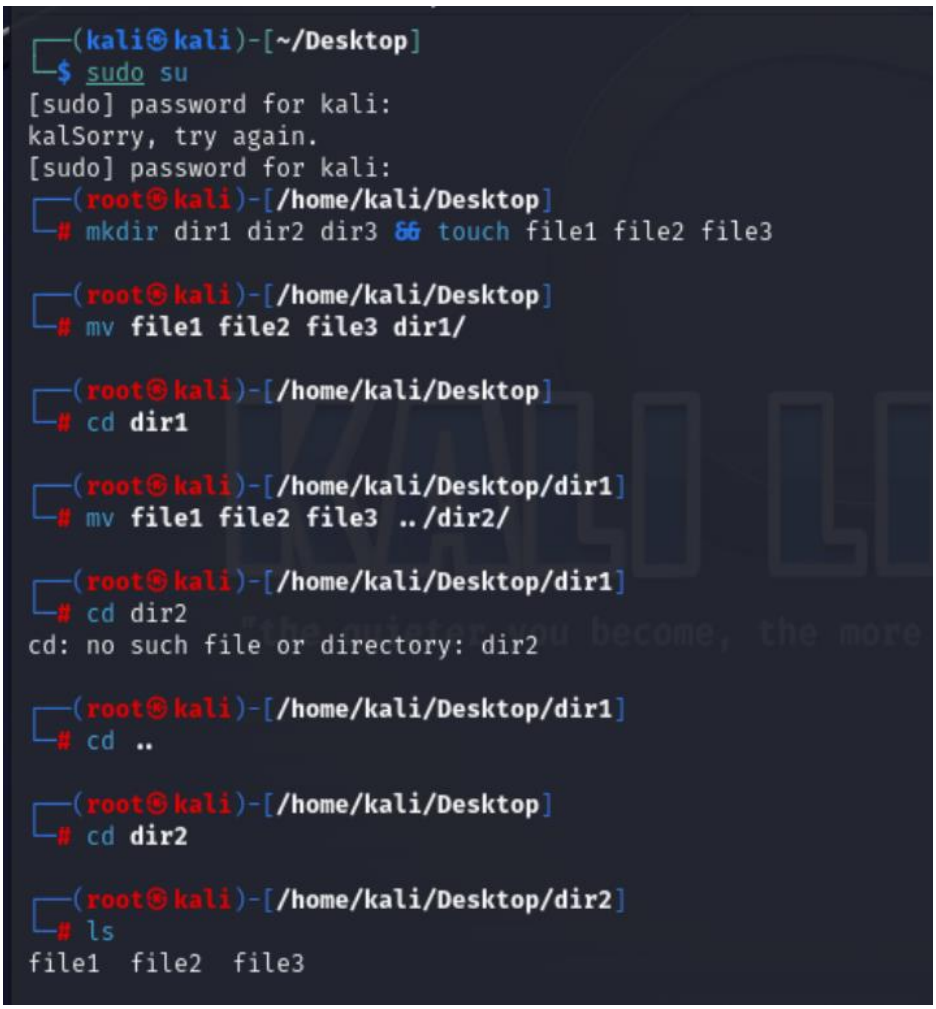
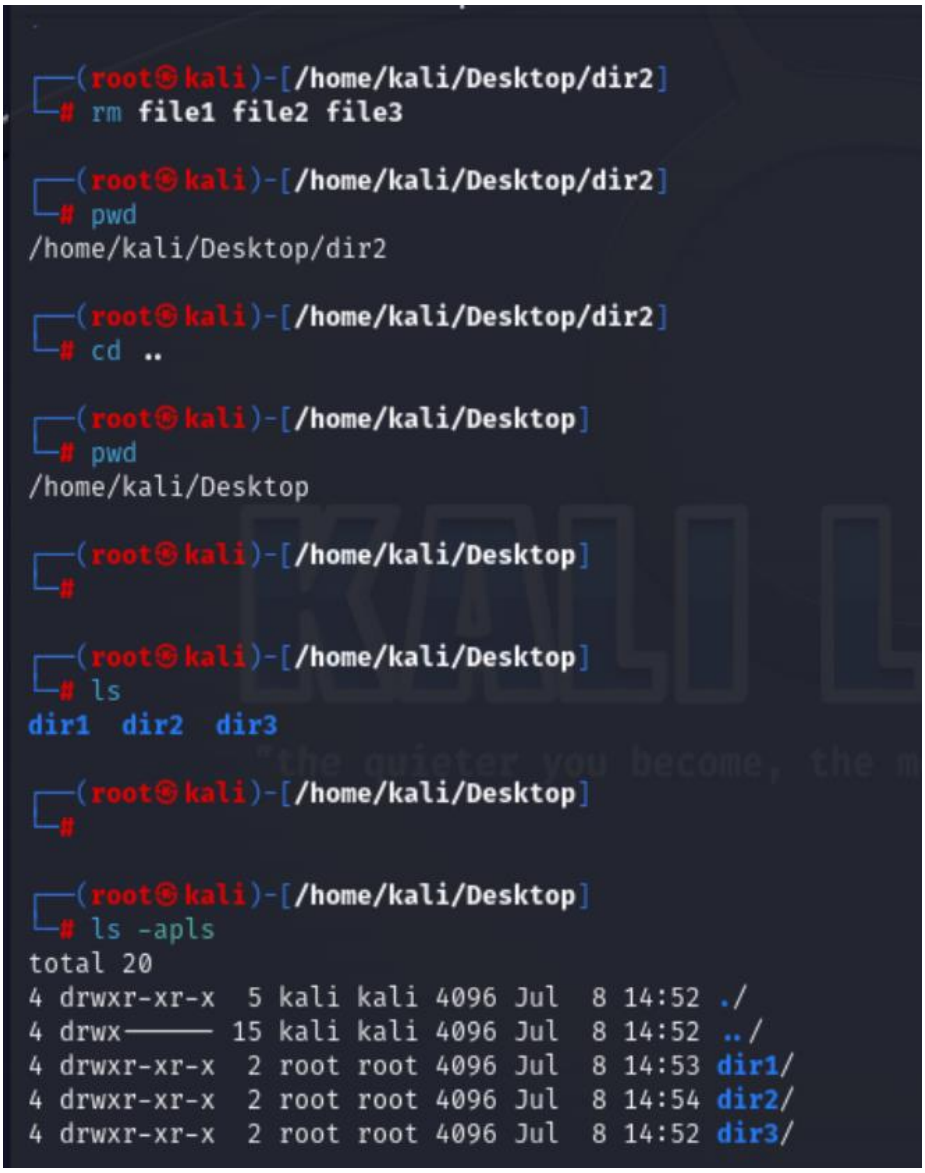
Jakub Jędrzejczak

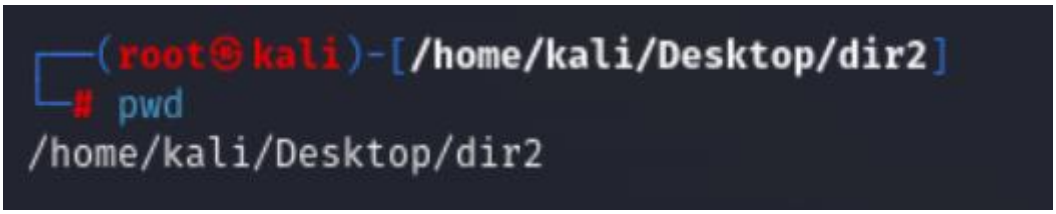
Part 1: Basic Commands

1.




┌──(root㉿kali)-[/home/kali/Desktop/dir2]
└─# rm file1 file2 file3
┌──(root㉿kali)-[/home/kali/Desktop/dir2]
└─# pwd
/home/kali/Desktop/dir2
┌──(root㉿kali)-[/home/kali/Desktop/dir2]
└─# cd ..
┌──(root㉿kali)-[/home/kali/Desktop]
└─# pwd
/home/kali/Desktop
┌──(root㉿kali)-[/home/kali/Desktop]
└─#
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ls
dir1 dir2 dir3
┌──(root㉿kali)-[/home/kali/Desktop]
└─#
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ls -apls
total 20
4 drwxr-xr-x 5 kali kali 4096 Jul 8 14:52 ./
4 drwx------ 15 kali kali 4096 Jul 8 14:52 ../
4 drwxr-xr-x 2 root root 4096 Jul 8 14:53 dir1/
4 drwxr-xr-x 2 root root 4096 Jul 8 14:54 dir2/
4 drwxr-xr-x 2 root root 4096 Jul 8 14:52 dir3/

2.


┌──(root㉿kali)-[/home/kali/Desktop/dir2]
└─# pwd
/home/kali/Desktop/dir2

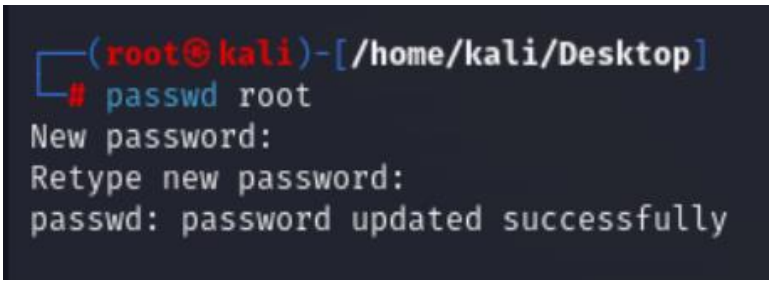
3.

LUB

4.

5.

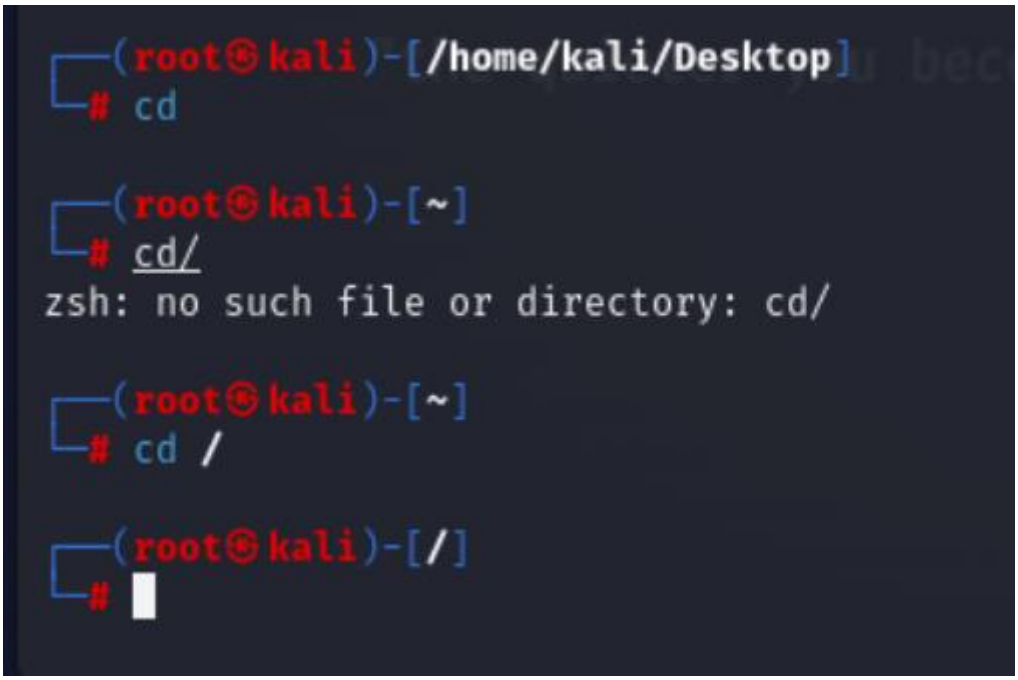
6.



