CEH v12 Lesson 6 : System Hacking & Manipulation

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 — System Hacking Concepts
- Exercise 2- Performing Online Password Attacks
- Exercise 3 — Creating Standalone Payloads

After completing this module, you will be able to:

- Disable the Windows 10 Firewall
- Use Wordlists
- Use Hydra to Guess Usernames and Passwords

After completing this module, you have further knowledge of:

- Gaining Access
- Escalating Privileges
- Maintaining Access
- Covering Tracks

Lab Duration

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

Exercise 1 — System Hacking Concepts

Before an attacker performs system hacking, various tasks would have been performed. These tasks help the attacker get ready for the attack and pinpoint the loopholes or weaknesses that can be exploited. These are linear steps that need to be performed before the system hacking occurs.

Beyond the vulnerability analysis stage, the system hacking stage occurs. It includes various tasks, such as:

- Gaining access
- Escalating Privileges
- Maintaining Access
- Clearing Logs

As noted above, these stages occur linearly. The entire process is as shown in the exhibit below:

MaintainingAccessFootprintingScanningEnumerationVulnerabilityAnalysisGainingAccessEscalatingPrivilegesMaintainingAccessCoveringTracks

Figure 1.1 Diagram displaying all stages of exploitation; Footprinting, Scanning, Vulnerability Analysis, Gaining Access, Escalating Privileges, Maintaining Access and Covering Tracks.

You have learned about footprinting, scanning, enumeration, and vulnerability analysis in the previous modules. In this exercise, you will learn about the concepts from gaining access to clearing logs.

Learning Outcomes

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

- Gaining Access
- Escalating Privileges
- Maintaining Access
- Covering Tracks

Your Devices

This exercise contains supporting materials for **Ethical Hacker v11**.

Gaining Access

Before an attacker gets into a system, they perform the previous stages, namely:

1. Footprinting
2. Scanning
3. Enumeration
4. Vulnerability Analysis

By this time, the attacker has narrowed down not only on the target but also on what must be exploited.

An attacker uses various methods to gain access to the system. The information gathered in the previous stages is practiced in the password cracking and vulnerability exploitation methods.

Password Cracking

An attacker employs various methods to gain access to the user credentials. In some cases, an attacker uses simple methods like social engineering.

After cracking a password, an attacker can perform privilege escalation to access the accounts with higher privileges. Typically, an attacker does not target the accounts that have administrative privileges because it may raise alarms if there are suspicious administrative activities — therefore, it is more desirable in most cases to focus on a regular user account.

There are various methods of password cracking.

- **Non-electric**: The attacker does not require technical knowledge. Examples are shoulder surfing, social engineering, and dumpster diving.
- **Active Online**: The attacker has an active connection with the target system to crack the passwords. Examples are dictionary, brute-force, hash injection, malware, Kerberos cracking, and password guessing.
- **Passive Online**: The attacker does not actively connect with the target. Examples are wire sniffing, Man-in-the-middle, and replay attacks.
- **Offline**: The uses a file containing passwords to conduct the attack. Examples are rainbow tables and distributed network attacks.

Vulnerability Exploitation

For vulnerability exploitation, an attacker finds vulnerabilities and explores the opportunity to exploit the vulnerability that can easily get the attacker into the system.

For example, It could be a SQL-based vulnerability that can lead to SQL Injection or a buffer-related vulnerability, such as buffer overflow — in which case an attacker can send a lot of data into the buffer to crash the application.

The core intent of vulnerability exploitation is to gain access to the system.

Escalating Privileges

After gaining access to a system, an attacker escalates privilege by exploiting vulnerabilities within applications or operating systems.

Privilege escalation can be of two types:

- **Horizontal**: an attacker gains another user's privileges with the same privileges as the compromised user.
- **Vertical**: an attacker gains the privileges of another user who has higher access to a system.

Privilege escalation can be performed using various methods, such as:

- Exploiting the misconfigured services
- Performing named pipe impersonation
- Exploiting the Spectre and Meltdown CPU vulnerabilities
- Conducting the Dylib hijacking attack
- Performing DLL hijacking
- Exploiting vulnerabilities
- Conducting path interception
- Executing malicious applications using scheduled tasks
- Exploiting incorrect permissions and privileges
- Using spoofed access tokens

- Misusing sudo privileges
- Exploiting kernel vulnerabilities

Maintaining Access

Once an attacker has access to a system, they want to maintain access to steal data or perform malicious activities inconspicuously.

Executing Applications

In this stage, an attacker can install trojans, spyware, rootkits, or even backdoors to give them access to a system and keep remote access. The goal is to remotely control the system to achieve a specific malicious objective, such as deleting or exfiltrating data or other disruptions to a system.

An attacker also uses various remote code execution methods. Some key methods include:

- **Exploitation for Client-Execution**: An attacker exploits various insecure software and exploits various vulnerabilities. Some of these applications are web browser-based, Office application-based, and third-party application-based.
- **Scheduled Task Exploitation**: An attacker schedules the malicious code in Linux and Windows systems. On a Linux system, the **at** command is used for scheduling the malicious code, and on a Windows system, the **schtasks** command is used.
- **Windows Management Instrumentation (WMI)-based**: An attacker uses WMI to gather system information and remotely interact with it.
- **Windows Remote Management (WinRM)**: An attacker uses the winrm command to execute the malicious code.
- **Service-based**: An attacker executes the malicious code to interact with the existing services. Alternatively, they can also execute code to start new malicious services that help maintain access.

Hiding Files

Once an attacker has gained access, they may steal information using steganography or maintain access by installing rootkits or using NTFS streams. To explain these terms in more detail:

- **Rootkits**: are programs that are installed on the target system. An attacker gets unlimited access to the system and administrative privileges with a rootkit. It exploits an operating system and application vulnerabilities and hides them by modifying the kernel and system files. By hiding itself, a rootkit can evade antimalware applications.
- **NTFS Streams**: NTFS Alternate Data Streams (ADS) store a file's metadata on a Windows system. An attacker can use ADS to inject malicious code into the files. Injecting ADS into the files does not modify the file, its size, or functionality. Therefore, the users do not see the change in ADS.
- **Steganography**: is about hiding data in different formats other than their original formats. For example, the attacker can hide confidential data in a graphic file. When users see the file, they cannot determine if it contains confidential data. The data can be hidden in images, audio, video, and text formats. Whenever it is not possible to use encryption, steganography is a good option and can be considered an alternative in some cases.

Covering Tracks

Like any other criminals, attackers do not want to leave any clues or traces backtracked to them to avoid penalization. Because of this, they cover their tracks by using various methods such as:

- **Disabling auditing**: when an attacker gets into a system, they can disable auditing. An attacker can use tools like Auditpol, a part of Windows. When auditing is disabled, no events will be logged.
- **Clearing logs**: this is the first place where a security administrator would check after a verified attack. Therefore, the attacker will likely remove all logs before exiting a system following an attack. The attacker can use tools like **wevtutil**, which is part of Windows. In a Linux system, you can clear all logs in the **/var/log** directories.
- **Covering tracks on the network**: an attacker uses various methods to cover a network, such as reverse HTTP shells and the reverse ICMP tunnels.
- **Covering tracks on the system**: an attacker uses NTFS streams to hide the malicious files to avoid being tracked by antimalware applications.

- **Using cipher.exe to delete text**: an attacker can remove sensitive data from a system using tools like cipher.exe. Once deleted, then data cannot be recovered.
- **Disabling Windows functionality**: before exiting the system after an attack, an attacker can delete volatile information by disabling the virtual memory. They can also utilize system restore points to allow a system to revert to its previous functional state — leaving no trace of the attack.

Exercise 2- Performing Online Password Attacks

An online password attack is performed on network services, such as SSH, HTTP, FTP, SMB, etc. Most of the time, servers or network devices are not equipped to block an online password attack. Therefore, these attacks can succeed without much effort. For example, an attacker might guess a user's password from a website login.

Password attacks can be of two types. The first type is the dictionary attack, which uses a list of common words. It continues to run through the list until a suitable match is found. On the other hand, a brute-force attack uses words based on a given character set. With an online password attack, either one of the methods can be used. However, a dictionary attack is mostly the choice because of the slow speed of the attack.

In this exercise, you will learn about performing an online password attack.

Disclaimer: The tools and techniques displayed in these exercises are to be used for the greater good of improving network security. Please do not use these techniques for malicious activities. Usage of all tools for attacking targets without prior mutual consent is illegal. Practice Labs assume no liability for any misuse or damage caused if these tools and techniques are used for malevolent activities.

Learning Outcomes

After completing this exercise, you will be able to:

- Disable the Windows 10 Firewall
- Use Wordlists
- Use Hydra to Guess Usernames and Passwords

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

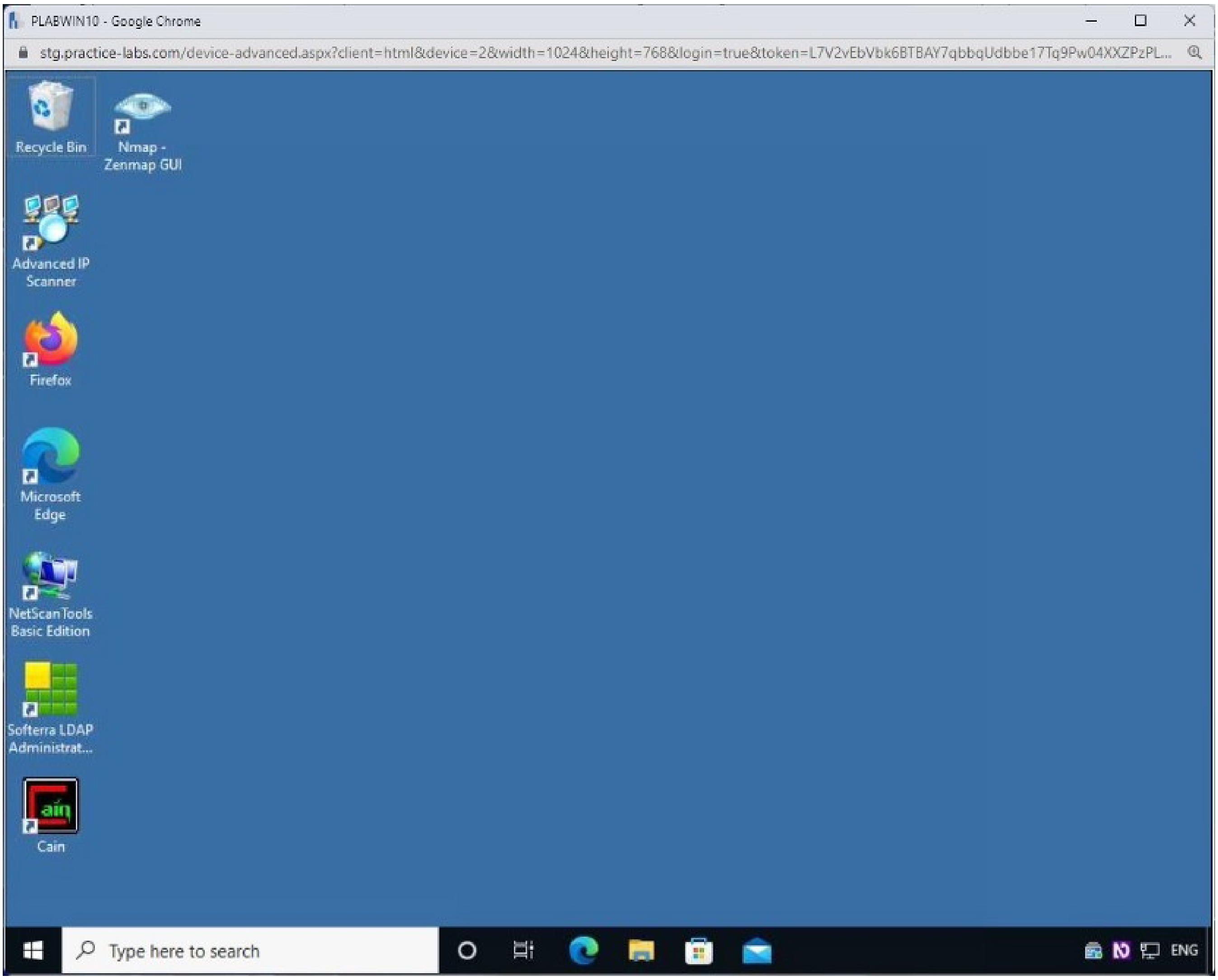
Task 1 — Disabling the Windows 10 Firewall

You will need to switch off the **Windows Firewall** to perform an attack on **PLABWIN10**. You can use attacking methods to bypass the Windows or any other firewall running on the target. However, for the sake of this module, you will switch off the Windows Firewall and proceed with the remaining tasks.

