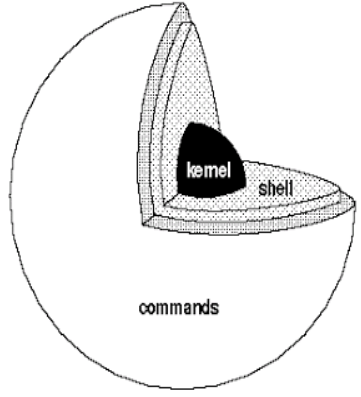


# 30 günde Cyber Security-1 öğren

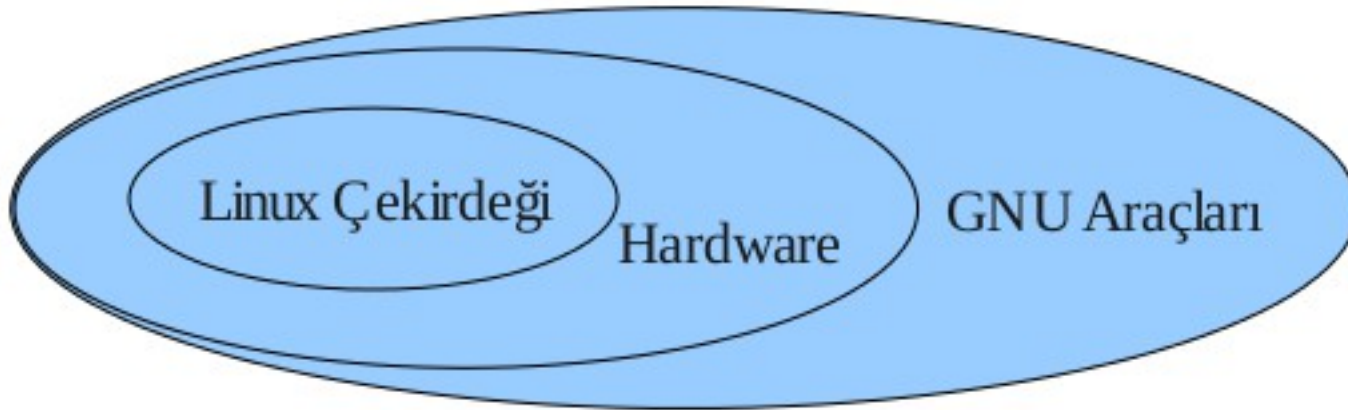
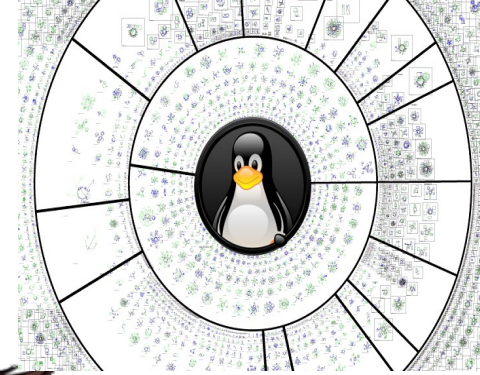
## 5&6. GÜN



Dosya Dizin İşlemleri  
Komut Satırı (Kabuk)  
Temel Komutlar -2  
Hostname ve Network Ayarları  
Servisler  
Linuxta Kullanıcı Yönetimi



**GNU**  
run free run GNU



# Dosya Dizin İşlemleri

- Dosya ve dizinler üzerinde çeşitli işlemler yapılabilir.
  - Oluşturulabilir.
  - Silinebilir.
  - Değiştirilebilir.
  - Listelenebilir, çalıştırılabilir.
  - Taşıma veya kopyalama yapılabilir.

# Dosya Dizin İşlemleri

- Dosya ve dizinler için tanımlanmış haklar mevcuttur. Bu haklar ve izinler değiştirilebilir.
  - Sahibi, grubu ve herkes.
  - Örneğin herkese okuma hakkı ver.

# Dosya İzinleri

- **Her dosyanın;**
  - Bir sahibi vardır.
  - Bir grubu vardır.
  - Sahibi, grubu ve herkes olmak üzere üç çeşit erişim izni vardır.
  - Bir dosya oluşturulurken varsayılan izinleri umask ile belirlenir.

# Dosya İzinleri

- **Her kullanıcının;**

- UID (login ismi), gid (login grubu) ve diğer gruplara üyeliği vardır.
- UID kimliğinizi gösterir. (Kullanıcı ve ID numarası)
- GID (Grup adı ve numarasını gösterir)

# Dosya İzinleri

- Linux için üç çeşit dosya izin kavramı vardır.
  - **Read(r)** : Dosya veya dizinlerin okunabilmesi için gerekli olan izindir. Dizinlerde listeleme özelliği olarak kullanılır.
  - **Write(w)** : Yeni bir dosya veya dizin oluşturmak, değiştirmek için gerekli olan izindir.
  - **Execute(x)** : Dosya çalıştırılması ya da dizine giriş hakkı için kullanılan izindir.

# Dosya İzinleri

- Linuxde dosya izinleri belli bir paradigma kullanılarak ifade edilir ve kullanılır.  
- **chmod 777 dosya\_ismi**



# Dosya İzinleri

- 7 sayısının ikilik sayı sistemindeki karşılığı (1 1 1)

0 : 000 → ---

1 : 001 → --x

2 : 010 → -w-

3 : 011 → -wx

4 : 100 → r--

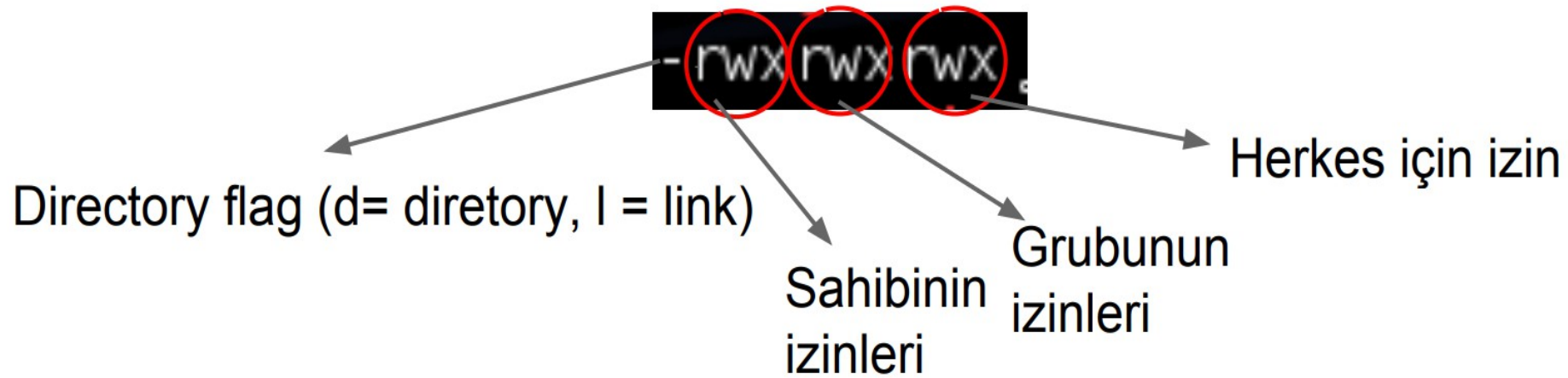
5 : 101 → r-x

6 : 110 → rw-

7 : 111 → rwx

# Dosya İzinleri

- Gösterilen bu izin öbeklerinden üç adet vardır.