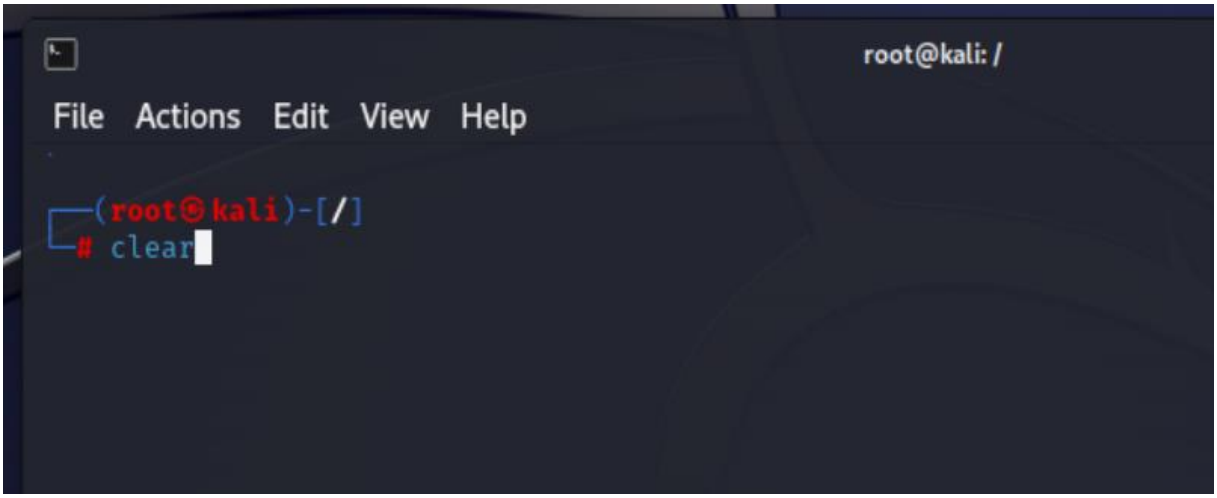
7. cd (change directory) jest komendą używaną w systemach operacyjnych Unix i podobnych do Unix, takimi jak Linux, do zmiany bieżącego katalogu roboczego.

8. cd / zmienia bieżący katalog roboczy na katalog główny (/), który jest najwyższym poziomem w hierarchii systemu plików Unix/Linux.

9.


(root㉿kali)-[/home/kali/Desktop]
cd
(root㉿kali)-[~]
cd/
zsh: no such file or directory: cd/
(root㉿kali)-[~]
cd /
(root㉿kali)-[/]
#

10.


root@kali: /
File Actions Edit View Help
(root㉿kali)-[/]
clear

11.


(root㉿kali)-[/]
nano favorite_os.txt
(root㉿kali)-[/]
ls
bin etc initrd.img lib32 media proc sbin sys var
boot favorite_os.txt initrd.img.old lib64 mnt root srv tmp vmlinuz
dev home lib lost+found opt run swapfile usr vmlinuz.old
(root㉿kali)-[/]
cat favorite_os.txt
linux
(root㉿kali)-[/]
#


┌──(root㉿kali)-[/]
└─# uname -o
GNU/Linux
┌──(root㉿kali)-[/]
└─# uname -o >> favorite_os.txt
┌──(root㉿kali)-[/]
└─# cat /etc/os-release >> favorite_os.txt
┌──(root㉿kali)-[/]
└─# cat favorite_os.txt
linux
GNU/Linux
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2023.4"
VERSION="2023.4"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"
┌──(root㉿kali)-[/]
└─#

12.

```
┌──(root㉿kali)-[/]
└─# cat favorite_os.txt
linux
GNU/Linux
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2023.4"
VERSION="2023.4"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"
```

Part 2: The Find Command

13.

```
┌──(root㉿kali)-[/]
└─# cd /home/kali/Desktop

┌──(root㉿kali)-[/home/kali/Desktop]
└─# touch .hiddenfile1 .hiddenfile2 .hiddenfile3
```

14.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ls -a
.  ..  dir1  dir2  dir3  .hiddenfile1  .hiddenfile2  .hiddenfile3
```

15.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# rm .hiddenfile1 .hiddenfile2 .hiddenfile3
```

16.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# sudo touch /bin/testfile1 /sbin/testfile2 /usr/bin/testfile3 /usr/sbin/testfile4 /etc/testfile5 /var/test
file6
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# find /bin /sbin /usr/bin /usr/sbin /etc /var -type f -name 'testfile*'
/usr/bin/testfile3
/usr/bin/testfile1
/usr/sbin/testfile2
/usr/sbin/testfile4
/etc/testfile5
/var/testfile6
```

17.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cd /

┌──(root㉿kali)-[/]
└─# find . -type f -name '[0-9][0-9][0-9]*'
./usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/metasploit-model-5.0.2/spec/dummy/public/422.h
tml
./usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/metasploit-model-5.0.2/spec/dummy/public/404.h
tml
./usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/metasploit-model-5.0.2/spec/dummy/public/500.h
tml
./usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/activestorage-7.0.8/db/migrate/20170806125915_
create_active_storage_tables.rb
./usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/activestorage-7.0.8/db/update_migrate/20190112
182829_add_service_name_to_active_storage_blobs.rb
./usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/activestorage-7.0.8/db/update_migrate/20211119
233751_remove_not_null_on_active_storage_blobs_checksum.rb
./usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/activestorage-7.0.8/db/update_migrate/20191206
030411_create_active_storage_variant_records.rb
./usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/actiontext-7.0.8/db/migrate/20180528164100_cre
ate_action_text_tables.rb
./usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/metasploit_data_models-6.0.3/db/migrate/014_ad
d_loots_fields.rb
./usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/metasploit_data_models-6.0.3/db/migrate/201305
22041110_create_task_services.rb
./usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/metasploit_data_models-6.0.3/db/migrate/201502
09195939_add_vuln_id_to_note.rb
./usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/metasploit_data_models-6.0.3/db/migrate/201304
30162145_enforce_address_uniqueness_in_workspace_in_hosts.rb
./usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/metasploit_data_models-6.0.3/db/migrate/201504
21211719_rename_automatic_exploitation_index.rb
./usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/metasploit_data_models-6.0.3/db/migrate/201502
05192745_drop_service_uniqueness_index.rb
```

18.

```
┌──(root㉿kali)-[/]
└─# find / -type f -name '[0-9][0-9][0-9][0-9][0-9]*' 2>/dev/null
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/activestorage-7.0.8/db/migrate/20170806125915_
reate_active_storage_tables.rb
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/activestorage-7.0.8/db/update_migrate/20190112
82829_add_service_name_to_active_storage_blobs.rb
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/activestorage-7.0.8/db/update_migrate/20211119
33751_remove_not_null_on_active_storage_blobs_checksum.rb
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/activestorage-7.0.8/db/update_migrate/20191206
30411_create_active_storage_variant_records.rb
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/actiontext-7.0.8/db/migrate/20180528164100_cre
te_action_text_tables.rb
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/metasploit_data_models-6.0.3/db/migrate/201305
2041110_create_task_services.rb
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/metasploit_data_models-6.0.3/db/migrate/201502
9195939_add_vuln_id_to_note.rb
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/metasploit_data_models-6.0.3/db/migrate/201304
0162145_enforce_address_uniqueness_in_workspace_in_hosts.rb
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/metasploit_data_models-6.0.3/db/migrate/201504
1211719_rename_automatic_exploitation_index.rb
```

19.

```
┌──(root㉿kali)-[/]
└─# find / -type f -name 'bash*' 2>/dev/null
/usr/share/metasploit-framework/modules/exploits/linux/local/bash_profile_persistence.rb
/usr/share/metasploit-framework/modules/exploits/unix/dhcp/bash_environment.rb
/usr/share/menu/bash
/usr/share/bash-completion/bash_completion
/usr/share/doc/adduser/examples/adduser.local.conf.examples/bash.bashrc
/usr/share/doc/metasploit-framework/modules/exploit/linux/local/bash_profile_persistence.md
/usr/share/doc/zsh-common/examples/Misc/bash2zshprompt
/usr/share/zsh/functions/Completion/bashcompinit
/usr/share/pkgconfig/bash-completion.pc
/usr/share/powershell-empire/empire/server/stagers/multi/__pycache__/bash.cpython-311.pyc
/usr/share/powershell-empire/empire/server/stagers/multi/bash.py
/usr/share/powershell-empire/empire/server/modules/python/privesc/multi/bashdoor.py
/usr/share/powershell-empire/empire/server/modules/python/privesc/multi/__pycache__/bashdoor.cpython-311.pyc
/usr/share/powershell-empire/empire/server/modules/python/privesc/multi/bashdoor.yaml
/usr/share/ri/3.1.0/system/Gem/Installer/bash_prolog_script-i.ri
/usr/share/perl5/Debian/Debhelper/Sequence/bash_completion.pm
/usr/share/texlive/texmf-dist/tex/latex/bashful/bashful.sty
/usr/share/locale/zh_CN/LC_MESSAGES/bash.mo
/usr/share/locale/sv/LC_MESSAGES/bash.mo
/usr/share/locale/it/LC_MESSAGES/bash.mo
/usr/share/locale/nb/LC_MESSAGES/bash.mo
/usr/share/locale/uk/LC_MESSAGES/bash.mo
/usr/share/locale/sr/LC_MESSAGES/bash.mo
/usr/share/locale/ga/LC_MESSAGES/bash.mo
/usr/share/locale/et/LC_MESSAGES/bash.mo
/usr/share/locale/eo/LC_MESSAGES/bash.mo
/usr/share/locale/el/LC_MESSAGES/bash.mo
/usr/share/locale/ru/LC_MESSAGES/bash.mo
/usr/share/locale/ja/LC_MESSAGES/bash.mo
/usr/share/locale/en@quot/LC_MESSAGES/bash.mo
```

20.

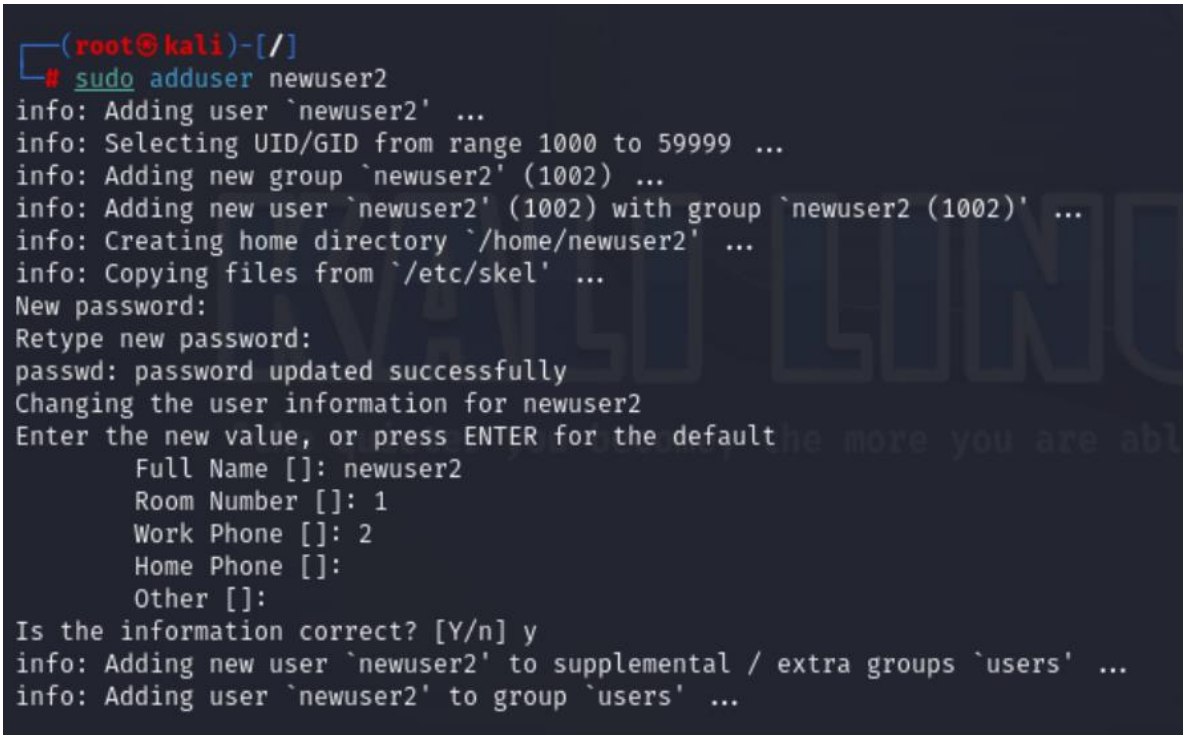
```
File  Actions  Edit  View  Help
/var/log/sysstat
/var/log/inetsim
/var/log/inetsim/report
/var/log/nginx
/var/log/gvm
/var/log/runit
/var/log/runit/ssh
/var/log/samba
/var/log/apt
/var/log/stunnel4
/var/log/speech-dispatcher
/var/log/journal
/var/log/journal/62515a8596cc47a486f33f8642473978
/var/log/lightdm
/var/log/apache2
/var/log/openvpn
/var/tmp
/var/tmp/systemd-private-1a0b8aab9d7949969430d1484c3fd50d-haveged.service-oaqQrz
/var/tmp/systemd-private-1a0b8aab9d7949969430d1484c3fd50d-haveged.service-oaqQrz/tmp
/var/tmp/systemd-private-1a0b8aab9d7949969430d1484c3fd50d-upower.service-Mto2VE
/var/tmp/systemd-private-1a0b8aab9d7949969430d1484c3fd50d-upower.service-Mto2VE/tmp
/var/tmp/systemd-private-1a0b8aab9d7949969430d1484c3fd50d-systemd-logind.service-i6HkmZ
/var/tmp/systemd-private-1a0b8aab9d7949969430d1484c3fd50d-systemd-logind.service-i6HkmZ/tmp
/var/tmp/systemd-private-1a0b8aab9d7949969430d1484c3fd50d-polkit.service-Im7SuM
/var/tmp/systemd-private-1a0b8aab9d7949969430d1484c3fd50d-polkit.service-Im7SuM/tmp
/var/tmp/systemd-private-1a0b8aab9d7949969430d1484c3fd50d-colord.service-8l2Omv
/var/tmp/systemd-private-1a0b8aab9d7949969430d1484c3fd50d-colord.service-8l2Omv/tmp
/var/tmp/systemd-private-1a0b8aab9d7949969430d1484c3fd50d-ModemManager.service-cFkX9u
/var/tmp/systemd-private-1a0b8aab9d7949969430d1484c3fd50d-ModemManager.service-cFkX9u/tmp
/media

┌──(root㉿kali)-[/]
└─# find / -type d -size -4M 2>/dev/null
```

