4 - born_to_be_root

BORN TO BE ROOT

- **bu projede bir sanal makineye (Oracle Box VM) linux distrosu (Debian) kuracağız. GUI'si olmayacak, tüm komutlar CLI'den girilecek. faydalı repolar:**
  - **https://github.com/HEADLIGHTER/Born2BeRoot-42**

bunlar yapım aşamalarının özeti, sadece evaluation da calısılabilir. yapım asamaları evo'da sorulmuyor.

- **Linux'ta sabit disklerin isimlendirilme mantığı şu şekildedir;**

> Sabit diskler eğer IDE kanalından bağlı ise "hda", "hdb" SCSI ve/veya SATA kanalına takılı ise "sda", "sdb" gibi isimler alırlar. Örneğin birinci sabit disk "hda" olarak adlandırılır. İkinci sabit disk "hdb" şeklinde adlandırılır. Buradan da anlaşılacağı üzere a'dan z'ye kadar -eğer mümkünse- 26 adet sabit disk olabilir. Diskleriniz günümüzün popüler HDD kanalı olan SATA'dan bağlı ise bu durumda örneğimizdeki isimler "sda" ve "sdb" olacaktır.Sabit disklerin bölümleri ise 1'den 63'e kadar numara ile temsil edilirler. Örneğin birinci sabit diskin birinci bölümü "hda1" veya "sda1" olarak adlandırılır. Sistemdeki CD/DVD sürücüler ise "sr0", "sr1" gibi isimler alırlar. Linux'ta her bir sabit disk max 63 parçaya bölünebilir.

- **dosyaların isimleri**
  - **/ is the root file system**
  - **/boot bilgisayarı boot edecek statik dosyaları tutuyor**
  - **/home kullanıcı kişisel dosyaları**
  - **/tmp geçici dosyalar**
  - **/usr statik veriler (static data)**
  - **/var değişken veriler (variable data)**
  - **/srv sistem tarafından sağlanan servis verileri**
  - **/opt add-on application software packages**
- **lsblk --> disklerin durumunu gösterir**
- **su - --> root ortamına geçmek için (admin olma)**
- **apt upgrade --> paketleri günceller**

1) sudo'yu kurma

su - dedikten sonra

- **apt update -y**
- **apt upgrade -y**
- **apt install sudo**

> sudo'nun başarıyla yüklenip yüklenmediğini görmek için
> dpkg -l | grep sudo

- **dpkg, Debian paket yönetim sisteminin temelini oluşturan yazılımdır. apt ondan daha da komplike bir paket yükleme simülatörüdür.**

2) sudo'ya user ekleme

sudoya kullanıcı ekleme -->

1) adduser user_name sudo

2) sudo visudo

user_name ALL=(ALL:ALL)ALL and then reboot

sudo'daki userları görme --> getent group sudo

sudo moduna girmek için --> sudo -v
artık başlarına sudo diyerek root komutlarını çalıştırabiliriz.

3) root kullanma

- **root iken normal user'a geçmek için --> login user_name**
- **sudo güncellemeleri yapan komut -->**

> sudo apt-get update -y
>
> **sudo apt-get upgrade**

- **git indirme --> sudo apt install git -y**

> versionunu ogrenme --> git --version

- **wget: web depolarından dosya indirmek için ücretsiz ve açık kaynak bir araçtır. indirmek için --> sudo apt-get install wget**
- **vim indirme --> sudo apt-get install vim**

oh_my_zsh kurma: terminali özelleştirir. kurmak için -->
sudo apt install zsh

zsh --version (diyerek versiyon numarasını öğrenebiliriz)

zsh diyip kurulumu yap. kurduktan sonra vim .zshrc'de tema seçebilirsin.

