

# Kök olmak için doğmuş

42 Notları



## Born2beroot

Bu proje bir Born2beroot yönergesidir. Bonus görevleri ve CentOS'u içermez.

### 🧭 Yol Haritası

1. Bölüm 1 (Debian'ı İndir)
2. Bölüm 2 (İndirmeler ve Ayarlamalar ve ve Konfigürasyonlar )
  - SSH için
  - UFW için
  - Sudo için
  - Şifre Politikalama
3. Bölüm 3 (Monitoring.sh ve Crontab Konfigürasyonları)
4. Bölüm 4 (Teslim ve Ön Değerlendirme)

## 5. Ekstralalar ve Kaynaklar

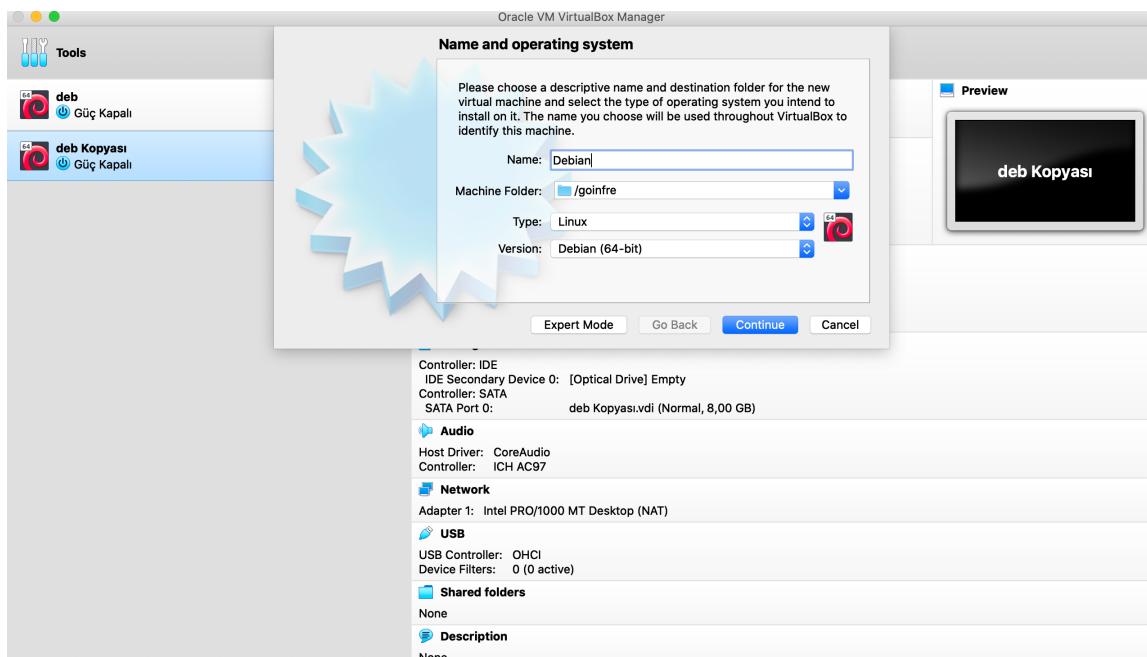
### 1 Bölüm 1 (Debian'ı İndir)

Önce VirtualBox'ı indirin ve ardından Debian'nın .iso dosyasını. İşte bağlantılar:

- VirtualBox
- Debian

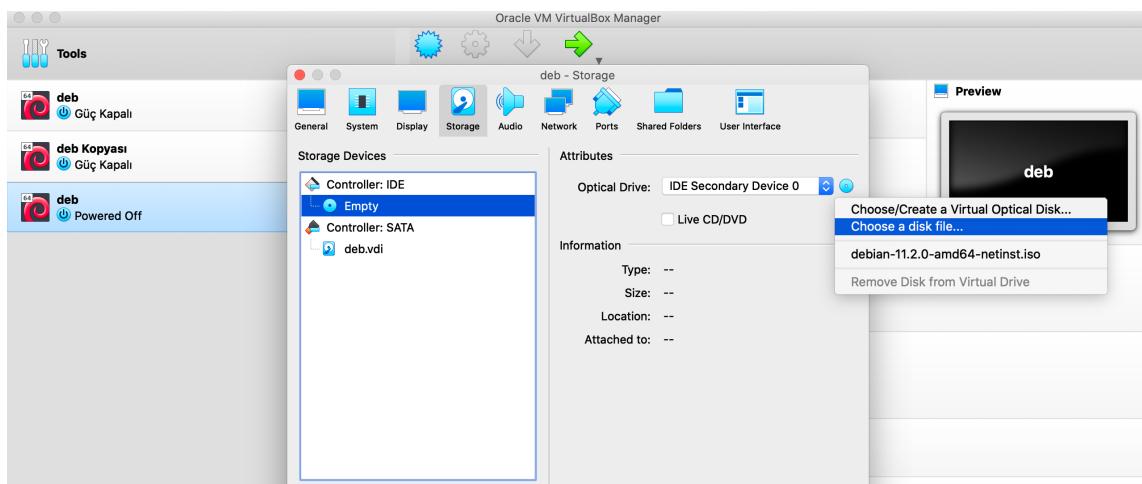
VirtualBox'ı kurduktan sonra açın:

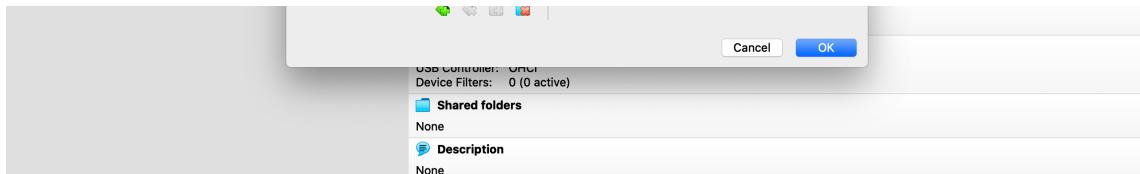
Ve yukarıda ki yeni tuşuna basın!