21.

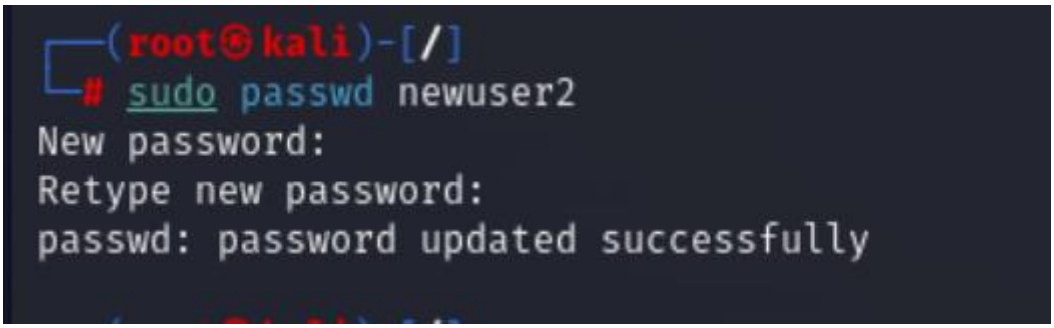
```
File  Actions  Edit  View  Help
/var/lib/apache2/conf/enabled_by_maint/security
/var/.updated
/var/testfile6
/var/log/postgresql/postgresql-16-main.log
/var/log/Xorg.0.log.old
/var/log/boot.log
/var/log/faillog
/var/log/macchanger.log
/var/log/fontconfig.log
/var/log/lastlog
/var/log/nginx/access.log
/var/log/nginx/error.log
/var/log/apt/history.log
/var/log/apt/eipp.log.xz
/var/log/apt/term.log
/var/log/stunnel4/stunnel.log
/var/log/wtmp
/var/log/Xorg.0.log
/var/log/alternatives.log
/var/log/dpkg.log
/var/log/lightdm/x-0.log.old
/var/log/lightdm/seat0-greeter.log
/var/log/lightdm/seat0-greeter.log.old
/var/log/lightdm/x-0.log
/var/log/lightdm/lightdm.log
/var/log/lightdm/lightdm.log.old
/var/log/btmp
/var/log/apache2/access.log
/var/log/apache2/error.log
/var/log/apache2/other_vhosts_access.log

┌──(root㉿kali)-[/]
└─# find / -type f -size -3M 2>/dev/null
```

Part 3: User & Group Management

1.



2.



3.

```
┌──(root㉿kali)-[/]
└─# sudo groupadd newgroup
```

4.

```
┌──(root㉿kali)-[/]
└─# sudo usermod -aG newgroup newuser1
```

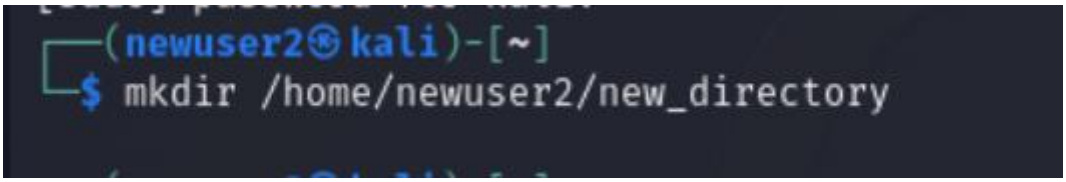
5.

```
┌──(root㉿kali)-[/]
└─# getent passwd | cut -d: -f1 | xargs -n1 groups
root : root
daemon : daemon
bin : bin
sys : sys
sync : nogroup
games : games
man : man
lp : lp
mail : mail
news : news
uucp : uucp
proxy : proxy
www-data : www-data
backup : backup
list : list
irc : irc
_apt : nogroup
nobody : nogroup
systemd-network : systemd-network
systemd-timesync : systemd-timesync
messagebus : messagebus
tss : tss
strongswan : nogroup
tcpdump : tcpdump
usbmux : plugdev
sshd : nogroup
dnsmasq : nogroup
avahi : avahi
speech-dispatcher : audio
pulse : pulse audio
```

6.

7.

8.



9.

mkdir /ścieżka do katalogu/… /directory

10.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo useradd -m -G sudo newuser3 && sudo passwd newuser3
useradd: user 'newuser3' already exists

┌──(root㉿kali)-[/home/kali]
└─# groups newuser3
newuser3 : newuser3 sudo

┌──(root㉿kali)-[/home/kali]
└─# id newuser3
uid=1003(newuser3) gid=1004(newuser3) groups=1004(newuser3),27(sudo)
```

Part 4: Permissions

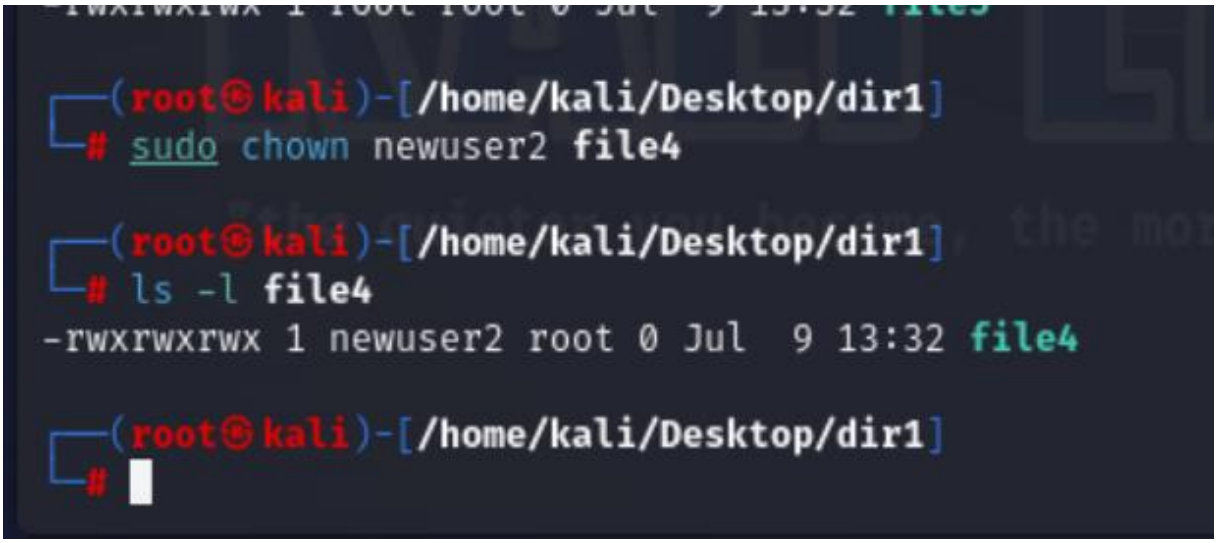
1.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cd /home/kali/Desktop/dir1

┌──(root㉿kali)-[/home/kali/Desktop/dir1]
└─# touch file4 file5

┌──(root㉿kali)-[/home/kali/Desktop/dir1]
└─# chmod a=w file4 file5

┌──(root㉿kali)-[/home/kali/Desktop/dir1]
└─#
```

2.

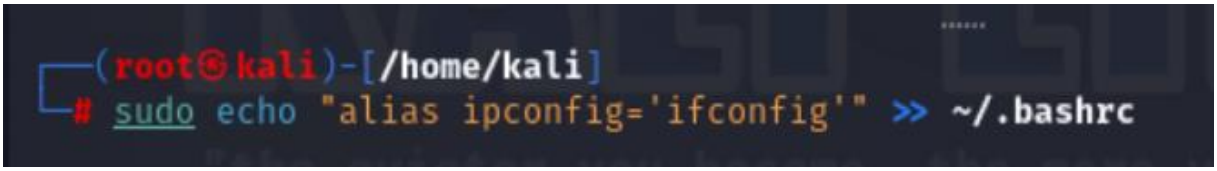
```
┌──(root㉿kali)-[/home/kali/Desktop/dir1]
└─# chmod 777 file4 file5

┌──(root㉿kali)-[/home/kali/Desktop/dir1]
└─# ls -l file4 file5
-rwxrwxrwx 1 root root 0 Jul  9 13:32 file4
-rwxrwxrwx 1 root root 0 Jul  9 13:32 file5

┌──(root㉿kali)-[/home/kali/Desktop/dir1]
```

3.

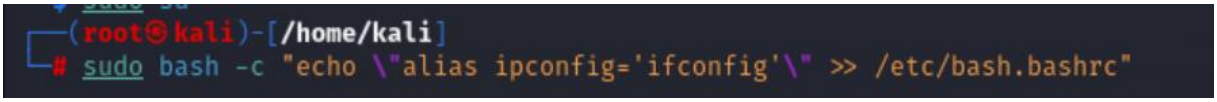


Part 5: ALIAS

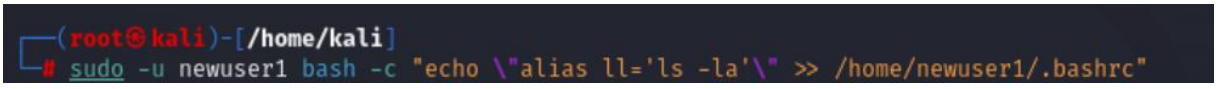
1.



2.

