

Module 14: Report Writing and Post Testing Actions

Objective

The objective this lab is how to prepare a documentation for your penetration testing report.

Scenario

At the end of a penetration test, the tester needs to provide the results of the pentest by preparing a report and submitting it to the clients. This report is the only tangible thing that clients get out of the entire process and therefore making it simple for everyone to understand and yet exhaustive is an art that every penetration tester needs to have. The report is also the basis for clients to get a second opinion if they disagree with the tester's findings. This can only be done if the process can be duplicated by someone else. Thus, the report needs to be as detailed as possible. Assumptions about target audience's technical knowledge and their interest should be avoided while drafting this report as they are the root causes of unnecessary confusions between clients and testers. A penetration testing report is written for three types of audiences: top management who are only concerned with the overall security posture of the organization, IT managers who are responsible for individual areas of the IT infrastructure, and IT staff who will ultimately implement the recommendations of the report. As a penetration tester you need to be able to write a report which satisfies all three audiences and leaves no confusion in anybody's mind about your findings.

Exercise 1: Generating Penetration Test Reports and Documenting all of them to KeepNote

Scenario

KeepNote is a note taking application that allows you to store your notes such as penetration test reports in a simple notebook hierarchy with rich-text formatting, images, and more.

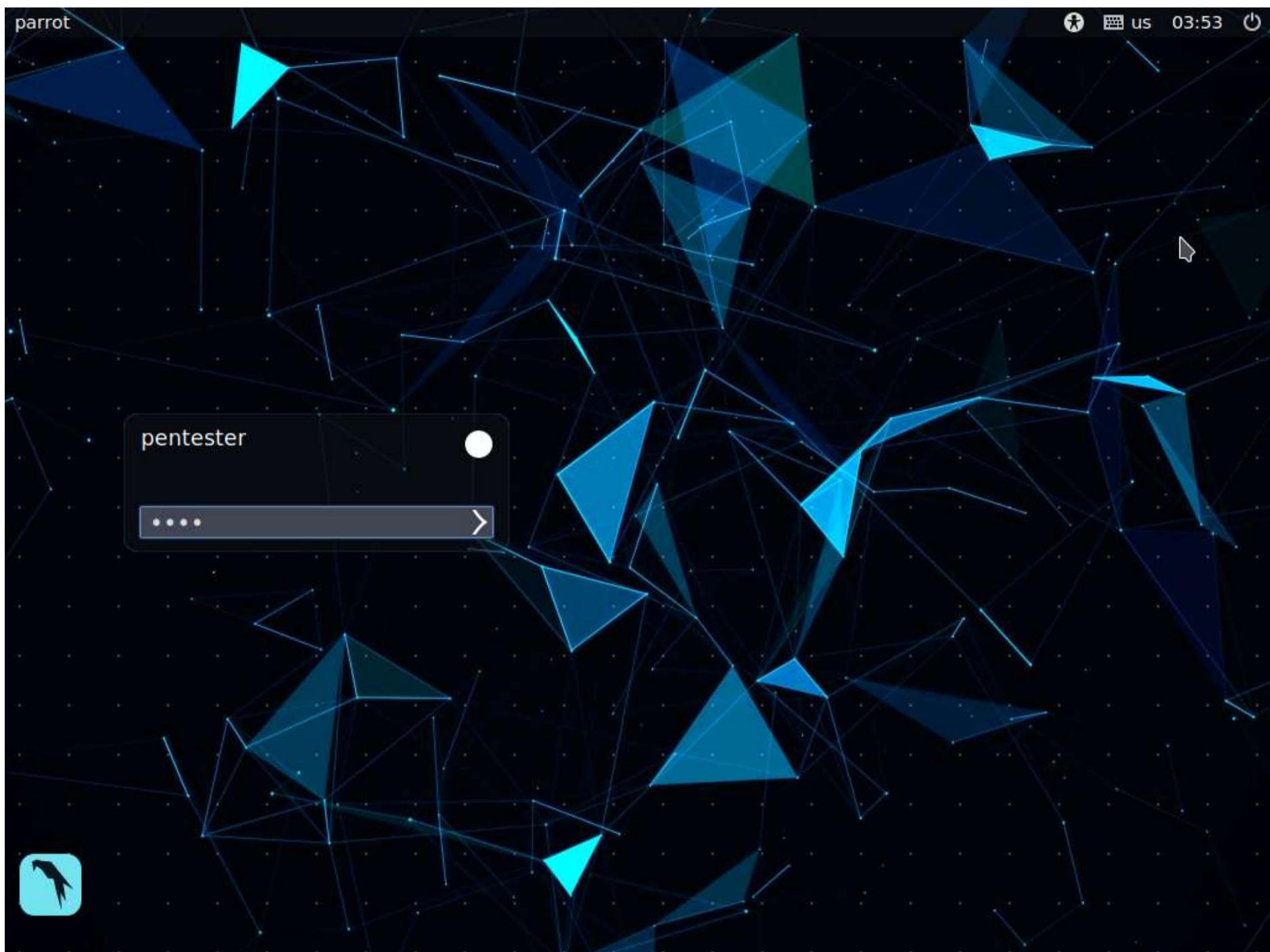
The objective of this lab is to help students learn how to:

- Import Penetration Test Reports from Penetration Test Folder to KeepNote
- Export a Final Penetration Test Report containing all the internal pentest reports

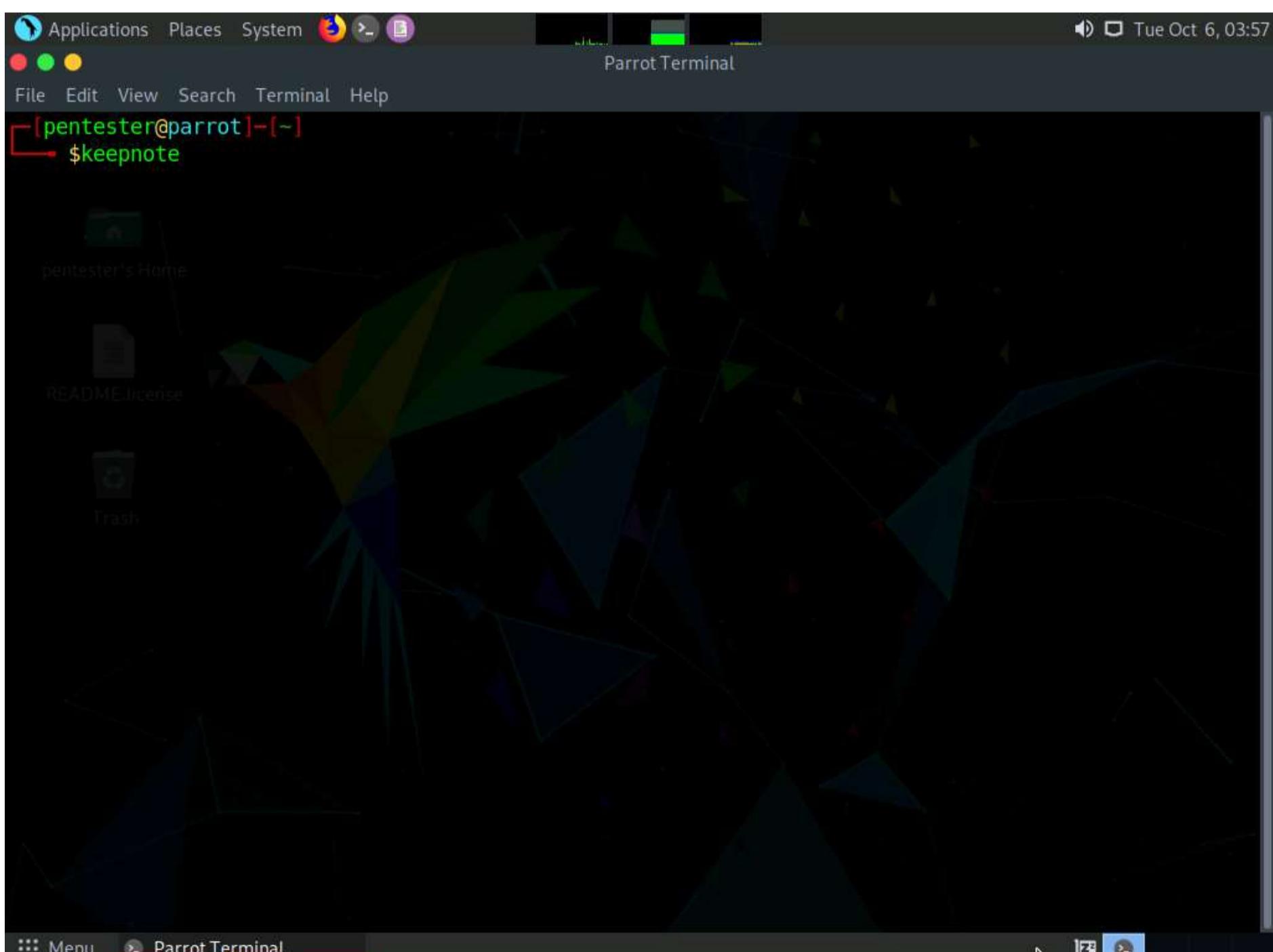
Lab Duration: 40 Minutes

1. By default, **CPENT-M14 Windows Server 2019** machine screen appears, click **Target_CPENT-M14 Parrot Security**. Type **toor** in the Password field and press **Enter**.