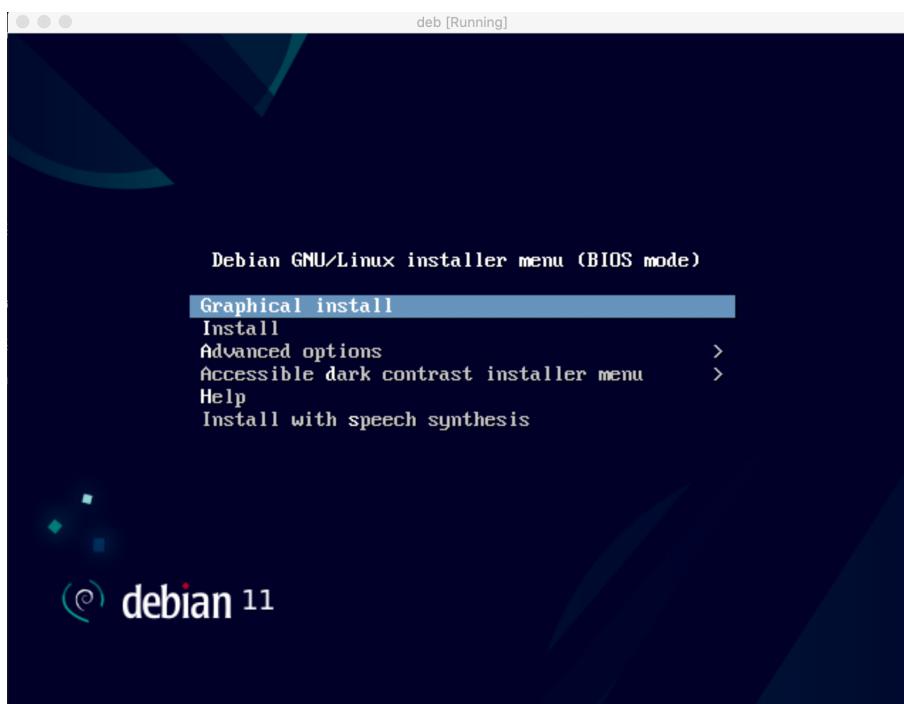
Devam devam devam.. ve ‘Makine Klasörü’ makine klasörünüzün yolunu ‘/goinfre’nin altı olacaktır. Sonra ki kısımda ise disk imajını soracaktır bu ‘.vdi’ olacaktır.

Ardından ‘.iso’ Debian dosyasını seçin. Oluşturduğunuz sanal makineye tıklayın ve yukarıdaki ‘ayarlar’'a tıklayın. ve oradan ‘Depolama’ya tıklayın, ‘Empty’ a tıklayın ve sağ pencerede ‘Optik Sürücü’ seçeneğinin yanındaki CD işaretine basın. Oradan, ‘Disk Dosyasını Seç’ e tıklayın ve indirdiğiniz debian ‘.iso’ dosyanızı seçin.



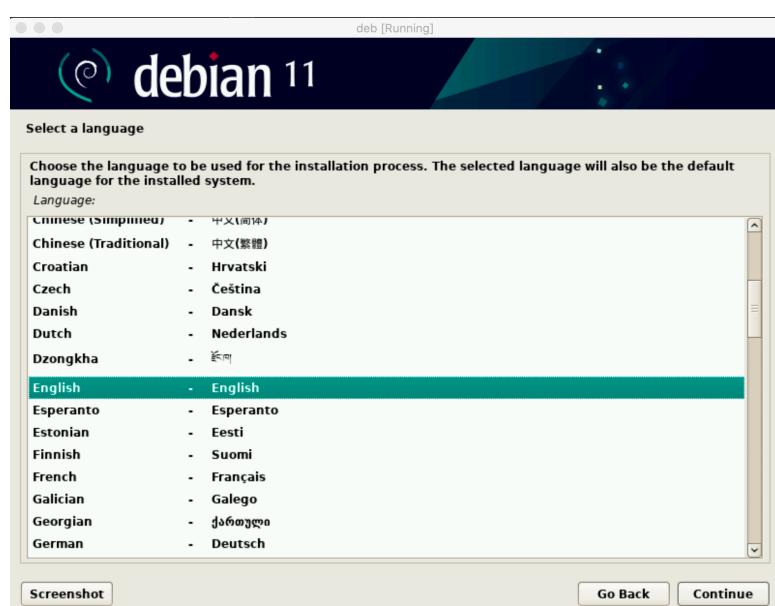


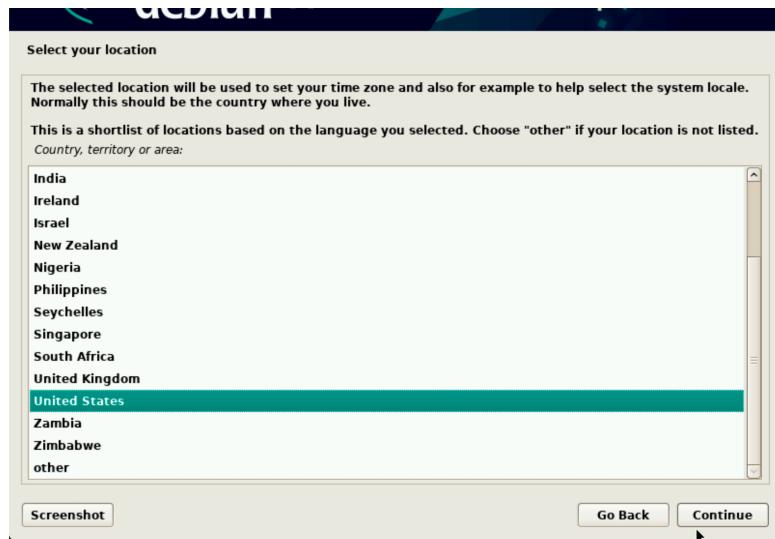
Bunları yaptıktan sonra sanal makinenizi başlatın ve şu ekranı göreceksiniz:

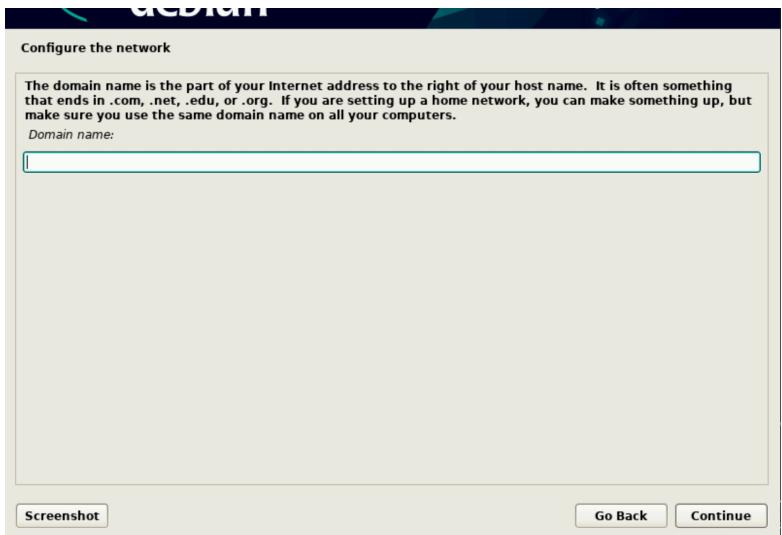


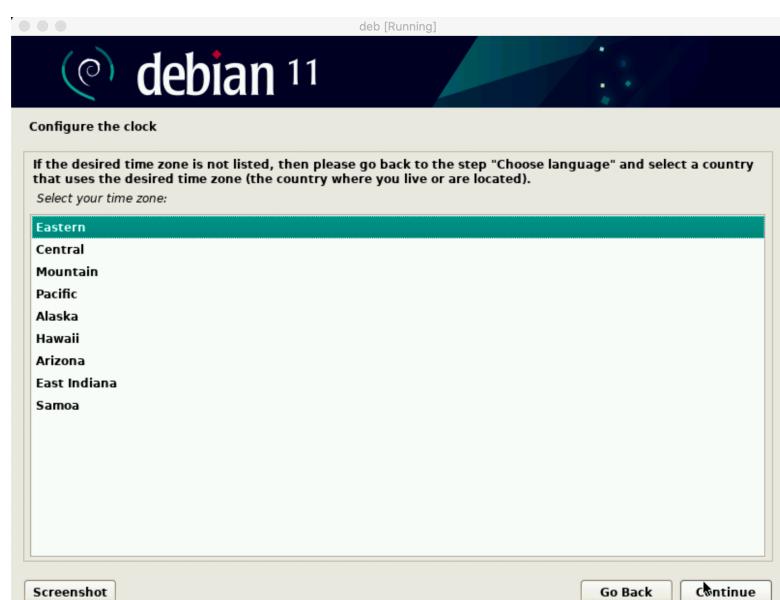
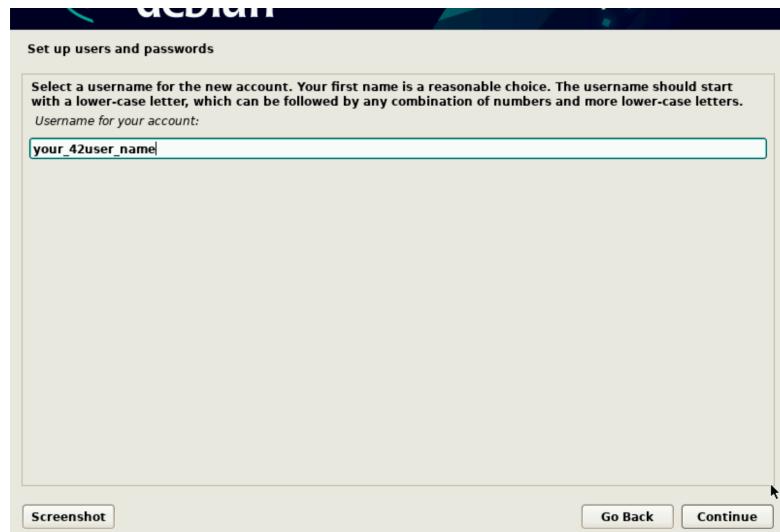
**'Graphical Install'** seçeneğini seçin. (Endişelenmeyin, bu seçenek Debian'ı GUI olarak kurmaz. Sadece kurulum aşaması için bir seçenektedir.)

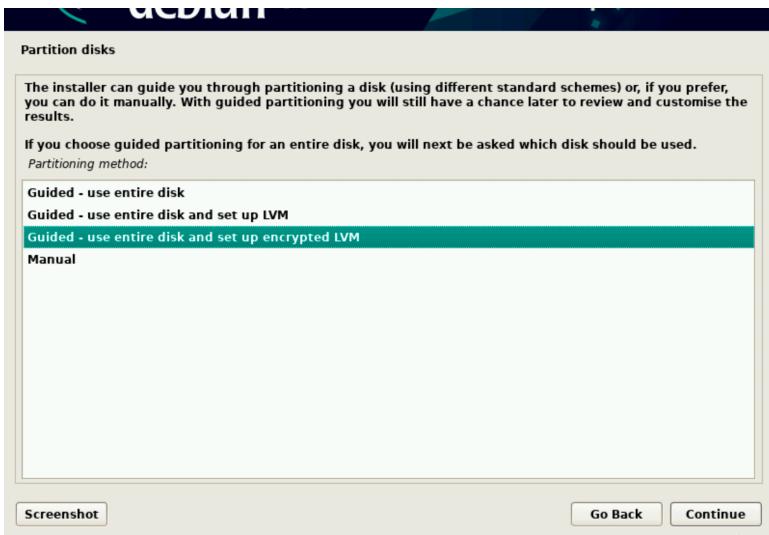
Sonra ki kısım kurulum için bütün resimleri içerir:

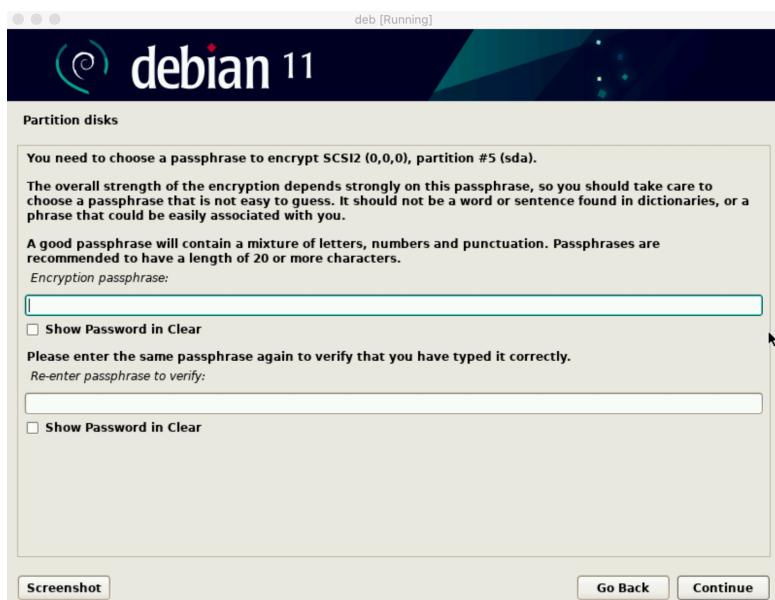
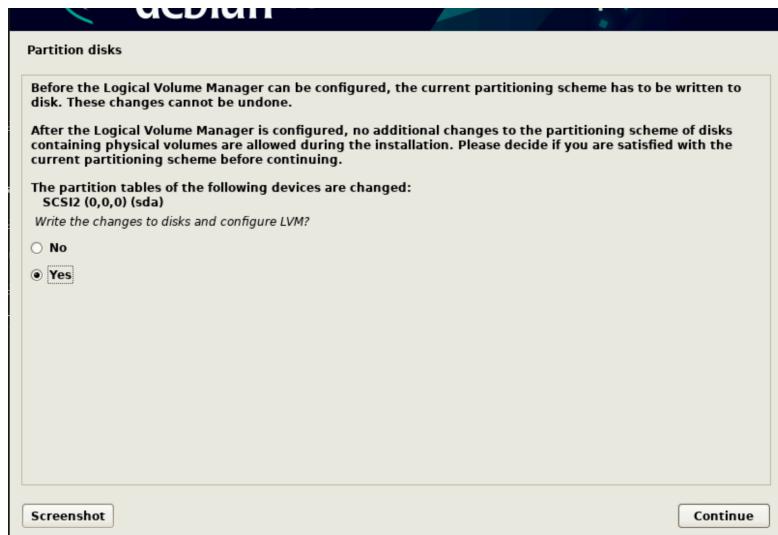