# Dosya İzinleri

- Dosya izinleri detaylı incelendiğinde aşağıdaki gibidir.

```
root@kali:~/Desktop# ls -l deneme.txt  
-rwxrwxrwx 1 root root 215 Oct  7 10:06 deneme.txt
```

İzinler

Sahibi

Grubu

# Dosya İzinleri

- chmod komutu dosya veya dizinlerin izinlerinde değişiklik yapabiliriz. Sayısal değer veya yazıyla bu değişiklikler yapılabilir

```
root@kali:~/Desktop# ls -l deneme.txt
-rwxrwxrwx 1 root root 215 Oct  7 10:06 deneme.txt
root@kali:~/Desktop# chmod 222 deneme.txt
root@kali:~/Desktop# ls -l deneme.txt
--w--w--w- 1 root root 215 Oct  7 10:06 deneme.txt
```

- Aşağıda ise yazı ile bu değişim yapılmıştır

```
root@kali:~/Desktop# ls -l deneme.txt
-rwxrwxrwx 1 root root 215 Oct  7 10:06 deneme.txt
root@kali:~/Desktop# chmod u-r,g-r,o-r deneme.txt
root@kali:~/Desktop# ls -l deneme.txt
--wx-wx-wx 1 root root 215 Oct  7 10:06 deneme.txt
```

PS: u = kullanıcı , g = grubu, o = herkes. +: ekler, - : siler. .

# # mkdir Komutu

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# mkdir -p intelrad /tmp/
root@kali:~/Desktop# ls /tmp/ -l
total 32
drwxr-xr-x 2 root      root      4096 Oct  8 09:02 intelrad
drwx----- 2 root      root      4096 Oct  8 04:27 pulse-7KuijalqVtuT
drwx----- 2 Debian-gdm Debian-gdm 4096 Oct  8 04:27 pulse-YKmt05D3yDXe
drwx----- 2 root      root      4096 Oct  8 04:27 ssh-3wUYBKD2p7qC
```

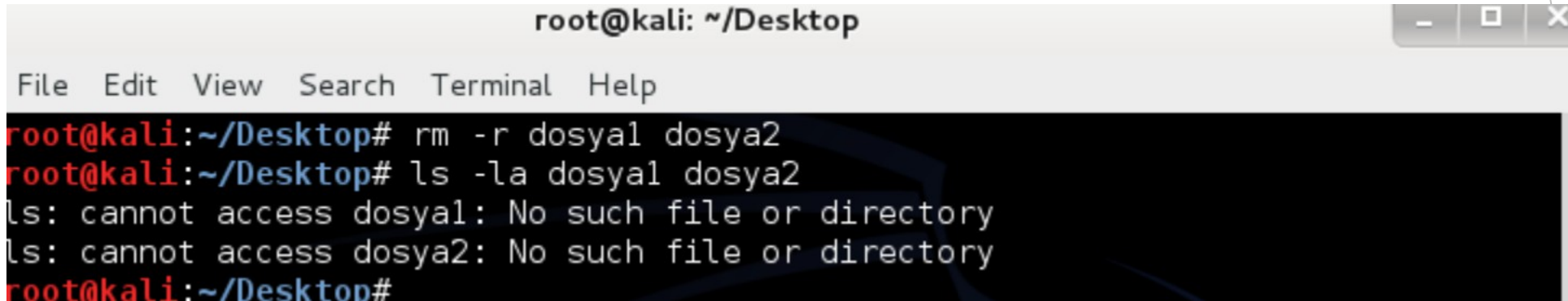
- Dizin oluşturmaya yarayan komuttur.
- Kullanımı : **mkdir [seçenek] [dizin\_adi] Dizin..**
- **-p** parametresi ile mevcut dizinin altında bir dizin oluşturulabilir.
- Ayrıntılı bilgi için man mkdir.

# # touch Komutu

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# touch dosya1 dosya2
root@kali:~/Desktop# ls -la dosya1 dosya2
-rw-r--r-- 1 root root 0 Oct  8 09:49 dosya1
-rw-r--r-- 1 root root 0 Oct  8 09:49 dosya2
root@kali:~/Desktop#
```

- Dosya oluşturmaya yarayan komuttur.
- Kullanımı : **touch [seçenek] [[dosya\_adi], ...]**
- Ayrıntılı bilgi için **man touch**

# # rm Komutu

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

```
root@kali:~/Desktop# rm -r dosya1 dosya2
root@kali:~/Desktop# ls -la dosya1 dosya2
ls: cannot access dosya1: No such file or directory
ls: cannot access dosya2: No such file or directory
root@kali:~/Desktop#
```

- Dosya/klasör silmek için kullanılan komuttur.
- Kullanımı : **rm [seçenek] [dosya]**
- **-r** parametresi ile rekürsif bir şekilde, verilen dosyanın içindeki tüm dosyalar silinebilir.
- Ayrıntılı bilgi için **man rm**

## # rm Komutu -2

- **-r** parametresi ile rekürsif bir şekilde, verilen dosyanın içindeki tüm dosyalar silinebilir.
- **-f** : Hiçbir şey sormadan siler.
- **-i** : Silinsin mi silinmesin mi ? Şeklinde sorar.
- **-v** : Ne yaptığı hakkında kullanıcıya anlık çıktı verir.
- **-r** : Dizin silmek için kullanılır.
- Ayrıntılı bilgi için **man rm**



## # cp Komutu

```
root@kali:~/Desktop# ls -la /tmp/intelrad
ls: cannot access /tmp/intelrad: No such file or directory
root@kali:~/Desktop# cp -r /root/Desktop/intelrad /tmp/
root@kali:~/Desktop# ls -la /tmp/intelrad
total 8
drwxr-xr-x  2 root root 4096 Oct  8 10:03 .
drwxrwxrwt 12 root root 4096 Oct  8 10:03 ..
root@kali:~/Desktop#
```

- Bir yerden, başka bir yere veri kopyalama.
- Kullanımı : cp [seçenek] [kaynak] [hedef]
- -r parametresi ile dizin içerisindeki herşeyi taşır.
- -p parametresi ile taşıma esnasında dosya haklarını korur.

## # cp Komutu - 2

- **-f** : Kopyalanacak yerde dosya var ise sormadan dosyayı siler ve kopyalar.
- **-i** : Kopyalanacak yerde dosya var ise silinsin mi silinmesin mi diye sorar.
- **-v** : Ne yaptığının bilgisini anlık olarak verir.
- **-s** : Kopyalama işlemi yerine kopyalanan dosya kaynak dosyanın sembolik linki olur.
- Ayrıntılı bilgi için **man cp**.

