Lab-5 TASK 1:

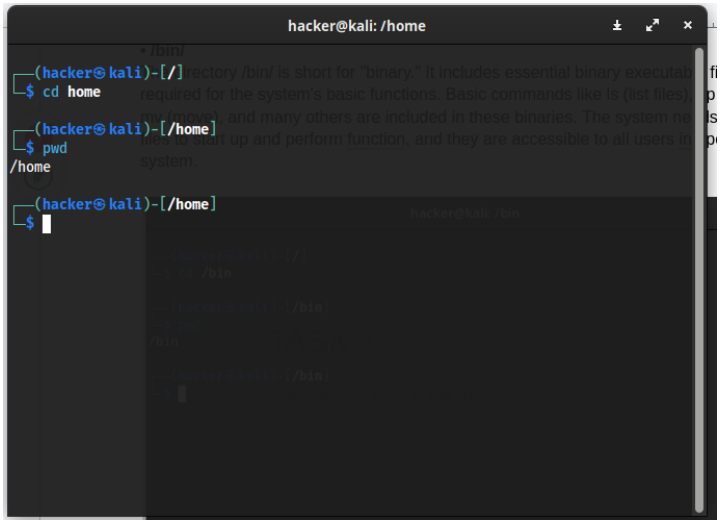
Navigation through multiple directories

• /bin/

The directory /bin/ is short for "binary." It includes essential binary executable files required for the system's basic functions. Basic commands like ls (list files), cp (copy), mv (move), and many others are included in these binaries. The system needs these files to start up and perform functions, and they are accessible to all users in the operating system.

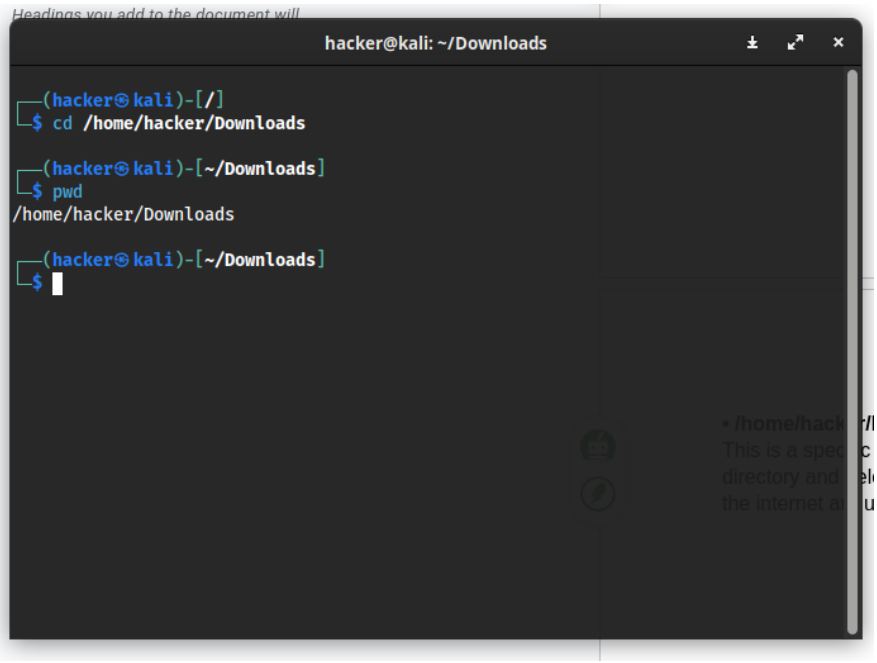
• /home/

The /home/ directory is where user home directories are located. Every user on the system typically has a username-specific subdirectory inside of /home/. Users can keep their private files and data in this location.