4) ssh yükleme

- **ssh yükleme -->**
  sudo apt install ssh –y
  ya da
  sudo apt install openssh-server -y

> ssh'ın başarıyla yüklenip yüklenmediğini görmek için
> dpkg -l | grep ssh

- **SSH sunucu durumunu kontrol edin --> sudo systemctl status ssh**
- **ssh sunucusunu restart etme --> sudo service ssh restart**
- **22 olan portu 4242 olarak değiştirme**

sudo vim /etc/ssh/sshd_config

#Port 22 --> Port 4242

- **Kimlik doğrulama mekanizmasından bağımsız olarak SSH girişini kök olarak devre dışı bırakmak için aşağıdaki satırı değiştirin.**
  Eski hali #PermitRootLogin prohibit-password
  Yeni hali PermitRootLogin no
- **sudo service ssh status diyerek ssh durumunu kontrol edebilirsin**
- **sudo service ssh restart diyerek ssh servislerini restart edebilirsin**
- **port numarasını kontrol etme -->**
  sudo grep Port /etc/ssh/sshd_config
- **sudo service ssh restart**

5) ufw (firewall) kurma

- **ufw sanal makinenin güvenlik duvarıdır. kurmak için**

> sudo apt install ufw -y
>
> **dpkg -l | grep ufw --> diyerek başarılı mı degil mi kontrol et**
>
> **sudo ufw enable --> güvenlik duvarını etkinleştirebilirsin**
>
> **sudo systemctl status ufw --> etkin mi değil mi diye kontrol eder**
>
> **etkinleşmezse reboot diyerek sistemi baştan başlat**

- **güvenlik duvarında ssh'ye izin vermek için**

> sudo ufw allow ssh
>
> **sudo ufw allow 4242 (portuna da izin veriyoruz)**

- **ufw'den bir kural silmek için:**
  - **sudo ufw status numbered**
  - **sudo ufw delete (silinecek kural numarası, mesela 1 ya da 3)**
- **ufw**
  - **default olarak pasiftir aktiflestirilmelidir**
  - **güvenlik duvarıdır**
  - **gui'si vardır**
  - **linuxlarda firewall default olarak iptables denilen bir şeydir. ama ufw daha minimal ve kolay oldugu icin onu kullaniyoruz.**

6) Sunucuya SSH ile Bağlanma

- **vm'de ayarlar->ağ->bağdaştırıcı1->gelişmiş->b. noktası->yeni bağlantı 4242 ve 4242 yaparsan**

> bir server ip'si atamış olursun.
>
> **daha sonra --> sudo systmctl restart ssh**
>
> **kontrol et --> sudo systemctl status ssh**
>
> **bu ip'te daha sonra normal iterm'den**
>
> **ssh <username>@127.0.0.1 -p 4242**
>
> **diyerek ve şifre girerek bağlanabilirsin. çıkmak için**
>
> **logout ya da exit diyebilirsin.**

-

Adım 8: Ana bilgisayar adını değiştir

- **login diyerek ve şifre girerek giriş yap**
- **root ol**
  - **sudo -s ya da**
  - **su -**

- **mevcut pc'nin adını kontrol et**

hostnamectl

- **bu adı değiştirme**

> hostnamectl set-hostname newName
>
> **vim /etc/hosts'ta da değiştiriyoruz**
>
> **localhost**
> **yeni_ismi**

- **reboot ettikten sonra hostnamectl dediğimizde artık bilgisayar ismi değişmiş olarak önümüze geliyor.**

Adım 9: sudo'yu yapılandırma

- **sudo kullanırken yapılan her işlem (tüm girdi ve çıktılar) kayıt altında tutulmalıdır. Kayıtların tutulduğu log dosyası /var/log/sudo/ klasörüne kaydedilmelidir. Bunu gerçekleştirmek için ilgili klasörü oluşturalım.**

