



TEMEL LINUX KOMUTLARINA GİRİŞ (5)



1. Temel Ağ Komutları
2. Kullanıcı ve Grup İşlemleri
3. Cron İşlemleri



1. TEMEL AĞ KOMUTLARI

- ❖ TCP/IP ağlarının oluşturulması sırasında yapılması gereken ilk görev ağ üzerinde bulunan tüm noktalara ağ adreslerinin atanmasıdır.
- ❖ IPV4 (32 bit) ve IPV6 (128 bit) olmak üzere iki çeşit IP adresi vardır.
- ❖ IPV4 sınıfına göre IP adresleri ve alt ağ maskeleri

Sınıf	İlk 8'li	Öntanımlı Maske
A	1-126	255.0.0.0
B	128-191	255.255.255.0
C	192-223	255.255.255.0
D	224-239	255.255.255.255
E	240-254	-

- ❖ Alt ağ maskeleri, kullanılarak ağdaki iki bilgisayarın veya cihazın aynı ağda olup olmadıklarını anlamamızı sağlar.

❖ Özel IP'ler

- ❖ Özel ağlarda adreslemeyi basitleştirmek, iç ağda daha fazla bilgisayara IP adresi atamak **NAT** (Network Address Translation) internet ağlarıyla çakışmayı önlemek için **bazı IP'ler rezerve edilmiştir.**
- ❖ Özel IP'ler **internet ağ geçitleri tarafından yönlendirilmez**, yalnızca **iç ağlarda kullanılırlar.**
- ❖ RFC 1918'de tanımlanan özel ağlar:
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16

❖ Protokoller

- ❖ **Protokol** iki ağ bilgisayarının **birbiriyle konuşma dilidir.**
- ❖ **TCP/IP katmanlı bir mimari olup her protokol, gerçek pakete bir takım bilgiler ekleyerek sarmalar ve bir sonraki katmanın protokolüne iletir.**
- ❖ Bu şekilde sarılıp en son fiziksel katmandan (bu genelde bir ethernet veya fiber kart oluyor) karşı tarafa iletilir.
- ❖ Karşı tarafta en dıştan başlanarak paket açılır.
- ❖ **Bir katmanda yönlendirme bilgisi varken, diğer katmanda **hangi hizmetin (portun) hedeflendiği** bilgisi bulunur.**
- ❖ Tüm bunların yanında **mesajların doğru gelip gelmediğini kontrol eden hata kontrol mekanizmaları** ve bu mekanizmalara ait ilave alanlar vardır.

❖ TCP Protokolü

❖ TCP protokolü, bağlantı bazlı **güvenli veri akışını sağlayarak** iletim katmanına (transmission layer) **çok önemli hizmetler sunar.**

❖ TCP protokolünün en önemli özellikleri şunlardır;

- Bağlantı noktaları arasında **veri iletişimini sağlaması**
- **Güvenli veri iletimine** olanak tanınması
- Bağlantıda olan iki bilgisayar arasında **akış kontrolü sağlaması**
- **Çoklama** (Multiplexing) yöntemi ile **birden fazla bağlantıya izin vermesi**
- Sadece bağlantı kurulduktan sonra **veri iletimi sağlaması**
- Gönderilen mesaj parçaları için **öncelik ve güvenlik tanımlaması yapılabilmesi**

❖ TCP protokollerine örnek olarak **FTP, SMTP, HTTP, IMAP** verilebilir.

❖ UDP Protokolü

- ❖ **UDP güvenli olmayan, bağlantısız veri akışı sağlar.**
- ❖ Bağlantının açılması, kapatılması gibi operasyonlara gerek yoktur.
- ❖ UDP toplu yayın (**broadcast**) – grup yayın (**multicast**) mesajları için **son derece kullanışlıdır.**
- ❖ UDP protokolü, **TCP protokolünden daha hızlı ve daha kolaydır.**
- ❖ **DNS ve SNMP** uygulama protokolleri **UDP üzerinde taşınırlar.**

❖ ICMP Protokolü

- ❖ Internet Protokolü, **ICMP Protokolünü kullanarak** işlem gören datagramların iletimi sırasında meydana gelen hataları, uyarı ve kontrol bilgilerini iletir.
- ❖ Bu mesajlar, ağ yöneticileri tarafından değerlendirilerek **ağ içerisinde meydana gelen aksaklıkların** belirlenmesinde kullanılabilir.
- ❖ ICMP mesajları genel olarak şu durumlarda üretilir.
 - IP datagramların **hedeflerine ulaşamaması durumunda**
 - Ağ geçitlerinin datagramları **hedeflerine yönlendiremeyecek kadar yoğun olması durumunda**
 - Datagramların hedeflerine yönlendirilebileceği **daha kısa bir rota olması durumunda**

❖ Port Numaraları

- ❖ Aynı hedefte birden fazla servis çalıştırmak için **port numarası** kullanılır.
- ❖ IP adresi, bir bilgisayar adreslerken, port numarası o **bilgisayardaki çalışan servisi adresler.**
- ❖ IP adresi bir binanın *kapı numarası* ise, *port numarası kaçınıcı* kat olduğunu veya daireyi gösterir.
- ❖ Örneğin aynı bilgisayarda **hem mail gönderim (SMTP)** hem de **web sunma (HTTP) hizmetleri** aynı anda bulunabilir.
- ❖ Mail gönderim için örneğin **Thunderbird uygulamasını**, sunulan web sayfasını görüntülemek için örneğin **Chrome uygulaması** kullanılır.
- ❖ Her iki uygulamada aynı sunucuya bağlanacak. Ancak *Thunderbird, 25 numaralı porttaki SMTP sunucuya, Chrome 80 numaralı porttaki web sunucuya bağlanır.*

