Born2Beroot

Sanal Makina Nasıl Çalışır

1. Birden çok işletim sistemi kullanmaya imkan sağlar.
2. Bilgisayarın sanal örneğini çalıştırırlar.
3. Fiziksel Olmayan bilgisiyar dosyasıdır.
4. Yazılım Tabanlı, “sanal” bir sürümünü oluşturma işlemidir.

CentOs ve Debian arasındaki temel farklar.

1. Debian apt’dir, CentOS yum.
2. CentOS kararlı bir yapıdadır(Az ve Öz güncelleme alıyor). Debian daha az kararlı(Çok Güncelleme Alıyor).
3. CentOS redhat tarafından lanse edilirken, Debian bireysel lanse ediliyor.
4. CentOS kendi güvenlik sistemiyle geliyor(Güvenlik Sisteminin Adı: Selinux).
5. CentOS kurumsal alanda daha çok tercih ediliyor, Debian bireysel.

Sanal Makinenin Amacı

1. Bir program açar gibi ikinci bir işletim sistemi çalıştırmak.
2. Birbirinden izole edilmiş, birden fazla işletim sistemi kurabilirsin.
3. Virüslü düşündüğünüz bir dosyayı burada açabilirsiniz.
4. Sanal ortamın dışına çıkamadığı için büyük bir güvenlik sağlıyor.

Aptitude ve APT arasındaki farklar.

1. Apt “Advanced Packaging Tool” (Gelişmiş Paket Aracı).
2. Aptitude işlevsellik açısından daha geniştir. Aptitude get, mark ve cache de dahil olmak üzere apt’nin işlevlerini bünyesinde barındırır.
3. Aptitude arayüze sahipken, apt sahip değildir.
4. Aptitude sisteme yüklendiğinde paketleri otomatik olarak izler. APT bu konuda yetersizdir.
5. Aptitude paketlerin ismi, tanimları, bağımlıkları vb. Gibi bir çok bilgiye erişebilir. Güçlü bir filtreleme ve arama yapısına sahiptir.
6. Aptitude eski paketleri takip eder. APT bu tur paketleri bünyesinde bulundurur.
7. Aptitude yaptığınız işlemlerin kaydını tutar(/var/log/aptitude)

APPArmor Nedir?

1. AppArmor bir güvenlik özelliğidir, Arka planda sessizce çalışır ve sisteme zarar verebilecek uygulamarı kontrol edip, sınırlandırır.
2. Selinux ve AppArmor ikiside MAC güvenliğini sağlar.

Simple Setup.

- Şifre Politikalarının nasıl olduğunu listeler.

```
chage -l <username>
```

- UFW Hizmetinin başlatıldığını kontrol eder.

```
sudo ufw status [numbered] (numbered: 1, 2, 3 diye sıralar.)
sudo systemctl status ufw
```

- Debian veya CentOS olup olmadığını kontrol eder.

```
uname -a (Tüm Bilgileri İçerir)
uname -v (Karnel Sürümünü ve yayınlandığı tarihle birlikte gösterir)
```

User.

/bu

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

```
id <username> (kullanıcı bilgilerini gösterir.)
```

- Bu kullanıcının eklendiğini ve "sudo" ve "user42" gruplarına ait olduğunu kontrol edin. *(!!!! pdf'te root harici oluşturulan kullanıcının hem sudo yetkilerine sahip olabilmesi için sudo grubuna, hem de user42 diye bir grup açılıp ona atanması isteniyor.)*

```
groups (grupları listeler)
```

- Aşağıdaki adımları takip ederek şifre politikası ile ilgili konu ile ilgili kuralların yerleştirildiğinden emin olunuz.

