İçindekiler

LİNUX RED HAT NOTLARI

Linux'ta 3 Katman vardır. Aslında her işletim sistemi 3 katmandan oluşur. Linux'ta biraz farklıdır.

1. Çekirdek (Kernel) Katmanı: İşletim sisteminin kalbi, beyni. Ram, işlemci ve diske hükmeder.
2. Shell (Komut Satırı) Katmanı: Kernel katmanın üzerinde çalışır. Çekirdeği hükmetmeni sağlayan katmandır. Sizler aslında sistemi Shell üzerinden kullanırsınız terminal ile. Oldukça kuvvetli bir katman. Kernel'e hükmeder. Hiçbir user-interface ihtiyacı olmadan Shell'den yapabilirsiniz. Bu yüzden güçlüdür.
3. User Interface: Bu olmadan da linux kullanabilir. Size bir sevimli görsel bir ekrandan Shell'e hükmetmeni sağlar. Shell'de Kernel'e hükmeder. Çark böyle döner. Bu katman keyfe kader bir katman.

Linux dünyasında dizin nedir?

Linux dünyasında Windows gibi harf yok (C, D, E gibi). Root altındaki gördüğün şeyler dizindir. etc, bin gibi. Mesela etc dizini tüm konfigürasyon dosyalarının olduğu dizindir. Mesela home dizini de Microsoft'taki users klasörüne benzer. Users dosyaları falan burada durur.

Dosya Nedir?

*Linux'ta HER ŞEY BİR DOSYADIR.!!!!!!

*Linux'ta büyük küçük harf duyarlılığı vardır.

"cd Desktop/" diye bırakırsan ve komutu çalıştırırsan bu Desktop dosyası olarak algılanır dizin olarak değil. Onun için "cd /Desktop/" demen lazım yani dizin için.

Terminalde karşınıza çıkan dosya klasör text vs. gibi şeylerin belli renkleri vardır.

Mavi: Klasörleri ifade eder.

Beyaz: Dosyayı ifade eder.

YAYGIN KULLANILAN KOMUTLAR

echo: kendisinden sonra gelen argümanı veya parametresini ekrana bastırır. Eğer mesela "echo $SHELL" dersek bize Shell'in yerini gösterir. Bir dosyanın dizindeki yerini öğrenmek istersen bu komutu kullanabilirsin.

cat: Dosyaların içeriğini terminalde gösterir.

"cat nano2 >> nano" →üzerine yazıyor.

tar: bir sıkıştırılmış dosyayı bir dizinde açmak için önceden o dizinin var olması lazım. Tar komutu dosyayı sıkıştırmaya ya da sıkıştırılmış dosyayı açmaya yarar.

find: sistemden direk arama yapar. Bir database araması yapmaz. O anda sistemden direk arama yapar.

"**find [dizin] -name [filename]**"

locate: aradığımız şeyi daha hızlı aramamızı sağlıyor. "find" komutu gibi sistemden aramaz, database araması yapar. Eğer o database güncel değilse sonuçta güncel olmaz. Find komutunda böyle bir şey yok. Neyse o. Locate komutu varken bulamayabilir yokken bulabilir. Locate ile arama yapmadan önce indeksi yani database güncellemeniz daha yararlı olur. Bu sayede doğru sonuç alma ihtimaliniz artar. Database güncellemek için ise şu komutu kullanabilirsin (Bu komut için root olun):

“**updatedb**”

Sonra locate kullanabilirsin:

“**locate** [**filename**]”

Linux dünyasında Shell text editörleri nedir?

Microsoft’taki Notepad’den biraz farklı. Terminal text editörleri önemlidir. Shell text editörleri tüm dosyaları eğer yetkiniz var ise değiştirmenizi, kaydetmenizi, kapatmanızı sağlayan araçlar. Bunlardan biri nano text editördür.

1. Nano

IP adresini nasıl değiştirebiliriz?

Öncelikle IP adresi dosyasının nerede olduğunu bilmek bizim için işimizi kolaylaştıracak bir hareket. Sistemdeki konfigürasyon dosyaları etc dizininde olur. Burada sysconfig diye bir dosya var. Bu dosyaya girip network ile ilgili dizin olmalı. O dizini bulup girin. Orada internet adınızı yazan mesela “ifcfg-eth0” gibi o dosyayı nano ile aç. Orada dhcp olan kısmı static yap ve altına yeni bir satır ekle oraya da “IPADDR=192.19.13.1” gibi bir IP adresi ver. IP adresi verirken dikkatli olman lazım. Ekstra olarak subnet eklememiz lazım. Bu küçük harf olmalı. Ya da “PREFİX=24” yazabilirsin. Buradaki 24 eğer sen ifconfig yazınca karşına 255.255.255.0 gibi bir şey çıkarsa sen c sınıfı bir networktesin. O yüzden 24 yazarsın. Eğer 255.255.0.0 ise 24 yerine 16 yazarız, 255.0.0.0 ise 8 yazarız.

Dosyayı nano ile açtığında görüntü olarak;

TYPE=

PROXY METHOD=

BROWSER=

BOOTPROTO=”dhcp”

DEFROUTE=

IPV4=

…

ONBOOT=”yes” gibi bir görüntü var.

Biz “dhcp” olan kısmı “static” olarak değiştireceğiz. Sonra IP adresi ekleyeceğiz, gateway, prefix, dns parametresi ekleyeceğiz. Ev kullanıcıları için default olarak gateway ve dns parametreleri modem ipsidir. Tüm bu değişiklikleri yaparken root olmanız lazım. Yani yetkiniz olması lazım.

Bu değişiklikleri yapınca hemen olmuyor. Bunun için bir şey daha yapmamız lazım. Network servisini yeniden başlatmamız lazım. Eğer root isen:

Network-scripts]$ systemctl restart network.service

ya da network service kısmını kapatıp açabiliriz:

1. **Network-scripts]$ systemctl stop network.service**
2. **Network-scripts]$ systemctl start network.service**

O da olmadı etherneti kapatıp açabiliriz:

1. **İfdown [ethernet_name]**
2. **İfup [ethernet_name]**

En güvenilir restart etmektir. Hem hız hem de güvenli olması için daha çok tercih edebilirsin.

BİRDEN ÇOK NİC KARTA STATİC IP ADRESİ ATANMASI ve HATA ÇÖZÜMLERİ

"**ip addr**" komutu ifconfig gibi bir komuttur.

Makineye üç adet ethernet kartı bağladık. 3'üne de static ip atadık ama sadece 1'inde oldu. Diğerleri dynamic ip adreslerini kullanmaya devam etti ya da bizim atadığımız ip adresini secondary ip olarak belirledi. Eğer eklediğiniz ethernet dosyalarını bulamazsan kendin eklemelisin. Atadığımız ethernet ip adreslerinin 2'sinin olmaması nedeni oluşturduğumuz dosyalarda dahil 3 ethernet dosyasının içindeki UNID tarafı birebir aynıydı. O yüzden hata aldık. Bu tarz durumlarda gerek MAC adresi olsun gerek UNID olsun son hanesini değiştirin. Sistemde de böyledir. Birer birer artarak değiştirir. Kontrolü kolaydır.

Linux'un çok fazla dağıtımı var ve bu dağıtımlara göre çözümler çok farklı olabilir. Burada da Linux'ta bir konfigürasyon dosyasının ne kadar önemli olduğunu gördük. Linux'ta bir şeyle uğraşırken asıl dosyaların yedeklerini al sonra işler sarpa sararsa üstüne yapıştırırsın.

PAKET KURULUMU? PAKET DERLEYİCİ (PAKET YÖNETİCİSİ) NEDİR?

Paket derleyici ilgili yazılımın sistemde gerekli yerlere yazılarak çalışır hale gelmesine sağlayan bir yazılımdır. Bu yazılımın görevi diğer yazılımların kurulmasını sağlamak, otomatikleştirmek ve kolaylaştırmaktır.

Debian tabanlı Ubuntu ve benzeri linux sistemleri Debian tabanlı dosya yöneticisi kullanırken Red Hat, Centos gibi linux sistemleri farklı bir dosya yöneticisi kullanır. Yani Debian tabanlı linux dağıtımları farklı bir paket derleyici kullanırken Centos, Red Hat gibi dağıtımlar ise farklı bir derleyici kullanır.

Red Hat paket yöneticisi: yum

Debian tabanlı: **apt**

- ➔ GNOME Desktop paketini kur. Artık GNOME kullanmaya başlayalım.
- ➔ https://www.cyberithub.com/how-to-install-gnome-desktop-gui-on-centos-7/ linkinden nasıl kurulacağına bakabilirsiniz.

wget: bir download yöneticisi. Terminal download yöneticisi sadece indirir. Bulunduğu dizine indirir.

wget [filepathlink]

.rpm uzantılı dosyalar centos red-hat için kurulum paketleridir. Yum ile rpm dosyalarını kuruyoruz. Peki dosyayı indirdik. Nasıl kuracağız?

"**sudo yum install ./google-chrome-stable_current_*rpm**"

Komutu işimizi görür. Buradaki "./" paketin çalıştırılacağını ifade ediyor. "*" işaretinin anlamı ise mesela "*.rpm", uzantısı rpm olan dosya. Yani * işareti dosyanın tam adını yazmadan belli başlı şeyleri yazıp diğerlerini yazmamamızı sağlar.

top: bu komut çalışan prosesleri gösterir.

tree: vereceğiniz dizinin ağaç yapısını verir.

PAKET KALDIRMA

"**sudo yum remove -y openoffice* libreoffice***"

Rpm dosyalarını çalıştırmanın diğer bir yolu ise **rpm** komutudur.

KULLANICI VE YETKİ İŞLEMLERİ

ROOT kullanıcısı: linux dağıtımların en yetkili,

Sıradan kullanıcı: sadece kendi dizininde yetkili kullanıcı

Yetkilendirilmiş kullanıcı: yetkisi ölçüsünde işlem yapabilen kullanıcı

ROOT yetkisi verilmiş kullanıcı: Sistemdeki her şeyi root yetkileriyle yapmaya yetkili kullanıcı

Centos-red-hat işletim sisteminde bir kullanıcıya yetki verilmezse sadece kendi home dizinine erişilebilir ve orada işlem yapabilir.

Aynı yetkilere sahip ortak olarak yetkilendirilmek istersen kullanıcıları aynı grup olarak düşünülebilir, yapılabilir.

-çalıştırma hakkı

-okuma hakkı

-yazma hakkı

Bu hakları aşağıdakiler alabilir.

-Dosyanın sahibi (dosya ya da dizini oluşturan) istenirse değiştirilebilir.