To switch off the **Windows Firewall** on **PLABWIN10**, perform the following steps:

Step 1

Ensure that you have connected to **PLABWIN10**. The desktop is displayed.

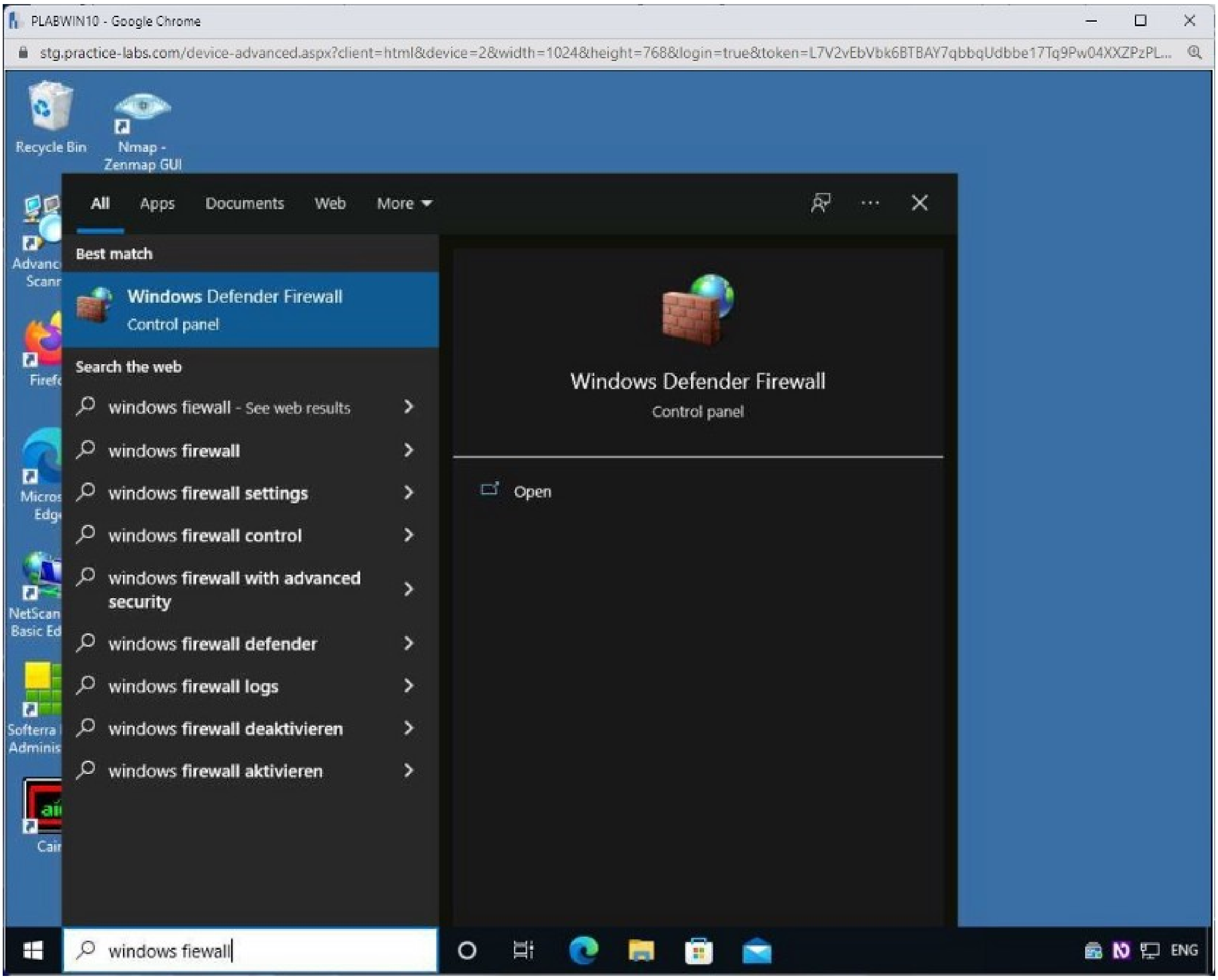

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=L7V2vEbVbk6BTBAY7qbbqUdbbe17Tq9Pw04XXZPzPL...
Recycle Bin
Nmap - Zenmap GUI
Advanced IP Scanner
Firefox
Microsoft Edge
NetScanTools Basic Edition
Softerra LDAP Administrat...
Cain
Type here to search
ENG

Step 2

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

```
windows firewall
```

From the search results, select the **Windows Defender Firewall**.

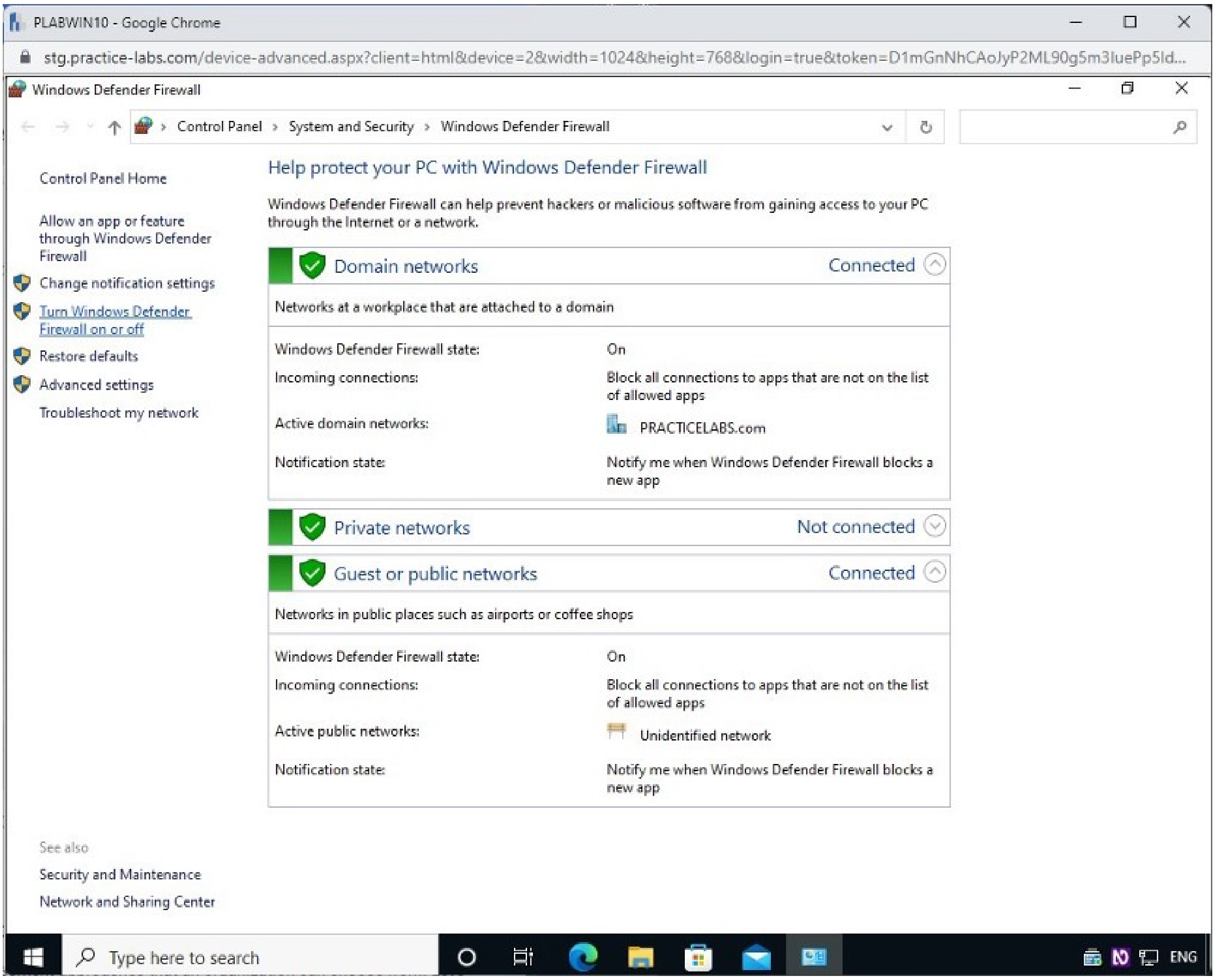

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=L7V2vEbVbk6BTBAY7qbbqUdbbe17Tq9Pw04XXZPzPL...
Recycle Bin
Nmap - Zenmap GUI
All
Apps
Documents
Web
More
Best match
Windows Defender Firewall
Control panel
Search the web
windows fiewall - See web results
windows firewall
windows firewall settings
windows firewall control
windows firewall with advanced security
windows firewall defender
windows firewall logs
windows firewall deaktivieren
windows firewall aktivieren
Windows Defender Firewall
Control panel
Open
ENG

windows fiewall

Step 3

The **Windows Defender Firewall** window is displayed.

On the **Help protect your PC with Windows Defender Firewall** page, click **Turn Windows Defender Firewall on or off** in the left-hand pane.



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5Id...

Windows Defender Firewall

Control Panel > System and Security > Windows Defender Firewall

Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center
Type here to search
ENG

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Domain networks — Connected

Networks at a workplace that are attached to a domain

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active domain networks:	PRACTICELABS.com
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Private networks — Not connected

Guest or public networks — Connected

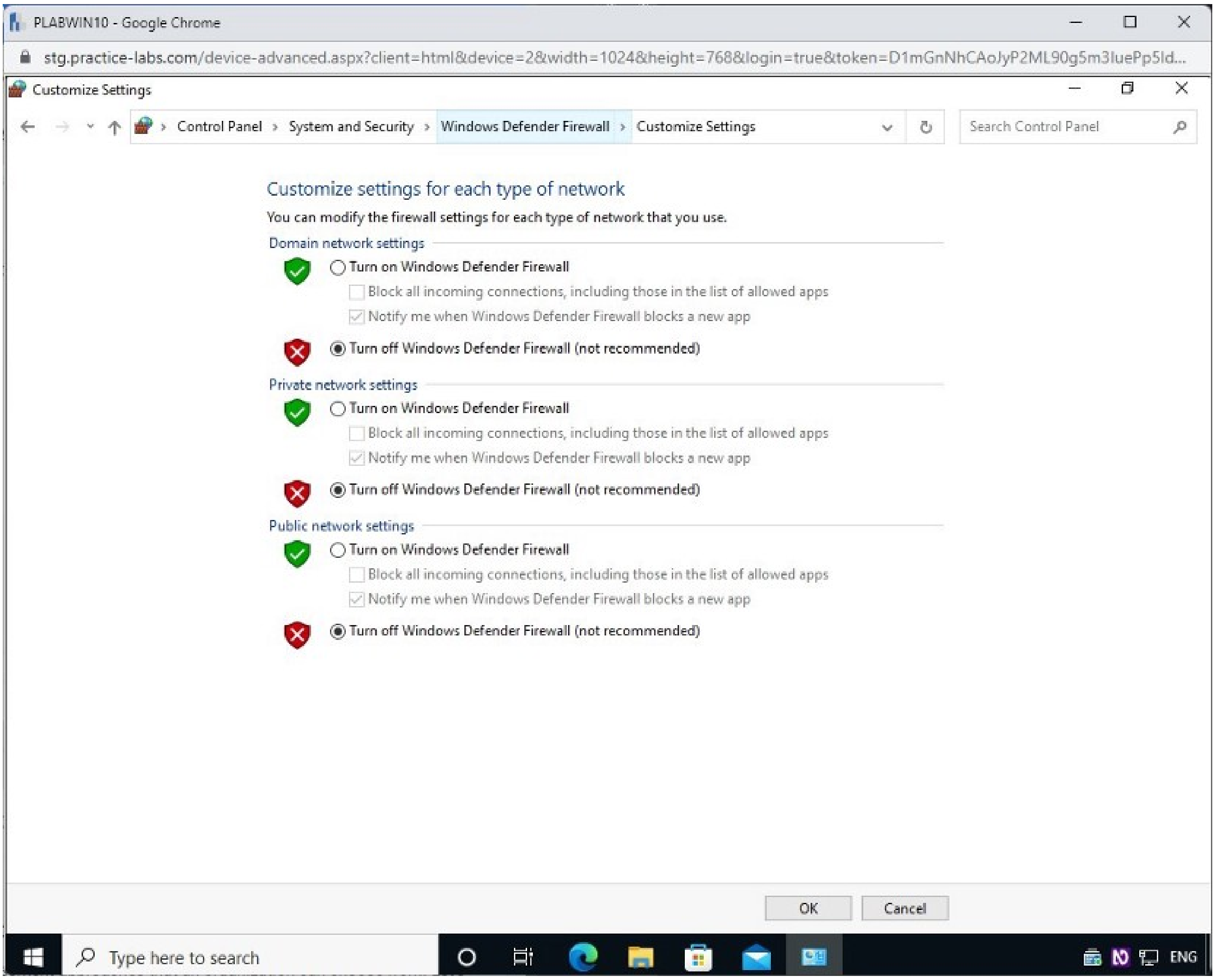
Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Unidentified network
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Step 4

On the **Customize settings for each type of network** page, select **Turn off Windows Defender Firewall (not recommended)** for **Domain**, **Private**, and **Public** network.