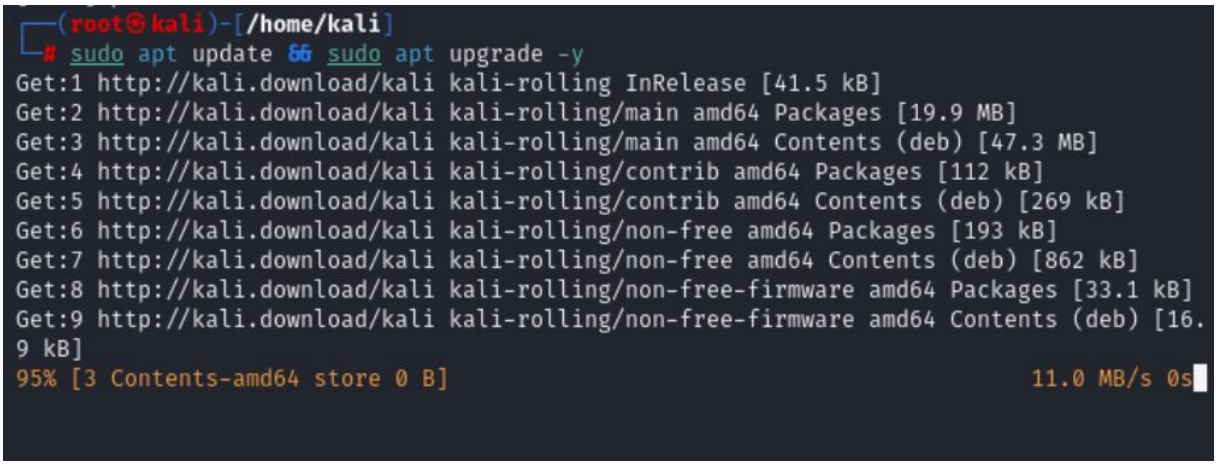


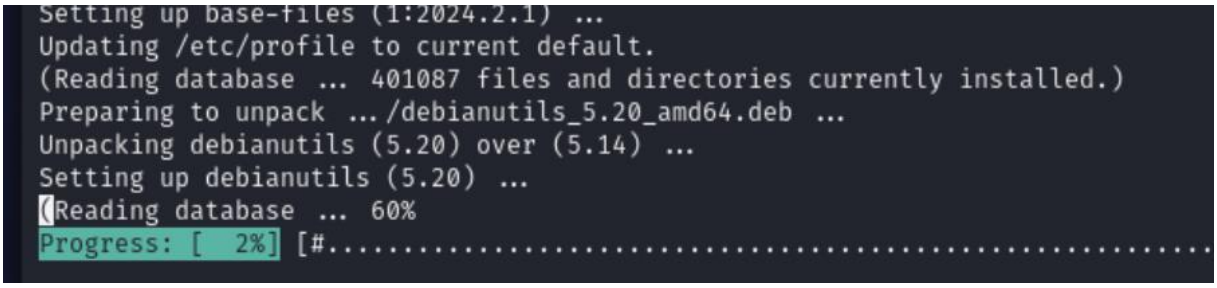
3.

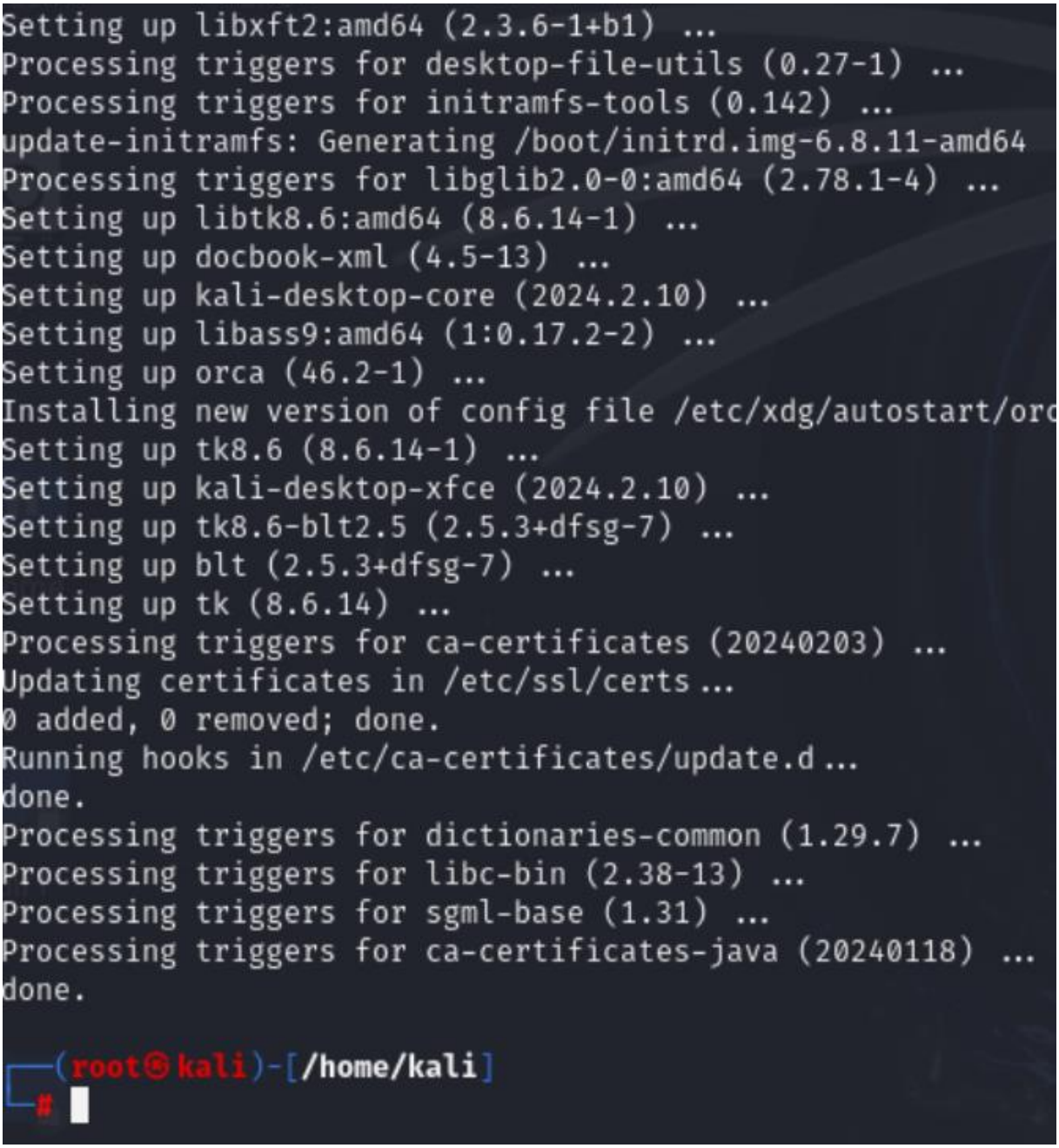


Part 6: System Update and Apt Usage

1.



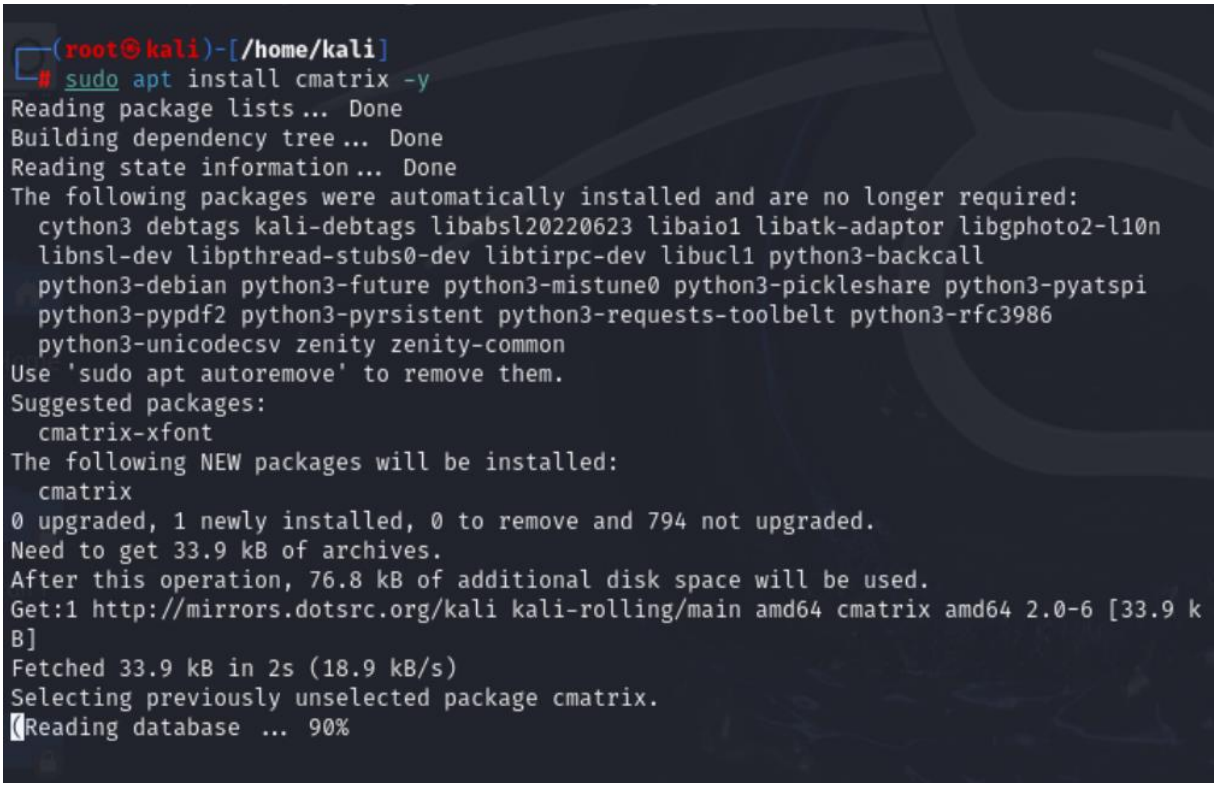

Setting up base-files (1:2024.2.1) ...
Updating /etc/profile to current default.
(Reading database ... 401087 files and directories currently installed.)
Preparing to unpack .../debianutils_5.20_amd64.deb ...
Unpacking debianutils (5.20) over (5.14) ...
Setting up debianutils (5.20) ...
(Reading database ... 60%
Progress: [2%] [#.....


Setting up libxft2:amd64 (2.3.6-1+b1) ...
Processing triggers for desktop-file-utils (0.27-1) ...
Processing triggers for initramfs-tools (0.142) ...
update-initramfs: Generating /boot/initrd.img-6.8.11-amd64
Processing triggers for libglib2.0-0:amd64 (2.78.1-4) ...
Setting up libtk8.6:amd64 (8.6.14-1) ...
Setting up docbook-xml (4.5-13) ...
Setting up kali-desktop-core (2024.2.10) ...
Setting up libass9:amd64 (1:0.17.2-2) ...
Setting up orca (46.2-1) ...
Installing new version of config file /etc/xdg/autostart/orc
Setting up tk8.6 (8.6.14-1) ...
Setting up kali-desktop-xfce (2024.2.10) ...
Setting up tk8.6-blt2.5 (2.5.3+dfsg-7) ...
Setting up blt (2.5.3+dfsg-7) ...
Setting up tk (8.6.14) ...
Processing triggers for ca-certificates (20240203) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
Processing triggers for dictionaries-common (1.29.7) ...
Processing triggers for libc-bin (2.38-13) ...
Processing triggers for sgml-base (1.31) ...
Processing triggers for ca-certificates-java (20240118) ...
done.
┌──(root㉿kali)-[/home/kali]
└─#

