Jun 19 · 9 min read

BORN2BEROOT

Ecole 42

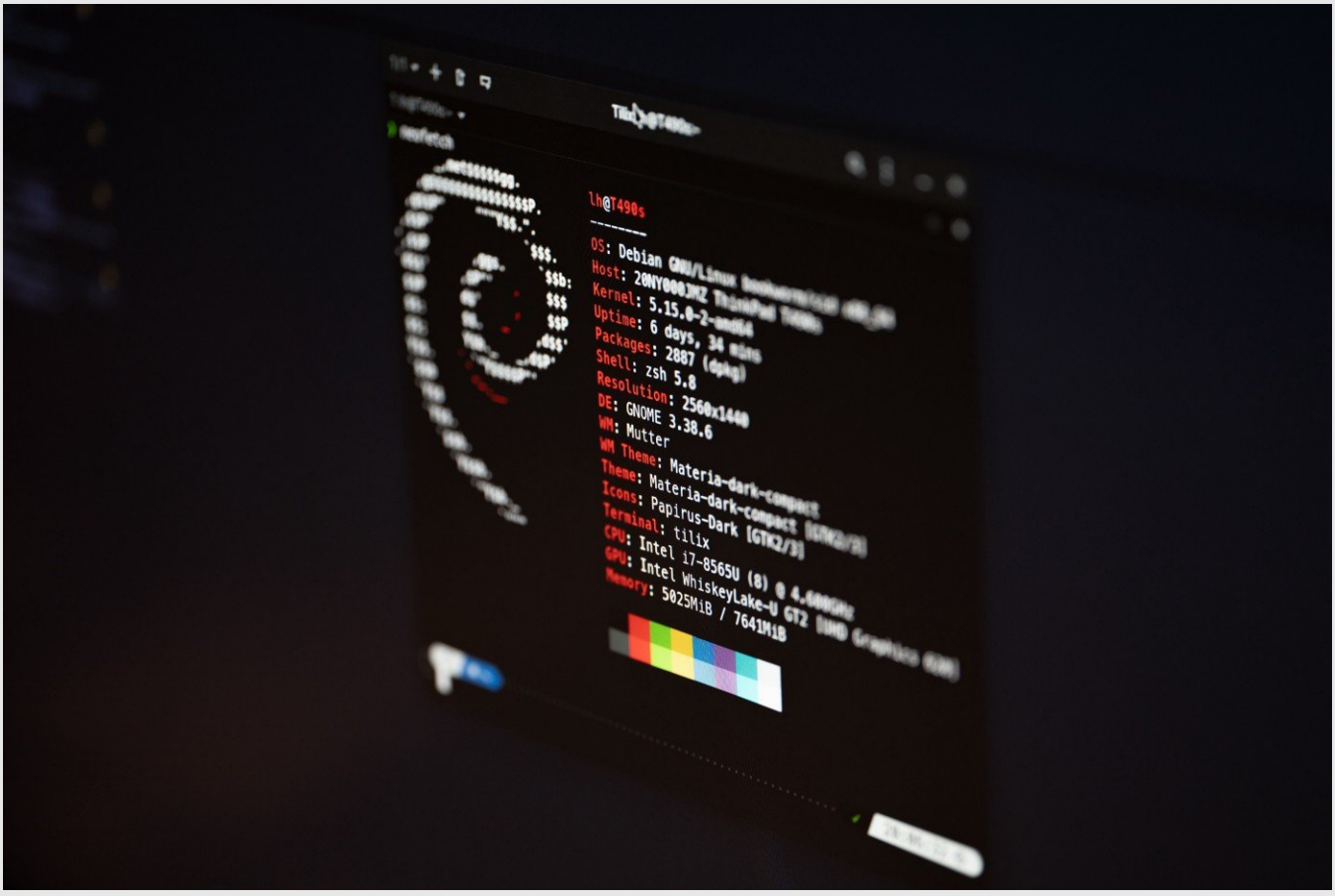

Photo by Lukas on Unsplash

Born2beroot projesini yaparken kendime aldığım notlar, arkadaşlarımın notları ve uyguladığım komutları burada evolation sayfasına göre ilerleyerek paylaşıyorum. Bu proje, bilgisayarımızın içinde sanal makine ile başka bir işletim sistemi kurup o işletim sistemine hakim olabilecek kadar bilgi edinmemizi sağlar. Ben de çoğu kişi gibi Debian seçtim. Debian üzerinden ilerleyeceğim.

