

# **Temel Linux Bilgileri**

# Niçin bir hacker Linux

- Çoğu (%90) hacking aracı Linux platformu için yazılıyor
- Açık-kaynak

# Temel Linux Kullanımı

**Temel Komut Serisi-1**

**Linux Dosya Sistemi**

**Linux Komut Serisi-2**

**Network Ayarları**

**Servisler**

**Kullanıcı Yönetimi**

**Process**

**Paket Yönetim Sistemi**

**Sistem İzleme**

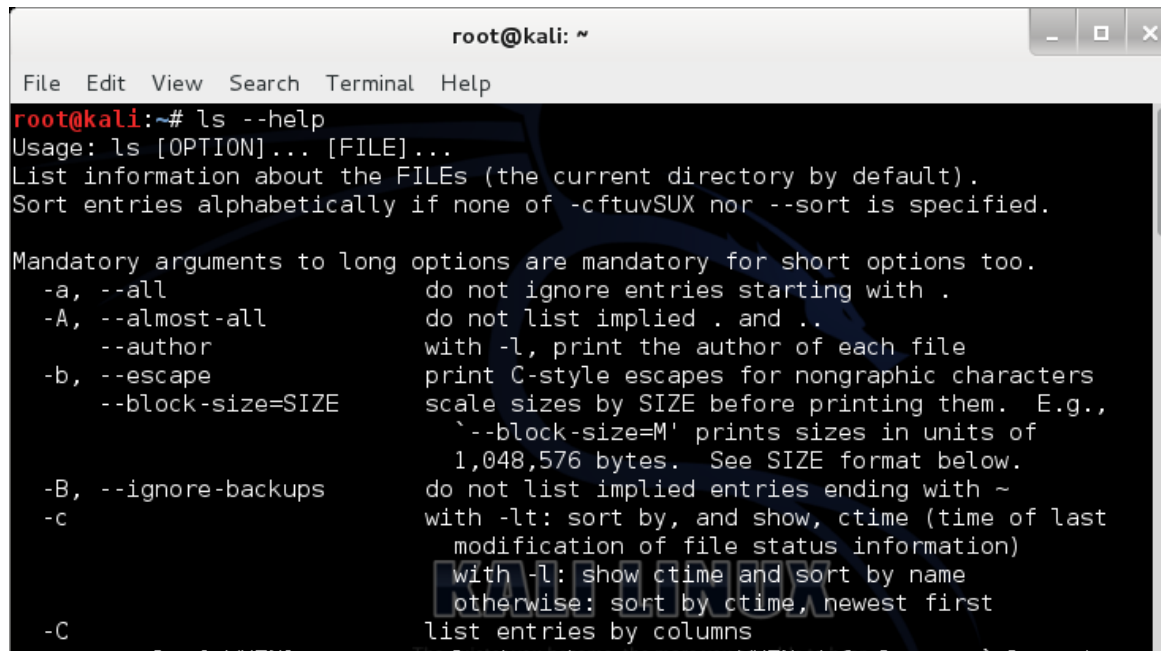
- Kullanıcının işletim sistemiyle iletişimini sağlayan program
- Verilen komutları işletim sistemine ve komutların çıktılarını kullanıcıya iletir.



- Farklı kabuk programları bulunmaktadır. Linux'ta genellikle "bash" kullanılır.

# Linux Komut Serisi – 1

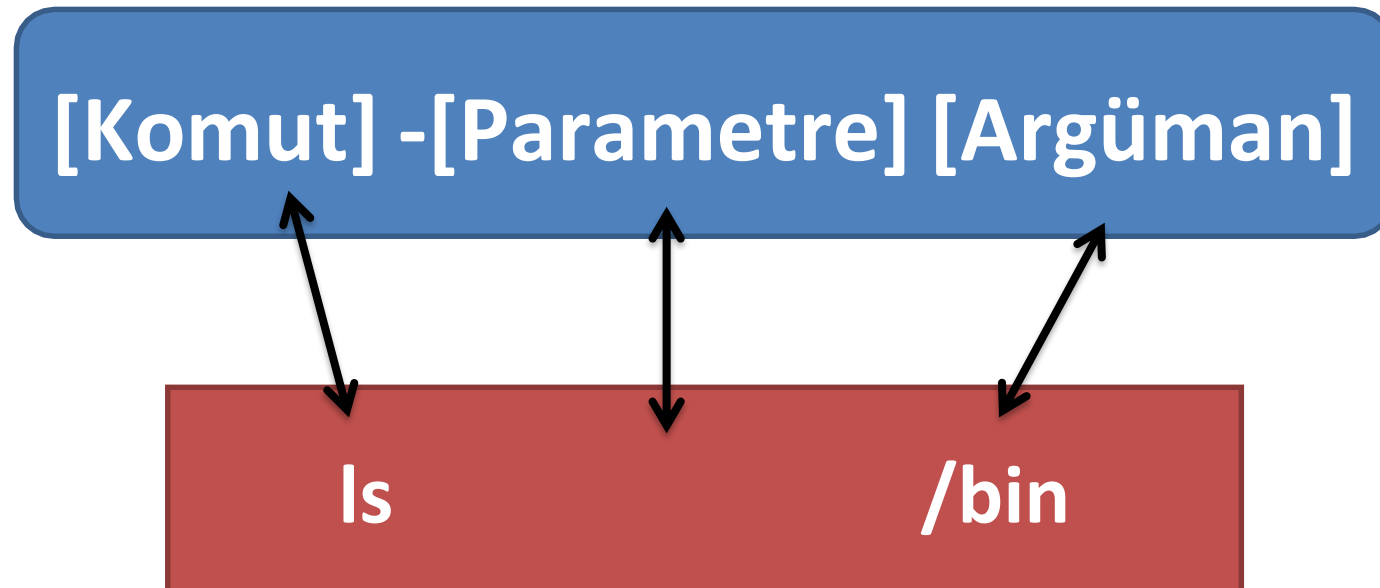
- Komutların bir çoğu parametre alır.
- Parametreler komut adından sonra bir boşluk bırakılarak yazılır.
- Parametreler genellikle '-' işareti ile başlar.
- Kullanılan parametreler ile spesifik işler yapılabilir.



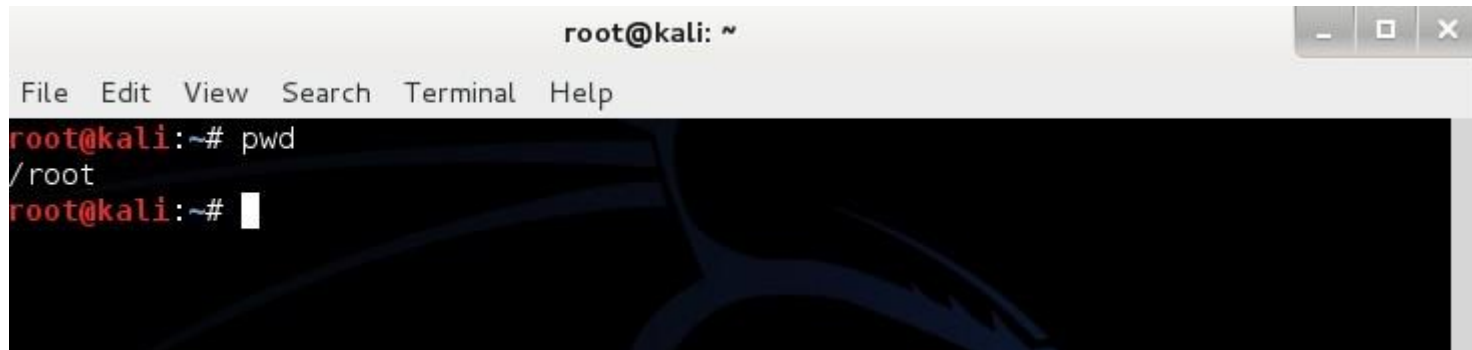
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ls --help  
Usage: ls [OPTION]... [FILE]...  
List information about the FILES (the current directory by default).  
Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.  
  
Mandatory arguments to long options 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.  
-B, --ignore-backups    do not list implied entries ending with ~  
-c                      with -lt: sort by, and show, ctime (time of last  
                        modification of file status information)  
                        with -l: show ctime and sort by name  
                        otherwise: sort by ctime, newest first  
-C                      list entries by columns
```

# Linux Komut Serisi – 1

- Temel olarak kural → komut ile ilgili parametrelerin birlikte kullanımı
- Komutun detaylı kullanımı için 'man [komut adı]'



# #pwd komutu

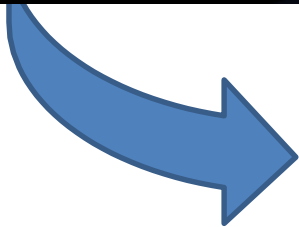
A screenshot of a terminal window titled 'root@kali: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal content shows the command 'pwd' being entered at the prompt 'root@kali:~#', followed by the output '/root' on the next line. The prompt 'root@kali:~#' is followed by a white cursor block.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# pwd
/root
root@kali:~#
```

- **pwd** komutu bulunulan dizini ekrana bastıran komuttur.
- Açılımı **p**rint **w**orking **d**irectory

# #man komutu

```
File Edit View Search T
root@kali:~# man grep
```



```
root@kali: ~
File Edit View Search Terminal Help
GREP(1) GREP(1)

NAME
    grep, egrep, fgrep, rgrep - print lines matching a pattern

SYNOPSIS
    grep [OPTIONS] PATTERN [FILE...]
    grep [OPTIONS] [-e PATTERN | -f FILE] [FILE...]

DESCRIPTION
    grep searches the named input FILES (or standard input if no files are
    named, or if a single hyphen-minus (-) is given as file name) for lines
    containing a match to the given PATTERN. By default, grep prints the
    matching lines.

    In addition, three variant programs egrep, fgrep and rgrep are
    available. egrep is the same as grep -E. fgrep is the same as
    grep -F. rgrep is the same as grep -r. Directly invoking any of these
```

- Manuel ifadesinin kısaltılmış halidir. Komut hakkında ayrıntılı bilgi almayı sağlar.
- Kali'de **/usr/share/man** kalsörü altında bulunur.
- **man** komutunun sayfa organizasyonu 8 bölüm altında tasarlanmıştır.



Section	Description
1	User Commands
2	Programming Interfaces for Kernel System Calls
3	Programming Interfaces to the C standard library
4	Special Files (usually devices, those found in /dev) and Driver
5	File Formats
6	Games and Screensavers
7	Miscellaneous
8	System Administration Commands

- Varsayılanda bölüm 1 manuellere açılır. İstediğimiz bölüm için bölüm numarasını yazıp açmamız gerekir.
- **man passwd** (man 1 passwd ile aynı manaya geliyor. passwd komutundan bahseder)
- **man 5 passwd** (passwd dosyasının formatından bahseder)

# #man komutu

```
root@kali:~# man 5 passwd
```



```
root@kali: ~  
File Edit View Search Terminal Help  
PASSWD(5) File Formats and Conversions PASSWD(5)  
  
NAME  
passwd - the password file  
  
DESCRIPTION  
/etc/passwd contains one line for each user account, with seven fields  
delimited by colons (":"). These fields are:  
  
• login name  
• optional encrypted password  
• numerical user ID  
• numerical group ID  
• user name or comment field  
• user home directory  
• optional user command interpreter
```

- Change Directory ifadesinin kısaltılmışıdır. Dizin değiştirmek için kullanılır.
- ‘..’ Linuxta bir üst dizini ‘.’ ise bulunulan dizini simgeler.
- **cd..** komutu ile bir üst klasöre çıkarken **cd.** yaparsak bulunduğumuz klasörde kalmış oluruz.
- **cd** komutunu parametresiz kullanırsak login olduğumuz kullanıcının dizinine gideriz.
- **cd** komutunu ‘**cd ~user**’ olarak kullanırsak yazdığımız kullanıcının home klasörüne gideriz.
- **cd –** şeklinde kullanım ise bizi bir önceki klasör konumuna götürür.

