

2.1 Introduction Linux (1991)

Presenter: H.O.

An Operating System (OS)	• Just like Windows, iOS, and macOS
Operating System?	• Software that manages all of the hardware resources associated with your desktop or laptop.
Zero Cost of Entry	• ... as in free. Install Linux without paying a penny for software or server licensing.
Open Source Software	• is code that is designed to be publicly accessible—anyone can see, modify, and distribute the code.

Linux Distributions (distros)



Linux Katmanları

- Bootloader** : Bilgisayar başlattığında ilk çalışan sistem
- Kernel** : OS Çekirdeği (en temel sistem ihtiyaçları)
CPU;memory, çevresel cihazlar
- Init System** : Kullanıcı başlangıç ayarları
- Deamons** : Arka tarafta çalışan servisler (Yazıcı, ses ve takvim vb.)
- Graphical server** : Görünür grafik ara yüzü
- Desktop environment:** Kullanıcı etkileşimli görsel kısım
- Applications** : Uygulamalar

Bootloader	• Manages boot process
Kernel	• The core of the system and manages the CPU, memory, and peripheral devices
Init system	• A sub-system that bootstraps the user space and is charged with controlling daemons
Daemons	• Background services such as printing, sound, scheduling
Graphical server	• The sub-system that displays the graphics on your monitor
Desktop environment	• The piece that the users actually interact with
Applications	• All other apps you use

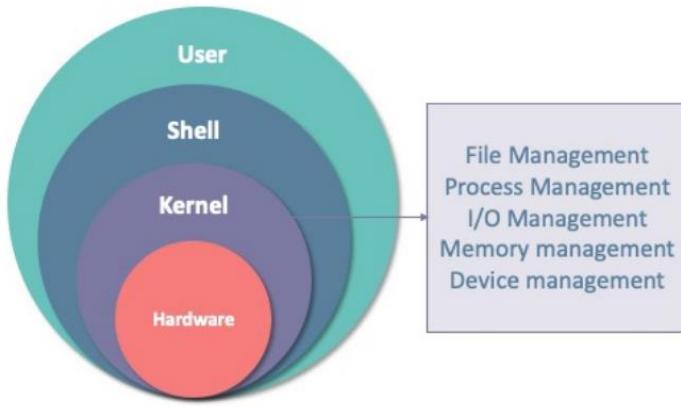
Shell:

Linux Komut çalıştırıp işlem yaptırdığımız ara yüz. User ile Kernel arasındaki ekilesimi mümkün kılar. Özellikle Sistemin diğer serverleri sorun yaşandığında buradan istenen her işlem yapılabilir. Sistemi kurtarabiliz.

A user interface for access to the operating system's services.

Command Line Interfaces (CLI) - Graphical User Interface (GUI)

Some Linux Shells: Tcsh, Zsh, Ksh, Bash (Bourne-Again Shell)



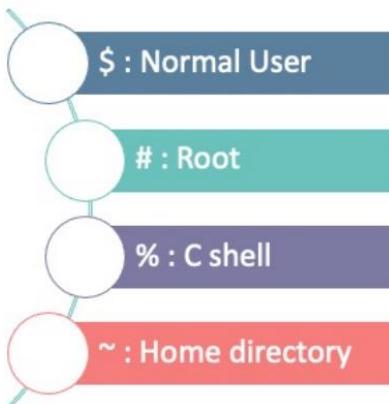
```
File Actions Edit View Help
kali@kali: ~
$ ls -al
total 960
drwxr-xr-x 22 kali kali 4096 Dec 24 05:37 .
drwxr-xr-x  4 root root 4096 Dec 18 07:07 ..
drwxr-x---  2 kali kali 4096 Dec 18 08:13 .android
-rw-r--r--  1 kali kali 1 Nov 17 09:46 .bash_history
-rw-r--r--  1 kali kali 220 Nov 17 09:06 .bash_logout
-rw-r--r--  1 kali kali 4583 Nov 17 09:06 .bashrc
-rw-r--r--  1 kali kali 3526 Nov 17 09:06 .bashrc.original
drwx----- 4 kali kali 4096 Dec 18 07:23 .browsersuite
drwxr-Xr-X  9 kali kali 4096 Dec 24 05:37 .cache
drwx----- 14 kali kali 4096 Dec 18 08:26 .config
drwxr-Xr-X  2 kali kali 4096 Nov 17 09:14 Desktop
-rw-r--r--  1 kali kali 53 Nov 17 09:39 .dmrc
drwxr-Xr-X  2 kali kali 4096 Nov 17 09:14 Documents
drwxr-Xr-X  2 kali kali 4096 Nov 17 09:14 Downloads
drwxr--r--  1 kali kali 11759 Nov 17 09:14 .face
```



Bazı Shell notasyonları

Shell komut satırında terminali açan kullanıcı bilgisi ve bulunulan dizin bilgileri ve aşağıda anlamları belirtilen notasyonlar yer alır.

- # En yetkili kullanıcı
- \$ Normal kullanıcı
- % Shell tiplerinden biri olan C Shell (MacOS'ta kullanılır)
- ~ Home directory
- / Kök dizini



```

File Actions Edit View Help
(kali㉿kali)-[~]
$ whoami
kali
(kali㉿kali)-[~]

File Actions Edit View Help
(root㉿kali)-[~]
# whoami
root
(root㉿kali)-[~]

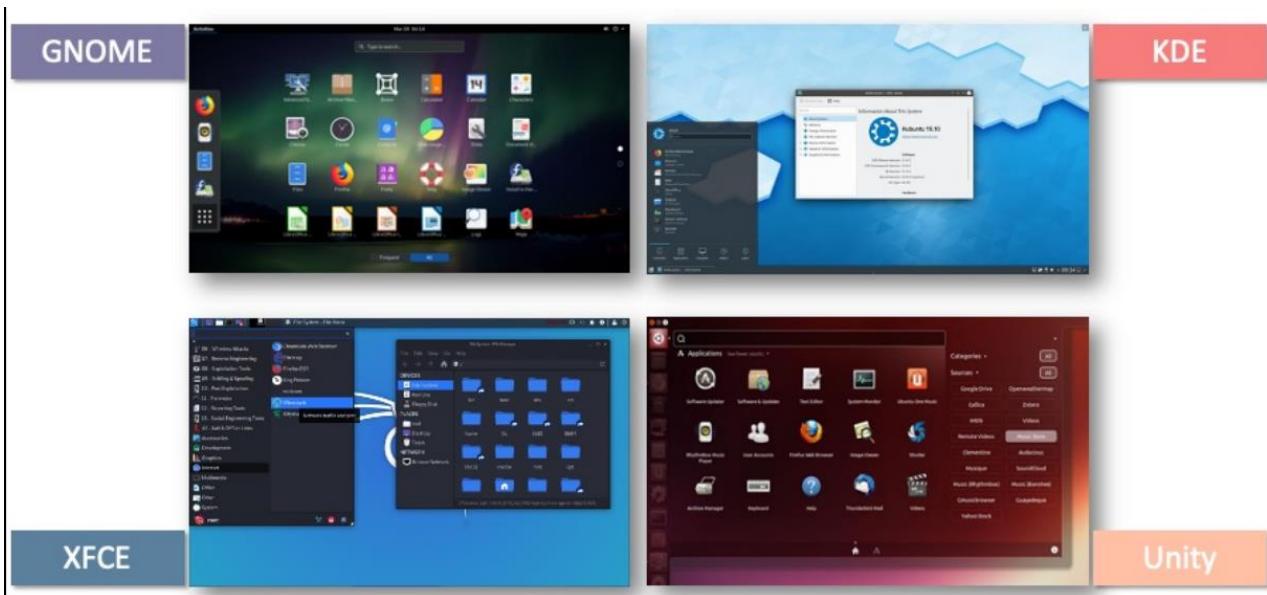
File Actions Edit View Help
(kali㉿kali)-[~]
$ pwd
/home/kali
(kali㉿kali)-[~]

```

Desktop Ara Yüzleri

Genel olarak görünüm farkı

Xfce Grafik ara yüzü daha etkin Kali kurulumunda default olarak gelen XFCE'yi seçmiştık.



2.2 / 2.3 Linux Komutları

Try hack me üzerinden sanal Linux başlatalım.

Bir Terminal ekranı açalım (Üst sekmeden terminal sekmesine basarak açmalıyız. Masaüstü sağ tıklarsan masaüstü directory'de açacağı için her komuta çalışmaz.)

Not: TRY hack me makine bilgileri: (bazen web sayfasından üstte sergilenmediği durumlarda)
<https://tryhackme.com/my-machine>

Kök dizin, bilgisayar dosya sistemlerinde en üstteki dizindir. Bazen ana dizin veya giriş dizini olarak da adlandırılır. Başka birçok dizin veya alt dizin içerebilir.

Home dizin ise kullanıcının ilk dizinidir.

Menu Komutları (Menu Commands)

Ctrl+a	komut satırı başına git
Ctrl+c	ekranı sil (^C)
Ctrl+z	çalışan programı durdur
Ctrl+e	komut satırı sonuna git
Ctrl+q	ekrandan çıkış
ctrl +u	kürsörün olduğu komut satırındaki her şeyi siler
ctrl _l	ekran temizleme
clear	ekran temizleme
tab	muhtemel kodları/parametreleri tamamlar

Dosya sistemleri ile etkileşim komutları (Commands to interact with the Filesystem)

Command	Full Name
ls	listing
cd	change directory
cat	concatenate
pwd	print working directory

#ls : listelemek ve özelliklerini görme

```
root@kali:~# ls
boot.ini    Downloads      KdNfeany.jpeg      Pictures      TheFatRat
csrf.html   eIaLalPY.jpeg  Music           Public        Veil
Desktop     Empire         MyPrettyBD.exe    r57shell.php  Videos
Documents   ipList.txt    owasp_zap_root_ca.cer Templates    yersinia.log
```

-a, --all	• do not ignore entries starting with .
-l	• use a long listing format
-h, --human-readable	• with -l and/or -s, print human readable sizes (e.g., 1K 234M 2G)
-s, --size	• print the allocated size of each file, in blocks
-S	• sort by file size, largest first
-t	• sort by modification time, newest first

ls → mevcut (içinde bulunan) dizinindeki dosyaların isimlerini yan yana sergiler.

ls folder4 → belirtilen dosyanın içindeki dosyaların isimlerini sergiler

```
tryhackme@linux1:~$ ls
access.log  folder1  folder2  folder3  folder4
tryhackme@linux1:~$ ls folder4
note.txt
```

Help parametresi ile komuta ilave olası parametreler sergilenebilir

Ana komut -- help veya **ana komut -h**

-h bazı komutlarda kullanılan parametre olduğu için **ana komut -h** komutunda help menüsü gelmeyebilir

ls --help → ls komutu ile ilgili ilave parametreler sergilenebilir.

Man ls -I → ls help benzeri
“Man” manuel sayfalar

```
root@kali:~# ls --help
Usage: ls [OPTION]... [FILE]...
List information about the FILES (the current directory by default).
Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.

Mandatory arguments to long options are mandatory for short options too.
-a, --all          do not ignore entries starting with .
-A, --almost-all   do not list implied . and ..
--author          with -l, print the author of each file
-b, --escape        print C-style escapes for nongraphic characters
--block-size=SIZE   scale sizes by SIZE before printing them; e.g.,
                   '--block-size=M' prints sizes in units of
                   1,048,576 bytes; see SIZE format below
```

```
root@kali:~# ls -al /usr/bin/
total 559540
drwxr-xr-x  2 root root    110592 Feb 13 15:16 .
drwxr-xr-x 14 root root     4096 Jan  2 10:06 ..
-rw-r--r--  1 root root    51936 Oct  2 2017 '[I'
-rw-r--r--  1 root root    2376 Aug 10 2013 otrace.sh
```

```
root@ip-10-10-235-11:~#
File Edit View Search Terminal Help
root@ip-10-10-235-11:~# ls al
ls: cannot access 'al': No such file or directory
root@ip-10-10-235-11:~# ls -al
total 792
drwxr-xr-x 39 root root 4096 Nov 12 17:30 .
drwxr-xr-x 23 root root 4096 Nov 12 17:30 ..
drwxr-xr-x  3 root root 4096 Aug 23 09:51 .aspnet
-rw-r--r--  1 root root 326 Mar 18 2021 .bash_aliases
lrwxrwxrwx  1 root root  9 Aug 16 2020 .bash_history -> /dev/null
-rw-r--r--  1 root root 3190 Sep 10 2020 .bashrc
drwxr-xr-x  3 root root 4096 Sep  1 2020 .bundle
drwx-----  4 root root 4096 Sep 10 15:37 .BurpSuite
drwx----- 18 root root 4096 Nov 12 17:31 .cache
drwx----- 24 root root 4096 Sep 10 15:38 .config
```

ls -alh → çalışan her şeyi liste halinde okunabilir sergilenebilir

ls komut; a, l ve h parametredir.

ls list information files
-a all
-l liste
-h human readable formatta

(veri büyüklüğü byte'dan kbyte'a cevirdi)

-f → file type ("/" dizin, exe, "@" link veya "bos" metin dosyası)

```
root@ip-10-10-235-11:~#
File Edit View Search Terminal Help
-rw-r--r--  1 root root 240 Sep  1 2020 .profile
-rw-------  1 root root 57 Mar 18 2021 .python_history
drwxr-xr-x  3 root root 4.0K Oct 29 11:50 Rooms
drwxr-xr-x  2 root root 4.0K Aug 17 2020 .rpmbuild
drwxr-xr-x  2 root root 4.0K Oct 29 12:02 Scripts
-rw-r--r--  1 root root 74 Aug 15 2020 .selected_editor
drwxr-xr-x  2 root root 4.0K Feb 22 2021 .set
drwx-----  2 root root 4.0K Mar 18 2021 .ssh
```

ls -alt → çalışan her şeyi liste halinde zaman sıralı (yeniden eskiye doğru) sergilenebilir

t zaman sıralı (yeniden eskiye)

Dikkat edilecek olursa son 3 ay ayrıntılı saatli sergilenebilir

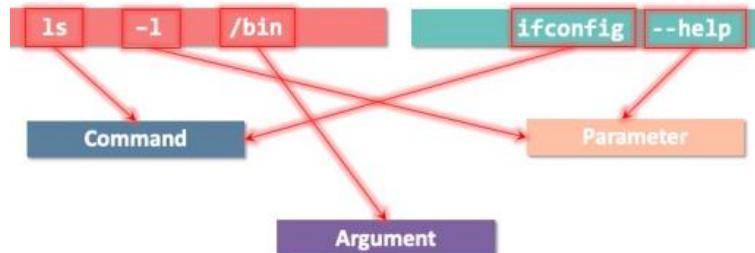
ls -l /root/desktop → Masa üstündekileri listeler

```
root@ip-10-10-235-11:~#
File Edit View Search Terminal Help
GNU coreutils online help: <http://www.gnu.org/software/coreutils/>
Full documentation at: <http://www.gnu.org/software/coreutils/ls>
or available locally via: info '(coreutils) ls invocation'
root@ip-10-10-235-11:~# root@ip-10-10-235-11:~# ls -alt
total 792
-rw-----  1 root root 507617 Nov 12 17:31 .xsession-errors
drwx----- 18 root root 4096 Nov 12 17:31 .cache
drwxr-xr-x 39 root root 4096 Nov 12 17:30 .
-rw-----  1 root root 44136 Nov 12 17:30 .ICEauthority
drwxr-xr-x  2 root root 4096 Nov 12 17:30 .vnc
-rw-----  1 root root 4753 Nov 12 17:30 .Xauthority
drwxr-xr-x 23 root root 4096 Nov 12 17:30 ..
drwxr-xr-x  2 root root 4096 Oct 29 12:02 Scripts
drwxr-xr-x  3 root root 4096 Oct 29 11:50 Rooms
-rw-r--r--  1 root root 439 Sep 15 10:02 .wget-hsts
-rw-rw-r--  1 root root 111 Sep 10 15:42 .install4j
drwx----- 24 root root 4096 Sep 10 15:38 .config
drwx-----  4 root root 4096 Sep 10 15:37 .BurpSuite
drwxr-xr-x  3 root root 4096 Aug 23 09:51 .aspnet
drwxr-xr-x  6 root root 4096 Aug 23 09:50 .dotnet
drwxr-xr-x  4 root root 4096 Aug 23 09:50 .nuget
drwx-----  2 root root 4096 Mar 18 2021 .ssh
drwxr-xr-x  7 root root 4096 Mar 18 2021 Pictures
```

ls komut

a, l ve h parametre

/root/Desktop argümandır.



Not: “*” (yıldız) her şeyi ifade eder.

ls -l /root/Desktop/* → /root/Desktop dizinindeki her şeyi listeler.

```

root@ip-10-10-163-87:~# ls -l /root/Desktop/*
lrwxrwxrwx 1 root root 5 Sep 10 2020 '/root/Desktop/Additional Tools' -> /opt/
-rw-r--r-- 1 root root 173 Aug 15 2020 /root/Desktop/mozo-made-15.desktop
  
```

ls -ls → dosayı listeler ve basta kapasite yuvarlaması yaparak sergiler

s size (büyükten küçüğe)

```

root@ip-10-10-235-11:~# ls -ls
total 32
4 drwxr-xr-x 3 root root 4096 Dec 29 2020 Desktop
4 drwxr-xr-x 2 root root 4096 Sep 10 2020 Downloads
4 drwxr-xr-x 2 root root 4096 Oct 30 2020 Instructions
4 drwxr-xr-x 2 root root 4096 Mar 18 2021 Pictures
4 drwxr-xr-x 3 root root 4096 Aug 16 2020 Postman
4 drwxr-xr-x 2 root root 4096 Oct 29 11:50 Rooms
4 drwxr-xr-x 2 root root 4096 Oct 29 12:02 Scripts
4 drwxr-xr-t 2 root root 4096 Aug 13 2020 thinclient_drives
6 lrwxrwxrwx 1 root root 19 Mar 18 2021 Tools -> /root/Desktop/Tools
root@ip-10-10-235-11:~#
  
```

```

root@ip-10-10-235-11:~# ls -ls
total 32
drwxr-xr-x 3 root root 4096 Dec 29 2020 Desktop
drwxr-xr-x 2 root root 4096 Sep 10 2020 Downloads
drwxr-xr-x 2 root root 4096 Oct 30 2020 Instructions
drwxr-xr-x 2 root root 4096 Mar 18 2021 Pictures
drwxr-xr-x 3 root root 4096 Aug 16 2020 Postman
drwxr-xr-x 3 root root 4096 Oct 29 11:50 Rooms
drwxr-xr-x 2 root root 4096 Oct 29 12:02 Scripts
drwxr-xr-t 2 root root 4096 Aug 13 2020 thinclient_drives
lrwxrwxrwx 1 root root 19 Mar 18 2021 Tools -> /root/Desktop/Tools
root@ip-10-10-235-11:~#
  
```

ls -IS → listesi küçükten büyüğe sıralar
“r” reverse order (ters sıralı)

ls -R → dizindeki ve altındaki dosyaların da içindeleri listeler (recursive) (büyük harf)
“R” recursive

ls -IS →
S (büyükten küçüğe)
Bas tarafta Kb yuvarlaması yok

```

root@ip-10-10-235-11:~# ls -lSr
total 32
lrwxrwxrwx 1 root root 19 Mar 18 2021 Tools -> /root/Desktop/Tools
drwxr-xr-t 2 root root 4096 Aug 13 2020 thinclient_drives
drwxr-xr-x 2 root root 4096 Oct 29 12:02 Scripts
drwxr-xr-x 3 root root 4096 Oct 29 11:50 Rooms
drwxr-xr-x 3 root root 4096 Aug 16 2020 Postman
drwxr-xr-x 2 root root 4096 Mar 18 2021 Pictures
drwxr-xr-x 2 root root 4096 Oct 30 2020 Instructions
drwxr-xr-x 2 root root 4096 Sep 10 2020 Downloads
drwxr-xr-x 3 root root 4096 Dec 29 2020 Desktop
root@ip-10-10-235-11:~#
  
```

ls -s rgb.txt → bulunulan dizinde belirtilen dosyanın boyutunu görebiliriz.

```

root@ip-10-10-163-87:/etc/X11# ls -s rgb.txt
20 rgb.txt
  
```

#cd : change directory

“cd” (change directory) diziniyle gidilen dosyayı mouse ile windows’ta açtığımız tam sayfa gibi düşünelim. Windows’ta açılan menüde/sayfada mouse ile işlem nasıl işlem yapabiliyorsak terminalde de komutlarla bulunulan dizinde işlem yapabilir.

```
root@kali:/usr/share/nmap/scripts# cd ..
root@kali:/usr/share/nmap#
root@kali:/usr/share/nmap# cd
root@kali:~# pwd
/root
root@kali:~# cd ./TheFatRat/tools/
root@kali:~/TheFatRat/tools#
root@kali:~/TheFatRat/tools# cd -
/root
```

cd → home dizine geri gelinir.

cd / → kök dizinine gider
(sisteme en yetkili kullanıcı)

cd Desktop → Desktop (Dikkat “D” harfi büyük)dizinine gider (o menüye erişilmiş olur)

cd tools → tools dizinine gider (o menüye erişilmiş olur)

cd	• Abbreviation of Change Directory.
..	• The symbol for upper folder;
.	• The symbol of current folder.
cd ..	• Moves us previous folder.
cd w/o parameter	• Moves to “home” folder of current user.
cd ~user	• Moves to home of named user.
cd -	• Moves to previous position.

ls -l → bulunulan dizini içeriğini listeler.

```
root@ip-10-10-163-87:~# cd Tools
root@ip-10-10-163-87:~/Tools# ls
Binex           Miscellaneous          'Password Attacks'    Steganography   wordlists
C2              mozo-made-20.desktop    PEAS                  Web
Decompilers     mozo-made-21.desktop    'Static Binaries'  Wireless
```

cd .. → bir üst dizine çıkar (c:/users/desktop’tan c:/users’ya gelir)

cd ../../ → iki üst dizine çıkar (c:/users/desktop’tan c: dizinine gelir)

DIKKAT: home (kök) dizininde de üste çıkışlırsa boşluğa gidilmiş olur. Bu durumda örneğin “cd desktop” komutu çalışmaz, çünkü kökü kaybettik.

cd /root/Desktop/ → belirtilen dizine gider (bas ve sondaki slash “/” işaretine dikkat)

cd ./bin → Halihazırda bulunulan dizin içinde varsa bin dizinine erişir
./dizin adı nokta bulunduğuımız dizini ifade eder.

cd - → bir önce bulunduğuımız dizine (bir üst dizine geri gelme değil) gider.

Pwd → Print working directory
Halihazırda bulunduğuum dizini sergiler

```
root@ip-10-10-163-87:~/Tools# cd Miscellaneous/
root@ip-10-10-163-87:~/Tools/Miscellaneous# pwd
/root/Tools/Miscellaneous
```

#cat İstenen dosyanın içeriğini sergilemek

“Concatenates” files and print on the standard output

Generally speaking, it is used to see the content of a text file

```
root@kali:~# cat myTextFile
Line 1
Line 2
Line 3
```

```
root@kali:~# cat >myTextFile
Brand New File
^C
root@kali:~# cat myTextFile
Brand New File
```

```
root@kali:~# cat >>myTextFile
The New Line
^C
root@kali:~# cat myTextFile
Line 1
Line 2
Line 3
The New Line
```

```
root@kali:~# cat myTextFile2
The Second Text File
root@kali:~# cat myTextFile myTextFile2
Brand New File
The Second Text File
```

touch mehmet.txt → bulunulan dizinde mehmet.txt adlı dosya oluşturduk.

DIKKAT: Touch yeni bir dizin oluşturmaz, dosya oluşturur.

Dosyaya “merhaba” ve “nasılsın” yazıp kaydettik.

cat mehmet.txt → dosyaya erişip içeriğini sergiler

```
/root
root@ip-10-10-235-11:~# touch mehmet.txt
root@ip-10-10-235-11:~# cat mehmet.txt
merhaba
nasılsın
```

cat *.txt → dizindeki tüm txt'lerin içeriğini sergiler.

```
root@ip-10-10-163-87:~# ls
Desktop  hackeracademy  new.txt  Postman  Scripts  thinclient drives  yeni.txt
Downloads  Instructions  Pictures  Rooms  selam  Tools
root@ip-10-10-163-87:~# cat *.txt
merhaba
ben huriye
nasilsiniz?
bu da yeni bir dosya
```

#echo

Displays a line of text

You can print environment variables using '\$' at the beginning.

```
root@kali:~# echo PATH  
PATH  
root@kali:~# echo $PATH  
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin  
root@kali:~# cat myTextFile  
My Text File  
root@kali:~# echo "A New Line" >>myTextFile  
root@kali:~# cat myTextFile  
My Text File  
A New Line  
root@kali:~# echo "A New File" >myTextFile  
root@kali:~# cat myTextFile  
A New File
```

Echo Hello World → Echo sonrası yazılan metin Ekrana yazılır. (Amacını sonra öğreneceğiz)

echo \$????? → Sistem içindeki bazı ortam değişkenlerinin değerini ekrana getirir.

Echo \$shell → kullandığımız shell'in değeri.

Echo home → kullanıcının home dizini sergiler.
(burada root)

echo \$Path → değişkenin değerini gösterir.

```
root@ip-10-10-217-110:~# echo Hello world  
Hello world  
root@ip-10-10-217-110:~# echo $SHELL  
/bin/bash  
root@ip-10-10-217-110:~# echo $HOME  
/root  
root@ip-10-10-217-110:~# echo $PATH  
/usr/bin:/bin:/sbin:/usr/local/bin:/usr/sbin
```

PATH Ortam değişkeni

Normalde içinde olduğunuz dizindeki dosyaları kullanamayız, çünkü erişemeyiz. **Path** değer olarak komutların dizininin olduğu dizin konumunu tutar. Bu değere karşılık gelen dizindeki dosyalar halihazırda kullandığımız komutların çalıştığı dosyalardır. Bu değişken sayesinde bulduğumuz her dizinde komutları çalıştırabiliyoruz. Halbuki komutları çalıştıran dosyalar başka dizinde ve çalışmamalıydı.

PATH işletim sisteminizin komut satırından veya Terminal penceresinden gerekli çalıştırılabilir dosyaların yerini belirlemek için kullandığı sistem değişkenidir. PATH sistem değişkeni Windows'da denetim masasındaki Sistem Yardımcı Programı kullanılarak, Linux ve Solaris'te ise kabuk başlangıç dosyanızdan ayarlanabilir.

Konsoldan girilen bir komutu çalıştırılmam için sırasıyla bazı dizinlere bakmak gereklidir. Eğer verilen komutun çalıştırılabilir dosyası bu dizinlerin altındaysa çalıştırır. Yani yola (PATH) ekliye çalıştırırı, yoksa çalıştırılmam. Yukarıda görülen ve birbirine ":" (iki nokta üst üste) işaretiley ayrılmış ifadelerin oluşturduğu yapıya yol (PATH) ortam değişkeni denir.

Konsol ekranı, bir komut çalıştırıldığı zaman komutu bulabilmek için bu dizinleri (path'de kayıtlı) tarar ve yazmış olduğunuz komutun bulunduğu dizini çalıştırır. Bu sayede işlerinizi konsol ekranı üzerinden yapabilirsiniz.

Tanım: Ortam değişkenleri, işletim sistemi ortamı hakkında bilgi depolar. Bu bilgiler, işletim sistemi yolu, işletim sistemi tarafından kullanılan işlemci sayısı ve geçici klasörlerin konumu gibi ayrıntıları içerir. **Ortam değişkenleri**, sistem genelinde mevcut olan ve ortaya çıkan tüm alt süreçler ve kabuklar tarafından miras alınan değişkenlerdir. (windows'ra windir, Linux'ta Path)

Kabuk değişkenleri, yalnızca geçerli kabuk örneği için geçerli olan değişkenlerdir. "zsh" ve "bash" gibi her kabuğun kendi iç kabuk değişkenleri kümesi vardır.

Linux'ta ortam değişkenlerini listelemenize ve ayarlamانıza izin veren birkaç komut vardır:

#printenv

Ortam değişkenlerini görüntülemek için en çok kullanılan komut **printenv**. Değişkenin adı komuta bağımsız değişken olarak iletilirse, yalnızca bu değişkenin değeri görüntülenir. Herhangi bir bağımsız değişken belirtilmemezse, **printenv** her satırda bir değişken olan tüm ortam değişkenlerinin listesini yazdırır.

Not: Terminal'in **File** menüsünden → “**New Tab from Preset**” alt alta veya yan yana birden fazla terminal ekranı açılabilir.

Echo \$Path → Sadece bin dizininin yolu tanımlı, Sadece buradaki komutları terminalden çalıştırılabiliriz.

cd bin → bin dosyasına girdik

ls -l → sistem için gerekli dosyalar **detailed**

ls → sistem için gerekli dosyalar **daha sade** terminalde sergilenebilir.

ls sbin → ifconfig ve password bilgileri (cripto) vb önemli ve yetkili kullanıcılar hariç diğer kullanıcıların kullanamayacağı dosyalar bu dizinde yer alır.

bin dizininde iken

ifconfig → komut çalışmıyor

```
root@kali:~# echo $PATH  
/usr/bin:/bin  
root@kali:~# ifconfig  
bash: ifconfig: command not found
```

çünkü bu komut dosyası bu dizinde yok ve path ortam değişkeninde tanımlı değil

sbin dizininde iken de

ifconfig → komut çalışmıyor.

./ifconfig → şimdi çalıştı, çünkü bulunan dizindeki ilgili komutu çalıştırmak için başında “.” (nokta) ile dizin yolunu belirtmeliyiz.

```
root@kali:/sbin# ifconfig  
bash: ifconfig: command not found  
root@kali:/sbin# ./ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001  
      inet 10.10.113.44 netmask 255.255.0.0 broadcast 10.10.255.255  
      inet6 fe80::22:96ff:fe90:ec1b prefixlen 64 scopeid 0x20<link>  
        ether 02:22:96:90:ec:1b txqueuelen 1000 (Ethernet)  
          RX packets 49664 bytes 3302619 (3.1 MiB)  
          RX errors 0 dropped 0 overruns 0 frame 0  
          TX packets 42119 bytes 216250700 (206.2 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 97007 bytes 218807066 (208.6 MiB)  
          RX errors 0 dropped 0 overruns 0 frame 0  
          TX packets 97007 bytes 218807066 (208.6 MiB)  
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

/sbin dizinin yolunu da Path komutuna eklemeliyiz ki o dizindeki dosyaları o dizin yolunu göstermeden çalıştırabilelim.

export PATH=\$PATH:/sbin → Var olan Path komutunda /sbin dizinini de eklemiş olduk.

veya

export PATH = /usr/bin:/bin:/sbin

ifconfig → görüldüğü gibi artık bu komut çalışmaktadır.

Her terminal için bu ayarı yapmak gerekebilir.

```
root@kali:~# echo $PATH
/usr/bin:/bin
root@kali:~# ifconfig
bash: ifconfig: command not found
root@kali:~# export PATH=$PATH:/sbin
root@kali:~# echo $PATH
/usr/bin:/bin:/sbin
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
      inet 10.10.113.44 netmask 255.255.0.0 broadcast 10.10.255.255
      ether 02:22:96:90:ec:1b txqueuelen 1000 (Ethernet)
      RX packets 68265 bytes 4576050 (4.3 MiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 59489 bytes 232221416 (221.4 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 139345 bytes 235986426 (225.0 MiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 139345 bytes 235986426 (225.0 MiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

su - → (SUPER USER) bu komutu sonrasında bu tarz global komutları her terminalde kullanabiliriz.

ifconfig → görüldüğü gibi artık bu komut çalışmaktadır.

Her terminal için bu ve benzeri ayarı yapmak artık gerekmeyez.

Bu komutla (**su -**) Path ortam değişkeninde gerekli değişiklikler otomatik yapılmış olur

export \$PATH → sorgulamada Path  değişkeninde değişikliği gördük.

```
root@kali:~# su -
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
      inet 10.10.113.44 netmask 255.255.0.0 broadcast 10.10.255.255
      ether 02:22:96:90:ec:1b txqueuelen 1000 (Ethernet)
      RX packets 83000 bytes 5558668 (5.3 MiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 71963 bytes 273916031 (261.2 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 169531 bytes 278535663 (265.6 MiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 169531 bytes 278535663 (265.6 MiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
root@kali:~#
```

Path değişkenini ilk haline geri döndürmek istersek;

export PATH = /usr/bin:/bin → bu komutla Path değişkeni girilen değeri alır. Yani burada ilk haline geri döner.

export PATH=`echo \$PATH | tr ":" "\n" | grep -v "çıkarılmak istenen dizin adı" | tr "\n" ":"` → bu kodla da istenen dizi PATH'dan çıkarılıyor ancak fazladan : (iki nokta üst üste) PATH değerinde kalıyor.

Path değişkenine birden fazla dizin eklemek istersek;

Export PATH =\$PATH:/sbin:/root/Desktop:/etc/ → bu komutla Path değişkeni değerine belirtilen dizinler eklenir.

```
root@kali:~/Desktop# export PATH=$PATH:/sbin:/root/Desktop:/etc/
root@kali:~/Desktop# echo $PATH
/usr/bin:/sbin:/root/Desktop:/etc/
```

#more

Dosyaları aşama aşama görmek istediğimizde kullanılır. Büyük dosyalarda kullanışlı bir komut

The screenshot shows a terminal window with a legend for the 'more' command keys:

more <fileName>	• to see the outputs which are bigger than one page.
<enter> or <space>	• to next page.
+123	• to go 123 lines more.
q	• to exit.

The terminal content is a log file named 'yersinia.log' showing network interface activity and logon attempts. A red box highlights the status bar at the bottom of the terminal window, which says '-More-- (7%)'.

cat /var/log/auth.log → görüldüğü gibi ekran gelen dosya çok büyük.

more /var/log/auth.log → dosyanın belli bir kısmını ekran getirdi ve dosyanın yüzde olarak neresinde olduğunu (burada %39) sergiler ve her enter'a basıldığında daha fazla satır ekrana getirir, yani ilerler. Sergileme yüzdesi terminal ekranının en altında görülebilir.

The screenshot shows a terminal window titled 'Shell No.2' displaying a large log file. The status bar at the bottom indicates '-More--(39%)'. The log file contains numerous entries from the system's authentication logs, including many failed password attempts from user 'pi'.

```
Nov 15 17:03:56 kali CRON[760]: pam_unix(cron:session): session closed for user root
Nov 15 17:03:59 kali CRON[761]: pam_unix(cron:session): session closed for user root
Nov 15 17:05:01 kali CRON[1254]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 15 17:05:01 kali CRON[1254]: pam_unix(cron:session): session closed for user root
Nov 15 17:05:15 kali sshd[1258]: rexec line 7: Deprecated option UsePrivilegeSeparation
Nov 15 17:05:15 kali sshd[1258]: rexec line 8: Deprecated option KeyRegenerationInterval
Nov 15 17:05:15 kali sshd[1258]: rexec line 9: Deprecated option ServerKeyBits
Nov 15 17:05:15 kali sshd[1258]: rexec line 14: Deprecated option RSAAuthentication
Nov 15 17:05:15 kali sshd[1258]: rexec line 17: Deprecated option RhostsRSAAuthentication
Nov 15 17:05:15 kali sshd[1260]: rexec line 7: Deprecated option UsePrivilegeSeparation
Nov 15 17:05:15 kali sshd[1260]: rexec line 8: Deprecated option KeyRegenerationInterval
Nov 15 17:05:15 kali sshd[1260]: rexec line 9: Deprecated option ServerKeyBits
Nov 15 17:05:15 kali sshd[1260]: rexec line 14: Deprecated option RSAAuthentication
Nov 15 17:05:15 kali sshd[1260]: rexec line 17: Deprecated option RhostsRSAAuthentication
Nov 15 17:05:15 kali sshd[1258]: reprocess config line 14: Deprecated option RSAAuthentication
Nov 15 17:05:15 kali sshd[1258]: reprocess config line 17: Deprecated option RhostsRSAAuthentication
Nov 15 17:05:15 kali sshd[1258]: Invalid user pi from 78.126.30.114 port 44790
Nov 15 17:05:15 kali sshd[1258]: pam_unix(sshd:auth): check pass; user unknown
Nov 15 17:05:15 kali sshd[1258]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=78.126.30.114
Nov 15 17:05:15 kali sshd[1260]: reprocess config line 14: Deprecated option RSAAuthentication
Nov 15 17:05:15 kali sshd[1260]: reprocess config line 17: Deprecated option RhostsRSAAuthentication
Nov 15 17:05:15 kali sshd[1260]: Invalid user pi from 78.126.30.114 port 44796
Nov 15 17:05:15 kali sshd[1260]: pam_unix(sshd:auth): check pass; user unknown
Nov 15 17:05:15 kali sshd[1260]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=78.126.30.114
Nov 15 17:05:17 kali sshd[1258]: Failed password for invalid user pi from 78.126.30.114 port 44790 ssh2
Nov 15 17:05:17 kali sshd[1260]: Failed password for invalid user pi from 78.126.30.114 port 44796 ssh2
Nov 15 17:05:18 kali sshd[1258]: Connection closed by invalid user pi 78.126.30.114 port 44790 [preauth]
Nov 15 17:05:18 kali sshd[1260]: Connection closed by invalid user pi 78.126.30.114 port 44796 [preauth]
Nov 15 17:09:01 kali CRON[1279]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 15 17:09:01 kali CRON[1279]: pam_unix(cron:session): session closed for user root
Nov 15 17:15:01 kali CRON[1357]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 15 17:15:01 kali CRON[1357]: pam_unix(cron:session): session closed for user root
Nov 15 17:17:01 kali CRON[1364]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 15 17:17:01 kali CRON[1364]: pam_unix(cron:session): session closed for user root
Nov 15 17:25:01 kali CRON[1381]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 15 17:25:01 kali CRON[1381]: pam_unix(cron:session): session closed for user root
--More--(39%)
```

more +123 /var/log/syslog.1 → dosyanın 123. satırına gider oradan itibaren sergiler. Terminal en altta yine toplama göre dosyanın neresinde olduğunu (yüzde olarak) sergiler

#less

More'dan farklı olarak Arama yapma imkânı da var. Ayrıca ileri geri gidilebilir.

