PART 1: Basic Commands

1.Log In to the SU user, Navigate to the Home/ desktop folder, and perform the following:
Zaloguj się jako użytkownik SU, przejdź do folderu Home/desktop i wykonaj następujące czynności:

A.Create Three New directories and Three New files, using a single command.
Utwórz trzy nowe katalogi i trzy nowe pliki za pomocą jednej komendy.

```
┌──(kali㉿kali)-[~]
└─$ mkdir dir1 dir2 dir3 && touch file1 file2 file3
```

B.Move the files to one of the directories.
Przenieś pliki do jednego z katalogów.

```
┌──(kali㉿kali)-[~]
└─$ mv file1 file2 file3 dir1/
```

C. Navigate to the directory which contains the files and move the files to another directory.
Przejdź do katalogu zawierającego pliki i przenieś je do innego katalogu.

```
┌──(kali㉿kali)-[~]
└─$ cd dir1/
```

```
┌──(kali㉿kali)-[~/dir1]
└─$ mv file1 file2 file3 ../dir2/
```

D Delete the files from the directory
Usuń pliki z katalogu.

```
┌──(kali㉿kali)-[~/dir1]
└─$ rm ../dir2/file1 ../dir2/file2 ../dir2/file3
```

2.Check the path of the current directory.
Sprawdź ścieżkę bieżącego katalogu.

```
┌──(kali㉿kali)-[~/dir1]
└─$ pwd
/home/kali/dir1
```

3.Navigate to the desktop directory and display the files and folders it contains
Przejdź do katalogu "desktop" i wyświetl zawartość plików i folderów.

```
┌──(kali㉿kali)-[~/dir1]
└─$ cd ~/Desktop
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l
total 0
```

4.Are there any hidden files or folders?
Czy istnieją jakieś ukryte pliki lub foldery?

No.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -a
.  ..
```

5.Check through which user you are connected to the system, using two ways.
Sprawdź, przez jakiego użytkownika jesteś podłączony do systemu, używając dwóch sposobów.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ whoami
kali
```

```
┌──(kali㉿kali)-[~/ukryte]
└─$ id -un
kali
```

6.Change a user's password

Zmień hasło użytkownika.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ passwd kali
Changing password for kali.
Current password:
New password:
Retype new password:
passwd: password updated successfully
```

7.What does the cd command perform?

co robi polecenie cd?

The cd (change directory) command is used in Unix-like operating systems to change the current working directory to a different directory specified by the user.

Polecenie cd (change directory) jest używane w systemach operacyjnych podobnych do Unix do zmiany bieżącego katalogu roboczego na inny katalog określony przez użytkownika.

Change to a specific directory: cd Documents

Zmiana na konkretny katalog: cd Documents

```
┌──(kali㉿kali)-[~]
└─$ cd Documents

┌──(kali㉿kali)-[~/Documents]
└─$
```

- Changes the current working directory to directory_name. The directory can be specified using either a relative or an absolute path.

Zmienia bieżący katalog roboczy na directory_name. Katalog może być określony za pomocą ścieżki względnej lub bezwzględnej.

Moving to the home directory: cd or cd ~

Przejście do katalogu domowego: cd lub cd ~

```
┌──(kali㉿kali)-[~/Documents]
└─$ cd ~

┌──(kali㉿kali)-[~]
└─$ cd
```

- Without any arguments, cd changes the current directory to the user's home directory.

Bez żadnych argumentów, cd zmienia bieżący katalog na katalog domowy użytkownika.

Using absolute paths: cd /path/to/directory

Używanie ścieżek bezwzględnych: cd /path/to/directory

```
┌──(kali㉿kali)-[~]
└─$ cd path/to/directory

┌──(kali㉿kali)-[~/path/to/directory]
└─$
```

- This command changes the current directory to the specified absolute path.

To polecenie zmienia bieżący katalog na określoną ścieżkę bezwzględną.

Using relative paths: cd ./directory

Używanie ścieżek względnych: cd ./directory

```
┌──(kali㉿kali)-[~/path/to]
└─$ cd ./directory

┌──(kali㉿kali)-[~/path/to/directory]
└─$
```

- This changes the current directory to a subdirectory within the current directory.

zmienia bieżący katalog na podkatalog w bieżącym katalogu

Parent Directory: cd ..

Katalog nadrzędny: cd ..

```
┌──(kali㉿kali)-[~/path/to/directory]
└─$ cd ..

┌──(kali㉿kali)-[~/path/to]
└─$
```

- Moves the current directory up one level to the parent directory.

Przesuwa bieżący katalog o jeden poziom wyżej do katalogu nadrzędnego.

Change to the Previous Directory: cd -

Zmiana na poprzedni katalog: cd -

```
┌──(kali㉿kali)-[~/path/to]
└─$ cd -
~/path/to/directory

┌──(kali㉿kali)-[~/path/to/directory]
└─$
```

Switches back to the previous working directory. This can be useful for toggling between two directories.

Przełącza z powrotem na poprzedni katalog roboczy. Może to być przydatne do przełączania między dwoma katalogami.

8.What does cd / perform?

co robi komenda cd / ?

Change to the Root Directory: cd /

Zmiana na katalog główny: cd /

```
┌──(kali㉿kali)-[~/path/to/directory]
└─$ cd /

┌──(kali㉿kali)-[/]
└─$
```

- Changes the current working directory to the root directory of the filesystem.

Zmienia bieżący katalog roboczy na katalog główny systemu plików.

9.Execute cd and cd/ and inspect the output

Wprowadz polecenie cd i cd/ i sprawdź wynik

```
┌──(kali㉿kali)-[~/Documents]
└─$ cd ~

┌──(kali㉿kali)-[~]
└─$ cd
```

```
┌──(kali㉿kali)-[~/path/to/directory]
└─$ cd /

┌──(kali㉿kali)-[/]
└─$
```

```
┌──(kali㉿kali)-[~/ukryte]
└─$ cd

┌──(kali㉿kali)-[~]
└─$
```

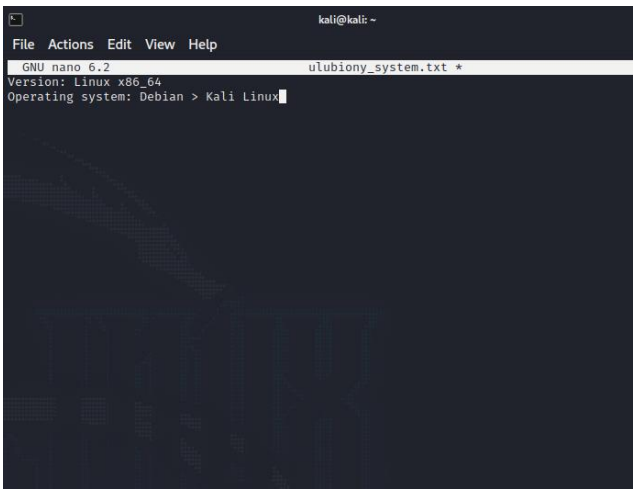
10.Clean the terminal from output

Wyczyść terminal z wyniku

```
┌──(kali㉿kali)-[~]
└─$ clear
```

11.Create a file using nano and write the name of your favorite operating system. In addition, find a way to display the type of the current operating system and add the output to the file.

Utwórz plik za pomocą nano i wpisz nazwę swojego ulubionego systemu operacyjnego. Ponadto znajdź sposób na wyświetlenie typu bieżącego systemu operacyjnego i dodaj wynik do pliku.



Linux is a core of the system, while Debian is the distribution of it.

The Linux kernel forms the core of the operating system and manages computer hardware. It is responsible for handling processes, memory management, devices, and facilitating communication between them.

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2022.2"
VERSION_ID="2022.2"
VERSION_CODENAME="kali-rolling"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
```

```
┌──(kali㉿kali)-[~]
└─$ uname -s -m
Linux x86_64
```

The first part (uname -s) shows the name of the operating system kernel, which is typically "Linux".

Pierwsza część (uname -s) pokazuje nazwę jądra systemu operacyjnego, która zwykle jest "Linux".

The second part (uname -m) shows the hardware architecture on which the operating system is running.

Druga część (uname -m) pokazuje architekturę sprzętową, na której działa system operacyjny.

12.Execute a command that will display the file’s content.

Wykonaj polecenie, które wyświetli zawartość pliku.

```
┌──(kali㉿kali)-[~]
└─$ cat ulubiony_system.txt
Version: Linux x86_64
Operating system: Debian > Kali Linux
```

13.Create Three hidden files.

Stworz ukryte pliki

```
┌──(kali㉿kali)-[~/ukryte]
└─$ touch .ukryty1 .ukryty2 .ukryty3

┌──(kali㉿kali)-[~/ukryte]
└─$ ls -a
.  ..  .ukryty1  .ukryty2  .ukryty3
```

ls –a = All files, hidden included.

14.Execute command that will display those files.

wykonaj komende która wyświetli te pliki

```
┌──(kali㉿kali)-[~/ukryte]
└─$ ls -a
.  ..  .ukryty1  .ukryty2  .ukryty3
```

15.Delete the hidden files that were created in step 13.

usun ukryte pliki z kroku 13

```
┌──(kali㉿kali)-[~/ukryte]
└─$ ls -a
.  ..  .ukryty1  .ukryty2  .ukryty3

┌──(kali㉿kali)-[~/ukryte]
└─$ rm .ukryty*

┌──(kali㉿kali)-[~/ukryte]
└─$ ls -a
.  ..
```

PART 2: The find command

16.Create files in each system directory and display the paths of those files.

Utwórz pliki w każdym katalogu systemowym i wyświetl ścieżki tych plików.

```
┌──(kali㉿kali)-[~]
└─$ sudo touch /bin/moj_plik
sudo touch /boot/moj_plik
sudo touch /dev/moj_plik
sudo touch /etc/moj_plik
sudo touch /home/moj_plik
sudo touch /lib/moj_plik
sudo touch /mnt/moj_plik
sudo touch /opt/moj_plik
sudo touch /proc/moj_plik
sudo touch /root/moj_plik
sudo touch /run/moj_plik
sudo touch /sbin/moj_plik
sudo touch /srv/moj_plik
sudo touch /sys/moj_plik
sudo touch /tmp/moj_plik
sudo touch /usr/moj_plik
sudo touch /var/moj_plik
[sudo] password for kali:
touch: cannot touch '/proc/moj_plik': No such file or directory
touch: cannot touch '/sys/moj_plik': Permission denied

┌──(kali㉿kali)-[~]
└─$ sudo find / -name "moj_plik"
/boot/moj_plik
/root/moj_plik
/etc/moj_plik
/mnt/moj_plik
/tmp/moj_plik
/var/moj_plik
/home/moj_plik
/run/moj_plik
find: '/run/user/1000/doc': Permission denied
find: '/run/user/1000/gvfs': Permission denied
/srv/moj_plik
/dev/moj_plik
/opt/moj_plik
/usr/lib/moj_plik
/usr/bin/moj_plik
/usr/sbin/moj_plik
/usr/moj_plik
```

17.Navigate to the root directory and display all the files that begin with three digits.

Przejdź do katalogu głównego i wyświetl wszystkie pliki, które zaczynają się od trzech cyfr.

```
┌──(kali㉿kali)-[~]
└─$ cd /
```

```
┌──(kali㉿kali)-[/]
└─$ ls
123  bin   etc         initrd.img.old  lib64       media  proc  sbin  tmp  vmlinuz
345  boot  home        lib             libx32      mnt    root  srv   usr  vmlinuz.old
678  dev   initrd.img  lib32           lost+found  opt    run   sys   var

┌──(kali㉿kali)-[/]
└─$ ls -d [0-9] [0-9] [0-9]*
ls: cannot access '[0-9]': No such file or directory
ls: cannot access '[0-9]': No such file or directory
 123   345   678
```

18.Search for all the files in the system that begin with five numbers.