# #cd Komutu

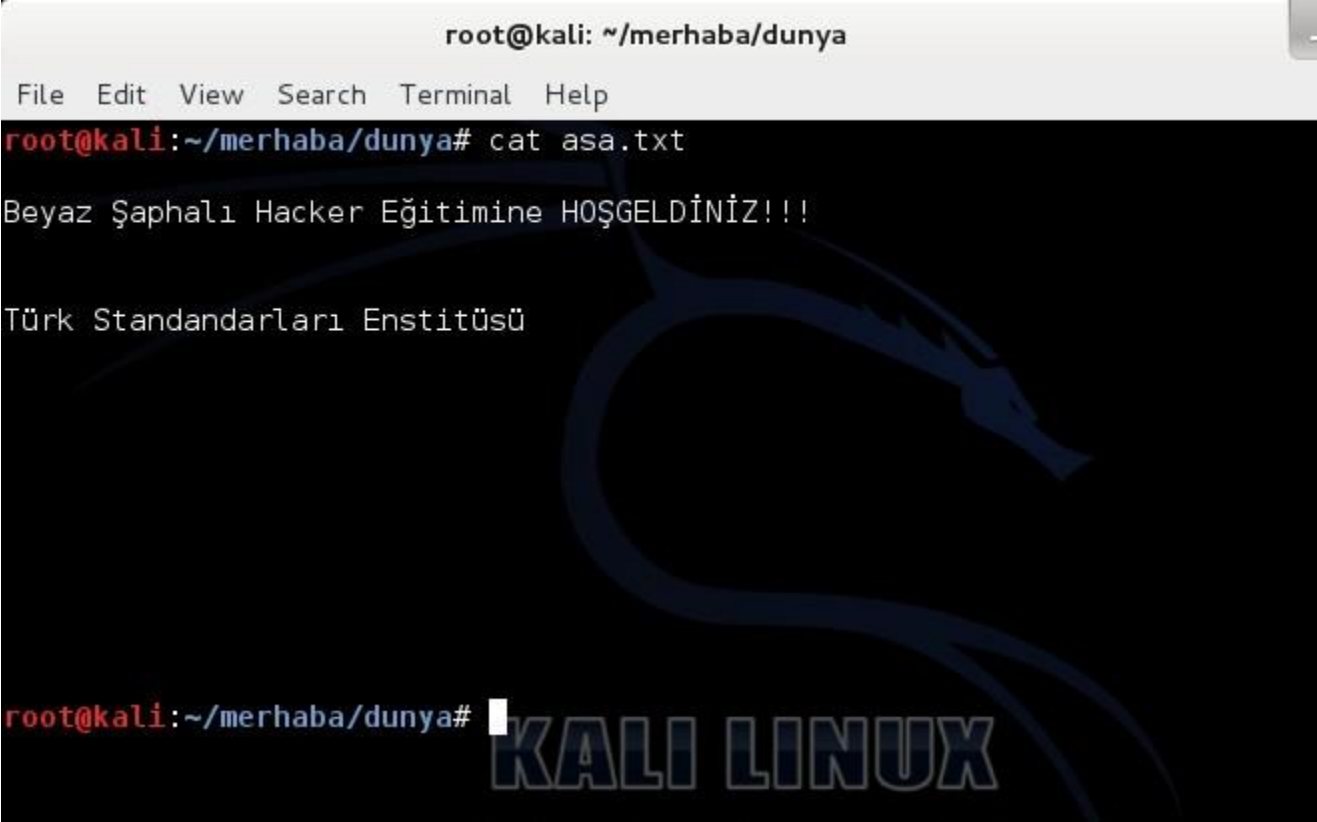
```
root@kali: ~/merhaba
File Edit View Search Terminal Help
root@kali:~/merhaba# cd dünya
root@kali:~/merhaba/dunya# pwd
/root/merhaba/dunya
root@kali:~/merhaba/dunya# cd ..
root@kali:~/merhaba# pwd
/root/merhaba
root@kali:~/merhaba# cd
root@kali:~# pwd
/root
```

- **ls** komutu dosya, dizin listelemek, özelliklerini görüntülemek için kullanılır.

Option	Long Option	Description
-a	--all	List all files, even those with names that begin with a period, which are normally not listed (i.e., hidden).
-d	--directory	Ordinarily, if a directory is specified, <b>ls</b> will list the contents of the directory, not the directory itself. Use this option in conjunction with the <b>-l</b> option to see details about the directory rather than its contents.
-F	--classify	This option will append an indicator character to the end of each listed name. For example, a "/" if the name is a directory.
-h	--human-readable	In long format listings, display file sizes in human readable format rather than in bytes.
-l		Display results in long format.
-r	--reverse	Display the results in reverse order. Normally, <b>ls</b> displays its results in ascending alphabetical order.
-S		Sort results by file size.
-t		Sort by modification time.

# #cat Komutu

- Dosya içeriğini okumak ve görüntülemek için kullanılır.

A screenshot of a Kali Linux terminal window. The title bar shows 'root@kali: ~/merhaba/dunya'. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal content shows the command 'cat asa.txt' being executed, followed by the output: 'Beyaz Şaphalı Hacker Eğitime HOŞGELDİNİZ!!!' and 'Türk Standandarları Enstitüsü'. The terminal background features a large, faint blue dragon logo and the text 'KALI LINUX' at the bottom. The prompt 'root@kali:~/merhaba/dunya#' is visible at the bottom left.

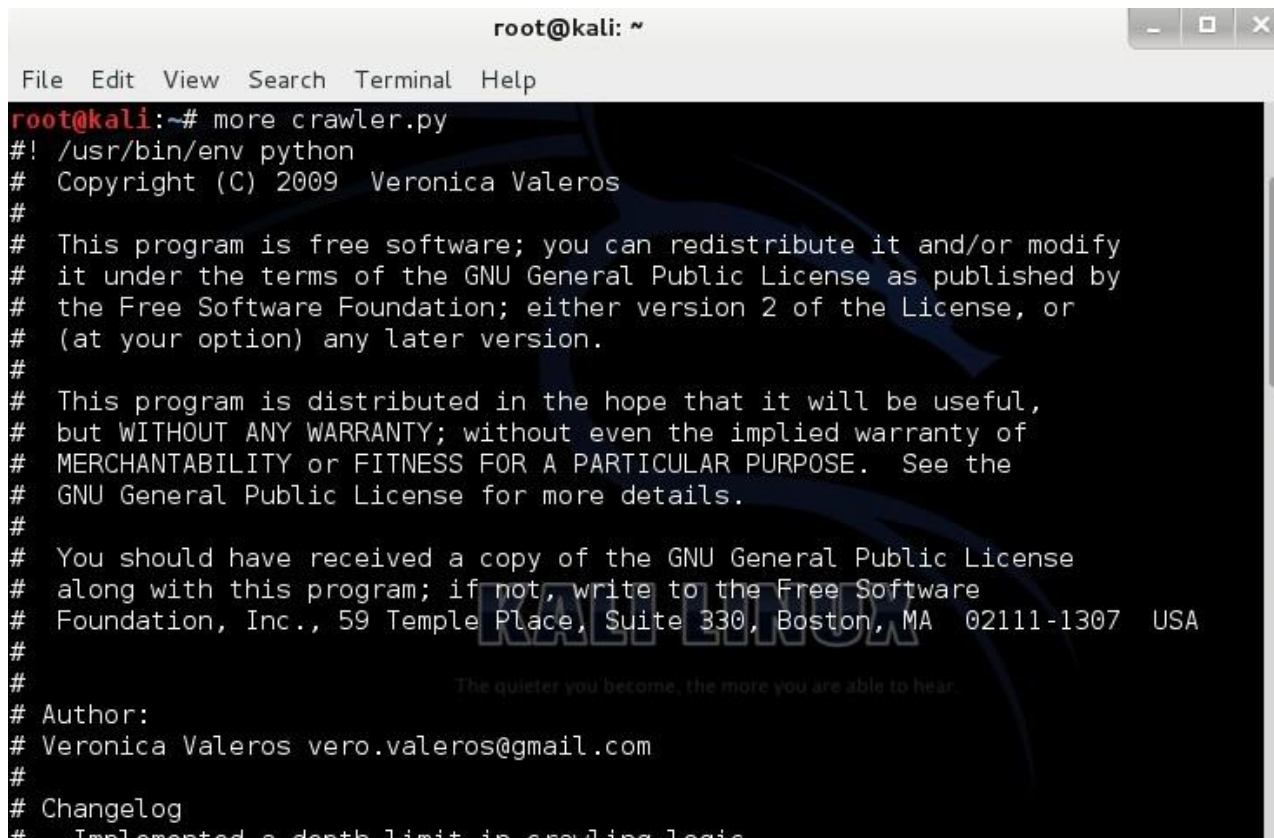
```
root@kali: ~/merhaba/dunya
File Edit View Search Terminal Help
root@kali:~/merhaba/dunya# cat asa.txt
Beyaz Şaphalı Hacker Eğitime HOŞGELDİNİZ!!!
Türk Standandarları Enstitüsü
root@kali:~/merhaba/dunya#
```

# #echo Komutu

- Kendinden sonra yazılan ifadeyi ekrana bastırır.
- Ortam Değişkenleri başına '\$' koyarak ekrana yazdırılabilir.

```
root@kali: ~/merhaba/dunya
File Edit View Search Terminal Help
root@kali:~/merhaba/dunya# echo HOME
HOME
root@kali:~/merhaba/dunya# echo $HOME
/root
root@kali:~/merhaba/dunya# echo cat tse
cat tse
root@kali:~/merhaba/dunya#
```

- İçeriği fazla olan ve normal olarak ekrana tam sığmayan dosyaları görüntülemek için kullanılır.
- Enter ya da space tuşu ile dökümanda ilerlenir.
- **q** tuşuyla çıkış yapılır.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# more crawler.py  
#!/usr/bin/env python  
# Copyright (C) 2009 Veronica Valeros  
#  
# This program is free software; you can redistribute it and/or modify  
# it under the terms of the GNU General Public License as published by  
# the Free Software Foundation; either version 2 of the License, or  
# (at your option) any later version.  
#  
# This program is distributed in the hope that it will be useful,  
# but WITHOUT ANY WARRANTY; without even the implied warranty of  
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the  
# GNU General Public License for more details.  
#  
# You should have received a copy of the GNU General Public License  
# along with this program; if not, write to the Free Software  
# Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA  
#  
# The quieter you become, the more you are able to hear.  
# Author:  
# Veronica Valeros vero.valeros@gmail.com  
#  
# Changelog  
# Implemented a depth limit in crawling logic
```



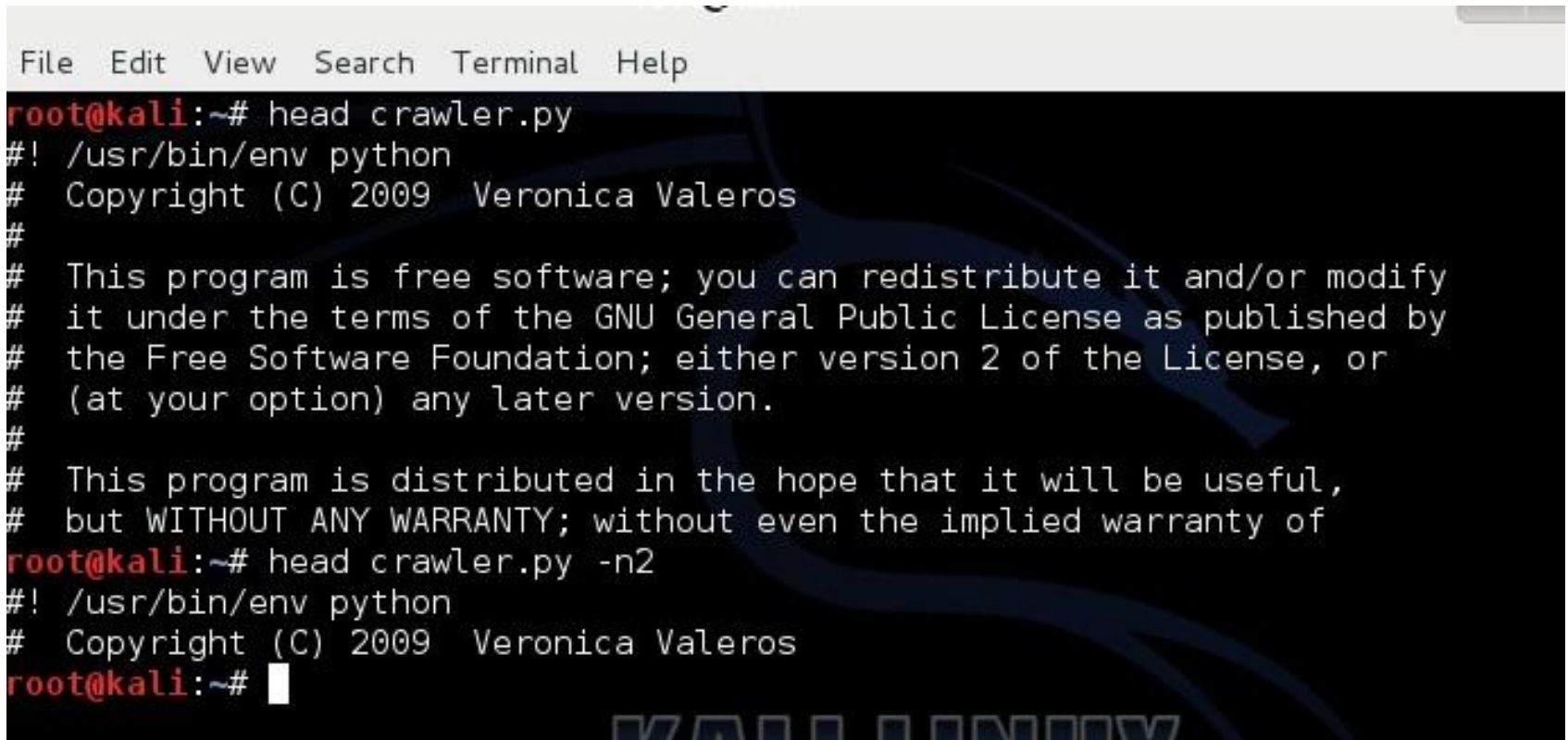
# #less Komutu

- **more** komutuna benzer bir komuttur ama daha gelişmiştir.
- **'/ifade'** ile istenen ifade için arama yapılabilir.
- **':sayı'** ile istenilen satıra gider.
- **q** ile çıkış yapılır.
- **More** komutu aksine geriye doğru da dosya içinde gezinilebilir.