The screenshot shows the less command interface. On the left, there is a help menu with colored rows for different commands:

less <fileName>	• Powerful than more.
/abc	• to search "abc".
:86	• to go to 86th line.
q	• to exit.
arrow keys	• to go back and forward.

To the right of the menu, a terminal window displays a log file named 'yersinia.log' with root privileges. The log contains several entries related to network interfaces and USB bus errors. A red box highlights the word 'RAMDISK' in one of the log entries.

less /var/log/syslog → sağa (→) sol (←) oklarla satırın ilerleyen (satırda tasan) kısımlarını görebiliriz (more'da olmuyordu)

/3389 → bu sayıyı veya kelimeyi arar ve sergiler "/"(slash) tuşuna basıp aranması istenen kelimeyi gireriz.
İstenen kelimelerin üstü boyanır (klasik wordda arama gibi)

:300 → 300. satırı (iki nokta üst üste işaret ile) ilerler.

q → exit

less -N /var/log/syslog → satır numaraları da görünür.
100g → satırda gider

The screenshot shows the less command interface with line numbers enabled (-N). The log file 'yersinia.log' is displayed, and the word 'RAMDISK' is highlighted in red, indicating it was searched for. Line numbers are visible to the left of each log entry.

#head

Dosyaya ilk bastan itibaren satırları (default 10 veya -n ile belirtilen sayıda) sergiler

#head <fileName>

• to see the head of given file (First 10 lines by default).

-n <number>

• to see first <number> lines.

```
root@kali:~# head vnc-brute.nse
local brute = require "brute"
local creds = require "creds"
local shortport = require "shortport"
local stdnse = require "stdnse"
local vnc = require "vnc"

description = [[
Performs brute force password auditing against VNC servers.
]]
```

Head /etc/passwd → İlgili dosyanın ilk 10 satırını (default) sergiler

-n 15 → ilk 15 satırı gösterir

Head -n 1 /etc/passwd → İlgili dosyanın ilk 1 satırını (default) sergiler

#tail

Dosyaya son eklenen satırları (default 10 veya -n ile belirtilen sayıda) sergiler ve sergileme -f komutuyla 2 sn.de bir yenilenebilir. Özellikle log kayıtlarını izlemede kullanılır.

#tail

• to see the last lines of a file (Last 10 lines by default).

-n <number>

• to see last <number> lines.

-f

• to repeat command every 2 seconds. Very handy to watch log files.

Ctrl+c

• to exit

```
root@kali:~# tail -f yersinia.log
```

```
gtk_gui_th_exit start...
gtk_gui_th_exit finish...
goodbye function called from F0898180

ints_destroy started...
ints_destroy finished...
Showing MOTD..
# yersinia finished on Mon May 28 17:18:35 2018
```

tail /var/log/auth.log ➔ İlgili dosyanın son 10 satırını (default) sergiler.

Tail -n 5 -f /var/log/auth.log ➔ ilgili dosyanın son 5 satırını sergiliyor ve 2 sn.de bir yenileniyor. (şu an değişiklik olmadığı için göremedik)

-n 12 ➔ son 12 satırı gösterir.
-f komut 2 sn.de bir tekrarlanır.

Tail -f /var/log/auth.log ➔ ilgili dosyanın son 10 satırını (default) sergiliyor ve 2 sn.de bir yenileniyor (şu an değişiklik olmadığı için göremedik ancak huriye hocanınca değişti çünkü makineye uzaktan bağlanmaya çalıştı)

Ctrl+c ile çıkış yapılır.

history ➔ terminale girilen tüm komutların listesi görülür.

#grep

Dosya veya dizin içinde arama komutu. Bulunan dosyayı sergiler. Sık kullanılan önemli bir komut.

#grep <pattern> <file>	• searches for <pattern> in each <file>.
-i, --ignore-case	• to case-insensitive search.
-e, --regexp=<pattern>	• to use regular expressions.
-r, --recursive	• to read all files under each directory, recursively.
-v, --invert-match	• to select non-matching lines.


```
root@kali:~# ls | grep ssl
dh_perl_openssl
openssl
osslsigncode
sslcaudit
sslscan
sslsniff
sslsplit
sslstrip
```



```
root@kali:~# grep eth0 yersinia.log
Network Interface eth0
eth0 iflinkname EN10MB
eth0 iflinkdesc Ethernet
eth0 MAC = 000c.29dc.f1d5
```

cd /var/log ➔ bu dizine geldim. Bundan sonra dizini yazmama gerek yok

grep RSA auth.log ➔ auth.log dosyasında RSA geçen kayıtları sergiledi.

grep sshd auth.log ➔ auth.log dosyasında sshd geçen kayıtları sergiledi.

Not: büyük küçük harf duyarlıdır.

grep -i sshd auth.log ➔ auth.log dosyasında sshd geçen kayıtları sergiledi. Büyük küçük harf duyarlığını “-i” parametresi ile kaldırındı.

“-i” insensitiv search (Büyük küçük harf duyarlığını kaldırır)

```

File Actions Edit View Help
root@kali:/var/log# grep RSA auth.log
Nov 15 17:05:15 kali sshd[1258]: rexec line 14: Deprecated option RSAAuthentication
Nov 15 17:05:15 kali sshd[1258]: rexec line 17: Deprecated option RhostsRSAAuthentication
Nov 15 17:05:15 kali sshd[1260]: rexec line 14: Deprecated option RSAAuthentication
Nov 15 17:05:15 kali sshd[1260]: rexec line 17: Deprecated option RhostsRSAAuthentication
Nov 15 17:05:15 kali sshd[1258]: reprocess config line 14: Deprecated option RSAAuthentication
Nov 15 17:05:15 kali sshd[1258]: reprocess config line 17: Deprecated option RhostsRSAAuthentication
Nov 15 17:05:15 kali sshd[1260]: reprocess config line 14: Deprecated option RSAAuthentication
Nov 15 17:05:15 kali sshd[1260]: reprocess config line 17: Deprecated option RhostsRSAAuthentication
Nov 15 17:48:46 kali sshd[1630]: rexec line 14: Deprecated option RSAAuthentication
Nov 15 17:48:46 kali sshd[1630]: rexec line 17: Deprecated option RhostsRSAAuthentication
Nov 15 17:49:08 kali sshd[1631]: rexec line 14: Deprecated option RSAAuthentication
Nov 15 17:49:08 kali sshd[1631]: rexec line 17: Deprecated option RhostsRSAAuthentication
Nov 15 18:42:32 kali sshd[1959]: rexec line 14: Deprecated option RSAAuthentication
Nov 15 18:42:32 kali sshd[1959]: rexec line 17: Deprecated option RhostsRSAAuthentication
Nov 15 18:43:07 kali sshd[1960]: rexec line 14: Deprecated option RSAAuthentication
Nov 15 18:43:07 kali sshd[1960]: rexec line 17: Deprecated option RhostsRSAAuthentication
Nov 15 18:57:17 kali sshd[2019]: rexec line 14: Deprecated option RSAAuthentication
Nov 15 18:57:17 kali sshd[2019]: rexec line 17: Deprecated option RhostsRSAAuthentication
Nov 15 19:30:53 kali sshd[2194]: rexec line 14: Deprecated option RSAAuthentication
Nov 15 19:30:53 kali sshd[2194]: rexec line 17: Deprecated option RhostsRSAAuthentication
Nov 15 19:31:04 kali sshd[2194]: reprocess config line 14: Deprecated option RSAAuthentication
Nov 15 19:31:04 kali sshd[2194]: reprocess config line 17: Deprecated option RhostsRSAAuthentication
Nov 15 19:31:30 kali sshd[2199]: rexec line 14: Deprecated option RSAAuthentication
Nov 15 19:31:30 kali sshd[2199]: rexec line 17: Deprecated option RhostsRSAAuthentication
Nov 15 19:31:31 kali sshd[2199]: reprocess config line 14: Deprecated option RSAAuthentication
Nov 15 19:31:31 kali sshd[2199]: reprocess config line 17: Deprecated option RhostsRSAAuthentication

```

grep -i err /* ➔ tüm dosyalarda “err” arama sonucunu sergiledi.

```

File Actions Edit View Help
Shell No. 2
./xrdp.log:[20200816-08:29:37] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-08:59:08] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:07:13] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:26:24] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:27:11] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:28:11] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:28:57] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:30:02] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:30:56] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:40:34] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:41:22] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:42:21] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:43:09] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:44:15] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:45:12] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:54:51] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:54:54] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:55:39] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:56:38] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:57:26] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:58:32] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-09:59:07] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-10:30:00] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-10:30:26] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-10:58:55] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdp.log:[20200816-11:13:25] [ERROR] Cannot read private key file /etc/xrdp/key.pem: Permission denied
./xrdn.log:[20200816-11:15:35] [ERROR] Cannot read private key file /etc/xrdn/kev.nem: Permission denied

```

grep -ic rsa auth.log ➔ ilgili .txt dosyasında “rsa” kelimesinin küçük büyük harf hassasiyeti gözetmeden kaç kez geçtiğini sergiler.

“c” count

```

File Actions Edit View Help
root@kali:/var/log# grep -ic rsa auth.log
26

```

cd /sbin ➔ bin dizinine geldin. Dizin içinde arama yapacağız.

ls -l ➔ dizindeki tüm dosyaları listeler.

ls -l | grep ifconfig ➔ listeden ifconfig geçenleri arar. Burada arama sonucu null.

"|" pipe işaretini sağ taraftaki komuta sol taraftaki komuta girdi yapar.

```
root@kali:/bin# cd /sbin
root@kali:/sbin# ls -l | grep ifconfig
-rwxr-xr-x 1 root root 83768 Sep 24 2018 ifconfig
```

```
root@ip-10-10-99-11:/sbin

File Edit View Search Terminal Help
lrwxrwxrwx 1 root root      9 Jun  9  2020 umount.nfs4 -> mount.nfs
-rwxr-xr-x 1 root root    10232 Sep 26 2018 umount.udisks2
-rwxr-sr-x 1 root shadow  34816 Jul 22 2020 unix_chkpwd
-rwxr-xr-x 1 root root   34816 Jul 22 2020 unix_update
-rwxr-xr-x 1 root root   35168 Apr  9  2019 ureadahead
-rwxr-xr-x 1 root root  36296 Aug 23 2018 veritysetup
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgcfgbackup -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgcfgrestore -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgchange -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgck -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgconvert -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgcreate -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgdisplay -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgexport -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgextend -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgimport -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgimportclone -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgmerge -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgmknodes -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgreduce -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgremove -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgrename -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgs -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgscan -> lvm
lrwxrwxrwx 1 root root      3 Jan 23 2020 vgsplit -> lvm
-rwxr-xr-x 1 root root  38992 Mar  5  2020 wipefs
-rwxr-xr-x 1 root root   1735 Dec 28 2017 wpa_action
-rwxr-xr-x 1 root root  139000 Sep 17 2019 wpa_cli
-rwxr-xr-x 1 root root  2265104 Sep 17 2019 wpa_supplicant
-rwxr-xr-x 1 root root  646304 Apr 18 2018 xfs_repair
-rwxr-xr-x 1 root root  94968 Nov 12 2017 xtables-multi
-rwxr-xr-x 1 root root  92352 Mar  5  2020 zramctl
root@ip-10-10-99-11:/sbin# ls -l | grep ifconfig
-rwxr-xr-x 1 root root  78960 Jan 10 2017 ifconfig
```

Cat /etc/passwd | head -n 5 → soldaki dosyanın ilk 5 satırını sergiledi.

veya

Head -n 5 /etc/passwd → dosyanın ilk 5 satırını sergiledi.

```
root@ip-10-10-99-11:/sbin# head -n 5 /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
root@ip-10-10-99-11:/sbin# cat /etc/passwd | head -n 5
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
```

cat /etc/passwd | grep sys → ilgili dosyada “sys” sözcük araması yapar.

veya

grep sys /etc/passwd → ilgili dosyada “sys” sözcük araması yapar.

```
root@ip-10-10-99-11:/sbin# cat /etc/passwd | grep sys
sys:x:3:3:sys:/dev:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
hplip:x:122:7:HPLIP _system user...:/var/run/hplip:/bin/false
root@ip-10-10-99-11:/sbin# grep sys /etc/passwd
sys:x:3:3:sys:/dev:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
hplip:x:122:7:HPLIP _system user...:/var/run/hplip:/bin/false
```

Grep -i- con /var/log/auth.log → aranan kelime bir kelimenin parçası da olabilir.

```
root@kali:~# grep -i con /var/log/auth.log
Nov 15 20:17:18 kali sshd[1360]: error: kex_exchange_identification: Connection closed by remote host
Nov 15 20:17:18 kali sshd[1360]: Connection closed by 141.98.10.142 port 58666
Nov 15 20:22:50 kali sshd[1388]: error: kex_exchange_identification: Connection closed by remote host
Nov 15 20:22:50 kali sshd[1388]: Connection closed by 209.141.33.121 port 43366
root@kali:~# grep -i -w config /var/log/auth.log
root@kali:~# grep -i -w config /var/log/*
```

Grep -i -w config /var/log/auth.log ➔ Exact match istersem yani tam kelime olarak uyanları aratmak istersem. Config tam aratması ile configuration kelimesi sergilenmez.

-w exact match olsun demek

```
/var/log/xrdp-sesman.log:[20200514-23:48:07] [INFO ] /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.  
conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log  
/var/log/xrdp-sesman.log:[20200515-15:17:48] [INFO ] /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.  
conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log  
/var/log/xrdp-sesman.log:[20200523-22:38:05] [INFO ] /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.  
conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log  
/var/log/xrdp-sesman.log:[20200601-15:13:29] [INFO ] /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.  
conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log  
/var/log/xrdp-sesman.log:[20200601-15:23:34] [INFO ] /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.  
conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log  
/var/log/xrdp-sesman.log:[20200601-15:29:28] [INFO ] /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.  
conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log  
/var/log/xrdp-sesman.log:[20200815-19:21:22] [INFO ] /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.  
conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log  
/var/log/xrdp-sesman.log:[20200815-22:11:50] [INFO ] /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.  
conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log  
/var/log/xrdp-sesman.log:[20200815-22:20:54] [INFO ] /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.  
conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log  
/var/log/xrdp-sesman.log:[20200815-22:26:44] [INFO ] /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.  
conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log  
/var/log/xrdp-sesman.log:[20200815-22:29:16] [INFO ] /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.  
conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log  
/var/log/xrdp-sesman.log:[20200815-22:34:07] [INFO ] /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.  
conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log  
/var/log/xrdp-sesman.log:[20200815-22:36:20] [INFO ] /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.  
conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log  
/var/log/xrdp-sesman.log:[20200815-22:42:12] [INFO ] /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.  
conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log  
/var/log/xrdp-sesman.log:[20200816-11:44:57] [INFO ] /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.  
conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log  
root@kali:~# grep -i -w config /var/log/*
```

Grep -i -v sshd /var/log/auth.log ➔ sshd kelimesi olmayan kayıtları sergiler.

-v sergilenmesi istenmeyen kayıtlar

```
File Actions Edit View Help Shell No.1  
root@kali:~# grep -i -v sshd /var/log/auth.log  
Nov 15 20:06:47 kali CRON[765]: pam_unix(cron:session): session closed for user root  
Nov 15 20:06:50 kali CRON[766]: pam_unix(cron:session): session closed for user root  
Nov 15 20:09:01 kali CRON[1277]: pam_unix(cron:session): session opened for user root by (uid=0)  
Nov 15 20:09:01 kali CRON[1277]: pam_unix(cron:session): session closed for user root  
Nov 15 20:15:01 kali CRON[1351]: pam_unix(cron:session): session opened for user root by (uid=0)  
Nov 15 20:15:01 kali CRON[1351]: pam_unix(cron:session): session closed for user root  
Nov 15 20:17:01 kali CRON[1356]: pam_unix(cron:session): session opened for user root by (uid=0)  
Nov 15 20:17:01 kali CRON[1356]: pam_unix(cron:session): session closed for user root  
Nov 15 20:25:01 kali CRON[1392]: pam_unix(cron:session): session opened for user root by (uid=0)  
Nov 15 20:25:01 kali CRON[1392]: pam_unix(cron:session): session closed for user root  
root@kali:~#
```

Grep -i -n sshd /var/log/auth.log ➔ sshd kelimesi geçen satırları sergile.

Grep -icn sshd /var/log/auth.log ➔ sshd kelimesi geçen satır sayısını sergile (26 imiş).

-r recursive * (yıldız) ile aynı

```

File Actions Edit View Help
root@kali:~# grep -i -n sshd /var/log/auth.log
9:Nov 15 20:17:18 kali sshd[1360]: rexec line 7: Deprecated option UsePrivilegeSeparation
10:Nov 15 20:17:18 kali sshd[1360]: rexec line 8: Deprecated option KeyRegenerationInterval
11:Nov 15 20:17:18 kali sshd[1360]: rexec line 9: Deprecated option ServerKeyBits
12:Nov 15 20:17:18 kali sshd[1360]: rexec line 14: Deprecated option RSAAuthentication
13:Nov 15 20:17:18 kali sshd[1360]: rexec line 17: Deprecated option RhostsRSAAuthentication
14:Nov 15 20:17:18 kali sshd[1360]: error: kex_exchange_identification: Connection closed by remote host
15:Nov 15 20:17:18 kali sshd[1360]: Connection closed by 141.98.10.142 port 58666
16:Nov 15 20:17:29 kali sshd[1361]: rexec line 7: Deprecated option UsePrivilegeSeparation
17:Nov 15 20:17:29 kali sshd[1361]: rexec line 8: Deprecated option KeyRegenerationInterval
18:Nov 15 20:17:29 kali sshd[1361]: rexec line 9: Deprecated option ServerKeyBits
19:Nov 15 20:17:29 kali sshd[1361]: rexec line 14: Deprecated option RSAAuthentication
20:Nov 15 20:17:29 kali sshd[1361]: rexec line 17: Deprecated option RhostsRSAAuthentication
21:Nov 15 20:17:29 kali sshd[1361]: Unable to negotiate with 141.98.10.142 port 41878: no matching key exchange method found. Their offer: diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1 [preauth]
22:Nov 15 20:22:50 kali sshd[1388]: rexec line 7: Deprecated option UsePrivilegeSeparation
23:Nov 15 20:22:50 kali sshd[1388]: rexec line 8: Deprecated option KeyRegenerationInterval
24:Nov 15 20:22:50 kali sshd[1388]: rexec line 9: Deprecated option ServerKeyBits
25:Nov 15 20:22:50 kali sshd[1388]: rexec line 14: Deprecated option RSAAuthentication
26:Nov 15 20:22:50 kali sshd[1388]: rexec line 17: Deprecated option RhostsRSAAuthentication
27:Nov 15 20:22:50 kali sshd[1388]: error: kex_exchange_identification: Connection closed by remote host
28:Nov 15 20:22:50 kali sshd[1388]: Connection closed by 209.141.33.121 port 43366
29:Nov 15 20:23:08 kali sshd[1389]: rexec line 7: Deprecated option UsePrivilegeSeparation
30:Nov 15 20:23:08 kali sshd[1389]: rexec line 8: Deprecated option KeyRegenerationInterval
31:Nov 15 20:23:08 kali sshd[1389]: rexec line 9: Deprecated option ServerKeyBits
32:Nov 15 20:23:08 kali sshd[1389]: rexec line 14: Deprecated option RSAAuthentication
33:Nov 15 20:23:08 kali sshd[1389]: rexec line 17: Deprecated option RhostsRSAAuthentication
34:Nov 15 20:23:08 kali sshd[1389]: Unable to negotiate with 209.141.33.121 port 51242: no matching key exchange method found. Their offer: diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1 [preauth]
root@kali:~# grep -icn sshd /var/log/auth.log
26

```

#uname Sistem bilgisi sergileme

#uname

- prints system information

-a, --all

- to print all information.

Uname -o → OS

Uname -n → host adı

Uname -a → sistem bilgisi hepsi

Linux kali :
 çekirdek/host adı
 5.7.0.-kali3-md 64 : distro
 SMP Debian ... (..26) : versiyon
 x86 64 GNU/Linux : OS

```

File Actions Edit View Help
root@kali:~# uname -a
Linux kali 5.7.0-kali3-amd64 #1 SMP Debian 5.7.17-1kali1 (2020-08-26) x86_64 GNU/Linux
root@kali:~# uname -o
GNU/Linux
root@kali:~# uname -n
kali

```

Output redirection

Symbol / Operator	Description
&	This operator allows you to run commands in the background of your terminal.
&&	This operator allows you to combine multiple commands together in one line of your terminal.
>	This operator is a redirector - meaning that we can take the output from a command (such as using cat to output a file) and direct it elsewhere.
>>	This operator does the same function of the > operator but appends the output rather than replacing (meaning nothing is overwritten).

Output Redirection

- to Redirect output instead of default channel (screen).
- to overwrite the output file with the result set.
- to append the result set to the target file.
- to use the results as an input for another command.

```
root@kali:~# echo Hello World >myTextFile
root@kali:~# cat myTextFile
Hello World
root@kali:~# echo Hello Again >>myTextFile
root@kali:~# cat myTextFile
Hello World
Hello Again
```

```
root@kali:~# cut -d: -f1 < /etc/passwd
root
daemon
bin
sys
sync
games
```

“>” Parametresi

Bir dosyayı “cat” komutuyla var olan dosya içeriğini değiştirmek (eski kayıtlar silinir) veya yoksa dosyayı oluştururken içeriğini de oluşturmak veya için kullanılır.

Bir dosyayı **Touch** komutuyla oluşturabiliriz. Ya da “**cat >**” komutuyla içini doldururken aynı anda dosyayı oluşturabiliriz

```
root@kali:~# cat > newFile
hello
world
bir cümle yazabilirim
^C
root@kali:~# cat newFile
hello
world
bir cümle yazabilirim
```

ekliyorum ben huriye →
Ctrl+c basınca çıkarız.
Cat new file → Dosyaya baktığımızda öncekileri silip
yeniden yazdı.

cat > newFile
Hello
world
Bir cümle yazabilirim →
Ctrl+c basınca çıkarız.
Cat new file → Dosyanın içini sergiler

cat > newFile
yen bir satır

```
root@kali:~# cat > newFile
yeni bir satır
ekliyorum
ben
Huriye
^C
root@kali:~# cat newFile
yeni bir satır
ekliyorum
ben
```

“>>” Parametresi

Var olan dosya içeriğine eski bilgilerin silinmeden sonunda yeni eklemeler yapmak için >> işaretini kullanılmalıdır.

cat >> newCatFile
yeni bir satır üstüne yeni bir satır ekledik ➔

Echo komutu ve “>”, “>>” parametreleriyle dosya oluşturma ve içerik yenileme/ ekleme

Echo hey ➔ ekrana yazar

Echo hey>welcome ➔ bulunduğu dizine welcome adlı dosya oluşturur ve içine “Hey” yazısı ekler

Cat welcome ➔ dosya içeriğini ekrana yazar

```
tryhackme@ip-10-10-139-73:~/folder1$ echo hey > welcome
tryhackme@ip-10-10-139-73:~/folder1$ ls
welcome
tryhackme@ip-10-10-139-73:~/folder1$ cat welcome
hey
tryhackme@ip-10-10-139-73:~/folder1$ █
```

Echo hello>> welcome ➔ belirtilen dosyaya **belirtilen ifadeleri** ekler.

Cat welcome ➔ dosya içeriğini ekrana yazar

```
tryhackme@ip-10-10-139-73:~/folder1$ echo hello >> welcome
tryhackme@ip-10-10-139-73:~/folder1$ cat welcome
hey
hello
tryhackme@ip-10-10-139-73:~/folder1$ █
```

Cat >> /root/newCatFile

Ekleme yapabilirim ➔ belirtilen dizindeki newCATFile dosyasına “**Ekleme yapabilirim**” satırı ekler.

Operator “&”

Bu komutla yazılan komutların işlemi arka planda çalışırken biz terminalde işleme devam edebiliriz. Çalışma süresi fazla olan işlemleri beklemeden çalışmaya devam etmemize imkan olması önemli bir özelliklektir.

Operator "&&"

Birden fazla komutu arka planda çalışmasını sağlayan Shell operatörüdür. Ancak önceki komut çalışıp işi bittikten sonra müteakip komut çalışır.

“<” Parametresi

Sağ taraftaki komutun çıktısının sağ tarafın girdisi olarak kullanılması komutu

cat < /etc/passwd → cat daha önce var olan /etc/passwd dosyasını al ve kullan (input) anlamındadır. Bu dosyayı cat isleyebilir.

cat>sayılar

```
1  
4  
0  
5  
9  
8
```

ctrl+c ile çıktıktı.

sort sayılar → sayılar.txt yi alır sort yapar (sıralar) ve ekrana getirir.

sort < sayılar > sıralanmış-dosya → o dosyayı al sıralanmış dosyaya input yap demek.

cat sıralanmış-dosya → sıraları ekran getirir.

cat sayılar → görüldüğü gibi txt içi bizin ilk girdiğimiz gibi.

pipe “|”

Bir komutun çıktısını diğer komutun girdisi yapmak için kullanılır. grep konusuyla isledik.

To send the output of one command to another command for further processing

Tek komut içinde birden fazla Pipe kullanımı

Cat /etc/passwd | tail -n3 | grep debian →

/etc/passwd dosyasında son 3 kayıt içinde “debian” sözcüğü olan kaydı sergiler.

```
Shell No.1  
File Actions Edit View Help  
root@kali:~# cat /etc/passwd | tail -n3 | grep debian  
debian-tor:x:136:145::/var/lib/tor:/bin/false
```

Nano text editörü

Nano newCatFile → ilgili dosyayı yeni (başka) bir terminalde acar. Bu açılan (aşağıda) terminalde değişiklikler yapabiliriz

Ctrl+X tuşuna başınca kaydetmek isteyip istemediğimizi sorar. “Y” (BÜYÜK HARF) tuşıyla kaydı onaylarsın.



The screenshot shows the nano 5.2 text editor interface. The menu bar includes File, Actions, Edit, View, Help, and a Shell No. 2 indicator. The main window displays the following text:

```
GNU nano 5.2
ekleme
yapabiliirim
3.satir
yeni
satir
degisiklik
```

The status bar at the bottom contains various keyboard shortcuts for file operations like Help (F1), Exit (Alt+F4), Write Out (Shift+F10), Read File (Shift+F11), Replace (Shift+F12), Cut (Ctrl+K), Paste (Ctrl+U), Execute (Ctrl+T), Justify (Ctrl+J), Location (Ctrl+C), Go To Line (Ctrl+G), Undo (M-U), Redo (M-F), Set Mark (M-A), To Bracket (M-B), Copy (M-C), Where Was (M-Q), and Next (M-W).

#mkdir

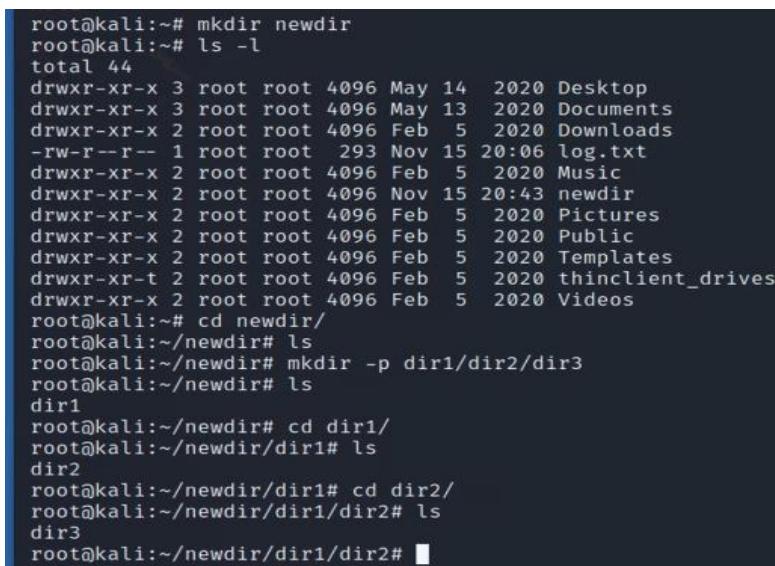
make directory (dizin oluşturma) komutu



mkdir newdir → dizin oluşturma

mkdir -p dir1/dir2/dir3 → recursive dizin oluşturma (iç içe dizin oluşturur)
-p recursive

Aşağıdaki terminalde istenen dizinlerin istenilen şekilde olduğunu gördük.



```
root@kali:~# mkdir newdir
root@kali:~# ls -l
total 44
drwxr-xr-x 3 root root 4096 May 14 2020 Desktop
drwxr-xr-x 3 root root 4096 May 13 2020 Documents
drwxr-xr-x 2 root root 4096 Feb 5 2020 Downloads
-rw-r--r-- 1 root root 293 Nov 15 20:06 log.txt
drwxr-xr-x 2 root root 4096 Feb 5 2020 Music
drwxr-xr-x 2 root root 4096 Nov 15 20:43 newdir
drwxr-xr-x 2 root root 4096 Feb 5 2020 Pictures
drwxr-xr-x 2 root root 4096 Feb 5 2020 Public
drwxr-xr-x 2 root root 4096 Feb 5 2020 Templates
drwxr-xr-t 2 root root 4096 Feb 5 2020 thinclient_drives
drwxr-xr-x 2 root root 4096 Feb 5 2020 Videos
root@kali:~# cd newdir/
root@kali:~/newdir# ls
root@kali:~/newdir# mkdir -p dir1/dir2/dir3
root@kali:~/newdir# ls
dir1
root@kali:~/newdir# cd dir1/
root@kali:~/newdir/dir1# ls
dir2
root@kali:~/newdir/dir1# cd dir2/
root@kali:~/newdir/dir1/dir2# ls
dir3
root@kali:~/newdir/dir1/dir2# █
```

mkdir hello World → 2 ayrı dizin oluşturma (arada boşlukla)

```
root@kali:~# mkdir hello world
root@kali:~# ls
Desktop Documents Downloads hello log.txt Music newdir Pictures Public Templates thinclient_drives Videos world
root@kali:~# ls -l
total 52
drwxr-xr-x 3 root root 4096 May 14 2020 Desktop
drwxr-xr-x 3 root root 4096 May 13 2020 Documents
drwxr-xr-x 2 root root 4096 Feb 5 2020 Downloads
drwxr-xr-x 2 root root 4096 Nov 15 20:47 hello
-rw-r--r-- 1 root root 293 Nov 15 20:06 log.txt
drwxr-xr-x 2 root root 4096 Feb 5 2020 Music
drwxr-xr-x 3 root root 4096 Nov 15 20:45 newdir
drwxr-xr-x 2 root root 4096 Feb 5 2020 Pictures
drwxr-xr-x 2 root root 4096 Feb 5 2020 Public
```

mkdir /root/yeniklasör → İçinde olmadığımız dizinde de yeni bir dizin oluşturabiliriz.

```
root@kali:~/hello# mkdir /root/yenibirklasor
root@kali:~/hello# cd /root
root@kali:~#
Desktop Documents Downloads hello log.txt Music newdir Pictures Public Templates thinclient_drives Videos world yenibirklasor
root@kali:~#
```

#touch

Olmayan dosyayı oluşturur. Var olan dosyanın ise modifikasyon time'ini günceller.
Dikkat: Touch komutu dizin oluşturmaz

Update the access and modification times of the file(s) to the current time.

A file argument that does not exist is created empty.

Touch log.txt → uzantısını belirterek ilgili dosyanın modifikasyon zamanını güncelledik

Touch downloads/ log.txt → dizin sonuna / işaretini konur.

```
root@kali:~# ls -l
total 56
drwxr-xr-x 3 root root 4096 May 14 2020 Desktop
drwxr-xr-x 3 root root 4096 May 13 2020 Documents
drwxr-xr-x 2 root root 4096 Feb 5 2020 Downloads
drwxr-xr-x 2 root root 4096 Nov 15 20:48 hello
-rw-r--r-- 1 root root 293 Nov 15 20:06 log.txt
drwxr-xr-x 2 root root 4096 Feb 5 2020 Music
drwxr-xr-x 3 root root 4096 Nov 15 20:45 newdir
drwxr-xr-x 2 root root 4096 Feb 5 2020 Pictures
drwxr-xr-x 2 root root 4096 Feb 5 2020 Public
drwxr-xr-x 2 root root 4096 Feb 5 2020 Templates
drwxr-xr-t 2 root root 4096 Feb 5 2020 thinclient_drives
drwxr-xr-x 2 root root 4096 Feb 5 2020 Videos
drwxr-xr-x 2 root root 4096 Nov 15 20:47 world
drwxr-xr-x 2 root root 4096 Nov 15 20:49 yenibirklasor
root@kali:~# less log.txt
root@kali:~# touch log.txt
root@kali:~# ls -l
total 56
drwxr-xr-x 3 root root 4096 May 14 2020 Desktop
drwxr-xr-x 3 root root 4096 May 13 2020 Documents
drwxr-xr-x 2 root root 4096 Feb 5 2020 Downloads
drwxr-xr-x 2 root root 4096 Nov 15 20:48 hello
-rw-r--r-- 1 root root 293 Nov 15 20:53 log.txt
drwxr-xr-x 2 root root 4096 Feb 5 2020 Music
drwxr-xr-x 3 root root 4096 Nov 15 20:45 newdir
drwxr-xr-x 2 root root 4096 Feb 5 2020 Pictures
```

#rm remove- dosya veya dizin silme

#rm	• Removes files or directories
-r, -R, --recursive	• remove directories and their contents recursively
-d, --dir	• remove empty directories
-f, --force	• ignore nonexistent files and arguments, never prompt


```
root@kali:~# ls -l temp*
temp1:
total 0

temp2:
total 0
-rw-r--r-- 1 root root 0 Jun 14 18:50 aFile
```

```
root@kali:~# rm -d temp2
rm: cannot remove 'temp2': Directory not empty
root@kali:~# rm -rf temp2
root@kali:~# ls -l temp*
ls: cannot access 'temp*': No such file or directory
```



```
root@kali:~# rm temp1
rm: cannot remove 'temp1': Is a directory
root@kali:~# rm -d temp1
root@kali:~# ls -l temp*
total 0
-rw-r--r-- 1 root root 0 Jun 14 18:50 aFile
```

rm new1 → New1 dizinin içinde başka dizin varsa bu komutla silemeyez.

rm -r new1 → alt alta dizinler varsa da siler.

rm -rf new1 → dosyayı zorlayarak siler.

r: recursive

f: force

Tehlikeli kod **rm -rf /** veya **rm -rf /*** → bulunduğu dizindeki her şeyi zorlayarak sil demektir.

mkdir hacker → hacker adlı directory/dizin oluşturduk.

rm -d hacker/ → hacker dizini bossa siler. Bos değilse silmez. Aşağıda iki durumda görülmektedir. (Dikkat Dizin sonunda / (slash) işaret var

```
root@kali:~# mkdir hacker
root@kali:~# rm -d hacker/
root@kali:~# ls -l
total 40
drwxr-xr-x 3 root root 4096 May 14 2020 Desktop
drwxr-xr-x 3 root root 4096 May 13 2020 Documents
drwxr-xr-x 2 root root 4096 Feb 5 2020 Downloads
-rw-r--r-- 1 root root 293 Nov 16 17:02 log.txt
drwxr-xr-x 2 root root 4096 Feb 5 2020 Music
drwxr-xr-x 2 root root 4096 Feb 5 2020 Pictures
drwxr-xr-x 2 root root 4096 Feb 5 2020 Public
drwxr-xr-x 2 root root 4096 Feb 5 2020 Templates
drwxr-xr-t 2 root root 4096 Feb 5 2020 thinclient_drives
drwxr-xr-x 2 root root 4096 Feb 5 2020 Videos
root@kali:~# mkdir -p hacker/academy/
root@kali:~# ls -l
total 44
drwxr-xr-x 3 root root 4096 May 14 2020 Desktop
drwxr-xr-x 3 root root 4096 May 13 2020 Documents
drwxr-xr-x 2 root root 4096 Feb 5 2020 Downloads
drwxr-xr-x 3 root root 4096 Nov 16 18:09 hacker
-rw-r--r-- 1 root root 293 Nov 16 17:02 log.txt
drwxr-xr-x 2 root root 4096 Feb 5 2020 Music
drwxr-xr-x 2 root root 4096 Feb 5 2020 Pictures
drwxr-xr-x 2 root root 4096 Feb 5 2020 Public
drwxr-xr-x 2 root root 4096 Feb 5 2020 Templates
drwxr-xr-t 2 root root 4096 Feb 5 2020 thinclient_drives
drwxr-xr-x 2 root root 4096 Feb 5 2020 Videos
root@kali:~# rm -d hacker/
rm: cannot remove 'hacker/': Directory not empty
```

Touch newFile → dosya oluşturur.

rm newFile → dosyayı direk silebiliriz.