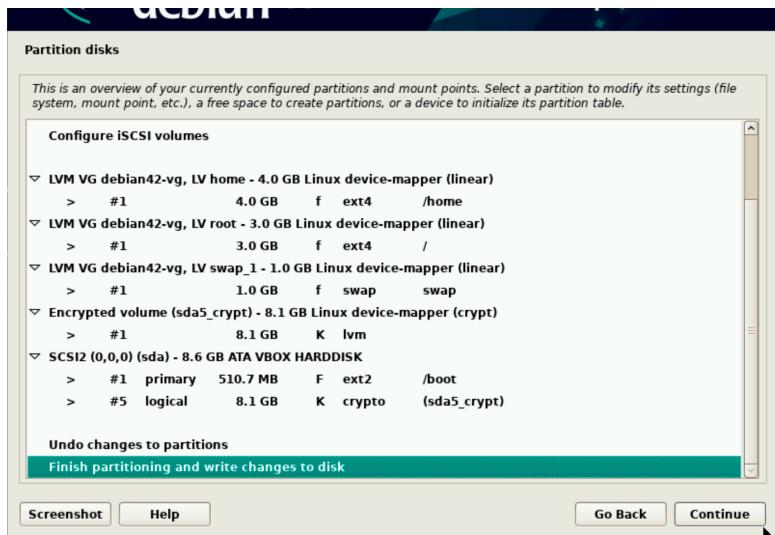


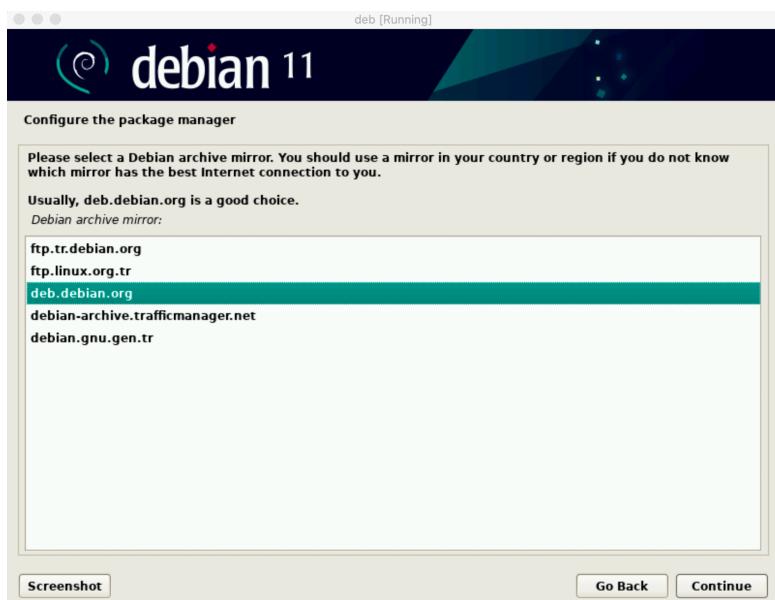
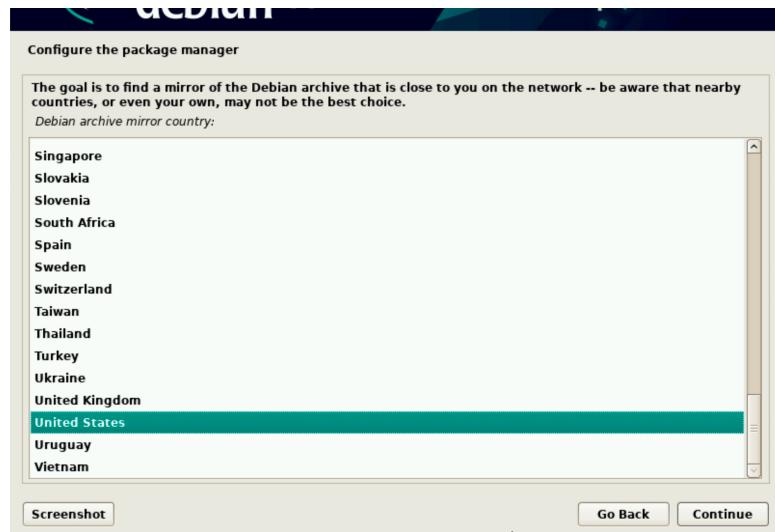


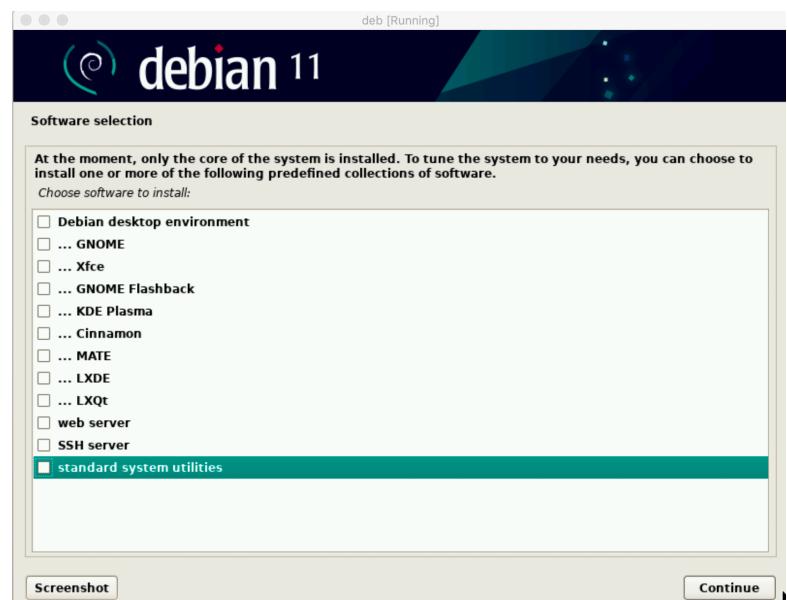
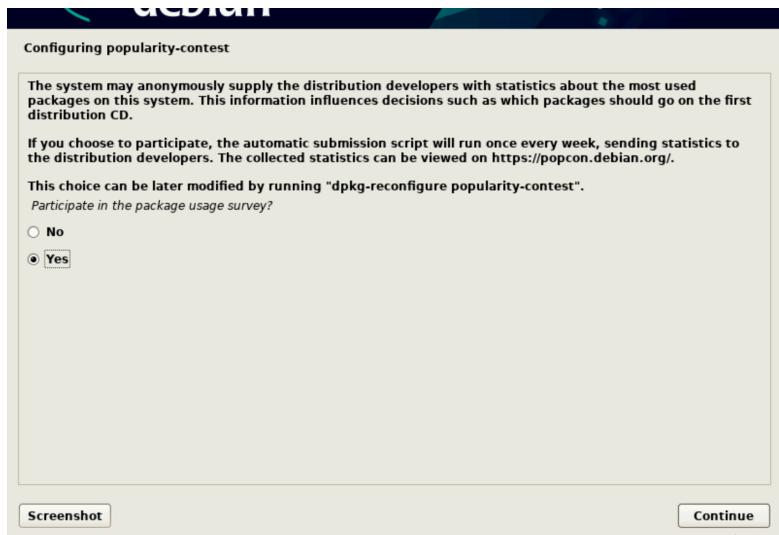