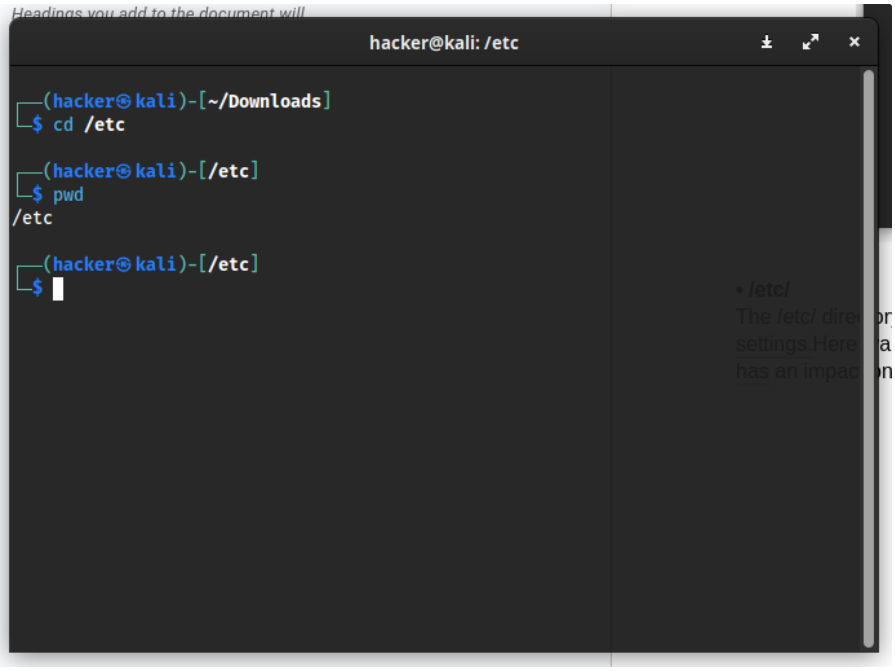
• **/home/hacker/Downloads/**

This is a specific user's Downloads directory. It's a subdirectory within the /home/ directory and belongs to a user named "hacker." This is where files downloaded from the internet are usually stored.



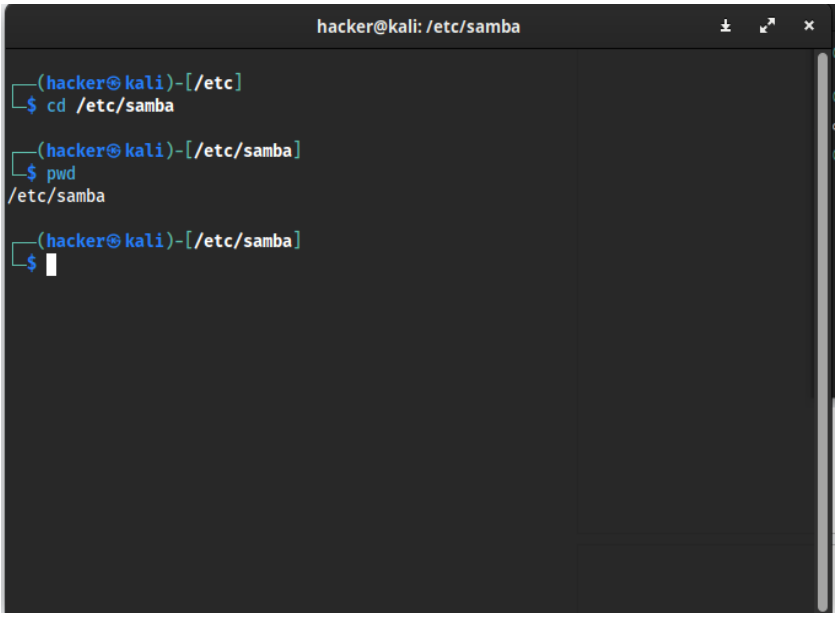
• **/etc/**

The /etc/ directory contains configuration files and system-wide configuration settings.Here, various configuration files for the system and applications are kept, which has an impact on how software functions and how the system functions as a whole.