Konum vererek dosya oluşturma ve silme
(. (nokta) veya ~ (Tilda) ile)

Touch ./Pictures/newFile → dosya oluşturur.

rm ./Pictures/ → dosyayı direk silebiliriz.

```
root@kali:~# touch newFile
root@kali:~# rm newFile
root@kali:~# ls -l
total 44
drwxr-xr-x 3 root root 4096 May 14 2020 Desktop
drwxr-xr-x 3 root root 4096 May 13 2020 Documents
drwxr-xr-x 2 root root 4096 Feb 5 2020 Downloads
drwxr-xr-x 3 root root 4096 Nov 16 18:09 hacker
-rw-r--r-- 1 root root 293 Nov 16 17:02 log.txt
drwxr-xr-x 2 root root 4096 Feb 5 2020 Music
drwxr-xr-x 2 root root 4096 Feb 5 2020 Pictures
drwxr-xr-x 2 root root 4096 Feb 5 2020 Public
drwxr-xr-x 2 root root 4096 Feb 5 2020 Templates
drwxr-xr-t 2 root root 4096 Feb 5 2020 thinclient_drives
drwxr-xr-x 2 root root 4096 Feb 5 2020 Videos
root@kali:~#
```

Başka dizindeki klasörleri onların yolunu göstererek de silebiliriz.

mkdir -p ./Pictures/dir3/dir4 → iç içe directory oluşturur.

“p” parents

Relativ Path == ./Pictures

Absolute Path == rooth/Pictures (tam adres)

#cp & #mv

kopyala- taşı (yeni adda verebiliriz)

Dikkat: cp : kopyala yapıştır (ctrl c ve ctrl v)
mv : kes yapıştır (ctrl x ve ctrl v)

#cp	• copy files and directories
-R, -r, --recursive	• copy directories recursively

#mv	• move (rename) files
-f, --force	• do not prompt before overwriting

```
root@kali:~# cp ipList.txt ./temp/
root@kali:~# ls ./temp/
ipList.txt
root@kali:~# cd temp/
root@kali:~/temp# mv ipList.txt newList.txt
root@kali:~/temp# ls
newList.txt
root@kali:~/temp# mv newList.txt /root/
root@kali:~/temp# cd ..
root@kali:~# ls *List.txt
ipList.txt  newList.txt
```

Copies the file with the same name to another folder

Renames the file!
(Moving the same folder with another name)

Moves the file with the same name to another folder

Root içinde hacker/academy dizinimiz var. Onu masaüstüne taşıyalım.

cp hacker/ .Desktop ➔ hatalı komut, hacker dizininin içi dolu (gözükmesse de gizli dosyalar olabilir)

cp -r hacker/ ./Desktop ➔ içi dolu dizini (hacker/) belirtilen yere (./Desktop/) taşır
(r) komutunu her zaman kullanmalı

```
root@kali:~# ls -l hacker/
total 4
drwxr-xr-x 2 root root 4096 Nov 16 18:09 academy
root@kali:~# ls -l hacker
total 4
drwxr-xr-x 2 root root 4096 Nov 16 18:09 academy
root@kali:~# cp hacker/ ./Desktop/
cp: -r not specified; omitting directory 'hacker/'
root@kali:~# cp -r hacker/ ./Desktop/
root@kali:~# ls
Desktop Documents Downloads hacker log.txt Music Pictures Public Templates thinclient_drives Videos
root@kali:~# pwd
/root
```

touch newFile ➔ bulunulan dizinde newFile adlı dosya oluşturur.

cp newFile ./Desktop/ ➔ newFile dosyasını masaüstüne kopyalar.
newFile dizin değil dosyadır. O yüzden dosya adının sonunda "/" (slash) işaret yok.

```
root@kali:~# cp Music/
cp: missing destination file operand after 'Music/'
Try 'cp --help' for more information.
root@kali:~# cp Music/ ./Desktop/
cp: -r not specified; omitting directory 'Music/'
root@kali:~# touch newFile
root@kali:~# cp newFile ./Desktop/
root@kali:~# ls -l newFile
-rw-r--r-- 1 root root 0 Nov 16 18:31 newFile
```

cp newFile /tmp/ ➔ yukarıdaki dosyayı (masaüstündeki) başka bir dizin (/tmp/) altına da kopyalayabiliriz (Dikkat . (Nokta) kullanmadık)

Desktop üzerindeki newFile kes yapıştır.

mv hacker/ /tmp/ ➔ dizin kes yapıştır

mv newFile /tmp/ ➔ dosya kes yapıştır

```
Shell No.1
File Actions Edit View Help
root@kali:~/Desktop# mv /tmp/hacker/ ~/Desktop/yenihacker
root@kali:~/Desktop# mv yenihacker/ eurotech
root@kali:~/Desktop# mv yenihacker/ eurotech/
mv: cannot stat 'yenihacker/': No such file or directory
root@kali:~/Desktop# mv eurotech/ yenibirisim/
root@kali:~/Desktop# mv yenibirisim yeni
root@kali:~/Desktop# mv yenibirisim yeni █ I
```

#find

Çok fazla parametresi var.

#find - search for files in a directory hierarchy

Wide range of uses

Searches by names, permissions, search depth, logical comparisons etc.

```
root@kali:~# find / -iname "*.nse"
/usr/share/golismero/wordlist/fingerprint/httprecon/httprecon.nse
/usr/share/nmap/scripts/finger.nse
/usr/share/nmap/scripts/ms-sql-xp-cmdshell.nse
/usr/share/nmap/scripts/http-vuln-wnr1000-creds.nse
/usr/share/nmap/scripts/dns-fuzz.nse
```

KER ACADEMY

euroTech Study

```
root@kali:~# find /root -maxdepth 1 \(\ -type d -not -perm 700 \) -exec ls -l "{}" +
/root:
total 764
-rw-r--r-- 1 root root    194 Sep  2  2013 boot.ini
drwxr-xr-x  2 root root   4096 Apr  3 11:14 Desktop
drwxr-xr-x  2 root root   4096 Apr 21  2017 Documents
```

Nerede neyi (Dosya ve directory) arayacağımızı belirtilmeliyiz.

find /var/ -name auth.log → /var/

dizininde “auth.log” olan dosyaları ara komutu. Cvp olumlu ise dosyanın konumunu verir

```
File Actions Edit View Help
Shell No.1
root@kali:~# find /var/ -name auth.log
/var/log/auth.log
root@kali:~# find /var/ -name aut.log
root@kali:~# find /var/ -name aut*.log
/var/lib/autopsy/autopsy.log
/var/log/auth.log
root@kali:~# find /var/ -name *.log
/var/lib/dkms/nvidia-current/440.100/5.7.0-kali3-amd64/x86_64/log/make.log
/var/lib/dkms/nvidia-current/440.100/5.4.0-kali3-amd64/x86_64/log/make.log
/var/lib/autopsy/autopsy.log
/var/log/alternatives.log
/var/log/vmware-vmodoolsd-root.log
/var/log/apache2/error.log
/var/log/apache2/other_vhosts_access.log
/var/log/apache2/access.log
/var/log/apt/history.log
```

find /var/ -name aut*.log → /var/

dizininde aut ile başlayan log dosyaları bul komutu

find /var/ -name *.log → /var/ dizininde log dosyalarını getir

```
root@kali:~# find /var/ -name .*.log
root@kali:~# find /var/ -name ".*"
/var/lib/lightdm/.gnupg
/var/lib/lightdm/.Xauthority
/var/lib/lightdm/.cache
/var/lib/lightdm/.config
/var/lib/coldord/.cache
/var/lib/gems/2.5.0/gems/rubygems-update-3.1.4/bundler/lib
/var/lib/gems/2.5.0/gems/rubygems-update-3.1.4/lib/rubygen
/var/lib/gems/2.5.0/gems/rubygems-update-3.1.4/.rubocop.yml
/var/lib/gems/2.5.0/gems/rubygems-update-3.1.4/tmp/.keep
/var/lib/gems/2.5.0/gems/rubygems-update-3.1.4/.bundle
/var/lib/gems/2.5.0/gems/bundler-1.17.3/lib/bundler/ssl_c
/var/lib/gems/2.5.0/gems/bundler-1.17.3/lib/bundler/templa
/var/lib/ieee-data/.lastupdate
/var/lib/postgresql/.gnupg
/var/lib/postgresql/.config
/var/cache/apparmor/ea9ed67a.0/.features
```

find /var/ -name “.*” → Gizli dizin veya dosyaları bulur.

find / -name auth.log → tüm dizinlerde ilgili dosyayı arar.

find /var/ -name *.log | grep auth →
/var/ dizininde tüm log dosyalarını bulur.
Bunların içinde auth gecenleri sergiler.

```
root@kali:~# find /var/ -name *.log | grep auth  
/var/log/auth.log
```

Find / -iname xorg → tüm dizininde adında xorg gecen tüm dosyaları bulur. Büyük küçük harf duyarlılığı olmasın dediğimiz için hepsini. “i” insensitive

find / -name xorg → tüm dizininde adında xorg gecen tüm dosyaları bulur. Büyük küçük harf duyarlılığı olmasın dediğimiz için büyük küçük harf duyarlıydı. Önceki sorguda gelen 2 tane dosyayı bu kez listelememi

```
root@kali:~# find / -iname xorg  
/usr/share/bug/xorg  
/usr/share/doc/xorg  
/usr/share/lintian/overrides/xorg  
/usr/share/X11/xkb/rules/xorg  
/usr/include/xorg
```

```
/usr/bin/Xorg  
/usr/lib/xorg  
/usr/lib/xorg/xorg
```

```
root@kali:~# find / -name xorg  
/usr/share/bug/xorg  
/usr/share/doc/xorg  
/usr/share/lintian/overrides/xorg  
/usr/share/X11/xkb/rules/xorg  
/usr/include/xorg  
/usr/lib/xorg
```

find /root/ -iname *.txt → tüm txt. Uzantılı dosyaları sergile (1 dosya)

veya

find ~ -iname *txt → tüm txt. Uzantılı dosyaları sergile (home/root sanal makinelerde aynı)
(1 dosya)

find /root/ -iname “*txt” → tırnak içinde olunca gizli dosyalarda sergilenebilir.

```
root@kali:~# find ~ -iname *.txt  
/root/log.txt  
root@kali:~# find ~ -iname “*.txt”  
/root/.local/share/torbrowser/tbb/x86_64/tor-browser_en-US/Browser/TorBrowser/Docs/ChangeLog.txt  
/root/.local/share/torbrowser/tbb/x86_64/tor-browser_en-US/Browser/TorBrowser/Docs/Licenses/Tor.txt  
/root/.local/share/torbrowser/tbb/x86_64/tor-browser_en-US/Browser/TorBrowser/Docs/Licenses/Torbutton.txt  
/root/.local/share/torbrowser/tbb/x86_64/tor-browser_en-US/Browser/TorBrowser/Docs/Licenses/No-CJK-Font.txt  
/root/.local/share/torbrowser/tbb/x86_64/tor-browser_en-US/Browser/TorBrowser/Docs/Licenses/HTTPS-Everywhere.txt  
/root/.local/share/torbrowser/tbb/x86_64/tor-browser_en-US/Browser/TorBrowser/Docs/Licenses/NoScript.txt  
/root/.local/share/torbrowser/tbb/x86_64/tor-browser_en-US/Browser/TorBrowser/Docs/Licenses/Firefox.txt  
/root/.local/share/torbrowser/tbb/x86_64/tor-browser_en-US/Browser/TorBrowser/Docs/Licenses/Libevent.txt  
/root/.local/share/torbrowser/tbb/x86_64/tor-browser_en-US/Browser/TorLauncher/TorLauncher.txt  
/root/.local/share/torbrowser/tbb/x86_64/tor-browser_en-US/Browser/TorBrowser/Docs/Licenses/Tor-Launcher.txt  
/root/.local/share/torbrowser/tbb/x86_64/tor-browser_en-US/Browser/TorBrowser/Docs/Licenses/Noto-Fonts.txt  
/root/log.txt  
/root/Desktop/PEASS/winPEAS/winPEASexe/winPEAS/obj/x64/Release/winPEAS.csproj.FileListAbsolute.txt  
/root/Desktop/PEASS/winPEAS/winPEASexe/winPEAS/obj/x64/Debug/winPEAS.csproj.FileListAbsolute.txt  
/root/Desktop/PEASS/winPEAS/winPEASexe/winPEAS/obj/x86/Release/winPEAS.csproj.FileListAbsolute.txt  
/root/Desktop/PEASS/winPEAS/winPEASexe/winPEAS/obj/x86/Debug/winPEAS.csproj.FileListAbsolute.txt  
/root/Desktop/PEASS/winPEAS/winPEASexe/winPEAS/obj/Release/winPEAS.csproj.FileListAbsolute.txt  
/root/Desktop/PEASS/winPEAS/winPEASexe/winPEAS/obj/Debug/winPEAS.csproj.FileListAbsolute.txt  
/root/.mozilla/firefox/80rbwt7m.default-esr/pkcs11.txt  
/root/.mozilla/firefox/80rbwt7m.default-esr/AlternateServices.txt  
/root/.mozilla/firefox/80rbwt7m.default-esr/revocations.txt  
/root/.mozilla/firefox/80rbwt7m.default-esr/SiteSecurityServiceState.txt  
/root/.mozilla/firefox/80rbwt7m.default-esr/TRRBlacklist.txt
```

find /etc/ -iname ssh -type d ➔
adı ssh olan sadece dizinleri (dosyalar değil) sergilettik.

“d” directory

find /etc/ -iname ssh type f ➔
adı ssh olan sadece dosyaları (dizinler değil) sergilettik.

“f” file

```
root@kali:~# find /etc/ -iname ssh -type d
/etc/ssh
/etc/sv/ssh
root@kali:~# cd /etc/ssh
ssh/    ssl/    ssllib/
root@kali:~# cd /etc/ssh/
root@kali:/etc/ssh# cd /etc/sv/ssh/
root@kali:/etc/sv/ssh# cd
root@kali:~# find /etc/ -iname ssh -type f
/etc/init.d/ssh
/etc/default/ssh
root@kali:~# cd /etc/init.d/ssh
bash: cd: /etc/init.d/ssh: Not a directory
```

Find / -iname openvpn -type f -user root

➔ Belirtilen (user) kullanıcıya ilişkin dosyaları arama

```
root@kali:~# find / -iname openvpn -type f -user root
/etc/network/if-up.d/openvpn
/etc/network/if-down.d/openvpn
/etc/init.d/openvpn
/etc/default/openvpn
/usr/share/bash-completion/completions/openvpn
/usr/sbin/openvpn
```

find /tmp/ -name “.*” -type f ➔ /tmp/ dizininin altındaki tüm gizli dosyaları bulun.

find /etc/ -type f ! -name “*.java” ➔ etc dizininde java uzantılı olmayan dosyaları bulur.

veya

find /etc/ -type f -not -name “*.java” ➔ etc dizininde java uzantılı olmayan dosyaları bulur.

! : hariç tutulan
not : hariç tutulan

#cut

kesip almak için

#cut	• print selected parts of lines from each FILE to standard output.
Common Usage	<ul style="list-style-type: none">• #cut -d"delimiter" -f[fieldNumber]• #cut -d":" -f3,4
-f, --fields=LIST	• select only these fields
-d, --delimiter=DELIM	• use DELIM instead of TAB for field delimiter
<pre>root@kali:~# nmap -sP 172.16.99.0/24 grep "Nmap scan" cut -d" " -f5 172.16.99.1 172.16.99.2 172.16.99.254 172.16.99.229</pre>	

nano ./Desktop/ikincibirism → daha önce oluşturmuş olduğumuz ilgili dosyayı nano text editöründe acar.

Açılan dosyaya kişi ad soyada yas ve şirket kayıtlarını yazdık, kaydettik ve kapattık.

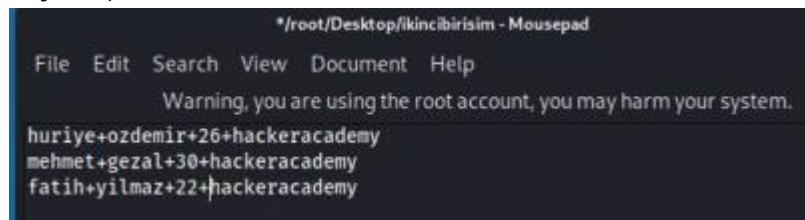
```
GNU nano 5.2
huriye ozdemir 26 hackeracademy
mehmet gezal 30 hackeracademy
fatih yilmaz 22 hackeracademy
```

“d” delimiter : formatı sağladığın işaretlemeler (burada boşluk)

Cut -d “ ” -f3 ./Desktop/ikincibirism → boşluğu delimiter olarak belirledim ve buna göre 3. Sütunu ekrana getirdim (yas)

Cut -d “ ” -f3,4 ./Desktop/ikincibirism → boşluğu delimiter olarak belirledim ve buna göre 3. ve 4. sütunu ekrana getirdim (yas ve şirket)

Boşluk yerine + (arti) kullandık



Cut -d “+” -f1 ./Desktop/ikincibirism → + (arti) delimiter olarak belirledim ve buna göre 1. sütunu ekrana getirdim (ad)

```
root@kali:~# nano ./Desktop/ikincibirism
root@kali:~# nano ./Desktop/ikincibirism
root@kali:~# cat ./Desktop/ikincibirism
huriye ozdemir 26 hackeracademy
mehmet gezal 30 hackeracademy
fatih yilmaz 22 hackeracademy

root@kali:~# cut -d " " -f3 ./Desktop/ikincibirism
26
30
22

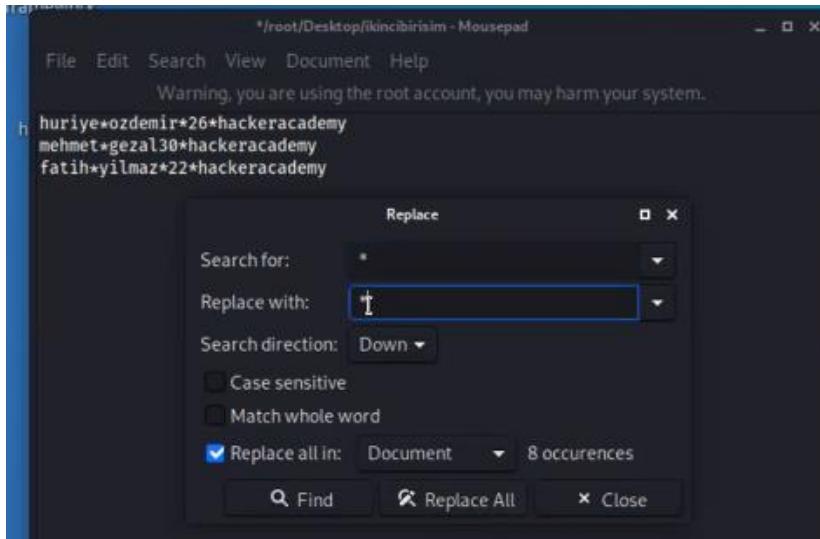
root@kali:~# cut -d " " -f3,4 ./Desktop/ikincibirism
26 hackeracademy
30 hackeracademy
22 hackeracademy
```

```
root@kali:~# cut -d "+" -f1 ./Desktop/ikincibirism
huriye
mehmet
fatih

root@kali:~# cut -d "+" -f1,3,4 ./Desktop/ikincibirism
huriye+ozdemir+26+hackeracademy
mehmet+gezal+30+hackeracademy
fatih+yilmaz+22+hackeracademy

root@kali:~# cut -d "+" -f1,4 ./Desktop/ikincibirism
huriye+hackeracademy
mehmet+hackeracademy
fatih+hackeracademy
```

Editörle tüm + (arti) yerine , (virgül) değiştirmesi yapabilirim.



grep mehmet ikincibirisim | cut -d "," -f2 ➔ ilgili dosyada (ikincibirisim) Mehmet'in olduğu yeri bulur ve 2. sütünün ekran'a getirir.

```
root@kali:~/Desktop# cut -d "," -f2,1,3 ikincibirisim | grep huriye
huriye,ozdemir,26
root@kali:~/Desktop# grep mehmet ikincibirisim | cut -d "," -f2
gezal
root@kali:~/Desktop# grep mehmet ikincibirisim
mehmet,gezal,30,hackeracademy
```

Önce kesip sonra grep yapalım ve farkları görelim.

cut -d "," -f1,2,3,4 ikincibirisim | grep huriye ➔

```
root@kali:~/Desktop# cut -d "," -f2 ikincibirisim | grep huriye
root@kali:~/Desktop# cut -d "," -f1,2,3,4 ikincibirisim | grep huriye
huriye,ozdemir,26,hackeracademy
root@kali:~/Desktop# cut -d "," -f1,2,3,4 ikincibirisim
huriye,ozdemir,26,hackeracademy
mehmet,gezal,30,hackeracademy
fatih,yilmaz,22,hackeracademy

root@kali:~/Desktop# cut -d "," -f1 ikincibirisim
huriye
mehmet
fatih

root@kali:~/Desktop# cut -d ":" -f1 ikincibirisim | grep huriye
huriye
root@kali:~/Desktop# cut -d ":" -f1 ikincibirisim | grep ozdemir
root@kali:~/Desktop#
```

cut -d ":" -f7 /etc/passwd/ ➔ bu dosyadaki tüm 7. sütunu ekran getir.

grep debian-tor /etc/passwd | cut -d ":" -f7 ➔ dosyada "debian-tor" ifadesi gecen satırları bulup bu satırların 7. sütununu ekran'a getir.

17.11.2021 Wednesday

#Locate

adi girilen dosyanın yolunu gösteriyor. Find'dan farkı dosyayı **locate.db** veri tabanındaki kayıtlardan aramasıdır.

Locate log.txt → veri tabanı kayıtlarından hızlı bir şekilde 3 adet log.txt dosya bilgisi sergilendi.

Masaüstüne Hackeracademy.txt adlı bir dosya oluşturup onu aratalım.

Locate hackeracademy.txt → veri tabanı kayıtları güncellenmediği için yeni oluşturulan text'i bulamadı.

```
root@kali:~# man locate
root@kali:~# locate log.txt
/root/log.txt
/usr/share/doc/cloud-init/examples/cloud-config-rsyslog.txt
/usr/share/doc/util-linux/getopt_changelog.txt
root@kali:~# locate hackeracademy.txt
root@kali:~#
```

Locate -S → veri tabanındaki kayıt bilgilerini sergiler. (Kali linux'de -S komutu olmaz)

#updatedb

veri tabanının güncellenmesi

Sonradan oluşturulan bir dosyanın **locate** komutu ile bulunabilmesi için "**updatedb**" komutu ile veri tabanının güncellenmesi gerekmektedir. Güncellemeye biraz uzun sürebilir (1 dk). Güncellemeye sonrası bahse konu doküman tekrar "locate" sorgulamasılığımızda bilgiler sergilenebilir.

```
root@kali:~# locate hackeracademy.txt
root@kali:~# locate -S
Database /var/lib/mlocate/mlocate.db:
      32,321 directories
      366,256 files
      22,470,522 bytes in file names
      8,608,907 bytes used to store database
root@kali:~# updatedb
root@kali:~# locate hackeracademy.txt
/root/Desktop/hackeracademy.txt
```

locate -i Burpsuite | grep Desktop → Burpsuite adlı **mlocate.db** (dosyaların konum kaydından) dosyası içindeki kayıtlardan Desktop ifadesi geçenleri sergiler-

“-i” ignore büyük küçük harf farketmez.

find /root/Desktop -iname “Burpsuite” → Bu komut masaüstü (DESKTOP) dizininde Burpsuite kelimesi geçenleri arar ve sergiler (FARKA DİKKAT)

```
root@kali:~# locate -i Burpsuite | grep Desktop
/root/Desktop/kali-burpsuite.desktop
```

#Whereis

Çalıştırılabilir (executable) bir dosyanın yerini ve manueli varsa onu da gösteriyor

where is hackeracademy.txt ➔ cevap veremez, çünkü executable değil

ifconfig ➔ Çalıştırılabilir bu dosyayı bulunamadı.

where is ifconfig ➔ ifconfig çalıştırılabilir dosyanın yerini gösterdi.

where is hashcat ➔ birden fazla dizinde yer aldığığini görüyoruz

where is burpsuite ➔ burpsuite çalıştırılabilir dosyanın yerini gösterdi.

```
root@kali:~# whereis hackeracademy.txt
hackeracademy:
root@kali:~# ifconfig
bash: ifconfig: command not found
root@kali:~# whereis ifconfig
ifconfig: /usr/sbin/ifconfig /usr/share/man/man8/ifconfig.8.gz
root@kali:~# whereis hashcat
hashcat: /usr/bin/hashcat /usr/lib/hashcat /usr/share/hashcat /usr/share/man/man1/hashcat.1.gz
root@kali:~# whereis burpsuite
burpsuite: /usr/bin/burpsuite
```

whereis -l ➔ arama yaptığı liste dizinlerin (source (s) ,manuel (m) ve binary (b)) bilgisini sergiledi.

whereis -m man ➔ man komutunun **manuel (m)** dizinlerin bilgisini sergiledi.

whereis - b man ➔ man komutunun **Binary (b)** dizinlerin bilgisini sergiledi.

whereis -s man ➔ man komutunun **source (c)** dizinlerin bilgisini olmadığı için sergilemedi.

whereis -s nvidia ➔ nvidia komutunun **source (s)** dizinlerin bilgisini sergiledi.

whereis nvidia ➔ nvidia komutunun **source(s)+manuel(m)+binary(b)** dizinlerin bilgisini sergiledi.

“l” liste (s+m+b)

“-s” source

“-m” manuel

“-b” Binary

```
root@kali:~# whereis -m man
man: /usr/share/man/man7/man.7.gz /usr/share/man/man1/man.1.gz
root@kali:~# whereis -b man
man: /usr/bin/man /usr/local/man /usr/share/man
root@kali:~# whereis -s man
man:
root@kali:~# whereis -s nvidia
nvidia: /usr/src/nvidia-current-440.100/nvidia
root@kali:~# whereis nvidia
nvidia: /usr/lib/x86_64-linux-gnu/nvidia /usr/lib/nvidia /etc/nvidia /usr/share/nvidia /usr/src/nvidia-current-440.100/nvidia
```

#Which

executable dosyaların dizin bilgisinin sergiler. Whereis'den bazı parametreler farklı

which ping → ilk bulduğu yer bilgisini sergiler

which -a ping → üm bulunan sonuçları sergiler
a: all

which log.txt → çalıştırılabilir dosya olmadığı için bulamadı.

Which ifconfig → su- komutu olmadan bilgiyi erişemedi

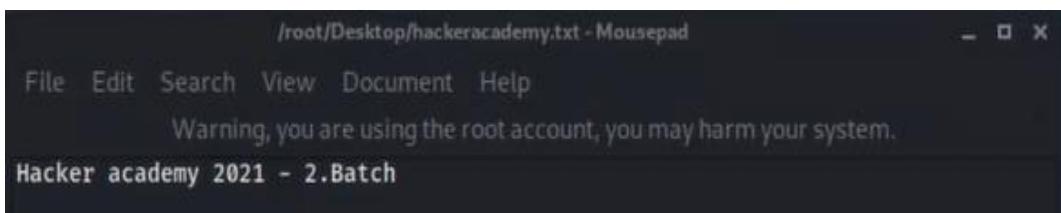
```
root@kali:~# which log.txt
root@kali:~# which -a ping
/usr/bin/ping
/bin/ping
root@kali:~# which ifconfig
root@kali:~# which -a ifconfig
root@kali:~# which -a adduser
root@kali:~# which -a ls metasploit
/usr/bin/ls
/bin/ls
```

Which -a ls metasploit → birden fazla executable dosya arama. Burada sadece ls dizinlerini buldu. Metasploit dosyasına erişemedi.

#wc Word count

Dosyanın içerisindeki satır sayısı, kelime sayısı ve karakter sayısını bulma

Önce masaüstünde bulunan (biraz önce oluşturmustuk) hackeracademy.txt dosyasına bir şeyler yazalım.



wc ./Desktop/hackeracademy.txt → belirtilen dokümanda 1 satır 5 kelime(öbek) 30 karakter varmış

wc -l ./Desktop/hackeracademy.txt → 1 satır

wc -w ./Desktop/hackeracademy.txt → 5 kelime (öbek)

wc -c ./Desktop/hackeracademy.txt → 30 karakter

"-l" line (satır) sayısı,

"-w" word (kelime) sayısı

"-c" character (karakter) sayısı

```
root@kali:~# man wc
root@kali:~# wc ./Desktop/hackeracademy.txt
      1  5 30 ./Desktop/hackeracademy.txt
root@kali:~# wc -l ./Desktop/hackeracademy.txt
      1 ./Desktop/hackeracademy.txt
root@kali:~# wc -c ./Desktop/hackeracademy.txt
      30 ./Desktop/hackeracademy.txt
root@kali:~# man wc
root@kali:~# wc -w ./Desktop/hackeracademy.txt
      5 ./Desktop/hackeracademy.txt
```

cat ile okutup wc komutu ile saydırma (pipe kullanarak)

cat ./Desktop/hackeracademy.txt | wc →

cat ./Desktop/hackeracademy.txt | wc -l →

```
root@kali:~# cat ./Desktop/hackeracademy.txt | wc
      1      5     30
root@kali:~# cat ./Desktop/hackeracademy.txt | wc -l
1
```

#tr translate or delete characters

karakterlerden birinin yerine başka bir karakter koyma veya karakteri silme

Bu kodu tek başına kullanıp dizinde veya metinde değişiklik yapamıyoruz. Manuelindeki formatta ta hedef metin gösterilmemiş. O yüzden önce Echoyla metin yazacağımız veya "cat" ile dosyaya erişip sonra tr ile karakter değişikliği yapacağız.

cat ./Desktop/hackeracademy.txt | tr a A → a yerine A yaptı

echo "Hello world" | tr l t → metinde (Hello World) l harfini t harfi ile değiştirdik.

echo "Hello world" | tr l L → metinde (Hello World) l harfini L harfi ile değiştirdik. Küçük harfi büyük harf yaptı

echo "Hello world" | tr [a-z] [A-Z] → metindeki tüm küçük harfleri büyük harfe çevirir.

echo "Hello world" | tr l t | tr e a → metindeki l yerine t, e yerine a yaptı

echo "Hello world" | tr l t && tr e a 0→ Bu şekilde sadece ilk değişikliği yaptı

```
root@kali:~# cat ./Desktop/hackeracademy.txt | tr a A
HAcker AcAdemy 2021 - 2.BAtch
root@kali:~# man tr
root@kali:~# echo "Hello World" | tr l t
Hetto World
root@kali:~# echo "Hello World" | tr l L
HeLLo WorLd
root@kali:~# echo "Hello World" | tr " " :
Hello:World
root@kali:~# echo "Hello World" | tr [a-z] [A-Z]
HELLO WORLD
root@kali:~# echo "Hello World" | tr l t && tr e a
Hetto World
^C
root@kali:~# echo "Hello World" | tr l t | tr e a
Hatto World
root@kali:~# █
```

```
cat ./Desktop/hackeracademy.txt | tr -d " " ➔ tr komutunu kullanarak karakter silme (boşluk)
```

```
cat ./Desktop/hackeracademy.txt | tr -d a ➔ tr komutunu kullanarak karakter silme (a harfi)  
"d" delete
```

```
root@kali:~# cat ./Desktop/hackeracademy.txt | tr -d " "  
Hackeracademy2021-2.Batch  
root@kali:~# cat ./Desktop/hackeracademy.txt | tr -d a  
Hcker cdemy 2021 - 2.Btch
```

Soru: Desktopta oluşturduğunuz bir dosyanın içeriğindeki boşlukları ":" (iki nokta üst üste) ile değiştirip, değişen sonucu başka bir dosyaya yazdırın. (Aşağıdaki her 2 seçenek de doğru)

Cözüm:

```
cat ./Desktop/hackeracademy.txt | tr " " : | cat >> ./Desktop/newfile ➔  
veya  
cat ./Desktop/hackeracademy.txt | tr " " : > ./Desktop/new2file ➔
```

Sadece tr komutu ile çözüm

```
tr " " : < ./Desktop/hackeracademy.txt > ./Desktop/new3file ➔  
veya  
< ./Desktop/hackeracademy.txt tr " " : > ./Desktop/ new4file ➔
```

Aşağıdaki şekilde ise dosya içini silmeden yeni bir satır ekler
tr " " : < ./Desktop/hackeracademy.txt >> ./Desktop/ new4file ➔

2.4 Linux User Management User Tasks

Single User - Single Task

- One user can effectively do one thing at a time
- Palm handheld computers - Palm OS

Single User - Multi Task

- A single user has several programs in operation at the same time
- MS Windows, MacOS

Multi User - Multi Task

- More than one users have several programs in operation at the same time
- Unix/Linux, mainframe operating systems

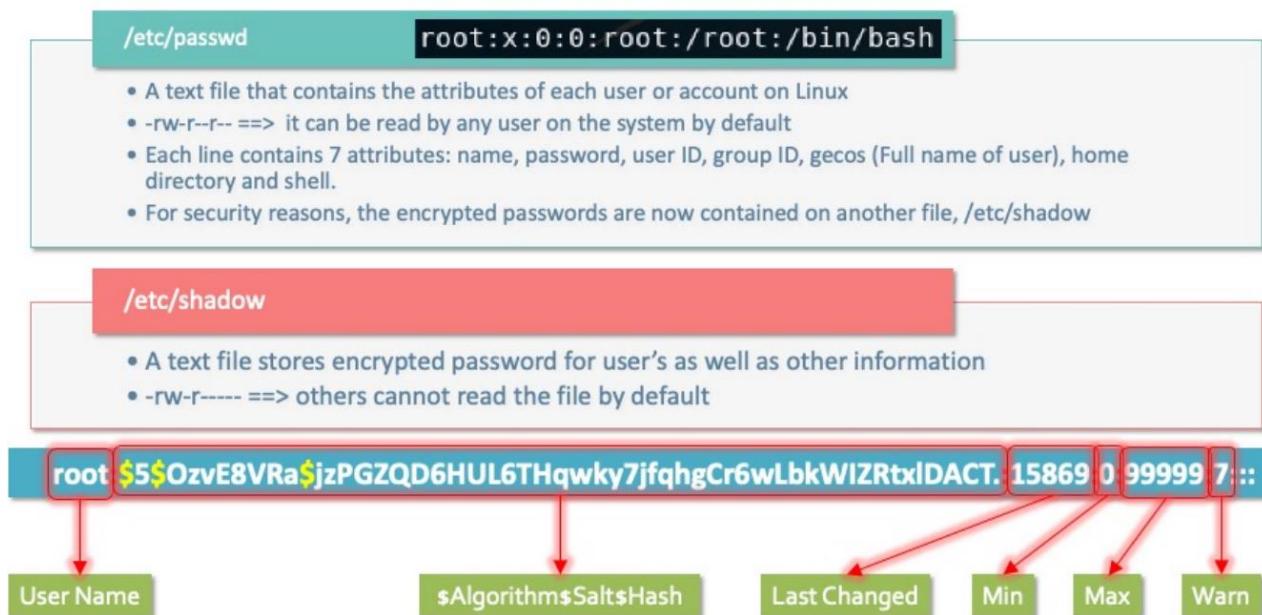
Real Time Operating Systems

- Scientific & industrial systems

Not: Linux'ta yapılandırma dosyaları **/etc** dizininde yer alır.

Parolalar açık olmayan şekilde muhafaza edilmelidir.

“passwd” parola dosyası 7 sütunludur.



User Management Commands

Kod	Maksadı
adduser	kullanıcı oluşturma
addgroup	grup oluşturma
deluser	kullanıcı silme
delgroup	Grup silme
chown	Dosya sahibini ve grubu değiştirme
id user	Kullanıcı Id'lerini sergileme
su -	(süper user) root kullanıcının yetkilerini kullanmaya izin verdiği kullanıcılar root yetki komutlarını kullanabilmesi için bu komutu yazmalıdır.
usermod	Kullanıcı yetkisini değiştirme veya grup ataması
groups	İlgili kullanıcı grubunu sergileme
sudoers file	Root kullanıcısında etc/sudoers adlı dosyaya sudo yetkisinin verildiği hesapları eklemeliyiz. Bunun yerine root kullanıcısı ilgili kullanıcıyı usermod komutuyla ile sudo grubuna dahil eder

Parolalar shadow dosyasında kriptolu olarak kayıtlıdır. Shell tipine göre algoritma farklı çalışır.

6 sütundur.

- User name
- Kriptolanmış parola
- Son değişiklik
- Min: parola değişimi için beklenmesi gereken min gün sayısı
- Max: Aynı parolayı kullanabileceği max gün sayısı
- Uyarı: Max (Parola değişimine) kaç gün kala uyarı verileceği

Portlarla çıkış yapan her servis için farklı kullanıcı kayıtları açılır.

less /etc/passwd ➔

cat /etc/shadow ➔ bunu sadece root kullanıcı açabilir.