Bilgisayarlarımızdaki Hypervisor yazılımı sayesinde sanallaştırma özelliğini

a. Project Overview

1. **Bir sanal makine nasıl çalışır?**
   Hali hazırda kullandığımız işletim sisteminin içinde sanal bir makine kullanabilmek için Virtual Box gibi programlara ihtiyaç duyarız. Donanım olarak ana bilgisayarımızın birincil işletim sistemine müdahale etmeden geride kalan donanımları (CPU, bellek vb.) kullanarak çalışır. Gerçek bir bilgisayar gibi işlev görse de sanal bilgisayar dosyasıdır. Ana bilgisayarımızda yapabileceğimiz tüm işlevleri gerçekleştirebilir mesela uygulama çalıştırabilir. Ana bilgisayarımızın içine Virtual Box gibi harici yazılımlarla kurduğumuz bu sanal makinelerdeki işletim sistemlerine guest denir.

2. **Sanal Makinelerin amacı nedir?**
   - Mevcut işletim sistemini yedekleyebiliriz.
   - Birden çok işletim sistemini aynı anda çalıştırabiliriz ve bunu yaptığımız zaman işlerimiz daha hızlı bitebilir.
   - Uygulamaları bulutta derleme ve dağıtma yapabiliriz.
   - Yeni bir işletim sistemi çıktığında Beta sürümlerini deneyebiliriz.
   - Uygulamaları başlangıçta amaçlandıkları işletim sisteminde çalıştırabiliriz.

3. **CentOS ve Debian arasındaki temel farklar?**
   - CentOS'ta yeni bir sürümün gelmesi çok uzun zaman alır, Debian daha kısa aralıklarla güncellenir.
   - CentOS'un arayüzü komplikedir, Debian ise kolaydır.
   - CentOS'un paket yöneticisi yum, Debian'ın ise apt'dir.

4. **Apt ve Aptitude arasındaki farklar nelerdir?**
   Ortak özellikleri ve aslında neden kıyaslandıklarından başlayacak olursak 2'si de Debian'ın paket yöneticisidir ve 2'si de paket kurma, kaldırma gibi fonksiyonları gerçekleştirebilirler.
   - Aptitude, apt'ye göre daha gelişmiştir ve apt'nin tüm işlevlerini (mark, cache ve get) kapsar. Aptitude'u genelde geliştiriciler kullanır.
   - Aptitude sisteme yüklediğimiz paketleri otomatik izleyip ona bağımlı olarak kurulan paketleri kaldırmamıza olanak sağlar fakat apt'nin böyle bir işlevi yoktur. (apt ancak belirli parametrelerle bunu yapabilir.)

- Aptitude'un arayüzü varken apt'nin yoktur.
- Aptitude modası geçmiş paketleri takip eder. Nedeni ise Debian'ın paketin dağıtımını durdurmuş olması olabilir. Apt ise tüm paketleri bünyesinde bulundurmayı sürdürür.

5. **APPArmor Nedir?**
   Ubuntu'nun 7.10 sürümünden itibaren default olarak dahil edilen önemli bir güvenlik özelliğidir. SELinux ile benzer bir yapısı vardır. Sistem açıldığı anda arka planda sessizce çalışmaya başlar. Sisteme zarar verecek herhangi bir servis yakaladığında ayarları kontrol edip sınırlandırma yapar. Hayati önem taşıdığı için kesinlikle kapatılmaması gerekir. Terminal üzerinde durumunu

```
apparmor-status
```

yazarak kontrol etmedikçe genelde fark etmeyiz.

. . .

b. Simple Setup

1. **Başlatma sırasında makinenin grafik ortamına sahip olmadığından emin olun.**
2. **Bu makineye bağlanmaya çalışmadan önce bir parola istenecektir.**
3. **Son olarak, değerlendirilen öğrencinin yardımıyla bir kullanıcıyla bağlantı kurun. Bu kullanıcı root olmamalıdır.**
4. **Seçilen şifreye dikkat edin, konuyla ilgili getirilen kurallara uymalıdır.**

```
chage -l username
```

yazarak şifre politikalarının her kullanıcıda nasıl olduğunu listeleyebiliriz. Bunlar bize verilen subject dosyasına uygun olarak ayarlanmalı yani
- Şifrenin süresi her 30 günde bir dolmalıdır.
- Şifre değiştirildikten en az 2 gün sonra tekrar değiştirilebilir olmalıdır.
- Kullanıcı şifresinin süresinin dolmasına 7 gün kala bir uyarı mesajı almalıdır.

