born2beroot

ek kaynak https://42resources.github.io/2022/02/23/Born2beroot

ek kaynak 2 https://www.youtube.com/watch?v=2w-2MX5QrQw&feature=youtu.be

sudo (root moduna geçmek için kullanılır)

apt-get (debian tabanlı linux dağıtımlarındaki paket yöneticisinin adıdır)

sudo apt-get update

sudo apt-get upgrade

---

kullanıcıyı bir gruba eklemek için kullanılır burada kendimizi sudo grubuna ekliyoruz

usermod -aG sudo username

-G, --groups için bir kısayoldur: usermod'a @ bir sonraki argümanın bir grup olduğunu söyler. Burada büyük harf -G kullanmanız gerektiğini unutmayın, çünkü kullanıcının birincil grubunu değiştirmek istemiyoruz, ancak kullanıcının ait olduğu ek grupların listesini değiştirmek istiyoruz.

-a --append için bir kısayoldur: Grubu, kullanıcının ait olduğu gruplar listesine eklemek anlamına gelir.

Birincil ve tamamlayıcı gruplar

Usermod kılavuz sayfasına göz attığınızda, kullanıcının ek gruplar listesine bir grup ekleyen -G ve bir kullanıcının birincil grubunu değiştiren -g olduğunu göreceksiniz.

Pragmatik cevap şudur: Sormanız gerekiyorsa, her zaman -G kullanmanız gerekir.

Deneyimlerime göre, bir kullanıcının birincil grubunu değiştirmek zorunda kalmak son derece nadirdir. Varolan birincil grupların amacı, temel olarak, bir dosya oluşturursanız,

Linux'un varsayılan olarak hangi gruba ait olduğunu bilmesi gerektiğidir (yani, açıkça bir grup belirtmezseniz.

getent group sudo ile sudo grubundaki kullanıcıları görebiliriz

---

bu bölümde ***sudo visudo*** komutunu kullanarak sudo yetkisine sahip bir kullanıcının hangi yetkilere sahip olacağını belirtiyoruz. Kendimize tüm yetkileri vereceğiz.

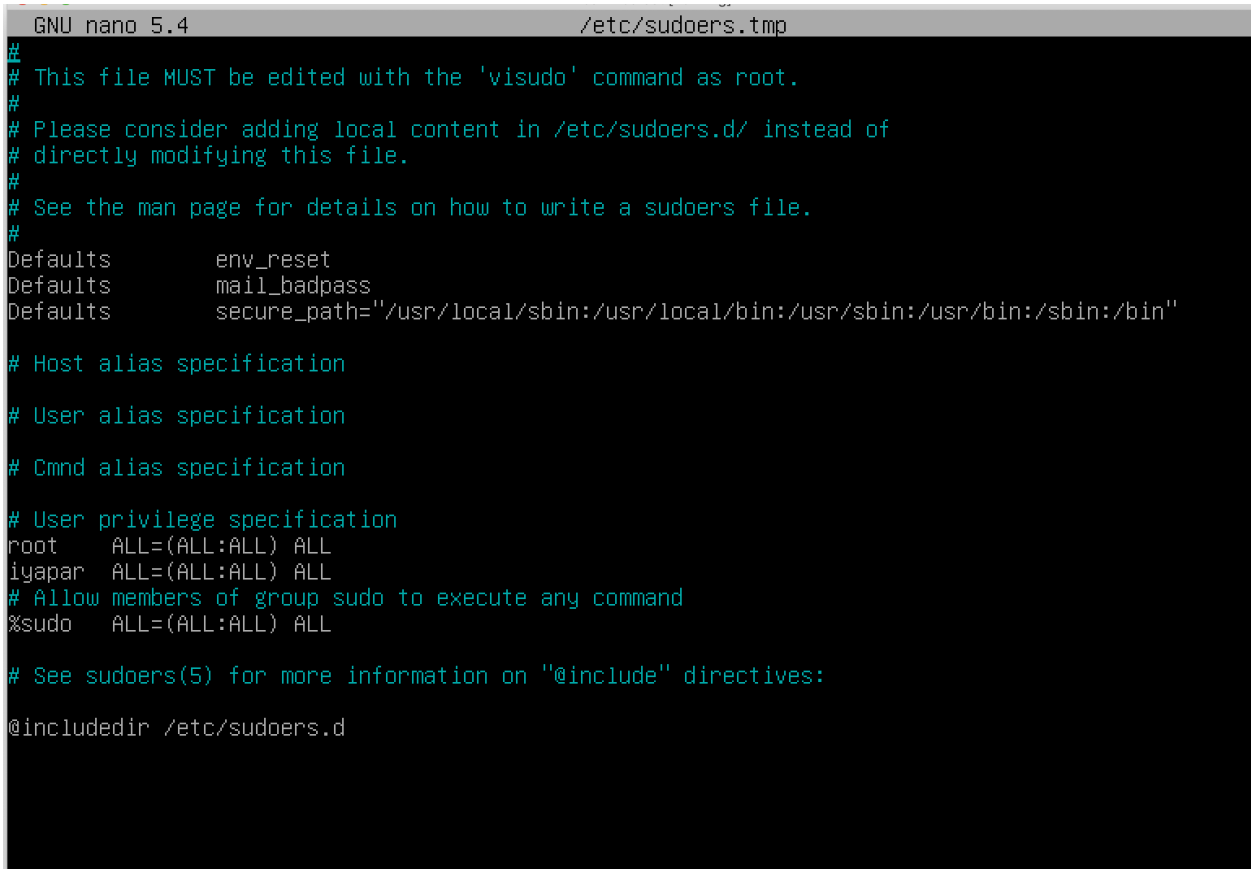
Kullanıcı **%** ile başlarsa , bir grubun adı olarak yorumlanır ve yönerge o gruptaki tüm kullanıcılar için geçerlidir. Böylece " **%admin ALL=(ALL) ALL** " satırı, grup **yöneticisine** ait herhangi bir kullanıcının herhangi bir kullanıcı veya grup olarak herhangi bir komutu çalıştırmasına izin verir.

Özel ALL kelimesi bu değerlerden herhangi biri için kullanılabilir ve herhangi birine izin verildiği anlamına gelir.

Burada " **root ALL=(ALL:ALL) ALL ", herhangi bir ana bilgisyar adında** oturum açan **root** kullanıcısının herhangi bir kullanıcı veya grup olarak herhangi bir komutu çalıştırabileceğini belirtir . Bu direktifin genel şekli şöyledir:

```
user hostname=(runas-user:runas-group) command
```

Özel ALL kelimesi bu değerlerden herhangi biri için kullanılabilir ve herhangi birine izin verildiği anlamına gelir.



Git'i yükleme

apt-get update -y

apt-get upgrade -y

apt-get install git -y

git --version ile git'in versiyonunu kontrol edebilirsiniz

sudo apt-get install wget

(wget, web depolarından dosya indirmek için ücretsiz ve açık kaynaklı bir araçtır.)