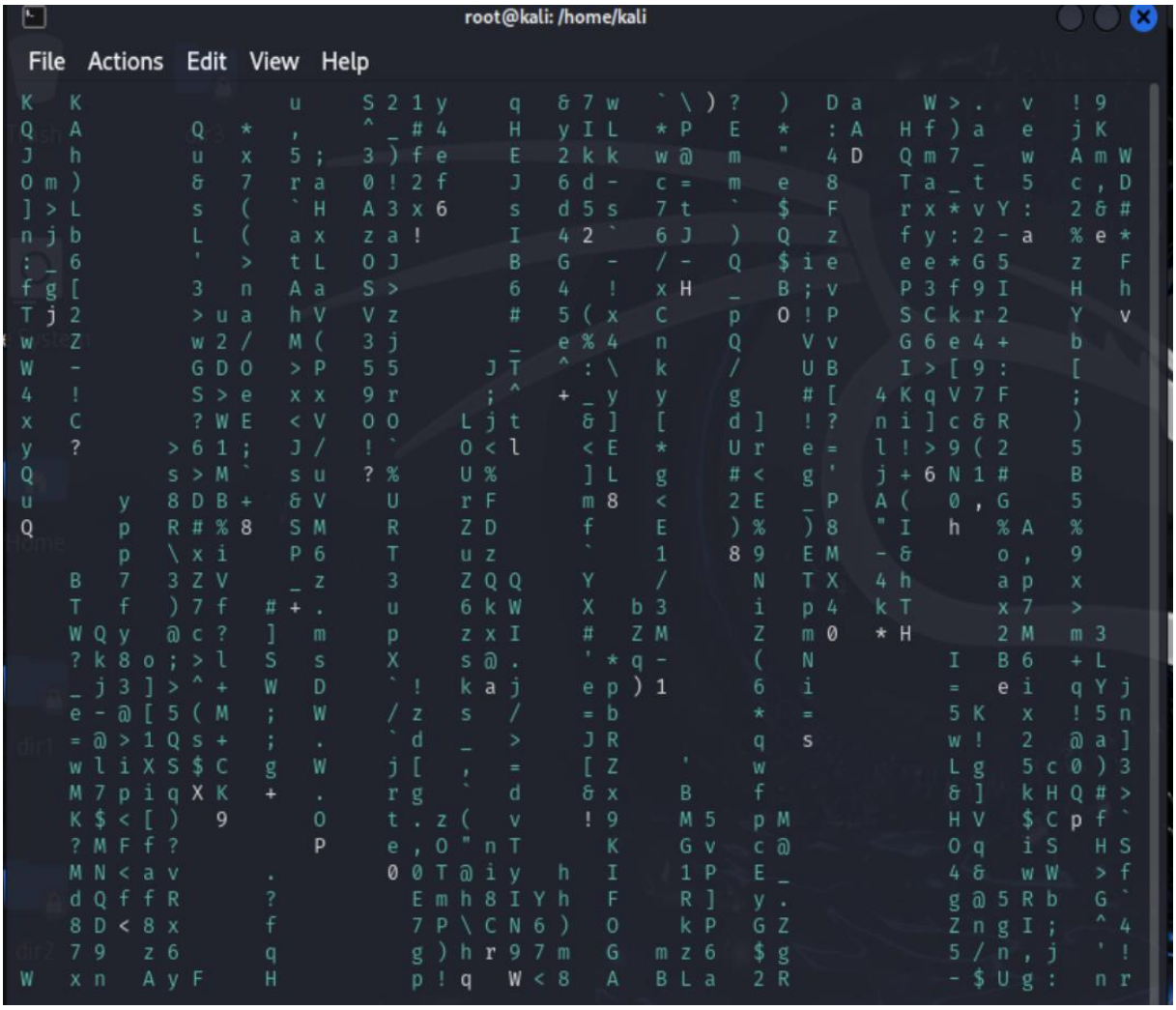
2.


┌──(root㉿kali)-[/home/kali]
└─# sudo nano /etc/apt/sources.list
┌──(root㉿kali)-[/home/kali]
└─# cat /etc/apt/sources.list
See https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
Additional line for source packages
deb-src http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
┌──(root㉿kali)-[/home/kali]

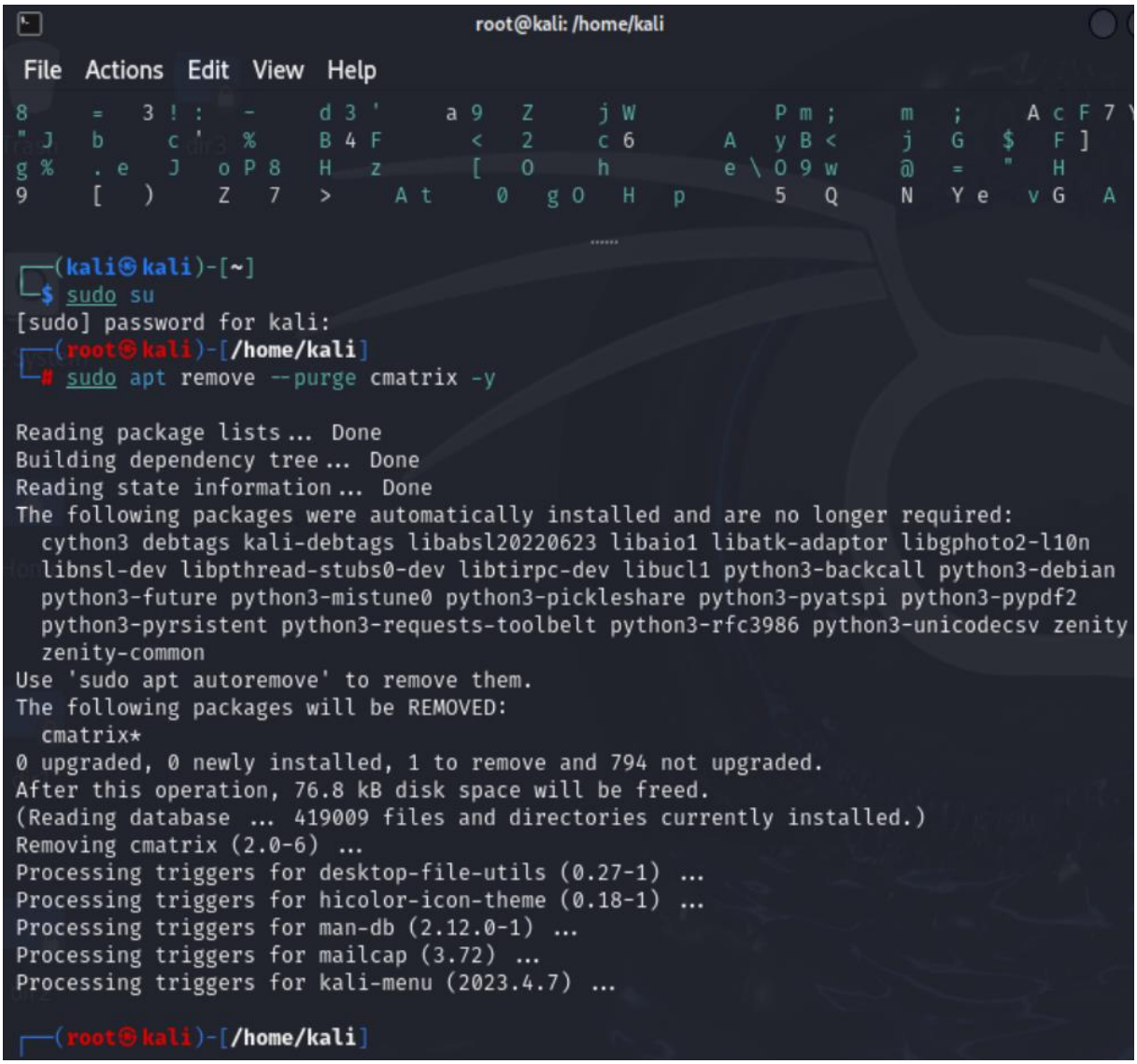
3.


┌──(root㉿kali)-[/home/kali]
└─# sudo apt install cmatrix -y
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
cython3 debtags kali-debtags libabsl20220623 libaio1 libatk-adaptor libgphoto2-l10n
libnsl-dev libpthread-stubs0-dev libtirpc-dev libucl1 python3-backcall
python3-debian python3-future python3-mistune0 python3-pickleshare python3-pyatspi
python3-pypdf2 python3-pyrsistent python3-requests-toolbelt python3-rfc3986
python3-unicodecsv zenity zenity-common
Use 'sudo apt autoremove' to remove them.
Suggested packages:
cmatrix-xfont
The following NEW packages will be installed:
cmatrix
0 upgraded, 1 newly installed, 0 to remove and 794 not upgraded.
Need to get 33.9 kB of archives.
After this operation, 76.8 kB of additional disk space will be used.
Get:1 http://mirrors.dotsrc.org/kali kali-rolling/main amd64 cmatrix amd64 2.0-6 [33.9 k
B]
Fetched 33.9 kB in 2s (18.9 kB/s)
Selecting previously unselected package cmatrix.
(Reading database ... 90%

cmatrix

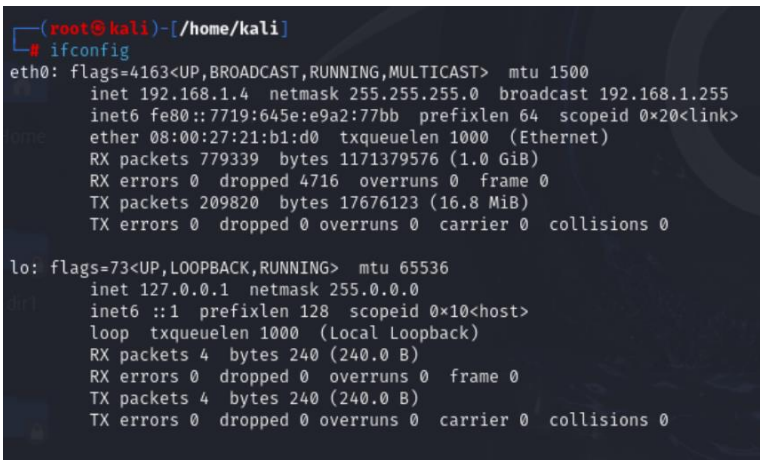


4.



Part 7: ifconfig and Address Settings

1.



2.

```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig | tr '[:lower:]' '[:upper:]'
ETH0: FLAGS=4163<UP,BROADCAST,RUNNING,MULTICAST>  MTU 1500
        INET 192.168.1.4  NETMASK 255.255.255.0  BROADCAST 192.168.1.255
        INET6 FE80::7719:645E:E9A2:77BB  PREFIXLEN 64  SCOPEID 0X20<LINK>
        ETHER 08:00:27:21:B1:D0  TXQUEUELEN 1000  (ETHERNET)
        RX PACKETS 779575  BYTES 1171393786 (1.0 GIB)
        RX ERRORS 0  DROPPED 4951  OVERRUNS 0  FRAME 0
        TX PACKETS 209820  BYTES 17676123 (16.8 MIB)
        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.

```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig | grep -E 'inet|netmask' | awk '{print $1, $2}'
inet 192.168.1.4
inet6 fe80::7719:645e:e9a2:77bb
inet 127.0.0.1
inet6 ::1
```

4.

```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig | grep -E 'inet|netmask' | awk '{print $1, $2}' > ip.log
```

5.

```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig | grep -E 'inet|netmask' | awk '{print $1, $2}' > ip.log

┌──(root㉿kali)-[/home/kali]
└─# echo "User: $(whoami)" >> ip.log

┌──(root㉿kali)-[/home/kali]
└─# echo "Last login sessions:" >> ip.log
```

```
┌──(root㉿kali)-[/home/kali]
└─# echo "Hostname: $(hostname)" >> ip.log

┌──(root㉿kali)-[/home/kali]
└─# ip.log
ip.log: command not found

┌──(root㉿kali)-[/home/kali]
└─# cat ip.log
inet 192.168.1.4
inet6 fe80::7719:645e:e9a2:77bb
inet 127.0.0.1
inet6 ::1
User: root
Last login sessions:
Do you want to install it? (N/y)Hostname: kali

┌──(root㉿kali)-[/home/kali]
└─#
```

6.

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

```
 GNU nano 8.0                    /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

auto eth0
iface eth0 inet static
    address 192.168.1.100
    netmask 255.255.255.0
    gateway 192.168.1.1

