# CEH v12 Lesson 6 : Compromising Web Servers

## Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 — Web Server Concepts, Attacks, Methodologies and Tools
- Exercise 2 — Upgrade Kali Linux

After completing this module, you will be able to:

- Enumerate a Web server using HTTPrint
- Use Skipfish to Perform Web server Reconnaissance
- Footprint using the nc Command
- Find the Web server Version using Metasploit Framework
- Find Files on a Web server using Metasploit Framework
- Scan for Options on a Web server using Metasploit Framework
- Check for WebDAV on a Web server using Metasploit Framework
- Create a Website Copy Using HTTrack Website CopierPerform a Slowloris Attack on a Web Server
- Perform Vulnerability Scanning Using Nikto
- Perform Web Application Brute Forcing Using DirBuster
- Verify Repositories
- Update Package Manager
- Install Packages and Patches

After completing this module, you will have further knowledge of:

- Web Servers Overview

- Web Server Components
- Web Server Attacks
- Web Server Attack Methodology and Tools
- Use common methods to prevent Web server Exploitation

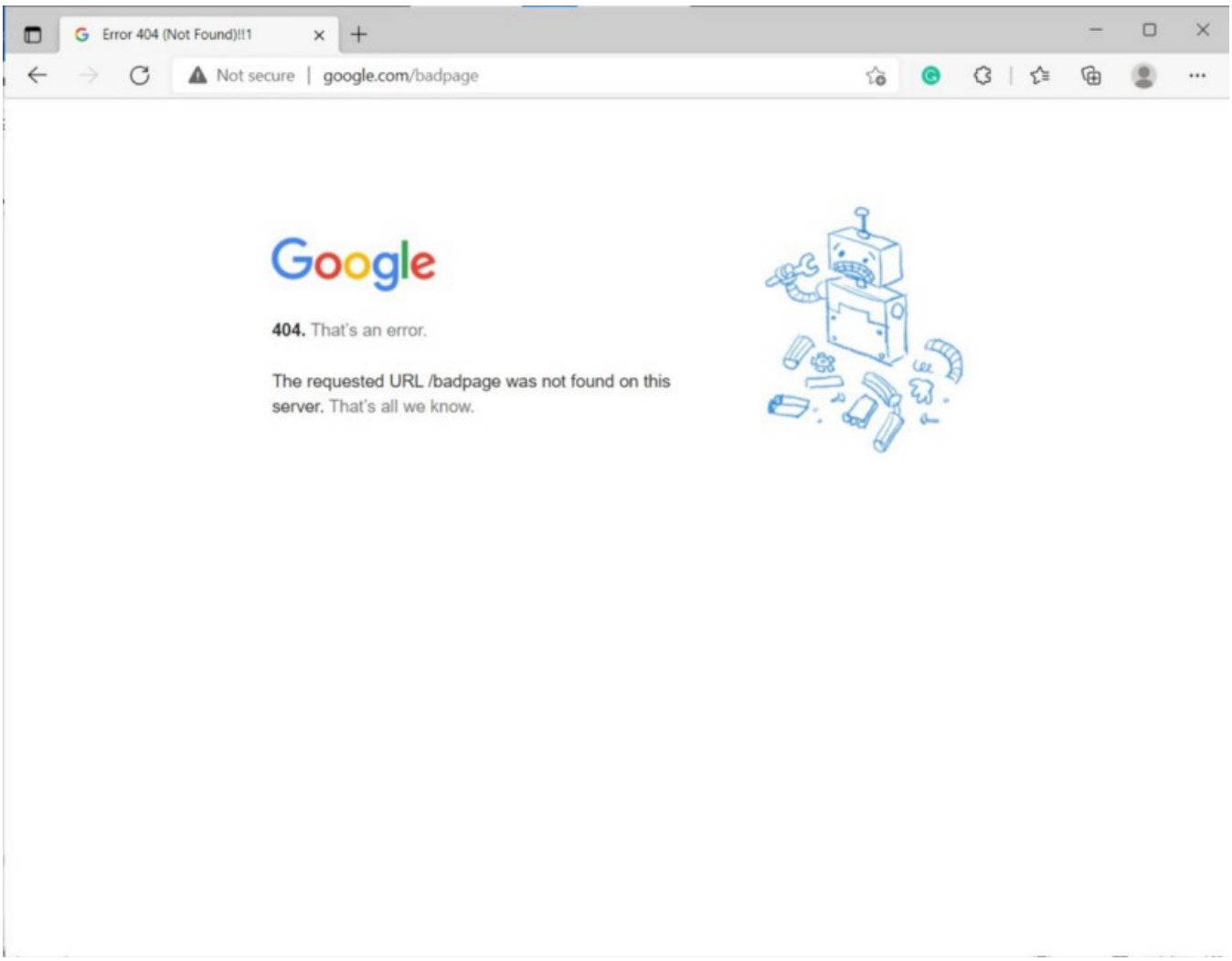
## Lab Duration

It will take approximately **1 hour and 30 minutes** to complete this lab

## Exercise 1 — Web Server Concepts, Attacks, Methodologies and Tools

A web server is a system that serves web pages to a client that makes a request. Assume that you type the google.com URL in the web browser's address bar. The web browser sends the request to the IP address mapped to the URL. After the web browser with the referenced URL receives the request, it checks for the requested resources. It could be the HTTP or HTTPS protocol used to initiate the request. In this case, you requested a domain name, it will display the homepage that is set for the domain name.

In most cases, the Web server returns the client's resources. However, if the resources do not exist on the Web server, the Web server responds with an error. For example, an error 404 is returned.




A web server consists of several components. Let's look at them in detail.

- **Root Directory**: It is the main directory that stores the files for a specific domain. For example, if it is www.example.com, the files related to this domain can be stored in a directory, such as /web/example/. If there are sub-directories, such as images, they are stored in the /web/example/images directory.
- **Server Root**: It is the directory that contains the configuration files for the server. It typically contains several sub-directories, such as conf, logs, and cgi-bin. The server root directory contains various components, such as executables, logs, and errors.
- **Virtual Document Tree**: It is the storage on another server or drive that is used when the primary drive's space is exhausted.
- **Virtual Hosting**: It is a method of hosting multiple websites on a single web server. The resource of each website is stored in a separate root directory.

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

In this exercise, you will learn about Web server attacks, attack methodologies, and attack tools.

## Learning Outcomes

After completing this exercise, you will be able to:

- Enumerate a Web server using HTTPrint
- Use Skipfish to Perform Web server Reconnaissance
- Footprint using the nc Command
- Find the Web server Version using Metasploit Framework
- Find Files on a Web server using Metasploit Framework
- Scan for Options on a Web server using Metasploit Framework
- Check for WebDAV on a Web server using Metasploit Framework
- Create a Website Copy Using HTTrack Website CopierPerform a Slowloris Attack on a Web Server
- Perform Vulnerability Scanning Using Nikto
- Perform Web Application Brute Forcing Using DirBuster

After completing this exercise, you will have further knowledge of:

- Web server Attacks
- Web server Attack Methodology and Tools

## Your Devices

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

PLABDC01Domain Controller192.168.0.1/24PLABWIN10Domain MemberWorkstation192.168.0.3/24PLABKALI01Domain MemberWorkstation192.168.0.5/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

### Web Server Attacks

The vulnerabilities can be inherent to the Web server, which means bugs or defects within the Web server code. Other Web server vulnerabilities can be external, such as:

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

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

Depending on the vulnerabilities found, an attacker can perform one or more attacks on the Web server. Some of these attacks are:

- **Denial-of-Service (DoS**): In this attack, the attacker sends a large volume of requests to the Web server. Consequently, the Web server becomes busy responding to these requests and stops responding to the requests from legitimate users. The requests sent by the attacker are so high in volume that the Web server cannot respond to them and eventually exhausts its resources and crashes.

- **Directory Traversal**: The attacker can navigate to the root directory and access all the files within the directory structure for the website. During this attack, the attacker not only finds the files within the directory structure, but can also execute commands. The attacker can use the ../ method in the URL to determine if they can perform this attack.
- **DNS Amplification**: The attacker uses bots with the spoofed IP addresses of the victim. The bots make requests for domain name resolution. The responses are sent to the victim's DNS server when the domain name resolution is performed.
- **DNS server hijacking**: In this attack, the attacker modifies the settings of a DNS server to redirect the users' name resolution requests to another DNS server. When the attacker's DNS server receives a user's request for a specific domain, it redirects the user to a spoofed site, which looks similar to the original site.
- **Man-in-the-Middle**: The attackers can intercept and alter the communication between two parties, the user and the Web server. Typically, this situation occurs when the Web server is configured with weak protocols like HTTP, which transmits the information in cleartext.
- **Sniffing**: The attackers sniff information to gain access to it. If the Web server is configured to use HTTP protocol, it makes the attacker's life easy.
- **Web server Misconfiguration**: It is one of the key reasons for attacks on web servers. An example of misconfiguration is default passwords or running unnecessary services. The attackers exploit them to gain access to the Web server.
- **HTTP-Response Splitting**: The attacker injects a piece of code into the input field of the response header and splits it into two parts. The attacker can achieve this because the web application has input validation vulnerabilities. Some of the key types of such attacks are SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).
- **Web Cache Poisoning**: The attacker flushes the content of the web server's cache and floods it with malicious content. When a user requests a web page, the Web server first checks its cache, and if the requested URL is found, it serves the malicious content to the user.

## Web Server Attack Methodology and Tools

Similar to any attack, web server attacks also follow a methodology. Let's look at the phases in the Web server attack methodology.

InformationGatheringWeb Server FootprintingWebsiteMirroringVulnerabilityScanningSessionHijackingWeb ServerPasswordHacking

Figure 1.1 Phases of the web server attack methodology, including the Information Gathering, Web Server Footprinting, Website Mirroring, Vulnerability Scanning, Session Hijacking and Web Server Password Hacking phases.

- **Information Gathering**: An attacker narrows down on a specific target and attempts to gather as much information as possible. Various sources can be used to gather this information. For example, whois.com can be used to gain information about a specific domain. Some of the key tools in information gathering are:
- Whois.domaintools.com — Whois Lookup
- https://pentest-tools.com — Find subdomains
- https://tools.dnsstuff.com — DNSstuff WHOIS
- https://who.is — WHOIS Search, Domain Name, Website, and IP Tools
- **Web server Footprinting**: An attacker attempts to gather information about a web server. This information can include the operating system and its version, sever name, etc. Several tools can be used in footprinting. Some of the key tools are:
- Telnet
- ID Serve
- Netcraft
- Httprecon
- Netcat
- Recon-ng
- Uniscan
- Nmap

- Skipfish
- **Website Mirroring**: An attacker makes a replica of the target website to study its structure. Some of the key tools used in this phase are:
- NCollector Studio
- HTTRack Website Copier
- WebCopier Pro
- Website Ripper Copier
- Crytotek WebCopy
- Website Ripper Copier
- Website eXtractor
- SurfOffline
- Web-Site-Downloader
- BackStreet Browser
- SiteSucker
- WebWhacker 5.0
- Offline Explorer
- WebAssistant Proxy Offline Browser
- **Vulnerability Scanning**: An attacker performs vulnerability scanning on a web server. After vulnerabilities are found, they can exploit one or more vulnerabilities. Some of the key tools used in this phase are:
- Acunetix Web Vulnerability Scanner
- Tenable.io
- Netsparker
- Fortify WebInspect
- Nikto

- **Session Hijacking**: An attacker can also perform this step to hijack one of the client sessions. Some of the key tools used in this phase are:
- Burp Suite
- Ethercap
- CookieCatcher
- JHijack
- **Web server Password Hacking**: An attacker performs a password cracking method to extract the web server's password. Some of the key tools used in this phase are:
- Hashcat
- THC Hydra
- Rainbow Crack
- Wfuzz
- Cain and Abel
- Medusa

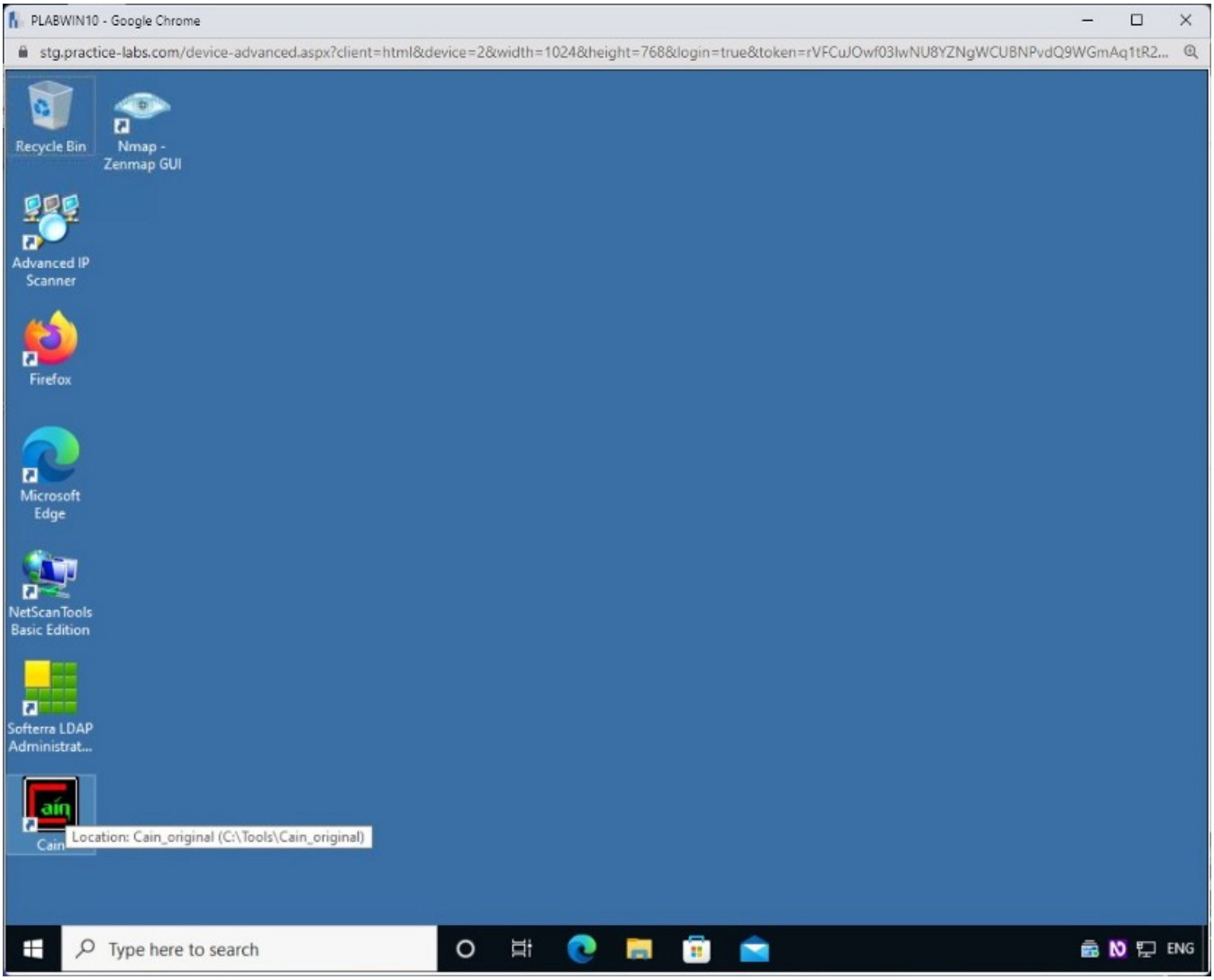
## Task 1 — Enumerate a Web Server using HTTPrint

Besides using the command line tools, you can also use HTTPrint to enumerate a web server.

In this task, you will learn how to use HTTPrint.

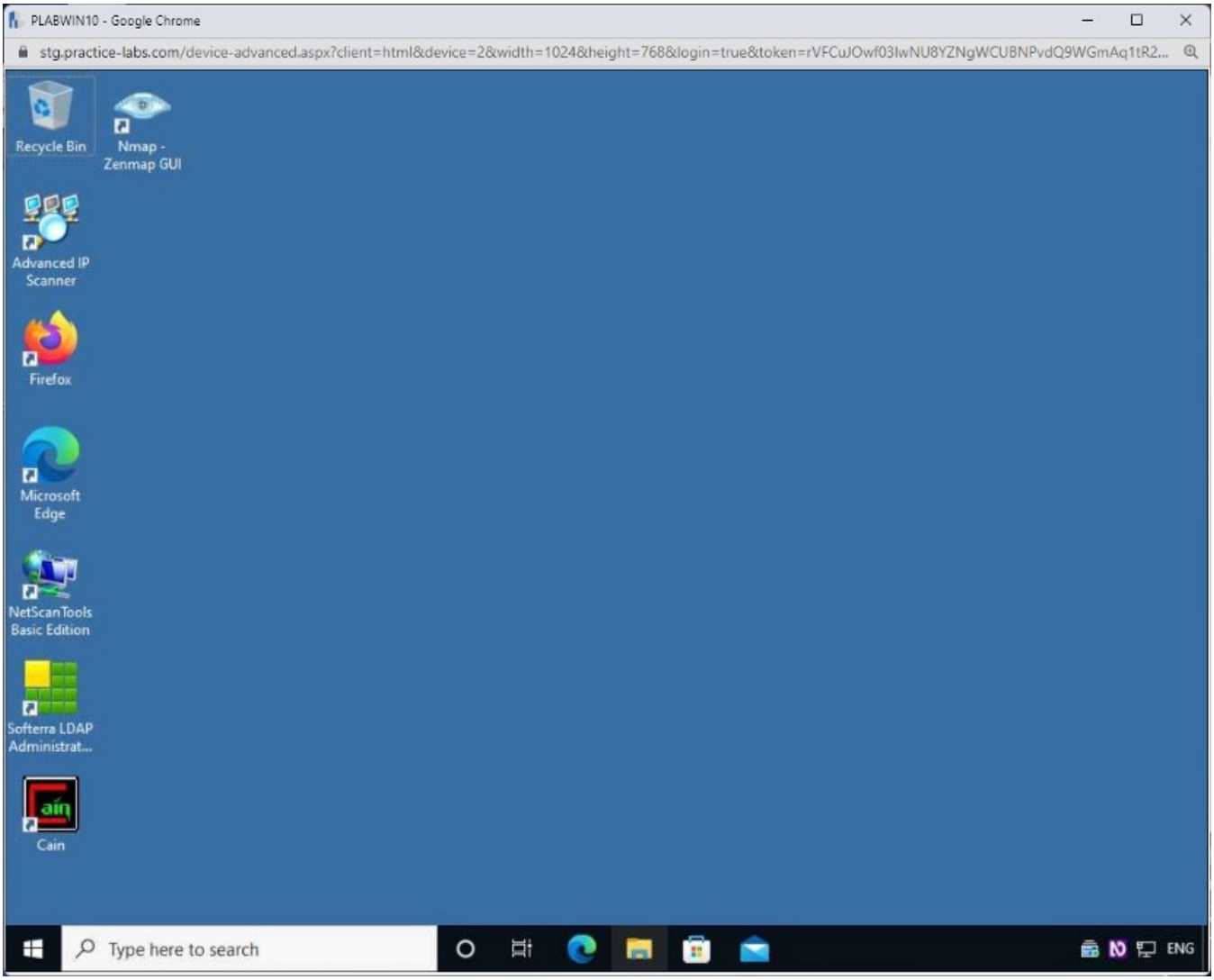
#### Step 1

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




**Step 2**

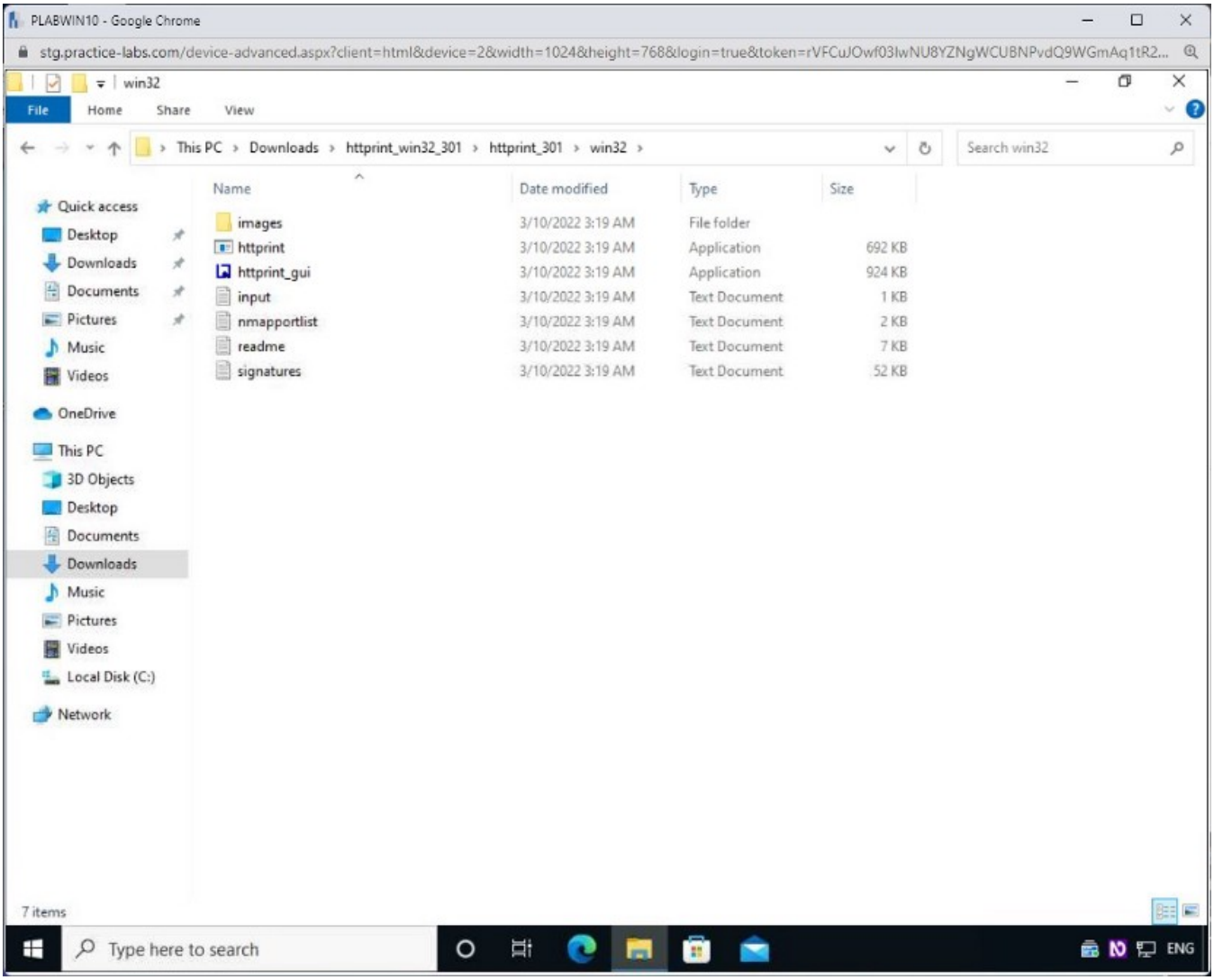
From the taskbar, click the **File Explorer** icon.




**Step 3**

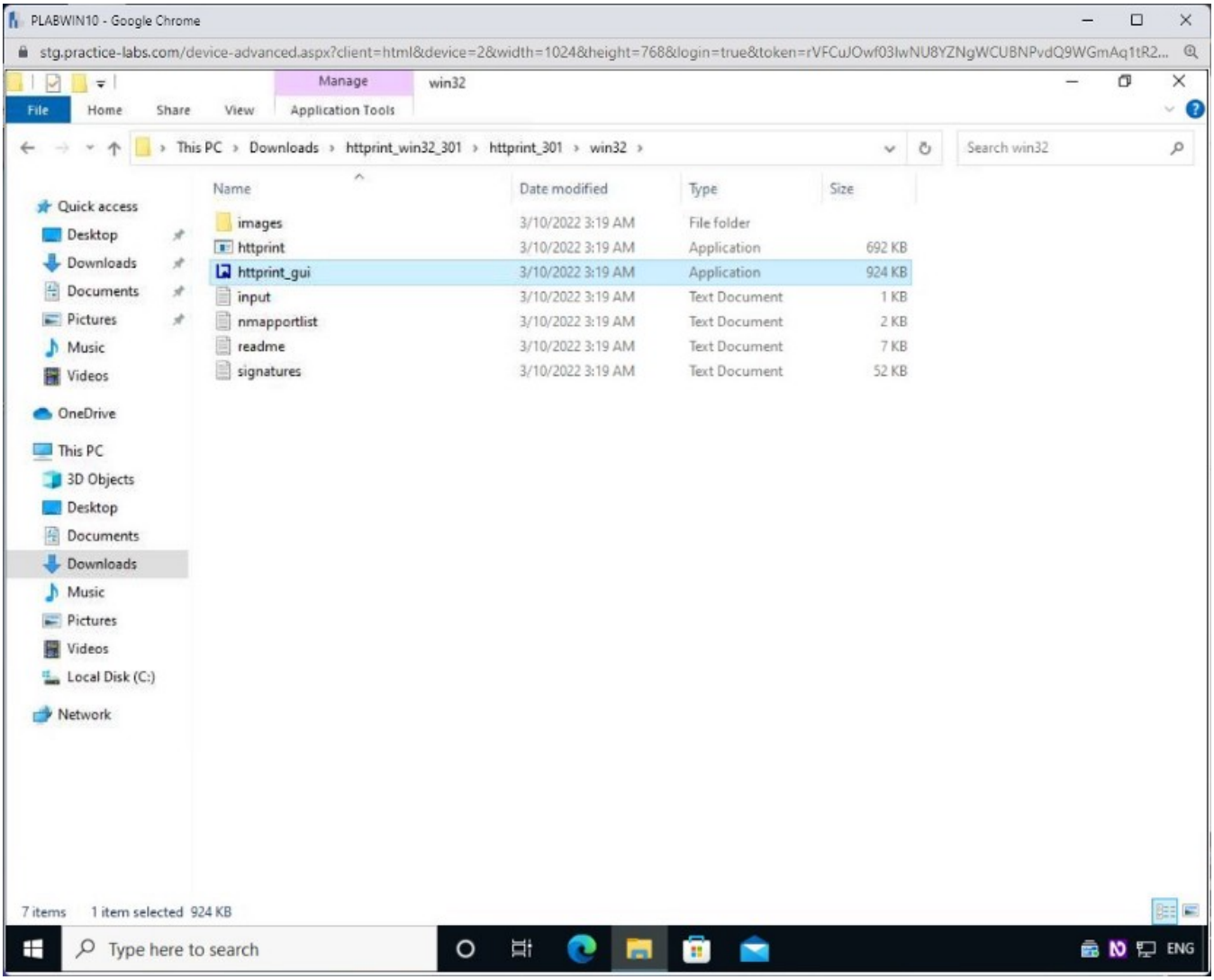
In the **File Explorer** window, navigate to the following path:

```
Downloads\httprint_win32_301\httprint_301\win32
```




### Step 4

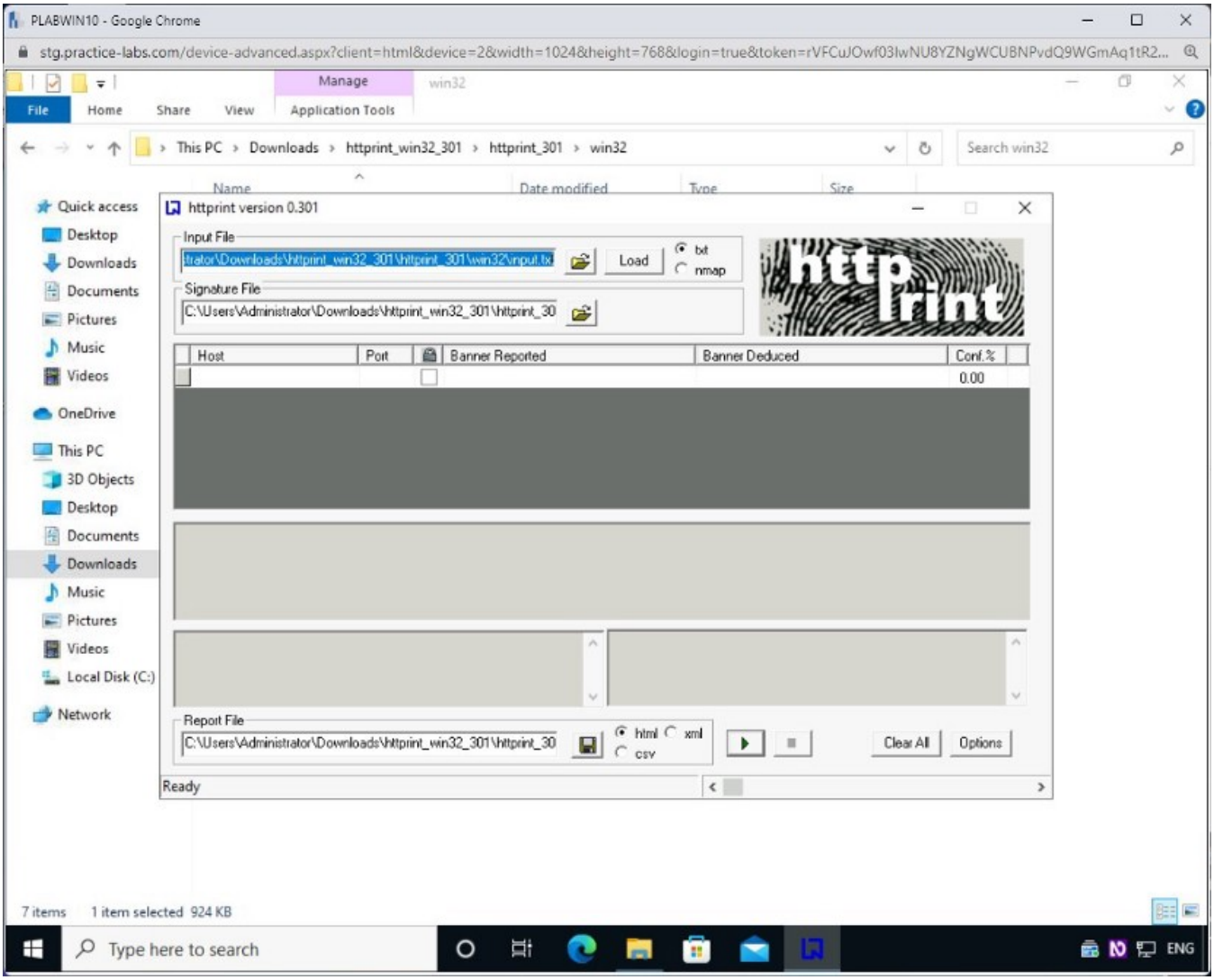
You are now in the **win32** folder. Double-click **httprint_gui**.




**Step 5**

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

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




**Step 6**

Enter the following information:

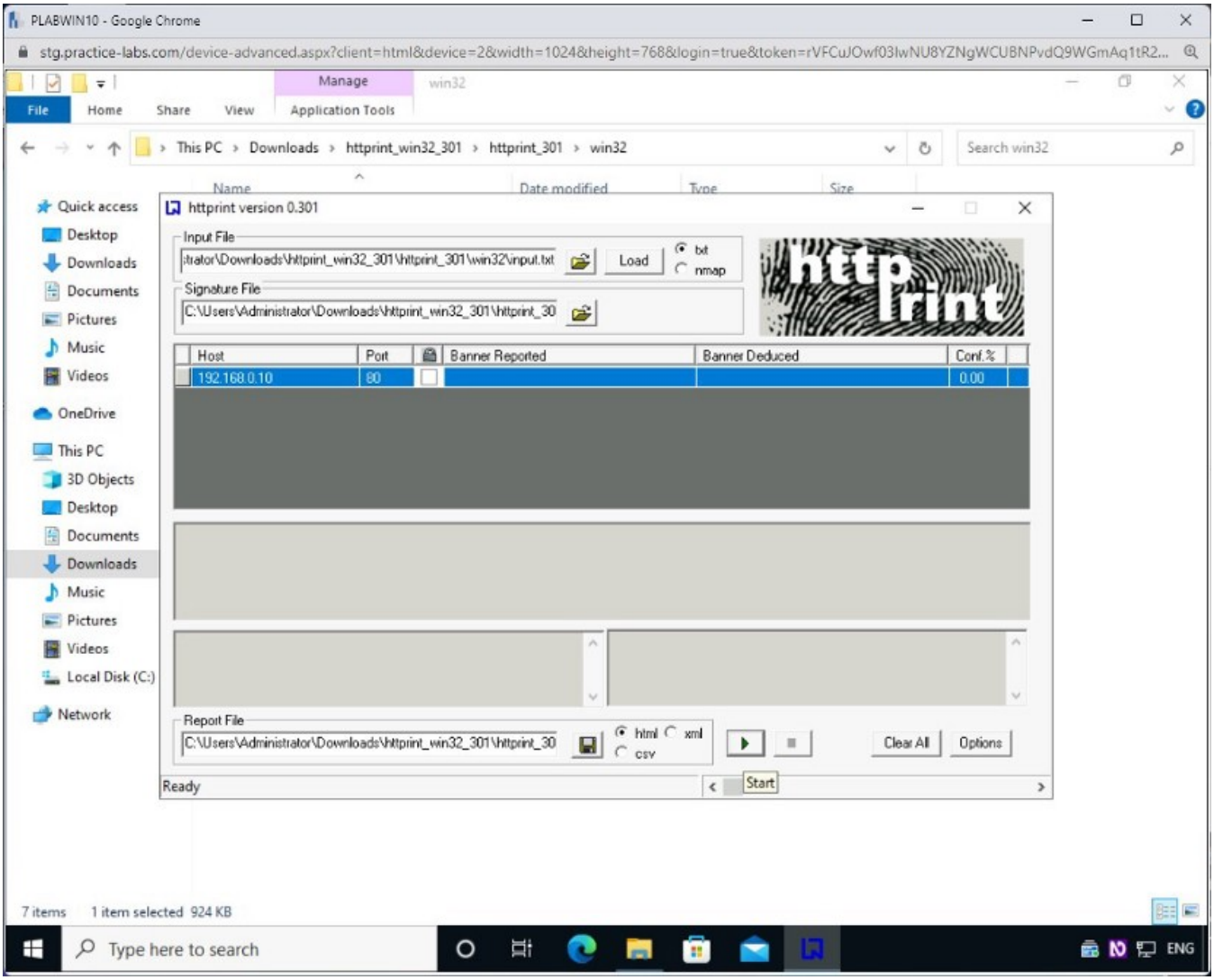
**Host:**

```
192.168.0.10
```

**Port:**

```
80
```

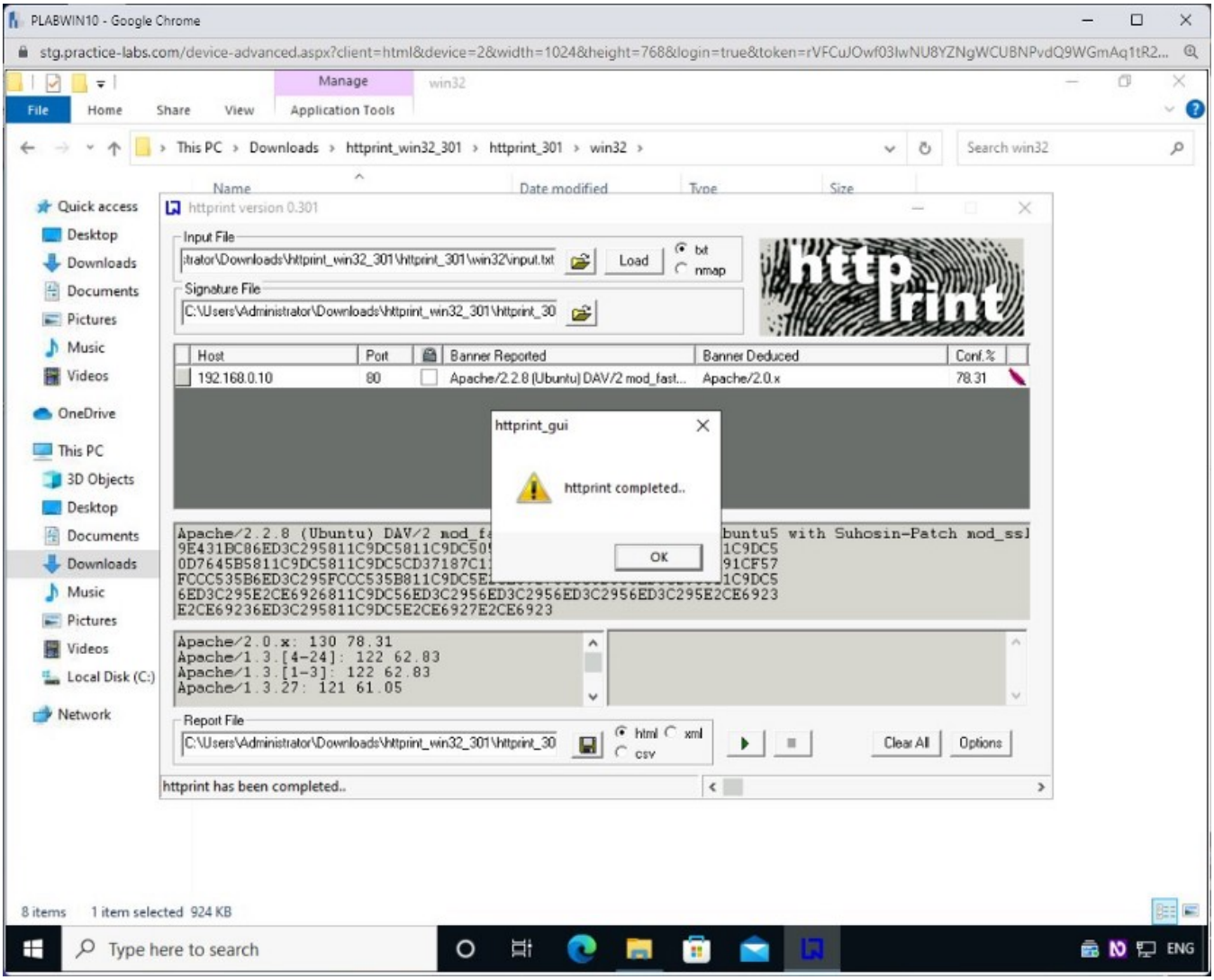
Click the **Start** arrow icon.




### Step 7

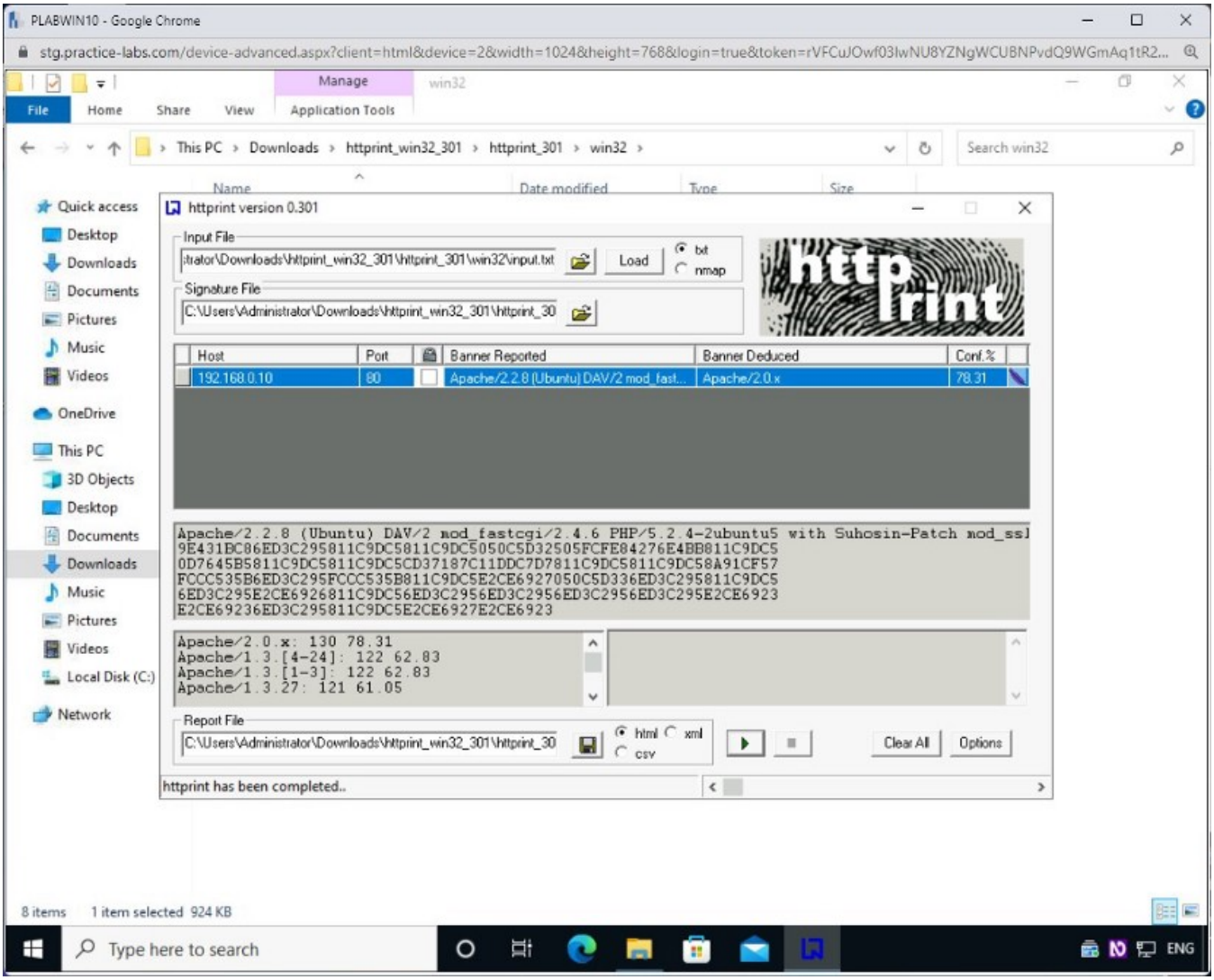
The **httprint_gui** dialog box is displayed. It prompts with a message that **httprint** is now completed.

Click **OK**.



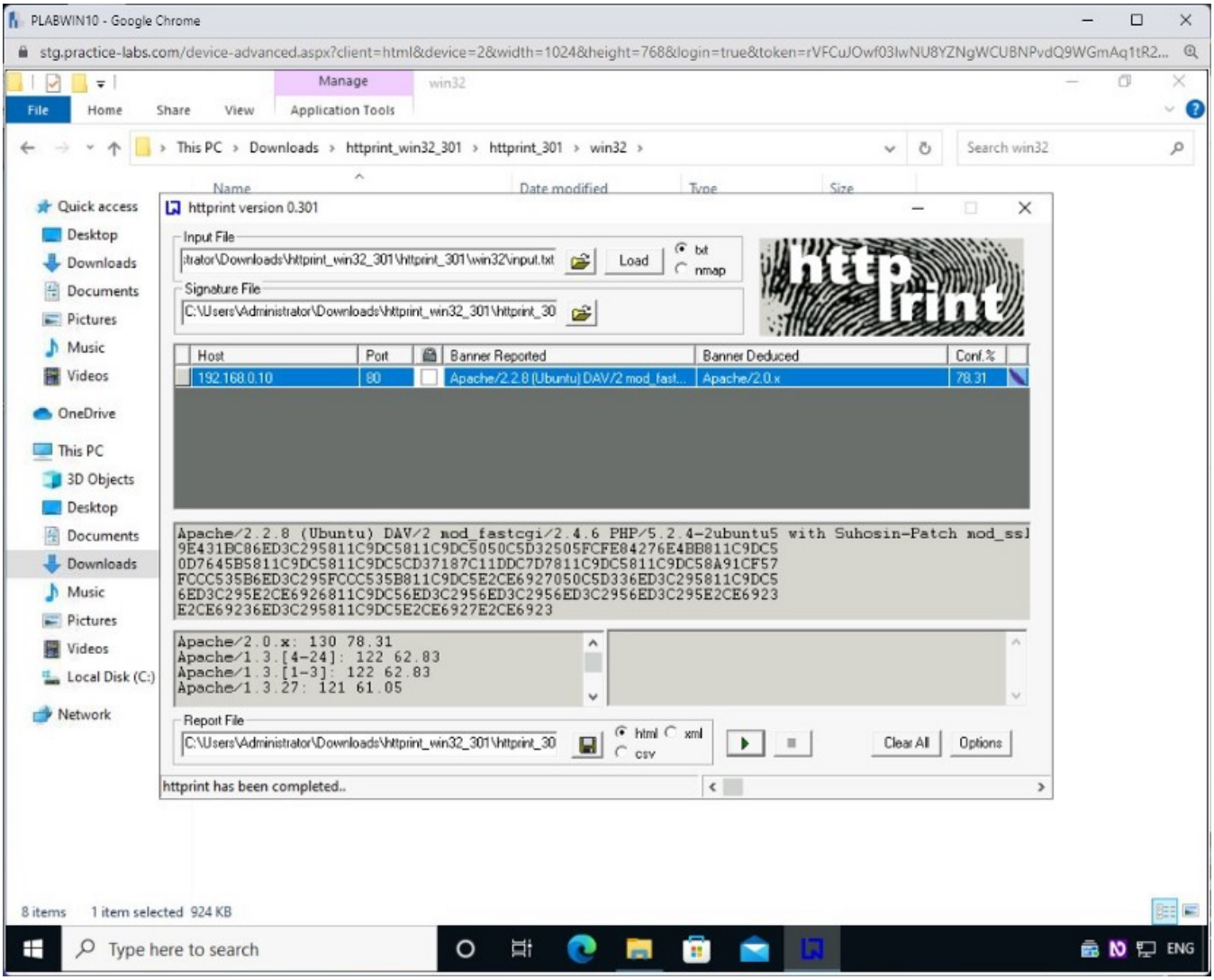

### Step 8

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




### Step 9

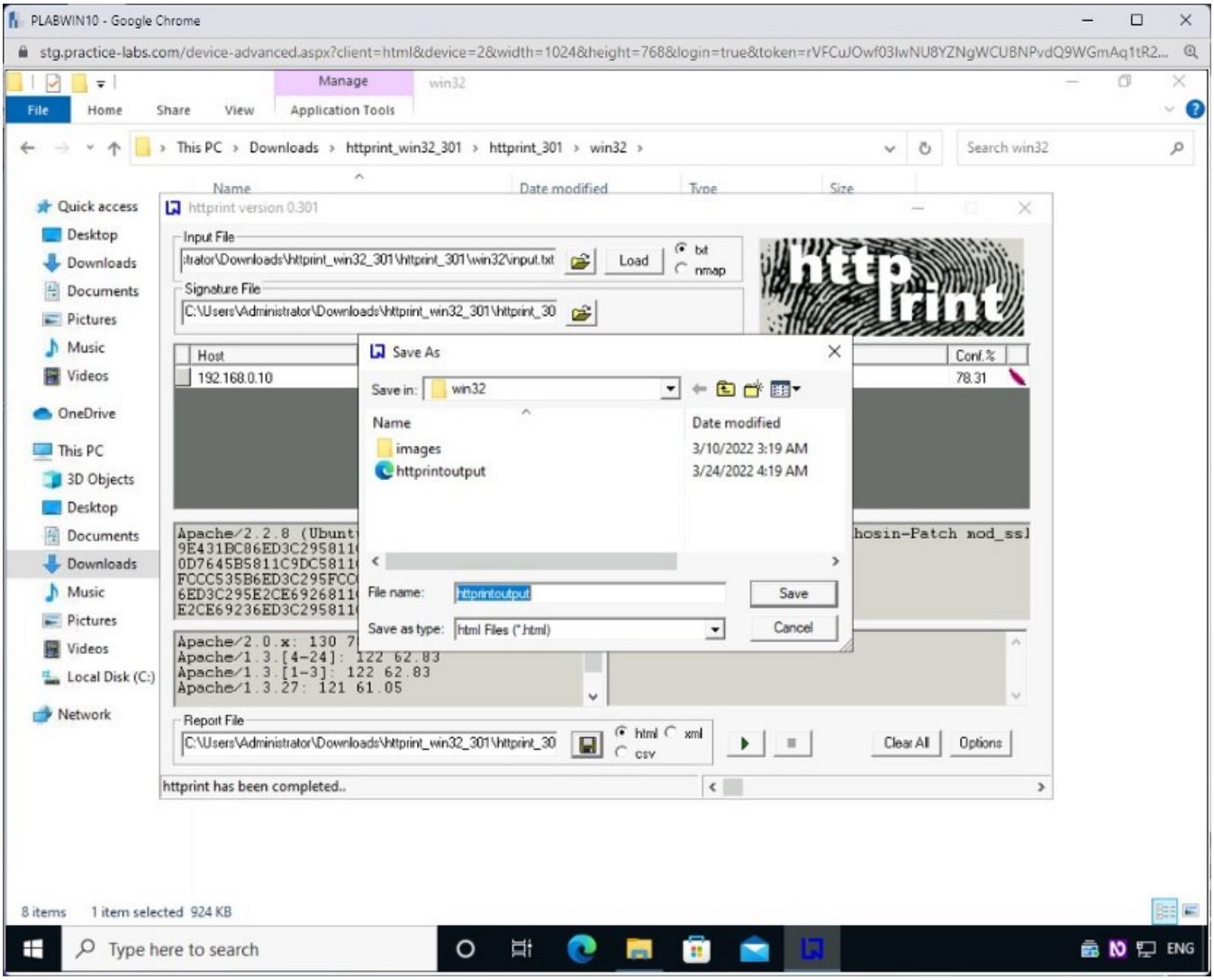
Save the file by clicking the **floppy disk** icon.