❖ Linux altında standart hizmetlerin listesi /etc/services dosyasında bulunur. Örneğin **cat /etc/services**

```
ftp-data      20/tcp
ftp           21/tcp
fsp           21/udp
ssh           22/tcp
ssh           22/udp
telnet        23/tcp
smtp          25/tcp
time          37/tcp
time          37/udp
```

❖ Bazı port ve hizmetler ağ yöneticileri tarafından sıklıkla kullanılır:

Protokol Port	Hizmet
TCP 20	FTP Veri
TCP 21	FTP Kontrol
TCP 22	SSH
TCP 23	Telnet
TCP 25, 465	SMTP, SSMTP
UDP 53	DNS
TCP 80, 443	HTTP, HTTPS
TCP 110, 945	POP3, POP3S
UDP 139	NetBIOS
TCP 143, 993	IMAP, IMAPS
UDP 161	SNMP

❖ Ağ Arayüzleri

- ❖ Linux altında ağ arayüzleri, /dev altında **sanal bir aygıt olarak yönetilir.**
- ❖ Fiziksel erişim türüne göre arayüzler farklı isimlerle çağrılır:

lo: loopback

eth: Ethernet kartları

slip: Seri port modemler

ppp: Noktadan noktaya

isdn: ISDN hat

fddi: Fiber hat

❖ ifconfig komutu

❖ Ağ kartlarına IP vermek ve devreye almak için kullanılır.

Hiçbir parametre vermeden kullanılırsa mevcut yapılandırmayı gösterir.

```
root@bilmuh:~# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe3a:5365 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:3a:53:65 txqueuelen 1000 (Ethernet)
    RX packets 56233 bytes 81804801 (78.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7456 bytes 487795 (476.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 36 bytes 3350 (3.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 36 bytes 3350 (3.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

❖ Eğer ifconfig, komutu verildiğinde aşağıdaki gibi bir hata ile karşılaşırsa:

```
root@bilmuh:~# ifconfig
-bash: ifconfig: komut yok
```

- **Debian işletim sisteminde aşağıda verildiği gibi temel ağ araçları yüklenmelidir.**

```
root@bilmuh:~# apt-get install net-tools
Paket listeleri okunuyor... Bitti
Bağımlılık ağacı oluşturuluyor... Bitti
Durum bilgisi okunuyor... Bitti
Aşağıdaki YENİ paketler kurulacak:
  net-tools
0 paket yükseltilecek, 1 yeni paket kurulacak, 0 paket kaldırılacak ve 30 paket yükselt
ilmeyecek.
243 kB arşiv dosyası indirilecek.
```


❖ Ağ arayüzünü **aktif etmek** ve **IP/netmask** ikilisini tanımlamak için şu şekilde kullanılır:

```
# ifconfig eth0 172.16.45.219 netmask 255.255.248.0 up
```

❖ Bir sunucuda birden çok ağ kartı olduğunu unutmayın.

❖ Bu durumda **eth0**, **eth1** şeklinde **ağ kartları olacaktır.**

❖ Ayrıca sunucuya sanal IP adresi yerine gerçek IP adresi atanmalıdır.

❖ Aktif edilmiş bir ağ arayüzünü **kapatmak** için

```
# ifconfig eth0 down
```

❖ Bilgisayarın IP adresi olması ağ üzerinde paket alışverişi yapmasını temin eder. **Ancak başka ağlara ulaşamaz.**

❖ Eğer kablosuz ağdan bağlanılıyorsa ve bu ağla ilgili bilgileri görmek için **iwconfig** komutu kullanılabilir.

```
ssstt@JavaTpoint:~$ iwconfig
lo          no wireless extensions.

wlan0      IEEE 802.11bgn  ESSID:"NETGEAR64"
Mode:Managed  Frequency:2.452 GHz  Access Point: C0:FF:D4:91:49:DF
Bit Rate=57.8 Mb/s   Tx-Power=20 dBm
Retry  long limit:7   RTS thr:off   Fragment thr:off
Power Management:on
Link Quality=47/70   Signal level=-63 dBm
Rx invalid nwid:0   Rx invalid crypt:0   Rx invalid frag:0
Tx excessive retries:0 Invalid misc:8   Missed beacon:0
```

❖ Kablosuz ağ ile ilgili yapılandırmalar için **ifconfig wlan0** komutu kullanılır.

❖ Kablolu ve kablosuz bağlantı için kullanılan **ethernet** ve **wireless** sürücülerile ilgili bilgi almak için

ethtool -i eth0 ve **ethtool -i wlan0**

komutu kullanılabilir.

❖ Eğer istatistiki bilgiler edinilmek istenirse bu sefer **-S** parametresi kullanılır.

Örneğin **ethtool -S wlan0**