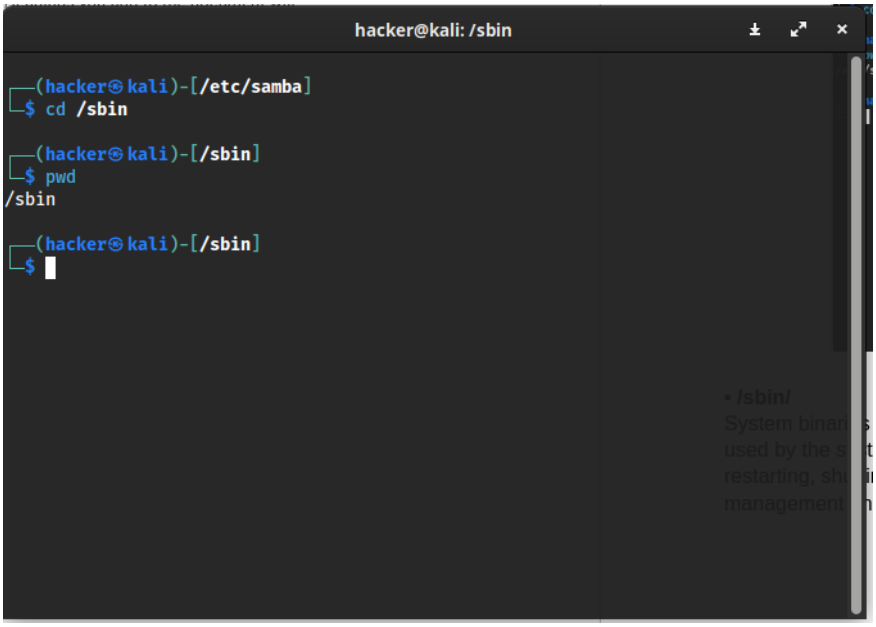
• **/etc/samba/**

Samba is a suite of programs that enables Windows systems and Unix-like systems to share files and printers. The configuration files for Samba, which enables file and printer sharing in a network environment, are probably located in the /etc/samba/ directory.



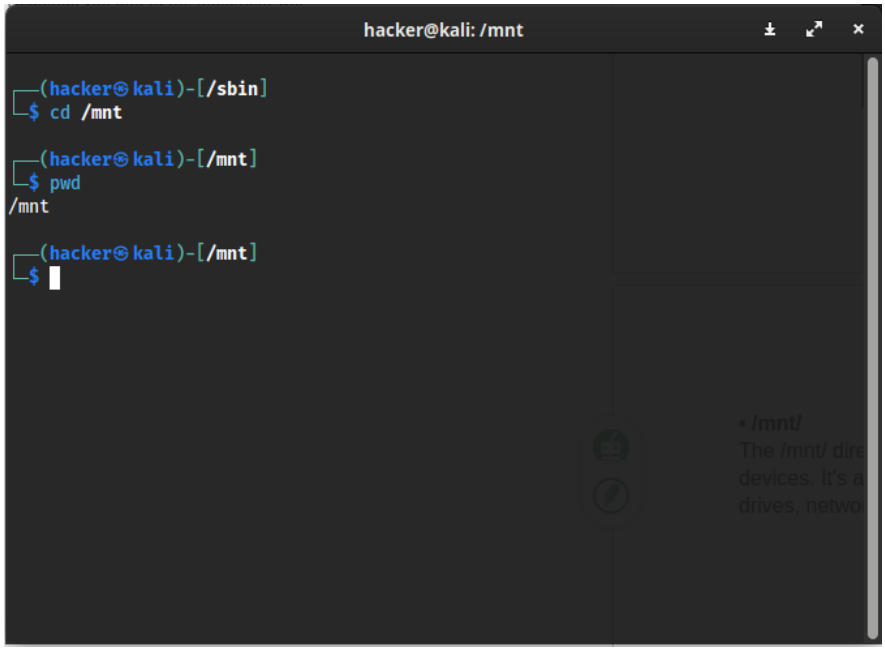
• **/sbin/**

System binaries (executable files) are located in the /sbin/ directory and are primarily used by the system administrator. These binaries are necessary for operations like restarting, shutting down, and configuring system settings as well as other system management and maintenance tasks.