Şifresiz kayıtların şifre kısmında “*” (yıldız) var. “!” (ünlem) de olabilir.

```
root@kali:~# less /etc/passwd
root@kali:~# cat /etc/shadow
root:$1$QIaXvaY9$Y2Gca/W3Y3zVGSWZPloB7
daemon:*:18290:0:99999:7 :::
bin:*:18290:0:99999:7 :::
sys:*:18290:0:99999:7 :::
sync:*:18290:0:99999:7 :::
games:*:18290:0:99999:7 :::
man:*:18290:0:99999:7 :::
lp:*:18290:0:99999:7 :::
mail:*:18290:0:99999:7 :::
news:*:18290:0:99999:7 :::
uucp:*:18290:0:99999:7 :::
proxy:*:18290:0:99999:7 :::
www-data:*:18290:0:99999:7 :::
backup:*:18290:0:99999:7 :::
list:*:18290:0:99999:7 :::
irc:*:18290:0:99999:7 :::
gnats:*:18290:0:99999:7 :::
nobody:*:18290:0:99999:7 :::
_apt:*:18290:0:99999:7 :::
systemd-timesync:*:18290:0:99999:7 :::
systemd-network:*:18290:0:99999:7 :::
systemd-resolve:*:18290:0:99999:7 :::
mysql:!:18290:0:99999:7 :::
tss:*:18290:0:99999:7 :::
strongswan:*:18290:0:99999:7 :::
ntp:*:18290:0:99999:7 :::
messagebus:*:18290:0:99999:7 :::
redsocks!:18290:0:99999:7 :::
rwhod:*:18290:0:99999:7 :::
```

Kullanıcı ekleme komutu (root yetkisinde olanlar açabilir)

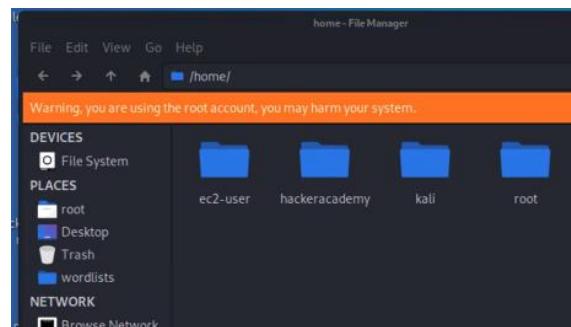
adduser ➔ direkt çalışmaz çünkü komuta ulaşamadı

su - ➔ kullanıcının yetkisini root yaptı.

Echo #path ➔ patha ulaştık. demekki root yetkili olduk.

Adduser ➔ hata verdi ama yol doğru

adduser hackeracademy ➔ Çalıştı ve yeni bir kullanıcı eklendi.
/home/hackeracademy dosyasının olduğunu gördük. Yeni bir grup da oluşturuyor.



su hackeracademy ➔ - (tire) olmadan yazımı. Kullanıcı oluştururuz ve root dizininden çıkmamış oluruz. İşler karışabilir.

printenv ➔ burada bilgiler root kullanıcı bilgileriyle karışmış olabilir.

su ➔ bu şekilde yazarsak parola girilmesi için parola yazan bir satır gelir.

sanal makine sayfası altında "i" (info) veya try hack me sitesi (<https://tryhackme.com/my-machine>) makine bilgilerinden parola bulunabilir.



```
File Actions Edit View Help
root@kali:~# adduser
bash: adduser: command not found
root@kali:~# su -
root@kali:~# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
root@kali:~# adduser
adduser: Only one or two names allowed.
root@kali:~# adduser hackeracademy
Adding user `hackeracademy' ...
Adding new group `hackeracademy' (1002) ...
Adding new user `hackeracademy' (1002) with group `hackeracademy' ...
Creating home directory `/home/hackeracademy' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for hackeracademy
Enter the new value, or press ENTER for the default
    Full Name []: huriye
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n]
root@kali:~# tail -n1 /etc/passwd
hackeracademy:x:1002:1002:huriye,,,:/home/hackeracademy:/bin/bash
```

su - hackeracademy → bu şekilde de kullanıcı oluştururuz ve ilgili kullanıcı home dizinine geçer.

printenv → kullanıcıyla ilgili bilgiler gelir

```
root@kali:~# su - hackeracademy
hackeracademy@kali:~$ printenv
SHELL=/bin/bash
PWD=/home/hackeracademy
LOGNAME=hackeracademy
HOME=/home/hackeracademy
LANG=en_US.UTF-8
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;
31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;
31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;
31:*.txz=01;31:*.tzo=01;31:*.tz=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:
*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mpg=01;35:*.mpeg=01;35:
*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:
*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;
35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;
35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;
1;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;
35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;
36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;
36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
TERM=xterm-256color
USER=hackeracademy
SHLVL=1
PATH=/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/usr/local/games:/usr/games
MAIL=/var/mail/hackeracademy
_=~/usr/bin/printenv
```

Root dizini için **printenv** yaptığımda root kullanıcı bilgilerini görebiliriz. Yeni açtığımız hesabı – (tire) kullanarak açtığımız terminalin bilgileri ile ayrı olduğunu (olması gereken budur) gördük- ISLER YOLUNDA

```
File Actions Edit View Help
root@kali:~# printenv
SHELL=/bin/bash
SESSION_MANAGER=local/kali:@/tmp/.ICE-unix/935,unix/kali:/tmp/.ICE-unix/935
5
WINDOWID=0
QT_ACCESSIBILITY=1
XDG_CONFIG_DIRS=/etc/xdg
XDG_MENU_PREFIX=xfce-
LANGUAGE=
SSH_AUTH_SOCK=/tmp/ssh-tVa8te5HLcCF/agent.935
DESKTOP_SESSION=xfce
SSH_AGENT_PID=978
XKL_XMODMAP_DISABLE=1
PWD=/root
LOGNAME=root
QT_QPA_PLATFORMTHEME=qt5ct
XDG_SESSION_TYPE=x11
PANEL_GDK_CORE_DEVICE_EVENTS=0
HOME=/root
LANG=en_US.UTF-8
XDG_CURRENT_DESKTOP=XFCE
VNCDESKTOP=kali:1 (root)
TERM=xterm-256color
COLORFGBG=15;0
DISPLAY=:1.0
SHLVL=2
XDG_RUNTIME_DIR=/home//.cache/xdg
QT_AUTO_SCREEN_SCALE_FACTOR=0
XDG_DATA_DIRS=/usr/share/xfce4:/usr/local/share/:/usr/share/:/usr/share
PATH=/usr/bin:/bin
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-Yfq23a3cRf,guid=1c9a474cf18fb6432e53f3b5619536c3
```

Göründüğü gibi root olmayan kullanıcının grup ekleme yetkisi yok.

```
File Actions Edit View Help  
hackeracademy@kali:~$ addgroup  
addgroup: Only root may add a user or group to the system.
```

Sudo adduser new ➔ HATA! sudo komutu ile root olmayan kullanıcının da root kullanıcıya özel kodları çalışma yetkisi olur. Ancak Root hesabında iken hangilerin sudo yetkisini kullanacağını belirtmiş olmalıyız. O yüzden bu kodla da user ekleyemedik.

Sudo : süper user do

```
[sudo] password for hackeracademy:  
hackeracademy is not in the sudoers file. This incident will be reported.  
hackeracademy@kali:~$ █
```

/etc/sudoers : Root dizininde ilgili dosyaya bu yetkinin (sudo) verildiği hesapları eklemeliyiz.

Bu dizini aşağıdaki kodla bulabiliriz.

Locate sudoers ➔ birçok dosya çıktı ama ilk dosya bizim hedefimiz.

```
File Actions Edit View Help  
root@kali:~# locate sudoers  
/etc/sudoers  
/etc/sudoers.d  
/etc/sudoers.d/90-cloud-init-users  
/etc/sudoers.d/README  
/etc/sudoers.d/kali-grant-root  
/usr/bin/cvtsudoers  
/usr/lib/sudo/sudoers.la  
/usr/lib/sudo/sudoers.so  
/usr/share/doc/sudo/examples/sudoers.dist  
/usr/share/doc/sudo/examples/sudoers.gz  
/usr/share/locale/ast/LC_MESSAGES/sudoers.mo  
/usr/share/locale/ca/LC_MESSAGES/sudoers.mo  
/usr/share/locale/cs/LC_MESSAGES/sudoers.mo  
/usr/share/locale/da/LC_MESSAGES/sudoers.mo  
/usr/share/locale/de/LC_MESSAGES/sudoers.mo  
/usr/share/locale/el/LC_MESSAGES/sudoers.mo  
/usr/share/locale/eo/LC_MESSAGES/sudoers.mo  
/usr/share/locale/eu/LC_MESSAGES/sudoers.mo  
/usr/share/locale/fi/LC_MESSAGES/sudoers.mo  
/usr/share/locale/fr/LC_MESSAGES/sudoers.mo  
/usr/share/locale/fur/LC_MESSAGES/sudoers.mo
```

Nano /etc/sudoers ➔ hedef dosyayı root kullanıcı ile açmalıyız ve nano text editörü ile açıp gerekli değişikliği yapmalıyız.

Şimdilik bunu yapmayalım. İşleri karıştırabiliriz.

Dosyanın içine girmeden terminal komutuyla sudo yetkisi verilebilecek hesabı tanımlayabiliriz

su - ➔ bu kodla root yetkilerini tekrar ele almış oluruz.

usermod -g sudo hackeracademy ➔ hackeracademy kullanıcısına sudo yetkisi verdik.

```
root@kali:~# usermod -g sudo hackeracademy
bash: usermod: command not found
root@kali:~# su -
root@kali:~# usermod -g sudo hackeracademy
root@kali:~# █
```

Sudo adduser new ➔ artık hackeracademy kullanıcısı sudo yetkisine sahip, çünkü yeni kullanıcı ekleyebildi. Root tarafından bu yetki tanınmadan önce bu kullanıcı user ekleyememişti.

Dikkat: her zaman root yetkilerini kullandığımız her komutun başına “sudo” komutunu yazmalıyız.

```
hackeracademy@kali:~$ sudo adduser new
[sudo] password for hackeracademy:
Adding user `new' ...
Adding new group `new' (1003) ...
Adding new user `new' (1003) with group `new' ...
Creating home directory `/home/new' ...
Copying files from `/etc/skel' ...
New password: █
```

addgroup badgers ➔ HATA! sudo kodu olmadan çalışmadı.

sudo addgroup badgers ➔ badgers grubu oluştı.

groups hackeracademy ➔ kullanıcının hangi grupta olduğunu görebiliriz.

sudo usermod -g badgers hackeracademy ➔ hackeracademy badgers grubuna ekledik. g (küçük) ile önceki gruptan çıkarır

groups hackeracademy ➔ kullanıcının badgers grubuna dahil olduğunu görebiliriz.

id ➔ terminalin açık olduğu kullanıcının dahil olduğunu tüm grupları görebiliriz.

id hackeracademy ➔ belirtilen kullanıcının dahil olduğunu tüm grupları görebiliriz.

```

File Actions Edit View Help
hackeracademy@kali:~$ addgroup badgers
addgroup: Only root may add a user or group to the system.
hackeracademy@kali:~$ sudo addgroup badgers
Adding group `badgers' (GID 1004) ...
Done.
hackeracademy@kali:~$ groups hackeracademy
hackeracademy : sudo
hackeracademy@kali:~$ usermod -g badgers hackeracademy
usermod: Permission denied.
usermod: cannot lock /etc/passwd; try again later.
hackeracademy@kali:~$ sudo usermod -g badgers hackeracademy
hackeracademy@kali:~$ groups hackeracademy
hackeracademy : badgers
hackeracademy@kali:~$ id
uid=1002(hackeracademy) gid=1002(hackeracademy) groups=1002(hackeracademy)
hackeracademy@kali:~$ id hackeracademy
uid=1002(hackeracademy) gid=1004(badgers) groups=1004(badgers)

```

Root dizininde iken

addgroup hacktivist ➔

usermod -a -G hacktivist hackeracademy ➔ Kullanıcıyı önceki gruptan çıkmadan bu gruba da ekleme

“**g**” (küçük) : kullanıcıyı bir önceki gruptan çıkarabilir , eni gruba dahil eder.

a append : kullanıcıyı birden fazla kullanıcı grubuna dahil etme **G** (büyük) ile kullanılır

“**G**” (büyük) birden fazla grup aynı anda oluşturabiliriz.

-g, --gid GROUP

The group name or number of the user's new initial login group. The group must exist.

Any file from the user's home directory owned by the previous primary group of the user will be owned by this new group.

The group ownership of files outside of the user's home directory must be fixed manually.

-G, --groups GROUP1[,GROUP2,...[,GROUPN]]

A list of supplementary groups which the user is also a member of. Each group is separated from the next by a comma, with no intervening whitespace. The groups are subject to the same restrictions as the group given with the **-g** option.

If the user is currently a member of a group which is not listed, the user will be removed from the group. This behaviour can be changed via the **-a** option, which appends the user to the current supplementary group list.

Kullanıcı silme

Sudo deluser new → new kullanıcısını siler.

Tail -n1 /etc/passwd → görüldüğü gibi new kullanıcı silinmiş

Man deluser → silinen kullanıcının dizinlerini de silme komutu

```
hackeracademy@kali:~$ sudo deluser new
Removing user 'new' ...
Warning: group 'new' has no more members.
Done.
hackeracademy@kali:~$ tail -n1 /etc/passwd
hackeracademy:x:1002:1005:huriye,,,:/home/hackeracademy:/bin/bash
```

#chown

DOSYA SAHİBİNİ VE GRUBU DEĞİŞTİRME

#chown

- change file owner and group

Common Usage

- #chown [owner]:[group] fileName

```
root@kali:~/temp# ls -l
total 0
-rw-r--r-- 1 root root 0 Jun 15 02:24 myFile
root@kali:~/temp#
root@kali:~/temp# chown nobody:games myFile
root@kali:~/temp#
root@kali:~/temp# ls -l
total 0
-rw-r--r-- 1 nobody games 0 Jun 15 02:24 myFile
```

Touch newFile → newFile oluşturduk.

sudo chown root : root newFile → dosyanın sahip kullanıcı bilgilerini değiştirdik.

ls -l → dosyanın sahip kullanıcı bilgilerini değiştirdiğini gördük.

ilk kısım kullanıcı, 2. kısım grup adıdır. On göre sadece birini değiştirebiliriz.

sudo chown hackracademy newFile → kullanıcıyı değiştirip grubu bırakma.

sudo chown :badgers newFile → sadece grubu değiştirme : (iki nokta üst üste) sonrası yazarak grub değiştirdiğimizi belirtmiş oluyoruz.

```

hackeracademy@kali:~$ ls
hackeracademy@kali:~$ touch newFile
hackeracademy@kali:~$ ls -l
total 0
-rw-r--r-- 1 hackeracademy badgers 0 Nov 17 20:40 newFile
hackeracademy@kali:~$ chown root:root newFile
chown: changing ownership of 'newFile': Operation not permitted
hackeracademy@kali:~$ sudo chown root:root newFile
hackeracademy@kali:~$ ls -l      I
total 0
-rw-r--r-- 1 root root 0 Nov 17 20:40 newFile
hackeracademy@kali:~$ chown hackeracademy newFile
chown: changing ownership of 'newFile': Operation not permitted
hackeracademy@kali:~$ sudo chown hackeracademy newFile
hackeracademy@kali:~$ ls -l
total 0
-rw-r--r-- 1 hackeracademy root 0 Nov 17 20:40 newFile
hackeracademy@kali:~$ sudo chown :badgers newFile
hackeracademy@kali:~$ ls -l
total 0
-rw-r--r-- 1 hackeracademy badgers 0 Nov 17 20:40 newFile

```

Not: Bir grup ve yetkileri belirlenip bu gruba dahil olanların belirtilen yetkilere sahip olması sağlanabilir

18.11.2021 Thursday

YENİ KULLANICI OLUSTURMA VE YETKILENDIRME

Yetkisiz kullanıcıların yetkili (root) yetkilerini nasıl kullanabileceğini (örneğin /sbin dizin dosyaları) görmüştük. Bu yetkiler kullanıcı oluşturma, grup oluşturma veya kullanıcıyı bir gruba ekleme vb işlemleri içerir. Bu yetkiyi önce yetkili hesabında tanımlamalıyız. Bu da yetki verilen hesabın sudo grubuna dahil edilmesiyle mümkün oluyor. Daha sonra yetki verilen hesabın kendisine tanınan yetki gereği çalıştırabileceği kodun başına sudo yazarak ilgili kodu çalıştırabilecektir.

Root kullanıcısında da bazı komutlar PATH 'de tanımlamayınca çalıştırılamayabiliyoruz.

su - →

echo \$PATH → artık tüm yetkileri çalıştırabilirim

adduser new → new adlı yeni bir kullanıcı oluştur.

Bu komut çalışınca;

Aynı zamanda aynı isimle grup da oluşur.

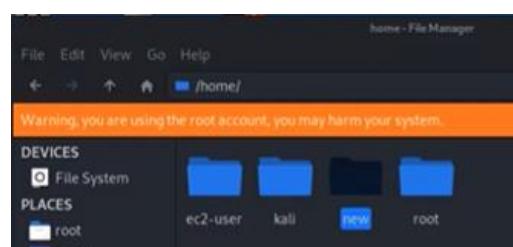
User Id Grup Id (1002) sergilendir.

Terminalde yeni kullanıcı için parola oluşturulması gerekiği bilgileri görünürmektedir.

Parola girilir.

Daha sonra Full name, Room Number, Work ve Home Phone bilgileri ve diğer bilgiler istenirse girilebilir.

En son Y (YES) tuşıyla ve direkt enter tuşıyla işlem tamamlanır.



Home dizinine baktığımızda new kullanıcı dosya olduğunu görebiliriz.

tail -n1 /etc/passwd → Bu kullanıcı bilgileri /etc/passwd dosyasına en son satır olarak ta eklenir. Bu komutla terminale gelen bilgilerde görüldüğü gibi yeni kullanıcı bilgileri eklenmiş. Hatırlanacağı üzere passwd dosyasında bilgiler açık olarak görülür. **/etc/shadow** klasöründe ise parola bilgisi kriptolu olarak kayıtlıdır.

Su - new → bu komuta new kullanıcısının dizinine geçiyor (parola istemeden). Terminalde bulunulan dizinden new kullanıcısında olduğumuzu görebiliyoruz. Ancak bazı terminallerde bulunulan dizin görülemiyor. Bu durumda kullanıcayı **whoami** komutuyla öğrenebiliriz.

Whoami → kullanıcı adını sergiler

Pwd → bulunduğuumuz dizini gördük

adduser yeni → **HATA!!!!!** Bu şekilde kullanıcı oluşturmaya izinli tek yetkili root kullanıcısıdır.

Sudo adduser yeni → **HATA!!!!!** new kullanıcı yetkisi henüz kullanıcı oluşturmaya izinli değil.

Root olmayan bir kullanıcıda iken terminale **exit** yazılırsa ilgili kullanıcı dizininden çıkarılır ve root dizinine geçilir. Root dizinine geçip orada new kullanıcısını sudo grubuna ekleyip kullanıcı ekleme vb yetkilere sahip olmasını sağlayacağız.

usermod -aG root new → Root kullanıcıyı new kullanıcıyı üyesi olduğu diğer grplardan çıkarmadan sudo grubuna ekledi.

```
root@kali:~# adduser new
Adding user 'new' ...
Adding new group 'new' (1002) ...
Adding new user 'new' (1002) with group 'new' ...
Creating home directory '/home/new' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for new
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:~# tail -n1 /etc/passwd
new:x:1002:1002:,:/home/new:/bin/bash
root@kali:~# su - new
new@kali:~$ whoami
new
new@kali:~$ pwd
/home/new
```

```
new@kali:~$ adduser yeni
adduser: Only root may add a user or group to the system.
new@kali:~$ sudo adduser yeni
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for new:
new is not in the sudoers file. This incident will be reported.

File Actions Edit View Help
new@kali:~$ exit
logout
root@kali:~# █
```

Nano /etc/sudoers → açılan text editörde kullanıcı ve grup ayarlarını yapabilirim.

Addgroup badgers → yeni grup tanımladık.

usermod -a -G badgers new →

Kullanıcıyı önceki gruptan çıkmadan bu gruba dahil ettik.

id new → kullanıcıları gördük.

```
root@kali:~# addgroup badgers
Adding group `badgers' (GID 1003) ...
Done.
root@kali:~# usermod -aG badgers new
root@kali:~# groups new
new : new sudo badgers
root@kali:~# id new
uid=1002(new) gid=1002(new) groups=1002(new),27(sudo),1003(badgers)
root@kali:~# █
```

less /etc/group ➔ açılan bilgilerden grupları ve kullanıcıları görebiliriz.

less /etc/group | grep sudo ➔ grupları ve kullanıcı bilgilerinden "sudo" gecen satırı yakalayıp görebiliriz.

```
root@kali:~# less /etc/group
root@kali:~# less /etc/group | grep sudo
sudo:x:27:kali,ec2-user,new
root@kali:~#
```

```
ge0ctac:x:140:
lightdm:x:141:
kpadmins:x:142:
kali:x:1000:
systemd-coredump:x:999:
nvpd:x:143:
ec2-user:x:1001:
xrdp:x:144:
debian-tor:x:145:
new:x:1002:
badgers:x:1003:new
(END)
```

Adduser user sudo ➔ bu komutla yeni bir kullanıcı ekler ve belirtilen grub'a dahil eder ancak try hack me sanal Linux OS'te çalışmadı (kullanıcı oluştururken grub'a da dahil etmek)

usermod -aG hacktivist new ➔ Kullanıcıyı (hacktivist) önceki gruptan çıkmadan bu grub'a (new) dahil ettik.

```
root@kali:~# su -
root@kali:~# adduser user sudo
adduser: The user 'user' does not exist.
root@kali:~# addgroup hacktivist
Adding group 'hacktivist' (GID 1004) ...
Done.
root@kali:~# usermod -aG hacktivist new
root@kali:~# id new
uid=1002(new) gid=1002(new) groups=1002(new),27(sudo),1003(badgers),1004(hacktivist)
root@kali:~#
```

usermod -aG root new ➔ Kullanıcıyı (new) önceki gruptan çıkmadan bu grub'a (root) dahil ettik.
Su -new ➔ new kullanıcı dizinine geçtik.

Adduser ikinci ➔ çalışmadı.

sudo adduser ikinci ➔ Çalıştı. Demek ki root grubuna dahil edilen bir kullanıcı dizininde iken root gibi komut yazılmıyor. Yine sudo yazılmalıdır.

```
root@kali:~# usermod -aG root new
root@kali:~# groups new
new : new root sudo badgers hacktivist
root@kali:~# su - new
new@kali:~$ adduser ikinci
adduser: Only root may add a user or group to the system.
new@kali:~$ sudo adduser ikinci
[sudo] password for new:
Adding user `ikinci' ...
Adding new group `ikinci' (1005) ...
Adding new user `ikinci' (1003) with group `ikinci' ...
Creating home directory `/home/ikinci' ...
Copying files from `/etc/skel' ...
New password:
```

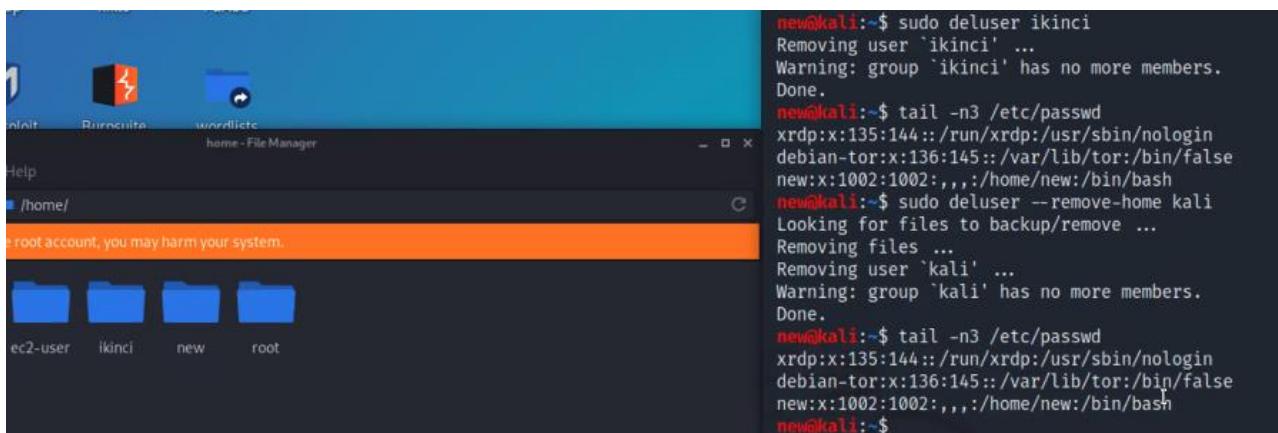
Sudo deluser ikinci ➔ kullanıcı siler

Dizin silinmedi ama kullanıcı silindi

Sudo rm -rf /home/ikinci ➔ alt dizinleriyle beraber belirtilen dizini siler

Yukarıda iki komut yerine aşağıdaki komutla kullanıcıyı ve dizinlerini silebiliriz.

Sudo deluser--remove -home kali ➔ dizinleriyle beraber kullanıcıyı siler.



```
new@kali:~$ sudo deluser ikinci
Removing user 'ikinci' ...
Warning: group 'ikinci' has no more members.
Done.
new@kali:~$ tail -n3 /etc/passwd
xrdp:x:135:144::/run/xrdp:/usr/sbin/nologin
debian-tor:x:136:145::/var/lib/tor:/bin/false
new:x:1002:1002:,:/home/new:/bin/bash
new@kali:~$ sudo deluser --remove-home kali
Looking for files to backup/remove ...
Removing files ...
Removing user 'kali' ...
Warning: group 'kali' has no more members.
Done.
new@kali:~$ tail -n3 /etc/passwd
xrdp:x:135:144::/run/xrdp:/usr/sbin/nologin
debian-tor:x:136:145::/var/lib/tor:/bin/false
new:x:1002:1002:,:/home/new:/bin/bash
new@kali:~$
```

2.5 Linux File System

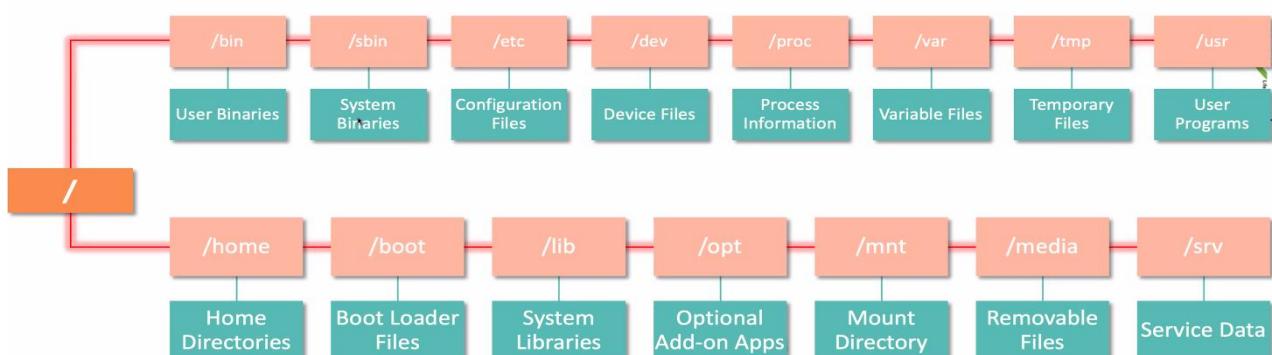
Linux File Hierarchy

Linux OS'te dizin ve dosya yapısı esastır. Windows OS'teki gibi C disk yapısı yoktur.

Linux File System is in tree structure

"/" represents the root folder

Other folders and files are like branches and leafs



/bin/ : kullanıcı ve sistem ayarları (komut dosyaları)

/sbin/ : sistem ayarları (Gizli)

/etc/ : Konfigürasyon dosyaları (app'ların çalışma ayarları) // Admin deyine etc gelsin

/dev/ : Dihaz dosyaları

/proc/ : Süreç bilgileri bu dizinde iken **cat meminfo** komutuyla ilgili dosya (hafıza) açılır
meminfo: hafıza bilgileri

Uptime : sistemin çalışma süresi

- /var** : değişken dosyaları
Log : loglar (sürekli değişir). İşlevle göre farklı loglar vardır. Kapasitesi dolunca ilgili log için başka bir log oluşur (1,2,3,...) Log kayıtları bu süre sonra silinir
- /tmp** : Geçici dosyalar
Cash'teki dosyalarıdır. Belirli bir süre sonra silinir.
- /usr** : Kullanıcı programları
Kaynak, kütüphane (kullanıcı) alt dizinleri var
- /home/** : Home dizini
- /boot/** : İlk çalışma dosyaları (Kernel'a ait dosyalar) Normalde değişmez. Listeleyince değişim tarihlerinden hacklendigimiz anlaşılabilir
- /lib** : Sistem kütüphaneleri
- /opt/** : Opsiyonel add on apps
- /mnt/** : Mount dizini
Linux, bir çok farklı dosya sistemi ile çalışmak üzere tasarlanmıştır. Farklı dosya sistemleri işletim sistemine mount komutu ile tanıtılır. (Bağlantı sağlanır). Bazı programlar diğer programların üzerine çalışır. Buna "mounted on" denir.
- /media/** : Çıkarılabilir dosyalar
- /srv/** : Service data
Burada sadece "tftp" adlı protokol mevcut

cd /bin/ ➔ change directory to binary

ls | more ➔ listeledik.
veya

ls | /bin/ | more ➔ belirtilen dizini more ile açtık. (yukarıdaki iki komut yerine)

Not: more ile açılan listede

"Space" tuşunda sayfa sayfa ilerler.
"Enter" tuşu ile daha yavaş ilerler
"q" çıkış

```
-rwxr-xr-x 1 root root          63440 Jan  5 2019 atk6-flood_mldrouter6
-rwxr-xr-x 1 root root          63440 Jan  5 2019 atk6-flood_redir6
-rwxr-xr-x 1 root root         71632 Jan  5 2019 atk6-flood_router26
-rwxr-xr-x 1 root root         63440 Jan  5 2019 atk6-flood_router6
-rwxr-xr-x 1 root root         63440 Jan  5 2019 atk6-flood_rs6
-rwxr-xr-x 1 root root         63440 Jan  5 2019 atk6-flood_solicit6
-rwxr-xr-x 1 root root         63440 Jan  5 2019 atk6-flood_unreach6
-rwxr-xr-x 1 root root        67536 Jan  5 2019 atk6-four2six
-rwxr-xr-x 1 root root       96208 Jan  5 2019 atk6-fragmentation6
-rwxr-xr-x 1 root root       75728 Jan  5 2019 atk6-fragrouter6
-rwxr-xr-x 1 root root       81648 Jan  5 2019 atk6-fuzz_dhcp6
-rwxr-xr-x 1 root root       77552 Jan  5 2019 atk6-fuzz_dhcps6
-rwxr-xr-x 1 root root      78000 Jan  5 2019 atk6-fuzz_ip6
-rwxr-xr-x 1 root root     100304 Jan  5 2019 atk6-implementation6
-rwxr-xr-x 1 root root      63440 Jan  5 2019 atk6-implementation6d
-rwxr-xr-x 1 root root      67536 Jan  5 2019 atk6-inject_alive6
--More--
```

sbin : sistem ayarları

ls /sbin/ | more ➔ belirtilen listeyi more ile sergilettik.

terminalde /bin/ dizininde iken

file ./cd ➔ dosyanın tipini sergiler.

file ./zcat ➔ dosyanın tipini sergiler.

```
root@kali:/boot# ls -l
total 162680
-rw-r--r-- 1 root root 223598 Jan  6 2020 config-5.4.0-kali2-amd64
-rw-r--r-- 1 root root 223599 Jan 20 2020 config-5.4.0-kali3-amd64
-rw-r--r-- 1 root root 229433 Aug 26 2020 config-5.7.0-kali3-amd64
drwxr-xr-x 5 root root 4096 Sep  2 2020 grub
-rw-r--r-- 1 root root 38295335 Jan 29 2020 initrd.img-5.4.0-kali2-amd64
-rw-r--r-- 1 root root 38761051 Aug 15 2020 initrd.img-5.4.0-kali3-amd64
-rw-r--r-- 1 root root 60499060 Sep  2 2020 initrd.img-5.7.0-kali3-amd64
-rw-r--r-- 1 root root 3624398 Jan  6 2020 System.map-5.4.0-kali2-amd64
-rw-r--r-- 1 root root 3626147 Jan 20 2020 System.map-5.4.0-kali3-amd64
-rw-r--r-- 1 root root 4199198 Aug 26 2020 System.map-5.7.0-kali3-amd64
-rw-r--r-- 1 root root 5618048 Jan  6 2020 vmlinuz-5.4.0-kali2-amd64
-rw-r--r-- 1 root root 5626240 Jan 20 2020 vmlinuz-5.4.0-kali3-amd64
-rw-r--r-- 1 root root 5624992 Aug 26 2020 vmlinuz-5.7.0-kali3-amd64
```

File Permissions

Owner : Dosyayı oluşturan useri ifade eder (sağ üsteki terminal görüntüsünde ilk sütun).

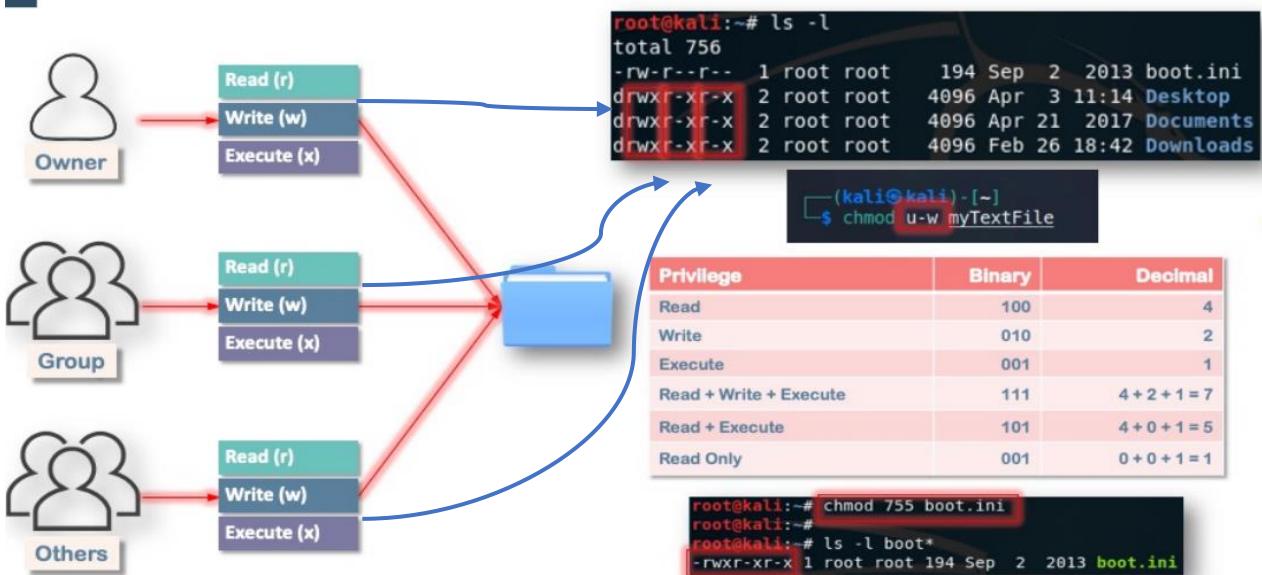
Group : Dosyanın grubunda olan user'leri ifade ediyor.

Other : Owner ve gruba dahil olmayan diğer user'lari ifade eder.

Sağ üsteki terminal görüntüsünde owner yetkileri ilk sütun, grup yetkileri 2., others yetkileri 3. sütundadır

Aşağıdaki **sağ üst** taraftaki örnekte write yetkisi sadece owner'da, read ve execute yetkisi herkeste.