```
root@kali: ~
File Edit View Search Terminal Help
#!/usr/bin/env python
# Copyright (C) 2009 Veronica Valeros
#
# This program is free software; you can redistribute it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the license or any later version.
#
# This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.
#
# Author: Veronica Valeros vero.valeros@gmail.com
#
# Changelog
# - Implemented a depth limit in crawling logic.
:
```

# #head Komutu

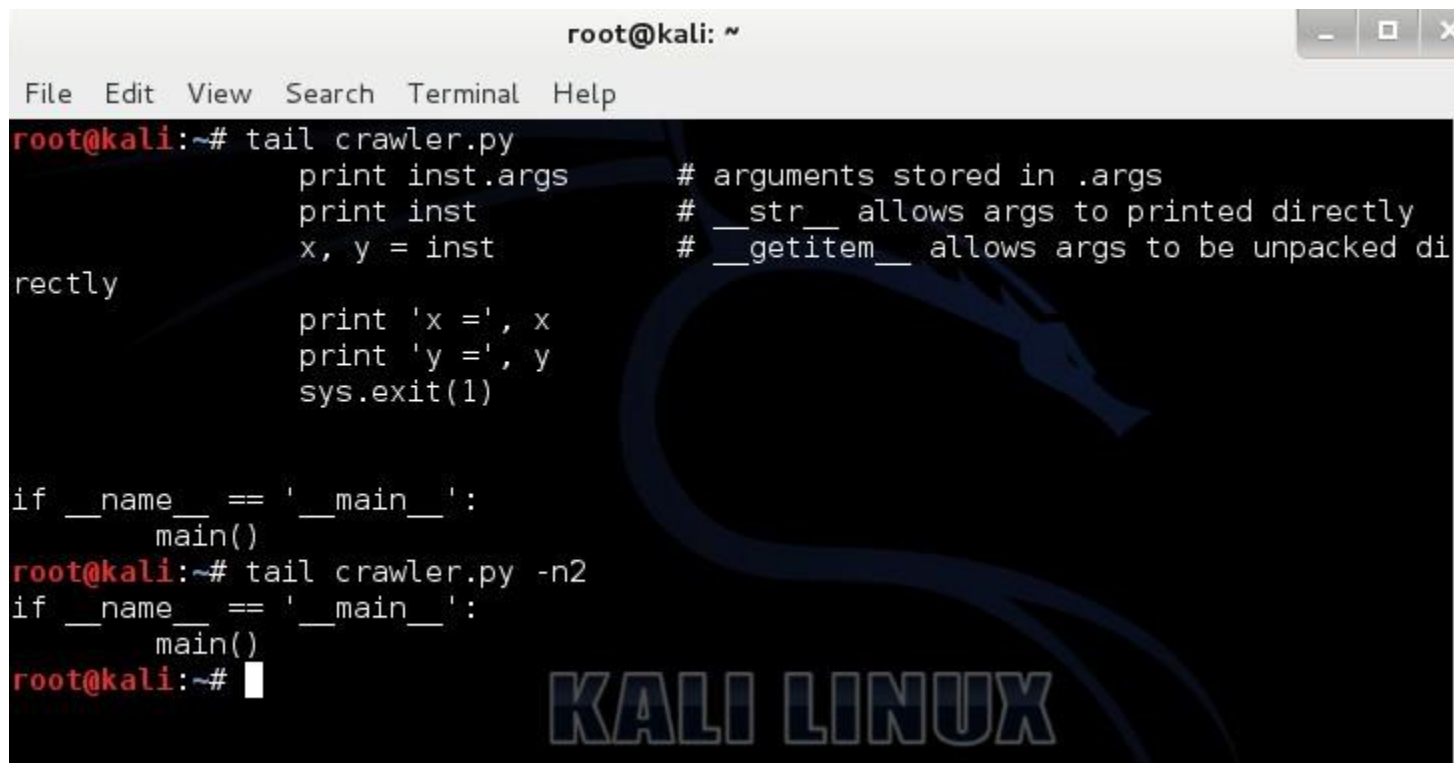
- Verilen dosyanın varsayılan olarak ilk 10 satırını getirir.
- **-n** parametresi ile istenen satır sayısı getirilir.

A screenshot of a terminal window with a menu bar (File, Edit, View, Search, Terminal, Help) and a dark background. The terminal shows the execution of the 'head' command on a file named 'crawler.py'. The first command, 'head crawler.py', displays the first 10 lines of the file, which include a shebang, a copyright notice, and a license statement. The second command, 'head crawler.py -n2', displays the first two lines of the file. The prompt 'root@kali:~#' is visible at the end of each command line.

```
File Edit View Search Terminal Help
root@kali:~# head crawler.py
#!/usr/bin/env python
# Copyright (C) 2009 Veronica Valeros
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
root@kali:~# head crawler.py -n2
#!/usr/bin/env python
# Copyright (C) 2009 Veronica Valeros
root@kali:~#
```

# #tail Komutu

- **head** komutunun tersine varsayılan olarak bir dosyanın son 10 satırını getirir.
- **-n** parametresi ile satır sayısı belirlenebilir.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# tail crawler.py  
    print inst.args      # arguments stored in .args  
    print inst           # __str__ allows args to printed directly  
    x, y = inst          # __getitem__ allows args to be unpacked di  
rectly  
    print 'x =', x  
    print 'y =', y  
    sys.exit(1)  
  
if __name__ == '__main__':  
    main()  
root@kali:~# tail crawler.py -n2  
if __name__ == '__main__':  
    main()  
root@kali:~#
```

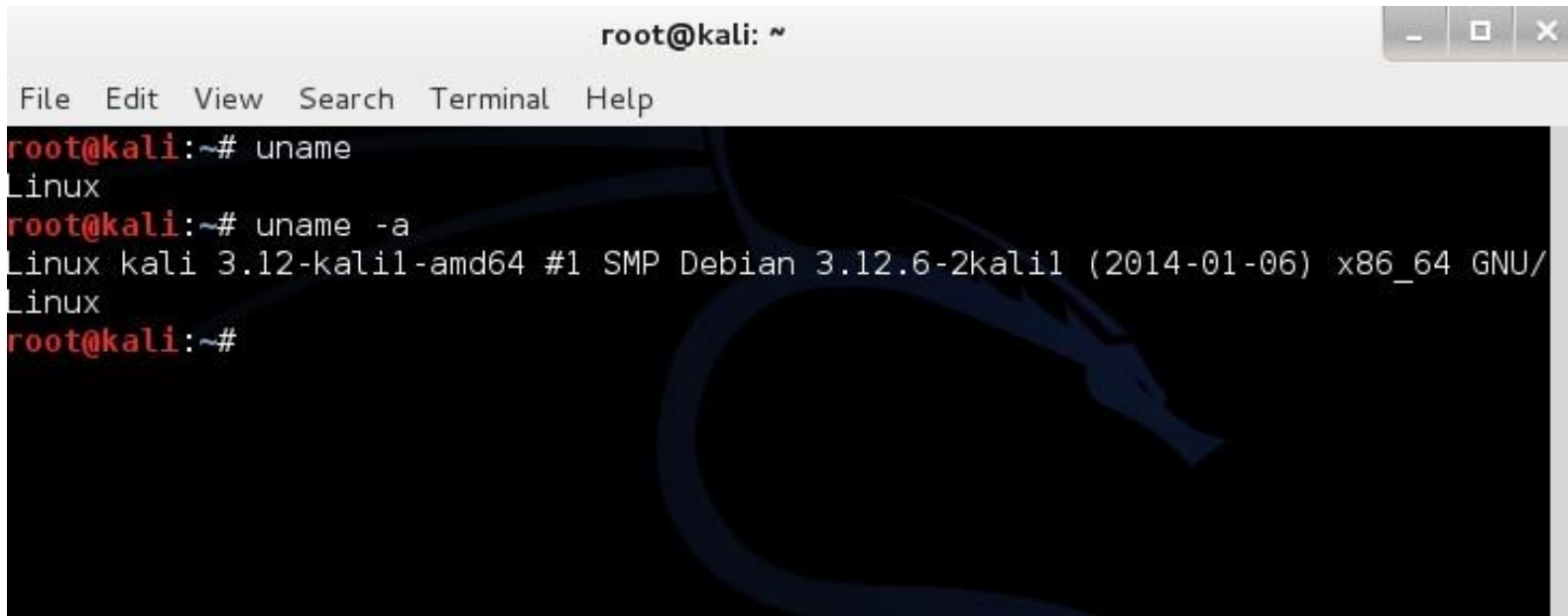
# #grep Komutu

- Verilen data içerisinde istenilen kriterlere ait kelimeleri aramak için kullanılan komuttur.
- **-i** ile büyük küçük harfe bakmadan arama yapar.
- **-E** ile regex ifadeler aranabilir.
- **-r** ile alt dizinlerde recursive olarak arama yapar.
- **-v** ile yazılan kriterle uyuşanlar dışındaki çıktıları ekrana getirir.

```
File Edit View Search Terminal Help
root@kali:~# ls | grep -r "gmail.com"
Desktop/crawler.py:# Veronica Valeros vero.valeros@gmail.com
Desktop/crawler.py:    print "| Author: Veronica Valeros, vero.valeros@gmail.c
m
Desktop/crawler.py:    print "| Author: Veronica Valeros, vero.valeros@gmail.c
m
.mozilla/firefox/jvh4sqmx.default/blocklist.xml:    <emItem blockID="i554" i
="lightningnewtab@gmail.com">
```

# #uname Komutu

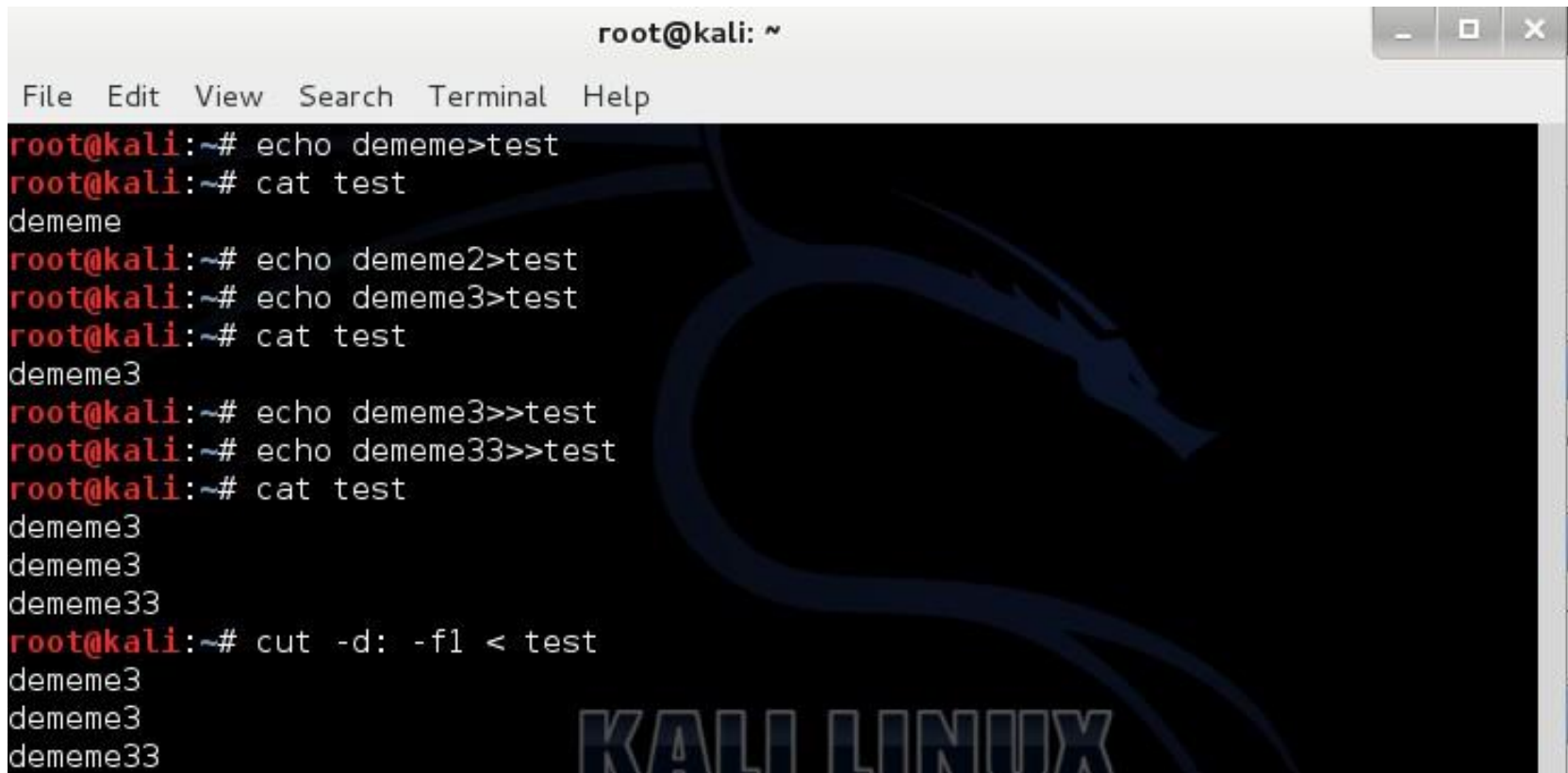
- **uname** komutu sistem bilgilerini getirir.
- **-a**, tüm bilgilerle birlikte gelir.