```
root@bilmuh:~# apt-get install ethtool
Paket listeleri okunuyor... Bitti
Bağımlılık ağacı oluşturuluyor... Bitti
Durum bilgisi okunuyor... Bitti
```

❖ Eğer **ethtool** komutu çalıştırılmasında hata olursa yukarıdaki gibi **paket** kurulumu yapılmalıdır!

- ❖ Ağ yapılandırması yapılmış bir sistemde ağ arayüzlerini başlatmak için **ifup** komutu kullanılır.
- ❖ Bu komut **/etc/network/interfaces** gibi yapılandırma dosyalarını okuyarak arayüzleri yapılandırır.
 - **ifup**
 - **ifdown**
- ❖ Ağ hizmetlerini başlatmak için:
/etc/init.d/networking start
- ❖ Ağ hizmetlerini yeniden başlatmak için:
/etc/init.d/networking restart

❖ ip komutu

- ❖ Linux ağ komutlarından olan ip komutu; **ip numarasını öğrenme, routing tablosu görüntüleme, arp ön belleği listeleme** gibi işlemler için kullanılır.
- ❖ **Linux 2.2 çekirdek sürümüyle birlikte gelişmiş fonksiyonlar sunan iproute2 paketi getirildi.**

```
root@bilmuh:~# ip
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { address | addrlabel | amt | fou | help | ila | ioam | l2tp |
                  link | macsec | maddress | monitor | mptcp | mroute | mrule |
                  neighbor | neighbour | netconf | netns | nexthop | ntable |
                  ntbl | route | rule | sr | tap | tcpmetrics |
                  token | tunnel | tuntap | vrf | xfrm }
      OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                  -h[uman-readable] | -iec | -j[son] | -p[retty] |
                  -f[amily] { inet | inet6 | mpls | bridge | link } |
                  -4 | -6 | -M | -B | -0 |
                  -l[oops] { maximum-addr-flush-attempts } | -br[ief] |
                  -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename] |
                  -rc[vbuf] [size] | -n[etns] name | -N[umeric] | -a[ll] |
                  -c[olor]}
```

❖ip ile ağ arayüzüne IP adresi tanımlamak için:

```
# ip addr add 192.168.50.5 dev eth1
```

❖Arayüzler hakkında bilgi almak için:

```
# ip addr show
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
```

```
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
```

```
    inet 127.0.0.1/8 scope host lo
```

```
    inet6 ::1/128 scope host
```

```
        valid_lft forever preferred_lft forever
```

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
```

```
    link/ether 00:50:56:b2:6d:8a brd ff:ff:ff:ff:ff:ff
```

```
    inet 172.16.45.219/21 brd 172.16.47.255 scope global eth0
```

```
    inet6 fe80::250:56ff:feb2:6d8a/64 scope link
```

```
        valid_lft forever preferred_lft forever
```

❖Arayüze ait IP adresini silmek için:

```
# ip addr del 192.168.50.5/24 dev eth1
```


❖ Ağ arayüzünü aktif etmek için:

```
# ip link set eth1 up
```

❖ Ağ arayüzünü kapatmak için:

```
# ip link set eth1 down
```

❖ Yönlendirme tablosunu görüntülemek için:

```
# ip route show
```

```
10.0.0.0/24 dev eth0 proto kernel scope link src 10.0.0.100  
169.254.0.0/16 dev eth0 scope link  
default via 10.0.0.1 dev eth0
```

❖ Sabit yönlendirme eklemek için:

```
# ip route add 10.0.2.0/24 via 192.168.5.10 dev eth0
```

❖ Varsayılan ağ geçidini tanımlamak için:

```
# ip route add default via 192.168.50.100
```

❖ Routing tablosunu görmek için

```
root@bilmuh:~# ip route
default via 10.0.2.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
```

❖ Arp ön belleğini görmek için

```
root@bilmuh:~# ip neigh
10.0.2.2 dev enp0s3 lladdr 52:54:00:12:35:02 STALE
```

❖ ip ile ağ arayüzüne IP adresi tanımlamak için

```
# ip addr add 192.168.50.5 dev eth1
```

❖ Aşağıdaki tabloda **net-tools** paketinde **yer alan komutlara karşılık gelen ip komutları verilmiştir:**

net-tools	iproute2
<code>ifconfig</code>	<code>ip addr</code>
<code>route</code>	<code>ip route</code>
<code>arp</code>	<code>ip neigh</code>
<code>ipmaddr</code>	<code>ip maddr</code>
<code>iptunnel</code>	<code>ip tunnel</code>
<code>nameif</code>	<code>ifrename</code>
<code>mii-tool</code>	<code>ethtool</code>

❖ IPv4 protokolünün tasarımından kaynaklanan sorunların aşılması ve verimliliğin sağlanması **IPv6 protokolünün tasarımında görülmüştür.**

❖ IPv6 yapılandırması **/etc/network/interfaces** dosyasında yapılır:

```
#IPV6 static configuration
iface eth0 inet6 static
pre-up modprobe ipv6
address 2607:f0d0:2001:000a:0000:0000:0000:0002
netmask 64
gateway 2607:f0d0:2001:000a:0000:0000:0000:0001
# END IPV6 configuration
```

❖ Ipv6 yönlendirmeyi kontrol etmek için:

```
# ip -6 route show
```

❖ Ipv6 ping atmak için:

```
# ping6 ipv6.google.com
```

❖ route komutu

❖ Sistemde yönlendiricisi tablosunu görmek için kullanılır.

```
root@bilmuh:~# route
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	_gateway	0.0.0.0	UG	100	0	0	enp0s3
10.0.2.0	0.0.0.0	255.255.255.0	U	100	0	0	enp0s3
link-local	0.0.0.0	255.255.0.0	U	1000	0	0	enp0s3

```
root@bilmuh:~# route -n
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	10.0.2.2	0.0.0.0	UG	100	0	0	enp0s3
10.0.2.0	0.0.0.0	255.255.255.0	U	100	0	0	enp0s3
169.254.0.0	0.0.0.0	255.255.0.0	U	1000	0	0	enp0s3

❖ Gateway, yerel ağdan internete çıkmak için kullanılan yönlendirme adresidir.