-Sahip grup

-others (dosyanın sahibi olmayan)

ÖRNEK

A. Öğrenciler diye bir dizin mevcut. Bu dizin üzerinde her öğrencinin ful yetkili olmasını istiyoruz. Bunun yanında bu dizinin sahibinin her şeyi yapabilmesini istiyoruz (Full hak). Bunun dışında kalanların sadece okumasını istiyoruz.
    i. Önce Öğrenciler diye bir dizin oluştururuz.
    ii. Sonra bu dizine yetki tanımlayabilmek için öğrenciler diye bir grup oluşturur mevcut öğrenci kullanıcılarını buraya dahil ederiz. Var olmayan öğrenci kullanıcılarını oluştururuz.
    iii. Grubun sahibine ful hak tanımlarız.
    iv. Öğrenci grubuna ful hak veririz.
    v. Others ise okuma hakkı alır.

B. Mevcut bir dosya üzerinde "ali" kullanıcısına tam hak vermek istiyoruz. Diğer hiç kimse buraya erişmesin istiyoruz.
    i. Ali kullanıcısına dosyanın sahibi yapılır ve ful hak verilir.
    ii. Grup ve others erişim izni almaz.

C. Centos-Red Hat işletim sisteminin ip adreslerini değiştirebilmesi için "feyza" kullanıcısına yetki vereceğiz bunu nasıl yaparız? Feyza dışında sadece root yetkili olsun.

i. **/etc/sysconfig/network-scripts/ens*** dosyaları üzerinde feyza kullanıcısına yazma yetkisi verilir. Eğer kullanıcı yoksa oluşturulur.

NOT

Linux'ta her şey dosya olduğundan her dosya üzerinde kullanıcılara ayrı ayrı hak verebiliriz.

KULLANICI İŞLEMLERİ

"**cat/etc/passwd**" komutu ile kullanıcıların ve grupların listesini görüntüleyebiliriz.

Linux dünyasında her kullanıcını bir USER ID sahibidir.

"**cat /etc/passwd**" →Bütün kullanıcıların listesi

"**sudo useradd [username]"**

"**sudo passwd [username]"**

Yukarıdaki komutlarla kullanıcı oluşturduk ama daha yetki vermedik. "cat /etc/passwd" komutuyla karşımıza çıkan kullanıcılarda "nologin" yazanların sisteme girmeye yetkisi yoktur. Eğer bir kullanıcıya Shell dizini tanımlarsanız o kullanıcı sisteme login olabilir, komut çalıştırabilir, sistemi kullanabilir /bin/bash gibi. nologin olanlar sistem kullanıcısı olduğu anlamına gelebilir.

"sudoers" dosyası root yetkisini düzenlediğimiz önemli bir dosya.

ROOT ÇALIŞTIRMA YETKİSİNİN TANIMI

Mesela "ali" diye bir kullanıcı oluşturduk. Onun yetkisini yükseltmek yani root olmasını istiyorsak:

1. Önce eğer "ali" kullanıcısındaysak root yetkisine sahip bir kullanıcıya geçip "sudo nano /etc/sudoers" komutunu çalıştıralım.
2. Açılan pencerede "whell" grubu altında "root ALL=(ALL) ALL" yazan yerin altına yetkisini yükselteceğimiz kullanıcının "[username] ALL=(ALL) ALL" şeklinde yazıp kaydediyoruz.
3. 2 numaralı işlem bittikten sonra sshd restart etmemiz gerekecek. Onun için de "sudo systemctl restart sshd" komutunu çalıştırırız. Bu işlemde tamamlandığında artık kullanıcımızın yetkisi yükselmiş oldu.

KULLANICI CONFİG DOSYALARI

Kullanıcı silmek için: "**sudo userdel [username]**". Bu komuttan sonra [username] dizini hala "home/" altında duruyor. Onu oradan silmek için:

"**sudo rm -Rf [username]/**"

Son komutu kullanmadan "**sudo -r userdel [username]**" kullanabilirsin. Ya da "**sudo rm --remove-home [username]"** de yapabilirsin. Bu hem kullanıcıyı sil hem de home dizinindeki o kullanıcının dizinini sil anlamına geliyor.

Eğer biz "/etc/shadow" dosyasına girersek karşımıza kullanıcıların şifreleri karşımıza çıkar ama şifreli olarak. Burada kullanıcıların isminin yanında "!! " ile başlarsa bu sistem kullanıcısı olduğunu ya da o kullanıcının şifresi yok ve login olamaz anlamına gelir. "!$" ile başlarsa bu kullanıcının şifresinin lock olduğunu yani kullanıcının pasif olduğunu gösterir. "!$" işaretlerindeki "!" işaretini kaldırarak şifrenin lock olmasını kaldırabiliriz.

"**usermod**" komutu ile kullanıcıların aktif ya da pasifliğini değiştirebiliriz.

"**sudo usermod -L [username]**" > [username]'in şifresini lock oldu ve artık o kullanıcıya girilmez.

"**sudo usermod -U [username]**" >[username]'in şifresinin lock kalktı ve artık o kullanıcıya girilebilir.

GRUP DOSYALARI

Grup oluşturma:

"**sudo groupadd [groupname]**"

Grup silme:

"**sudo groupdel [groupname]**

Belli kullanıcıları aynı gruba dahil etmek istersek

"**sudo useradd -g [groupID] [username]**"

Komutu işimizi görür ama kullanıcıyı sildiğinizde o kullanıcının grubu da otomatikman siliniyor. O gruba başka kullanıcı dahil ise silinmez. Bir grubu silmek istediğinizde eğer o gruba dahil bir kullanıcı varsa grup silinmeyecektir.

SORU 1

Yeni oluşturulacak Hatice isimli kullanıcının root olabilmesi için ne yaparız?

a. Root grubuna Hatice'yi ekleriz.
b. Sudoers dosyasına Hatice kullanıcısına eklemek.

SORU 2

Yeni oluşturulacak Gizem kullanıcısı root olabilme yetkisi verilmek isteniyor. Bunun yanında bu işlemin direk olarak sudoers dosyasına dahil edilerek yapılmasına istenmiyor. Bunun yerine var olan gruplardan yararlanmak isteniyor. Root grubunun kullanılması da istenmiyor.

a. "sudoers" dosyasına baktığımızda wheel grubunun da tüm komutları çalıştırma yetkisi olduğu gözükecek. O yüzden eğer Gizem whell grubuna dahil edilirse root olur. O zaman şöyle bir çıkarımda bulunulabilir:
   Eğer bir kullanıcı root olabilme hakkıyla oluşturulmak isteniyorsa whell grubuna dahil edilerek oluşturulabilir.
   "**sudo useradd -g [whellgroupID] {username]**"

Bir kullanıcıyı gruba almak için iki komutumuz var:

1. "**sudo usermod -aG wheel gizem**"
2. Grup dosyasını açarak manuel olarak elimizle wheel satırına kullanıcıları ekleyebiliriz.

GROUP VE KULLANICI ENTEGRASYONU

Bir kullanıcıyı gruba eklemek için diğer bir komut ise:

1. "**sudo gpasswd -a [username] [groupname]**": kullanıcıyı ilgili gruba ekler.
2. "**sudo gpasswd -d [username] [groupname]**" : kullanıcıyı ilgili gruptan siler.

SORU 3

Yeni oluşturulacak “hale” kullanıcısı Root olabilme yetkisi olacak. Bunun yanında Salih, Mehmet, Hüseyin kullanıcıları da gene root olma yetkisine sahip olacak. Bununla birlikte bu 4 kullanıcı hem ortak haklara sahip olabilme hakkı hem de aynı diğer haklara sahip olabilmeleri için en kısa şekilde yapılması gereken işlem ne olmalıdır? (Whell, root grubu kullanılmamalıdır.)

i. “Asistants” diye bir grup oluşturulur ve bu gruba 4 kullanıcı dahil edilir. Sonra SUDOERS dosyasında bu grup yetkilendirilir. Eğer gerekiyorsa diğer yetki tanımlamaları da yapılır.

DOSYA VE DİZİN İZİNLERİNE GİRİŞ

Linux dünyasında her dosya ve dizinin bir yetkisi var. Bu izin yetkilerini görmek için:

“**ls -l**” komutu işini görür.

Karşına

drwxr-xr-x. 4 [username] [username] …

drwxr-xr-x. 5 // // …

.
.
.

gibi devam eder. Burada baştaki harfler her biri bir şey temsil ediyor. Eğer komutu çalıştırıp baktığınızda “**d**” görürseniz onun dizin olduğunu anlamına gelir. Diğer harfler 3 kısımdan oluşur ve bunlar “-“ ile ayrılır. İlk kısım olan ”**rwxr**” kısmı sahibini ifade eder. Sahibi de dosyanın oluşturan kullanıcıdır.

d: dizin

1.kısım= rwxr: Dosyanın sahibi. Sahip ise dosyayı oluşturan kullanıcı (Sahip) (ilk username sahiptir)

2.kısım= xr: dosyayı oluşturan primary grubu (Sahip grubu) (primary grup kullanıcı oluştuğunda hangi gruba dahil ise o gruptur.) (ikinci username sahip grubudur.)

3.kısım= others (diğerleri): Sahip ve sahip grubu dışında kalan herkes

Bu 3 kısmı da değiştirebiliriz. Others kısmı diğer 2 kısım değişince zaten değişmiş olur. Bunları düzenleyince de dosyaya erişim yetkilerini ayarlayabiliriz.

Bu 3 kısma izin tanımlayabiliriz. Bunlar

Write= -w = yazma

Read= -r = okuma

Execute= -x = çalıştırma

İzinlerini verebiliriz. Mesela “rwx” demek yaz, oku, çalıştır izni vermiş oluruz. Bu izinleri değiştirmek için “chmod” komutunu kullanacağız.

"**chmod –**" : izni çıkartmak için kullanılıyor.
"**chmod +**" : izni eklemek için kullanılıyor.

ÖRNEK

Desktop üzerinde oluşturulan deneme dosyasının tüm izinlerini çıkartalım. ("**u**" parametresi dosyanın sahibini gösterir. "**o**" da others anlamına geliyor ve "**g**" de grubu ifade eder. "**a**" parametresi herkesi ifade eder.)

Eğer dosyanın tüm kısımlarındaki yetkileri tamamen silmek istersek:

"**chmod -rw [filename]**" işimizi görebilir.

Ama mesela sırayla önce others yetkilerini sonra sahip grubu yetkilerini en sonda sahip yetkilerini çıkartalım:

"**chmod o-r [filename]**": others grubunun r hakkı çıktı.

"**chmod g-rw [filename]**": sahip grubunun rw hakkı çıktı.

"**chmod u-rw [filename]**": sahibin rw hakkı çıktı.

Ya da 3 komutu tek satırda

"**chmod u-rw,g-rw,o-r [filename]**" şeklinde yazabiliriz.

Yani genel komut şöyle:

"**chmod [hangikullanıcı(u, g or o] -[hangiizinlerçıkacak(r,w or x)] [dosyaadı]**"

SORU

1. Desktop üzerindeki deneme dosyasına tüm grupların "rwx" haklarıyla erişmesi için ne yapılması gerekir?
    i. "**chmod a+rwx deneme**"

    b. Deneme2 dosyası için sadece others okuma ve yazma yetkisi verilsin ve sahip grubuna da read hakkı verelim.
        i. "**chmod g+r,o+rw deneme**"

Ekstra olarak şu komutta izinleri çıkarmak için kullanılabilir:

"**chmod a= [filename]**" : dosyanın tüm izinlerini kaldırır.