**Step 10**

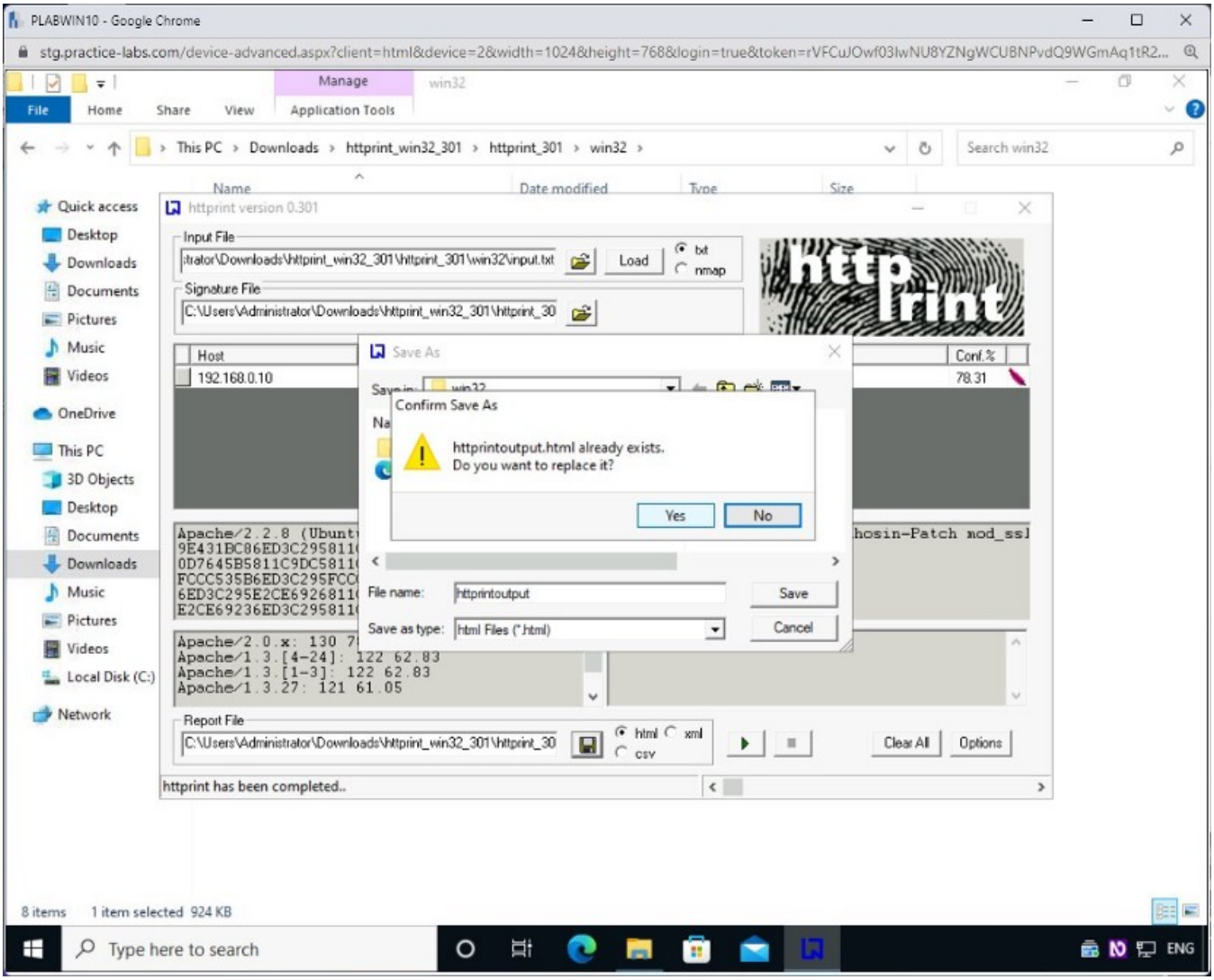
The **Save As** dialog box is displayed. Keep the default name and click **Save**.

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



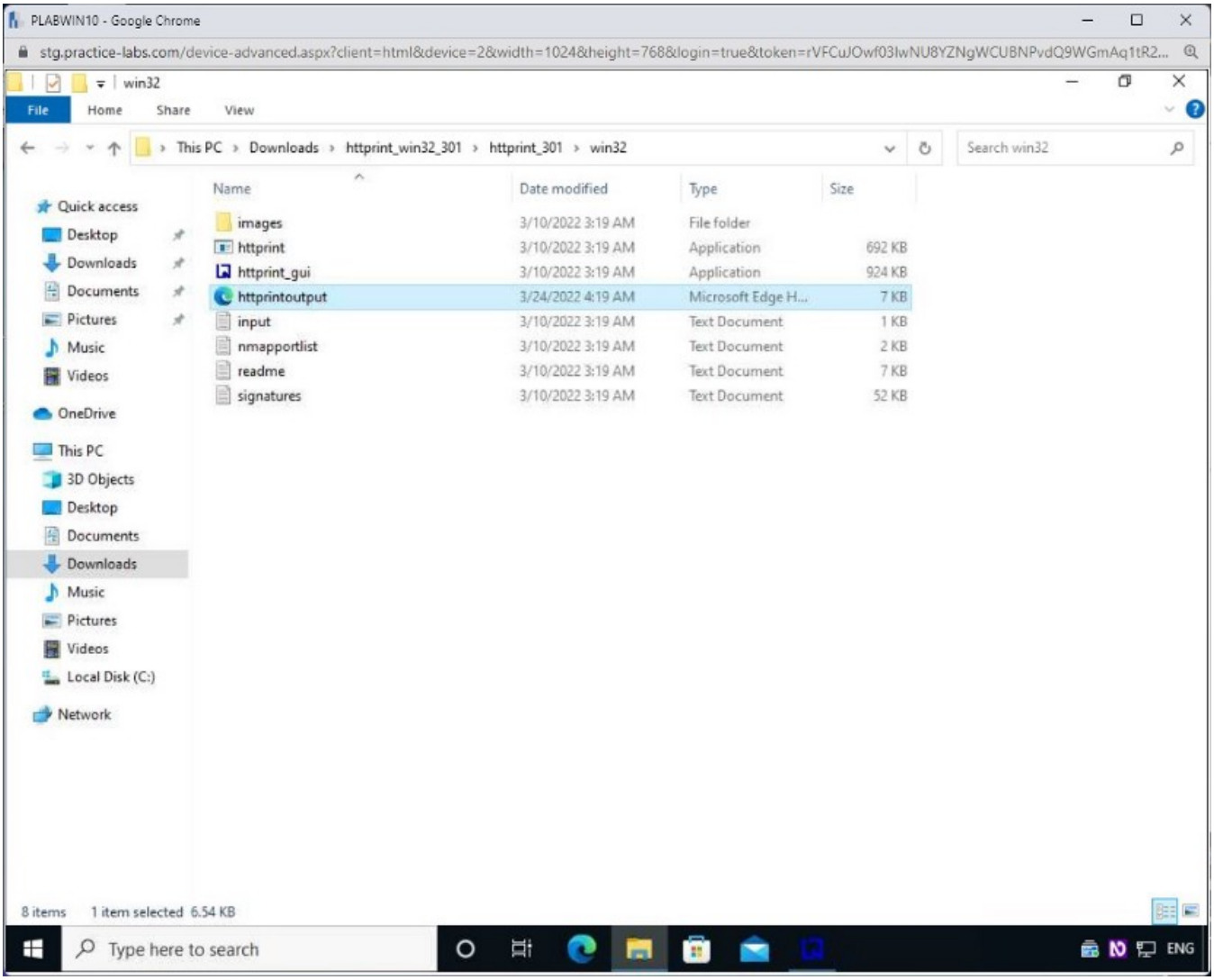

### Step 11

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




### Step 12

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

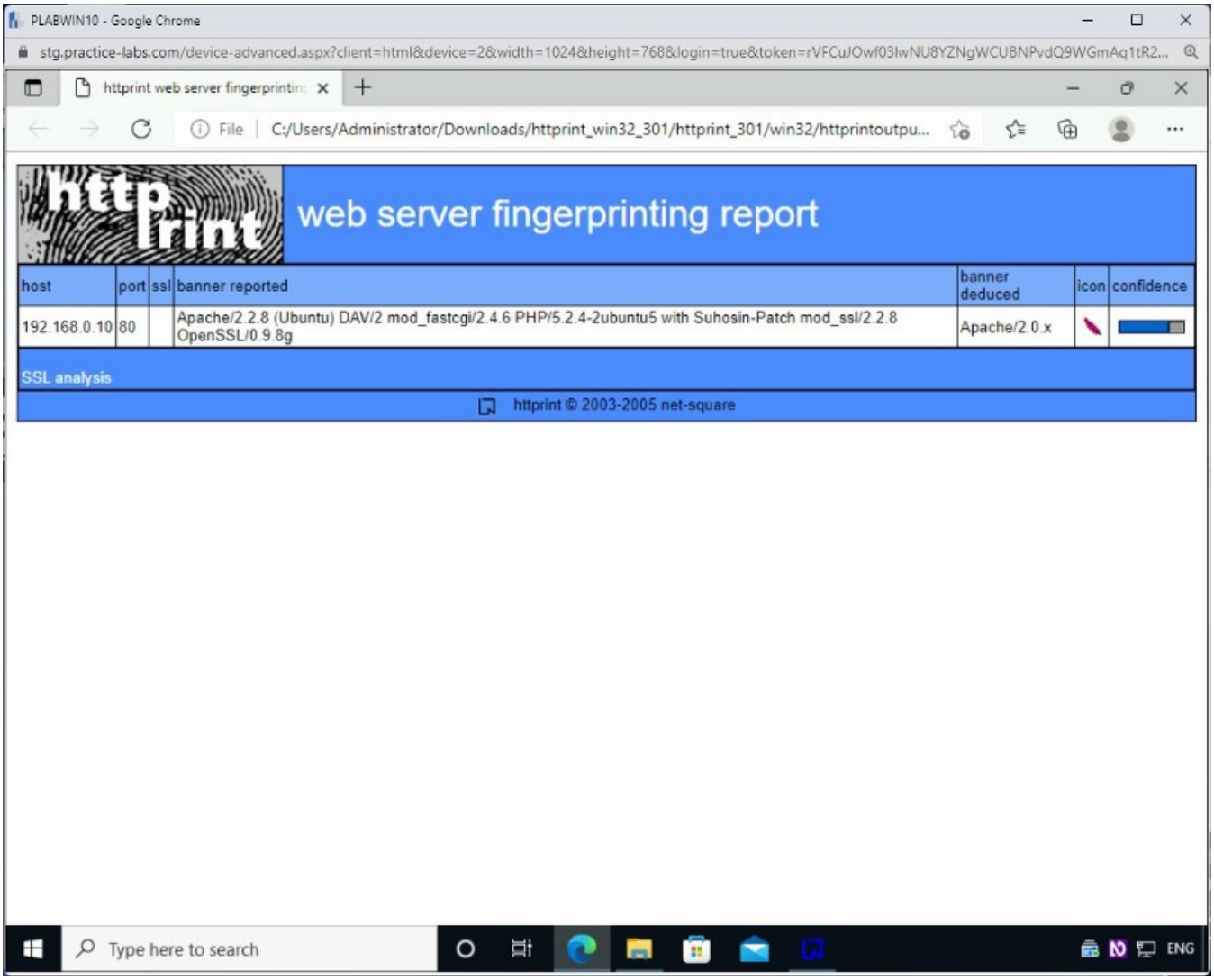



**Step 13**

**Microsoft Edge** opens the report, as it is in **HTML** format.

As you can see, the same information that you viewed within the **HTTPrint** tool is shown.

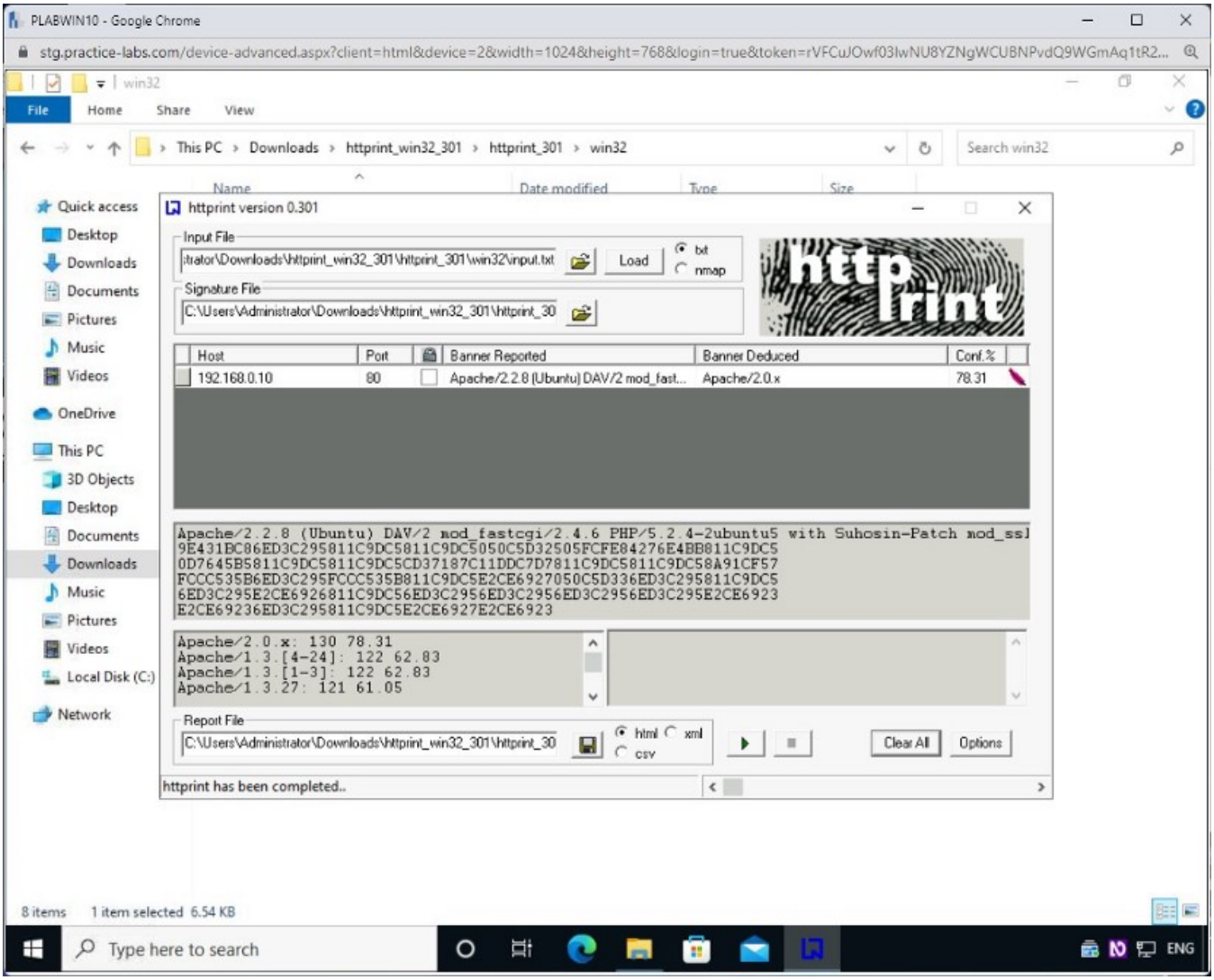
Close **Internet Explorer**.




**Step 14**

Switch back to the **HTTPrint** tool.

Click **Clear All**.




**Step 15**

Enter the following information:

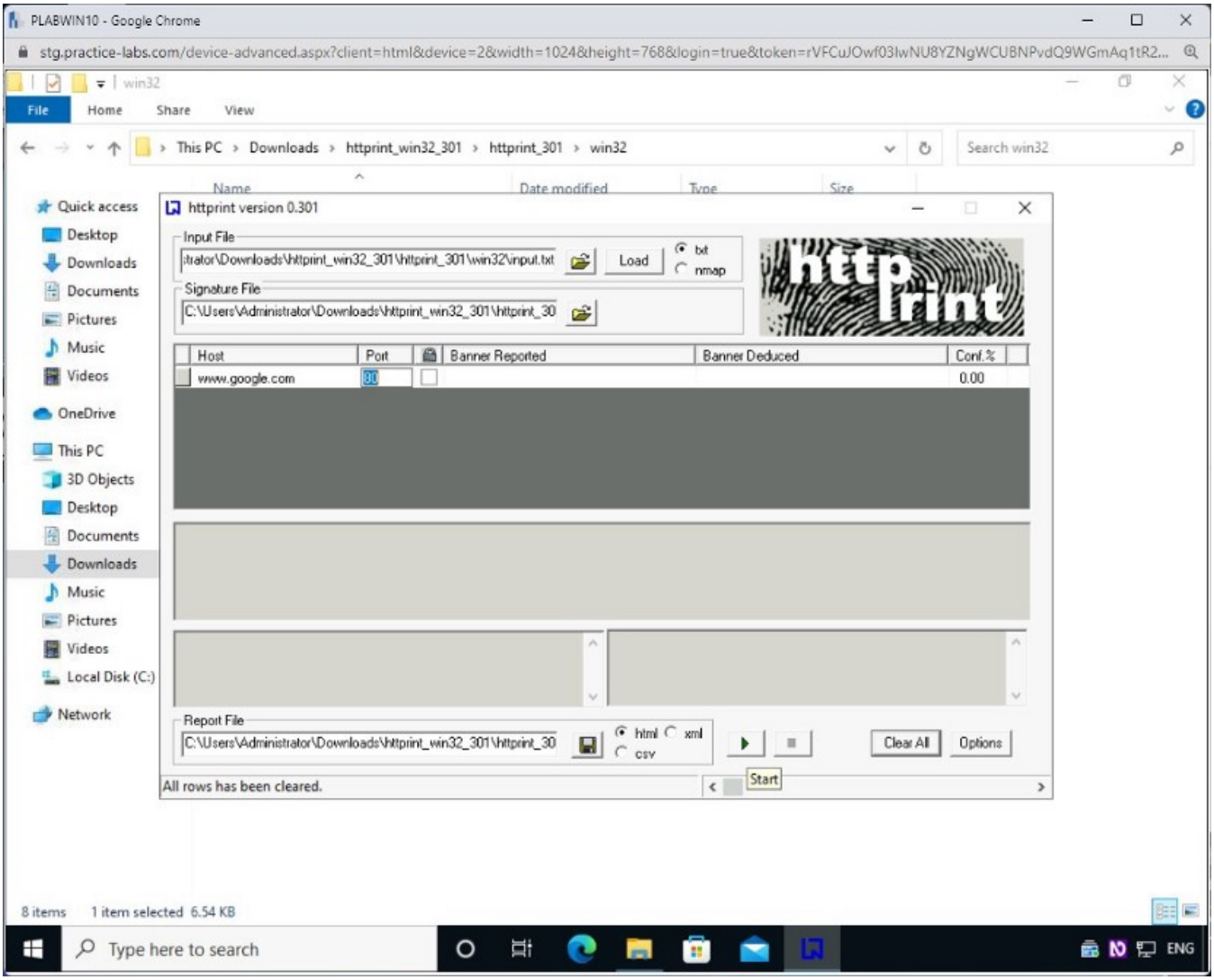
**Host:**

www.google.com

**Port:**

80

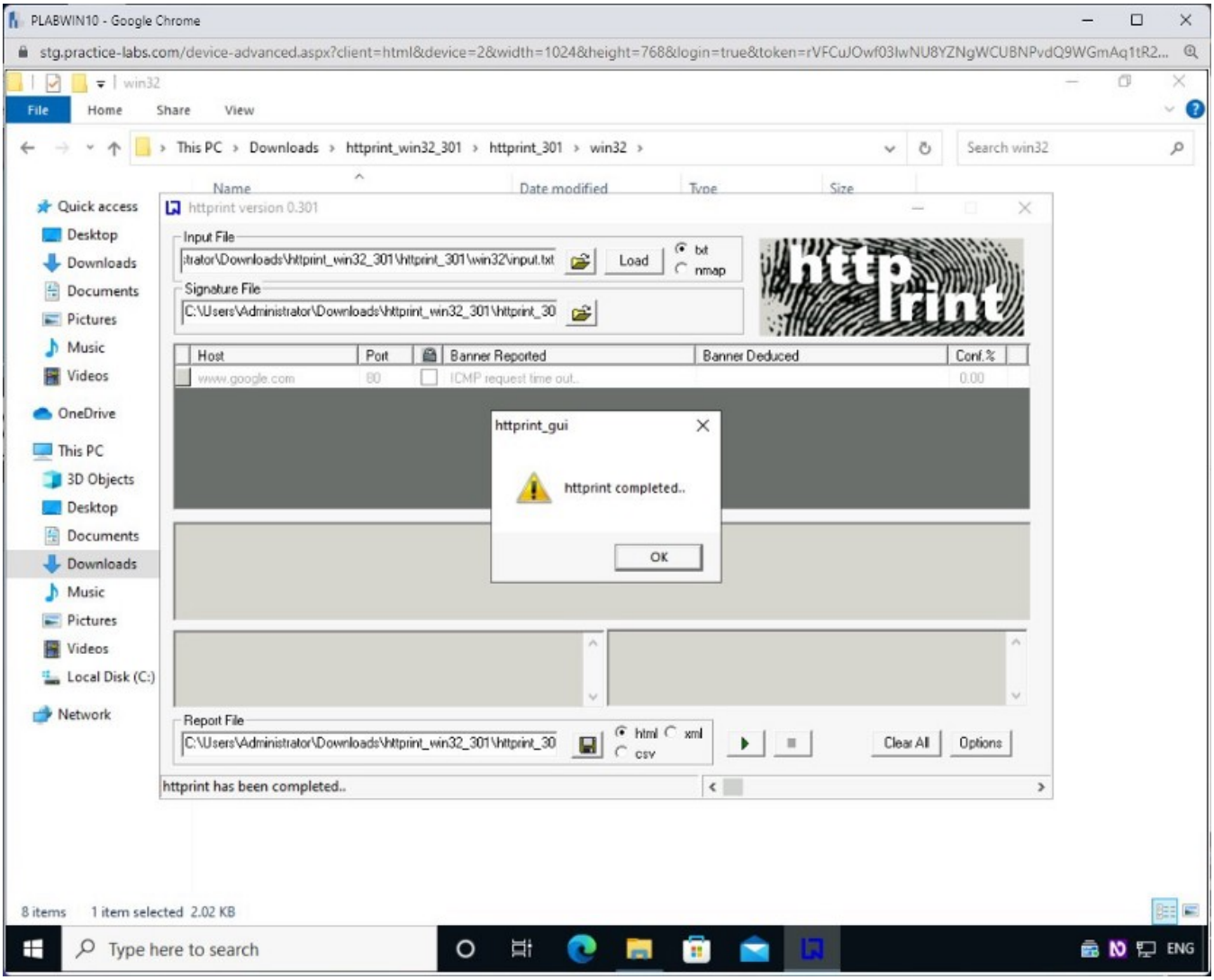
Click the **Start** arrow icon.




**Step 16**

The **httprint_gui** dialog box is displayed.

Click **OK** to close it.



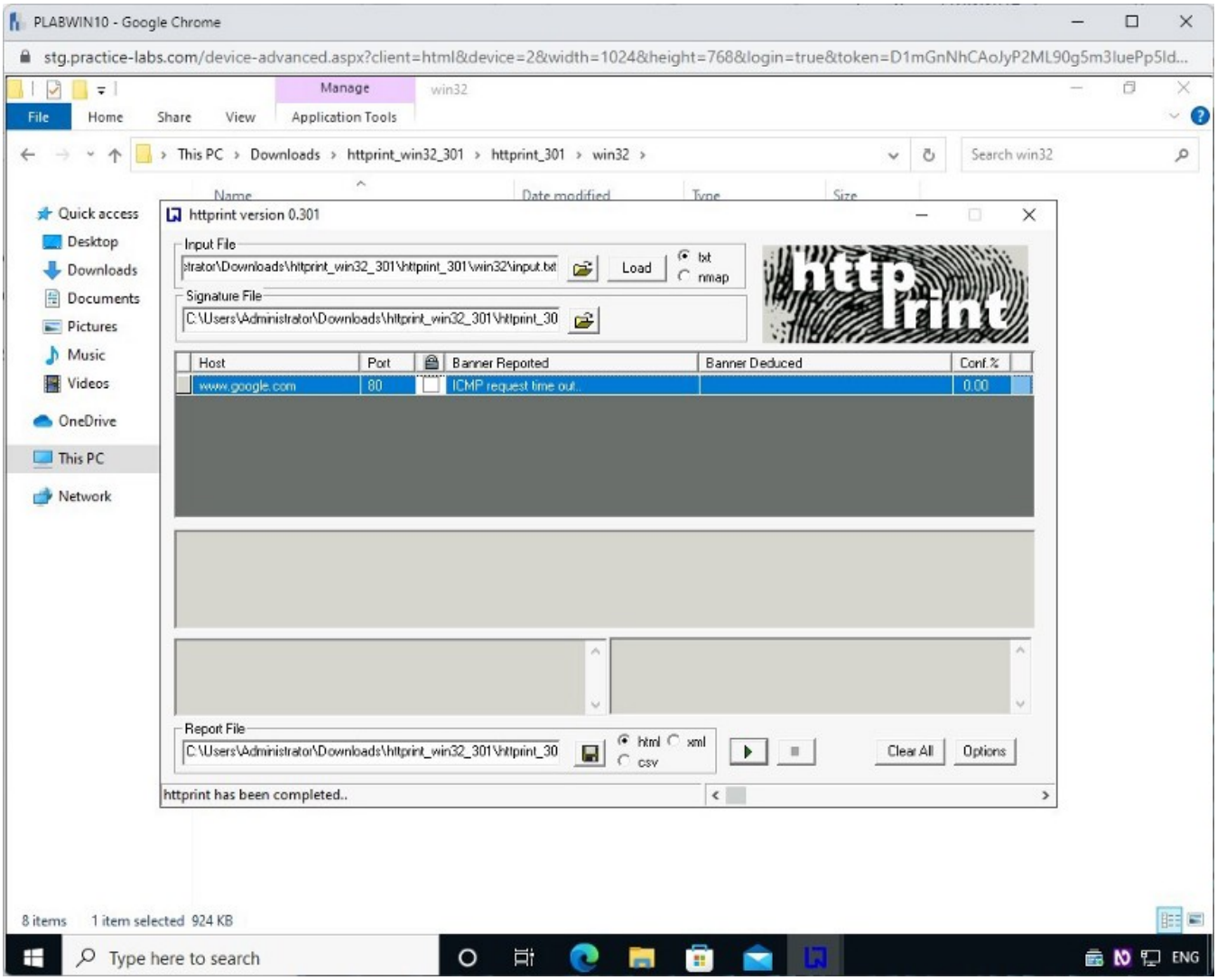

**Step 17**

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

- A network firewall is preventing the ICMP packets from going out.
- The target you are trying to fingerprint prevents ICMP packets from being sent to the network.

If either of the above statements are true; you will get this error message.

***Note**: when you fingerprinted the internal web server (**192.168.0.10**) you did not get an error. The reason that this was successful is that your system and web server are on the same network and subnet.*




Close all open windows.

## Task 2 — Use Skipfish to Perform Web server Reconnaissance

Skipfish is a tool that is available in Kali Linux. The sole purpose of Skipfish is to perform a deep reconnaissance of a web server and deployed applications. Using Skipfish, you can collect a great deal of information, which will help you detect the vulnerabilities.

You can then close said vulnerabilities to ensure optimal protection for the server. As suc,h this is the first task you should perform after deploying a web server.

In this task, you will learn to use Skipfish.

### Step 1

Connect to **PLABKALI01**.

Log in using the following credentials:

**Username**:

```
root
```

**Password**:

**Password**

The desktop of **PLABKALI01** is displayed.

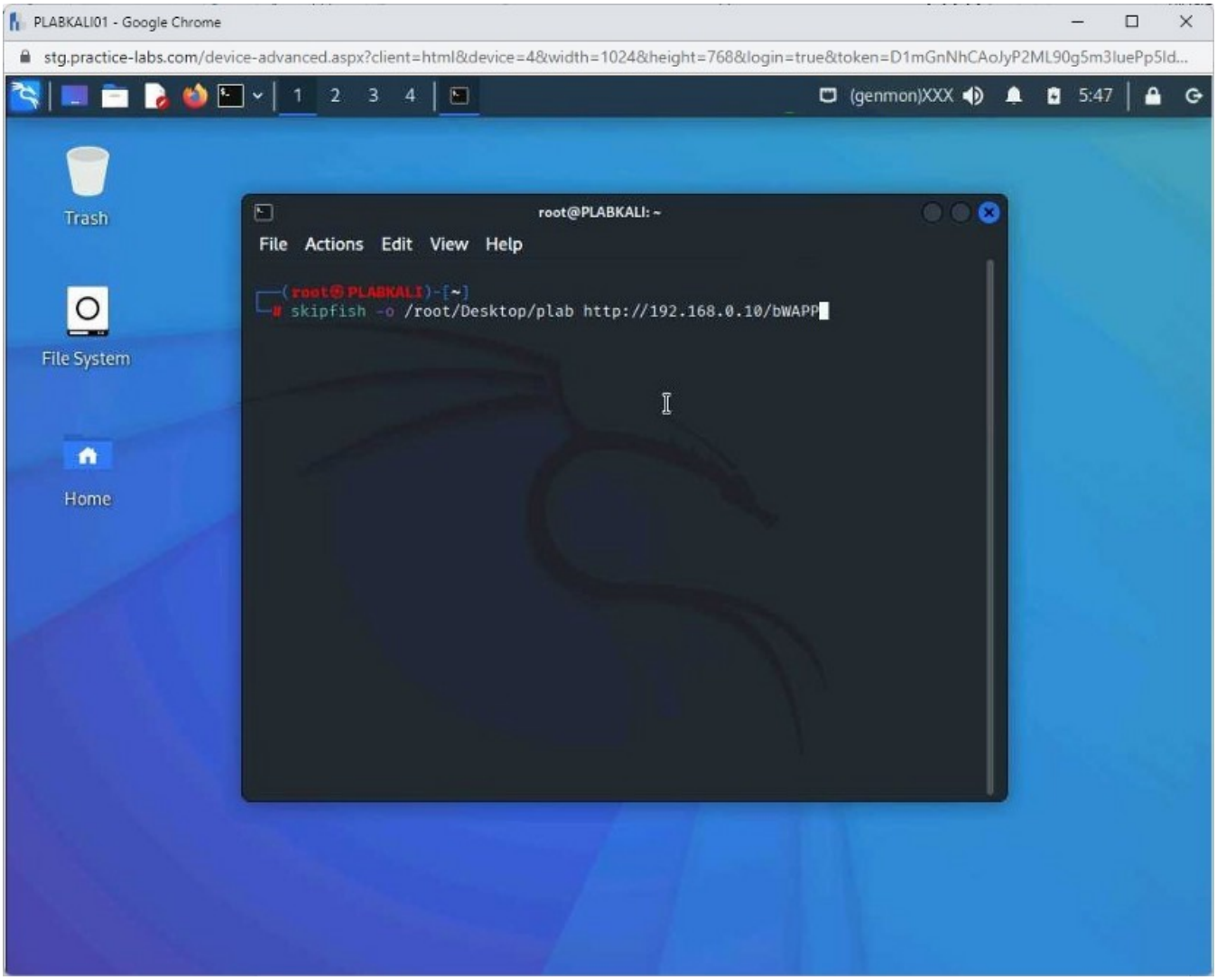
Open a new terminal window by clicking the **Terminal Emulator** icon on the taskbar.

To use **Skipfish**, type the following command:

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

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

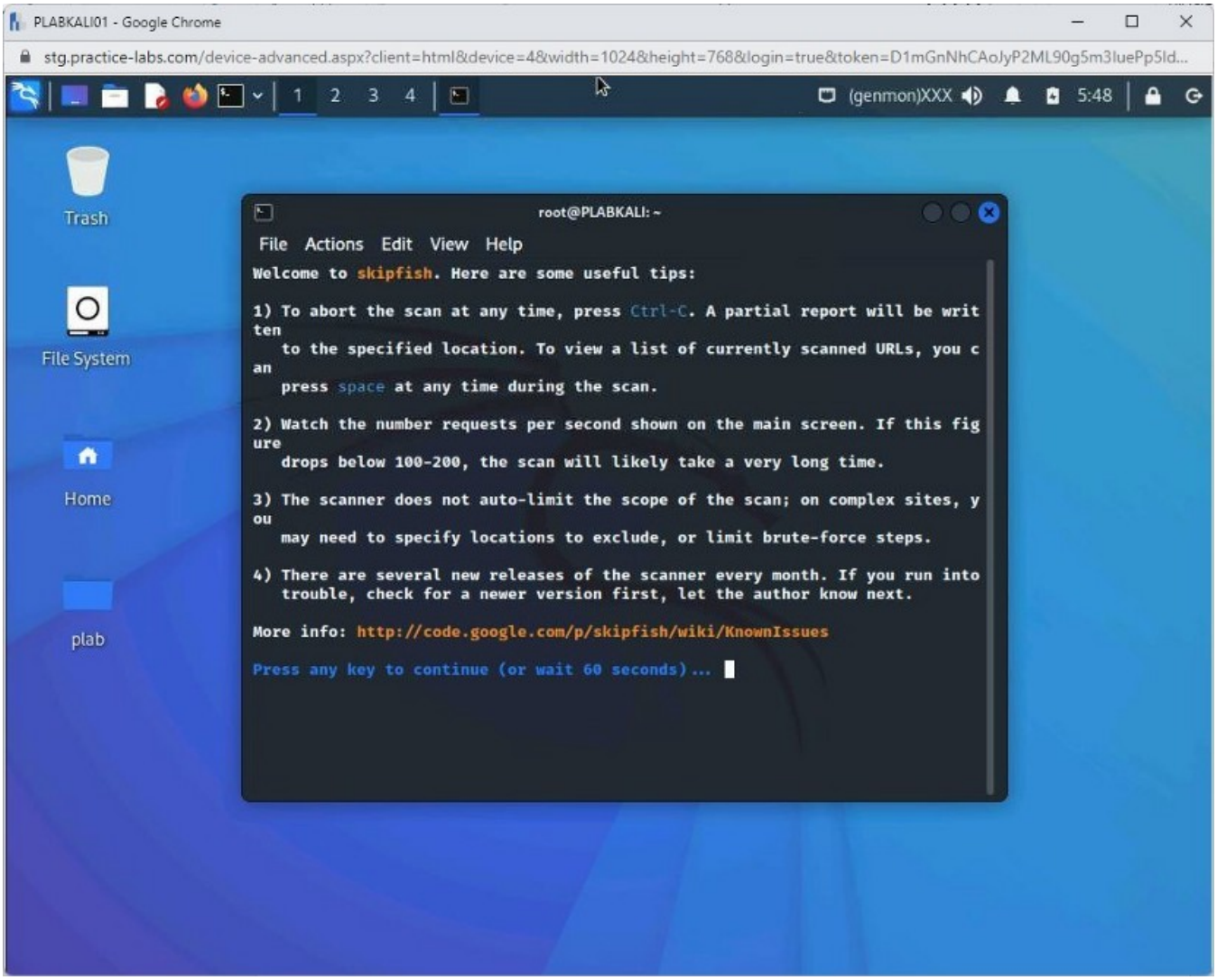
Press **Enter**.




**Step 2**

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

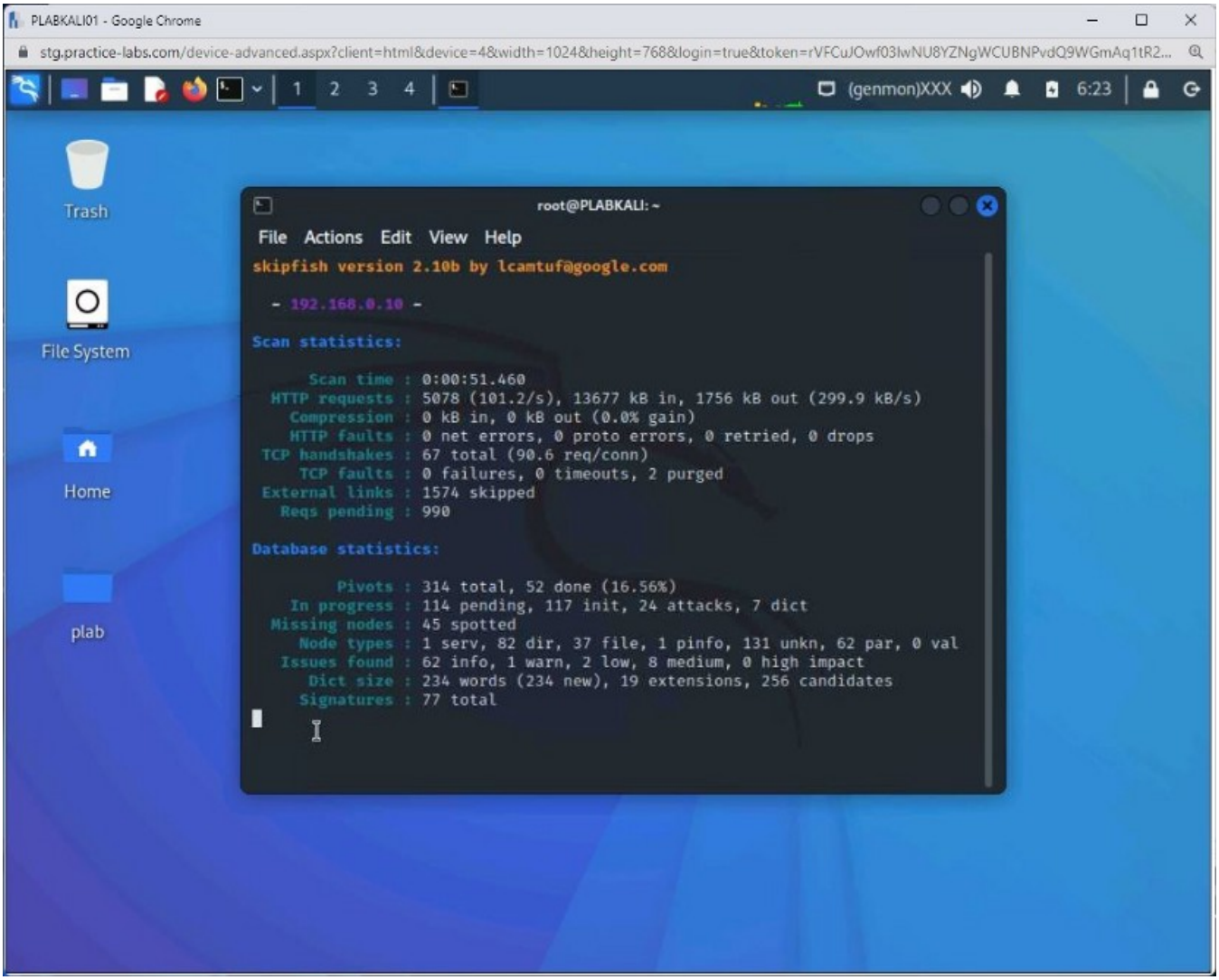
Notice that the **plab** directory is now created on the desktop.




**Step 3**

The scanning process is initiated, of which the duration depends on the size of the application.

**Alert**: In the lab environment, it may take up to **30 minutes**.

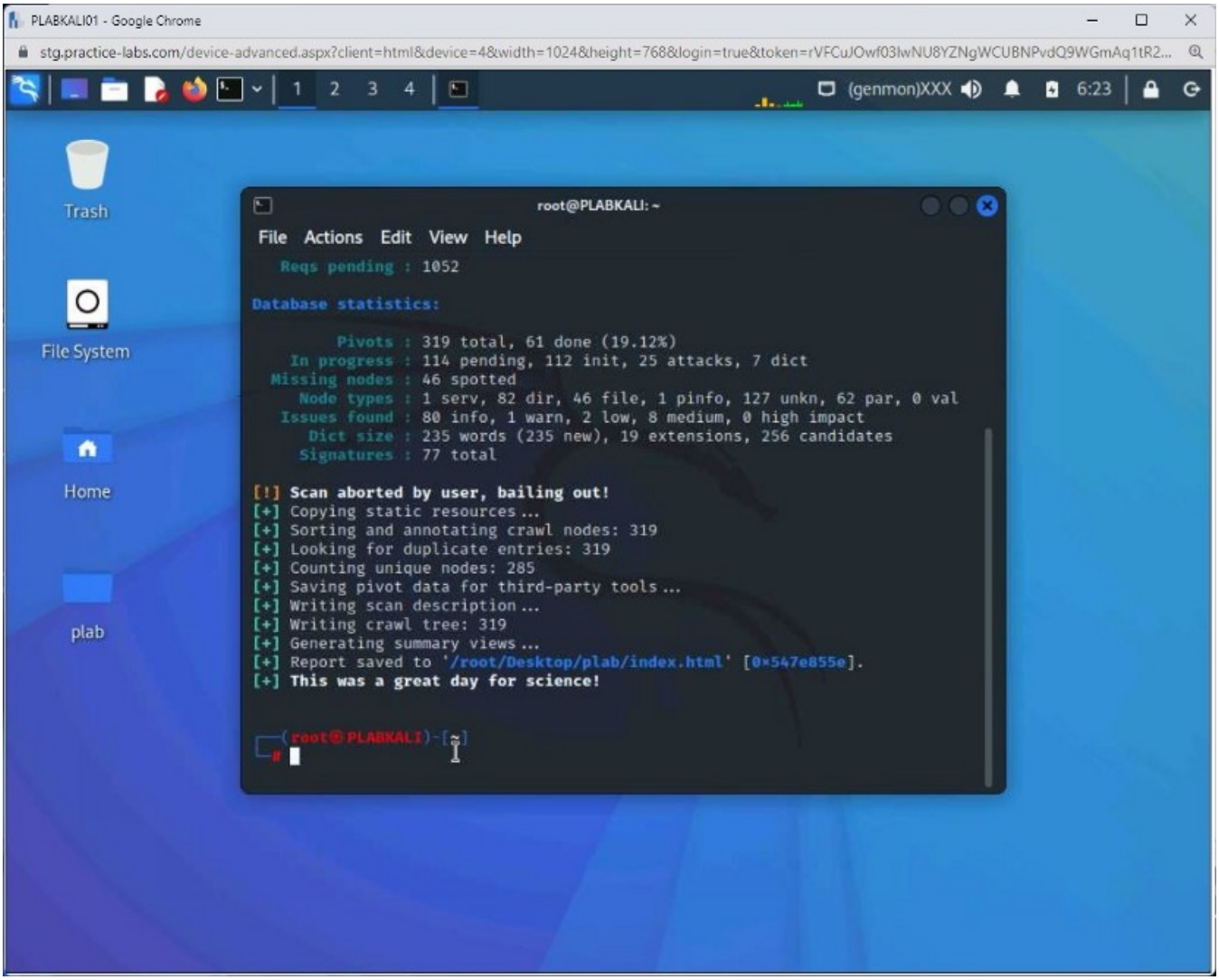



**Step 4**

You can stop the scanning process by pressing the **Ctrl + C** keys.

However, in a real environment, you must let the process complete to get an overall picture on security posture.