❖ Gateway (Ağ geçidi) adresini değiştirmek için

```
# route add default gw 10.0.0.1
```

❖ Bir hosta erişimi yönlendirme yapılabilir.

❖ Örneğin **10.0.2.5** IP'li hosta erişimleri **eth1** üzerinden yapmak üzere bir yönlendirme yapmak için

```
# route add -host 10.0.2.5 eth1
```

❖ ping komutu

❖ **Basit bir ICMP haberleşmesidir.**

❖ **Ping komutunun amacı hedef bilgisayarın ayakta olup olmadığını, paket kaybı oranını ve cevap süresini tespit etmektir.**

```
$ ping www.example.com
```

```
PING www.example.com (93.184.216.119) 56(84) bytes of data.  
64 bytes from 93.184.216.119: icmp_req=1 ttl=47 time=156 ms  
64 bytes from 93.184.216.119: icmp_req=2 ttl=47 time=155 ms  
64 bytes from 93.184.216.119: icmp_req=3 ttl=47 time=156 ms
```

```
--- www.example.com ping statistics ---
```

```
3 packets transmitted, 3 received, 0% packet loss, time  
10498ms
```

```
rtt min/avg/max/mdev = 155.899/156.049/156.244/0.478 ms
```

❖ **5 sn aralıklarla ping atmak için:**

```
$ ping -i 5 www.google.com
```

❖ ping komutu

❖Belli sayıda ICMP isteği göndererek sonlandırmak için (örnekte 2 istek gönderilmekte):

```
$ ping -c 2 173.194.39.169
```

```
PING 173.194.39.169 (173.194.39.169) 56(84) bytes of data.
```

```
64 bytes from 173.194.39.169: icmp_req=1 ttl=44 time=84.0 ms
```

```
64 bytes from 173.194.39.169: icmp_req=2 ttl=44 time=84.9 ms
```

```
--- 173.194.39.169 ping statistics ---
```

```
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
```

```
rtt min/avg/max/mdev = 84.026/84.464/84.903/0.526 ms
```

❖Sadece ping istatistiklerini görmek için:

```
$ ping -c 5 -q 127.0.0.1
```

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
```

```
--- 127.0.0.1 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
```

```
rtt min/avg/max/mdev = 0.021/0.029/0.033/0.005 ms
```

❖ traceroute komutu

- ❖ Hedef bilgisayara giderken paketlerin yönlendirme neticesinde hangi geçitlerden geçerek ilerlediğini görmek için kullanılır.
- ❖ Bu sayede hedef bilgisayara ulaşmada bir sıkıntı varsa sıkıntının aradaki hangi noktada olduğu tespit edilebilir.

```
root@bilmuh:~# traceroute www.btu.edu.tr
traceroute to www.btu.edu.tr (79.123.219.23), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.476 ms  0.456 ms  0.447 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
```

- ❖ n parametresi verilerek çıktının gelme süresi hızlandırılabilir.
- ❖ Bu durumda DNS çözümlemesi atlanacaktır.

❖ netstat komutu

❖ Ağ bağlantılarını, **yönlendirme tablolarını** ve **ağ arayüzlerinin istatistiklerini** görüntüler. Parametreler:

❖ **-rn**: Yönlendirme tablosunu gösterir.

```
# netstat -rn
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	MSS	Window	irtt
Iface						
10.0.0.0	0.0.0.0	255.255.255.0	U	0	0	
0 eth0						
169.254.0.0	0.0.0.0	255.255.0.0	U	0	0	
0 eth0						
0.0.0.0	10.0.0.1	0.0.0.0	UG	0	0	
0 eth0						

❖ netstat komutu

❖-s: Protokol istatistiklerini gösterir.

```
# netstat -s
```

```
Ip:
```

```
2374203 total packets received
9728 with invalid addresses
0 forwarded
0 incoming packets discarded
2364474 incoming packets delivered
2196461 requests sent out
```

```
Icmp:
```

```
5375 ICMP messages received
1487 input ICMP message failed.
ICMP input histogram:
  destination unreachable: 2706
  timeout in transit: 324
  redirects: 48
  [...]
```

❖ netstat komutu

❖ **-ta**: Bütün TCP bağlantılar ve dinlenen portları gösterir.

```
# netstat -ta
```

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

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	*:imap	*	LISTEN
tcp	0	0	*:pop3s	*:*	LISTEN
tcp	0	0	*:mysql	*:*	LISTEN

❖ **-ta**: Bütün TCP bağlantılar ve dinlenen portları gösterir.

❖ **-ua**: Bütün **UDP** *bağlantıları ve dinlenen portları* gösterir.

❖ **-ape**: *TCP, UDP ve UNIX soket bağlantıları ile bu bağlantıların durumlarını* gösterir.

❖ netcat komutu

- ❖ **netcat**, istemci/sunucu mimarisiyle çalışan ağ trafiğini analiz etmeye yarayan bir araçtır.
- ❖ Ağ sorunlarını çözmek için karşıdaki bir porta istemci olarak **bağlanarak sunucunun cevaplarını analiz edebilir** veya bir **sunucu gibi bir portu dinleyip istemcilerden** gelen istekleri analiz edebilirsiniz.
- ❖ Böylece **haberleşmeden kaynaklı sorunları** çözebilirsiniz.

