SCALE FOR PROJECT BORN2BEROOT

1. Introduction

Lütfen aşağıdaki kurallara uyunuz: …

2. Guidelines

- Git reposunda döndürülen çalışmaya not verin. Double-check that the Git repository belongs to the student.
- Ayrıca, boş bir klasörde "git klonunun" kullanıldığını kontrol edin.
- Not vermeyi kolaylaştırmak için kullanılan tüm komut dosyalarını (test veya otomasyon komut dosyaları) birlikte inceleyin.

3. Preliminaries

- Savunma ancak değerlendirilen öğrenci veya grup mevcutsa gerçekleşebilir. Böylece herkes birbiriyle bilgisini paylaşarak öğrenir. - Herhangi bir çalışma gönderilmemişse (veya yanlış dosya, yanlış dizin veya yanlış dosya isimleri) not 0 olur ve değerlendirme süreci sona erer.
- Bu proje için, onların Git reposunu istasyonlarında klonlamanız gerekiyor.

4. General instructions

- "signature.txt" dosyasının klonlanmış havuzun kökünde bulunduğundan emin olun.
- "signature.txt" dosyasındaki imzanın, değerlendirilecek sanal makinenin ".vdi" dosyasındakiyle aynı olup olmadığını kontrol edin.
- Basit bir "fark", iki imzayı karşılaştırmanıza izin vermelidir.
- Değerlendirilen öğrenciye ".vdi" dosyasının nerede olduğunu sorun. - Önlem olarak, bir kopyasını saklamak için ilk sanal makineyi çoğaltabilirsiniz.
- Değerlendirilecek sanal makineyi başlatın.
- Bir şey beklendiği gibi çalışmıyorsa veya iki imza farklıysa, değerlendirme burada durur.

5. Mandatory part

- Proje, katı kurallara uyarak bir sanal makine oluşturmak ve yapılandırmaktan ibarettir. Değerlendirilen öğrenci savunma sırasında size yardımcı olmak zorunda kalacaktır. Aşağıdaki noktaların tümüne uyulduğundan emin olun.

a. Project overview

- ***Değerlendirilen öğrenci size basitçe şunları açıklamalıdır :***

- **Bir sanal makine nasıl çalışır ?**

- **Virtual Box vb. programlar ile** işletim sistemi içinde sanal bir makine oluşturularak **birden çok işletim sistemi kullanmaya imkan** sağlanır.
- Sanal makineler, donanımdan ayrılmış katmanda bir **bilgisayarın sanal örneğini çalıştırırlar**.
- Sanal makineler, işletim sistemini bir yazılım yerine bilgisayarın **yerel donanımında çalıştıklarına inandırarak çalışır,** dolayısıyla bir bilgisayarın tüm kabiliyetlerine sahiptir.
- Sanal makine (Virtual Machine-VM), gerçek bir bilgisayar gibi işlev gören ama **fiziksel olmayan bir bilgisayar dosyasıdır aslında…**
- Diğer fiziksel bilgisayardan farklı değildir. Dosyalarınızı depolamak için bir **CPU(işlemci), bellek ve disklere sahiptir** ve **gerekirse internete** bağlanabilir. Sanallaştırma, **fiziksel bir bilgisayardan "ödünç alınan"** ayrılmış miktarlarda CPU, bellek ve depolama ile bir bilgisayarın **yazılım tabanlı, "sanal" bir sürümünü oluşturma işlemidir.**
- Depolama için pay almakla birlikte fiziksel pcden ayrılmış, **fiziksel bilgisayara müdahale edemeyen alanı da temsil eder.** Birincil bilgisayar müdahale edemez.
- **VB anapc donanımını** farklı işletim sistemleri arasında **paylaştırır.** Yani işlemciyi, belleği, diski normalde tek bir işletim sistemi kullanacakken bu sayede **birden fazla işletim sistemi kullanabilir**. Misafir işletim sistemleri bu sayede sanal bir makinede çalıştıklarını fark etmeden, gerçek bir donanım üzerinde çalışıyormuş gibi işlem yaparlar…
- Sanal makineler, bilgisayarın işletim sistemindeki bir pencerede çalışır. Kullanıcılar bu ortamlarda **uygulamalar çalıştırabilir, veri depolayabilir** ve herhangi bir bilgisayarda yapılabilecek herhangi bir eylemi gerçekleştirebilir.
- Sanal makinelerin kurulduğu fiziksel işletim sistemlerine host(ana bilgisiyar) virtual box yardımıyla açılan yazılımsal işletim sistemleri ise guest (misafir) denir.