A terminal window titled 'root@kali: ~' with standard window controls. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows the execution of 'uname' and 'uname -a' commands. The background features a faint Kali Linux dragon logo.

```
root@kali:~# uname
Linux
root@kali:~# uname -a
Linux kali 3.12-kali1-amd64 #1 SMP Debian 3.12.6-2kali1 (2014-01-06) x86_64 GNU/
Linux
root@kali:~#
```

# Çıktı Yönlendirme

- Komut çıktıları dosyalara yönlendirilebilir.
- **>** işareti ile bir komutun çıktısı bir dosyanın üzerine yazılır.
- Aynı işlem **>>** işareti ile yapılırsa, çıktı dosyanın sonuna eklenir.
- **<** ise komuta girdi vermek için kullanılabilir.

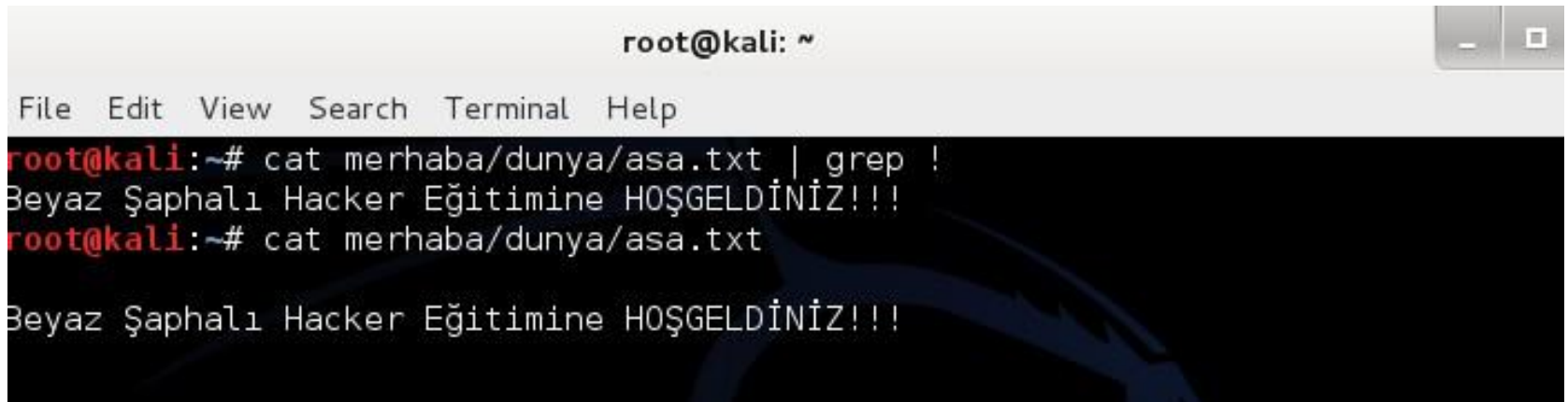


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# echo dememe>test  
root@kali:~# cat test  
dememe  
root@kali:~# echo dememe2>test  
root@kali:~# echo dememe3>test  
root@kali:~# cat test  
dememe3  
root@kali:~# echo dememe3>>test  
root@kali:~# echo dememe33>>test  
root@kali:~# cat test  
dememe3  
dememe3  
dememe33  
root@kali:~# cut -d: -f1 < test  
dememe3  
dememe3  
dememe33
```

KALI LINUX

# Çıktı Yönlendirme

- Bir komutun çıktısını diğer bir komuta girdi olarak vermek için **|** (pipe) kullanılır.

A screenshot of a Kali Linux terminal window. The title bar shows 'root@kali: ~' and standard window controls. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal content shows two commands being executed. The first command is 'cat merhaba/dunya/asa.txt | grep !', which outputs 'Beyaz Şaphalı Hacker Eğitime HOŞGELDİNİZ!!!'. The second command is 'cat merhaba/dunya/asa.txt', which outputs the same text. The background of the terminal has a dark theme with a faint blue dragon-like graphic.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# cat merhaba/dunya/asa.txt | grep !
Beyaz Şaphalı Hacker Eğitime HOŞGELDİNİZ!!!
root@kali:~# cat merhaba/dunya/asa.txt
Beyaz Şaphalı Hacker Eğitime HOŞGELDİNİZ!!!
```

# Temel Linux Kullanımı

Temel Komut Serisi-1

Linux Dosya Sistemi

Linux Komut Serisi-2

Network Ayarları

Servisler

Kullanıcı Yönetimi

Process

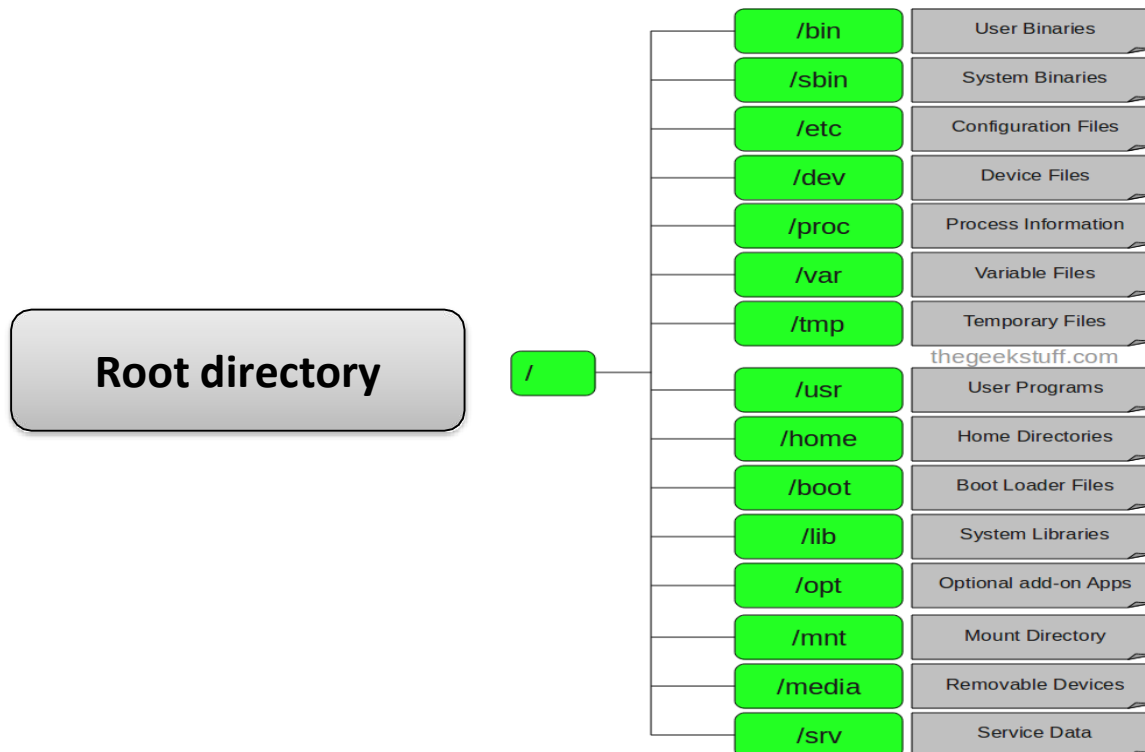
Paket Yönetim Sistemi

Sistem İzleme



# Linux Dosya Sistemi

- Linux dosya yapısı, ağaç sisteminin bir benzeridir. Root kök dizinini ifade eder. Altındaki dosya ve klasörler ise ağaç yaprakları gibi düşünülebilir.
- Linux'te bağlanma noktası yani mount point önemlidir. Tüm temel dosya ve klasörler root'a bağlanır ve işareti '/' dir.



# Linux Dosya Sistemi

- Linux 'teki dosya hiyerarşisi genel olarak şu şekildedir:
  - **/bin**: Kullanıcı ve sistem yöneticisine ait çalıştırılabilir dosyaları barındırır.
  - **/dev**: Donanımlara erişebilmek için gerekli dosyaları barındırır. (/media)
  - **/etc**: Sistemde çalışan servislerin konfigürasyonları için gerekli dosyaları barındırır. (Telnet, ssh, samba, apache, dhcp vb.) Servisleri başlatma betikleri de burada bulunur /etc/init.d
  - **/lib**: Sistem kütüphanelerini barındırır.
  - **/sbin**: Sistem yöneticisine ait çalıştırılabilir dosyaları barındırır.
  - **/home**: Kullanıcılara ait dizindir.
  - **/mnt**: Sisteme dışarıdan bağlanacak olan donanım aygıtlarının, bağlantı noktalarını belirten dizindir.
  - **/root**: Bir sistemde en yetkili kullanıcı olan "root" kullanıcısına ait dizindir.
  - **/tmp**: Geçici dosyaların yer aldığı dizindir.
  - **/usr**: Paylaşılan dosyaların barındığı dizindir. Burada çalışabilen dosyalar bulunmakla beraber, doküman ve kullanıcı programlarına ait dosyalar da yer almaktadır.
  - **/var**: Sistem ve programlara ait log mesajları, email gibi mesajların bulunduğu dizindir. /var/www altında apache sunucu açılarak web sayfası oluşturulabilir. /var/log/dmesg içinde açılış kayıtları, /var/log/apache2
  - **/proc**: Sistem hakkında gerekli bilgilerin bulunduğu sanal dizindir. Bilgisayar boot olduğunda Ram de oluşturulur. Sistemde çalışan geçici süreçler bu dizin altında çalışırlar.
  - **/boot**: Linux Kernelini barındıran (vmlinuz), sistem haritalarını ve ikinci seviye boot yükleyicilerini barındıran dizin. Linux açıldığında vmlinuz RAM e yüklenir ve donanımlar taranır sürücü yazılımları yüklenmeye başlar. Power On Self Test yapar. Boot yükleyicileri (bootloader) grub ve lilo olmak üzere /boot altındadır Linux'te.
  - **/opt**: Add-on yazılımların bulunduğu alandır.

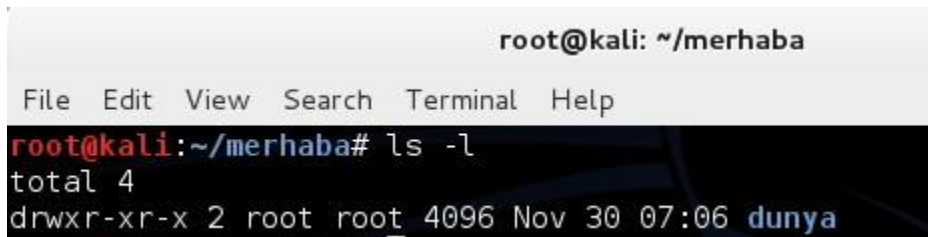
# Dosya İzinleri 1

- **drwxrwxrwx** sırasıyla ilk üçlü Owner (u), 2. üçlü grup (g), 3. üçlü diğer tüm kullanıcıların (o ya da a) haklarını belirtir.
- d dizin olduğunu, l sembolik link, - özel izin yok
- Rakam bölümü dosyaya bağlı hardlink sayısı
- Root root ise owner:group ikilisini temsil eder

```
root@kali:/# ls -la
total 184
drwxr-xr-x 28 root root 4096 Apr  8 04:22 .
drwxr-xr-x 28 root root 4096 Apr  8 04:22 ..
drwxr-xr-x  2 root root 4096 Apr  7 09:15 abcdef
drwxr-xr-x  2 root root 4096 Apr  7 09:15 abcdefg
drwxrwxrwx  3 root root 4096 Apr  7 09:00 root
drwxr-xr-x  2 root root 4096 Feb 23  2015 bin
drwxr-xr-x  3 root root 4096 Feb 23  2015 boot
```