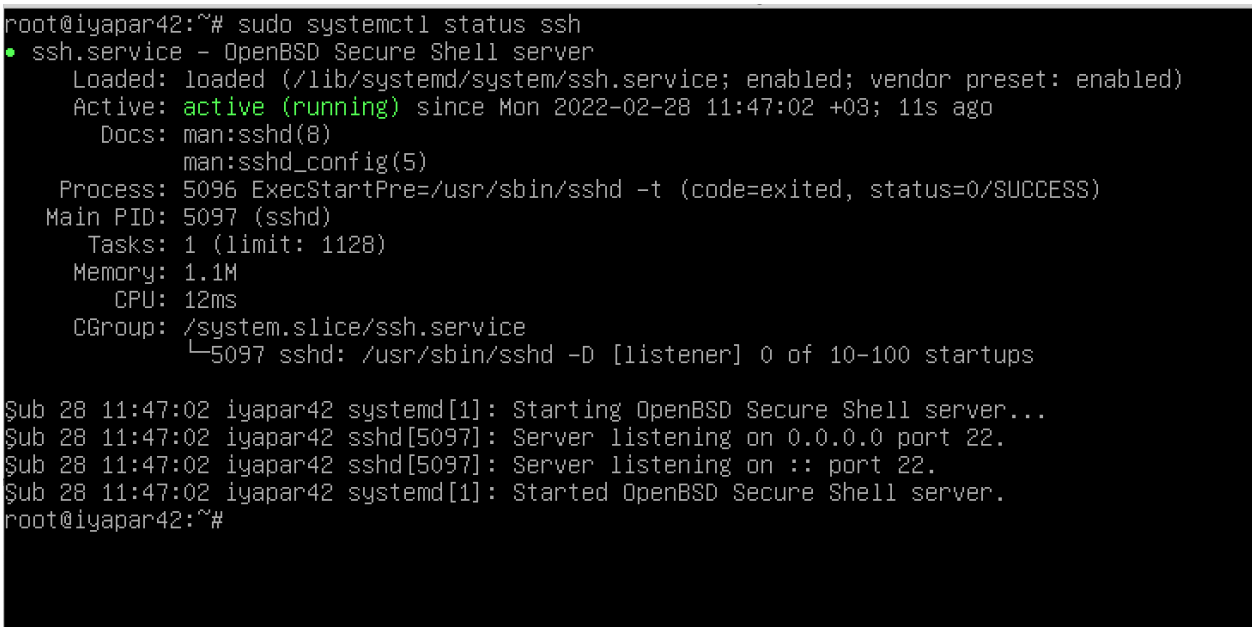
sudo apt-get install vim

(vim'i indiriyoruz.)

SSH yükleme ve SSH hizmetini yapılandırma

`sudo apt install openssh-server`

SSH serveri yükledikten sonra durumunu ***sudo systemctl status ssh*** komutu ile kontrol edebiliriz



sudo service ssh restart ile ssh'ı tekrardan tekrardan başlatıyoruz

ssh portunu 22 den 4242 ye çeviriyoruz bunun için : ***sudo vim /etc/ssh/sshd_config***

not : # Port 22 olarak gözükecektir başındaki # işaretini silmelisiniz ki yorum satırından çıksın

bunun sebebi ssh'ın varsayılan portu 22 dir Varsayılan SSH bağlantı noktasını değiştirmek ve birisinin tahmin bile edemediği bir şeye ayarlamak her zaman iyidir, bu da sisteminizi olağan saldırı girişimlerinden kurtaracaktır.

```
#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 4242
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:
```

Bağlantı noktası ayarlarının doğru olup olmadığını kontrol edin

sudo grep Port /etc/ssh/sshd_config

En basit ifadeyle, grep (global regular expression print), bir arama dizesi için giriş dosyalarını arayan ve onunla eşleşen satırları yazdıran küçük bir komut ailesidir.

burada ssh servisini tekrardan yeniden başlatmalıyız ***sudo service ssh restart***

UFW'yi yükleme ve yapılandırma

Karmaşık Güvenlik Duvarı,(UFW) kullanımı kolay olacak şekilde tasarlanmış bir netfilter güvenlik duvarını yönetmek için kullanılan bir programdır.

apt-get install ufw komutu ile ufw'yi kuruyoruz.

ufw version ile kontrol edebilirsiniz.

sudo ufw enable ile ufw'yi etkinleştiriyoruz

sudo ufw status numbered ile aktiflik durumunu kontrol edebilirsiniz

şimdi ise kuralları yapılandıracağız ***sudo ufw allow ssh*** (bu komut ile ufw ssh portundan gelen trafiğe standart trafiğe izin verir yani 22 portuna alt kısımda onları silmeyi gösterdim.)

şimdi ise kendi ayarladığımız 4242 ssh portunu izinlere ekleyeceğiz.

bunun için ***sudo ufw allow 4242*** komutunu kullanıyoruz

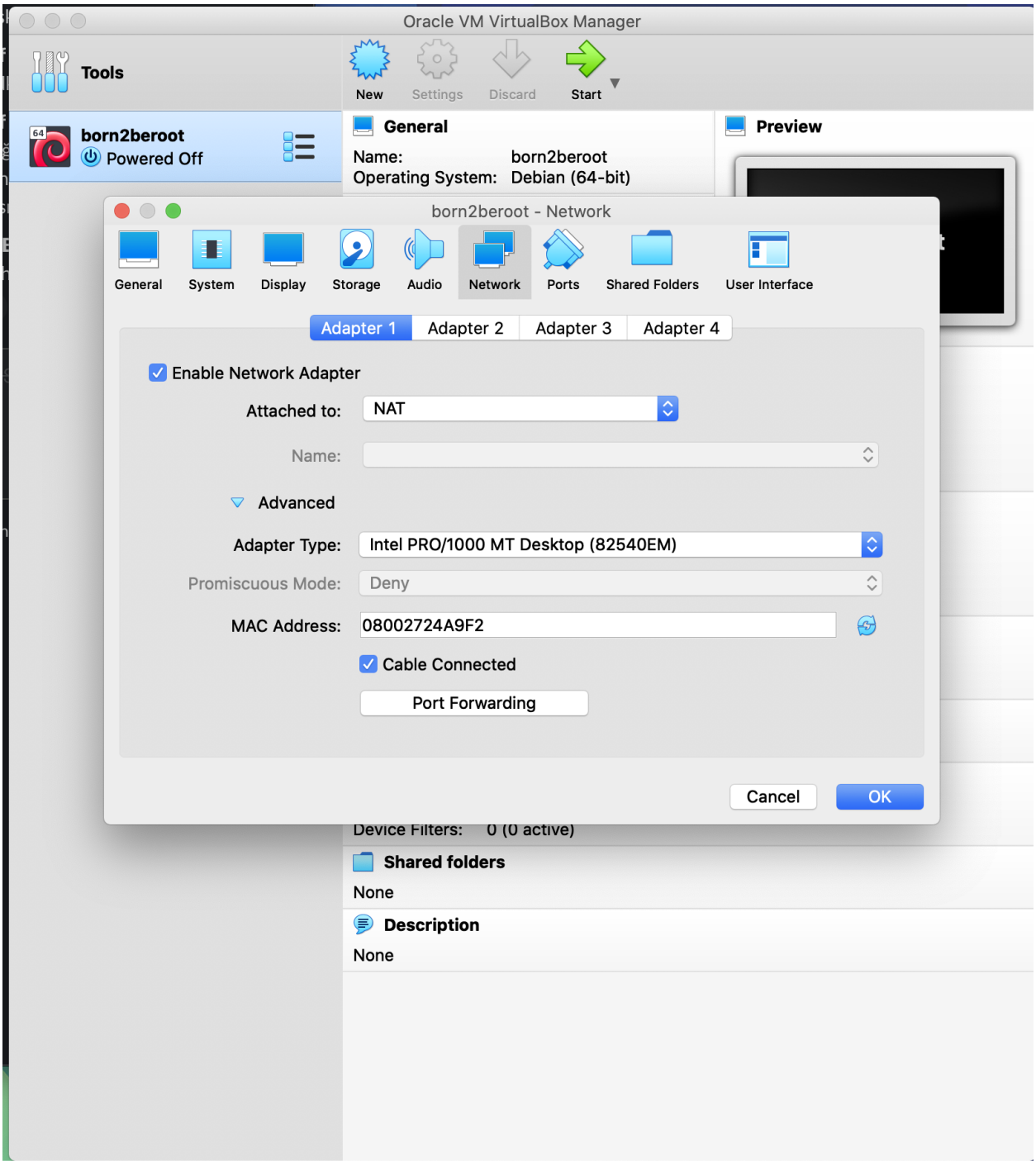
```
root@iyapar42:~# sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
4242                       ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
4242 (v6)                  ALLOW       Anywhere (v6)

root@iyapar42:~#
```

sudo ufw status kısmında 22 portundan gelen tcp/ip trafiğine de izin veriliyorsa bunu silmemiz gerek ***sudo ufw status numbered*** yazarak 22 portundan gelen tcp ve v6'nın kaç numarada olduğuna bakın