Aşağıdaki **sağ alt** taraftaki örnekte write yetkisi sadece owner'da, execute yetkisi herkeste, read yetkisi owner ve group üyelerinde



Dosya Erişim Yetkisi Değiştirme/Belirleme

#chmod

“u” user (owner)

“g” group

“o” others

7= (rwx) read+write+execute

6= (rw-) read+write

5= (r-x) read+execute

4= (r-) read

3= (-wx) write+ execute

2= (-w-) write

1= (--x) execute

0= (---) null (hiçbiri)

```
root@kali:~# ls -l
total 40
drwxr-xr-x 3 root root 4096 May 14 2020 Desktop
drwxr-xr-x 3 root root 4096 May 13 2020 Documents
drwxr-xr-x 2 root root 4096 Feb 5 2020 Downloads
-rw----- 1 root root 262 Nov 18 19:54 log.txt
drwxr-xr-x 2 root root 4096 Feb 5 2020 Music
drwxr-xr-x 2 root root 4096 Feb 5 2020 Pictures
drwxr-xr-x 2 root root 4096 Feb 5 2020 Public
drwxr-xr-x 2 root root 4096 Feb 5 2020 Templates
drwxr-xr-t 2 root root 4096 Feb 5 2020 thinclient_drives
drwxr-xr-x 2 root root 4096 Feb 5 2020 Videos
root@kali:~# chmod 630 log.txt
root@kali:~# ls -l
total 40
drwxr-xr-x 3 root root 4096 May 14 2020 Desktop
drwxr-xr-x 3 root root 4096 May 13 2020 Documents
drwxr-xr-x 2 root root 4096 Feb 5 2020 Downloads
-rw---- 1 root root 262 Nov 18 19:54 log.txt
drwxr-xr-x 2 root root 4096 Feb 5 2020 Music
drwxr-xr-x 2 root root 4096 Feb 5 2020 Pictures
drwxr-xr-x 2 root root 4096 Feb 5 2020 Public
drwxr-xr-x 2 root root 4096 Feb 5 2020 Templates
drwxr-xr-t 2 root root 4096 Feb 5 2020 thinclient_drives
drwxr-xr-x 2 root root 4096 Feb 5 2020 Videos
root@kali:~#
```

chmod 630 log.txt ➔ log.txt icin verilen yetkiler

user'a read-write (6)

group'a write -execute (3)

others'a null (0)

chmod 755 log.txt ➔ log.txt icin verilen yetkiler

user'a read-write-execute (7)

group'a read -execute (5)

others'a read -execute (5)

chmod u 5 log.txt ➔ log.txt icin user'a read ve execute yetkisi tanindi

chmod g 3 log.txt ➔ log.txt icin grup'a write ve execute yetkisi tanindi

chmod o 0 log.txt ➔ log.txt icin others icin tüm yetkiler kaldırıldı.

chmod u-w log.txt → aşağıda görüldüğü gibi log.txt için yazma yetkisi user için kaldırıldı

chmod g +w log.txt → aşağıda görüldüğü gibi log.txt için yazma yetkisi group için verildi

chmod o+w log.txt → aşağıda görüldüğü gibi log.txt için yazma yetkisi others için verildi

chmod o-wrx log.txt → aşağıda görüldüğü gibi log.txt'de tüm yetkisi others için kaldırıldı

```
root@kali:~# ls -l
total 40
drwxr-xr-x 3 root root 4096 May 14 2020 Desktop
drwxr-xr-x 3 root root 4096 May 13 2020 Documents
drwxr-xr-x 2 root root 4096 Feb 5 2020 Downloads
-rw-r--r-- 1 root root 245 Nov 18 16:56 log.txt
drwxr-xr-x 2 root root 4096 Feb 5 2020 Music
drwxr-xr-x 2 root root 4096 Feb 5 2020 Pictures
drwxr-xr-x 2 root root 4096 Feb 5 2020 Public
drwxr-xr-x 2 root root 4096 Feb 5 2020 Templates
drwxr-xr-t 2 root root 4096 Feb 5 2020 thinclient_drives
drwxr-xr-x 2 root root 4096 Feb 5 2020 Videos
root@kali:~# su -
root@kali:~# chmod u-w log.txt
root@kali:~# ls -l
total 40
drwxr-xr-x 3 root root 4096 May 14 2020 Desktop
drwxr-xr-x 3 root root 4096 May 13 2020 Documents
drwxr-xr-x 2 root root 4096 Feb 5 2020 Downloads
-r--r--r-- 1 root root 245 Nov 18 16:56 log.txt
drwxr-xr-x 2 root root 4096 Feb 5 2020 Music
drwxr-xr-x 2 root root 4096 Feb 5 2020 Pictures
drwxr-xr-x 2 root root 4096 Feb 5 2020 Public
drwxr-xr-x 2 root root 4096 Feb 5 2020 Templates
drwxr-xr-t 2 root root 4096 Feb 5 2020 thinclient_drives
drwxr-xr-x 2 root root 4096 Feb 5 2020 Videos
```

```
root@kali:~# chmod g+w log.txt
root@kali:~# ls -l
total 40
drwxr-xr-x 3 root root 4096 May 14 2020 Desktop
drwxr-xr-x 3 root root 4096 May 13 2020 Documents
drwxr-xr-x 2 root root 4096 Feb 5 2020 Downloads
-r--rw-r-- 1 root root 262 Nov 18 19:54 log.txt
drwxr-xr-x 2 root root 4096 Feb 5 2020 Music
drwxr-xr-x 2 root root 4096 Feb 5 2020 Pictures
drwxr-xr-x 2 root root 4096 Feb 5 2020 Public
drwxr-xr-x 2 root root 4096 Feb 5 2020 Templates
drwxr-xr-t 2 root root 4096 Feb 5 2020 thinclient_drives
drwxr-xr-x 2 root root 4096 Feb 5 2020 Videos
root@kali:~# chmod o-r log.txt
root@kali:~# ls -l
total 40
drwxr-xr-x 3 root root 4096 May 14 2020 Desktop
drwxr-xr-x 3 root root 4096 May 13 2020 Documents
drwxr-xr-x 2 root root 4096 Feb 5 2020 Downloads
-r--rw-r-- 1 root root 262 Nov 18 19:54 log.txt
drwxr-xr-x 2 root root 4096 Feb 5 2020 Music
drwxr-xr-x 2 root root 4096 Feb 5 2020 Pictures
drwxr-xr-x 2 root root 4096 Feb 5 2020 Public
drwxr-xr-x 2 root root 4096 Feb 5 2020 Templates
drwxr-xr-t 2 root root 4096 Feb 5 2020 thinclient_drives
drwxr-xr-x 2 root root 4096 Feb 5 2020 Videos
```

chmod 744 log.txt → log.txt üzerinde user her şeyi yapar, grup ve other sadece okur.

cp log.txt /tmp/ → dosyayı ortak bir yere kopyalayalım.

(sudo) adduser n → newuser newuser adlı kullanıcı oluşturalım.

Su -newuser → Ardından other olan bir huriye dizinine gecelim dosyaya yetkisini inceleyelim.

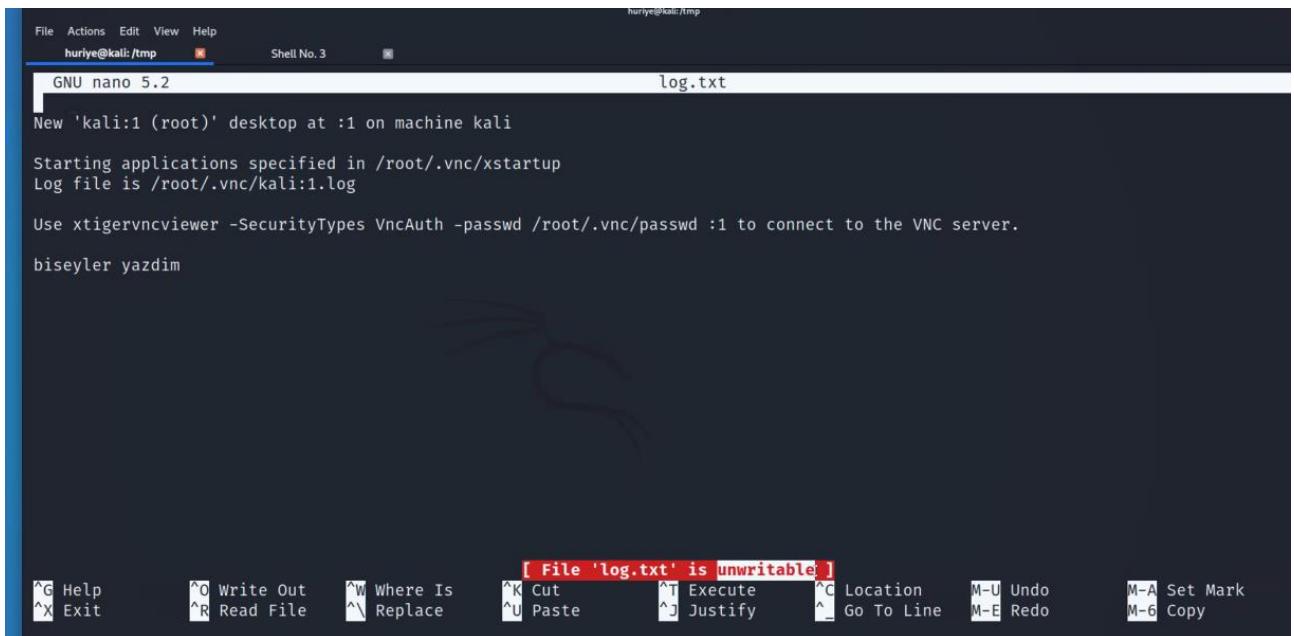
Görüldüğü gibi other olan newuser kullanıcısı sadece read yetkisine sahip .

```
root@kali:~# ls -l /tmp/
total 32
-rwxr--r-- 1 root root 262 Nov 18 20:34 log.txt
drwx----- 2 root robt 4096 Nov 18 16:56 ssh-10sBLWijBuUD
drwx----- 3 root root 4096 Nov 18 16:56 systemd-private-86207e3503634a87ad522b237fb70d0b-colord.service-uQABCh
drwx----- 3 root root 4096 Nov 18 16:55 systemd-private-86207e3503634a87ad522b237fb70d0b-haveged.service-0WQ30i
drwx----- 3 root root 4096 Nov 18 16:56 systemd-private-86207e3503634a87ad522b237fb70d0b-ModemManager.service-2bpU6i
drwx----- 3 root root 4096 Nov 18 16:56 systemd-private-86207e3503634a87ad522b237fb70d0b-systemd-logind.service-jYLDQg
drwx----- 3 root root 4096 Nov 18 16:56 systemd-private-86207e3503634a87ad522b237fb70d0b-upower.service-4ACXpj
drwxrwxrwt 2 root root 4096 Nov 18 16:55 VMwareDnD
root@kali:~# r--
```

Cat >> log.txt → Yazmaya çalıştık ancak izin verilmedi.

```
huriye@kali:/tmp$ cat >> log.txt
-bash: log.txt: Permission denied
```

Nano text editörde de yazma yetkisi olmadığı uyarısını görüyoruz.



```
huriye@kali:~/tmp
```

File Actions Edit View Help
huriye@kali: /tmp Shell No. 3

GNU nano 5.2 log.txt

New 'kali:1 (root)' desktop at :1 on machine kali

Starting applications specified in /root/.vnc/xstartup

Log file is /root/.vnc/kali:1.log

Use xtigervncviewer -SecurityTypes VncAuth -passwd /root/.vnc/passwd :1 to connect to the VNC server.

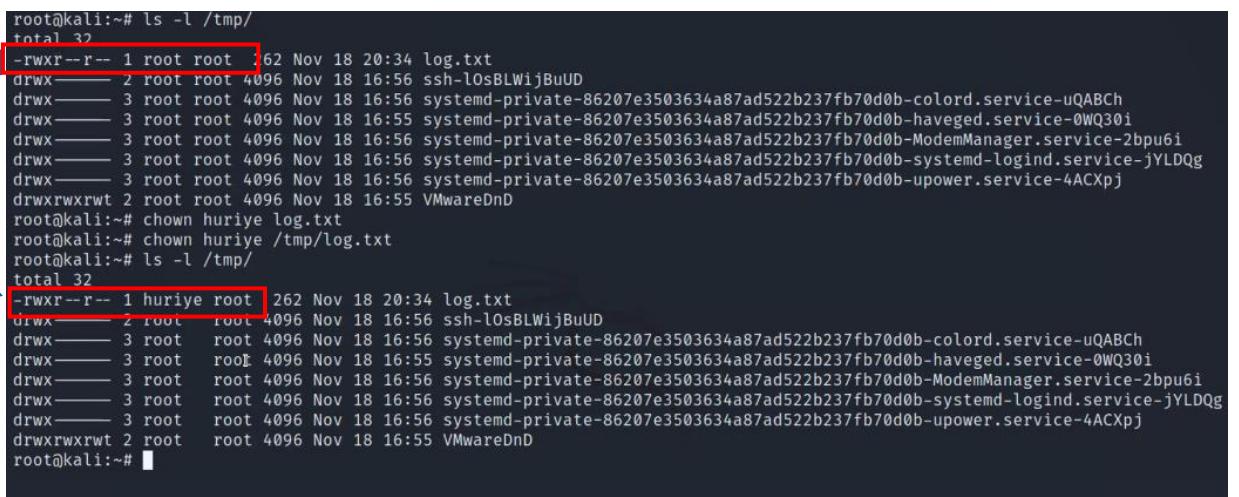
biseyler yazdim

[File 'log.txt' is unwritable!]

^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 M-A Set Mark M-6 Copy

chown huriye /tmp/log.txt → Dosyanın ownerini değiştirdik (eskiden root idi)

Aşağıda da görüldüğü gibi artık newuser kullanıcısı log.txt üzerinde tüm yetkilere sahip oldu.



```
root@kali:~# ls -l /tmp/
total 32
-rwxr--r-- 1 root root 262 Nov 18 20:34 log.txt
drwx----- 2 root root 4096 Nov 18 16:56 ssh-10sBLWijBuUD
drwx----- 3 root root 4096 Nov 18 16:56 systemd-private-86207e3503634a87ad522b237fb70d0b-colord.service-uQABCh
drwx----- 3 root root 4096 Nov 18 16:55 systemd-private-86207e3503634a87ad522b237fb70d0b-haveged.service-0WQ30i
drwx----- 3 root root 4096 Nov 18 16:56 systemd-private-86207e3503634a87ad522b237fb70d0b-ModemManager.service-2bpw6i
drwx----- 3 root root 4096 Nov 18 16:56 systemd-private-86207e3503634a87ad522b237fb70d0b-systemd-logind.service-jYLDQg
drwxrwxrwt 2 root root 4096 Nov 18 16:56 systemd-private-86207e3503634a87ad522b237fb70d0b-upower.service-4ACXpj
drwxrwxrwt 2 root root 4096 Nov 18 16:55 VMwareDnD
root@kali:~# chown huriye log.txt
root@kali:~# chown huriye /tmp/log.txt
root@kali:~# ls -l /tmp/
total 32
-rwxr--r-- 1 huriye root 262 Nov 18 20:34 log.txt
drwx----- 2 root root 4096 Nov 18 16:56 ssh-10sBLWijBuUD
drwx----- 3 root root 4096 Nov 18 16:56 systemd-private-86207e3503634a87ad522b237fb70d0b-colord.service-uQABCh
drwx----- 3 root root 4096 Nov 18 16:55 systemd-private-86207e3503634a87ad522b237fb70d0b-haveged.service-0WQ30i
drwx----- 3 root root 4096 Nov 18 16:56 systemd-private-86207e3503634a87ad522b237fb70d0b-ModemManager.service-2bpw6i
drwx----- 3 root root 4096 Nov 18 16:56 systemd-private-86207e3503634a87ad522b237fb70d0b-systemd-logind.service-jYLDQg
drwxrwxrwt 2 root root 4096 Nov 18 16:55 VMwareDnD
root@kali:~#
```

Okuma ve değişiklik yapabildik

cat log.txt →
cat >>log.txt →

```

huriye@kali:/tmp$ cat log.txt
New 'kali:1 (root)' desktop at :1 on machine kali

Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/kali:1.log

Use xtigervncviewer -SecurityTypes VncAuth -passwd /root/.vnc/passwd :1 to connect to the VNC server.

biseyler yazdim
huriye@kali:/tmp$ cat >> log.txt
yeni bir satir
hello world
^C
huriye@kali:/tmp$ cat log.txt
New 'kali:1 (root)' desktop at :1 on machine kali

Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/kali:1.log

```

Chmod u -r /tmp/log.txt → log.txt icin user'dan read yetkisini kaldırırdık (bunu root dizininde iken yapmalıyız)

ls -l → huriye user'dan read yetkisinin kalktığını gördük.

Cat.log.txt → huriye user'dan dosyaya erişemedik

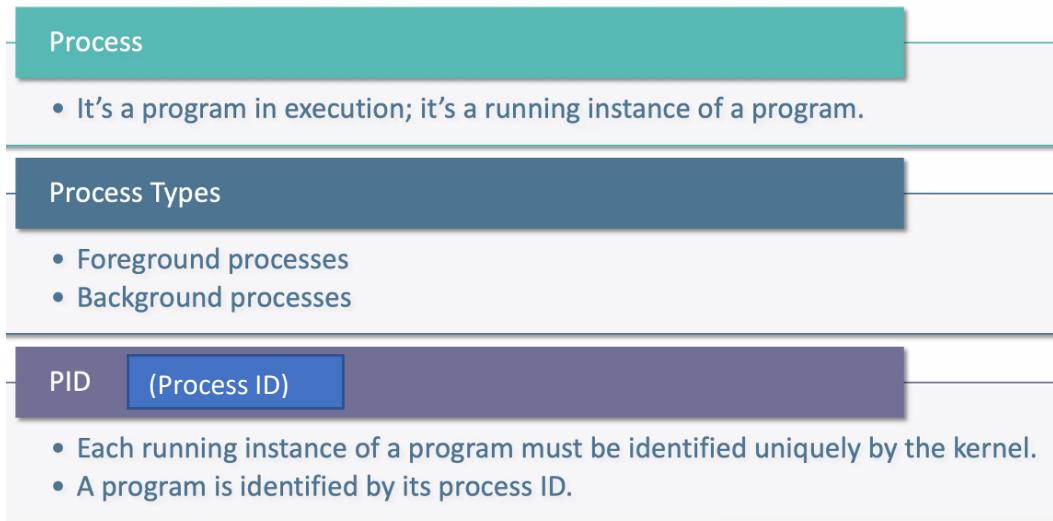


```

huriye@kali:/tmp$ ls -l
total 32
drwxr--r-- 1 huriye root 289 Nov 18 20:48 log.txt
drwxr--r-- 2 root root 4096 Nov 18 16:56 ssh-losBLWijBuUD
drwxr--r-- 3 root root 4096 Nov 18 16:56 systemd-private-86207e3503634a87ad522b237fb70d0b-colord.service-uQABCh
drwxr--r-- 3 root root 4096 Nov 18 16:55 systemd-private-86207e3503634a87ad522b237fb70d0b-havaged.service-0WQ30i
drwxr--r-- 3 root root 4096 Nov 18 16:56 systemd-private-86207e3503634a87ad522b237fb70d0b-ModemManager.service-2bpU6i
drwxr--r-- 3 root root 4096 Nov 18 16:56 systemd-private-86207e3503634a87ad522b237fb70d0b-systemd-logind.service-jYLDQg
drwxr--r-- 3 root root 4096 Nov 18 16:56 systemd-private-86207e3503634a87ad522b237fb70d0b-upower.service-4ACXpj
drwxrwxrwt 2 root root 4096 Nov 18 16:55 VMwareDnD
huriye@kali:/tmp$ cat log.txt
cat: log.txt: Permission denied
huriye@kali:/tmp$ 

```

2.8 Processes



Monitoring Running Process

Kod	Maksadi
ps	Çalışan process bilgileri sergileme
pstree	Çalışan process bilgilerini ağaç seklinde sergileme
fg	Belirtilen program ön yüzde çalışır. Terminalde onun bilgileri akar, o yüzden terminal kullanılamaz
bg	Belirtilen program backgroundda çalışır. Terminal kullanılmaya devam edilebilir.
jobs	Processların durumunu raporlar
Kill -9	Belirtilen processi kapatır
top	İstatistik bilgiler ve ayrıntılı process bilgiler mevcut (ps'den daha ayrıntılı)

#ps

#ps	* report a snapshot of the current processes.
#ps -ef, #ps -ely	* To see every process on the system using standard syntax
#ps aux	* To see every process on the system using BSD syntax
#ps -aux	* print all processes owned by a user named "x", as well as printing all processes that would be selected by the -a option.
#pstree	* display a tree of processes

NOT: PID programlar için sabit değildir. Sadece 1 no'lu PID her zaman init'dir

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.0	0.2	220348	8620	?	Ss	03:07	0:07	/sbin/init
root	2	0.0	0.0	0	0	?	S	03:07	0:00	[kthreadd]
root	4	0.0	0.0	0	0	?	I<	03:07	0:00	[kworker/0:0H]
root	6	0.0	0.0	0	0	?	I<	03:07	0:00	[mm_percpu_wq]
root	7	0.0	0.0	0	0	?	S	03:07	0:00	[ksoftirqd/0]
root	8	0.0	0.0	0	0	?	I	03:07	0:07	[rcu_sched]
root	9	0.0	0.0	0	0	?	I	03:07	0:00	[rcu_bh]
root	10	0.0	0.0	0	0	?	S	03:07	0:00	[migration/0]
root	11	0.0	0.0	0	0	?	S	03:07	0:00	[watchdog/0]
	12	0.0	0.0	0	0	?	S	03:07	0:00	[kworker/0:1H]

man ps → kodların manuelini incelemeyi unutmamalıyız.

ps → Çalışan process bilgiler

PID : Process ID

TTY : çalışan her Terminalde atanmış değer

Zaman :

Komuta:

bash Terminali işleyen kabuk tipi

ps bu komutun çalışması için gerekli dosya

root@kali:~# ps			
	PID	TTY	TIME CMD
	1355	pts/0	00:00:00 bash
	1361	pts/0	00:00:00 ps

ps -ef → Çalışan tüm process bilgiler. “ps” komutuyla sadece 2 process görmüştük

Göründüğü gibi başka kullanıcının (xrdp) çalıştırıldığı process var

TTY ?(soru işaretçi) ise terminalden çalışmadığı anlamına gelir

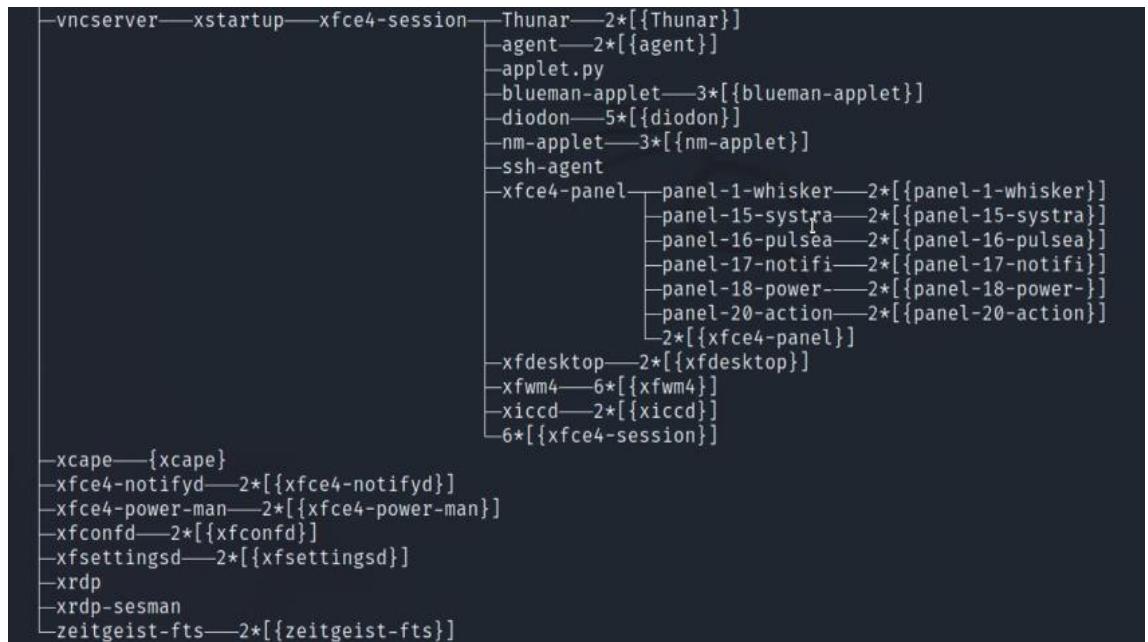
PID 1 her zaman init processdir

UID	PID	PPID	C	S	TIME	TTY	TIME	CMD
root	1	0	0	17:11	?		00:00:02	/sbin/init splash
root	2	0	0	17:11	?		00:00:00	[kthreadd]
root	3	2	0	17:11	?		00:00:00	[rcu_gp]
root	4	2	0	17:11	?		00:00:00	[rcu_par_gp]
root	6	2	0	17:11	?		00:00:00	[kworker/0:0H-kblockd]
root	9	2	0	17:11	?		00:00:00	[mm_percpu_wq]
root	10	2	0	17:11	?		00:00:00	[ksoftirqd/0]
root	11	2	0	17:11	?		00:00:00	[rcu_sched]
root	12	2	0	17:11	?		00:00:00	[migration/0]
root	13	2	0	17:11	?		00:00:00	[cpuhp/0]
root	14	2	0	17:11	?		00:00:00	[cpuhp/1]
root	15	2	0	17:11	?		00:00:00	[migration/1]
root	16	2	0	17:11	?		00:00:00	[ksoftirqd/1]
root	18	2	0	17:11	?		00:00:00	[kworker/1:0H-kblockd]
root	20	2	0	17:11	?		00:00:00	[kdevtmpfs]
root	851	1	0	17:12	?		00:00:00	/usr/sbin/xrdp-sesman
root	874	1	0	17:12	?		00:00:10	/usr/bin/Xtigervnc :1 -
xrdp	875	1	0	17:12	?		00:00:00	/usr/sbin/xrdp

ps -ely → ps -ey'ye nazaran daha da fazla bilgiler farklı formatta sergilendi.

S	UID	PID	PPID	C	PRI	NI	RSS	SZ	WCHAN	TTY	TIME	CMD
S	0	1	1	0	80	0	11156	25599	-	?	00:00:02	systemd
S	0	2	0	0	80	0	0	0	-	?	00:00:00	kthreadd
I	0	3	2	0	60	-20	0	0	-	?	00:00:00	rcu_gp
I	0	4	2	0	60	-20	0	0	-	?	00:00:00	rcu_par_gp
I	0	6	2	0	60	-20	0	0	-	?	00:00:00	kworker/0:0H-kblockd
I	0	9	2	0	60	-20	0	0	-	?	00:00:00	mm_percpu_wq
S	0	10	2	0	80	0	0	0	-	?	00:00:00	ksoftirqd/0
I	0	11	2	0	80	0	0	0	-	?	00:00:00	rcu_sched
S	0	12	2	0	-40	-	0	0	-	?	00:00:00	migration/0
S	0	13	2	0	80	0	0	0	-	?	00:00:00	cpuhp/0
S	0	14	2	0	80	0	0	0	-	?	00:00:00	cpuhp/1
S	0	15	2	0	-40	-	0	0	-	?	00:00:00	migration/1
S	0	16	2	0	80	0	0	0	-	?	00:00:00	ksoftirqd/1
I	0	18	2	0	60	-20	0	0	-	?	00:00:00	kworker/1:0H-kblockd
S	0	20	2	0	80	0	0	0	-	?	00:00:00	kdevtmpfs
I	0	21	2	0	60	-20	0	0	-	?	00:00:00	netns
S	0	22	2	0	80	0	0	0	-	?	00:00:00	kaudittd
S	0	23	2	0	80	0	0	0	-	?	00:00:00	xenbus

pstree → processleri parent-child (ağaç) modelinde sergiler.



pstree -al → processleri parent-child (ağaç) modelinde diğer ağaç modele nazaran ayrıntılı sergiler.

```
File Actions Edit View Help
           |---panel-15-systra /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libsystray.so 15 18874377 systray Notification Area Area where notification icons appear
           |   |---2*[{panel-15-systra}]
           |---panel-16-pulsea /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libpulseaudio-plugin.so 16 18874378 pulseaudio PulseAudio Plugin Adjust the audio volume of the PulseAudio sound system
           |   |---2*[{panel-16-pulsea}]
           |---panel-17-notifi /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libnotification-plugin.so 17 18874379 notification-plugin Notification Plugin Notification plugin for the Xfce panel
           |   |---2*[{panel-17-notifi}]
           |---panel-18-power- /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libxfce4powermanager.so 18 18874380 power-manager-plugin Power Manager Plugin Display the battery levels of your devices and control the brightness of your display
           |   |---2*[{panel-18-power-}]
           |---panel-20-action /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libactions.so 20 18874381 actions Action Buttons Log out, lock or other system actions
           |   |---2*[{panel-20-action}]
           |   |---2*[{xfce4-panel}]
           |---xfdesktop
           |   |---2*[{xfdesktop}]
           |---xfwm4
           |   |---6*[{xfwm4}]
```

ps -aux → tüm kullanıcıların processlerini gösterir. (-ely gibi ancak format farklı)

Memory kullanım bilgileri ve önceliklendirme mevcut

Bazı Linux OS'lerde ps -au x (x user ile u arasında boşluk var)

a all
u user
x gösterilmesi istenilen tek bir user varsa onun adı yazılır.

```
File Actions Edit View Help
root@kali:~# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      1  4.1  0.2 167928 11160 ?        Ss   17:07  0:03 /sbin/init splash
root      2  0.0  0.0     0     0 ?        S    17:07  0:00 [kthreadd]
root      3  0.0  0.0     0     0 ?        I<  17:07  0:00 [rcu_gp]
root      4  0.0  0.0     0     0 ?        I<  17:07  0:00 [rcu_par_gp]
root      5  0.0  0.0     0     0 ?        I   17:07  0:00 [kworker/0:0-events]
root      6  0.0  0.0     0     0 ?        I<  17:07  0:00 [kworker/0:0H-kblockd]
root      7  0.2  0.0     0     0 ?        I   17:07  0:00 [kworker/0:1-events]
root      8  0.0  0.0     0     0 ?        I   17:07  0:00 [kworker/u30:0-events_u]
root      9  0.0  0.0     0     0 ?        I<  17:07  0:00 [mm_percpu_wq]
root     10  0.0  0.0     0     0 ?        S   17:07  0:00 [ksoftirqd/0]
root     11  0.1  0.0     0     0 ?        I   17:07  0:00 [rcu_sched]
root     12  0.0  0.0     0     0 ?        S   17:07  0:00 [migration/0]
root     13  0.0  0.0     0     0 ?        S   17:07  0:00 [cpuhp/0]
root     14  0.0  0.0     0     0 ?        S   17:07  0:00 [cpuhp/1]
root     15  1.0  0.0     0     0 ?        S   17:07  0:00 [migration/1]
root     16  0.0  0.0     0     0 ?        S   17:07  0:00 [ksoftirqd/1]
root     17  0.0  0.0     0     0 ?        I   17:07  0:00 [kworker/1:0-rcu_gp]
root     18  0.0  0.0     0     0 ?        I<  17:07  0:00 [kworker/1:0H-kblockd]
root     20  0.0  0.0     0     0 ?        S   17:07  0:00 [kdevtmpfs]
root     21  0.0  0.0     0     0 ?        I<  17:07  0:00 [netns]
root     22  0.0  0.0     0     0 ?        S   17:07  0:00 [kauditfd]
root     23  0.0  0.0     0     0 ?        S   17:07  0:00 [xenbus]
root     24  0.0  0.0     0     0 ?        S   17:07  0:00 [xenwatch]
```

ps -aux → x yerinde colord kullanıcısının adını yazarak sadece onun bilgilerini sergilettik.

ps aux → aux başında - (eksi) olmadığı durumda BSD formatında sergiler

Wireshark programını terminalden açalım. Terminale sadece “**wireshark**” yazarız- Terminalde sadece wireshark uygulaması logları akar.

Ctrl+z tuşıyla programı dondurduk.
Ancak sonlandırmadık.

ps → Çalışan process bilgileri

Jobs → processlerin statüsünü de gösterir.

```
root@kali:~# ps
  PID TTY      TIME CMD
 1355 pts/0    00:00:00 bash
 1666 pts/0    00:00:01 wireshark
 1742 pts/0    00:00:00 ps
root@kali:~# jobs
[1]+  Stopped                  wireshark
root@kali:~#
```

fg 1 → forward ground-jobs ta listelenen 1 nolu wireshark process tekrar aktive olur. Terminalde o program çalışır, Başka is yapamayız.

bg 1 → background-jobs ta listelenen 1 nolu wireshark process arka planda tekrar aktive olur terminali kullanabiliriz

0

```
root@kali:~# jobs
[1]+  Stopped                  wireshark
root@kali:~# bg 1
[1]+ wireshark &
root@kali:~# 18:30:50.352      Warn invalid source position for vertical gradient
18:30:50.352      Warn invalid source position for vertical gradient
18:30:50.352      Warn invalid source position for vertical gradient
18:30:50.352      Warn invalid source position for vertical gradient
```

firefox & → firefox programı backgroundda çalışmaya devam eder.

```
root@kali:~# firefox &
[2] 1759
root@kali:~# Sandbox: seccomp sandbox violation: pid 1814, tid 1814, syscall 315, args 1814 140073983726016
56 0 10 140073983726016.
Sandbox: seccomp sandbox violation: pid 1859, tid 1859, syscall 315, args 1859 139943632146560 56 0 10 13994
3632146560.
Sandbox: seccomp sandbox violation: pid 1900, tid 1900, syscall 315, args 1900 140195193674560 56 0 10 14019
5193674560.
```

Maltego & → maltego programı backgroundda çalışmaya devam eder. Terminalde işlem yapmaya devam edebiliriz.

```
root@kali:~# jobs
[1]-  Running                  wireshark &
[2]+  Running                  maltego &
```

Arka planda çalışan uygulamayı “**fg**” komutuyla ön plana alır ve **Ctrl+C** ile kapatabiliriz ya da “**kill**” ile direkt kapatabiliriz.

Ps -ef | grep wireshark → Çalışan tüm process bilgilerinden sadece wireshark ile ilgili olanları sergiler

```
root@kali:~# ps -ef | grep wireshark
root      1666  1355  0 18:23 pts/0    00:00:02 wireshark
root      2684  1355  0 18:51 pts/0    00:00:00 grep wireshark
root@kali:~# ps -ef | grep 1666
root      1666  1355  0 18:23 pts/0    00:00:02 wireshark
root      2693  1355  0 18:52 pts/0    00:00:00 grep 1666
```

kill -9 -1 → 1 PID nolu processi kapatır (init) kill-9 beraber kullanılır.

kill -9 -1666 → 1666 PID nolu processi kapatır. Wireshark imiş.

Wireshark'in PID degeri olan 1666 'yi grep ile ps listesinden öğreniriz.

```
root@kali:~# kill -9 1666
root@kali:~# man kill
[1] Killed wireshark
```

kill -l → Sinyalleri görüntüler.

Not: ps listesinde “[]” köseli parantez ile gösterilen programlar kernel'in kullandığı programlardır. Onları kapatırken dikkatli olunmalıdır.

Not: Bunlar siber için önemli kodlar. Arka planda neler çalıştığını gözlemelemek açısından faydalı bilgiler

Not: Yetkisiz herhangi bir kullanıcı da root'un processlerini görebilir.

Not: Yetkisiz kullanıcı root'un başlattığı processi kapatamaz.

Ps -ef →

```
root@kali:~# ps -ef
UID      PID  PPID  C STIME TTY          TIME CMD
root      1      0  0 17:11 ?        00:00:02 /sbin/init splash
root      2      0  0 17:11 ?        00:00:00 [kthreadd]
root      3      2  0 17:11 ?        00:00:00 [rcu_gp]
root      4      2  0 17:11 ?        00:00:00 [rcu_par_gp]
root      6      2  0 17:11 ?        00:00:00 [kworker/0:0H-kblockd]
root      9      2  0 17:11 ?        00:00:00 [mm_percpu_wq]
root     10      2  0 17:11 ?        00:00:00 [ksoftirqd/0]
root     11      2  0 17:11 ?        00:00:00 [rcu_sched]
root     12      2  0 17:11 ?        00:00:00 [migration/0]
root     13      2  0 17:11 ?        00:00:00 [cpuhp/0]
root     14      2  0 17:11 ?        00:00:00 [cpuhp/1]
root     15      2  0 17:11 ?        00:00:00 [migration/1]
root     16      2  0 17:11 ?        00:00:00 [ksoftirqd/1]
root     18      2  0 17:11 ?        00:00:00 [kworker/1:0H-kblockd]
root     20      2  0 17:11 ?        00:00:00 [kdevtmpfs]
```

Tekrar arka planda bir process başlatalım, öldürelim

Maltego & ➔ Arka planda çalıştık. (yetki sorunu oldu ama çalıştı)

Jobs ➔ uygulamaların statüsüne baktık.

Kill -9 4097 ➔ PID 4097 (Maltego) öldürdü.

```
huriye@kali:~$ kill -9 3487
```

```
-bash: kill: (3487) - Operation not permitted
```

Jobs ➔ PID 4097 (Maltego) çalışmadığını gördük.

```
huriye@kali:~$ maltego &
[1] 4097
huriye@kali:~$ ./../platform/lib/nbexec: WARNING: environment variable DISPLAY is not set

huriye@kali:~$ jobs   I
[1]+  Running                  maltego &
huriye@kali:~$ kill -9 4097
huriye@kali:~$ jobs
[1]+  Killed                  maltego
huriye@kali:~$ jobs
huriye@kali:~$
```

2.9 Linux System Monitoring

Monitoring Running Process

#top

(5 sn-de bir güncellenen görev yöneticisidir)

#top provides a dynamic real-time view of a running system.

Like Task Manager of Windows systems.