- **CentOS ve Debian arasındaki temel farklar.**

- Debian paket yöneticisi **apt'di**r Centos'un **yum**
- CentOS'un **yeni sürümleri genellikle uzun bir aradan sonra** yayınlanır ve bu nedenle bu sistemler çok kararlıdır. **Debian** Centos'a göre **daha fazla güncelleme** alıyor.
- **Centos kurumsal alanda** daha fazla tercih edilir. **Debian ise bireysel kullanıcılar** açısından daha çok tercih edilir.
- **Centos RedHat t**opluluğu tarafından desteklenir. **Debian bireyler tarafından** desteklenir.
- Centos kendine ait bir **siber güvenlik sistemiyle** gelir adı da **Selinux.**
- **Centosun arayüzü karışıktır**, Debianın daha kolay.

- **Sanal makinelerin amacı.**
    - Örneğin bilgisayarınızda Windows bulunuyor. Fakat siz aynı anda bir başka işletim sistemine daha ihtiyaç duyuyorsunuz. Bu durumda bilgisayarınıza **Pardus ya da MacOS** kurabilir, bunları aynı anda çalıştırabilirsiniz. Tıpkı Windows cihazınızda **bir program açar gibi** ikinci bir işletim sistemini çalıştırabilirsiniz.
    - Aynı makinede, **birbirinden izole edilmiş birden çok işletim sistemi aynı anda** var olabilir; yani **farklı bir makineye ihtiyacınız olmaz.**
    - Farklı işletim sistemleri aynı anda aynı bilgisayar üzerinde çalıştırılabildiğinden **işlem sürecini hızlanır…**
    - Hazırlamış olduğunuz **bir web sitesinin diğer işletim sistemlerinde nasıl çalışacağını,** nasıl sonuçlar doğuracağını test edebilirsiniz.
    - Ya da **virüslü olduğunu düşündüğünüz bir dosyayı** burada açabilir ve test edebilirsiniz.

- Sanal makinelerin en önemli avantajları **büyük bir güvenlik sağlıyor** olmalarıdır. Çünkü **sanal makinen** sağladığı kaynağı kullanan yazılım, **içinde bulunduğu sanal ortamın dışına çıkamaz**. Host üzerinde bir değişikliğe sebep olmaz.
- Geliştiricilerin yeni test senaryolarını çalıştırmak, farklı işletim sistemlerindeki test süreci aşamasını hızlandırmak.
- Mevcut işletim sistemini yedekleme.
- **Eski bir işletim sistemini yükleyerek** eski bir uygulamayı çalıştırmak.
- Geliştiricileriniz için tamamen yeni bir ortam sağlamaktan çok daha basittir. Sanallaştırma, geliştirme ve test senaryolarını çok daha hızlı çalıştırma sürecini kolaylaştırır.
- Bir VM'de konuk işletim sisteminin kullanılması güvenliği şüpheli uygulamaları çalıştırmanıza ve ana bilgisayar işletim sisteminizi korumanıza olanak sağlar.

- Değerlendirilen öğrenci Debian'ı seçtiyse: **aptitude ve apt'nin arasındaki farkı** ve **APPArmor'un ne olduğunu açıklamalıdır.**

Aptitude ve Apt arasındaki farklar.

