Born2beroot detayına kadar öğrenme vol2

############
https://www.techtarget.com/searchnetworking/definition/TCP
TCP (Transmission Control Protocol)İletim Kontrol Protokolü, Bağlantıya yönelik güvenli bir protokol. İletilecek veriler önce uygulama tarafından bir veri akışı olarak gönderilir, ardından işletim sistemi tarafından uygun biçime dönüştürülür.

TCP, verileri sunucu ve istemci arasında güvenli iletimi sağlayacak şekilde düzenlemek için kullanılır. Ağ üzerinden gönderilen verilerin, miktarı ne olursa olsun bütünlüğünü garanti eder. Bu nedenle, iletilen tüm verilerin ulaşmasını gerektiren diğer üst düzey protokollerden veri iletmek için kullanılır.

> Bu protokollerin örnekleri şunlardır:

> Güvenli Kabuk(**Secure Shell)** (SSH), Dosya Aktarım Protokolü(**File Transfer Protocol)** (FTP), Telnet: Eşler arası dosya paylaşımı ve Telnet'in durumunda, bir dosyaya erişmek için başka bir kullanıcının bilgisayarında oturum açmak için.

> Basit Posta Aktarım Protokolü(**Simple Mail Transfer Protocol)** (SMTP), Postane Protokolü(**Post Office Protocol)** (POP), İnternet İleti Erişim Protokolü(**Internet Message Access Protocol)** (IMAP): E-posta göndermek ve almak için.

> HTTP: Web erişimi için.

Bu örneklerin tümü, TCP/IP yığınının uygulama katmanında bulunur ve taşıma katmanındaki TCP'ye aşağı doğru veri gönderir.

TCP neden önemlidir?

> TCP önemlidir çünkü bilgilerin internet üzerinden iletilme şekline ilişkin kuralları ve standart prosedürleri belirler. Mevcut haliyle internetin temelidir ve ilgili yer, donanım veya yazılımdan bağımsız olarak veri iletiminin tek tip olarak yapılmasını sağlar.

> TCP esnektir ve yüksek düzeyde ölçeklenebilirdir, yani ona yeni protokoller eklenebilir ve bunları barındırır. Aynı zamanda tescilli değildir, yani hiç kimse veya şirket ona sahip değildir.

Location in the TCP/IP stack (TCP/IP yığınındaki konum)

> TCP/IP yığını, verilerin TCP/IP protokolü kullanılarak ağlar üzerinden nasıl düzenlendiğini ve değiş tokuş edildiğini temsil eden bir modeldir. İstemciden sunucuya ve tersi yönde ilerlerken, verilerin bir dizi protokol tarafından işlenme ve paketlenme biçimini temsil eden bir dizi katmanı tasvir eder.

> TCP, UDP gibi diğer protokollerle birlikte taşıma katmanında bulunur. Bu katmandaki protokoller, daha sınırlı hata kontrol kabiliyetine sahip olduğu için UDP

hariç, verilerin kaynağa hatasız iletimini sağlar.

Kurulan toplam bağlantı sayısını bulmamız isteniyor bu yüzden TCP insune değeri elde edilecektir.

- Aktif bağlantı sayısı.

```
ctcp=$(cat /proc/net/sockstat | awk '$1 == "TCP:" {print $3}')
```

```
#Connexions TCP: $ctcp ESTABLISHED
```

Aktif TCP bağlantılarına bakmak için bu kullanılabilir.

```
akaraca@akaraca42:~$ cat /proc/net/sockstat
sockets: used 80
TCP: inuse 2 orphan 0 tw 0 alloc 3 mem 1
UDP: inuse 1 mem 0
UDPLITE: inuse 0
RAW: inuse 0
FRAG: inuse 0 memory 0
```

Bağlantı sayısını bulmak için;

```
akaraca@akaraca42:~$ cat /proc/net/sockstat | awk '$1 == "TCP:" {print $3}'
2
```

TCP inuse, kurulan toplam bağlantı sayısını temsil ediyor.
TCP orphan(kimsesiz bırakılan, yetim, öksüz vs), artık,öksüz,yetim tcp bağlantıları temsil ediyor. (herhangi bir kullanıcı dosyası tanıtıcısına eklenmemiş)
TCP tw, TIME_WAIT bağlantıları
TCP alloc, Alloc: Ayrılan TCP soketleri (tüm türler) (allow types)
TCP mem, ?????????????