İZİNLERİN RAKAMLA TANIMLANMASI

r=4

w=2

x=1 'i ifade eder. Bir dosyaya okuma + yazma + çalıştırma hakkı vermek istiyorsanız:

4 (Okuma) +2 (yazma) +1 (Çalıştırma)=7(rwx)

4 (Okuma) +2 (yazma) +1 (Çalıştırma)=7(rwx)

4 (Okuma) +2 (yazma) +1 (Çalıştırma)=7(rwx) olur.

Buradan da:

"**chmod 777 [filename]**" : herkese her hakkı vermiş olduk.

DOSYA VE DİZİN SAHİPLİĞİ

Eğer terminale "id neşe" gibi bir komut yazarsanız neşe kullanıcısının id numarasını bana göster demek istiyorsunuz. Eğer öyle bir kullanıcı varsa size id verir ama yoksa vermez. Sizde öyle bir kullanıcı var mı yok mu anlamış olursunuz.

Bir dosyanın sahibini değiştirmek için "**chown**" komutunu kullanırız:

"**sudo chown nese deneme**": deneme dosyasının sahibini "Neşe" yap.

Dosya değiştirmek istiyorsan:

"**sudo chgrp [groupname] deneme**"

Hem sahibi hem de grubu aynı satırda yazacak olursak:

"**sudo chown -R [username]:[groupname] [filename]**"

DİZİN İZİNLERİ VE FARKLARI

Bir "dizin1" adında dizin kuralım. Sonra dizin1'in altına dizin2, dizin2'nin de altına dizin3 kuralım.

|-dizin1
|-|-dizin2
|-|-|-dizin3

"**chmod 700 dizin1**"

gibi olacak yani. Bir dizin üzerinde yaptığınız değişiklikler alt dizini etkilemez. Eğer alt dizinin de etkilenmesini istiyorsak:

"**chmod -R 700 dizin1**"

Bir dizin altında ikinci bir dizin oluşturabilmek için çalıştırma (execute -x) izni lazım.

SİSTEM DOSYALARI ÜZERİNDE İZİNLER VE YETKİLER

Örnek: Paket kurulumu görevini tamamen "Neşe" kullanıcısına devretmek istiyoruz bunun dosya yetkileri tarafında ne yapmak gerekir?

a. Bir grup oluşturur ve o grubun içine istediğimiz kullanıcıları ekler ve /etc/yum.conf dosyasının sahip grubunu oluşturduğumuz grup yaparız. Gerekli okuma, yazma ve çalıştırma yetkileri ayarlanacaksa onlar ayarlanır ve artık o grubun içindeki kullanıcılar bu dosyaya erişme yetkisine sahip olur.

Örnek: Sunucunun ip adresini değiştirebilme yetkisini "sysmanagment" grubuna verilmesi isteniyor. Bunun için ne yapılması gerekir?

a. Öncelikle **"/etc/sysconfig/network-scripts"** dizinine gelip burada "**ifcfg-ens33**" gibi bir dosyanın özelliklerini yani izinlerine ve sahiplerine "**ls -l | grep ifcfg-ens33**" komutuyla bakabiliriz. Sonrasında "**sudo chgrp sysmanagment ifcfg-ens33**" komutuyla sahip grubunu değiştiririz. Yeni sahip grubuna yazma yetkisi vermek içinde "**sudo chmod 664 ifcfg-**

ens33" komutu işimizi görür. Ve artık "ifcfg-ens33" dosyasına "sysmanagment" grubu yazma ve okuma yetkisine sahip olur.

Örnek: Kullanıcı ve grup oluşturma hakkını sysmanagment grubuna vermek istiyoruz. Ne yapmalıyız?

a. Linux'ta kullanıcıların listesi /etc/passwd dosyasında bulunur. Ben bu dosyanın izinlerini ve sahip grubunu değiştirirsem istediğim olur. Grup içinde "/etc/group" dosyasını aynı şekilde değiştiririm. Bir de kullanıcı parolaları için "/etc/shadow" dosyasının yetkilerini değiştiririm. En sonda "/home" dizini üzerinde yazma yetkisi verilir kullanıcı oluştuğunda buraya klasör oluşturduğu için.
b. A şıkkındaki işlemleri yaptıktan sonra "Hayri" diye bir kullanıcı oluştururursak passwd, group ve shadow içine. /home dizinine de "Hayri" diye bir klasör oluştururuz. Bunları yaptık ama bir hamle daha kaldı. Hayri adlı kullanıcıyı oluştururken hangi kullanıcıdan oluşturduysak Hayri'nin hakları onda kalır. Bunu passwd dosyasından görebiliriz. Bu hakkı Hayri'ye verirsek problemi çözmüş oluruz.

Örnek: 10 adet kullanıcıyı password ve gruplarıyla birlikte toplu olarak oluşturabilmek için ne yapılabilir? (home dizini ilk başta dikkate alınmayabilir.)

a. "/etc/shadow, /etc/passwd" gibi dosyalara erişim izni olan bir kullanıcı ile terminal üzerinden bu dosyaları açarak kullanıcıları gerekli bilgilerle birlikte oluştururuz. Sonrasında home dizininde kullanıcıların klasörlerini oluşturmak için "**sudo mkhomedir_helper [username]** " komutunu kullanarak oluşturabiliriz. Böylece toplu kullanıcı oluşturmuş olduk.

Örnek: Sistemde yetkisi olmayan bir kullanıcı parolası nasıl değiştirilir?

a. Kullanıcı arayüzünden, "**account settings**" kısmından değiştirebilirim ya da terminale değiştirmek istediğim kullanıcıyla girerek "**passwd**" komutuyla değiştiririm.

NOT: Bir kullanıcı kendi şifresini değiştirirken belli bir şifre politikası üzerinden yapar. Eğer sistem şifreyi bu politikaya uygun görmezse beğenmez. Fakat root olarak bir kullanıcının şifresini değiştirmek istersek o zaman istediği şifreyi yapabilir çünkü root her şeyi yapar. Bu şifre politikası değiştirmekte mümkündür.

Örnek: Linux Centos üzerinde parola politikaları belirlenebilir mi? Eğer belirlenirse nasıl belirlenir?

a. Öncelikle password politikasını düzenleyen dosyayı bulup düzenlememiz lazım. O da **"/etc/security/pwquality.conf"** dosyasıdır. Bu dosyaya girdikten sonra şifre politikasını "**dicpath="** kısmından değiştiririz.
b. Ek olarak bu password politikasını değiştirmek için komutta vardır.
    i. "**authconfig –passminlen=12 –update**"

dersek minimum parola uzunluğu 12 olmuş olur ve "pwquality" dosyasında "dicpath" kısmına bakarsak boş olan kısmın bazı özelliklerle dolmuş olduğunu görürüz.

NOT: Linux sistemlerinde belli password kuralı vardır. Mesela centos7 üzerinde min. 6 karakter ister. Yani en az 3 karakter girsin diye bir komut versen de sistem buna izin vermez uyarı verir.

Ek olarak bu password politikalarını deneme özelliği var hiçbir kullanıcı oluşturmadan. Bunun için "**pwscore**" komutu kullanılabilir. Bu komutla password puanı gösterir sana ne kadar güvenli olduğu ile ilgili. Eğer password kurallarını derinlemesine ayarlarsan bu puan değişir.

"**pwquality.conf**" dosyasını açtığında **dichpath** kısmında bazı bölümler görürsün. Bunlar:

minlen=12 : minimum karakter sayısını ifade eder.

minclass=1 : minimum class sayısını ifade eder (büyük harf, küçük harf, sayı,sembol gibi). Bunun 2, 3 gibi değer olması şifre güvenliğini artırabilir.

maxrepeat=0 : maksimum tekrar eden karakter sayısını ifade eder. Bunun yüksek olması işinizi zorlaştırabilir.

maxclassrepeat=0 : maksimum tekrar eden class sayısını ifade eder. Mesela değer 2 olsa iki aynı sınıfın üst üste 3 veya daha fazla karakterini reddeder (qqq22 gibi)

lcredit=0 : Burada değeri değiştireceksek "-" ile gösteririz. "-1" olursa en az bir tane küçük harf olacak anlamına gelir.

ucredit=0 : Burada değeri değiştireceksek "-" ile gösteririz. "-1" olursa en az bir tane büyük harf olacak anlamına gelir.

dcredit=0 : Burada değeri değiştireceksek "-" ile gösteririz. "-1" olursa en az bir tane rakam olacak anlamına gelir.

ocredit=0 : Burada değeri değiştireceksek "-" ile gösteririz. "-1" olursa en az bir tane alfanümerik olmayan bir karakter olacak anlamına gelir.

gibi yazılar görürsün. Bunların yanına eğer eklenmediyse "difok=[number]" eklersin. "difok" parametresi yeni şifrenizde mevcut şifrenizle kıyasladığınızda en az kaç tane farklı olacak onu ayarlarsınız. Böylece kendi password politikanızı oluşturabilirsiniz. Silmek içinse dichpat'in içindeki yukarıdaki belirtilen bölümleri silersek olur.

Neden "pwqulaity" dosyasına bakıyoruz veya nereden biliyoruz bu dosyaya bakacağımıza denilebilir. Bunu "**/etc/pam.d"** dizini içindeki "**system-auth"** dosyasından görebiliyoruz. Bu dosyanın içerisine girdiğimizde password kısmını görürüz. Burada parola için "pwquality" dosyasına bakmanız gerektiğini ve hatta yine parola kısmında şifrelerin shadow dosyasında sha512 kriptolama metodu ile saklandığını gösterir. Linux'ta her şey bir dosya olduğundan ezberden çok mantığı kavranırsa birçok problem karşısında daha rahat çözümler bulunabilir. Birçok şeyi buralardan kontrol etmeyi öğrenmek gerekir.

Ayrıca "**/etc/login.defs"** dosyasına baktığımızda minimum karakter sayısının 5 olduğunu gösterir veya sizde kaçsa onu. İşte password kuralını değiştirseniz bile sistem hala bu kurallar üzerinde belli yetkilere sahip ve bu dosyada da neden minimum 3 gibi bir rakam veremediğimizi görüyoruz. Burada bunu değiştirince minimum karakterin değişmesi lazım. Buradan da yapılabilirdi kurallar.

Şu ana kadar yapılan işlemler yerel kullanıcı veri tabanında yaptığımız değişikliklerdi. Yani oluşturulan gruplarla, kullanıcılarla, yapılan konfigürasyonlarla etkilediğimiz sadece o an kullandığımız sunucudur. Çünkü şu ana kadar yerelle uğraştık.

PROCESS YÖNETİMİ

Terminal ekranına girdiğinizde çalışan işlemleri görmek için "ps" komutu işimizi görür.

ps: Terminale sadece "ps" yazarsak sadece o terminal ekranında çalışan işlemleri görürsünüz.