Wyszukaj wszystkie pliki w systemie, które zaczynają się od pięciu cyfr.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# sudo find / -type f -name '[0-9][0-9][0-9][0-9][0-9]*'
```

Sudo command is not necessary in this example, because we have root privilege actually.

19.Search for all the files in the system that start with the word „bash”

Znajdź wszystkie pliki w systemie, które zaczynają się od słowa „bash”.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# find / -type f -name 'bash'
/etc/apparmor.d/abstractions/bash
find: ‘/run/user/1000/doc’: Permission denied
find: ‘/run/user/1000/gvfs’: Permission denied
/usr/bin/bash
/usr/share/menu/bash
/usr/share/lintian/overrides/bash
```

20. Search for all the directories that are smaller than 4 MB.

Znajdź wszystkie katalogi mniejsze niż 4 MB.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─#  find / -type d -size -4M
```

21.Search for all the files that are smaller than 3MB.

Znajdź wszystkie pliki mniejsze niż 3 MB.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# sudo find / -type f -size -3M
```

PART 3: User & Group management

1.Create a user in two different ways.

Stwórz użytkownika na dwa różne sposoby.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# adduser pierwszy
Adding user `pierwszy' ...
Adding new group `pierwszy' (1007) ...
Adding new user `pierwszy' (1005) with group `pierwszy' ...
Creating home directory `/home/pierwszy' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
No password has been supplied.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for pierwszy
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
```

```
┌──(root㉿kali)-[/home/kali]
└─# useradd drugi
```

```
drugi
pierwszy
```

2.When generating a user in the longer method, create a password.

Przy tworzeniu użytkownika w dłuższy sposób, ustaw hasło.

New password: (password)

```
┌──(root㉿kali)-[/home/kali]
└─# passwd drugi
New password:
Retype new password:
passwd: password updated successfully
```

3.Create a new group.

Utwórz nową grupę.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo addgroup nowagrupa
Adding group `nowagrupa' (GID 1008) ...
Done.
```

4.Move a user to the newly created group.

Przenieś użytkownika do nowo utworzonej grupy.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo usermod -a -G nowagrupa pierwszy
```

5.Which command allows to find all users and their groups.

Jakie polecenie pozwala znaleźć wszystkich użytkowników i ich grupy.

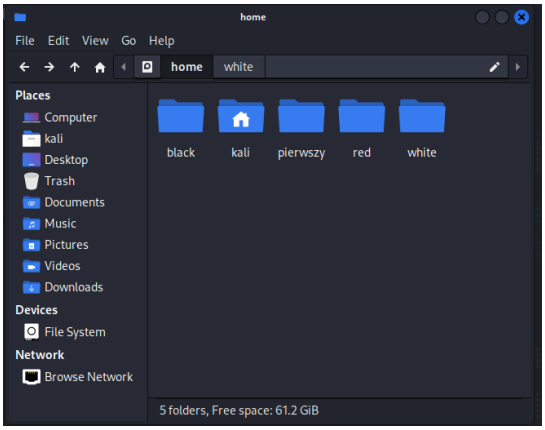
```
┌──(root㉿kali)-[/home/kali]
└─# nano /etc/group
```

```
  GNU nano 6.2
ssl-cert:x:117:postgres
plocate:x:118:
wireshark:x:119:kali
tcpdump:x:120:
bluetooth:x:121:kali
i2c:x:122:
avahi:x:123:
stunnel4:x:999:stunnel4
rtkit:x:124:
Debian-snmp:x:125:
sslh:x:126:
kali-trusted:x:127:
postgres:x:128:
nm-openvpn:x:129:
nm-openconnect:x:130:
pulse:x:131:
pulse-access:x:132:
scanner:x:133:saned,kali
saned:x:134:
sambashare:x:135:
inetsim:x:136:
lightdm:x:137:
colord:x:138:
geoclue:x:139:
kpadmins:x:140:
kali:x:1000:
vboxsf:x:141:kali
kaboxer:x:142:kali
pipewire:x:143:
fwupd-refresh:x:998:
polkitd:x:997:
Debian-gdm:x:144:
white:x:1001:
black:x:1002:
red:x:1003:
offensive:x:1004:black
defensive:x:1005:red,white
drugi:x:1006:
pierwszy:x:1007:
nowagrupa:x:1008:pierwszy
```

6.What is the location of all the user directories in the system?

Gdzie znajdują się wszystkie katalogi użytkowników w systemie?

```
┌──(root㉿kali)-[/home/kali]
└─# ls -la /home
total 64
drwxr-xr-x  7 root     root      4096 Jun 27 10:34 .
drwxr-xr-x 19 root     root     36864 May 12  2022 ..
drwxr-xr-x  4 black    black     4096 Jun 16 04:10 black
drwxr-xr-x 17 kali     kali      4096 Jun 27 10:29 kali
drwxr-xr-x  4 pierwszy pierwszy  4096 Jun 27 10:34 pierwszy
drwxr-xr-x  4 red      red       4096 Jun 16 04:19 red
drwxr-xr-x  4 white    white     4096 Jun 16 04:09 white
```



7.Switch to another user.

Przełącz się na innego użytkownika.

```
┌──(kali㉿kali)-[~]
└─$ su pierwszy
Password:
┌──(pierwszy㉿kali)-[/home/kali]
└─$ su trzeci
Password:
┌──(trzeci㉿kali)-[/home/kali]
```

8.Create a directory with that user.

Utwórz katalog z tym użytkownikiem.

```
┌──(trzeci㉿kali)-[/home/kali]
└─$ sudo mkdir /home/Trzeci/nowy
```

```
┌──(trzeci㉿kali)-[/home/kali]
└─$ ls -l /home/trzeci
total 4
drwxr-xr-x 2 root root 4096 Jun 27 10:58 nowy
```

9.Which operation should be performed to create a directory.

Jaką operację należy wykonać, aby utworzyć katalog.

mkdir /nameofdirectory…

10.Switch to root user, create a new user, and add him to the sudo group via a single command.

Przełącz się na użytkownika roota, utwórz nowego użytkownika i dodaj go do grupy sudo jednym poleceniem.

```
┌──(kali㉿kali)-[~]
└─$ sudo su root -c 'useradd -m admin4 && usermod -aG sudo admin4'
```

Part 4: Permissions

1. Create two new files in one of the directories you created in part 1, and grant only write permission to all files inside the directory.

Utwórz dwa nowe pliki w jednym z katalogów utworzonych w części 1 i nadaj tylko uprawnienia do zapisu wszystkim plikom wewnątrz tego katalogu.

```
┌──(kali㉿kali)-[~]
└─$ cd dir1/

┌──(kali㉿kali)-[~/dir1]
└─$ touch plik1 plik2

┌──(kali㉿kali)-[~/dir1]
└─$ ls
plik1  plik2
```

```
┌──(kali㉿kali)-[~/dir1]
└─$ chmod a=w plik1 plik2

┌──(kali㉿kali)-[~/dir1]
└─$ ls -l
total 0
--w--w--w- 1 kali kali 0 Jun 28 09:35 plik1
--w--w--w- 1 kali kali 0 Jun 28 09:35 plik2
```

2. Grant the highest permission to files and verify the change.

Nadaj najwyższe uprawnienia do plików i sprawdź zmianę.

```
┌──(kali㉿kali)-[~/dir1]
└─$ chmod 777 plik1 plik2

┌──(kali㉿kali)-[~/dir1]
└─$ ls -l
total 0
-rwxrwxrwx 1 kali kali 0 Jun 28 09:35 plik1
-rwxrwxrwx 1 kali kali 0 Jun 28 09:35 plik2
```

3. Choose one file and change the owner of the file.

Wybierz jeden plik i zmień właściciela pliku.

```
┌──(kali㉿kali)-[~/dir1]
└─$ sudo chown admin1 plik1

┌──(kali㉿kali)-[~/dir1]
└─$ ls -l
total 0
-rwxrwxrwx 1 admin1 kali 0 Jun 28 09:35 plik1
-rwxrwxrwx 1 kali   kali 0 Jun 28 09:35 plik2
```

Part 5: ALIAS

1. Change the command ifconfig to ipconfig.

Zmień polecenie ifconfig na ipconfig

```
┌──(kali㉿kali)-[~]
└─$ alias ipconfig='ifconfig'

┌──(kali㉿kali)-[~]
└─$ ipconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.242  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fedb:966a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:db:96:6a  txqueuelen 1000  (Ethernet)
        RX packets 273  bytes 53287 (52.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 45  bytes 12590 (12.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.242  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fedb:966a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:db:96:6a  txqueuelen 1000  (Ethernet)
        RX packets 273  bytes 53287 (52.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 45  bytes 12590 (12.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
```

2. Apply the change to all users.

Zastosuj tę zmianę dla wszystkich użytkowników.

The /etc/bash.bashrc file is used to configure Bash shell settings for all users of the system.

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/bash.bashrc
```

At end of file, put the alias line.

```
  GNU nano 7.2                          /etc/bash.bashrc
# update the values of LINES and COLUMNS.
shopt -s checkwinsize

# set variable identifying the chroot you work in (used in the prompt below)
if [ -z "${debian_chroot:-}" ] && [ -r /etc/debian_chroot ]; then
    debian_chroot=$(cat /etc/debian_chroot)
fi

# set a fancy prompt (non-color, overwrite the one in /etc/profile)
# but only if not SUDOing and have SUDO_PS1 set; then assume smart user.
#if ! [ -n "${SUDO_USER}" -a -n "${SUDO_PS1}" ]; then
#  PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
#fi

# Commented out, don't overwrite xterm -T "title" -n "icontitle" by default.
# If this is an xterm set the title to user@host:dir
#case "$TERM" in
#xterm*|rxvt*)
#    PROMPT_COMMAND='echo -ne "\033]0;${USER}@${HOSTNAME}: ${PWD}\007"'
#    ;;
#*)
#    ;;
#esac

# enable bash completion in interactive shells
#if ! shopt -oq posix; then
#  if [ -f /usr/share/bash-completion/bash_completion ]; then
#    . /usr/share/bash-completion/bash_completion
#  elif [ -f /etc/bash_completion ]; then
#    . /etc/bash_completion
#  fi
#fi

# if the command-not-found package is installed, use it
if [ -x /usr/lib/command-not-found -o -x /usr/share/command-not-found/command-not-found ]; then
        function command_not_found_handle {
                # check because c-n-f could've been removed in the meantime
                if [ -x /usr/lib/command-not-found ]; then
                   /usr/lib/command-not-found -- "$1"
                   return $?
                elif [ -x /usr/share/command-not-found/command-not-found ]; then
                   /usr/share/command-not-found/command-not-found -- "$1"
                   return $?
                else
                   printf "%s: command not found\n" "$1" >&2
                   return 127
                fi
        }
fi
alias ipconfig='ifconfig'
```