# # mv Komutu

```
root@kali:~/Desktop# ls -la prodaft
ls: cannot access prodaft: No such file or directory
root@kali:~/Desktop# mv -f intelrad/ prodaft
root@kali:~/Desktop# ls -la prodaft/
total 8
drwxr-xr-x 2 root root 4096 Oct  8 09:40 .
drwxr-xr-x 9 root root 4096 Oct  8 10:15 ..
root@kali:~/Desktop#
```

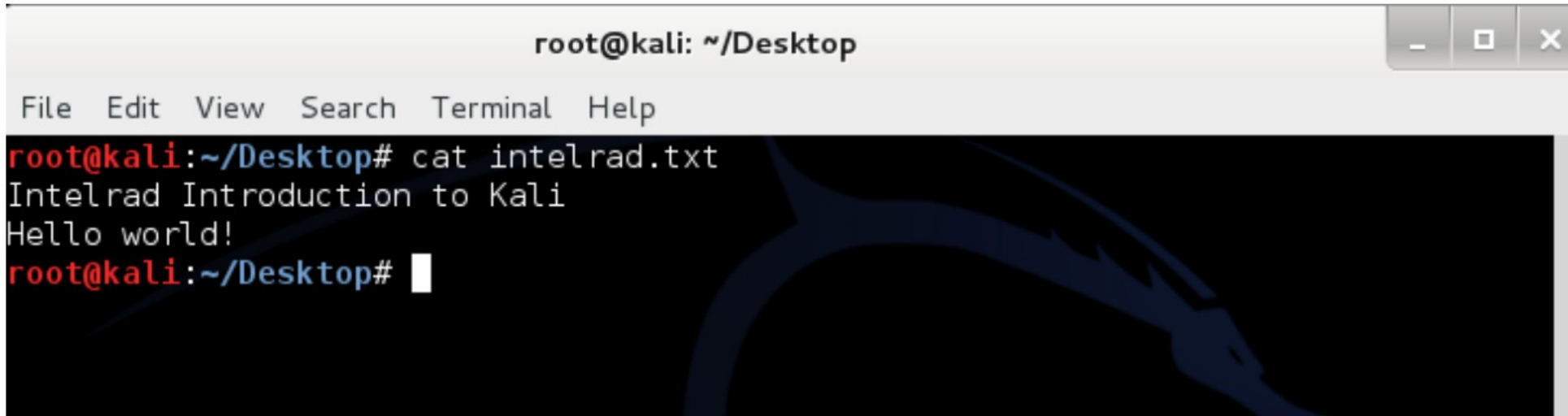
- Bir veya klasörlerin ismini değiştirmek veya taşımak için kullanılan komut.
- Kullanımı : **mv** [seçenek] [kaynak] [hedef]
- **-f** parametresi ile kaynak dosya hedef dosyaya kopyalanır ve herhangi bir şey sorulmaz.
- Ayrıntılı bilgi için **man mv**

## # chown Komutu

```
root@kali:~/Desktop# ls -la intelrad.txt
-rw-r--r-- 1 root root 0 Oct  8 10:20 intelrad.txt
root@kali:~/Desktop# chown intelrad:intelrad intelrad.txt
root@kali:~/Desktop# ls -la intelrad.txt
-rw-r--r-- 1 intelrad intelrad 0 Oct  8 10:20 intelrad.txt
root@kali:~/Desktop#
```

- Dosyanın sahibini ve grubunu değiştirmeyi sağlayan komuttur.
- Kullanımı: **chown [seçenek] [sahibi]:[grubu] file**
- Ayrıntılı bilgi için **man chown**.

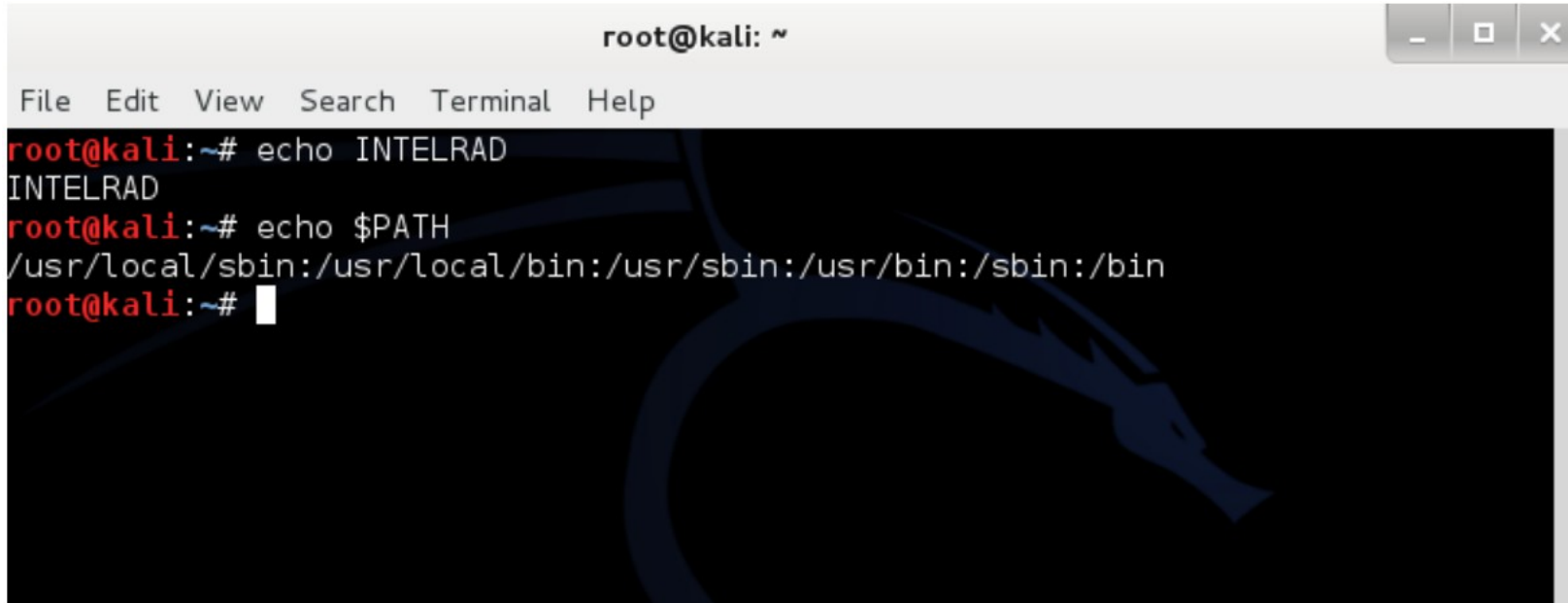
# # cat Komutu

A terminal window titled 'root@kali: ~/Desktop' with standard window controls. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows the command 'cat intelrad.txt' being executed, which outputs the contents of the file: 'Intelrad Introduction to Kali' and 'Hello world!'. The prompt returns to 'root@kali:~/Desktop#'.

