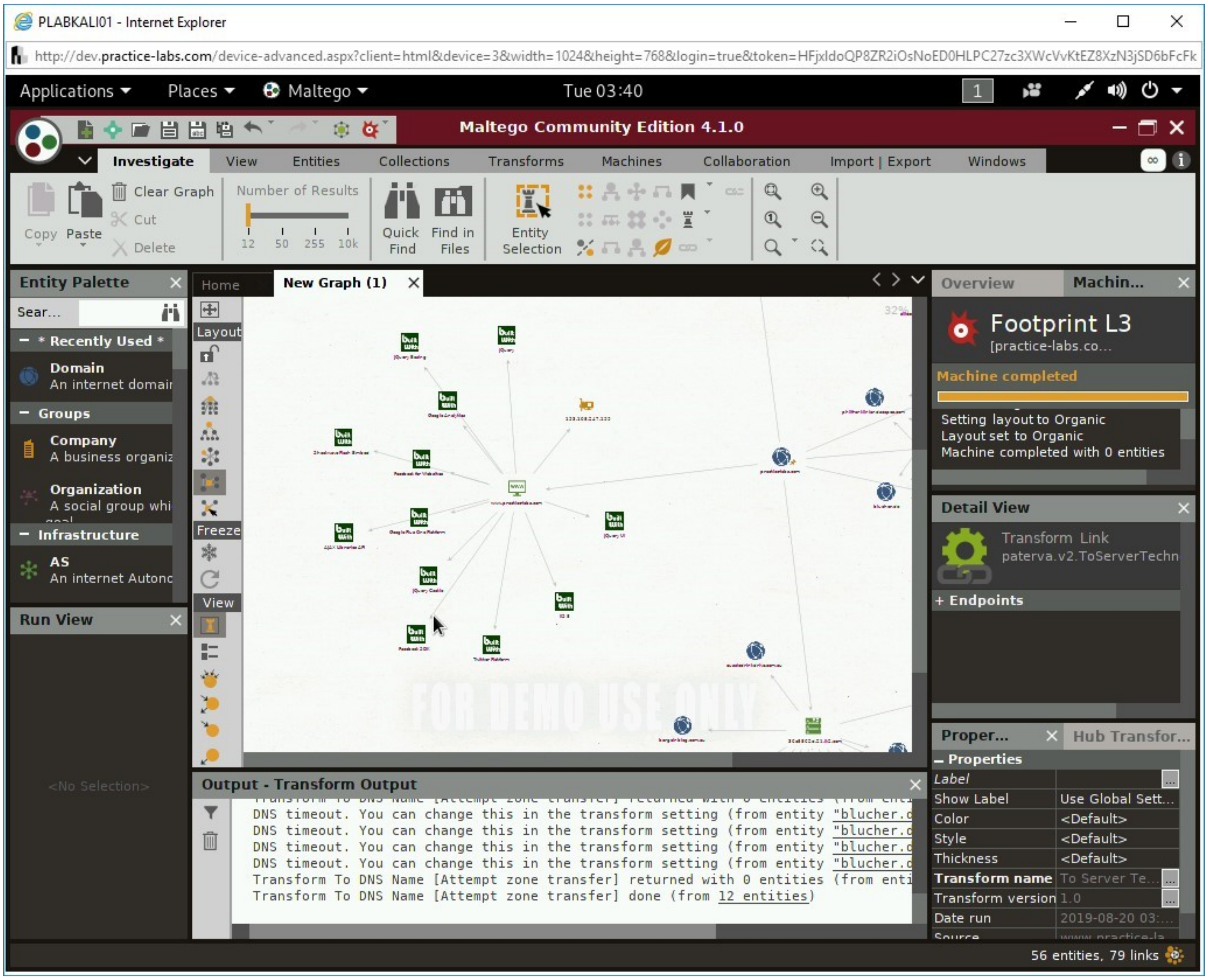
Running Transforms 50% 1 of 17 entities

Figure 3.86 Screenshot of PLABKALI01: Deselecting the domain names.