Ya da bu komut ilede bakılabilir.

```
akaraca@akaraca42:/usr/local/bin$ ss -s
Total: 80
TCP:   3 (estab 1, closed 0, orphaned 0, timewait 0)

Transport Total     IP        IPv6
RAW       0         0         0
UDP       1         1         0
TCP       3         2         1
INET      4         3         1
FRAG      0         0         0
```

```
akaraca@akaraca42:/usr/local/bin$ ss -s | awk '$1 == "TCP" {print $3}'
2
```

Eğerki sadece sunucu üzerinden bağlantı kurarsam tek bir bağlantı olduğunu göreceğiz.

```
root@akaraca42:~# ss -s
Total: 74
TCP:   2 (estab 0, closed 0, orphaned 0, timewait 0)

Transport Total     IP        IPv6
RAW       0         0         0
UDP       1         1         0
TCP       2         1         1
INET      3         2         1
FRAG      0         0         0
```

```
root@akaraca42:~# ss -s | awk '$1 == "TCP" {printf $3}'
1root@akaraca42:~# _
```

```
root@akaraca42:~# bash /usr/local/bin/monitoring.sh

Broadcast message from root@akaraca42 (tty1) (Thu Mar 24 06:03:14 2022):

        #Architecture: Linux akaraca42 5.10.0-12-amd64 #1 SMP Debian 5.10.103-1 (2022-03-07) x86_64
GNU/Linux
        #CPU physical: 1
        #vCPU: 2
        #Memory Usage: 72/1982MB (3.64%)
        #Disk Usage: 1590/28Gb (6%)
        #CPU load: 3.2%
        #Last boot: 2022-03-24 04:59
        #LVM use: yes
        #Connexions TCP: 1 ESTABLISHED
        #User log: 1
        #Network: IP 10.0.2.15  (08:00:27:ee:c6:71)
        #Sudo: 272 cmd
```

##################

- Sunucuyu kullanan kullanıcı sayısı.

```
ulog=$(users | wc -w)
```

```
#User log: $ulog
```

Kullanıcı sayısını bulmak için;

```
akaraca@akaraca42:~$ users
akaraca
akaraca@akaraca42:~$ users | wc
      1       1       8
akaraca@akaraca42:~$ users | wc -l
1
akaraca@akaraca42:~$ users | wc -w
1

Broadcast message from root@akaraca42 (somewhere) (Thu Mar 24 06:00:01 2022):

        #Architecture: Linux akaraca42 5.10.0-12-amd64 #1 SMP Debian 5.10.103-1 (2022-03-07) x86_64 GNU/Linux
        #CPU physical: 1
        #vCPU: 2
        #Memory Usage: 73/1982MB (3.71%)
        #Disk Usage: 1590/28Gb (6%)
        #CPU load: 3.2%
        #Last boot: 2022-03-24 04:59
        #LVM use: yes
        #Connexions TCP: 2 ESTABLISHED
        #User log: 1
        #Network: IP 10.0.2.15  (08:00:27:ee:c6:71)
        #Sudo: 270 cmd
```

Sunucu üzerinden root kullanıcısına girerek artış gerçekleşiyor mu kontrol ettim.

```
akaraca@akaraca42:~$ users
akaraca root
akaraca@akaraca42:~$ users | wc
      1       2      13
akaraca@akaraca42:~$ users | wc -l
1
akaraca@akaraca42:~$ users | wc -w
2

Broadcast message from root@akaraca42 (somewhere) (Thu Mar 24 06:02:01 2022):

        #Architecture: Linux akaraca42 5.10.0-12-amd64 #1 SMP Debian 5.10.103-1 (2022-03-07) x86_64 GNU/Linux
        #CPU physical: 1
        #vCPU: 2
        #Memory Usage: 77/1982MB (3.91%)
        #Disk Usage: 1590/28Gb (6%)
        #CPU load: 3.2%
        #Last boot: 2022-03-24 04:59
        #LVM use: yes
        #Connexions TCP: 2 ESTABLISHED
        #User log: 2
        #Network: IP 10.0.2.15  (08:00:27:ee:c6:71)
        #Sudo: 271 cmd
```

##########################

- Sunucunun IPv4 ve MAC (Media Access Control) adresleri.

```
ip=$(hostname -I)
```

```
mac=$(ip link show | awk '$1 == "link/ether" {print $2}')
```

```
#Network: IP $ip ($mac)
```