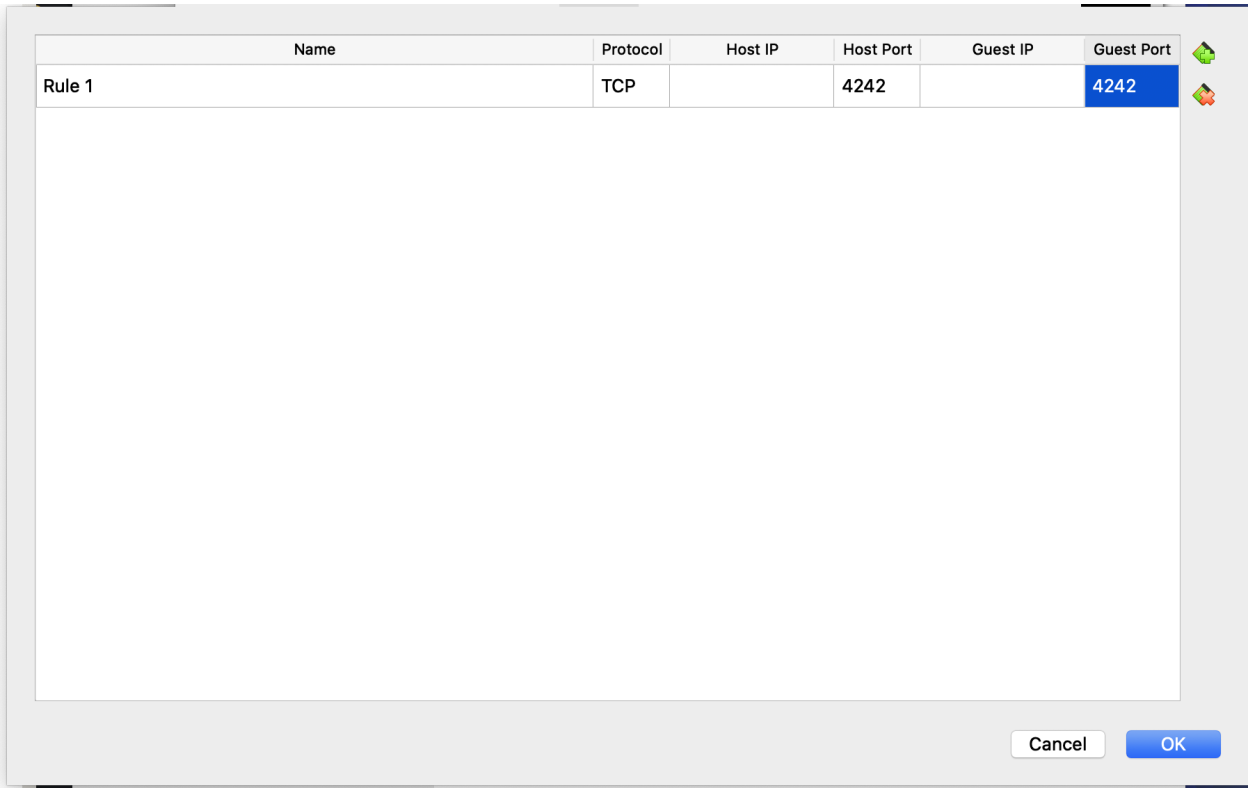
sonrasında ise ***sudo ufw delete numara*** ile 22 portlarını silin eğer yanlış bir işlem yaparsanız tüm trafiği silin ve ***sudo ufw allow ssh*** ve ***sudo ufw allow 4242*** yi

tekrardan yazarak silme işlemini tekrardan yapın

şimdi ise sanal makinayı KAYDEDİP çıkış yapın ve ayarlar kısmından network kısmına gelin



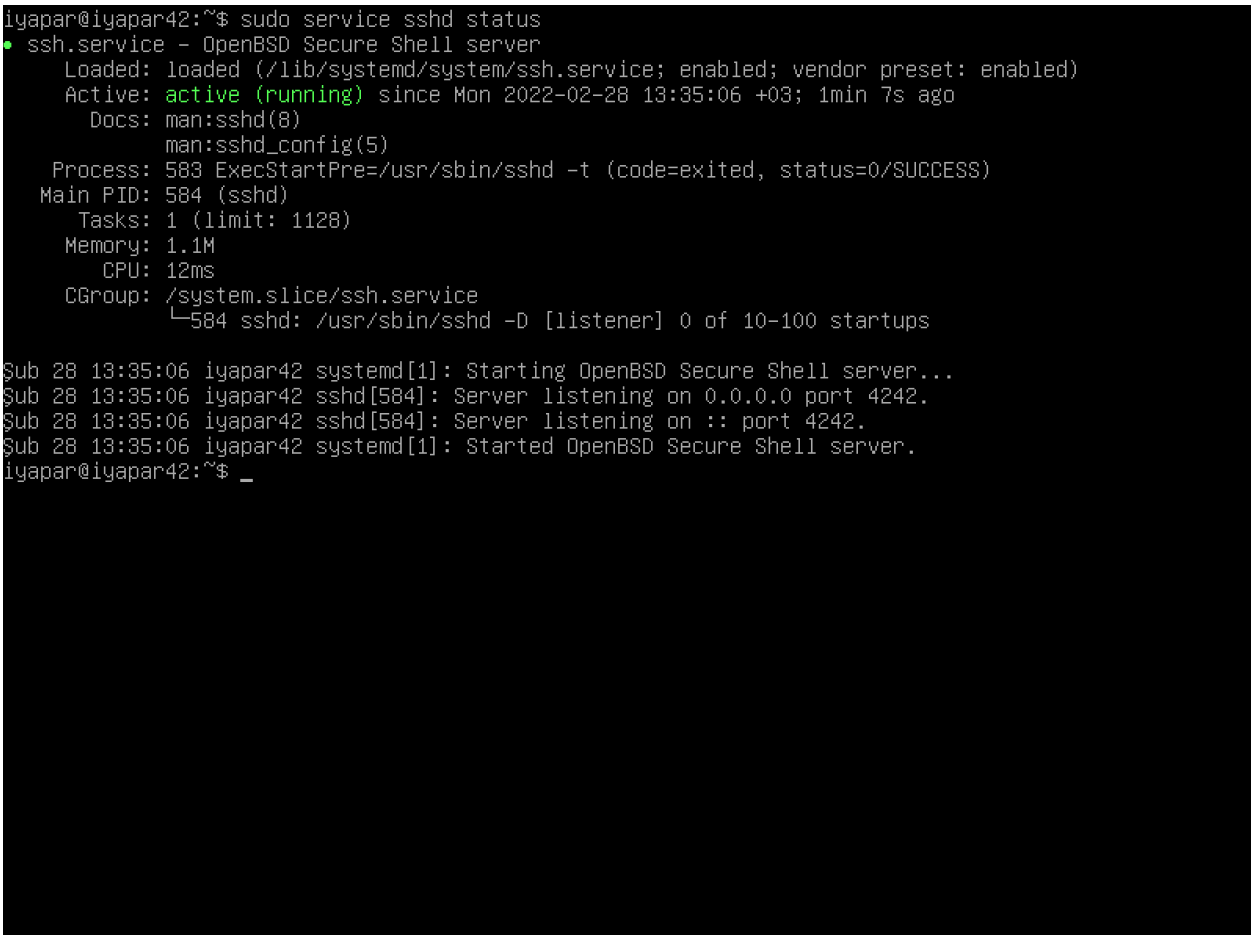
sonrasında ise sağdaki yeşil + tuşuna basarak host port ve guest port kısmını 4242 yapıp kaydedip çıkın



bu işlemlerden sonra sanal makinayı çalıştırıp ***sudo systemctl restart ssh*** komutunu girip ssh'ı yenileyin

bu işlemleri yapmamızın sebebinin normal iterm'de ***ssh your_username@127.0.0.1 -p 4242 komut satırıyla serverimize terminalden 4242 portu ile bağlanabilmek için olduğunu düşünüyorum tam emin değilim***

sudo service sshd status ile kontrol edebilirsiniz



sonrasında ise iterm'e ssh your_username@127.0.0.1 -p 4242 yazarak sanal sunucunuza terminalden bağlanabilirsiniz.