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# cat intelrad.txt
Intelrad Introduction to Kali
Hello world!
root@kali:~/Desktop#
```

- **Cat** komutu dosya içeriğini okumak ve görüntülemek için kullanılır.
- İçeriğin tamamını görüntüler

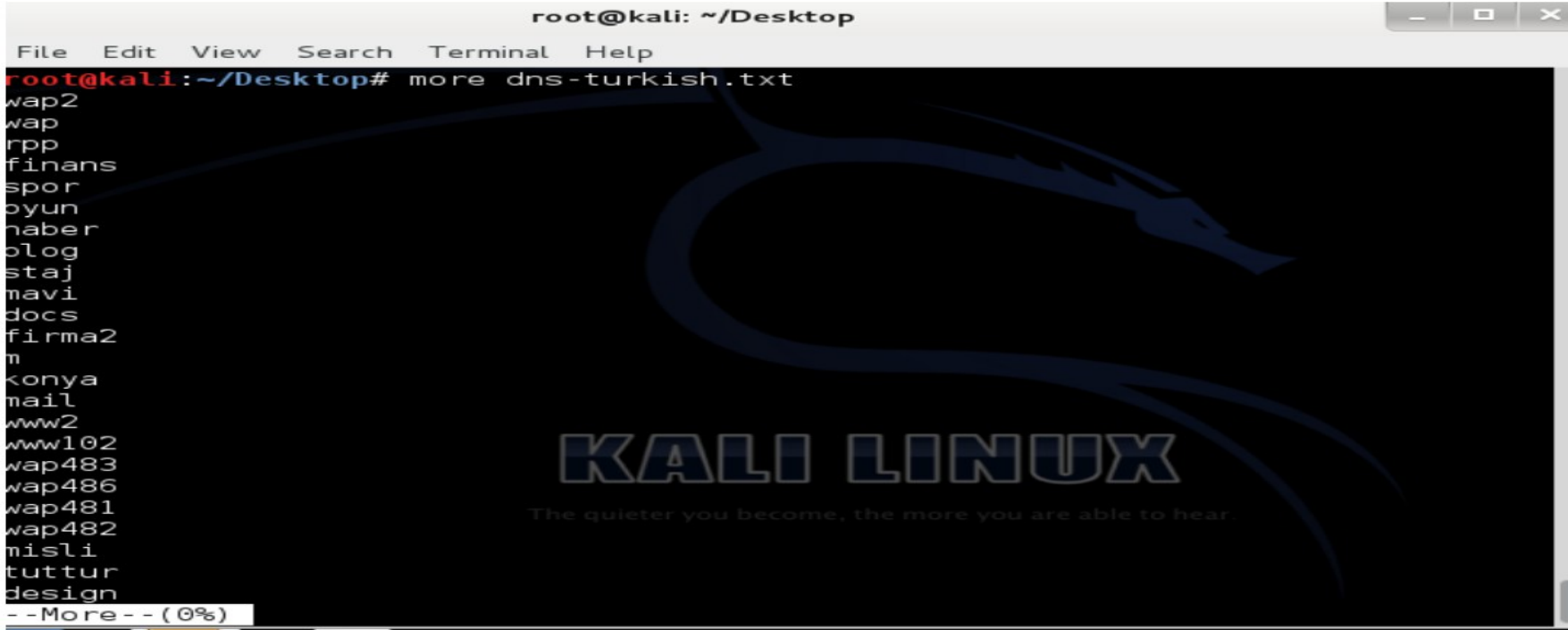
# # echo Komutu

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

- **Echo** komutu kendinden sonra yazılan ifadeyi ekrana yazdırır.
- Ayrıca ortam değişkenlerini de başına \$ koyarak echo ile yazdırabiliriz.

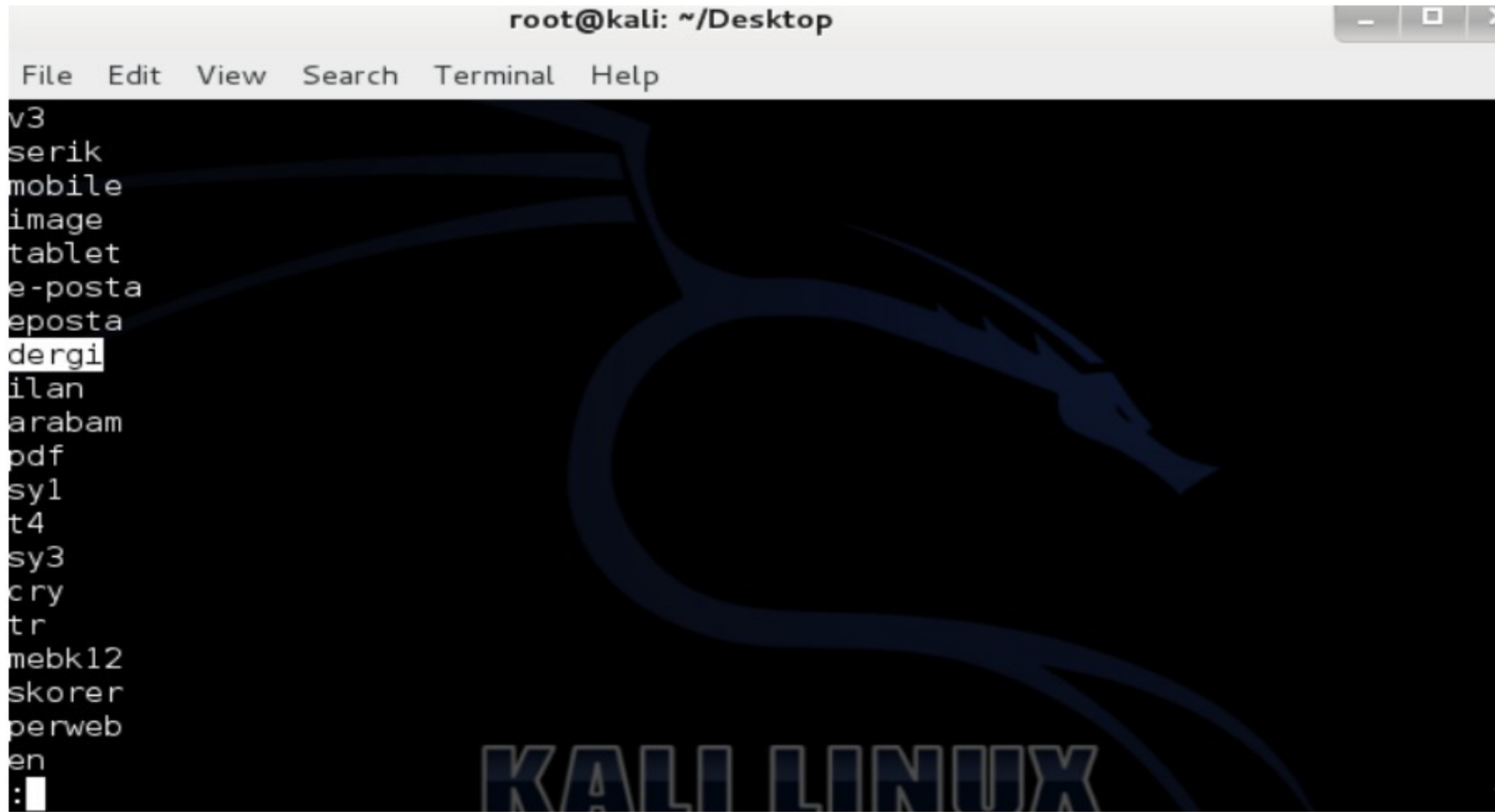
# # more Komutu



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# more dns-turkish.txt
wap2
wap
rpp
finans
spor
oyun
haber
blog
staj
mavi
docs
firma2
n
konya
mail
www2
www102
wap483
wap486
wap481
wap482
misli
tuttur
design
--More-- (0%)
```

- İçeriği fazla olan dosyaları okumak için geliştirilmiştir. Dosyanın terminale sığacak kadar olan kısmını açar. Devamını görmek için space tuşu kullanılabilir.
- q tuşu ile istenilen yerde dosya kapatılabilir.