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

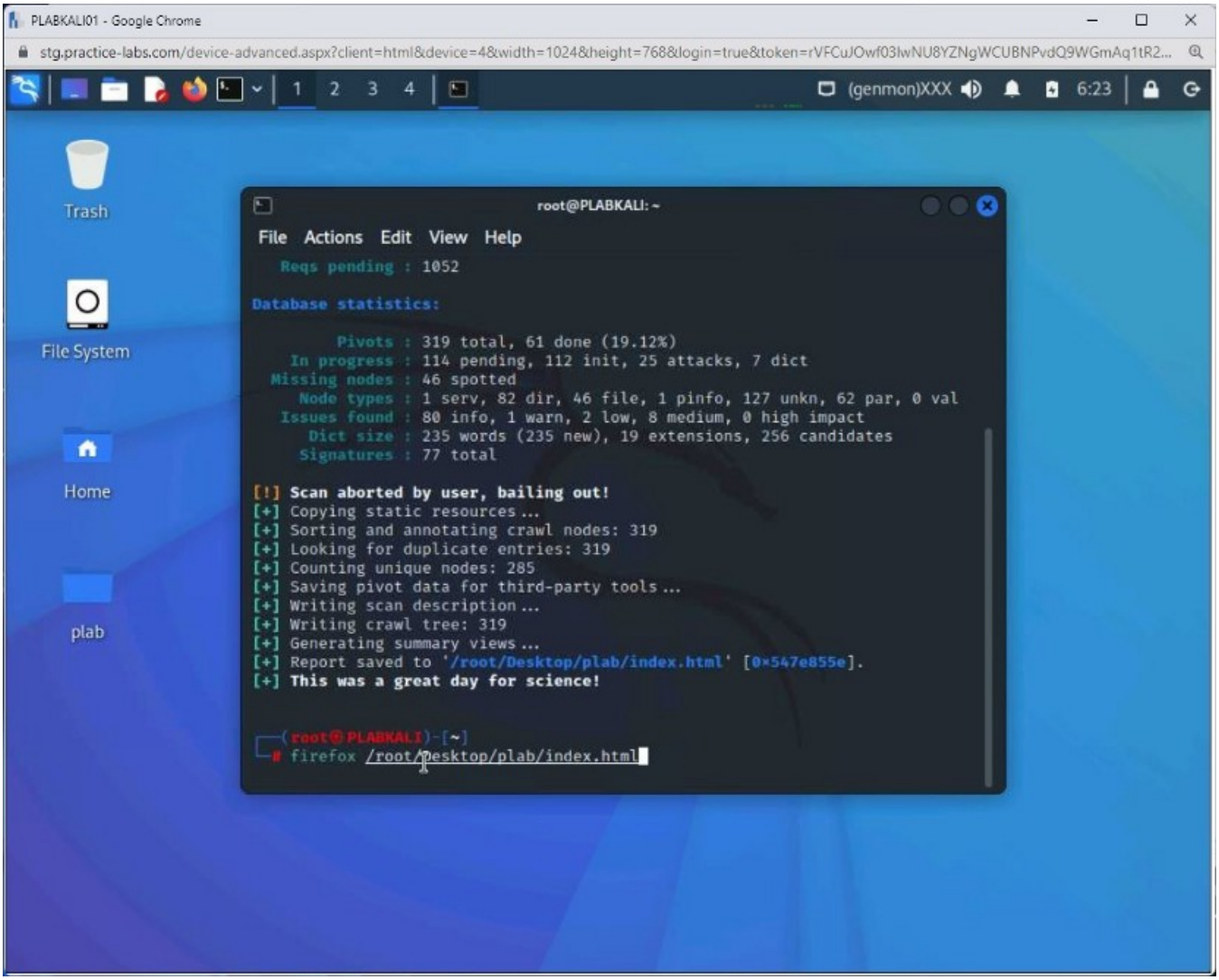



### Step 5

To view the scan report, type the following command:

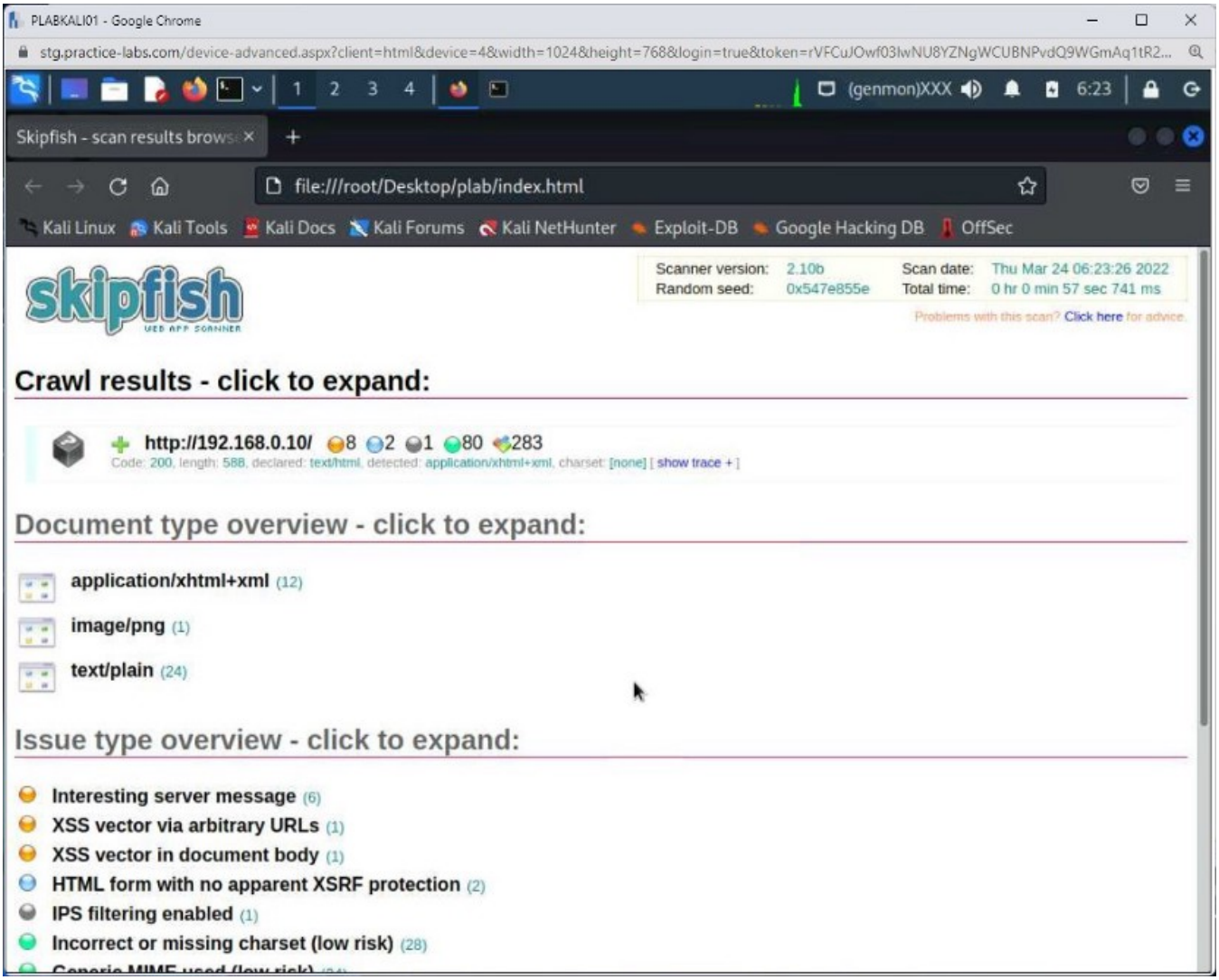
```
firefox /root/Desktop/plab/index.html
```

Press **Enter**.



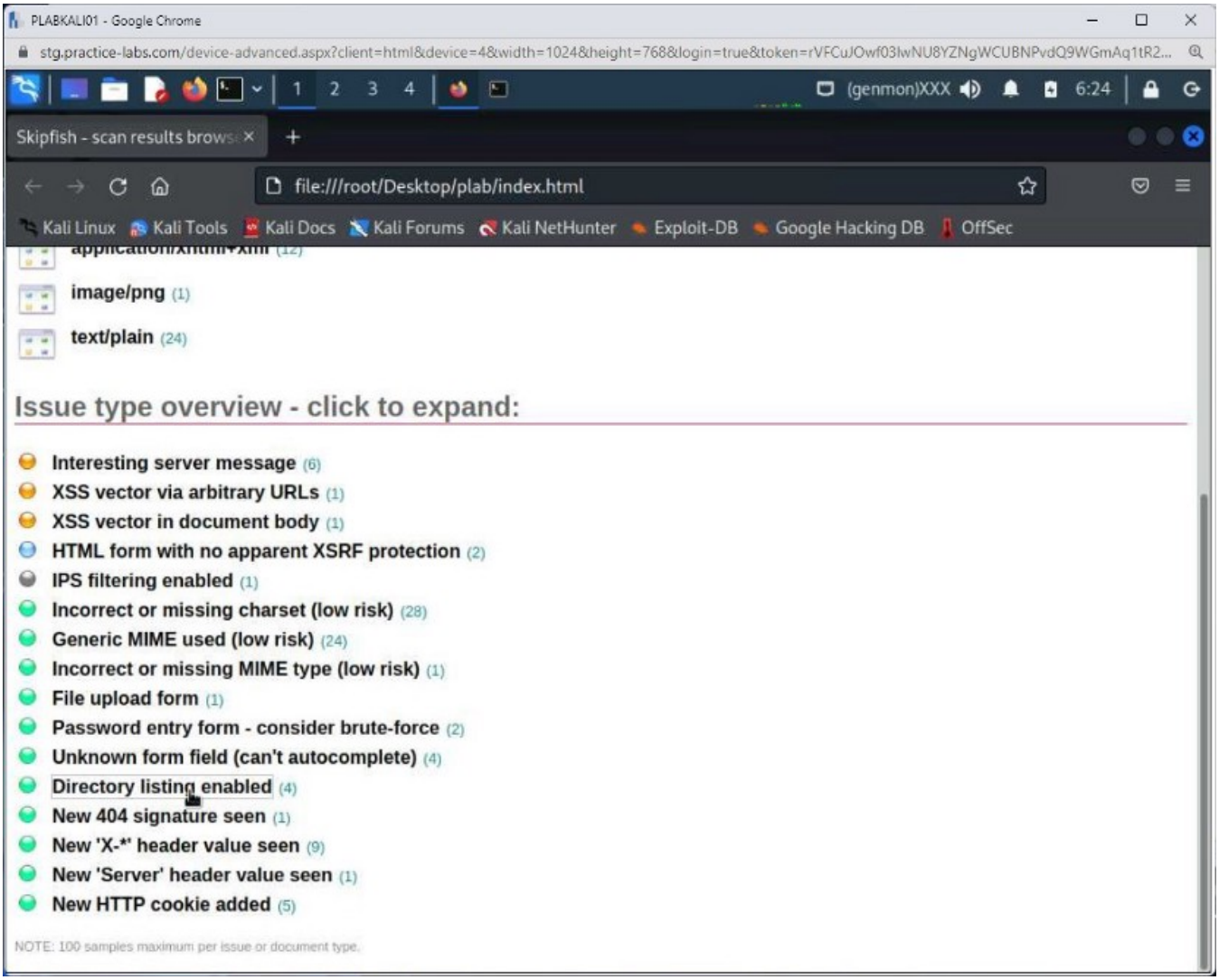

### Step 6

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



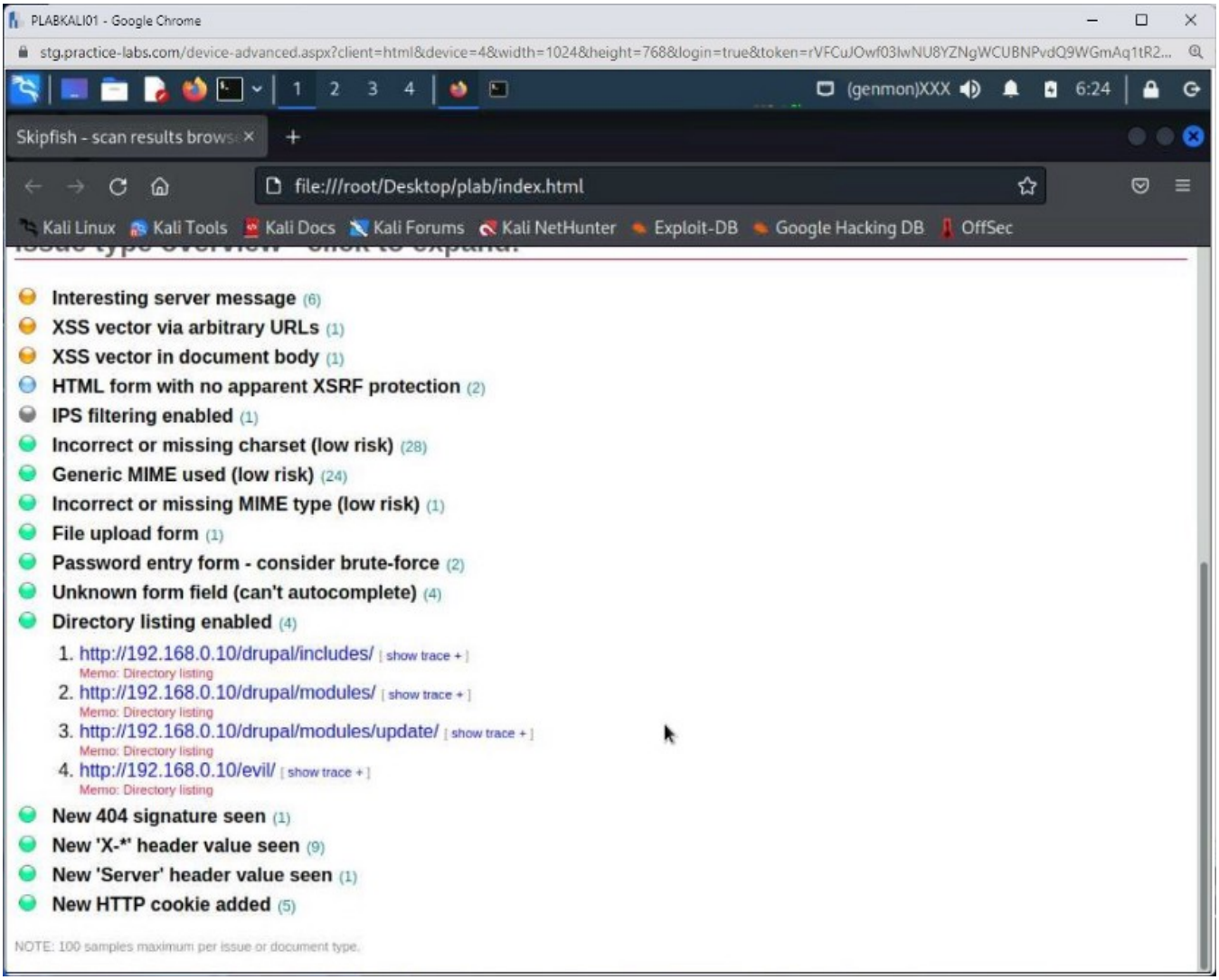

### Step 7

Scroll down and click on **Directory listing enabled** in the **Issue type overview** section.




### Step 8

Several different paths are shown that have directory listing enabled.




Close the Firefox window and keep the terminal window open.

## Task 3 — Footprint Using the nc Command

Netcat (or the nc command) is a multi-purpose tool that can read and write network connections as well as perform network debugging and exploration. It can also be used for footprinting a web server.

In this task, you will use the nc command to footprint a web server.

### Step 1

Connect to **PLABKALI01**. Ensure that the terminal window is open.

Clear the screen by entering the following command:

```
clear
```

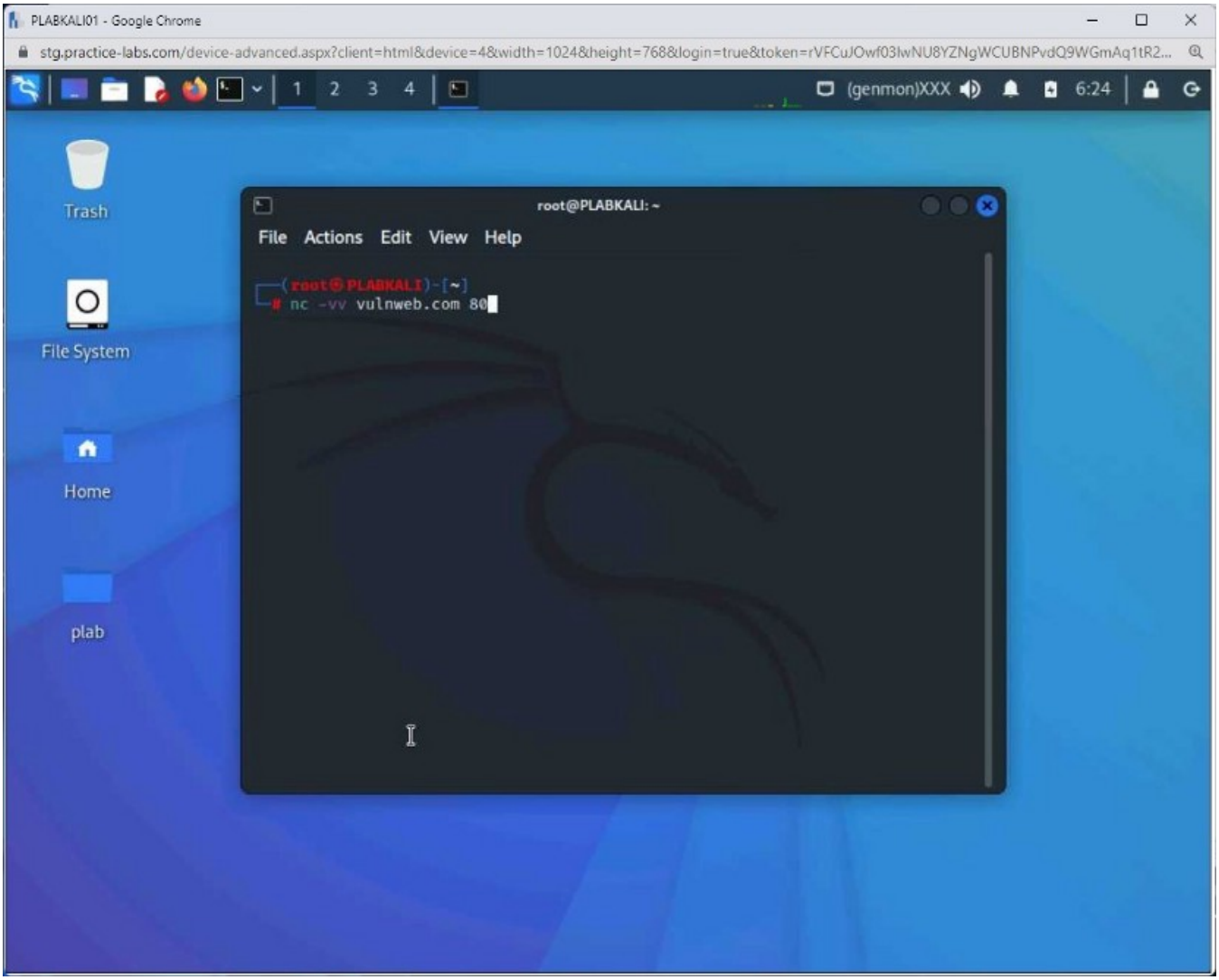
Press **Enter**.

Type the following command:

```
nc -vv vulnweb.com 80
```

Press **Enter**.

***Note**: You can use **-v** for verbose output and double **vv** for more verbose output. You need to pass the website name as the argument and the port number you want to use.*



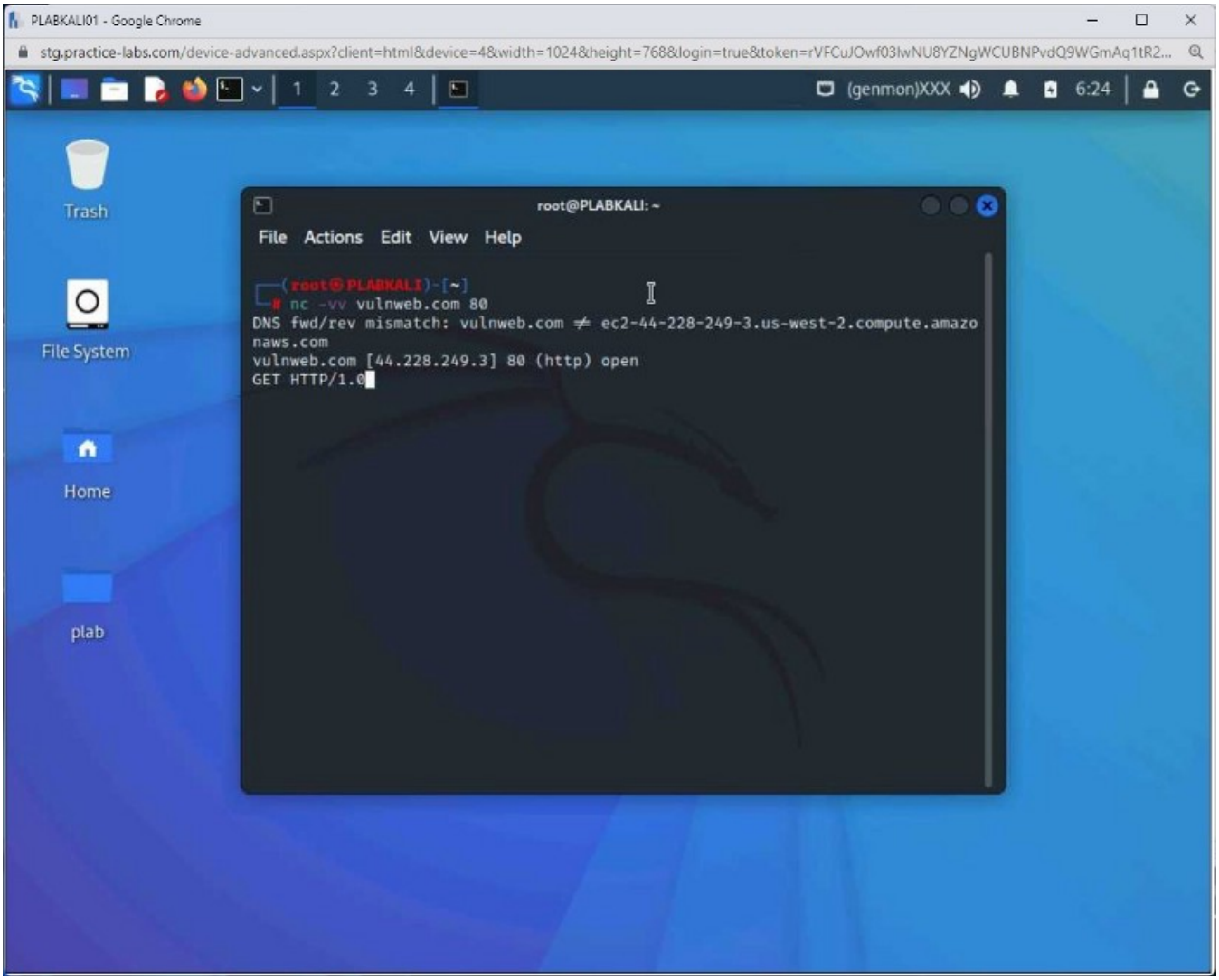

**Step 2**

The **nc** command displays some bit of details.

Next, in the blank line, you need to enter the following command:

```
GET HTTP/1.0
```

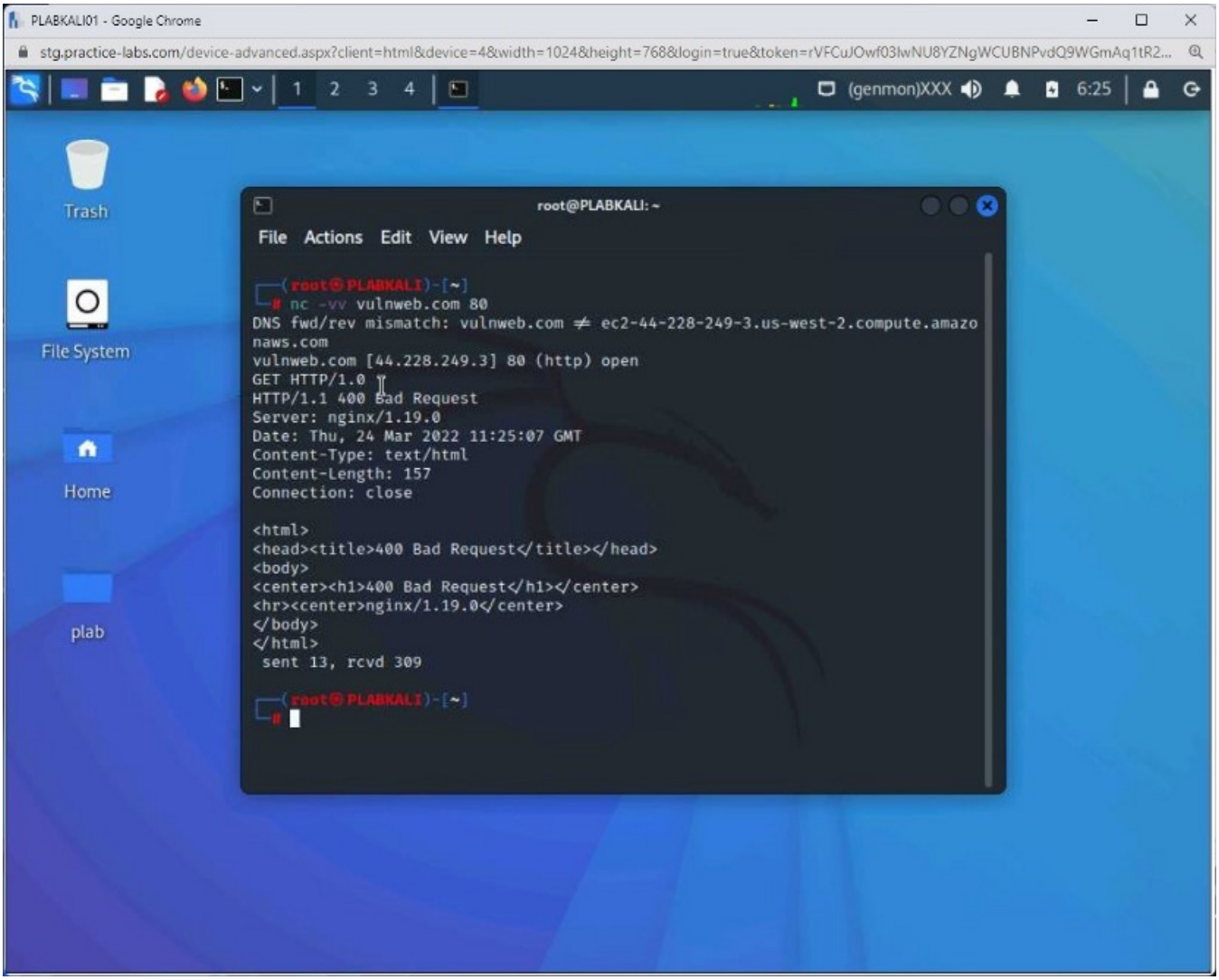
Press **Enter**.




### Step 3

The output of the **GET** command is displayed.

Notice that it has been able to determine the web server name and version. With this information, you can determine the vulnerabilities and exploit them.




Keep the terminal window open.

## Task 4 — Find the Web Server Version using the Metasploit Framework

The Metasploit framework is the most widely used tool in exploiting vulnerabilities, and a free edition is available in Kali Linux. Metasploit has a modular and flexible architecture that helps you develop new exploits as more and more vulnerabilities are discovered.

Metaspolit is also used in penetration testing, and can be used either with or without a database. If you configure it with a database, then Metasploit will track what you do within the framework.

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

In this task, you will find the web server version using the Metasploit Framework.

### Step 1

Connect to **PLABKALI01**. Ensure that the terminal window is open.

Clear the screen by entering the following command:

```
clear
```

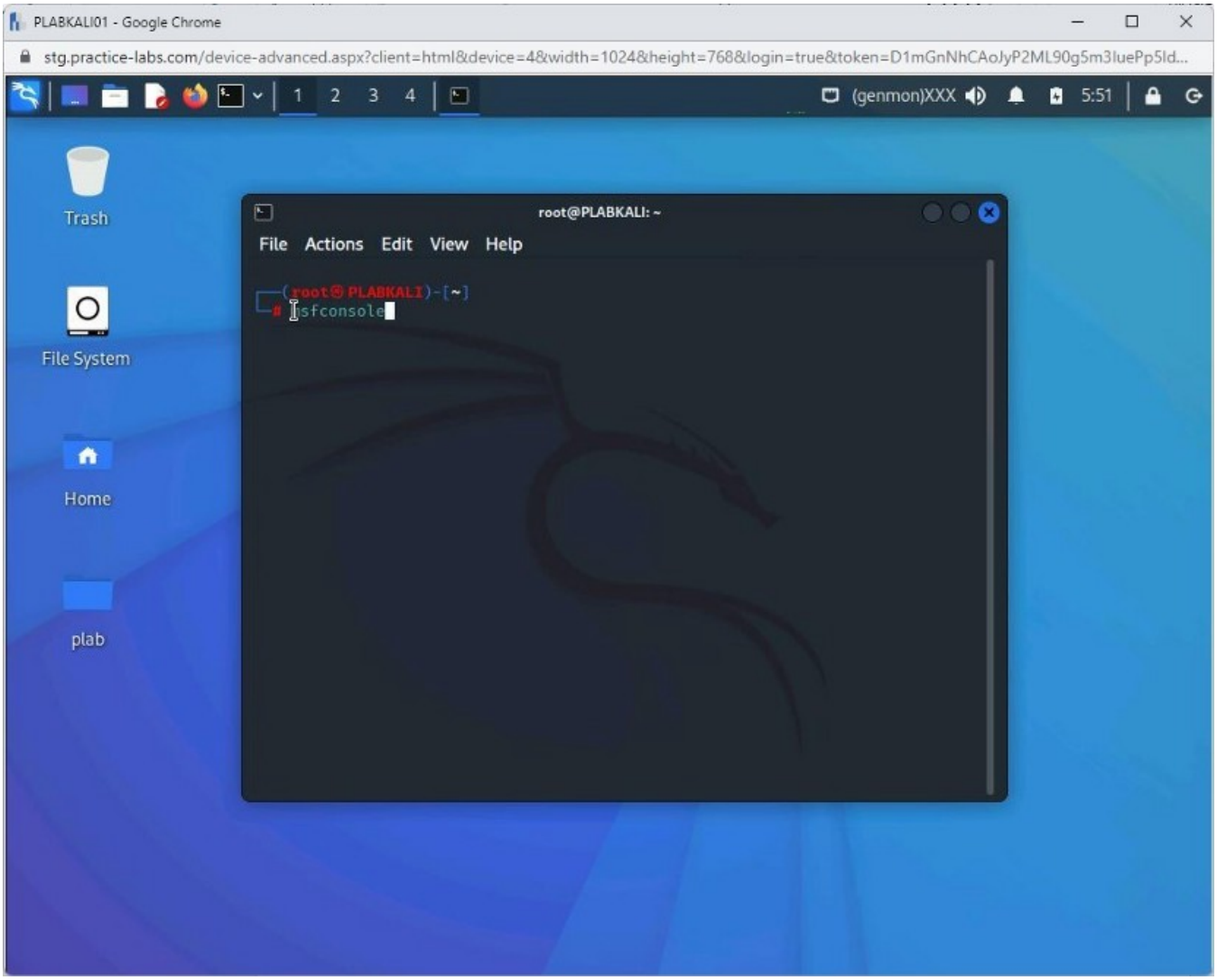
Press **Enter**.

In the terminal window, you can start the Metasploit Framework Console. To do this, type the following command:

```
msfconsole
```

Press **Enter**.

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



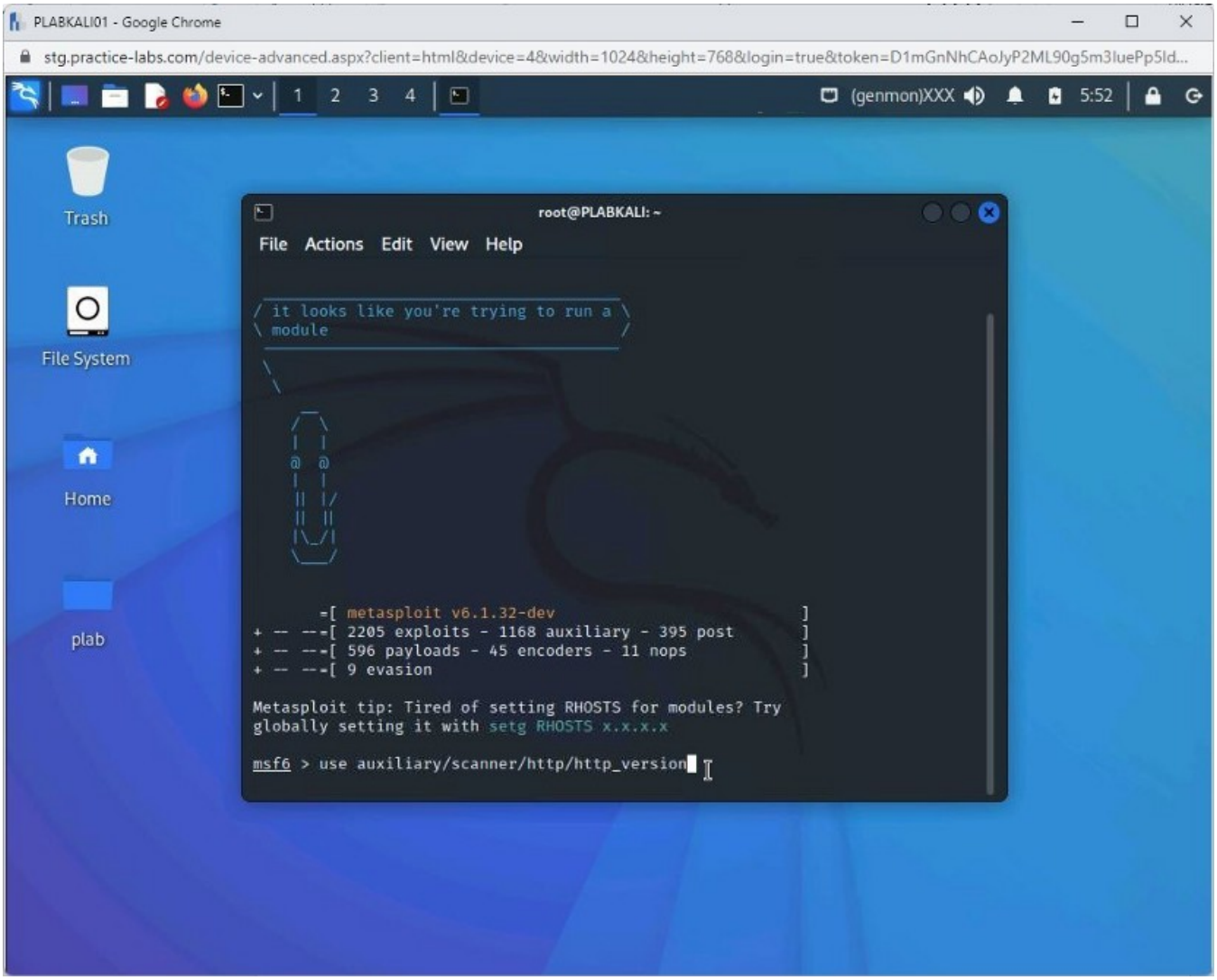

**Step 2**

After the initialization, you are navigated to the Metasploit Framework prompt.

To find the server version, you need to load the **http_version** module. To do this, type the following command:

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

Press **Enter**.

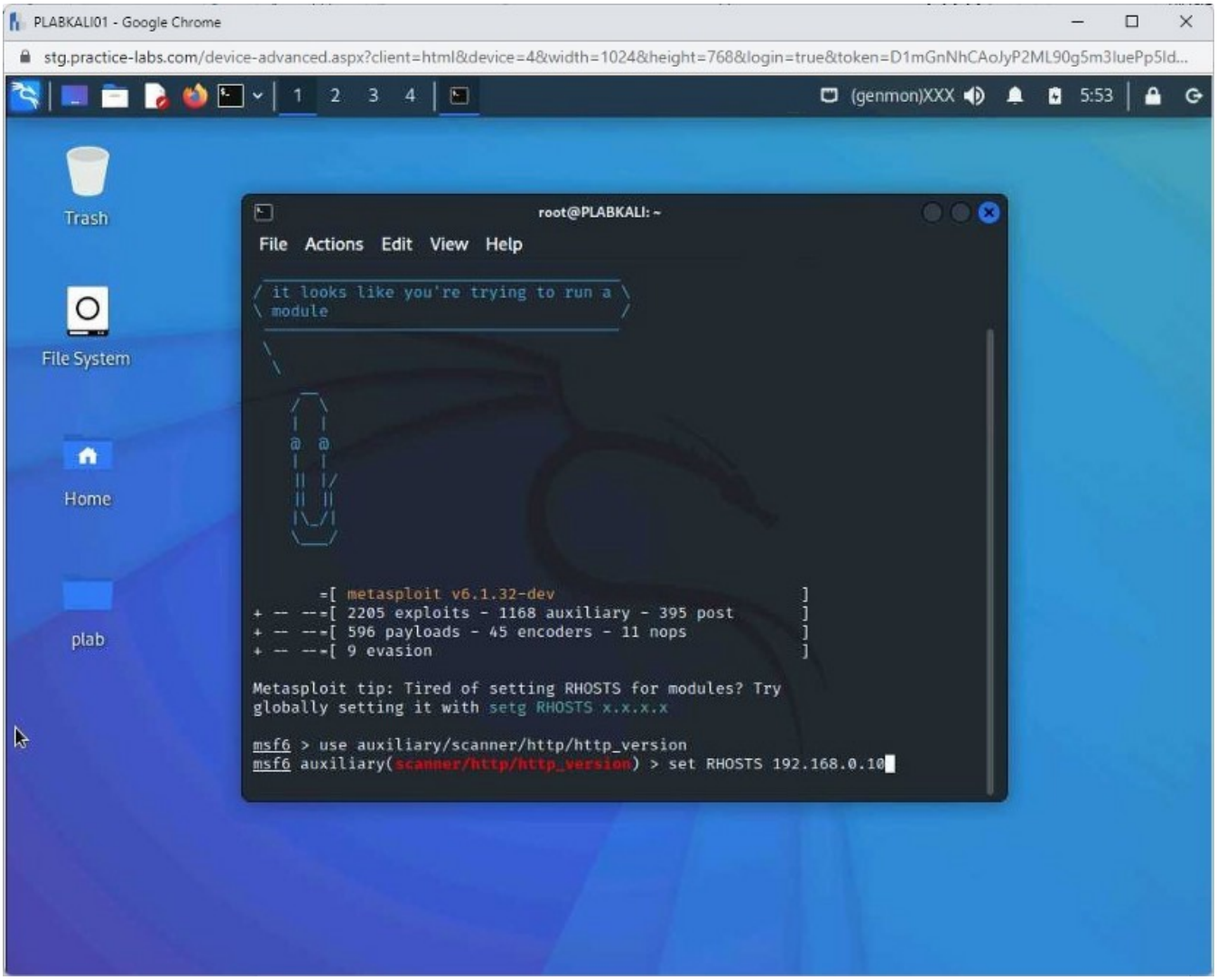



### Step 3

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

```
set RHOSTS 192.168.0.10
```

Press **Enter**.



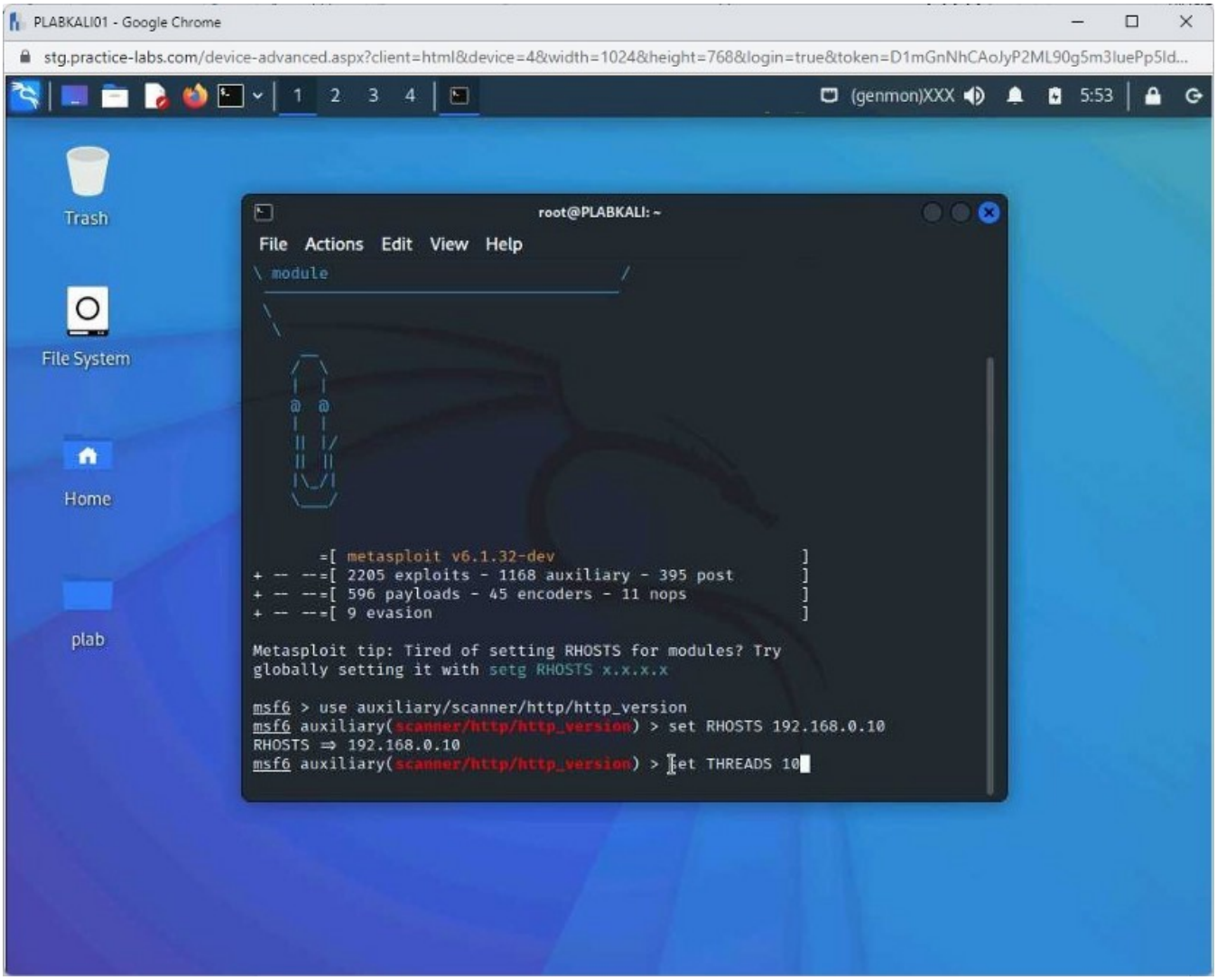

**Step 4**

Next, you will need to set the number of threads.

To do this, type the following command:

```
set THREADS 10
```

Press **Enter**.

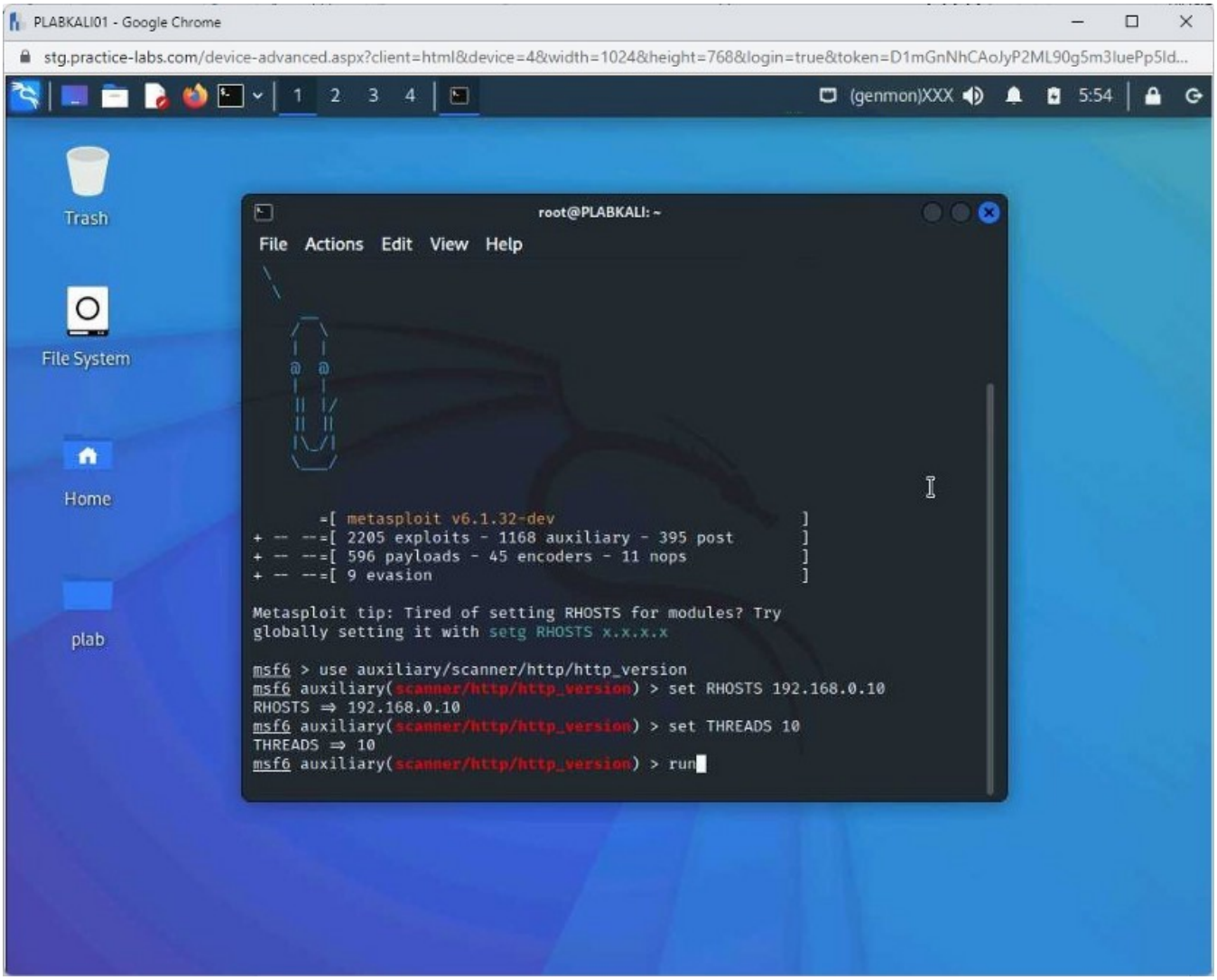



### Step 5

Now, type the following command to execute the payload:

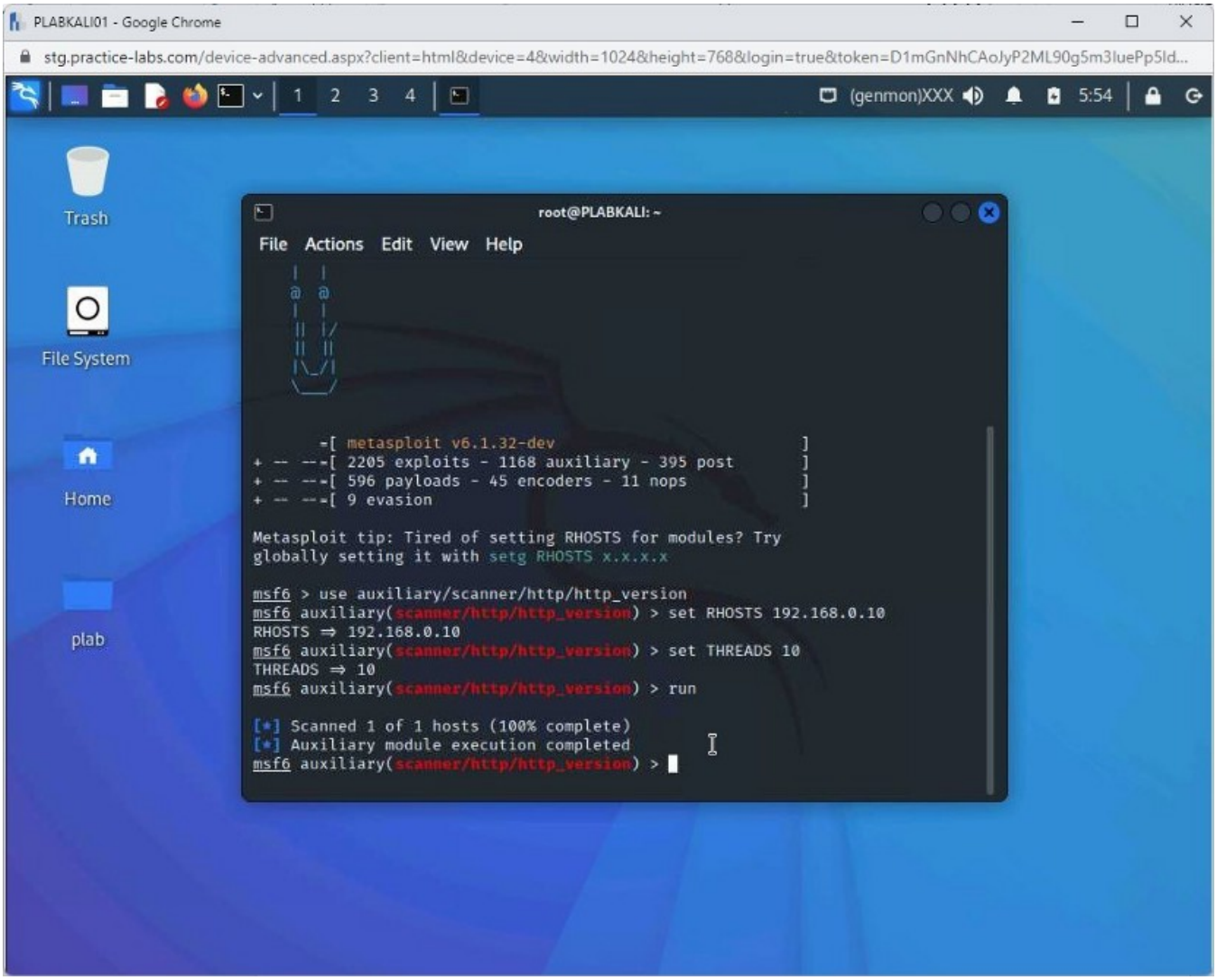
```
run
```

Press **Enter**.




**Step 6**

The details of the server are now displayed.