                [ Read 10 lines ]
^G Help      ^O Write Out  ^F Where Is   ^K Cut       ^T Execute   ^C Location
```

Part 8: Remote Control and Telnet Services

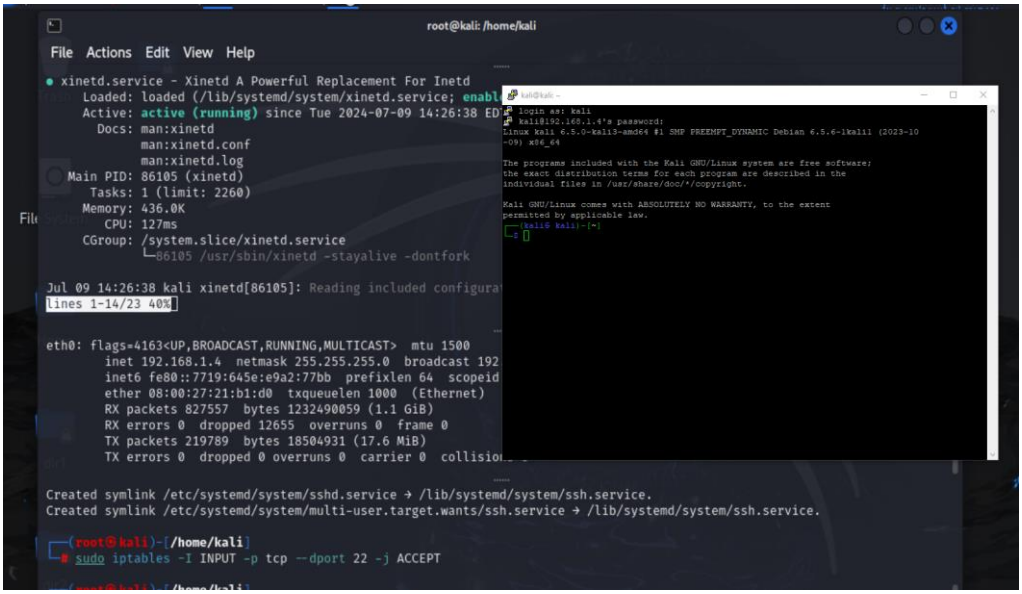
1.

2.

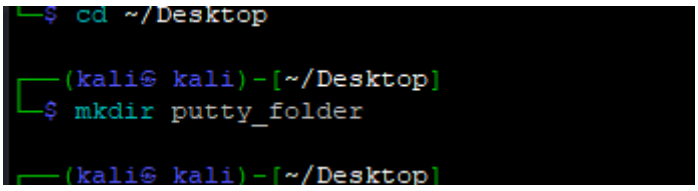
3.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo systemctl status xinetd
● xinetd.service - Xinetd A Powerful Replacement For Inetd
     Loaded: loaded (/lib/systemd/system/xinetd.service; enabled; preset: disabled)
     Active: active (running) since Tue 2024-07-09 14:26:38 EDT; 39s ago
       Docs: man:xinetd
             man:xinetd.conf
             man:xinetd.log
   Main PID: 86105 (xinetd)
      Tasks: 1 (limit: 2260)
     Memory: 436.0K
        CPU: 127ms
     CGroup: /system.slice/xinetd.service
             └─86105 /usr/sbin/xinetd -stayalive -dontfork

Jul 09 14:26:38 kali xinetd[86105]: Reading included configuration file: /etc/xinetd.d/ser>
Jul 09 14:26:38 kali xinetd[86105]: Reading included configuration file: /etc/xinetd.d/ser>
Jul 09 14:26:38 kali xinetd[86105]: Reading included configuration file: /etc/xinetd.d/tel>
Jul 09 14:26:38 kali xinetd[86105]: Server /usr/sbin/in.telnetd is not executable [file=/e>
Jul 09 14:26:38 kali xinetd[86105]: Error parsing attribute server - DISABLING SERVICE [fi>
Jul 09 14:26:38 kali xinetd[86105]: Reading included configuration file: /etc/xinetd.d/tim>
Jul 09 14:26:38 kali xinetd[86105]: Reading included configuration file: /etc/xinetd.d/tim>
Jul 09 14:26:38 kali xinetd[86105]: removing telnet
Jul 09 14:26:38 kali xinetd[86105]: 2.3.15.4 started with libwrap loadavg labeled-networki>
Jul 09 14:26:38 kali xinetd[86105]: Started working: 0 available services
```

4.



5.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls
dir1  dir2  dir3  putty_folder

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

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

┌──(kali㉿kali)-[~/Desktop/putty_folder]
└─$ touch putty_file

┌──(kali㉿kali)-[~/Desktop/putty_folder]
└─$ ls
putty_file

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

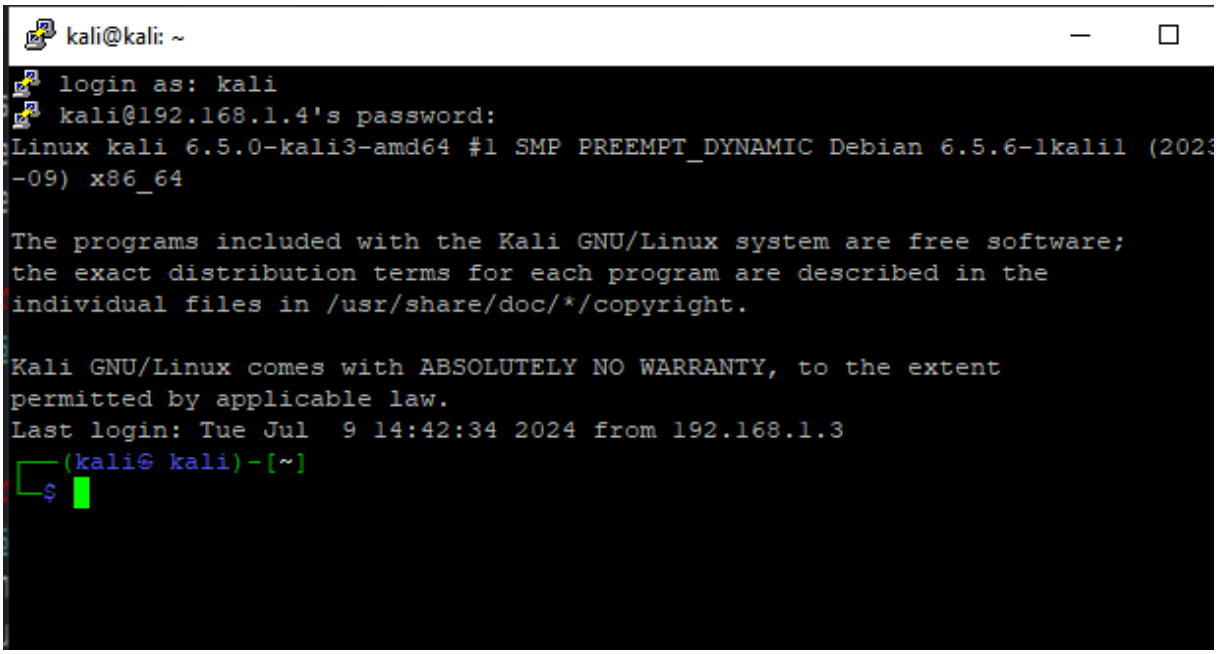
Part 9: SSH Connection

1.

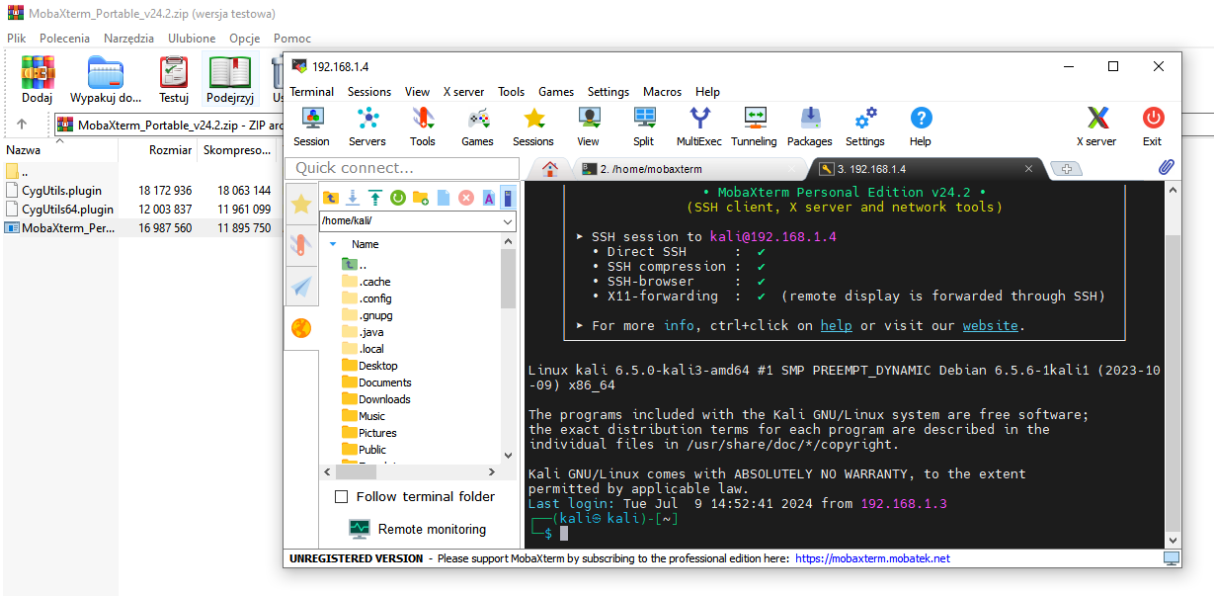
sudo apt install openssh-server -y

```
┌──(root㉿kali)-[/home/kali]
└─# sudo systemctl start ssh

┌──(root㉿kali)-[/home/kali]
└─# sudo systemctl enable ssh
Synchronizing state of ssh.service with
Executing: /lib/systemd/systemd-sysv-ins

┌──(root㉿kali)-[/home/kali]
└─# sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell ser
     Loaded: loaded (/lib/systemd/system
     Active: active (running) since Tue
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 98994 (sshd)
      Tasks: 1 (limit: 2260)
     Memory: 1.3M
        CPU: 16ms
     CGroup: /system.slice/ssh.service
             └─98994 "sshd: /usr/sbin/ss

Jul 09 14:50:53 kali systemd[1]: Startin
Jul 09 14:50:53 kali sshd[98994]: Server
Jul 09 14:50:53 kali sshd[98994]: Server
Jul 09 14:50:53 kali systemd[1]: Started
```

2.


kali@kali: ~
login as: kali
kali@192.168.1.4's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023
-09) x86_64
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jul 9 14:42:34 2024 from 192.168.1.3
(kali㉿kali)-[~]
$

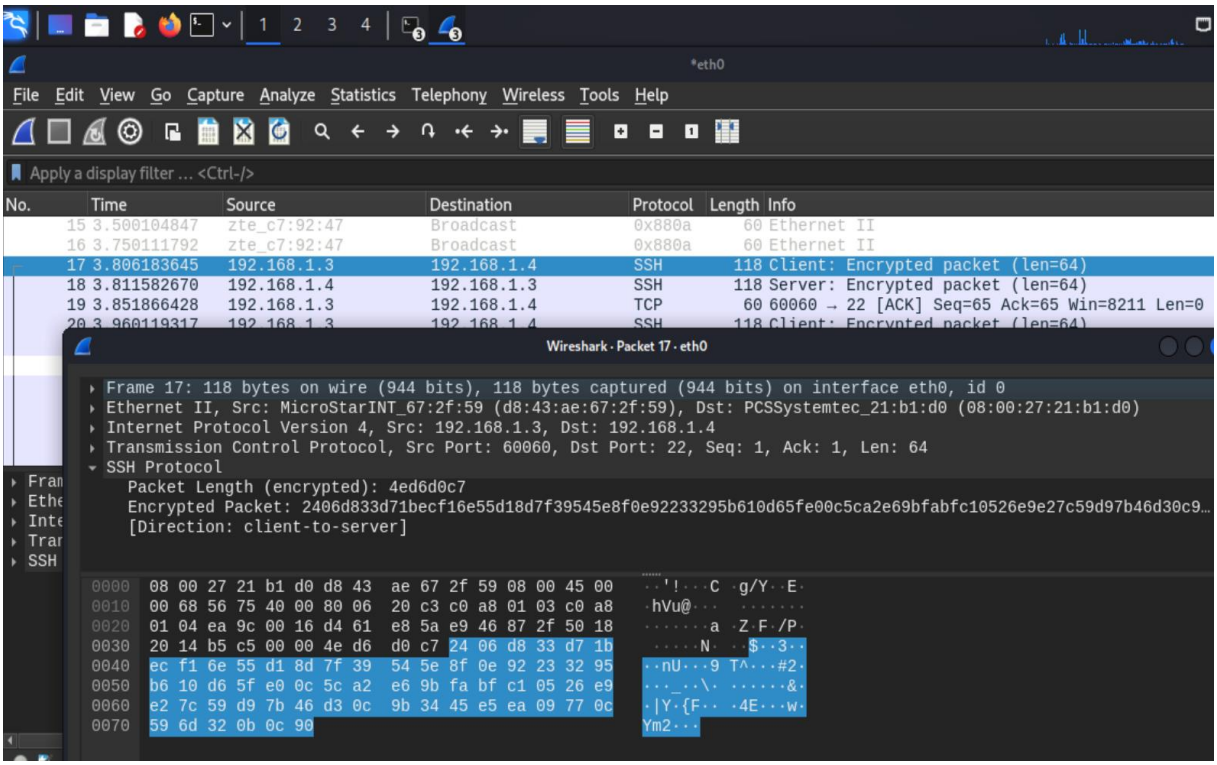
3.