> sudo mkdir /var/log/sudo
>
> **daha sonra sudo vim /etc/sudoers'a girip şu 3ünü ekle**
>
> **Defaults log_input,log_output**
>
> **Defaults logfile="/var/log/sudo/sudo.log"**
>
> **Defaults requiretty (çünkü güvenlik sebepleriyle TTY modu aktif hale getirilmelidir)**
>
> **bunlar tüm girilen sudo komutlarının kayıtlarını /var/log/sudo'da tutmamıza yarayan komutlar**
>
> **daha sonra :wq! ile çık**

- **TTY sistemi terminale erişim için kullanılan protokoldür. sanal terminal gibi düşünülebilir. Bir de bunun muadili pts vardır o da uzak terminal olarak adlandırılır.**

> who komutuyla hangi kullanıcı hangi terminali kullanıyor görebilirsin. tty komutunu da kullanabilirsin.

parola ayarları yapma

- **sudo vim /etc/login.defs ile girelim. PASS_MAX/MIN/WARN day'leri değiştirelim (30/2/7)**

- **Yanlış bir parola olması durumunda sudo kullanarak kimlik doğrulamasını 3 denemeyle (varsayılan 3'tür) sınırlamak için dosyaya aşağıdaki satırı ekleyin. vim /etc/sudoers**

> Defaults passwd_tries=3

- **Yanlış şifre durumunda özel bir hata mesajı eklemek için aşağıdaki komutu ekleyin:**

> Defaults badpass_message="yanlis sifre!"

- **bunlar yeni kullanıcılar için. halihazırdaki kullanıcıların parola ayarlarını değiştirmek istiyosan:**

> sudo chage --mindays 2 user_name
>
> **sudo chage --maxdays 30 user_name**
>
> **sudo chage --warndays 10 user_name**
>
> **güncel bilgileri almak için de**
>
> **sudo chage -l user_name diyoruz**
>
> **bunlar kaynağa göre olsa da subject'e göre eskimiş. pushlarken dikkat et.**

- **parola kalitesi kontrolü yapan paketi indir**

> sudo apt install libpam-pwquality -y

- **daha sonra sudo vim /etc/pam.d/common-password dosyasını aç**
- **25. satır'daki password requisite pam_pwquality.so satırına**

> en fazla 3 giriş hakkı vermek için
>
> **retry=3**
>
> **Şifrenin en az bir büyük harf içermesini zorunlu kılmak için:**

ucredit=-1

> Şifrenin en az bir küçük harf içermesi zorunlu kılmak için:

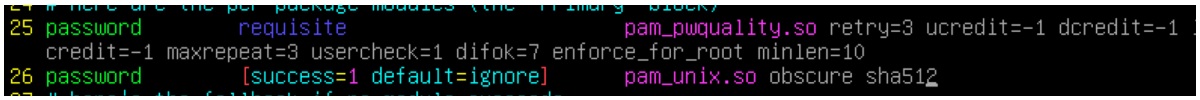
lcredit=-1

> Şifrenin en az bir sayısal karakter içermesini zorunlu kılmak için:

> **dcredit=-1**
>
> **En fazla 3 ardışık aynı karakter ayarlamak için:**
>
> **maxrepeat=3**
>
> **Bir biçimde <kullanıcı adı> içeriyorsa parolayı reddetmek için:**
>
> **usercheck=1**
>
> **Yeni şifrede gerekli değişiklik sayısını eski şifreden 7'ye ayarlamak için:**
>
> **difok=7**
>
> **Tüm bu şifre politikasını root kullanıcısı üzerinde uygulamak için**
>
> **enforce_for_root**
>
> **Şifre minimum uzunluğunu 10 karakter olarak ayarlamak için:**
>
> **minlen=10**

ekleyelim.