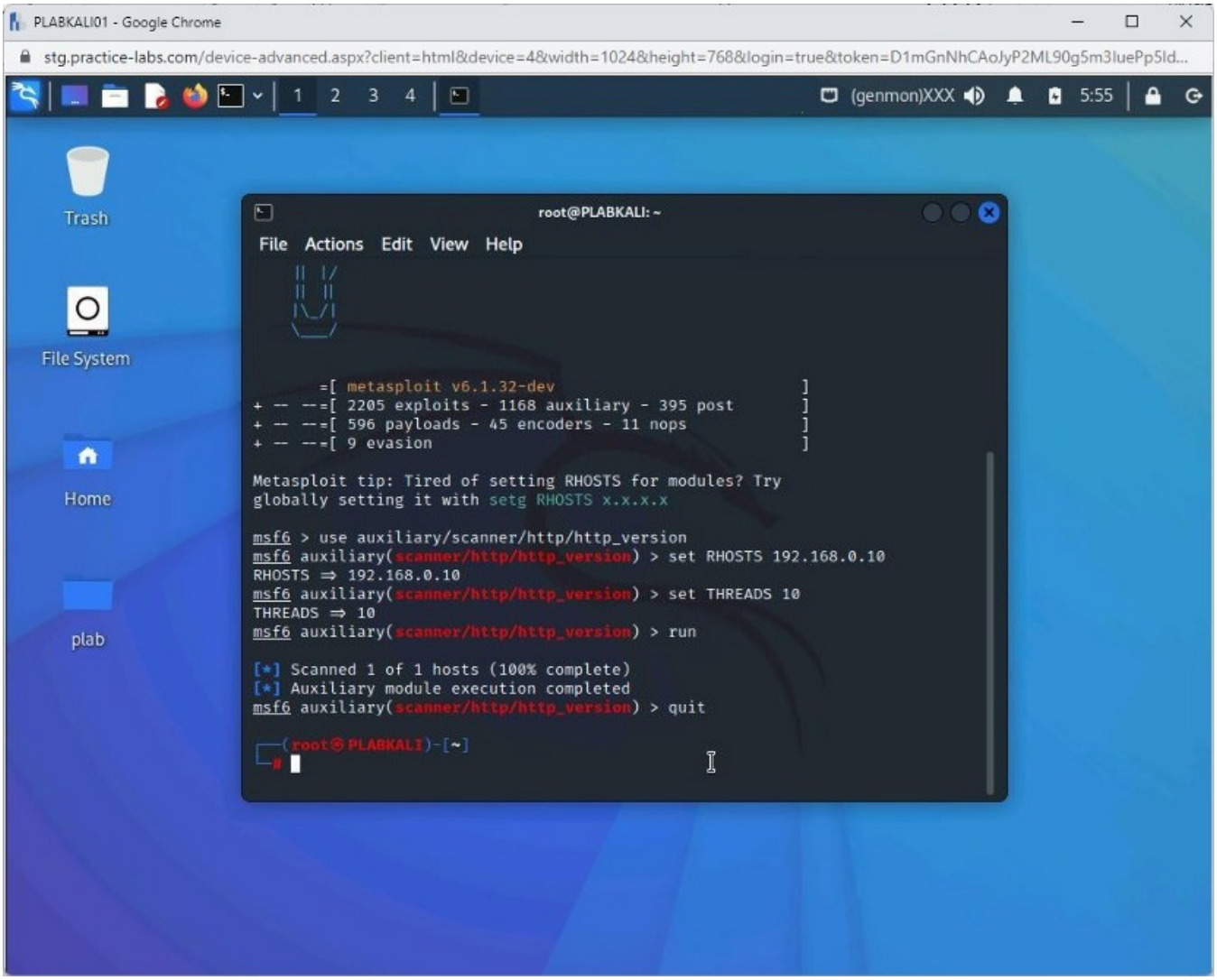

**Step 7**

To exit from the console, type the following command:

```
quit
```

Press **Enter**.

You will be returned to the root prompt.




Keep the terminal window option

## Task 4 — Find Files on a Web server using Metasploit Frameworks

You can use the Metasploit Framework for various reasons, from finding files to penetrating a system or network. In this task, you will learn to find files on a web server using Metasploit Framework. To do this, perform the following steps:

### Step 1

Connect to **PLABKALI01**. Ensure that the terminal window is open.

In the previous task, you had exited from the Metasploit Framework console. As you had logged out, you need to start the console once again with the Msfconsole command.

If you had to remain in the console and use another module instead of http_version, you could have used the back command.

Clear the screen by entering the following command:

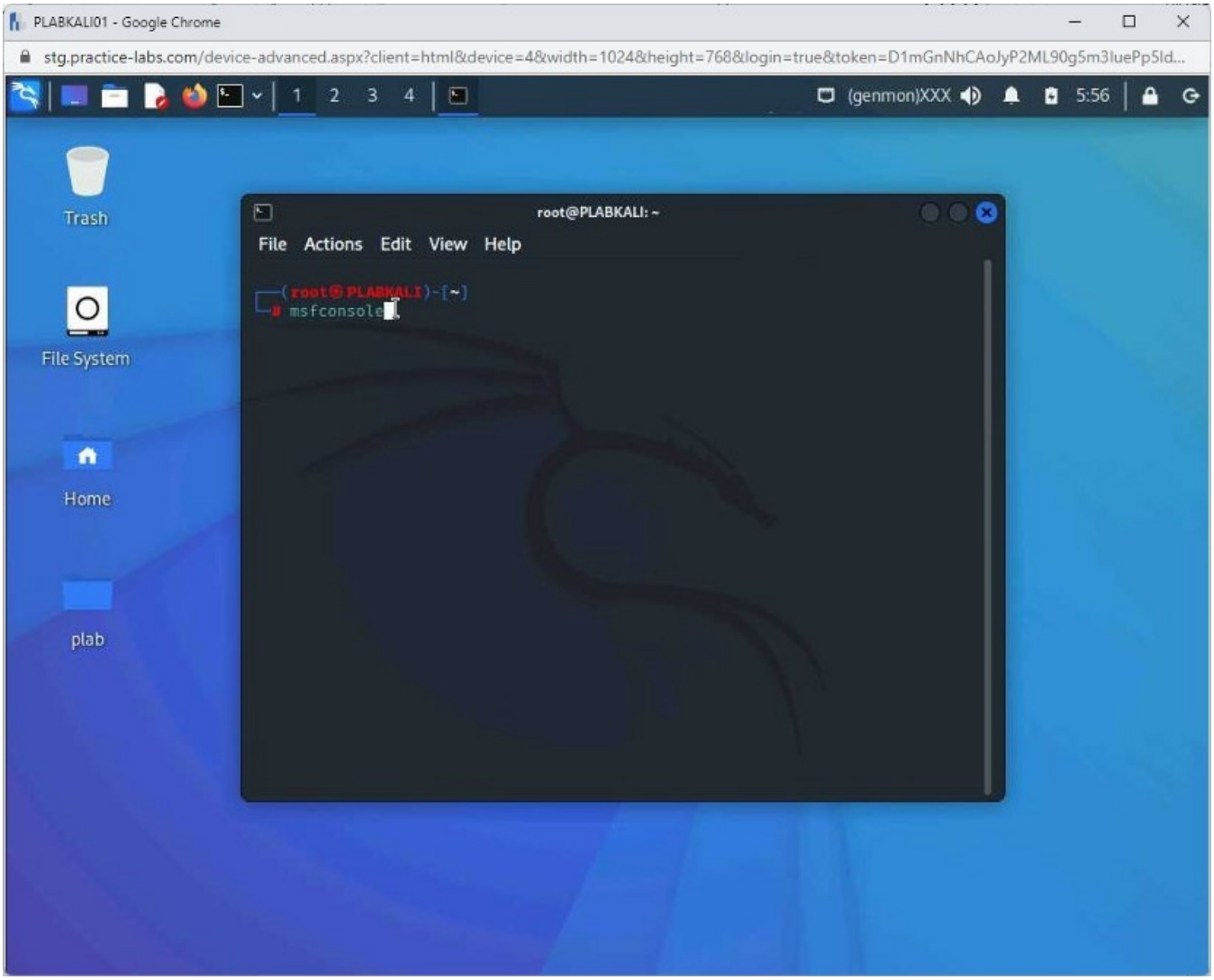
```
clear
```

Press **Enter**.

In the terminal window, you can start the Metasploit Framework Console. To do this, type the following command:

```
msfconsole
```

Press **Enter**.



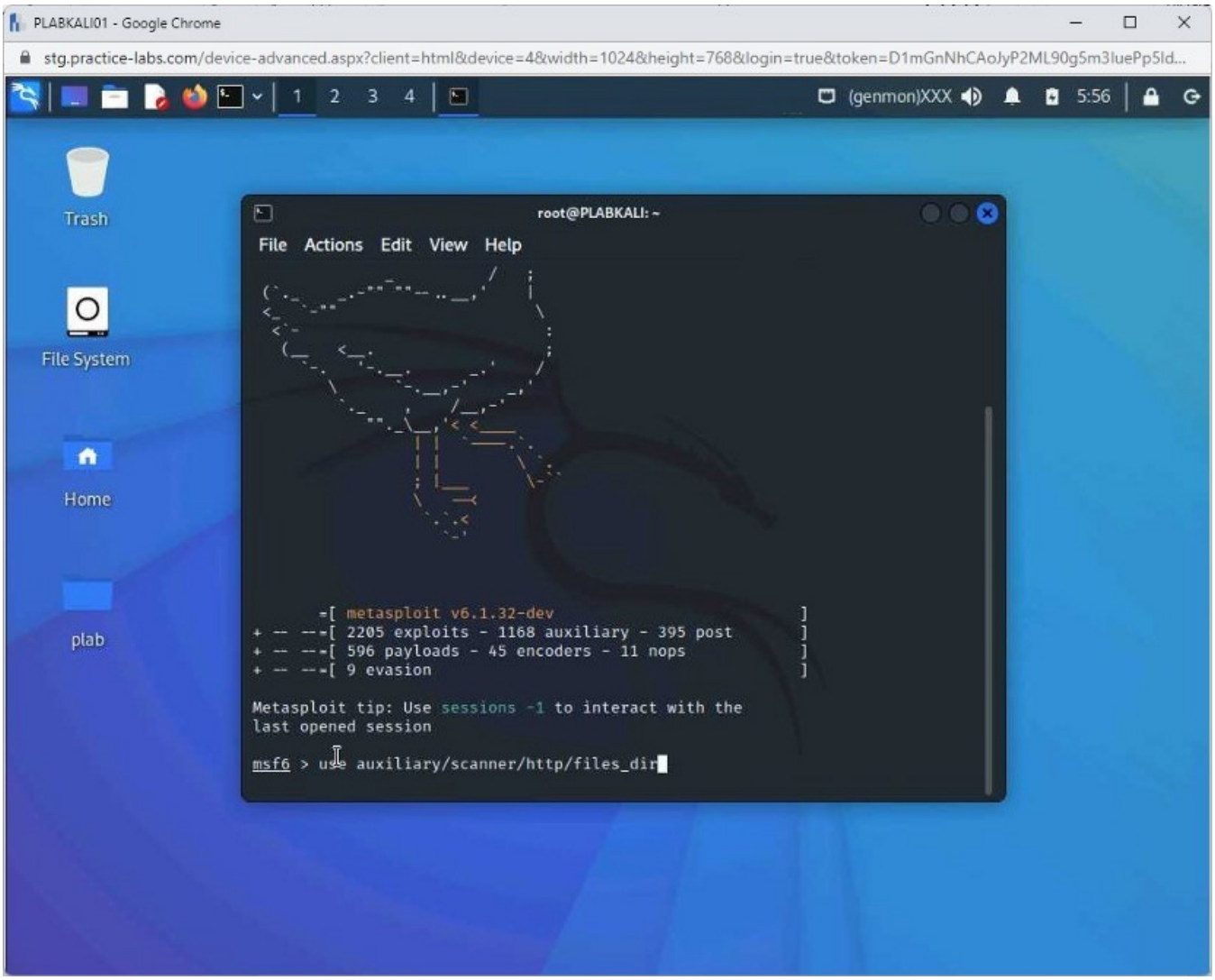

**Step 2**

After the initialization, you are navigated to the Metasploit Framework prompt.

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

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

Press **Enter**.



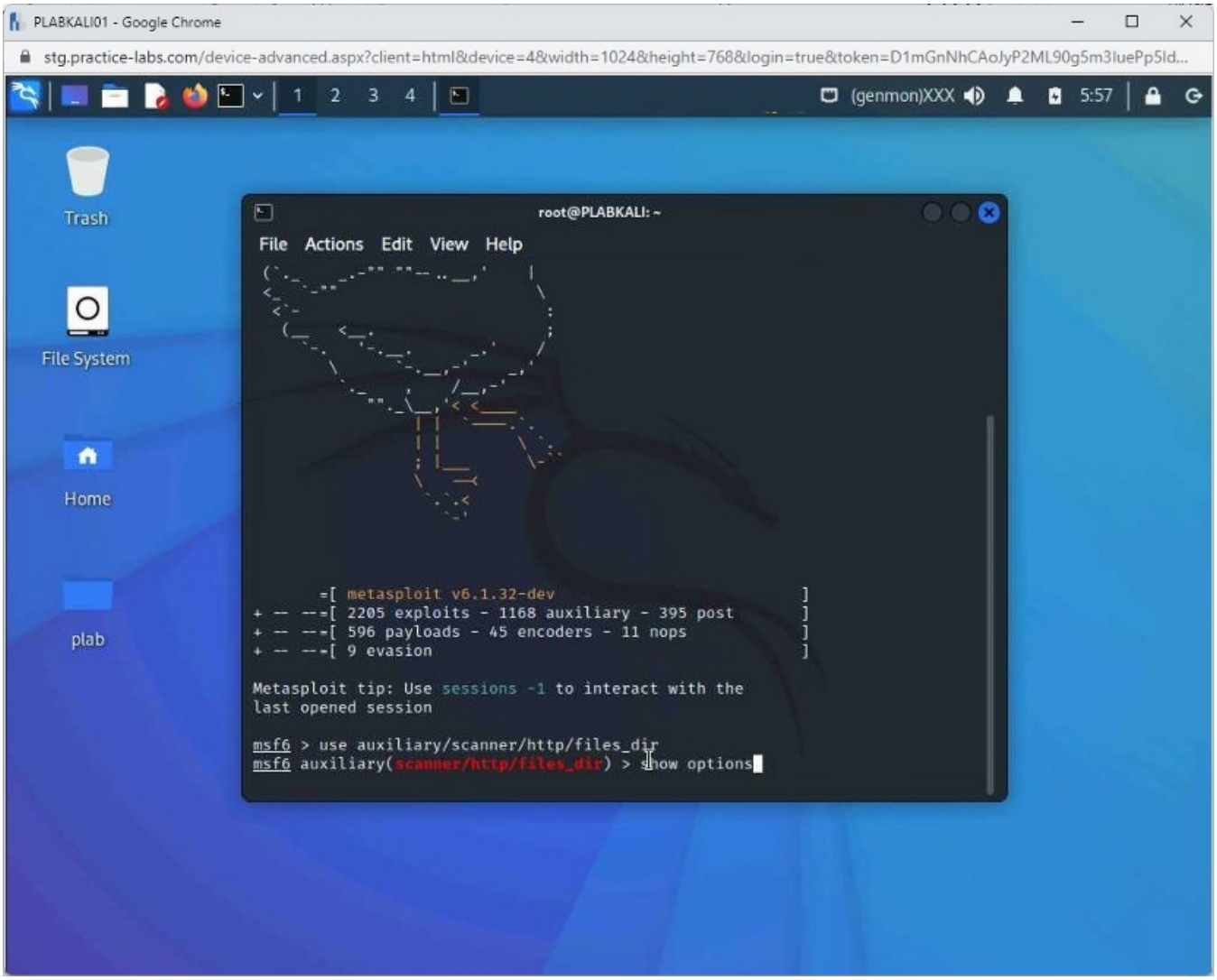

### Step 3

The **files_dir** module is now loaded.

To check the configuration options for the **files_dir** module, type the following command:

```
show options
```

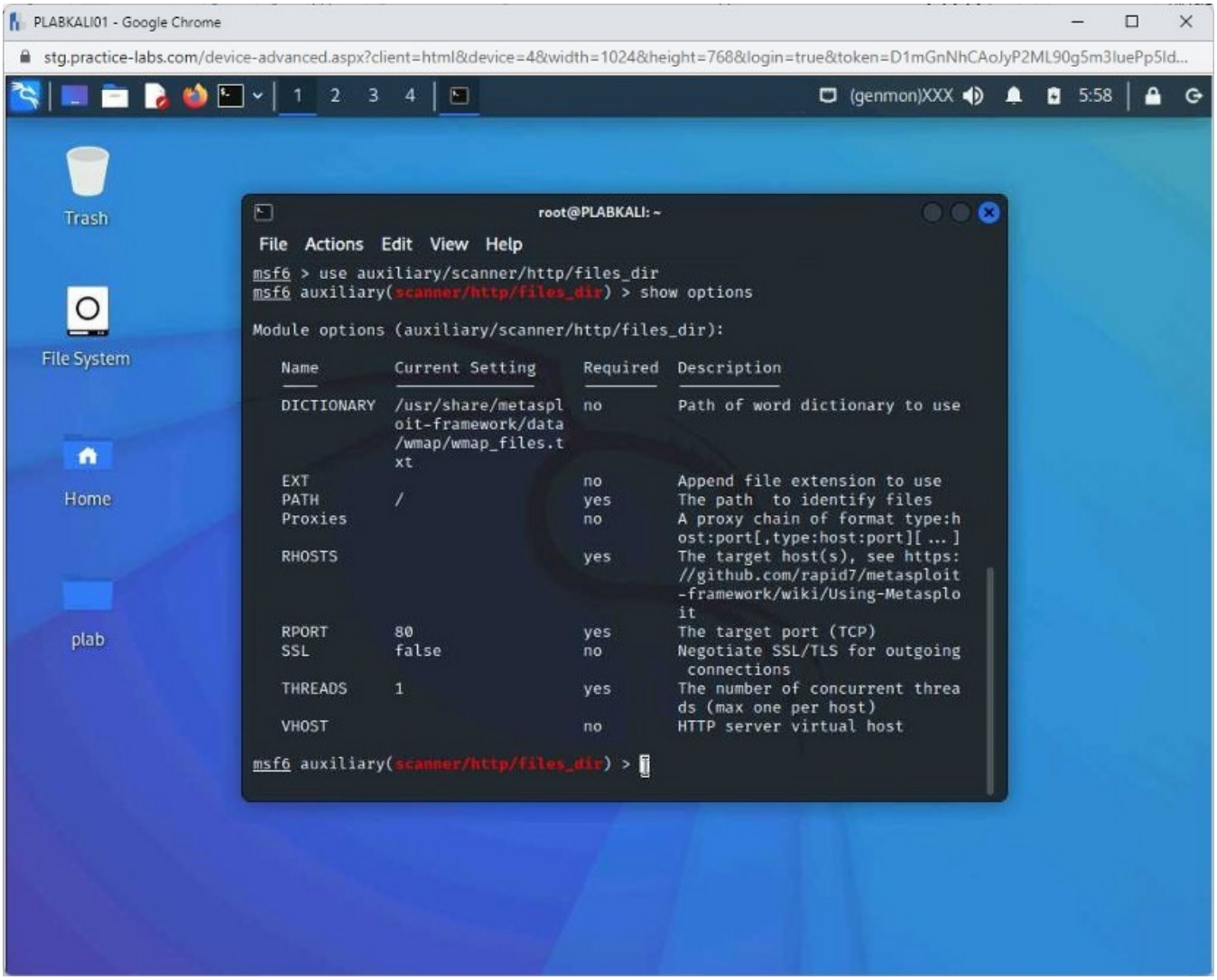
Press **Enter**.




### Step 4

Various options are displayed. Some of these are configured by default, and some need to be configured.

Notice that the **DICTIONARY** option is already configured with a built-in dictionary that contains the keywords for searching on the target system.




**Step 5**

Clear the screen by entering the following command:

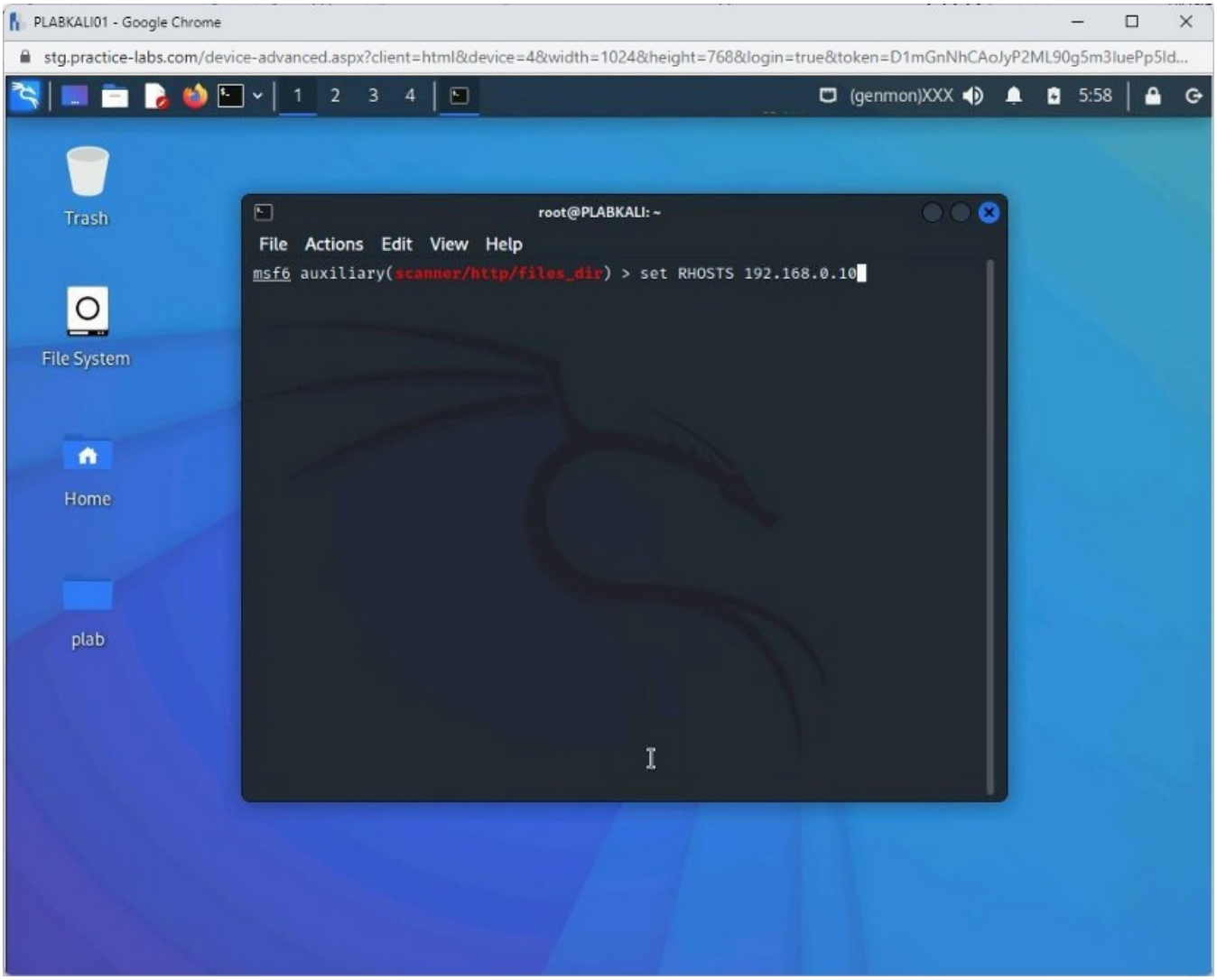
```
clear
```

Press **Enter**.

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

```
set RHOSTS 192.168.0.10
```

Press **Enter**.

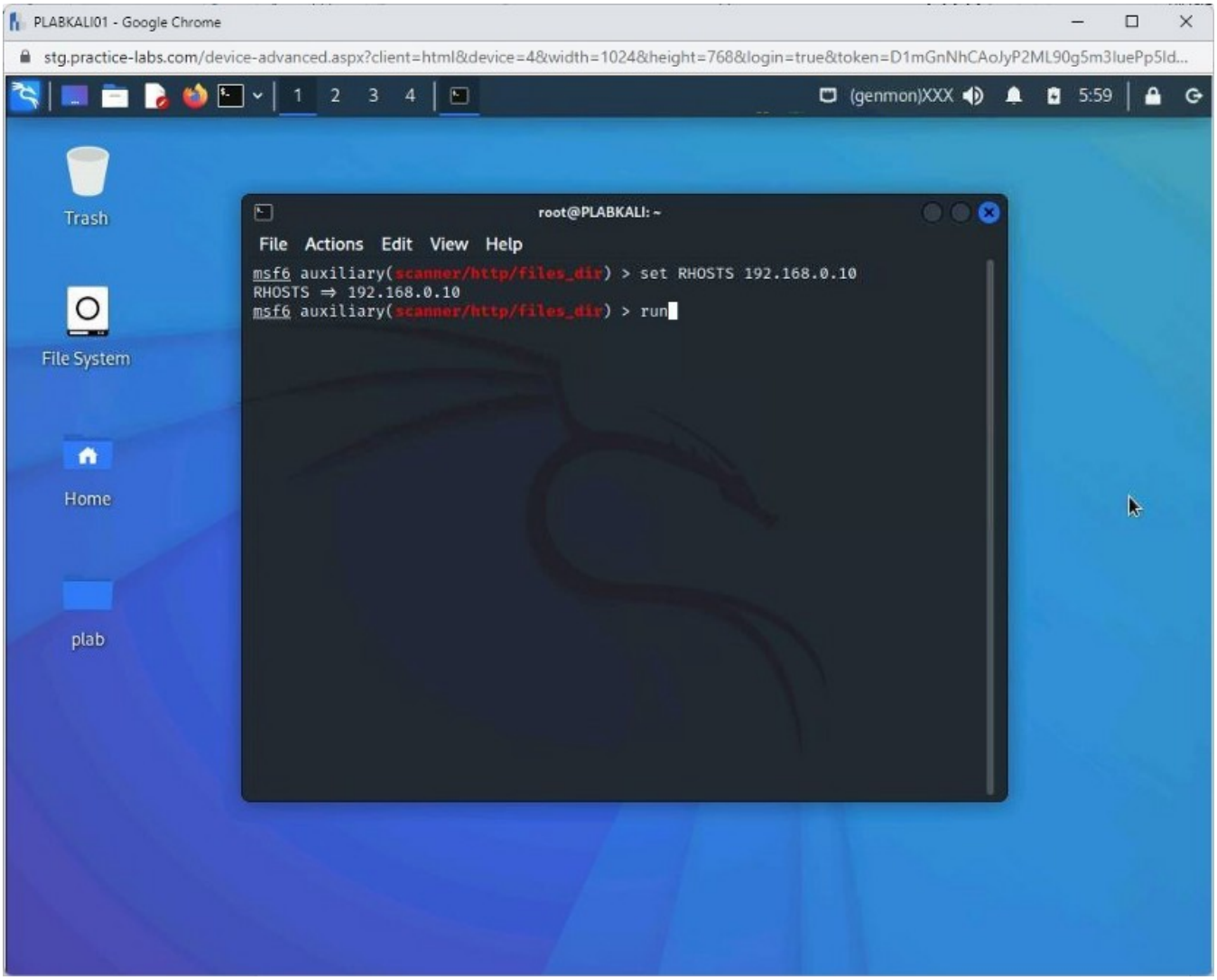



### Step 6

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

```
run
```

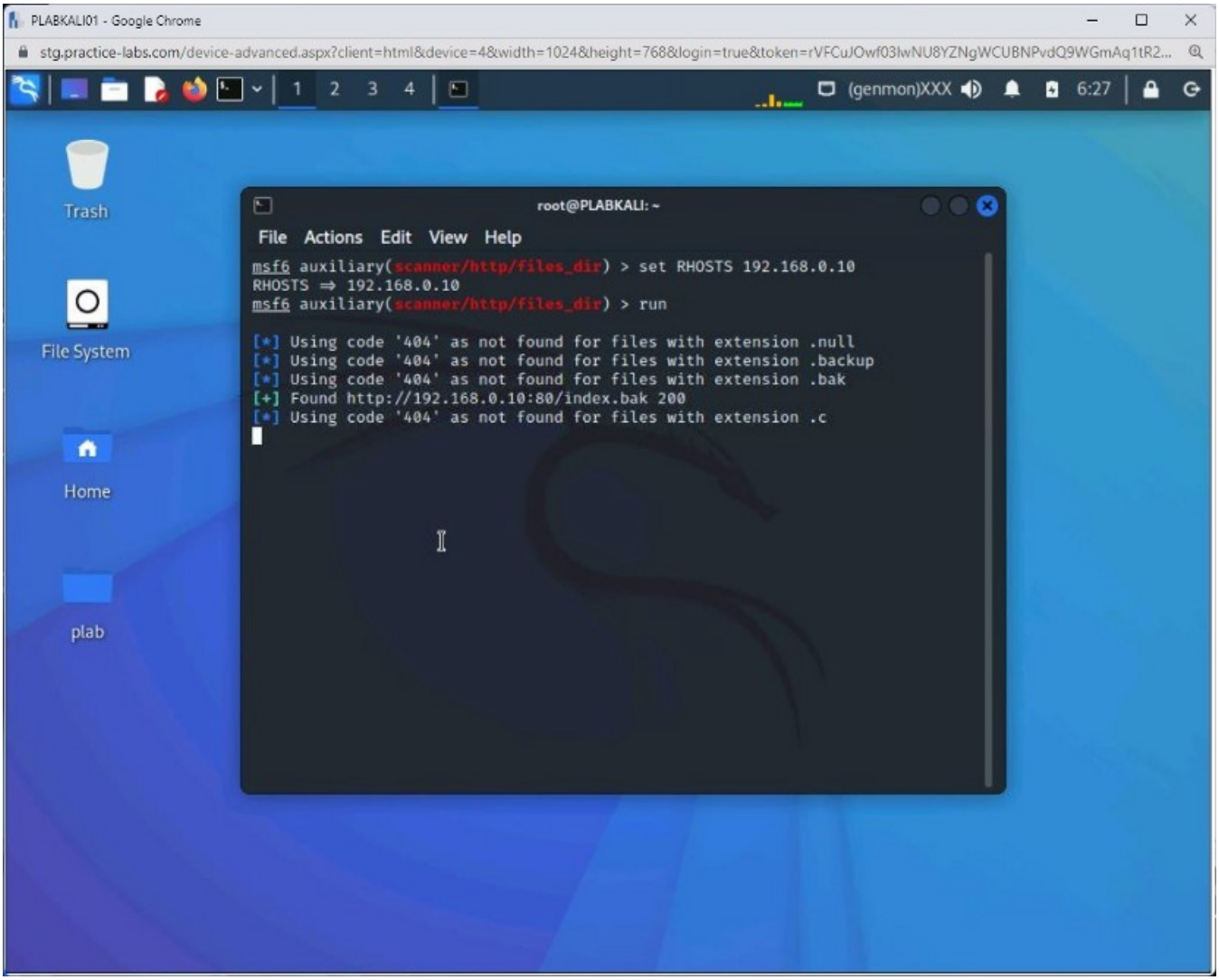
Press **Enter**.




**Step 7**

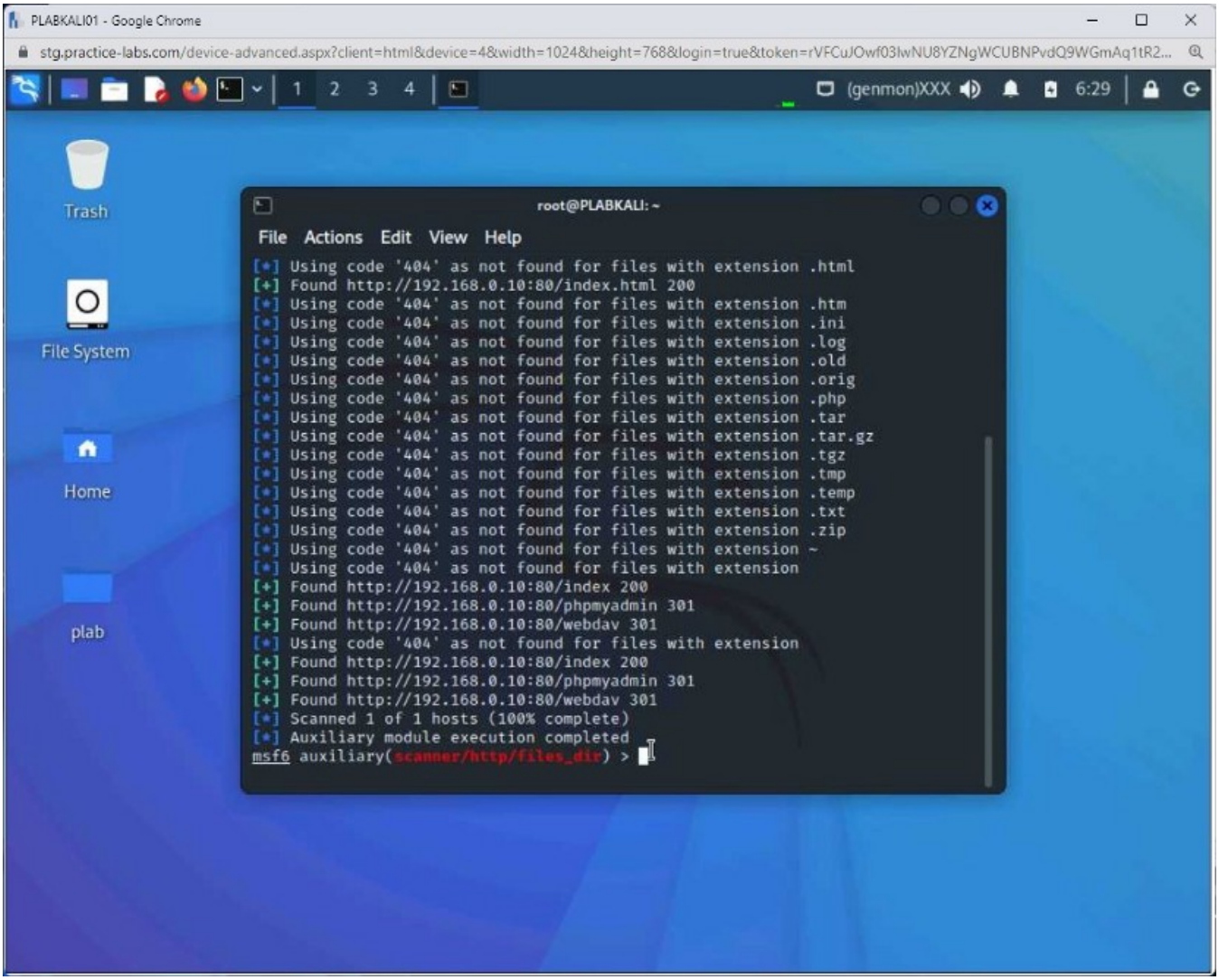
The payload is now executed on the target host. It is now attempting to find files of specific types.

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




**Step 8**

Once the process is completed, several files that can be useful to an attacker are found.




Keep the terminal window open.

## Task 5 — Scan for Options on a Web server using Metasploit Framework

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

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

### Step 1

Reconnect to **PLABKALI01**. Ensure that you are on the Metasploit Framework terminal.

Clear the screen by entering the following command:

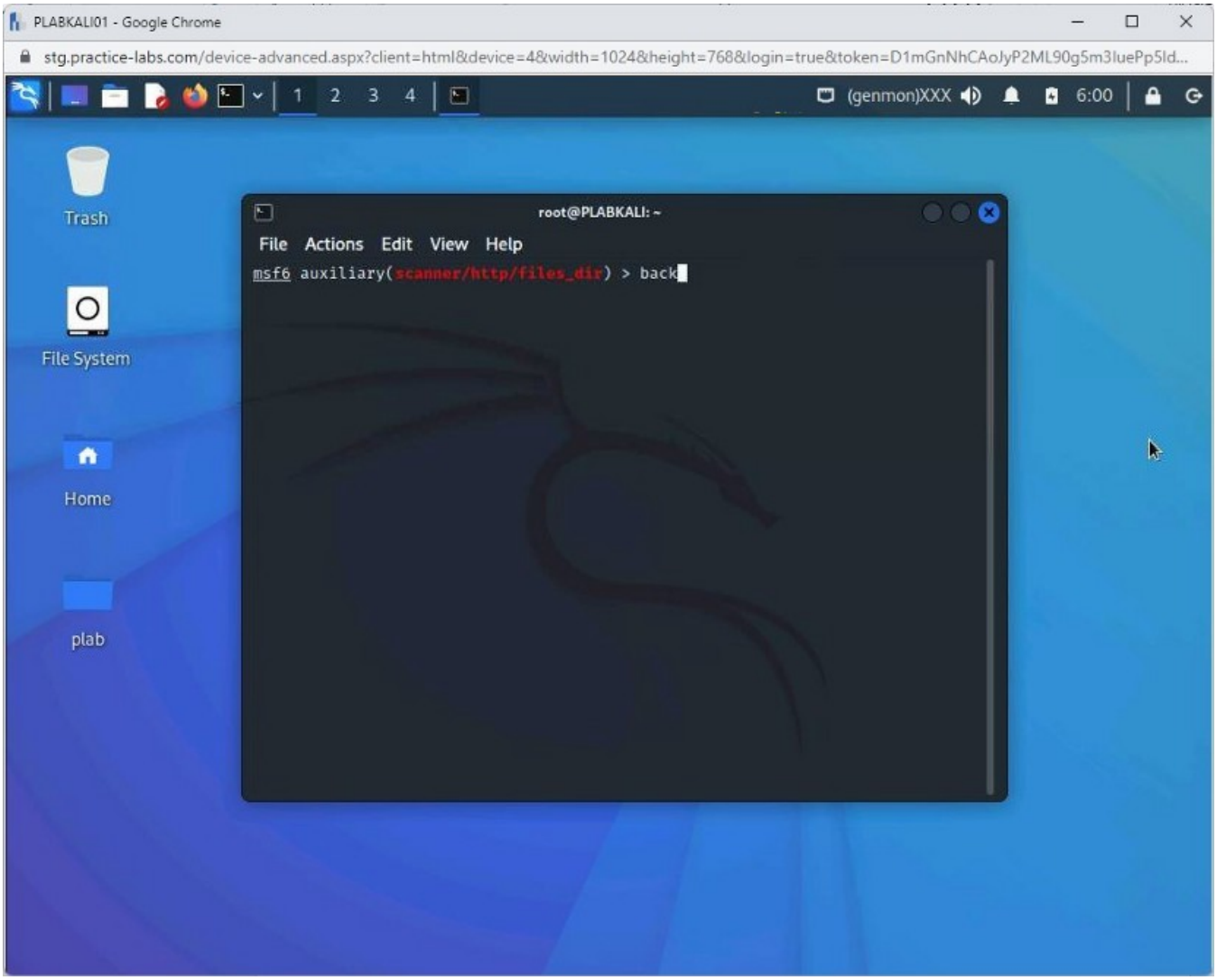
```
clear
```

Press **Enter**.

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

```
back
```

Press **Enter**.

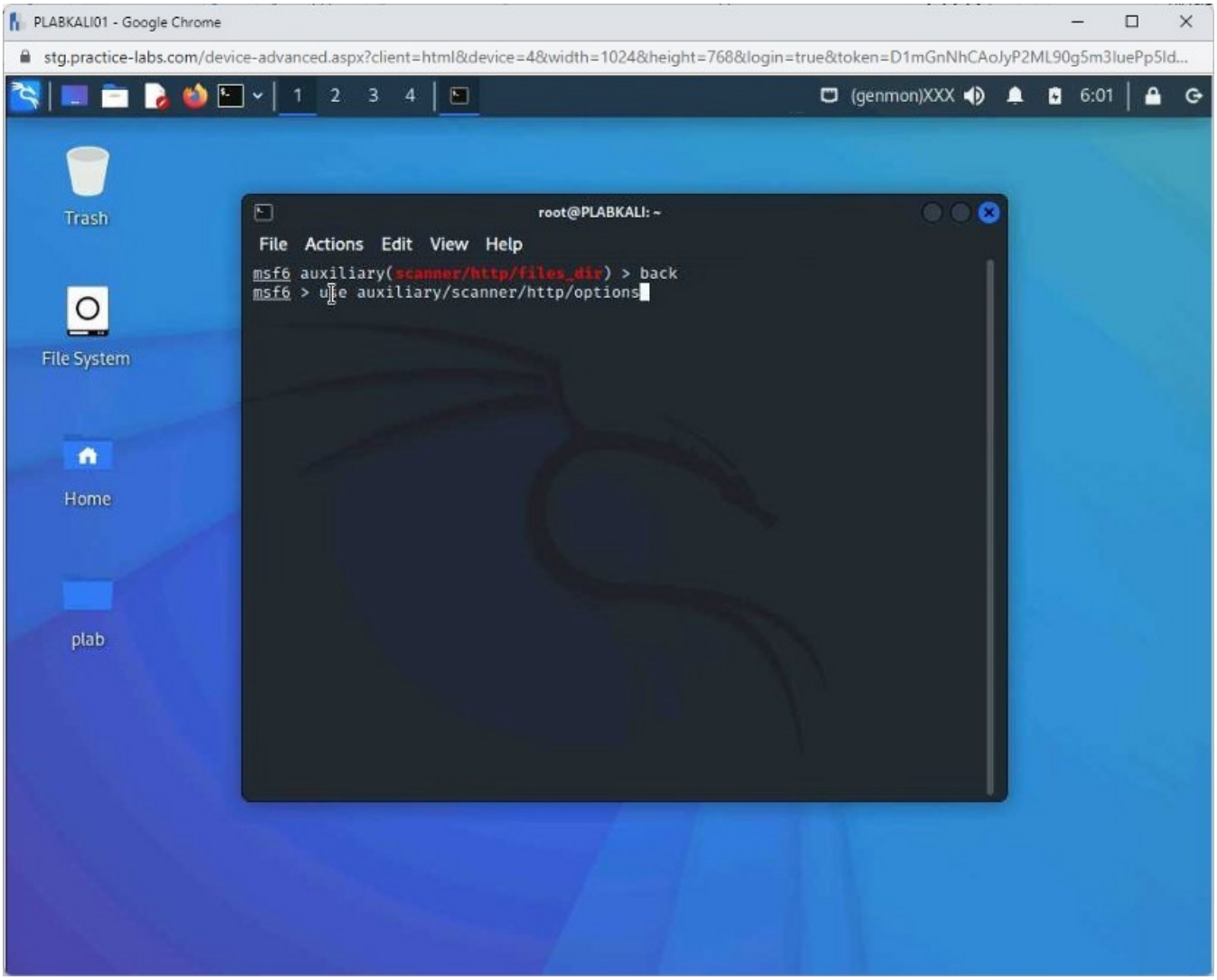



### Step 2

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

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

Press **Enter**.

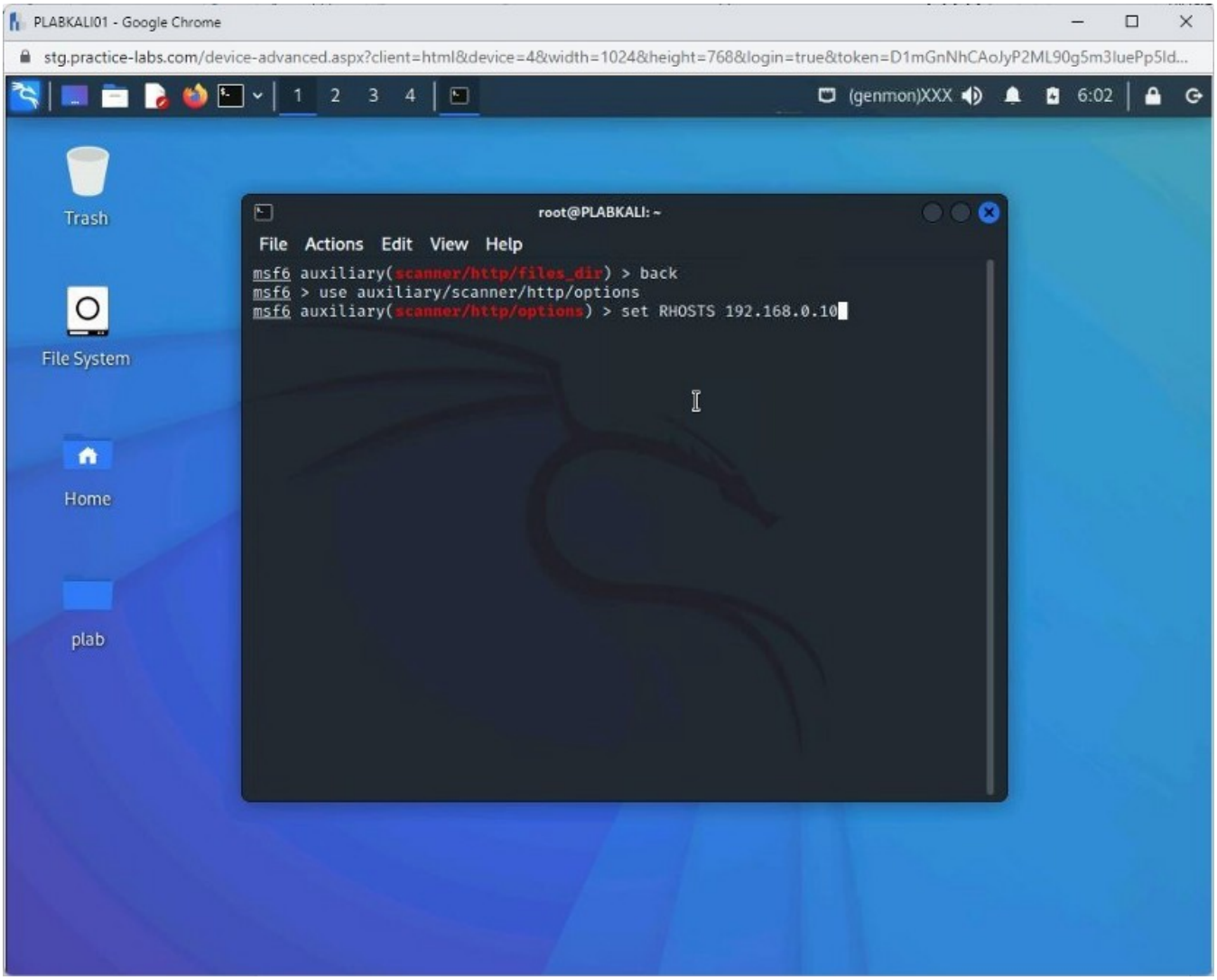



### Step 3

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

```
set RHOSTS 192.168.0.10
```

Press **Enter**.