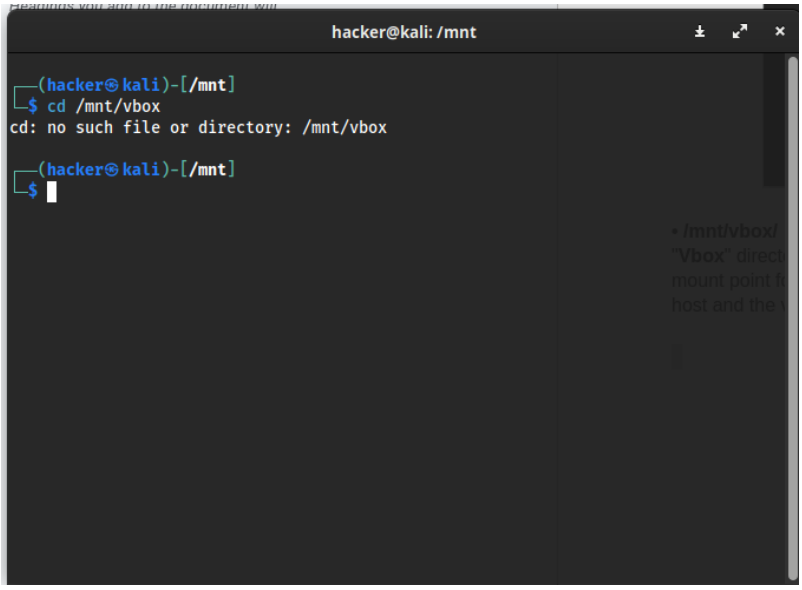
• **/mnt/**

The /mnt/ directory is used as a mount point for temporarily mounting filesystems and devices. It's a common location to temporarily mount external devices such as USB drives, network shares, or additional hard drives.



• **/mnt/vbox/**

"**Vbox**" directory, which is a specific subdirectory of the /mnt/ directory. It may serve as a mount point for a virtual machine's (VM) shared folder, enabling file sharing between the host and the virtual machine. But i didn't have this directory as i am not using any Vhost right now