## Step 21

On the **Select relevant domains.** dialog box, deselect all domain names and click **Proceed with th…**

The footprinting process is now complete with **12 entities**.



```
Setting layout to Organic
Layout set to Organic
Machine completed with 0 entities
```

```
DNS timeout. You can change this in the transform setting (from entity "blucher.c
DNS timeout. You can change this in the transform setting (from entity "blucher.c
DNS timeout. You can change this in the transform setting (from entity "blucher.c
DNS timeout. You can change this in the transform setting (from entity "blucher.c
Transform To DNS Name [Attempt zone transfer] returned with 0 entities (from enti
Transform To DNS Name [Attempt zone transfer] done (from 12 entities)
```

| Proper... | Hub Transfor... |
|---|---|
| Properties | |
| Label | |
| Show Label | Use Global Sett... |
| Color | <Default> |
| Style | <Default> |
| Thickness | <Default> |
| Transform name | To Server Te... |
| Transform version | 1.0 |
| Date run | 2019-08-20 03:... |

Figure 3.87 Screenshot of PLABKALI01: Showing the output of the Footprint option.

## Task 9 - Use the AnyWho Website

There are a number of tools available on the Internet that can help you find information about specific people, one of these is AnyWho.

To use the AnyWho Website, perform the following steps:

### *Step 1*

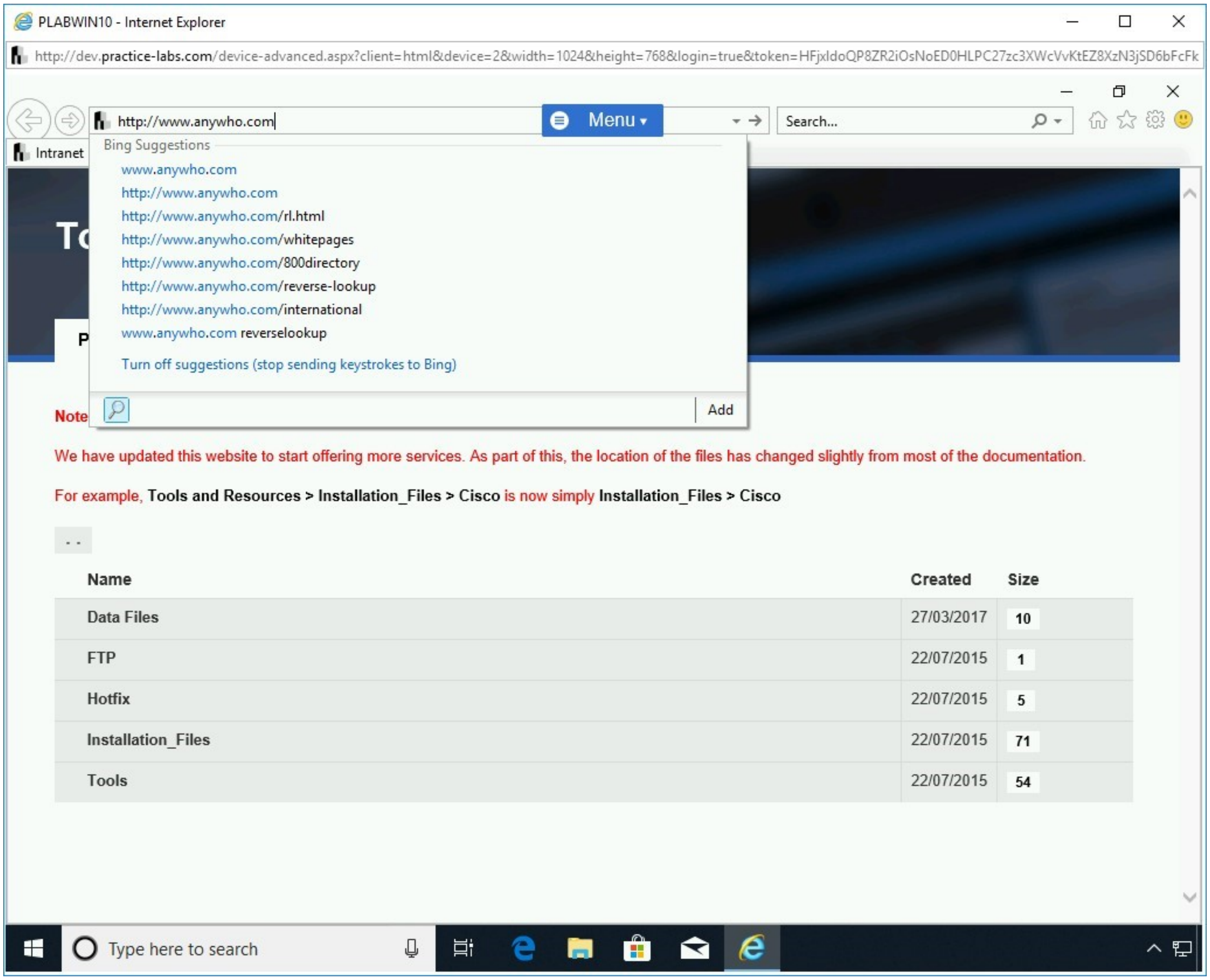
Connect to **PLABWIN10**.