Click **OK**.



PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5Id...
Customize Settings
Control Panel > System and Security > Windows Defender Firewall > Customize Settings
Search Control Panel
OK
Cancel
Type here to search
ENG

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Domain network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Private network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Public network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

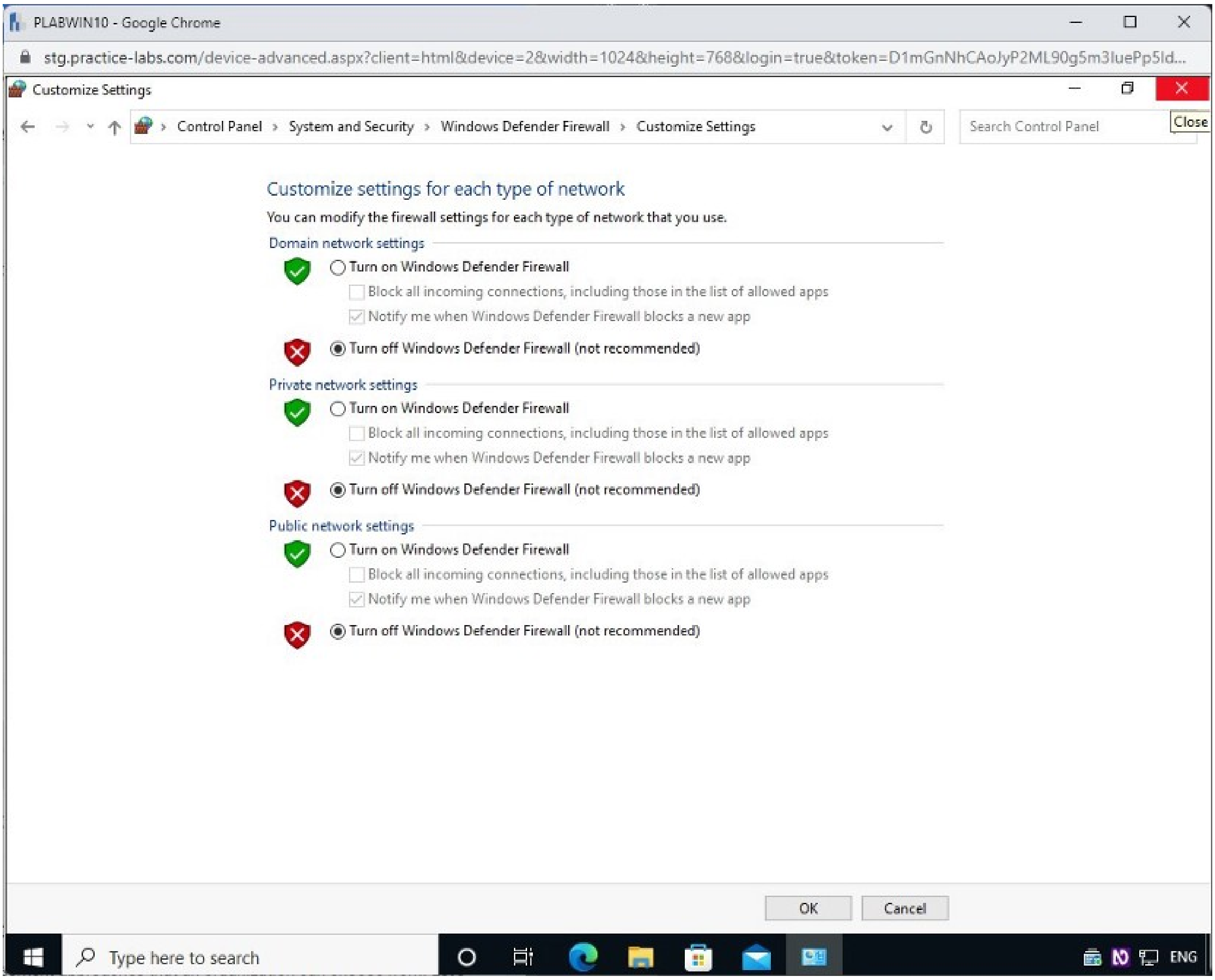
☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Step 5

On the **Help protect your PC with Windows Defender Firewall** page, notice that **Windows Defender Firewall** is now turned off for **Domain**, **Private**, and **Public** networks.

Close the **Control Panel** window.



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5ld...

Customize Settings

Control Panel › System and Security › Windows Defender Firewall › Customize Settings

Search Control Panel

Close

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Domain network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Private network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Public network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

OK Cancel

Type here to search

ENG

Task 2 — Using Wordlists

In a dictionary attack, a list of words known as wordlist is pre-defined and used to match against the victim’s password. There are ready-made password lists available on the Internet that contain generic and popular less secure passwords.

A password list can be a few bytes large, or it can also be gigabytes — as the more words in a password file, the bigger the size. If you do not intend to use a pre-defined wordlist, you can create your own. Some tools are available that can help you create a wordlist. Some of the tools that are used commonly are:

- **Wyd**: Password Profiling Tool
- **Crunch**: Password Cracking Wordlist Generator
- **CeWL**: Password Cracking Custom Word List Generator
- **RSMangler**: Keyword Based Wordlist Generator for Brute forcing

In this task, you will learn about the wordlists.

Step 1

Connect to **PLABKALI01**.

Log in using the following credentials:

Username:

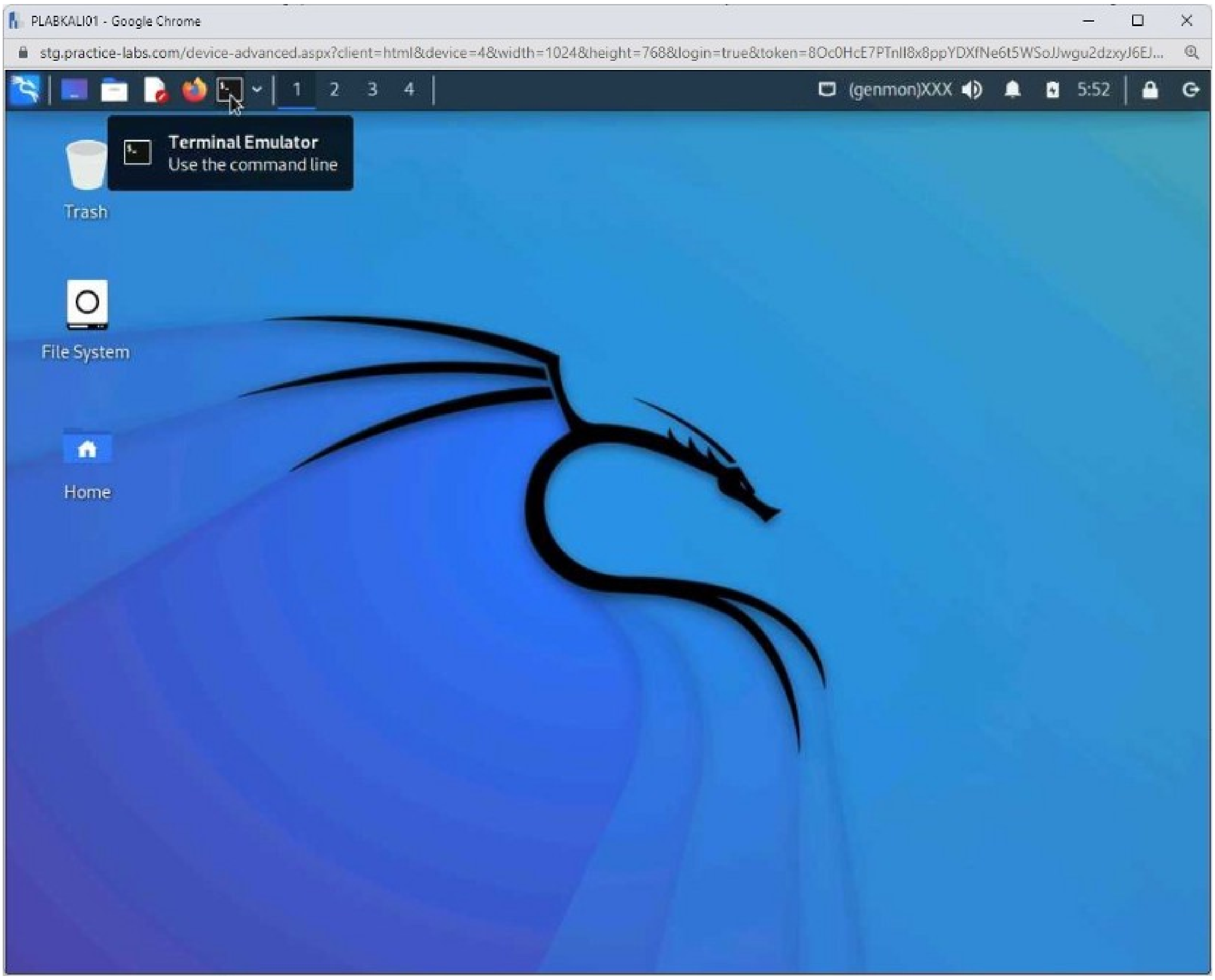
```
root
```

Password:

Passw0rd

The desktop of **PLABKALI01** is displayed.

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

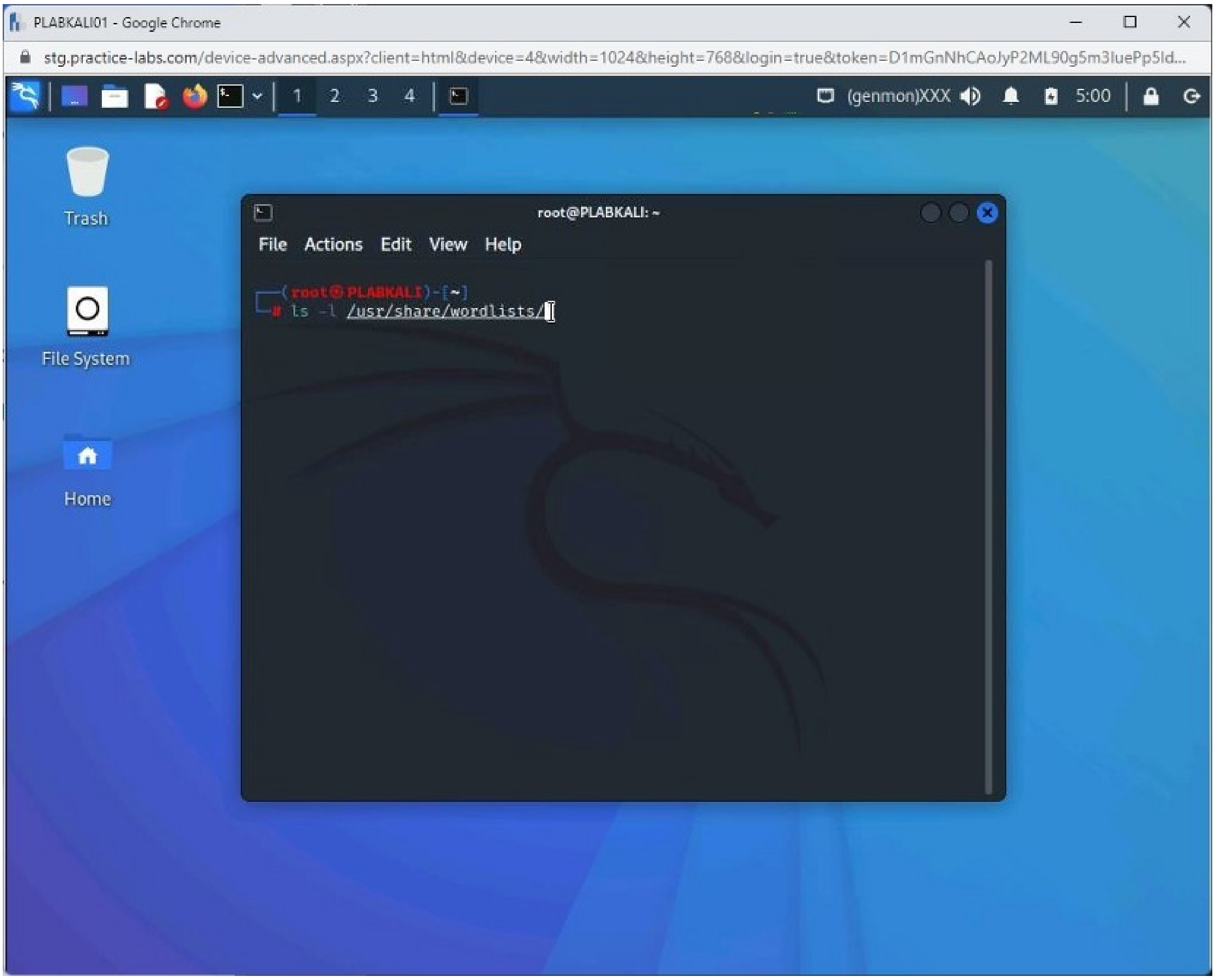

PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=8Oc0HcE7PTnlI8x8ppYDXfNe6t5WSoJwgu2dzxyJ6EJ...
1
2
3
4
(genmon)XXX
5:52
Terminal Emulator
Use the command line
Trash
File System
Home