Mesela terminalden bir uygulama açtığınızda o an terminalde bir işlem yapamadığınızı görürsünüz. Bu durumdan kurtulmak için "^C" ya da "^Z" yapılırsa çıkabilirsiniz ama bu ikisi arasındaki temel fark "^C" yaptığınızda çıkarsınız ama işlem arka planda devam ederken "^Z" de ise tamamen kapanır işlem ve o işlemden çıkarsınız. Bunu da ps komutuyla anlayabilirsiniz. O uygulamayı tekrar çalıştırmak için de "**bg**" komutu işimizi görür. Arka planda çalışmasını sağlar.

ps -aux: Asıl "**task manager**" budur. Tüm prosesleri gösterir.

ps -u [username] : belirlediğiniz kullanıcının açtığı işlemleri görmek istiyorsan bu komut işini görür.

ps -aux | grep opera: opera işlemlerini size gösterir (kimin açtığı, id vs.).

Sistemde her proses kendine has ID sahibidir. "ps" komutu ile ID kullanarakta kullanabiliriz.

"kill" komutu ile belirtilen prosesi kapatabilir, daha kaba bir tabirle öldürebiliriz.

"**kill [processid]**"

"-9" parametresi ile zorla kapatabilirsiniz prosesi.

Ek olarak bir de "**top**" komutu da işlemleri gösterir. Bu komut kendini yaklaşık 3 saniyede bir günceller. "-d" parametresi ile kullanıp bu saniyeyi değiştirebiliriz. Mesela "**top -d 1**" dediğimizde artık 1 saniyede bir kendini güncelleyecek.

DİSK İŞLEMLERİ

Sizin fiziksel diskinize veya sanal diskinize verilerin belli bir kurallar dahilinde güvenli ve güvenilir bir şekilde yazılmasını sağlayan yazılıma dosya sistemi denir. Bütün işletim sistemleri farklı dosya sistemini kullanabilir, destekleyebilir. Her işletim sistemi her dosya sistemini görmez, kullanmaz. Kendine özgü dosya sistemlerini kullanabilir ve desteklediği sistemler vardır.

Linux dünyasında diskler Windows'tan farklı görünür. Diskler "/dev" ile ifade edilir. Her disk "/dev" ile başlar. Bu adresleme şeklidir. Windows'taki "C:" gibi disklerin karşılığıdır. Mesela Linux'ta;

/dev/hda: IDE disklerini ifade eder.

/dev/sda: SATA disklerini ifade eder.

/dev/sdb: Çok büyük ihtimalle bu ikinci eklediğiniz SATA bir disktir. Yani değişen şey son harfidir. Bir diski göstereceksiniz bu örneklerdeki gibi göstermelisiniz. Sistemde hangi sistemlerin takıldığını görmek istiyorsanız (bu erişildiği ya da formatlandığı anlamına gelmiyor), sadece sistemde o anki diskleri görmek isterseniz:

"**sudo fdisk -l**"

Belli başlı bazı araçlarla diski yazdırma ve okuma işlemlerini yapabiliyoruz. Bunlardan biri "**fdisk**" aracıdır.

SORU: Bir diski nasıl formatlarız?

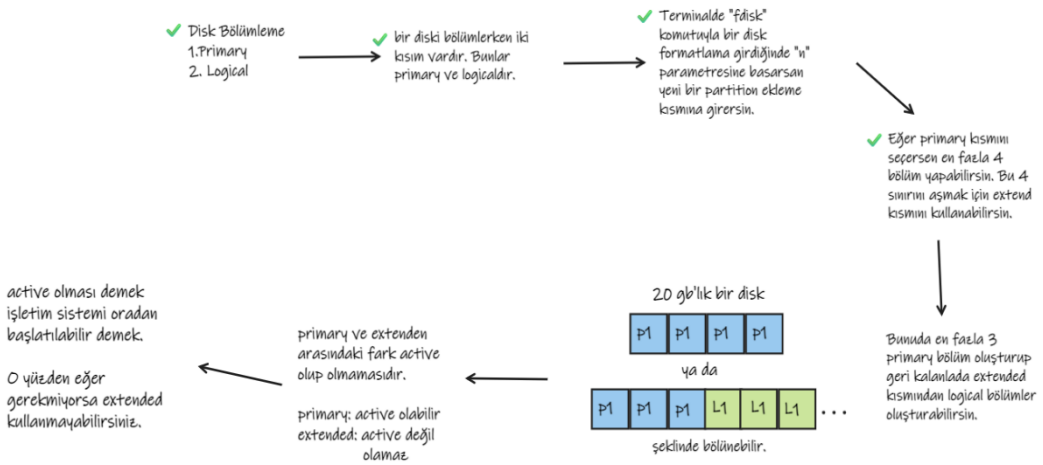
a. İlk araç olarak "fdisk" kullanılabilir. Bunun için "fdisk" aracına hangi diski biçimlendirmek istediğimizi, hangi disk üzerine işlem yapacağımıza söylememiz lazım. Bunu da şöyle kullanabiliriz;

"**sudo fdisk /dev/[diskname (for example :sdb)]**"

Dedikten sonra artık değiştirmeye hazırız. Eğer "m" tuşuna basıp çalıştırırsak bize "fdisk" kullanılarak neler yapabileceğimizi gösterir.

SORU: Partition (disk bölümü) nedir?

a. Bir fiziksel disk üzerinde birbirinden farklı, bağımsız olarak oluşturulabilen bölümlere partition denir. Her biri farklı dosya sistemleri ile formatlayabilir, farklı şekilde okunup yazılması sağlanabilir. İşte birbirinden bağımsız olarak formatlanabilmesi buradan gelir.
Farklı dosya sistemlerini kullanabilir. Partition dosya sisteminden bağımsız olarak oluşturulan bir bölümdür. Sonuç olarak bir fiziksel disk üzerinde bir tarafta linux dosya sistemleri çalışıp linux görebilirken diğer tarafta Microsoft dosya sistemleri çalışıp Microsoft görebilir. Bunu da partition olanak veriyor. Yani diskleri bölümleyebilmek. Bu partition yapılarını da farklı disk sistemlerine göre formatlayabilmeniz buna olanak sağlıyor.
Diski ne ile parçaladığınızın önemi yok. Fakat formatladığınız dosya sistemi çok önemli. Formatladığınız dosya sistemi hedeflediğiniz işletim sisteminde çalışmıyorsa o işletim sistemi dosya sistemini okuyup yazamaz.
Disk bölmenin bir kuralı var. Öncelikle iki türlü partition seçebilirim. Bunlar "**primary"** ve "**logical"** olarak geçer.



İşletim sistemi başlarken onu başlatan bölüm "**active partitiondır (boot partition**)". Ve "active partition" ve "boot partition" primary olmak zorunda. İşletim sistemi başlangıç dosyalarını tutan bölüm "active partition" denir.

mkfs: Bu komut bir linux dosya sistemi yapılandırmasını sağlar. Kullanımı;

"**sudo mkfs.xfs /dev/sdb1**" gibidir.

fd: Bu komut mevcuttaki disklerin bölümlerini gösterir. İşletim sisteminin diskini gösterir.

Diske Yazma: İçine dosya, dizin oluşturmak.

DOSYA SİSTEMİ

"ext, ext2, ext3" …" gibi devam eden "ext" Linux'un geleneksel dosya sistemi denilebilir. Ayrıca "xfs", "jfs", "reiser" adlarında dosya sistemleri mevcut Linux'ta. Daha farklı dosya sistemleri de bulunabilir. "FAT16, FAT32, NTFS" ise Microsoft'a özgü dosya sistemleridir. Linux'ta "xfs" ve "ext" yaygın olarak kullanılır.

ext: ilk, en eski dosya sistemi. Şu an çok fazla kullanılmıyor.

ext2: maksimum 2 Gb gibi bir sınırı var.

ext3: Bu dosya sistemiyle birlikte artık loglanabilir dosya sistemi mevcut oldu.

ext4: 2008 yılından beri kullanılmaya başladı. Debian ve Red-hat tabanlı linux sistemleri destekler.

Jfs: IBM tarafından linux için geliştirilen bir dosya sistemi (1980).

xfs: Centos'un otomatik olarak formatladığı dosya sistemidir. Genelde ticari sürümlerde kullanılır. İlk 2002 yılında ortaya çıktı. Güvenilir ve loglanabilir.

Centos'ta FAT32 desteklenirken NFTS desteklenmez. Farklı linux sürümlerinde bu değişebilir.

Disk bölümleme de dosya tipini değiştirmek için "**fdisk**" komutunu kullanarak "**l**" parametresi ile disk bölüm tiplerini görüntüleyip belirlediğiniz ID numarasını "**t**" parametresini çalıştırdıktan sonra yazdığınızda "**System**" kısmında belirlediğiniz bölüm tipi gözükür. Bunu da "**p**" parametresi ile yapabilirsiniz. Bu işlemde formatlamıyoruz sadece türünü değiştiriyoruz.

Bir diske erişebilmek için, diske yazabilmek için "**MOUNT"** etmemiz gerek. Şu ana kadar disk oluşturduk, "partition" yaptık, "partition" üzerinde formatlama işlemi yaptık ama en önemlisi "Mount" işlemini daha yapmadık. Bunun için "**mount**" komutunu kullanırız. Diskler nasıl mount edilir, cd romlar nasıl mount edilir ve USB bellekleri nasıl mount edilebilir? Linux'ta her şey mount mantığıyla çalışır.

Peki nasıl yapacağız?

Genelde mount edilecek "drive" ya da "diskleri", **"/etc/mnt**" altına koyulur ama istediğin her yere koyabilirsin. Nereye mount edersen o diski yazıp çizmek istersen o dizini kullanırsın.

Diski adresleyen "/etc/sdb1" gibi yazan şey diski adresler ama okuma ve yazma hakkı vermez. Okuma ve yazma hakkı veren diski mount ettiğiniz dizindir. O yüzden o dizine gelip yaparız.

Bir diski "mount" etmek için: "**sudo mount /dev/sdb1 [nereye_mount_edersen_oranın_dizini]"**

Bir diski "unmount" etmek için: "**sudo umount /dev/sdb1**" (Bunun için diskin olduğu dizinde olmalısınız.)

Bu bir disk olduğunda sabittir. İçindekiler onunla o nereye giderse oraya gider. Ama içindeki dosyaları silebilir, taşıyabilir veya istediğinizi yapabilirsiniz.

SORU: Yeni eklenen bir disk üzerinde 2 adet disk bölümleme oluşturulacak. Bu bölümler "primary partition" olacak. İlk bölüm "ext3", ikinci bölüm "ext4" olarak formatlanacak. Bu işlemler nasıl yapılmalıdır?

a. Öncelikle "**sudo fdisk -l**" komutuyla diskleri görüntülerim sonra ilgili diskin adresini bulduktan sonra "**sudo fdisk /dev/sdc**" komutuyla bölümleme kısmına giriş yaparım. Burada bölümlemeleri yaparım. Sonra formatlamaya geçerim. Bunun içinde "mkfs" komutu işimi görür. Bunun için "**sudo mkfs.ext3 /dev/sdc1**" ve "**sudo mkfs.ext4 /dev/sdc2**" komutları ile formatlarım. Sonrasında belirlediğim bir dizine "mount" ederim. Bunun komutu da "**sudo mount /dev/sdc1 /mnt/sdc1disk/**" gibi olur. Aynı işlemi diğer bölümlediğim kısım için de yapar ve işlemi sonlandırırım.