To apply the changes, you can either log out and log back in, or load the configuration file:

```
┌──(kali㉿kali)-[~]
└─$ source  /etc/bash.bashrc
Command 'shopt' not found, did you mean:
  command 'shout' from deb libshout-tools
Try: sudo apt install <deb name>

┌──(kali㉿kali)-[~]
└─$ ipconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.134  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe42:2da1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:42:2d:a1  txqueuelen 1000  (Ethernet)
        RX packets 259  bytes 30411 (29.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 3718 (3.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ su wito
Password:
┌──(wito㉿kali)-[/home/kali]
└─$ ipconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.134  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe42:2da1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:42:2d:a1  txqueuelen 1000  (Ethernet)
        RX packets 260  bytes 30629 (29.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 3718 (3.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3. Choose any command and change it for one of the users.

Wybierz dowolne polecenie i zmień je dla jednego z użytkowników.

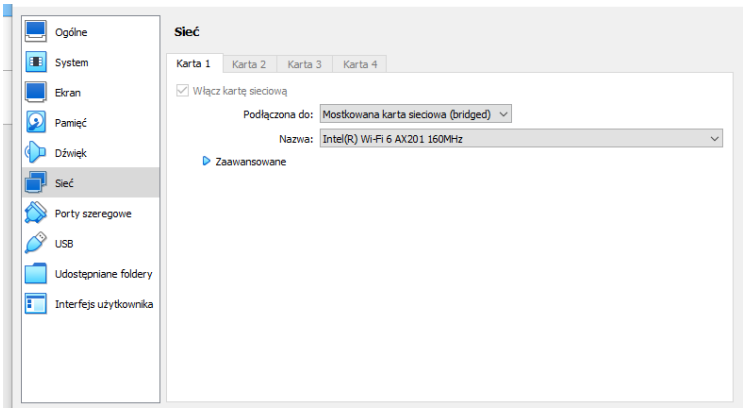
```
┌──(kali㉿kali)-[~]
└─$ nano plik.txt

┌──(kali㉿kali)-[~]
└─$ source plik.txt

┌──(kali㉿kali)-[~]
└─$ alias
diff='diff --color=auto'
egrep='egrep --color=auto'
fgrep='fgrep --color=auto'
grep='grep --color=auto'
history='history 0'
ip='ip --color=auto'
ipconfig=ifconfig
l='ls -CF'
la='ls -A'
listuj=ls
ll='ls -l'
ls='ls --color=auto'
which-command=whence

┌──(kali㉿kali)-[~]
└─$ su wito
Password:
┌──(wito㉿kali)-[/home/kali]
└─$ alias
alias diff='diff --color=auto'
alias egrep='egrep --color=auto'
alias fgrep='fgrep --color=auto'
alias grep='grep --color=auto'
alias ip='ip --color=auto'
alias ipconfig='ifconfig'
alias l='ls -CF'
alias la='ls -A'
alias ll='ls -l'
alias ls='ls --color=auto'

┌──(wito㉿kali)-[/home/kali]
└─$
```

```
  GNU nano 6.2                                  plik.txt
if [ "$USER" = "kali" ]; then
    alias listuj='ls'
fi
```

Part 6: System Update and Apt Usage

1. Make sure that the virtual machine is set on bridge network, and update the system.

Upewnij się, że maszyna wirtualna jest skonfigurowana do działania w trybie sieci mostkowej oraz zaktualizuj system.




```
┌──(kali㉿kali)-[~/dir1]
└─$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.9 MB]
14% [2 Packages 115 kB/19.9 MB 1%]
```

2. Verify that the sources in sources.list are updated. If they aren't, update them.

Sprawdź, czy źródła w pliku sources.list są zaktualizowane. Jeśli nie, dokonaj aktualizacji.

```
┌──(kali㉿kali)-[~/dir1]
└─$ sudo apt update
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
2087 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

3. Download a package called cmatrix and execute it.

Pobierz pakiet o nazwie cmatrix i uruchom go.

```
┌──(kali㉿kali)-[~/dir1]
└─$ sudo apt install cmatrix
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
cmatrix is already the newest version (2.0-6).
The following packages were automatically installed and are no longer
  cython3 dconf-cli debtags evolution-data-server evolution-data-serv
  fonts-noto-color-emoji gir1.2-accountsservice-1.0 gir1.2-evince-3.0
  gir1.2-gcr-3 gir1.2-gdm-1.0 gir1.2-geoclue-2.0 gir1.2-gmenu-3.0 gir
  gir1.2-gnomebg-4.0 gir1.2-gnomebluetooth-3.0 gir1.2-gnomedesktop-3.
  gir1.2-gst-plugins-base-1.0 gir1.2-gtksource-4 gir1.2-gweather-4.0
  gir1.2-javascriptcoregtk-4.1 gir1.2-javascriptcoregtk-6.0 gir1.2-js
  gir1.2-nma4-1.0 gir1.2-polkit-1.0 gir1.2-rsvg-2.0 gir1.2-soup-3.0 g
  gir1.2-webkit-6.0 gir1.2-webkit2-4.1 gkbd-capplet gnome-backgrounds
  gnome-session-common gstreamer1.0-pipewire ibus ibus-data ibus-gtk
  im-config kali-debtags libarmadillo10 libcamel-1.2-64 libcfitsio9 l
  libebackend-1.2-11 libebook-1.2-21 libebook-contacts-1.2-4 libecal-
  libedata-book-1.2-27 libedata-cal-2.0-2 libedataserver-1.2-27 libec
  libfftw3-single3 libgdal30 libgdm1 libgeos3.10.2 libgnome-menu-3-0
  libgnomekbd8 libgssdp-1.2-0 libgupnp-1.2-1 libgupnp-igd-1.0-4 libil
  libjavascriptcoregtk-6.0-1 libmozjs-115-0 libopenexr25 libopenh264-
  libpoppler118 libpython3.10-dev libspatialite7 libsuperlu5 libwebki
  libzxingcore1 python-mpltoolkits.basemap-data python3-debian python
  python3-pyshp python3.10 python3.10-dev python3.10-minimal switchen
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 2087 not upgraded.
```

```
┌──(kali㉿kali)-[~]
└─$ sudo cmatrix
```

4. Permanently delete cmatrix.

Trwale usuń cmatrix.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt remove cmatrix
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
```

Part 7: Ifconfig and Address Settings

1. Execute the ifconfig command.
Wykonaj polecenie ifconfig.

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.242  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fedb:966a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:db:96:6a  txqueuelen 1000  (Ethernet)
        RX packets 1184  bytes 1302004 (1.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 320  bytes 24718 (24.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Change the output of the command to uppercase letters.
Zmień wynik polecenia na wielkie litery.

```
┌──(kali㉿kali)-[~]
└─$ ifconfig | tr '[:lower:]' '[:upper:]'
ETH0: FLAGS=4163<UP,BROADCAST,RUNNING,MULTICAST>  MTU 1500
        INET 192.168.1.242  NETMASK 255.255.255.0  BROADCAST 192.168.1.255
        INET6 FE80::A00:27FF:FEDB:966A  PREFIXLEN 64  SCOPEID 0X20<LINK>
        ETHER 08:00:27:DB:96:6A  TXQUEUELEN 1000  (ETHERNET)
        RX PACKETS 1191  BYTES 1303214 (1.2 MIB)
        RX ERRORS 0  DROPPED 0  OVERRUNS 0  FRAME 0
        TX PACKETS 320  BYTES 24718 (24.1 KIB)
        TX ERRORS 0  DROPPED 0 OVERRUNS 0  CARRIER 0  COLLISIONS 0

LO: FLAGS=73<UP,LOOPBACK,RUNNING>  MTU 65536
        INET 127.0.0.1  NETMASK 255.0.0.0
        INET6 ::1  PREFIXLEN 128  SCOPEID 0X10<HOST>
        LOOP  TXQUEUELEN 1000  (LOCAL LOOPBACK)
        RX PACKETS 4  BYTES 240 (240.0 B)
        RX ERRORS 0  DROPPED 0  OVERRUNS 0  FRAME 0
        TX PACKETS 4  BYTES 240 (240.0 B)
        TX ERRORS 0  DROPPED 0 OVERRUNS 0  CARRIER 0  COLLISIONS 0
```

„tr” is used to translate or transliterate characters in text. For example, it can convert all lowercase letters to uppercase letters.

3. Filter the command to display only the IP and subnet mask.
Przefiltruj wynik polecenia, aby wyświetlić tylko adres IP i maskę podsieci.

```
┌──(kali㉿kali)-[~]
└─$ ifconfig | grep -E 'inet |netmask '
        inet 192.168.1.242  netmask 255.255.255.0  broadcast 192.168.1.255
        inet 127.0.0.1  netmask 255.0.0.0
```

The -E option in the grep command enables extended regular expressions (regex). This means you can use more advanced regex features without escaping special characters.

4. Write the output to a file called "ip.log".
Zapisz wynik do pliku o nazwie "ip.log".

```
┌──(kali㉿kali)-[~]
└─$ ifconfig > ip.log
```

5. Add to the "ip.log" file the following: whoami, last, and hostname.
Dodaj do pliku "ip.log" następujące dane: whoami, last oraz hostname.

```
┌──(kali㉿kali)-[~]
└─$ whoami >> ip.log
echo "── Last logins ──" >> ip.log
last >> ip.log
echo "── Hostname ──" >> ip.log
hostname >> ip.log
```

6. Set a static IP in the terminal.
Ustaw statyczny adres IP w terminalu.

```
┌──(kali㉿kali)-[~]
└─$ sudo ip addr add 192.168.1.100/24 dev eth0

┌──(kali㉿kali)-[~]
└─$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1
000
    link/ether 08:00:27:db:96:6a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fedb:966a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

It was given static adres IP example.„[192.168.1.100]” for eth0
eth0 - This is the name assigned to the first Ethernet network interface in the system.

Part 8: Remote Control and Telnet Services

1.Install telnet on the operation system.

1. Zainstaluj usługę Telnet w systemie operacyjnym.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install telnetd
```

```
┌──(root㉿kali)-[/home/kali]
└─# apt install xinetd
```

```
┌──(root㉿kali)-[/home/kali]
└─# service xinetd status
● xinetd.service - Xinetd A Powerful Replacement For Inetd
     Loaded: loaded (/usr/lib/systemd/system/xinetd.service; disabled; preset: disabled)
     Active: active (running) since Sun 2024-07-07 10:19:12 EDT; 21s ago
 Invocation: 2bb777a77a524b59b26583eede19ecca
       Docs: man:xinetd
             man:xinetd.conf
             man:xinetd.log
   Main PID: 3287 (xinetd)
      Tasks: 1 (limit: 2242)
     Memory: 476K
        CPU: 49ms
     CGroup: /system.slice/xinetd.service
             └─3287 /usr/sbin/xinetd -stayalive -dontfork

Jul 07 10:19:12 kali xinetd[3287]: Reading included configuration file: /etc/xinetd.d/discard [>
Jul 07 10:19:12 kali xinetd[3287]: Reading included configuration file: /etc/xinetd.d/discard-u>
Jul 07 10:19:12 kali xinetd[3287]: Reading included configuration file: /etc/xinetd.d/echo [fil>
Jul 07 10:19:12 kali xinetd[3287]: Reading included configuration file: /etc/xinetd.d/echo-udp >
Jul 07 10:19:12 kali xinetd[3287]: Reading included configuration file: /etc/xinetd.d/servers [>
Jul 07 10:19:12 kali xinetd[3287]: Reading included configuration file: /etc/xinetd.d/services >
Jul 07 10:19:12 kali xinetd[3287]: Reading included configuration file: /etc/xinetd.d/time [fil>
Jul 07 10:19:12 kali xinetd[3287]: Reading included configuration file: /etc/xinetd.d/time-udp >
Jul 07 10:19:12 kali xinetd[3287]: 2.3.15.4 started with libwrap loadavg labeled-networking opt>
Jul 07 10:19:12 kali xinetd[3287]: Started working: 0 available services
lines 1-24/24 (END)
```

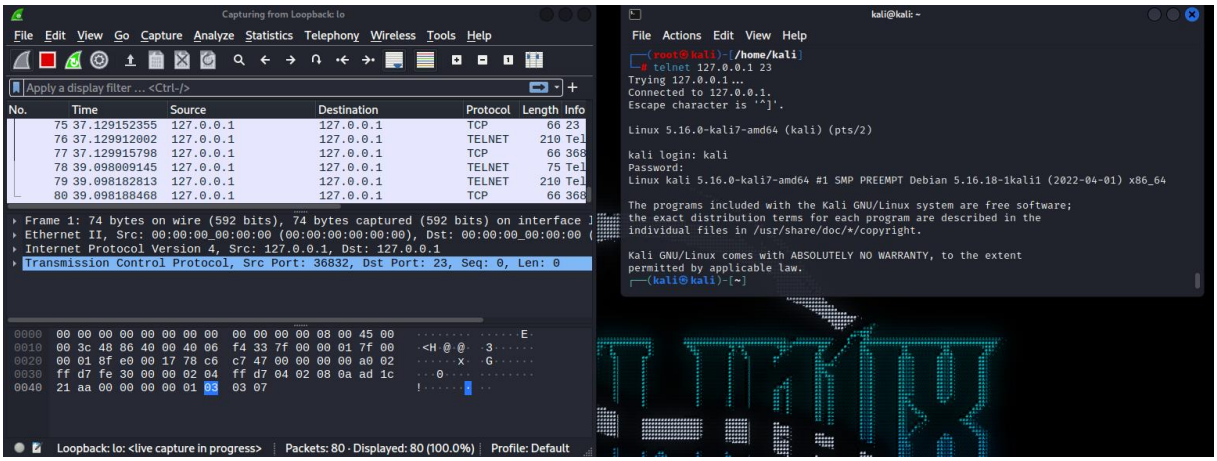
service xinetd status = check the status of service

```
  GNU nano 6.2                    /etc/xinetd.d/telnet
service telnet

{

flags = REUSE

socket_type = stream

wait = no

user = root

server = /usr/sbin/telnetd

log_on_failure += USERID

disable = no

}
```

Most important in this code is the line server = /usr/sbin/telnetd , in older version the path way was different, so it should be checked.