Step 2

The **Terminal** window is displayed. First, let’s look at the pre-defined wordlists available in Kali Linux. To do this, type the following command:

```
ls -l /usr/share/wordlists/
```

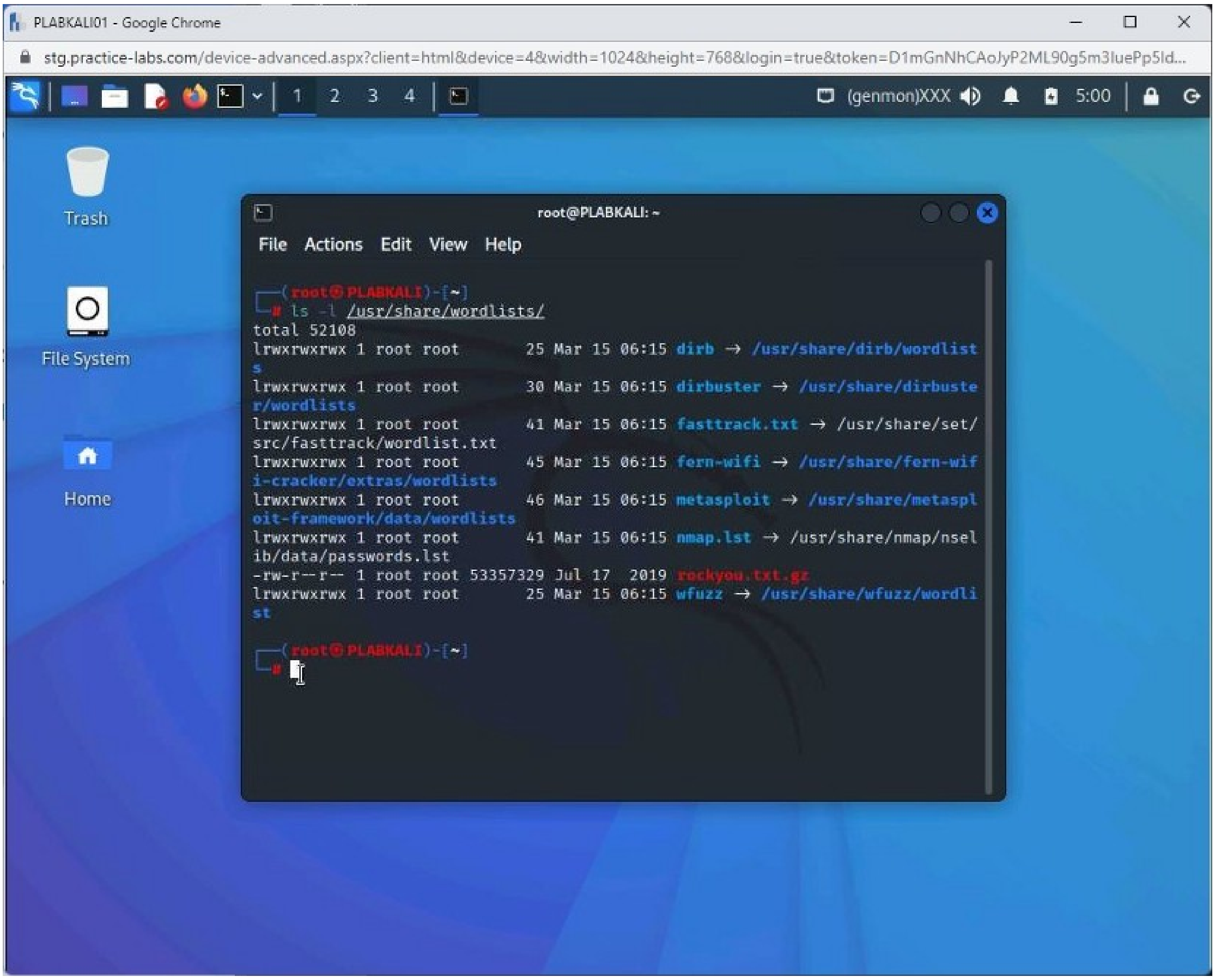
Press **Enter**.


PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5Id...
1
2
3
4
(genmon)XXX
5:00
Trash
File System
Home
root@PLABKALI: ~
File
Actions
Edit
View
Help

```
┌──(root㉿PLABKALI)-[~]
└─# ls -l /usr/share/wordlists/
```

Step 3

Notice that several wordlist files are displayed.



PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5ld...
1 2 3 4
(genmon)XXX 5:00
Trash
File System
Home
root@PLABKALI: ~
File Actions Edit View Help

```
┌──(root㉿PLABKALI)-[~]
└─# ls -l /usr/share/wordlists/
total 52108
lrwxrwxrwx 1 root root       25 Mar 15 06:15 dirb → /usr/share/dirb/wordlist
s
lrwxrwxrwx 1 root root       30 Mar 15 06:15 dirbuster → /usr/share/dirbuste
r/wordlists
lrwxrwxrwx 1 root root       41 Mar 15 06:15 fasttrack.txt → /usr/share/set/
src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root       45 Mar 15 06:15 fern-wifi → /usr/share/fern-wif
i-cracker/extras/wordlists
lrwxrwxrwx 1 root root       46 Mar 15 06:15 metasploit → /usr/share/metaspl
oit-framework/data/wordlists
lrwxrwxrwx 1 root root       41 Mar 15 06:15 nmap.lst → /usr/share/nmap/nsel
ib/data/passwords.lst
-rw-r--r-- 1 root root 53357329 Jul 17  2019 rockyou.txt.gz
lrwxrwxrwx 1 root root       25 Mar 15 06:15 wfuzz → /usr/share/wfuzz/wordli
st

┌──(root㉿PLABKALI)-[~]
└─#
```

Step 4

Clear the screen by entering the following command:

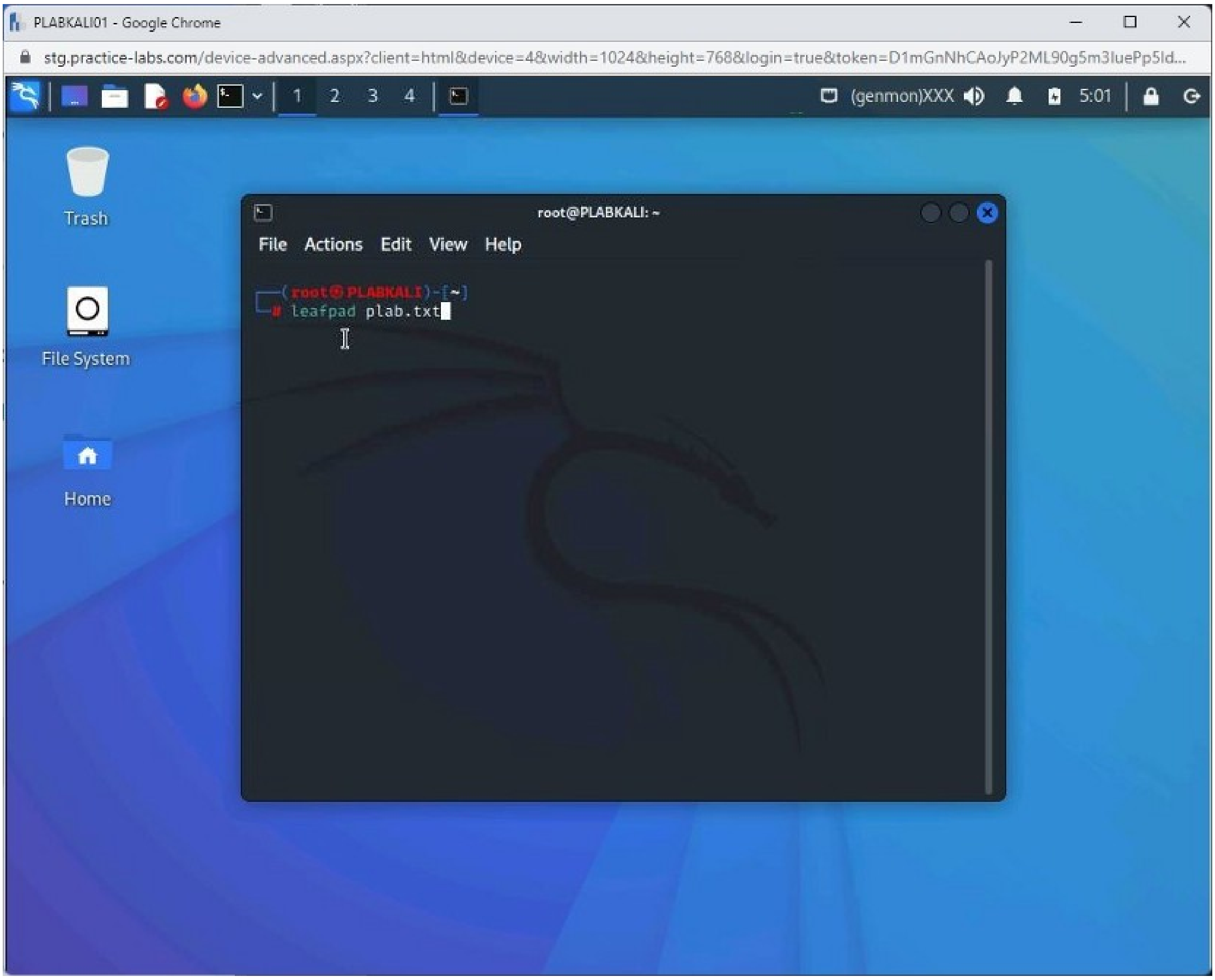
```
clear
```

Press **Enter**.

You can use a pre-defined wordlist, but for the purposes of this demonstration, we will create our own.

```
leafpad plab.txt
```

Press **Enter**.



PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5ld...
1 2 3 4
(genmon)XXX 5:01
Trash
File System
Home
root@PLABKALI: ~
File Actions Edit View Help

```
┌──(root㉿PLABKALI)-[~]
└─# leafpad plab.txt
```

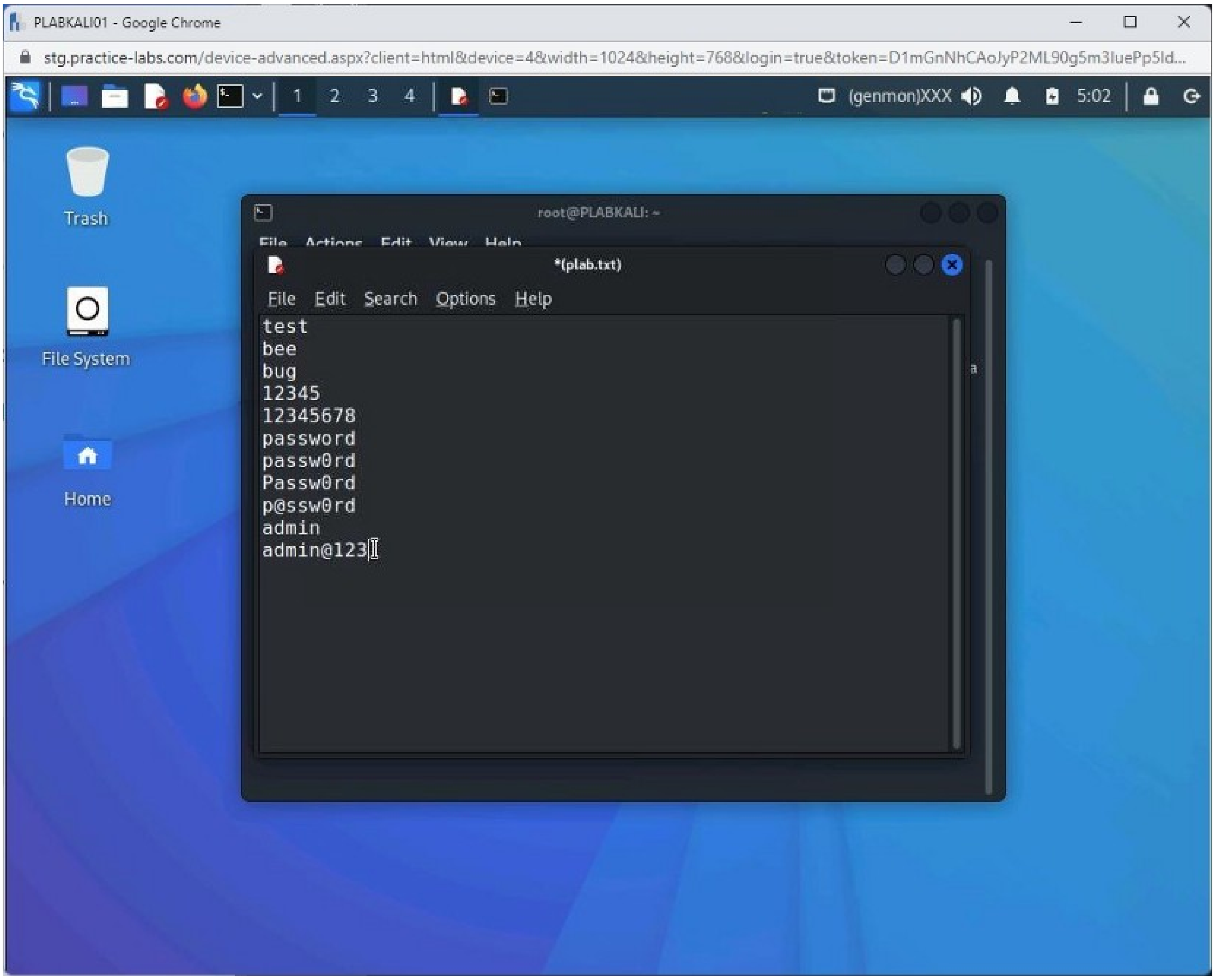
Step 5

Leafpad opens with a file named **(plab.txt**).

Type the following words:

```
test
bee
bug
12345
12345678
password
passw0rd
Passw0rd
p@ssw0rd
admin
admin@123
```

Press **Enter** after each word except the last one.



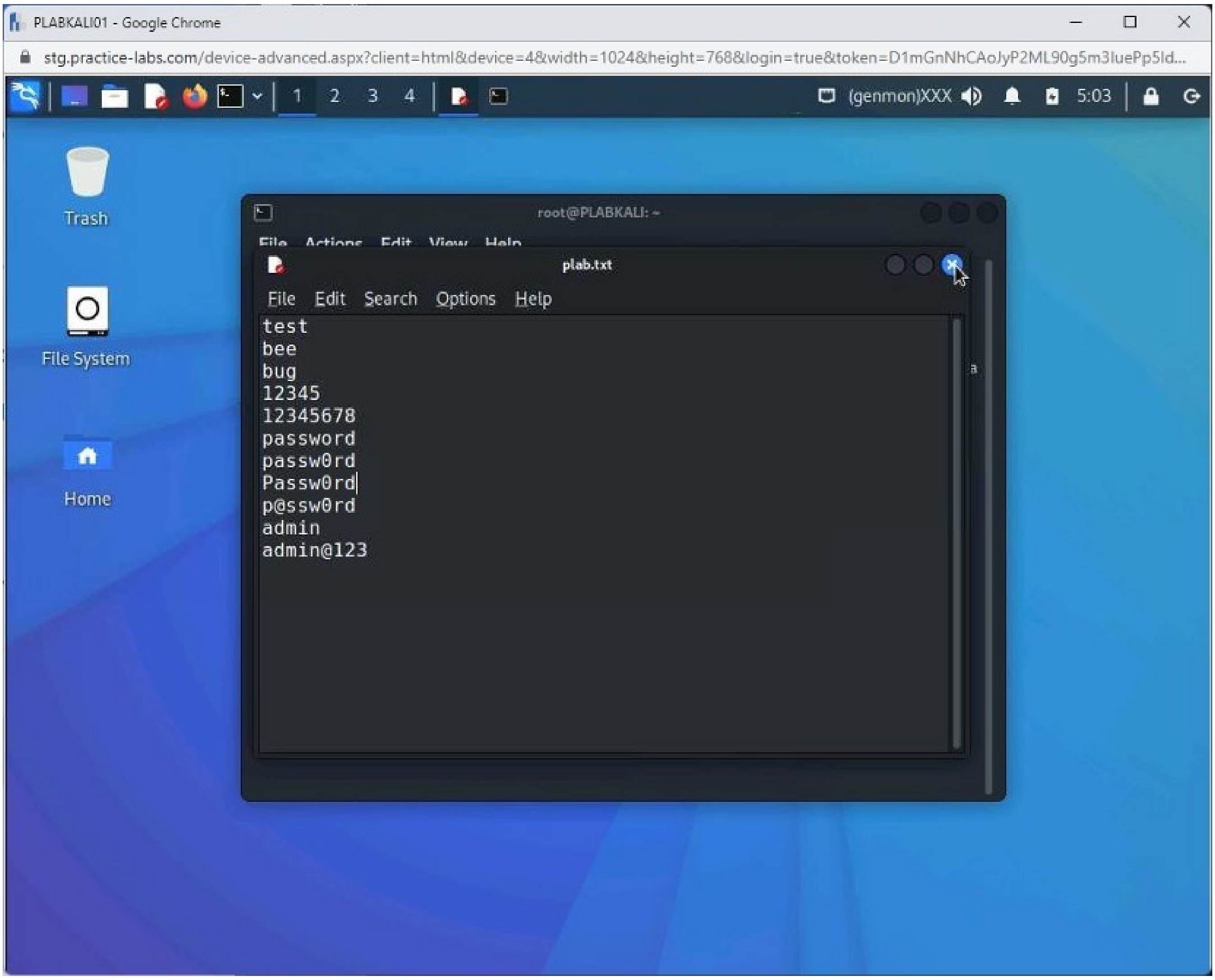
PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5ld...
(genmon)XXX
5:02
Trash
File System
Home
root@PLABKALI: ~
File Actions Edit View Help
*(plab.txt)
File Edit Search Options Help

```
test
bee
bug
12345
12345678
password
passw0rd
Passw0rd
p@ssw0rd
admin
admin@123
```

Step 6

Press **Ctrl + S** to save the file.

Close the **plab.txt** file.


PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5ld...
1 2 3 4
(genmon)XXX
5:03
Trash
File System
Home
root@PLABKALI: ~
File Actions Edit View Help
plab.txt
File Edit Search Options Help

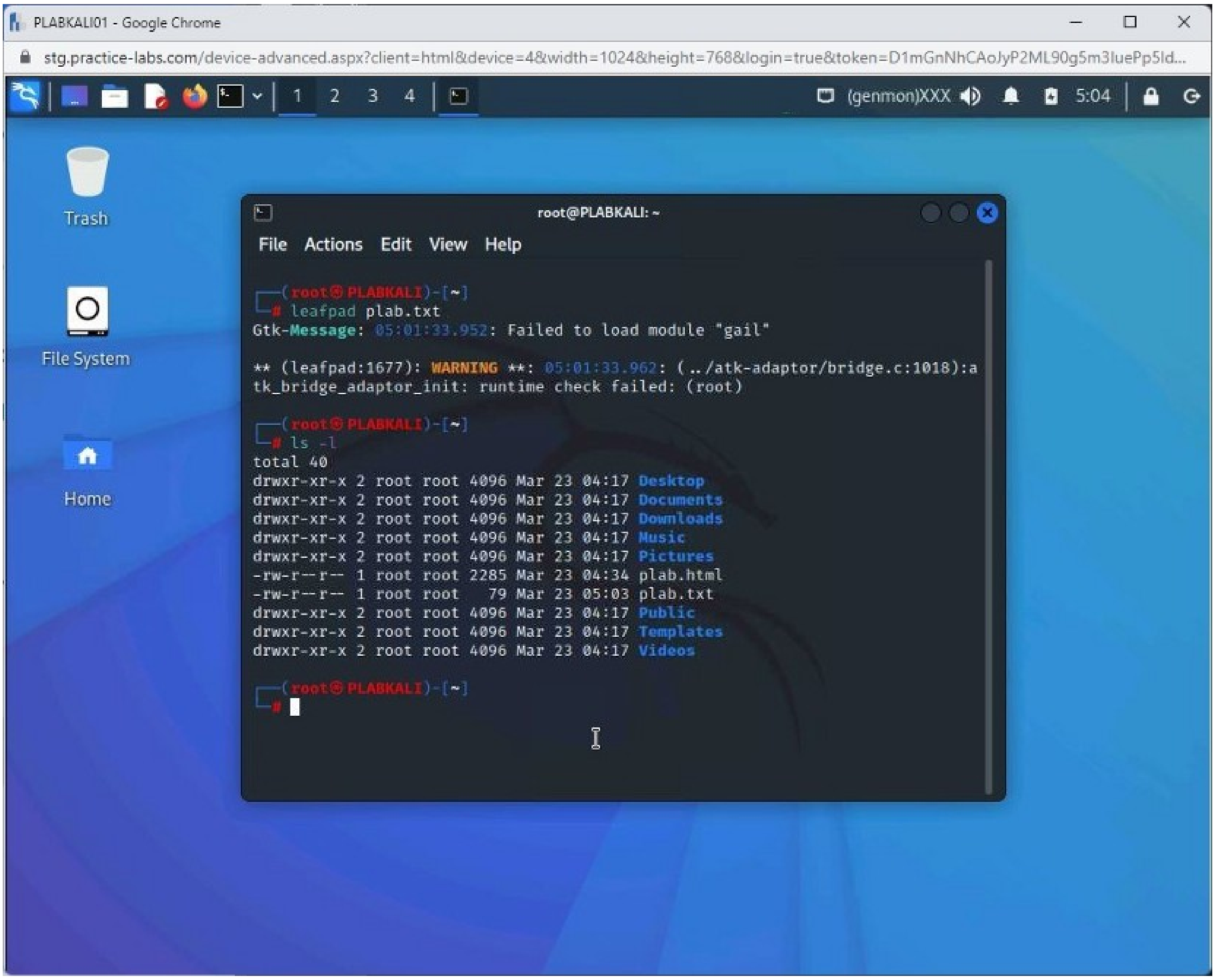
```
test
bee
bug
12345
12345678
password
passw0rd
Passw0rd
p@ssw0rd
admin
admin@123
```

Step 7

Let's verify if the **plab.txt** is created. Type the following command in the terminal window:

```
ls -l
```

Press **Enter**. Notice that the **plab.txt** file is created.


PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5Id...
1 2 3 4
(genmon)XXX 5:04
Trash
File System
Home
root@PLABKALI: ~
File Actions Edit View Help

```
┌──(root㉿PLABKALI)-[~]
└─# leafpad plab.txt
Gtk-Message: 05:01:33.952: Failed to load module "gail"

** (leafpad:1677): WARNING **: 05:01:33.962: (../atk-adaptor/bridge.c:1018):a
tk_bridge_adaptor_init: runtime check failed: (root)

┌──(root㉿PLABKALI)-[~]
└─# ls -l
total 40
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Desktop
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Documents
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Downloads
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Music
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Pictures
-rw-r--r-- 1 root root 2285 Mar 23 04:34 plab.html
-rw-r--r-- 1 root root   79 Mar 23 05:03 plab.txt
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Public
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Templates
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Videos

┌──(root㉿PLABKALI)-[~]
└─# 
```

Step 8

Clear the screen by entering the following command:

```
clear
```

Press **Enter**.