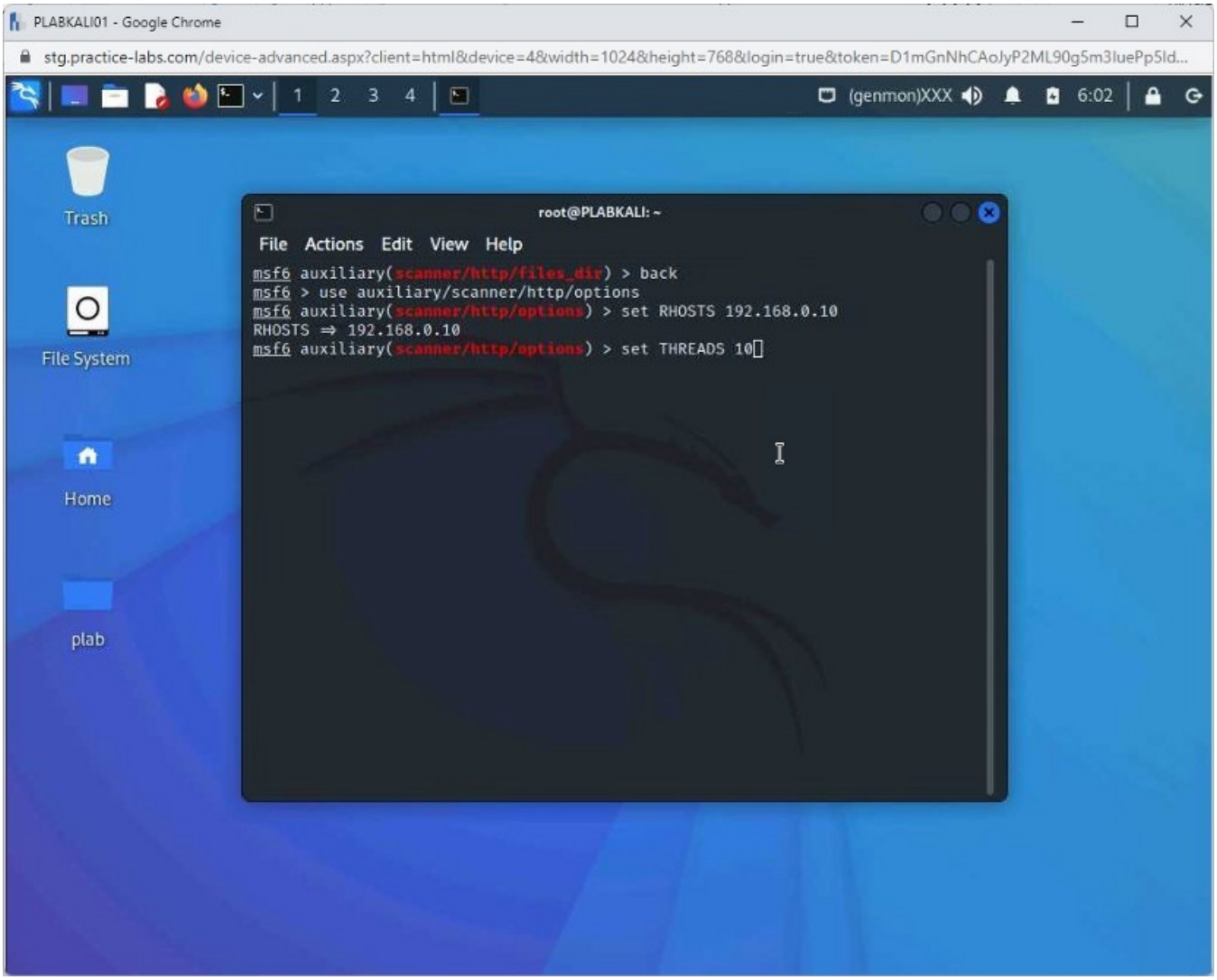



**Step 4**

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

```
set THREADS 10
```

Press **Enter**.

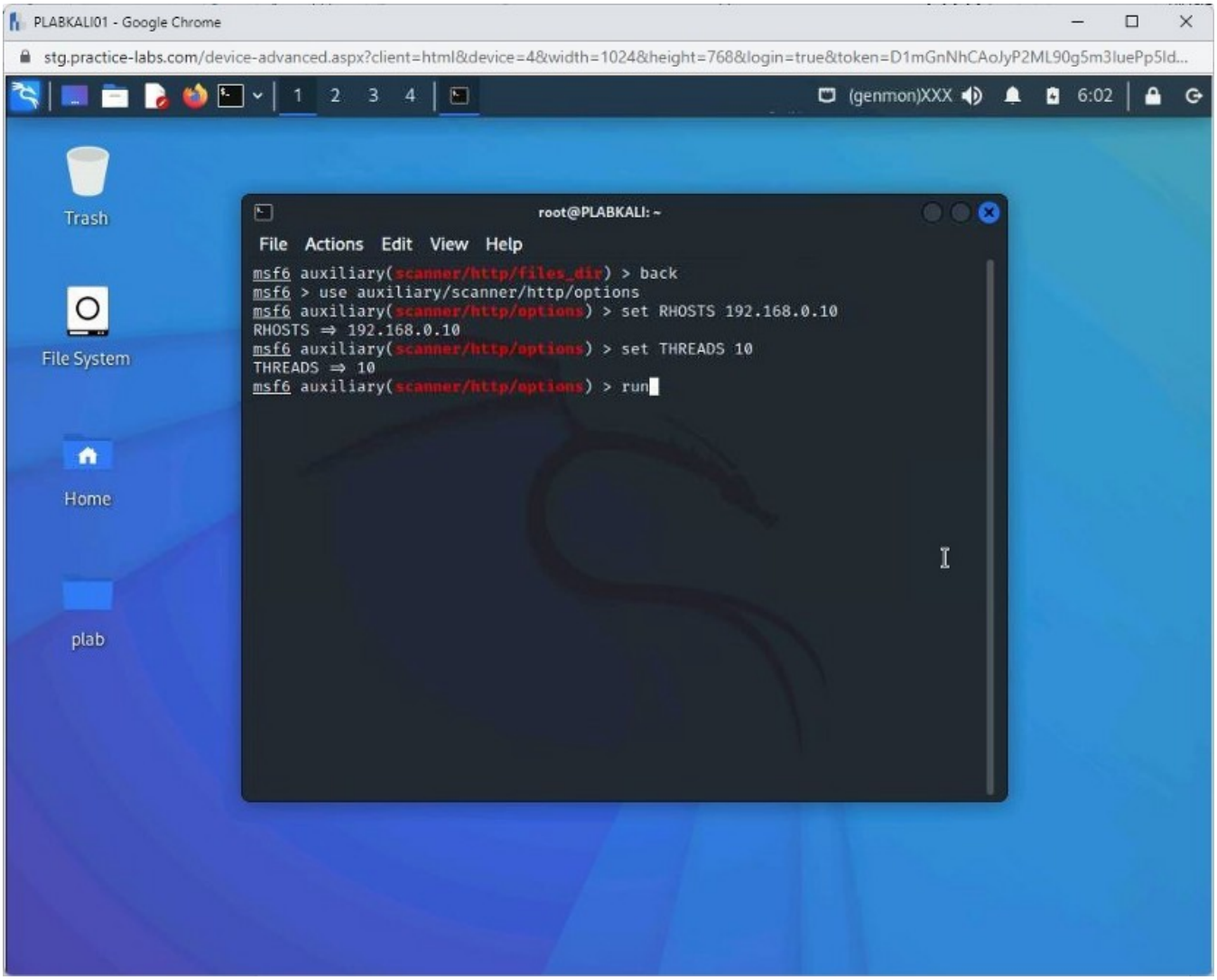



**Step 5**

Now, type the following command to execute the payload:

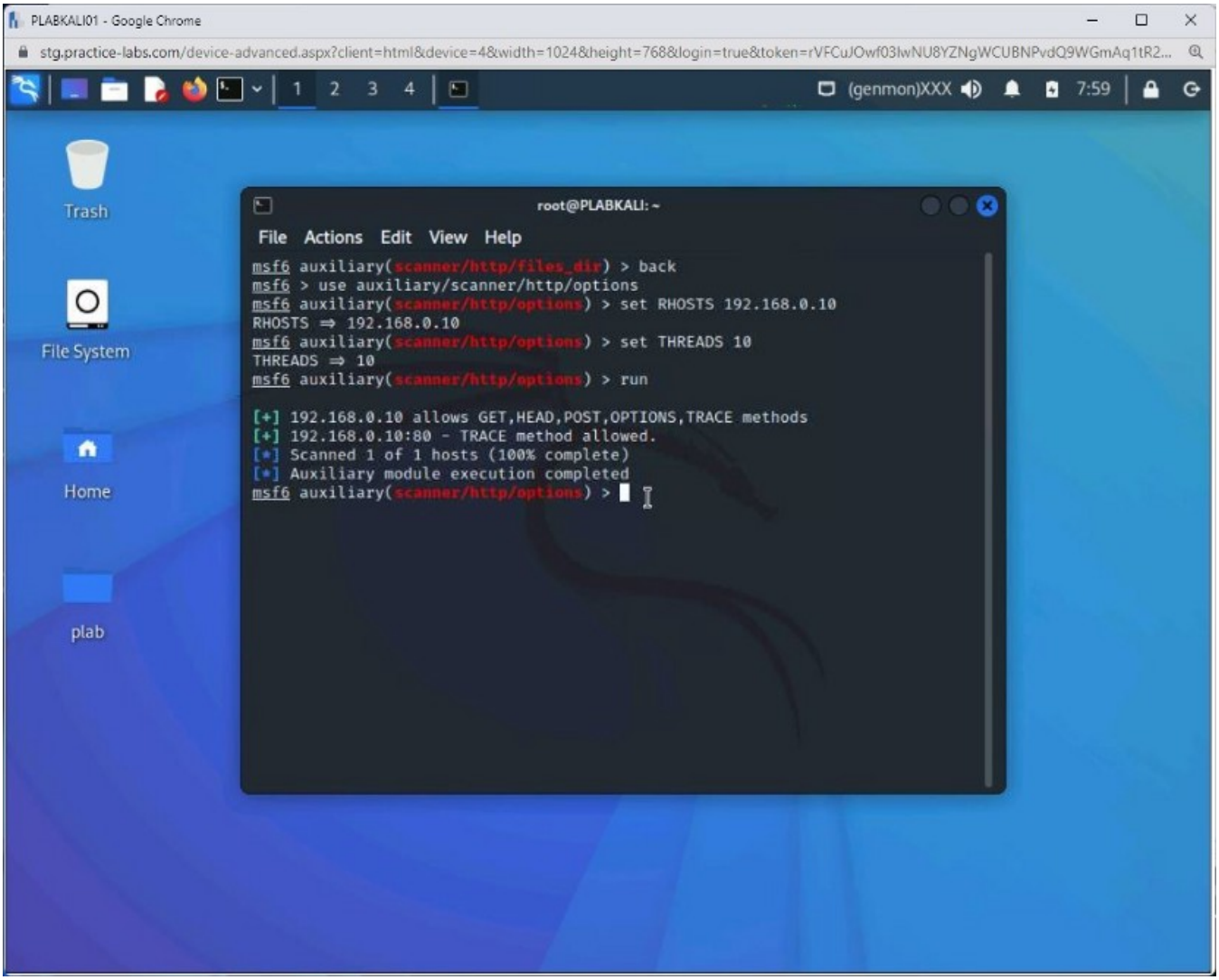
```
run
```

Press **Enter**.




**Step 6**

Notice that the output lists the options configured on the web server.




Keep the terminal window open.

## Task 6 — Check for WebDAV on a Web server using Metasploit Framework

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

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

### Step 1

Reconnect to **PLABKALI01**. Ensure that you are on the metasploit framework terminal.

Clear the screen by entering the following command:

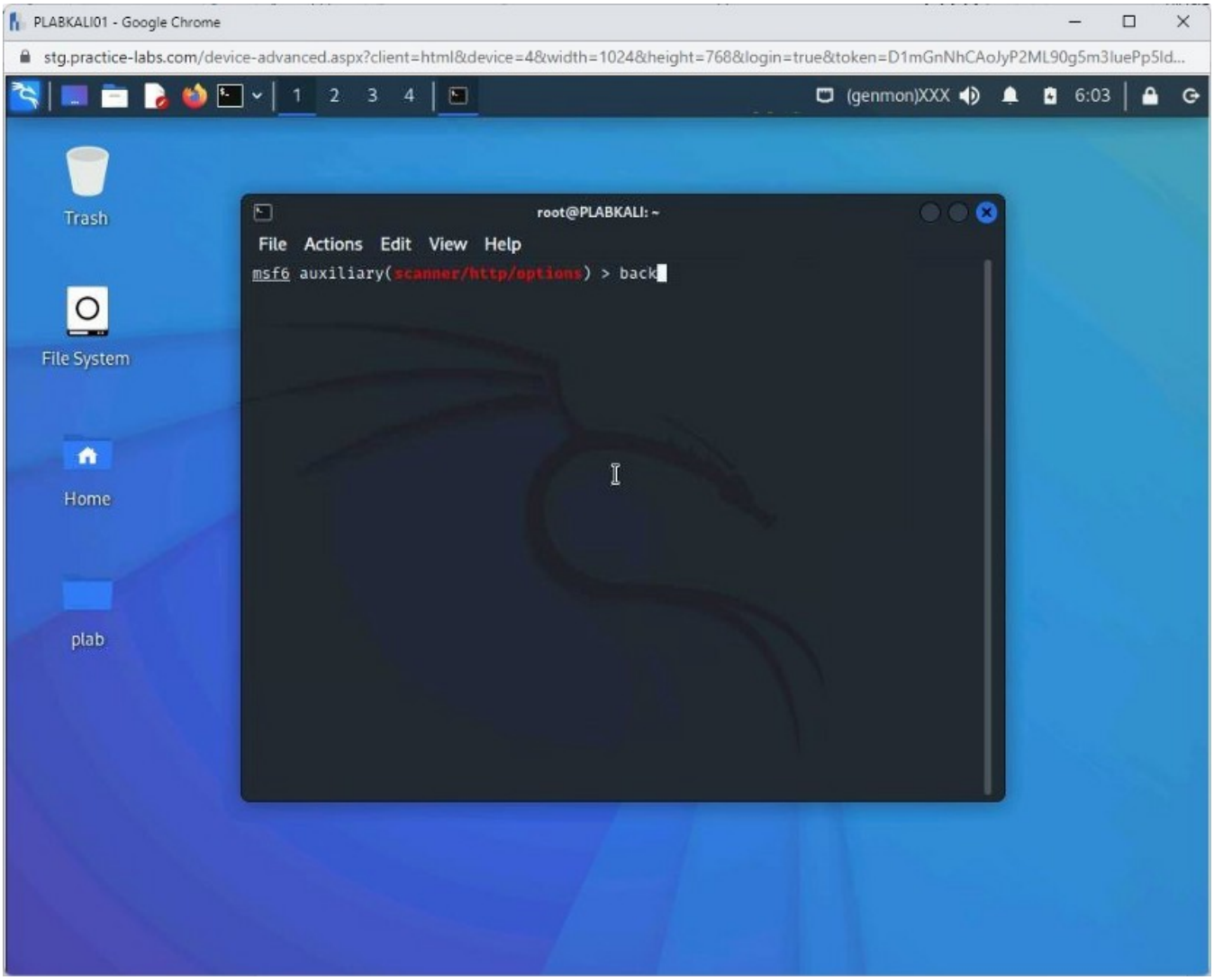
```
clear
```

Press **Enter**.

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

```
back
```

Press **Enter**.

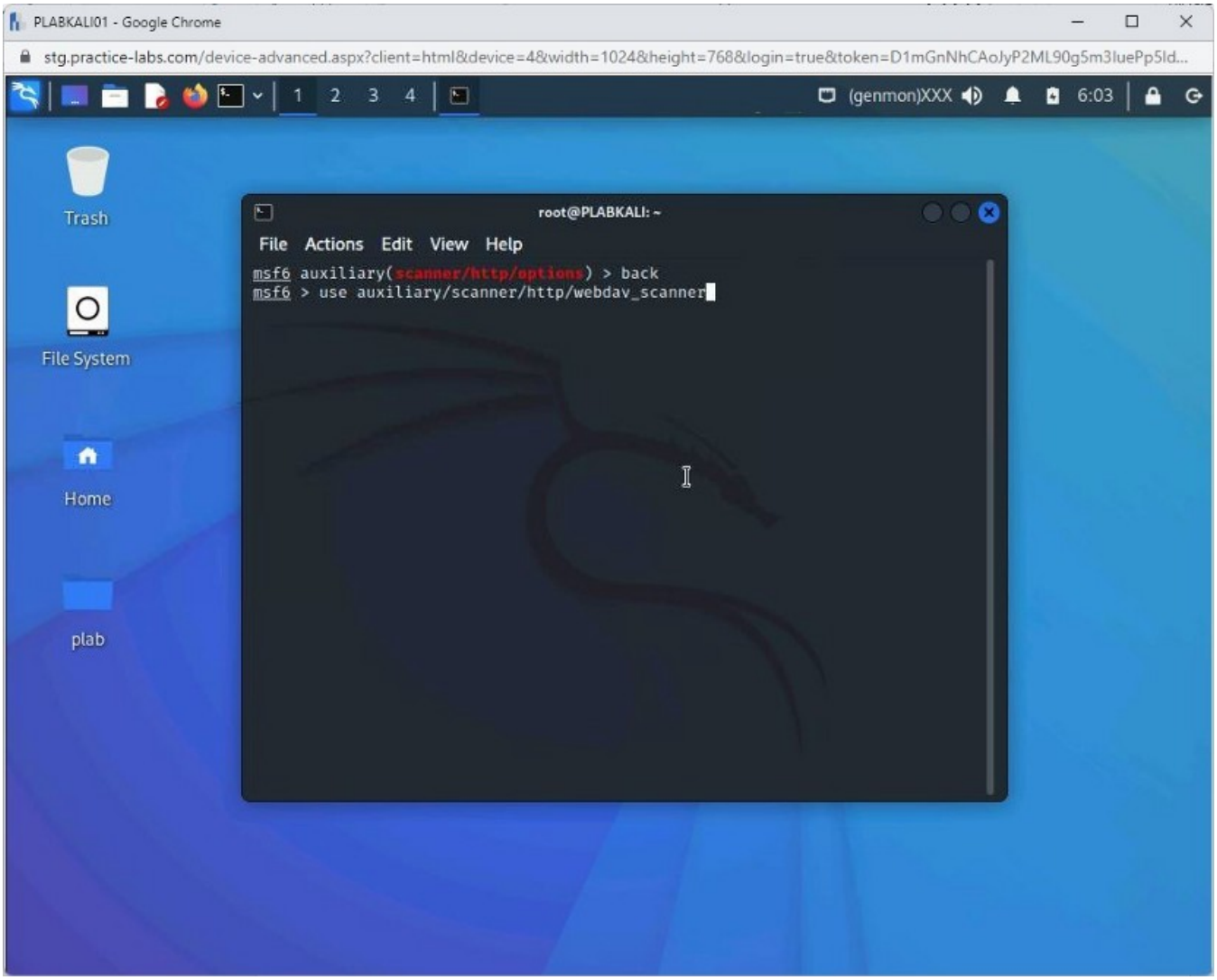



### Step 2

You are back on the Metasploit Framework prompt.

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

Press **Enter**.

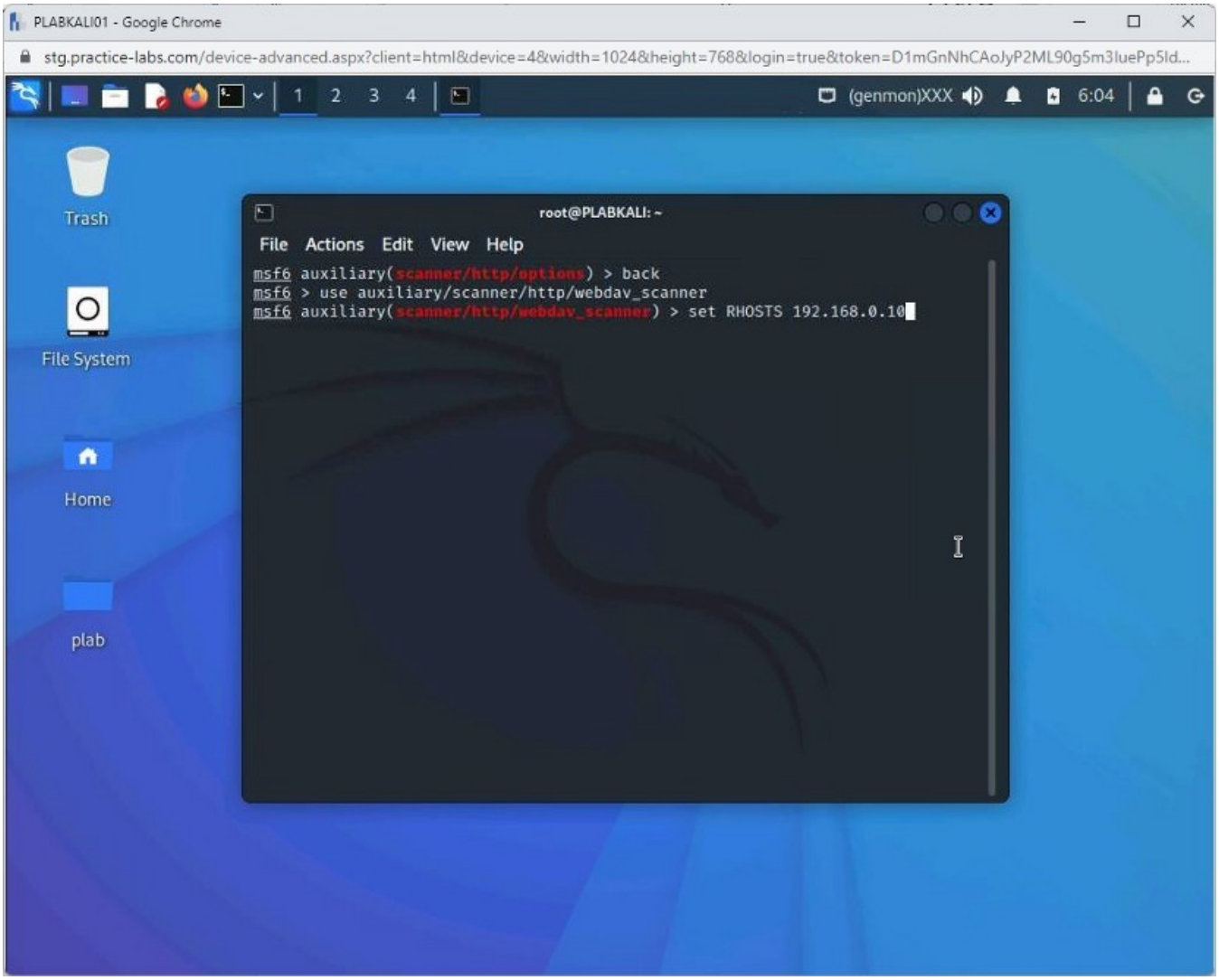



### Step 3

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

```
set RHOSTS 192.168.0.10
```

Press **Enter**.

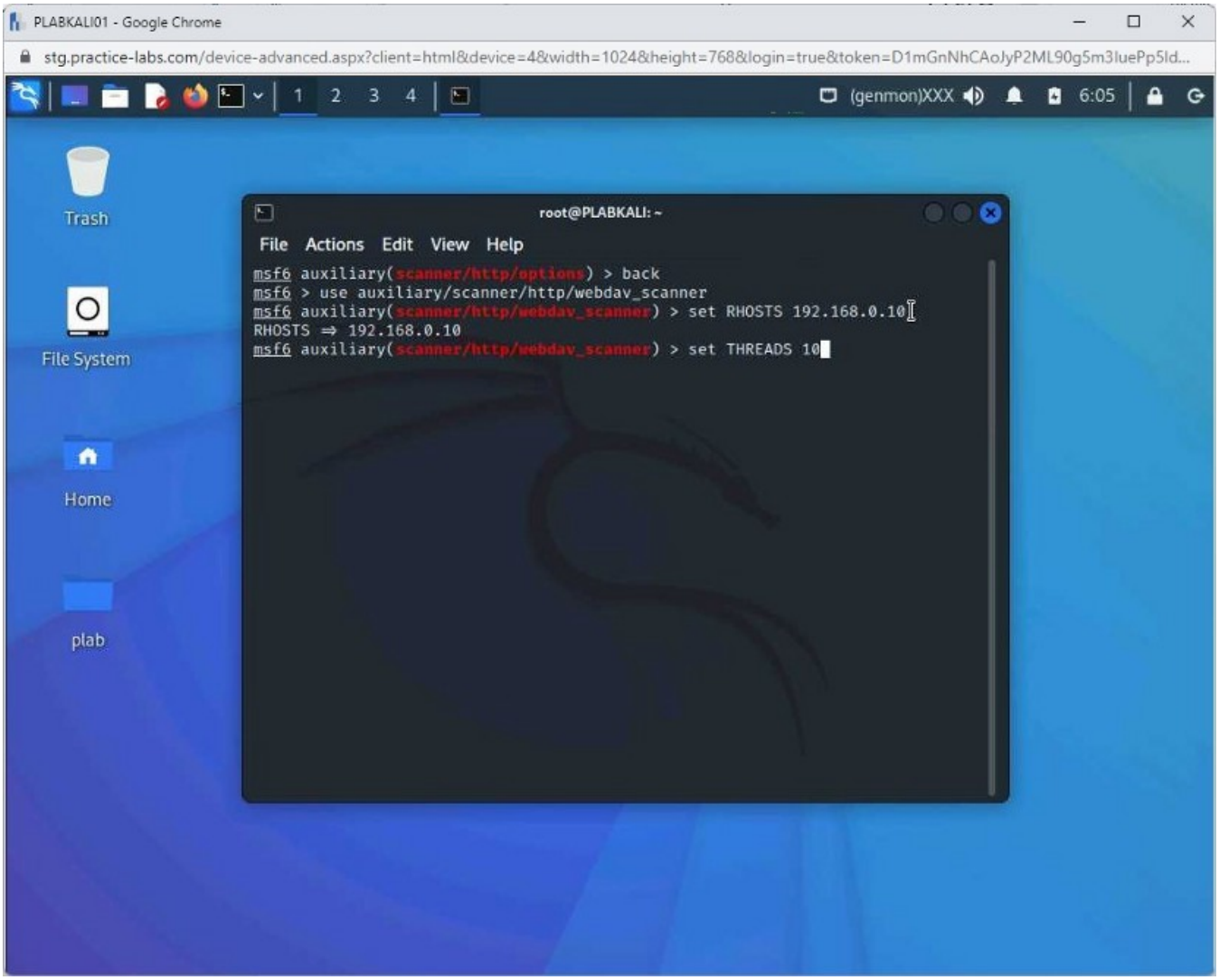



### Step 4

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

```
set THREADS 10
```

Press **Enter**.

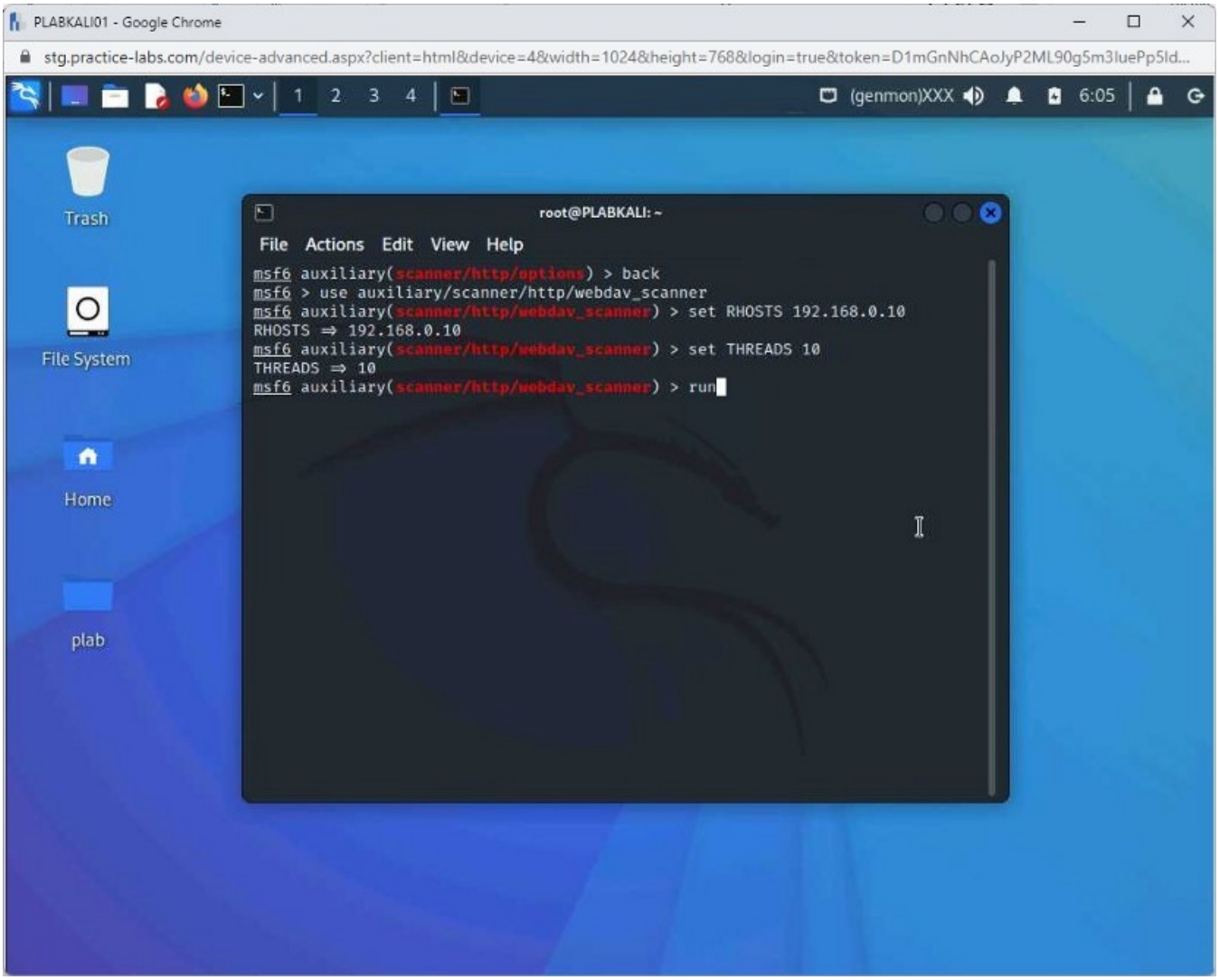



### Step 5

Now, type the following command to execute the payload:

```
run
```

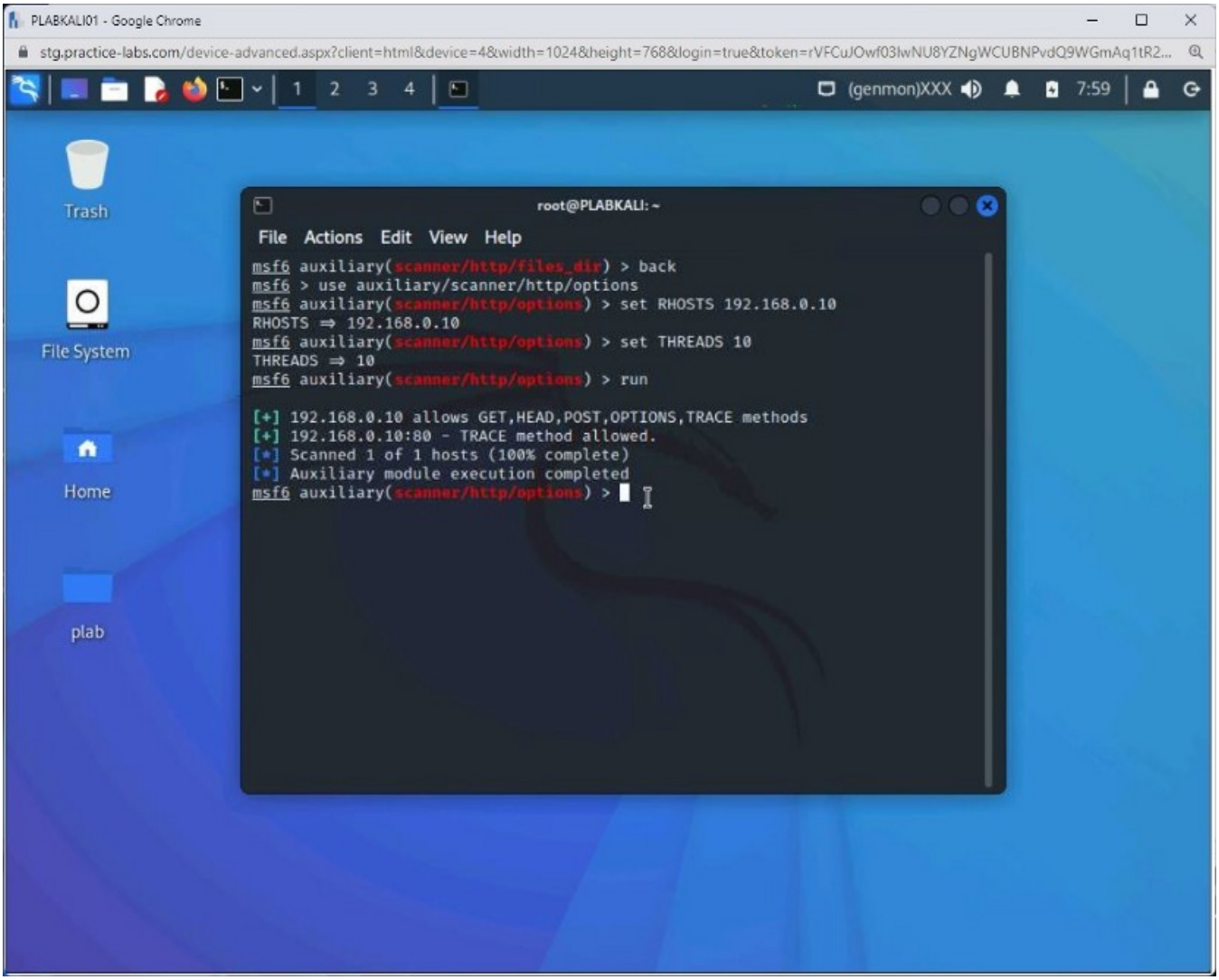
Press **Enter**.




**Step 6**

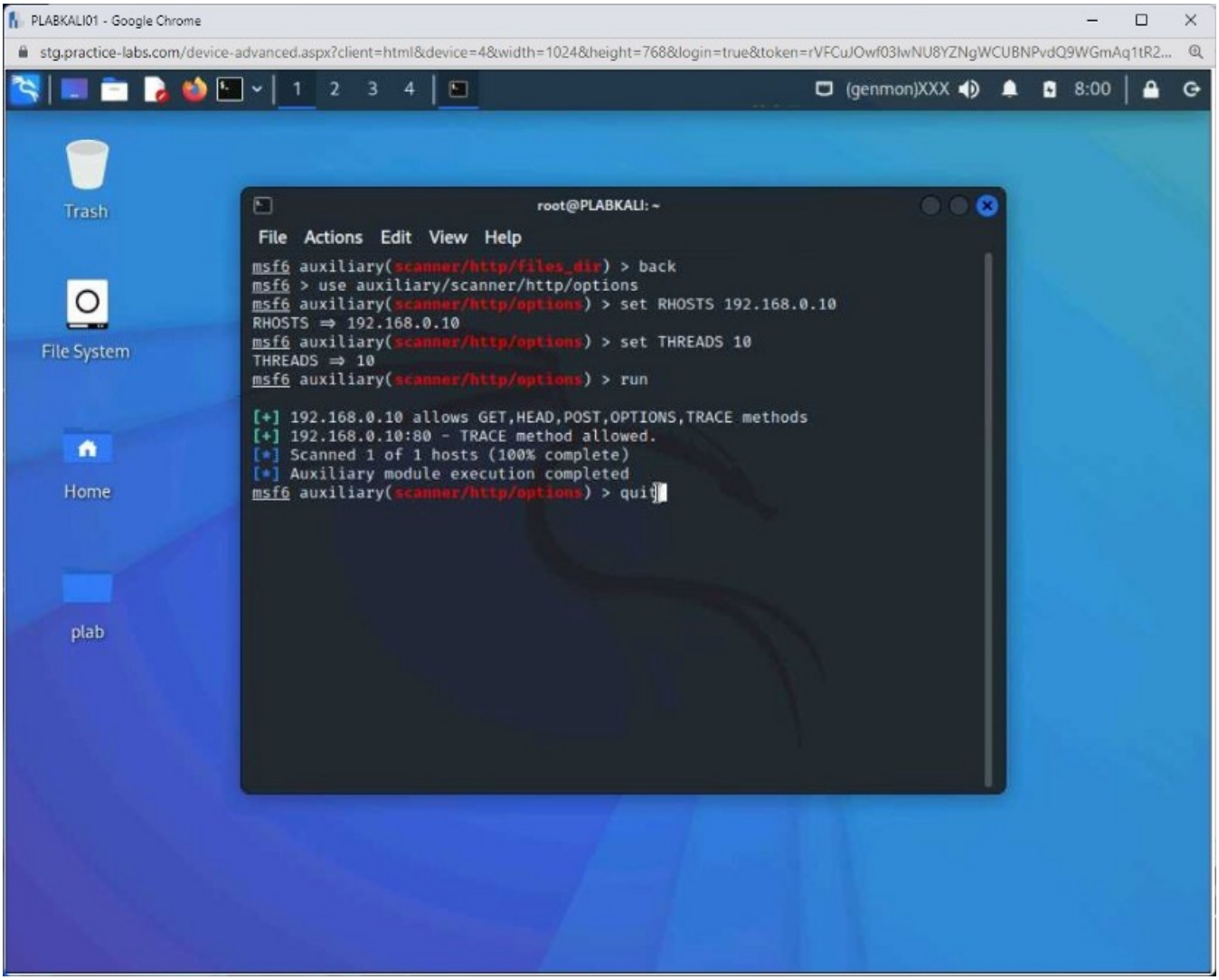
Notice the output.

It states that **WebDAV** is disabled.



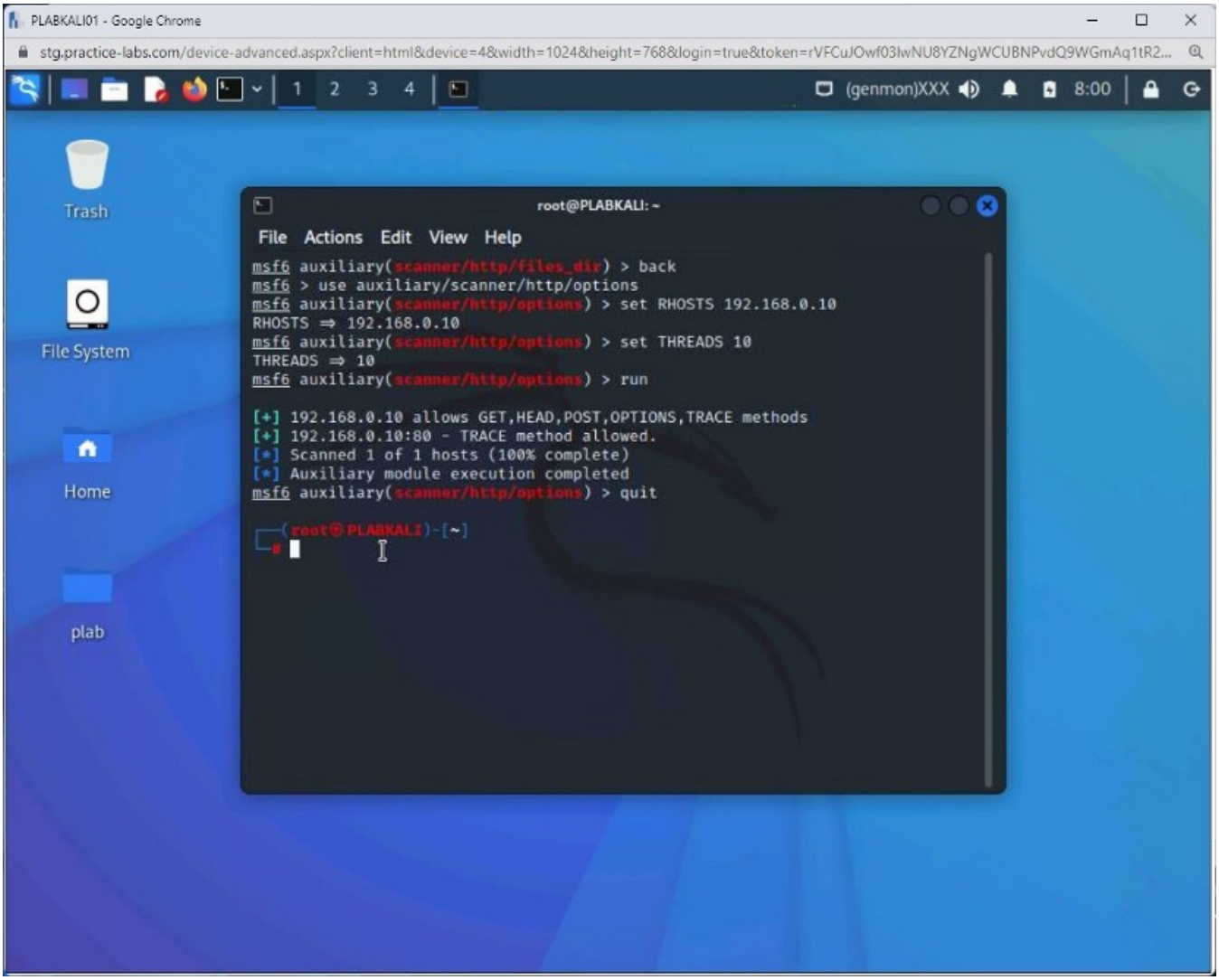

### Step 7

Type the **quit** command to exit from **Msfconsole**.




### Step 8

You are back on the terminal window.




## Task 7 — Create a Website Copy Using HTTrack Website Copier

HTTrack Website Copier is a tool that can make a replica or mirroring copy of a website on your local system. It downloads all resources from a target website, including images and HTML pages and creates the exact directory structure on your local system.

You can also specify the number of levels within the website navigation. For example, if there is a hierarchical structure within the website, these are considered levels.

In this task, you will learn to create a website copy using HTTrack Website Copier.

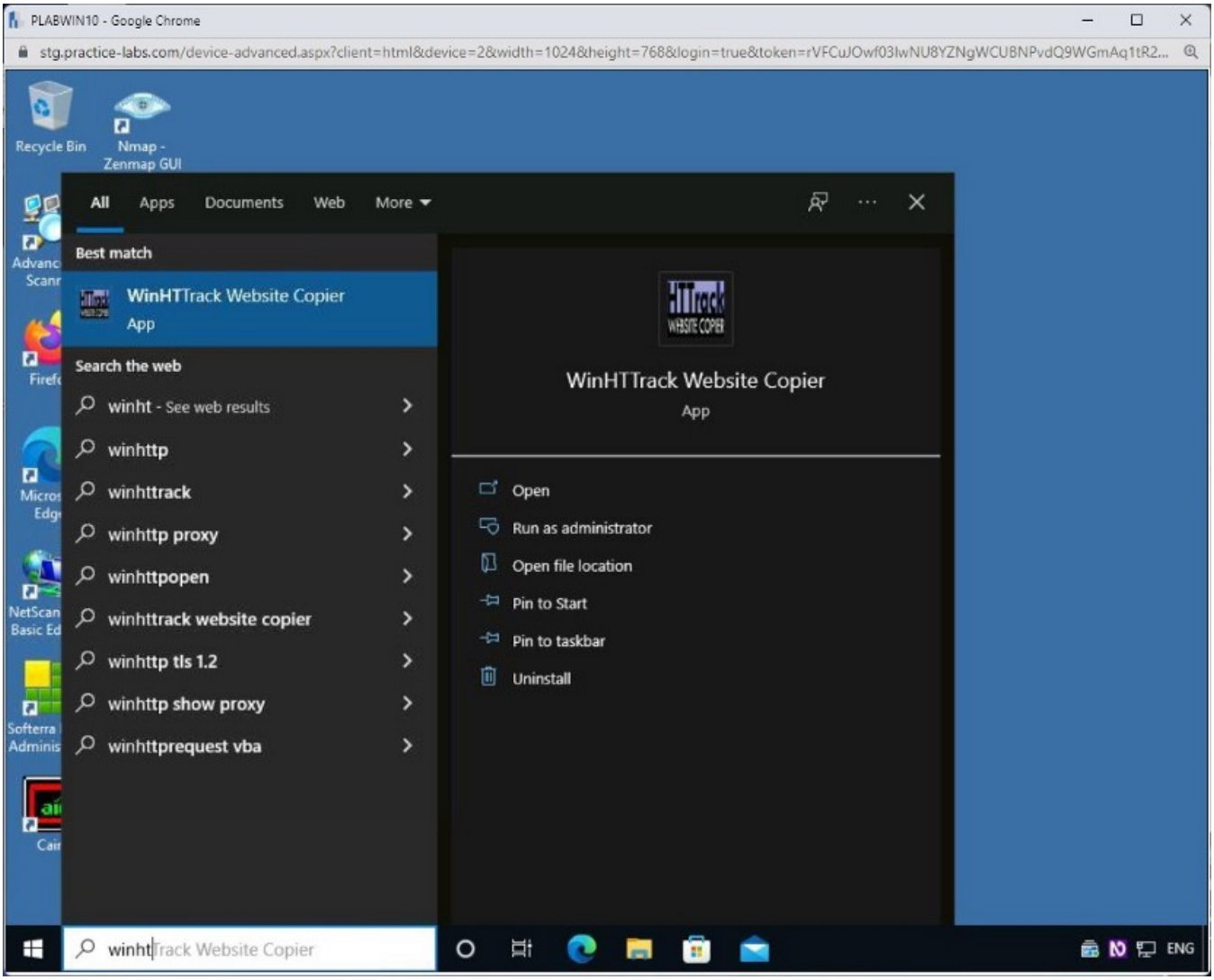
### Step 1

Connect to **PLABWIN10**.

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

```
winht
```

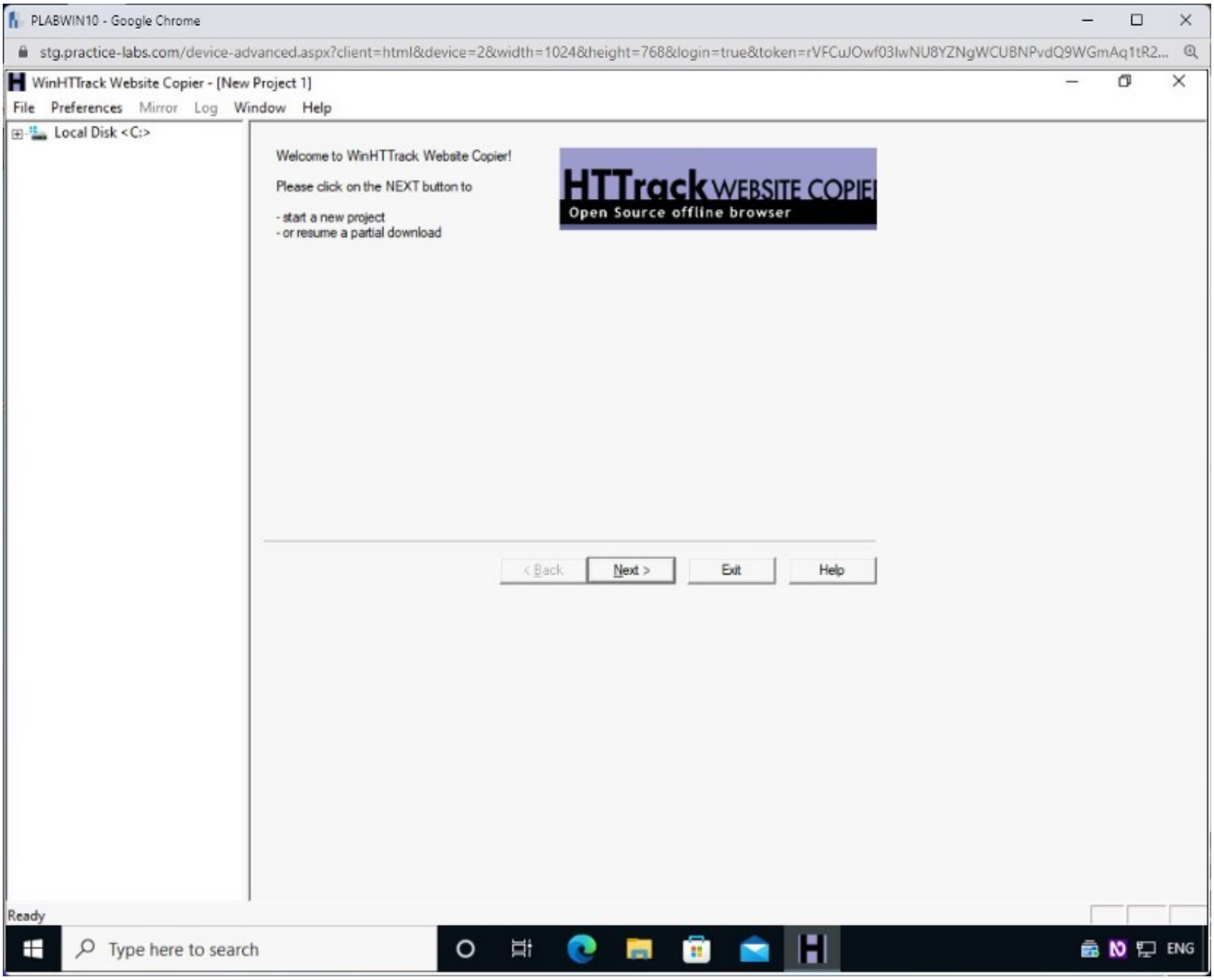
From the search results, select **WinHTTrack Website Copier**.