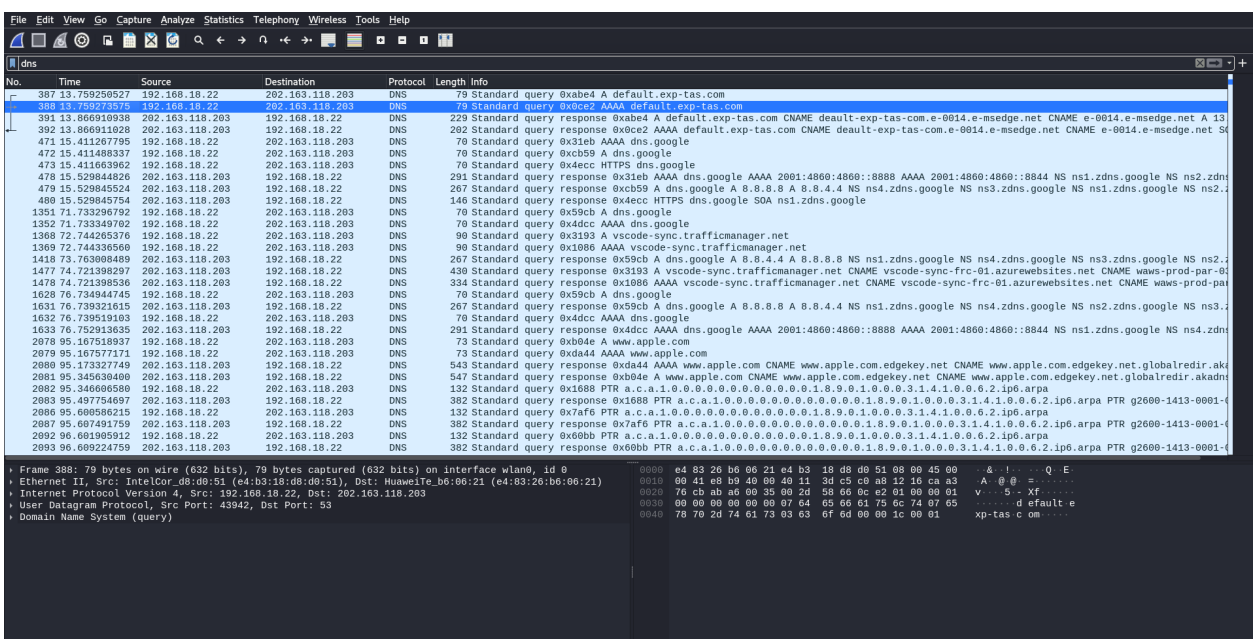
As i have no directory named as **/etc/ufw** so i am using **/etc** directory for future tasks. Here is the screenshot attached where i use the **ls -la** command to check permission for each file available in **/etc** directory

```
hacker@kali: /etc

┌──(hacker㉿kali)-[~]
└─$ cd /etc/gufw
cd: no such file or directory: /etc/gufw

┌──(hacker㉿kali)-[~]
└─$ cd /etc

┌──(hacker㉿kali)-[/etc]
└─$ pwd
/etc
┌──(hacker㉿kali)-[/etc]
└─$ ls -la
total 1840
drwxr-xr-x 205 root     root      12288 Jun 12 03:06 .
drwxr-xr-x  21 root     root       4096 Jul 26 01:17 ..
-rw-r--r--   1 root     root       3040 Dec 25  2022 adduser.conf
-rw-r--r--   1 root     root       3609 Nov 24  2022 adduser.conf.dpkg-save
-rw-r--r--   1 root     root       3623 Nov 24  2022 adduser.conf.update-old
-rw-r--r--   1 root     root         44 Aug 21 11:54 adjtime
-rw-r--r--   1 root     root        198 Feb  6  2023 aliases
drwxr-xr-x   3 root     root       4096 Nov 24  2022 alsa
drwxr-xr-x   2 root     root      36864 Jul 31 20:22 alternatives
-rw-r--r--   1 root     root        401 Jan 11  2023 anacrontab
drwxr-xr-x   8 root     root       4096 Apr 25 06:34 apache2
-rw-r--r--   1 root     root        433 Aug 23  2020 apg.conf
drwxr-xr-x   3 root     root       4096 Apr 11 14:35 apparmor
drwxr-xr-x   9 root     root       4096 Jul 31 20:24 apparmor.d
-rw-r--r--   1 root     root        833 Jan 27  2023 appstream.conf
drwxr-xr-x   8 root     root       4096 Jun 28 01:28 apt
drwxr-xr-x   2 root     root       4096 Apr 11 14:41 arp-scan
drwxr-xr-x   3 root     root       4096 May 20 18:02 avahi
-rw-r--r--   1 root     root       1994 May 12  2022 bash.bashrc
-rw-r--r--   1 root     root         45 Jan 25  2020 bash_completion
drwxr-xr-x   2 root     root       4096 Jun 28 00:58 bash_completion.d
-rw-r--r--   1 root     root        367 Jul 29  2019 bindresvport.blacklist
drwxr-xr-x   2 root     root       4096 Jun 28  2022 binfmt.d
drwxr-xr-x   2 root     root       4096 Jan 30  2023 bluetooth
drwxr-xr-x   3 root     root       4096 Nov 24  2022 ca-certificates
-rw-r--r--   1 root     root       6250 Apr 11 13:40 ca-certificates.conf
-rw-r--r--   1 root     root       5529 Nov 24  2022 ca-certificates.conf.dpkg-old
-rw-r--r--   1 root     root        119 Jan 11  2022 catdocrc
drwxr-s---   2 root     dip        4096 Jan 30  2023 chatscripts
drwxr-xr-x   3 root     root       4096 Nov 24  2022 chromium
drwxr-xr-x   2 root     root       4096 Apr 11 14:43 cifs-utils
drwxr-xr-x   3 root     root       4096 Nov 24  2022 cloud
drwxr-xr-x   2 root     root       4096 Jul  4 16:58 console-setup
drwxr-xr-x   2 root     root       4096 Feb 24 18:20 cracklib
drwxr-xr-x   2 root     root       4096 Jul 31 20:23 cron.d
drwxr-xr-x   2 root     root       4096 Jul 31 20:23 cron.daily
```

Lab-5 TASK 2:

```
hacker@kali: /etc

┌──(hacker㉿kali)-[/etc]
└─$ ping www.apple.com

PING www.apple.com(g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca)) 56 data bytes
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=1 ttl=55 time=
102 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=2 ttl=55 time=
102 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=3 ttl=55 time=
101 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=4 ttl=55 time=
98.2 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=5 ttl=55 time=
109 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=6 ttl=55 time=
96.6 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=7 ttl=55 time=
104 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=8 ttl=55 time=
120 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=9 ttl=55 time=
96.0 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=10 ttl=55 time
=97.5 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=11 ttl=55 time
=107 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=12 ttl=55 time
=96.0 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=13 ttl=55 time
=110 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=14 ttl=55 time
=97.0 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=15 ttl=55 time
=101 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=16 ttl=55 time
=99.1 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=17 ttl=55 time
=97.8 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=18 ttl=55 time
=97.3 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=19 ttl=55 time
=96.0 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=20 ttl=55 time
=110 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=21 ttl=55 time
=118 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=22 ttl=55 time
=102 ms
64 bytes from g2600-1413-0001-0981-0000-0000-0000-1aca.deploy.static.akamaitechnologies.com (2600:1413:1:981::1aca): icmp_seq=23 ttl=55 time
```