Open **Internet Explorer**.

In the address bar, type the following URL:

```
http://www.anywho.com
```

Press **Enter**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=HFjxldoQP8ZR2iOsNoED0HLPC27zc3XWcVvKtEZ8XzN3jSD6bFcFk
http://www.anywho.com
Menu
Search...
Intranet
Bing Suggestions
www.anywho.com
http://www.anywho.com
http://www.anywho.com/rl.html
http://www.anywho.com/whitepages
http://www.anywho.com/800directory
http://www.anywho.com/reverse-lookup
http://www.anywho.com/international
www.anywho.com reverselookup
Turn off suggestions (stop sending keystrokes to Bing)
Add
Type here to search

Note

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

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

. .

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

Figure 3.88 Screenshot of PLABWIN10: Entering the AnyWho Website URL in the Internet Explorer address bar.

## *Step 2*

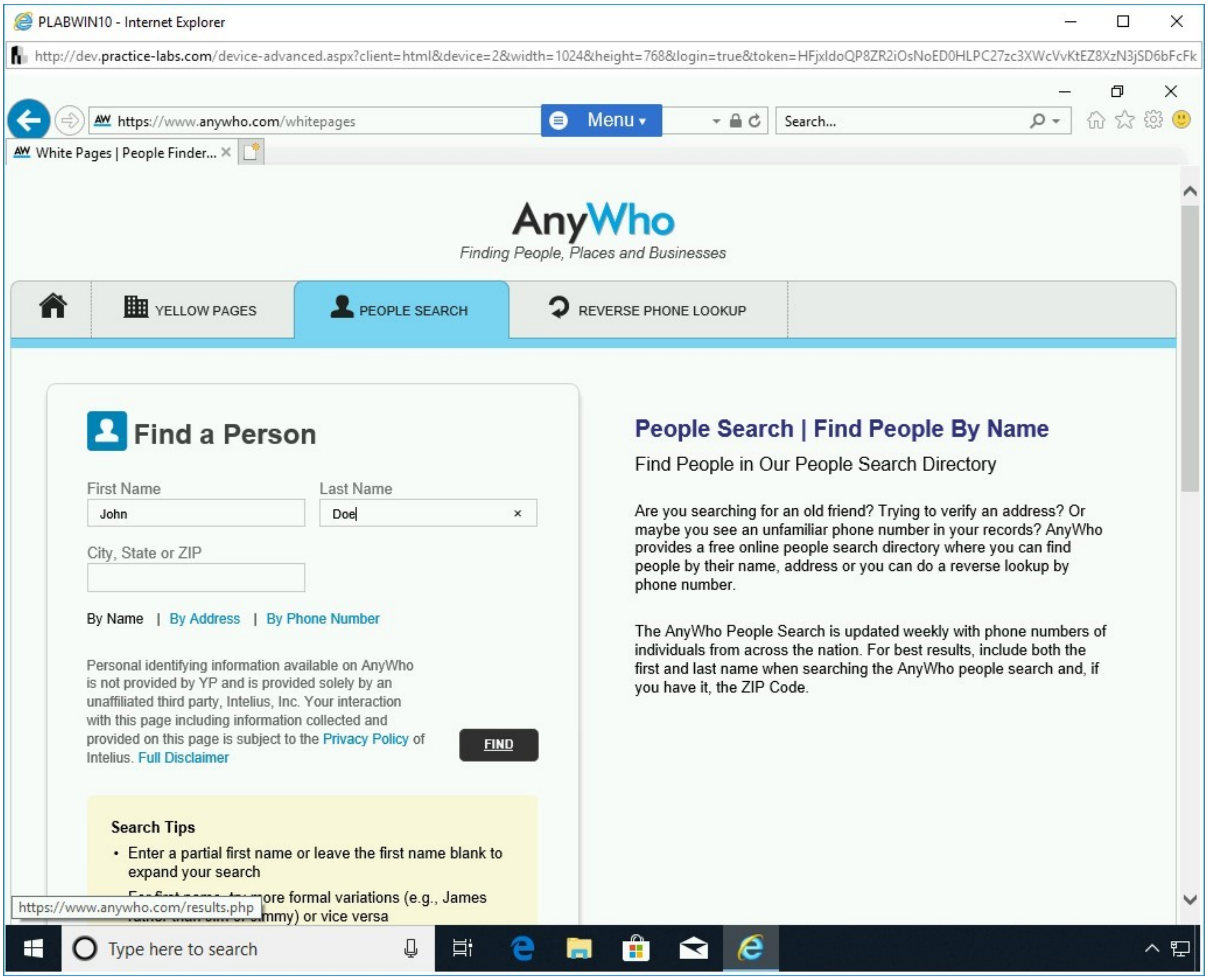
The AnyWho homepage is loaded.

Enter the following information:

```
First Name: John
Last Name: Doe
```

Click **Find**.

> ***Note:*** *For this task, a fake name is being used. You can use your own name to search in the AnyWho database.*



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=HFjxIdoQP8ZR2iOsNoED0HLPC27zc3XWcVvKtEZ8XzN3jSD6bFcFk
https://www.anywho.com/whitepages
Menu
Search...
White Pages | People Finder...
AnyWho
Finding People, Places and Businesses
YELLOW PAGES
PEOPLE SEARCH
REVERSE PHONE LOOKUP
Find a Person
By Name | By Address | By Phone Number
FIND
https://www.anywho.com/results.php
Type here to search

First Name: John

Last Name: Doe

City, State or ZIP:

Personal identifying information available on AnyWho is not provided by YP and is provided solely by an unaffiliated third party, Intelius, Inc. Your interaction with this page including information collected and provided on this page is subject to the Privacy Policy of Intelius. Full Disclaimer

Search Tips

- Enter a partial first name or leave the first name blank to expand your search
- For first name, try more formal variations (e.g., James rather than Jim or Jimmy) or vice versa

People Search | Find People By Name

Find People in Our People Search Directory

Are you searching for an old friend? Trying to verify an address? Or maybe you see an unfamiliar phone number in your records? AnyWho provides a free online people search directory where you can find people by their name, address or you can do a reverse lookup by phone number.