- İlk olarak, yeni bir kullanıcı oluşturun.

```
adduser <username> (yüksek seviyeli)
useradd <username> (düşük seviyeli kullanıcı)
```

- Konu kurallarına uyarak istediğiniz şifreyi atayın.

```
passwd <username>
sudo chage -l <username> (oluşturduğun kullanıcının şifre
politikalarına uyup uymadığını buradan denetlersin.
min day, max day, warn message)
```

- Değerlendirilen öğrenci şimdi size 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 ayalanır)
sudo /etc/security/pwdquality.conf (Katı kurallarla şifre belirlemek
için yüklediğimiz) **sudo apt install**

libpam-pwquality komutuyla yüklediğimiz paketten sonra oluşan,
katı şifreleme politikalarını belirleyen dosya difok 7
minlen 10, lcredit -1, ucredit -1,dcredit -1, maxrepeat 3, userchack 1, enforcing 1, enforce_for_root**)
```

- **enforce_for_root**, yazdığımızda root yetkilerine difok hariç hepsini ekliyor.
- **!!! enforcing** Eğer sıfırdan farklı bir değer aldıysa yazılan şifre katı şifre politikalarına uymuyorsa 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.
- Artık yeni bir kullanıcınız olduğuna göre, değerlendirilen öğrenciden önünüzde bir **"evaluating**" grup oluşturmasını isteyin ve bu kullanıcıya atayın.

```
addgroup <evaluating> (grubu kur)
cat /etc/group | grep evaluating (kurulan grubu gör)
usermod -aG <groupname> <username> (evaluating grubuna bir kullanıcı ata)
```

- Son olarak, bu kullanıcının "evaluating" gruba ait olduğunu kontrol edin.

```
id <username> YA DA
cat /etc/group | grep evaluating YA DA
groups <username>
```

Şifre politikasının avantaj ve dezavantajlarını açıklayın.

1. İnsanlar genelde basit şifreler seçmeye meyilli olduğundan. Şifre oluşturmadan önce bir takım ön koşullar getirilir. Böylelikle basit şifre olasılıklarının önüne geçiliyor.
2. Şifre politikaları çok fazla koşul istediğinden genelde şifre unutmaları, hesap kilitlenmesi ve şifre oluştururken yine tekrar aynı kurallar içerisinde seçme gibi vakit kayıpları olabiliyor.
3. Hackerlar tarafından şifre tahmin riskini azaltıyor.
4. Saldırganın iş yükü ve harcadığı zaman artığı için hedef olmaktan çıkıyoruz.

Hostname and Partitions

- Makinenin hostname'inin aşağıdaki gibi doğru biçimde biçimlendirildiğini kontrol edin. (Yani değerlendirilmekte olan öğrencinin <intrakullanıcıadı42>)

```
hostname
```

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

```
Sudo hostnamectl set-hostname <new-name>
Sudo vim /etc/hosts
Vim içinde 127.0.1.1 yanına newhostname'inin yaz
Reboot
-Hostname
```

- Yeniden başlatıldığında ana bilgisayar adı güncellenmemişse değerlendirme burada durur.
- Artık makineyi orijinal hostname olarak geri yükleyebilirsiniz.
- Değerlendirilen öğrenciye bu sanal makine için bölümleri nasıl görüntüleyeceğini sorun. Çıktıyı konuda verilen örnekle karşılaştırın.

```
lsblk (sanal makine bölümleri ile ilgili ayrıntılı bilgiler verir.
Mevcut tüm blok cihazlar hakkında bilgi verir.)
```

- ***çıkan ekran hakkındaki bazı bilgiler...***
- SDA ilk diski temsil eder. Sonraki blok cihaz bölümleri sda'nın yanında ondalık sayı alarak gösterilir.
  - sr0: çıkarılabilir cihazı temsil eder. 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 öncelikli cihazları temsil ederken Sda4 sonrası logical birimler olduklarını gösterir.
- mountpoint = Bu, cihazın monte edildiği bağlama noktasını görüntüler.

LVM'nin nasıl çalıştığı ve bunun neyle ilgili olduğu hakkında bir açıklama.

1. Büyük disk alanı ihtiyacı olan sistemlerde LVM ile disk veri kümeleri oluşturularak yada sisteme yeni bir disk daha eklenerek toplam disk boyutu arttırılabilir.
2. LVM(logical volume manager) ile birden fazla diski tek bir disk bölümü olarak kullanabilir ve disk yönetimi işlemlerinde büyük kolaylık sağlar.

SUDO

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