SORU: Yeni eklenen bir disk üzerinde 1 adet "partition" oluşturulacak ve bu "partition" FAT32 şeklinde formatlanacak. Bu işlem nasıl gerçekleşir?

a. İlgili diski gerektiği şekilde bölerim. Sonra formatlama işlemini gerçekleştiririm. En sonda "mount" ederek işlemi sonlandırırım.

SORU: 3. disk üzerinde 2 adet "primary partition" oluşturulacak. Bu bölümler NTFS dosya sistemiyle formatlanmak isteniyor. Bu işlem nasıl gerçekleşir?

a. Red-hat tabanlı Centos7 işletim sisteminde "mkfs.ntfs" adında bir komut yok o yüzden formatlama sırasında böyle bir kullanım yaparsak hata ile karşılaşırız. NTFS dosya sistemini desteklemiyor default olarak Centos7. NTFS ile formatlamak için ilk başta disk bölümlenir. Sonrasında iş formatlama kısmına gelir ama problem buradadır. NTFS desteklenmediği için onu destekler hale getirmemiz lazım. Bunun için yöntemlerden biri paket kurulumudur. Öncelikle hangi paketi kurmamız gerekeceğini bilmemiz lazım. Ekleyeceğimiz paket NTFS desteği için "**epel-release**" paketidir. Bu bir ön gereksinim paketi olduğundan henüz ntfs desteği kazanmadık. Red-hat ön paketini kurmadan ntfs desteği kazanamayız. Kuracağımız diğer paketler "**ntfsprogs**" ile "**ntfs-3g**" paketleridir. Komutlar ise şöyle:
"**sudo yum install ntfsprogs**" sonra

"**sudo yum install ntfs-3g**" komutunu kullanarak paketleri yükleriz.

Bunları yaptıktan sonra artık "mkfs.ntfs" adında bir komut oluştu ve disklerimizi formatlayabiliriz.

SORU: 4.disk üzerinde 6 adet "partition" oluşturmak isteniyor. Bu disk bölümlerinden 1-ext2, 2-ext3, 3-ext4, 4-xfs ve 5-6-NTFS olarak formatlanacaktır. Bu işlem nasıl gerçekleşebilir?

a. Öncelikle ilgili diskin bölümleme kısmına terminalden girerek 3 primary ve 3 extended bölüm oluştururum. Çünkü en fazla 4 primary olabiliyor. Bu engeli ortadan kaldırmak için böyle bir yöntem yaparım. Sonrasında extended üzerinden logical tipler oluştururum 3 adet. "l" ve "t" parametrelerini kullanarak gerekli olanları linux veya NTFS yapar kaydedip çıkarım. Sonra gerekli format tipleriyle bölümlediğim diskleri formatlarım ve işlemi sonlandırırım.

Şu ana kadar "fdisk" komutuyla işlemleri yaptık. Bu araç oldukça kullanışlı olmasına rağmen daha bu işlemleri yapmak için daha basit bir aracımız daha var. O da "cfdisk" aracıdır. Bu araçla belirlediğiniz disk adresine (/dev/sdd1 gibi) girerek "partition type", gibi birçok kısmı buradan düzenleyebiliriz. Nispeten daha güvenli bir araçtır çünkü "extended" kısmı görünmez.

DİSK İŞLEMLERİ GPARTED

Bu sistem aracı ile GUİ kullanarak grafik bir arayüzden de disklerinizi kontrol edebiliyorsunuz. Red-hat tabanlı Centos7 sisteminde default olarak gelmiyor. O yüzden yüklememiz lazım. "**sudo yum install gparted**" komutu işimizi görür ama Gparted kurmak için önce "epel-release" paketini yüklemek gerek. Çünkü bu ön gereksinimdir. Gparted aracı GUİ kullanan orta düzey kullanıcılar için, Linux'u bir client olarak kullanan kullanıcılar için faydalı bir araçtır.

DUAL BOOTİNG GRUB

Bir makine içerisinde iki veya daha fazla işletim sisteminin kullanılmasına, açılışta seçilmek suretiyle, hangi işletim sisteminde devam edeceksin sorusu gelmesi işlemi "**dual booting**" demektir. Aynı anda değil ama açılışta sormak suretiyle iki veya daha fazla sistemin kullanılmasıdır denilebilir kısaca. Linux'taki "boot loader" **GRUB'tır**. Yani Centos7 sisteminin boot etmesini sağlayan GRUB'tır. GRUB'ın işi işletim sistemini sizin tercihinize göre açmak.

Linux Centos7 sistemini sanal makineden açtığımızda karşımıza çıkan boot sayfasını değiştirmek istersek nasıl değiştiririz?

a. Linux'ta her şey bir dosya olduğundan GRUB dosyasını değiştirirsem istediğim sonucu alabilirim. Bunun için kök dizinine gittiğimizde boot dizini gözükür. GRUB boot işini yaptığından muhtemelen dosyası boot dizini altındadır. Bu dizine girdiğimizde grub dizinleri görülür. Burada doğru dizini bulup girdiğimizde "grub.cfg" dosyası karşımıza çıkar. Bu dosya içerisinde belli başlı değişiklikler yaparak istenileni yapabiliriz. Burada "menuentry" kısmında tırnak işaretleriyle belirlenmiş ismi değiştirip kaydedersek, yeniden başlattığımızda boot ekranında yeni yazdığımız ismin göründüğünü görebiliriz.
b. Ek olarka "grub.cfg" dosyasına bir Windows girişi eklemek istersek menuentry kısmına örnek bir Windows girişi eklenebilir.

Resimdeki kodu ilgili bölüme girip kaydettikten sonra sistemi yeniden başlatırsak eklediğimiz kısmın boot ekranında "Windows" adında gözüktüğünü göreceksiniz. İlgili kodu girerken küçük büyük harf duyarlılığına dikkat etmelisiniz.

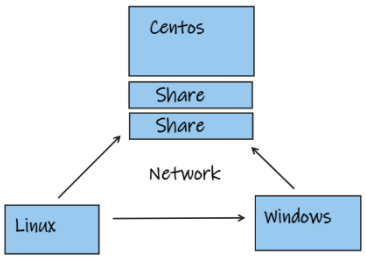
c. B şıkkında yapılmak istenileni yapmak için bir başka yol daha var. Bir dosyamız daha var. Aslında official anlamında bu dosya kullanılıyor. Bu dosya "/etc/grub.d/" dizininin dosyalarını listelediğimizde "40_custom" adında bir dosya görünür. İçi boş olan bu dosyaya resimdeki komutu girip kaydederiz. Bu dosya "grub.cfg" dosyasına müdahale etmemizin önüne geçen bir dosyadır. Tek başına bir önemi yok çünkü bu dosyayı "grub.cfg" dosyasına basmamız lazım. Bunun için komutumuz ise

"**grub2-mkconfig --output=/boot/grub2/grub.cfg**" komutudur. Bu komut "grub.cfg" dosyasını resetler ve manuel olarak yazdığımız komut varsa onun üzerine yazar. Buradan da anlaşılacağı gibi eğer yanlış bir konfigürasyon yaptığıysanız bu komut kullanarak resetler ve eski haline geri döndürebilirsiniz. Bu yol yani c şıkkındaki yol resmi yoldur. Daha güvenilirdir ve daha az hata yapma imkânı verir. Amaç hata yüzdesini düşürmektir.

SAMBA

Linux dosyalarını dış dünyayla paylaşabilmek için "Samba" kullanılır. Samba Server ile bir Linux'tan başka bir Linux'a ya da başka bir linuxtan kendi linuxunuza bağlanmak için, paylaşım olayı için Samba kullanılır. Bağlanmak için Samba client, file share için Samba server kurulur. Windows için bir şey kurmaya gerek yok. Yani Samba server görevleri;

1. Paylaşım yönetmek
2. Print server
3. Master browser
4. Domain browser



Samba server 3 temel servisten oluşur. Bunlar NMBD, SMBD ve WİNBİND servisleridir.

1. NMBD servisi: Ana servis olmakla birlikte, NET BIOS ağlarına girmeyi sağlayan, windowsla bağlantıyı ve bütün temel ağ tarama işlemlerini gerçekleştiren servis
2. SMBD: Kimlik doğrulanması ve dosya aktarımlarını sağlayan servis
3. WİNDBİND: Domain ortamlarında bizim bulunmamızı sağlayan

Servisler bir işletim sisteminde belli görevleri yapılmasını sağlayan ve hiçbir kullanıcının başlatılmasına muhtaç olmayan programlardır.

Centos7 işletim sisteminde terminalden IP konfigürasyonlarını yaptıktan sonra firewall kısmını kapatabilir ya da port açabiliriz Samba için. Her Linux işletim sisteminde Firewall vardır. Firewall, TCP/IP protokolü üzerinden iletişim kurulan portların açılıp kapanmasını sağlayan yazılımlardır. Yapacağımız işlemler için firewall'u kapatabiliriz. İlk önce firewall olup olmadığına bakmak için

"**systemctl status firewalld**" komutunu kullanırız. Eğer açıksa kapatmak için;

"**sudo systemctl stop firewalld**" komutunu kullanırız.

Şimdi ise Samba'yı sisteme eklemektir. Bunun içinde;

"**sudo su**"

"**yum -y install samba-client samba-common**" komutlarını kullanırız. Bu işlemlerden sonra Samba paket dosyalarını konfigürasyonlarız. Bu pakete ait config dosyasını bulup onun üzerinden işlem yaparız. Aradığımız dosyayı da bulmak için;

“cd /etc” sonra “ls -l | grep samba” komutunu kullanarak bulabilir sonra bu dizine girdiğimizde karşımıza config dosyasının çıktığını görebiliriz. Örnek config dosyasında neler yapabileceğiniz görebilirsiniz. Çok ayrıntılı bir konfigürasyon dosyasıdır. “smb.config” dosyasında global kısım makinenin adı vs. ifade ederken dosyanın devamında gözüken paylaşımlar da verilen izinlerdir.

```
[share1]
path = /samba/share1
browsable =yes
writable = yes
guest ok = yes
read only = no
force user = root
[share2]
path = /samba/share2
browsable =yes
writable = yes
guest ok = yes
read only = no
force user = root
```

Yukarıdaki resimde gözüken bir dosya paylaşımı eklersek belirtilen dosyaya, artık bu dizin erişime açık anlamına gelmez. Bunun için birkaç işlem daha yapmamız lazım. Eğer belirtilen dizinler yoksa onları oluştururuz. Sonra dizinlerin üzerinde yetki ayarlaması yaparız belirlediğimiz şekilde. Bunları yapınca da daha bitmiyor. Araya **“SeLinux (Security-Enhanced Linux)**” giriyor. “SeLinux” red-hat tabanlı linux sistemlerinde otomatik gelen ve sistemden bağımsız kullanıcıların işlemlerini minimum haklarla yapmasını isteyen ve bunu uygular. Root olmanıza rağmen bazı işlemlerde engel alıyorsanız bunun sebebi budur. Bunu “smb.cfg.example” dosyasında gözükür nedeni. Bunu istemezseniz “SeLinux” un engellediği dizinler için ekstra düzenlemeler yapmamız lazım. Bu komut “chcon” komutudur. “smb.cfg.example” dosyasında da “SeLinux” hakkında bilgi veriyor. İlgili dizinde “SeLinux”u etkisiz hale getirmek istiyorsanız;

“**chcon -t samba_share_t [directory path]**” işinizi görecektir.