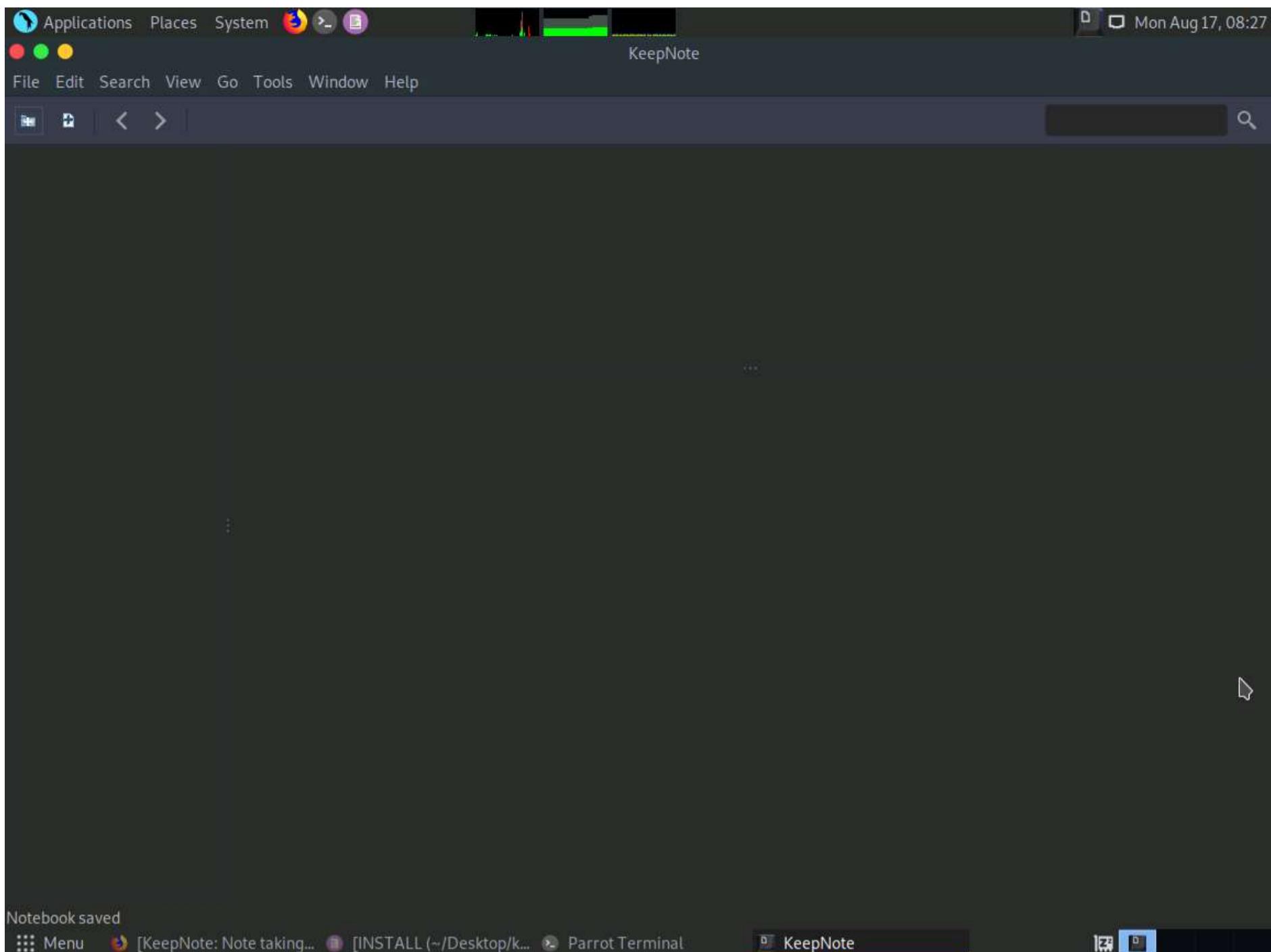


2. Open Terminal window and type **keepnote** and press Enter

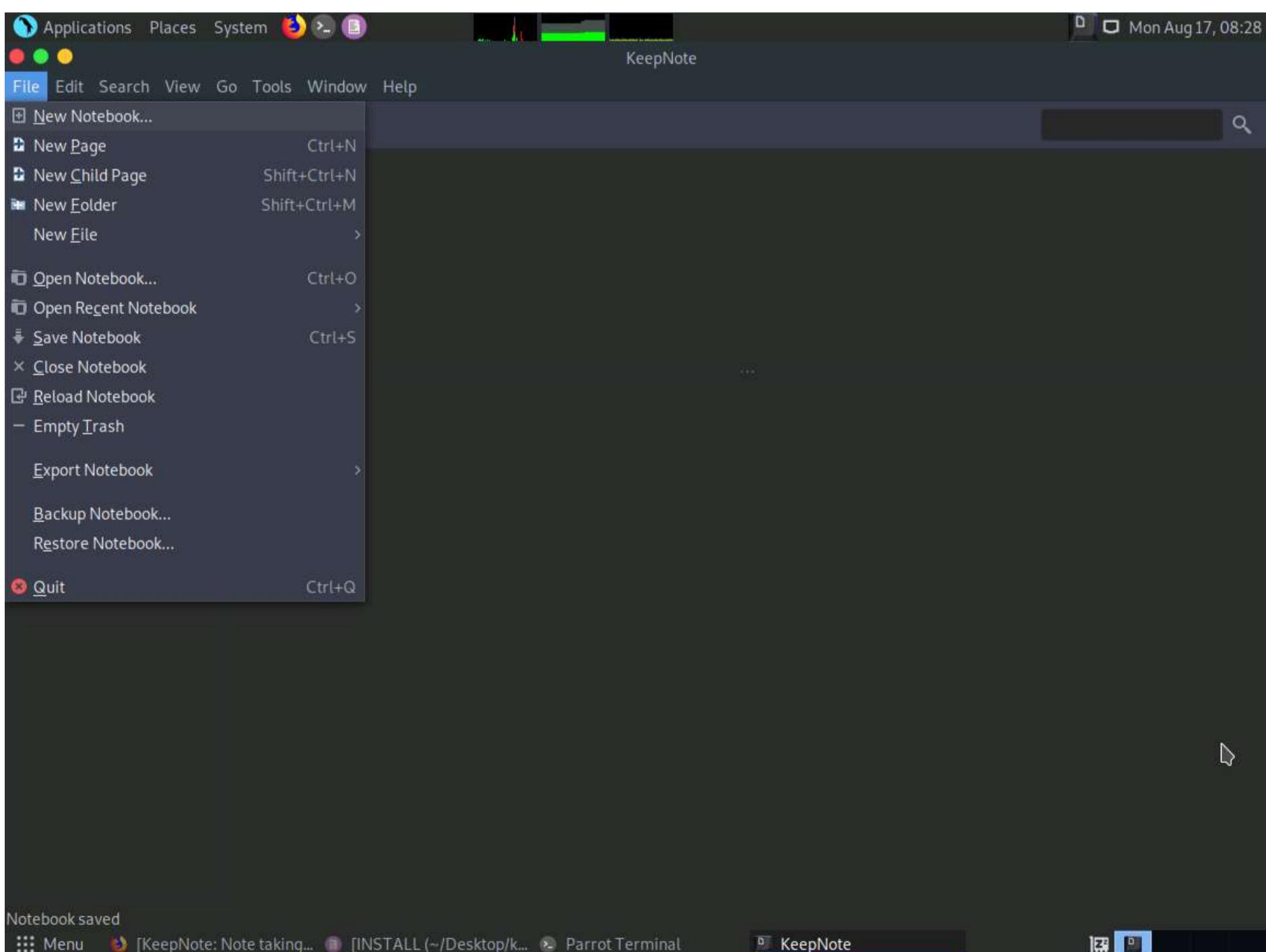


3. KeepNote main window appears as shown in the screenshot.



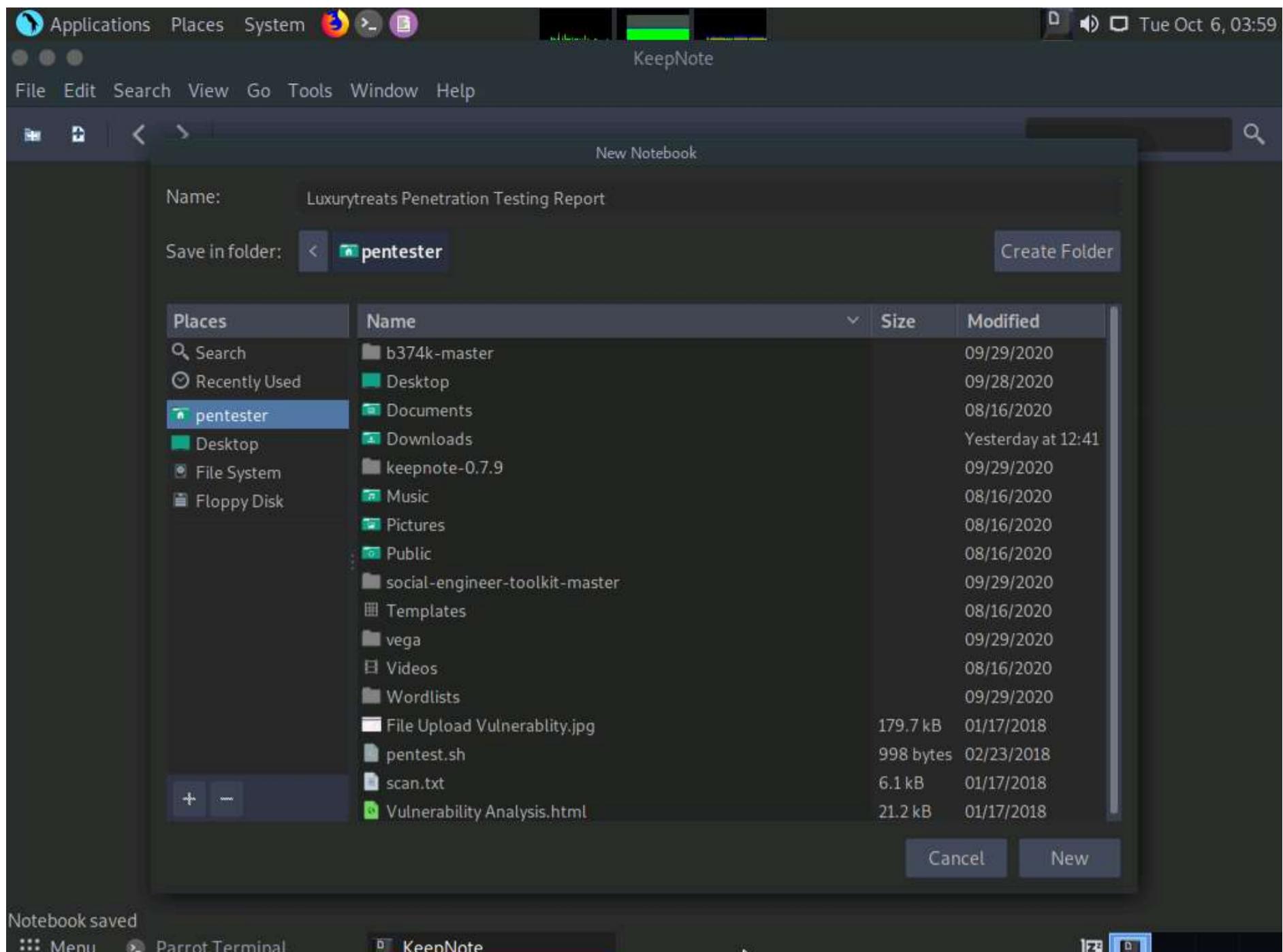


4. Select **File** from the menu bar and click **New Notebook....**



5. A **New Notebook** window appears, name the Notebook as **Luxurytreats Penetration Testing Report**, choose a location where you want to save the file (in this lab, **pentester** folder) and click **New** button.

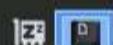




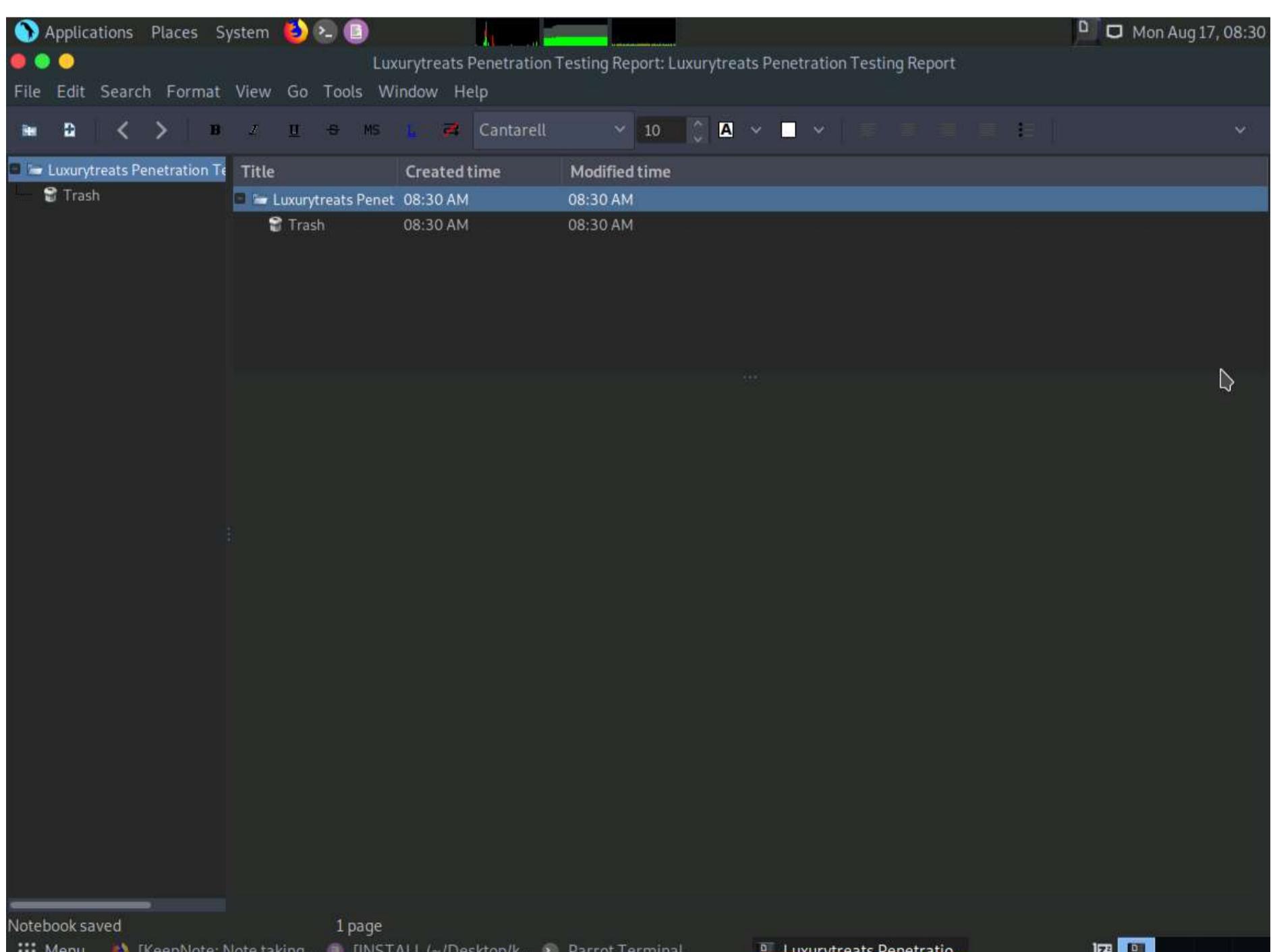
Notebook saved

Menu Parrot Terminal

KeepNote

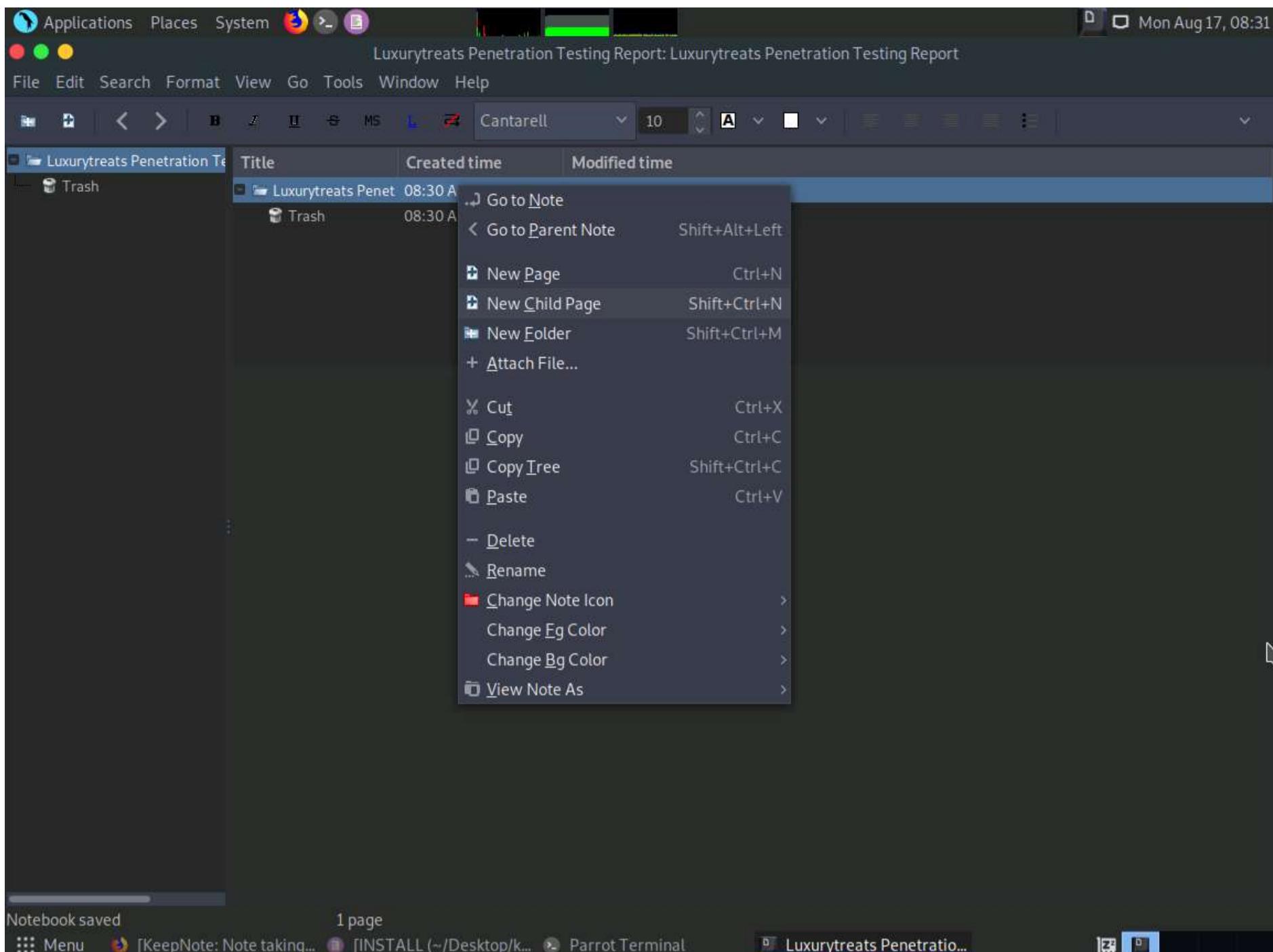


6. Click on the **Luxurytreats Penetration Testing Report** option in the left-pane. A new notebook named **Luxurytreat Penetration Testing Report** has been created as shown in the screenshot.