Wireshark screenshot:



Wireshark · Packet 388 · wlan0

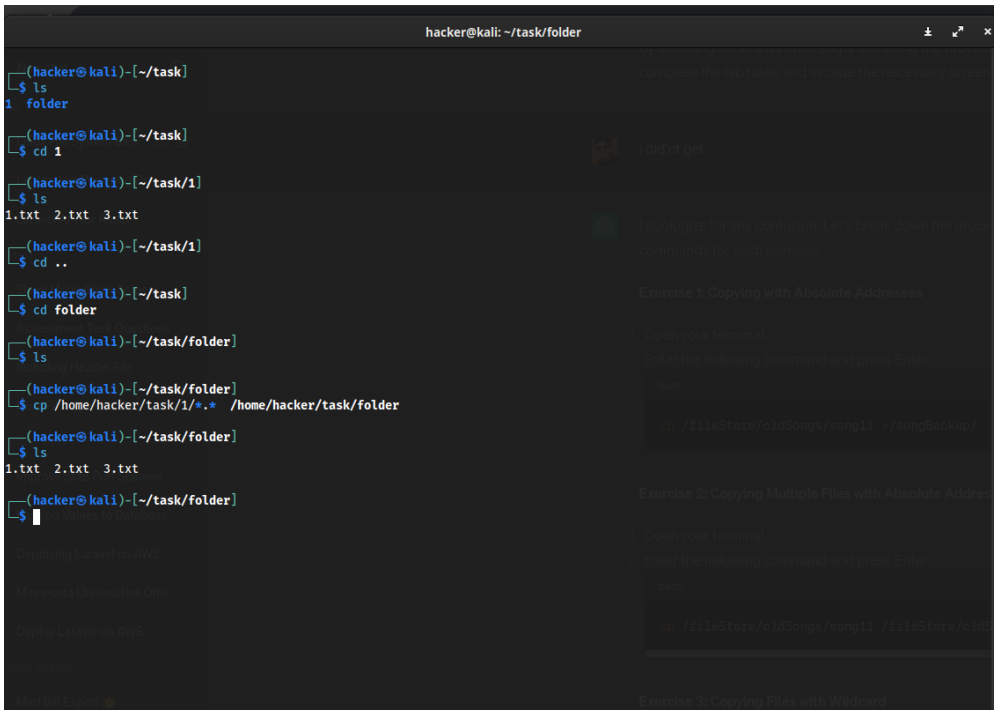
```
  ▸ Destination: HuaweiTe_b6:06:21 (e4:83:26:b6:06:21)
  ▸ Source: IntelCor_d8:d0:51 (e4:b3:18:d8:d0:51)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 192.168.18.22, Dst: 202.163.118.203
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 65
    Identification: 0xe8b9 (59577)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x3dc5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.18.22
    Destination Address: 202.163.118.203
▾ User Datagram Protocol, Src Port: 43942, Dst Port: 53
    Source Port: 43942
    Destination Port: 53
    Length: 45
    Checksum: 0x5866 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 28]
  ▸ [Timestamps]
    UDP payload (37 bytes)
▾ Domain Name System (query)
    Transaction ID: 0x0ce2
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
    [Response In: 392]

0000  e4 83 26 b6 06 21 e4 b3  18 d8 d0 51 08 00 45 00   ··&··!·· ···Q··E·
0010  00 41 e8 b9 40 00 40 11  3d c5 c0 a8 12 16 ca a3   ·A··@·@· =·····
0020  76 cb ab a6 00 35 00 2d  58 66 0c e2 01 00 00 01   v····5·- Xf·····
0030  00 00 00 00 00 00 07 64  65 66 61 75 6c 74 07 65   ·····d efault·e
0040  78 70 2d 74 61 73 03 63  6f 6d 00 00 1c 00 01      xp-tas·c om·····
```