```
┌──(root㉿kali)-[/home/kali]
└─# netstat -tulpn

┌──(root㉿kali)-[/home/kali]
└─# sudo nano /etc/xinetd.d/telnet

┌──(root㉿kali)-[/home/kali]
└─# netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name


┌──(root㉿kali)-[/home/kali]
└─# service xinetd restart

┌──(root㉿kali)-[/home/kali]
└─# service xinetd status
● xinetd.service - Xinetd A Powerful Replacement For Inetd
     Loaded: loaded (/usr/lib/systemd/system/xinetd.service; disabled; preset: disabled)
     Active: active (running) since Sun 2024-07-07 10:22:32 EDT; 8s ago
 Invocation: daf4293545d94bbbb7d02948d40a79cb
       Docs: man:xinetd
             man:xinetd.conf
             man:xinetd.log
   Main PID: 4184 (xinetd)
      Tasks: 1 (limit: 2242)
     Memory: 472K
        CPU: 48ms
     CGroup: /system.slice/xinetd.service
             └─4184 /usr/sbin/xinetd -stayalive -dontfork

Jul 07 10:22:32 kali xinetd[4184]: Reading included configuration file: /etc/xinetd.d/discard-u>
Jul 07 10:22:32 kali xinetd[4184]: Reading included configuration file: /etc/xinetd.d/echo [fil>
Jul 07 10:22:32 kali xinetd[4184]: Reading included configuration file: /etc/xinetd.d/echo-udp >
Jul 07 10:22:32 kali xinetd[4184]: Reading included configuration file: /etc/xinetd.d/servers [>
Jul 07 10:22:32 kali xinetd[4184]: Reading included configuration file: /etc/xinetd.d/services >
Jul 07 10:22:32 kali xinetd[4184]: Reading included configuration file: /etc/xinetd.d/telnet [f>
Jul 07 10:22:32 kali xinetd[4184]: Reading included configuration file: /etc/xinetd.d/time [fil>
Jul 07 10:22:32 kali xinetd[4184]: Reading included configuration file: /etc/xinetd.d/time-udp >
Jul 07 10:22:32 kali xinetd[4184]: 2.3.15.4 started with libwrap loadavg labeled-networking opt>
Jul 07 10:22:32 kali xinetd[4184]: Started working: 1 available service
lines 1-24/24 (END)
```

As you can see, there is 1 avilable service started working process.




```
┌──(root㉿kali)-[/home/kali]
└─# netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name

tcp6       0      0 :::23                   :::*                    LISTEN      4184/xinetd
```

netstat –tulpn = is for check open ports status. Port 23 is open now for telnet serivce.

2. Restart the service.

2. Uruchom ponownie usługę.

```
┌──(root㉿kali)-[/home/kali]
└─# service xinetd restart
```

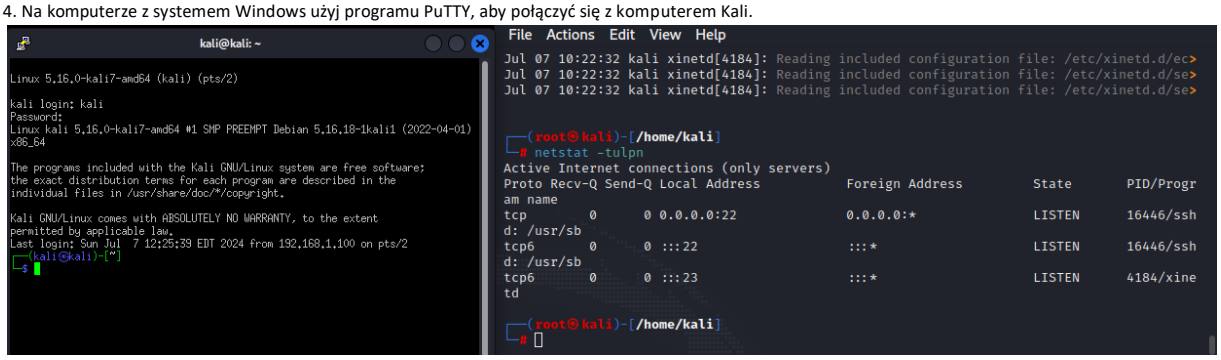
3. Check the status of the service.

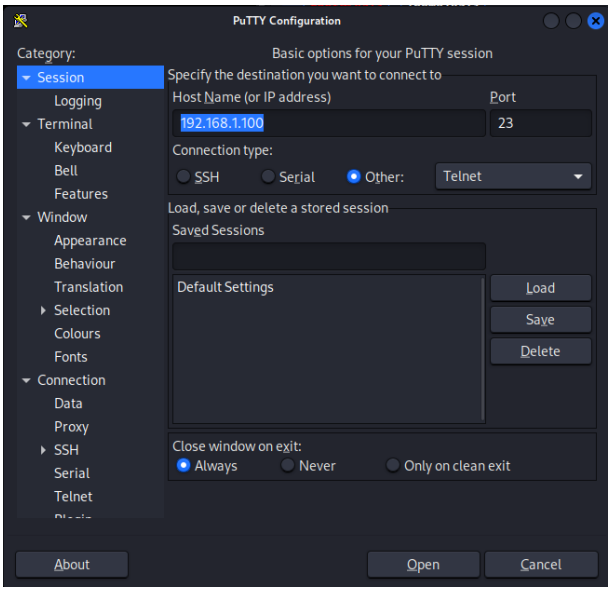
3. Sprawdź status usługi.

```
┌──(root㉿kali)-[/home/kali]
└─# service xinetd status
```

4. In the Windows machine, use puTTY to connect to the Kali machine.

4. Na komputerze z systemem Windows użyj programu PuTTY, aby połączyć się z komputerem Kali.





5. Create directories and files to verify that the connection works.

5. Utwórz katalogi i pliki, aby sprawdzić, czy połączenie działa.

Part 9: SSH Connection

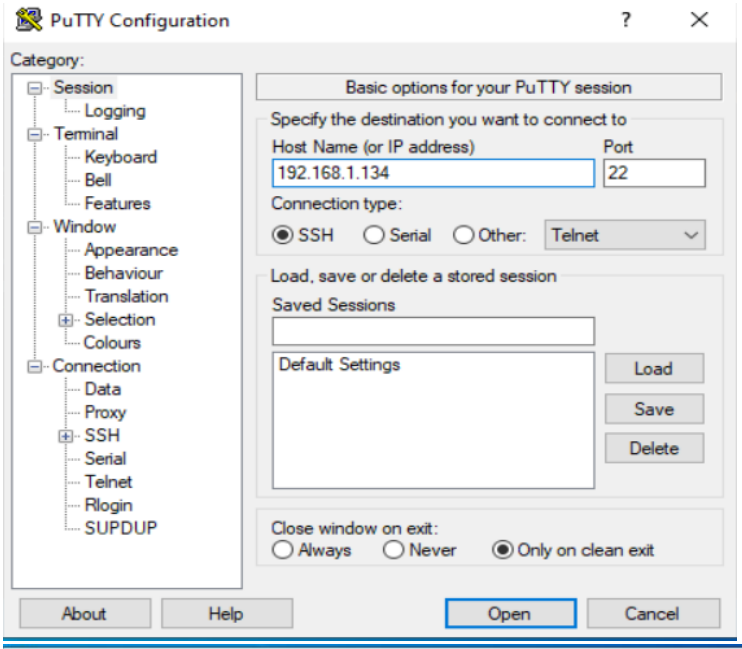
1. Start the SSH service and verify that the service runs.

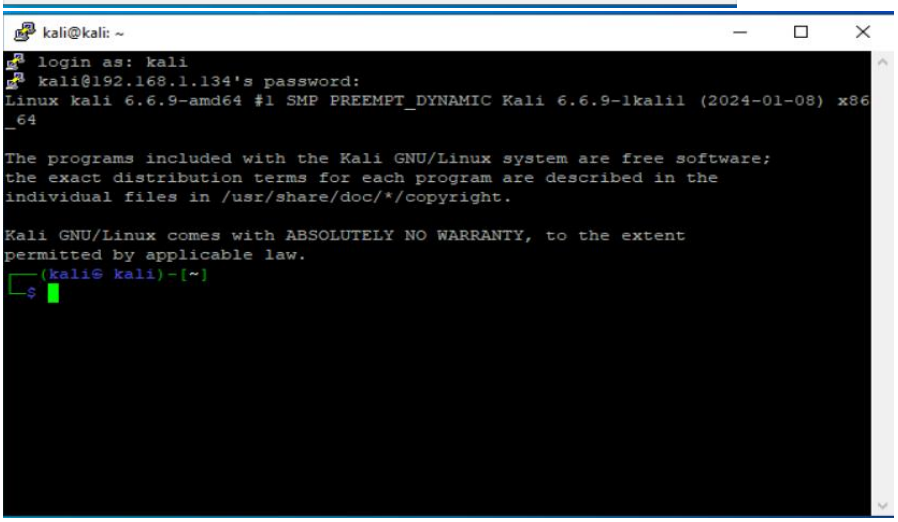
1. Uruchom usługę SSH i sprawdź, czy usługa działa.