# # less Komutu



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
v3
serik
mobile
image
tablet
e-posta
eposta
dergi
ilan
arabam
pdf
sy1
t4
sy3
cry
tr
mebk12
skorer
perweb
en
:
```



## # less Komutu

- **More** komutuna benzer bir komuttur. Farklı olarak dosya içerisinde kelime arayabilir, satır numarasına gidilebilir.
- `/dergi` = “dergi” ifadesi geçen yerleri bulur.
- `:25` = “25” numaralı satıra gider.

# Linux Komut Satırı

## Arama - Tarama



# # find Komutu

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# find /root/Desktop/ intelrad/ -perm 755  
/root/Desktop/  
/root/Desktop/birevbirmutfak  
/root/Desktop/intelrad  
/root/Desktop/intelrad/benibul  
/root/Desktop/netstress-3.0.7/netstress_randomip_staticport  
/root/Desktop/flash  
/root/Desktop/alacarte-made.desktop  
intelrad/
```

- Dizinleri veya dosyaları arama komutudur.
- Kullanımı: find [seçenek] [Dizin] [ifade]
- Yukarıdaki örnekte arama izinlere göre gerçekleştirilmiştir. -perm parametresine verilen değer ile taranan veri bulunduğunda arama durmuştur.

## # find Komutu - 2

**find** yol ismi opsiyon/parametre çalıştırılması gereken komut

- **find /belirlenenyol -name “\*l\*”** → girilen yol/dizin içinde bulunan, içinde l harfi geçen dosyaları arar.
- **find /belirlenenyol -type f -size -10K** → 10 kb’dan küçük dosyaları için arama yapar
- **find /belirlenenyol -ctime -2** → son 2 gün içinde değişiklik yapılmış dosyalar için arama yapar
- **find /belirlenenyol -user kullanıcıadı** → kullanıcıya ait dosyalar için arama yapar

## # find Komutu - 3

- **find /home -user kullanıcıadı -exec /bin/rm {} “;”** → kullanıcı sahibini siler
- **find /etc/apt -iname “source.list”** → büyük-küçük harf ayrımı yapmadan source.list için /etc/apt içerisinde arama yapar
- **find /var -name log -type d** → /var dizini içinde log kelimesi geçen dizinleri arar, d parametresi burada (directory) dizini temsil eder
- **find /home -type d -exec rmdir –ignore-tail-on-non-empty {} +; →** bütün mevcut boş dizinleri bulur ve siler

## # locate Komutu

- **locate** → hızlı bir arama türüdür. Bunun nedeni daha önceden kullanılmış dosyaların yollarını sisteme kaydeden metin belgesinden almasıdır
- **locate dosyaadı** → girilen dosyanın yolunu bulmamızı sağlar  
diyalektik@m:~\$ locate pwd  
/bin/pwd
- **locate -i dosyaadı** → arama yaparken küçük-büyük harf ayrımı yapmaz  
diyalektik@m:~\$ locate PWD  
diyalektik@m:~\$ locate -i PWd  
/bin/pwd

## # locate Komutu - 2

- **sudo updatedb** → yapılan son değişiklikleri kendi veritabanına ekler. Bu sayede locate ile arama yapmak kolaylaşır



# Linux ile Verileri Sıralama: sort komutu





# # sort Komutu

- **esc + l** → nano içerisinde bir metin yazarken; uzun kelimeleri kırarak alt satıra atmamızı sağlar
- **sort yazıadı** → yazı içerisindeki satırları alfabetik sıraya göre sıralar
- **sort -u yazıadı** → yazı içerisindeki satırları alfabetik olarak sıralarken tekrar eden satır başlarını tekrar sıralamaz

## # sort Komutu - 2

- **sort -n yazıadı** → metin içindeki sayıları sıraya göre sıralar
- **sort -ru yazıadı** → tekrar edenleri almadan, yazıyı ters çevirir
- **sort -k 3 yazıadı** → her cümlenin 3. kelimesine göre sıralama yapar
- **sort -n d1 d2 d3 → baskadosya** → karmaşık olan dosyaları başka bir dosyaya sıralar

# # head Komutu

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# head dns-turkish.txt
wap2
wap
rpp
finans
spor
oyun
haber
blog
staj
mavi
root@kali:~/Desktop# head -n 3 dns-turkish.txt
wap2
wap
rpp
root@kali:~/Desktop#
```

- **Head** komutu varsayılan olarak verilen dosyanın ilk 10 satırını getirir.
- **n** parametresi, verilen değer kadar satırı görüntüler.
- Daha fazla bilgi için: **man head**

## # tail Komutu

```
root@kali:~/Desktop# tail dns-turkish.txt
zdfageh\228lter
zdfapensionen
zensus
zensus2011
zfa
zilverfonds
zoek
_sip
_spf
_tls
root@kali:~/Desktop# tail -n 3 dns-turkish.txt
_sip
_spf
_tls
root@kali:~/Desktop#
```

- tail komutu parametresiz olarak dosya açtığımızda dosyanın son 10 satırını getirir.
- n parametresi ile kullanıldığında, dosya sonundan n parametresine verilen değer kadar satır görüntüler.

# # grep Komutu

```
root@kali:~/Desktop# grep "intelrad" intelrad.txt
intelrad
root@kali:~/Desktop# grep -i "intelrad" intelrad.txt
Intelrad Introduction to Kali
intelrad
INTELRAD
root@kali:~/Desktop#
```

- **grep** komutu, kelime arama komutudur. Verilen data içerisinde istenilen kelimeye uygun satırı getirir. Bu bölümde anlatılan en önemli komuttur.
- **-i**, Büyük küçük harf duyarsızlığı parametresidir.
- **-r**, İle düzenli ifadeler (regex) kullanılabilir.
- Daha fazla bilgi: **man grep**

# # uname Komutu