> 25 ve 26. satırların son hali şöyle olmalı



> **değişikliklerin etkinleşmesi için sistemi yeniden başlatın:**
>
> **sudo reboot**

yeni kullanıcı oluşturma

- **sudo adduser new_user**
- **id newUserName diyerek olusup olusmadıgını kontrol et**
- **sudo chage -l new_userdiyerek kullanıcının yeni normlara uygun bir parola girip girmediğini kontrol et.**
- **groups diyerek o anki default kullanıcının hangi grupta olduğunu görebilirsin**
- **spesifik bir kullanıcının hangi gruplarda oldugunu ogrenmek icin**

> groups <userName>

- **user silmek icin deluser kullan**

> sudo deluser <userName>

- **bir kullanıcının ana dizinini silmek için**

> sudo deluser --remove-home <userName>

- **bir kullanıcıyı toptan silmek için sudo deluser**

> --remove-all-files <userName>

- **tüm kullanıcıların listesini almak için harika bir yol**

> compgen -u

- **etc/passwd ve etc/shadow şifreleri tutan linux dizinleridir. Shadow dosyasında kullanıcıların şifrelenmiş parolalarını ve SSH anahtarına sahip olup olmadıklarını görebilirsiniz**

> sudo cat /etc/shadow

- **<userName> belirtmeden direkt sudo passwd dersen root'un şifresini değiştirirsin. bir kullanıcının şifresini değiştirmek istiyosan da sudo passwd user_name demelisin. root olarak giriliysen sudo demene gerek yok.**
- **şifre değiştirmek için**

> psswd

yeni bir group oluşturma

- **grup oluşturma**

> sudo addgroup <groupName>

- **gruba kullanıcı ekleme**

> sudo adduser <userName> <groupName>

- **bir kullanıcının hangi gruplara üye oldugunu görmek icin**
  Groups <user>

> ya da

id <user>

- **getent group --> grupları görme komutu**
- **getent group group_name --> spesifik bir gruptaki userları görme**
- **groupdel g_name --> grup silme**
- **gruptan kullanıcı silme --> gpasswd --delete user_name group_name**

crontab

- **crontab ile belirlediğin bir zamanda belli bir komut, script ya da programı çalışması için programlayabilirsin. /etc/crontab'da bulunur bu komutları tutan dosya. mesela**
- **/usr/local/bin/monitoring.sh içine şunları yaz**
  #!/bin/bash
  arc=$(uname -a)
  pcpu=$(grep "physical id" /proc/cpuinfo | sort | uniq | wc -l)
  vcpu=$(grep "^processor" /proc/cpuinfo | wc -l)
  fram=$(free -m | grep Mem: | awk '{print $2}')
  uram=$(free -m | grep Mem: | awk '{print $3}')
  pram=$(free | grep Mem: | awk '{printf("%.2f"), $3/$2*100}')
  fdisk=$(df -Bg | grep '^/dev/' | grep -v '/boot$' | awk '{ft += $2} END {print ft}')
  udisk=$(df -Bm | grep '^/dev/' | grep -v '/boot$' | awk '{ut += $3} END {print ut}')
  pdisk=$(df -Bm | grep '^/dev/' | grep -v '/boot$' | awk '{ut += $3} {ft+= $2} END {printf("%d"), ut/ft*100}')
  cpul=$(top -bn1 | grep '^%Cpu' | cut -c 9- | xargs | awk '{printf("%.1f%%"), $1 + $3}') lb=$(who -b | awk '$1 == "system" {print $3 " " $4}')
  lvmt=$(lsblk -o TYPE | grep "lvm" | wc -l)
  lvmu=$(if [$lvmt -eq 0]; then echo no; else echo yes; fi)
  # net-tools araclari gerekli:
  ctcp=$(cat /proc/net/tcp | wc -l | awk '{print $1-1}' | tr '' ' ')
  ulog=$(users | wc -w)
  ip=$(hostname -I)
  mac=$(ip link show | awk '$1 == "link/ether" {print $2}')
  # Journalctl calistirilabilir cunku komut dosyasi sudo cron'dan yurutulur.
  cmds=$(journalctl _COMM=sudo | grep COMMAND | wc -l)
  wall " #Architecture: $arc
  #CPU physical: $pcpu
  #vCPU: $vcpu
  #Memory Usage: $uram/${fram}MB ($pram%) #Disk Usage: $udisk/${fdisk}Gb ($pdisk%)
  #CPU load: $cpul
  #Last boot: $lb
  #LVM use: $lvmu