# Dosya İzinleri 2

- Her dosya ve klasörün bir sahibi ve bir de grubu vardır.
- Bu dosya ve klasör üzerinde sahibinin, grubunun ve bunların dışındaki herkesin ayrı ayrı yetkileri vardır.
- Linux'ta 3 çeşit izin kavramı vardır. Bunlar:
  - Read (r)
  - Write (w)
  - Execute(x)
- Read hakkının sayısal değeri 4'tür
- Write hakkının sayısal değeri 2'dir
- Execute hakkının sayısal değeri 1'dir.
- **chmod** komutu ile sayısal değerler kullanılarak sırasıyla dosya sahibine, sahibin üye olduğu gruba ve geri kalanlara hak verilir.
- Tüm haklar verildiğinde sayısal değer 7'ye eşit olur (4+2+1)
- **chmod 755 dosya1** ifadesi **dosya1**'in sahibine full yetki, geri kalan herkese okuma ve çalıştırma yetkisi verir.



```
root@kali: ~/merhaba
File Edit View Search Terminal Help
root@kali:~/merhaba# ls -l
total 4
drwxr-xr-x 2 root root 4096 Nov 30 07:06 dunya
```

Dosya Sahibi – Dosya Sahibi Grubu

# Setuid ve Setgid

- **Kali'de sahip (u) ve grup (g) bölümlerinin çalışma kısmında 's' bulunursa setuid/setgid izni verilmiş demektir.**
- Anlamı: Normal bir kullanıcıya o dosya/dizin üzerinde yazma ve çalıştırma hakkı verilmiş demektir. Güvenlik zafiyetidir. Dikkatli ayarlanması gerekir.
- **Diğer tüm kullanıcılar (o) bölümünde çalıştırma (x) kısmında 't' bulunursa sticky bit izni verilmiş demektir.**

# SUID/SGID'li bin dosyalarını bulma

- **find / -perm +4000 -user root -type f -print**
- **find / -perm +2000 -user root -type f -print**
- **/** says start at the top (root) of the file system and search every directory
- **-perm** says look for the permissions that follow
- **+4000** is the numerical representation of the SUID bit permission
- **-user** says look for files that are owned by the following user
- **root** is the user whose files we are looking for
- **-type** defines the type of file we are looking for
- **f** represents a regular file (not directories or special files)
- **-print** tells the command to print to standard out the path to the file

# Temel Linux Kullanımı

Temel Komut Serisi-1

Linux Dosya Sistemi

**Linux Komut Serisi-2**

Network Ayarları

Servisler

Kullanıcı Yönetimi

Process

Paket Yönetim Sistemi

Sistem İzleme

# #mkdir komutu

- Dizin oluşturmak için kullanılır.
- **-p**: Oluşturulan klasörün üst klasörlerini de oluşturur.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# mkdir deneme2  
root@kali:~# ls  
crawler.py deneme deneme2 Desktop merhaba test text  
root@kali:~#
```

```
root@kali: ~/ahmet  
File Edit View Search Terminal Help  
root@kali:~# mkdir ahmet/deneme  
mkdir: cannot create directory `ahmet/deneme': No such file or  
root@kali:~# mkdir -p ahmet/deneme  
root@kali:~# ls  
ahmet crawler.py deneme deneme2 Desktop merhaba test tex  
root@kali:~# cd ahmet  
root@kali:~/ahmet# ls  
deneme  
root@kali:~/ahmet#
```



# #touch komutu

- Dosya oluşturmak için kullanılır.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# mkdir -p sunum/[0{1..9}.10]-linux  
root@kali:~# ls sunum  
[01.10]-linux [03.10]-linux [05.10]-linux [07.10]-linux [09.10]-linux  
[02.10]-linux [04.10]-linux [06.10]-linux [08.10]-linux  
root@kali:~# touch sunum/[0{1..9}.10]-linux/dosya-{a..f}  
root@kali:~# ls sunum/[01.10]-linux/  
dosya-a dosya-b dosya-c dosya-d dosya-e dosya-f  
root@kali:~#
```

# #rm/rmdir komutu

- Dosya/klasör silmek için kullanılır.
- İçi dolu klasörleri silmek için **-r** parametresi kullanılarak bu işlem recursive (özyineleme) yapılabilir.
- Silmeden önce sorması için **-i** parametresi ile birlikte kullanılmalı.

```
File Edit View Search Terminal Help
root@kali:~# ls
ahmet crawler.py deneme deneme2 Desktop merhaba sunum test t
root@kali:~# rm sunum
rm: cannot remove `sunum': Is a directory
root@kali:~# rm -r sunum
root@kali:~# ls
ahmet crawler.py deneme deneme2 Desktop merhaba test text
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# rm -i text
rm: remove regular empty file `text'? y
root@kali:~# ls
ahmet crawler.py deneme deneme2 Desktop merhaba test
root@kali:~# rm -i test
rm: remove regular file `test'? y
root@kali:~# ls
ahmet crawler.py deneme deneme2 Desktop merhaba
root@kali:~#
```

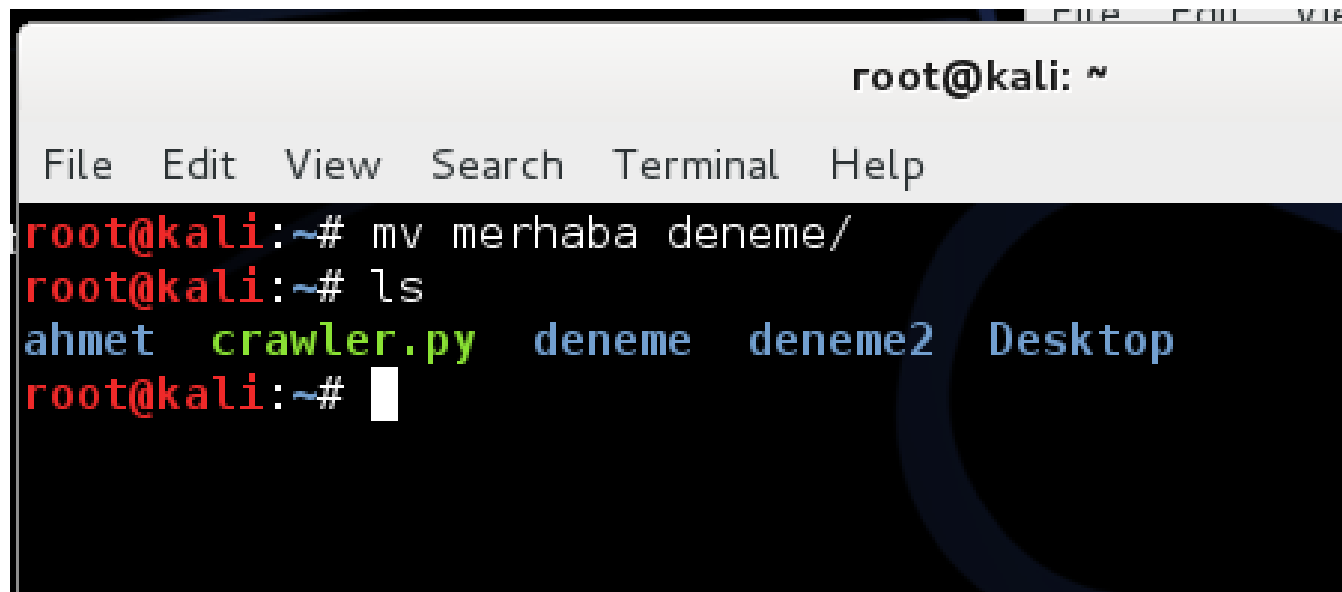
# #cp komutu

- Veri kopyalamak için kullanılır.
- Klasör kopyalanırken **-r** parametresi ile kullanılmalıdır.
- **-p** parametresi ile kullanılırsa taşıma esnasında dosya haklarını korur.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ls deneme  
klasor  
root@kali:~# cp -r deneme2 deneme  
root@kali:~# ls deneme  
deneme2  klasor  
root@kali:~#
```

# #mv komutu

- Dosya ve klasörleri taşımak yada yeniden adlandırmak için kullanılır.
- Genel kullanım şekli **mv [kaynak1],[kaynak2,..kaynak n] [hedef]** olarak özetlenebilir.
- **-f** parametresi ile kaynak dosya hedef üzerine hiçbir şey sorulmaksızın kopyalanır.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# mv merhaba deneme/  
root@kali:~# ls  
ahmet  crawler.py  deneme  deneme2  Desktop  
root@kali:~#
```

# #find komutu

- Dosya ve dizinleri aramak için kullanılır.
- Çok kapsamlı bir kullanımı vardır.
- Dosya tiplerine, isimlerine, izinlerine, aramanın yapacağı derinliğe, mantıksal kıyaslamalara göre arama yapılabilir.

```
root@kali:~# find /root -maxdepth 1 \( -type f -not -perm 0600 \) -or \( -type d
-not -perm 0700 \) -exec ls -l "{}" +
/root:
ahmet
crawler.py
deneme
deneme2
Desktop

/root/ahmet:
deneme

/root/deneme:
deneme2
klasor
merhaba
```

# #cut komutu

- Verilen bir ifadeyi belirtilen ayıraca göre parçalara böler.
- Bir text içinde ihtiyacımız olan spesifik bir kısmı (**kullanıcı adı veya IP gibi**) almak için kullanılır.
- Genel kullanımı **cut -d 'ayırac' -f[sayı1,[sayı2,,]]** şeklindedir.
- **-f** parametresi ile bölünmüş metnin hangi kolonlarıyla ilgileniyorsak onu belirtiriz.
- **-d** parametresi ile de ayıracın ne olacağını söyleriz.

```
root@kali: ~/deneme/merhaba/dunya
File Edit View Search Terminal Help
root@kali:~/deneme/merhaba/dunya# cat
Fatma DEMİR
Ahmet CAN
Ayşe YILDIRIM
Mehmet YURDAER
Ali ALPASLAN
Hasan CANSIZ

root@kali:~/deneme/merhaba/dunya# cat | cut -d " " -f1
Fatma
Ahmet
Ayşe
Mehmet
Ali
Hasan

root@kali:~/deneme/merhaba/dunya#
```

- **awk** aslında text processing için tasarlanmış bir programlama dilidir.
- Başlı başına bir kullanımı olmasına karşın cut komutunun yetersiz kaldığı yerlerde basitçe problemi çözmemize yardımcı olur.

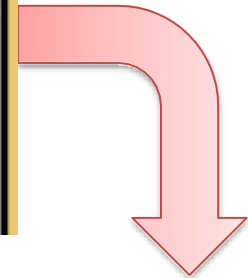
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ls  
ahmet crawler.py deneme2 sample2.txt  
awk.txt deneme Desktop sanayi.txt  
root@kali:~# cat awk.txt  
tse hacker eğitim beyaz şapka  
root@kali:~# #Kelimeler arasındaki boşluk birden fazla  
root@kali:~# cat awk.txt | cut -d " " -f2  
hacker  
root@kali:~# cat awk.txt | cut -d " " -f2,4  
hacker  
root@kali:~# cat awk.txt | awk 'BEGIN { FS=" "; } { print $2,$4 }'  
hacker beyaz  
root@kali:~#
```

- Bazı komut çıktılarında gerekli bilgileri çekmek için awk kurtarıcı olabilir.

# #chown komutu

- Change Owner ifadesinin kısaltılmışı olan komuttur. Bir dosya yada klasörün sahibi ve grubunu değiştirmeye izin verir.
- Kullanımı **chown [parametre] [sahibi ]:[grubu] dosya** şeklindedir.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ls -al
total 124
drwxr-xr-x 17 root root 4096 Dec  2 15:27 .
drwxr-xr-x 23 root root 4096 Sep 18 02:29 ..
drwxr-xr-x  2 root root 4096 Dec  2 15:23 asa
-rw----- 1 root root 2153 Dec  2 15:26 .bash_history
```



```
File Edit View Search Terminal Help
root@kali:~# chown ahmet:ahmet asa
root@kali:~# ls -al
total 124
drwxr-xr-x 17 root root 4096 Dec  2 15:27 .
drwxr-xr-x 23 root root 4096 Sep 18 02:29 ..
drwxr-xr-x  2 ahmet ahmet 4096 Dec  2 15:23 asa
-rw----- 1 root root 2153 Dec  2 15:26 .bash_history
```



# Temel Linux Kullanımı

Temel Komut Serisi-1

Linux Dosya Sistemi

Linux Komut Serisi-2

Network Ayarları

Servisler

Kullanıcı Yönetimi

Process

Paket Yönetim Sistemi

Sistem İzleme

- Vmware Ağ Ayarları

- Bridge

Yerel ağda bulunan DHCP sunucudan bir ip adresi alabilir ve yerel ağa kendi IP adresi ile erişebilir.

- NAT

Yerel ağa erişim, vmware tarafından bir IP adresine dönüşüm ile sağlanır.

- HostOnly

Tamamen dış dünyaya kapalı bir sistemdir. Sadece host üzerindeki sanal makinalar birbirleri ile haberleşebilir.

Player>Manager>Virtual Machine Settings>Network Adapters

# Network Ayarları

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:4f:2f:59  
          inet addr:192.168.66.130  Bcast:192.168.66.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe4f:2f59/64  Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:40137 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:323843 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:19204095 (18.3 MiB)  TX bytes:19489842 (18.5 MiB)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128  Scope:Host  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1  
          RX packets:12698 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:12698 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:903768 (882.5 KiB)  TX bytes:903768 (882.5 KiB)
```

• **ifconfig** komutu mevcut ağ kartlarının bilgilerini getirir.

- **ifconfig** komutu yanına istenen ağ kartının ismi yazılırsa sadece o ağ kartının bilgileri gelir.