5. **Değerlendirici yardımıyla UFW hizmetinin başlatıldığını kontrol edin.**

```
sudo ufw status // listeyi gösterir.
sudo systemctl status ufw // ufw aktif mi diye kontrol etmemizi sağlar.
```

6. **Değerlendirici yardımıyla SSH hizmetinin başlatıldığını kontrol edin.**

```
sudo systemctl status ssh
```

7. **Değerlendirici yardımıyla seçilen işletim sisteminin Debian veya CentOS olup olmadığını kontrol edin.**

uname -a // a parametresi all olarak geçer ve tüm bilgileri kapsar.
uname -v // alternatif olarak -v parametresi de kullanılabilir. Kernel sürümü özelliklerini vs. gösterir.

. . .

c. User

1. **Değerlendirilmekte olan öğrencinin oturum açma bilgilerine sahip bir kullanıcının sanal makinede bulunmasını ister.**

id username // kullanıcı bilgilerini gösterir.

2. **Bu kullanıcının eklendiğini ve sudo ve user42 gruplarına ait olup olmadığını kontrol et.** (subject dosyasında root harici oluşturulan kullanıcının hem sudo yetkilerine sahip olabilmesi için sudo grubuna, hem de user42 diye bir grup açılıp ona atanması isteniyor.)

3. **Şifre politikası ile ilgili kuralların yerleştirildiğinden emin olunuz.**

Yeni kullanıcı oluştur.

> ***adduser username → (yüksek seviyeli)***
> ***useradd username → (düşük seviyeli)***

Kurallara uyarak istediğin şifreyi ata.

> ***passwd username***
> ***sudo chage -l username*** *→ oluşturulan kullanıcının şifre politikalarına uyup uymadığını buradan denetleriz. min day, max day, warn message.*

4. **Sanal makinesinde konuyla ilgili istenen kuralları nasıl ayarlayabildiğini açıklamalıdır. Normalde bir veya iki değiştirilmiş dosya olmalıdır.**

> ***sudo vim /etc/login.defs*** *(burada max days 30, min days 2, warn 7 olarak ayarlanır.)*
> ***sudo vim /etc/security/pwquality.conf*** *(Katı kurallarla şifre belirlemek için yüklediğimiz sudo* **apt install libpam-pwquality** kom*utuyla yüklediğimiz paketten sonra oluşan, katı şifreleme politikalarını belirleyen dosya difok minlen10, credit -1, ucredit -1, maxrepeat 3, userchack 1, enforcing 1, enforce_for_root)*

Not: *enforcing* → Eğer sıfırdan farklı bir değer aldıysa yazılan şifre katı şifre politikalarına uymadığı için girilen şifreyi reddeder. Enforcing=0 yazıldığında ise girilen şifre katı şifre politikalarına uymasa da yalnızca warning hatası verir ve girilen düşük seviyeli şifreyi de kabul eder.

5. **Artık yeni bir kullanıcınız olduğuna göre, değerlendirilen öğrenciden önünüzde bir "evaluating" grup oluşturmasını isteyin ve bu kullanıcıya atayın.**

6. **Son olarak, bu kullanıcının "evaluating" grubuna ait olduğunu kontrol edin.**

> ***id username*** *YA DA*
> ***groups***

7. **Değerlendirilen öğrenciden bu şifre politikasının avantajlarını ve uygulamasının avantaj ve dezavantajlarını açıklamasını isteyin.**

- Günümüzde bile birçok insan şifresini 1234567 veya 0000 gibi ardışık ya da

tekrarlanan sayılardan oluşturur. Dolayısıyla bunun önüne geçebilmek için şifre yaratmadan önce bir takım ön koşul sunulur ve bu şartlara uygun şekilde şifre oluşturulması istenir.