#Connexions TCP : $ctcp ESTABLISHED
#User log: $ulog
#Network: IP $ip ($mac)
#Sudo: $cmds cmd"

> Uname -a —> sırasıyla şunları verir... kernel, hostname, kernel ana dağıtım bilgisi, kernel versiyon, işlemcinin mimaribilgileri, işletim sistemi bilgisi
>
> **Cpu physical -> işlemci**
>
> **vCpu —> sanal işlemci sayısı**
>
> **CPU load —> Anlık işlemci yükü/kullanımı**
>
> **Last boot —> sanal makinenin en son açıldığı an**
>
> **Connexions TCP —> ssh ile sunucuyla bağlantı kuranların sayısıFree bellek hakkında bilgi, kullanılan alan, kapasite, boş alan vs....**
>
> **Free -m : mebi byte**
>
> **Awk komutu -> grepe benzer şekilde örüntü temelli tarama işlemi**
>
> **Top -> sunucu hakkındaki anlık istatistikleri verir.**

- **cron belli zaman sürecinde bir işi otomasyona bağlamaya yarayan metoddur.**
- **00 12,15 * * * [komut-veya-script]**

> şu demektir
>
> **00 – Her Saat (00 Saat başlangıcı) 12,15 – Öğlen 12’de ve Akşam 15’de * – Her Gün * – Her Ay * – Haftanın Her Günü şu komutu çalıştır**
>
> - *** * * ***

- **@reboot bir defa ve başlangıçta.**
- **@yearly ya da @annually: Yılda bir defa (0 0 1 1 *)**
- **@monthly ayda bir defa (0 0 1 * *)**
- **@weekly haftada bir defa (0 0 * * 0)**
- **@daily ya da @midnight günde bir defa (0 0 * * *)**
- **@hourly saatte bir defa (0 * * * *)**
- **Bir crontab dosyası aşağıdaki gibi yazılır.**

> * * * * * /calıstirilacak/komut/yada/script

- **burada**
  - **birinci yıldız --> minute 0-59**
  - **ikinci yıldız --> hour 0-23**
  - **üçüncü yıldız --> day of month 1-31**
  - **dördüncü yıldız --> month 1-12**
  - **besinci yıldız --> day of week 0-6**
- **öncelikle netstat araçlarını yüklüyoruz**

> sudo apt update -y
> sudo apt install -y net-tools

- **crontab'ı açın ve cron'u kök olarak ayarlayan kuralı ekleyin.**
  sudo crontab -u root –e
  sudo crontab -e
  en alttaki # m h dom mon dow command satırını
  ***/5 * * * * bash /usr/local/bin/monitoring.sh olacak şekilde ayarla**

> böylece her 5 dakikada bir bilgi gelecek ekrana.

- **monitoring.sh'a parola istememesi için**

> sudo visudo
> user_name ALL=(ALL)NOPSSWD: /usr/local/bin/monitoring.sh ekliyoruz
> sudo reboot
> sudo bash /usr/local/bin/monitoring.sh --2> çalıştırıyoruz

- **Savunmada sorulacak crontab servisini durdurma ve yeniden başlatma: Durdurmak için:**

> sudo service cron stop
>
> **Başlatmak için:**
>
> **sudo service cron start**

- **Bir listeyi belirtmek için virgül (,) kullanılır, örneğin 1,4,6,8, yani 1,4,6,8'de çalıştırılır.**
- **Aralıklar bir tire (-) ile belirtilir ve listelerle birleştirilebilir, örneğin 1-3,9-12 yani 1 ile 3 ve ardından 9 ile 12 arasında anlamına gelir.**