eğer bağlanma sırasında ssh satırı alırsanız bilgisayarınızın ssh id'si değişmiş demektir onu sıfırlamak için iterm'de ***rm .ssh/known_hosts*** komutunu giriniz sorununuz çözülmüş olacaktır

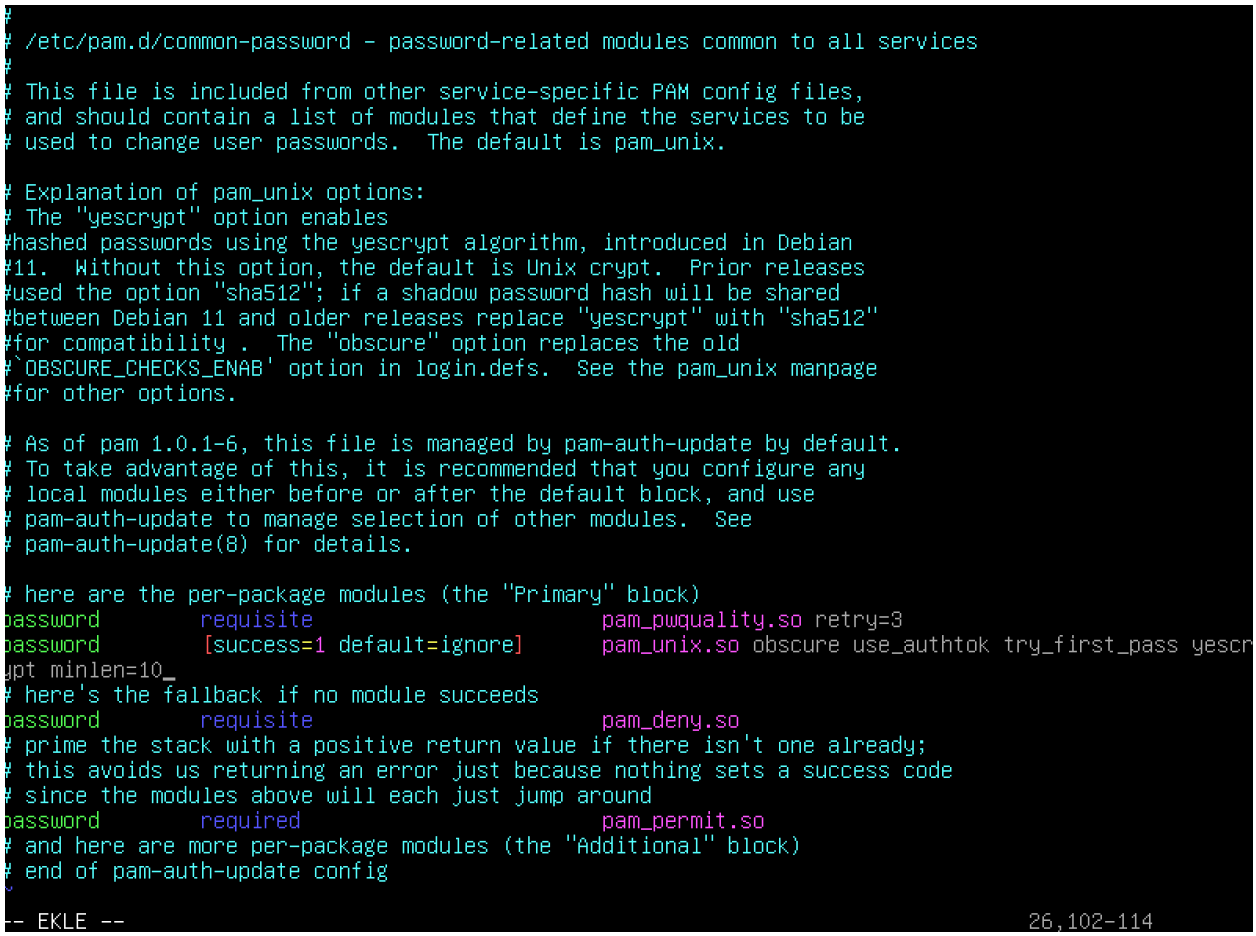
---

PASSWORD QUALITY

pdf'de belirlenen şifre belirleme politikalarını uygulamak için ***sudo apt-get install libpam-pwquality*** komutu ile bir kütüphane indiriyoruz bu kütüphane ile şifre belirleme politikalarını uygulayacağız.

sudo vim /etc/pam.d/common-password ile bu yere gidin ve succes=1 olan yerin en sonuna fotoğrafta'da göründüğü gibi minlen=10 ekleyin bunun sebebi bir kullanıcı şifre

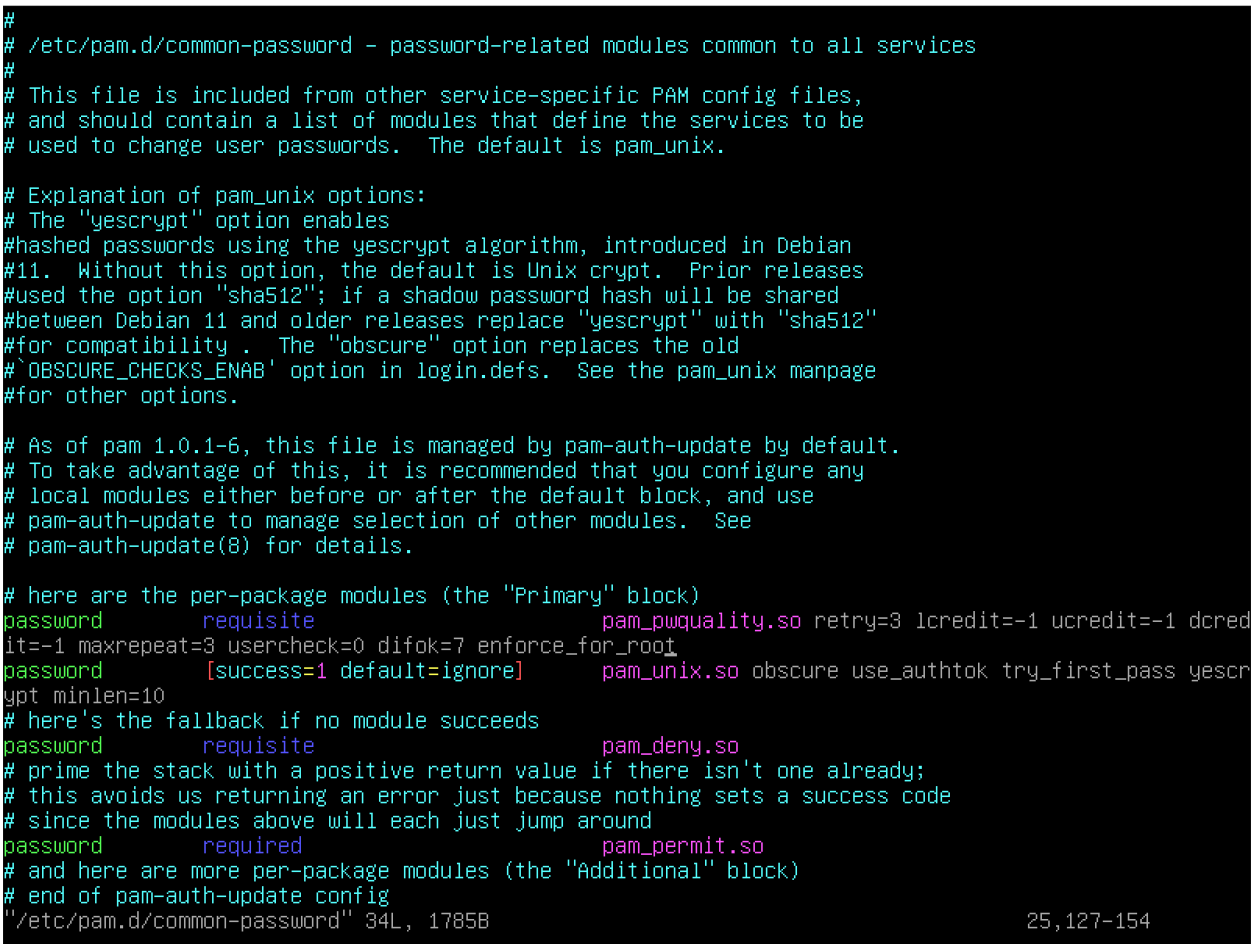
belirlerken minimum 10 karakter olması gereksinimi içindir.