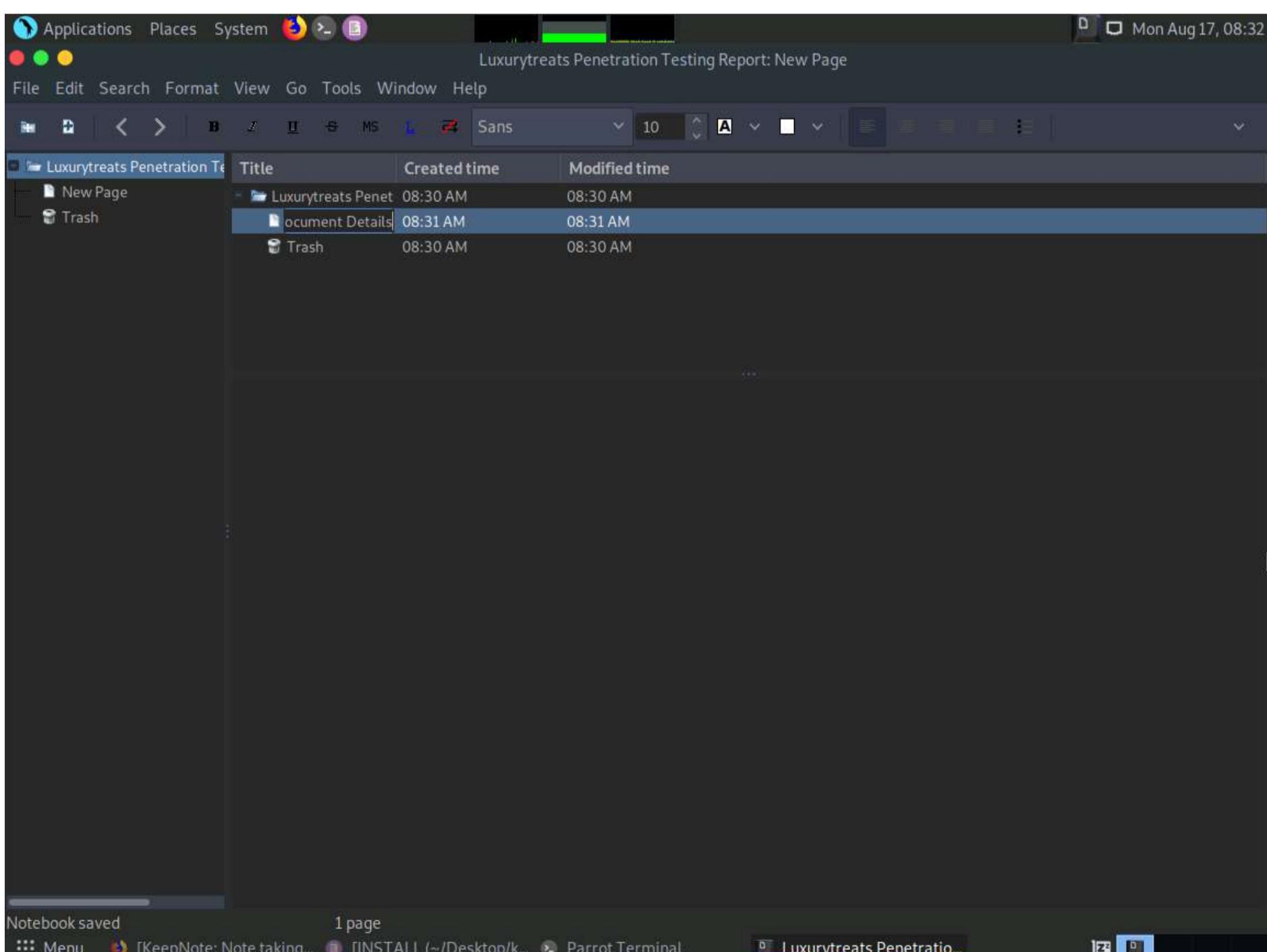


7. Right-click the **Luxurytreats Penetration Testing Report** node in the left pane and select **New Child Page**.





8. A new child page will be created. You need to name the page as **Document Details** and press **Enter**.



9. Select **Document Details** node from the left pane and in the lower section of KeepNote window, enter the details of the penetration testing report as given below.



Document Title: Luxurytreats Penetration Testing Report

Company: X-SECURITY

Recipient: Luxurytreats

Date: August 18, 2020

Classification: Confidential

Document Type: Report

Version: 1.0

Author: John

Pen testers: Micheal, Marshall, Sean, and Adam

Reviewed By: Allen and Bacon

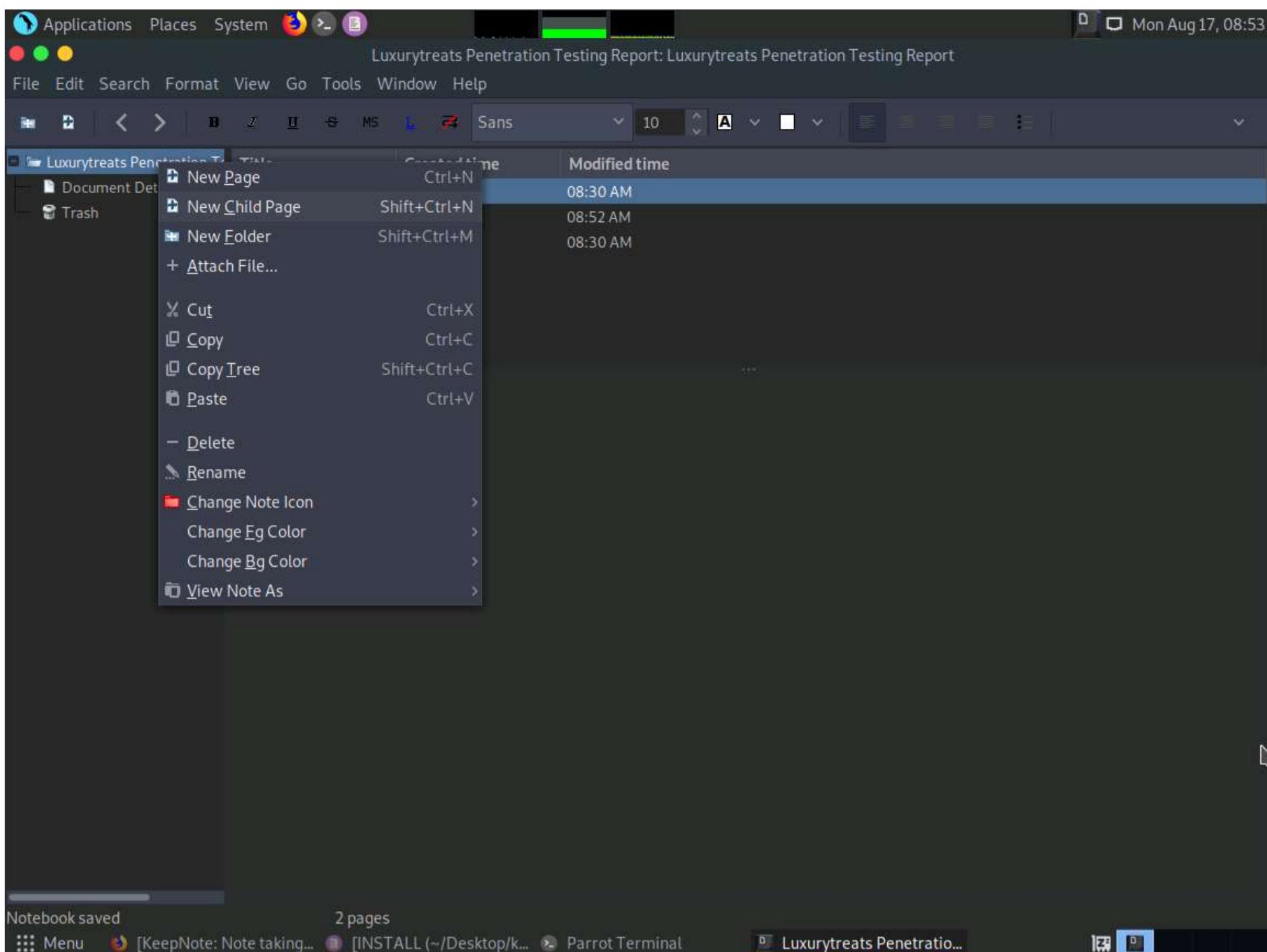
Approved By: Clark

The screenshot shows a dark-themed interface for a notebook application. At the top, there's a toolbar with icons for Applications, Places, System, and a browser. The title bar reads "Luxurytreats Penetration Testing Report: Document Details". The menu bar includes File, Edit, Search, Format, View, Go, Tools, Window, and Help. Below the menu is a toolbar with various editing tools like bold, italic, underline, etc. A table titled "Document Details" is displayed, showing one row with the file name "Document Details", its creation time "05:41 AM", and modification time "05:55 AM". To the left of the table is a sidebar with a tree view showing a folder named "Luxurytreats Penetration Test" and a "Trash" item. The main workspace below the table contains the document content. At the bottom, there's a status bar with "Notebook saved", "0 pages", and tabs for "Parrot Terminal" and "Luxurytreats Penetrati...".

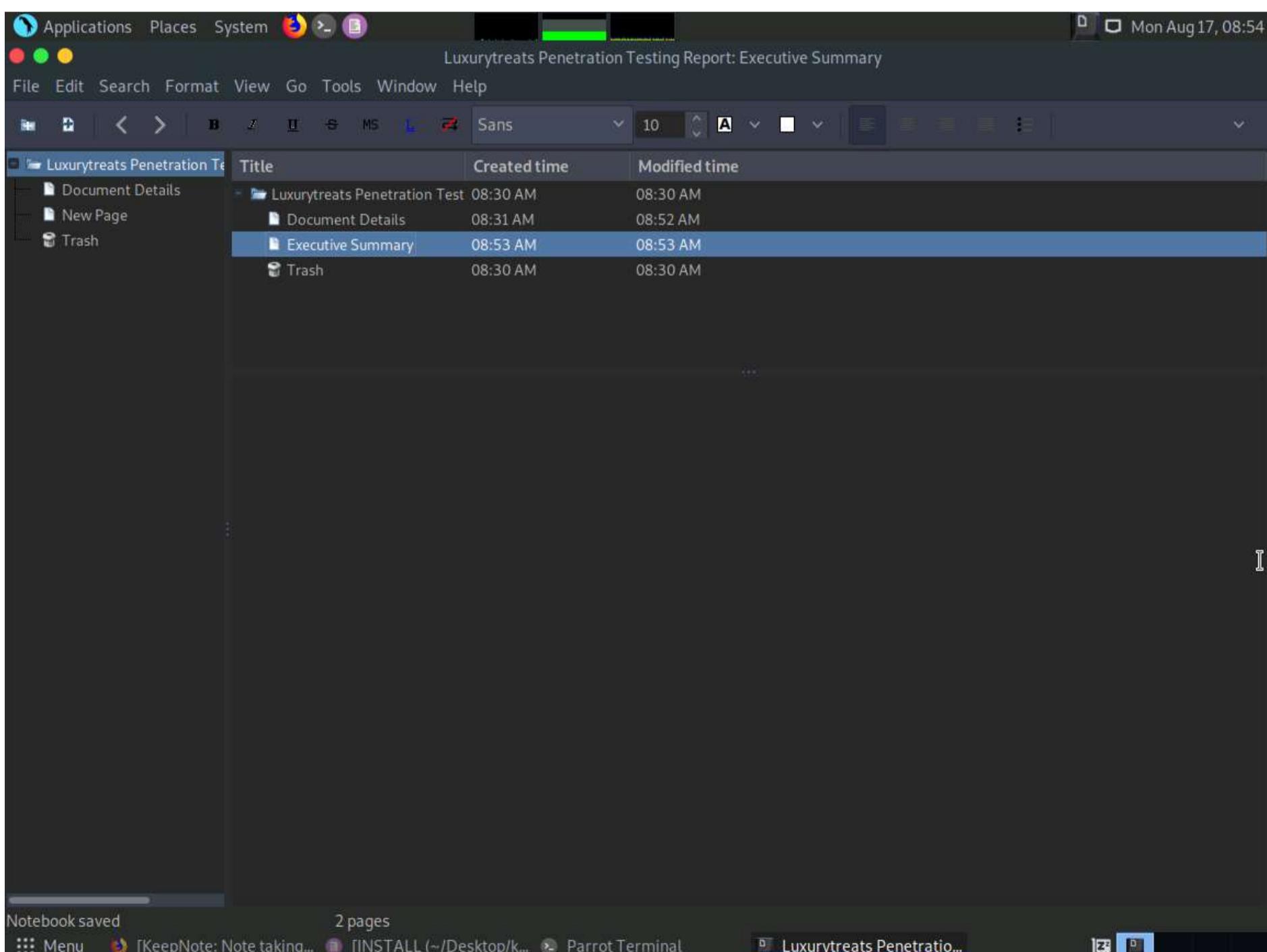
Document Title: Luxurytreats Penetration Testing Report
Company: X-SECURITY
Recipient: Luxurytreats
Date: August 18, 2020
Classification: Confidential
Document Type: Report
Version: 1.0
Author: John
Pen testers: Micheal, Marshall, Sean, and Adam
Reviewed By: Allen and Bacon
Approved By: Clark