❖ En temel kullanımı telnet gibi bir sunucu portuna bağlanmaktır.

```
$ nc -v google.com 80
Connection to google.com 80 port [tcp/http] succeeded!
GET /
HTTP/1.0 302 Found
Location: http://www.google.com.tr/?
gws_rd=cr&ei=u12sUu72AcXBSwbt-IGYBw
Cache-Control: private
Content-Type: text/html; charset=UTF-8
[...]
```

❖ Belli bir portta soket açıp dinlemek için:

```
$ nc -l -v 1234
Listening on [0.0.0.0] (family 0, port 1234)
```

❖ Bir port aralığındaki port erişilebilirliğini test etmek için:

```
$ nc -v -w 1 10.0.0.10 -z 20-25
```

```
nc: connect to 10.0.0.10 port 20 (tcp) failed: Connection  
refused
```

```
Connection to 10.0.0.10 21 port [tcp/ftp] succeeded!
```

```
Connection to 10.0.0.10 22 port [tcp/ssh] succeeded!
```

```
nc: connect to 10.0.0.10 port 23 (tcp) failed: Connection  
refused
```

```
nc: connect to 10.0.0.10 port 24 (tcp) failed: Connection  
refused
```

```
nc: connect to 10.0.0.10 port 25 (tcp) failed: Connection  
refused
```

-w parametresi zaman aşımı değeri belirtmek içindir.

❖ whois komutu

❖ Hedef sistemle ilgili bilgi almak için bu komut kullanılır.

❖ **Eğer bu araç Debian işletim sisteminde kurulu değilse apt-get install whois komutu ile kurulur.**

```
root@bilmuh:~# whois derinteknoloji.com.tr
** Domain Name: derinteknoloji.com.tr
Frozen Status: -
Transfer Status: The domain is LOCKED to transfer.

** Registrant:
    seckin yilmaz
    Hidden upon user request
    Hidden upon user request
    Hidden upon user request
    Hidden upon user request

** Registrar:
NIC Handle           : tyh14
Organization Name    : Turkticaret.Net Yazılım Hizmetleri Sanayi Ticaret A.Ş.
Address               : Uludag Universitesi Gorukle Kampusu
                     : Ulutek Tek. Bol. Arge Binasi Yani Ek Bina Nilufer
                     : - Bursa Türkiye
Phone                 : 90-224-2248640
Fax                   : 90-224-2249520
```

❖ nslookup komutu

- ❖ DNS sunucu ile haberleşip DNS sorguları yapmak için kullanılmaktadır.
- ❖ **Temel kalıbı şu şekildedir: nslookup [seçenek] [sorgu]**

```
root@bilmuh:~# nslookup www.derinteknoloji.com.tr
Server:          178.233.140.110
Address:         178.233.140.110#53
```

```
Non-authoritative answer:
www.derinteknoloji.com.tr      canonical name = derinteknoloji.com.tr.
Name:   derinteknoloji.com.tr
Address: 31.186.11.122
```

❖ dig komutu

❖ DNS sorgularını yapmak için kullanılan nslookup'ın yerini almış daha kapsamlı bir komuttur.

❖ Genel biçimi:

\$ **dig @server name type**

server: DNS cache sunucu
name: Sorgulanacak alan adı
type: Sorgu türü, ANY, A, MX, SIG gibi.

```
root@bilmuh:~# dig www.btu.edu.tr @8.8.8.8
```

```
; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> www.btu.edu.tr @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18263
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.btu.edu.tr.                IN      A

;; ANSWER SECTION:
www.btu.edu.tr.                1369    IN      A      79.123.219.23

;; Query time: 60 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Tue Nov 28 02:25:26 +03 2023
;; MSG SIZE rcvd: 59
```

```
root@bilmuh:~# dig www.btu.edu.tr
```

```
; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> www.btu.edu.tr
```

```
;; global options: +cmd
```

```
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38080
```

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags:; udp: 1220
```

```
; COOKIE: edd99a6825e06e9e220c6ade656524b96ffc1ffffbb4cd13f (good)
```

```
;; QUESTION SECTION:
```

```
;www.btu.edu.tr.                IN      A
```

```
;; ANSWER SECTION:
```

```
www.btu.edu.tr.                3600    IN      A      79.123.219.23
```


❖ Dig ile birlikte kullanılan bazı seçenekler:

+`[no]tcp`

TCP kullan veya kullanma, normalde DNS sorguları UDP ile yapılır.

+`[no]all`

Bütün görüntülüne seçeneklerini aç veya kapat

+`time=T`

Sorgu için T sn'lik bir zaman aşımı

+`[no]answer`

DNS cevabını görüntüle veya görüntüleme

```
$ dig pardus.org.tr NS +noall +answer
```

```
; <<>> DiG 9.8.4-rpz2+r1005.12-P1 <<>> pardus.org.tr NS +noall  
+answer  
;; global options: +cmd  
pardus.org.tr.      20909 IN      NS      ns1.ulakbim.gov.tr.  
pardus.org.tr.      20909 IN      NS      ns2.ulakbim.gov.tr.
```

host komutu

❖ Bilgi alma komutudur.

❖ Temel kullanımı: **host <hedef_adres>**

```
^Croot@bilmuh:~# host www.derinteknoloji.com.tr
www.derinteknoloji.com.tr is an alias for derinteknoloji.com.tr.
derinteknoloji.com.tr has address 31.186.11.122
derinteknoloji.com.tr mail is handled by 10 mx.turkticaret.net.
```

❖ Çeşitli parametrelerle birlikte kullanılabilir.