```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start
sudo service ssh status
[sudo] password for kali:
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: active (running) since Fri 2024-07-12 11:08:45 CEST; 11ms ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 1658 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1660 (sshd)
      Tasks: 1 (limit: 4544)
     Memory: 2.7M (peak: 3.0M)
        CPU: 21ms
     CGroup: /system.slice/ssh.service
             └─1660 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jul 12 11:08:45 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ...
Jul 12 11:08:45 kali sshd[1660]: Server listening on 0.0.0.0 port 22.
Jul 12 11:08:45 kali sshd[1660]: Server listening on :: port 22.
Jul 12 11:08:45 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

2. Connect via puTTY to the Linux machine.

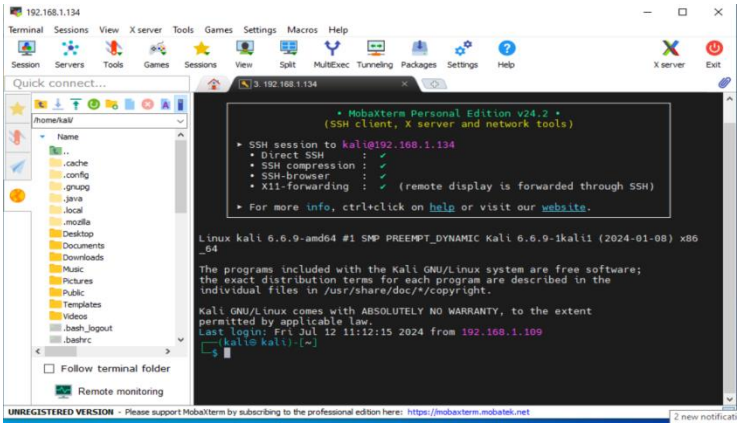
2. Połącz się za pomocą PuTTY z komputerem z systemem Linux.





3. Connect to Kali Linux with MOBA.

3. Połącz się z Kali Linux za pomocą MOBA.

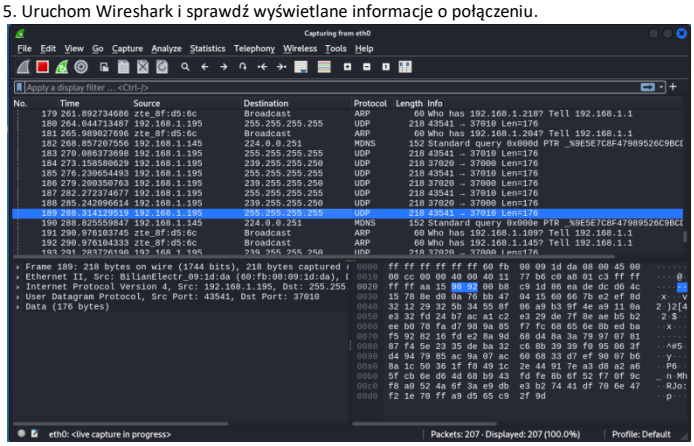


4. Connect to the Kali Machine from your phone.

4. Połącz się z Kali Machine za pomocą swojego telefonu.

5. Run Wireshark and inspect the information that is displayed about the connection.

5. Uruchom Wireshark i sprawdź wyświetlane informacje o połączeniu.

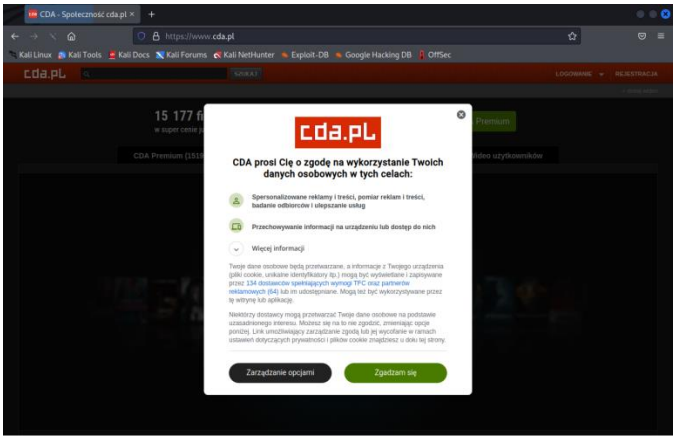


Part 10: Apache Webserver

1. Change the index file to a website of your choice. Verify that the site works.

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/apache2/sites-available/000-default.conf

┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart apache2
```

```
kali@kali: ~
File  Actions  Edit  View  Help
  GNU nano 6.2                  /etc/apache2/sites-available/000-default.conf
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        ##DocumentRoot /var/www/html
        redirect "/" https://cda.pl
        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
                                                [ Read 31 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line M-E Redo
```



Part 11: VSFTPD

Download the latest version of VSFTPD.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
```

2. Configure VSFTPD and run the service.

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/vsftpd.conf
```

```
  GNU nano 7.2                    /etc/vsftpd.conf
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=YES
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=NO
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# If enabled, vsftpd will display directory listings with the time
# in  your  local  time  zone.  The default is to display GMT. The
```

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start vsftpd
sudo systemctl enable vsftpd
```

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.134
```

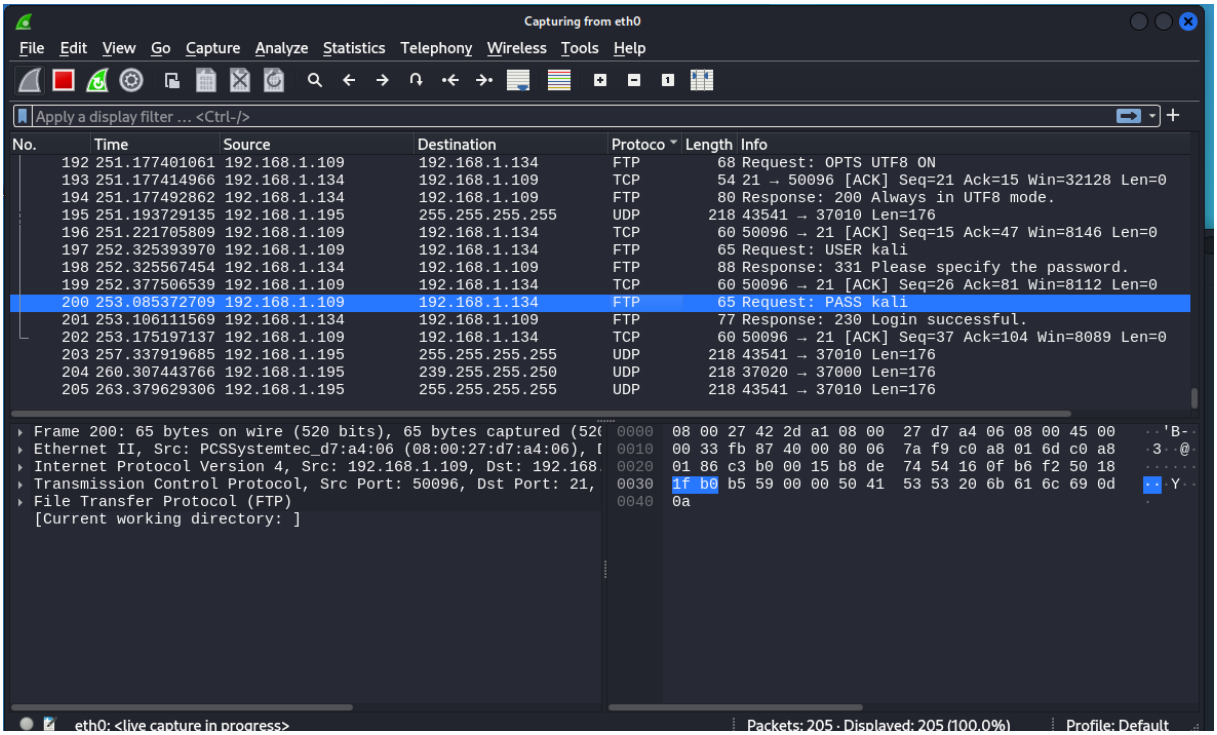
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: disabled)
     Active: active (running) since Thu 2024-07-11 19:42:44 CEST; 6min ago
    Process: 16939 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCC>
   Main PID: 16941 (vsftpd)
      Tasks: 3 (limit: 4544)
     Memory: 1.7M (peak: 18.1M)
        CPU: 55ms
     CGroup: /system.slice/vsftpd.service
             ├─16941 /usr/sbin/vsftpd /etc/vsftpd.conf
             ├─17824 /usr/sbin/vsftpd /etc/vsftpd.conf
             └─17866 /usr/sbin/vsftpd /etc/vsftpd.conf

Jul 11 19:42:44 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Jul 11 19:42:44 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.
Jul 11 19:42:57 kali vsftpd[16977]: pam_unix(vsftpd:auth): authentication failure; logname= uid>
lines 1-16/16 (END)
```

3. Transfer a file from the Kali machine to the Windows machine.

cmd > ftp 192.168.1.134 [ftp server adres]
lcd C:\Users\NEW\Desktop
cd /home/kali
put teksty.txt [file which was created in Desktop Win10]

```
C:\Windows\system32>ftp 192.168.1.134
Connected to 192.168.1.134.
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
User (192.168.1.134:(none)): kali
331 Please specify the password.
Password:
230 Login successful.
ftp> pwd
257 "/home/kali" is the current directory
ftp> put teksty.txt
teksty.txt: File not found
ftp> lcd Desktop
Desktop: File not found
ftp> lcd C:\Users\NEW\Desktop
Local directory now C:\Users\NEW\Desktop.
ftp> put teksty.txt
200 PORT command successful. Consider using PASV.
553 Could not create file.
ftp> put teksty.txt
200 PORT command successful. Consider using PASV.
553 Could not create file.
ftp> put teksty.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
```

4. Run Wireshark and reconnect to the FTP server (Kali machine). Try to find the password and explain why the password is in plaintext.



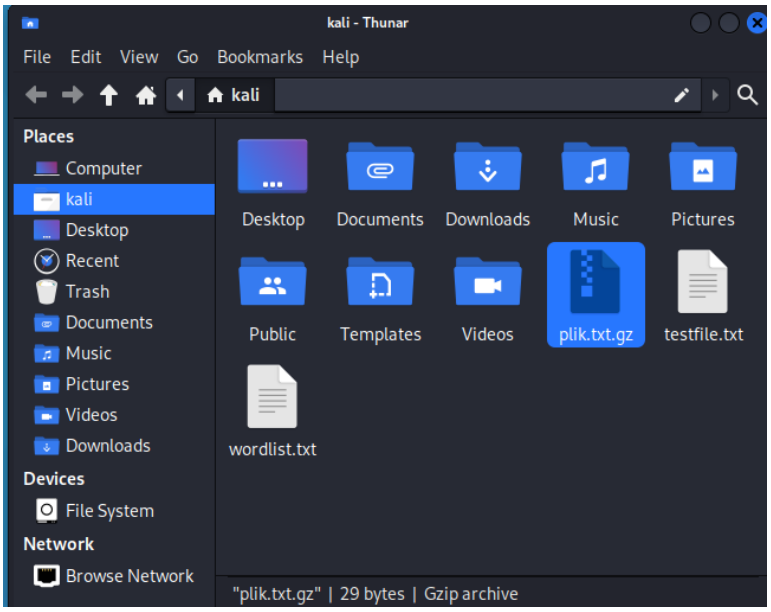
Passwords are transmitted in plaintext in FTP because the protocol lacks encryption by default, exposing them to interception by anyone monitoring network traffic. This inherent vulnerability underscores the need for secure alternatives like FTPS or SFTP, which encrypt data transmissions to protect sensitive information during file transfers.