### Step 2

On the **Welcome** page in the right pane, click **Next**.

***Note:*** *You may be prompted to choose the language. Keep the default language as* ***English****.*

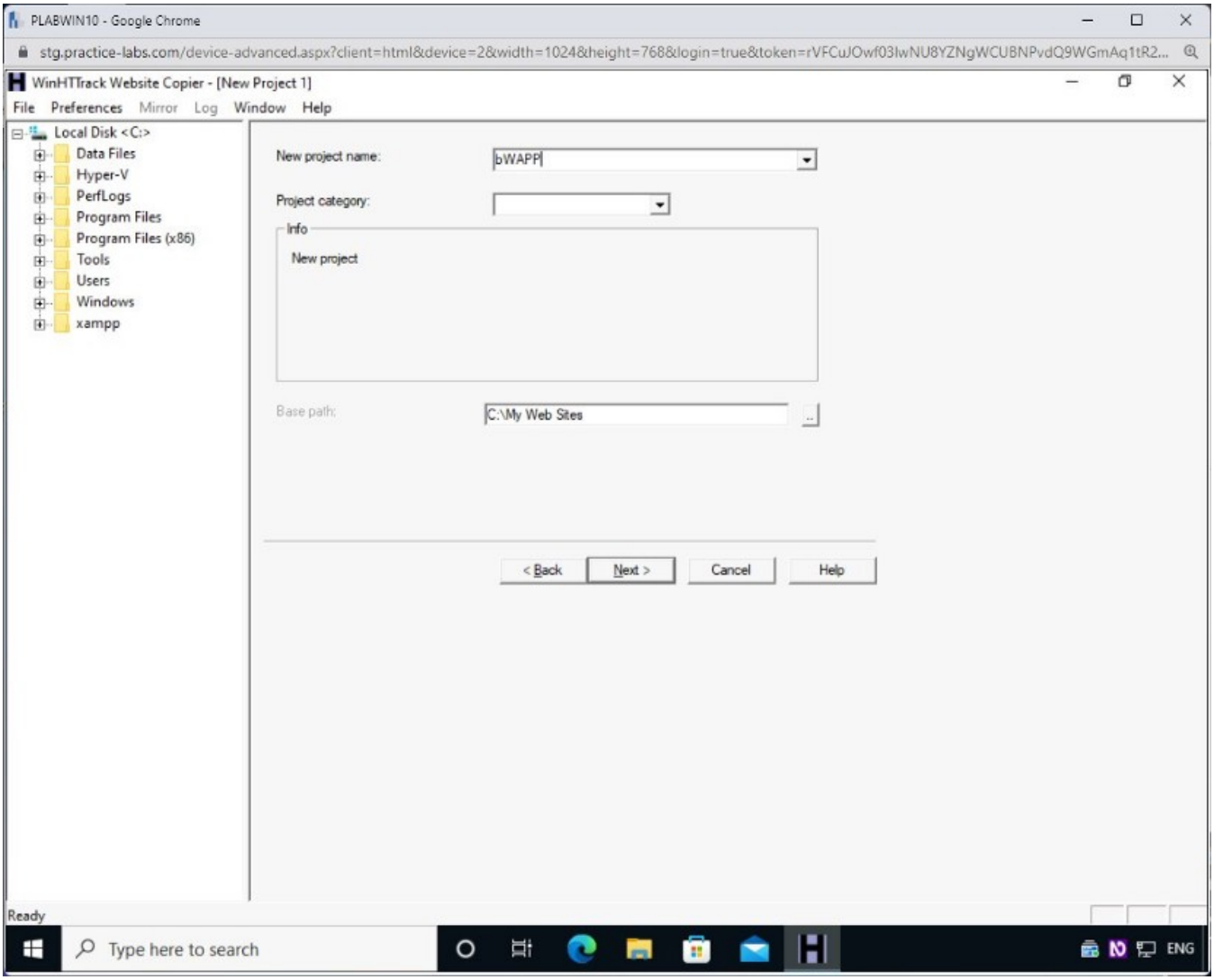



**Step 3**

In the **New project name** drop-down, type the following name:

```
bWAPP
```

Click **Next**.

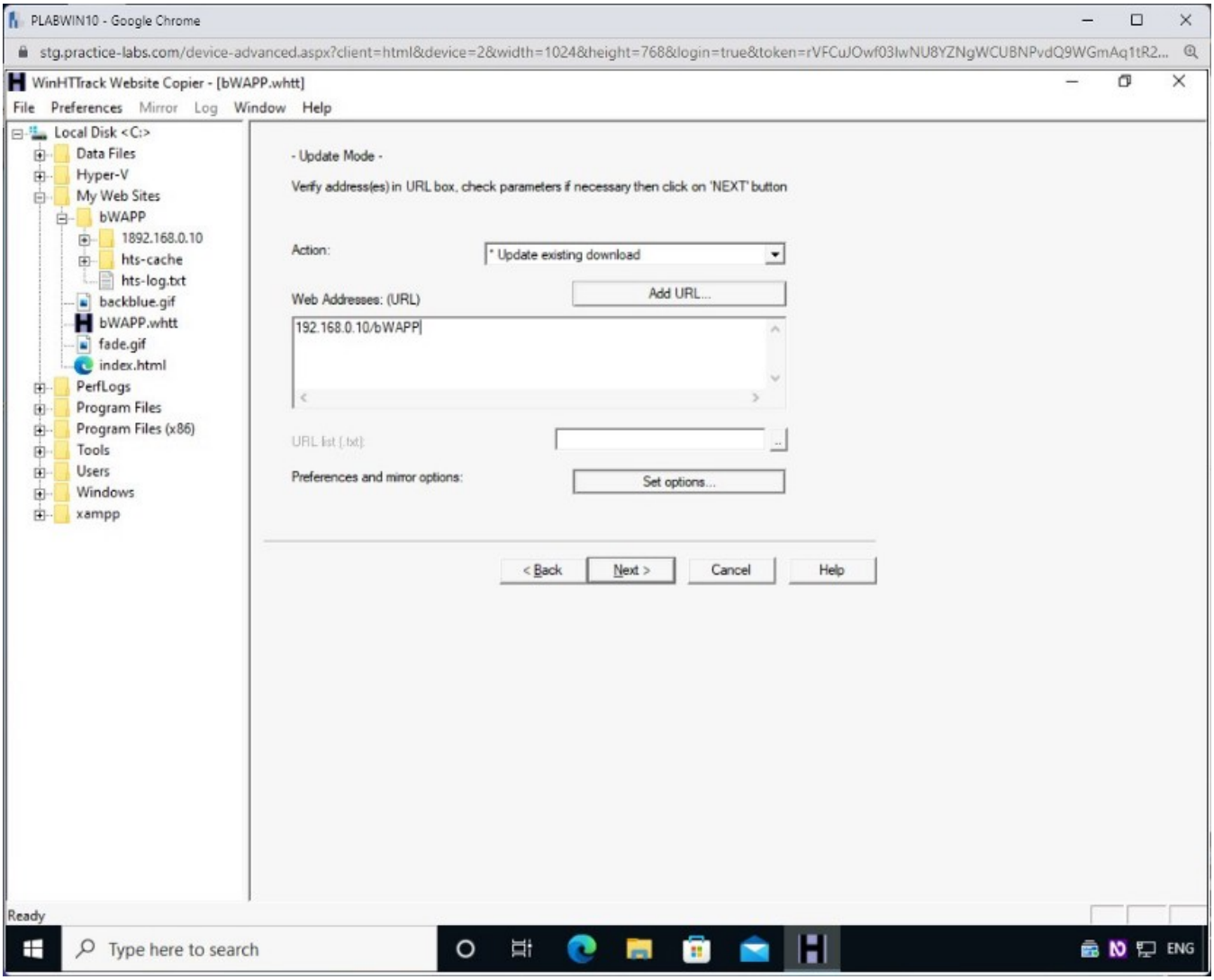



**Step 4**

In the **Web Addresses (URL)** text box, type the following URL:

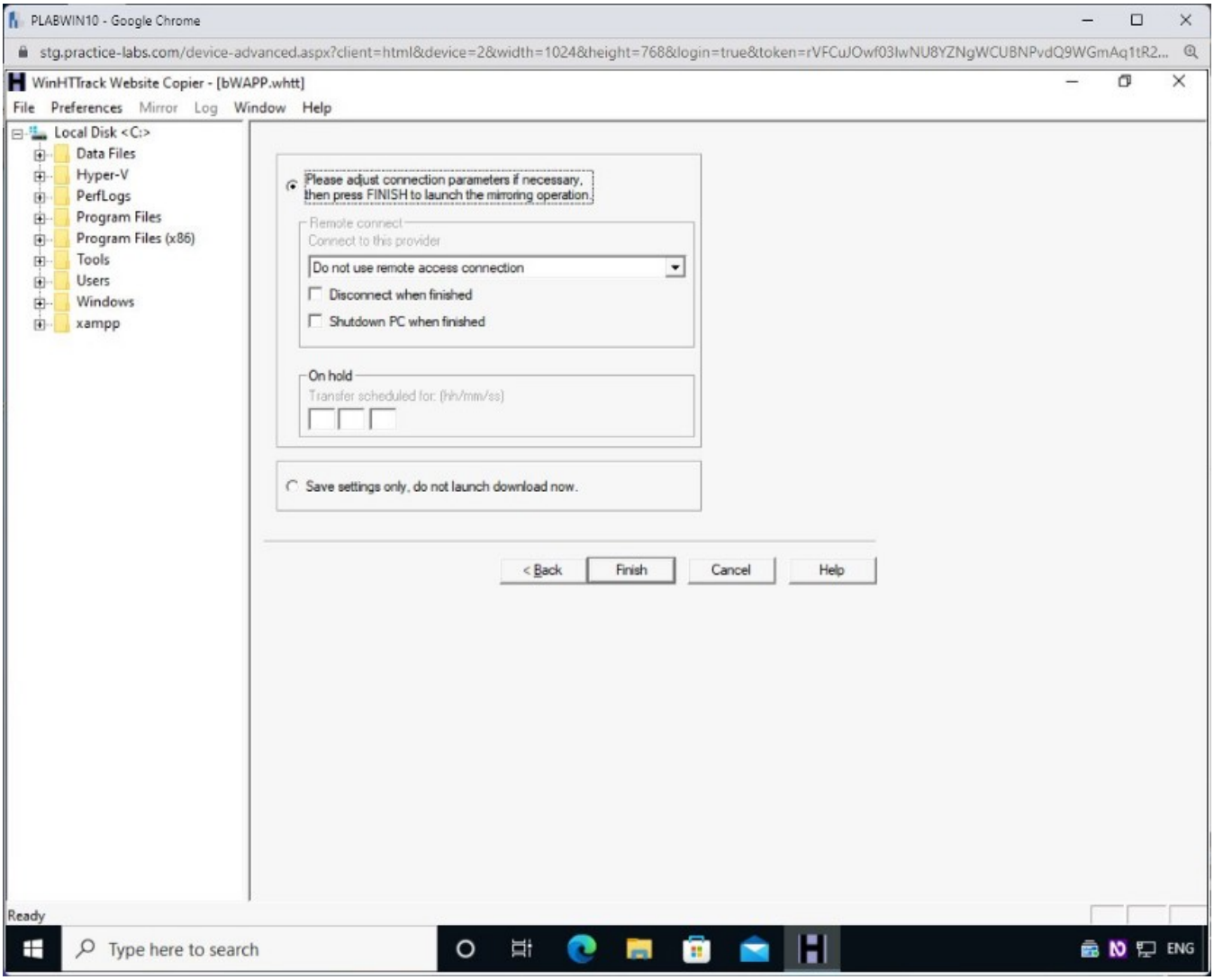
```
192.168.0.10/bWAPP
```

Click **Next**.




### Step 5

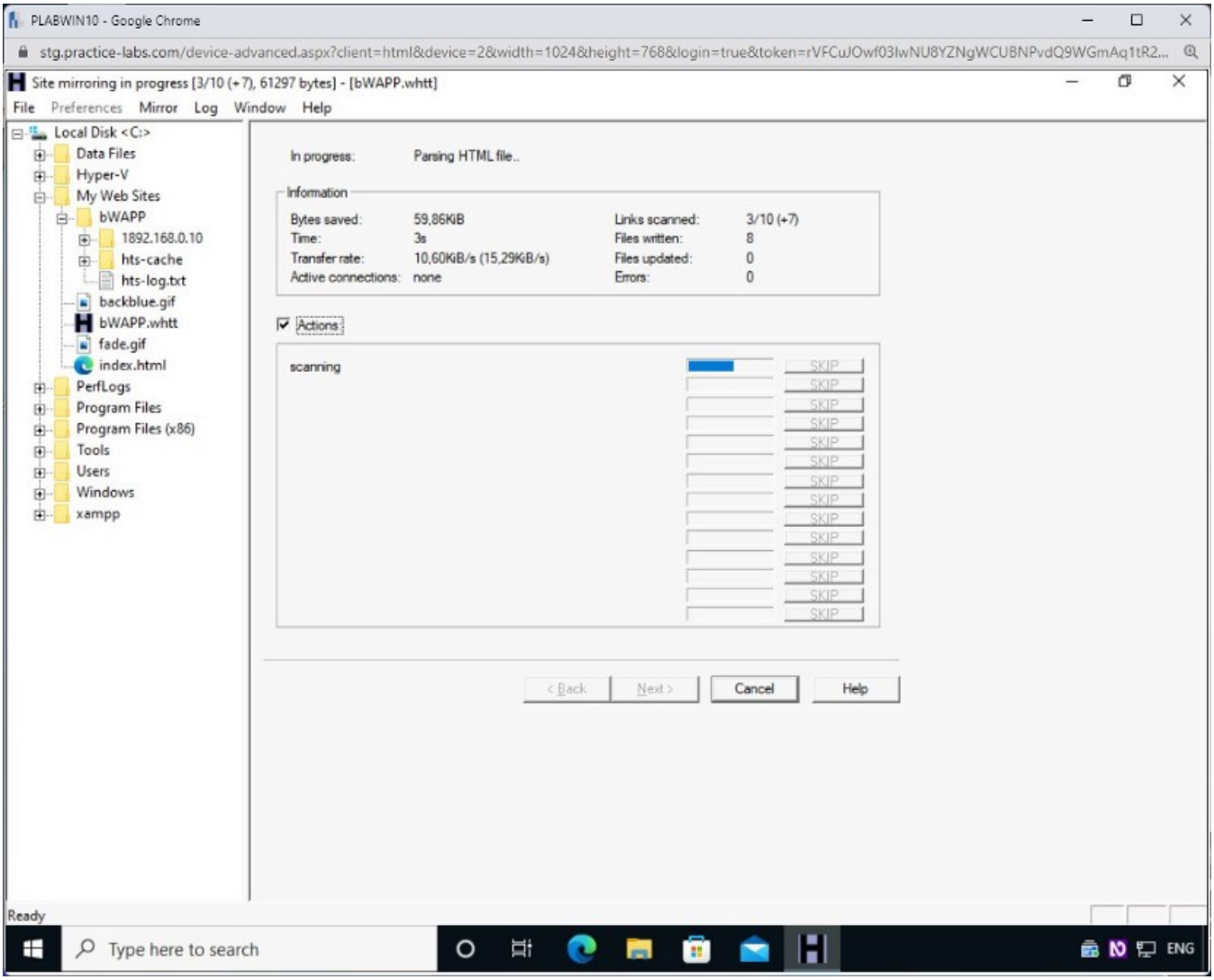
On the next page, click **Finish**.




**Step 6**

The website mirroring starts.

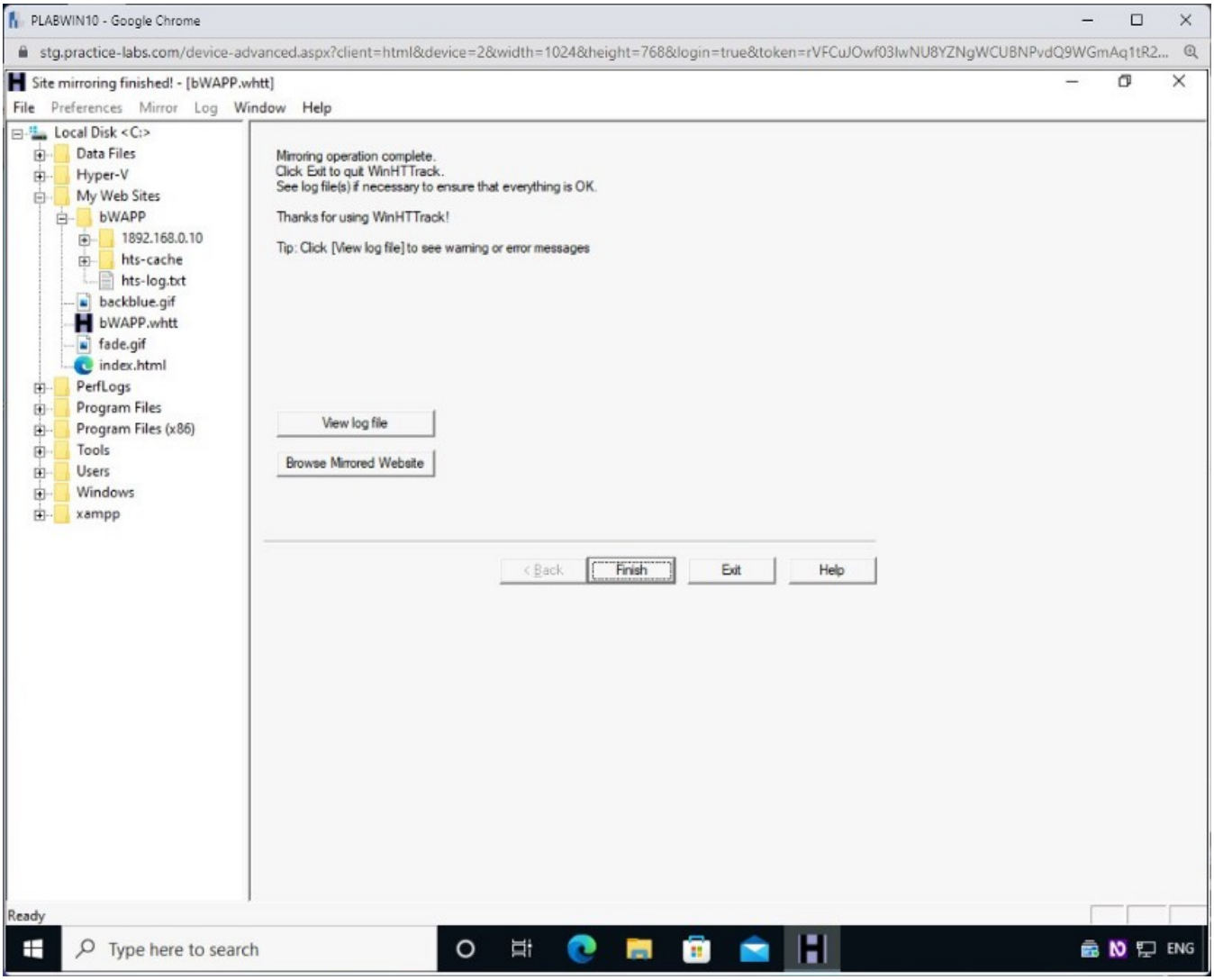
may take a few minutes, depending on the website's size.




**Step 7**

The website mirroring process is now completed.

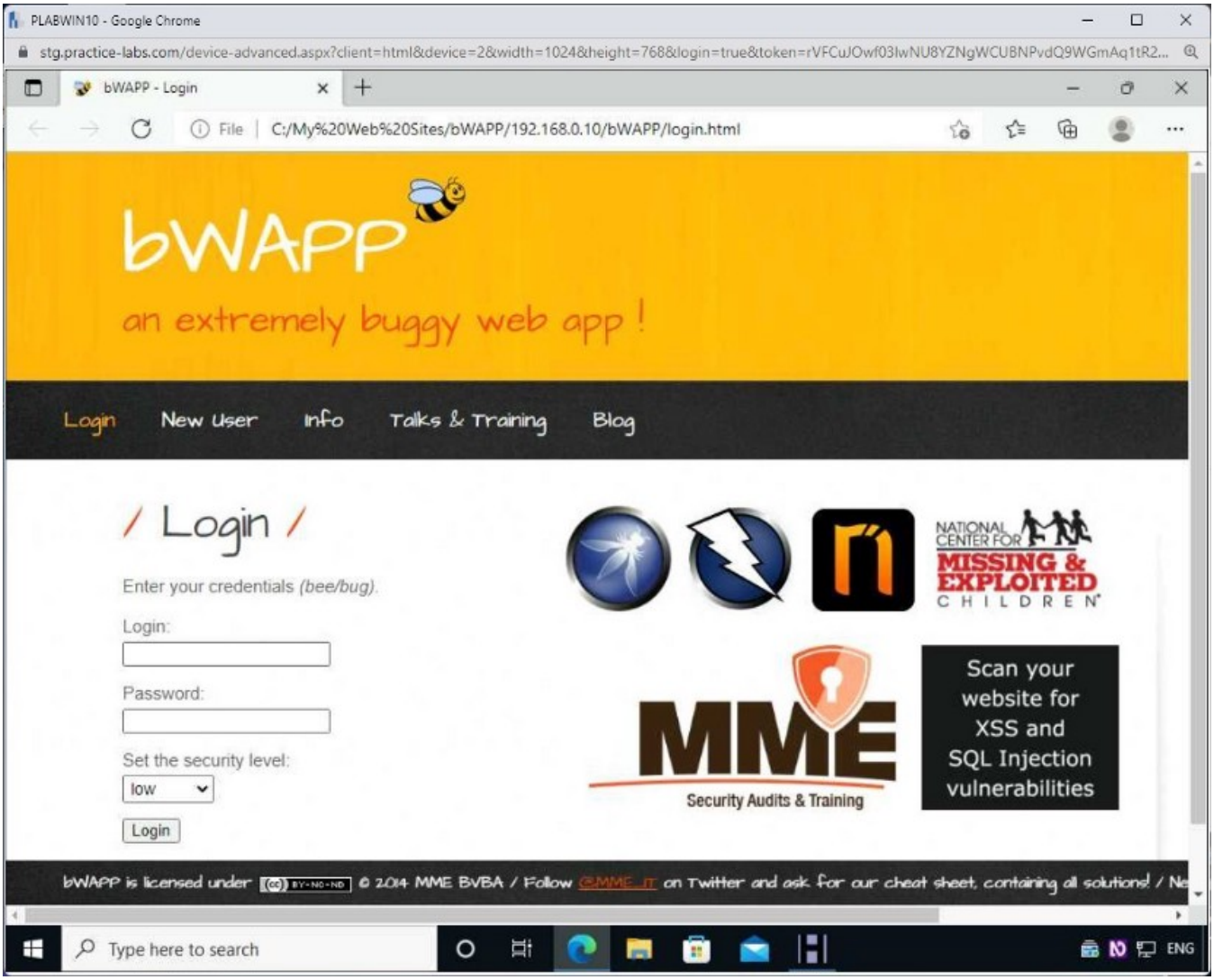
Click **Browse Mirrored Website**.




**Step 8**

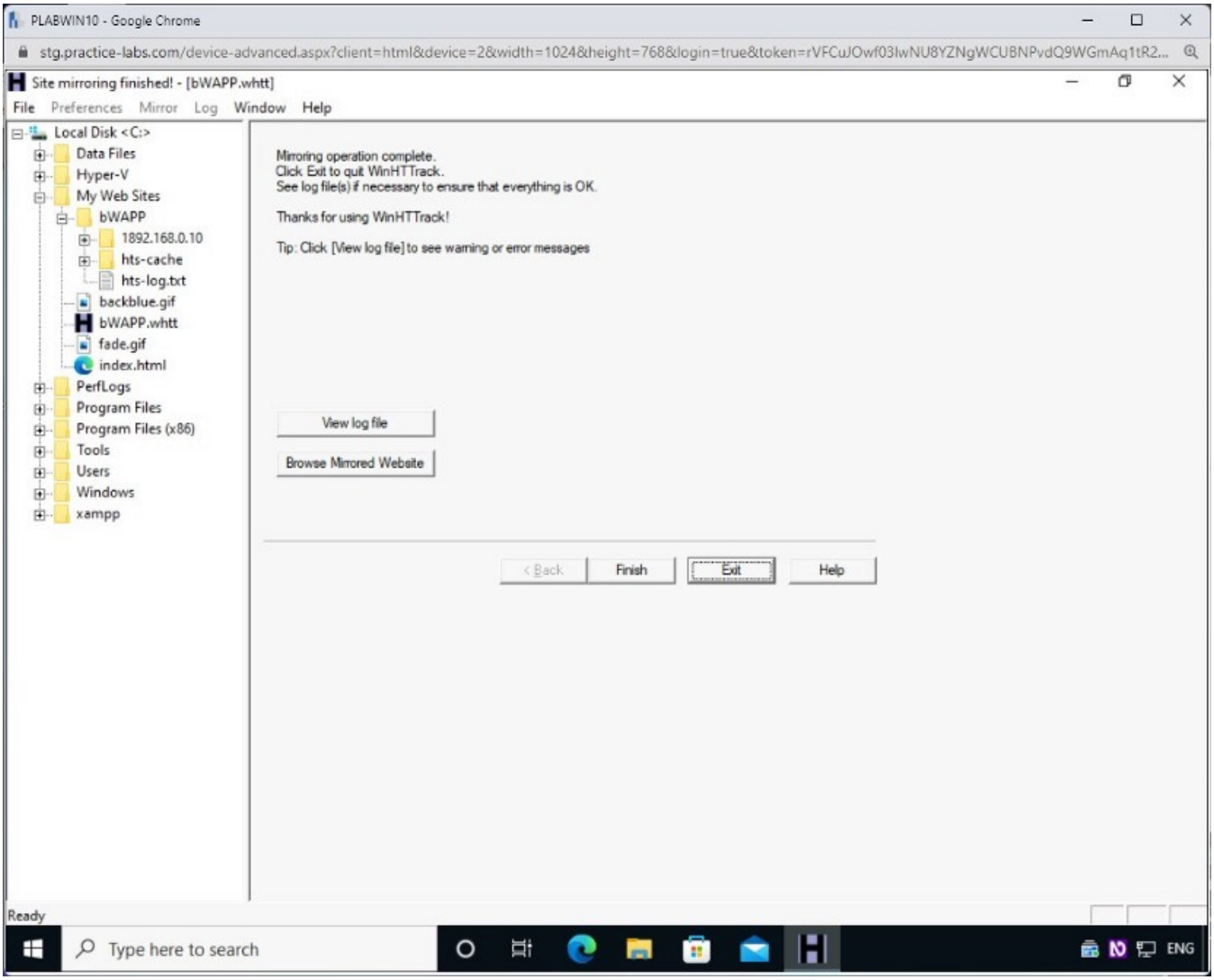
Notice that in the browser window, the login page of the mirrored website is displayed.

Close the **Microsoft Edge** window.



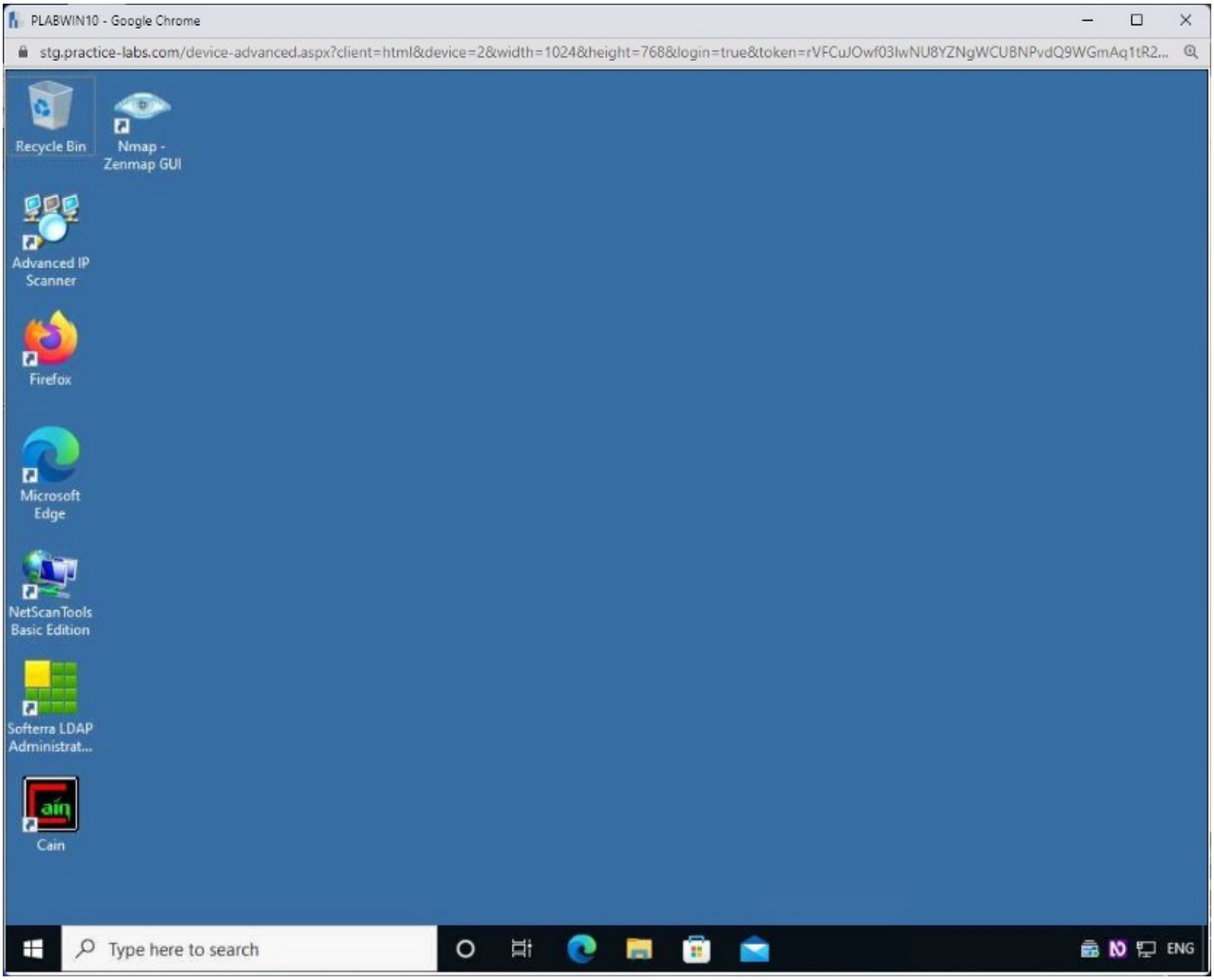

**Step 9**

Click **Exit** to close **HTTrack**.




**Step 10**

You are back on the **PLABWIN10** desktop.




## Task 8 — Perform Vulnerability Scanning Using Nikto

Nikto is an open-source web server vulnerability scanning tool. It can scan for vulnerabilities, such as outdated server components, headers, authorization guessing, and class checks. It is by default installed in Kali Linux.

In this task, you will learn to perform vulnerability scanning using Nikto.

### Step 1

Reconnect to **PLABKALI01**. Ensure that the terminal window is open.

Clear the screen by entering the following command:

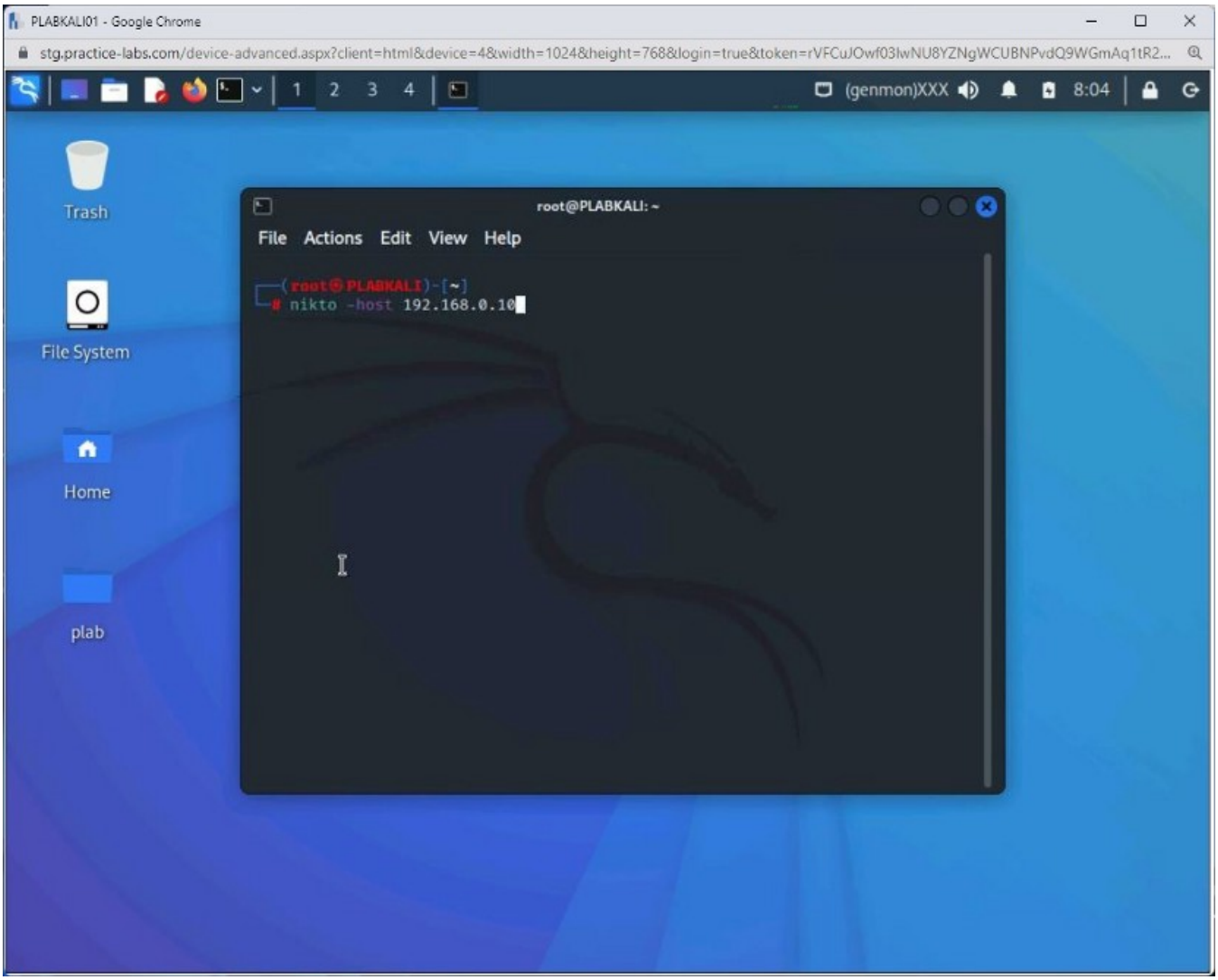
```
clear
```

Press **Enter**.

Type the following command:

```
nikto -host 192.168.0.10
```

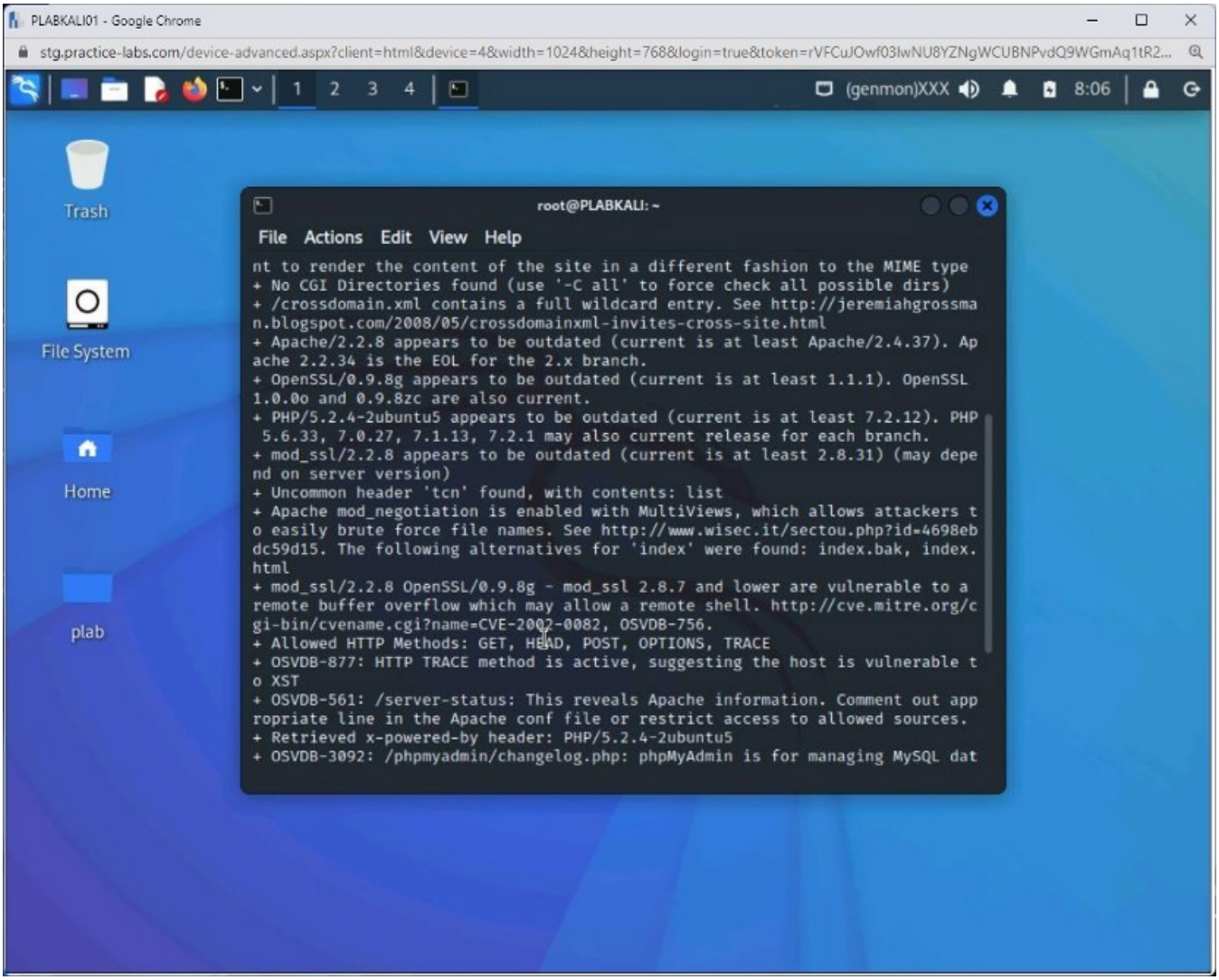
Press **Enter**. The -host parameter takes the web server name or IP address as an argument.




### Step 2

The vulnerability scanning process starts.

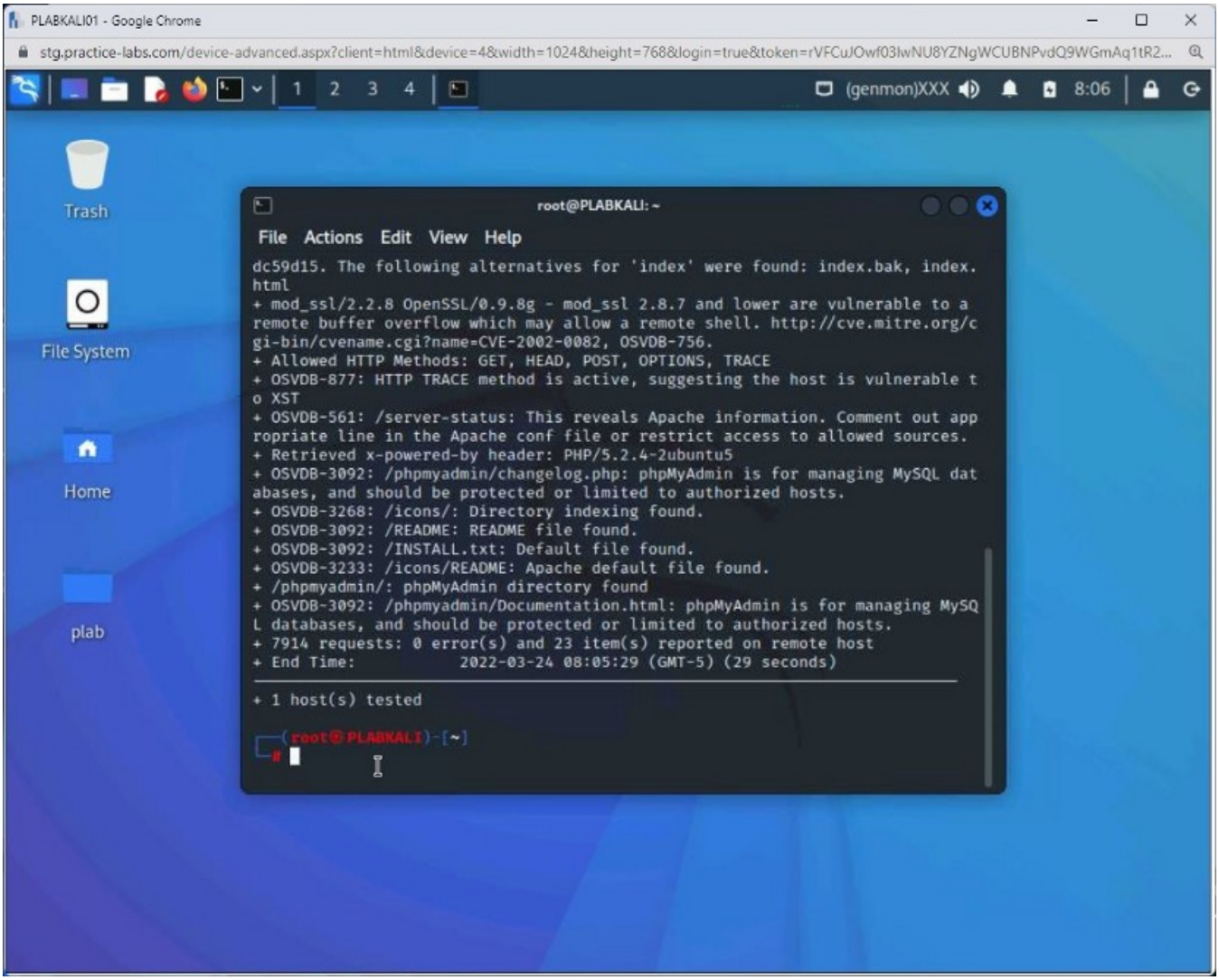
It takes a few minutes to scan the server for vulnerabilities.




**Step 3**

When the vulnerability scanning process finishes, it lists several vulnerabilities.

In the output, it provides the count of the vulnerabilities with the scan date and time.




## Task 9 — Perform Web Application Brute Forcing Using DirBuster

There are several tools or websites that you can use to traverse through a website's directory structure. When configuring a web server with a website, it is best to ensure that you have not enabled directory listing. If enabled, an attacker can exploit the server and get the listing.

In this task, you will learn to perform directory traversal using a multi-threaded tool named DirBuster, which can brute force applications to find their directory structure. To perform web application brute force using DirBuster, perform the following steps:

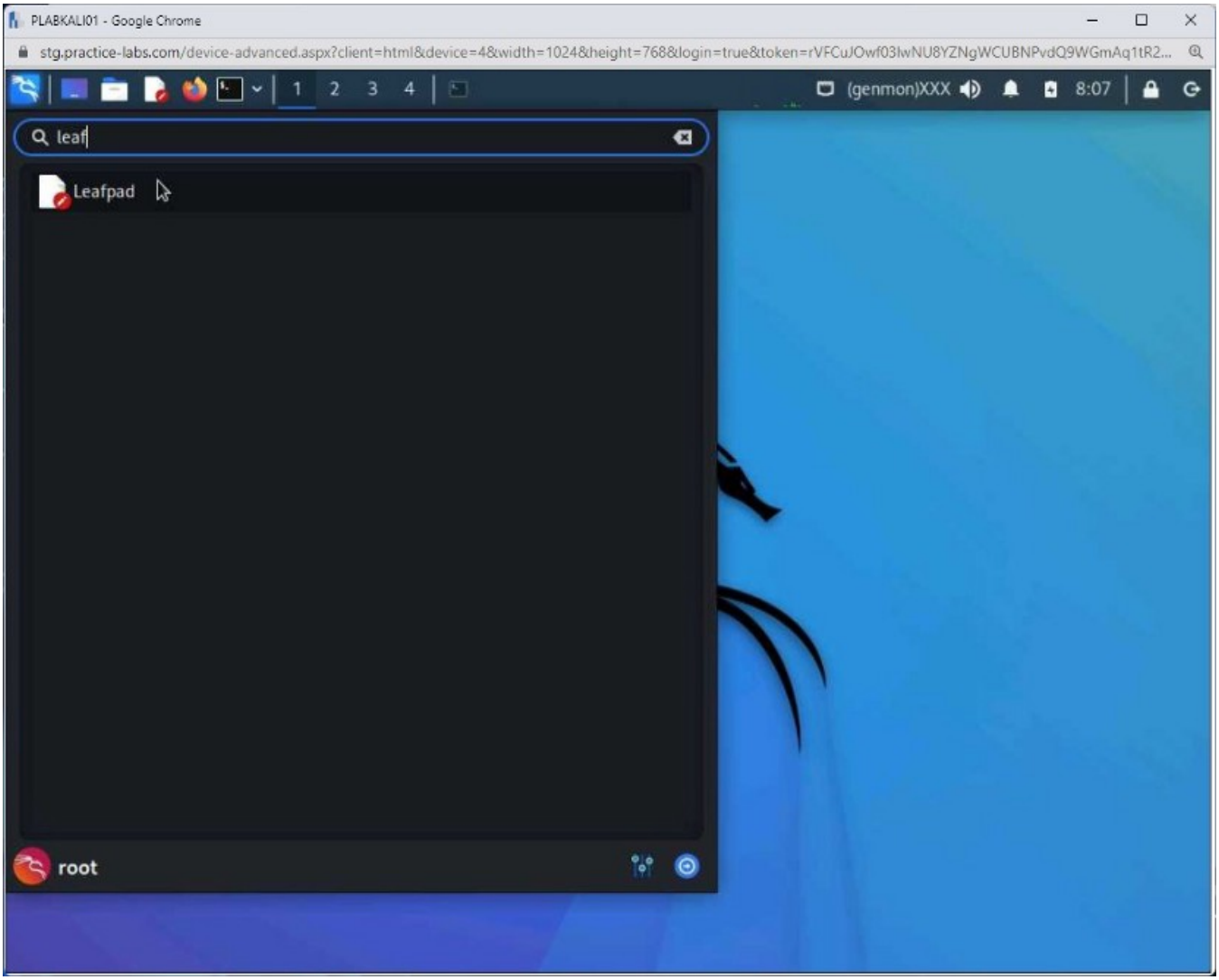
### Step 1

Connect to **PLABKALI01**. Minimize the terminal window.