- **Karakter /bir adımı tanıtmak için kullanılabilir, örneğin 2/5'ten başlamak, ardından her 5'te bir (2,7,12,17,22...). Sonunu sarmazlar.**
- **Bir alandaki yıldız işareti (*), o alan için tüm aralığı belirtir (örneğin 0-59, dakika alanı için). Aralıklar ve adımlar birleştirilebilir, örneğin */2 ilgili alan için minimumdan başlamayı ve ardından her 2'de bir, örneğin dakikalar için 0 (0,2...58), aylar için 1 (1,3 ... 11) vb.**
- **https://crontab.guru/**

sanal makineler nasıl çalışır

- **sanal makineler bilgisayarın varolan donanımlarını kısmi olarak paylaşarak varolan sistemin sanal bir taklidini yaratırlar. bunu da hypervisor adlı bir program sayesinde yapar.**
- **kullanım alanları**
  - **yeni os denemeleri**
  - **mevcut os yedekleme**
- **vm'nin avantajları**
  - **çeviklik ve hız**
  - **maliyet**
  - **güvenlik**
- **debian centOs farkı**
  - **debian çoklu mimari destekliyor centOs desteklemiyor**
  - **centOs redhat debian debiancılar tarafından destekleniyor**
  - **centOs daha karmaşık ve komplike**
  - **debian'da sayısız paket vardır centOs sınırlıdır.**
  - **centOs daha çok iş için kullanılan bir distrodur**
- **debian paket yöneticisi apt'dir Centos'un yum.**
- **apt - advanced packaging tool. yazılım yüklemeye yarayan bir yazılımdır.**
- **Aptitude, işlevselliğe bir kullanıcı arabirimi ekleyen, böylece bir kullanıcının etkileşimli olarak bir paket aramasına ve yüklemesine veya kaldırmasına izin veren gelişmiş paketleme aracının ön ucudur. İlk olarak Debain için oluşturulan Aptitude, işlevselliğini RPM tabanlı dağıtımlara da genişletiyor. (RPM = RedHat Package Manager yani Redhat Paket yöneticisi anlamına gelmektedir.) Aptitude işlevselliği apt- get'den daha geniştir. aptitude alt-paketleri de indirirken apt indirmez. aptitude outdated paketlerin takibini yapar, apt yapmaz.**
- **SELinux (Security-Enhanced Linux) Linux' da zorunlu erişim denetimi (MAC) mekanizmasına gerçekleşmesini sağlayan bir projedir.**
- **SELinux'un 3 modu vardır. Bunlar:**

> enforcing: Kaynaklara erişimin SELinux politikasına göre belirlendiği moddur.
>
> **permissive: Bu modda erişimler SELinux politikası zorlanmaz. Ancak erişim politikasına uymayan durumlar bir günlük dosyasına yazılır. (Redhat’te /var/log/audit/audit.log dosyasına varsayılan olarak yazılır)**
>
> **disabled: SELinux tamamen devre dışıdır. Sadece DAC kuralları geçerlidir.**

- **appArmor ise çok daha basit bir güvenlik protokolüdür. Arka planda sessizce çalışır. Sisteme zarar verebilecek ayarları, servisleri ve diğer ayarları kontrol edip sınırlandırır. Sistem açılışlarında default olarak aktiftir.**
- **SELinux ve APPArmor arasındaki fark? "Bu güvenlik sistemleri, uygulamaları birbirinden yalıtmak için araçlar sağlar ve bir uygulamanın güvenliği ihlal edildiğinde bir saldırganı sistemin geri kalanından yalıtır. SELinux kural kümeleri inanılmaz derecede karmaşıktır ancak bu karmaşıklıkla süreçlerin nasıl izole edildiği üzerinde daha fazla kontrole sahip olursunuz. Bu ilkelerin oluşturulması otomatikleştirilebilir. Bu güvenlik sistemine karşı bir grev, bağımsız olarak doğrulamanın çok zor olmasıdır. AppArmor (ve SMACK) çok basittir.**
- **pushlamadan önce user42 olusturdugunuzdan ve kullanicinin ona üye oldugundan emin olun...**

EVALUATION

- **.vdi numarası kontrol et**

> yapman gereken b2br reposuna signature.txt içinde sanal makinenin .vdi kodunu atamaktır. bunun için makinenin dizininde shasum b2broot.vdi deyip cıkan sayıyı .txt'e at ve sonrasında git add/commit/push. bu iki sayi birebir aynı olmalıdır.