✓ Show packet bytes

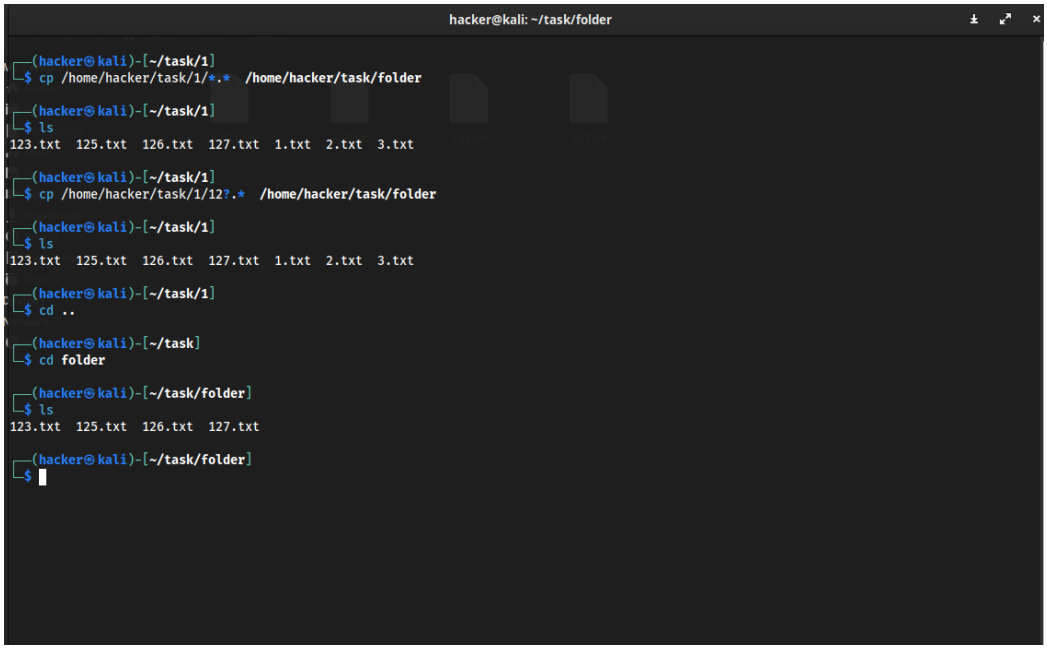
Close Help

Lab-6 Task 2:

COPY:



CP using ? while card



Move using wild card

```
hacker@kali: ~/task/moving_here

┌──(hacker㉿kali)-[~/task/folder]
└─$ ls
123.txt  125.txt  126.txt  127.txt

┌──(hacker㉿kali)-[~/task/folder]
└─$ mkdir /home/hacker/task/moving_here

┌──(hacker㉿kali)-[~/task/folder]
└─$ mv /home/hacker/task/1/12?.*  /home/hacker/task/moving_here

┌──(hacker㉿kali)-[~/task/folder]
└─$ ls
123.txt  125.txt  126.txt  127.txt

┌──(hacker㉿kali)-[~/task/folder]
└─$ cd /home/hacker/task/moving_here

┌──(hacker㉿kali)-[~/task/moving_here]
└─$ ls
123.txt  125.txt  126.txt  127.txt

┌──(hacker㉿kali)-[~/task/moving_here]
└─$
```

Deleting the empty folder

```
hacker@kali: ~/task

┌──(hacker㉿kali)-[~/task/moving_here]
└─$ ls
123.txt  125.txt  126.txt  127.txt

┌──(hacker㉿kali)-[~/task/moving_here]
└─$ cd ..

┌──(hacker㉿kali)-[~/task]
└─$ ls
1  folder  moving_here

┌──(hacker㉿kali)-[~/task]
└─$ rm folder
rm: cannot remove 'folder': Is a directory

┌──(hacker㉿kali)-[~/task]
└─$ rm -r folder

┌──(hacker㉿kali)-[~/task]
└─$
```

ITECH1102 Week 10 lab sheet: Security 1
Part 1 – Investigate the history of Malware

- 1
  Year: 2001
  Name: Code Red
  Impact: Denial of service (DoS) attacks were quickly launched by this malware on vulnerable web servers. It highlighted the requirement for improved web server security procedures.