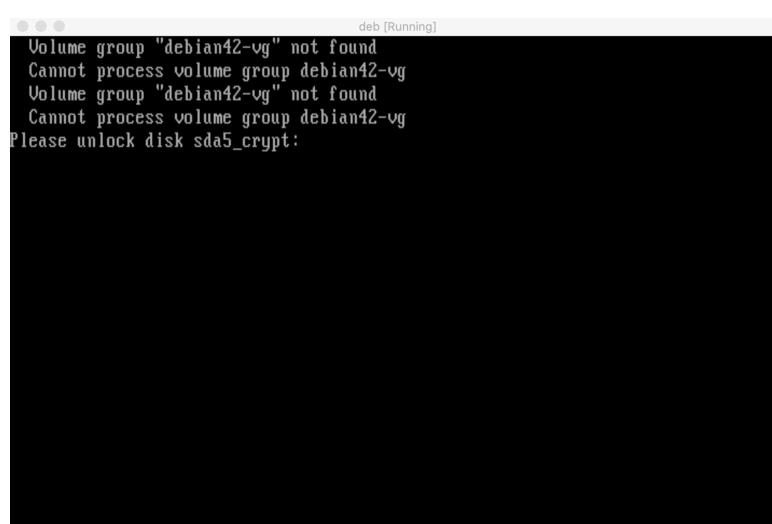


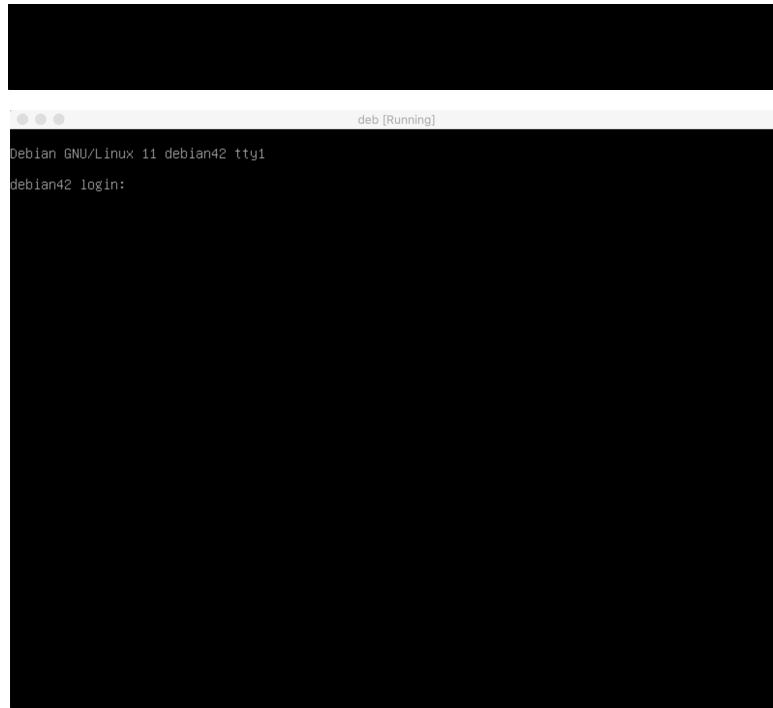


❖ Ve sonunda 1. Bölüm burada biter ❖

## 2 Bölüm 2 (İndirmeler ve Ayarlamalar ve ve Konfigürasyonlar)

Bu ekranı göreceksiniz. Sanırım bu giriş ekranı. :d





Bu komutu çalıştırarak diskinizin bölümlerini ve şifreli bölümlerini görebilirsiniz:

```
lsblk
```

İndirmelere ve yapılandırmalara devam etmeden önce şunları bilmekte fayda var:

- Root olmak:

```
su -
```

- Güncellenmesi gereken bir paket var mı yok mu arar ve varsa bulur yoksa bulmaz:

```
apt update
```

- Güncellenmesi gereken bir paket varsa onu bu komut yapıyor ve güncelliyor:

```
apt upgrade
```

### ☞ Kullanıcı Komutları

Bunların haricinde, sanal makinenizde ki bütün kullanıcıları görme komutu:

```
getent passwd
```

Kullanıcı ekleme ve silme komutları (**root olmalısın**):

```
adduser <user_name> - deluser <username>
```

### 🍇 Grup Komutları

Sanal makinenizdeki grupları görme komutu:

```
getent group or getent group <group_name> → Bir grup altındaki
```

## kullanıcılar

Grup ekleme ve silme komutları (**root olmalısın**):

```
groupadd <group_name> - groupdel <group_name>
```

### 💡 Kullanıcılar ve Grupların Birlikten Doğan Komutları

Bir kullanıcının hangi grupta olduğunu görmek için bu komut:

```
groups <user_name>
```

Bir gruba kullanıcı ekleme ve bir kullanıcıyı gruptan çıkarma komutu (**root olmalısın**):

```
usermod -aG <group_name> <user_name> - gpasswd --delete <user_name>
<group_name>
```

## 🛠 Paketleri İndirme ve Dosyaları Konfigüre Etme

### 💻 SSH için

SSH'ı yükleme komutu:

```
apt install openssh-server
```

SSH etkinlik sorğu komutu ve SSH başlatma komutları:

```
systemctl status ssh - systemctl start ssh - systemctl enable ssh
```

### 🧬 SSH Port Değiştirme

Şu dizine gitmelisin:

```
nano /etc/ssh/sshd_config
```

Bu ayarları değiştirmelisin:

- #Port 22 → Port 4242
- #PermitRootLogin prohibit-password → PermitRootLogin no
- Ve evet, '#' işaretini de kaldırın, yazdıklarınızı yorum satırı haline getirir '#' bu işaret. :)
- He bu arada o işaret sadece o iki ayar için. Sakın hepsi için kaldırma. :d

```
deb [Running]
/etc/ssh/sshd_config
# 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 22
#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:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
```

```

GNU nano 5.4          deb [Running]
/etc/ssh/sshd_config *

# 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:

#LoginGraceTime 2m
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

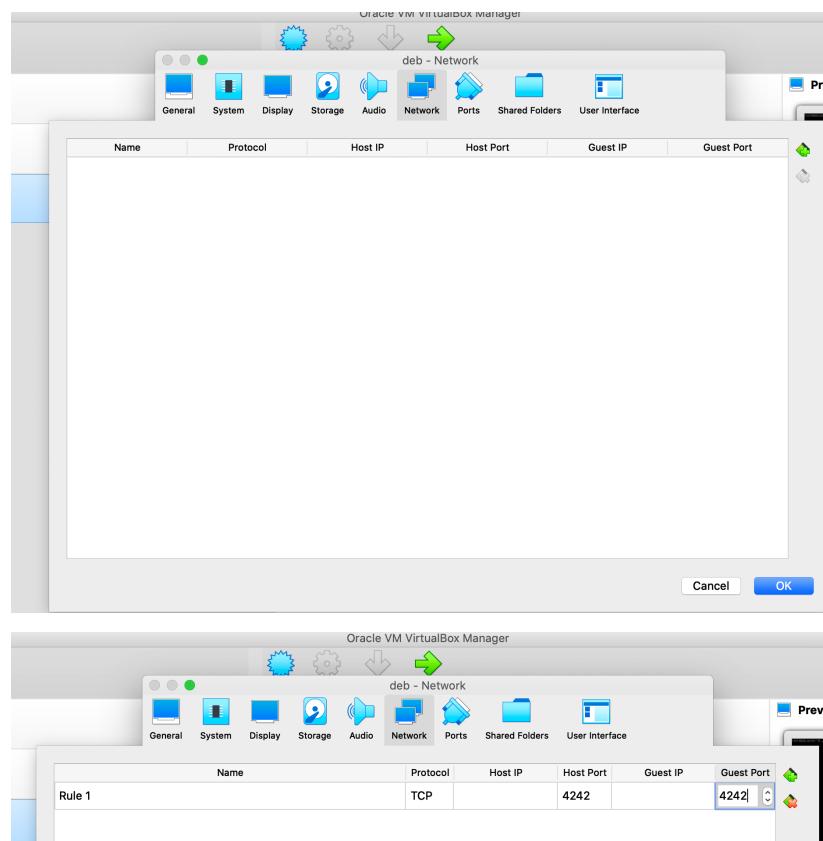
G Help   W Write Out  K Where Is  C Cut  T Execute  L Location  M-U Undo
X Exit   R Read File  P Replace  U Paste  J Justify  O Go To Line  M-E Redo

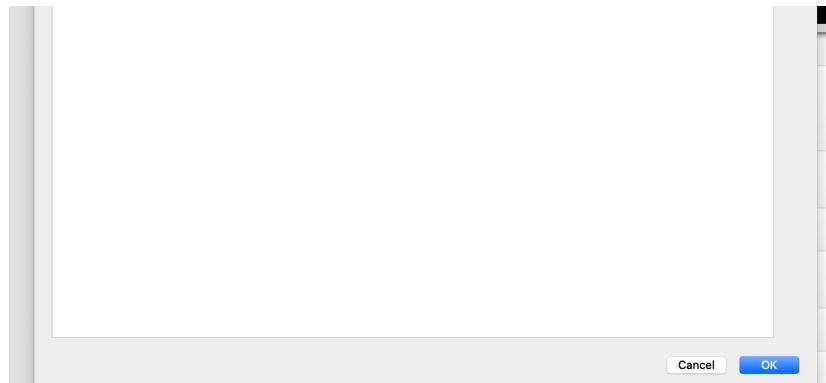
```

Tamam, bu ayarları yaptıktan sonra şu komutla yeniden başlatın:

```
service sshd restart
```

Ardından VirtualBox'ınıza gelin ve üst kısımdaki **'ayarlar'a**, ardından **'Ağ'a** basın, daha sonra alta bir **'Gelişmiş'** bölümü olacak, oraya tıklayın ve **'Port Yönlendirme'ye** basın. Sağda yeşil '+' işaretli olan bir düğme göreceksiniz, evet ona basın ve tablo görünecektir. **'Ana Makine Port'u ve 'Misafir Port'u** bölümlerinde resimdeki gibi yapın. Zaten resim ekliyorum, neden açıklama gereği duydum bilmiyorum. Her neyse, tamam ve tamam'a basın ve bitirin işi.





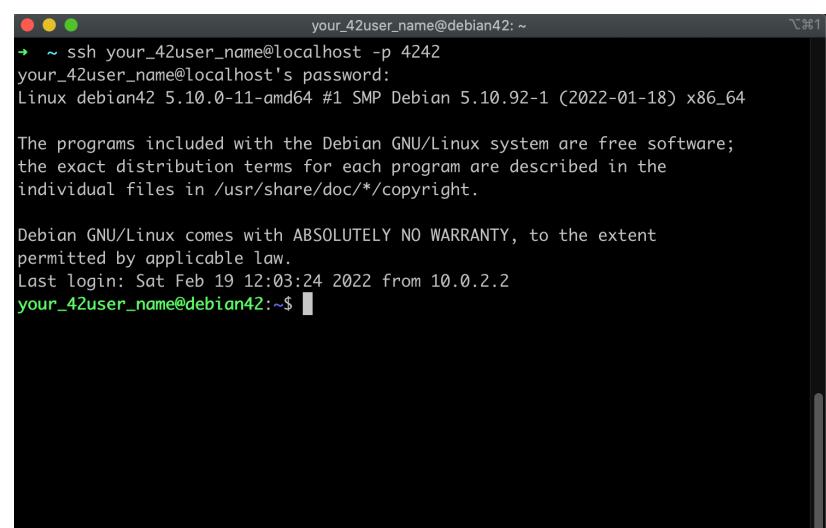
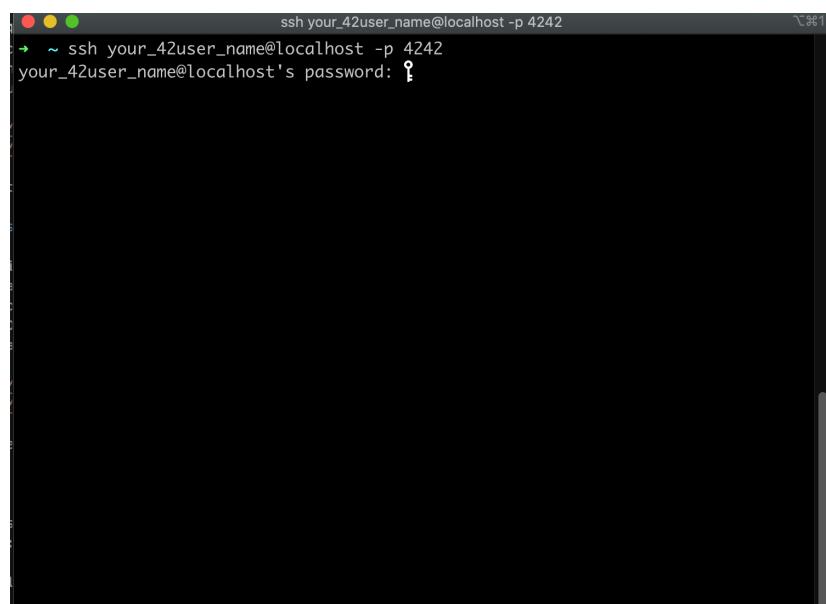
Bunları yaptıktan sonra sanal makineyi yeniden başlatın (**root olmalısın**):

```
reboot
```

Bu ayarlardan sonra artık fiziksel makineden sanal makineye bağlanabilirsiniz. Nasıl mı? İşte bu kadar:

- Terminalinizi fiziksel makineden açın ve aşağıdaki komutu yazın

```
ssh your_42user_name@localhost -p 4242
```



Ve sanal makinenizdeki kullanıcının şifresini girerek fiziksel makinenin terminalinden sanal makineye erişebilirsiniz.