```
File Edit View Search Terminal Help
root@kali:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:4f:2f:59
          inet addr:192.168.66.130  Bcast:192.168.66.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe4f:2f59/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40137 errors:0 dropped:0 overruns:0 frame:0
          TX packets:323843 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19204095 (18.3 MiB)  TX bytes:19489842 (18.5 MiB)
```

- **ifconfig** komutu ile istediğimiz ağ kartına ip adresi atayabiliriz.

```
File Edit View Search Terminal Help
root@kali:~# ifconfig eth0 192.168.66.133 netmask 255.255.255.0
root@kali:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:4f:2f:59
          inet addr:192.168.66.133  Bcast:192.168.66.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe4f:2f59/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40137 errors:0 dropped:0 overruns:0 frame:0
          TX packets:323843 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19204095 (18.3 MiB)  TX bytes:19489842 (18.5 MiB)
```

# Network Ayarları

- Bulunduğumuz ağda bir dhcp sunucu varsa yeni bir IP talepte edebiliriz.
- Bunun için önce ağ servisini durdurulur.
- Daha sonra ip isteyeceğimiz ağ kartını aktif hale getirip ağ servisi başlatılır.

51

```
root@kali:~# service networking stop
[ ok ] Deconfiguring network interfaces...done.
root@kali:~# ip link set eth0 up
root@kali:~# /etc/init.d/networking start
[....] Configuring network interfaces...Internet Systems Consortium DHCP Client 4.2.2
Copyright 2004-2011 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:0c:29:4f:2f:59
Sending on   LPF/eth0/00:0c:29:4f:2f:59
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 8
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPOFFER from 192.168.66.254
DHCPACK from 192.168.66.254
Reloading /etc/samba/smb.conf: smbd only.
bound to 192.168.66.130 -- renewal in 714 seconds.
done.
```

50

# Temel Linux Kullanımı

Temel Komut Serisi-1

Linux Dosya Sistemi

Linux Komut Serisi-2

Network Ayarları

Servisler

Kullanıcı Yönetimi

Process

Paket Yönetim Sistemi


Sistem İzleme

- Servisler **/etc/init.d** klasörü altında bulunmaktadır.

```
File Edit View Search Terminal Help
root@kali:~# ls /etc/init.d/
apache2          kmod              redsocks
arpwatch         lvm2              rlinetd
atd              metasploit        rmnologin
atftpd           miredo            rpcbind
avahi-daemon     motd              rsync
beef-xss         mountall-bootclean.sh rsyslog
binfmt-support   mountall.sh       samba
bluetooth        mountdevsubfs.sh  saned
bootlogs         mountkernfs.sh    screen-cleanup
bootmisc.sh      mountnfs-bootclean.sh sendsigs
checkfs.sh       mountnfs.sh       single
checkroot-bootclean.sh mtab.sh           skeleton
checkroot.sh     mysql             smartd
console-screen.sh nessusd            smartmontools
console-setup    networking        snmpd
cron              network-manager  speech-dispatcher
cryptdisks       nfs-common        ssh
cryptdisks-early nginx              sslh
darkstat         ntp               stunnel4
dbus             openvas-administrator sudo
dns2tcp          openvas-manager   thin
dradis           openvas-scanner   truecrypt
exim4            openvpn           udev
```

- Sistemdeki mevcut servislerin durumunu görmek için **service --status-all** komutu çalıştırılmalıdır.

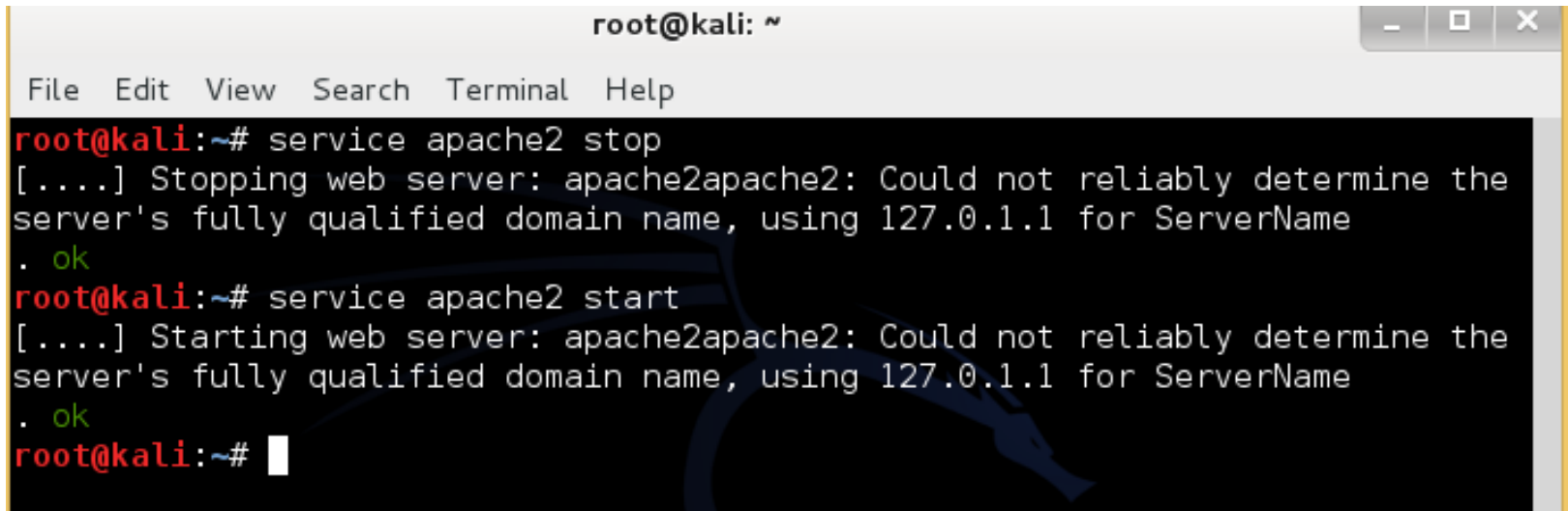
```
File Edit View Search Terminal Help
root@kali:~# service --status-all
[ - ] apache2
[ ? ] arptwatch
[ + ] atd
[ ? ] atftpd
[ + ] avahi-daemon
[ - ] beef-xss
[ ? ] binfmt-support
[ + ] bluetooth
[ - ] bootlogs
[ ? ] bootmisc.sh
[ ? ] checkfs.sh
[ ? ] checkroot-bootclean.sh
[ - ] checkroot.sh
[ ? ] console-screen.sh
[ - ] console-setup
[ + ] cron
[ ? ] cryptdisks
[ ? ] cryptdisks-early
[ ? ] darkstat
[ + ] dbus
[ ? ] dns2tcp
[ - ] dradis
```

The image shows a terminal window with a Kali Linux desktop background. The background is dark with a blue dragon logo and the text "KALI LINUX" and "The quieter you become, the more you are able to hear". The terminal window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The command "service --status-all" is entered, and the output shows a list of services with their status indicated by brackets and symbols: [ - ] for stopped, [ ? ] for unknown, and [ + ] for running.



# WEB Servisinin Başlatılması

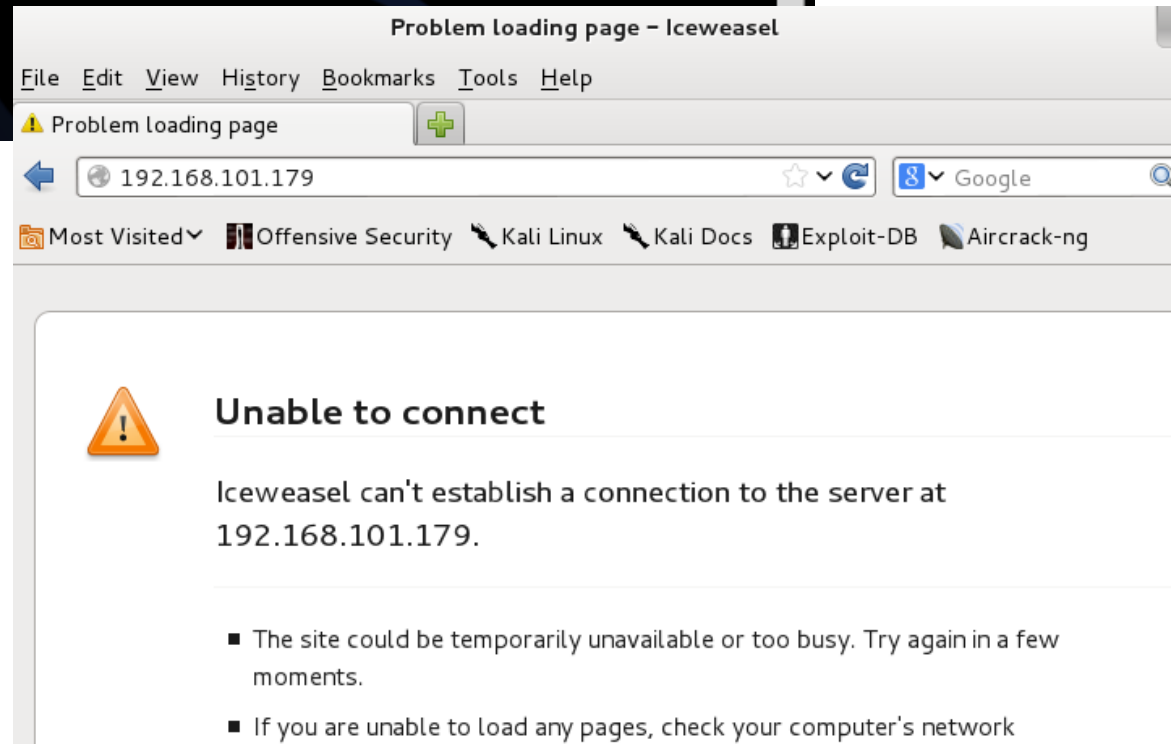
- Web üzerinden yayın yapabilmek için apache http servisi kullanılır.
- Servisi başlatmak: **service apache2 start** ya da **/etc/init.d/apache2 start**
- Servisi durdurmak için aynı komutların sonuna **stop** yazılır.

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
root@kali:~# service apache2 stop
[....] Stopping web server: apache2apache2: Could not reliably determine the
server's fully qualified domain name, using 127.0.1.1 for ServerName
. ok
root@kali:~# service apache2 start
[....] Starting web server: apache2apache2: Could not reliably determine the
server's fully qualified domain name, using 127.0.1.1 for ServerName
. ok
root@kali:~#
```

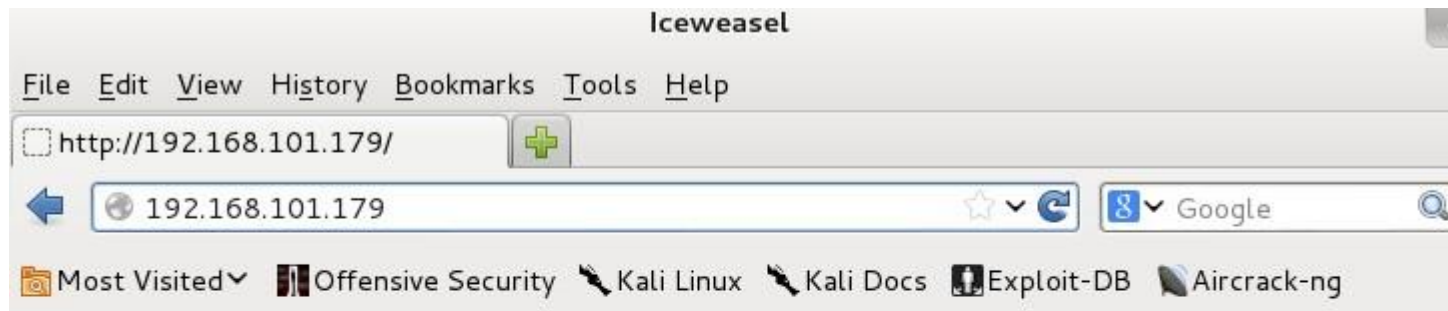
# WEB Servisinin Başlatılması

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig eth0 | head -n2  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:4f:2f:59  
          inet addr:192.168.101.179  Bcast:192.168.101.255  Mask:255.255.255.0  
root@kali:~# ifconfig eth0 | head -n2 | tail -n1  
          inet addr:192.168.101.179  Bcast:192.168.101.255  Mask:255.255.255.0  
root@kali:~# ifconfig eth0 | head -n2 | tail -n1 | cut -d: -f2  
192.168.101.179  Bcast  
root@kali:~# ifconfig eth0 | head -n2 | tail -n1 | cut -d: -f2 | cut -d " " -f1  
192.168.101.179  
root@kali:~#
```



# WEB Servisinin Başlatılması

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# service apache2 start  
[....] Starting web server: apache2  
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName  
httpd (pid 3593) already running  
. ok  
root@kali:~#
```