```
root@kali:~/Desktop# uname
Linux
root@kali:~/Desktop# uname -a
Linux kali 3.7-trunk-686-pae #1 SMP Debian 3.7.2-0+kali6 i686 GNU/Linux
root@kali:~/Desktop#
```

- uname komutu sistem bilgilerini listeler. Bu bilgiler makine donanım tipi, network hostadı, işletim sistemi ve işlemci tipi ile ilgili bilgilerdir.
- -a, tüm bu bilgileri birlikte getirir.
- Ayrıntılı bilgi: man uname



**sudo apt update && sudo apt upgrade**

**sudo apt install python-pip**

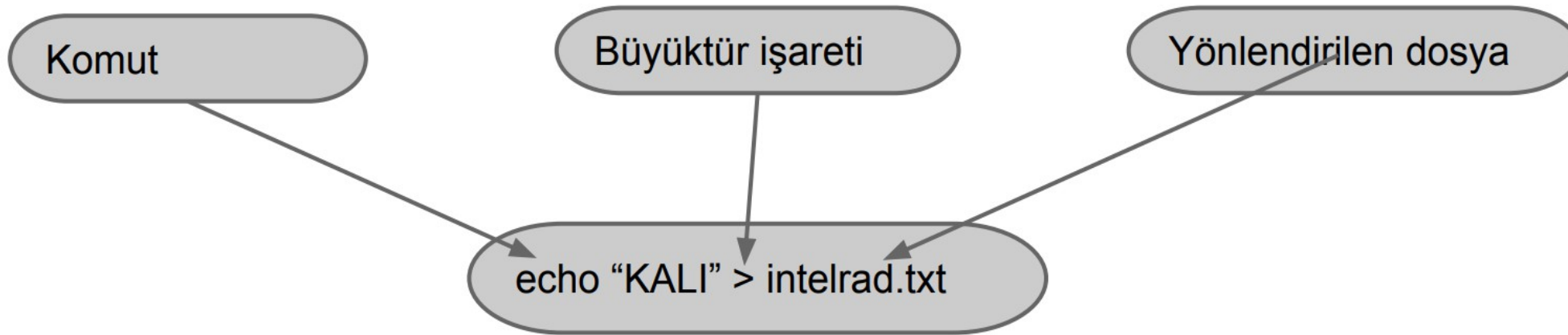
**sudo pip install cheat**

**pip install youtube-dl → youtube-dl 'ın son sürümünü yükler**

**youtube-dl youtubelinki → girilen youtube linkindeki videoyu indirir**

# Çıktı Yönlendirme

- Komutların çıktısı dosyalara yönlendirilebilir.



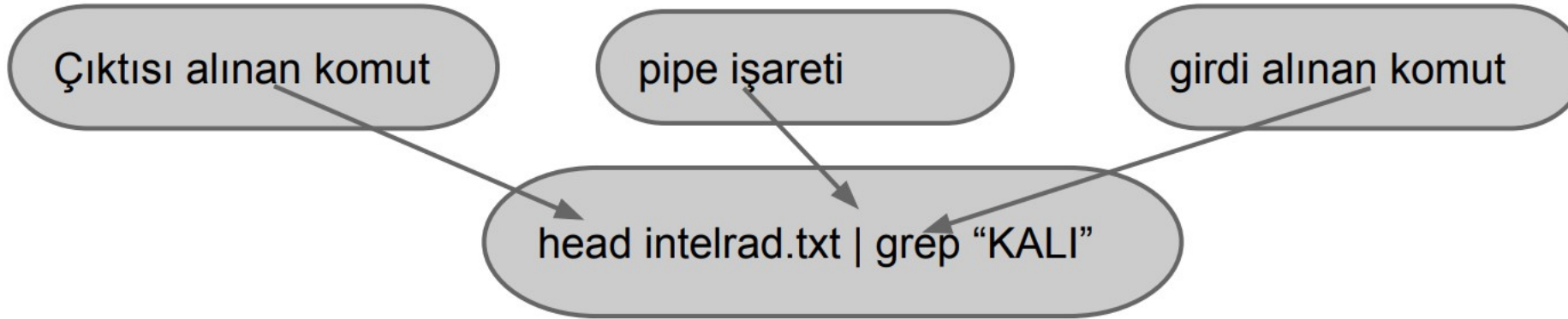
- Yukarıdaki komut intelrad.txt dosyasını oluşturup içine “KALI” sözcüğünü ekleyecektir.
- “>>” ifadesi kullanılırsa yönlendirilen ifade dosyanın sonuna eklenir.



# Çıktı Yönlendirme (pipe)

- Bir komutun çıktısı, diğer bir komuta girdi olarak verilebilir. Bu işlem linux da pipe ile gerçekleştirilir. Çoklu olarak bu işlem gerçekleştirilebilir.(piping)
- “ | “ işareti *altgr* + veya *altgr* + “-” ile yapılabilir.

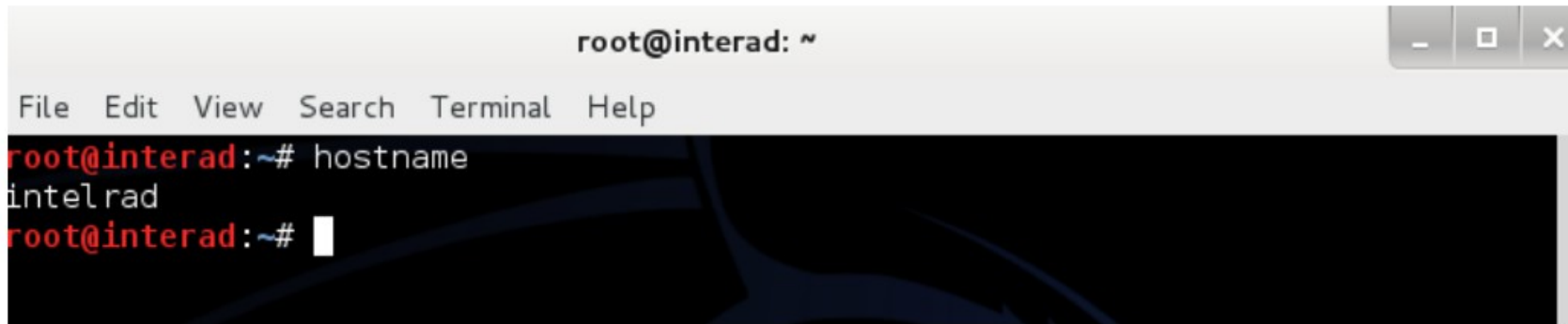
# Çıktı Yönlendirme (pipe)



- Bu komut **intelrad.txt** dosyasının ilk 10 satırını **grep** komutuna aktarır. Grep komutu **"KALI"** kelimesinin geçtiği satırları ekrana yazdırır.

# Hostname

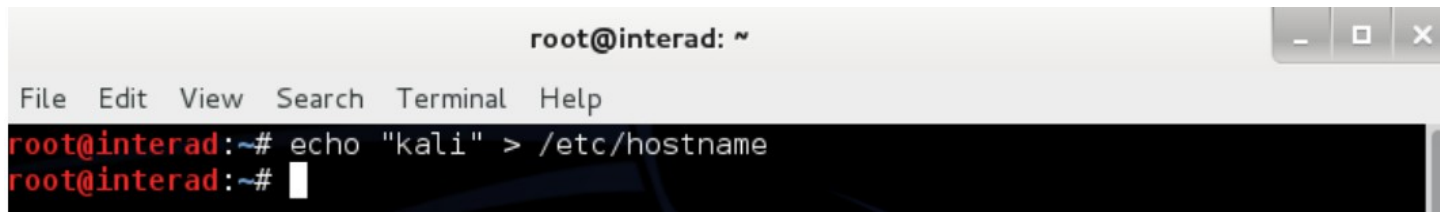
- **Hostname** komutu, bilgisayarın adını görüntüleyen ve değiştirebilen komuttur.

A terminal window titled 'root@interad: ~' with standard window controls. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal content shows the command 'hostname' being executed, resulting in the output 'intelrad'. The prompt returns to 'root@interad:~#'.