10. Right-click the **Luxurytreats Penetration Testing Report** node in the left pane and select **New Child Page**.



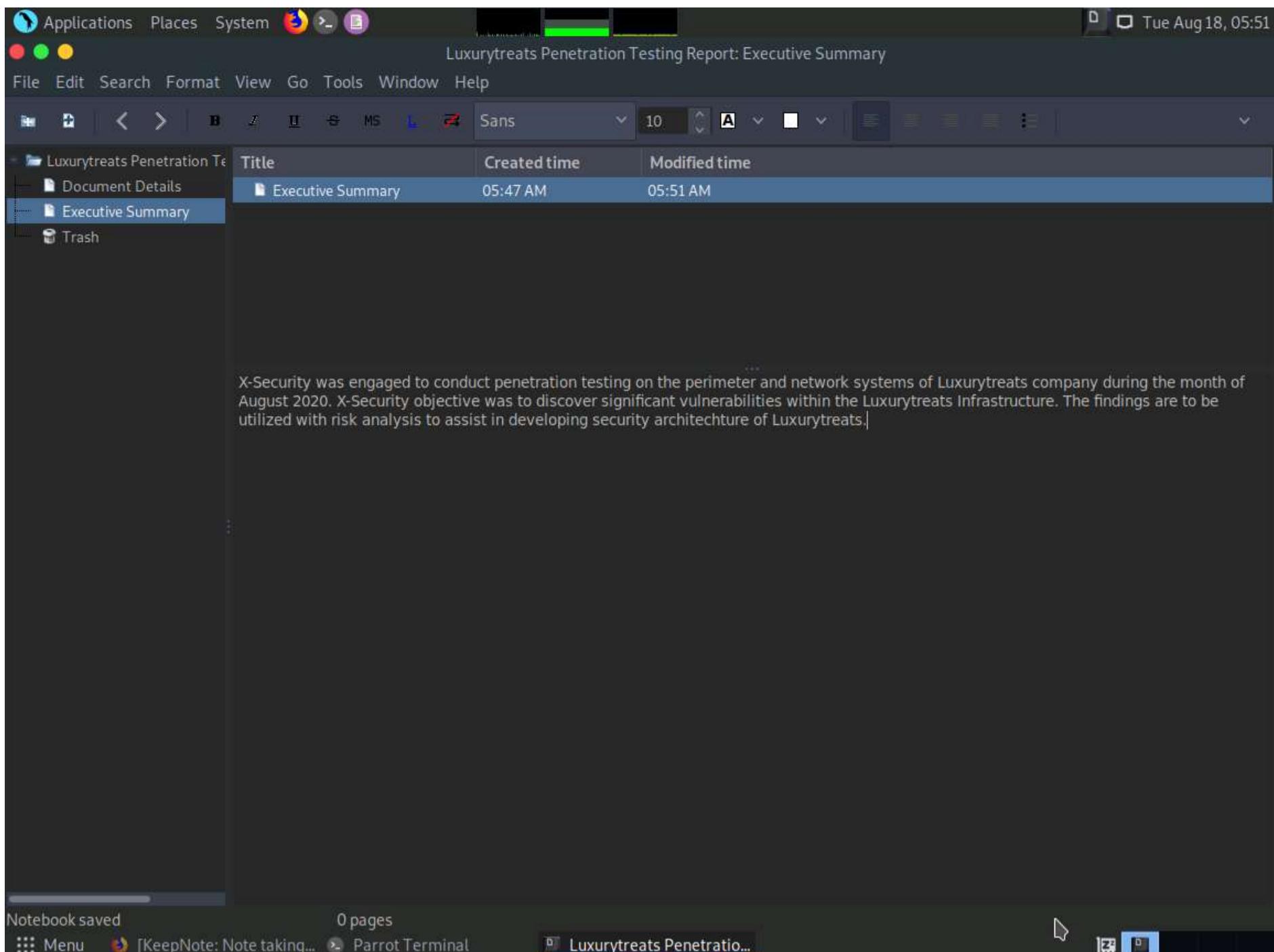


11. A new child page will be created. You need to name the page as **Executive Summary** and press **Enter**.

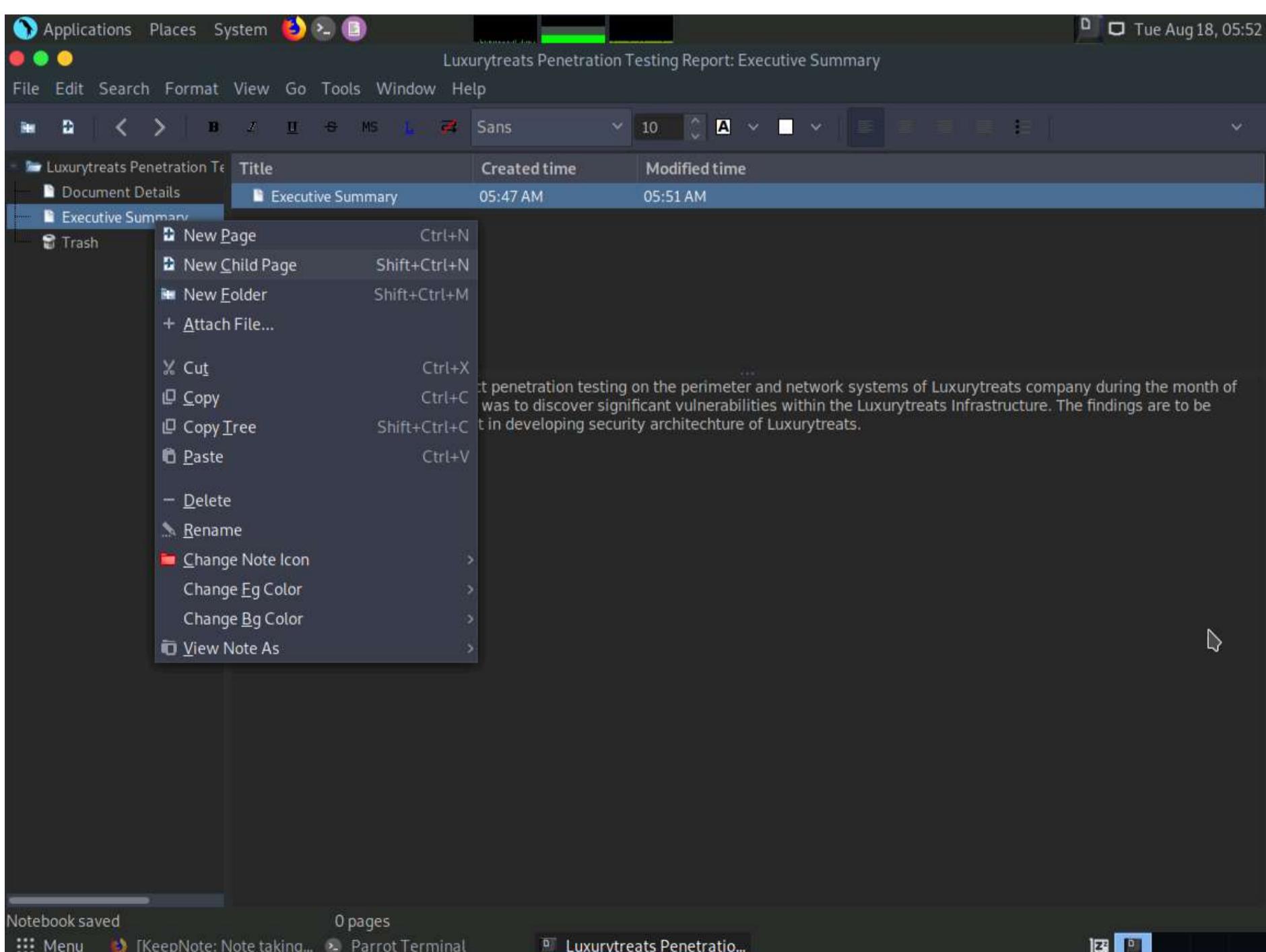


12. Select **Executive Summary** node from the left pane and in the lower section of KeepNote window and enter the **Executive Summary** as shown in the screenshot.

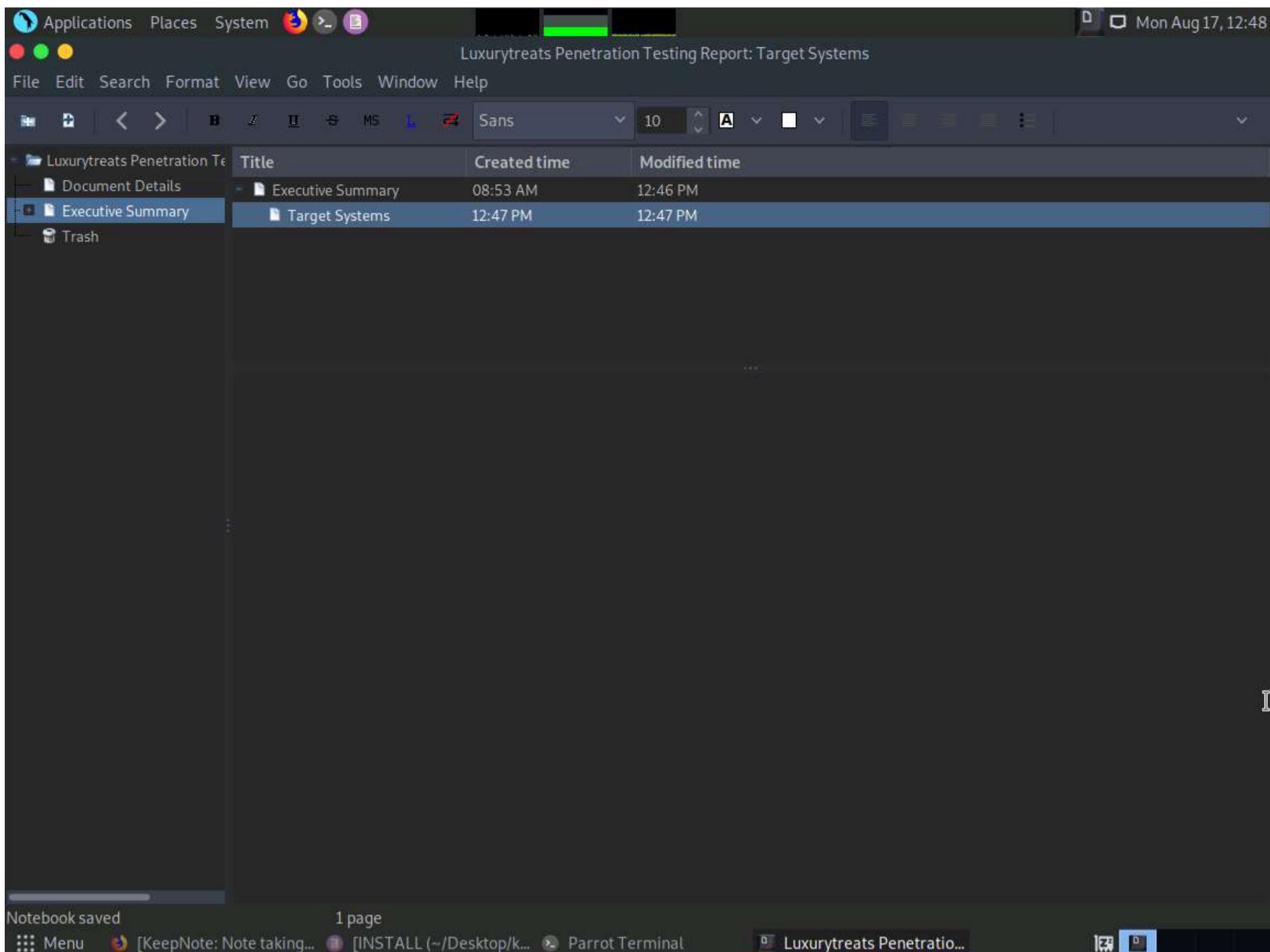




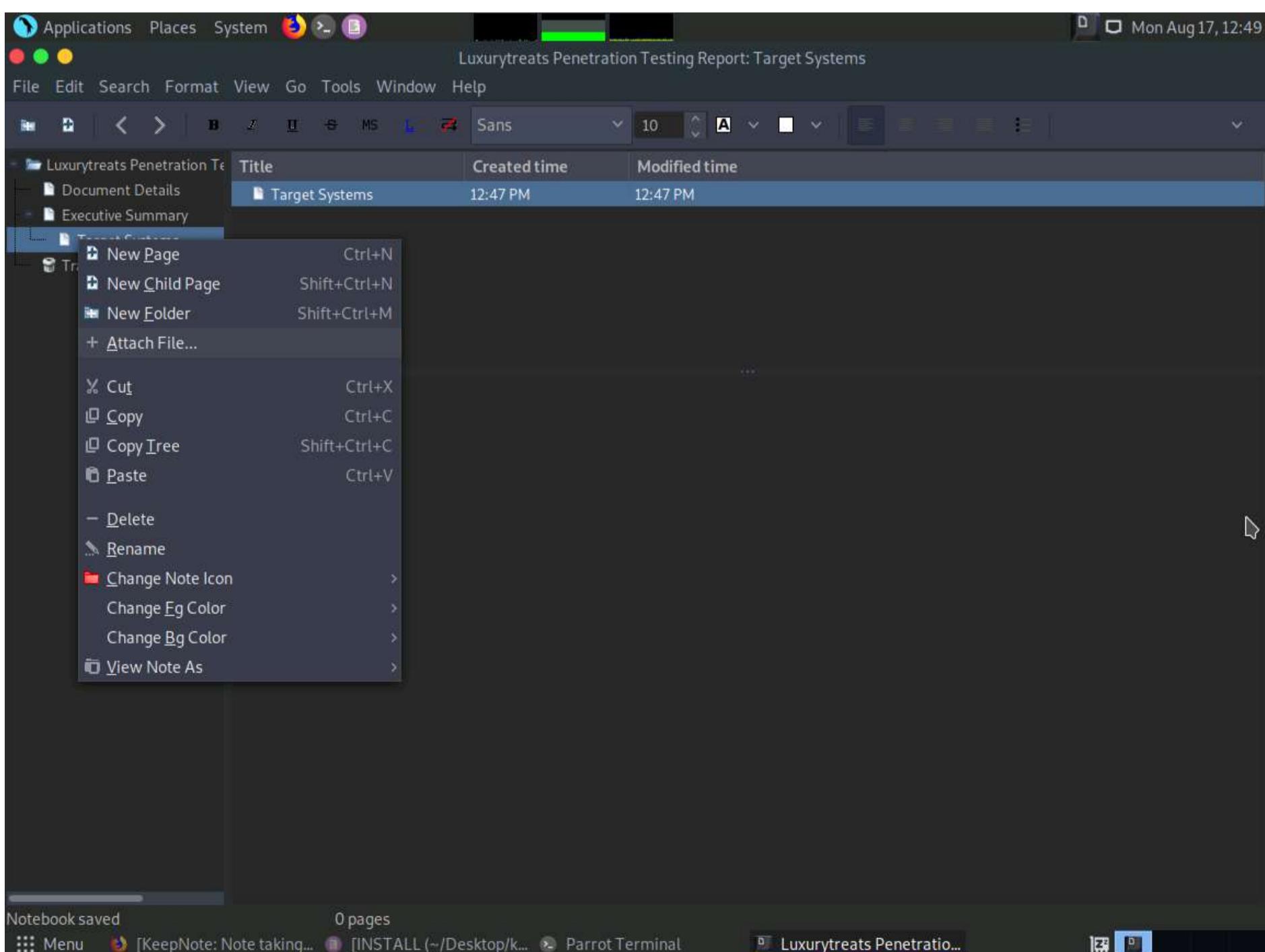
13. Right-click the **Executive Summary** child page in the left pane and select **New Child Page**.