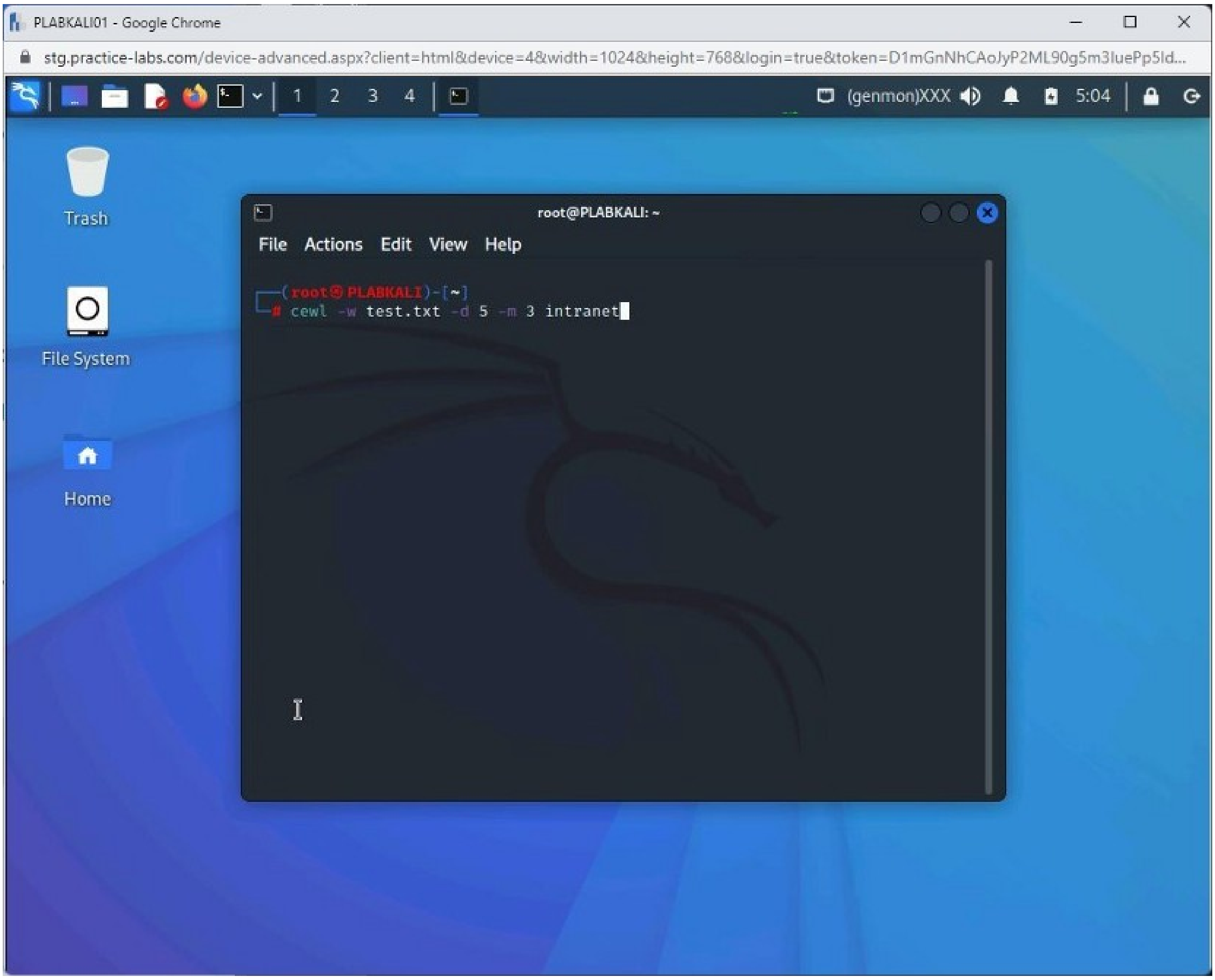
Kali contains a tool named **cewl**, which generates wordlists.

Type the following command:

Note: *The parameter -w defines the name of the wordlist. The -d parameter defines the depth of the search in a Website. The -m parameter defines the minimum word length.*

```
cewl -w test.txt -d 5 -m 3 intranet
```

Press **Enter**.

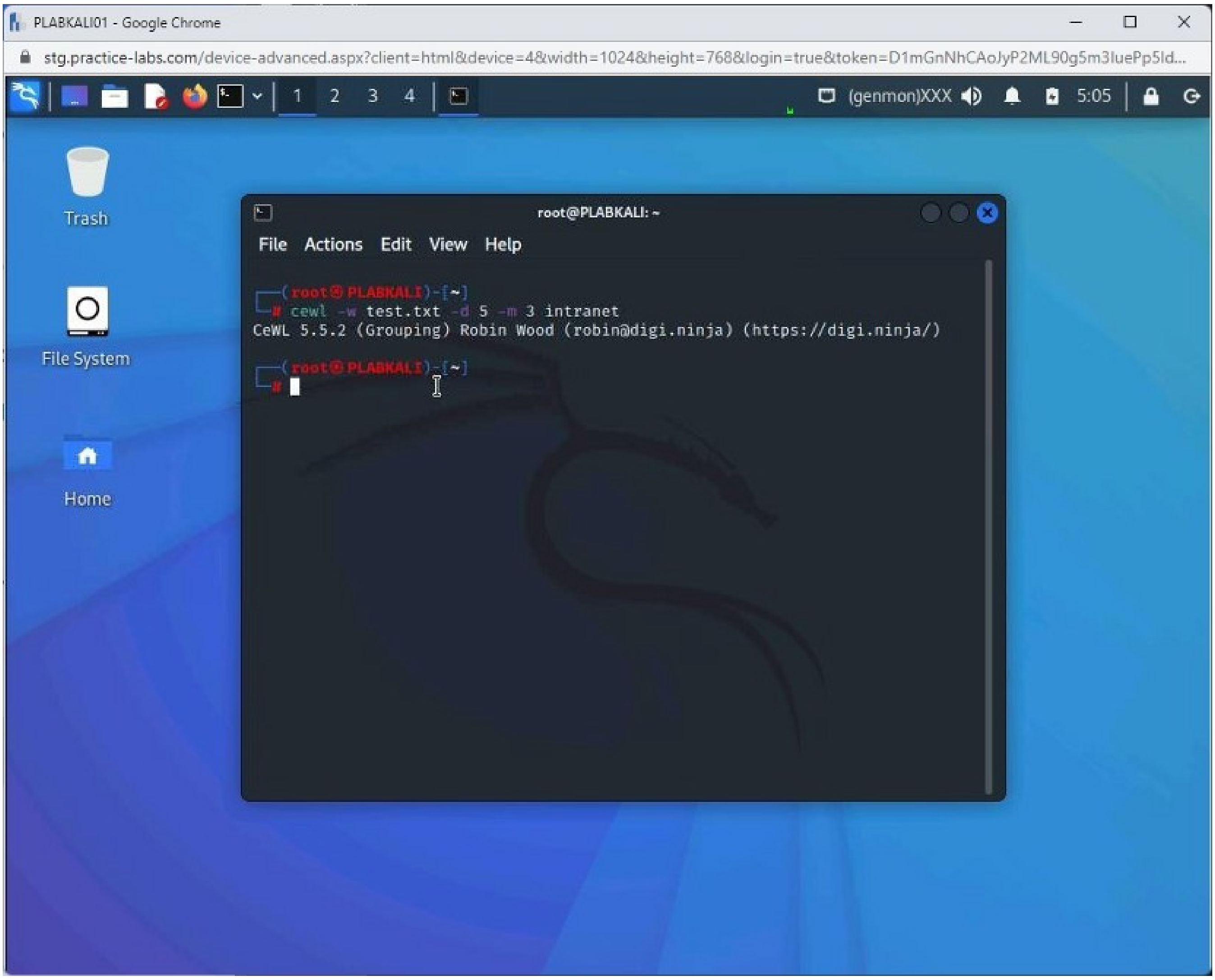


PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5Id...
1
2
3
4
(genmon)XXX
5:04
Trash
File System
Home
root@PLABKALI: ~
File
Actions
Edit
View
Help

```
┌──(root㉿PLABKALI)-[~]
└─# cewl -w test.txt -d 5 -m 3 intranet
```

Step 9

The command runs successfully without any error.



```
┌──(root㉿PLABKALI)-[~]
└─# cewl -w test.txt -d 5 -m 3 intranet
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

┌──(root㉿PLABKALI)-[~]
└─# 
```

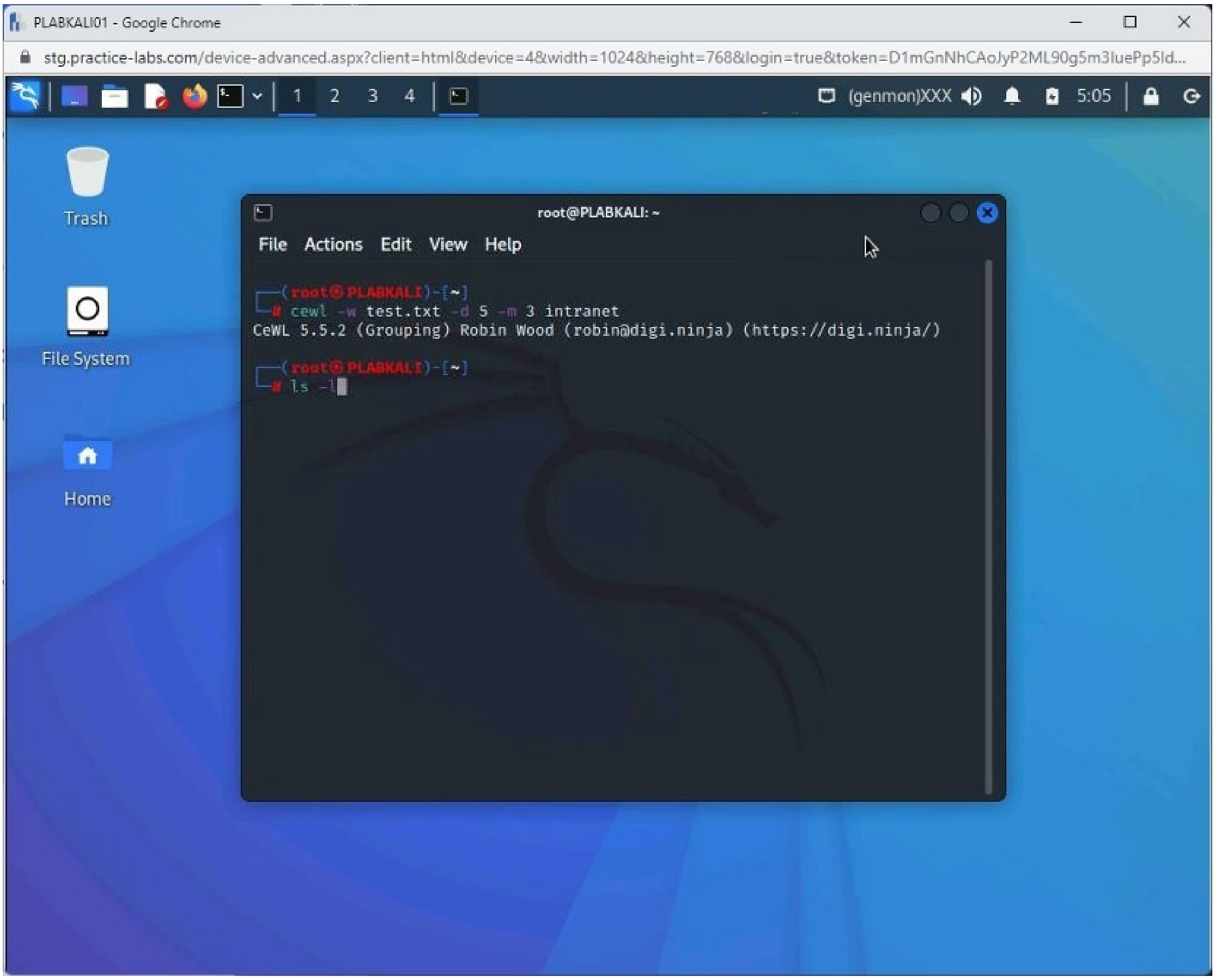
PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5ld...
(genmon)XXX
5:05
Trash
File System
Home
root@PLABKALI: ~
File Actions Edit View Help

Step 10

Let’s verify if the **test.txt** file has been created. Type the following command:

```
ls -l
```

Press **Enter**.