```
root@bilmuh:~# host -t NS btu.edu.tr
btu.edu.tr name server ns2.btu.edu.tr.
btu.edu.tr name _server ns1.btu.edu.tr.
```

2. KULLANICI VE GRUP İŞLEMLERİ

- ❖ Linux'e giriş yapabilmeniz için bir kullanıcı adınız olması gerekir.
- ❖ Ön tanımlı olarak sadece root kullanıcısı gelmektedir.
- ❖ Tüm yetkilendirmeler kullanıcı adı veya kullanıcı grubu üzerinden yapılmaktadır.
- ❖ Eklenen kullanıcıların kaydı **/etc/passwd** ve **/etc/shadow** dosyalarında tutulmaktadır.
- ❖ **/etc/passwd** dosyası **kullanıcıların parola bilgileri dışındaki tüm tanımlamalar tutulur.**
- ❖ **/etc/shadow** **dosyasında ise parola ve parola kullanım süresi, değiştirme süresi** gibi bilgiler tutulur.

❖ Örnek bir shadow dosyasının içeriği aşağıdaki gibidir.

root:\$6\$cFNz8/e8\$z9cQK3sUC0OPVWw6nu/QGV1cnKpBJj20ESD2RnWRNWy
lvLQW5q.kmeAHrrOfAPLB33JpoqpEQTkFiovqDbFe50:15972:0:99999:7: : :

❖ **/etc/shadow** dosyasında “:” karakteri ayraç karakteri olarak kullanılır.

Dosyadaki değerler sırayla şu anlama gelir.

1. Kullanıcı adı
2. Şifrelenmiş parola (Hash fonksiyonu alınmış)
3. Parolanın en son değişim tarihi (Burada tarih gün sayısıdır. 1 ocak 1970’ten itibaren)
4. Asgari parola değiştirme periyodu
5. En uzun parola geçerlilik süresi
6. Parolanın son kullanma tarihi (Uyarı burada 7 gün varsayılandır)
7. Parolanın süresi dolduktan sonra geçebilecek gün sayısı
8. Kullanıcı hesabının süresinin dolacağı tarih (Burada boş bırakılmıştır.)

❖ Örnek bir passwd dosyasının içeriği aşağıdaki gibidir.

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

❖ Dosyadaki alanların açıklaması

1. Kullanıcı adı
2. x karakteri. Eskiden parolanın kendisi tanımlanırdı. Artık parola /etc/shadow dosyasında tanımlanıyor.
3. Kullanıcı numarası(ID)
4. Grup numarası(GID)
5. Kullanıcı açıklaması
6. Ev dizini
7. Kabuk yolu

❖ Kullanıcı Ekleme

- ❖ Bir sunucuya kullanıcı eklemek için **useradd** komutu kullanılır.
- ❖ Bu komut aşağıdaki parametreleri alır:
 - m: kullanıcı ev dizinini oluştur
 - d: kullanıcı ev dizini yolu
 - s: kullanıcı kabuğu
 - g: kullanıcı grubu
 - c: Açıklama
- ❖ **useradd fatih**
- ❖ **useradd fatih -s /bin/csh -m -d /home/ismail -g bilmuh**
- ❖ **Kullanıcı parolasını değiştirme: passwd fatih**

❖ Usermod

Kullanıcı için

- **ilave gruplara eklenebilir,**
- **mevcut kullanıcı adı başka bir kullanıcı ile değiştirilebilir,**
- **kullanıcı hesabı kilitlenebilir,**
- **hesap kilidi kaldırılabilir.**

Örnek:

- **Bahattin kullanıcısının hesabı kilitlenir.**

```
usermod -L bahattin
```

- **Duru kullanıcısını admin ve apache grubuna eklemek için**

```
usermod -G admin,apache duru
```

❖ Grup yönetimi

- ❖ Grup **eklemek** için **groupadd**, **silmek** için de **groupdel** komutu kullanılır.
- ❖ Groupadd komutu **otomatik olarak sıradan bir** Grup numarası(GID) atar.
- ❖ **Farklı bir GID** vermek için **-g** parametresi kullanılır.

❖ Örnek:

groupadd sistemci

groupadd sistemci

- ❖ Bir kullanıcı ve grup numarasını öğrenmek için **id** komutu kullanılır.

❖ Örnek: **id pardus**

uid=1004(pardus) gid=1006(pardus) gruplar=1006(pardus),1003(admin),1007(apache)

❖ **Parola ömür süresi yapılandırması :**

❖ **/etc/shadow** dosyasında şifrelenmiş parolaya ek olarak parolanın ne kadar süre sonra değiştirileceğini bilgisi tutulmaktadır.

❖ Bu süreyi değiştirmek için **chage** komutu kullanılır.

❖ Bu komut parolanın son değiştirme tarihinden değiştirilmesi gereken güne kadar olan geçen sürenin gün cinsinden miktarını değiştirir.

❖ Bu bilgi sistem tarafından kullanıcının ne zaman parolasını değiştirmek gerektiğini bulmakta kullanılır.

❖ **-M parametresi ile azami gün sayısı belirtilir.**

❖ **-m ile de parola değişikliği için geçecek asgari süre belirtilir.**

❖ **Bu değerleri sistem genelinde tanımlamak** için **/etc/login.defs** dosyasındaki **PASS_MAX_DAYS** ve **PASS_MIN_DAYS** değerleri kullanılır.

❖ Kullanıcı Silme

❖ **userdel** komutu kullanılır.

❖ Bu komut, sadece kullanıcı adı verilerek kullanıldığında kullanıcının */etc/passwd* ve */etc/shadow* dosyalarından kaydını siler.

❖ **userdel ahmet**

- Yukarıdaki komut çalıştırıldığında ev dizini silinmez.
- **Kullanıcıyı ev dizinindeki dosyalarla birlikte tamamen silmek için **-r** parametresi kullanılır.**

❖ **userdel -r ahmet**

❖ Kullanıcı Girişlerini Kısıtlama

- ❖ Root dışındaki kullanıcıların geçici olarak sisteme girişini engellemek için **/etc/nologin** dosyası oluşturmak yeterlidir.
- ❖ Kullanıcı giriş yapmaya çalıştığında bu dosyadaki yazan metin ekrana yazılacak kullanıcının girişine izin verilmeyecektir.
- ❖ Eğer tek bir kullanıcının giriş yapılmaması isteniyorsa **usermode -L** veya **passwd -l** komutu ile kullanıcı hesabı kilitlenebilir.

❖ Kullanıcı taslak dosyaları

- ❖ Her yeni kullanıcı açıldığında **kullanıcı ev dizinine otomatik olarak bazı dosyaları kopyalamak için /etc/skel** dizini kullanılır.