- - Apt ve aptitude … İkisi de Debian'ın paket yöneticisidir ve ikisinin de paket kurma, kaldırma, arama vs. her türlü etkinliği gerçekleştirebilir.
- Apt "**Advanced Packaging Tool**" (**APT**) "(Gelişmiş Paket Aracı)
- **Aptitude işlevsellik** açısından apt den daha geniştir. Aptitude **get, mark ve cache** de dahil olmak üzere apt'nin işlevlerini bünyesinde barındırır.
- Aptitude arayüze sahipken apt sahip değildir.
- **Aptitude,** sisteme yüklediğiniz **paketleri otomatik olarak izler**…. Diyelimki A paketini kurdunuz, bu paket kendisine bağımlı olan bir kaç farklı kitaplık ve paket daha kurdu, daha sonra bu A paketini sistemden kaldırmak istediğinizde; -şayet- A paketini kurarken sisteminize yüklemiş olduğunuz diğer kitaplıklar, paketler öksüz kalacaksa onların da sisteminizden kaldırır. **Apt-get bu konuda yetersizdir. Aptitude,** paketlerin kurulumunda o paket tarafından **tavsiye edilen paketleri de kurar**… A paketini kurarken, A paketinin yanında tavsiye edilen başka bir B paketi de olabilir.
- Aptitude **paketlerin ismi, tanımları, bağımlılıkları vb. gibi bir çok bilgiye** kolayca ulaşabilmenizi saglar. Ayrıca çok **güçlü filtreleme ve arama** yeteneklerine sahiptir. Bu sayede **aradığınız pakete hızlıca ulaşabilirsiniz.**
- **Aptitude, modası geçmiş paketleri takip eder**…. Debian bir paketin dağıtımını durdurmuş olabilir. **Apt bu tür paketleri sisteminizde bulundurmaya devam eder**.
- **Aptitude yaptığınız işlemlerin kaydını tutar….** aptitude ile **kurulan, kaldırılan, güncellenen paketlerin kaydını /var/log/aptitude** dosyasında tutar. Bu kayit gecmiste paketler ile ilgili ne tur islemler yapmis oldugumuzu gorebilmemiz acisindan cok onemlidir…
- Yani apt komutu apt-cache ve apt-get get- mark komutlarının çok kullanılan komutlarını bir araya getirip, nadir kullanılan ve anlaşılması güç olan komutlarını bir kenara bırakıyor… **Apt komutu apt-cache ve apt-get komutlarına göre biraz daha ALL in ONE d**iyebileceğimiz bir daha geniş işlevselliğe sahip bir komut olmuş durumda. Ayrıca son kullanıcı memnuniyetini düşünülerek yapılmış bir komut

APPArmor nedir?

- **AppArmor,** Ubuntu 7.10'dan beri Ubuntu'ya varsayılan olarak dahil edilen önemli bir **güvenlik özelliğidir. Arka planda sessizce çalışır**. **Sisteme zarar verebilecek ayarları, servisleri ve diğer ayarları kontrol edip sınırlandırır.** Sistem açılışlarında **default** olarak **aktiftir.**
- Ubuntu için geliştirilmiş olan bir "Security Framework" yapısıdır. *Red Hat* ve *Fedora* sistemlerdeki **SELİNUX benzer bir yapısı** bulunmaktadır. Sistemin arka planında **her daim çalışmaya devam** eder ve siz ne olduğunu genelde fark etmezsiniz terminalden durumuna bakmadıkça veya bildirimlerini görmedikçe ne olduğunu hiç araştırmayacak bile olabilirsiniz.
- AppArmor **sisteme verilebilecek zararı sınırlandırır** veya yapılan bu işlemi tamamen durduran bir uygulamadır.