Output is updated in every 5 seconds by default

Down arrow to see more processes, "q" to quit.

```
top - 00:43:09 up 21:15,  1 user,  load average: 0.08, 0.05, 0.02
Tasks: 213 total,   1 running, 168 sleeping,   0 stopped,   0 zombie
%Cpu(s): 0.4 us, 0.1 sy, 0.0 ni, 99.5 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 3054256 total, 548344 free, 1250280 used, 1255632 buff/cache
KiB Swap: 2094076 total, 2094076 free,      0 used. 1564948 avail Mem

          PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
    1011 root      20   0 4407492 453336 99300 S  1.3 14.8  7:13.63 gnome-shell
      914 root      20   0 656420  75428 33112 S  0.3  2.5  1:48.69 Xorg
    1227 root      20   0 448992  36248 29200 S  0.3  1.2  1:22.52 vmtoolsd
    8719 root      20   0      0      0      0 I  0.3  0.0  0:00.22 kworker/1:1
    8730 root      20   0  47148  3960  3208 R  0.3  0.1  0:00.27 top
      1 root      20   0 220348  8620  6344 S  0.0  0.3  0:07.76 systemd
      2 root      20   0      0      0      0 S  0.0  0.0  0:00.03 kthreadd
      4 root      20  -20      0      0      0 I  0.0  0.0  0:00.00 kworker/0:0H
```

Top → Yukarıdaki terminale benzer bilgiler sergilendi.
İstatistik bilgiler ve ayrıntılı process bilgiler mevcut

NOT: Top açıkken "h" tuşuna basınca help menü gözükmür (renklendirme vb. islemeler yapılabilir)

Zombi Task: Islevini yitirmiş ancak tam kapanmamış Process

Soru : Tüm kullanıcıların tüm **processlerini** listeleyip,
İçerisinde sadece "**bin**" gecen satırların
PID numaralarını,
numerik olarak **büyükten küçüğe sıralayacak** şekilde gösteriniz.

Çözüm: `ps -aux | grep bin | tr -s " " | cut -d " " -f2| sort -n -r`

ps -aux Tüm kullanıcıların tüm **processleri** listele
ps -ef → Tüm kullanıcıların tüm **processleri** listele

grep bin → İçerisinde sadece "**bin**" gecen satırlar
grep -w bin → sadece bin olan satırlar (kelimenin içinde geçenleri içermez)

tr -s " " → Mükerrer Boşlukları teke indirir

cut -d " " → **PID** numaralarını,

sort → Sayıları ilk karakterine göre sıralar
sort -n → Sayıları küçükten büyüğe numerik sıralama
sort -n -r → Sayıları küçükten büyüğe reverse numerik sıralama yani büyükten küçüğe sıralama

Not : sort sayıları ilk karakterine göre sıralar 1, 11, 2, 21, gibi

Yusuf beyin hatalı çözümü:

`ps -aux -n --sort=-pid,+pid | tr -s " " | grep -iw bin` →

Sıralama yapılmış ancak satırındaki PID hariç bilgilerde sergilenmiş

Yusuf beyin doğru çözümü:

`ps -aux -n --sort=-pid,+pid | tr -s " " | grep -iw bin | cut -d " " -f3` →

Online Linux Terminal
<https://bellard.org/jslinux/>

Android Linux Kod App'i
<https://play.google.com/store/apps/details?id=com.inspiredandroid.linuxcommandbibliotheca>

Status of disk

#df

disk file system

Linux tabanlı işletim sistemlerinde disk boyutunu öğrenmek için df komutu kullanılır. Çıktının daha okunabilir olması için h parametresi de kullanılabilir.

Man df → manuel

df → diskin kullanım oranları bilgisi sergilenir.

df -h → daha anlaşılır

h: human readable

xvda1 işletimi sisteminin kurduğu dizinin adı (en fazla alanı kullanan)

```
root@kali:~# df
Filesystem      1K-blocks    Used Available Use% Mounted on
udev            1984572      0   1984572  0% /dev
tmpfs           403200     844   402356  1% /run
/dev/xvda1     25669860 12859600 11483260 53% /
tmpfs           2015996      0   2015996 0% /dev/shm
tmpfs            5120       0     5120  0% /run/lock
tmpfs            4096       0     4096  0% /sys/fs/cgroup

root@kali:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G  0  1.9G  0% /dev
tmpfs           394M  844K 393M  1% /run
/dev/xvda1      25G  13G  11G 53% /
tmpfs           2.0G  0  2.0G  0% /dev/shm
tmpfs            5.0M  0  5.0M  0% /run/lock
tmpfs            4.0M  0  4.0M  0% /sys/fs/cgroup
```

Status of RAM

Swap (Takas) Alanı Nedir ? Swap (Takas) Alanı, işletim sistemi tarafından sabit diskinizde ayrılmış bir bölümdür. İşlenecek veriler ön belleğe (RAM) sığmadığı zaman bu bölüm “RAM” gibi kullanılır ve böylelikle veri akışının ve proseslerinin devam etmesi sağlanır.

cd /proc/ → /proc dizininde sistemle ilgili kayıtlar mevcuttur. Sistem durumu için onlara bakılır
ls → PID ve sistem bilgileri

```
root@kali:/proc# ls
1   1022 1057 1083 1122 12 1239 135 15 1630 209 26 299 49 57 729 808 9 966  bus  diskstats  fs  keys  locks  pagetypeinfo  softirqs  timer_list  zoneinfo
10  1034 1058 1084 1134 120 1244 136 1504 1684 21 27 3 5 570 730 824 919 967  cgroups  dma  interrupts  key-users  meminfo  partitions  stat  tty
1000 1035 1059 1099 1138 1201 1249 138 1507 178 22 270 30 50 58 731 825 920 975  cmdline  driver  iomem  kmsg  misc  pressure  swaps  uptime
1005 1038 1060 11 1142 1212 1257 14 1514 18 222 274 329 51 6 733 826 924 991  consoles  dynamic_debug  ioports  kpagegroup  modules  sched_debug  sys  version
1012 1046 1061 1101 1153 1215 1263 1485 1554 2 23 275 4 52 68 735 848 932 996  cpufreq  execdomains  irq  kpagecount  mounts  schedstat  sysrq-trigger  vmallocinfo
1013 1051 1070 1114 1161 122 13 1486 16 20 24 28 48 55 71 736 868 944  acpi  crypto  fb  kallsyms  kpageflags  mtrr  self  sysvipc  vmstat
1017 1054 1074 1116 1191 1233 131 1496 1629 208 25 29 485 56 72 738 873 945  buddyinfo  devices  filesystems  kcore  loadavg  net  slabinfo  thread-self  xen
```

cat meminfo ➔ hafıza kullanım durumu
cat /proc/meminfo ➔ hafıza kullanım durumu

top ➔ Yukarıda anlatıldı hafıza kullanım durumunu sergiler.

q ile sayfadan çıkarılır

Status of CPU

```
root@kali:~# cat /proc/meminfo
MemTotal:      3054256 kB
MemFree:       81308 kB
MemAvailable: 1278484 kB
Buffers:        195540 kB
Cached:         1093080 kB
SwapCached:      0 kB
Active:        1379108 kB
Inactive:     1286684 kB
Active(anon): 1058604 kB
```

#vmstat

Virtual Memory Statistics

man vmstat ➔

vmstat 2 3 ➔ 2 sn arayla 3 kez kontrol edip CPU durumunu sergileyecək

```
root@kali:/proc# man vmstat
root@kali:/proc# vmstat 2 3
procs      memory      swap      io      system      cpu
r b    swpd   free   buff   cache   si   so   bi   bo   in   cs   us   sy   id   wa   st
0 0    0 2715420 65516 638500   0   0   114   22  118  127   1   0  97   1   1
0 0    0 2715484 65516 638540   0   0     0   0   419  337   1   0  99   0   0
0 0    0 2715484 65516 638540   0   0     0   0   303  248   1   0  99   0   0
root@kali:/proc# vmstat 3 7
procs      memory      swap      io      system      cpu
r b    swpd   free   buff   cache   si   so   bi   bo   in   cs   us   sy   id   wa   st
0 0    0 2715436 65524 638540   0   0   112   22  119  128   1   0  98   1   1
0 0    0 2715428 65524 638540   0   0     0   0   422  334   0   0  99   0   0
0 0    0 2715428 65524 638540   0   0     0   0   219  177   0   0 100   0   0
0 0    0 2715492 65524 638540   0   0     0   0   178  155   0   0 100   0   0
0 0    0 2715492 65524 638540   0   0     0   0   149  140   0   0 100   0   0
0 0    0 2715492 65524 638540   0   0     0   0   149  150   0   0 100   0   0
0 0    0 2715492 65524 638540   0   0     0   0   167  161   0   0 100   0   0
```

Sol üstteki r ve b harfinin anlamı

Procs

r: The number of runnable processes (running or waiting for run time).
b: The number of processes in uninterruptible sleep.

vmstat 2 ➔ 2 sn arayla kontrol edip CPU durumunu sergileyecək. Ancak hiç durmaz.

cat /proc/cpuinfo ➔ /proc dizininde sistemle ilgili kayıtlar mevcuttur. Sistem durumu için onlara bakılır.

```
root@kali:~# cat /proc/cpuinfo
processor       : 0
vendor_id      : GenuineIntel
cpu family     : 6
model          : 70
model name     : Intel(R) Core(TM) i7-4770HQ CPU @ 2.20GHz
stepping        : 1
microcode      : 0x19
cpu MHz        : 2195.226
```

2.6 Linux Network Configuration

Netstat -a → tüm protokol bilgileri

Netstat -t → tcp protokol bilgileri

```
root@kali:~# netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp     0      0 localhost:33580           localhost:5901       ESTABLISHED
tcp     0      0 localhost:33586           localhost:5901       ESTABLISHED
tcp     0      0 localhost:5901            localhost:33580       ESTABLISHED
tcp     0      0 ip-10-10-178-88.eu:http   ip-10-100-2-28.eu:45992 ESTABLISHED
tcp     0      0 ip-10-10-178-88.eu:http   ip-10-100-2-28.eu:45796 ESTABLISHED
tcp     0      0 localhost:5901            localhost:33586       ESTABLISHED
root@kali:~#
```

Netstat -tn → tcp (t) protokol bilgilerinin alan adı çözümlemesi yapmadan (-n) sergiler

Netstat -l → listen (l) modunda olanların bilgilerinin alan adı çözümlemesi yapmadan sergiler

Netstat -p → program (p) adı bilgilerini sergiler

Netstat -tlnp → tcp (t) protokolünü program (p) adıyla birlikte ad çözümlemesi yapmadan (n) listeler (l)

```
root@kali:~# netstat -tlnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp     0      0 127.0.0.1:5901           0.0.0.0:*           LISTEN    869/Xtigervnc
tcp     0      0 0.0.0.0:80              0.0.0.0:*           LISTEN    924/python
tcp     0      0 0.0.0.0:22              0.0.0.0:*           LISTEN    818/sshd: /usr/sbin
tcp6    0      0 ::1:5901               ::*:*                LISTEN    869/Xtigervnc
tcp6    0      0 ::1:3350               ::*:*                LISTEN    843/xrdp-sesman
tcp6    0      0 :::22                 ::*:*                LISTEN    818/sshd: /usr/sbin
tcp6    0      0 :::3389               ::*:*                LISTEN    866/xrdp
root@kali:~#
```

Netstat -au → udp protokol bilgilerini sergiler

```
root@kali:~# netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
udp     0      0 0.0.0.0:bootpc          0.0.0.0:*
udp     0      0 0.0.0.0:bootpc          0.0.0.0:*
root@kali:~#
```

Netstat -nr → Routing bilgisi ad çözümlemesi yapmadan sergiler (**netstat -n -route**)

```
root@kali:~# netstat -nr
Kernel IP routing table
Destination      Gateway          Genmask         Flags  MSS Window irtt Iface
0.0.0.0          10.10.0.1        0.0.0.0         UG        0 0          0 eth0
10.10.0.0        0.0.0.0          255.255.0.0     U         0 0          0 eth0
root@kali:~#
```

Netstat -s

```
root@kali:~# netstat -s
Ip:
  Forwarding: 2
  130 total packets received
    1 with invalid addresses
    0 forwarded
    0 incoming packets discarded
  129 incoming packets delivered
  129 requests sent out
  20 outgoing packets dropped
```

2.7 Linux Services

Her isi yapan farklı hatta aynı isi yapan farklı servisler vardır. Kimisi ağ üzerinde, kimisi ağa bağlı olmayan arka tarafta bilgisayarda çalışan servisler

groups → gruptara baktım (bu kullanıcı sudo'ya dahil)

sudo su - → parola istemeden kullanıcı geçişini yaptık.

```
kali@kali:~$ groups
kali cdrom floppy sudo audio dip video plugdev netdev bluetooth lpadmin scanner
kali@kali:~$ sudo su -
root@kali:~#
```

cd /etc/ → ag bağlantısı için gerekli servisleri incelemek için Ethernet dizinine geçtik.

ls -l | grep init → init için gerekli servisin olduğu dizini buradan bulurum.

cd init.d/ → belirtilen dizine ilerledim.

ls → listeledim.

```

root@kali:~# cd /etc/
root@kali:/etc# ls -l | grep init
drwxr-xr-x 2 root      root      4096 Sep  2  2020 cryptsetup-initramfs
drwxr-xr-x 2 root      root      4096 Sep  2  2020 init.d
drwxr-xr-x 5 root      root      4096 Aug 15 2020 initramfs-tools
root@kali:/etc# cd init.d/
root@kali:/etc/init.d# ls
apache2          cron          kmod          openvpn        rsync          sudo
apache-htcacheclean cryptdisks   lightdm       pcscd         rsyslog        sysstat
apparmor         cryptdisks-early lm-sensors   miredo        rwhod          tor
atftpd           dbus          networking   plymouth      samba-ad-dc  udev
avahi-daemon    dns2tcp      mysql        postgresql   postfdns     saned        x11-common
binfmt-support  haveged      nfs-common  procps       ptnet        screen-cleanup xl2tpd
bluetooth        hddtemp      nginx       pulseaudio-enable-autospawn smarntools  xrdp
cloud-config    hwclock.sh   nmbd        redsocks    smbd
cloud-final     inetsim      ntp          rlinetd    ssh
cloud-init      iodined      nvidia-persistenced  rlinetd    sslh
cloud-init-local ipsec       open-vm-tools rpcbind    stunnel4
console-setup.sh keyboard-setup.sh
root@kali:/etc/init.d#

```

ps -ef → tüm procesleri görüntülemek için

Burda adının sonunda “d” olanlar **daemon / servisleri** ifade eder.

```

root      739      1  0 17:06 ?
00:00:00 /lib/systemd/systemd-logind
root      805      1  0 17:06 ?
00:00:00 /usr/sbin/ModemManager
root      818      1  0 17:06 ?
00:00:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root      823      1  0 17:06 ttys1
00:00:00 /sbin/getty -o -p -- \u --noclear ttys1 linux
root      824      1  0 17:06 ttys0
00:00:00 /sbin/getty -o -p -- \u --keep-baud 115200,38400,9600 ttys0 vt220
root      843      1  0 17:06 ?
00:00:00 /usr/sbin/xrdp-sesman
xrdp     866      1  0 17:06 ?
00:00:00 /usr/sbin/xrdp
root      869      1  0 17:06 ?
00:00:41 /usr/bin/Xtigervnc :1 -desktop kali:1 (root) -auth /root/.Xauthority -geometry 190
root      919      1  0 17:07 ?
00:00:00 /usr/bin/perl /usr/bin/vncserver :1 -depth 24 -geometry 1900x1200
root      920      919  0 17:07 ?
00:00:00 /bin/bash /root/.vnc/xstartup
root      924      1  0 17:07 ?
00:00:02 python -m websockify 80 localhost:5901 -D
root      932      920  0 17:07 ?
00:00:00 xfce4-session
root      944      1  0 17:07 ?
00:00:00 dbus-launch --autolaunch 62b1088a95414ca18f7f59443db7e460 --binary-syntax --close-
root      945      1  0 17:07 ?
00:00:00 /usr/bin/dbus-daemon --syslog-only --fork --print-pid 5 --print-address 7 --sessio-
root      966      1  0 17:07 ?
00:00:00 /usr/bin/dbus-launch --exit-with-session --sh-syntax
root      967      1  0 17:07 ?
00:00:01 /usr/bin/dbus-daemon --syslog --fork --print-pid 5 --print-address 7 --session
root      975      932  0 17:07 ?
00:00:00 /usr/bin/ssh-agent x-session-manager
root      991      1  0 17:07 ?
00:00:00 /usr/libexec/at-spi-bus-launcher
root      996      991  0 17:07 ?
00:00:00 /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf
root     1000      1  0 17:07 ?
00:00:00 /usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
root     1006      1  0 17:07 ?
00:00:00 /usr/libexec/at-spi2-registrvd --use-gnome-session
root     1012      1  0 17:07 ?
00:00:00 /usr/bin/gpg-agent --sh -daemon --write-env-file /root/.cache/gpg-agent-info
root     1013      932  0 17:07 ?
00:00:02 xfwm4
root     1017      1  0 17:07 ?
00:00:00 /usr/libexec/gvfsd
root     1022      1  0 17:07 ?
00:00:00 /usr/libexec/gvfsd-fuse /home//.cache/xdg/gvfs -f

```

ps -ely → ağaç modelden bakalım.

PID 1 services adlı service “init” servisini ifade eder.

```

root@kali:~# ps -ely
S  UID   PID  PPID C PRI  NI   RSS   SZ WCHAN TTY      TIME CMD
S  0     1    0  0 80  0 11284 26110 - ? 00:00:04 systemd
S  0     2    0  0 80  0 0      0 0 - ? 00:00:00 kthreadd
I  0     3    2  0 60 -20 0 0 - ? 00:00:00 rcu_gp
I  0     4    2  0 60 -20 0 0 - ? 00:00:00 rcu_par_gp
I  0     6    2  0 60 -20 0 0 - ? 00:00:00 kworker/0:0H-kblockd
I  0     9    2  0 60 -20 0 0 - ? 00:00:00 mm_percpu_wq
S  0    10    2  0 80  0 0 0 - ? 00:00:00 ksoftirqd/0
I  0    11    2  0 80  0 0 0 - ? 00:00:00 rcu_sched
S  0    12    2  0 -40 - 0 0 - ? 00:00:00 migration/0
S  0    13    2  0 80  0 0 0 - ? 00:00:00 cpuhp/0
S  0    14    2  0 80  0 0 0 - ? 00:00:00 cpuhp/1
S  0    15    2  0 -40 - 0 0 - ? 00:00:00 migration/1
S  0    16    2  0 80  0 0 0 - ? 00:00:00 ksoftirqd/1
I  0    18    2  0 60 -20 0 0 - ? 00:00:00 kworker/1:0H-kblockd
S  0    20    2  0 80  0 0 0 - ? 00:00:00 kdevtmpfs
I  0    21    2  0 60 -20 0 0 - ? 00:00:00 netns
S  0    22    2  0 80  0 0 0 - ? 00:00:00 kauditd
S  0    23    2  0 80  0 0 0 - ? 00:00:00 xenbus
S  0    24    2  0 80  0 0 0 - ? 00:00:00 xenwatch
S  0    25    2  0 80  0 0 0 - ? 00:00:00 khungtaskd

```

su - →

service --status-all → sistemdeki tüm servisleri statüsünü (acık - kapalı şeklinde) görüntüleriz. Başında “+” olanlar aktif, “-“ olanlar kapalı, “?” işaret olanlar ise durumu belirlenememiş anlamındadır.

service --status-all | head -n15

veya

service --status-all | tail -n15 → basta veya sonda belli sayıda kaydı görüntüleyebilirim

Belirli bir servisin durumunu **ayrintılı** sorgulayalım.

```
root@kali:~# service --status-all
[ -I] apache-htcacheclean
[ - ] apache2
[ - ] apparmor
[ - ] atftpd
[ - ] avahi-daemon
[ + ] binfmt-support
[ - ] bluetooth
[ - ] cloud-config
[ - ] cloud-final
[ + ] cloud-init
[ + ] cloud-init-local
[ - ] console-setup.sh
[ + ] cron
[ - ] cryptdisks
```

Service sshd status → sshd servisinin statüsünü görüyoruz.

```
root@kali:~# service sshd status
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: disabled)
  Active: active (running) since Mon 2021-11-22 19:22:39 UTC; 2min 9s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Process: 803 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 814 (sshd)
   Tasks: 1 (limit: 4651)
  Memory: 2.3M
    CGroup: /system.slice/ssh.service
            └─814 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Nov 22 19:22:39 kali sshd[803]: /etc/ssh/sshd_config line 14: Deprecated option RSAAuthentication
Nov 22 19:22:39 kali sshd[803]: /etc/ssh/sshd_config line 17: Deprecated option RhostsRSAAuthentication
Nov 22 19:22:39 kali sshd[814]: /etc/ssh/sshd_config line 7: Deprecated option UsePrivilegeSeparation
Nov 22 19:22:39 kali sshd[814]: /etc/ssh/sshd_config line 8: Deprecated option Key_regeneration_interval
Nov 22 19:22:39 kali sshd[814]: /etc/ssh/sshd_config line 9: Deprecated option ServerKeyBits
Nov 22 19:22:39 kali sshd[814]: /etc/ssh/sshd_config line 14: Deprecated option RSAAuthentication
Nov 22 19:22:39 kali sshd[814]: /etc/ssh/sshd_config line 17: Deprecated option RhostsRSAAuthentication
Nov 22 19:22:39 kali sshd[814]: Server listening on 0.0.0.0 port 22.
Nov 22 19:22:39 kali sshd[814]: Server listening on :: port 22.
Nov 22 19:22:39 kali systemd[1]: Started OpenBSD Secure Shell server.
```

ps aux | grep sshd → PID kontrol edelim 814 olduğunu teyit ettik

```
root@kali:~# ps aux | grep sshd
root      814  0.0  0.1 12912  6976 ?        Ss   19:22  0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root     1313  0.0  0.0  6112  648 pts/0   S+  19:26  0:00 grep sshd
root@kali:~# ps aux | grep sshd
root      814  0.0  0.1 12912  6976 ?        Ss   19:22  0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root     1315  0.0  0.0  6112  644 pts/0   S+  19:26  0:00 grep sshd
root@kali:~#
```

sshd kapatalım ve bir daha durumuna bakalım.

service sshd stop → servisi kapatma komutu

Service sshd status → sshd servisinin statüsünü (inactive olduğunu) görüyoruz.

```

root@kali:~# service sshd stop
root@kali:~# service sshd status
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/sshd.service; enabled; vendor preset: disabled)
  Active: inactive (dead) since Mon 2021-11-22 19:30:59 UTC; 9s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Process: 803 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Process: 814 ExecStart=/usr/sbin/sshd -D $SSHD_OPTS (code=exited, status=0/SUCCESS)
 Main PID: 814 (code=exited, status=0/SUCCESS)

Nov 22 19:22:39 kali sshd[814]: /etc/ssh/sshd_config line 9: Deprecated option ServerKeyBits
Nov 22 19:22:39 kali sshd[814]: /etc/ssh/sshd_config line 14: Deprecated option RSAAuthentication
Nov 22 19:22:39 kali sshd[814]: /etc/ssh/sshd_config line 17: Deprecated option RhostsRSAAuthentication
Nov 22 19:22:39 kali sshd[814]: Server listening on 0.0.0.0 port 22.
Nov 22 19:22:39 kali sshd[814]: Server listening on :: port 22.
Nov 22 19:22:39 kali systemd[1]: Started OpenBSD Secure Shell server.
Nov 22 19:30:59 kali sshd[814]: Received signal 15; terminating.
Nov 22 19:30:59 kali systemd[1]: Stopping OpenBSD Secure Shell server...
Nov 22 19:30:59 kali systemd[1]: ssh.service: Succeeded.
Nov 22 19:30:59 kali systemd[1]: Stopped OpenBSD Secure Shell server.

```

Makineye bağlanmaya çalıştık ancak hata verdi. Çünkü sshd kapalı

```

Last login: Mon Nov 22 19:29:48 on ttys000
|huriye@Huriyes-MacBook-Pro ~ % ssh root@52.215.81.124
ssh: connect to host 52.215.81.124 port 22: Connection refused
huriye@Huriyes-MacBook-Pro ~ %

```

service sshd start ➔ servisi açma komutu

Service sshd status ➔ sshd servisinin statüsünü (kapalı olduğunu) görüyoruz.

```

root@kali:~# service sshd start
root@kali:~# service sshd status
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/sshd.service; enabled; vendor preset: disabled)
  Active: active (running) since Mon 2021-11-22 19:37:29 UTC; 18s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Process: 1362 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 1363 (sshd)
   Tasks: 3 (limit: 4651)
  Memory: 3.2M
     CGroup: /system.slice/sshd.service
             └─1363 sshd: /usr/sbin/sshd -D [listener] 1 of 10-100 startups
                 ├─1364 sshd: [accepted]
                 └─1365 sshd: [net]

Nov 22 19:37:29 kali sshd[1363]: /etc/ssh/sshd_config line 14: Deprecated option RSAAuthentication
Nov 22 19:37:29 kali sshd[1363]: /etc/ssh/sshd_config line 17: Deprecated option RhostsRSAAuthentication
Nov 22 19:37:29 kali sshd[1363]: Server listening on 0.0.0.0 port 22.
Nov 22 19:37:29 kali sshd[1363]: Server listening on :: port 22.
Nov 22 19:37:29 kali systemd[1]: Started OpenBSD Secure Shell server.
Nov 22 19:37:42 kali sshd[1364]: reexec line 7: Deprecated option UsePrivilegeSeparation
Nov 22 19:37:42 kali sshd[1364]: reexec line 8: Deprecated option Key_regeneration_interval
Nov 22 19:37:42 kali sshd[1364]: reexec line 9: Deprecated option ServerKeyBits
Nov 22 19:37:42 kali sshd[1364]: reexec line 14: Deprecated option RSAAuthentication
Nov 22 19:37:42 kali sshd[1364]: reexec line 17: Deprecated option RhostsRSAAuthentication

```

Makineye bağlanmaya çalıştık. Parola sordu. SSHD açık olduğunu anladık. Parola girilince bağlantı gerçekleşir

```

|huriye@Huriyes-MacBook-Pro ~ % ssh root@52.215.81.124
The authenticity of host '52.215.81.124 (52.215.81.124)' can't be established.
ECDSA key fingerprint is SHA256:Q2q+Mvj8LY4Pu7f0hDC8PpfQTHKNlnU+KXQt/fXnEzw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

```

Not: sshd port 22 üzerinden secure,
telnet port 23 üzerinde açık bağlantı yapar

SSHD açıkken netstat'ta görüntüleyebilirken kapatınca görüntüleyemedik

netstat -tlnp ➔
service sshd stop ➔
netstat -tlnp ➔

```
root@kali:~# netstat -tlnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State      PID/Program name
tcp        0      0 127.0.0.1:5901          0.0.0.0:*             LISTEN    870/Xtigervnc
tcp        0      0 0.0.0.0:80              0.0.0.0:*             LISTEN    919/python
tcp        0      0 0.0.0.0:22              0.0.0.0:*             LISTEN    1363/sshd: /usr/sbi
tcp6       0      0 ::1:5901                ::*:*                  LISTEN    870/Xtigervnc
tcp6       0      0 ::1:22                 ::*:*                  LISTEN    1363/sshd: /usr/sbi
tcp6       0      0 ::1:3350                ::*:*                  LISTEN    845/xrdp-sesman
tcp6       0      0 ::1:3389                ::*:*                  LISTEN    867/xrdp
root@kali:~# service sshd stop
root@kali:~# netstat -tlnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State      PID/Program name
tcp        0      0 127.0.0.1:5901          0.0.0.0:*             LISTEN    870/Xtigervnc
tcp        0      0 0.0.0.0:80              0.0.0.0:*             LISTEN    919/python
tcp6       0      0 ::1:5901                ::*:*                  LISTEN    870/Xtigervnc
tcp6       0      0 ::1:3350                ::*:*                  LISTEN    845/xrdp-sesman
tcp6       0      0 ::1:3389                ::*:*                  LISTEN    867/xrdp
```

Pstree ➔ “systemd” kök olmak üzere birçok servis çalıştığını görebiliriz.

```
root@kali:~# pstree
systemd—ModemManager—2*[{ModemManager}]
|   NetworkManager—2*[{NetworkManager}]
|   Xtigervnc—4*[{Xtigervnc}]
|   2*[agetty]
|   at-spi-bus-laun—dbus-daemon
|   |   3*[{at-spi-bus-laun}]
|   at-spi2-registr—2*[{at-spi2-registr}]
|   blueman-tray—2*[{blueman-tray}]
|   colord—2*[{colord}]
|   cron
|   3*[dbus-daemon]
|   2*[dbus-launch]
|   dconf-service—2*[{dconf-service}]
|   2*[dhclient—3*[{dhclient}]]
|   gpg-agent
|   gvfs-afc-volume—3*[{gvfs-afc-volume}]
|   gvfs-goa-volume—2*[{gvfs-goa-volume}]
|   gvfs-gphoto2-vo—2*[{gvfs-gphoto2-vo}]
|   gvfs-mtp-volume—2*[{gvfs-mtp-volume}]
|   gvfs-udisks2-vo—3*[{gvfs-udisks2-vo}]
|   gvfsd—gvfsd-trash—2*[{gvfsd-trash}]
|   |   2*[{gvfsd}]
|   gvfsd-fuse—5*[{gvfsd-fuse}]
|   gvfsd-metadata—2*[{gvfsd-metadata}]
|   haveged
|   obexd
|   polkitd—2*[{polkitd}]
|   python—2*[python]
|   qterminal—bash—su—bash—su—bash—sudo—su—bash—systemctl—pager
|   |   bash—pstree
|   |   2*[{pstree}]
```

Başka bir servise bakalım.

Service udev status ➔

```
[root@kali:~# service udev status
● systemd-udevd.service - Rule-based Manager for Device Events and Files
  Loaded: loaded (/lib/systemd/system/systemd-udevd.service; static)
  Active: active (running) since Mon 2021-11-22 19:22:12 UTC; 24min ago
  TriggeredBy: ● systemd-udevd-kernel.socket
                ● systemd-udevd-control.socket
    Docs: man:systemd-udevd.service(8)
          man:udev(7)
        Main PID: 302 (systemd-udevd)
           Status: "Processing with 20 children at max"
          Tasks: 1
         Memory: 15.2M
        CGroup: /system.slice/systemd-udevd.service
                  └─302 /lib/systemd/systemd-udevd

Nov 22 19:22:11 kali systemd[1]: Starting Rule-based Manager for Device Events and Files...
Nov 22 19:22:12 kali systemd[1]: Started Rule-based Manager for Device Events and Files.
Nov 22 19:22:13 kali systemd-udevd[311]: Using default interface naming scheme 'v245'.
root@kali:~# ]
```

DIKKAT: process olarak bahse konu servisi (udev) gördük ancak Netstat listesinde göremedik. Çünkü ağ servisi değil. Cihaz içinde çalışan bir servis imiş PID 302'yi yukarıdan buluştuk zaten.

ps -aux | grep 302 ➔

netstat -tlnp |grep 302 ➔

```
[root@kali:~# ps -aux | grep 302
root      302  0.0  0.1  23580  7128 ?          Ss   19:22   0:00 /lib/systemd/systemd-udevd
root     2107  0.0  0.0   6112   700 pts/0    S+   19:48   0:00 grep 302
root@kali:~# netstat -tlnp | grep 302
root@kali:~# netstat -tlnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp      0      0 127.0.0.1:5901          0.0.0.0:*          LISTEN     870/Xtigervnc
tcp      0      0 0.0.0.0:80            0.0.0.0:*          LISTEN     919/python
tcp6     0      0 ::1:5901              ::*:*               LISTEN     870/Xtigervnc
tcp6     0      0 ::1:3350              ::*:*               LISTEN     845/xrdp-sesman
tcp6     0      0 ::::3389              ::*:*               LISTEN     867/xrdp
root@kali:~# ]
```

Not: Servisler kill komutıyla değil, stop ile inactive hale getirilmelidir.

Commands to Manage service

systemctl ➔ system control and manager Bazlarında bu komut, bazlarında service komutu çalışmamayabilir.

Systemctl status apache2 == service apache2 status

Systemctl status sshd ➔ kapalı olduğunu gördük.

Systemctl start sshd ➔ servisi açtık

```
root@kali:~# man systemctl
root@kali:~# systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/sshd.service; enabled; vendor preset: disabled)
  Active: inactive (dead) since Mon 2021-11-22 19:45:40 UTC; 31min ago
    Docs: man:sshd(8)
          man:sshd_config(5)
 Process: 1362 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Process: 1363 ExecStart=/usr/sbin/sshd -D $SSHD_OPTS (code=exited, status=0/SUCCESS)
 Main PID: 1363 (code=exited, status=0/SUCCESS)

Nov 22 19:42:19 kali sshd[1472]: reexec line 14: Deprecated option RSAAuthentication
Nov 22 19:42:19 kali sshd[1472]: reexec line 17: Deprecated option RhostsRSAAuthentication
Nov 22 19:42:40 kali sshd[1472]: reprocess config line 14: Deprecated option RSAAuthentication
Nov 22 19:42:40 kali sshd[1472]: reprocess config line 17: Deprecated option RhostsRSAAuthentication
Nov 22 19:42:49 kali sshd[1472]: Failed password for root from 34.252.211.194 port 46984 ssh2
Nov 22 19:42:52 kali sshd[1472]: Connection closed by authenticating user root 34.252.211.194 port 46984 [preauth]
Nov 22 19:45:40 kali sshd[1363]: Received signal 15; terminating.
Nov 22 19:45:40 kali systemd[1]: Stopping OpenBSD Secure Shell server...
Nov 22 19:45:40 kali systemd[1]: ssh.service: Succeeded.
Nov 22 19:45:40 kali systemd[1]: Stopped OpenBSD Secure Shell server.
root@kali:~# systemctl start sshd
root@kali:~#
```

Bir ağ servisinin çalışmama nedenini tespit etmek ve çözüm üretmek

Systemctl status sshd ➔ açıldığını gördük.

```
root@kali:~# systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/sshd.service; enabled; vendor preset: disabled)
  Active: active (running) since Mon 2021-11-22 20:17:59 UTC; 18s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
 Process: 2309 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 2310 (sshd)
   Tasks: 1 (limit: 4651)
  Memory: 1.3M
 CGroup: /system.slice/sshd.service
         └─2310 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Nov 22 20:17:59 kali sshd[2309]: /etc/ssh/sshd_config line 14: Deprecated option RSAAuthentication
Nov 22 20:17:59 kali sshd[2309]: /etc/ssh/sshd_config line 17: Deprecated option RhostsRSAAuthentication
Nov 22 20:17:59 kali sshd[2310]: /etc/ssh/sshd_config line 7: Deprecated option UsePrivilegeSeparation
Nov 22 20:17:59 kali sshd[2310]: /etc/ssh/sshd_config line 8: Deprecated option Key_regeneration_interval
Nov 22 20:17:59 kali sshd[2310]: /etc/ssh/sshd_config line 9: Deprecated option ServerKeyBits
Nov 22 20:17:59 kali sshd[2310]: /etc/ssh/sshd_config line 14: Deprecated option RSAAuthentication
Nov 22 20:17:59 kali sshd[2310]: /etc/ssh/sshd_config line 17: Deprecated option RhostsRSAAuthentication
Nov 22 20:17:59 kali sshd[2310]: Server listening on 0.0.0.0 port 22.
Nov 22 20:17:59 kali sshd[2310]: Server listening on :: port 22.
Nov 22 20:17:59 kali systemd[1]: Started OpenBSD Secure Shell server.
root@kali:~#
```

Yetkisiz kullanıcıyla bu servilerin statüsünü görüntüleyebilir ancak açıp/ kapatamayız.
Ancak yetkisiz kullanıcı da sudo komutuyla açıp/ kapatabilir

```

root@kali:~# su - kali
kali@kali:~$ service sshd status
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/sshd.service; enabled; vendor preset: disabled)
  Active: active (running) since Mon 2021-11-22 20:17:59 UTC; 1min 54s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Process: 2309 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 2310 (sshd)
   Tasks: 1 (limit: 4651)
  Memory: 2.0M
   CGroup: /system.slice/sshd.service
           └─2310 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

kali@kali:~$ service sshd stop
└─ AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to stop 'sshd.service'.
Multiple identities can be used for authentication:
 1. kali,,, (kali)
 2. Debian (ec2-user)
Choose identity to authenticate as (1-2): 1
Password: Failed to stop sshd.service: Connection timed out
See system logs and 'systemctl status sshd.service' for details.
kali@kali:~$ polkit-agent-helper-1: pam_authenticate failed: Authentication failure
^C
kali@kali:~$ sudo service sshd stop

```

Service status all → apache2 kapali olduğunu gördük.

```

kali@kali:~$ sudo su -
root@kali:~# service --status-all
[ - ] apache-htcacheclean
[ - ] apache2 [
[ - ] apparmor
[ - ] atftpd
[ - ] avahi-daemon
[ + ] binfmt-support

```

Systemctl status apache2 == service apache2 status

```

root@kali:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
  Active: inactive (dead)

```

```

root@kali:~# service apache2 status
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
  Active: inactive (dead)

```

Apache servisini TRY hack me'de açamayacağımız ancak şahsi bilgisayarlarda sanal makinede açılacaktır. TRY hack ME'de çalışmama sebebini tespit edelim ve çözüm üretelim

service apache2 start ➔ HATA!...Apache2'yi açamadık.

journalctl -xe ➔ hata raporunda buraya gitmem gerekiği belirtilmiştir.

Bunun kurulum dosyasına bakıyoruz. **init.d/** dizininde bulamadık. **etc/** içinde bulduk.