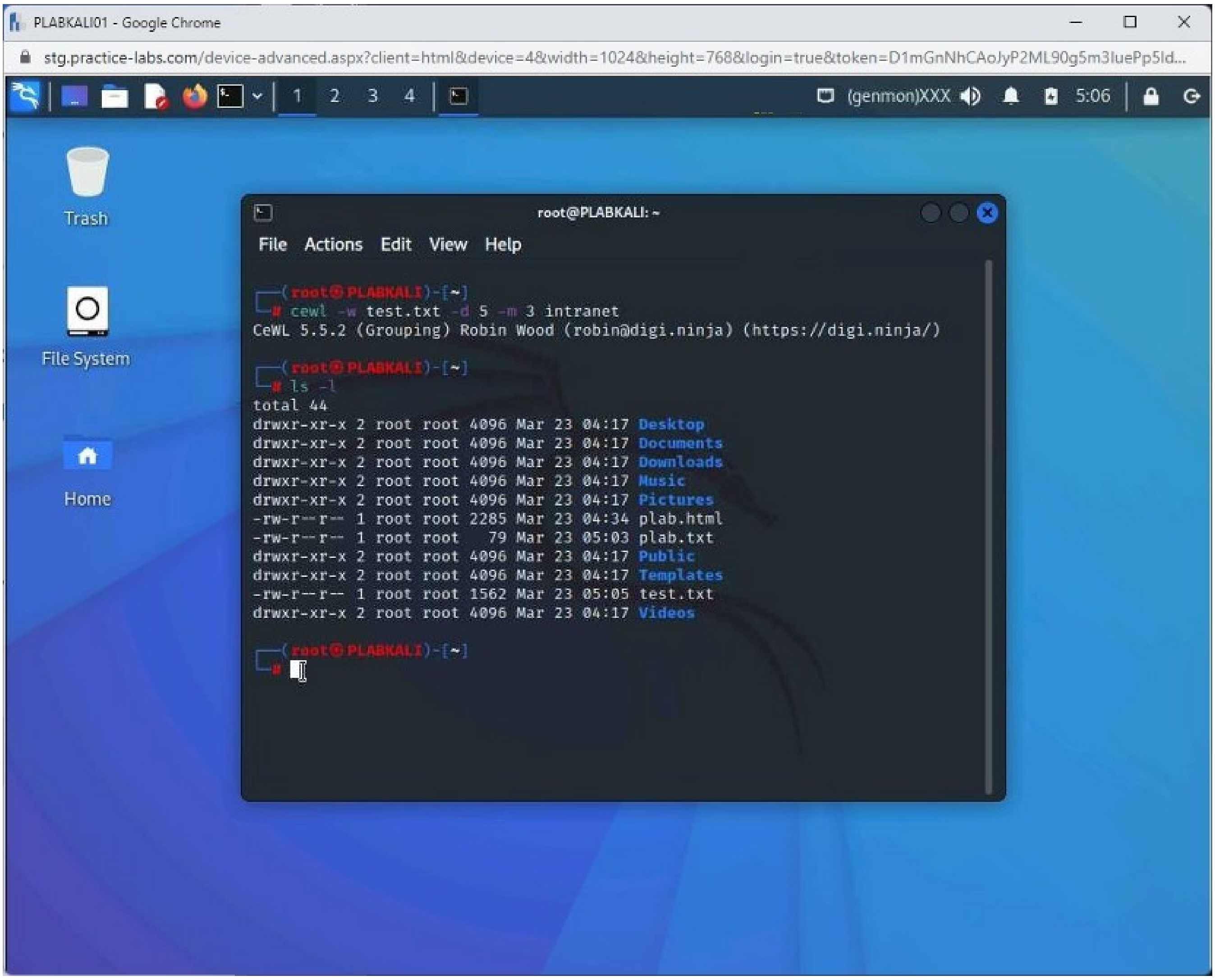
PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5ld...
1 2 3 4
(genmon)XXX 5:05
Trash
File System
Home
root@PLABKALI: ~
File Actions Edit View Help

```
┌──(root㉿PLABKALI)-[~]
└─# cewl -w test.txt -d 5 -m 3 intranet
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

┌──(root㉿PLABKALI)-[~]
└─# ls -l
```

Step 11

Notice that the **test.txt** file has been created.



PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5Id...
1 2 3 4
(genmon)XXX
5:06
Trash
File System
Home
root@PLABKALI: ~
File Actions Edit View Help

```
┌──(root㉿PLABKALI)-[~]
└─# cewl -w test.txt -d 5 -m 3 intranet
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

┌──(root㉿PLABKALI)-[~]
└─# ls -l
total 44
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Desktop
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Documents
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Downloads
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Music
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Pictures
-rw-r--r-- 1 root root 2285 Mar 23 04:34 plab.html
-rw-r--r-- 1 root root   79 Mar 23 05:03 plab.txt
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Public
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Templates
-rw-r--r-- 1 root root 1562 Mar 23 05:05 test.txt
drwxr-xr-x 2 root root 4096 Mar 23 04:17 Videos

┌──(root㉿PLABKALI)-[~]
└─# 
```

Step 12

Clear the screen by entering the following command:

```
clear
```

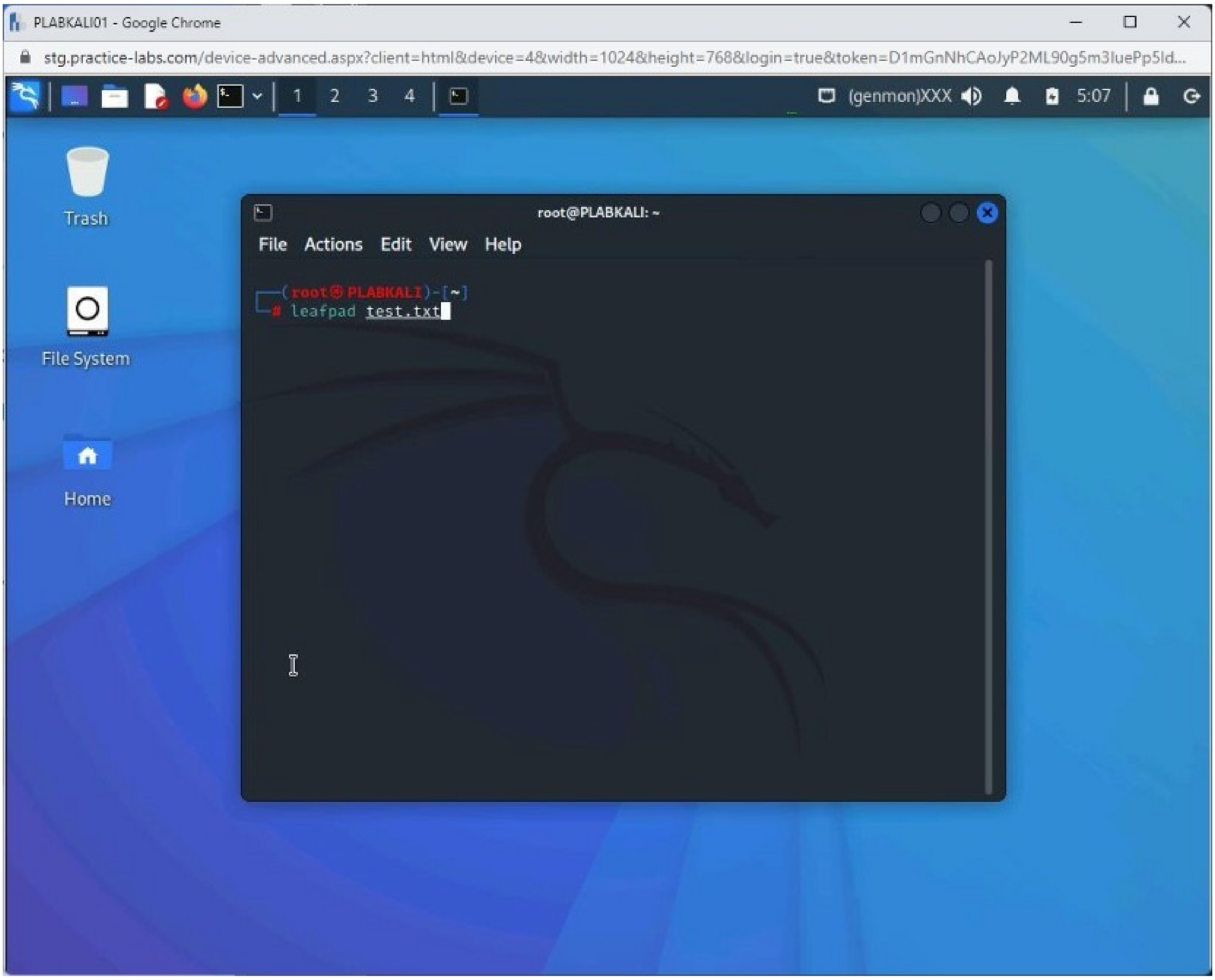
Press **Enter**.

Let’s open the **test.txt** file and see the stored words in it.

Type the following command:

```
leafpad test.txt
```

Press **Enter**.



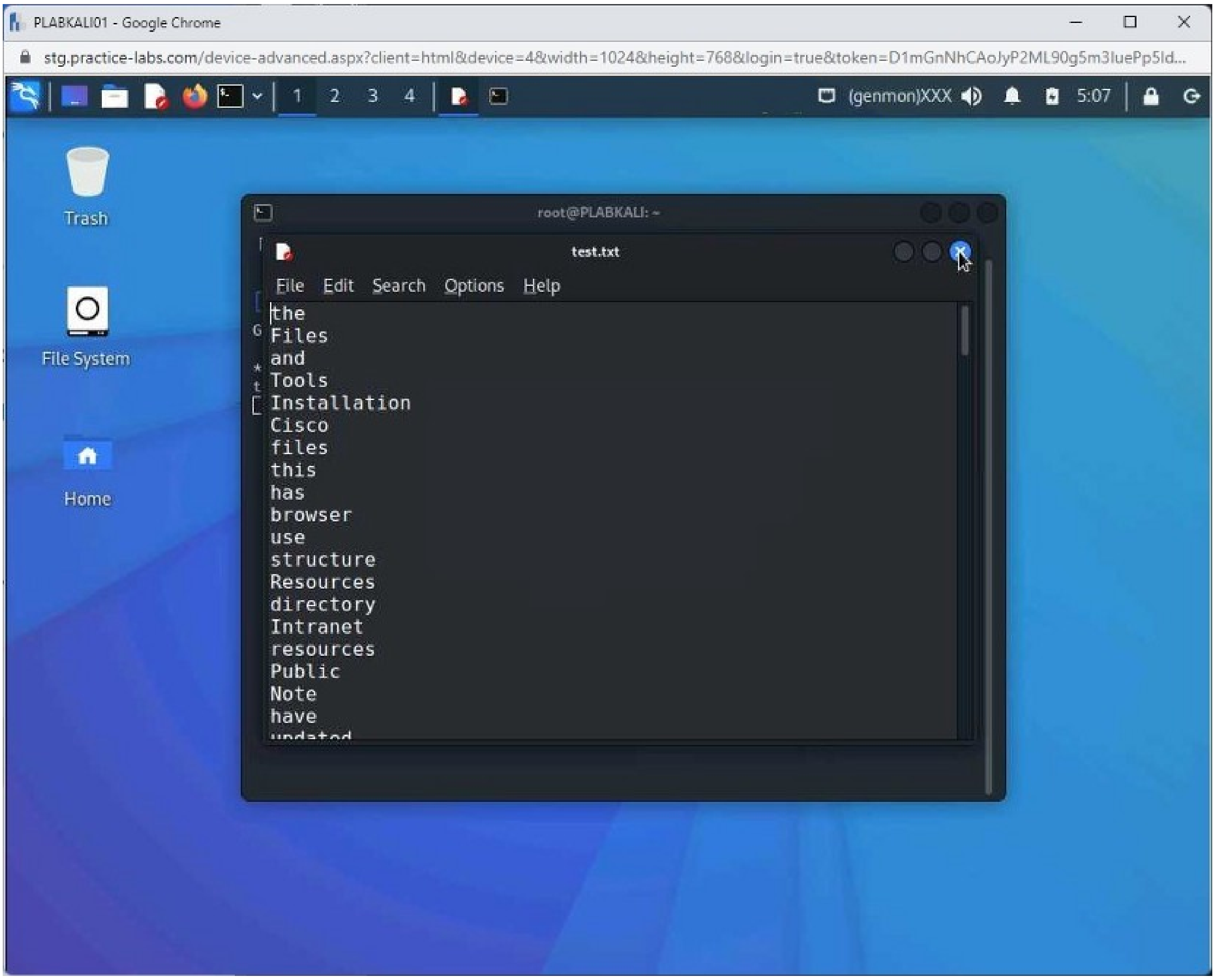
PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5Id...
1 2 3 4
(genmon)XXX 5:07
Trash
File System
Home
root@PLABKALI: ~
File Actions Edit View Help

```
┌──(root㉿PLABKALI)-[~]
└─# leafpad test.txt
```

Step 13

The **test.txt** file is now open. It has captured several words from the Intranet Website.