- **Selinux ve AppArmor** ikisi de MAC(Mandatory Access Control) zorunlu erişim kontrolü **güvenliğini sağlamaktadır**.
- **AppArmor** Ubuntu sistemlerde hayati önem taşıdığı için **kesinlikle kapatılmaması gerekmektedir**.
- Apparmorun sisteminizdeki durumun öğrenmek için **apparmor-status** komutunu vermeniz gerekir.

a. **Simple setup**
b.

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

- bunun kontrollerinden biri **chage -l <username>** (şifre politikalarının her bir kullanıcıda nasıl olduğunu listeliyor, bizde min day 2, Max day 30, warn massage 7 olmalı pdf'te istendiği gibi..)
- ayrıca oluşturulan (root ve oluşturulan kullanıcı) parolalarda pdf'in istediği katı şifre politikalarına uygunluğa dikkat edilmeli (Min 1 büyük harf, min 1 rakam, username, difok, enforce vs. vs. kuralları…)

- Değerlendirici yardımıyla UFW hizmetinin başlatıldığını kontrol edin.
- **sudo ufw status numbered** (listeyi 1, 2, 3 diye sıralıyor)
- **sudo ufw status** (listeyi gösteriyor)
- **sudo systemctl status ufw**

- Değerlendirici yardımıyla SSH hizmetinin başlatıldığını kontrol edin.

sudo systemctl status ssh

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

- **uname -a** (all info)

ya da

- **uname -v** (Kernel sürümünün dağıtıma özel sürüm bilgisini, yayınlandığı tarihle birlikte gösterir.)

a. **User**
b.

- Değerlendirilmekte olan öğrencinin oturum açma bilgilerine sahip bir kullanıcının sanal makinede bulunmasını ister.
  - **cat /etc/passwd | grep home** (yazınca aoner42 çıkıyor)
    - *ya da*

- **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.)*

  - **cat /etc/group | grep sudo**
  - **cat /etc/group | grep user42**

    ya da
  - **id <username>**

    ya da
  - **groups**

- 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, minlen10, credit -1, ucredit -1, maxrepeat 3, userchack 1, enforcing 1, enforce_for_root**)

      ***!!! **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 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>**

- **Son olarak, değerlendirilen öğrenciden bu şifre politikasının avantajlarını ve uygulamasının avantaj ve dezavantajlarını açıklamasını isteyin**. Tabii ki, Pdf böyle istiyor cevabı sayılmaz… Bir şey beklendiği gibi çalışmıyorsa veya net bir şekilde açıklanmıyorsa değerlendirme burada durur.

- araştırmalara göre hala pek çok insan şifrelerini tahmin edilebilmesi en kolay yollardan seçer ya da şifresini değiştirmeye ihtiyaç duyduğunda eski şifresine çok benzer bir şifre oluşturur. Bunu engellemek için kullanıcıların önüne **şifre oluşturmadan önce bir takım ön koşullar** getirilir ve bunlara göre şifre oluşturulmaları istenir. **Böylelikle basit şifre olasılıklarının önüne geçilmiş olur.**
- Fakat şifrelerin zorluk dereceleri, uzunlukları, 3 farklı karakterden oluşma kuralı gibi sınırlamalar kullanıcıların **parolalarını sık sık unutmalarına, hesaplarının kitlenmesine, yeni şifre oluşturmak için tekrar aynı kurallar etrafında şifre seçme gibi vakit kayıplarına** neden olmaktadır. Sürekli değiştirilmesi gerektiği için uzunluk ve karakter çeşitliliği açısından **akılda tutulması zordur**…
- fakat aynı zamanda şifrelemedeki bu çeşitlilik ve sürekli değiştirilmesi **hackerlar tarafından şifre tahmin riskini azaltmaktadır.**
- minlen= 10, 20, 15 olması parola ne kadar uzunsa kırmak daha zor ve zaman alıcıdır.
- alfabe **harici karakterler** kullanılmasının sebebi **belirli cümle kalıplarının birçok kullanıcı tarafından kullanımını engellemektir.** İki kişi de şifresinde galatasaray kelimesini kullanıyor ama farklı karakter zorunluluğu sebebiyle kimi galatasaray??? Diyor kimi galata_saray!* diyor….
- **büyük küçük harf k**ullanımı kombinasyonu hacker'ın kullanması gereke**n şifre kombinasyonlarını arttırır** ve zaman alır…
- numara koymak da aynı şekilde kombinasyonları arttırır…
- katı şifre politikaları sayesinde **saldırganın iş yükü ve harcadığı zaman arttığı gibi bulma olasılığı azalır.** Kırılması uzun süren şifreler üzerinde saldırganlar fazla zaman kaybetmeyerek kırılması **kolay şifrelere yönelirler bu da saldırganların hedefi olmaktan çıkartmış olur** bizi… şifre oluştururken amaç kırılması imkansız değil kırılması zor parola bulmaktır bu da bizi hedef olmaktan çıkarır…