MobaXterm_Portable_v24.2.zip (wersja testowa)
Plik Polecenia Narzędzia Ulubione Opcje Pomoc
Dodaj Wypakuj do... Testuj Podejrzyj
MobaXterm_Portable_v24.2.zip - ZIP arc
Nazwa Rozmiar Skompreso...
CygUtils.plugin 18 172 936 18 063 144
CygUtils64.plugin 12 003 837 11 961 099
MobaXterm_Per... 16 987 560 11 895 750
192.168.1.4
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit
Quick connect...
2. /home/mobaxterm
3. 192.168.1.4
/home/kali/
Name
.cache
.config
.gnupg
.java
.local
Desktop
Documents
Downloads
Music
Pictures
Public
Follow terminal folder
Remote monitoring
• MobaXterm Personal Edition v24.2 •
(SSH client, X server and network tools)
▸ SSH session to kali@192.168.1.4
• Direct SSH : ✓
• SSH compression : ✓
• SSH-browser : ✓
• X11-forwarding : ✓ (remote display is forwarded through SSH)
▸ For more info, ctrl+click on help or visit our website.
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10
-09) x86_64
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jul 9 14:52:41 2024 from 192.168.1.3
(kali㉿kali)-[~]
$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

4.


20:56
linux
023
-10-09) x86_64
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jul 9 14:54:47 2024 from 192.168.1.3
(kali㉿kali)-[~]
$
***
{}
Ctrl

5.



Part 10: Apache Webserver

1.

sudo apt install apache2

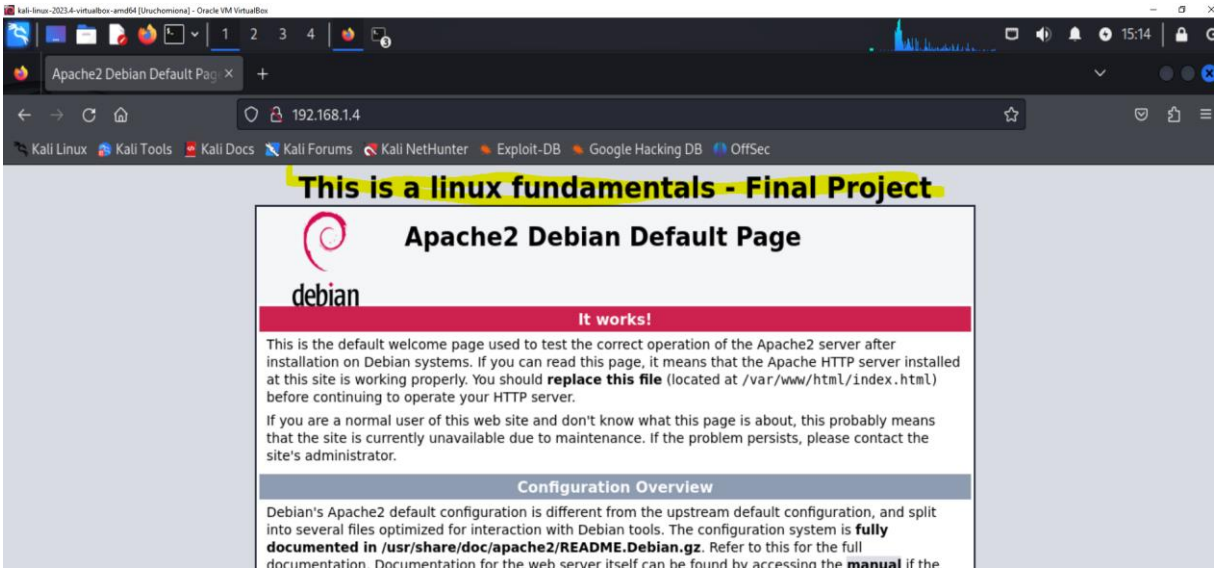
cd /var/www/html

┌──(root㉿kali)-[/var/www/html]