password requisite pam_pwquality.so retry=3 kısmını bulun ve bunları ekleyin **lcredit =-1**

ucredit=-1 dcredit=-1 maxrepeat=3 usercheck=0 difok=7 enforce_for_root

bu şekilde görünmelidir



sırasıyla en az bir küçük harf en az bir büyük harf en az bir rakam en fazla aynı harften üç tekrar parolanın kullanıcı adını bir içerip içermediği eski şifrenin en az 7 karakter yeni şifreden farklı olması gerektiği force_for_root root kullanıcıları için de aynı kuralların geçerli olduğu şifre belirleme politikaları bunlardır. -1 en az anlamına gelir.

şimdi ise şifrenin kaç günde bir değiştirilmesi gerektiği kuralını değiştireceğiz yukarıdaki kuralları kaydedip çıkın ve ***sudo vim /etc/login.defs*** komutunu çalıştırın.

PASS_MAX_DAYS 9999 (bir şifreyi en fazla x gün kullanabilirsiniz.)

PASS_MIN_DAYS 0 (şifre değişiklikleri arasında izin verilen minimum gün sayısı.)

PASS_WARN_AGE 7 (şifre değiştirme süresi gelmeden en az x gün önceden bildirim verir.)

bu satırı bulun ve

30

2

7

olarak değiştirin

sonrasında ise ***sudo reboot*** ile sistemi yeniden başlatın.

---

grup oluşturma

sudo groupadd user42

sudo groupadd evaluating

2 grup oluşturuyoruz ve diğerinin adı user42 olacak pdf de böyle belirtiyor.

getent group ile kontrol edebilirsiniz.

tüm yerel kullanıcılara bakmak için

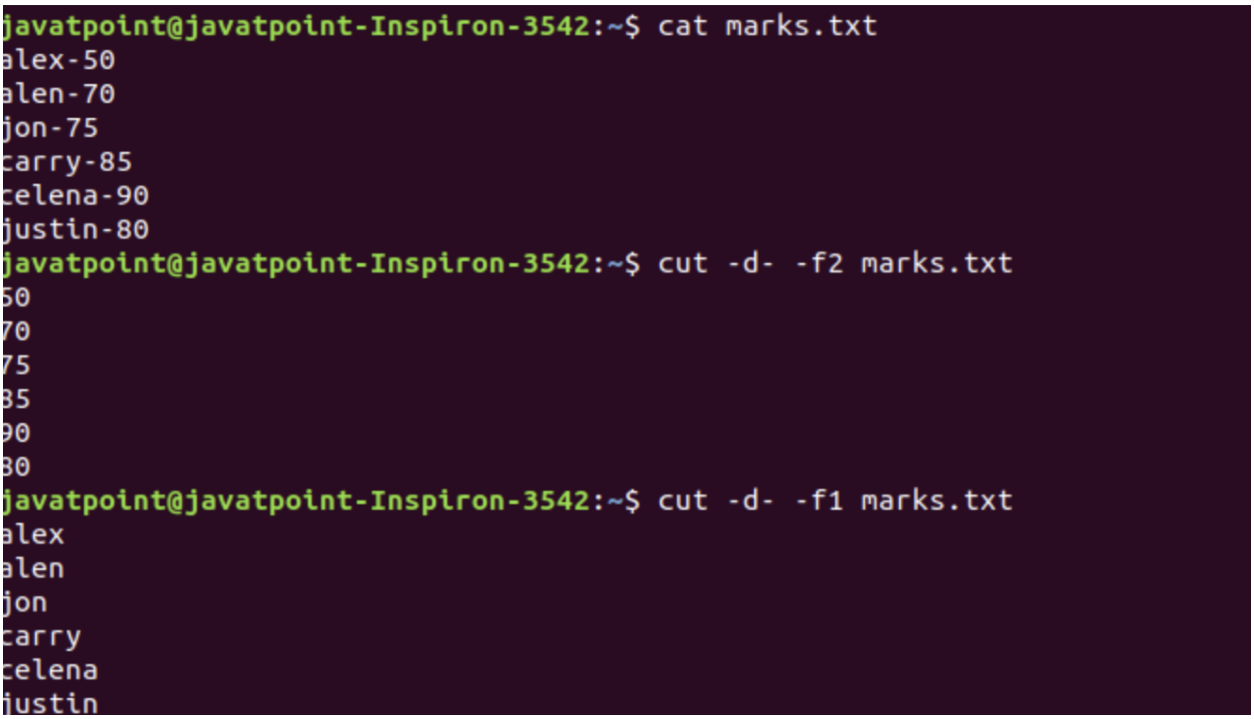
cut -d: -f1 /etc/passwd komutunu kullanabilirsiniz

Linux cut komutu, bir dosyanın belirli bir sütununu seçmek için kullanışlıdır. Belirli bir bölümü bayt konumuna, karaktere ve alana göre kesmek için kullanılır ve bunları standart çıktıya yazar. Bir satırı keser ve metin verilerini çıkarır. Onunla bir argüman iletmek gerekir; aksi takdirde bir hata mesajı verecektir.

Belirli bir bölümü kesmek için sınırlayıcıyı belirtmek gerekir. Bir sınırlayıcı, bölümlerin bir metin dosyasında nasıl ayrılacağına karar verir. Sınırlayıcılar boşluk (' '), kısa çizgi (-), eğik çizgi (/) veya başka bir şey olabilir. '-f' seçeneğinden sonra sütun numarası belirtilir.

d, --delimiter=DELIM: Bir sınırlayıcı ile belirli bir bölümü kesmek için kullanılır.