Open the **Applications** menu, and in the search field type the following:

```
Leaf
```

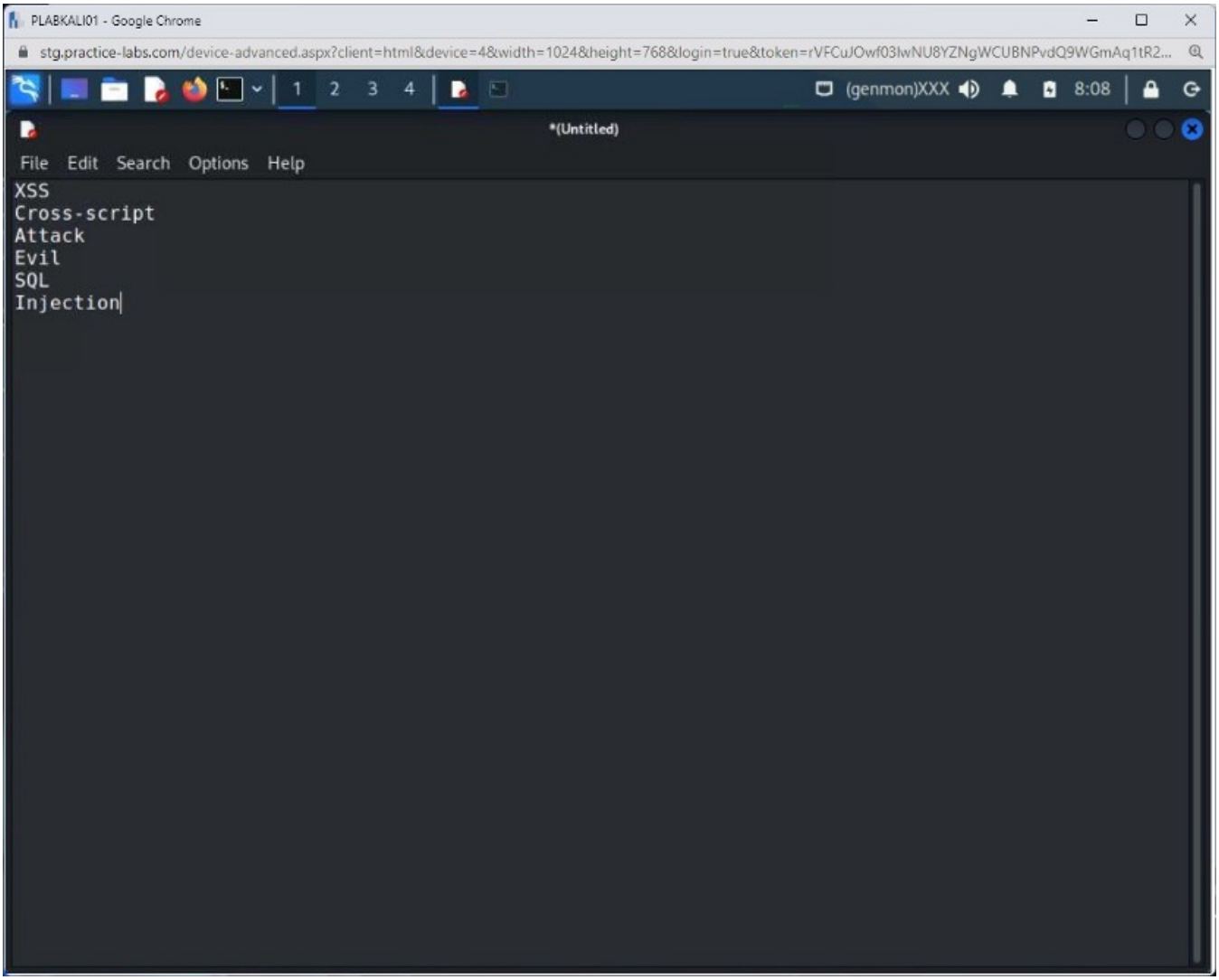
Click the **Leafpad** icon.




### Step 2

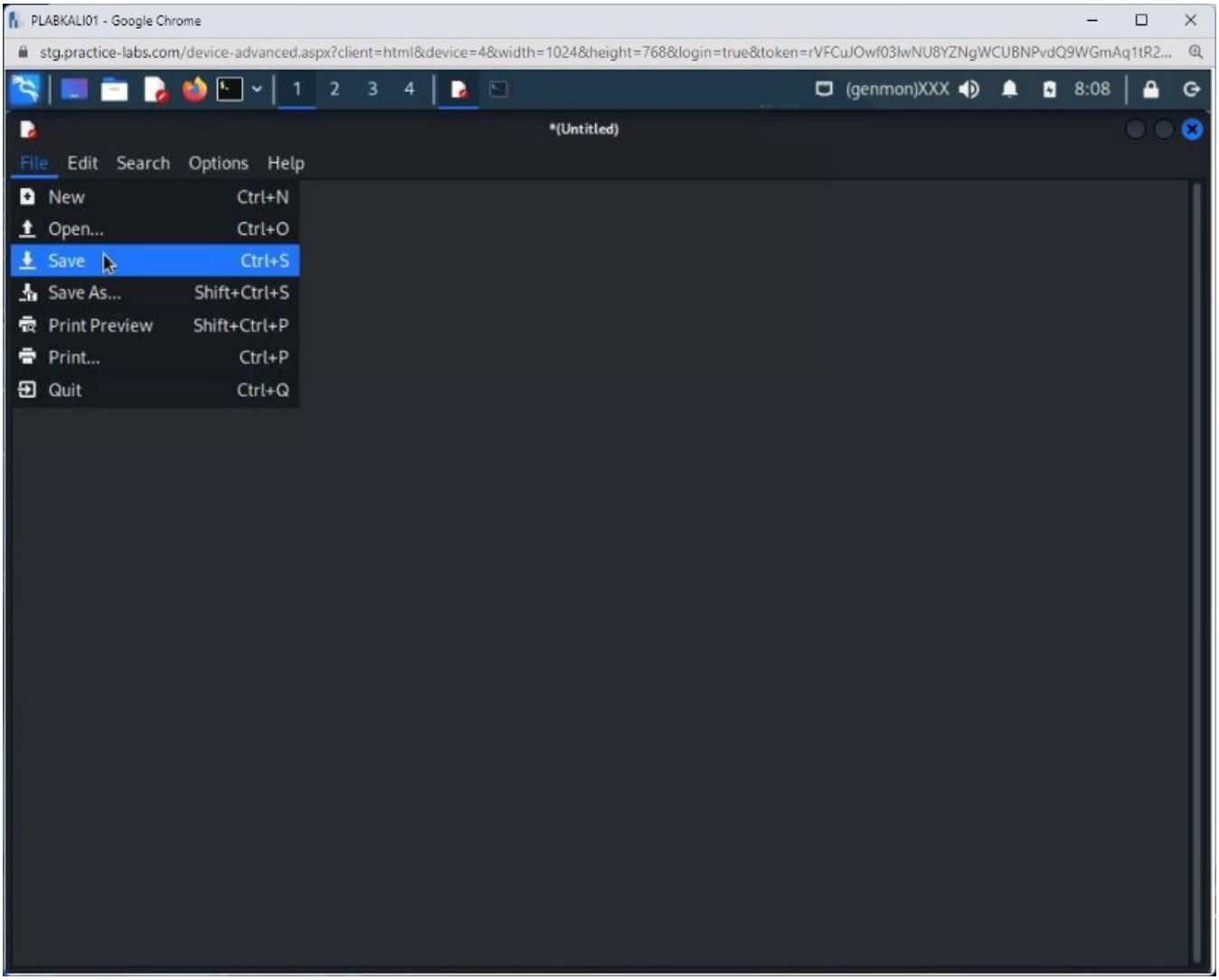
The **(Untitled)** window is opened. Type the following words:

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




### Step 3

Click **File**, and then select **Save**.




**Step 4**

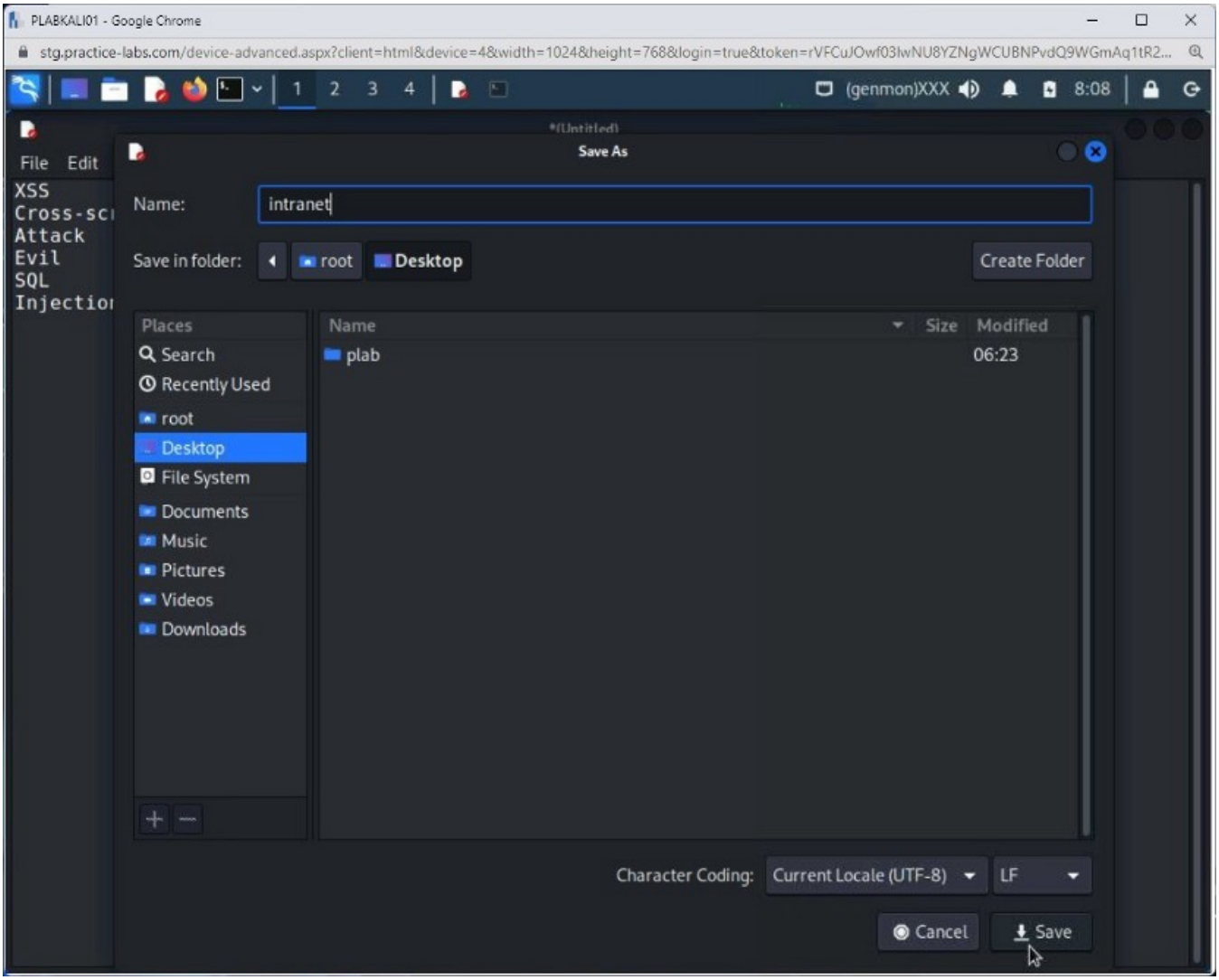
The **Save As** dialog box is displayed.

From the left-hand pane, select **Desktop**.

In the **Name** text box, type the following name:

```
intranet
```

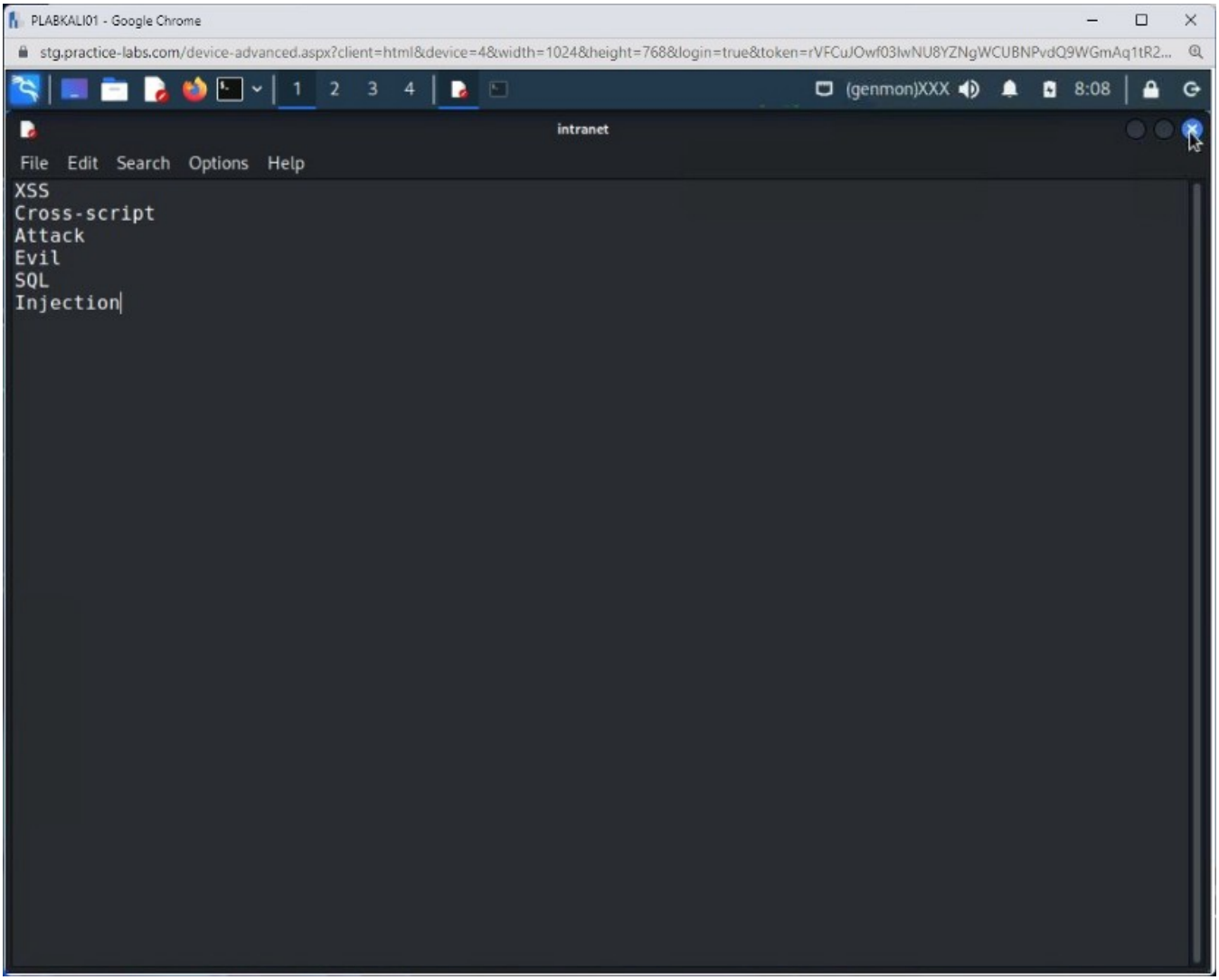
Click **Save**.




### Step 5

Notice that the file name is now changed to the **intranet**.

Close the **Leaf Editor** window.




**Step 6**

Restore the terminal window.

Clear the screen by entering the following command:

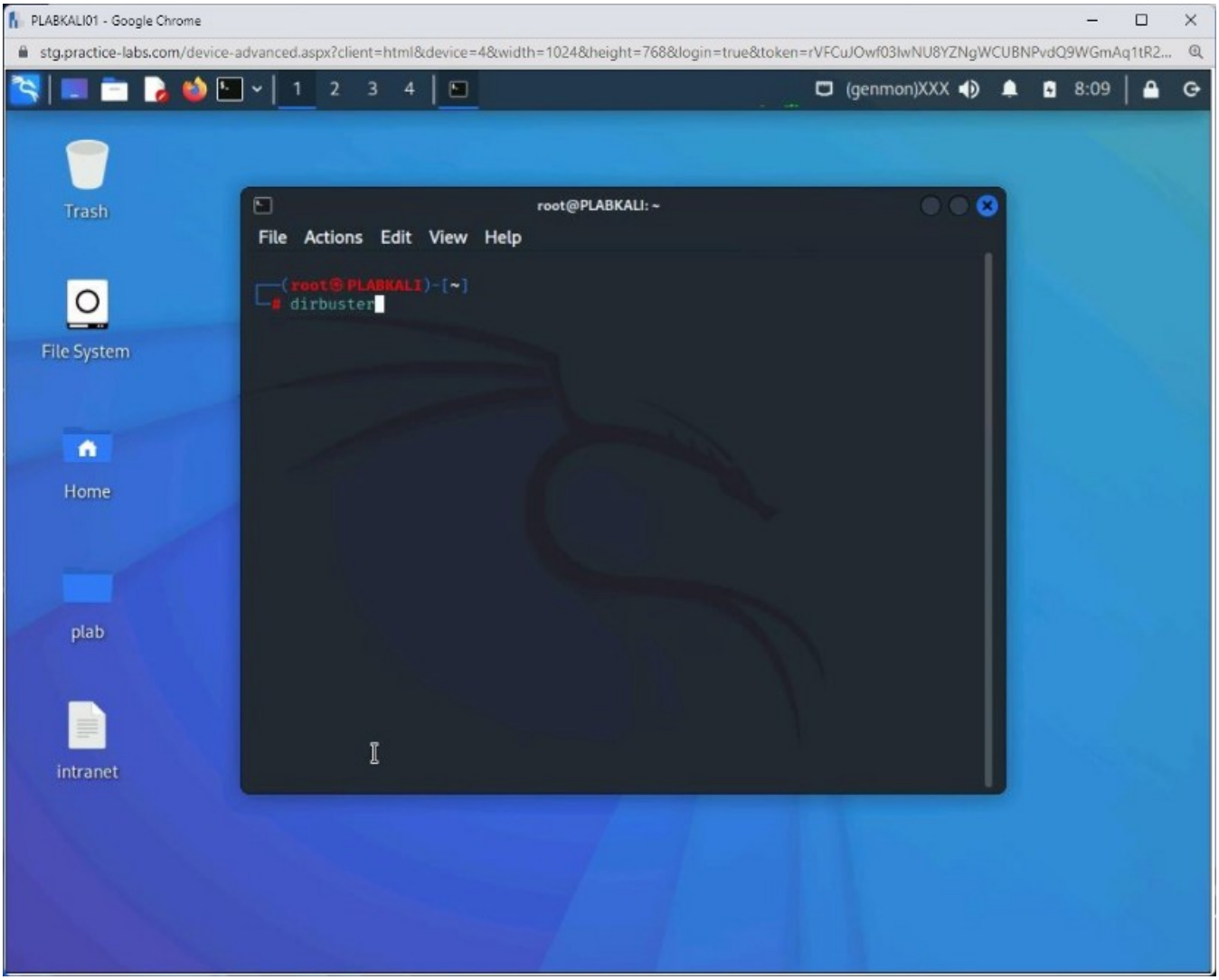
```
clear
```

Press **Enter**.

Type the following command:

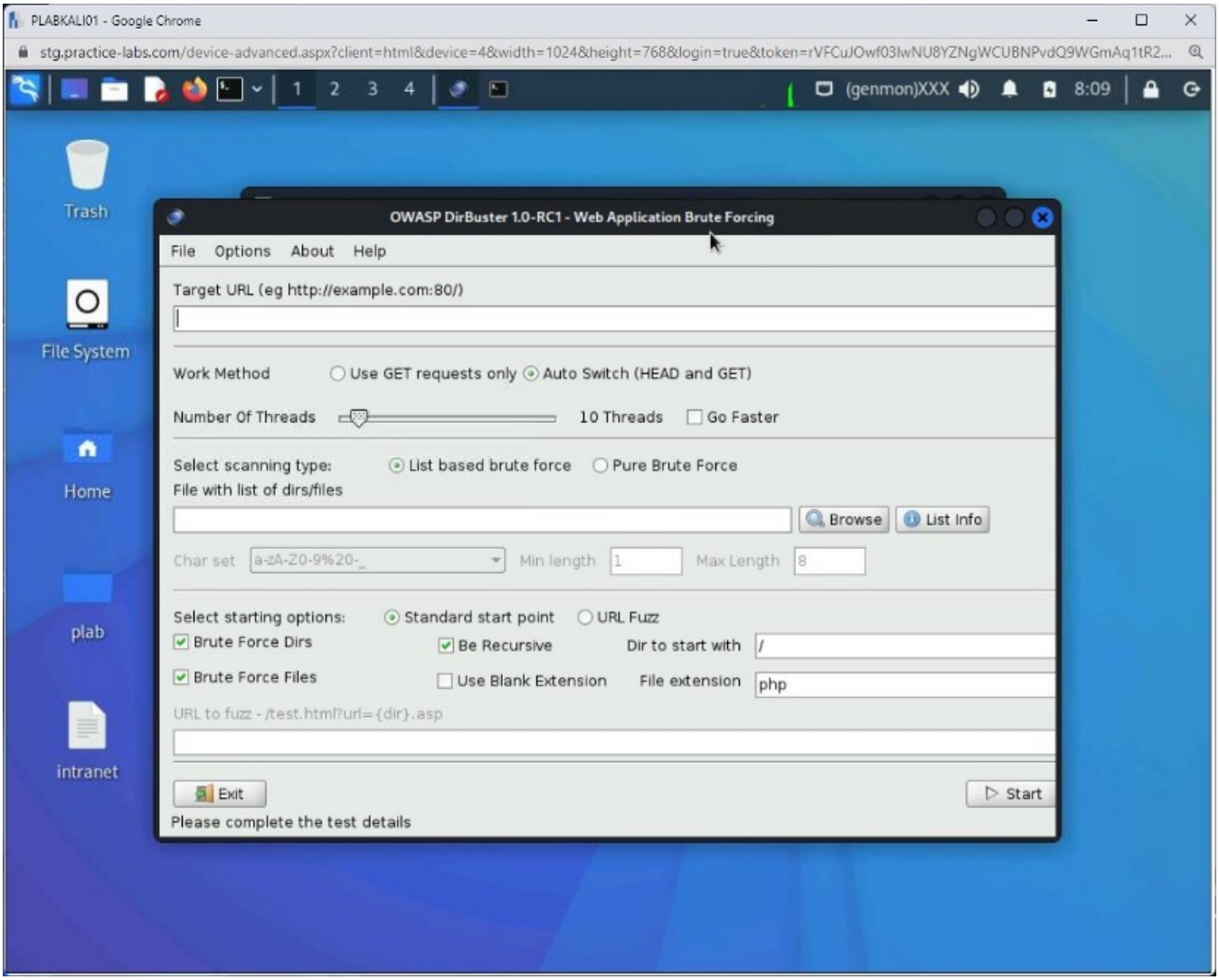
```
dirbuster
```

Press **Enter**.




**Step 7**

The **OWASP DirBuster** window is displayed.




### Step 8

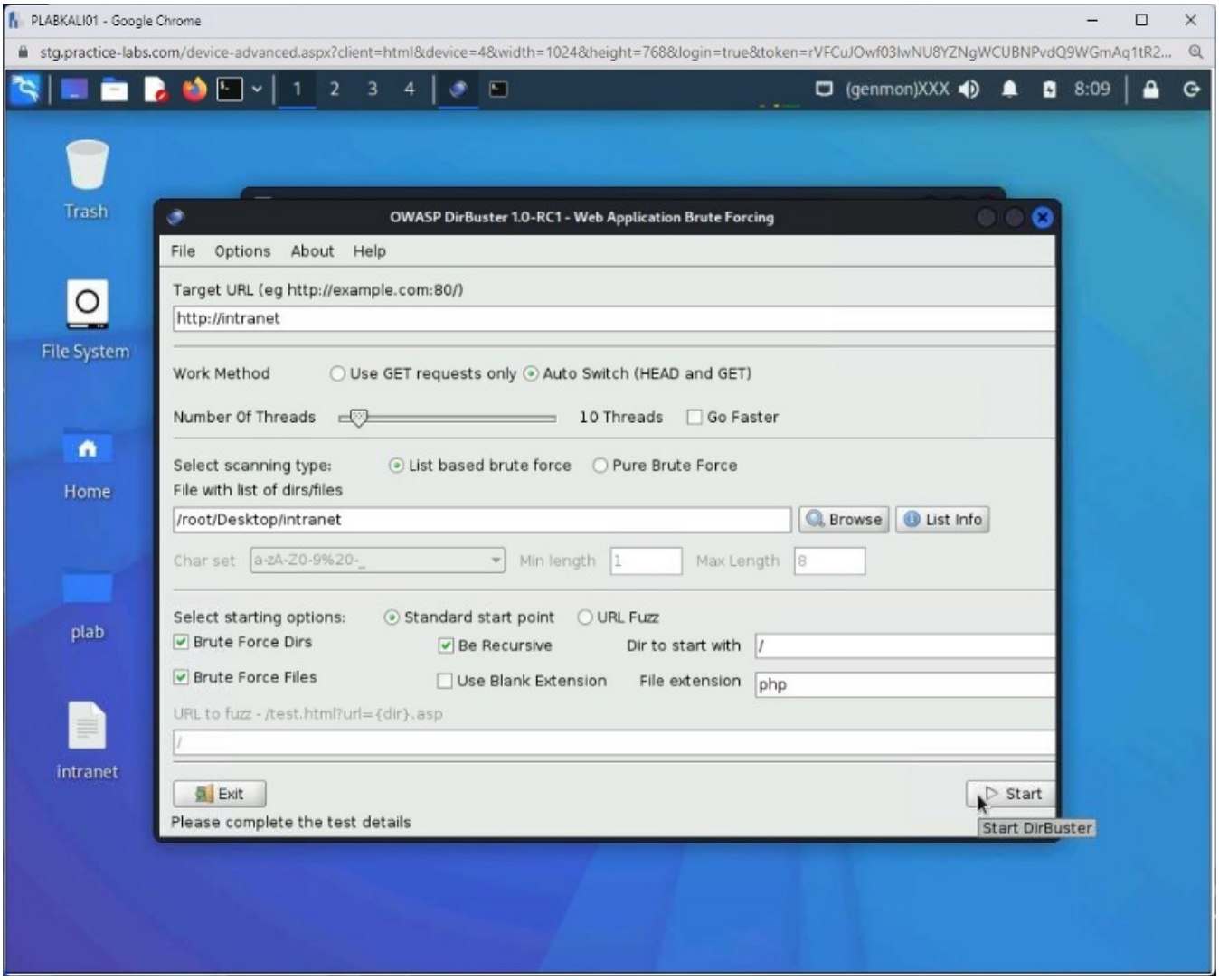
In the **Target URL** text box, type the following URL:

```
http://intranet
```

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

```
/root/Desktop/intranet
```

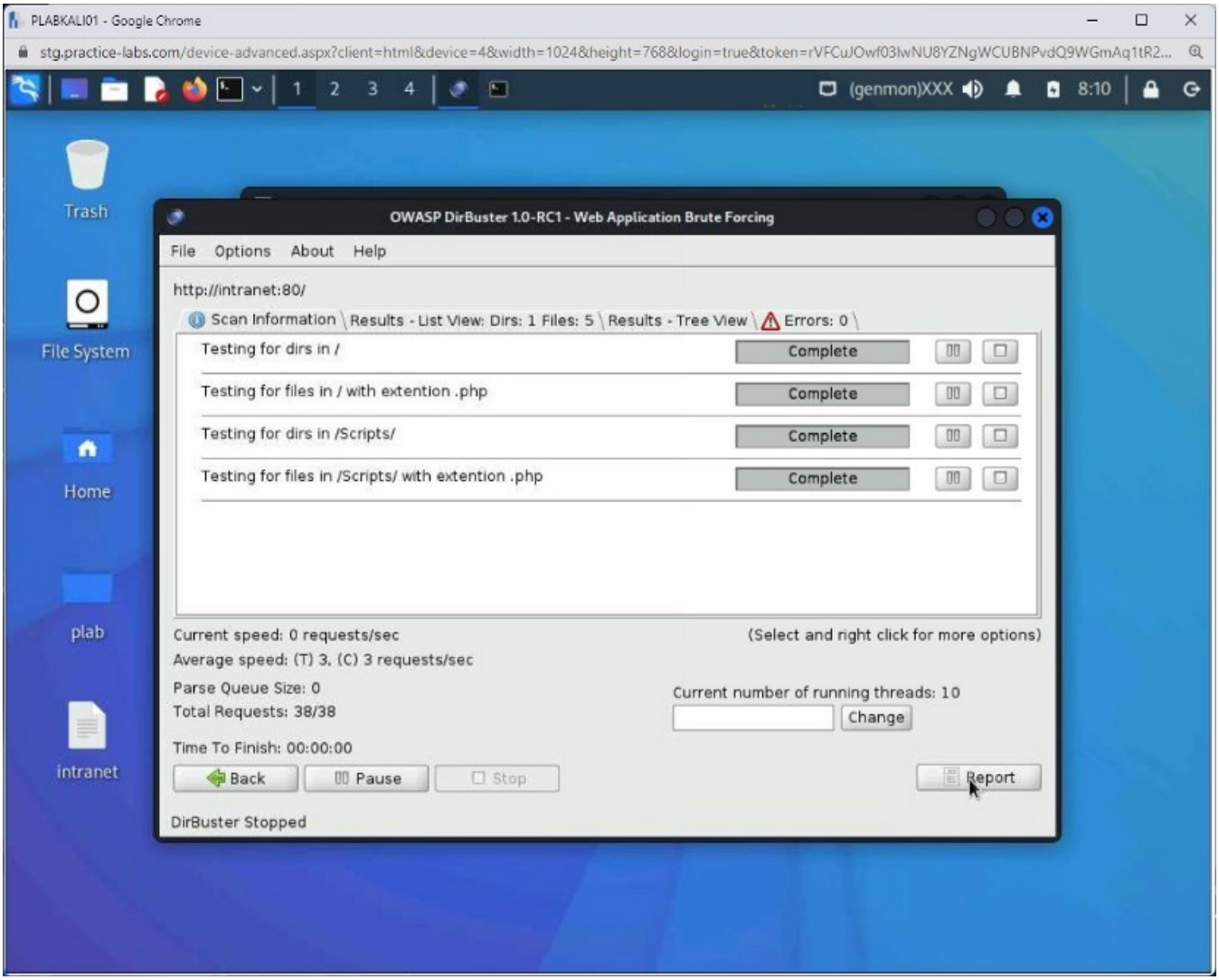
Click **Start**.




**Step 9**

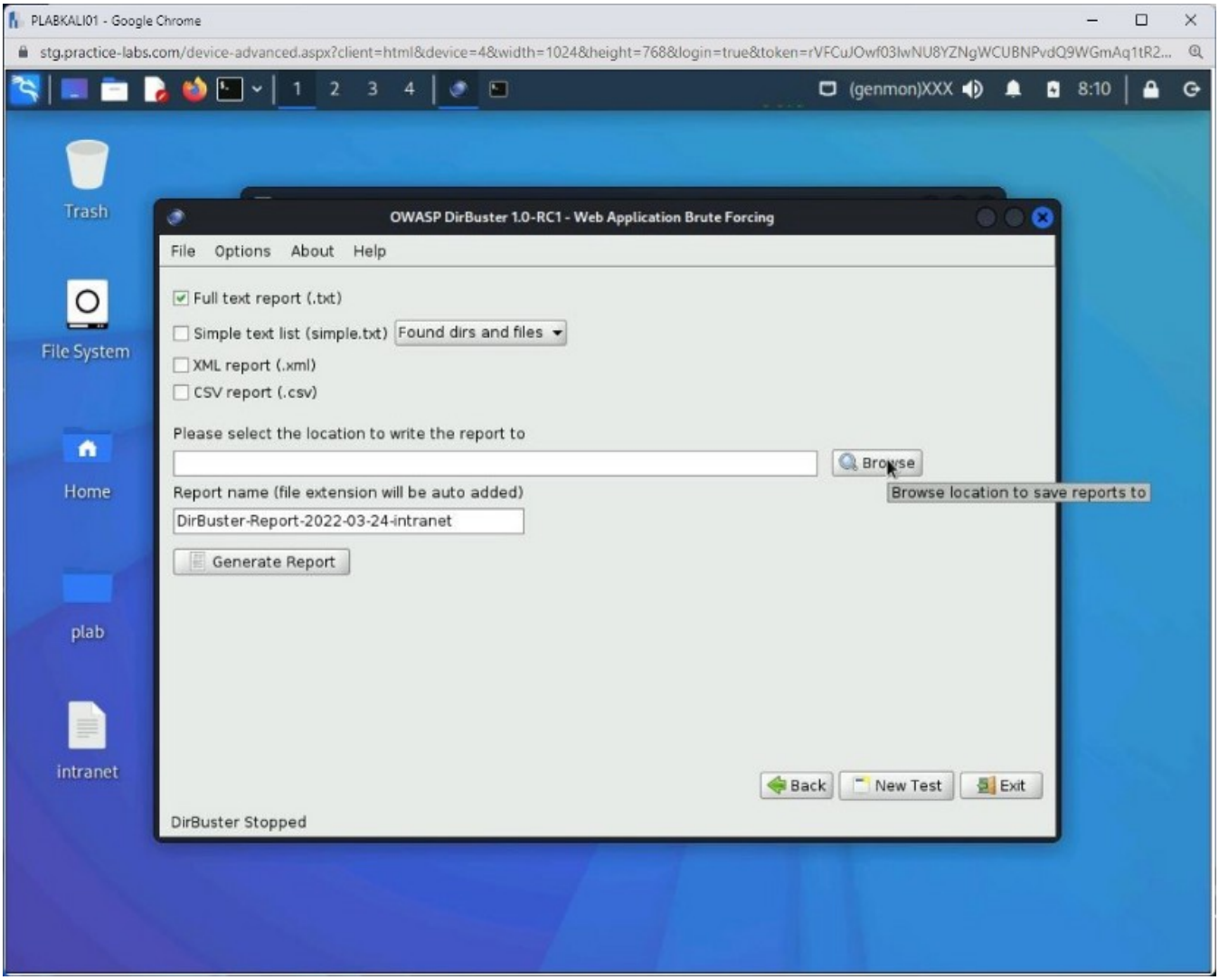
The scanning process starts.

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



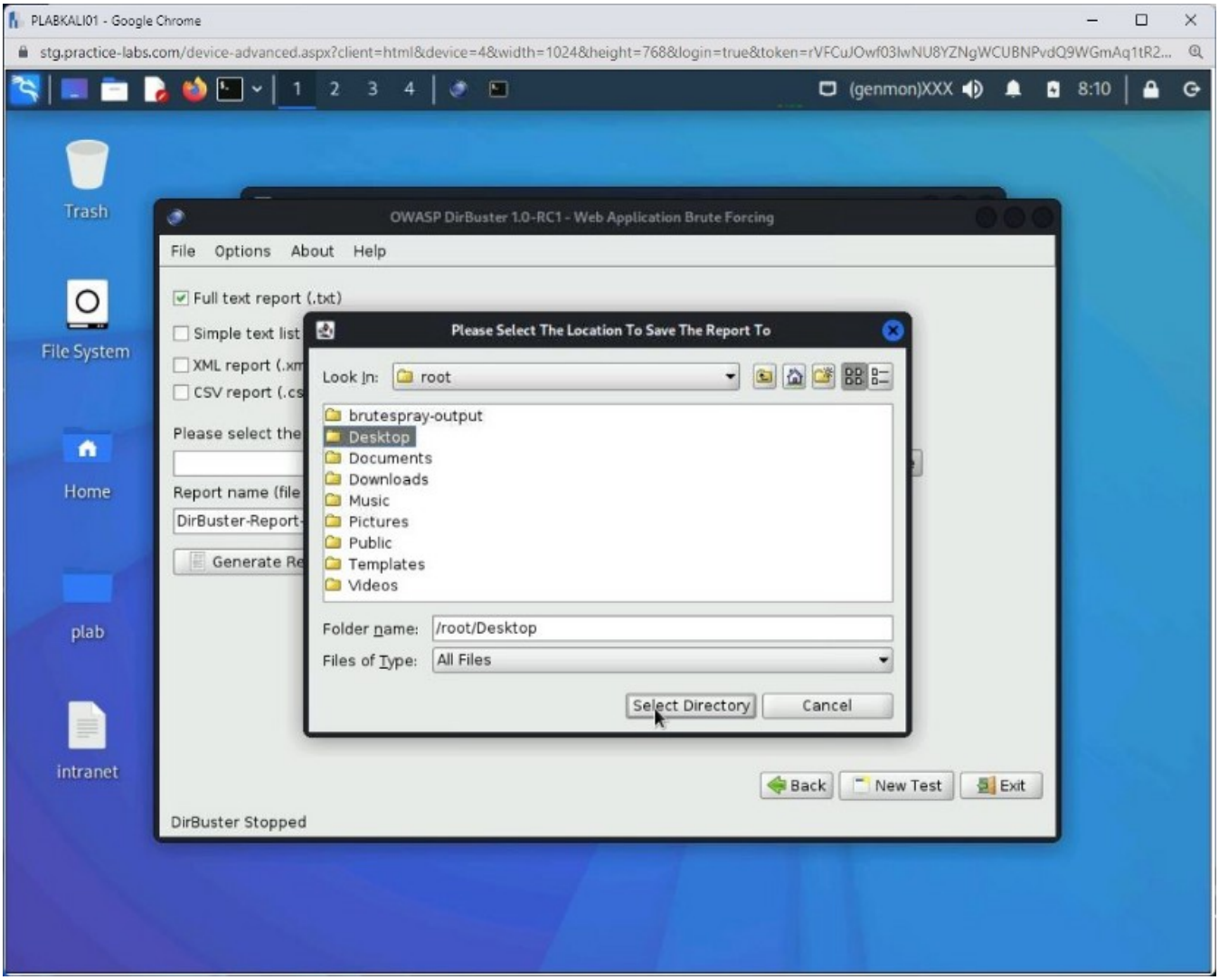

**Step 10**

Click **Browse**.



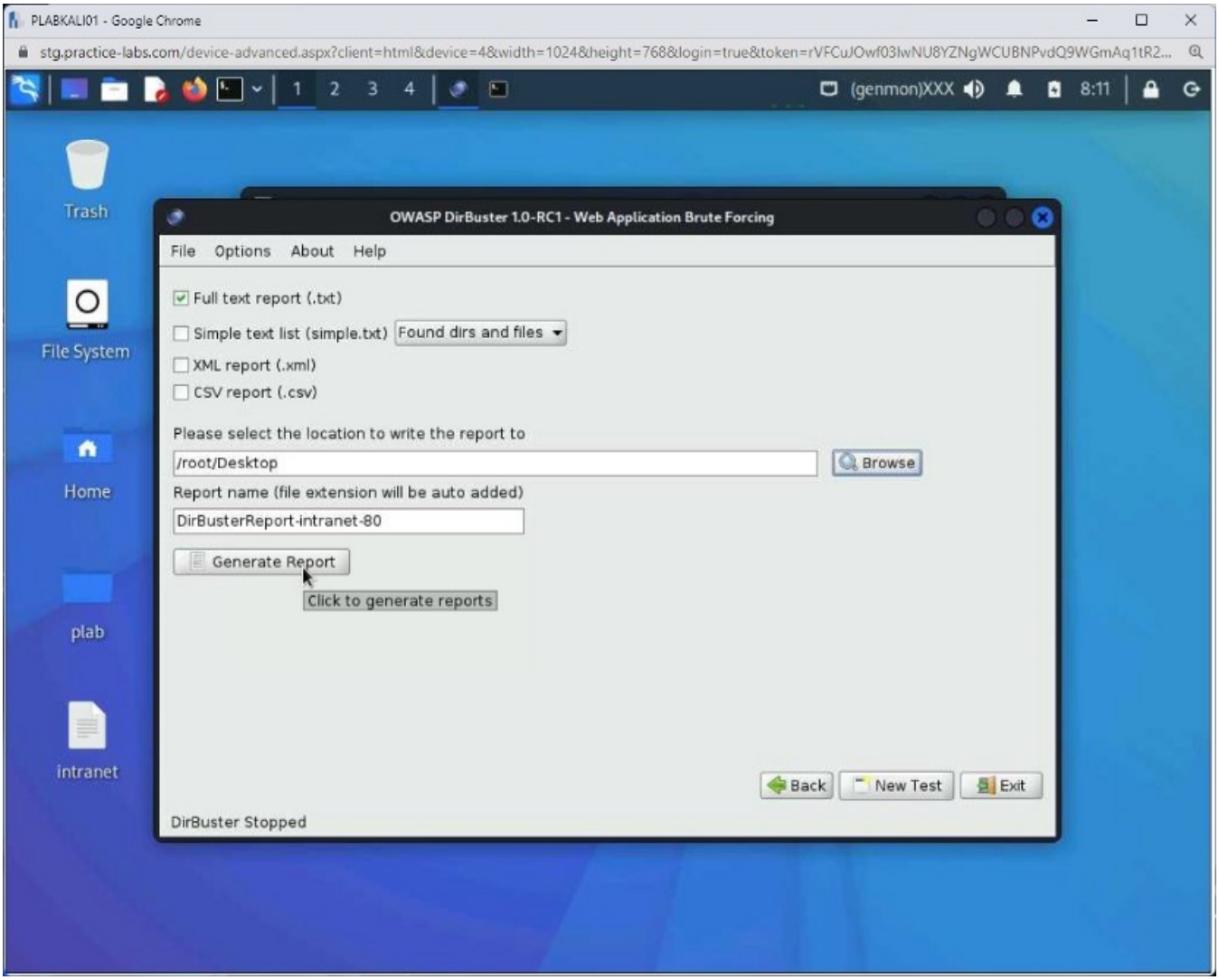

**Step 11**

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




**Step 12**

Click **Generate Report**.

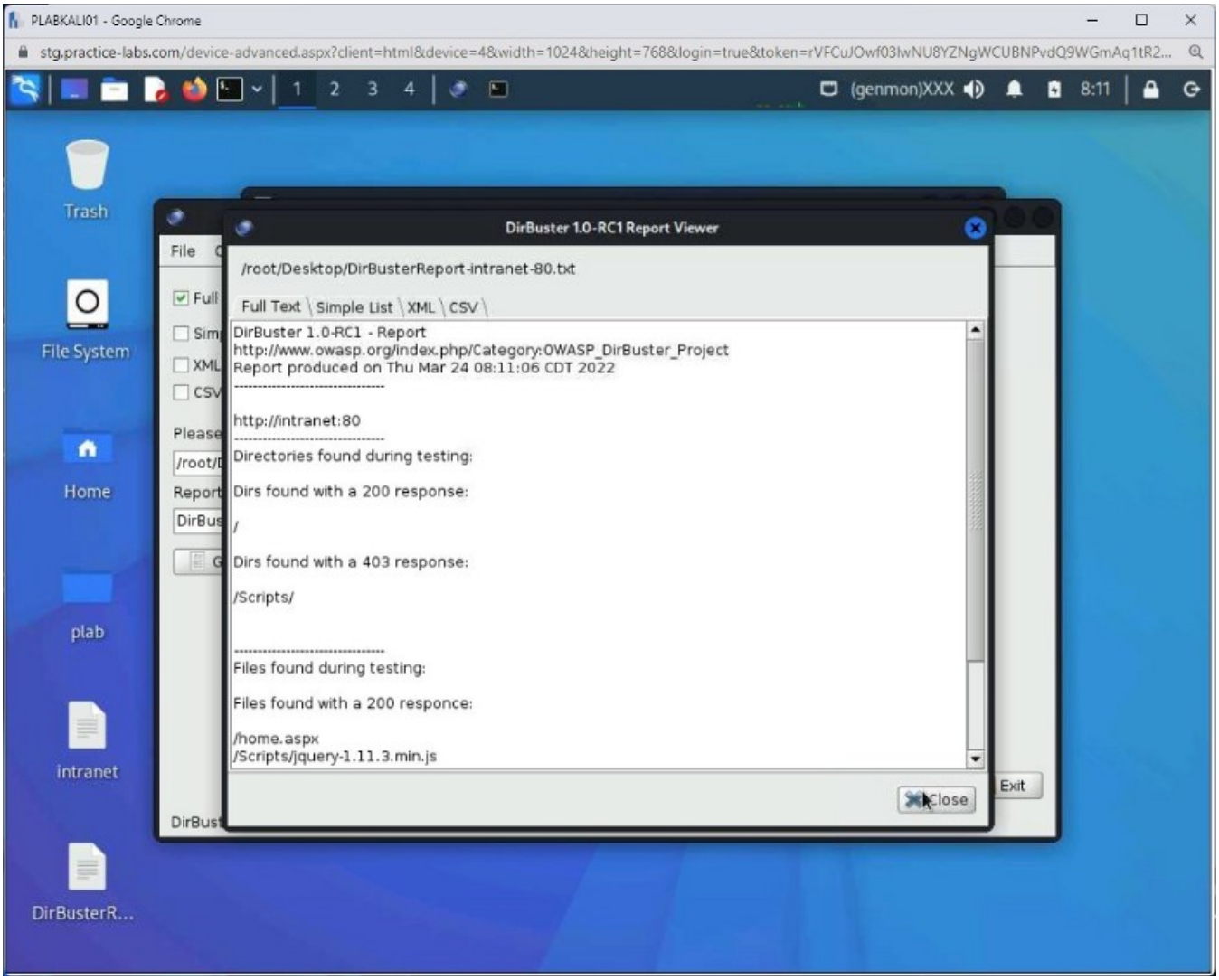



**Step 13**

The **DirBuster 1.0-RC1 Report Viewer** dialog box is displayed.

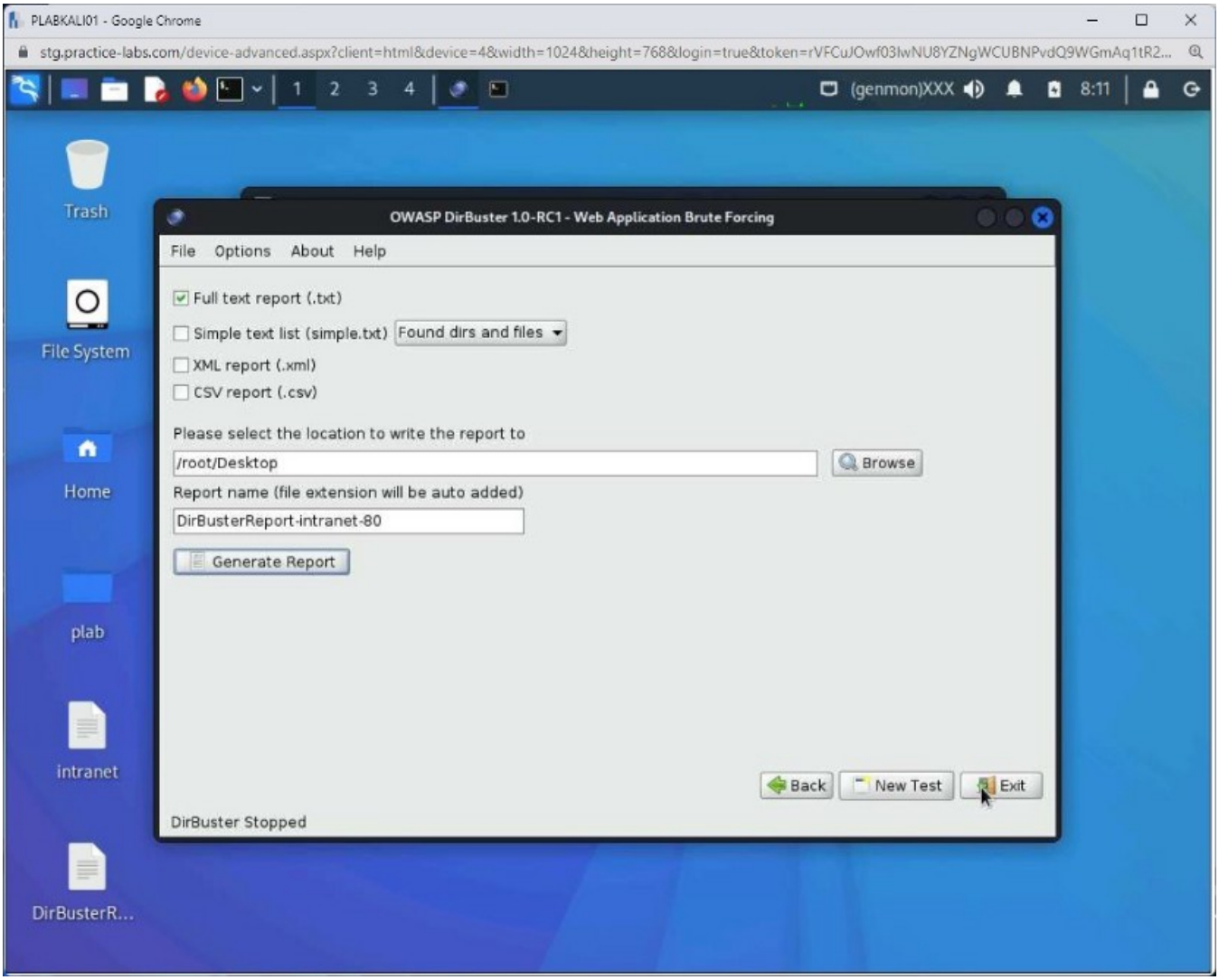
Notice the list of all files and directories that have been discovered.