```
usermod -aG sudo <username> YA DA
cat /etc/group | grep sudo YA DA
groups <username>
```

  - PDF, sudo için katı kurallar uygular. **Öğrenci, ilk adımda kendi seçtiği örnekleri kullanarak sudo'nun değerini ve işleyişini açıklamalıdır**
    - Sudo, sıradan kullanıcıların sisteme yönetici olarak bağlanmaları gerekmeden yönetici yetkisi gerektiren işlemleri
      yapabilmesini sağlayan bir programdır.
    - Sudo ile belirli yönetici yetkilerini kullanacak kullanıcılara root parolasının paylaşılması gibi güvenlik açısından sıkıntı
      çıkartabilecek durumlar engellenmiş olur.
    - Sudo yetkisiyle yapılan işlemlerde kimin hangi işlemi yaptığının takibi daha kolaydır sudo Log dosyasında gözüküyor kimin
      hangi işlemi yaptığı...
  - İkinci adımda, PDF'in getirdiği kuralların uygulanmasını size göstermelidir.

```
sudo visudo** YA DA
sudo vim /etc/sudoers
```

- "/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
```

- Son olarak, sudo üzerinden bir komut çalıştırmayı deneyin.
  - mesela bir kullanıcının şifresini değiştir sudo yardımı ile
- "/var/log/sudo/" klasöründeki dosya(lar)ın güncellenip güncellenmediğine bakın.

```
sudo cat /var/log/sudo/sudo.log (komutu ile değiştirdiğin şifrenin
                                 bilgisi buraya gitmiş mi bak)
```

UFW ve UFW ne olduğunu ve onu kullanmanın değerini açıklamalıdır.

"UFW" programının sanal makineye düzgün şekilde yüklenip yüklenmediğini kontrol edin. Düzgün çalışıp çalışmadığını kontrol edin.

```
- systemctl status ufw (yapıldığında sadece 4242 portunun açık
                        bırakıldığı gözükmelidir)
- systemctl status ufw (active olmalı)
```

1. ipv4 ve ipv6 firewall güvenlik yöntemi yapmamıza izin verir.
2. Güvenlik işlerini yapmamıza yarayan güvenlik duvarı.
3. İptables güvenlik duvarı yapılandırmasını kolaylaştırmak için UFW geliştirildi.
4. Firewall, zararlı yazılımlara karşı bir duvar örür ve bunların ağ yolu ile bilgisayara sızmasının önüne geçer.
5. güvenlik duvarı dediğimiz yapı temelde, bilgisayarımızın ya da sunucumuzun internet dünyasında güvenli hale gelmesini sağlayan kurallar setidir. Belirli portların açılması, kapatılması, sınırlanması, ip bazlı engelleme vs pek çok spesifik kural tanımlanabiliriz.

- UFW'deki aktif kuralları listeleyin. 4242 numaralı bağlantı noktası için bir kural bulunmalıdır.

```
sudo ufw status numbered (8080 numaralı bağlantı noktasını açmak için
yeni bir kural ekleyin. Etkin kuralları listeleyerek bunun
eklendiğini kontrol edin.)
sudo ufw allow 8080 (Son olarak, değerlendirilen öğrencinin
```

```
                    yardımıyla bu yeni kuralı silin.)
sudo ufw delete <silinecek satır>
```

SSH VE SSH NE OLDUĞUNU VE ONUN KULLANMANIN DEĞERİ NEDİR?