## It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

# SSH Servisinin Başlatılması

- Uzaktan bağlantı için SSH servisi kullanılır.
- Servisi başlatmak: **service ssh start** ya da **/etc/init.d/ssh start** komutları kullanılır.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# service ssh start  
[ ok ] Starting OpenBSD Secure Shell server: sshd.  
root@kali:~#
```

# Samba servisinin açılması

- Samba ile iki bilgisayar arasında paylaşım sürücüsü oluşturulabilir
- `/etc/samba/smb.conf` dosyası yapılandırılır
- Windows 7'de paylaşım sürücüsü oluşturulur

# Temel Linux Kullanımı

Temel Komut Serisi-1

Linux Dosya Sistemi

Linux Komut Serisi-2

Network Ayarları

Servisler

Kullanıcı Yönetimi

Process

Paket Yönetim Sistemi

Sistem İzleme

# Linux'ta Kullanıcı Yönetimi

Temel olarak 4 çeşit işletim sistemi vardır. Bunlar;

- Single User - Single Task
- Single User - Multi Task
- **Multi User - Multi Task**
- Real Time Operating System

- Linux bunlardan **multi user -multi task** yani çok kullanıcı ve çok görevli işletim sistemleri kategorisine girer.
- Linux bir sisteme, aynı anda birden fazla kullanıcı login olabilir ve diğer kullanıcılardan bağımsız bir şekilde kendi işlemlerini yürütebilir.
- Windows da MM örnektir. Uzak masaüstü ile bağlanıldığında bir kullanıcı için bir görev çalışıyor bıraktıktan sonra diğer kullanıcı da oturum açar çalışan işlemi etkilemeden işlem yapabilir.

# Linux'ta Kullanıcı Yönetimi

- Linux işletim sisteminde kullanıcı bilgileri **/etc/passwd** dosyasında tutulur.
- Sistemde ki mevcut grupların bilgileri ise **/etc/group** dosyasında tutulur.
- Aktif kullanıcıların şifre özetleri ise **/etc/shadow** dosyasında tutulur.
- Normal haklara sahip kullanıcılar **/etc/passwd** ve **/etc/group** dosyalarının içeriğini görebilir ama içeriği değiştiremez.
- **/etc/shadow** dosyasının içeriğini ise sadece root kullanıcısı ve sudo (superuser) hakkına sahip kullanıcılar görebilir.



- Bu dosya kullanıcı bilgilerini saklar.
- **file** komutu ile ASCII text dosyası olduğu görülebilir.
- Her yeni kullanıcı için yeni bir girdi oluşturulur ve genel formu şu şekildedir.
- isim:şifre:uid:gid:yorum:evdizini:kabuk
- **isim** : Kullanıcının login ismi
- **şifre** : x
- **uid** : Kullanıcı ID'si
- **gid** : Grup ID'si
- **yorum** : Kullanıcı adı ya da bir yorum
- **evdizini** : Kullanıcının varsayılan ev dizini
- **kabuk** : Kullanıcı için ön tanımlı kabuk

Sistemdeki grupların bilgileri tutulur.

Genel formu şu şekildedir.

grup\_ismi:grup\_şifresi:grup\_id:üye

A terminal window titled 'root@kali' with a menu bar containing 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows the command 'cat /etc/group' being executed. The output lists system groups in the format 'group\_name:x:group\_id:user\_list'. The groups listed are: root, daemon, bin, sys, adm, tty, disk, lp, mail, news, uucp, man, proxy, kmem, dialout, fax, voice, cdrom, floppy, and tape. The terminal has a dark background with a faint 'KALI' logo and the text 'The quieter' visible on the right side.

```
root@kali:~# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:
floppy:x:25:
tape:x:26:
uucp:x:27:
```

- Bu dosya şifre özetlerini ve şifreler hakkındaki bilgileri tutan bir ASCII text dosyasıdır.
- Sadece root ve sudo hakkına sahip kullanıcılar tarafından görüntülenebilir.
- Kayıtların genel formu şu şekildedir.

```
root@kali:~# cat /etc/shadow
root:$6$zmDf0i3Y$EVBX5MjvJYwZ1yKtP9PK6H9dVB4kagVW9qiDBKMxg74/q1qJctoD4gjpB2A17F5
enZwxWGXusTeNaz6j2Wrre/:16331:0:99999:7:::
```

```
root@kali:~# cat /etc/shadow
root:$6$zmDf0i3Y$EVBX5MjvJYwZ1yKtP9PK6H9dVB4kagVW9qiDBKMxg74/q1qJctoD4gjpB2A17F5
enZwxWGXusTeNaz6j2Wrre/:16331:0:99999:7:::
```

## isim:şifre:sondeğişim:min:max:warn:inactive:expire:flag

- **isim** : Kullanıcı adı
- **şifre** : Parolanın şifre özeti, \* yada ! varsa hesap aktif değildir.
- **sondeğişim** : Şifrenin değişmesinden itibaren kaç gün geçmiş
- **min** : Tekrar parola değiştirmeden önce geçmesi gereken süre
- **max** : Parola değiştirmek zorunluluğu için tanımlı en fazla süre
- **warn** : Parolanın geçerliliği dolmadan kaç gün önce uyarsın
- **inactive** : Parolanın geçerliliği dolup hesap bloklandıktan sonra kaç gün geçmiş
- **expire** : Parolanın en son değiştirildiği tarihten itibaren hesabın kaç gün blokeli olduğu
- **flag** : Reserve edilmiş alan

# Sisteme Kullanıcı Ekleme/Silme

- Sisteme kullanıcı eklemek için kullanılan iki komut var. **adduser** ve **useradd**.
- Sistemde ki kullanıcıyı silmek içinde iki komut var. **deluser** ve **userdel**.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# useradd user1  
root@kali:~# cat /etc/shadow | tail -n1  
user1:!:16406:0:99999:7:::  
root@kali:~# userdel user1  
root@kali:~# cat /etc/shadow | tail -n1  
saned*:~:16078:0:99999:7:::  
root@kali:~#  
root@kali:~#
```

- `# hostname` ile bilgisayarın adını görüntüleyebilir.
- `# hostname YeniBilgisayarAdı` ile bilgisayar adını değiştirebilirsiniz.

# Temel Linux Kullanımı

Temel Komut Serisi-1

Linux Dosya Sistemi

Linux Komut Serisi-2

Network Ayarları

Servisler

Kullanıcı Yönetimi

Process

Paket Yönetim Sistemi

Sistem İzleme



Process kavramı

Çalışan süreçleri izleme

Arka plan Process

Süreç Sonlandırma



- Çalışmakta olan program parçacığına süreç denir.
- Her sürecin kendisine ait unique bir ID'si(PID) vardır.
- Process (süreç işlemleri) bu PID üzerinden ilerler.
- Linux'ta aynı anda birden fazla kullanıcı için birden fazla süreç çalıştırabilir.

# Çalışan Süreçleri İzleme

- Sistemde çalışan süreçleri ve durumları öğrenmek için **ps** komutu kullanılır.
- Temel kullanımı aşağıdaki gibidir.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ps  
  PID TTY          TIME CMD  
 3370 pts/0    00:00:00 bash  
 3471 pts/0    00:00:00 ps  
root@kali:~#
```

# Çalışan Süreçleri İzleme

- ❖ Çalışan tüm süreçleri görmek için **ps** komutu **a**, **u** ve **x** parametreleri ile birlikte kullanılmalıdır.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ps aux  
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND  
root         1   0.8   0.0  10652   836 ?        Ss   12:45   0:01 init [2]  
root         2   0.0   0.0     0     0 ?        S    12:45   0:00 [kthreadd]  
root         3   0.0   0.0     0     0 ?        S    12:45   0:00 [ksoftirqd/0]  
root         4   0.0   0.0     0     0 ?        S    12:45   0:00 [kworker/0:0]  
root         5   0.0   0.0     0     0 ?        S<   12:45   0:00 [kworker/0:0H]  
root         6   0.0   0.0     0     0 ?        S    12:45   0:00 [kworker/u64:0]  
root         7   0.0   0.0     0     0 ?        S    12:45   0:00 [migration/0]  
root         8   0.0   0.0     0     0 ?        S    12:45   0:00 [rcu_bh]  
root         9   0.1   0.0     0     0 ?        S    12:45   0:00 [rcu_sched]  
root        10   0.0   0.0     0     0 ?        S    12:45   0:00 [watchdog/0]  
root        11   0.0   0.0     0     0 ?        S<   12:45   0:00 [khelper]  
root        12   0.0   0.0     0     0 ?        S    12:45   0:00 [kdevtmpfs]
```

# Çalışan Süreçleri İzleme

- Süreçleri görüntülemek için top komutu da kullanılabilir.
- top komutunda gösterilen veri anlık olarak güncellenir.
- Windows Task Manager benzeri çalışır.

```
root@kali: ~
File Edit View Search Terminal Help
top - 13:00:35 up 14 min, 2 users, load average: 0.04, 0.05, 0.05
Tasks: 124 total, 1 running, 123 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.7 sy, 0.0 ni, 99.0 id, 0.0 wa, 0.0 hi, 0.3 si, 0.0 st
KiB Mem: 1021640 total, 487764 used, 533876 free, 31048 buffers
KiB Swap: 1748988 total, 0 used, 1748988 free, 217196 cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU  %MEM    TIME+  COMMAND
 2536 root        20   0 138m  29m 6752 S   0.3   2.9   0:12.04 Xorg
 3190 root        20   0 432m  16m 12m S   0.3   1.7   0:00.52 gnome-settings-
 3227 root        20   0 394m  35m 14m S   0.3   3.6   0:01.49 gnome-panel
 3272 root        20   0 251m  26m 17m S   0.3   2.6   0:05.46 vmtoolsd
 3363 root        20   0 223m  18m 11m S   0.3   1.9   0:04.69 gnome-terminal
 3515 root        20   0 23108 1596 1152 R   0.3   0.2   0:00.02 top
    1 root        20   0 10652  836  696 S   0.0   0.1   0:01.10 init
    2 root        20   0     0     0     0 S   0.0   0.0   0:00.00 kthreadd
    3 root        20   0     0     0     0 S   0.0   0.0   0:00.09 ksoftirqd/0
    5 root         0 -20     0     0     0 S   0.0   0.0   0:00.00 kworker/0:0H
    6 root        20   0     0     0     0 S   0.0   0.0   0:00.02 kworker/u64:0
    7 root        rt    0     0     0     0 S   0.0   0.0   0:00.00 migration/0
    8 root        20   0     0     0     0 S   0.0   0.0   0:00.00 rcu bh
```

- Kill komutuna ait sinyaller aşağıdaki gibidir
  - 1 (SIGHUP) : Bazı servisler tarafından konfigürasyon dosyalarını yeniden okunması için kullanılmaktadır.
  - 9(SIGKILL) : Bir süreci tamamen öldürmek için kullanılır.
- Benzeri sayılabilecek **killall** ve **pkill** gibi komutlarda mevcuttur.

# Temel Linux Kullanımı

Temel Komut Serisi-1

Linux Dosya Sistemi

Linux Komut Serisi-2

Network Ayarları

Servisler

Kullanıcı Yönetimi

Process

Paket Yönetim Sistemi

Sistem İzleme

# Paket Yönetim Sistemi

- Paket, Program Kavramları
- Repository Kavramı
- Paket Yönetim Sistemleri
- Kaynak Koddan Kurulum



# Paket, Program Kavramları

- Paket, programların işletim sistemine kurulacak hale getirilmiş (derlenmiş) versiyonudur. Paketler programla ilgili metadata (versiyon, dependency vb.) içerirler.
- Yazılımları sıfırdan yüklemek, güncellemek için paketlerden faydalanırız.
- Farklı Linux dağıtımları için oluşturulmuş paketler diğerleri için uygun değildir. Mesela Ubuntu için hazırlanmış paketler RedHat için uygun değildir.



# Debian Linux PMS

- Binary paketleri: .deb formatlı dpkg ile kurulabilen
  - `dpkg -i <paket adı>`
- Source paketleri: .dsc, orig.tar.gz formatlı ve dpkg-source/apt-get aracı ile derlenebilen
  - `apt-get source <paketadı>`
  - `tar jxvf <paketadı>`
  - `./configure && make && make install`
- Paketlerin dayandıkları diğer paketler, kütüphaneler dependency olarak adlandırılır.
- If GCC package depends on binutils
  - Önce binutils yüklememiz gerekmektedir GCC yüklemesini durdurmamız gerekmektedir

# Repository Kavramı

- Paket yönetim sistemlerinin kullandığı kaynaklardır.
- Paket yönetim sistemleri bir programı aradığında bu kaynak adreslerden bakar ve indirir.
- Linux sürümlerinin hepsinde paket yönetim sistemi olduğu için repository kullanırlar.(Synaptic aracı GUI si olan)
- Ubuntu, Backtrack ve Kali gibi dağıtımlarda /etc/apt/source.list dosyasının altında sistem için tanımlanmış repository'ler bulunur. #cat /etc/apt/sources.list
- apt-get komutu ile gerekli yüklemeler ve güncellemeler yapılır.