14. A new child page will be created. You need to name the page as **Target Systems** and press **Enter**. In this page, you will be attaching the file that contains the result of nmap subnet scan. The file containing the subnet scan is located in **pentester** folder.

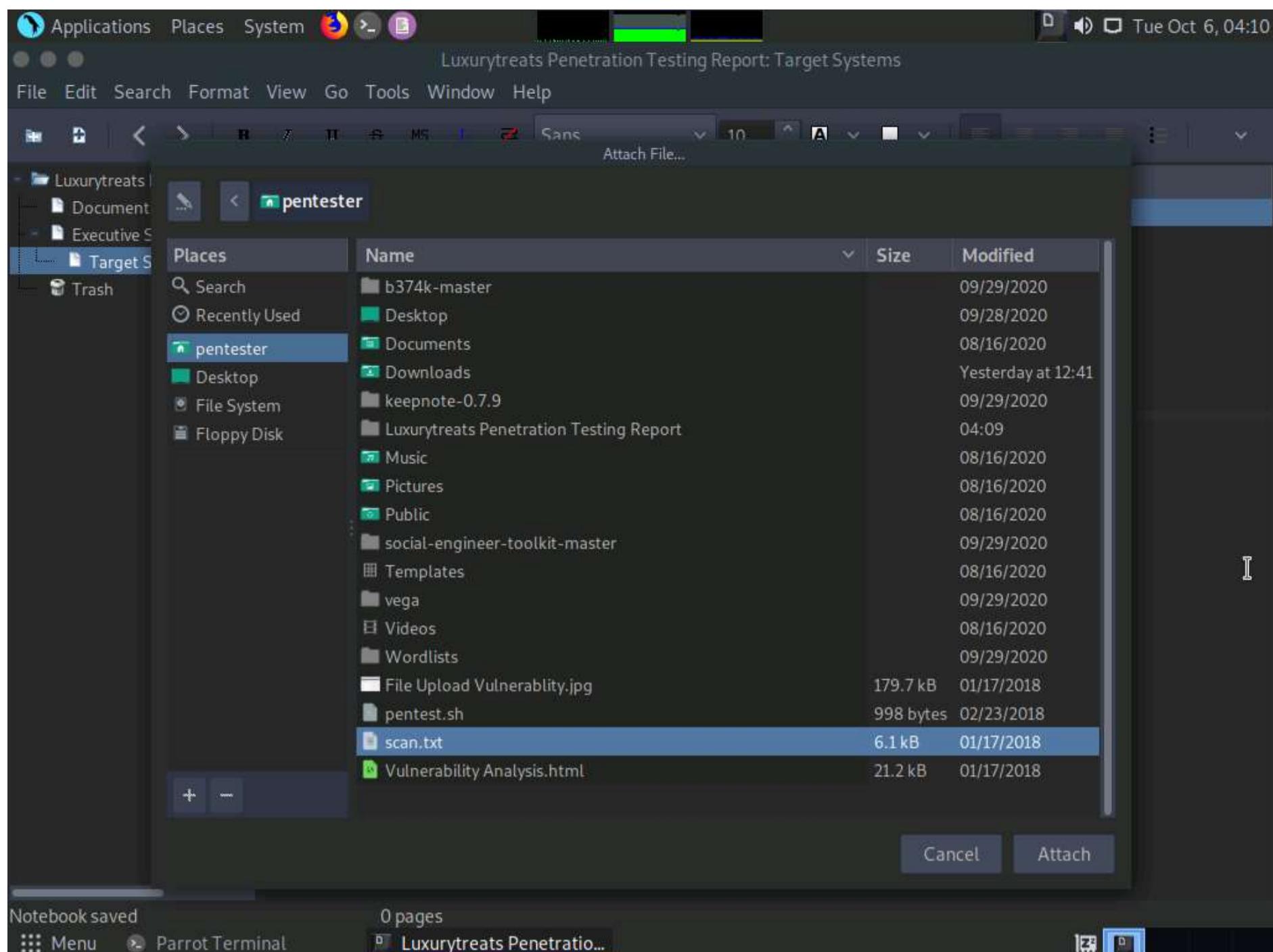


15. Expand the **Executive Summary** node. Right-click on **Target Systems** node in the left pane and select **Attach File...** option.



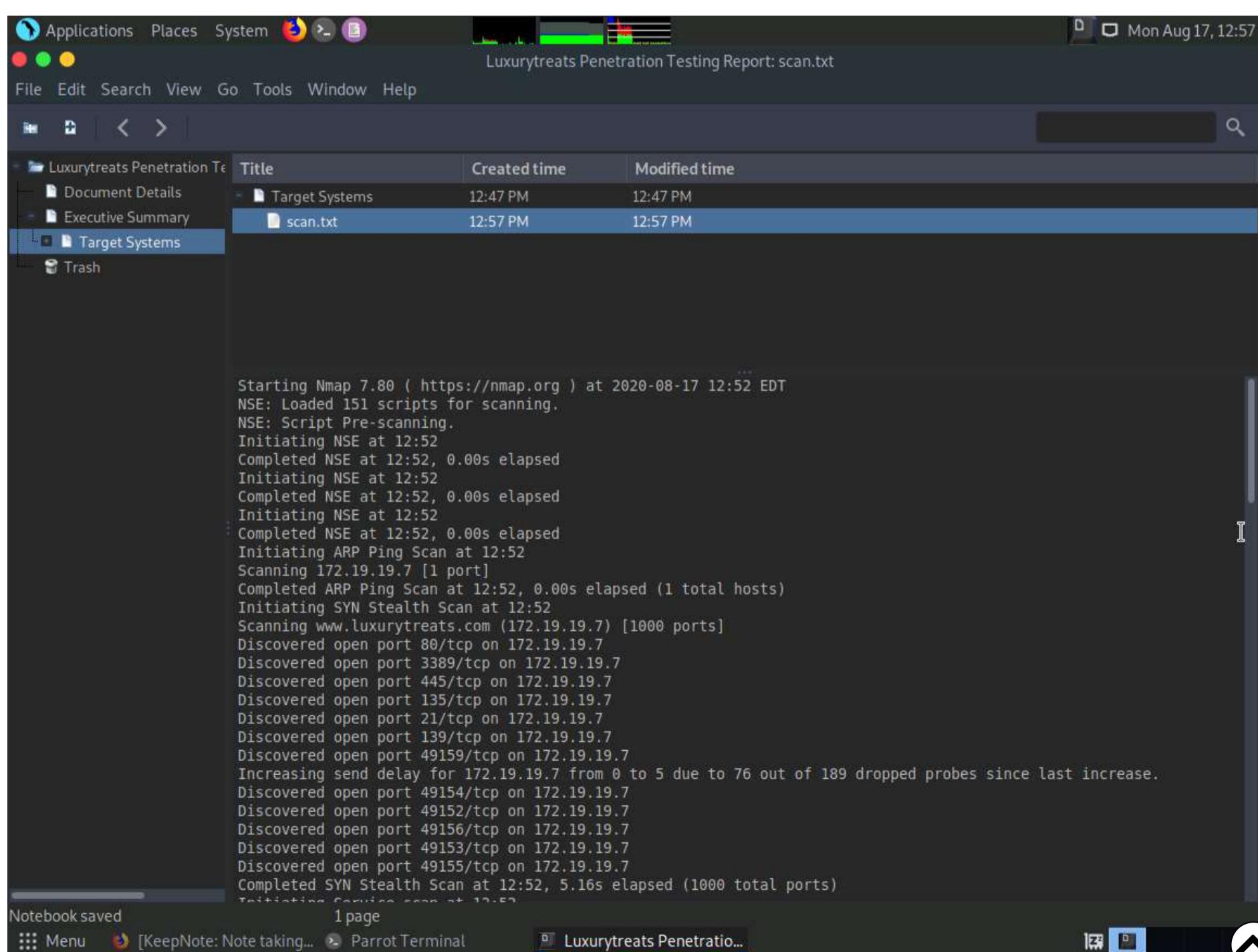
16. **Attach File...** window appears, navigate to **pentester** folder, select **scan.txt** file and click **Attach** button



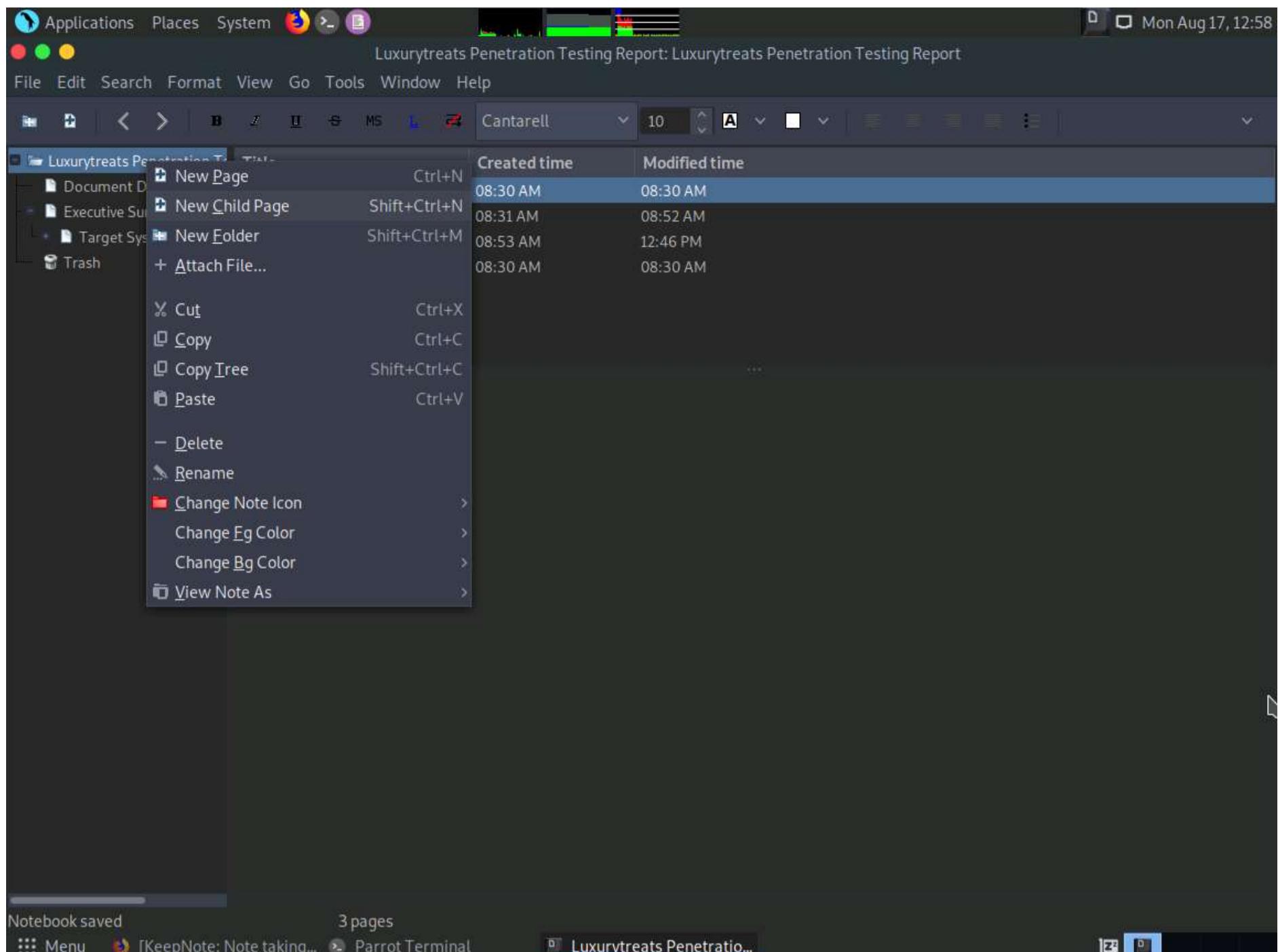


17. You will observe that **scan.txt** file is attached under **Target Systems** page. Click on **Scan.txt** to view the scan result.

Note: The results appearing in your lab may vary from the ones displayed in the screenshot.



18. Right-click the **Luxurytreats Penetration Testing Report** node in the left pane and select **New Child Page**.



19. A new child page will be created. You need to name the page as **Comprehensive Technical Report** and press **Enter**. In this report, you will be featuring all the vulnerabilities found during penetration testing, and attach the screenshots/reports of the respective exploitation phenomenon. In this lab, we will prepare a report for vulnerability assessment.