- SSH hizmetinin sanal makineye düzgün şekilde yüklenip yüklenmediğini kontrol edin.

```
vim /etc/ssh/sshd_config (SSH hizmetinin sadece 4242 portundan
çalıştığını gösteren –> #port 4242 ve Güvenlik sebebiyle SSH'a
root olarak bağlanmayı yasaklayan PermitRootLogin no olmalı)
```

- Düzgün çalışıp çalışmadığını kontrol edin.

```
systemctl status ssh (port 4242 için active ve enable olmalı)
```

1. Linux sunuculara erişim sağlamak için SSH protokolü kullanıyoruz. Yani uzaktaki bir sunucuya bağlanmak, ona komutlar ve dosyalar göndermek üzere kullanılan şifrelenmiş bir uzaktan sağlayıcı protokolüdür. Çoğu kullanıcı SSH bağlantısını varsayılan ayarlar ile kullanıyor. Ancak bu şekilde bir kullanım güvenlik risklerini de beraberinde getiriyor.
   SSH erişimi dışarı açık bir sunucunun root parolasının kırılması sunucu açıldıktan sonra dakikalar içinde gerçekleşebilir. (Biz de projede ssh erişimini root kullanıcısına kapatarak güvenli bir ssh bağlantısı oluşturmaya çalışıyoruz. Etc/ssh/sshd_config klasöründe permitrootlogin no diyerek ssh erişimini root kullanıcısına yasaklıyoruz...)
2. 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)
3. Sadece belirlediğimiz adreslerden SSH erişimi sağlamak istiyorsak güvenlik duvarı(UFW) burada çok işe yarar
4. UFWyi ilk olarak aktif hale getiriyoruz. Ufw enable, ufw allow 4242 gibi komutlar sadece belirlenen SSH adreslerinden

erişim yapabilmemizi sağlar ve SSH ile belirttiğimiz 4242 portu ÖNLEMİNE EK BİR ÖNLEM OLARAK GÖRÜLEBİLİR....

5. 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 aoner42@localhost -p 4242 (giriş sağla son olarak)
```

Script Monitoring

1. Size kodu göstererek senaryolarının nasıl çalıştığını açıkamalıdır.

```
vim /usr/local/sbin/monitoring.sh
```

▼ 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
Awk komutu -> grepe benzer şekilde örüntü temelli tarama işlemi
Top -> sunucu hakkındaki anlık istatistikleri verir.

Cron Nedir

1. belirli işlerin belirli zamanlarda tekrarlanarak yapılmasını bir otomasyona bağlayarak kolaylaştırır. Bir görevin ilerleyen

   zamanda tekrarlamak için komut verme işlemine cron denir.

2. ❖ cron Job zamanlanmış görev anlamına gelir. İleri tarihli bir görevin bir seferlik veya belli aralıklarla tekrar ederek yapılmasını istiyorsak kullanılacak komut dosyası.

- Değerlendirilen öğrencinin, sunucu başladığından itibaren her 10 dakikada bir çalışacak şekilde komut dosyasını nasıl kurduğu.

```
crontab -u root -e (crontab'e -u—> root olarak gir -e —> editle)
/10 * * * * bash /usr/local/sbin/monitoring.sh.
(*dakikası)(*saati)(*ayın günü)(*yılın ayı)(*haftanın günü)
——> bu işlemi gerçekleştir örn: 34552 (5. Ayın beşinci
günü ve her salısı saat 04:03'te)
```

- Komut dosyasının doğru çalışması doğrulandıktan sonra, değerlendirilen öğrenci bu komut dosyasının her dakika çalışmasını sağlamalıdır.

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

- Komut dosyasının dinamik değerlerle doğru şekilde çalıştığından emin olmak için istediğinizi çalıştırabilirsiniz.
- Son olarak, değerlendirilen öğrenci, sunucu başlatıldığında komut dosyasının kendisini değiştirmeden komut dosyasının çalışmasını durdurmalıdır. Bu noktayı kontrol etmek için sunucuyu son bir kez yeniden başlatmanız gerekecek.

```
sudo systemctl status cron (cronun durumu hakkında bilgi)
sudo systemctl stop cron (o an çalışan cron durdurulur
ancak reboot sonrası Active halinde çalışır çünkü enable)

sudo systemctl disable cron (reboot sonrası çalışmaz ama
disable öncesi stop demezseniz Active halindedir ve reboot
yapana kadar o an ki cron çalışmaya devam eder)

reboot
```

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

!!!!/etc dosyası:etc dosyası ve alt dizinlerinde sistemle ilgili bütün konfigürasyon dosyaları bulunur.