- 2
  Year: 2001
  Name: Code Red
  Impact: By taking advantage of a flaw in Microsoft SQL Server, Slammer caused significant network outages. The swift spread of it significantly reduced internet traffic.

- 3

  Year: 2003
  Name: Slammer (SQL Slammer)
  Impact:Internet traffic is slowed down as a result of widespread network disruptions caused by rapid propagation.

- 4
  Year: 2017
  Name: WannaCry
  Impact:File encryption and demands for ransom payments, which have an impact on crucial systems like healthcare.

- 5
  Year: 2010
  Name: Zeus
  Impact: By using stolen banking credentials, criminals can steal identities and cause financial losses.

Part 2 – Cyber Safety

In the present era, ensuring our safety on the Internet is compulsory. Here are some essential tips to stay secure online:

Use Strong and Unique passwords.
Mix letters, numbers, and symbols to create strong complex passwords. Use uncommon words and information that can be guessed, such as birthdays.

Enable Two-Factor Authentication (2FA):
switch on Two-factor authentication. By requiring a second method of identity verification, like a text message or app, this adds an extra layer of security.

Keep Software Updated:
Update your operating system, programs, and antivirus software frequently. Security patches that protect against well-known vulnerabilities are frequently included in updates.

Beware of Phishing Attempts:
Consider attention when responding to unidentified emails or messages that request personal information. Don't open attachments from shady sources or click on suspicious links.

Secure Wi-Fi Connections:
Use unique, strong passwords for your Wi-Fi networks. Avoid using public Wi-Fi for sharing sensitive data and doing personal activities. Always consider using a VPN to encrypt your online traffic.

Monitor Privacy Settings:
On social media sites and other online accounts, change the privacy settings. Don't share too much personal information online.

Regularly Back Up Data:
Make a backup of your crucial files on an external drive or in the cloud. Your data is secure even if there is a hardware malfunction or cyberattack.

Use Secure Websites:
Make sure the website uses "https://" and has a padlock icon in the address bar before sharing sensitive information or conducting an online transaction.

Be Concious with Downloads:
Download software, applications, and files only from reliable websites. Do not download files from unreliable websites or pop-up ads.

Educate Yourself:
Keep up with the most recent cybersecurity threats and recommended procedures. Become informed so that you and your family can identify potential risks.

Personal Rating: 8/10

I am committed to maintaining a high level of personal effort to maintain cyber safety.Best practices like using secure passwords, keeping software up to date, and being watchful of online threats are things I consistently do. However, there is always room for improvement, so I am actively trying to stay informed about changing cybersecurity trends in order to further improve my online security.

Part 3 – Botnets.

Botnets are complex networks of hacked servers, devices, and computers that are controlled by bad actors. These networked devices, also known as "bots," are frequently infected with malware, which enables the attacker to control them from a distance. From a few to hundreds of thousands of devices, this network can be a strong and disruptive force on the internet.

The main function of botnets is to carry out various cybercriminal activities, frequently without the device owners' knowledge. One of the most frequent applications is the launch of Distributed Denial of Service (DDoS) attacks, in which the botnet floods a target server or website with a tremendous amount of traffic, rendering it inaccessible. Additionally, botnets are used to distribute malware, send spam emails, steal sensitive data from data breaches, and even mine cryptocurrencies using a method called cryptojacking.

Botnet defense is a difficult task. It necessitates a collaboration between technological advancements and global cooperation. Security professionals are working to locate and destroy the command and control servers that operate the botnet. To stop devices from joining a botnet, it is crucial to regularly update software and use powerful security tools.

In order to build a botnet, devices must be infected using a variety of techniques, including phishing emails, malicious downloads, and software exploits. These devices can be remotely controlled by the botnet operator once they are infected, who can then coordinate their actions to accomplish their objectives.

The dynamic nature of cyberthreats and the demand for preventative cybersecurity measures are highlighted by botnets. As technology develops, so do cybercriminals' strategies. preventing bot attacks