Sunucunun IP adresini çekmek için;

```
akaraca@akaraca42:~$ hostname
akaraca42
akaraca@akaraca42:~$ hostname --help
Usage: hostname [-b] {hostname|-F file}         set host name (from file)
       hostname [-a|-A|-d|-f|-i|-I|-s|-y]       display formatted name
       hostname                                 display host name

       {yp,nis,}domainname {nisdomain|-F file}  set NIS domain name (from file)
       {yp,nis,}domainname                      display NIS domain name

       dnsdomainname                            display dns domain name

       hostname -V|--version|-h|--help          print info and exit

Program name:
       {yp,nis,}domainname=hostname -y
       dnsdomainname=hostname -d

Program options:
    -a, --alias            alias names
    -A, --all-fqdns        all long host names (FQDNs)
    -b, --boot             set default hostname if none available
    -d, --domain           DNS domain name
    -f, --fqdn, --long     long host name (FQDN)
    -F, --file             read host name or NIS domain name from given file
    -i, --ip-address       addresses for the host name
    -I, --all-ip-addresses all addresses for the host
    -s, --short            short host name
    -y, --yp, --nis        NIS/YP domain name
```

“hostname -I” komutu ile tüm ip adreslerini görüntülemek için;

```
akaraca@akaraca42:~$ hostname -I
10.0.2.15
```

MAC adreslerini görüntülemek için;

```
akaraca@akaraca42:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:ee:c6:71 brd ff:ff:ff:ff:ff:ff
```

```
akaraca@akaraca42:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:ee:c6:71 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 82057sec preferred_lft 82057sec
    inet6 fe80::a00:27ff:feee:c671/64 scope link
       valid_lft forever preferred_lft forever
```

lo, geri döngü arabirimidir(**loopback interface)**. Bu, sistemin kendi kendisiyle iletişim kurmak için kullandığı özel bir ağ arabirimidir.
ether: Bir ağa bağlanmak için kimlik doğrulama prosedürünün bir parçası olarak gerekli olabilecek arayüzünüzün donanım adresi "ether" ile işaretlenmiştir.
Mac ve **IP adresleri**, ağa bağlı olan cihazı tanımlar. **Mac**, bilgisayarın ev adresimiz gibi fiziksel adresidir. Böylece bir ağda, bir **Mac adresi** kullanılarak çeşitli cihazlar tanımlanabilir. **IP adresi** ise ağ bağlantısını bir sayı vererek tanımlar.

MAC adresini çekmek için;

```
akaraca@akaraca42:~$ ip link show | awk '$1 == "link/ether" {print $2}'
08:00:27:ee:c6:71
```

################

- sudo ile çalıştırılmış komut sayısı.

```
cmds=$(journalctl _COMM=sudo | grep COMMAND | wc -l)
```

```
#Sudo: $cmds cmd"
```

journalctl, systemd'nin günlük kaydı hizmeti olan Journald'den günlükleri sorgulamak ve görüntülemek için bir yardımcı programdır. Journald, günlük verilerini düz metin biçimi yerine ikili biçimde sakladığından, Journalctl, Journald tarafından işlenen günlük mesajlarını okumanın standart yoludur.

```
akaraca@akaraca42:~$ journalctl
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
-- Journal begins at Thu 2022-03-17 07:05:10 EDT, ends at Thu 2022-03-24 06:06:45 EDT. --
Mar 17 07:05:10 akaraca42 su[544]: (to root) akaraca on tty1
Mar 17 07:05:10 akaraca42 su[544]: pam_unix(su:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 07:05:25 akaraca42 su[544]: pam_unix(su:session): session closed for user root
Mar 17 07:06:17 akaraca42 su[552]: pam_unix(su:auth): authentication failure; logname=akaraca uid=1000 euid=0 tty=tty1 ruser=a>
Mar 17 07:06:20 akaraca42 su[552]: FAILED SU (to root) akaraca on tty1
Mar 17 07:06:28 akaraca42 su[554]: (to root) akaraca on tty1
Mar 17 07:06:28 akaraca42 su[554]: pam_unix(su:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 07:36:21 akaraca42 su[554]: pam_unix(su:session): session closed for user root
Mar 17 07:38:01 akaraca42 sudo[679]:  akaraca : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/visudo
Mar 17 07:38:01 akaraca42 sudo[679]: pam_unix(sudo:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 07:42:56 akaraca42 sudo[679]: pam_unix(sudo:session): session closed for user root
Mar 17 07:58:15 akaraca42 sudo[697]: pam_unix(sudo:auth): authentication failure; logname=akaraca uid=1000 euid=0 tty=/dev/tty>
Mar 17 07:58:23 akaraca42 sudo[697]:  akaraca : 3 incorrect password attempts ; TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sb>
Mar 17 08:07:42 akaraca42 sudo[704]: pam_unix(sudo:auth): authentication failure; logname=akaraca uid=1000 euid=0 tty=/dev/tty>
Mar 17 08:07:52 akaraca42 sudo[704]:  akaraca : 3 incorrect password attempts ; TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sb>
Mar 17 08:08:04 akaraca42 sudo[706]: pam_unix(sudo:auth): authentication failure; logname=akaraca uid=1000 euid=0 tty=/dev/tty>
Mar 17 08:08:12 akaraca42 sudo[706]:  akaraca : 3 incorrect password attempts ; TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sb>
Mar 17 08:11:36 akaraca42 sudo[710]: pam_unix(sudo:auth): authentication failure; logname=akaraca uid=1000 euid=0 tty=/dev/tty>
Mar 17 08:11:44 akaraca42 sudo[710]:  akaraca : TTY=tty1 ; PWD=/var/log ; USER=root ; TSID=000001 ; COMMAND=/usr/bin/mkdir sudo
```