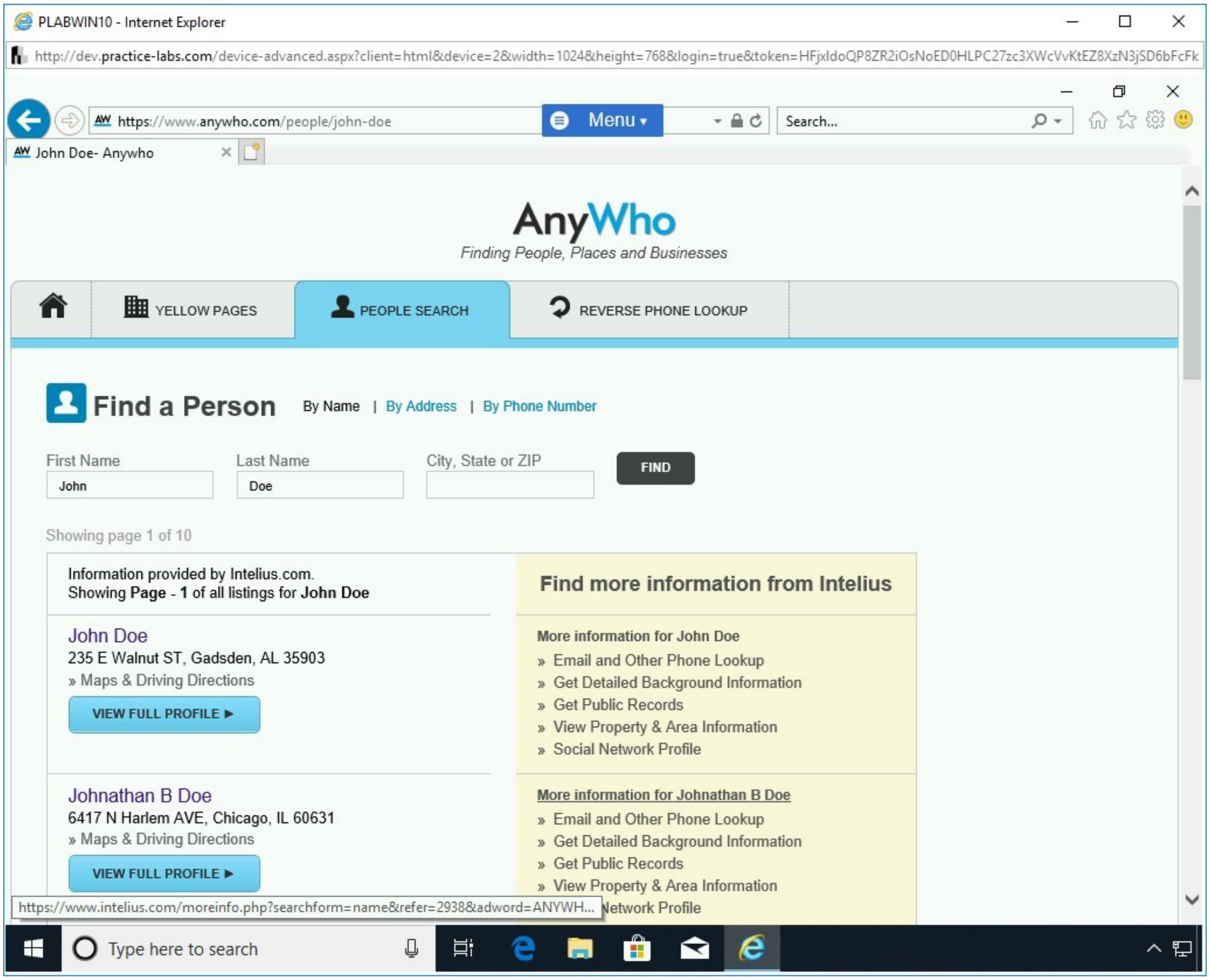
The AnyWho People Search is updated weekly with phone numbers of individuals from across the nation. For best results, include both the first and last name when searching the AnyWho people search and, if you have it, the ZIP Code.

Figure 3.89 Screenshot of PLABWIN10: Entering the name to search.

## Step 3

Note that several results are displayed.