Bu işlemi yaptıktan sonra da “smb.service” ve “nmb.service”lerini enable etmemiz gerekiyor. Eğer bunlar yoksa “yum install samba samba-client” komutu ile yükleyebilirsiniz.

“systemctl enable smb.service”

“systemctl enable nmb.service”

Sonra

“systemctl start smb.service”

“systemctl start smb.service”

Sonrasında da yine aynı dosyaları “start” ile başlatacağız ve artık belirlediğimiz dosyalarımız paylaşıma açık hale gelir. Bu dosyaya Windows üzerinden erişmek için “C: /Windows/System32/drivers/etc” klasörünün içindeki host dosyasına “netbıos” isminizi ve linux’un IP adresini girmemiz lazım. Sonrasında “HOME+R” kombinasyonuyla açılan regedit kısmına \\[dosyayayazdığınızisim]\ diye girerseniz dosyalara ulaşabilirsiniz.

Şu ana kadar bir dosyayı paylaşıma açmak için şunları yaptık:

1. Belirlenen dosyayı paylaşıma açmak için smb.config dosyasına adresiyle birlikte dosyayı ekledik.
2. Paylaşıma açmak için ayarladığımız dosyanın izinlerini konfigürasyon ettik.
3. Firewall kısmını kontrol ettik ve eğer aktif durumda ise kapalı hale getirdik.
4. Selinux etkisiz hale gelmesi için "**chcon -t samba_share_t [directory path]"** komutunu kullanarak ilgili dosya ya da dosyaların üzerinden etkisiz hale getirdik.
5. Samba serverlar olan "smb.server" ve "nmb.server" serverlarını enable yapıp start ettik.
6. Eğer Windows üzerinden bir erişim sağlanacaksa "C: /Windows/system32/drivers/etc/host" dosyasına netbıos isminizi IP adresinizle birlikte girdik.
7. "HOME+R" kombinasyonuyla açılan kısma "\\[girdiğin isim]\" yazarak dosyaları gördük.

SeLinux yazılımını dosya bazlı değilde tamamen kapatmak istersek konfigürasyon dosyasını açmamız ve orada değişiklik yapmamız lazım. Bunun için açılan dosyada "SELINUX=enforcing" kısmını "SELINUX=disable" yapıyoruz ve sistem yeniden başlayana kadar uyguladığımız işlem geçerli olacaktır ve Selinux tamamen kapalı olacaktır. Bir başka yol ise "getenforce" ve "setenforce" komutlarını kullanmaktır.

getenforce: Selinux açık mı kapalı onu gösterir. (enforcing: açık, permissive:kapalı)

setenforge: Selinux açıp kapamaya yarar. Komutun yanına "0" yazarsak kapırken "1" yazarsak açılır.

Şimdi de Linux Client üzerinden dosyaya erişim sağlamak istersek Linux server tarafında Selinux ve firewall tarafını yine aynı şekilde yaptıktan sonra kaynak linux sistemindeki dosya paylaşımını görmek için başka bir linux sisteminin terminalinden ya da GNOME üzerinden yapabiliriz. Eğer terminalden yaparsak SAMBA Client paketini yüklemek lazım eğer yoksa. Onun için de;

"sudo yum -y install samba samba-client" komutu kullanılabilir. Sonra ise

"sudo smbclient -L //[targetIP]/" komutu ile dosya paylaşımını listeleyebiliriz.

"sudo smbclient //[targetIP]/" ile smb'ye bağlanabiliriz. Buradan dosya paylaşımında paylaşılan dosyalar üzerinde belli işlemler yapabiliriz. Smb komutlarının detaylarını https://www.samba.org/samba/docs/current/man-html/smbclient.1.html sitesinden öğrenebilirsiniz.

Eğer GNOME üzerinden yapacaksak Desktop kısmındaki Home klasörüne tıklarsak orada "other locations" kısmında arama yeri var. Oraya smb ile yaptığımızdan "smb://[hedefIP]/" şeklinde yazarsak dosyalar karşımıza çıkacaktır.

SAMBA PAROLA PAYLAŞIMLI DOSYA

Şu ana kadar dosya paylaşımlarını yaparken paylaşılan dosyayı şifresiz yaptığımız için isteyen herkes dosyaları değiştirebiliyor. Bunun önüne geçmek için, dosya paylaşımında şifre koymak istersek mesela bir gruba ait kullanıcılar sadece erişsin diyorsan o zaman;

1. Bir grup oluşturulur.

2. Bir kullanıcı oluşturulur ve kullanıcı oluşturulan gruba dahil edilir.

3. Paylaşım dosyaları üzerinde gerekli izin düzenlemeleri yapılır.

4. smbpasswd -a [username] ile parola koyulur paylaşım dosyasına.

5. smb.config dosyasında şifre koyulan dosyanın ayarlarından "guest ok" kısmını "no" diye değiştirip "valid user= [username]" ya da "valid user=@[groupname]" şeklinde satır ekleyip kaydedilir.

6. Artık belirtilen dosyay girmek için şifre ve kullanıcı adı gerekecektir.

Tüm bunlar yapılırken firewall ve Selinux kısımlarını kapalı olması gerekir.

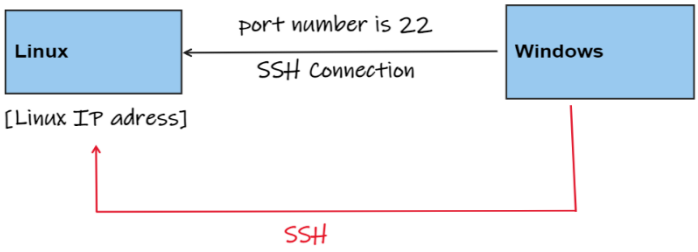
SAMBA MİNİMAL (Sadece Siyah Bir Ekran)

Minimal kurulumda karşımıza sadece terminal ekranı gelir. Buradan login olup işlemleri yaparız. Böyle bir kurulumda çoğu şey olmadığından "ifconfig", "nano" gibi komutlar vs. indirmemiz gerekir. Mesela ifconfig için "net-tools" indirmek gerekir. Bu sistemde Samba kurarız aynı GNOME ya da KDE'de olduğu gibi. Yani siyah bir ekranda çalışmak deneyimini böylece tatmış oluruz.

LİNUX OpenSSH SERVİSİ VE UZAK SSH BAĞLANTISI

Linux makinelerini uzaktan yönetebiliriz. Uzaktan olması daha mantıklıdır çünkü sistem odasına gidip bir sunucunun başında oturmak çokta söz konusu değildir. Windows kullananlar makinenin remoot kısmını açarlar ve böyle kullanırlar. Linux'ta remoot Desktop özelliği yoktur. O yüzden Linux'u SSH (Secure Shell) ile uzaktan yönetiriz.

Sunucu tarafında ssh servisi çalıştırılır, client tarafında ise client servisi çalıştırılır ve güvenli şekilde bağlanabilir. SSH otomatik olarak 22 numaralı portu kullanır. Bu yönetimin terminal ekranından farkı yoktur. Linux uzaktan böyle yönetilir.



Linux'ta kurulması gereken SSH paketi "**OpenSSH**" paketidir. Servisin adı ise "**shhd**" servisidir. Eğer Linux'a önceden Samba yüklediyseniz kurulu gelir büyük ihtimalle. Kontrol etmek için "**systemctl restart sshd**" komutunu kullanıp hata vermiyorsa vardır. Statüsünü görmek için "**systemctl status sshd**" komutu işimize yarar. Aktif olup olmadığını buradan bakabilirsin.

Windows'ta otomatik olarak ssh istemcisi olmaz. Bunun için servisler, araçlar vardır. Yani Windows'tan Linux sistemine uzaktan bağlantı için bir araç gerekir (Putty gibi). Fakat Linux ve MacOS sistemlerde ssh istemcisi otomatik olarak geliyor. Bunun için Linux'ta "ssh" komutunu kullanırız.

"**ssh [IP adress]**" ya da

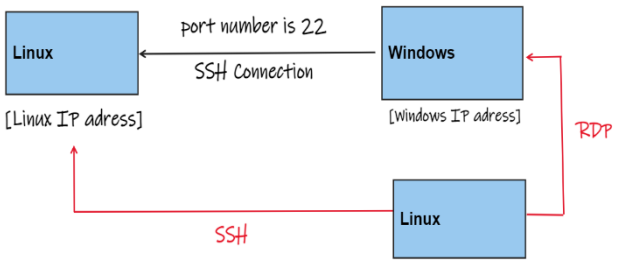
"**ssh -l [username] [IP adress]**" komutlarından birisi işimizi görür.

Linux bir makineye uzaktan Windows ve başka bir Linux makineden bağlantıyı gördük. Peki ya Windows bir makineye Linux üzerinden nasıl bağlantı sağlarız?

Windows'ta ssh yerine "**Remote Desktop Protocol**" kullanırız. Çünkü Windows GUI dayalı bir işletim sistemine sahipken Linux terminal üzerinden işlem yapar. "**RDP**" bağlantısı yapmak gerekiyor. Bunun için terminalden değil bir araç kullanırız. Centos7 sürümünde "utilies" kısmında "Remote Desktop Viewer" aracını açarak gerekli IP adresini ve kullanıcı ismini (bağlanacağımız makinenin kullanıcısı) girerek uzaktan bağlantı sağlayabiliriz. Bunun için uzaktan bağlanacağımız Windows makinenin remote olma

iznini vermesi gerekiyor. Bunu da bilgisayar özelliklerine girdikten sonra gelişmiş sistem ayarlarından değiştirilebilir.

Şu ana kadar yaptıklarımızı bir şekilde gösterecek olursak aşağıdaki gibi olur.