Part 12: Gzip

1.Locate a gzip file on the file system (gz extension).

```
┌──(root㉿kali)-[/home/kali]
└─# find / -name "*.gz"
/etc/console-setup/cached_Uni2-Fixed16.psf.gz
/etc/console-setup/cached_UTF-8_del.kmap.gz
/etc/console-setup/cached_Lat2-Fixed16.psf.gz
/etc/alternatives/DROP_AGGREGATE.7.gz
/etc/alternatives/pg_archivecleanup.1.gz
/etc/alternatives/CREATE_TYPE.7.gz
/etc/alternatives/ALTER_FOREIGN_TABLE.7.gz
/etc/alternatives/CREATE_TEXT_SEARCH_TEMPLATE.7.gz
/etc/alternatives/pager.1.gz
/etc/alternatives/DROP_SEQUENCE.7.gz
/etc/alternatives/MOVE.7.gz
/etc/alternatives/ALTER_LARGE_OBJECT.7.gz
/etc/alternatives/BEGIN.7.gz
/etc/alternatives/INSERT.7.gz
/etc/alternatives/ALTER_SEQUENCE.7.gz
/etc/alternatives/which.1.gz
/etc/alternatives/DROP_FUNCTION.7.gz
/etc/alternatives/Xvnc.1.gz
/etc/alternatives/ALTER_MATERIALIZED_VIEW.7.gz
/etc/alternatives/ALTER_ROUTINE.7.gz
/etc/alternatives/pg_dump.1.gz
/etc/alternatives/CREATE_ACCESS_METHOD.7.gz
/etc/alternatives/traceroute6.1.gz
/etc/alternatives/ROLLBACK_TO_SAVEPOINT.7.gz
/etc/alternatives/DROP_DOMAIN.7.gz
/etc/alternatives/DROP_SERVER.7.gz
/etc/alternatives/lzmore.1.gz
/etc/alternatives/telnet.1.gz
/etc/alternatives/DROP_OPERATOR_CLASS.7.gz
/etc/alternatives/ALTER_TYPE.7.gz
/etc/alternatives/mp3-decoder.1.gz
/etc/alternatives/DROP_TEXT_SEARCH_PARSER.7.gz
/etc/alternatives/DROP_SCHEMA.7.gz
/etc/alternatives/animate-im6.1.gz
/etc/alternatives/DELETE.7.gz
/etc/alternatives/upx.1.gz
```

2. Extract the files from a particular gz file.




```
┌──(root㉿kali)-[/home/kali]
└─# gunzip plik.txt.gz
```

```
┌──(root㉿kali)-[/home/kali]
└─# ls
Desktop    Downloads  Pictures  Templates  plik.txt      wordlist.txt
Documents  Music      Public    Videos     testfile.txt
```

3. Create four files and move them to a gzip file.

```
┌──(root㉿kali)-[/home/kali]
└─# touch plik1.txt plik2.txt plik3.txt plik4.txt

┌──(root㉿kali)-[/home/kali]
└─# cat plik* > wszystkie.txt
```

```
┌──(root㉿kali)-[/home/kali]
└─# gzip wszystkie.txt
```

Or

```
┌──(root㉿kali)-[/home/kali]
└─# gzip plik*
```

Part 13: Questions

Answer the following questions.
1. What are root folders? Choose three and explain about them.

Root folders are the top-level directories in a file system from which all other directories branch out. In Unix-like operating systems, such as Linux, these root folders are crucial for the organization and functioning of the system. Here are three important root folders and their explanations:

1. „/”

The root directory is the top-level directory of the entire file system. It contains all other directories and files. Every file and directory in a Unix-like system starts from the root directory. It is symbolized by a single forward slash (/).

2. „/home”

The /home directory is where user-specific files and directories are stored. Each user on the system has a subdirectory under /home, typically named after their username. For example, a user named "wito" would have a home directory at /home/wito. This directory contains the user’s personal files, configuration settings, and application data.

3. „/etc”

The /etc directory contains configuration files for the system. It includes system-wide configuration files and shell scripts that are used to boot and initialize system settings. For example, the /etc/passwd file contains information about user accounts, and the /etc/fstab file contains information about disk drives and partitions.

Summary:

/ - The root directory, the top-level directory in the file system.

/home - Directory where user-specific files and directories are stored.

/etc - Directory containing configuration files for the system.

2. Explain the following terms:

-Encoding

Definition: Encoding is the process of converting data from one form to another. It is primarily used to ensure that data can be properly consumed by different types of systems.

Purpose: The main purpose of encoding is data transformation for usability and interoperability. It does not involve any secret or key and is not intended to provide any security.

Examples:

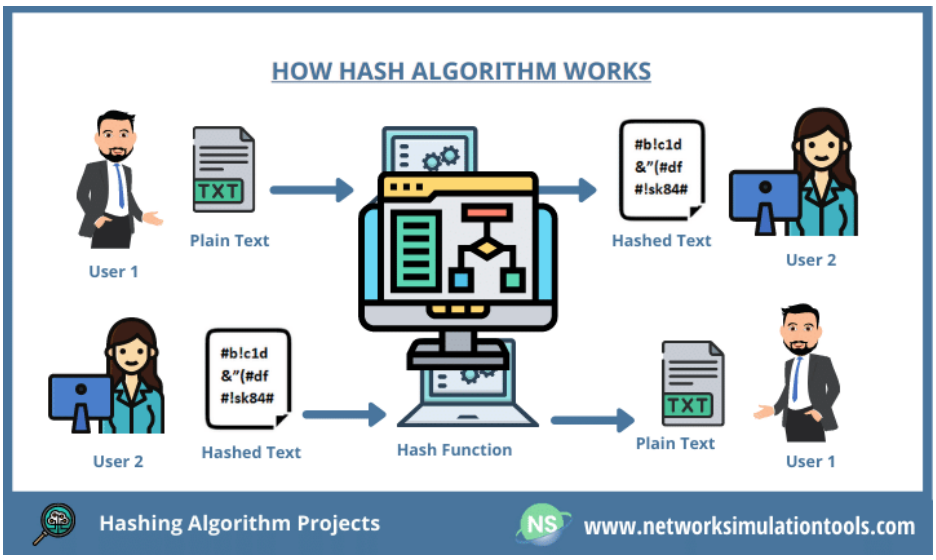
Base64 Encoding: Used to encode binary data, such as images or files, into text to ensure safe transmission over text-based protocols like email.

URL Encoding: Converts characters into a format that can be transmitted over the internet, ensuring that special characters are correctly interpreted by web servers.

- Hashing

Definition: Hashing is the process of converting data into a fixed-size string of characters, which is typically a digest that uniquely represents the input data.

Purpose: Hashing is used to verify data integrity. It is a one-way function, meaning that once data has been hashed, it cannot be easily converted back to its original form.



Examples:

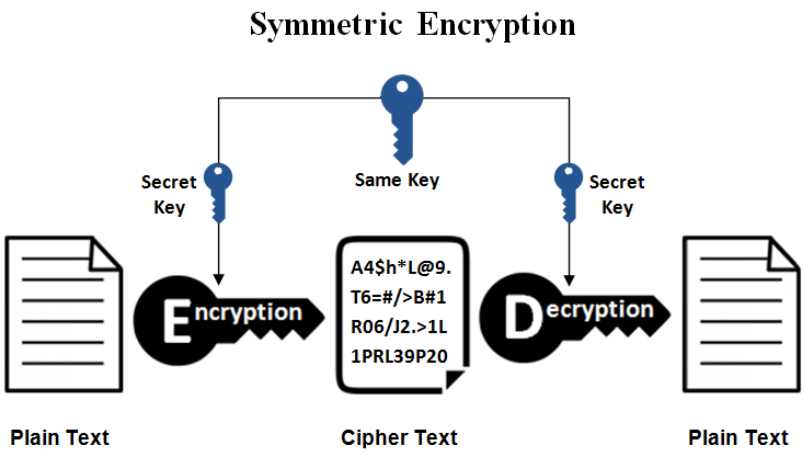
MD5: Produces a 128-bit hash value, commonly used for checksums.

SHA-256: Part of the SHA-2 family, producing a 256-bit hash value, often used in cryptographic applications.

- Symmetric encryption

Definition: Symmetric encryption uses the same key for both encryption and decryption of data.

Purpose: It is used for data confidentiality. Since both the sender and receiver use the same key, the key must be kept secret from unauthorized parties.



Examples:

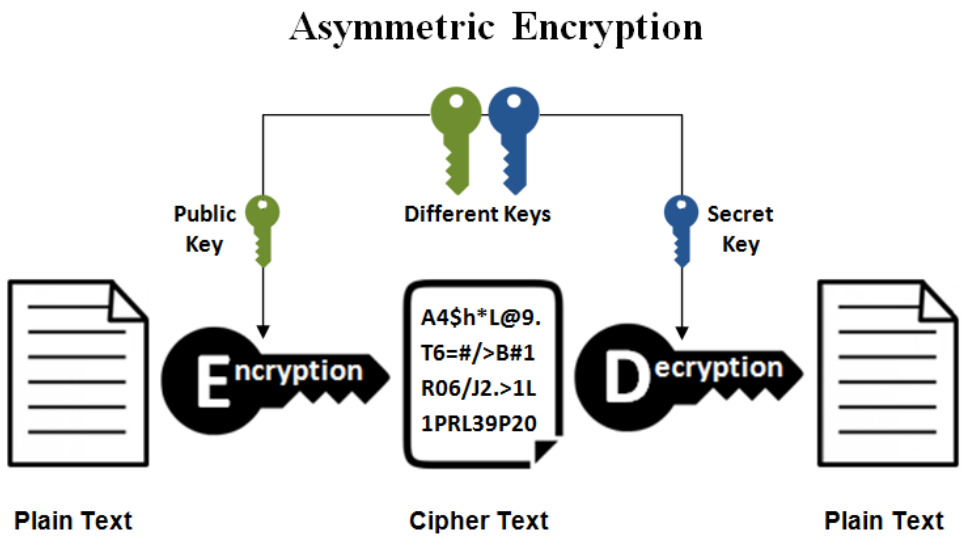
AES (Advanced Encryption Standard): A widely used encryption algorithm that supports 128, 192, and 256-bit keys.

DES (Data Encryption Standard): An older encryption standard that uses a 56-bit key.

- Asymmetric encryption

Definition: Asymmetric encryption, also known as public-key cryptography, uses a pair of keys - a public key and a private key. Data encrypted with the public key can only be decrypted with the corresponding private key and vice versa.

Purpose: It is used for secure data transmission and digital signatures. The public key can be shared openly, while the private key is kept secret.



Examples:

RSA: A widely used asymmetric encryption algorithm suitable for secure data transmission.

ECC (Elliptic Curve Cryptography): A newer form of asymmetric encryption that offers the same level of security with smaller key sizes compared to RSA.

Summary

Encoding: Transforms data for usability and compatibility without providing security.

Hashing: Generates a fixed-size string (hash) to verify data integrity; it's a one-way function.

Symmetric Encryption: Uses the same key for encryption and decryption, ensuring data confidentiality.

Asymmetric Encryption: Uses a pair of keys (public and private) for secure data transmission and digital signatures.

3. When enabling SSH, usually, the configuration file needs to be changed.

-Why?
Changing the configuration file when enabling SSH is often necessary to customize the behavior and security settings of the SSH service. The default configuration might not be suitable for all environments, and adjustments can help secure the connection, define allowed users, specify authentication methods, and configure other options such as port numbers and timeout settings. The main configuration file for SSH is typically /etc/ssh/sshd_config.

Common reasons for changing the SSH configuration file include:

*Changing the default port to avoid common attacks on port 22.

*Disabling root login to enhance security.

*Enforcing stricter authentication methods, such as key-based authentication instead of password-based authentication.

*Restricting which users or groups can access the server via SSH.

*Configuring idle timeouts to close inactive sessions automatically.

-Do you know any other configuration file and in which service?

Yes, here are a few examples of other configuration files and their respective services:

***Apache Web Server**: The main configuration file is usually /etc/httpd/conf/httpd.conf or /etc/apache2/apache2.conf. This file is used to configure the behavior of the Apache web server, including settings for virtual hosts, modules, security, and performance.

***Nginx Web Server**: The main configuration file is typically /etc/nginx/nginx.conf. This file configures server blocks, proxy settings, SSL certificates, logging, and more.

***MySQL Database Server**: The main configuration file is usually /etc/my.cnf or /etc/mysql/my.cnf. This file is used to configure MySQL server settings such as buffer sizes, caching, logging, and authentication.

-What is the usage of SSH?