└─# ls

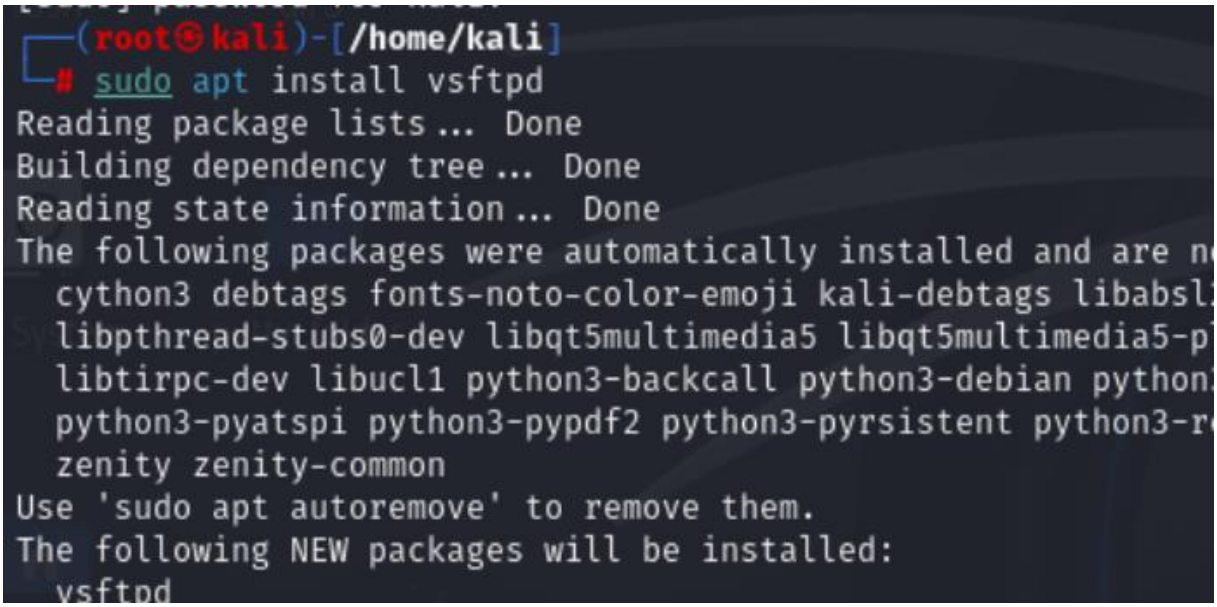
index.html index.nginx-debian.html

`sudo nano index.html`

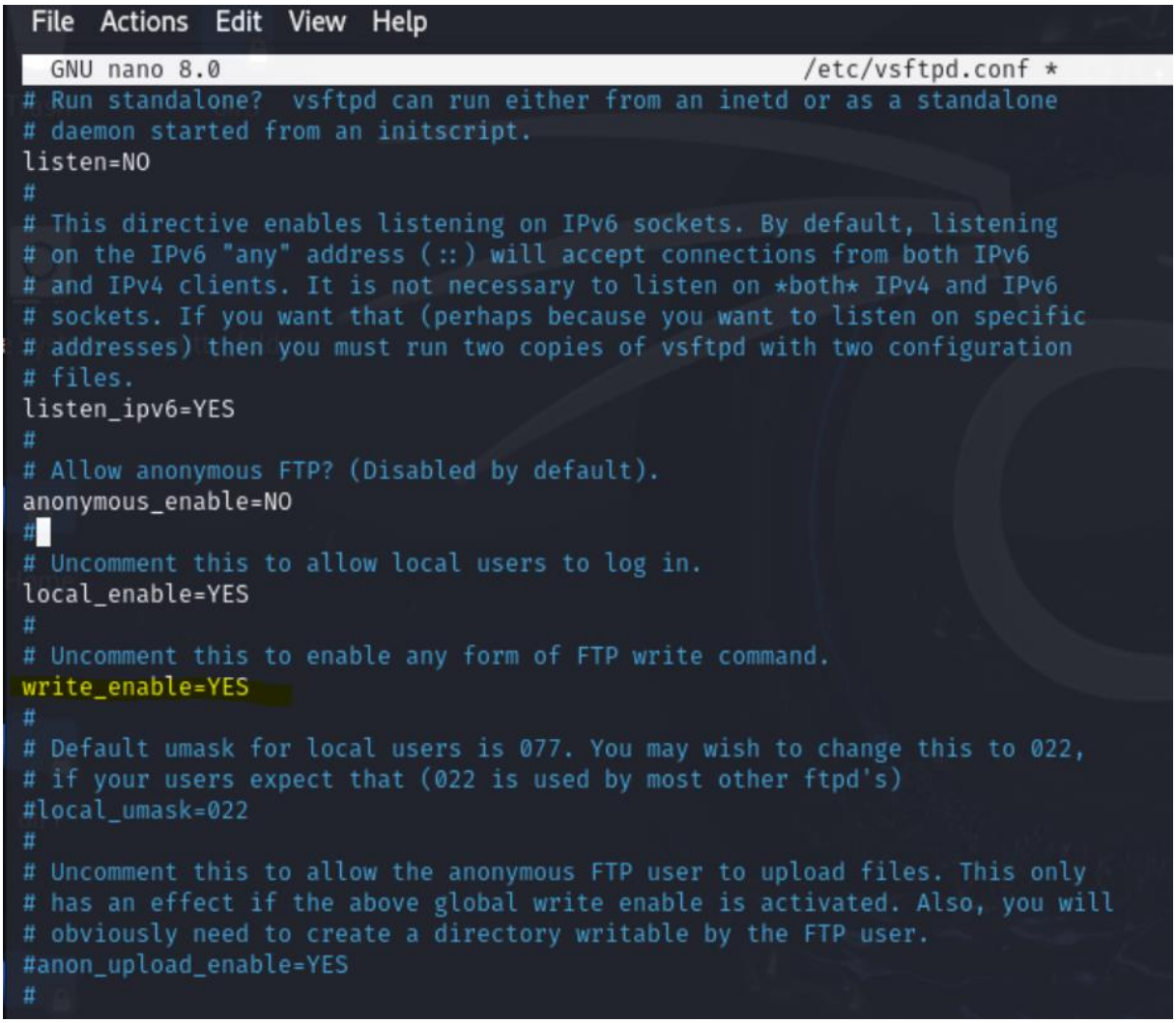


Part 11: VSFTPD

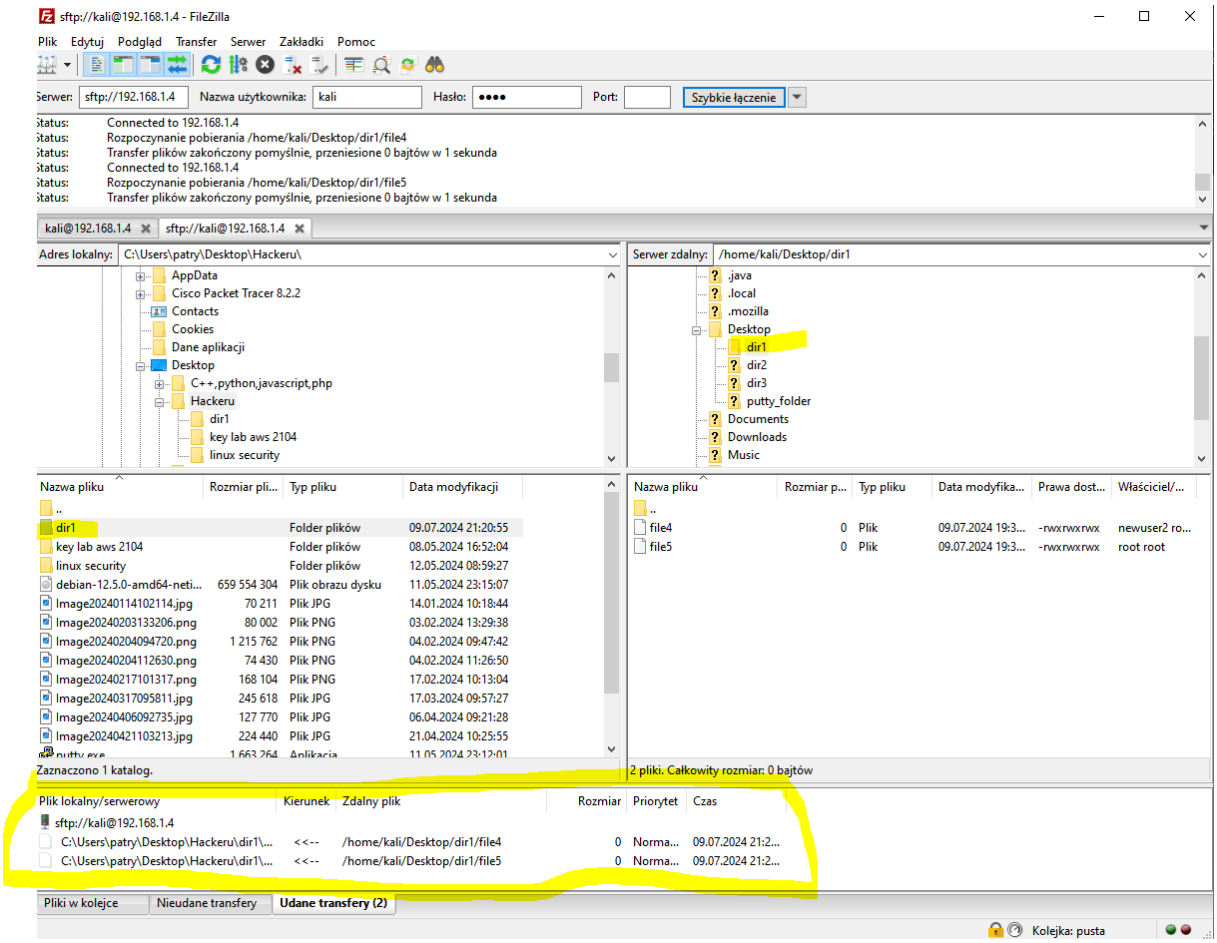
1.



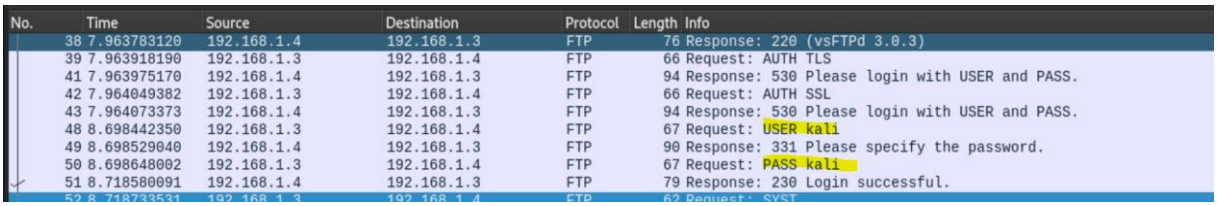
2.


File Actions Edit View Help
GNU nano 8.0 /etc/vsftpd.conf *
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# 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=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# 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
#

3.



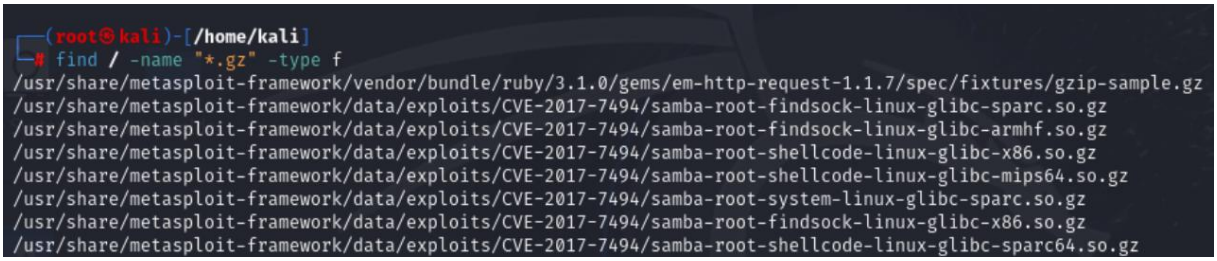
4.



Hasła są przesyłane w postaci tekstowej (plaintext) w czasie autoryzacji. Dzieje się tak dlatego, że FTP nie zapewnia domyślnie żadnego mechanizmu szyfrowania dla transmisji danych, w tym również dla danych uwierzytelniających

Part 12: Gzip

1.



2.

3.

Part 13: Questions

1.

/ (katalog główny): To podstawa hierarchii systemu plików w systemach Unixowych. Wszystko na systemie znajduje się pod tym katalogiem.

/bin (binaria): Zawiera podstawowe binarne pliki wykonywalne, niezbędne do podstawowego funkcjonowania systemu, takie jak ls, cp, rm, itp.

/etc (pliki konfiguracyjne): Przechowuje pliki konfiguracyjne systemowe potrzebne przez różne aplikacje i usługi działające na systemie, w tym konfiguracje sieciowe, skrypty startowe

2.

Encoding: Proces przekształcania danych z jednej formy do drugiej w celu transmisji, przechowywania lub szyfrowania. Zapewnia, że dane są poprawnie reprezentowane i przesyłane między różnymi systemami lub sieciami.

(Hashing) Proces przekształcania danych wejściowych (takich jak tekst lub pliki) w stałej długości ciąg znaków (wartość skrótu) za pomocą algorytmu matematycznego. Jest używane głównie do weryfikacji integralności danych i przechowywania haseł.

Symmetric encryption: Szyfrowanie, które używa jednego klucza zarówno do szyfrowania, jak i deszyfrowania danych. Nadawca i odbiorca używają tego samego klucza, co przyspiesza operacje, ale wymaga bezpiecznego rozprowadzenia klucza.

Asymmetric encryption: Szyfrowanie, które używa pary kluczy (publicznego i prywatnego) do operacji szyfrowania i deszyfrowania. Klucz publiczny jest używany do szyfrowania, a klucz

prywatny do deszyfrowania. Zapewnia bezpieczną wymianę kluczy bez konieczności bezpiecznego kanału do dystrybucji klucza.

3.

Why?

Podczas włączania SSH (Secure Shell), plik konfiguracyjny (sshd_config dla demona SSH) musi być zmieniony, aby ustawić różne parametry takie jak numer portu, dozwolonych użytkowników, metody uwierzytelniania, itp. Konfiguracja ta zapewnia, że SSH działa bezpiecznie i zgodnie z wymaganiami systemu.

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

Apache HTTP Server: Plik konfiguracyjny httpd.conf lub apache2.conf.

Nginx: Plik konfiguracyjny zwykle nazwany nginx.conf.

MySQL/MariaDB: Plik konfiguracyjny my.cnf do ustawień serwera bazy danych.

What is the usage of SSH?

Bezpieczny dostęp zdalny do systemów (zdalny dostęp do powłoki).

Bezpieczny transfer plików (SCP, SFTP).

Przekierowania portów i tunelowanie.

Is SSH encrypted?

Tak, SSH szyfruje całą komunikację między klientem a serwerem, w tym dane logowania i dane wymieniane podczas sesji.

4.

Kernel to główny komponent systemu operacyjnego zarządzający zasobami systemowymi (CPU, pamięć, urządzenia) i zapewniający podstawowe usługi dla wszystkich innych części systemu operacyjnego i aplikacji. Działa jako pośrednik między sprzętem a oprogramowaniem, umożliwiając komunikację i kontrolę nad zasobami systemowymi.

5.

Krok 1: Konfiguracja sieci

Upewnić się, że obie maszyny wirtualne są podłączone do tego samego sieci lub mogą się wzajemnie osiągnąć za pośrednictwem sieci (konfiguracja sieci mostkowej lub sieci wewnętrznej).

Krok 2: Uzyskanie adresów IP

Przypisać statyczne lub dynamiczne adresy IP do każdej maszyny wirtualnej, upewniając się, że znajdują się w tej samej podsieci.

Krok 3: Test ping

Użyć polecenia ping, aby sprawdzić łączność między maszynami wirtualnymi, wysyłając żądania ICMP echo i odbierając odpowiedzi ICMP echo.

Krok 4: Ustanowienie SSH (opcjonalnie)

Skonfigurować SSH na obu maszynach wirtualnych, jeśli wymagany jest bezpieczny dostęp do powłoki. Zaktualizuj pliki konfiguracyjne SSH (sshd_config dla serwera, ssh_config dla klienta), jeśli to konieczne.

6.

Ping jest narzędziem sieciowym używanym do testowania dostępności hosta w sieci protokołu Internet Protocol (IP). Wysyła pakiety żądania ICMP echo do docelowego hosta i oczekuje na pakiety odpowiedzi ICMP echo. Ping mierzy czas przebiegu (RTT) i utratę pakietów między źródłem a docelowym adresem.

7.

Trzy liczby (na przykład 777) reprezentują uprawnienia pliku w systemach Unixowych (Linux, Unix). Każda liczba odpowiada ustawieniom uprawnień dla właściciela pliku, członków grupy i innych (wszyscy inni użytkownicy) odpowiednio:

Pierwsza cyfra (właściciel): Uprawnienia dla właściciela pliku.

Druga cyfra (grupa): Uprawnienia dla użytkowników w grupie pliku.

Trzecia cyfra (inni): Uprawnienia dla wszystkich innych użytkowników.

Cyfry są zapisane w systemie ósemkowym (bazie 8), gdzie:

4: Uprawnienia do odczytu

2: Uprawnienia do zapisu

1: Uprawnienia do wykonania

Dodanie tych wartości daje ustawienie uprawnień:

7: Odczyt, zapis i wykonanie (4 + 2 + 1)

6: Odczyt i zapis (4 + 2)

5: Odczyt i wykonanie (4 + 1)

4: Tylko odczyt (4)

3: Zapis i wykonanie (2 + 1)

2: Tylko zapis (2)

1: Tylko wykonanie (1)

8.

W systemach plików obsługujących wielkość liter nazwy folderów są rozróżniane pod względem wielkości liter. Oznacza to, że możesz utworzyć dwa foldery o takiej samej nazwie, ale różniące się wielkością liter, np. folder i Folder są traktowane jako różne foldery.

9. telnet: Protokół komunikacyjny służący do zdalnego logowania się do hostów w sieci TCP/IP. Jest niezabezpieczony, ponieważ przesyła dane, w tym hasła, w formie tekstowej, co może prowadzić do przechwycenia danych przez nieautoryzowane osoby.

SSH (Secure Shell): Protokół sieciowy zapewniający bezpieczny dostęp do zdalnej powłoki lub przesyłania plików w sieci. SSH zapewnia szyfrowaną komunikację, co chroni poufne dane, takie jak hasła, podczas transmisji.

Crontab: W systemach Unixowych i pokrewnych, crontab to plik konfiguracyjny używany do harmonogramowania zadań systemowych. Określa on, kiedy i jakie polecenia mają być wykonywane automatycznie.

FTP (File Transfer Protocol): Protokół służący do transferu plików między komputerami w sieci TCP/IP. FTP jest nieszyfrowany, co oznacza, że dane mogą być przesyłane w postaci tekstowej, co stanowi potencjalne ryzyko bezpieczeństwa.

SFTP (SSH File Transfer Protocol): Rozszerzenie protokołu SSH, które zapewnia bezpieczny transfer plików i zarządzanie nimi w sieci. SFTP używa SSH do zapewnienia szyfrowanej komunikacji, chroniąc przesyłane dane.

gziptar: To nie jest standardowy termin, ale może odnosić się do zastosowania kompresji gzip w archiwizacji plików, często używanej z narzędziem tar do tworzenia skompresowanych archiwów.

bash: Bash (Bourne Again Shell) to popularna powłoka (interpreter poleceń) w systemach Unixowych i pokrewnych. Jest to główny interfejs tekstowy umożliwiający interakcję z systemem operacyjnym za pomocą poleceń.

Apache: Apache jest popularnym serwerem HTTP używanym do hostowania stron internetowych. Obsługuje protokoły HTTP i HTTPS oraz wspiera skrypty CGI oraz różne dodatki dla dynamicznych stron internetowych.