d. 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.

- öğrenci, **LVM'nin nasıl çalıştığı ve bunun neyle ilgili olduğu hakkında size kısa bir açıklama yapmalıdır.**

- LVM (logical volume manager) ile **birden fazla diski tek bir disk bölümü olarak kullanabilir** ve disk yönetimi işlemlerinde büyük kolaylık sağlar. **Disk alanının yetersiz kaldığı durumlarda** LVM ile oluşturulan disk veri kümesine kolaylıkla **yeni disk veya disk bölümleri ilave edebilir**, ihtiyaca göre disk alanı şekillendirilebilir. Yani istenildiğinde **mevcut disk alanı üzerinde istenilen boyutlandırmanın yeniden yapabilmesini sağlar.**
- **Büyük disk alanı ihtiyacı olan sistemlerde LVM ile** disk veri kümeleri oluşturularak ya da sisteme yeni **bir disk daha eklenerek** toplam disk boyutu arttırılabilir.
- 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.

c. SUDO

- "Sudo" programının sanal makine**ye 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)

d. UFW

- "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)

- - **Değerlendirilen öğrenci size temel olarak UFW'nin ne olduğunu ve onu kullanmanın değerini açıklamalıdır.**
- Ubuntu üzerinde kullanılan firewall uygulamasıdır. UFW (Uncomplicated Firewall) ile **ipv4 veya ipv6 firewall güvenlik yönetimi yapmamıza imkan verir.**