# apt-get Paket Yönetimi

- Paket yüklemek için
  - apt-get install PaketAdı
  - dpkg -i <paket adı.deb>
- Paket aramak için
  - apt-cache search PaketAdı
- Paket dependency arama
  - apt-cache depends PaketAdı
- Paket güncellemek için
  - apt-get update
  - apt-get --upgrade install
  - apt-get update PaketAdı
  - apt-get upgrade PaketAdı
- Süreci arayüzden yürütmek için
  - apt-get install synaptic
- Linux Güncelleştirme
  - apt-get dist-upgrade
- Paket kaldırmak için
  - apt-get remove PaketAdı
- Tüm paketler
  - dpkg --get-selections (dpkg -l)
- Sadece yüklü paketler
  - dpkg --get-selections | grep -v deinstall

# Kaynak Koddan Kurulum

- Kaynak koddan kurulum yapmak için kaynak kodu indirilen programın sırasıyla
  - **./configure&& make&& makeinstall** komutları ile çalıştırılması gerekir.
  - **./configure** sistemdeki gereksinimleri denetler. Kesin olması gereken bir bileşen bulunmuyorsa hata verir. Hata giderildikten sonra baştan çalıştırılır.
  - **make** komutu gerekli check işlemi yapıldıktan sonra programı derler (compilation). Burada eğer hata alınıyorsa hata giderilmelidir. Aksi takdirde derlenmemiş bir program kurulmaz.
  - **make install** komutu ile derlenmiş program kurulur.

# Paket indirme

1. `/etc/apt/sources.list`
2. `apt-cache search <paketadı>`
3. `apt-get update`
4. `apt-get install <paket adı> (wget)`
5. `apt-get upgrade <paket adı>`
6. `apt-get install -f`

# Temel Linux Kullanımı

Temel Komut Serisi-1

Linux Dosya Sistemi

Linux Komut Serisi-2

Network Ayarları

Servisler

Kullanıcı Yönetimi

Process

Paket Yönetim Sistemi

Sistem İzleme

- Disk Durumu
- Ram Durumu
- CPU Durumu
- Ağ Durumu



- Kullanılan diskin durumunu görmek için **df** veya **fdisk** komutu kullanılır.
- -h parametresi ile çıktı daha anlaşılır halde gözükür.

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# df -h
```

Filesystem	Size	Used	Avail	Use%	Mounted on
rootfs	38G	13G	24G	36%	/
udev	10M	0	10M	0%	/dev
tmpfs	100M	580K	100M	1%	/run
/dev/disk/by-uuid/c9a29388-6cec-4125-ad9a-485db95861d8	38G	13G	24G	36%	/
tmpfs	5.0M	0	5.0M	0%	/run/lock
tmpfs	542M	224K	541M	1%	/run/shm



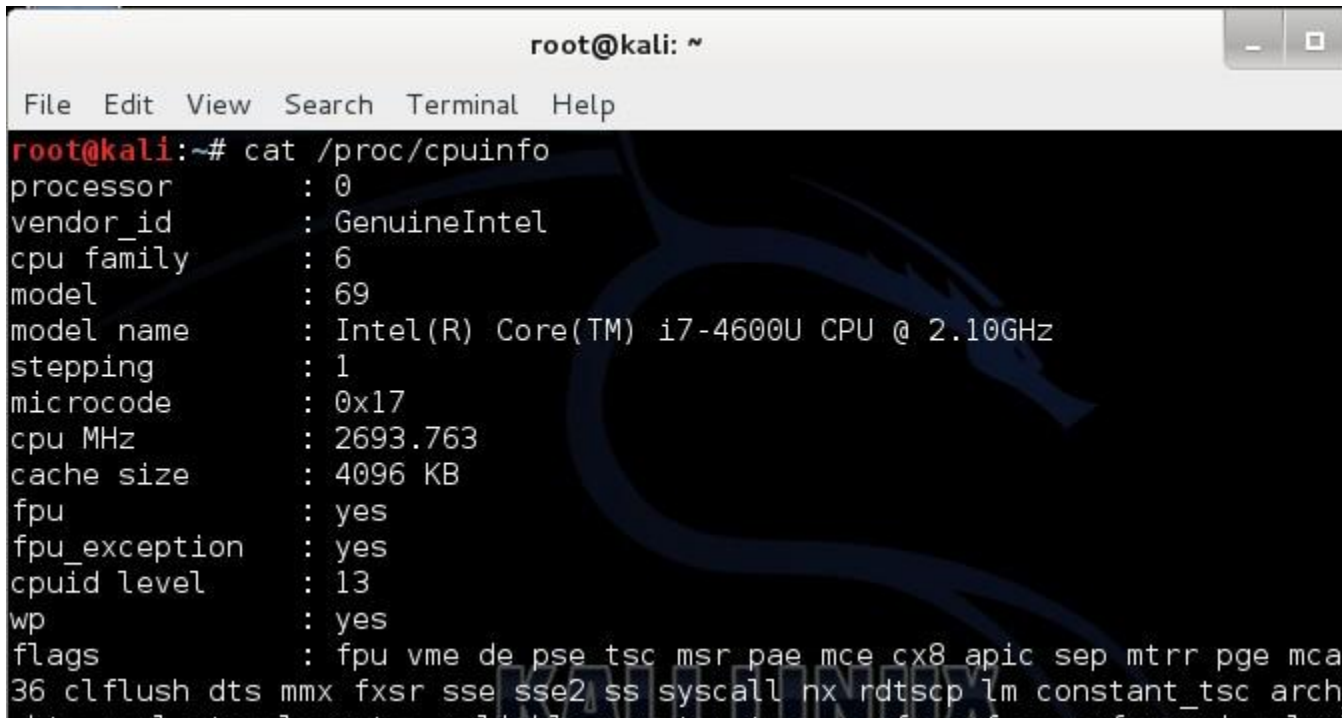
# RAM Durumu

- RAM durumunu görmek için **top** ya da **free** komutu kullanılabilir veya **/proc/meminfo** dosyasına bakılabilir.

```
root@kali: ~  
File Edit View Search Terminal Help  
top - 15:08:17 up 41 min, 2 users, load average: 0.10, 0.10, 0.22  
Tasks: 124 total, 1 running, 123 sleeping, 0 stopped, 0 zombie  
%Cpu(s): 0.0 us, 0.3 sy, 0.0 ni, 99.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st  
KiB Mem: 1021640 total, 491552 used, 530088 free, 31520 buffers  
KiB Swap: 1748988 total, 0 used, 1748988 free, 217592 cached  
  
  PID USER      PR  NI  VIRT  RES  SHR S %CPU  %MEM    TIME+  COMMAND  
    1 root        20   0 10652   836  696 S   0.3   0.1   0:01.13 init  
  1951 root        20   0 98.8m 4564 3688 S   0.3   0.4   0:03.52 vmtoolsd  
  2536 root        20   0 140m 30m 6916 S   0.3   3.1   0:16.63 Xorg  
  3705 root        20   0 23108 1584 1152 R   0.3   0.2   0:00.02 top  
    2 root        20   0     0     0     0 S   0.0   0.0   0:00.00 kthreadd  
    3 root        20   0     0     0     0 S   0.0   0.0   0:00.12 ksoftirqd/0  
    5 root         0 -20     0     0     0 S   0.0   0.0   0:00.00 kworker/0:0H  
    6 root        20   0     0     0     0 S   0.0   0.0   0:00.02 kworker/u64:0  
    7 root        rt    0     0     0     0 S   0.0   0.0   0:00.00 migration/0  
    8 root        20   0     0     0     0 S   0.0   0.0   0:00.00 rcu_bh  
    9 root        20   0     0     0     0 S   0.0   0.0   0:00.30 rcu_sched
```

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# cat /proc/meminfo | head  
MemTotal:          1021640 kB  
MemFree:            529100 kB  
Buffers:            31532 kB  
Cached:             217636 kB  
SwapCached:          0 kB  
Active:             243200 kB  
Inactive:           185336 kB  
Active(anon):       179876 kB  
Inactive(anon):      624 kB  
Active(file):        63324 kB
```

- CPU durumunu analiz etmek için iki farklı komut vardır. Bunlar **vmstat** ve **top** komutlarıdır.
- **/proc/cpuinfo** dosyası da CPU hakkında bilgi verir.

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command 'cat /proc/cpuinfo' has been executed, displaying the following CPU information:

```
root@kali:~# cat /proc/cpuinfo
processor       : 0
vendor_id      : GenuineIntel
cpu family     : 6
model          : 69
model name     : Intel(R) Core(TM) i7-4600U CPU @ 2.10GHz
stepping       : 1
microcode      : 0x17
cpu MHz        : 2693.763
cache size     : 4096 KB
fpu            : yes
fpu_exception  : yes
cpuid level    : 13
wp             : yes
flags          : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
36 clflush dts mmx fxsr sse sse2 ss syscall nx rdtscp lm constant_tsc arch
```

- Sistemin son açılışından şuana kadarki durumu hakkında rapor veren bir komuttur.
- Kuyrukta bekleyen, çalışan kernel thread'ler, diskler, sistem çağrıları ve CPU aktivitesi ile ilgili istatistik bilgi verir.
- Komuta verilen ilk parametre kaç saniyede bir rapor üretileceğini, ikinci parametre ekrana kaç defa çıktı verileceğini belirtir.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# vmstat 2 5  
procs -----memory----- --swap-- -----io----- -system-- ----cpu----  
r b   swpd   free   buff  cache   si   so    bi    bo    in   cs us sy id wa  
0 0     0 518016 31704 223360    0    0   93    3  104  165  6 13 81  1  
2 0     0 518000 31704 223360    0    0    0    0   83  215  1  2 97  0  
0 0     0 518000 31704 223360    0    0    0    0  306  526 11 13 76  0  
0 0     0 518000 31704 223360    0    0    0    0   32   79  1  0 99  0  
0 0     0 518000 31704 223360    0    0    0    0   32   77  0  1 99  0
```

- Ağ durumu analizi için **netstat** komutu kullanılmaktadır.
- Ağ istatistikleri, route tablosu, aktif ve pasif bağlantılar gibi bir çok bilgiyi kullanıcıya sunar.
- Komuttan sonra gelen parametreler ile kullanılır.
  - **-s** parametresi ile ağ istatistikleri
  - **--route** ile route tablosu
  - **-t** ile tcp bağlantıları
  - **-u** ile udp bağlantıları gözetlenebilir

```
root@kali:~# netstat --route
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
default          192.168.0.1     0.0.0.0         UG        0  0          0 eth0
192.168.0.0      *               255.255.255.0   U         0  0          0 eth0
```

```
File Edit View Search Terminal Help
root@kali:~# netstat -u
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp      0      0 192.168.0.14:56215     ns3.uydunet.net:domain ESTABLISHED
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# netstat -s
Ip:
  10273 total packets received
    0 forwarded
    0 incoming packets discarded
  10273 incoming packets delivered
  6904 requests sent out
Icmp:
```

**Şimdi sıra sizde...!**

# Faydalı diğer komutlar

- 2 ayrı ip adresi çıktısı var
- Bu dosyaları tek bir dosyada birleştirip, aynı ip adreslerini temizleyip, büyükten küçüğe sıralayıp, kaç adet ip adresimiz olduğunu tespit edelim
- Kullanılacak komutlar: sort, cat, uniq, vim

# Faydalı diğer komutlar

- Bir adet password listesi oluşturup önceki aşamadaki ip listesinin yanına **paste komutu** ile ekleyelim
- **sed komutu** ile 192 ile başlayan ip adreslerini yanlış yazdığımızı varsayıp 172 olarak değiştirelim
- **tr komutu** ile küçük harflerin hepsini büyük harfe çevirelim
- **chmod** ile dosya sahibine tüm hakları, grup ve diğer tüm kullanıcılara ise okuma ve çalıştırma haklarını verip
- **stat komutu** ile de dosya hakkındaki bilgileri görüntüleyelim



- Bazen aynı komutları girmek sıkıcı olabilir
- Onun yerine tek kelimeyle sık kullandığımız uzun komutlar çağırabilir
- Geçici olarak

```
alias netbiostarama='nbtscan -r 192.168.100.1-50/24'
```

- Kalıcı olarak makine yeniden başlatıldığında da kullanabilmek için aynı komutu ~/.bashrc dosyası içine eklenmelidir.

- Belirlenen vakitlerde bazı işlerin çalışmasını /etc/crontab yapılandırma dosyası üzerinden otomatikleştirebiliriz
- **service crontab start** ile servis açılır
- Nbtscan ile belirli saatlerde isim çözümlemesi yapmak istiyoruz bunu bash script olarak yazıp otomatikleştirebiliriz

#	Minute	Hour	Day of Month	Month	Day of Week	Command
#	(0-59)	(0-23)	(1-31)	(1-12 or Jan-Dec)	(0-6 or Sun-Sat)	
	0	2	12	*	*	/usr/bin/find