***Note**: If an AutoComplete notification appears, click **No**.*


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=HFjxldoQP8ZR2iOsNoED0HLPC27zc3XWcVvKtEZ8XzN3jSD6bFcFk
https://www.anywho.com/people/john-doe
Menu
Search...
John Doe- Anywho
AnyWho
Finding People, Places and Businesses
YELLOW PAGES
PEOPLE SEARCH
REVERSE PHONE LOOKUP
Find a Person
By Name | By Address | By Phone Number
FIND
VIEW FULL PROFILE ▶
VIEW FULL PROFILE ▶
Type here to search

First Name: John
Last Name: Doe
City, State or ZIP:

Showing page 1 of 10

Information provided by Intelius.com.
Showing Page - 1 of all listings for John Doe

John Doe
235 E Walnut ST, Gadsden, AL 35903
» Maps & Driving Directions

Johnathan B Doe
6417 N Harlem AVE, Chicago, IL 60631
» Maps & Driving Directions

Find more information from Intelius

More information for John Doe
» Email and Other Phone Lookup
» Get Detailed Background Information
» Get Public Records
» View Property & Area Information
» Social Network Profile

More information for Johnathan B Doe
» Email and Other Phone Lookup
» Get Detailed Background Information
» Get Public Records
» View Property & Area Information
Network Profile

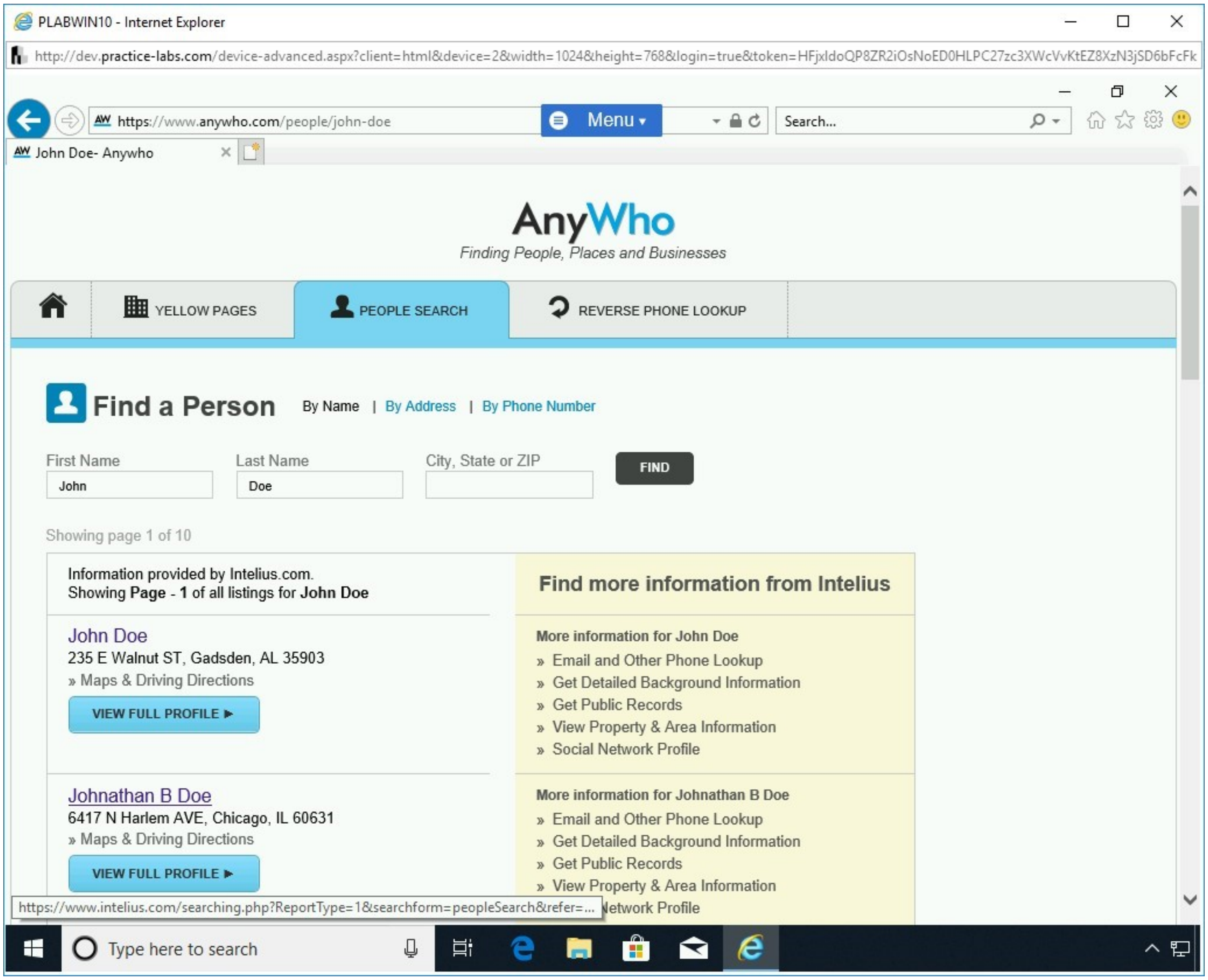
https://www.intelius.com/moreinfo.php?searchform=name&refer=2938&adword=ANYWH...