- Sunulan ön koşullarda uzunluk, en az 5 karakterden oluşsun gibi şartlar kullanıcıların şifrelerini kısa zamanda unutmasına ve daha birçok sıkıntıya sebep olsa da hackerlar tarafından şifrenin kırılması riskini azaltır.
- minlen=10, 15, 20 uzunluğunda olması aslında kullanıcı için ne kadar zorlu olsa da hacker için kırılması zor bir şifre uzunluğudur.
- Alfabe dışında özel karakterler kullanılması alışılmışın dışına çıkıp klasikleşmiş ifadelerden kaçınmak için önemlidir.
- Büyük küçük harf ve sayısal karakter kullanımı da hacker'ın işini zorlaştıran ve normalden daha fazla şifre kombinasyonu denemesi gereken etkenlerden biridir.
- Katı şifre kuralları sayesinde kırılması imkansız değil ama kırılması zor bir şifre oluşturarak hacker'ın iş yükü ve harcadığı zaman artacağı için hacker da kırılması daha kolay olan parolalara yöneleceğinden dolayı hedef olmaktan çıkmış oluruz.

. . .

d. Hostname and Partitions

1. **Makinenin hostname'inin aşağıdaki gibi doğru biçimde biçimlendirildiğini kontrol edin.** (Yani değerlendirilmekte olan öğrencinin kullanıcıadı42)

```
hostname
```

2. **Oturum açmayı sizinkiyle değiştirerek bu hostname'i değiştirin, ardından makineyi yeniden başlatın.**

3. **Değerlendirilen öğrenciye bu sanal makine için bölümleri nasıl görüntüleyeceğini sorun. Çıktıyı konuda verilen örnekle karşılaştırın.**

> ***lsblk*** *// sanal makine ile ilgili detaylı bilgi verir. Mevcut tüm blok cihazlar hakkında bilgi verir.*

Ekranda görüntülenen bazı bilgiler:
- **SDA:** İlk diski temsil eder. Sonraki blok cihazlar hakkında bilgi verir.
- **sr0:** Çıkarılabilir cihazı temsil eder.
- **cd -rom:** Listelenen cihazlar içinde çıkarılabilir olup olmayanları gösteren bölüm "RO"dur. (RO = removable)
- **RO = 0** ise çıkarılamaz blok cihaz
- **RO = 1** ise çıkarılabilir blok cihaz
- **sda:** Birincil cihazdır. sda (1– 4) arası öncelikli cihazları temsil ederken sda4 sonrası logical birimler olduklarını gösterir.
- **mountpoint:** Cihazın monte edildiği bağlama noktasını görüntüler.

4. **LVM nedir, nasıl çalışır? Açıklayınız.**

- LVM (logical volume manager) ile birden fazla diski tek bir disk bölümü olarak kullanabilir ve disk yönetimi işlemlerinde çok kolaylık sağlar. Disk alanının yetersiz kaldığı durumlarda LVM ile oluşturulan disk veri kümesine disk bölümleri ilave edebilir, ihtiyaca göre disk alanı boyutlandırılabilir.
- Büyük disk alanı ihtiyacı olan sistemlerde LVM ile disk veri kümeleri oluşturularak ya da sisteme yeni bir disk ilave edilerek toplam disk boyutu artırılabilir.
- VMlerde de ilk olarak tüm disk alanı sanal makineye tahsis edilmez. İhtiyaç olduğunda ise lvm sayesinde sanal makineye ihtiyacı kadar alan yeniden tahsis edilir, boyutlandırılır. Bu yöntem ise verimi arttırır. Kullanıcının dosyalarını silmeden veya bir yere taşıyıp tekrar yüklemeden alana sahip olması anlamına gelir.
- Aynı zamanda eski sürücüdeki belgeler değişikliğe ve kesintiye uğramadan yeni sürücüye aktarılabilir.

SUDO

1. **"Sudo" programının sanal makineye düzgün şekilde yüklenip yüklenmediğini kontrol edin. Öğrenci artık yeni kullanıcınızı "sudo" grubuna atadığını göstermelidir.**

> ***usermod -aG sudo username*** *YA DA*
> ***groups username***

2. **Sudo'nun değerini ve işleyişini açıklayınız.**

- Sudo, kullanıcıların sisteme yönetici olarak bağlanmalarını gerektirmeden admin yetkisi gerektiren işlemleri yapabilmesini sağlar.
- Sudo ile belirli yönetici yetkilerini kullanacak kullanıcılara root parolasının paylaşılması gibi güvenlik açısından sorun yaratabilecek durumlar engellenmiş olur.
- Sudo yetkisiyle yapılan işlemlerde kimin hangi işlemi yaptığının takibi daha kolaydır. sudo log dosyasından bu verilere erişebiliriz.