Cd etc/init.d/ ➔

ls -l | grep apache ➔ bulamadık.

cd etc/ ➔ "/etc" dizini Linux'ta yapılandırma dosyaları yer aldığı dizindir.

ls -l | grep apache ➔ bulduk

find /var/log -iname apache ➔ bulamadı.

find /var/log -iname apache* ➔ dosya buldu.

cd var/log/ ➔

ls -l | grep apache2 ➔

cd ./apache2/ ➔

ls ➔

pwd ➔

cat error.log ➔ boşmuş.

catacces.log ➔ boşmuş.

```
root@kali:/var/log# ls -l | grep apache
drwxr-x--- 2 root      adm          4096 Jan 29  2020 apache2
root@kali:/var/log# cd apache2/
root@kali:/var/log/apache2# ls
access.log  error.log  other_vhosts_access.log
root@kali:/var/log/apache2# pwd
/var/log/apache2
root@kali:/var/log/apache2# less error.log
root@kali:/var/log/apache2# cat error.log
root@kali:/var/log/apache2# cat access.log
```

dosyasına bakalım. Etc içinde olduğuna göre ağ üzerinde çalışan bir servis. Demek ki çalışabilmesi için porta ihtiyaç vardır. Port bilgisine ulaşmaya çalışalım.

cd /etc/apache2/ ➔

less apache2.conf ➔ bir şey bulamadık.

less port.conf ➔ port 80 ve 443'ü kullandığını öğrendik.

netstat -tlnp ➔ 80 no.lu portun (TCP) dolu olduğunu gördük. Başka bir servis (python) çalıştığını gördük. Aynı anda iki servis tek bir port üzerinde çalışmaz.

```
root@kali:~# service apache2 start
Job for apache2.service failed because the control process exited with error code.
See "systemctl status apache2.service" and "journalctl -xe" for details.
root@kali:~# cd /etc/ap
apache2/  apparmor/  apparmor.d/  apport/  apt/
root@kali:~# cd /etc/ap
apache2/  apparmor/  apparmor.d/  apport/  apt/
root@kali:~# cd /etc/apache2/
root@kali:/etc/apache2# ls
apache2.conf  conf-available  conf-enabled  envvars  magic  mods-available  mods-enabled  ports.conf  sites-available  sites-enabled
root@kali:/etc/apache2# less apache2.conf
root@kali:/etc/apache2# less ports.conf
root@kali:/etc/apache2# netstat -tnlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 127.0.0.1:5901              0.0.0.0:*                  LISTEN      870/Xtigervnc
tcp        0      0 0.0.0.0:80                 0.0.0.0:*                  LISTEN      919/python
tcp6       0      0 ::1:5901                   ::*:                     LISTEN      870/Xtigervnc
tcp6       0      0 ::1:3350                   ::*:                     LISTEN      845/xrdp-sesman
tcp6       0      0 ::1:3389                   ::*:                     LISTEN      867/xrdp
root@kali:/etc/apache2#
```

Apache'nin çalıştığı portu değiştirmek sorunu çözülmüş oluruz.

cd /etc/apache2/ ➔

nano ports.conf ➔ editörle açtık. Listen 80 yerine kullanılmayan başka bir port yazalım. Yukarıdaki portları disinda örneğin 8080 yapalım ve kaydedelim.

cat ports.conf ➔ Değiştiğini görelim

Aşağıdaki uyarıya göre başka bir yerde daha port bilgisini değiştirmeliyiz.

```
root@kali:/etc/apache2# nano ports.conf
root@kali:/etc/apache2# cat ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 8080

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
root@kali:/etc/apache2#
```

cd /etc/apache2/sites-enabled ➔ uyarıda belirtilen dizine gittik.

Nano 000-default.conf ➔ editörle açtık ve düzelttik. VirtualHost * 80 yerine yine 8080 yapalım ve kaydedelim

cat 000-default.conf ➔ değiştiğini gördük.

```
root@kali:/etc/apache2/sites-enabled# nano 000-default.conf
root@kali:/etc/apache2/sites-enabled# cat 000-default.conf
<VirtualHost *:8080>
    # 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

    # 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
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
root@kali:/etc/apache2/sites-enabled#
```

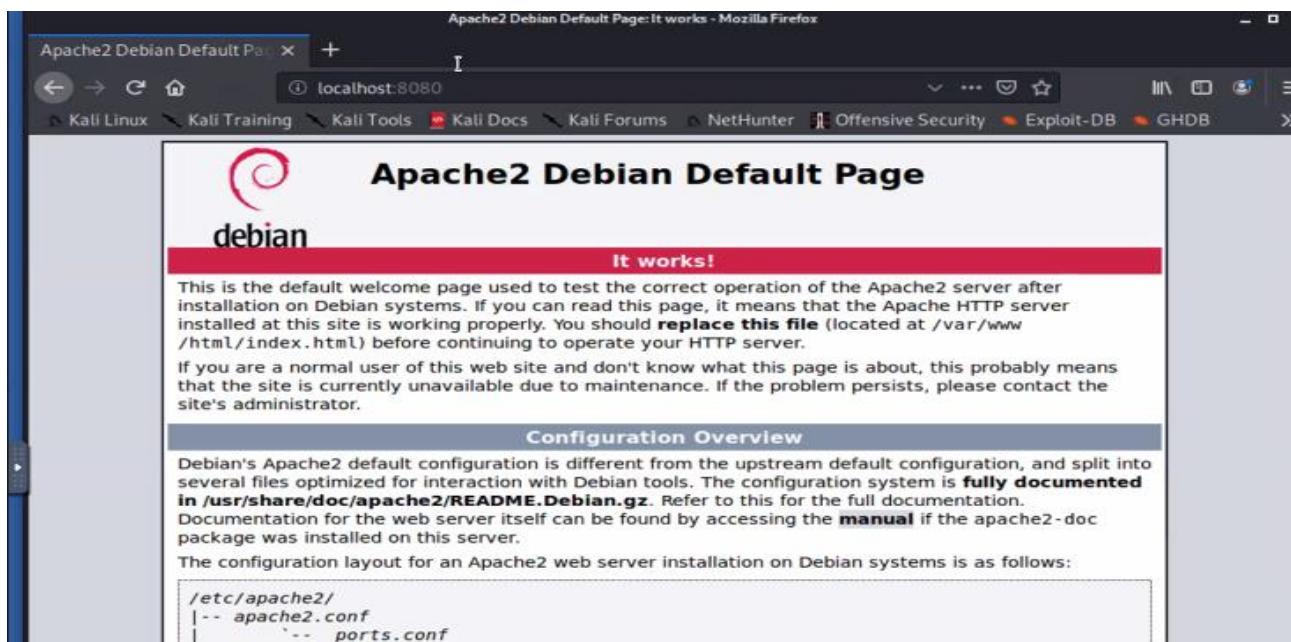
service apache2 start → çalıştı.

service apache2 status → çalıştığını gördük.

```
root@kali:~# service apache2 start
root@kali:~# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2021-11-22 20:54:51 UTC; 5s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Process: 3186 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 3190 (apache2)
    Tasks: 6 (limit: 4651)
   Memory: 14.1M
      CGroup: /system.slice/apache2.service
              └─3190 /usr/sbin/apache2 -k start
                  ├─3191 /usr/sbin/apache2 -k start
                  ├─3192 /usr/sbin/apache2 -k start
                  ├─3193 /usr/sbin/apache2 -k start
                  ├─3194 /usr/sbin/apache2 -k start
                  └─3195 /usr/sbin/apache2 -k start

Nov 22 20:54:51 kali systemd[1]: Starting The Apache HTTP Server ...
Nov 22 20:54:51 kali apachectl[3189]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1.
Nov 22 20:54:51 kali systemd[1]: Started The Apache HTTP Server.
lines 1-19/19 (END)
```

Browser'i açtık ve “localhost:8080” ‘e gittiğimizde sayfa açıldı.



Sayfada belirtiği üzere bu sayfanın olduğu dizine terminal üzerinden gidebiliriz. Buraya kendi web sayfası html kodlarını ekleyebiliriz.

cd /var/www/html/ →

nano index.html → editörle kendi web sayfasının kodlarını ekleyebiliriz. Sadece site adını değiştirdik. (Hacker Academy)

```
index.html  index.nginx-debian.html  
root@kali:/var/www/html# nano index.  
index.html          index.nginx-debian.html  
root@kali:/var/www/html# nano index.html
```

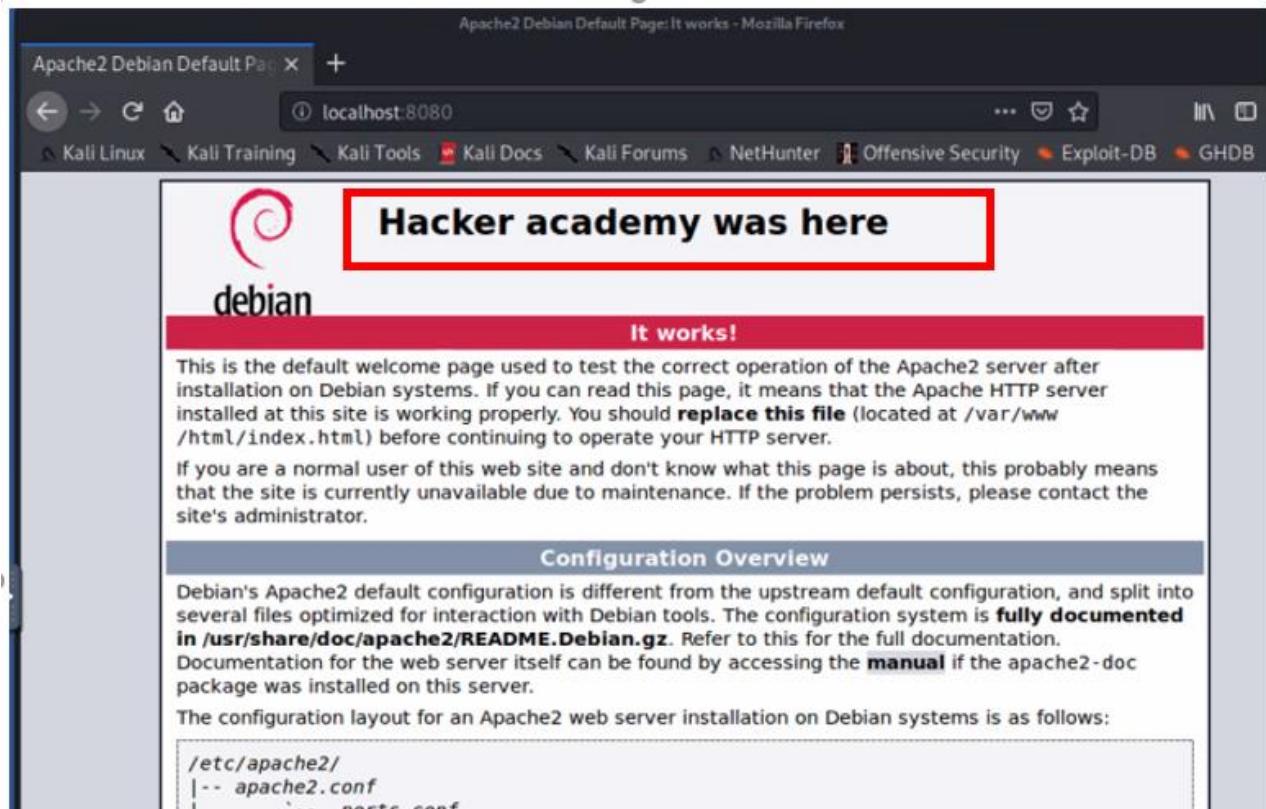
```
File Actions Edit View Help
kali㉿kali: ~ ┌─────────────────────────────────────────────────────────────────┐
                               Shell No. 2 └─────────────────────────────────────────────────┘
GNU nano 5.2                                     index.html
[ ] <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
      *
      {
        margin: 0px 0px 0px 0px;
        padding: 0px 0px 0px 0px;
      }

      body, html {
        padding: 3px 3px 3px 3px;
        background-color: #D8DBE2;

        font-family: Verdana, sans-serif;
        font-size: 11pt;
        text-align: center;
      }

      div.main_page {
        position: relative;
        display: table;
        width: 800px;
      }
    </style>
  </head>
  <body>
    <div>
      <h1>It works</h1>
      <p>This is the default web page for this server.<br/>
         The web server software is running but no content has been added, yet.</p>
    </div>
  </body>
</html>
[ Read 368 lines ]
^G Help          ^O Write Out      ^W Where Is       ^K Cut
^X Exit          ^R Read File      ^A Replace        ^U Paste
                                         ^T Execute
                                         ^J Justify
                                         ^C Local
                                         ^_ Go To
```

Browserı yenilediğimizde yaptığımız değişikliği gördük.



Package Management Concepts

Wireshark'ta incelediğimiz package ile karıştırmayalım. Burada OS için kusulan programların çalışması için tüm dosyalara paket adı verilir. Elimizde sadece kaynak kodu varsa da, biz paket oluşturabiliriz

Linux Package Managers

Linux içinde paketleri kurabilmek için kullanılan araçlar mevcuttur.

DPKG – Debian Package Management System

- APT (Advanced Packaging Tool)
- Aptitude Package Manager
- Synaptic Package Manager

RPM (Red Hat Package Manager)

- YUM (Yellowdog Updater, Modified)
- DNF – Dandified Yum

Pacman Package Manager – Arch Linux

Zypper Package Manager – openSUSE

Repository (REPO):

indirilecek paketlerin lokasyonu

A storage location from which software packages may be retrieved

Package management systems look for the repositories for the packages

Since they all have package management systems, Linux distros use repositories

In Debian-based distros such as Kali and Ubuntu

repos are in /etc/apt/source.list

"apt-get" to install and update packages

```
root@kali:~# cat /etc/apt/sources.list
deb http://http.kali.org/kali kali-rolling main non-free contrib
# deb-src http://http.kali.org/kali kali-rolling main non-free contrib
deb http://security.debian.org/debian-security wheezy/updates main
```

```

root@kali:~# cat /etc/apt/sources.list
#
# deb cdrom:[Kali GNU/Linux 2020.1rc4 _Kali-last-snapshot_ - Official amd64 DVD Binary-1 with firmware 20200124-09:35]/
kali-rolling main non-free
#deb cdrom:[Kali GNU/Linux 2020.1rc4 _Kali-last-snapshot_ - Official amd64 DVD Binary-1 with firmware 20200124-09:35]/ kali-rolling main non-free
deb http://http.kali.org/kali kali-rolling main non-free contrib
# deb-src http://http.kali.org/kali kali-rolling main non-free contrib
# This system was installed using small removable media
# (e.g. netinst, live or single CD). The matching "deb cdrom"
# entries were disabled at the end of the installation process.
# For information about how to configure apt package sources,
# see the sources.list(5) manual.
root@kali:~#

```

Sağ tıklayıp open linke basalım.

Burası Kali linuxun paketlerini indirdiği yer adları (repository)

Index of /kali/pool/contrib/a

Name	Last modified	Size	Description
Parent Directory		-	
alien-arena/	2020-11-11 12:46	-	
alsa-tools/	2021-09-19 18:00	-	
amoeba/	2021-11-21 06:00	-	
anbox/	2021-11-22 00:19	-	
assaultcube/	2021-02-05 18:00	-	
astra-toolbox/	2021-10-18 00:24	-	
astromenace/	2020-07-21 14:50	-	
astrometry-data-2mass/	2015-11-20 21:23	-	
atari800/	2021-10-12 06:00	-	

Apache/2.4.10 (Debian) Server at http.kali.org Port 80

Index of /kali/dists

Name	Last modified	Size	Description
Parent Directory		-	
debian-testing/	2021-11-23 12:01	-	
kali-bleeding-edge/	2021-07-22 23:44	-	
kali-debian-picks/	2021-11-15 12:22	-	
kali-dev-only/	2021-11-23 11:04	-	
kali-dev/	2021-11-23 12:02	-	
kali-experimental/	2021-11-15 10:35	-	
kali-last-snapshot/	2021-09-06 08:19	-	
kali-rolling-only/	2021-01-25 09:44	-	
kali-rolling/	2021-11-23 12:05	-	

Apache/2.4.10 (Debian) Server at http.kali.org Port 80

Command Line Interface

#apt

To install a package	*apt-get install <packageName>
To search for a package	*Apt-cache search <packageName>
To update packages and upgrade the installed programs	*apt-get update *apt-get upgrade
To uninstall a package	*apt-get remove <packageName>
To manage apt-get in GUI	*apt-get install synaptic

```

root@kali:~# apt-get update && apt-get upgrade
Get:1 http://security.debian.org/debian-security wheezy/updates InRelease [54.0 kB]
Get:2 https://packages.microsoft.com/ubuntu/14.04/prod trusty InRelease [2,846 B]
Get:4 http://security.debian.org/debian-security wheezy/updates/main i386 Packages [594 kB]
Get:3 http://ftp.hands.com/kali kali-rolling InRelease [30.5 kB]

```

Man apt → manuel sayfası

Update : güncelleme (burada listeyi günceller)

Upgrade: yükseltme (en yeni versiyona geçiş)

apt update → listeyi güncelledik (ilk basta bu komutu çalıştırılmalıdır)

apt install synaptic → synaptic adlı programı yükledik.

Y/n ile onay istiyor ve vazgeçme hakkı veriyor.

App autoremove → bu komut kullanılmayan bazı uygulamaları kaldırır. Biraz önce kurulum yaparken Y (YES) ile onay verince bu komutu çalışmasını da onayladık.

```
root@kali:~# apt update
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [17.9 MB]
Get:3 http://kali.download/kali kali-rolling/non-free amd64 Packages [210 kB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [111 kB]
Fetched 18.2 MB in 3s (7,207 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
1822 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@kali:~# apt install synaptic I
```

Programın kurulum öncesi verdiği bilgiler ve onay kısmı (sadece son kısmı)

```
libnet-libidn-perl libnet-ssleay-perl libsocket6-perl libstdc++6 libterm-readline-gnu-perl libtext-charwidth-perl libtext-iconv-perl libtirpc-common libtirpc3 libxapian3.2 perl perl-base
34 upgraded, 20 newly installed, 2 to remove and 1787 not upgraded.
Need to get 30.4 MB of archives.
After this operation, 52.9 MB of additional disk space will be used.
Do you want to continue? [Y/n] I
```

Bazı programlar ve portlar hakkında bilgi veren bir uyarı çıktı.

q (quit) ile uyarı sayfasını kapatarak kurulumu devam ettik ve kurulumu tamamladık.

Synaptic → Çalışmadı

which veya where is ile sorgulayalım

Which synaptic → bulamadı

Whereis synaptic → buldu. /bin dizini içine atmamış.

```
root@kali:~# synaptic  
bash: synaptic: command not found  
root@kali:~# which synaptic  
root@kali:~# whereis synaptic  
synaptic: /usr/sbin/synaptic /usr/share/synaptic /usr/share/man/man8/synaptic.8.gz  
root@kali:~#
```

apt list → bu şekilde uygulamanın tam adını görebiliriz. Yanda listenin sadece bir kısmını görüyoruz.

```
zvmcloudconnector-common/kali-rolling 1.4.1-4 all  
zynaddsubfx-data/kali-rolling 3.0.5-2 all  
zynaddsubfx-dssi/kali-rolling 3.0.5-2 amd64  
zynaddsubfx-lv2/kali-rolling 3.0.5-2 amd64  
zynaddsubfx-vst/kali-rolling 3.0.5-2 amd64  
zynaddsubfx/kali-rolling 3.0.5-2 amd64  
zypper-common/kali-rolling 1.14.42-2 all  
zypper-doc/kali-rolling 1.14.42-2 all  
zypper/kali-rolling 1.14.42-2 amd64  
zytrax/kali-rolling 0+git20201215-1 amd64  
zziplib-bin/kali-rolling 0.13.72+dfsg.1-1.1 amd64  
zzuf/kali-rolling 0.15-1+b1 amd64  
root@kali:~#
```

apt search synaptic → listede aranan program ismi olanları sergiler.

```
root@kali:~# apt search synaptic  
Sorting ... Done  
Full Text Search ... Done  
apt-cacher/kali-rolling 1.7.23 all  
  Caching proxy server for Debian/Ubuntu/Devuan software repositories  
  
muon/kali-rolling 4:5.8.0-2 amd64  
  graphical package manager  
  
packagekit/kali-rolling 1.2.4-1 amd64 [upgradable from: 1.1.13-2+b1]  
  Provides a package management service  
  
python3-brian/kali-rolling 2.4.2-7 all  
  simulator for spiking neural networks  
  
synaptic/kali-rolling,now 0.90.2+b1 amd64 [installed]  
  Graphical package manager  
  
xserver-xorg-input-libinput/kali-rolling 1.2.0-1 amd64 [upgradable from: 0.30.0-1]  
  X.Org X server -- libinput input driver  
  
xserver-xorg-input-synaptics/kali-rolling 1.9.1-2 amd64  
  Synaptics TouchPad driver for X.Org server  
  
xserver-xorg-input-synaptics-dev/kali-rolling 1.9.1-2 all  
  Synaptics TouchPad driver for X.Org server (development headers)
```

Apt remove synaptic → programı kaldırır.

dpkg -l → sistemde kurulu olan uygulamaları listeler. çok fazla olan bu listenin hepsi sayfayasgimadı. Aşağıya ilerleyip incelemeye devam edebiliriz. Ya da sadece hedef uygulamaya bakalım.

dpkg -l | grep synaptic → direkt hedef uygulamaya bakalım.

veya

dpkg -l synaptic → direkt hedef uygulamaya bakalım (apt search'te çıkan sonuçlardan sadece birisini, ki en önemlisini sergiledi)

```
root@kali:~# dpkg -l synaptic
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/half-inst/trig-aWait/Trig-pend
| / Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name          Version       Architecture Description
||-->
+++
ii  synaptic      0.90.2+b1    amd64        Graphical package manager
root@kali:~#
```

.deb : paketlerin uzantısı

find /root -iname *.deb ➔ adında deb ile bitenleri aratalım.

Hepsi aynı uzantıda olduğunu gördük. **/var/cache/apt/archives/**

```
/var/cache/apt/archives/libobt2v5_3.6.1-9_amd64.deb
/var/cache/apt/archives/gnome-disk-utility_3.34.0-2+b1_amd64.deb
/var/cache/apt/archives/libvte-2.91-common_0.60.3-1_amd64.deb
/var/cache/apt/archives/libdiodon0_1.10.0-1_amd64.deb
/var/cache/apt/archives/libcryptsetup12_2%3a2.3.3-1kali1_amd64.deb
/var/cache/apt/archives/libwpe-1.0-1_1.6.0-1_amd64.deb
/var/cache/apt/archives/python3-samba_2%3a4.11.5+dfsg-1+b1_amd64.deb
/var/cache/apt/archives/libiptc0_1.8.5-2_amd64.deb
/var/cache/apt/archives/python3-paste_3.4.2+dfsg1-1_all.deb
/var/cache/apt/archives/libdrm-intel1_2.4.102-1_amd64.deb
/var/cache/apt/archives/network-manager-vpnc-gnome_1.2.6-3_amd64.deb
```

cd /var/cache/apt/archives/ ➔ hedef dizine (yükleme paketlerinin olduğu yere) gittik.

ls ➔ listeledik.

```
xtermcvnviewer_1%3a1.3.9-10_amd64.deb
xvfb_2%3a1.20.8-2_amd64.deb
xxd_2%3a8.2.0716-3_amd64.deb
yelp_3.36.0-1_amd64.deb
yelp-xsl_3.36.0-1_all.deb
youtube-dl_2020.03.24-1_all.deb
youtube-dl_2020.06.16.1-1_all.deb
zeitgeist-core_1.0.2-3_amd64.deb
zenity_3.32.0-5_amd64.deb
zenity-common_3.32.0-5_all.deb
zlib1g_1%3a1.2.11.dfsg-2_amd64.deb
zlib1g-dev_1%3a1.2.11.dfsg-2_amd64.deb
zsh_5.8-5_amd64.deb
zsh-common_5.8-5_all.deb
root@kali:/var/cache/apt/archives#
```

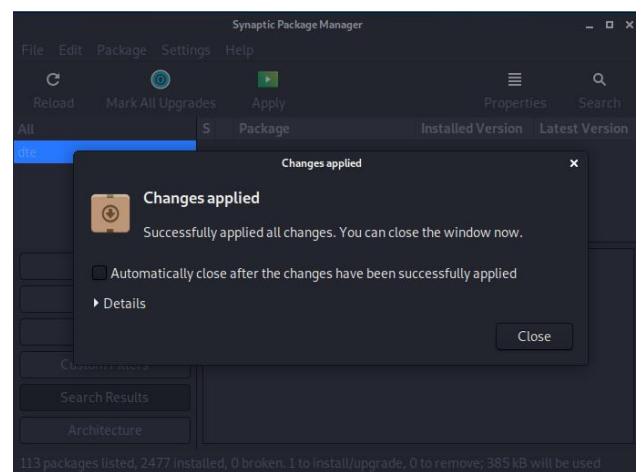
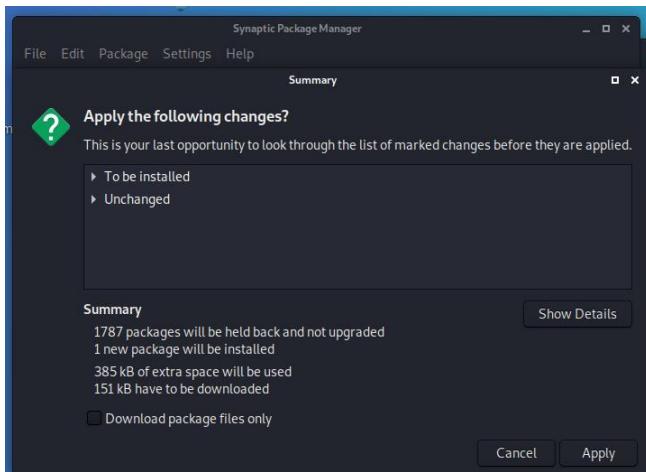
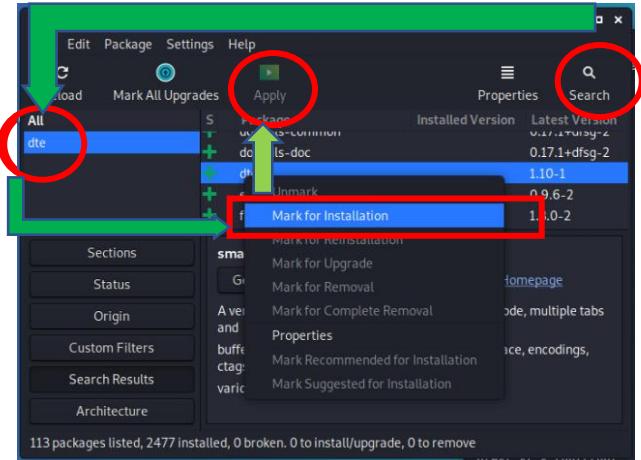
dpkg -c autopsy_2.24-4_all.deb ➔ belirtilen paketi açarız

-c contents

```
-rw-r--r-- root/root      3260 2008-09-29 02:42 ./usr/share/autopsy/pict/menu_t_hg_link.jpg
-rw-r--r-- root/root      2418 2008-09-29 02:42 ./usr/share/autopsy/pict/menu_t_hg_org.jpg
-rw-r--r-- root/root      3736 2008-09-29 02:42 ./usr/share/autopsy/pict/menu_t_hm_cur.jpg
-rw-r--r-- root/root      3361 2008-09-29 02:42 ./usr/share/autopsy/pict/menu_t_hm_link.jpg
-rw-r--r-- root/root      2462 2008-09-29 02:42 ./usr/share/autopsy/pict/menu_t_hm_org.jpg
-rw-r--r-- root/root      1448 2008-09-29 02:42 ./usr/share/autopsy/pict/sanit_b_norm.jpg
-rw-r--r-- root/root      1558 2008-09-29 02:42 ./usr/share/autopsy/pict/sanit_b_san.jpg
-rw-r--r-- root/root     18357 2008-09-29 02:42 ./usr/share/autopsy/pict/sanitized.jpg
-rw-r--r-- root/root      1963 2008-09-29 02:42 ./usr/share/autopsy/pict/srch_b_lorig.jpg
-rw-r--r-- root/root      2180 2008-09-29 02:42 ./usr/share/autopsy/pict/srch_b_lun.jpg
-rw-r--r-- root/root      2111 2008-09-29 02:42 ./usr/share/autopsy/pict/srch_b_str.jpg
-rw-r--r-- root/root      2445 2008-09-29 02:42 ./usr/share/autopsy/pict/srch_b_un.jpg
-rw-r--r-- root/root      1357 2008-09-29 02:42 ./usr/share/autopsy/pict/tab_close.jpg
-rw-r--r-- root/root      1253 2008-09-29 02:42 ./usr/share/autopsy/pict/tab_help.jpg
-rw-r--r-- root/root      2906 2008-09-29 02:42 ./usr/share/autopsy/pict/tl_t_data_cur.jpg
-rw-r--r-- root/root      2580 2008-09-29 02:42 ./usr/share/autopsy/pict/tl_t_data_link.jpg
-rw-r--r-- root/root      2216 2008-09-29 02:42 ./usr/share/autopsy/pict/tl_t_notes_link.jpg
-rw-r--r-- root/root      1715 2008-09-29 02:42 ./usr/share/autopsy/pict/tl_t_notes_org.jpg
-rw-r--r-- root/root      2844 2008-09-29 02:42 ./usr/share/autopsy/pict/tl_t_tl_cur.jpg
-rw-r--r-- root/root      2518 2008-09-29 02:42 ./usr/share/autopsy/pict/tl_t_tl_link.jpg
```

/ust/bin/synaptic → kısa yolunu yazınca programın çalıştığını gördük

Search ile **dte**'yi aratıp bulup sağ tıklayıp **Mark for Installation** yapalım. Sonrasında **Apply** butonuna basalım.



Firefox 'da <http://www.gnu.org/software/software.html> açalım.

Sayfanın en altında yer alan uygulama listesinden "hello" uygulamasını açalım <http://www.gnu.org/software/hello/>

<https://mirrors.ocf.berkeley.edu/gnu/hello/> açalım.

The GNU Hello program produces a familiar, friendly greeting. Yes, this is another implementation of the classic program that prints "Hello, world!" when you run it.

However, unlike the minimal version often seen, GNU Hello processes its argument list to modify its behavior, supports greetings in many languages, and so on. The primary purpose of GNU Hello is to demonstrate how to write other programs that do these things; it serves as a model for [GNU coding standards](#) and [GNU maintainer practices](#).

GNU Hello is written in C. For implementations in other programming languages, notably including translation into other languages, please see the [GNU Gettext](#) distribution.

Download

Stable source releases can be found on the main GNU download server ([HTTPS](#), [HTTP](#), [FTP](#)) and its [mirrors](#); please [use a mirror](#) if possible.

“Hello-2-10-tar-gz-sig” sağ tıklayalım “Copy Link Location” seçelim.

File Name	File Size	Date
Parent directory/	-	-
hello-2.10.tar.gz.sig	819 B	2014-Nov-16 12:08
hello-2.10.tar.gz	708.9 KIB	2014-Nov-16 12:08
hello-2.9.tar.gz	190 B	2013-Oct-09 23:49
hello-2.9.tar.gz	706.7 KIB	2013-Oct-09 23:49
hello-2.8.tar.gz	190 B	2012-Apr-20 17:55
hello-2.8.tar.gz	681.1 KIB	2012-Apr-20 17:55
hello-2.6-2.7.d	189 B	2011-Mar-28 22:44
hello-2.6-2.7.d	164.5 KIB	2011-Mar-28 22:44
hello-2.7.tar.xz	189 B	2011-Mar-28 22:44
hello-2.7.tar.xz	392.5 KIB	2011-Mar-28 22:44
hello-2.7.tar.xz	189 B	2011-Mar-28 22:44
hello-2.7.tar.xz	585.6 KIB	2011-Mar-28 22:44
hello-2.6.tar.xz	189 B	2010-Apr-07 23:13
hello-2.6.tar.xz	388.0 KIB	2010-Apr-07 23:13

Terminale wget komutuyla beraber kopyaladığımız linki yazacağız ve uygulamayı indireceğiz.

The non-interactive network downloader.
#wget

wget https://mirrors.ocf.berkeley.edu/gnu/hello/hello-2.10.tar.gz →
ls →

```
root@kali:~# Wget https://mirrors.ocf.berkeley.edu/gnu/hello/hello-2.10.tar.gz
bash: Wget: command not found
root@kali:~#
root@kali:~# wget https://mirrors.ocf.berkeley.edu/gnu/hello/hello-2.10.tar.gz
--2021-11-23 18:50:27-- https://mirrors.ocf.berkeley.edu/gnu/hello/hello-2.10.tar.gz
Resolving mirrors.ocf.berkeley.edu (mirrors.ocf.berkeley.edu) ... 169.229.226.30, 2607:f140:8801::1:30
Connecting to mirrors.ocf.berkeley.edu (mirrors.ocf.berkeley.edu)|169.229.226.30|:443... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 725946 (709K) [application/octet-stream]
Saving to: 'hello-2.10.tar.gz'

hello-2.10.tar.gz          100%[=====] 708.93K   290KB/s   in 2.4s

2021-11-23 18:50:31 (290 KB/s) - 'hello-2.10.tar.gz' saved [725946/725946]

root@kali:~# ls
Desktop  Documents  Downloads  hello-2.10.tar.gz  log.txt  Music  Pictures  Public  Templates  thinclient_drives  Videos
root@kali:~#
```

#tar

an archiving utility

tar -xvf hello-2.10.tar.gz ➔ zip dosyayı extract yaptık.

ls -l ➔ listede zipin açıldığını gördük

```
root@kali:~# ls -l
total 756
drwxr-xr-x  3 root root  4096 May 14  2020 Desktop
drwxr-xr-x  3 root root  4096 May 13  2020 Documents
drwxr-xr-x  2 root root  4096 Feb  5  2020 Downloads
drwxr-xr-x 11 root root  4096 Nov 16  2014 hello-2.10
-rw-r--r--  1 root root 725946 Nov 16  2014 hello-2.10.tar.gz
-rw-r--r--  1 root root   245 Nov 23 16:55 log.txt
drwxr-xr-x  2 root root  4096 Feb  5  2020 Music
drwxr-xr-x  2 root root  4096 Feb  5  2020 Pictures
drwxr-xr-x  2 root root  4096 Feb  5  2020 Public
drwxr-xr-x  2 root root  4096 Feb  5  2020 Templates
drwxr-xr-t  2 root root  4096 Feb  5  2020 thinclient_drives
drwxr-xr-x  2 root root  4096 Feb  5  2020 Videos
root@kali:~#
```

cd hello-2.10 ➔ dosyanın içine gittik

ls ➔ listeledik

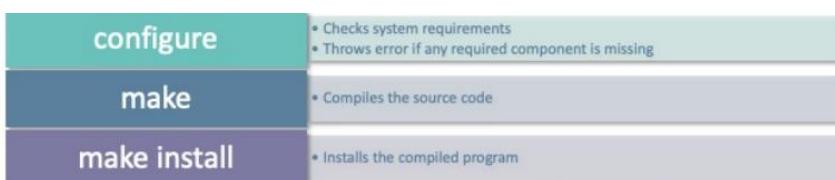
```
root@kali:~# cd hello-2.10
root@kali:~/hello-2.10# ls
ABOUT-NLS  build-aux  config.in    contrib  GNUmakefile  lib      Makefile.am  NEWS    README-dev  tests
acllocal.m4 ChangeLog  configure    COPYING   hello.1     m4      Makefile.in  po      README-release THANKS
AUTHORS   ChangeLog.0 configure.ac doc      INSTALL    maint.mk  man      README    src      TODO
root@kali:~/hello-2.10#
```

“./Configürasyon” ile sistemi kontrol ederiz.

“Make” ile derlemeliyiz.

“Make install” ile kurmalıyız.