- **sanal makineye giriş yapın**
- **kullanıcı parolası uygun mu değil mi diye kontrol edin**

> chage -l bkaramol

- **ufw kontrolü yap**

> sudo systemctl status ufw
>
> **ufw'nin izinlerine bakmak istiyosan da**
>
> **sudo ufw status numbered**

- **ssh kontrolü yap**

> sudo systemctl status ssh

- **OS kontrolü yap**

> uname -a

- **user kontrolü yap**

> id bkaramol
>
> **bütün kullanıcıların listesini görmek için /etc/passwd gitmelisin**
>
> **cut -d: -f1 /etc/passwd**

- **yeni kullanici olustur**

> sudo adduser bkaramol2

- **yeni kullanıcının parolasını değiştir**

> passwd bkaramol2

- **şifre politikalarını nası belirledin?**

1) sudo vim /etc/login.defs (max/min/warn_days ayarladim)

2) sudo /etc/security/pwdquality.conf (difok= vs. ayarladim)

- **evaluating isimli yeni bi grup olustur**

> sudo addgroup evaluating

- **yeni kullanıcıyı bu gruba ata**

> sudo adduser bkaramol2 evaluating

- **yeni kullanıcı atanmıs mı kontrol et**

> groups bkaramol2 (ya da)
>
> **id bkaramol2**

- **şifre politikasının avantaj ve dezavantajlarını anlat**

> güvenlik cart curt

- **makinenin server adına bak**

> hostname

- **makinenin adını değiştir**

> 1) sudo hostnamectl set-hostname new_name
>
> **2) sudo vim /etc/hosts'ta da değiştir**
>
> **3) reboot**

- **diskleri göster**

> lsblk
> SDA ilk diski temsil eder. Sonraki blok cihaz bölümleri sda’nın yanında ondalık sayı alarak gösterilir.
>
> **sr0: çıkarılabilir cihazı temsil eder. CD/DVD olan.**
>
> **Cd - rom. Listelenen cihazlar içinde çıkarılabilir olup olmayanaları gösteren bölüm “RO”dur. (RO = removable) RO = 0 ise çıkarılamaz block device RO = 1 ise çıkarılabilir block device sda birincil cihazdır**
>
> **sda(1-4) arası primary diskleri temsil ederken Sda4 sonrası logical birimler olduklarını gösterir.**
>
> **mountpoint = Bu, cihazın monte edildiği bağlama noktasını görüntüler.**

- **yeni kullancıyı sudo'ya atayıp kontrol et**

> 1) sudo adduser bkaramol2 sudo
>
> **2) id bkaramol2**

- **sudo visudo ile yazdıklarını anlat**
- **sudo komutlarının kayıtlarının tutuldugu /var/log/sudo/sudo.log'un calıstıgını kontrol et**

> cd /var/log/sudo
>
> **sudo cat sudo.log**

- **yeni bir porta izin ver**

> sudo ufw allow/deny 8080

- **yeni port iznini sil**

> sudo ufw delete 8080
>
> **ya da numbered diyip numarasını sil**

- **ssh kontrolü yap**

> sudo vim /etc/ssh/sshd_config
>
> **1) nopermitlogin no olmalı**
>
> **2) port 4242 olmalı**
>
> **3) sudo systemctl status ssh --> enabled/active olmalı**
>
> **değilse**
>
> **4) sudo ssh enable**