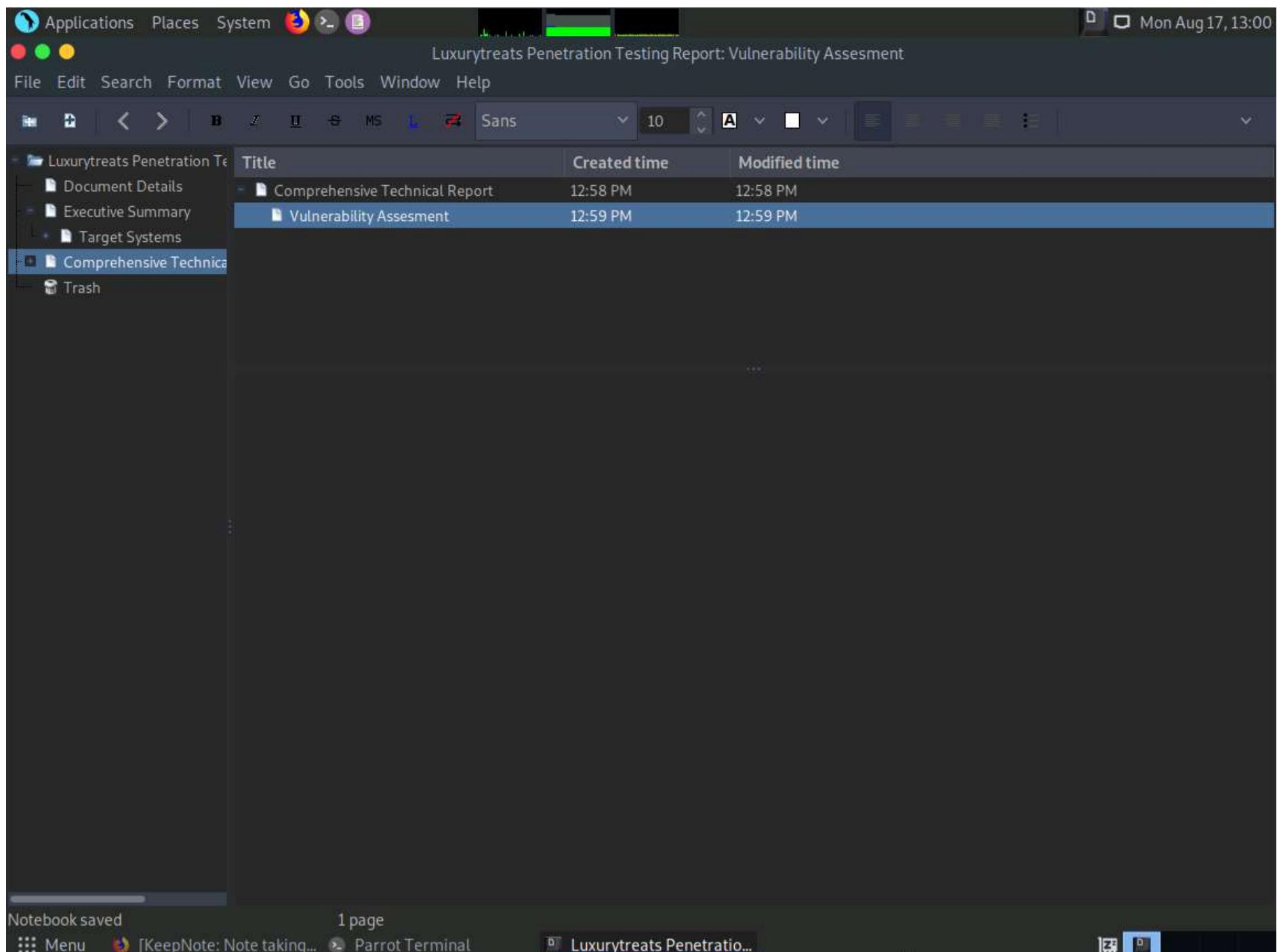
The screenshot shows a dark-themed application window titled "Luxurytreats Penetration Testing Report: Comprehensive Technical Report". The left pane displays a hierarchical file structure under "Luxurytreats Penetration Test". The right pane is a blank workspace. The status bar at the bottom shows "Notebook saved", "3 pages", and the system tray includes "Menu", "[KeepNote: Note taking...]", and "Parrot Terminal".

20. Right-click the **Comprehensive Technical Report** child page in the left pane and select **New Child Page**.

The screenshot shows the same application window. A context menu is open over the "Comprehensive Technical Report" page in the left pane. The menu options include: Go to Note, Go to Parent Note, New Page, New Child Page, New Folder, Attach File..., Cut, Copy, Copy Tree, Paste, Delete, Rename, Change Note Icon, Change Eg Color, Change Bg Color, and View Note As.

21. A new child page will be created. You need to name the page as **Vulnerability Assessment** and press **Enter**.





22. Expand **Comprehensive Technical Report** node in the left pane. Select **Vulnerability Assessment** node under **Comprehensive Technical Report** and in the lower section of KeepNote window and write a report associated with the vulnerability found in a target (in the earlier labs, for instance, **File Upload** vulnerability) as shown in the screenshot.

Note: If you have a screenshot, you can also attach it as proof of concept.



Luxurytreats Penetration Testing Report: Vulnerability Assesment

File Edit Search Format View Go Tools Window Help

Sans 10

Title	Created time	Modified time
Comprehensive Technical Report	12:58 PM	12:58 PM
Vulnerability Assesment	12:59 PM	01:12 PM

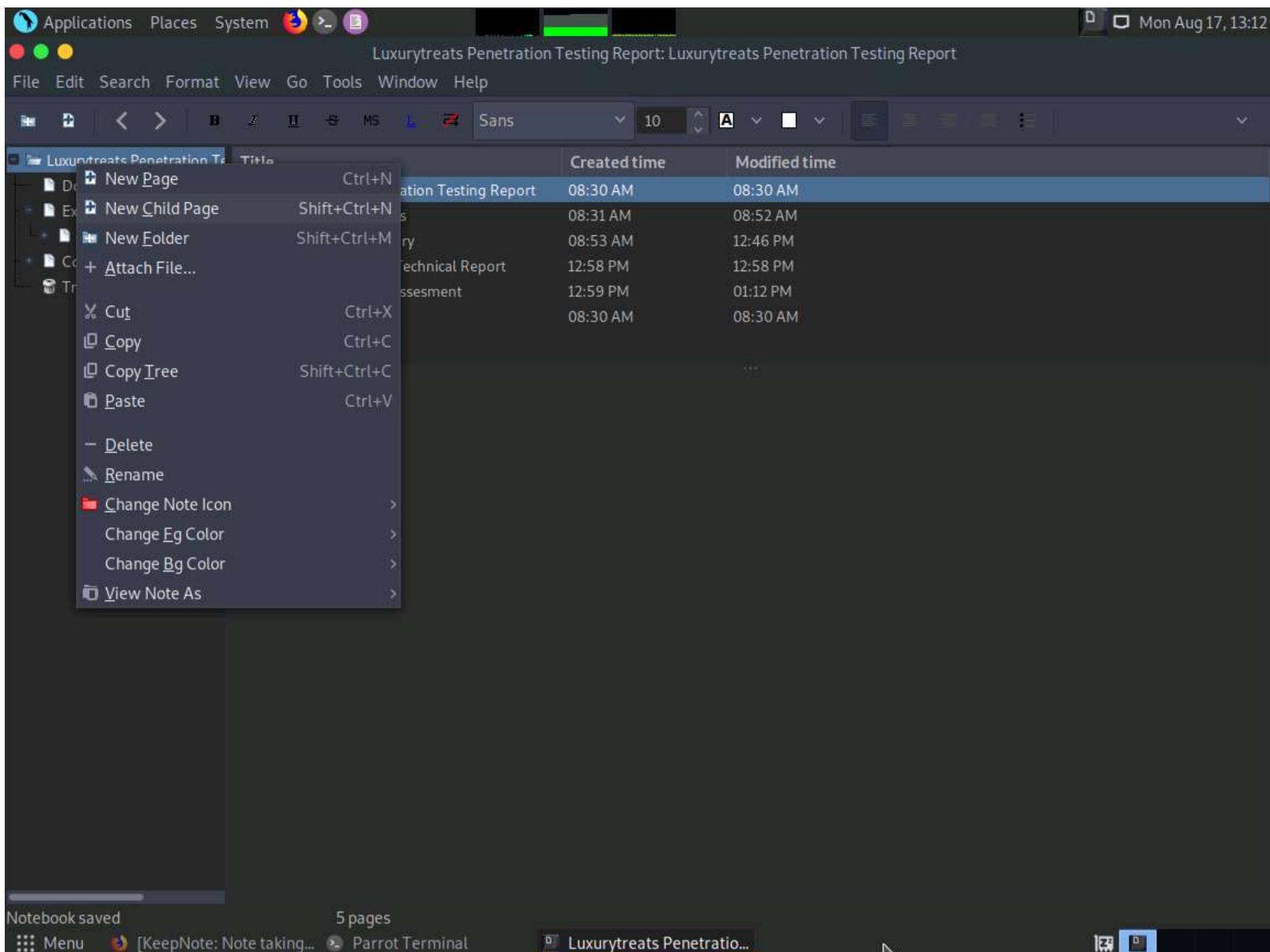
Category: Malicious file upload/ Shell Upload
Threat Description: Wordpress Appearance Editor supports editing files such as archive.php and 404.php, which allow attackers to upload file content with that of a shell, thereby giving access to server hosting the web application.
Impact: If the vulnerability is exploited attackers can gain unrestricted access to server hosting web application.
Result Analysis: The target web application was found to have file upload vulnerability which resulted in gaining access to server.
Recommendations:
1. Enforce strong passwords for the Wordpress admin account.
2. Disable write access to Wordpress theme files such as archive.php, 404.php, footer.php and comments.php.

Notebook saved 1 page

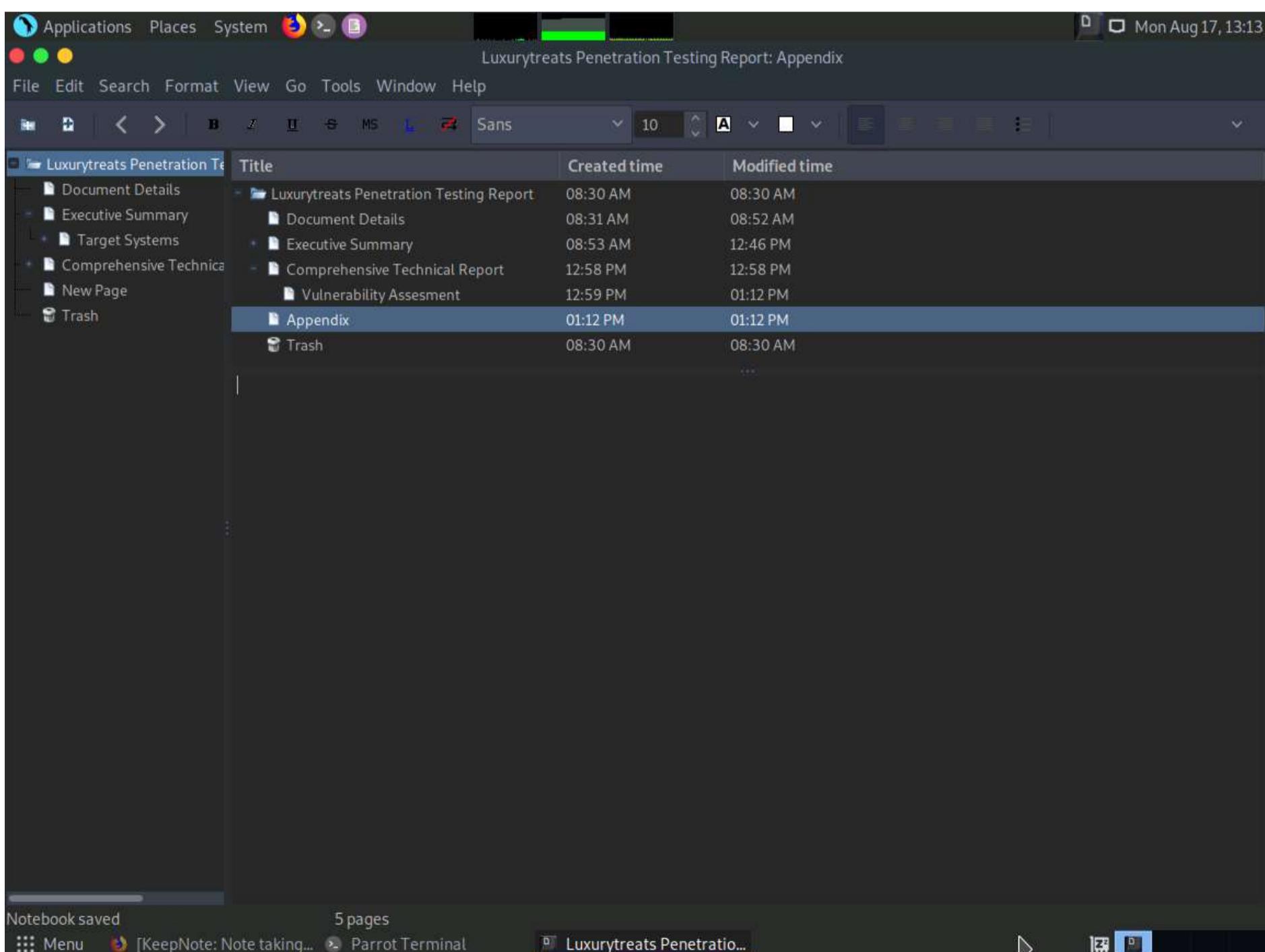
Menu [KeepNote: Note taking... Parrot Terminal Luxurytreats Penetratio...]

23. Right-click the **Luxurytreats Penetration Testing Report** node in the left pane and select **New Child Page**. In general, vulnerability analysis reports are too lengthy and they disturb the continuity of the penetration test report. Hence, you will be attaching this vulnerability analysis file at the end of the pentest report.
Assume that you have come to the end of the report. Therefore, you will be attaching the vulnerability analysis file here (under a child page named Appendix).