3. **Kuralların uygulanıp uygulanmadığını kontrol ediniz.**

> ***sudo visudo***

4. **“/var/log/sudo/” klasörünün var olduğunu ve en az bir dosyaya sahip olduğunu doğrulayın. Bu klasördeki dosyaların içeriğini kontrol edin, Sudo ile kullanılan komutların geçmişini görmelisiniz.**

> ***cd /var/log/sudo***
> ***ls -l***

5. **Son olarak, sudo üzerinden bir komut çalıştırmayı deneyin.**
Örnek: Bir kullanıcının şifresini sudo yardımı ile değiştir.

> ***passwd username***
> ***passwd ornekSifre***

6. “/var/log/sudo/” klasöründeki dosya(lar)ın güncellenip güncellenmediğine bakın.

> ***sudo cat /var/log/sudo/sudo.log*** *// değiştirilen şifre bilgisinin buraya gelip gelmediğini kontrol et.*

. . .

d. UFW

1. **UFW programının sanal makineye düzgün yüklenip yüklenmediğini kontrol et. Ardından düzgün çalışıp çalışmadığını kontrol et.**

> ***systemctl status ufw*** *// sadece 4242 portunun açık olduğu görüntülenir.*
> ***systemctl status ufw*** *// active olmalı*

2. **UFW (Uncomplicated Firewall) nedir ve neden kullanılır?**

UFW: Güvenlik duvarı yönetim aracıdır. Hem konsol hem de grafiksel arayüz üzerinden port ve güvenlik duvarı işlemlerimizi gerçekleştirmeye yarayan araçtır.

- Firewall uygulamasıdır. UFW ile ipv4 veya ipv6 firewall güvenlik yönetimi yapmamıza izin verir.
- Genel olarak SSH işlemleri içerisinde port açma/değiştirme/kapatma gibi eylemlerde kullanılır.
- Default olarak birçok portun kapalı durumda tutulduğu sistemlerde açılan her

port bir güvenlik sorunu oluşturabilir. Dolayısıyla bu süreç kontrollü bir şekilde yönetilmeli ve iletişimin devam etmediği portlar tekrar pasif konumda tutulabilir.

- Firewall, hangi paketlerin sisteme girip çıkmasına izin verileceğine karar veren programdır. Hangi bağlantı noktasının dış dünya ile (hatta yerel ana bilgisayar üzerinde) iletişim kurmasına izin verildiğine karar vermek güvenlik duvarının sorumluluğundadır.
- Güvenlik duvarı, bir ya da birden fazla bilgisayarın ağ üzerinden diğer bilgisayarlara olan erişimlerini engellemek, izin vermek veya sınırlamak için kullanılan yazılımdır.
- Firewall, zararlı yazılımlara karşı bir duvar örer ve bunların ağ yolu ile bilgisayara sızmasını önler. Kısacası firewall internette güvenli kalmanın yöntemlerinden biridir.

. . .

e. SSH

1. **SSH hizmetinin makineye düzgün yüklenip yüklenmediğini kontrol edin. Düzgün çalışıp çalışmadığını kontrol edin.**

2. **SSH nedir ve neden kullanılır?**

SSH: Uzak sunucu bağlantı protokolüdür. Güvenli olmayan bir ağ üzerinde güvenli şekilde çalıştırılması için şifreleme ile kullanılan ağ protokolüdür.

- Uzak sunucu bağlantı protokolüdür. Güvenli olmayan bir ağ üzerinde güvenli şekilde çalıştırılması için şifreleme ile kullanılan ağ protokolüdür.
- Çoğu kullanıcı SSH bağlantısını default ayarlar ile kullanıyor. Fakat bu kullanım güvenlik sorunlarına yol açıyor. SSH erişimi dışarı açık bir sunucunun root parolasının kırılması, sunucu açıldıktan sonra dakikalar içersinde gerçekleşebilir. (Projede ssh erişmini root kullanıcısına kapatarak güvenli bir ssh bağlantısı oluşturmaya çalışıyoruz.)

> ***etc/ssh/sshd_config*** *klasöründe* ***permitrootlogin no*** *diyerek ssh erişimini root kullanıcısına yasaklıyoruz.*

- Diğer önemli bir değişiklik ise port değişikliğidir. SSH bağlantısının port'u default olarak 22'dir. Portu değiştirerek saldırganların 22 protundan sunucya erişimini engelleyeceğiz. (Kendimiz 4242 portundan bağlanarak güvenli bir SSH bağlantısı oluşturmaya çalışıyoruz.)
- Sadece belirlediğimiz adreslerden SSH erişimi sağlamak istiyorsak UFW burada çok faydalı olur.
- UFW'yi ilk olarak aktif hale getirmeliyiz. UFW enable, ufw allow 4242 gibi komutlar sadece belirlenen SSH adreslerinden erişim yapabilmemizi sağlar. SSH ile belirttiğimiz 4242 portu ***önleme ek bir önlem*** olarak görülebilir.