► Evet, SSH bu kadardı.. ►

## 💡 UFW İçin

UFW'yi İndirme:

```
apt install ufw
```

### **UFW ile ilgili bazı komutlar**

Bize gelen tüm istekleri reddedin:

```
ufw default deny incoming
```

Tüm giden isteklere izin ver:

```
ufw default allow outgoing
```

Sistem başlangıcında UFW'yi etkinleştirin (Bunu yaptıktan sonra sanal makinenizi yeniden başlatın):

```
ufw enable
```

UFW'nin durumunu kontrol edin:

ufw status – ufw status numbered → kuralları numaralandır

4242 numaralı bağlantı noktasına gelen isteklere izin verin veya bu bağlantı noktasını (4242) reddedin:

```
ufw allow 4242 – ufw deny 4242
```

The terminal window shows the following session:

```
root@debian42:~# ufw status
Status: active
root@debian42:~# ufw allow 4242
Rule added
Rule added (v6)
root@debian42:~# ufw status
Status: active
To          Action      From
--          ----      --
4242        ALLOW      Anywhere
4242 (v6)   ALLOW      Anywhere (v6)

root@debian42:~#
```

Kural silmek için:

ufw delete allow 4242 → bu komut 'izin verilen' 4242 kuralını siler ufw

delete deny 4242 → bu da 'reddedilen' 4242 kuralını siler

ufw delete 1 → 1. kuralı siler

## ► Evet, UFW bu kadardı.. ►

### :godmode: Sudo için:

Sudo'yu çok çok katı kurallara göre yapılandırma (soğuk espri :/)

Sudo'yu indirin:

```
apt install sudo
```

Konfigürasyon ayarlarına geçmeden önce kullanıcınızı 'sudo' grubu altına ekleyin:

```
usermod -aG sudo <user_name>
```

Tamam, çok şey yaptık, şimdi yapılandırma ayarlarına geçelim: :d  
visudo → Bu komutla konfigürasyon dosyasına girelim

Böyle bir ekran gelmeli:

```
GNU nano 5.4 deb [Running] /etc/sudoers.tmp
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
#
# Host alias specification
#
# User alias specification
#
# Cmnd alias specification
#
# User privilege specification
root    ALL=(ALL:ALL) ALL
#
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
#
# See sudoers(5) for more information on "@include" directives:
#
@includedir /etc/sudoers.d

[ Read 27 lines ]
```

The terminal window shows the nano editor with the /etc/sudoers.tmp file open. The file content is the standard sudoers configuration. The status bar at the bottom indicates "Read 27 lines". Below the status bar are various nano key bindings.

Buraya bazı katı kurallar ekleyin:

```
Defaults      passwd_tries=3 → 3 kere yanlış girme hakkı
Defaults      badpass_message="Çok Yanlış Bir Şifre" → yanlış girilirse hata
mesajı
(yanlız o yanlış değil 'yanlış') → (yanız o yanlış değil 'yalnız') →
sürekli okuyunca dilim sürsstü (kendi çapımda gereksiz bir eğlenmeydi kusura
bakmayın)
Defaults      requiretty → sudo komutu için terminal gerekliliği
Defaults      logfile="/var/log/sudo/sudo.log" → girilen her sudo komutunun
tutulacağı kayıt yeri
Defaults      log_input, log_output → sudo komutunun girdi ve çıktıları
Defaults      iolog_dir="/var/log/sudo/" → girdi ve çıktıların yolu
```

Sonuç olarak şu şekilde görünmeli:

```
GNU nano 5.4 deb [Running] /etc/sudoers.tmp
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults    passwd_tries=3
Defaults    badpass_message="Çok Yanlış Bir Şifre"
Defaults    requiretty
```

The terminal window shows the nano editor with the /etc/sudoers.tmp file open. The file now includes the specified changes: "passwd\_tries=3", "badpass\_message='Çok Yanlış Bir Şifre'", and "requiretty". The status bar at the bottom indicates "Read 27 lines". Below the status bar are various nano key bindings.

```

Defaults env_reset
Defaults mail_badpass
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/snap/bin"
Defaults passwd_tries=3
Defaults badpass_message="Wrong Password!!!"
Defaults requiretty
Defaults logfile="/var/log/sudo/sudo.log"
Defaults log_input, log_output
Defaults iolog_dir="/var/log/sudo/"
# Host alias specification

# User alias specification

# Cmd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
%your_42user_name        ALL=(ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:
@includedir /etc/sudoers.d

```

[ Read 32 lines ]

G Help W Write Out M Where Is K Cut T Execute C Location M-U Undo  
 X Exit R Read File R Replace U Paste J Justify G Go To Line M-B Redo

Bunları doğrulamak için ‘root’tan çıkış sudo komutu ile neler yapılabileceğini deneyebilirsiniz...

▶ Evet, Sudo bu kadardı.. ▶

## ☒ Şifre Politikası

**İlk olarak, parola değiştirme sıklığını yapılandırın:**

```
nano /etc/login.defs
```

Şu ayarı bulmalısın ‘pass aging control’:

```

GNU nano 5.4          deb [Running]
/etc/login.defs
# for private user groups, i. e. the uid is the same as gid, and username is
# the same as the primary group name: for these, the user permissions will be
# used as group permissions, e. g. 022 will become 002.
#
# Prefix these values with "0" to get octal, "0x" to get hexadecimal.
#
ERASECHAR      0177
KILLCHAR       025
UMASK         022

#
# Password aging controls:
#
#      PASS_MAX_DAYS  Maximum number of days a password may be used.
#      PASS_MIN_DAYS  Minimum number of days allowed between password changes.
#      PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS  99999
PASS_MIN_DAYS  0
PASS_WARN_AGE   7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN          1000
UID_MAX         60000
# System accounts
#SYS_UID_MIN     100
#SYS_UID_MAX     999

#
# Min/max values for automatic gid selection in groupadd
#

```

root@debian42:~#

Sonra bunu yap:

```
PASS_MAX_DAYS  30
PASS_MIN_DAYS  2
PASS_WARN_AGE   7
```

⚠ Evet, hepsi bu, ancak bu ayar root ve sizden (usr) sonraki kullanıcılar için geçerlidir. Kullanıcınızı ve kökünüzü değiştirmek için bunu yapın

Önce sana bu olayı kanıtlayayım:

chage -l root ve chage -l <user\_name> → Bu yeterli bir kanıttı :d

Değiştirmek için:

chage root ve chage <user\_name>

```
root@debian42:~# chage -l root
Last password change : Feb 19, 2022
Password expires       : never
Password inactive     : never
Account expires        : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
root@debian42:~# chage root
Changing the aging information for root
Enter the new value, or press ENTER for the default
      Minimum Password Age [0]: 2_
```

Ne yapacağını biliyorsun..