Click **Close**.




### Step 14

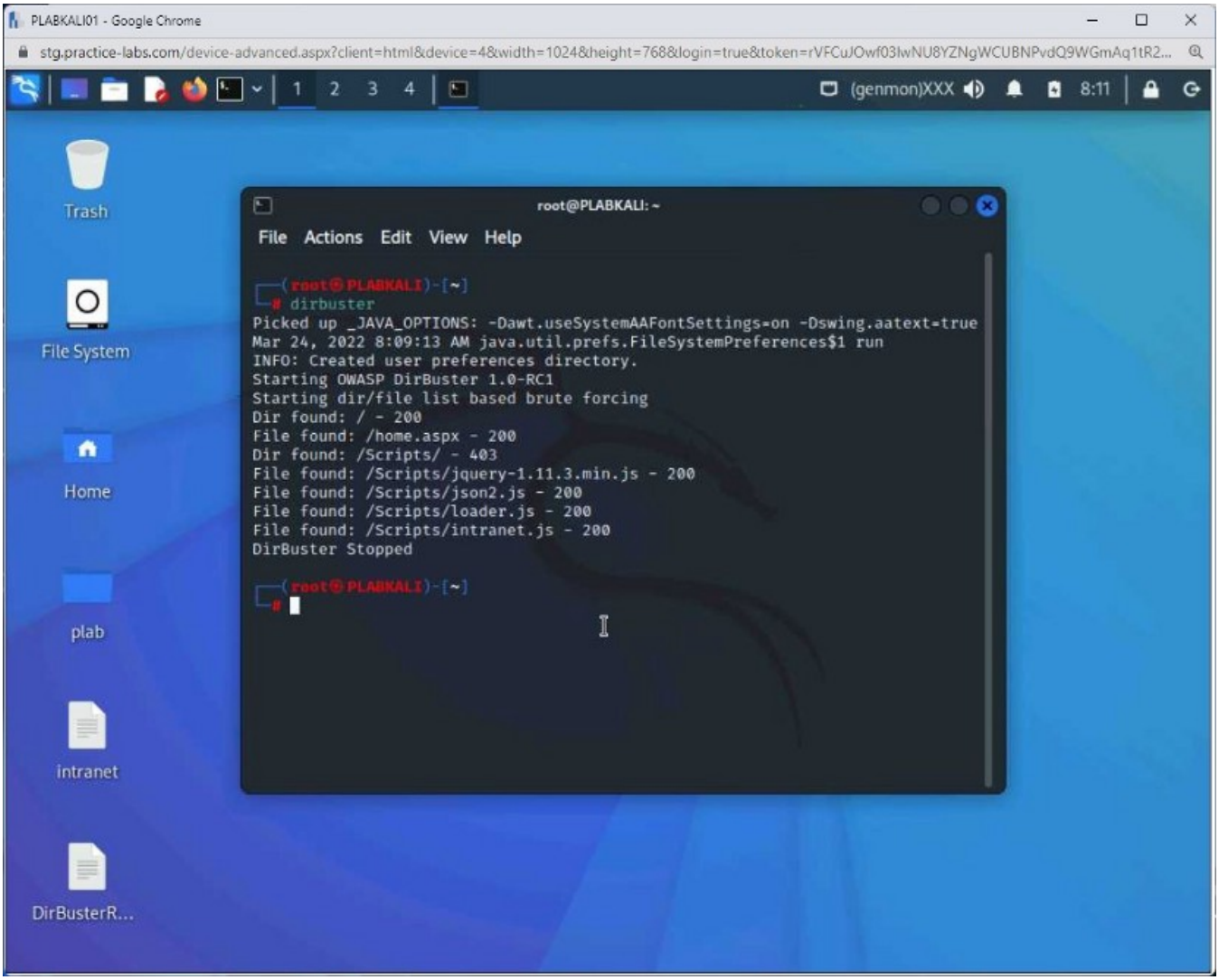
Click **Exit** to close the **DirBuster** window.




**Step 15**

You are back on the terminal window.

Notice that a brief about the files and directories are also displayed.




Close all open windows and proceed to the next exercise.

## Exercise 2 — Upgrade Kali Linux

Updates and packages work in different ways in Windows and Linux. In Windows, you can select specific updates and install them, and It allows you to update installed software individually.

In Linux however, this method works differently. In Linux, you do not upgrade or patch the individual packages. You can only remove an existing package and install a newer version. Alternatively, you can run the **apt upgrade** command to upgrade all packages at once.

Kali Linux is a Debian-based Linux that works with rolling updates about four times a year. When you have one version of Kali Linux installed, you can update applications or even the operating system with a newer version by running a few commands.

In this exercise, you will learn to update Kali Linux.

## Learning Outcomes

After completing this exercise, you will be able to:

- Verify Repositories
- Update Package Manager
- Install Packages and Patches

## Your Devices

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

PLABDC01Domain Controller192.168.0.1/24PLABKALI01Domain MemberWorkstation192.168.0.5/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2019.2 — Linux Kali Workstation192.168.0.5/24

## Task 1 — Verify the Repositories

Kali Linux works with repositories from where it downloads packages, and maintains a list of said repositories — of which you can find the list from the /etc/apt/sources.list file. Kali Linux also contains the /etc/apt/source.list.d/ directory, that contains repositories files. If you need to add a custom repository, you can create a custom source file and add it to this directory.

However, each custom file needs to have a unique name. When you add files into this directory, you do not need to edit the sources.list file. You can remove the file from this directory to remove the custom source.

In this task, you will verify the repositories used to upgrade Kali and packages.

### Step 1

Clear the screen by entering the following command:

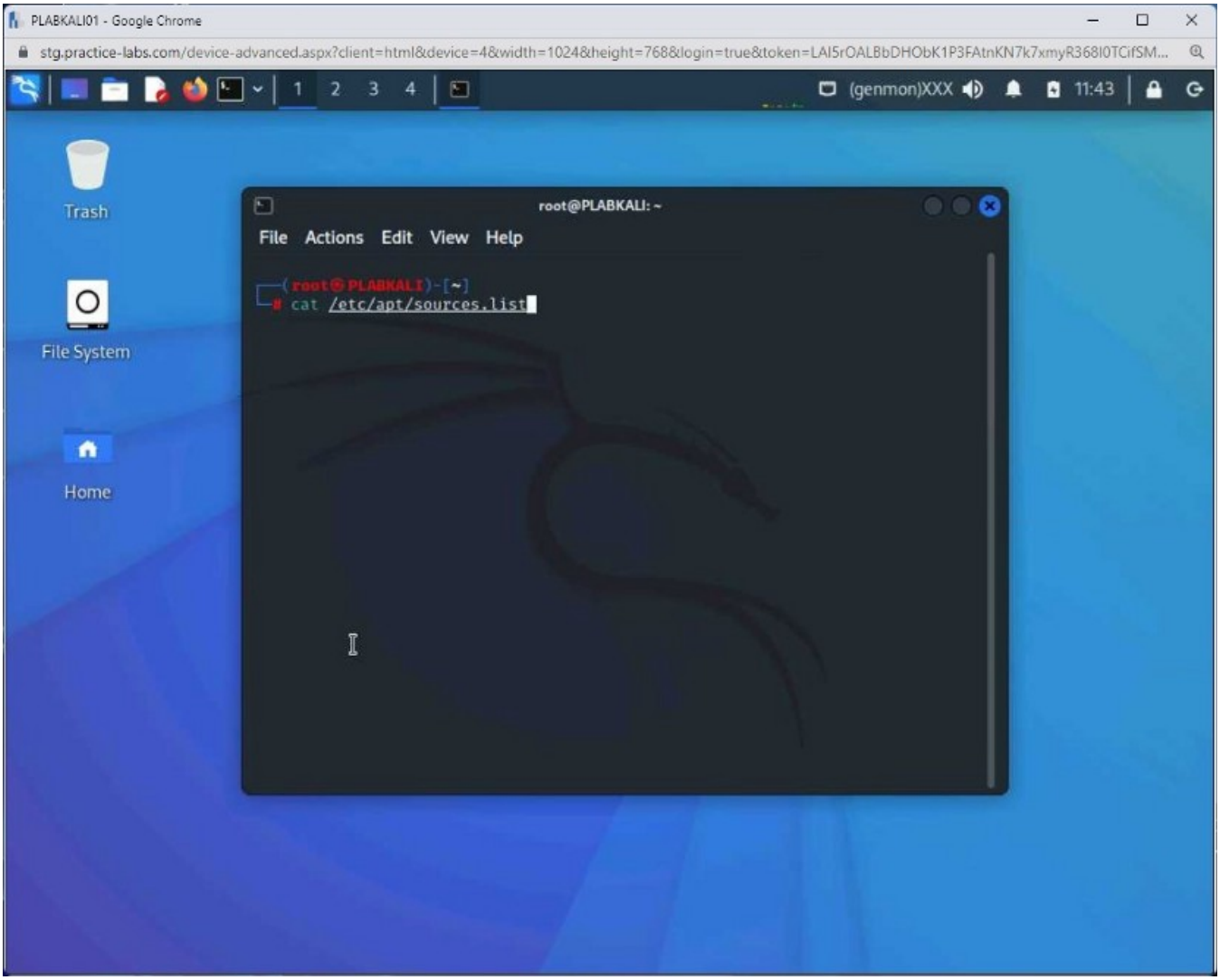
```
clear
```

Press **Enter**.

To verify the sources, type the following command:

```
cat /etc/apt/sources.list
```

Press **Enter**.

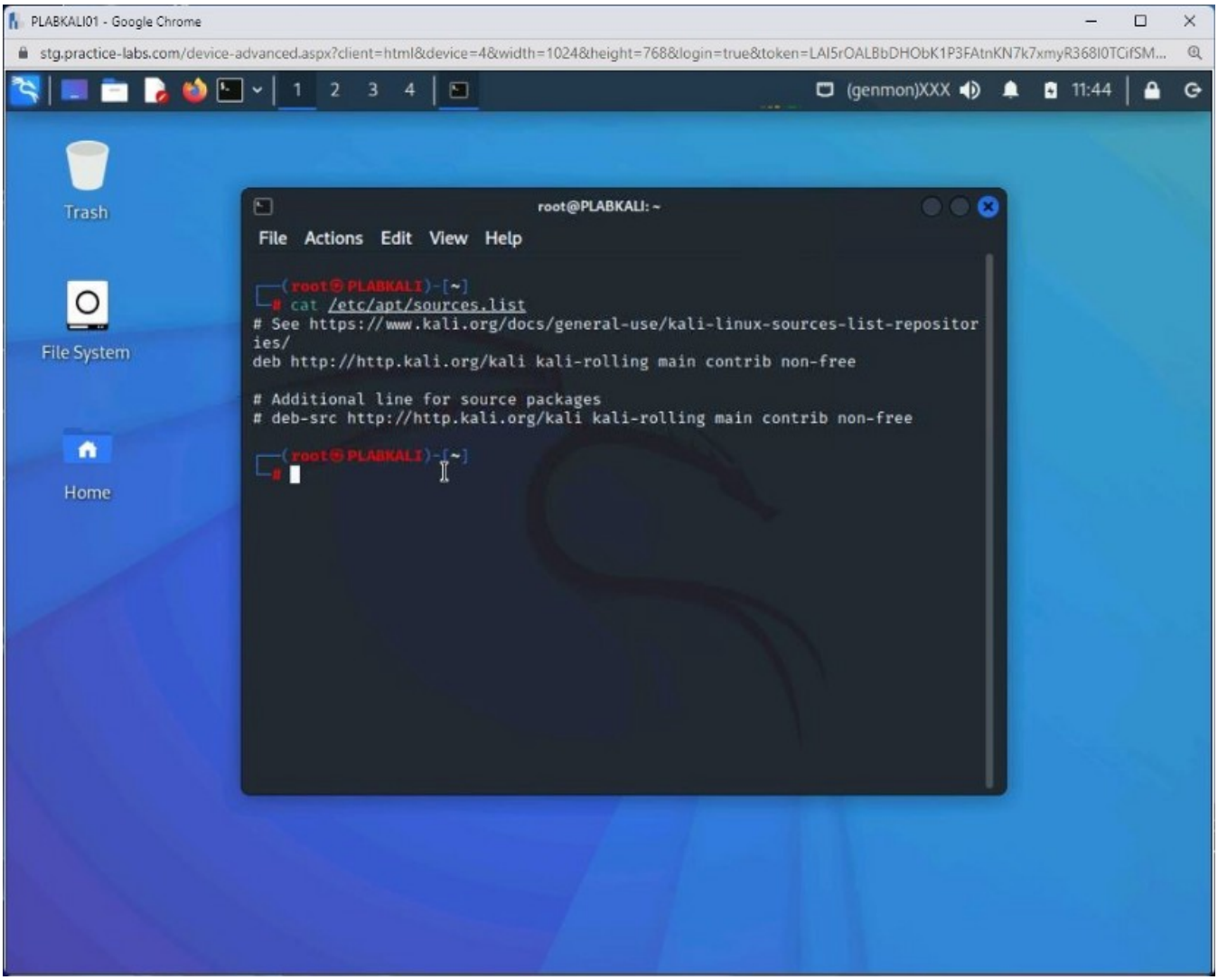



**Step 2**

The output shows three rows in which repositories are listed.

Two of the rows are commented with #. There is only one row that lists the following:

```
http://http.kali.org/kali kali-rolling main contrib non-free
```



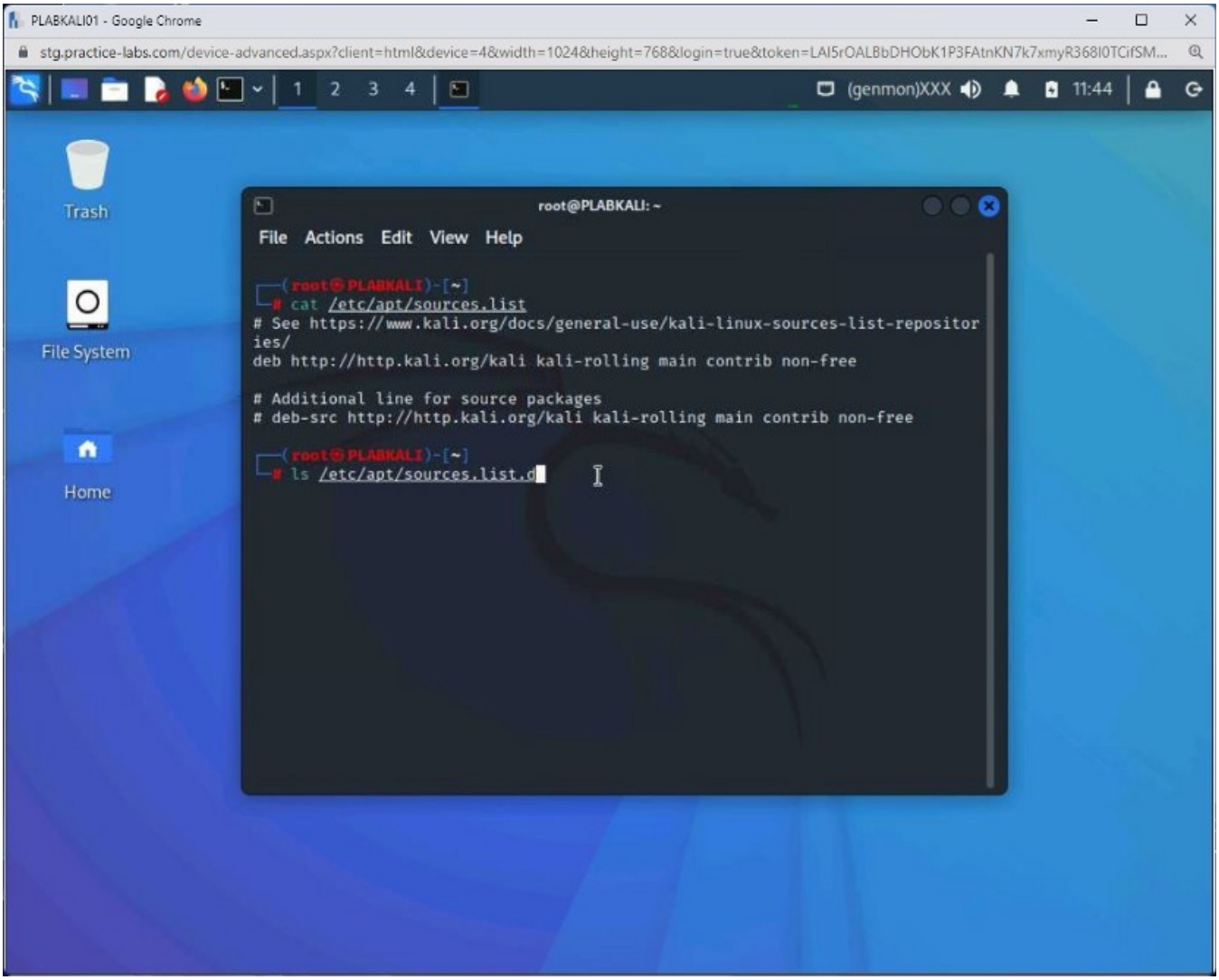

**Step 3**

Let's now view if there are any files in the /etc/apt/source.list.d/ directory.

To do this, type the following command:

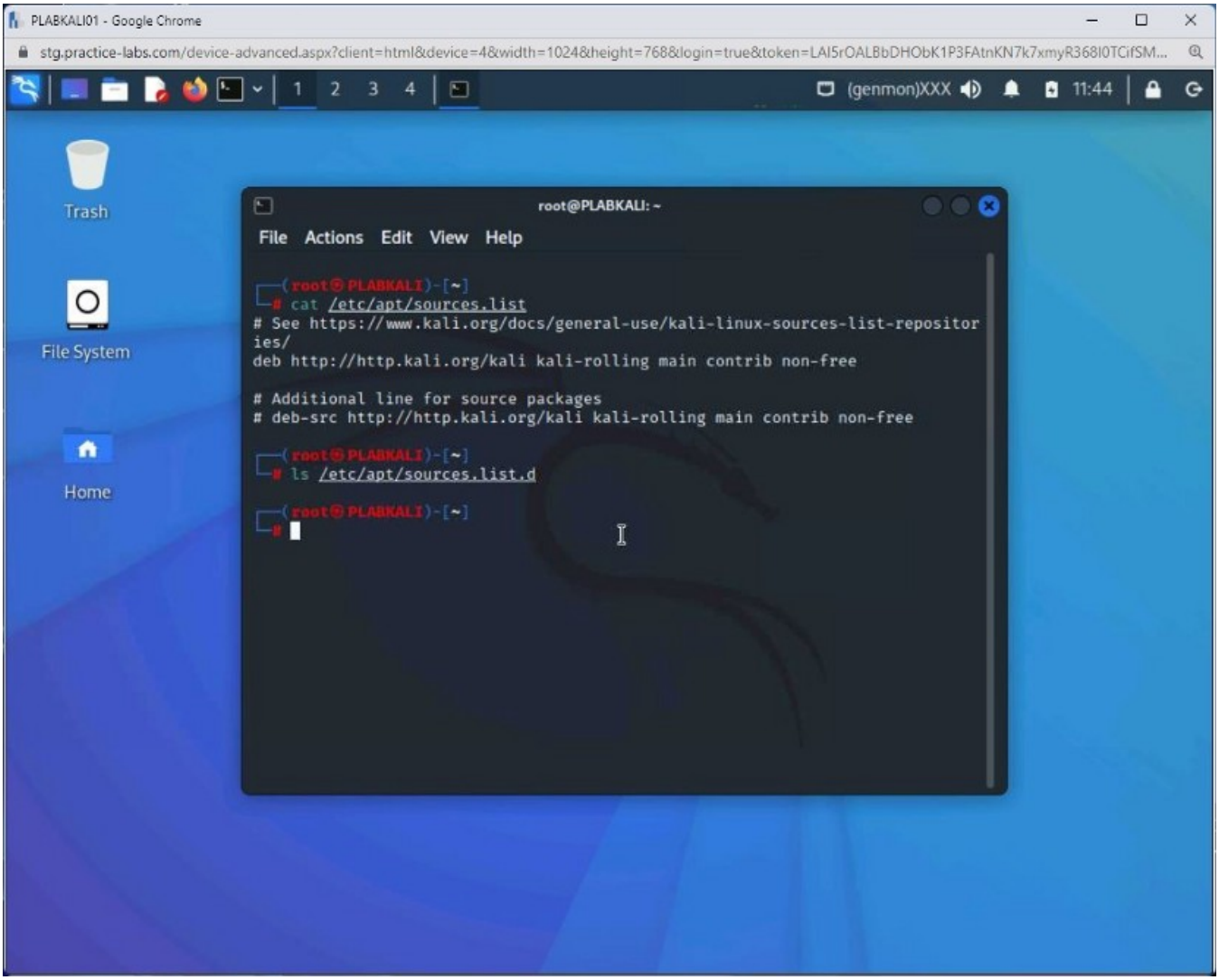
```
ls /etc/apt/sources.list.d
```

Press **Enter**.




**Step 4**

The output does not list any files.




Keep the terminal window open.

## Task 2 — Update Package Lists

Whenever you plan to install software on Kali Linux, it is always advisable to update the package repository. This is required to get the latest versions of software for which you need to get the latest package lists.

To update the package lists, perform the following command:

### Step 1

Clear the screen by entering the following command:

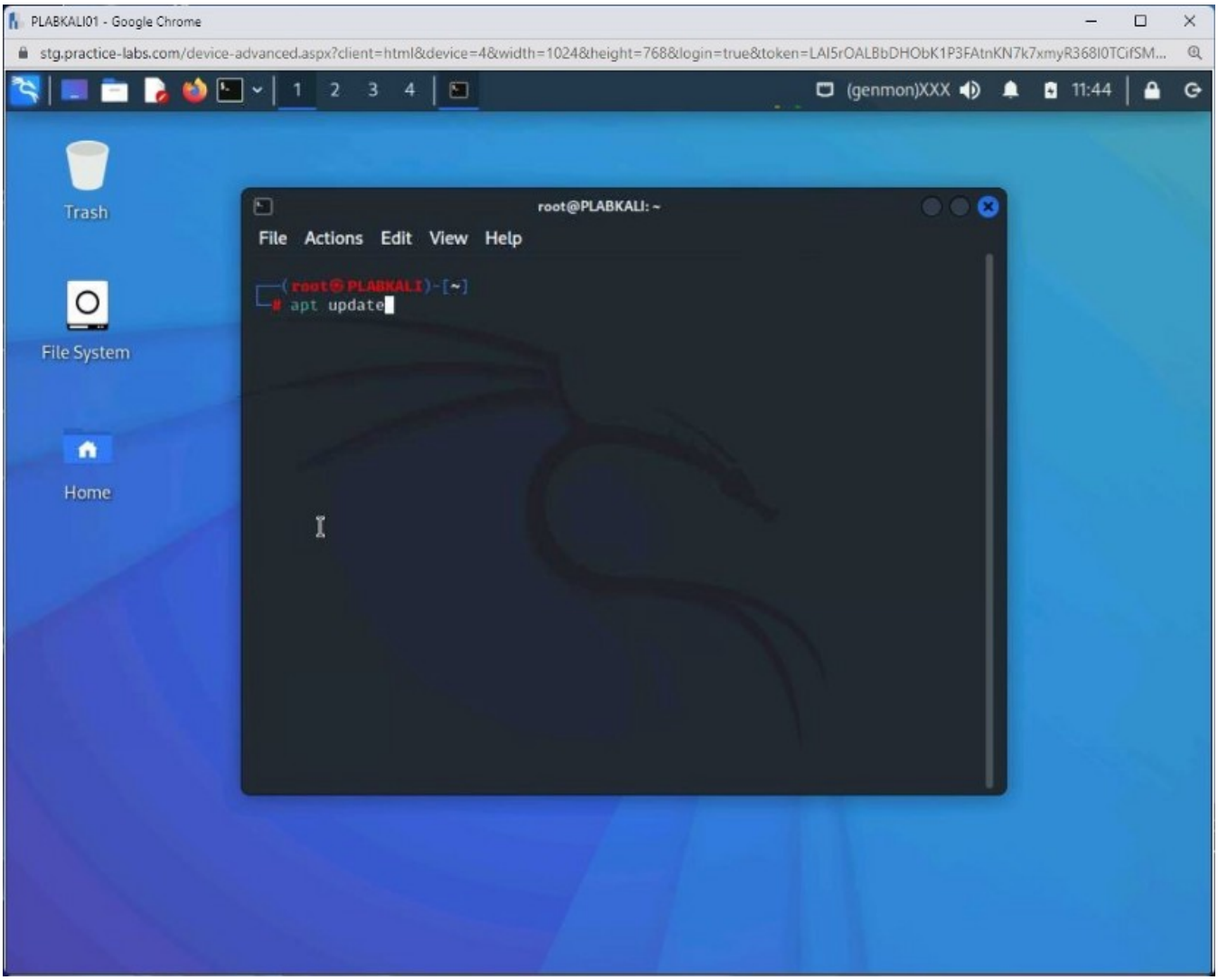
```
clear
```

Press **Enter**.

To get the latest package lists, type the following command:

```
apt update
```

Press **Enter**.

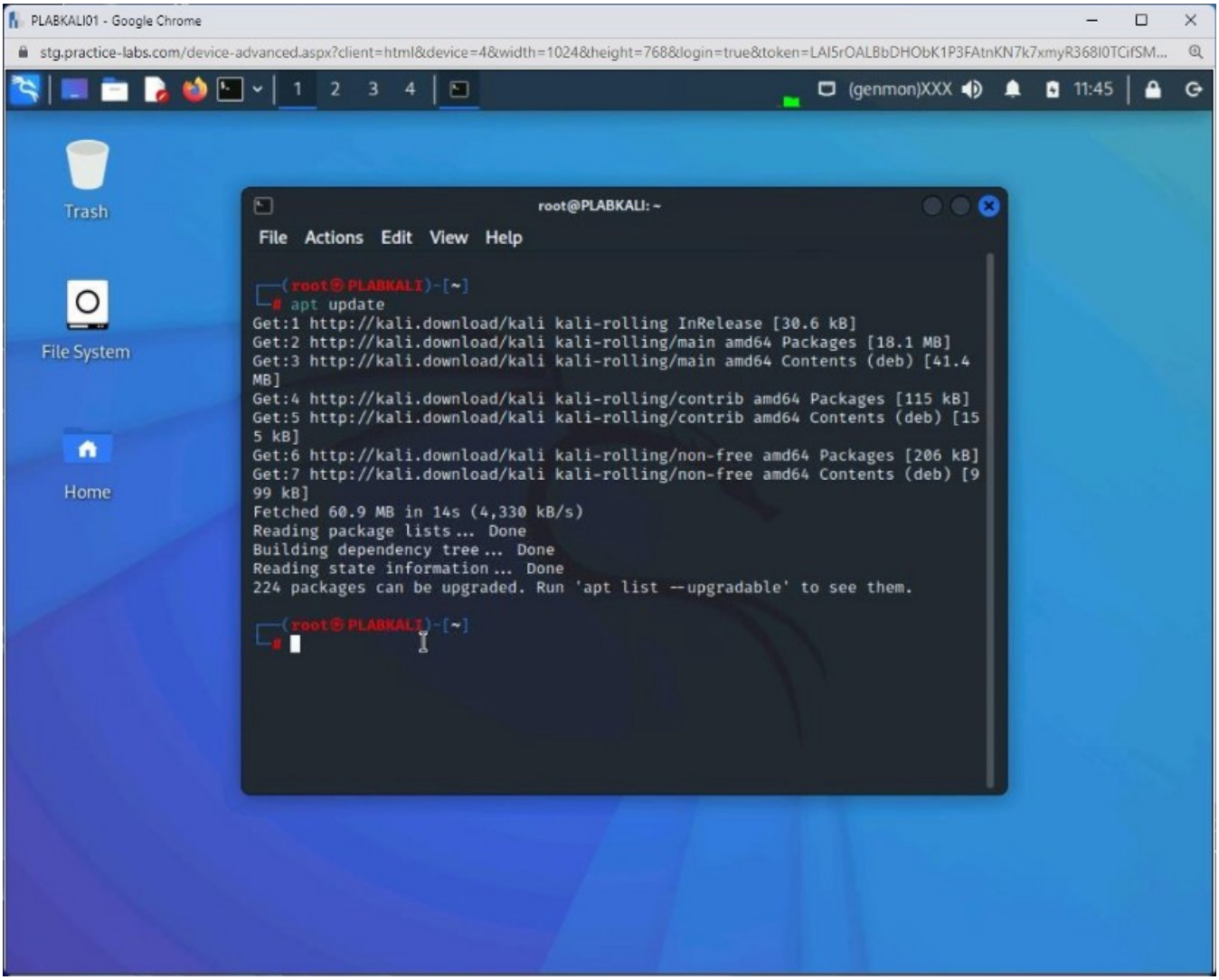



**Step 2**

The package lists are now updated.

he output displays the size of each package list. The output also displays the number of packages that can be upgraded.

***Note:*** *The number of packages may differ from the screenshots in the lab environment.*




## Task 3 — Install Packages and Patches

There are different methods to install or upgrade packages in Linux. You can upgrade the package without deleting the old ones, or delete the old ones and install new versions. Kali Linux has three different commands that are run with the apt package manager:

- **upgrade**: It installs the new versions of the packages and retains the old ones without deleting them.
- **full-upgrade**: It upgrades the existing packages. It can also remove the old packages if required.
- **dist-upgrade**: It handles the dependencies and package upgrades. It can also remove obsolete packages if required.

In this task, you will perform and execute the full-upgrade and dist-upgrade command.

### Step 1

Clear the screen by entering the following command:

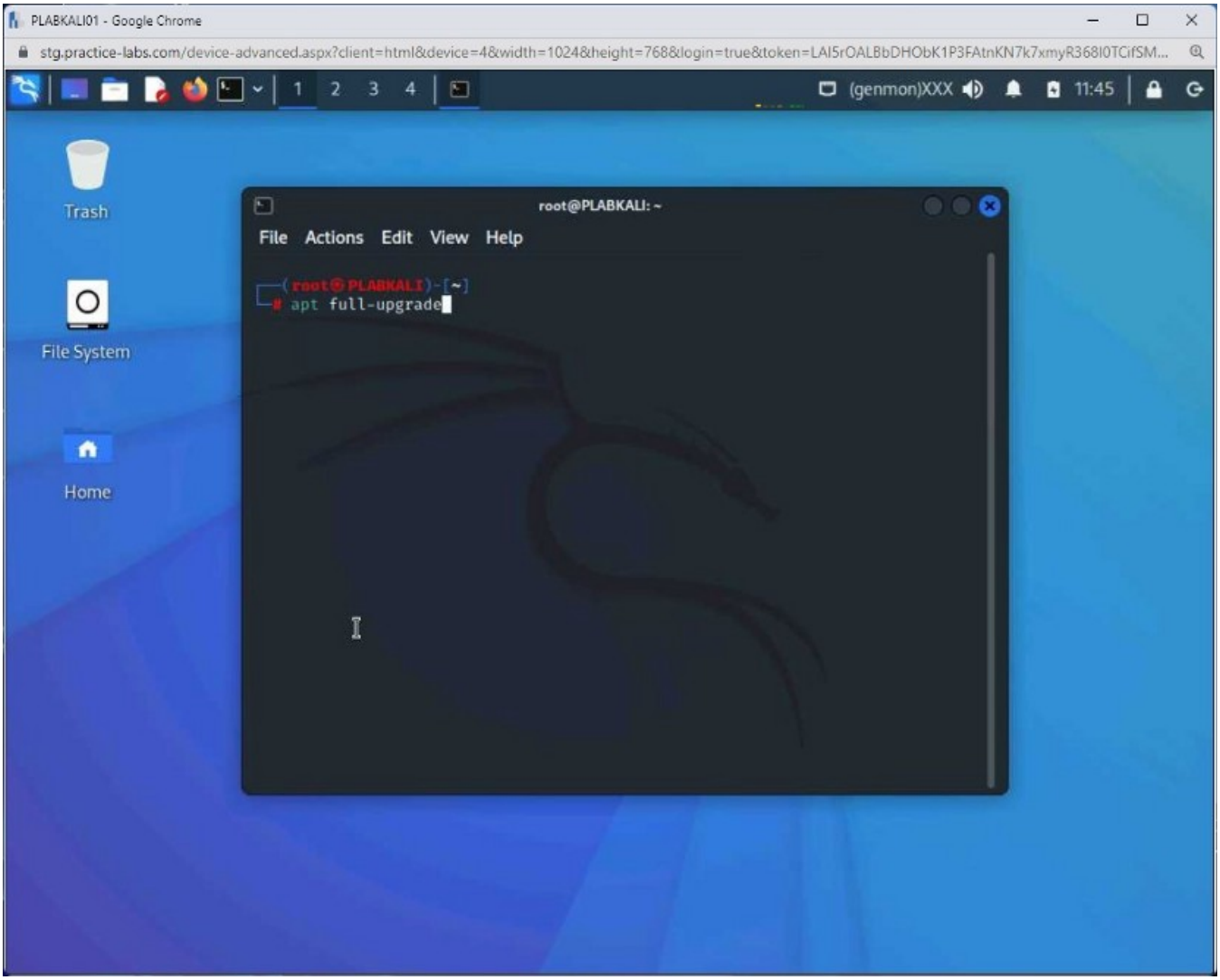
```
clear
```

Press **Enter**.

Type the following command:

```
apt full-upgrade
```

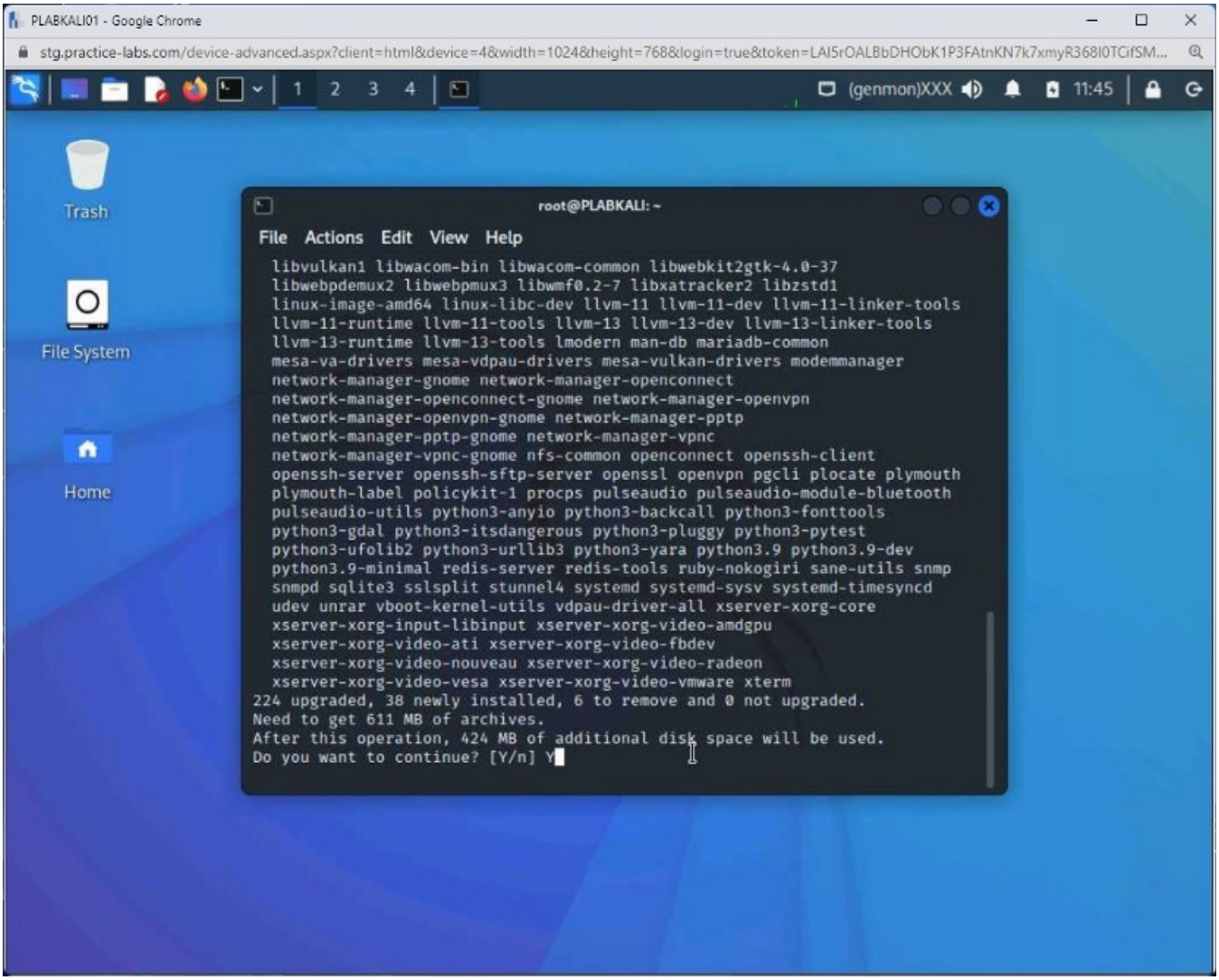
Press **Enter**.




**Step 2**

The **apt full-upgrade** command executes and provides a summary of the packages that will be upgraded, installed, removed, and not upgraded.

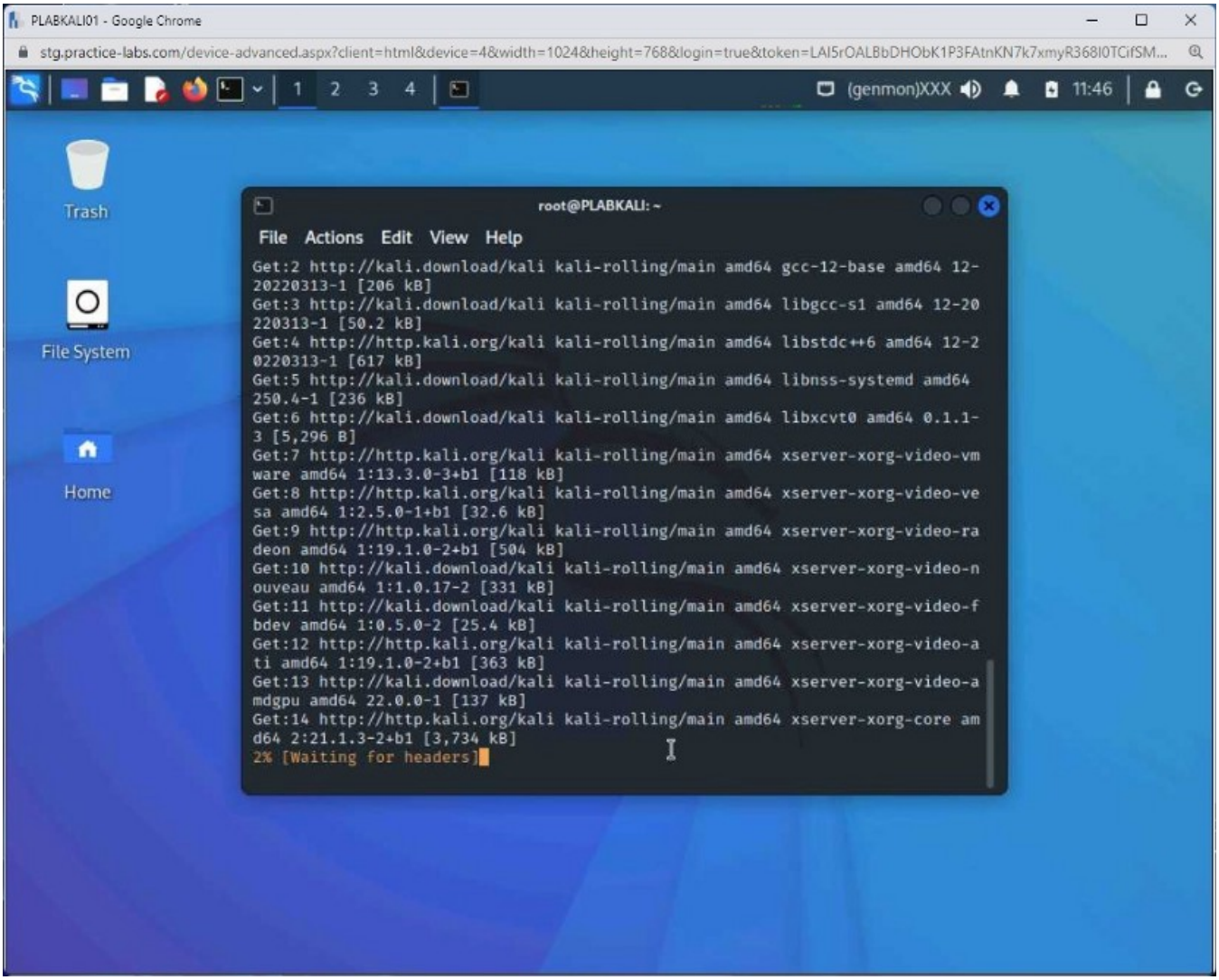
Type **Y** and press **Enter** to continue.




### Step 3

The full-upgrade process starts.

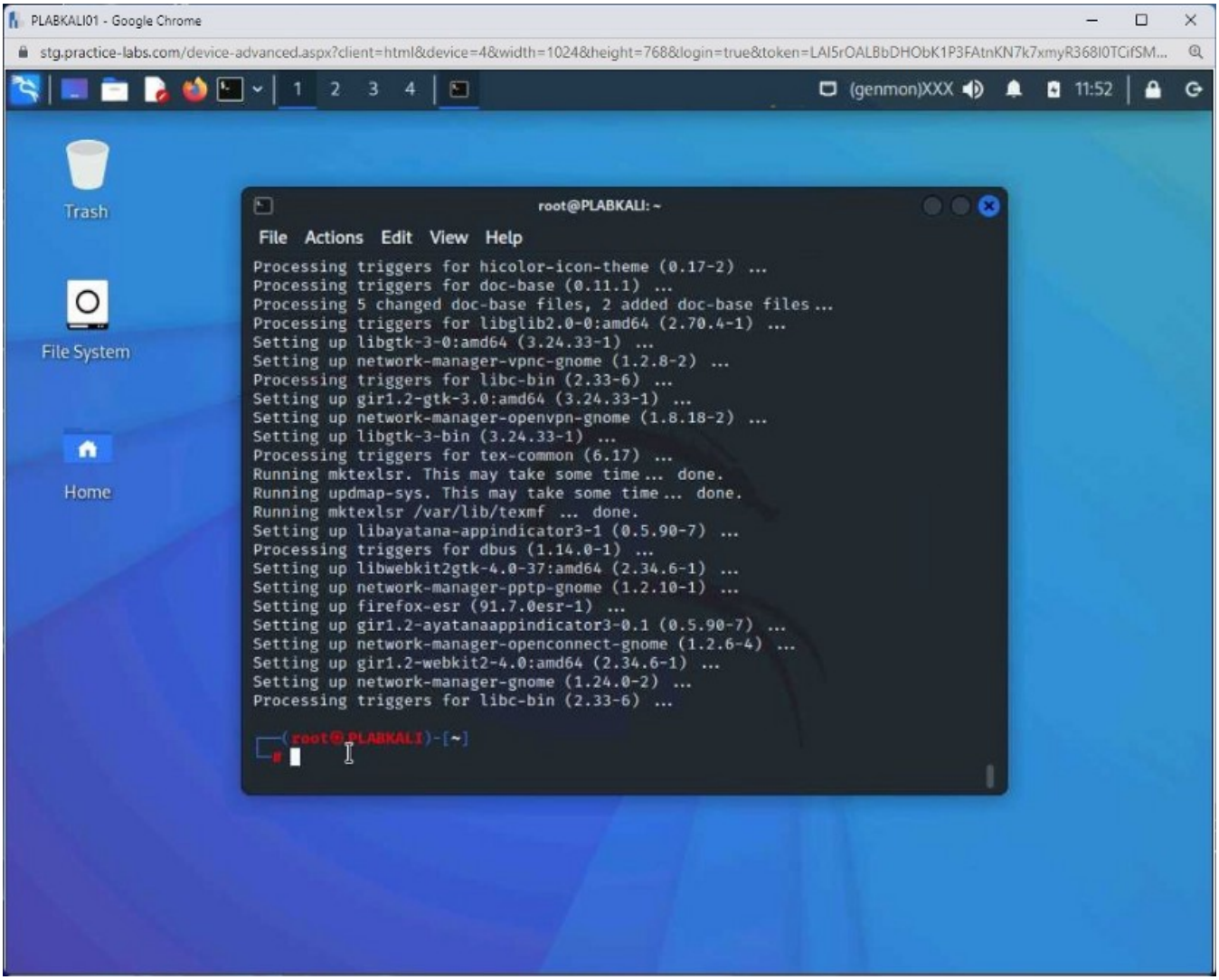
Depending on the upgraded, installed, or removed packages, it may take a while to complete this process.




**Step 4**

The entire process takes a long time to execute. Therefore, you can press **Ctrl** + **C** to terminate the process if you are running out of time.

If you have time remaining in the lab, you can continue to let the process run.


PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=LAI5rOALBbDHObK1P3FAtnKN7k7xmyR368I0TCifSM...
1 2 3 4
(genmon)XXX
11:52
Trash
File System
Home
root@PLABKALI: ~
File Actions Edit View Help
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for doc-base (0.11.1) ...
Processing 5 changed doc-base files, 2 added doc-base files ...
Processing triggers for libglib2.0-0:amd64 (2.70.4-1) ...
Setting up libgtk-3-0:amd64 (3.24.33-1) ...
Setting up network-manager-vpnc-gnome (1.2.8-2) ...
Processing triggers for libc-bin (2.33-6) ...
Setting up gir1.2-gtk-3.0:amd64 (3.24.33-1) ...
Setting up network-manager-openvpn-gnome (1.8.18-2) ...
Setting up libgtk-3-bin (3.24.33-1) ...
Processing triggers for tex-common (6.17) ...
Running mktexlsr. This may take some time ... done.
Running updmap-sys. This may take some time ... done.
Running mktexlsr /var/lib/texmf ... done.
Setting up libayatana-appindicator3-1 (0.5.90-7) ...
Processing triggers for dbus (1.14.0-1) ...
Setting up libwebkit2gtk-4.0-37:amd64 (2.34.6-1) ...
Setting up network-manager-pptp-gnome (1.2.10-1) ...
Setting up firefox-esr (91.7.0esr-1) ...
Setting up gir1.2-ayatanaappindicator3-0.1 (0.5.90-7) ...
Setting up network-manager-openconnect-gnome (1.2.6-4) ...
Setting up gir1.2-webkit2-4.0:amd64 (2.34.6-1) ...
Setting up network-manager-gnome (1.24.0-2) ...
Processing triggers for libc-bin (2.33-6) ...
(root@PLABKALI)-[~]