```
root@interad: ~
File Edit View Search Terminal Help
root@interad:~# hostname
intelrad
root@interad:~#
```

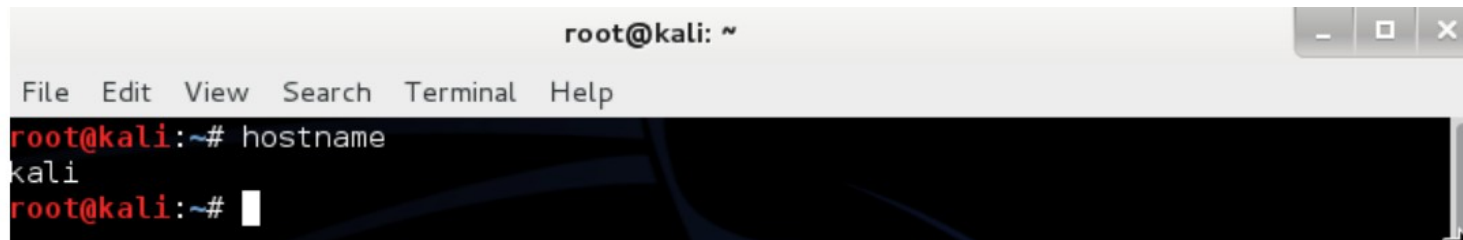
# Hostname

- Aşağıdaki komut ile **hostname** değiştirilebilir.



```
root@interad: ~  
File Edit View Search Terminal Help  
root@interad:~# echo "kali" > /etc/hostname  
root@interad:~#
```

- Terminali yeniden açtığımızda aşağıdaki gibidir.



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

# Network Ayarları

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:a4:7e:25  
          inet addr:192.168.1.102  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fea4:7e25/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:1605 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:609 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:414613 (404.8 KiB)  TX bytes:94603 (92.3 KiB)  
  
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:124 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:124 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:7440 (7.2 KiB)  TX bytes:7440 (7.2 KiB)
```

- **ifconfig** komutu mevcut ağ kartlarının bilgilerini ekrana getirir.

# Network Ayarları

- **ifconfig** komutu ile ağ arayüzlerine IP adresi atanabilir.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig eth0 192.168.1.117 netmask 255.255.255.0  
root@kali:~# ifconfig eth0  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:a4:7e:25  
          inet addr:192.168.1.117  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fea4:7e25/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:1640 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:609 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:416973 (407.2 KiB)  TX bytes:94603 (92.3 KiB)  
  
root@kali:~#
```

- **ifconfig** komutundan sonra hangi ağ kartının ismi yazılır ise yalnızca o ağ kartının özellikleri görüntülenir.

# Network Ayarları

- IP adresini elle atayabildiğimiz gibi, otomatik olarak dhcp sunucudan da talep edebiliriz.
- Bunun için önce ağ servisini durduruyoruz.

```
root@kali:~# /etc/init.d/networking stop
[....] Deconfiguring 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:a4:7e:25
Sending on   LPF/eth0/00:0c:29:a4:7e:25
Sending on   Socket/fallback
DHCPRELEASE on eth0 to 192.168.1.1 port 67
Reloading /etc/samba/smb.conf: smbd only.
done.
root@kali:~#
```

# Network Ayarları

- Daha sonra ağ kartımızı aktif hale getiriyoruz.

```
File Edit View Search Terminal Help
root@kali:~# ip link set eth0 up
root@kali:~#
```



# Network Ayarları

- Son olarak network servisini çalıştırıyoruz ve ağ kartına ip adresi alma işlemini tamamlıyoruz.

```
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:a4:7e:25
Sending on   LPF/eth0/00:0c:29:a4:7e:25
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPOFFER from 192.168.1.1
DHCPACK from 192.168.1.1
Reloading /etc/samba/smb.conf: smbd only.
bound to 192.168.1.102 -- renewal in 107581 seconds.
done.
root@kali:~#
```

```
root@kali:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:a4:7e:25
          inet addr:192.168.1.102  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea4:7e25/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3653 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1452 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1043719 (1019.2 KiB)  TX bytes:214727 (209.6 KiB)

root@kali:~#
```

# Servisler

- Servislerin amacı güvenlik testlerinde yardımcı öğeler olarak kullanılabilmesidir.

**Örneğin;** Bir sisteme sızma denemesi gerçekleştirildi ve başarılı, sızılan sistemden tftp ile veri alınması gerekiyor. Bu durumda Kali üzerinde tftp servisi çalıştırılarak gerekli bilgiler sunucudan kolaylıkla transfer edilebilir.

# Web Servisinin Başlatılması

- Apache httpd servisini başlatmak için;

# service apache2 start

# /etc/init.d/apache2 restart

```
root@kali:~# /etc/init.d/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:~# service apache2 restart
[....] Restarting web server: apache2apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
... waiting apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
. ok
root@kali:~#
```

- Her iki komutta servisi başlatma, durdurma ve restart etmek için kullanılabilir.

# SSH Servisinin Başlatılması

- Ssh servisini başlatmak için;

# service ssh start

# /etc/init.d/ssh restart

komutlarından birini vermek yeterlidir.

```
root@kali:~# service ssh start
[ ok ] Starting OpenBSD Secure Shell server: sshd.
root@kali:~# /etc/init.d/ssh restart
[ ok ] Restarting OpenBSD Secure Shell server: sshd.
root@kali:~#
```

# FTP Servisinin Başlatılması

- **FTP servisi** olarak vsftpd kullanılmaktadır. Bu servis aşağıdaki gibi başlatılır.

```
# service vsftpd start
```

```
# /etc/init.d/vsftpd start
```

```
root@kali:~# service vsftpd start
Starting FTP server: vsftpd.
root@kali:~# netstat -nat | grep 21
tcp        0      0 0.0.0.0:21 0.0.0.0:*    LISTEN
```

# Linux Kullanıcı Yönetimi



```
~$sudo useradd  
~$sudo usermod  
~$sudo groupadd
```

# Linux'ta Kullanıcı Yönetimi

- Linux çoklu kullanıcı özelliği nedir?
- Linux işletim sistemlerinde ayarlanabilirlik ve birden çok kullanıcının aynı anda login olabilmesi mümkündür.
- Windows' taki çoklu kullanıcı hesabı ile benzer değildir.
- Birden çok kullanıcının sisteme login olabilmesi ile çok kullanıcılı bir platform sağlanmış olur..

# Linux'ta Kullanıcı Yönetimi

- Linux işletim sisteminde kullanıcı bilgileri `/etc/passwd` dosyasında tutulur.
- Gruplar hakkındaki bilgiler `/etc/group` dosyası içerisinde bulunur.
- Kullanıcı şifrelerinin hashleri `/etc/shadow` dosyasın içerisinde bulunur.
- `/etc/passwd`' i tüm kullanıcılar görebilir.
- `/etc/shadow` dosyasını sadece root görebilir.



# /etc/passwd

- /etc/passwd dosyası kullanıcı bilgilerini saklar.
- Bir ASCII dosyası, her bir kullanıcı için bir girdi kullanarak saklanır.  
Taslak olarak şöyledir:
  - isim:şifre:kid:gid:yorum:evdizini:kabuk
  - isim : Login ismi
  - şifre : Encrypt hali ile şifre
  - kid : Kullanıcı ID
  - gid : İlk grup ID'si.
  - yorum : Yorum, genellikle gerçek isim yazılır.
  - evdizini : Kullanıcının /home dizinini gösterir.
  - kabuk : Öntanımlı olan shell'i.

# /etc/passwd

- Bu dosyanın görünümü aşağıdaki gibidir.