Close this file.


PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5Id...
1 2 3 4
(genmon)XXX
5:07
Trash
File System
Home
root@PLABKALI: ~
test.txt
File Edit Search Options Help

```
the
Files
and
Tools
Installation
Cisco
files
this
has
browser
use
structure
Resources
directory
Intranet
resources
Public
Note
have
updated
```

Keep the terminal window open.

Task 3 — Using Hydra to Guess Usernames and Passwords

Hydra is a tool that can perform dictionary attacks against several protocols, such as HTTP, FTP, SMB, SSH, etc. Hydra is designed to conduct attacks against authentication services, running using a protocol, such as HTTP.

In this task, you will use Hydra to guess usernames and passwords. To do this, perform the following steps:

Step 1

Connect to **PLABKALI01**. The command prompt window should be open.

Clear the screen by entering the following command:

```
clear
```

Press **Enter**.

Now, you will use **Hydra** to perform a dictionary attack using **plab.txt** that you had created.

Note: *In reality, the wordlist will never be so small, but for the sake of demonstration, we can use this wordlist.*

You have a vulnerable application, **bWAPP**, running on **192.168.0.10**. You will use the **plab.txt** file to perform a dictionary attack against this application. To do this, type the following command:

Note*: The hydra command takes the following parameters inputs:*

-t*: Defines the number of logins to try simultaneously.*

-V*: Displays each attempt of login and password.*

-f*: Stops the dictionary attack after a suitable match for username and password is found.*

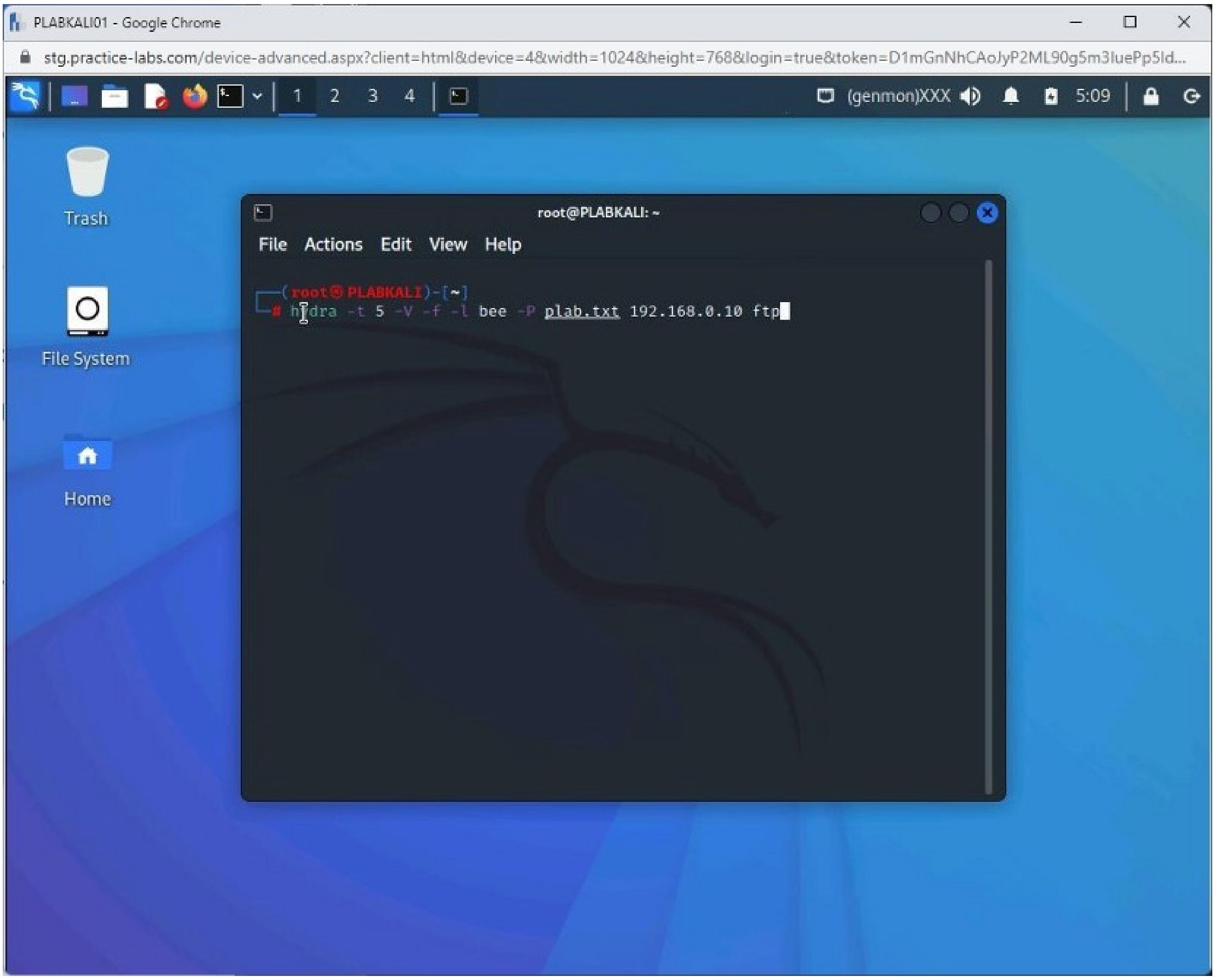
-l username*: Defines a username that needs to be cracked. If you do not know the username, you can use the -L parameter and provide a username list similar to a wordlist. For example, the bee was the username for the bWAPP application.*

-P *wordlist: Defines the wordlist containing probable passwords. You can use the -p parameter for a single password. The website name or IP address: Defines the Website name or IP address.*

Protocol*: Defines the services on which the dictionary attack is launched.*

```
hydra -t 5 -V -f -l bee -P plab.txt 192.168.0.10 ftp
```

Press **Enter**.


PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=D1mGnNhCAoJyP2ML90g5m3luePp5ld...
1 2 3 4
(genmon)XXX
5:09
Trash
File System
Home
root@PLABKALI: ~
File Actions Edit View Help

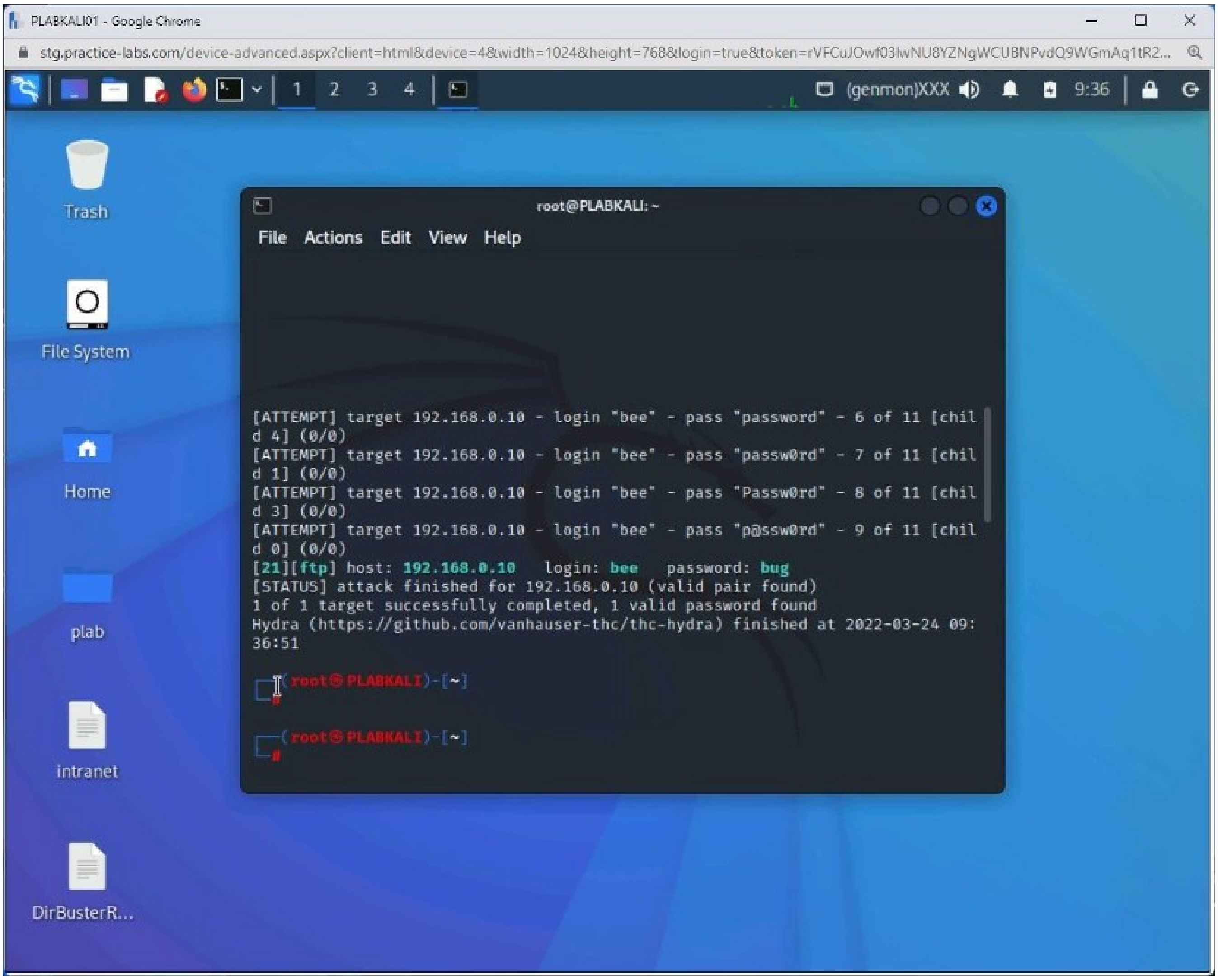
```
┌──(root㉿PLABKALI)-[~]
└─# hydra -t 5 -V -f -l bee -P plab.txt 192.168.0.10 ftp
```

Step 2

Let’s see if **Hydra** has been able to find out the password for the user, **bee**.

Note: *Depending on the size of the wordlist, the time to get the results will vary.*

Notice the text in green. You have been able to crack the password for this **FTP** service on the host, **192.168.0.10**.



PLABKALI01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=4&width=1024&height=768&login=true&token=rVFCuJOwf03IwNU8YZNgWCUBNPvdQ9WGmAq1tR2...
1
2
3
4
(genmon)XXX
9:36
Trash
File System
Home
plab
intranet
DirBusterR...
root@PLABKALI: ~
File
Actions
Edit
View
Help

```
[ATTEMPT] target 192.168.0.10 - login "bee" - pass "password" - 6 of 11 [chil
d 4] (0/0)
[ATTEMPT] target 192.168.0.10 - login "bee" - pass "passw0rd" - 7 of 11 [chil
d 1] (0/0)
[ATTEMPT] target 192.168.0.10 - login "bee" - pass "Passw0rd" - 8 of 11 [chil
d 3] (0/0)
[ATTEMPT] target 192.168.0.10 - login "bee" - pass "p@ssw0rd" - 9 of 11 [chil
d 0] (0/0)
[21][ftp] host: 192.168.0.10   login: bee   password: bug
[STATUS] attack finished for 192.168.0.10 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-24 09:
36:51

┌──(root㉿PLABKALI)-[~]
└─#

┌──(root㉿PLABKALI)-[~]
└─#
```