SSH (Secure Shell) is a protocol used to securely access and manage network devices and servers over an unsecured network. Its primary uses include:

***Remote Command Execution**: Allows users to execute commands on a remote server.

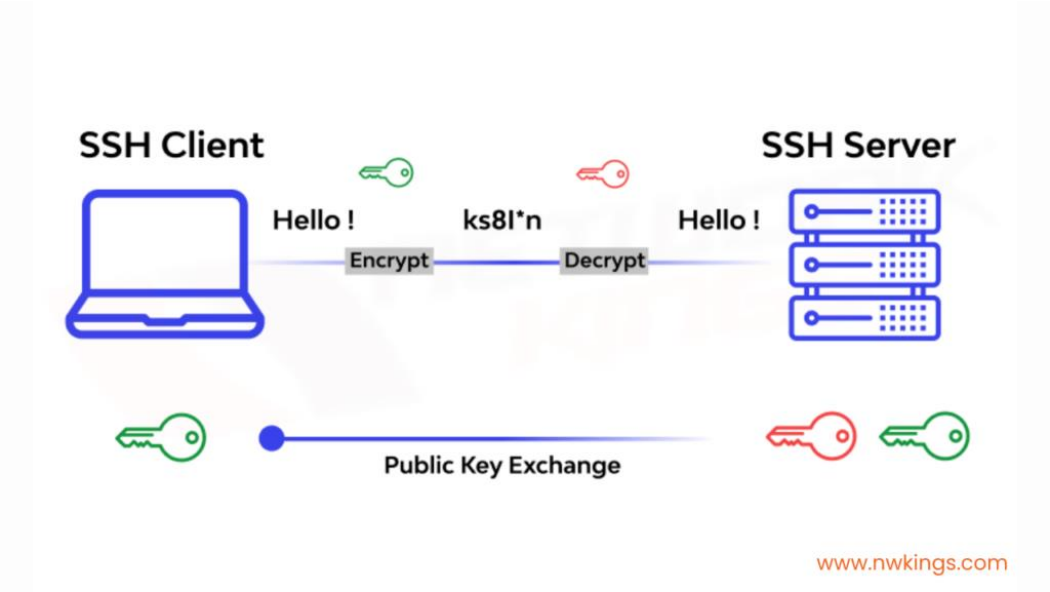
***Secure File Transfer**: Through protocols such as SCP (Secure Copy) and SFTP (SSH File Transfer Protocol).

***Tunneling and Port Forwarding**: Securing the transmission of other protocols via SSH.

***Remote Management**: Administering servers, networking devices, and other remote systems securely.

-Is SSH encrypted?

Yes, SSH is encrypted. It uses strong encryption algorithms to ensure that the data transmitted between the client and the server is secure and cannot be easily intercepted or read by unauthorized parties. The encryption provides confidentiality, integrity, and authenticity of the data, making SSH a secure method for remote communication.



Summary

Changing the SSH configuration file is necessary to customize security settings and behavior of the SSH service.

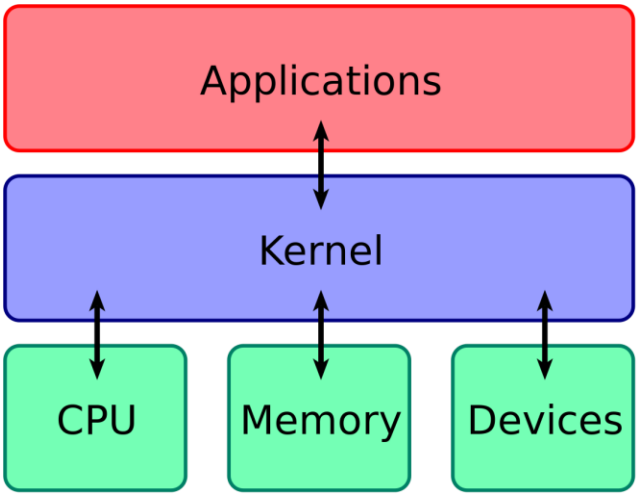
Other configuration files include /etc/httpd/conf/httpd.conf for Apache, /etc/nginx/nginx.conf for Nginx, and /etc/my.cnf for MySQL.

SSH usage includes remote command execution, secure file transfer, tunneling, and remote management.

SSH is encrypted, ensuring secure communication between the client and the server.

4. What is the kernel?

The kernel is a core component of an operating system that acts as a bridge between applications and the underlying hardware of a computer. It is responsible for managing system resources and facilitating communication between hardware and software components.



5. What should be performed to create a connection between two virtual machines? Explain each step.

To create a connection between two virtual machines (VMs), typically for communication or data transfer, you can follow these steps:

a) **Network Configuration in Virtualization Software**:

First, ensure that both virtual machines are configured to use the same type of virtual network. Virtualization software like VMware Workstation, VirtualBox, or Hyper-V allows you to create various types of virtual networks (bridged, NAT, host-only, etc.).

Explanation: Virtual networks emulate physical networks and enable communication between VMs as if they were separate physical machines connected to the same network.

b) **Assign IP Addresses**:

Each VM should be assigned a unique IP address within the same subnet. You can either set these IP addresses manually (static IP) or configure them to obtain IP addresses automatically through DHCP (Dynamic Host Configuration Protocol).

Explanation: IP addresses allow VMs to identify and communicate with each other within the virtual network.

c) **Verify Firewall and Network Settings**:

Ensure that firewall settings on both VMs allow incoming and outgoing connections on the relevant ports and protocols, especially if specific services or applications need to communicate between the VMs.

Explanation: Firewalls can block network traffic, so configuring them correctly ensures that communication between VMs is not obstructed.

d) **Test Connectivity**:

Use commands like ping to verify connectivity between the VMs. For example, from one VM's command line, ping the IP address of the other VM to check if there is successful communication.

Explanation: Testing connectivity confirms that the network configuration is correct and that VMs can communicate with each other as expected.

e) **Enable File Sharing or Services (if needed)**:

If you intend to transfer files or share resources between VMs, ensure that the necessary file sharing or service protocols (such as SMB/CIFS for Windows or NFS for Unix-based systems) are configured and running on the respective VMs.

Explanation: Enabling file sharing or services allows VMs to exchange data or share resources securely over the network.

By following these steps, you can establish a network connection between two virtual machines, enabling them to communicate and transfer data effectively within the virtualized environment.

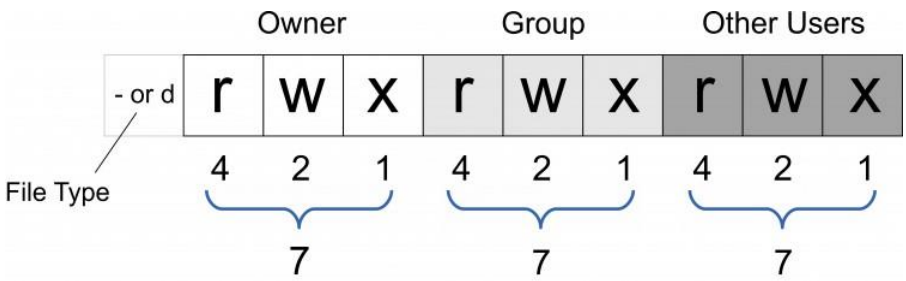
6. What is ping?

Ping is a command-line utility used to test connectivity between devices on a network by sending ICMP echo request packets and waiting for responses. It helps diagnose network issues such as connectivity problems, latency, or packet loss by measuring the round-trip time between the sender and receiver.
Ping jest narzędziem wiersza poleceń używanym do testowania połączenia między urządzeniami w sieci poprzez wysyłanie pakietów żądania ICMP echo i oczekiwanie na odpowiedzi. Pomaga diagnozować problemy sieciowe, takie jak problemy z połączeniem, opóźnienia czy utrata pakietów, mierząc czas potrzebny na przesłanie pakietu i otrzymanie odpowiedzi z powrotem.

```
bob@suse1:~> ping 192.168.198.130
PING 192.168.198.130 (192.168.198.130) 56(84) bytes of data.
64 bytes from 192.168.198.130: icmp_seq=1 ttl=64 time=6.14 ms
64 bytes from 192.168.198.130: icmp_seq=2 ttl=64 time=0.778 ms
64 bytes from 192.168.198.130: icmp_seq=3 ttl=64 time=0.599 ms
64 bytes from 192.168.198.130: icmp_seq=4 ttl=64 time=0.558 ms
64 bytes from 192.168.198.130: icmp_seq=5 ttl=64 time=0.615 ms
64 bytes from 192.168.198.130: icmp_seq=6 ttl=64 time=0.608 ms
64 bytes from 192.168.198.130: icmp_seq=7 ttl=64 time=0.645 ms
64 bytes from 192.168.198.130: icmp_seq=8 ttl=64 time=0.619 ms
64 bytes from 192.168.198.130: icmp_seq=9 ttl=64 time=0.698 ms
^C
--- 192.168.198.130 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8000ms
rtt min/avg/max/mdev = 0.558/1.252/6.149/1.732 ms
```

7. When granting permissions over files and folders, we use three numbers. What are the numbers and what do they mean? Why do we write them three times (777)?

When granting permissions on files and folders in Unix-like systems, we use three numbers known as octal notation (e.g., 777). Each digit represents permissions for different user categories: the first digit for the owner, the second for the group, and the third for others. These numbers specify read (4), write (2), and execute (1) permissions, respectively. Writing them three times (777) sets the same permissions for all user categories—owner, group, and others—on the specified file or directory, ensuring universal access rights.
Przyznając uprawnienia do plików i katalogów w systemach typu Unix, używamy trzech liczb, znanych jako notacja ósemkowa (np. 777). Każda cyfra reprezentuje uprawnienia dla różnych kategorii użytkowników: pierwsza cyfra dotyczy właściciela, druga grupy, a trzecia innych użytkowników. Te liczby określają odpowiednio uprawnienia do odczytu (4), zapisu (2) i wykonania (1). Zapisując je trzykrotnie (777), ustawiamy te same uprawnienia dla wszystkich kategorii użytkowników — właściciela, grupy i innych — na określonym pliku lub katalogu, zapewniając uniwersalne prawa dostępu.