```
root@kali:/etc# ls -lah passwd
-rw-r--r-- 1 root root 2.1K Aug 26 04:05 passwd
root@kali:/etc# cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
```

- isim:şifre:kid:gid:yorum:evdizini:kabuk

## /etc/group

- /etc/group'un içindeki dosyada grupların özellikleri tutulur.

Taslak aşağıdaki gibidir:

- grup\_ismi:grup\_şifresi:grup\_id:üye

```
root@kali:/etc# ls -lah group
-rw-r--r-- 1 root root 968 Sep 25 08:00 group
root@kali:/etc# cat 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:
```

## **/etc/shadow**

- Bu dosya şifreleri ve şifrelerle ilgili zaman bazlı bilgileri de tutan, ASCII formatında dosyalanmış bilgileri içerir.
- Yalnızca root tarafından görüntülenebilir.

# /etc/shadow

## Yapısı:

- isim:şifre:sondeğişim:min:max:warn::inactive  
:expire:flag
- isim : Kullanıcı adı
- şifre : Encrypt edilmiş şifre, \* yada ! varsa hesap bloklanmıştır.
- sondeğişim : Şifrenin değiştiği günden itibaren kaç gün geçmiş
- min : Şifrenin değişmiş olabileceği günden önce kaç gün geçmiş
- max : Şifrenin kesin olarak değişmiş olduğu günden sonra kaç gün geçmiş.

# /etc/shadow

- **Yapı (devam):** - warn : Şifrenin geçerliliğinin dolmadan kaç gün önce uyarı Verileceğini bildirir.
- inactive : Hesap bloklanmış duruma geçtikten sonra kaç gün geçmiş.
- expire : Hesabın bloklanmış olduğu gün sayısı.
- flag : Reserve edilmiş alan. (kullanılmıyor).

```
File Edit View Search Terminal Help
root@kali:/etc# ls -lah shadow
-rw-r----- 1 root shadow 1.3K Aug 26 04:05 shadow
root@kali:/etc# cat shadow
root:$6$kw8oFhBT$6M9j3MssnjDp9Iu2ZJfJJYamopsCB80V2hKzNfQSUUTqvGSn4rwgnbeU2MAsPww3a0rfH
b8gig3z30RCLEYNgi0:15939:0:99999:7:::
daemon*:15820:0:99999:7:::
bin*:15820:0:99999:7:::
sys*:15820:0:99999:7:::
sync*:15820:0:99999:7:::
games*:15820:0:99999:7:::
```

- isim:şifre:sond:min:max:warn:inact:exp:flag

# Sisteme Kullanıcı Ekleme

- **Useradd** komutu, yeni bir kullanıcı oluşturma ya da var olan bir kullanıcı bilgilerini güncelleme amacıyla kullanılabilir.
- **useradd [kullanıcı\_adi]**
- **-g** parametresi ile eklenecek kullanıcının grubuda belirlenebilir.
- **useradd -g [grup\_ismi] [kullanıcı\_ismi]**

# Sisteme Kullanıcı Ekleme

- **adduser username sudo** → kullanıcıyı sudoers grubuna ekler (root yetkisi verir)
- **sudo su newuser** → kullanıcı geçişi sağlar
- **id** → sistemdeki kullanıcıları gösterir
- **cat /etc/group** → sisteme ait grupları gösterir (yazıcı grupları, tarayıcı grupları, kullanıcı grupları vb.)
- **groups kullanıcıadı** → kullanıcı adının mevcut olduğu grupları gösterir



# Sisteme Kullanıcı Ekleme

- Kullanıcılara parola vermek için **passwd** komutu kullanılır.
- **passwd [username]**
- Normal kullanıcılar eski şifreyi bilmeden bunu yapamazlar. **Root** kullanıcı yapabilir.

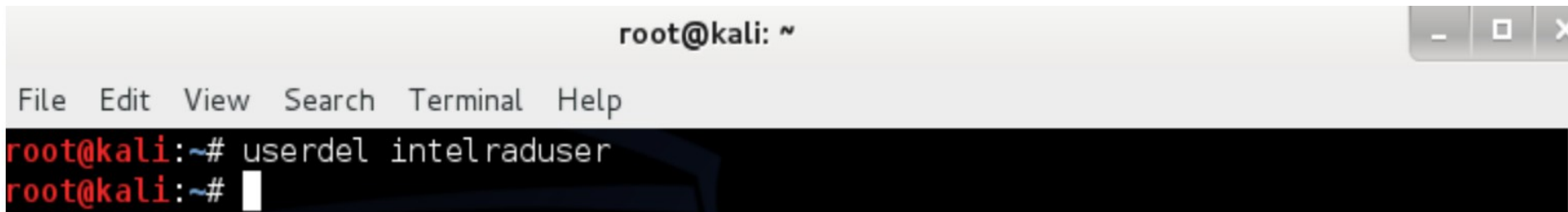
```
root@kali:~# useradd intelraduser
root@kali:~# passwd intelraduser
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kali:~#
```

# Sisteme Kullanıcı Ekleme

- **chage -l ‘kullanıcıadı’** komutu kullanıcının şifre bilgilerini gösterir
- Kullanıcıyı belli bir zamanda sonlandırmak için ***chage -E ‘yıl/ay/gün’ ‘kullanıcıadı’*** komutunu kullanmamız gerekir.

# Sistemden Kullanıcı Silme

- **Userdel** ve **deluser** komutları kullanılabilir.
- **userdel [kullanıcı\_adı]**
- **-r** parametresi ile kullanıcıya ait dizinler de silinebilir.

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 shows the command 'userdel intelraduser' being entered and executed. The prompt changes from 'root@kali:~#' to 'root@kali:~#' with a cursor at the end.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# userdel intelraduser  
root@kali:~#
```

# Linux Parola Güvenliği

- Linux işletim sisteminde hesapların parolaları /etc/shadow dosyasında hash+salt olarak saklanır.
- Salt her seferinde değişken olarak atanan bir değerdir. Yani parolanın hash değeri sürekli değişir.
- Parola formatı:

```
root:$6$kw8oFhBT$6M9j3MssnjDp9Iu2ZJfJYamopsCB80V2hKzNfQSUUTqvGSn4rwgnbeU2MAsPww3a0rfHb8gig3z30RCLEYnGI0:15939:0
```

# Linux Parola Güvenliği

- Parola Formatı:
  - root : kullanıcı adı
  - İlk \$ ile ikinci \$ arasındaki sayı hangi şifreleme algoritmasının kullanıldığını belirtir.

# Linux Parola Güvenliği

**Bu değer;**

- \* 1 ise MD5
- \* 2a ise Blowfish (OpenBSD)
- \* 5 ise SHA256
- \* 6 ise SHA512 'dir.
- İkinci \$ ile üçüncü \$ arasındaki karakterler salt değeridir.
- Hash değerlerini kullanarak (rainbow table) gerçekleştirilecek olan ataklara karşı alınmış bir önlemdir.

**Haftanın Videosu:)**