f1 1. sütunu f2 ise 2. sütunu göstermek için kullanılır



sudo adduser new_username *ile yeni bir kullanıcı oluşturuyoruz*

"Değerlendirme" grubuna bir kullanıcı atayın (Bu, savunma yaptığınız zaman içindir)

sudo usermod -aG user42 your_username

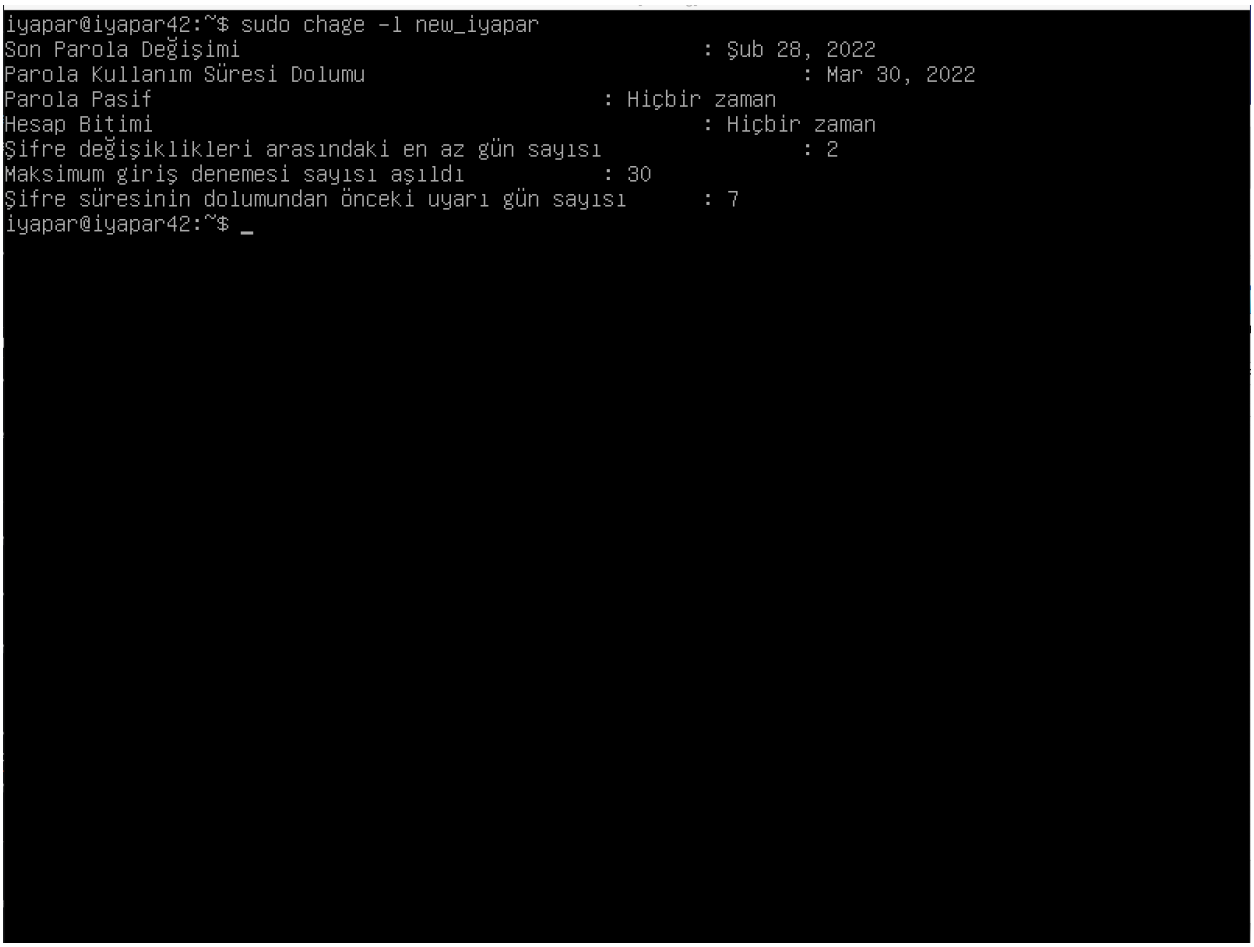
sudo usermod -aG evaluating your_new_username

bu şekilde de kontrol edebilirsiniz

getent group user42

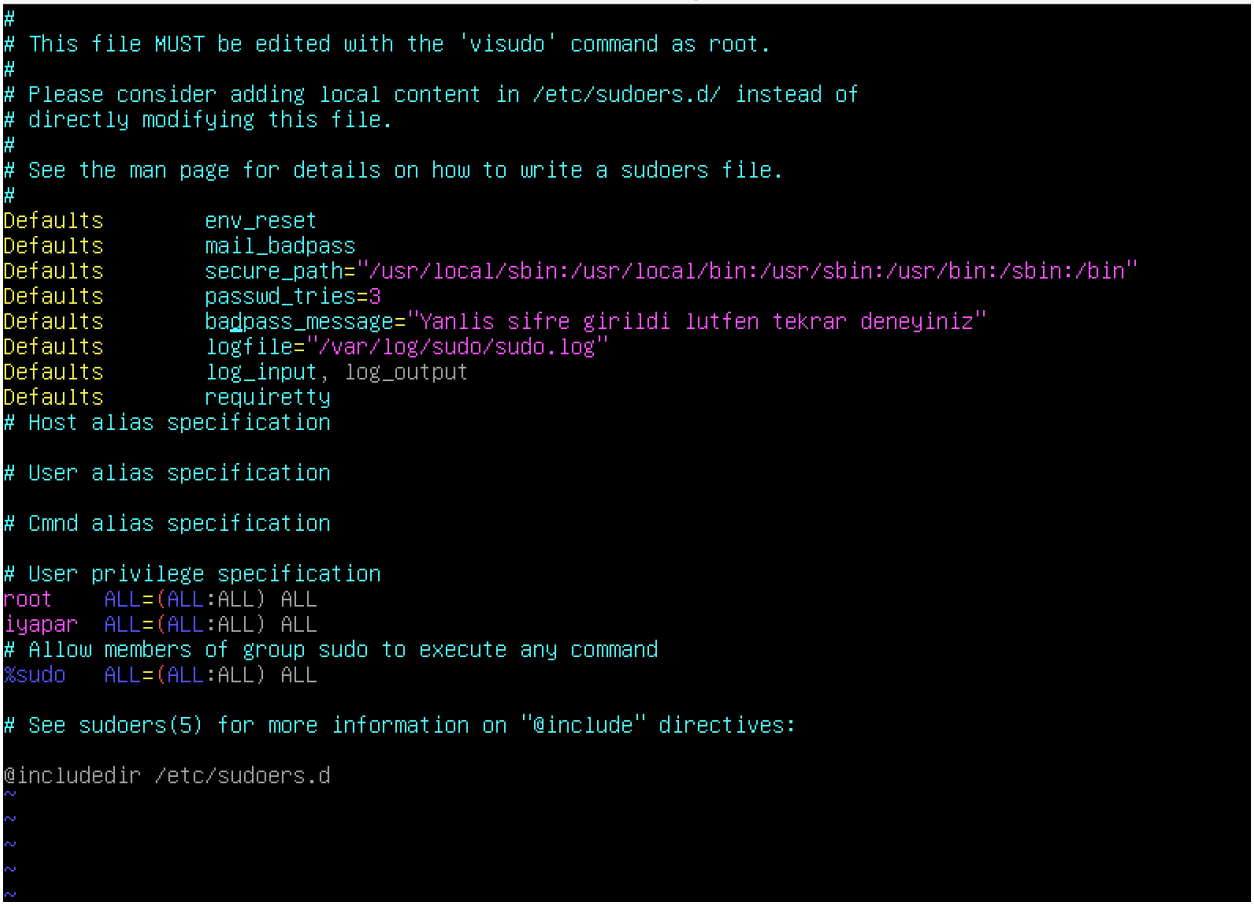
getent group evaluating

sudo chage -l new_username ile yeni oluşturduğunuz kullanıcının şifre politikasını kontrol edebilirsiniz bunu daha önceden değiştirmiştik -l varsayılan değerler ile direkt ekrana bastırır -l koymazsanız bu değerleri değiştirebilirsiniz.



sudoers grubunu yapılandırma

sudo vim /etc/sudoers bu yere gidin



sırasıyla default olarak secure_path'in altına bunları ekleyin

secure_path : olan kısım Güvenlik nedeniyle sudo tarafından bu yollara ulaşılamaz.

passwd_tries : maksimum 3 yanlış şifre denemesi yapılabilir.

baspass_message : yanlış şifre girilmesi durumunda ekrana gelecek hata mesajı.

logfile : sudo komutu her kullanıldığında bu yerde log kayıtları tutulacak eğer böyle bir .log dosyasını o yere gidip kendiniz oluşturmalısınız ***sudo /var/log/sudo touch sudo.log***

log_input log_output : bir komutun giriş ve çıkış akışlarının günlüğe kaydedilmesini sağlar.

requiretty : sudo , cronjobs veya web sunucusu eklentileri gibi arka plan programlarından veya diğer bağımsız işlemlerden kullanılmasını önler.