KVM

Linux üzerindeki sanallaştırma yazılımı olan KVM, "opensource" kaynak, ücretsiz ve lisanslıdır. Centos7 üzerine kuracağımız bir KVM ile işlemler yapacağız. Normalde Minimal Paket içinde KVM kurulması daha mantıklı iken GNOME üzerinden de kurulabilir. Her iki türlü de terminaldeki komutumuz:

"**sudo yum -y install qemu-kvm qemu-img virt-manager libvirt libvirt-python libvirt-client virt-install virt-viewer bridge-utils**"

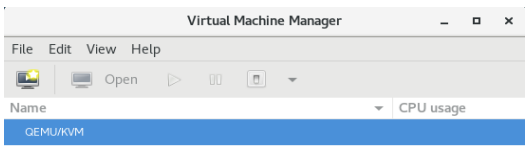
Bu komut ile KVM için gereken paketlerimiz kurulacaktır. Ardından;

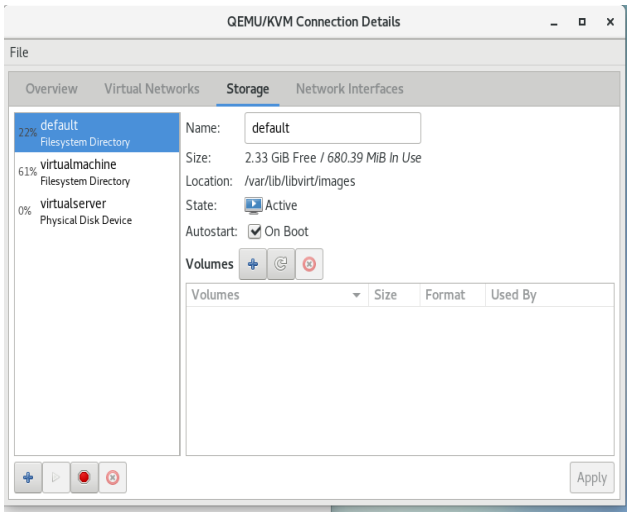
"systemctl enable libvirtd" ve

"systemctl start libvird" komutlarını çalıştır. Sonra;

Yukarıdaki komut aslında bir ön gereksinimdi. Şimdi GUI üzerinden KVM yönetmek için birkaç paket daha yüklememiz gerekiyor. Onlarda:

"**sudo yum -y install xorg-x11-xauth xorg-x11-fonts-* xorg-x11-utils**" komutu ile yönetmek için gereken paketleri kurmuş oluruz. Artık "Virtual Machine Manager" adında bir araç eklendi GNOME Desktop üzerine. Oradan KVM'i açabiliriz. Terminalden "virt-manager" diye de açabiliriz. Ayrıca Samba da yüklersek dosyaları kopyalama, paylaşma da bize yardımcı olur. O yüzden Samba da yüklemeliyiz.

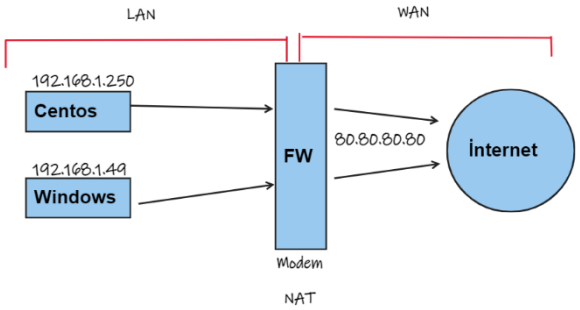




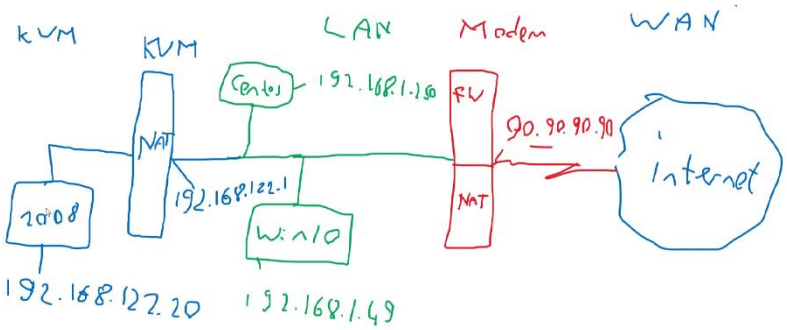
KVM'i açtığımızda karşımıza yukarıdaki şekilde gösterildiği gibi ekran çıkar. Burada "QEMUKVM" kısmına sağ tıklayıp details kısmına tıklarız. Açılan pencerede de 4 farklı bölüm vardır. Buralardan KVM ayarları yaparız. Storage kısmından KVM için ayırdığımız dizini ekleriz. Dizin ekledikten sonra dizinde önceden gönderdiğimiz iso dosyaları vardır. Bunlar Centos7 ve Windows11'dir. Görüleceği dizinde yeterli alan olmadığından KVM'e bir disk tanımlarız. Bu diski sadece KVM kullanır, görür, kullanır. Yani asıl işletim sistemimiz Centos7 bu diski çalıştıramaz, paylaşıma açamaz. Bunun içeriğini göreceğiniz tek yer KVM'dir.

KVM otomatik olarak NAT yapar.

NAT: İnternete IP vererek çıkarız. Evlerimizdeki modemler NAT yapar. Yani bir makinemizdeki IP adresimiz modeme gider oradan internete başka bir IP adresiyle çıkar. Başka bir IP adresi her makine için aynı olacaktır. O yüzden internete aynı IP ile çıkarız. Bu işlemi yapan NAT'tır.



İşin içine KVM girdiğinde de NAT olduğunda;

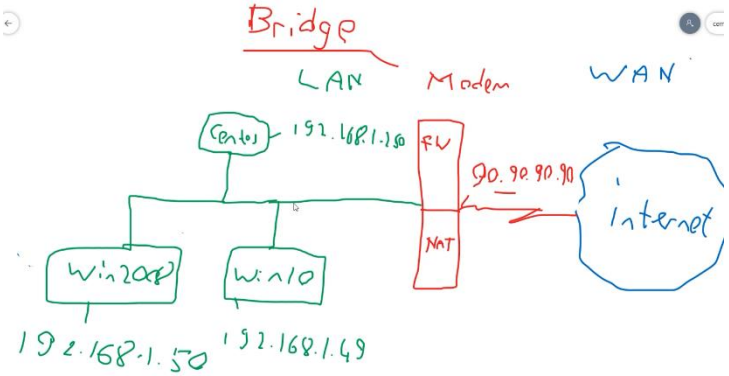


Böyle bir durum olur. Buda işi oldukça zorlaştırır. O yüzden KVM' de NAT yerine Bridge kullanırsak daha hızlı bir iletişim kurabiliriz.

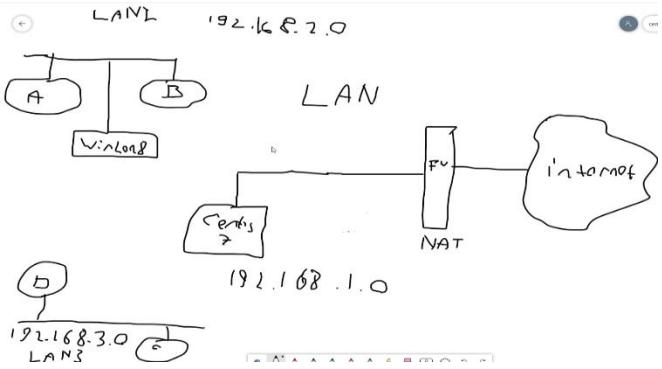
KVM aracında kurduğumuz sanal makinelerin network bağlantı tiplerini düzeltmek içinse "Virtual Network" ve "Network Interface" kısımlarından düzenleme yaparız. Bunun için Virtual Network kısmındaki bölümü sileriz sonra "Network Interface" kısmındaki "ens33" bölümünü siler ve aynı yerden ens33'ü yeniden oluştururuz gerekli ayarlamaları yaparak. Brigde kısmını seçerek sanal makinenin içine sanal makine kurduğumuzda en içteki sanal makinenin internete girmesi için dıştaki sanal makine köprü görevi görür. Bunu "/etc/sysconfig/networscripts" klasöründeki dosyalardan görebilirsin. En içteki sanal makinede de ssh gibi uygulamalar yapılabilir.

LİNUX KVM VİRTUAL NETWORK TİPLERİ-ISOLE NETWORK

İsole Network derken biz istersek bağlantı sağlarız istersek sağlamayız. Sanal içinde sanal makine kurarken en içteki makineye bir isole Network yaparsam dıştaki makinenin networküne istersem



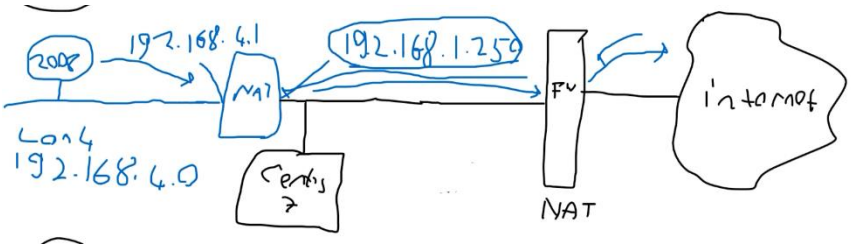
bağlanırım istersem bağlanmam. Ya isole ederek networklerin birbirlerine kavuşamamaları sağlarım. Ya da oluşturmuş olduğum networkü fiziksel networküme yönlendiririm. İsole Networkler kendi içindeler ve birbirlerine erişemezler. Yani şöyle bir durum olur.



KVM üzerinde bir "Virtual Network" kurduğumuzda bu isole ya da forward olabilir. Network konfigürasyon dosyasına bu oluşturulan network ile ilgili bir ethernet kart, bir dosya oluştuğu gözlemlenir. Yani sanal adaptör eklenir ("ifconfig" ile bakılırsa görülür.)

NAT, ROUTE, OPEN Network

Eğer KVM NAT yaparsa internete gidiş yolu şöyle olur:



Route ise kendi IP'si varsa kendi IP'si ile "FW" kısmına gider. Yani NAT kendi IP'sini enkapsüle edip başka bir IP'ye bağlanıp "FW" kısmına gider. Ortada ROUTE yapılmış bir network varsa IP değiştirme yoktur. Kendi IP'si ile gider. Route yaptığımızda internete çıkamayabiliriz. Mesela ROUTE yaptığımızda 192.168.5.53 gibi bir IP ile girmeye çalıştığımızda fiziksel makinemizdeki IP'ye gönder paketleri öyle internete gir gibi bir şey diyoruz. OPEN Network'te ise firewall yoktur. Port açıp kapatmak yoktur. Ama çalışma tekniği olarak ROUTE mantığıyla çalışır.

LİNUX KVM ÇOKLU NETWORK KART KONFİGÜRASYONU

Birden çok network kartı bağlayıp bunları KVM üzerinde oluşturduğumuz networkleri bunlardan birine bağlayarak oradan internete erişim sağlanmasını isteyebiliriz. Önceden KVM'deki networkleri asıl sanal makinemizdeki tek bir network kartına bağlamıştık ve hepsi aynı yerden internete erişmeye çalışıyordu diyebiliriz.

Şimdiye kadar bir Linux red-hat tabanlı bir sanal makinede sanal bir makine kurmaya çalıştık. KVM olarak adlandırılan bu aracı Windows üzerinden yönetmek zor. Onun için Windows işletim sistemine sahip makineye KVM için olan bir remote araç yüklemeliyiz.