- Hem konsol hem de **GUI** (grafiksel arayüz) üzerinden port ve **güvenlik duvarı işlemlerini gerçekleştirmemize olanak veren bir güvenlik duvarı aracı** olarak ifade edilebilir. **default pasif modda** bulunan UFW yönetici tarafından aktifleştirilerek kullanılabilir.
- Genel olarak SSH işlemleri içerisinde port açma/değiştirme/kapatma aşamalarında faydalandığımız UFW…
- Default olarak bir çok portun kapalı durumda tutulduğu sistemlerde **açılan her port bir güvenlik sorunu oluşturabilir.** Bu nedenle kontrollü bir şekilde süreç yönetilmeli, iletişimin devam etmediği portlar tekrar pasif konumda tutulmalıdır.
- Firewall yani 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 t**anımlanabiliriz.
- **Linux** tabanlı işletim sistemlerind**e güvenlik duvarı varsayılan olarak iptables'dı**r. Ancak iptables Linux'e çok aşina olmayan kullanıcılar için **biraz komplike olabilir.** Linux acemisi iseniz **firewall ayarlarını yapmak için ufw komut setini kurup** kullanabilirsiniz.
- Ubuntu için varsayılan güvenlik duvarı yapılandırma aracı ufw'dir. **iptables güvenlik duvarı yapılandırmasını kolaylaştırmak için geliştirilen ufw**, IPv4 veya IPv6 ana bilgisayar tabanlı güvenlik duvarı oluşturmak için kullanıcı dostu bir yol sağlar.
- **Güvenlik duvarı,** hangi paketlerin sisteme girip çıkmasına izin verileceğine karar verme fikridir. **Hangi bağlantı noktasının dış dünya ile** (hatta yerel ana bilgisayar üzerinde) **iletişim kurmasına izin verildiğine** karar vermek güvenlik duvarının sorumluluğundadır. **Bir paketi kabul etmesini, reddetmesini veya bırakmasını emredersiniz.**
- Güvenlik duvarı (firewall), **iç ve dış trafiği denetlememizi sağlayan** bir cihazdır. Bu duvar sayesinde **bilgisayarımızdaki yazılımlar bizim iznimiz dışında bilgi vermez.** Yani **bilgisayardan internete doğru bilgi alışverişinin iznimiz dışına çıkmasını engellenmiş olur.** Güvenlik Duvarı olan Firewall, kısaca **bir bilgisayar savunma mekanizması donanımıdır.** *Bir ağ ile internete bağlı olan tüm bilgisayarlar birçok virüs, zararlı yazılım ve bilgisayara sızabilecek hacker tehdidi altındadır.***Firewall, bilgisayarı bu tehditlerden koruyan donanımdır.**
- Firewall, **zararlı yazılımlara karşı bir duvar örür ve bunların ağ yolu ile bilgisayara sızmasının önüne geçer.** Kısacası, Firewall internette güvenli kalma yöntemlerinden biridir
- Güvenlik duvarı, bir ya da birden fazla **bilgisayarın bilgisayar ağı üzerinden diğer bilgisayarlara olan erişimlerini engellemek, izin vermek veya sınırlamak için kullanılan yazılımdır.**
- Güvenlik duvarı sunucuya internet üzerinden gelen trafiği kontrol ederek "Şu IP numarasına 443 numaralı port üzerinden bağlantıya izin ver", "Diğer tüm bağlantıları reddet" gibi kuralları yazmamıza olanak sağlar…
- Güvenlik duvarı ile hangi programların, hangi iletişim protokollerinin, hangi ip adreslerinin, hangi portların, hangi kullanıcıların **dışarıdan içeriye(dış bilgisayarlardan kullandığımız bilgisayara) veya içeriden dışarıya ulaşıp ulaşamayacağı tanımlanabilir.**
- **Güvenlik duvarı (firewall)**, iç ve dış trafiği denetlememizi sağlayan bir cihazdır. Bu duvar sayesinde bilgisayarımızdaki yazılımlar bizim iznimiz dışında bilgi vermez. Yani **bilgisayardan internete doğru bilgi alışverişinin iznimiz dışına çıkmasını engellenmiş olur**. **Güvenlik duvarı**, bir bilgisayar (veya yerel ağ) ile başka bir ağın (İnternet gibi) arasına girerek gelen ve giden ağ trafiğini kontrol eder. Bir **güvenlik duvarı** ile güvenlik duvarının kuralları, hangi trafiğe izin verildiğini ve hangilerinin izin verilmediğini belirler.

- 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>**

e. SSH

- 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)

- **Değerlendirilen öğrenci size temel olarak SSH'nin ne olduğunu ve onu kullanmanın değerini anlatabilmelidir.**
    - **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 i**le 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…)
    - Diğer önemli değişiklik port değişikliğidir. SSH bağlantısının portu varsayılan olarak 22'dir. **Portu değiştirerek saldırganların 22 portundan sunucuya erişimini engelleyeceğiz.** (Biz de 4**242 portundan bağlanarak güvenli bir SSH bağlantısı oluşturmaya** çalışıyoruz)
    - Sadece belirlediğimiz adreslerden SSH erişimi sağlamak istiyorsak güvenlik duvarı(UFW) burada çok işe yarar
    - 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….

- 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)
    -

f. Script Monitoring

- Size kodu göstererek senaryolarının nasıl çalıştığını.

vim /usr/local/sbin/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?**

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