Ana bilgisayar adını değiştir (!!!Bu, savunduğunuz zaman içindir!!!)

Mevcut ana bilgisayar adını kontrol edin ***hostnamectl***

ana bilgisayar adını değiştir ***sudo vim /etc/hosts***

old_hostname'yi new_hostname ile değiştirin:

```
127.0.0.1 yerel ana bilgisayar
127.0.0.1 yeni_ana bilgisayar adı
```

sonrasında ise ***sudo reboot*** ile yeniden başlatın ve ***hostnamectl*** ile kontrol edin.

Crontab yapılandırması

crontab yapılandırması ne anlama gelir ?

crontab , düzenli bir programda çalıştırmak istediğiniz komutların bir listesi ve ayrıca bu listeyi yönetmek için kullanılan komutun adıdır. Crontab, "cron tablosu" anlamına gelir, çünkü görevleri yürütmek için iş zamanlayıcı *cronunu kullanır; cron* , belirli bir programa göre görevleri sizin için otomatik olarak gerçekleştirecek sistem sürecidir.

netstat araçlarını yükleyin

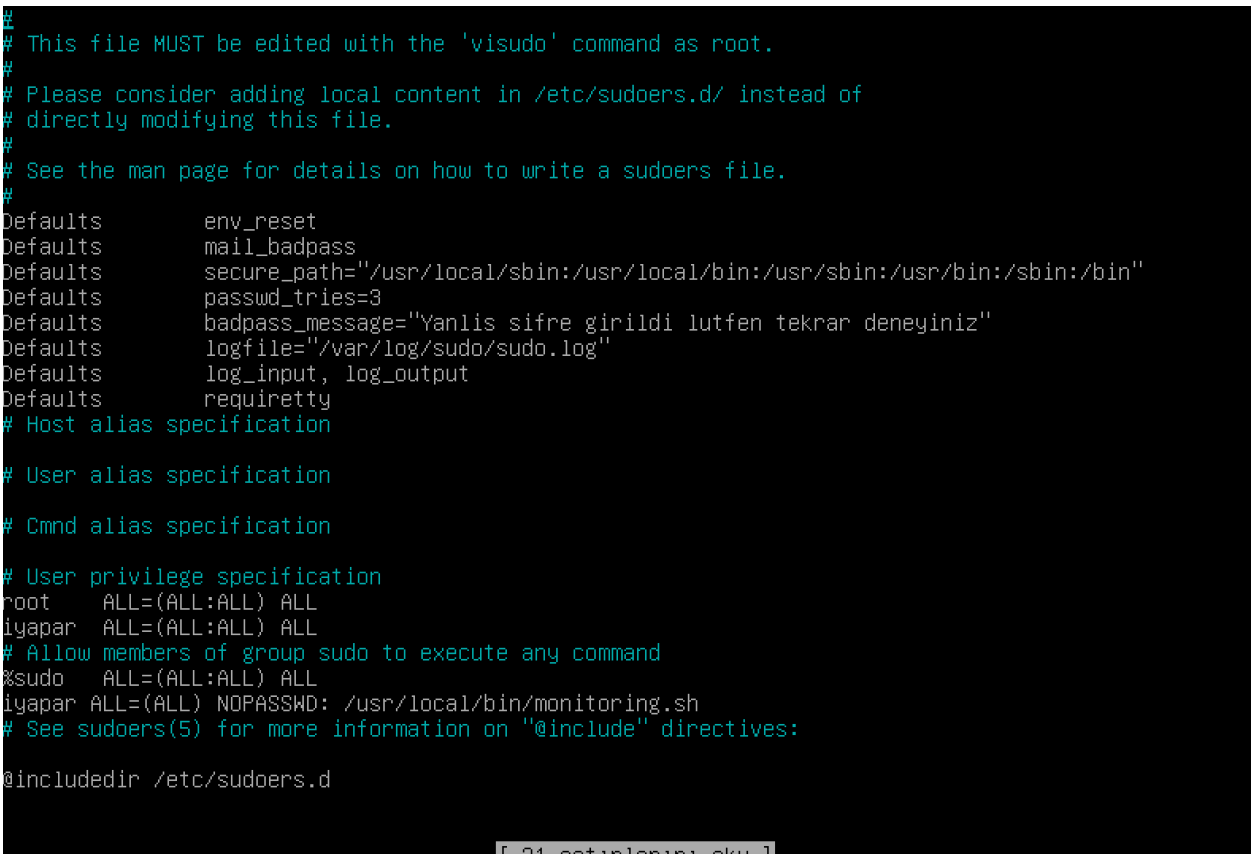
sudo apt-get install -y net-tools

sudo apt-get update

netstat ağ bağlantıları, yönlendirme tabloları ve ağ arayüzü istatistiklerini görüntüleyen bir komut satırı aracıdır.

şimdi ise /usr/local/bin/ dizininde touch ile monitoring.sh dosyası oluşturun.

sudo visudo komutuna your_username ALL=(ALL) NOPASSWD: /usr/local/bin/monitoring.sh satırını ekleyin visudo şu şekilde görünecektir.



sonrasında ***sudo reboot*** ile sistemi yeniden başlatın.

Sanal makina nasıl çalışır ?

bir sanal makina bilgisayardan ayrılan ram-depolama alanı gibi değerleri alır ve bunu sadece o sanal makinada kullanılanıma uygun olacak şekilde ayarlar.

Seçtiğin işletim sistemi nedir ?

Debian

Debian ile CentOS arasındaki farklar nelerdir ?

CentOS rpm paket yöneticisine sahiptir Debian ise apt-get paket yöneticisine sahiptir.

CentOS repoları daha az sıklıkla güncellenirken Debian repoları daha sık bir şekilde güncellenir

CentOS Red hat Linux tarafından desteklenir ve daha kararlı bir dağıtımdır bunun sebebi paket güncellemeleri daha az sıklıkla gerçekleşir.

CentOS, Fedora ve RedHat ailesinden gelmektedir Debian tabanlı sistemler ise Ubuntu Kali vb diye ayrılır Debian tabanlı sistemlerin paket yöneticisinin çekirdeğini DPKG oluşturur DPKG, APT-GET gibi yüksek seviyeli araçlar, paketleri uzak kaynaktan çekmeye ve karışık paket ilişkilerini halletmeye yarar. CentOS paket yöneticisinin çekirdeğini DNF oluşturur.

Sanal makinelerin amacı nedir ?

tek bir fiziksel bilgisayarda çalışarak çoklu işletim sistemi kullanma olanağı sağlar. Böylece fiziksel alan, zaman, yönetim, donanım ve yazılım masraflarından tasarruf sağlar.

aptitude ve apt arasındaki farklar ve APParmor nedir ?

Aptitude APT'ın kullanıcı arabirimidir. Yazılım paketlerini listelemeye, onları seçip kurmaya ve kaldırmaya yarar.
APT debian tabanlı sistemlerin paket yöneticisidir APT ile yazılım kurma, yazılım kaldırma, sistemi güncelleme, çekirdeği derleme gibi işlemleri terminal üzerinden gerçekleştirebilirsiniz.

Aptitude yaptığınız islemlerin kaydını tutar.

Aptitude, paketlerin kurulumunda o paket tarafından Recommend (tavsiye) edilen paketleride kurar.