3. **SSH hizmetinin yalnızca 4242 numaralı bağlantı noktasını kullandığını doğrulayın. Değerlendirilen öğrenci, yeni oluşturulan kullanıcı ile giriş yapabilmeniz için SSH kullanmanıza yardımcı olmalıdır. Bunu yapmak için bir anahtar veya basit bir şifre kullanabilirsiniz. Değerlendirilen öğrenciye bağlı olacaktır. - Tabii ki konuda belirtildiği gibi "root" kullanıcısı ile SSH kullanamayacağınızdan emin olmalısınız.**

> ***ssh root42@localhost -p 4242*** *// root olarak dene ve kabul edilmediğini göster.*
> ***ssh username@localhost -p 22*** *// 22 portundan dene ve kabul edilmediğini göster.*
> ***ssh username@localhost -p 4242*** *// son olarak giriş sağlayabiliriz.*

f. Script Monitoring

1. **Kodu göstererek senaryoların nasıl çalıştığını açıklayın.**

> ***vim /usr/local/bin/monitoring.sh***

- uname -a → Sırasıyla şunları verir: kernel, hostname, kernel ana dağıtım bilgisi, kernel versiyon, işlemcinin mimari bilgileri, 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 sayısı
- Free bellek hakkında bilgi, kullanılan alan, kapasite, boş alan vs.. Free -m: mebi byte (megabyte değildir. 2'nin katları anlamına gelen ikili sistemden gelir.)
- awk komutu → grep'e benzer şekilde örüntü temelli tarama işlemi
- top → sunucu hakkında anlık istatistikleri verir.

2. **Cron nedir?**

- Bir görevi belirli bir zaman sonra tekrarlamak için komut verme işlemine cron denir. Belirli işlerin belirli zamanlarda tekrarlanarak yapılmasını bir otomasyona bağlayarak kolaylaştırır.
- cron job zamanlanmış görev anlamına gelir. İleri tarihli bir görevin bir seferlik veya

belli aralıklarla tekrar ederek yapılmasını istiyorsak kullanılacak komut dosyası.

3. **Sunucu başladığından itibaren her 10 dakikada bir çalışacak şekilde komut dosyasını nasıl kurduğunu göster.**

> ***crontab -u root -e*** *// u parametresi root olarak bir, e parametresi ise editle anlamına gelir.*
>
> ****/10 * * * * bash /usr/local/sbin/monitoring.sh***
> *Sırasıyla: m -> dakika, h -> saat, ayın günleri, yılın ayları, haftanın günleri*
> *Örnek:* ***12345 → 4. ayın 3. günü ve her haftanın 5. gününde saat 02:01'de*** *çalışır.*

4. **Komut dosyasının düzgün çalışması doğrulandıktan sonra, bu komut dosyasının her dakika çalışmasını sağlayın.**

> ****/1 * * * * bash /usr/local/sbin/monitoring.sh***

5. **Son olarak, sunucu başlatıldığında komut dosyasının kendisini değiştirmeden komut dosyasının çalışmasını durdurmalısınız. Bu noktayı kontrol etmek için sunucuyu son 1 kez başlatmanız gerekecek.**

> ***sudo systemctl status cron*** *// cron'un durumu hakkında bilgi verir.*
> ***sudo systemctl stop cron*** *// o an çalışan cron durdurulur ancak reboot sonrası active halde çalışır çünkü enable*
> ***sudo systemctl disable cron*** *// reboot sonrası çalışmaz ama disable öncesi stop demezseniz active haldedir ve reboot yapana kadar o an ki cron çalışmaya devam eder.*
> ***reboot*** *// sanal makineyi yeniden başlatmamızı sağlar.*

- Başlangıçta komut dosyasının hala aynı yerde bulunduğunu, haklarının değişmediğini ve değiştirilmediğini kontrol etmek gerekecektir.

> ***NOT:*** */etc dosyası ve alt dizinlerinde sistemle ilgili bütün konfigürasyon dosyaları bulunur.*

 --