sudo ile ilgili yapılan işlemleri sıralar.

```
Mar 17 08:26:17 akaraca42 sudo[813]:  akaraca : TTY=tty1 ; PWD=/ ; USER=root ; TSID=000008 ; COMMAND=/usr/bin/apt-get install vim
Mar 17 08:26:17 akaraca42 sudo[813]: pam_unix(sudo:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 08:26:22 akaraca42 sudo[813]: pam_unix(sudo:session): session closed for user root
Mar 17 08:27:13 akaraca42 sudo[933]:  akaraca : TTY=tty1 ; PWD=/ ; USER=root ; TSID=000009 ; COMMAND=/usr/bin/apt-get install vim
Mar 17 08:27:13 akaraca42 sudo[933]: pam_unix(sudo:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 08:27:14 akaraca42 sudo[933]: pam_unix(sudo:session): session closed for user root
Mar 17 08:28:13 akaraca42 sudo[939]:  akaraca : TTY=tty1 ; PWD=/ ; USER=root ; TSID=00000A ; COMMAND=/usr/bin/vim /etc/pam.d/common-password
Mar 17 08:28:13 akaraca42 sudo[939]: pam_unix(sudo:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 08:29:51 akaraca42 sudo[939]: pam_unix(sudo:session): session closed for user root
Mar 17 08:31:29 akaraca42 sudo[945]:  akaraca : TTY=tty1 ; PWD=/ ; USER=root ; TSID=00000B ; COMMAND=/usr/bin/apt-get install libpam-pwquality
Mar 17 08:31:29 akaraca42 sudo[945]: pam_unix(sudo:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 08:31:31 akaraca42 sudo[945]: pam_unix(sudo:session): session closed for user root
Mar 17 08:32:28 akaraca42 sudo[1090]:  akaraca : TTY=tty1 ; PWD=/ ; USER=root ; TSID=00000C ; COMMAND=/usr/bin/apt-get install libpam-pwquality
Mar 17 08:32:28 akaraca42 sudo[1090]: pam_unix(sudo:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 08:32:29 akaraca42 sudo[1090]: pam_unix(sudo:session): session closed for user root
Mar 17 08:33:32 akaraca42 sudo[1096]:  akaraca : TTY=tty1 ; PWD=/ ; USER=root ; TSID=00000D ; COMMAND=/usr/bin/vim /etc/pam.d/common-password
```

Komut satırı içerisinde sudo ile yapılan işlemleri sıralar.

```
akaraca@akaraca42:~$ journalctl _COMM=sudo | grep COMMAND
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
Mar 17 07:38:01 akaraca42 sudo[679]:  akaraca : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/visudo
Mar 17 07:58:23 akaraca42 sudo[697]:  akaraca : 3 incorrect password attempts ; TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/visudo
Mar 17 08:07:52 akaraca42 sudo[704]:  akaraca : 3 incorrect password attempts ; TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/groupadd user42
Mar 17 08:08:12 akaraca42 sudo[706]:  akaraca : 3 incorrect password attempts ; TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/visudo
Mar 17 08:11:44 akaraca42 sudo[710]:  akaraca : TTY=tty1 ; PWD=/var/log ; USER=root ; TSID=000001 ; COMMAND=/usr/bin/mkdir sudo
Mar 17 08:11:56 akaraca42 sudo[715]:  akaraca : TTY=tty1 ; PWD=/var/log ; USER=root ; TSID=000002 ; COMMAND=/usr/bin/mkdir sudo
Mar 17 08:13:27 akaraca42 sudo[726]:  akaraca : TTY=tty1 ; PWD=/var/log/sudo ; USER=root ; TSID=000003 ; COMMAND=/usr/bin/cat sudo.log
Mar 17 08:13:46 akaraca42 sudo[731]:  akaraca : TTY=tty1 ; PWD=/var/log ; USER=root ; TSID=000004 ; COMMAND=/usr/bin/rm -rf sudo
```

Kaç komut kullanıldığı görüntülenir.

```
akaraca@akaraca42:~$ journalctl _COMM=sudo | grep COMMAND | wc -l
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
214
```