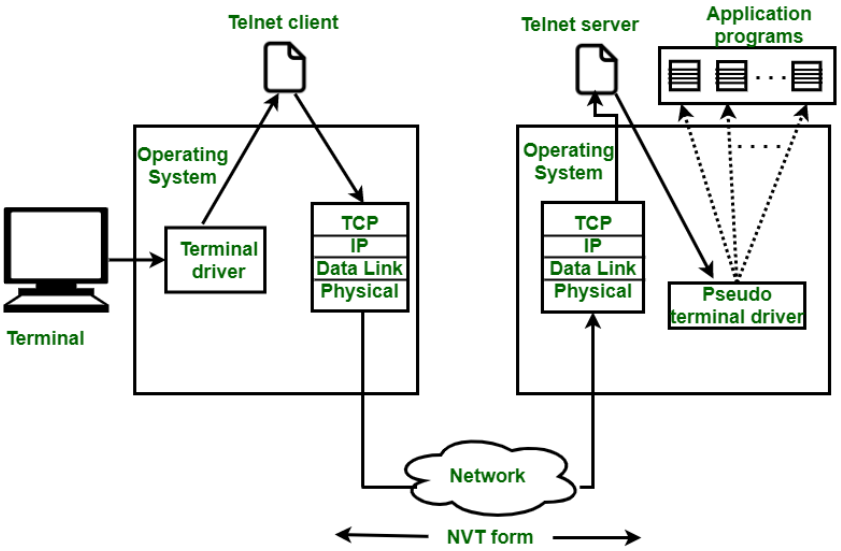


8. Can we create two folders with the same name, one in lowercase letters and the other in uppercase letters?

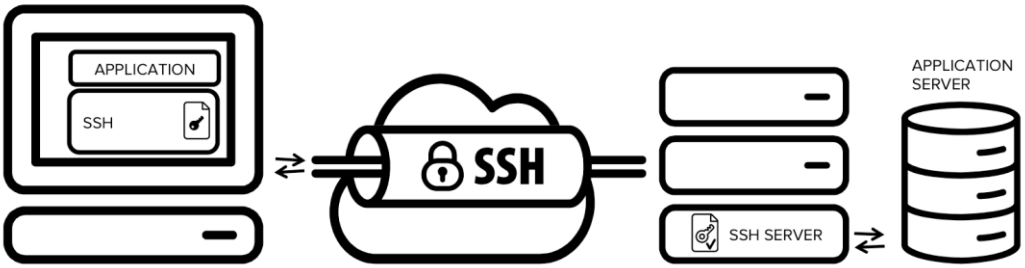
In Unix-like systems such as Linux and macOS, you can create two directories with the same name but different letter cases (Folder and folder) because these systems treat filenames as case-sensitive. However, in Windows, while the filesystem supports case sensitivity, the default behavior for most filesystems (NTFS) is case-insensitive. Therefore, attempting to create such directories would typically result in an error indicating that the directory already exists.
W systemach typu Unix, takich jak Linux i macOS, można utworzyć dwa katalogi o tej samej nazwie, różniących się wielkością liter (Folder i folder), ponieważ te systemy traktują nazwy plików jako wrażliwe na wielkość liter. Natomiast w systemie Windows, chociaż system plików obsługuje wrażliwość na wielkość liter, domyślne zachowanie większości systemów plików (NTFS) jest niewrażliwe na wielkość liter. Dlatego próba utworzenia takich katalogów zazwyczaj kończy się błędem wskazującym, że katalog już istnieje.

9. Define the following concepts:

- telnet
Telnet is a network protocol used for remote access to computers over a network, allowing users to log in and execute commands on a remote machine, but it transmits data, including passwords, in plaintext, making it insecure for modern network use.
Telnet to protokół sieciowy używany do zdalnego dostępu do komputerów przez sieć, umożliwiający użytkownikom logowanie i wykonywanie poleceń na zdalnej maszynie, jednak przesyła dane, w tym hasła, w postaci tekstu jawnej, co czyni go nieszyfrowanym i niebezpiecznym w dzisiejszych sieciach.



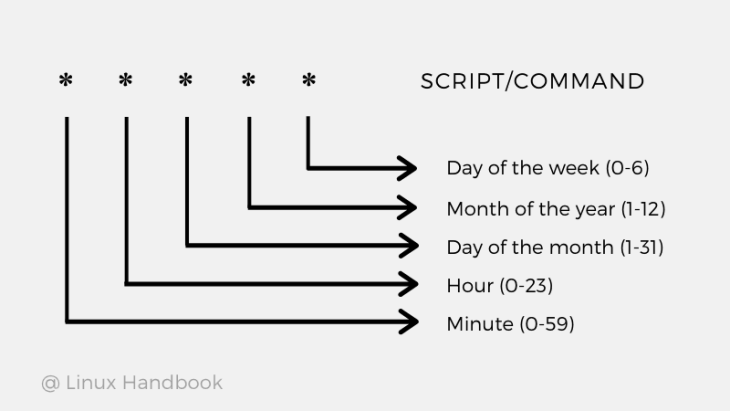
- SSH
SSH (Secure Shell) is a cryptographic network protocol that provides secure access to a remote computer over an unsecured network. It encrypts data during transmission, offering secure remote login, command execution, and file transfer capabilities, replacing insecure protocols like Telnet.
SSH (Secure Shell) to kryptograficzny protokół sieciowy zapewniający bezpieczny dostęp do zdalnego komputera przez niezabezpieczoną sieć. Szyfruje dane podczas transmisji, oferując bezpieczne logowanie zdalne, wykonywanie poleceń oraz transfer plików, zastępując niezabezpieczone protokoły, takie jak Telnet.



-Crontab

Crontab is a Unix utility used to schedule jobs (commands or scripts) to run periodically at fixed times, dates, or intervals. It allows users to automate repetitive tasks such as backups, updates, and maintenance on Unix-like systems.

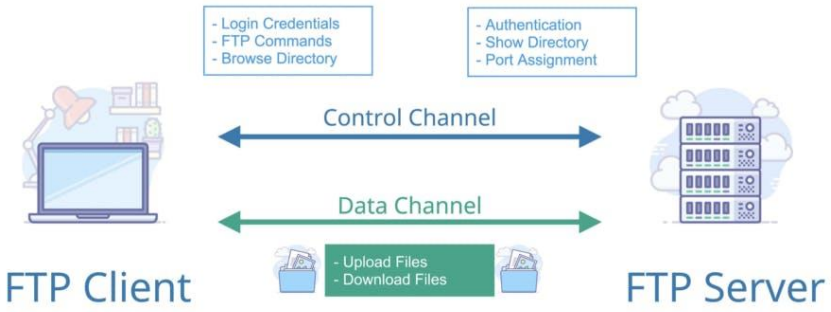
Crontab to narzędzie w systemach Unixowych służące do harmonogramowania zadań (komend lub skryptów), które mają być wykonywane periodycznie o stałych godzinach, datach lub interwałach czasowych. Umożliwia automatyzację powtarzalnych zadań, takich jak backupy, aktualizacje i konserwacja systemów.



-FTP

FTP (File Transfer Protocol) is a standard network protocol used for transferring files between a client and a server on a computer network. It operates over a clear-text channel, making it less secure for transmitting sensitive data unless used with additional security measures like FTPS or SFTP.

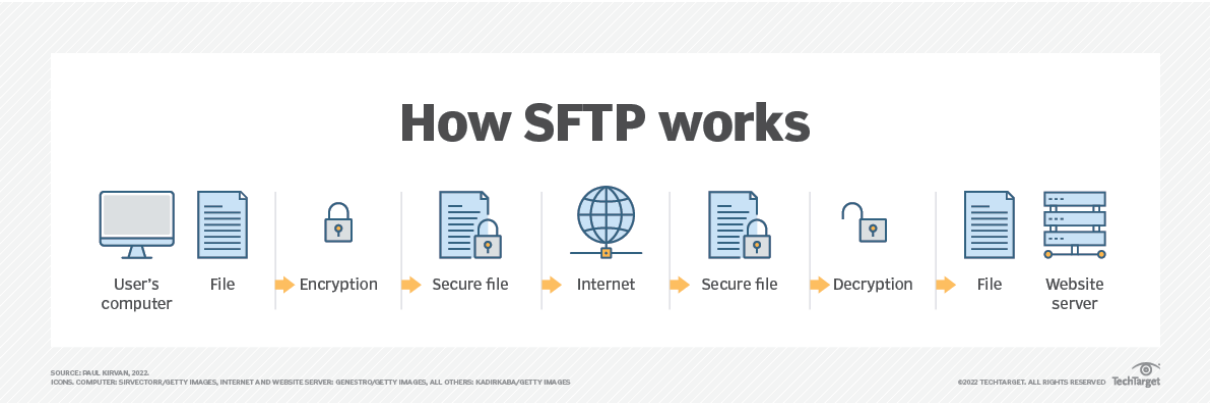
FTP (File Transfer Protocol) to standardowy protokół sieciowy używany do transferu plików między klientem a serwerem w sieci komputerowej. Działa w trybie tekstowym, co czyni go mniej bezpiecznym do przesyłania wrażliwych danych, chyba że jest używany z dodatkowymi środkami bezpieczeństwa, takimi jak FTPS lub SFTP.



-SFTP

SFTP (SSH File Transfer Protocol) is a secure extension of SSH that provides secure file transfer and manipulation capabilities over a secure channel. It uses encryption to protect data during transmission, ensuring confidentiality and integrity, unlike traditional FTP.

SFTP (SSH File Transfer Protocol) to bezpieczne rozszerzenie protokołu SSH, które zapewnia bezpieczny transfer i manipulację plikami poprzez zabezpieczony kanał. Używa szyfrowania do ochrony danych podczas transmisji, zapewniając poufność i integralność, w przeciwieństwie do tradycyjnego FTP.



- gzip tar

gzip tar: gzip and tar are Unix utilities often used together to compress and archive files and directories into a single file. tar bundles multiple files into an archive, while gzip compresses the tar archive to reduce its size, commonly used for backups and distribution of files.

gzip i tar to narzędzia w systemie Unix często używane razem do kompresji i archiwizacji plików i katalogów w jednym pliku. tar łączy wiele plików w archiwum, podczas gdy gzip kompresuje archiwum tar, zmniejszając jego rozmiar, powszechnie stosowane do backupów i dystrybucji plików.

Syntax

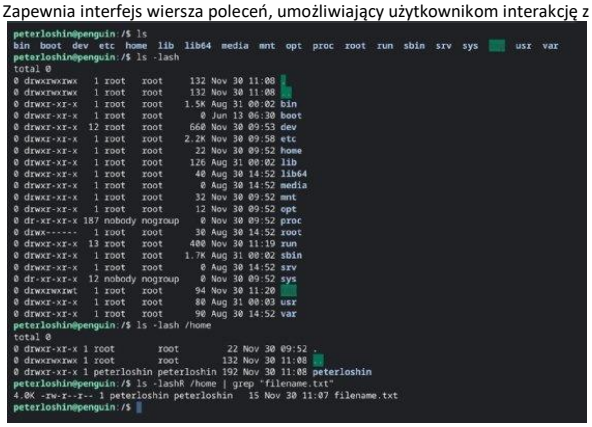
tar [options] [archive-file] [file or directory to be archived]

- tar
  - tar –cvf techplayon.tar techplayon (compressing)
  - tar –xvf techplayon.tar (uncompressing)
- gzip
  - tar –czvf techplayon.tar.gz techplayon (compressing)
  - tar –xzvf techplayon.tar.gz (uncompressing)

-bash

Bash (Bourne Again SHell) is a Unix shell and command language interpreter, commonly used as the default shell on Linux and macOS. It provides a command-line interface for users to interact with the operating system, run commands, and execute scripts.

Bash (Bourne Again SHell) to interpreter poleceń i powłoka systemu Unix, powszechnie używana jako domyślna powłoka na systemach Linux i macOS. Zapewnia interfejs wiersza poleceń, umożliwiający użytkownikom interakcję z systemem operacyjnym, uruchamianie poleceń i wykonywanie skryptów.



-Apache

Apache HTTP Server, commonly referred to as Apache, is an open-source web server software that delivers web content across the internet. It powers a significant portion of websites globally, providing features such as SSL/TLS encryption, virtual hosting, and URL rewriting for customization.

Apache HTTP Server, zwany także Apache, to oprogramowanie serwera WWW typu open-source, które dostarcza zawartość internetową przez sieć. Obsługuje znaczną część witryn internetowych na całym świecie, oferując funkcje takie jak szyfrowanie SSL/TLS, wirtualne hostowanie i przepisywanie adresów URL do dostosowywania.

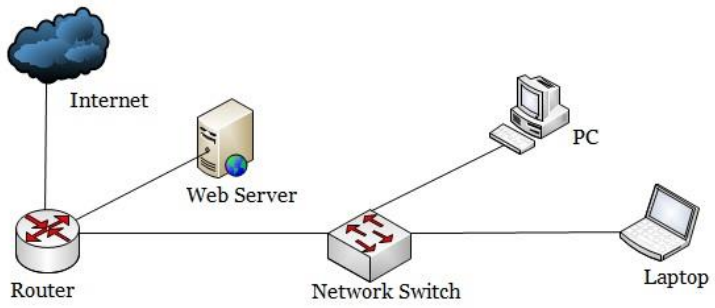


Fig: Network with Apache Web Server