- **ssh nedir?**

> Linux sunuculara erişim sağlamak için SSH protokolü kullanıyoruz. SSH, also known as Secure Socket Shell, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network. Yani uzaktaki bir sunucuya bağlanmak, ona komutlar ve dosyalar göndermek üzere kullanılan şifrelenmiş bir uzaktan bağlantı sağlayıcı protokolüdür.Diğer önemli değişiklik port değişikliğidir. SSH bağlantısının portu varsayılan olarak 22'dir. Portu değiştirerek saldırganların 22 portundan sunucuya erişimini engelleyeceğiz. (Biz de 4242 portundan bağlanarak güvenli bir SSH bağlantısı oluşturmaya çalışıyoruz).

- **iTerm'den ssh'a bağlan**

> ssh bkaramol@127.0.0.1 -p 4242

- **monitoring.sh açıkla**

sort → alfabetik sıralar

uniq → tekrar eden satırları ayırır.

$1,$2 → sutünları tutar

xargs → öncesinde kullanılan çıktıyı bir sonraki komuta iletir.

arc -> mevcut işletim sisteminin mimarisini ve kernel versiyonunu gösterir

pcpu-> fiziksel işlemci sayısı

vcpu-> sanal işlemci sayısı

fram -> sunucunun erişilebilir ram miktarı

uram -> kullanılan ram miktarı

pram -> yüzde olarak kullanılan miktarı verir

fdisk -> sunucunun erişilebilir depolama alanı

udisk -> sunucunun kullanılan depolama alanı

pdisk-> diskin yüzde olarak kullanımını verir

cpul -> yüzde olarak işlemci kullanım oranını verir.

lb -> son yeniden başlatma tarihi ve saati (last boot)

lvmt -> LVM ile yapılandırılmış diskin bilgisini verir.

lvmu-> LVMnin aktif olma bilgisini verir

ctcp-> mevcut aktif bağlantı sayısı

ulog-> sunucuyu kullanan kullanıcı sayısı

ip -> sunucu ip adresi verir

mac-> sunucu mac adresi verir

cmds-> sudo ile çalıştırılmış komut sayısı

Cpu physical -> işlemci

vCpu → sanal işlemci sayısı

CPU load → Anlık işlemci yükü/kullanımı

> **Last boot → sanal makinenin en son açıldığı an**
>
> **Connexions TCP → ssh ile sunucuyla bağlantı kuranların sayısı**
>
> **Free bellek hakkında bilgi, kullanılan alan, kapasite, boş alan vs…. Free -m : mebi byte**
>
> **Awk komutu -> grepe benzer şekilde örüntü temelli tarama işlemi**
>
> **Top -> sunucu hakkındaki anlık istatistikleri verir.**

- **cron nedir?**

> belirli işlerin belirli zamanlarda tekrarlanarak yapılmasını bir otomasyona bağlayarak kolaylaştırır. Bir görevin ilerleyen zamanda tekrarlamak için komut verme işlemine cron denir.

- **cron'u nası kurdun?**

> 1) crontab -u root -e
>
> **2) */10 * * * * bash /usr/local/bin/monitoring.sh**
>
> **her 10 dakikada bir .sh komutunu calıstır.**

- **cron baslat/durdur**

> 1) sudo service cron stop
>
> **2) sudo service cron start**
>
> **3) sudo systemctl disable cron**
>
> **4) reboot**

- **ide, ssci, sata**
- **LVM nedir. logical volume manager. LVM disk bölümlendirme metodudur. bu sayede bilgisayarın sadece belli bir kısmını sanal makineye ayırabilirsin, dinamik boyutlu olan bu hafıza yerlerini arttırıp azaltabilirsin. physical/logical volume'lerden oluşur. bu ikisi birleşerek voluma group'u oluşturur. yani bir disk bölümlendirme tekniği olan LVM sayesinde disk alanını resetlemeden büyültebilir ya da küçültebilirsin.**