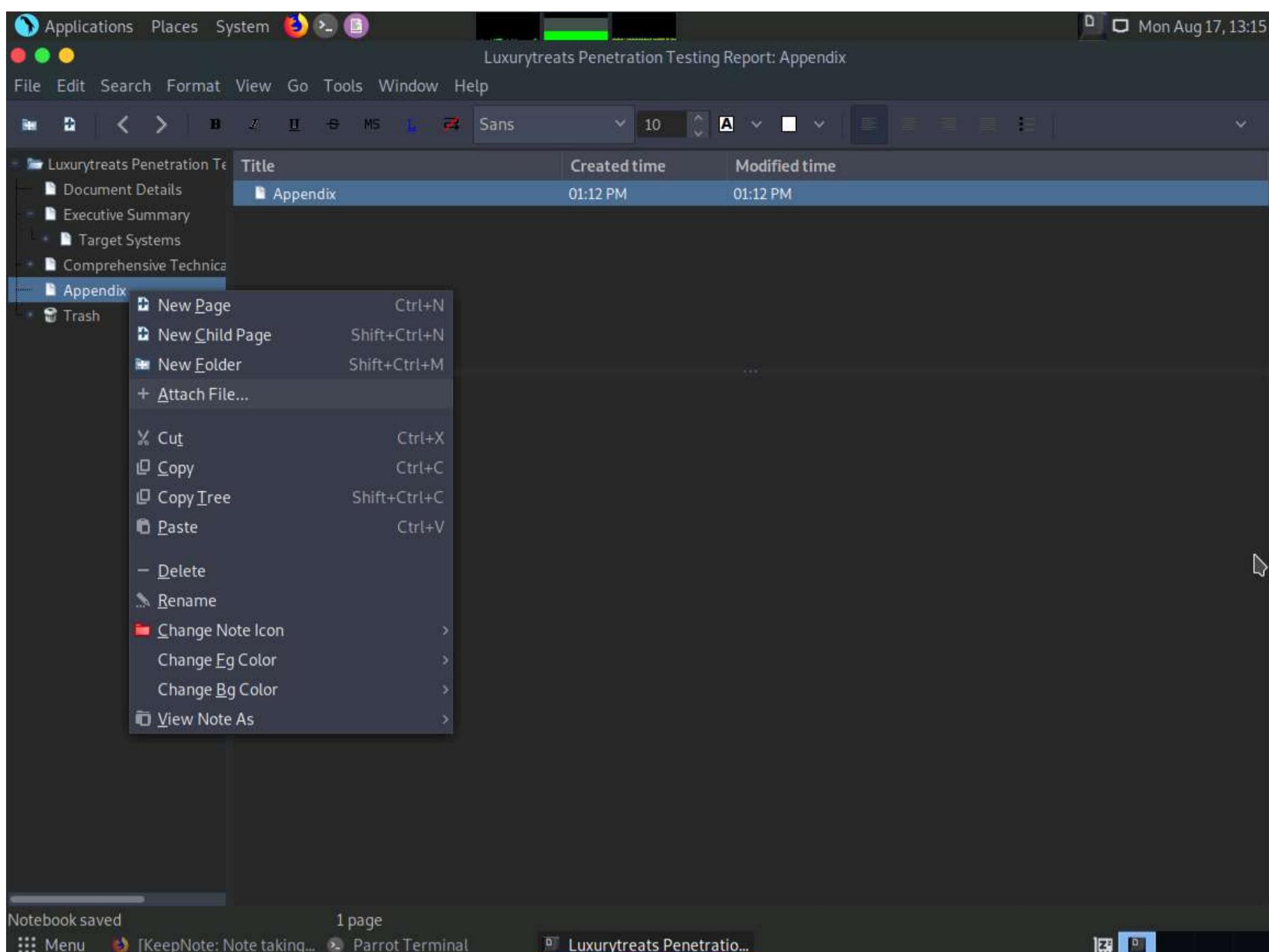


24. A new child page will be created. You need to name the page as **Appendix** and press **Enter**.

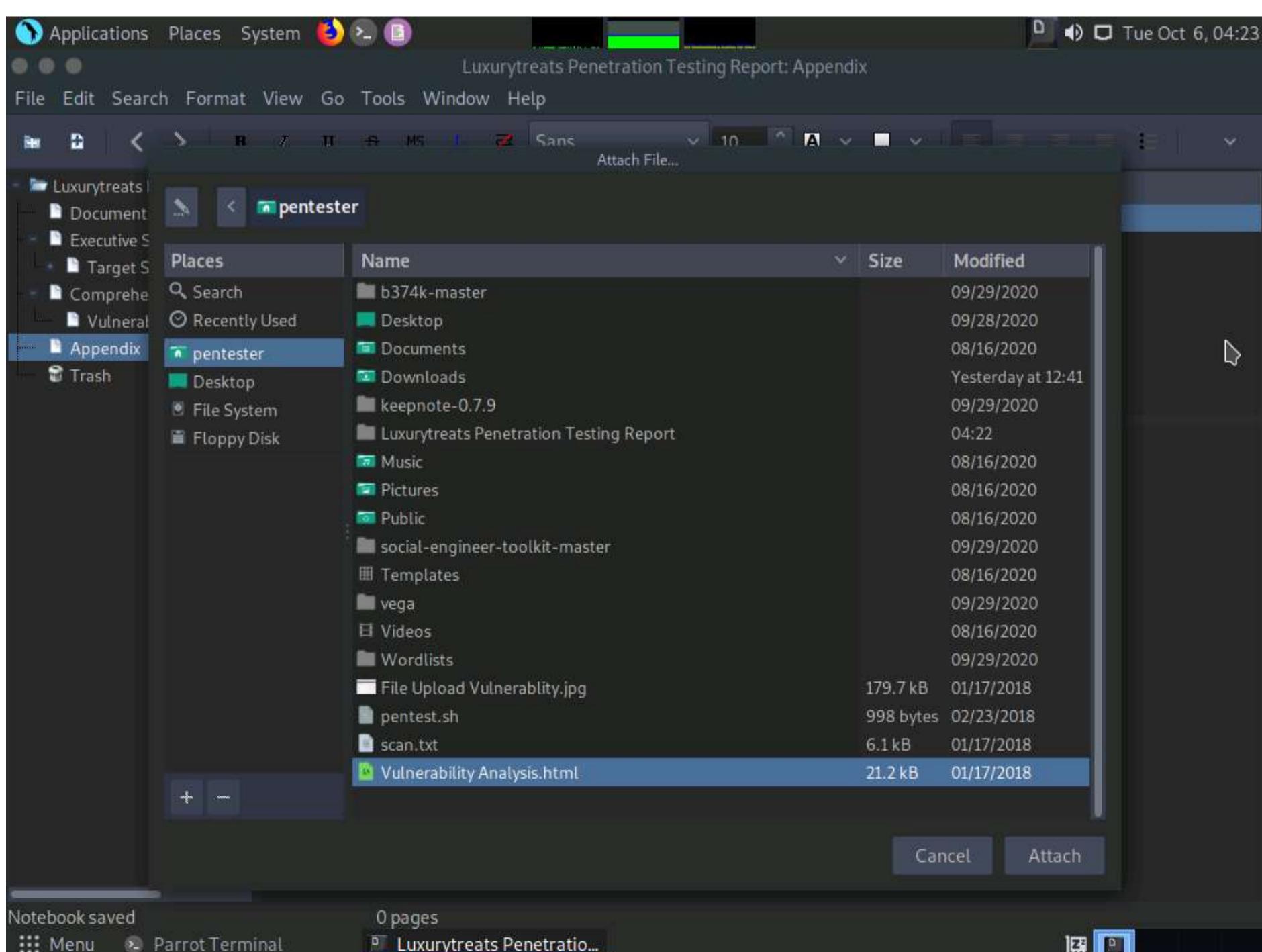


25. Right-click on **Appendix** node in the left pane and select **Attach File...** option.





26. **Attach File...** window appears, navigate to **pentester** folder, select **Vulnerability Analysis.html** file and click **Attach** button.



27. You will observe that **Vulnerability Analysis.html** file is attached under **Appendix** page as shown in the screenshot.



Luxurytreats Penetration Testing Report: Vulnerability Analysis.html

Title	Created time	Modified time
Document Details	01:12 PM	01:12 PM
Appendix	01:19 PM	01:19 PM
Vulnerability Analysis.html	01:19 PM	01:19 PM
Executive Summary		
Target Systems		
Comprehensive Techniques		
Appendix		
Trash		

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
<head id="ctl00_Head1"><link href="App_Themes/Default/00.reset.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/01.960_24_col.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/02.text.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/03.layout.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/BreadCrumb.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/Form.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/buttons.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/grids.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/left-menu.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/styles.css" type="text/css" rel="stylesheet" /><link type="text/css" href="Resources/jquery-ui/jquery-ui-1.8.16.custom.css" rel="stylesheet" /><link type="text/css" href="Resources/jquery-libs/autocomplete/styles.css" rel="stylesheet" /><title>ECCVApp</title>
<link href="Content/bootstrap.css" rel="stylesheet" /><link href="Content/bootstrap.min.css" rel="stylesheet" /><link href="Content/Site.css" rel="stylesheet" /><link href="Hotels/css/style.css" media="screen" rel="stylesheet" type="text/css" /><link href="Hotels/css/extensions.css" media="screen" rel="stylesheet" type="text/css" /><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /><meta name="description" /><meta name="keywords" />

<style type="text/css">
.demoHeaders {
margin-top: 2em;
}
```

Notebook saved 1 page

Menu [KeepNote: Note taking... Parrot Terminal Luxurytreats Penetratio...

28. Go to the **File** menu and select **Export Notebook --> HTML....**

Luxurytreats Penetration Testing Report: Vulnerability Analysis.html

- New Notebook...
- New Page Ctrl+N
- New Child Page Shift+Ctrl+N
- New Folder Shift+Ctrl+M
- New File >
- Open Notebook... Ctrl+O
- Open Recent Notebook >
- Save Notebook Ctrl+S
- Close Notebook
- Reload Notebook
- Empty Trash
- Export Notebook >
 - HTML...
- Backup Notebook...
- Restore Notebook...
- Quit Ctrl+Q

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
<head id="ctl00_Head1"><link href="App_Themes/Default/00.reset.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/01.960_24_col.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/02.text.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/03.layout.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/BreadCrumb.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/Form.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/buttons.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/grids.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/left-menu.css" type="text/css" rel="stylesheet" /><link href="App_Themes/Default/styles.css" type="text/css" rel="stylesheet" /><link type="text/css" href="Resources/jquery-ui/jquery-ui-1.8.16.custom.css" rel="stylesheet" /><link type="text/css" href="Resources/jquery-libs/autocomplete/styles.css" rel="stylesheet" /><title>ECCVApp</title>
<link href="Content/bootstrap.css" rel="stylesheet" /><link href="Content/bootstrap.min.css" rel="stylesheet" /><link href="Content/Site.css" rel="stylesheet" /><link href="Hotels/css/style.css" media="screen" rel="stylesheet" type="text/css" /><link href="Hotels/css/extensions.css" media="screen" rel="stylesheet" type="text/css" /><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /><meta name="description" /><meta name="keywords" />

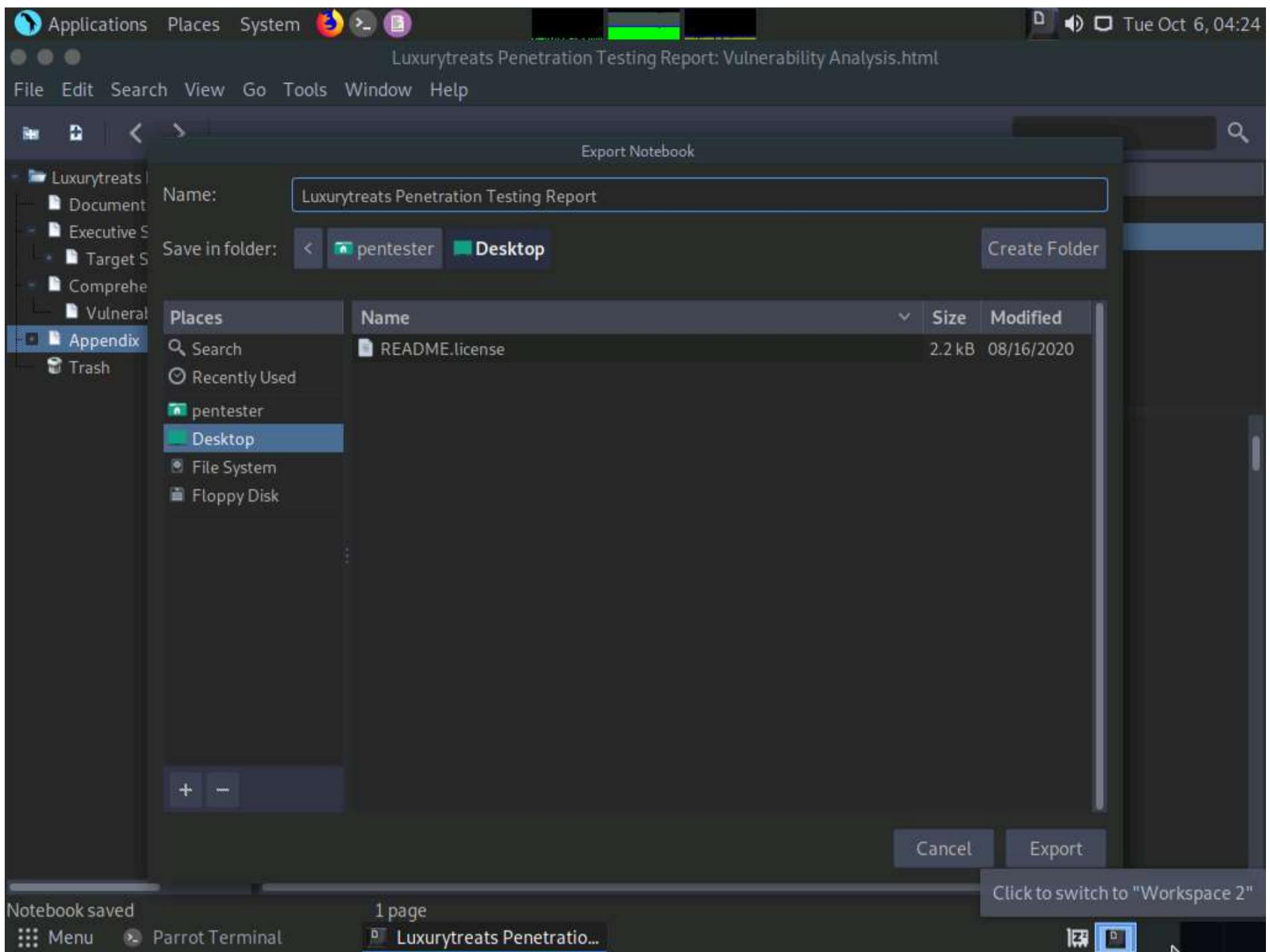
<style type="text/css">
.demoHeaders {
margin-top: 2em;
}
```

Notebook saved 1 page

Menu [KeepNote: Note taking... Parrot Terminal Luxurytreats Penetratio...