```
# ls -al /etc/skel/
```

```
toplam 40
```

```
drwxr-xr-x    5 root root  4096 Kas  9 16:48 .
drwxr-xr-x 153 root root 12288 Ara  4 14:00 ..
-rw-r--r--    1 root root   220 Ara 30 2012 .bash_logout
-rw-r--r--    1 root root  3206 Eki 10 2012 .bashrc
drwxr-xr-x    3 root root  4096 Mar 24 2013 .config
drwxr-xr-x    4 root root  4096 Mar 24 2013 .mozilla
-rw-r--r--    1 root root   675 Ara 30 2012 .profile
drwxr-xr-x    4 root root  4096 Mar 24 2013 .thunderbird
```

- ❖ Bu dizine açılacak **her bir yeni dosya yeni kullanıcıların ev dizinine kullanıcı hakları** ile kopyalanacaktır.

❖ su (switch user) komutu

❖ Root şifresi biliniyorsa root kullanıcısı olarak giriş yapmak için

`su -` veya `su root` veya `su - root`

Not: Debian işletim sisteminde *root* kullanıcısında herhangi bir kısıtlama ile karşılaşmamak için `su root` yerine `su - root` kullanılmalıdır.

3. CRON İŞLEMLERİ

- ❖ Cron sistemi UNIX dünyasındaki **zamanlayıcının adıdır.**
- ❖ Zamanlanan iş olup olmadığı crond **servisi tarafından dakikada bir kontrol edilir.**
- ❖ **Vakti geldiğinde belirtilen komutlar işletilir.**
- ❖ Sistem genelinde olduğu gibi **her bir kullanıcı da izin verilmişse kendi zamanlayıcısını tanımlayabilir.**
- ❖ Sistem geneline ait işler ***/etc/crontab*** dosyasında tanımlanır.

```

root@bilmuh:~# cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |
# * * * * * user-name command to be executed
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/
cron.daily; }
47 6 * * 7 root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/
cron.weekly; }

```

- ❖ **Yukarıdaki değerlerin yerine “*” sembolü konulursa geçerli bütün değerler için çalıştır anlamına gelir.**
- ❖ **Her bir sütun için 2-6 gibi aralık belirtilebildiği gibi, 1,5,7 gibi birden fazla değer de belirtilebilir.**
- ❖ **Periyodik yapılacak işler için 0-59/15, */5 gibi kullanımlar da geçerlidir.**
- ❖ **Kullanıcı kısmı**, komutun hangi sistem kullanıcısı yetkileriyle çalıştırılacağını belirler.

❖ Her gün gece 02:18 de yedekle.sh'ı çalıştır.

```
18 2 * * * root /root/scripts/yedekle.sh
```

❖ Haftanın 1. günü saat 5'te her 10 dakikada bir çalıştırır.

- 0-59/10 5 * * 1 root /usr/local/bin/gonder

❖ Her 5 dakikada bir çalıştırır.

- */5 * * * * root /usr/libexec/atrun

❖Örnek: Her hafta Salı günü 22:50'de root dizini altındaki *a.txt* dizinini *root dizini altındaki YEDEK klasörüne* altına kopyalayan komutu yazınız.

❖Çözüm: nano /etc/crontab

```
GNU nano 7.2 /etc/crontab
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |
# * * * * * user-name command to be executed
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc>
47 6 * * 7 root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc>
52 6 1 * * root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc>
50 22 * * 2 root cp a.txt /root/YEDEK/
```

- ❖Günlük yapılan işler **/etc/cron.daily/**
- ❖Haftalık yapılan **/etc/periodic/weekly,**
- ❖Aylık yapılanlar **/etc/periodic/monthly**

dizinde tanımlanmıştır.

- ❖Linux vakti geldiğinde bu dizinlerdeki tüm dosyaları isim sırasına göre çalıştırır.

- ❖Örneğin

```
# ls /etc/cron.daily/
```

```
apache2 apt aptitude apt-show-versions bsdmainutils dpkg locate  
logrotate man-db ntp passwd quota samba sysstat
```

```
# ls /etc/cron.weekly/
```

```
apt-xapian-index man-db
```

```
# ls /etc/cron.monthly/
```

```
readahead-monthly
```

❖ Sistemdeki Kullanıcı için Crontab

- ❖ Her bir kullanıcı kendi işlerini **crontab** komutunu kullanarak tanımlayabilir.
- ❖ Crontab komutuna **-l** parametresi verildiğinde var olan işler listelenir.