## Şimdi şifre oluşturma kurallarımızı ekleyelim

Bunu indirelim:

```
apt install libpam-pwquality
```

Bu yol takip et:

```
nano /etc/security/pwquality.conf
```

Böyle bir şeyle karşılaşacaksınız:

```
GNU nano 5.4          /etc/security/pwquality.conf
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
# minlen = 8
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
# dcredit = 0
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
# ucredit = 0
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
# lcredit = 0
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
# ocredit = 0
#
# The minimum number of required classes of characters for the new
# password (digits, uppercase, lowercase, others).
[I Read 79 lines]
[G Help   ^O Write Out  ^W Where Is  ^K Cut    ^T Execute  ^C Location M-U Undo
^X Exit   ^R Read File  ^Y Replace   ^U Paste   ^J Justify  ^L Go To Line M-B Redo]
```

İşte değiştirmeniz gerekenler:

```
difok = 7
minlen = 10
dcredit= -1
ucredit= -1
```

```
enforce_for_root
enforcing= 1
maxrepeat= 3
usercheck = 1
dictcheck = 1
```

Açıklamalarını yazmayacağım, zaten yazılmış...

⚠ Evet, hepsi bu, ancak bunları yaptıktan sonra root, kullanıcınız ve oluşturduysanız diğer tüm kullanıcılar için şifreleri değiştirmeniz gerekiyor.

Nasıl mı?

```
passwd root ve passwd <user_name>
```

🏁 \*\*Ve Sonunda 2. Bölüm Biter \*\* 🏁

### 3 Bölüm 3 (Monitoring.sh ve Crontab

#### Konfigürasyonları

##### Monitoring.sh

İncelemek isterseniz yukarıda ‘monitoring.sh’ dosyasını paylaştım.

Monitoring.sh

##### Crontab (cron)

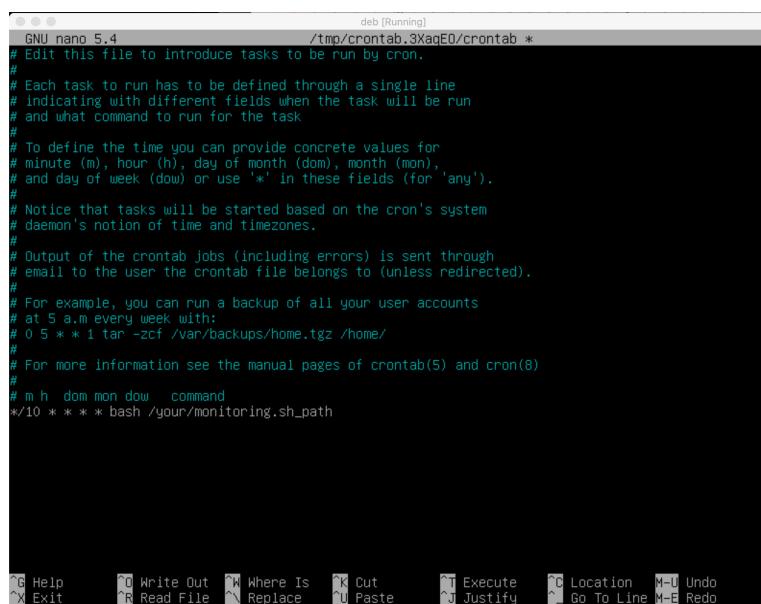
Bu komutu yazın:

```
crontab -e
```

Ve en alta bunu yaz:

```
*/10 * * * * bash /your/monitoring.sh_path
```

Açıklama yapmayacağım, dosya da yine açıklaması var..



```
GNU nano 5.4          deb [Running]
/tmp/crontab.3XaqE0/crontab *
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
*/10 * * * * bash /your/monitoring.sh_path
```

🏁 \*\* Ve Sonunda 3. Bölüm Tüm Zorluklarla Biter .. 🏁

### 4 Bölüm 4 (Teslim ve Ön Değerlendirme)

Artık her şey bittiğine göre, disk imzanızı alma zamanı:

Öncelikle '/goinfre' içeresine kurduğumuz dosyanın içine girip sanal makinenizi bulmalısınız. Nerede olduğunu bilmediğim için oraya gittiğini varsayıyorum.

Şunu yazmalısın:

shasum <your\_virtual\_machine>.vdi → Çıkması biraz vakit alabilir.

Disk imzanız geldiğinde 'signature.txt' dosyası oluşturun içine bu imzayı yapıştırın ardından ve push'layın. Bu kadar. Buraya kadar geldiyseniz 🎉 TEBRİKLER!!! 🎉

## ❖❖ Ve Sonunda 4. Bölüm Burada Biter.. ❖❖

## 5 Ekstralalar ve Kaynaklar

### ✚ Ekstralalar

1. SSH kullanarak arkadaşlarınızın sanal makinesine bağlanabilirsiniz.
2. Netchat ile arkadaşlarınızla terminal üzerinden sohbet edebilirsiniz..

Malzemeler:

- ifconfig → yok ise apt install net-tools → IPv4 adresi ve

- Port

```
netstat -anvp tcp | awk 'NR<3 || /LISTEN/'
```

### NetChat'i Nasıl Kullanılır?

Her şeyden önce, arkadaşınızın bilgisayarının açık olan portunu terminale yazın::

nc -l <port> → ve ENTER, ve bekle..

Ardından arkadaşınızın IPv4 adresini yazıp kendi bilgisayarınızdan port numarasını açın ve mesajlaşmaya başlayın :d

```
nc <arkadaşının_IPv4_adresi> <port>
```

### 🧠 Kaynaklar

1. Aptitude vs apt
2. Sudo
3. SELinux
4. AppArmor
5. SSH
6. awk command
7. sudo config
8. List Users Commands

## ❖❖ Ve Sonunda README.md Burada Biter.. ❖❖

**Son olarak Debian Kullanıcı ve root şifrelerinizi**

## unutursanız

❖ Debian Şifre Reset'leme