Figure 3.90 Screenshot of PLABWIN10: Showing the results for the person searched.

## Step 4

Click the second result, which is **John B Doe**.

***Note**: This is a live website; search results may vary.*



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=HFjxldoQP8ZR2iOsNoED0HLPC27zc3XWcVvKtEZ8XzN3jSD6bFcFk
https://www.anywho.com/people/john-doe
Menu
Search...
John Doe- Anywho
AnyWho
Finding People, Places and Businesses
YELLOW PAGES
PEOPLE SEARCH
REVERSE PHONE LOOKUP
Find a Person
By Name | By Address | By Phone Number
FIND
VIEW FULL PROFILE ▶
Type here to search

First Name: John

Last Name: Doe

City, State or ZIP:

Showing page 1 of 10

Information provided by Intelius.com.
Showing Page - 1 of all listings for John Doe

John Doe
235 E Walnut ST, Gadsden, AL 35903
» Maps & Driving Directions

Johnathan B Doe
6417 N Harlem AVE, Chicago, IL 60631
» Maps & Driving Directions

Find more information from Intelius

More information for John Doe
» Email and Other Phone Lookup
» Get Detailed Background Information
» Get Public Records
» View Property & Area Information
» Social Network Profile

More information for Johnathan B Doe
» Email and Other Phone Lookup
» Get Detailed Background Information
» Get Public Records
» View Property & Area Information
» Social Network Profile