```
# crontab -l  
# Her gün gece 02:18 de yedekle.sh'ı çalıştır  
18 2 * * * /root/scripts/yedekle.sh > /dev/null 2>&1
```

```
# Her 5 dakikada bir çalıştırır  
*/5 * * * * /usr/libexec/atrun > /dev/null 2>&1
```

- ❖ **'-e'** parametresi ile **cron işleri düzenlenebilir.**

```
crontab -e
```

- ❖ Yukarıdaki komut verildiğinde metin düzenleyici- ön tanımlı olarak **vi editörü** ile birlikte açılır.

❖ **root kullanıcısı isterse başka kullanıcıların crontab'larına müdahale edebilir.**

❖ Bunun için **–e parametresinden sonra –u parametresi ile** aşağıdaki gibi crontab'ında **değişiklik yapılacak kullanıcının adı verilir.**

crontab –e –u pardus

❖ Kullanıcılara ait cron tanımları, ***/var/spool/cron/crontabs*** dizini altında saklanır.

❖ **ls /var/spool/cron/crontabs/
pardus root**

UYGULAMA SORULARI

Aşağıdaki soruları okuldaki sunucuya bağlandıktan sonra linux komutları yazarak çözünüz.

1. Kendi ip adresinizi kablolu ve kablosuz ağ için öğreniniz. Bu öğrendiğiniz IP hangi sınıf ve türdendir.
2. Bir kullanıcı *www.turkiye.gov.tr* adresine erişememiştir. Bunun kendi bilgisayarında sorun olduğu için mi yoksa bu web sitesinin barındığı sunucuya erişilememesinden kaynaklandığı tespit etmek istiyor. Bunu hangi komut ile gerçekleştirebilir.
3. *www.turkiye.gov.tr* adresine erişimi ağda hangi aşamalardan geçerek gerçekleşmektedir?
4. *www.turkiye.gov.tr* alan adının sahibi kimdir? Öğreniniz.
5. *www.turkiye.gov.tr* adresinin IP adresini öğreniniz.

Aşağıdaki soruları kendi kurduğunuz sunucu üzerinde root olarak giriş yaptıktan sonra linux komutları yazarak çözünüz.

1. Bir sistem yöneticisi, **ağ istatistiğini** görmek istemektedir. Bunun için **hangi komutu yazmalıdır?**
2. Kendi kurduğunuz sunucuda **hangi standart servisler var** ve **bunlar hangi portları kullanmaktadır?** Öğreniniz.
3. Teknik_Servis ve Muhasebe adında grup oluşturunuz.
4. *ali, veli, ayse ve leyla* adında **4 tane kullanıcıyı (useradd komutu ile) oluşturunuz**. Ali ve leyla teknik servis, Ayse ve Veli Muhasebe grubunda olsun. **Bu kullanıcılara 123 şifresini veriniz.**
5. **Leyla adındaki kullanıcıyı ev dizini ile birlikte kaldırınız.**
6. Sistemde kaç tane kullanıcı var? Öğreniniz. Kendi giriş yaptığınız kullanıcının grubunu öğreniniz.
7. **/etc/passwd** dosyasının **içerisine** bir kullanıcı (kamil adında) **elle yazarak oluşturulursa ne olur?** **Bu kullanıcı oluşur mu?** **Oluşursa bu kullanıcının ev dizini ne olur?** Bu kullanıcı **/etc/passwd** dosyasından silinirse kalkar mı?

8. Ali adındaki kullanıcıyı kilitleyiniz. Bu kullanıcı ile sisteme giriş yapmaya çalışınız.
9. root ev dizininde rapor adında bir klasör oluşturunuz. Bunun içerisine not.txt dosyası oluşturup içerisinde İstiklal Marşının iki dizesi olsun.

Daha sonra bu rapor klasörünü arşivleyip sıkıştırarak (gzip ile) yedekleyecek ve bu dosyayı /opt dizini içerisine kaydedecek bir cron işlemi tanımlayınız.

Bu cron işlemi her hafta Pazartesi olsun. Saat ve dakika olarak ise örneğin cron işlemini 15:25'te yazarsanız işlemi gerçekleştirilecek saat 15:30 olsun. (5 dakika sonrası için)

Cron işleminin gerçekleştirilip gerçekleştirmediğini test ediniz.

10. Cron işlemi ile rapor adındaki klasörü her gün yedeklenirken bunun üzerine yazılma olmasın. Örneğin rapor klasörü, 28-11-2023yedek.tar.gz şeklinde /opt dizinine yedeklensin.

11. Cron işlemi yaparak rapor adındaki klasör her 5 dakikada bir /opt/ dizini altına yedekleyecek komutu yazınız. Bu tarz bir yedekleme yapıldığında sunucu sisteminde yürütülen süreçleri gözlemleyiniz. Eğer rapor klasörü oldukça büyük olsaydı (100 GB gibi) bu tarz sunucuya otomatik işlemler yaptırılması sistemin performansını nasıl etkiler?

12. Arşivleyip yedeklediğiniz rapor klasörü ile ilgili bir tane yedeği /tmp dizini altına açıp okuyunuz.

KAYNAKLAR

- ❖ Pardus LPI-Sertifikasyon-Kitabı
- ❖ Linux Komut Satırı, Kemal DEMİREZ, Abaküs Kitap Yayın Dağıtım Hizmetleri, 2019