AppArmor, sistem yöneticisinin programların yeteneklerini program başına farklı tanımlarla kısıtlamasına olanak tanıyan bir Linux çekirdek güvenlik modülüdür.

UFW service başlatılmış mı diye kontrol et

sudo ufw status

SSH service başlatılmış mı diye kontrol et

sudo systemctl status ssh

Sistemin Debian mı CentOS'mu olup olmadığını kontrol et

hostnamectl

---

kullanıcı sudo ya ekli mi diye kontrol et

getent group sudo

Öncelikle yeni bir kullanıcı oluştur, şifreyi kurallara uygun olarak koy, bu kuralları nasıl oluşturduğunu açıkla.

sudo vim /etc/pam.d/common-password

minlen=10 şifrenin minimum uzunluğu

retry=3 maximum 3 deneme hakki

lcredit=-1 en az 1 küçük harf

ucredit=-1 en az 1 büyük harf

dcredit=-1 en az 1 sayı

maxrepeat=3 en fazla 3 arka arka aynı karakter

usercheck=0 şifre kullanıcı adını içeriyor mu diye kontrol

difok=7 yeni şifre eski şifreden minimum 7 karakter farklı olmalı

enforce_for_root root kullanıcıları için de aynı şeylerin geçerli olduğunu belirtir

---

Evaluating adında bir grup oluştur, bu gruba oluşturduğun yeni kullanıcı ata ve kontrol et.

sudo groupadd evaluating

sudo adduser evaluating_user

getent group evaluating

şifre kurallarının avantajları

bir şifreye büyük, küçük harf, rakam, özel karakterler eklemek o şifrenin bulunmasını zorlaştırır.

hostname'in <ogrenci ismi>42 formatına uygun olup olmadığını kontrol et

hostnamectl

hostnameyi degistir ve reboot at

hostnamectl set-hostname new_hostname

sudo reboot

sudo nun yüklü olup olmadığını kontrol etme ***sudo —version***

sudo'nun amacı sudoers gibi alt pluginlerle şifre süresini belirleme şifre gereksinimi belirleme gibi şeyleri ayarlamak ve bazı önemli komutları sadece root yetkisine sahip kişilerin kullanabilmesi.

/var/log/sudo klasörünün olup olmadığına bak ve içinde en azında bir dosyanın olduğunu teyit et

sudo visudo

UFW çalışıyor mu kontrol et ***sudo ufw status***

UFW nin ne olduğunu açıkla

Karmaşık Güvenlik Duvarı, kullanımı kolay olacak şekilde tasarlanmış bir netfilter güvenlik duvarını yönetmek için kullanılan bir programdır.

UFW'nin aktif kurallarını listele, 4242 portu listede olmalı ***sudo ufw status***

8080 portu için yeni bir kural ekle, kontrol et yeni kuralı sil ***sudo ufw allow 8080***

sudo ufw status numbered sudo ufw delete number

basitçe SSH nedir anlat

SSH, veya Secure Shell, kullanıcılara sunucularını internet üzerinden kontrol etmesini ve düzenlemesini sağlayan uzak yönetim protokolüdür.

SSH servisinin sadece 4242 portunu kullandığından emin ol **sudo grep Port /etc/ssh/sshd_config**

Yeni oluşturulan kullanıcı ile SSH kullanarak bağlantı kurunuz

ssh your_username@127.0.0.1 -p 4242

crontab'ı kontrol et ve ne olduğunu açıkla

sudo crontab -u root -e

monitoring.sh dosyasını kontrol et

/usr/local/bin/monitoring.sh

sudo groupadd xx

sudo groupdel xx

getent group xx

sudo adduser xx

sudo userdel xx

usermod -aG sudo your_username

cat /etc/passwd (tüm kullanıcılar)

sudo grep Port /etc/ssh/sshd_config

sudo grep Defaults /etc/sudoers

sudo vim /etc/pam.d/common-password

#!/bin/bash

explainshell.com

awk **Awk, verileri işlemek ve raporlar oluşturmak için kullanılan bir betik dilidir. awk komut programlama dili derleme gerektirmez ve kullanıcının değişkenleri, sayısal işlevleri, dize işlevlerini ve mantıksal operatörleri kullanmasına izin verir. Awk, bir programcının bir belgenin her satırında aranacak metin kalıplarını ve bir eşleşme bulunduğunda yapılacak eylemi tanımlayan ifadeler biçiminde küçük ama etkili programlar yazmasını sağlayan bir yardımcı programdır. Awk, çoğunlukla desen tarama ve işleme için kullanılır. Belirtilen kalıplarla eşleşen satırlar içerip içermediklerini görmek için bir veya daha fazla dosyayı arar ve ardından ilişkili eylemleri gerçekleştirir.**

sort **metin dosyalarının satırlarını sırala**

uniq **tekrarlanan satırları rapor et veya atla**

wc **her dosya için yeni satır, kelime ve bayt sayılarını yazdır -l yeni satır yazdır**

free -m **Sistemdeki boş ve kullanılan bellek miktarını görüntüleme -m megabyte cinsi**

df -Bg **dosya sistemi disk alanı kullanımını rapor et -B boyutları yazdırmadan önce ölçeklendir -g gb -m mb**

top **display Linux tasks**

who -b **kimin oturum açtığını göster | son sistem önyükleme zamanı**

```
#!/bin/bash
arc=$(uname -a)
```

Tüm sistem mimarisin gösterir

```
pcpu=$(grep "physical id" /proc/cpuinfo | sort | uniq | wc -l)
```

sort satırları arar uniq tekrar edilen satırları atlar wc -l her satır için byte değerlerini yazar

```
vcpu=$(grep "^processor" /proc/cpuinfo | wc -l)
fram=$(free -m | awk '$1 == "Mem:" {print $2}')
```

sistemdeki bellek miktarini görüntüleme -m megabyte cinsinden 1. argüman mem’e eşitse 2. argümanı ekrana yaz

uram=$(free -m | awk '$1 == "Mem:" {print $3}')
pram=$(free | awk '$1 == "Mem:" {printf("%.2f"), $3/$2*100})'

argüman 1 mem'e eşitse float olarak 3. argüman ile 2. argümanın yüzdesini alacak

fdisk=$(df -Bg | grep '^/dev/' | grep -v '/boot$' | awk '{ft += $2} END {print ft}')

df disk kullanımının alanı -B yazdırmadan önce ölçeklendir -g gigabyte -m megabyte

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}')*

grep ^dev satır başındaysa al grep -v sadece sonunda boot olanları al anlamına gelir

cpul=$(top -bn1 | grep '^%Cpu' | cut -c 9- | xargs | awk '{printf("%.1f%%"), $1 + $3}')

top linux işlemlerini göster. -b düzenlid mod xargs standart komut satırları oluşturma ve yürütme.

-n yineleme veya kare sayısını belirtir.

-1 bir veya çoklu cpu parametleri için kullanılır
X D

cut -c 9- 9. sıradakini alma

lb=$(who -b | awk '$1 == "system" {print $3 " " $4}')

who -b kimin oturum açtığını göster | son sistem önyükleme zamanı

lvmt=$(lsblk | grep "lvm" | wc -l)
lvmu=$(if [$lvmt -eq 0]; then echo no; else echo yes; fi)

koşul doğruysa then ve fi arasında değerler yürütülür

ctcp=$(cat /proc/net/sockstat{,6} | awk '$1 == "TCP:" {print $3}')in
ulog=$(users | wc -w)

TCP6 ile iliskili bu yere bak

wc her dosya için yeni satır, kelime ve bayt sayılarını yazdır -w kelime sayısını yazdırır

ip=$(hostname -I)
mac=$(ip link show | awk '$1 == "link/ether" {print $2}')
cmds=$(journalctl _COMM=sudo | grep COMMAND | wc -l)

journalctl - Systemd günlüğünü sorgula _comm sudo için özel bir parametre

```
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"
```