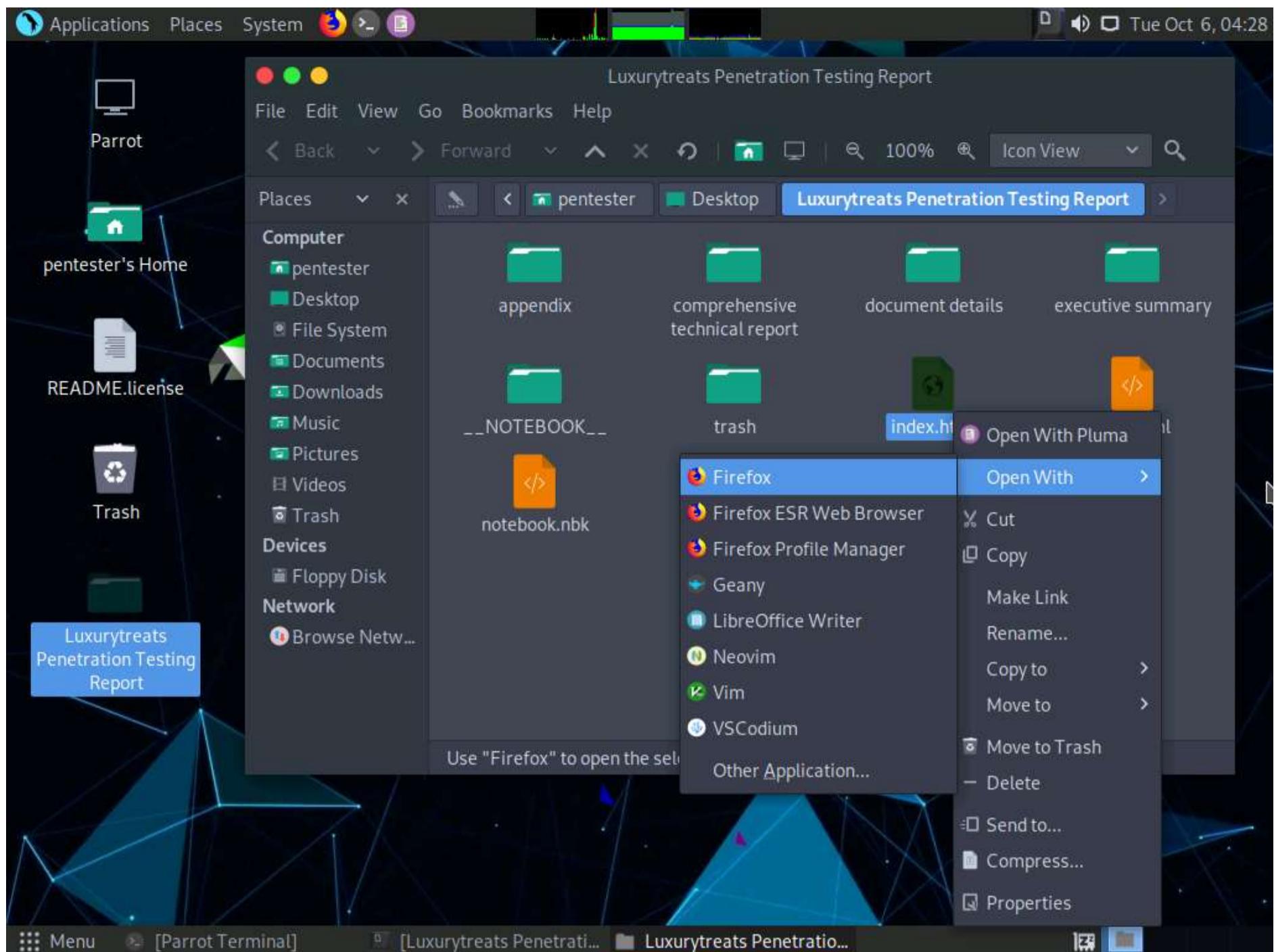
29. Export Notebook window appears; specify the **Luxurytreats Penetration Testing Report**, choose the location as **Desktop** and click **Export**. Here, we will change the name because the folder named **Luxurytreats Penetration Testing Report** will be saved by default at the time of creating a notebook in KeepNote.

Note: You can minimize or close the KeepNote window.

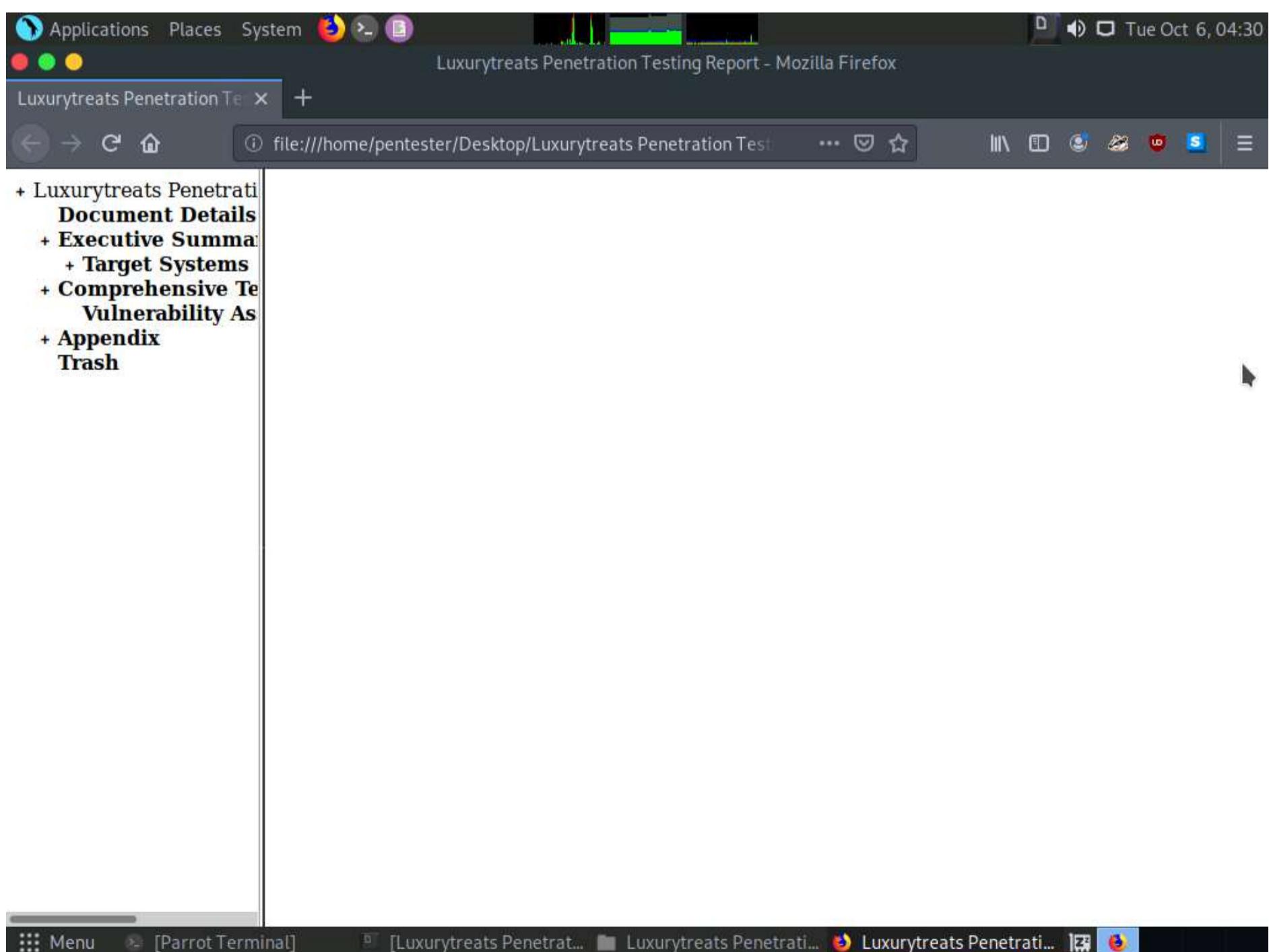


30. Now, the report is saved in the name **Luxurytreats Penetration Testing Report** in **Desktop** folder. Navigate to the **Desktop**, open **Luxurytreats Penetration Testing Report** folder, and right-click **index.html** file and choose **Firefox** as shown in the screenshot.





31. The file opens in the web browser displaying the index of the report in the left pane. You may select each section in the left pane to view a detailed report associated with it in the right pane.



32. Click **Document Details** link in the left pane. You will be displayed with the details of the document in the right pane of the browser window as shown in the screenshot.

The screenshot shows a Linux desktop environment with a terminal window titled '[Parrot Terminal]' in the background. In the foreground, a Mozilla Firefox window is open, displaying a penetration testing report. The title bar reads 'Luxurytreats Penetration Testing Report - Mozilla Firefox'. The address bar shows the URL 'file:///home/pentester/Desktop/Luxurytreats Penetration Test'. The left sidebar contains a tree view with the following structure:

- + Luxurytreats Penetration Test
- + **Document Details** (selected)
- + Executive Summary
- + Target Systems
- + Comprehensive Test Plan
- + Vulnerability Assessment
- + Appendix
- Trash

The right pane displays the following document details:

- Document Title: Luxurytreats Penetration Testing Report
- Company: X-SECURITY
- Recipient: Luxurytreats
- Date: August 18, 2020
- Classification: Confidential
- Document Type: Report
- Version: 1.0
- Author: John
- Pen testers: Micheal, Marshall, Sean, and Adam
- Reviewed By: Allen and Bacon
- Approved By: Clark

33. Click the **Executive Summary** section in the left pane. This displays detailed information regarding the section as shown in the screenshot.



Luxurytreats Penetration Testing Report - Mozilla Firefox

file:///home/pentester/Desktop/Luxurytreats Penetration Test

+ Luxurytreats Penetrati
Document Details
+ Executive Summa
+ Target Systems
+ Comprehensive Te
Vulnerability As
+ Appendix
Trash

x-Security was engaged to conduct penetration testing on the perimeter and network systems of Luxurytreats company during the month of August 2020. X-Security objective was to discover significant vulnerabilities within the Luxurytreats infrastructure. The finding are to be utilized with risk analysis to assist in developing security architecture of Luxurytreats.

34. Expand the **Executive Summary** node, expand the **Target Systems** node and then click **scan.txt** link. This displays all the machines found during the scan as shown in the screenshot.

Luxurytreats Penetration Testing Report - Mozilla Firefox

file:///home/pentester/Desktop/Luxurytreats Penetration Test

+ Luxurytreats Penetrati
Document Details
+ Executive Summa
+ Target Systems
scan.txt
+ Comprehensive Te
Vulnerability As
+ Appendix
Trash

```
Starting Nmap 7.60SVN ( https://nmap.org ) at 2020-08-17 05:17 EST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:17
Completed NSE at 05:17, 0.00s elapsed
Initiating NSE at 05:17
Completed NSE at 05:17, 0.00s elapsed
Initiating Ping Scan at 05:17
Scanning www.luxurytreats.com (172.19.19.11) [4 ports]
Completed Ping Scan at 05:17, 0.22s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 05:17
Scanning www.luxurytreats.com (172.19.19.11) [1000 ports]
Discovered open port 445/tcp on 172.19.19.11
Discovered open port 139/tcp on 172.19.19.11
Discovered open port 135/tcp on 172.19.19.11
Discovered open port 21/tcp on 172.19.19.11
Discovered open port 49156/tcp on 172.19.19.11
Discovered open port 3389/tcp on 172.19.19.11
Discovered open port 80/tcp on 172.19.19.11
Increasing send delay for 172.19.19.11 from 0 to 5 due to 29 out of 71 dropped probes since last increase.
Increasing send delay for 172.19.19.11 from 5 to 10 due to 34 out of 84 dropped probes since last increase.
Warning: 172.19.19.11 giving up on port because retransmission cap hit (6).
Discovered open port 49157/tcp on 172.19.19.11
Discovered open port 49154/tcp on 172.19.19.11
Discovered open port 49153/tcp on 172.19.19.11
Discovered open port 49155/tcp on 172.19.19.11
Discovered open port 49152/tcp on 172.19.19.11
Completed SYN Stealth Scan at 05:18, 43.48s elapsed (1000 total ports)
Initiating Service scan at 05:18
Scanning 12 services on www.luxurytreats.com (172.19.19.11)
Service scan Timing: About 58.33% done; ETC: 05:19 (0:00:39 remaining)
Completed Service scan at 05:19, 58.60s elapsed (12 services on 1 host)
Initiating OS detection (try #1) against www.luxurytreats.com (172.19.19.11)
Retrying OS detection (try #2) against www.luxurytreats.com (172.19.19.11)
Retrying OS detection (try #3) against www.luxurytreats.com (172.19.19.11)
Retrying OS detection (try #4) against www.luxurytreats.com (172.19.19.11)
Retrying OS detection (try #5) against www.luxurytreats.com (172.19.19.11)
Initiating Traceroute at 05:19
Completed Traceroute at 05:19, 1.01s elapsed
Initiating Parallel DNS resolution of 2 hosts at 05:19
```

35. This way, you can create a penetration test report and use it to assess the security posture of an organization. Close all the opened windows.

In this lab, you have learned how to:

- Import Penetration Test Reports from Penetration Test Folder to KeepNote
- Export a Final Penetration Test Report containing all the internal pentest reports