Install from Source Code



```
(kali㉿kali)-[~]
$ cd hello-2.10
(kali㉿kali)-[~/hello-2.10]
$ ls
ABOUT-NLS  build-aux  config.in    contrib  GNUmakefile  lib      Makefile.am  NEWS    README-dev  tests
acllocal.m4 ChangeLog  configure    COPYING   hello.1     m4      Makefile.in  po      README-release THANKS
AUTHORS   ChangeLog.0 configure.ac doc      INSTALL    maint.mk  man      README    src      TODO
(kali㉿kali)-[~/hello-2.10]
$ ./configure
(kali㉿kali)-[~/hello-2.10]
$ sudo make install
[sudo] password for kali:
make install-recursive
make[1]: Entering directory '/home/kali/hello-2.10'
Making install in po
make[2]: Entering directory '/home/kali/hello-2.10/po'
installing bg.mo as /usr/local/share/locale/bg/LC_MESSAGES/hello.mo
installing ca.mo as /usr/local/share/locale/ca/LC_MESSAGES/hello.mo
installing da.mo as /usr/local/share/locale/da/LC_MESSAGES/hello.mo
installing de.mo as /usr/local/share/locale/de/LC_MESSAGES/hello.mo
installing el.mo as /usr/local/share/locale/el/LC_MESSAGES/hello.mo
installing eo.mo as /usr/local/share/locale/eo/LC_MESSAGES/hello.mo
installing es.mo as /usr/local/share/locale/es/LC_MESSAGES/hello.mo
```

./configure ➔ Sistemi kontrol eder (bu bir dosyadır. o yüzden dosya ./ ile çalışır))

```
checking for CFPrefrencesCopyAppValue... no
checking for CFLocaleCopyCurrent... no
checking for GNU gettext in libc... yes
checking whether to use NLS... yes
checking where the gettext function comes from... libc
checking that generated files are newer than configure..
configure: creating ./config.status
config.status: creating Makefile
config.status: creating po/Makefile.in
config.status: creating config.h
config.status: executing depfiles commands
config.status: executing po-directories commands
config.status: creating po/POTFILES
config.status: creating po/Makefile
```

make ➔ derleme işlemini yaptı (make komut iken configure dosyadır)

```
src/netto.c &&
mv -f $depbase.Tpo $depbase.Po
gcc -g -O2 -o hello src/hello.o ./lib/libhello.a
rm -f lib/charset.alias-t lib/charset.alias && \
/bin/bash ./lib/config.charset 'x86_64-unknown-linux-gnu' > lib/charset.alias-t
&& \
mv lib/charset.alias-t lib/charset.alias
rm -f lib/ref-add.sed-t lib/ref-add.sed && \
sed -e '/^#/d' -e 's/@''PACKAGE''@/hello/g' lib/ref-add.sin > lib/ref-add.sed-t
&& \
mv lib/ref-add.sed-t lib/ref-add.sed
rm -f lib/ref-del.sed-t lib/ref-del.sed && \
sed -e '/^#/d' -e 's/@''PACKAGE''@/hello/g' lib/ref-del.sin > lib/ref-del.sed-t
&& \
mv lib/ref-del.sed-t lib/ref-del.sed
make[2]: Leaving directory '/root/hello-2.10'
make[1]: Leaving directory '/root/hello-2.10'
root@ip-10-10-101-103:/root/hello-2.10#
```

(sudo) make install ➔ kurulum yaptık.

```
.alias ; \
    rm -f /usr/local/lib/charset.tmp ; \
fi ; \
fi
/bin/mkdir -p '/usr/local/share/info'
/usr/bin/install -c -m 644 ./doc/hello.info '/usr/local/share/info'
install-info --info-dir='/usr/local/share/info' '/usr/local/share/info/hello.info'
/bin/mkdir -p '/usr/local/share/man/man1'
/usr/bin/install -c -m 644 hello.1 '/usr/local/share/man/man1'
make[3]: Leaving directory '/root/hello-2.10'
make[2]: Leaving directory '/root/hello-2.10'
make[1]: Leaving directory '/root/hello-2.10'
root@ip-10-10-101-103:/root/hello-2.10#
```

./hello → Çalıştığını gördük.
Mutlu son

```
root@ip-10-10-191-193:~/hello-2.10# ./hello  
Hello, world!
```

Path değişkenini bu programın kısa yolunu eklersek artık her yerde **hello** yazınca program çalışır.

export PATH=\$PATH:/root/hello-2.10
hello →

```
root@kali:~/hello-2.10# export PATH=$PATH:/root/hello-2.10  
root@kali:~/hello-2.10# echo $PATH  
/usr/bin:/bin:/root/hello-2.10  
root@kali:~/hello-2.10# cd  
root@kali:~# hello  
Hello, world!  
root@kali:~#
```

apt remove hello → hello programını kaldırır.

Apt purge == apt autoremove → disk temizliği yapar.

Script Yazma

(Kaynak : <https://www.shellscale.sh/>)

<https://tryhackme.com/room/bashscripting>

Exploit geliştirme. Aktif Siberçiler kullanır

cd /etc/init.d → çalıştırılabilir dosyalar

file openvpn → Dosya tipine bakalım

```
root@kali:/etc/init.d# file openvpn  
openvpn: POSIX shell script, ASCII text executable
```

nano apache2 → Çalışabilir bir sistem dosyasını text editörle açalım ve içine bakalım. İlk satırdaki **!/bin/sh** notu bunu bash script kod olduğu anlamına gelir . Not satırları # (diaz) ile baslar

Bu servis, çalıştırıldığımda veya işlem yaptığımda bu kodlara istinaden reaksiyon gösterir

```
GNU nano 5.2                                         apache2
#!/bin/sh
### BEGIN INIT INFO
# Provides:          apache2
# Required-Start:    $local_fs $remote_fs $network $syslog $named
# Required-Stop:     $local_fs $remote_fs $network $syslog $named
# Default-Start:    2 3 4 5
# Default-Stop:     0 1 6
# X-Interactive:    true
# Short-Description: Apache2 web server
# Description:      Start the web server
# This script will start the apache2 web server.
### END INIT INFO

DESC="Apache httpd web server"
NAME=apache2
DAEMON=/usr/sbin/$NAME

SCRIPTNAME="${0##*/}"
SCRIPTNAME="${SCRIPTNAME##*[0-9][0-9]}"
if [ -n "$APACHE_CONFDIR" ] ; then
    if [ "${APACHE_CONFDIR##*/etc/apache2-}" != "${APACHE_CONFDIR##*/etc/apache2-}" ] ; then
        DIR_SUFFIX="${APACHE_CONFDIR##*/etc/apache2-}"
    else
        DIR_SUFFIX=
    fi
elif [ "${SCRIPTNAME##apache2-}" != "$SCRIPTNAME" ] ; then
    DIR_SUFFIX="-${SCRIPTNAME##apache2-}"
    APACHE_CONFDIR=/etc/apache2$DIR_SUFFIX
else
    DIR_SUFFIX=
    APACHE_CONFDIR=/etc/apache2
fi

[ Read 355 lines ]
^G Help      ^O Write Out   ^W Where Is      ^K Cut          ^T Execute      ^C Location     M-U Undo
^X Exit      ^R Read File   ^Y Replace      ^U Paste        ^J Justify      ^_ Go To Line   M-E Redo
                                         M-A Set Mark
                                         M-6 Copy
```

Echo \$SHELL ➔ kabuk
sh
zsh
bash

Shell kabuklarının farkları (ksh ve bash tüm özellikleri barındırıyor)

Unix Shell application comparison table					
Application	sh	csh	ksh	bash	tcsh
Job control	N	Y	Y	Y	Y
Aliases	N	Y	Y	Y	Y
Input/Output redirection	Y	N	Y	Y	N
Command history	N	Y	Y	Y	Y
Command line editing	N	N	Y	Y	Y
Vi Command line editing	N	N	Y	Y	Y
Underlying Syntax	sh	csh	ksh	sh	csh

Script Örneği:

Masaüstünde myscript adlı bir dosya oluşturalım ve içini doldurup kaydedelim

```
* /root/Desktop/myscript - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
#!/bin/bash
# bu bir yorum satırı
echo "Merhaba" |
```

ls -l ➔ listede oluşturduğumuz dosyayı gördük.

./myscript ➔ çalışmadı (Dikkat dosyayı uzantı şeklinde yazarız)

Dizine baktık, gördük. Çalışmadı. Listeleyince x (executable) yetkisi olmadığını gördük.

Executable yapmadan aşağıdaki şekilde çalıştırabiliriz.

sh myscript ➔ çalıştı.

zsh myscript ➔ çalıştı.

bash myscript ➔ çalıştı.

yetki verip çalıştırıralım

chmod 777 myscript ➔ hepsini maksimum yetki verdik.

chmod +x ➔ hepsine executable ekledik.

./myscript ➔ çalıştı (Dikkat dosyayı uzantı şeklinde yazarız).

Export PATH=\$PATH:/root/Desktop ➔ masaüstünün dizin bilgisini #PATH'e ekledik.

Myscript ➔ çalıştı (Dikkat uzantı vermedik sadece dosya adını yazdık).

```

root@kali:~# cd Desktop/
root@kali:~/Desktop# ls
kali-burpsuite.desktop  kali-msfconsole.desktop  myscript
kali-dirb.desktop       kali-nikto.desktop      PEASS
kali-hashcat.desktop   kali-nmap.desktop       wordlists
root@kali:~/Desktop# file myscript
myscript: empty
root@kali:~/Desktop# file myscript
myscript: ASCII text
root@kali:~/Desktop# file myscript
myscript: Bourne-Again shell script, ASCII text executable
root@kali:~/Desktop# ./myscript
bash: ./myscript: Permission denied
root@kali:~/Desktop# ls -l
total 32
-rwxr-xr-x 1 root root 134 May 13 2020 kali-burpsuite.desktop
-rwxr-xr-x 1 root root 97 May 13 2020 kali-dirb.desktop
-rwxr-xr-x 1 root root 106 May 13 2020 kali-hashcat.desktop
-rw-r--r-- 1 root root 135 May 13 2020 kali-msfconsole.desktop
-rwxr-xr-x 1 root root 100 May 13 2020 kali-nikto.desktop
-rwxr-xr-x 1 root root 97 May 13 2020 kali-nmap.desktop
lrw-r--r-- 1 root root 53 Nov 23 20:30 myscript
drwxr-xr-x 4 root root 4096 May 14 2020 PEASS
lrwxrwxrwx 1 root root 20 May 13 2020 wordlists → /usr/share/wordlists
root@kali:~/Desktop# █

```

Dosyayı güncelledik.

\$1 : ilk girdi anlamındadır.

```

/root/Desktop/myscript - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
#!/bin/bash

# bu bir yorum satiri

echo "Merhaba $1"
pwd      I
whoami
hostname

```

Path'e ekledik ama biz yine uzantı şeklinde çalışıralım

Cd desktop ➔ dosyanın olduğu dizine gittik

./myscript huriye ➔ çalıştı (huriye \$1'e eşleşti)

```

root@kali:~/Desktop# ./myscript huriye
Merhaba huriye
/root/Desktop
root
kali
root@kali:~/Desktop# █

```

Script Örneği:

Dosyayı değiştirdik (ilk satırı ikinci bir girdi olacağını belirttik)

```
* /root/Desktop/myscript - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
#!/bin/bash

# bu bir yorum satiri

echo "Merhaba $1 $2"
pwd
whoami
hostname
```

./myscript huriye özdemir → çalıştı (huriye \$1'e özdemir \$2'ye eşleşti)

```
Kali
root@kali:~/Desktop# ./myscript huriye ozdemir
Merhaba huriye
/root/Desktop
root
kali
```

Script Örneği:

Yapılan işlemi yenidosya adlı başka bir dosyaya yazın ve yeni dosyayı okusun

```
* /root/Desktop/myscript - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
#!/bin/bash

# bu bir yorum satiri

echo "Merhaba $1" >> yenidosya && cat yenidosya
```

Ls →

./myscript "hayriye demir" → çalıştı (hayriye demir \$1'e eşleşti. Dikkat Tırnak içi tek parametre)

Masaüstüne yenidosya adlı dosya oluşturdu. ve içindeki bilgiyi ekrana getirdi

Is → yenidosya'nın listeye eklendiğini gördük.

```
root@kali:~/Desktop# ls
kali-burpsuite.desktop  kali-hashcat.desktop    kali-nikto.desktop  myscript  wordlists
kali-dirb.desktop       kali-msfconsole.desktop  kali-nmap.desktop   PEASS
root@kali:~/Desktop# ./myscript huriye
Merhaba huriye
root@kali:~/Desktop# ls
kali-burpsuite.desktop  kali-hashcat.desktop    kali-nikto.desktop  myscript  wordlists
kali-dirb.desktop       kali-msfconsole.desktop  kali-nmap.desktop   PEASS    yenidosya
root@kali:~/Desktop#
```

Script Örneği: Masaüstünde bir dosyaya yazacağımız script ile Apache programının konfigürasyon portu içindeki 80 portunu 8080 olarak değiştireceğiz.

Adım-1: Konfigürasyon dosyasının dizinini bir değişkene atadık.

```
apache_conf=/etc/apache2/ports.conf
```

Adım-2 Ekrana “checking Configuration file” yazdırıyalım.

```
Echo "checking Configuration file"
```

Adım-3: Listen 80 metnini yakalayalım ve boşluk delimeter olarak ikinci sütundaki 80 sayısını alalım (portu bulalım) bu değeri previousport adlı değişkene atayalım.

Not: parantez içi bir değerleri değişkene atarken parantez başına \$ işaretini kullanırız

```
previousport=$(grep -i "Listen 80" $apache_conf | cut -d ' ' -f2)
```

Adım-4: Sonra ekrana eski port bilgisini yazdırıyalım.

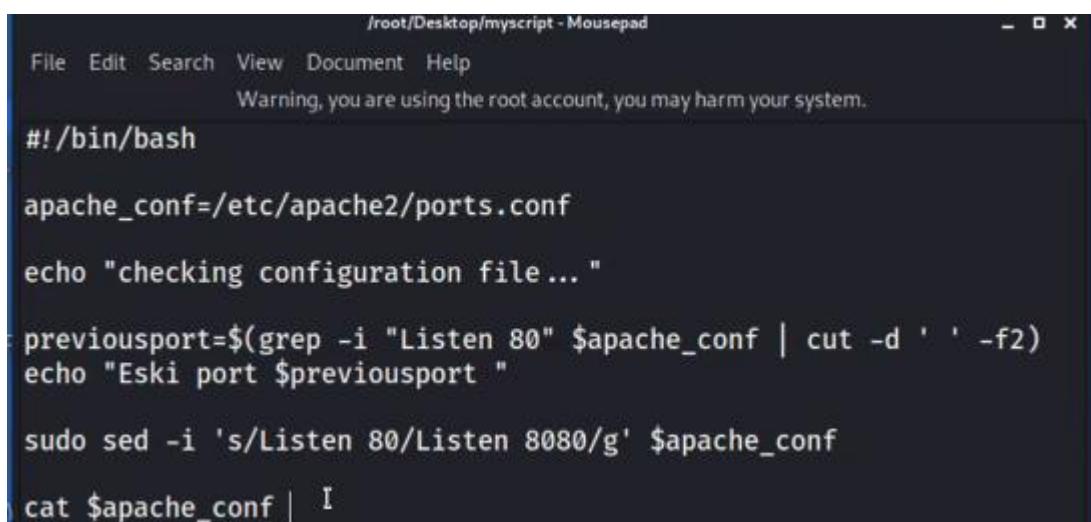
```
Echo "eski Port = previousport"
```

Adım-5: Port değerini 8080 olarak değiştirelim.

```
Sudo sed -i 's/Listen 80/Listen 8080/g'
```

Adım-6: Degeri yazdırıyalım.

```
cat $apache_conf
```



```
/root/Desktop/myscript - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.

#!/bin/bash

apache_conf=/etc/apache2/ports.conf

echo "checking configuration file ..."

previousport=$(grep -i "Listen 80" $apache_conf | cut -d ' ' -f2)
echo "Eski port $previousport"

sudo sed -i 's/Listen 80/Listen 8080/g' $apache_conf

cat $apache_conf | I
```

```
root@kali:~/Desktop# ./myscript
checking configuration file ...
Listen 80
root@kali:~/Desktop# []
```

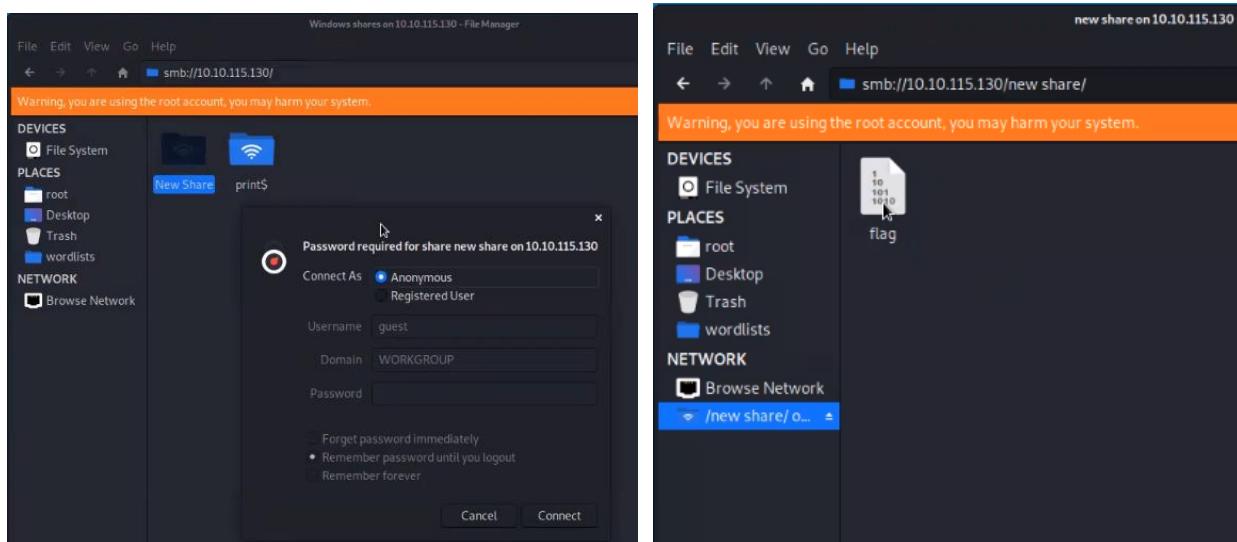
BADGERS		CYBERSMURFS		BOL7		HACTIVISTS	
Basic Commands:	ls	help		more		head	
	pwd	cd		less		tail	
	man	cat		whereis		grep	
	mkdir	echo	Output redirection : < >>	cut		uname	
	touch	find		tr		which	
	rm	mv		cp		file	
	locate					ifconfig	
	history						
		File management		ps		df	
		su	All directories under /	top		proc/meminfo	
User management	sudo	chmod		fg		vmstat	
	adduser	File permissions		bg		/proc/cpuinfo	
	deluser		List of the services /etc/init.d	jobs		netstat	
	usermod	service		kill		w	
	groups	systemctl					
	id						
Package management	chown						
	sudoers file						
		Installing from source code					

SMB bağlantısı (Linux cihazlar dosya paylaşımı)

SMB (Server Message Block) servisi üzerinde paylaşılan dosyalar **Samba** sistemiyle ilgili ipucu vardı. Google'dan nasıl erişilebileceğini bulabiliriz. File Manager (Windows'ta File Browser) SMB://HedefIPAdresi yazınca hedef dizine erişilir. Kullanıcı adı ve parola gereklidir.

SMB://110.10.115.130 →

Dosyaya erişmek isteyince kullanıcı bilgileri ve password girilir. Sonra dosya açılır.



Terminal üzerinden de bağlantı yapılabilir ancak her iki cihazında **smb** ve **nmb** servisleri çalışır durumda olmalıdır.

Sudo systemctl restart smb ➔ smb servisi açma komutu- password girilir.

Sudo systemctl restart nmb ➔ nmb servisi açma komutu- password girilir.

smbclient -L// HedefIpAdresi ➔ smb bağlantısını yapıp paylaşılan dosyalari listeler

```
[suleyman@SMBSRV samba]$ sudo systemctl restart nmb
[suleyman@SMBSRV samba]$ smbclient -L //192.168.0.107/
Unable to initialize messaging context
Enter WORKGROUP\suleyman's password:
```

Sharename	Type	Comment
print\$	Disk	Printer Drivers
paylas	Disk	65 x 24
etc	Disk	
IPC\$	IPC	IPC Service (Samba Server 4.9.1)
suleyman	Disk	Home Directories

Reconnecting with SMB1 for workgroup listing.

Server	Comment
-----	-----
Workgroup	Master
-----	-----
WORKGROUP	

smbclient //HedefIpAdresi/Paylas ➔ smb bağlantısı ve erişilmek istenen dosya adı yazılır.

2*tab 'a basılırsa kullanılabilicek komutlar ekrana gelir. (touch, cat ve nano komutları yok)

```
smb: \>
?
      dir      lock      posix_encrypt   recurse      tcon
..      du       logoff    posix_mkdir     reget       tdis
allinfo echo     logon     posix_open     rename     tid
altname exit    lowercase  posix_rmdir    reput      timeout
archive get     ls        posix_unlink   rm        translate
backup  geteas   mask     posix_whoami   rmdir      unlock
blocksize getfacl md      print       scopy      utimes
cancel   hardlink mget    prompt      setea      volume
case_sensitive help   mkdir    put        setmode    vuid
cd      history  more     pwd        showacls   wdel
chmod   iosize   mput    q         showconnect
chown   l        newer   queue      stat
close   lcd     notify  quit      symlink
del     link    open    rd        tar
deltree listconnect posix  readlink  tarmode
smb: \> ls
```

Örneğin;

ls ➔ paylaş klasörü içeriğini listeler

more hosts ➔ karşı cihaz paylaş klasörü içinde bulunan hosts dosyası içini sergiler

mkdir test ➔ karşı cihaz paylaş klasörü içinde bulunan test adlı dizin oluşturur.

Karşı cihaz paylaş klasörü içinde bulunan bir dosyayı kendi cihazına kopyalayabiliriz.

FTP SERVER Baglantisi

FTP server IP adresi bilinmelidir. Bizim bu soruda bağlanılan cihazın içindeki FTP server bağlanıyoruz. O yüzdé FTP IP adresi cihazın IP adresi

FTP [IP adresi] ➔ Kullanıcı adı girilmesi isteniyor. Burada root veya Sudo yetkisi olan hesap bilgileri girmelidir

Name: sammy

Password: sam

ftp servere bağlandı bilgisi gelir.

ls ➔ FTP listelenir

cd files ➔ FTP içinde var olan tek dosyaya girelim.

ls ➔ files dosyası içeriğini listeleyelim.

```
sammy@jessie:~$ ftp 10.10.45.173
Connected to 10.10.45.173.
220 Welcome to HackerAcademy FTP service.
Name (10.10.45.173:hacker): sammy
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 1002    1002      4096 Jun 15 14:40 files
226 Directory send OK.
ftp> cd files
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  2 1002    1002      725946 Nov 16  2014 hello.tar.gz
-rw-r--r--  1 0        0          14 Jun 15 13:47 test.txt
226 Directory send OK.
```

Linux kodlar

<https://explainshell.com/>

Linux Challenge

<https://tryhackme.com/room/linuxosfundfb>

Linux Terminalden başka bir OS'e ssh bağlantısı

ssh HedefCihazAdı@HedefCihazIP ➔ parola girilir (ancak parola girildiği terminal ekranından anlaşılmaz)

1. Cihazın Hostname ?

hostname ➔ Linux Terminalde cihazın adı (kullanıcı adı değil) sergilenebilir. Cevap :jessie:

2. Bu cihazda Kullanıcılar kimler?

ls -l home ➔ Linux Terminalde cihaz kullanıcılarına ait dizinleri sergiler. Ancak silinmiş bir kullanıcının dizini burada kalmış olabilir

tail /etc/passwd ➔ sistem kullanıcıları dışında farklı adlarla olan kullanıcılar cihazın kullanıcılarıdır. Cevap: hacker, sammy, vagrant

Answer the questions below

What is the hostname of the machine?

jessie

Correct Answer

Who are the users on this machine? Give space to separate each user. (Sort alphabetic order)

hacker, sammy, vagrant

Correct Answer

3. Local Makine ip adresi?

ifconfig ➔ path ortam değişkenine tanımlı olsaydı bu komutla ip adresini görebilirdik
/sbin/ifconfig/ ➔ dizin yolunu vererek dosyaya erişir ve IP adresini görebiliriz.

LocalHost genelde 127.0.0.1 dir.

4. Gateway IP adresi?

netstat -nr ➔ routing tablosunu sergiler.

5. Linux sistemin Kernel Versiyonu nedir?

Uname -a ➔ detaylı sistem bilgileri görünür.

6. Root dizininin mount edilmiş olan disk adı nedir?

df -h ➔ sistem üzerindenki disk bilgilerinin human readable olarak sergiletir

7. Sistemin kb cinsinden memory büyülüğu?

Cat /proc/meminfo ➔ ilk satırda yer alır

8. Init Process'in PID'si?

Cevap her zaman 1'dir.

Ps -aux | more ➔ process bilgileri

Top ➔

9. Sistemin kb cinsinden memory büyülüğu?

➔ ilk satırda yer alır

10. file.20000 adlı dosyanın içinde kaç tane satır var ?

find / -iname file.20000 ➔ root dizininde (/ işaret onu ifade eder) aradım ancak yetkili kullanıcı olmadığı için her dosyaya erişemedim ancak ilgili dosyayı bulduk

cd /home/hacker/dir-2/dir-20/dir-200/ ➔ ilgili dizine gittik

ls ➔ dizini listeledik

cat file.20000 ➔ icini açtık (sayılamayak kadar büyük sayıda satır)

wc -l file.2000 ➔ 2000 satır sayısı bilgisi ekrana geldi.

What is the IP address of the local machine?	<input type="text" value="127.0.0.1"/>	Correct Answer
What is the gateway IP address of the machine?	<input type="text" value="10.10.0.1"/>	Correct Answer
What is the kernel version of the system?	<input type="text" value="3.16.0-9-amd64"/>	Correct Answer
What is the name of the disk that the root directory is mounted?	<input type="text" value="xvda1"/>	Correct Answer
What is the memory (kB) of the system?	<input type="text" value="1022620"/>	Correct Answer
What is the PID of init process?	<input type="text" value="1"/>	Correct Answer
How many total lines are in "file.20000"?	<input type="text" value="2000"/>	Correct Answer Hint

11. Home dizinindeki gizli dosya

ls -l → gizli dosya görünmez

ls -al → gizli dosyalar dahil sergilenir

12. sammy'nin passwordu?

very-important_file → gizli dosyanın içinde yazıyor

13. htop.dep tipi?

find htop.dep → home/sammy/htop.deb altında olduğunu gördük

cd home/sammy/ → sammy hesabının home dizinine geçtik

ls → listede htop.deb dosyasını gördük

sammy kullanıcısının parola bilgisini biliyoruz. Oraya geçi bundan sonraki soruları cevaplayacağız

su -sammy → gelen ekrana parolayı girince kullanıcı değiştirdik.

file htop.deb → ilgili dosyanın tipini görebiliriz

14. hello-2-10.tr.gz dosyasının görevi ?

ls → ilgili dosya sammy home dizininde olduğunu gördük

tar -xvf hello-2-10.tr.gz → zip dosyasını extract ettik

cd hello-12.10/ → açılan dizine girdik

cat TODO → içinde ceap yazılı “* submit a new hello.pot.”

What is the name of the secret file under the home folder?

Correct Answer

What is the password of sammy?

Correct Answer

What is the type of htop.deb file?

Correct Answer

Hint

What is the task in the hello-2.10.tar.gz file?

Correct Answer

Hint

15. space dizinini a.tar.gz ismiyle arşivle? Derste ziplemeyi öğrenmemiştik. Google'dan bulabiliyoruz. Farklı şekilde arşivlemek mümkün ancak en sık kullanılan aşağıdakidir.

ls -l → dizini gördük.
tar -czvf a.tar.gz space/ →
“c” create
“z” ziple (sıkıştır)
“v” verbose (ayrintı)
“f” file

16. tar.gz dosyasının boyutu ?

Tar birleştirir. gz ise sıkıştırır. Aşağıda z komutu olmadan tar.la arşivleyerek daha büyük bir dosya olurdu. Bunu göstermek için başka bir adla o şekilde arşivleyelim ve boyutlarına bakalım

tr -cvf a-tar-gz space/ →
ls -l → bir önceki soruda oluşturduğumuz zip.li dosyayı gördük.

```
sammy@jessie:~$ tar -czvf a.tar.gz space/
space/
space/OneMegaByte
sammy@jessie:~$ tar -cvf a.tar.gz space/
space/
space/OneMegaByte
sammy@jessie:~$ ls -al
total 1860
drwxr-xr-x  4 sammy sammy   4096 Nov 29 11:27 .
drwxr-xr-x  5 root  root    4096 Jun 15 12:52 ..
-rw-r--r--  1 sammy sammy 1054720 Nov 29 11:29 a.tar.gz
-rw-----  1 sammy sammy     319 Jun 15 15:13 .bash_history
-rw-r--r--  1 sammy sammy    220 Jun 15 12:52 .bash_logout
-rw-r--r--  1 sammy sammy   3515 Jun 15 12:52 .bashrc
drwxr-xr-x 11 sammy sammy   4096 Nov 16 2014 hello-2.10
-rw-r--r--  2 sammy sammy 725946 Nov 16 2014 hello-2.10.tar.gz
-rw-r--r--  1 sammy sammy  75316 May  1 2014 htop.deb
-rw-r--r--  1 sammy sammy    675 Jun 15 12:52 .profile
-rw-r--r--  2 sammy sammy    600 Jun 15 14:46 sammy.flag
-rw-r--r--  1 sammy sammy    252 Jun 15 14:19 scissors.txt
drwxr-xr-x  2 sammy sammy   4096 Jun 15 14:37 space
```

17 Running services in network

netstat -tlnp → root kullanıcısı olmadıgın için ayrıntılı bilgi vermedi
sudo Netstat -tlnp → sudo komutuyla birlikte calisti ve yansida görülen servisleri sırayla cevaba yazacaktık.

18 FTP'de bulunan dosyalar

Bir önce gördüğümüz vsftpd ftp'nin değişmiş bir servisidir. Port nosu 21 olduğundan anlayabiliriz.

How to see FTP files in Linux ile google'yuca cevabı görebiliriz.

ftp 10.010.115.130 → makinenin ftp'sine erişeceğiz. Kullanıcı adı ve parola istediler (hacker ve sam ile girebilirim) Terminalde artık bulunan dizin olarak satır baslarında “ftp” yazar.

ls →
cd files → dizine gittik.
ls → 2 dosya varmış.

```

sammy@jessie:~$ sudo netstat -tnlp
[sudo] password for sammy:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State      PID/Program name
tcp        0      0 0.0.0.0:445              0.0.0.0:*               LISTEN     476/smbd
tcp        0      0 0.0.0.0:139              0.0.0.0:*               LISTEN     476/smbd
tcp        0      0 0.0.0.0:21               0.0.0.0:*               LISTEN     435/vsftpd
tcp        0      0 0.0.0.0:22               0.0.0.0:*
```

FTP erişim ve dizine erişme

```

sammy@jessie:~$ ftp 10.10.115.130
Connected to 10.10.115.130.
220 Welcome to HackerAcademy FTP service.
Name (10.10.115.130:hacker): sammy
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 1002      1002          4096 Jun 15 14:40 files
226 Directory send OK.
ftp> cd files
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    2 1002      1002        725946 Nov 16 2014 hello.tar.gz
-rw-r--r--    1 0        0             14 Jun 15 13:47 test.txt
226 Directory send OK.
ftp> exit
221 Goodbye.
sammy@jessie:~$
```

Archive and gzip the space folder. Give "a.tar.gz" name to this file. Which command and parameter did you use to archive the folder?

Correct Answer

Hint

What is the size (byte) of this tar.gz file?

Correct Answer

Which services are running on the network? Write by alphabetic order.

Correct Answer

Hint

Which files are hosted on FTP?

Correct Answer

Hint

19. File Manager (Windows'ta File Browser) SMB://HedefIPAdresi yazınca hedef dizine erişilir.

SMB://110.10.115.130 → Dosyaya erişmek isteyince kullanıcı bilgileri ve password girilir. Sonra dosya açılır.

20. Scissors.txt icindeki ülkeleri listeleme
cut -d “-” -f3 scissors.txt → delimeter – “tire” olacak şekilde 3. Sütun sergile

```
sammy@jessie:~$ cut -d"-" -f3 scissors.txt
Country
Belgium
United Kingdom
Germany
Netherlands
France
Turkey
Greece
Italy
```

21. Scissors.txt üzerinde yetki ayarlama
chmod 641 scissors.txt → user read+write, group read, others execute

```
sammy@jessie:~$ less /etc/group
sammy@jessie:~$ less /etc/group | grep sudo
sudo:x:27:vagrant,sammy
```

22. Sudo grubunda yer alan kullanıcıları bulma

cd etc/group | sudo →

Which file is shared on SMB?

flag

Correct Answer

Hint

How can you list only countries in scissors.txt file?

cut -d"-" -f3 scissors.txt

Correct Answer

How can you give read and write permission to users, only read permission to group and only execute permission to others for scissors.txt file? Write the full command in a numerical way.

chmod 641 scissors.txt

Correct Answer

Which user is in the sudo group?

sammy, vagrant

Correct Answer

23. root kullanıcısına geçiş yap secret adlı dosya içeriğini yaz.

sudo su → sudo grubunda olduğumuz için root kullanıcıı olduk
ls → secret adlı dosyayı gördük
cat secret → dosyanın içinde “hackeracademy” yazdığını gördük.

24. htop.den paketini bul ve yükle

apt install / htop.deb → normalde yüklenir ancak güncel olmadığı için yükleyemedi.
dpkg -i htop.deb → kurulum yapar
“-i”: install

25. Dışarıda kurulan paketler için oluşturulmuş source listin adını bulma (debians' source list haricinde)

cd /etc/apt →
ls →

google'dan “add source list for installing external Packages” arayalım

cd /etc/apt/source.list.d/ →
ls → sublime-text.list adlı dosya varmış
cat sublime-text.list → dosyada kısayol mevcut

26. Antiword uygulama versiyonu öğrenme

Antiword –version → burada versiyonun kısa sekli vardır.
Dpkg -l | grep antiword → burada versiyonun tamamı vardır.

27. /usr dizininde içinde “hackeracademy” gecen dosyayı bul

grep -ir hackeracademy /usr/* → /usr/r dosyasında bu ibarenin geçtiğini bulduk
Not: Find dosya adını bulur, içeriğini değil

Switch user to root and read the content of the secret file.

HackerAcademy

Correct Answer

Find and install the htop.deb package. Which command and parameter did you use to install .deb package?

dpkg -i htop.deb

Correct Answer

What is the name of the source list for installing external packages other than debians' source.list file?

sublime-text.list

Correct Answer

💡 Hint

What is the version of antiword application?

0.37-10+b1

Correct Answer

Find the file containing hackeracademy keyword in the /usr directory. What is the full path of this file?

/usr/r

Correct Answer

28. List services

Find and inspect the newly added service other OS

Check the sttaus os service and strat

Resolve th error by checking the bash script of the service

After resolving the error, start the service

Get the name of the file under the root home folder

NOT: Bunları kendi makinemizde yapacağız. Öncesinde ssh ile başka makineye bağlanmıştır

cd /etc/systemd/system → sistem dizini

ls -lt → hackeracademy.service en yeni eklene servis adı olduğunu gördük.

“t” : time zaman sıralı listeler

status hackeracademy.service → statüsünün inactive olduğunu gördük.

start hackeracademy.service → başlattık.

status hackeracademy.service → statüsünün hala inactive olduğunu gördük.

Sebebi de root/hackceracademy dizinin olmaması olduğu yazıyor.

Nano hackeracademy.service → dosyayı text editör ile açalım ve bunun hangi servisi calistirdigini gördük

Nano /usr/sbin/hackeracademy.sh → scriptler yazıyor. Burada root dizinin hackeracademy adlı bir dizin olunca calistigini anlayabiliyoruz. Bu servis aslında ip adresini bulup başka dosyaya yazan bir servis.

```

File Actions Edit View Help
GNU nano 2.2.6 File: /usr/sbin/hackeracademy.sh

#!/bin/bash
NOW=$(date "+%d/%m/%Y %H:%M:%S")
if [ -d "/root/hackeracademy/" ]
then
    echo "$NOW - Directory /root/hackeracademy exists." >> /var/log/hackeracademy.service.log
    ip4=$(./sbin/ip -o -4 addr list eth0 | awk '{print $4}' | cut -d/ -f1)
    echo $ip4 >> /root/ip_address_of_mine.txt
    echo $ip4 >> /var/log/hackeracademy.service.log
else
    echo "Error: Directory /root/hackeracademy does not exists."
fi
echo "Betik calisti, Calisma Zamani = $NOW" >> /var/log/hackeracademy.service.log

```

mkdir hackeracademy → root/ dizinindeyken bahse konu dizini oluşturalım.

Ls -l → oluşturduğunu gördük

start hackeracademy.service → başlattık.

systemctl status hackeracademy.service → statüsünün başlatıldığı olduğunu gördük.

ls -l → servisin çalışmasıyla servis scriptte belirtilen dosyayı oluşturdu ve içine ip yazdı.

Cevap dosyanın adı : **ip_address_of_mine.txt**

29. root ip=?

Passwd → eski parolayı sormadan yeni parola (2 defa girilerek) belirlenebilir.

History → yanlışlıkla parolanın terminale yazıldığını ve bu şekilde ulaşabileceğimizi gördük.

Parolanın arasında olan “\n” new line karakteridir.

```

File Actions Edit View Help
root@jessie:~# passwd: Authentication token manipulation error
root@jessie:~# passwd: password unchanged
root@jessie:~#
root@jessie:~# history
1 adduser hacker
2 exit
3 echo -e "1EIsH6eYdGTaNrr\n1EIsH6eYdGTaNrr" | passwd
4 exit
5 exit
6 tail -f /var/log/hackeracademy.service.log
7 date

```

Name of the file under the Root Home Folder: **ip_address_of_mine.txt**

Password of root: **1EIsH6eYdGTaNrr**

List services.

Find and inspect the newly added service to the operating system.

Check the status of service and start.

Resolve the error by checking the bash script of the service.

After resolving the error, start the service.

Get the name of the file under the root home folder.

Correct Answer

What is the root password?

Correct Answer