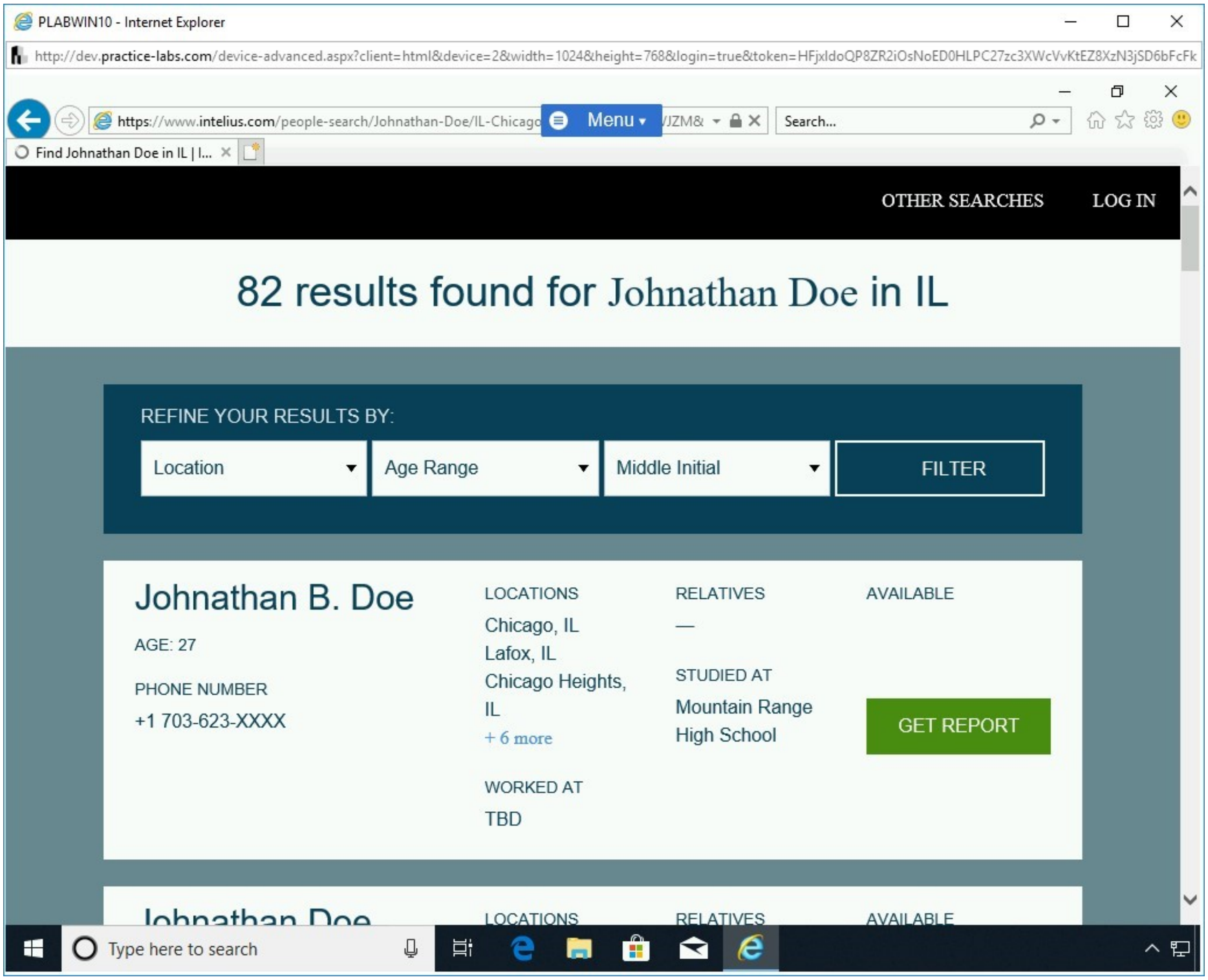
https://www.intelius.com/searching.php?ReportType=1&searchform=peopleSearch&refer=...

Figure 3.91 Screenshot of PLABWIN10: Clicking a search result.

## Step 5

Observe the types of information given.

As a visitor, you can access limited information. You have to be a paid member to view more.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=HFjxldoQP8ZR2iOsNoED0HLPC27zc3XWcVvKtEZ8XzN3jSD6bFcFk

https://www.intelius.com/people-search/Johnathan-Doe/IL-Chicago...JZM&

82 results found for Johnathan Doe in IL

Johnathan B. Doe

AGE: 27

PHONE NUMBER
+1 703-623-XXXX

LOCATIONS
Chicago, IL
Lafox, IL
Chicago Heights, IL
+ 6 more

WORKED AT
TBD

RELATIVES
—

STUDIED AT
Mountain Range High School

AVAILABLE

Johnathan Doe

LOCATIONS

RELATIVES

AVAILABLE

Figure 3.92 Screenshot of PLABWIN10: Showing the details of a searched person.

# Review

Well done, you have completed the **Footprinting and Reconnaissance** Practice Lab.

# Summary

You completed the following exercises:

- Exercise 1 - Reconnaissance Tools and Techniques
- Exercise 2 - Conducting Active Reconnaissance in a Network

- Exercise 3 - Conducting Passive Reconnaissance in a Network

You should now be able to:

- Know the Terminology
- Know Tools Used in Reconnaissance
- Know the Need for Reconnaissance or Footprinting
- Know Footprinting Countermeasures
- Identify Live Hosts on a Network
- Perform Discovery Scans
- Perform Port Scanning
- Fingerprint an Operating System
- Perform Service Probing
- Use the WHOis Website
- Perform Social Media Exploitation
- Use SHODAN
- Use Google Hacking Database
- Perform DNS Querying
- Use theHarvester
- Create a Temporary E-mail Account
- Use Maltego
- Use the AnyWho Website

# Feedback

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