LİNUX KVM STORAGE DİZİN

KVM üzerinde storage kısmından oluşturduğumuz diskle kurduğumuz Centos7 sistemini yedeklemek, daha sonra kullanabilmek için ya da disk oluşturmayıp asıl sanal makinemize eklediğimiz bir diskten bir partition oluşturup bu partition kısmını bir dizine formatlayıp mount edersek, sonrasında KVM içindeki kurduğumuz işletim sistemini "clone" kısmından bu dizine yedekleyebiliriz. Bu da daha sonra kullanabilmek için oldukça işimize yarar.

NOT: Eğer network bridge modda olduğunda ping alamıyorsanız bunun nedeni bridge moda aldığınızda config dosyasına dns bilgilerinin otomatik olarak gelmemesinden kaynaklanır. Eğer böyle bir durumla karşılaşırsanız manuel olarak kendiniz eklemelisiniz dnsleri.

Minimal kurulu bir Centos'a KVM kurulu yapabiliyoruz. Bunu da

FİZİKSEL MAKİNEDE CENTOS VE KVM KURULUMU

Fiziksel bir makineye Centos kurduğumuzda sanal makineden ssh ile bağlantı yapabiliriz ya da Windows üzerinden bir ssh uygulamasıyla. Sanal da ne yaptıysak fiziksel makinede, makinenin başında olmadan uzaktan yöneterek belli konfigürasyonları yapabiliriz. Bunun için KVM ile bağlanarak network ayarlarını yapabilir, terminal ekranından ssh ile bağlanıp gerekli konfigürasyonları yapabilir ya da paylaşım yaparak Windows üzerinden paylaşım yapılan dosyalara bir şeyler ekleyebilir bir şeyler çıkarabilir ya da ayarlayabiliriz.

"**nmcli d**" komutu makinedeki ethernet kartlarının durumunu aktifliğini gösteriyor.

Makinedeki wireless kartını başta kurmadıysanız ve aktif olmasını istiyorsanız ilgili konfigürasyon dosyasındaki "onboot" kısmını "yes" diye değiştirerek reboot yaptığınızda artık aktif olacaktır. Kapatmak için ise no yaparsanız yine istediğiniz olacaktır.

Şimdi sırada fiziksel bir Centos kurulu makineye uzaktan bağlanarak "WebVirtMgr" adlı bir open source yüklemekte. Bu sayede uzaktan birçok sunucuyu aynı ekrandan yönetebiliyoruz. Öncelikle KVM'de kurduğumuz Management bir makineye bunu yüklemek. Bunun adımları ise sırayla söyle;

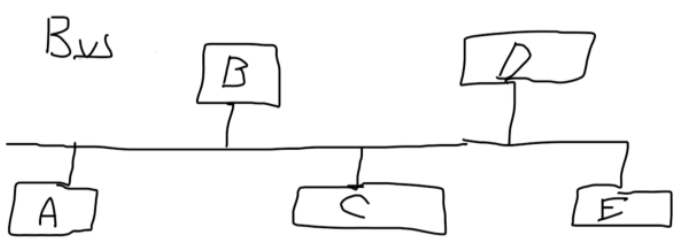
1. **"yum -y install epel-release"**
2. **yum -y install git python-pip libvirt-python.x86_64 libxml2-python python-websockify supervisor nginx**
3. **"yum -y install gcc python-devel"**
4. "**pip install numpy**"
5. **yum -y install git python-pip libvirt-python libxml2-python**
6. "**pip install –upgrade pip**" → eğer 3.adım hata verirse 4.adımı yap sonra 3 sonra 5'ten devam et.
7. "**mkdir www**"
8. "**cd www/**"
9. "**git clone git://github.com/retspen/webvirtmgr.git**"
10. "**pip install -r requirements.txt**"
11. **"./manage.py syncdb**"
12. conf.d]# "**touch webvirtmgr.conf**"
13. www]# "**chown -R nginx:nginx webvirtmgr/**"
14. "**cd /etc/supervisord.d**"
15. "supervisord.d]# "**touch webvirtmgr.ini**"
16. "**nano webvirtmgr.ini**"
17. "**systemctl restart supervisord.service**"
18. "**cd /var/www/webvirtmgr/**"
19. "**git pull**"
20. **"./manage.py collectstatic**"
21. "**systemctl restart supervisord.service**"
22. **"./manage.py runserver 0:8000**" ya da **"./manage.py runserver 0:8001**": sondaki rakam eğer yazdığınız doluysa son hanesini değiştirip devam edin.

https://github.com/retspen/webvirtmgr/wiki/Install-WebVirtMgr linki ile de kurulumu buradan da yapabilirsiniz.

LİNUX VE TEMEL NETWORK

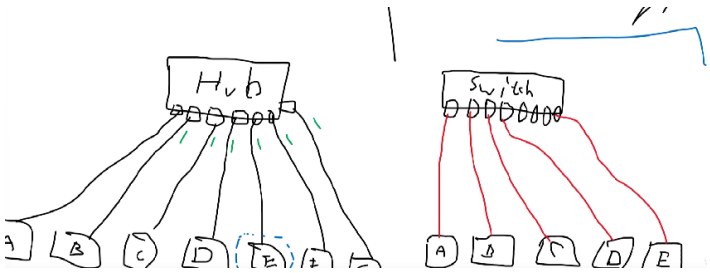
Birbiriyle veri iletişimi sağlamak için gereken altyapının tamamına network denir. Belli kuralları vardır. Bu kuralları protokoller belirler. İki makinenin bir iletişim kurması için bağlı olması lazım. Buna fiziksel katman denir. Fiziksel katmanın üstünde protokoller giriyor. Geçmişten günümüze birçok protokoller kullanılmışken şu an çoğunlukla TCP/IP protokolü kullanılıyor.

İlk başlarda "**BUS**" topolojisi ortaya çıktı. Mühendisler makineleri tek bir kablo şeklinde birbirine bağlayıp iletişime geçsin dendi (Çizgi modeli). Ama kablo da bir kopukluk olunca tüm iletişim kopuyordu. O yüzden çok kullanılmadı. Sonra "**RİNG**" topolojisi ortaya çıktı. Burada da halka şeklinde bir



model oluştu. Bilet mantığıyla hedef olmayan makine yanıt vermesin diye bir yol çizen bu model kopukluk hatasını düzeltirken performans olarak yetersizdi.

Günümüzde ise “**STAR**” topolojisine gelindi. Günümüzün network yapıları oluştu bu modelle. “HUB” portlar oluşturuldu. Sonra her makine bir porta bağlandı. Hepsi ayrı bir kablodan bağlıydı. Sonra “**HUB**”un getirdiği dezavantajları düzeltmek için “**SWİTCH**”e geçildi. Switch MAC adresi tuttuğundan aldığı paketi sadece hedefe yollar. HUB ise MAC adresi tutmadığı için aldığı paketi herkese gönderir. Dezavantajı da budur zaten. Artık HUB yerine “SWİTCH”ler kullanılıyor.



Şu ana kadar 2 katman kullandık. Makineleri birbirine fiziksel olarak taktık ve paketleri birbirlerine paketleri göndermek için bir cihaz kullandık. Ama bu veri neye göre oluşacak ve hangi yolu izleyecek onu belirleyen protokoller belirler. Şimdi de **TCP/IP** protokolünü ele alacağız. Protokoller networkün dilidir.

TCP/IP

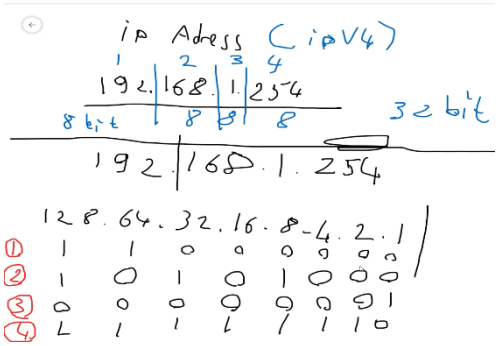
Mac Adress

Her makinede nic kart var. Bu networke giriş yapabilmek için gerekli bir karttır. Mac adresi de bu kartlarla birlikte gelir. Yani Mac adresi kartın parametresidir. Switch’in yolunu bulmasını bu sağlar. Tek olmalıdır, başka bir tane daha aynı MAC adresi olmamalıdır. Kartı networkte tanımlar.

IP adress

TCP/IP protokolüne göre ağ üzerinde kendisine tanıdığı parametredir. Essiz ve benzersiz olmalıdır. Peki IP adres nasıl belirlenir?

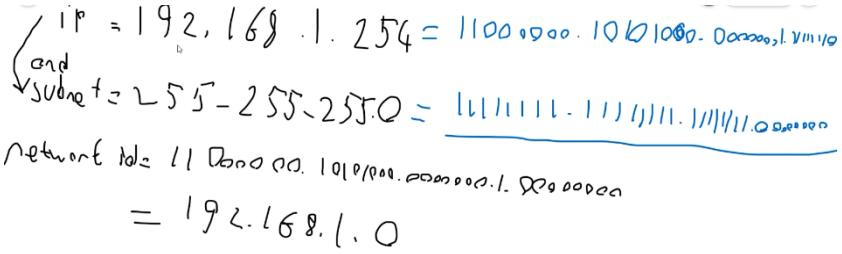
Bilgisayar hep ikilik düzlemde çalışır. Ama bunları akılda tutmak zor olduğundan bizler onluk yazalım bilgisayar ikilik anlasın mantığıyla yola çıkmışlar. IP adresi 4 bölümden oluşur. Bunlar “.” İle ayrılır. Her bir bölüm 8 bitten oluşur. Toplam 32 bittir.



Subnet Mask

Bir IP'nin hangi networkte bulunduğunu anlamamızı sağlayan bir parametredir. Yani bir bilgisayarın hangi ağa bağlantılı olduğunu söyler. Subnet nasıl oluşturulur?

IP oluşturma mantığıyla aynıdır. Ama Subnet parametresi yalnız başına hükmü yok. IP ile birleşince bir anlama varıyor. Bu iki parametre, IP ile Subnet birleşince yani "and" işlemi uygulanınca "Network ID" veriyor.



Bir Networkte kaç cihaz olacağı nasıl hesaplanır?

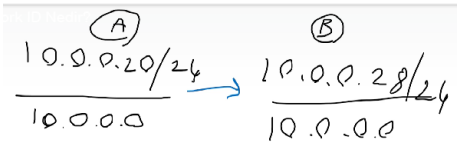
$\mathbf{2^{bit} - 2}$ şeklinde hesaplanır. Buradaki bir Subnet bölümlerinde kaç 0 varsa o kadar 8 ekleriz. Yani mesela 255.255.255.0 olan bir subnette $2^8 - 2$ adet cihaz olurken, 255.255.0.0 olan bir subnette ise $2^{16} - 2$ adet cihaz ve 255.0.0.0 ise $2^{24} - 2$ adet olur.

255.255.255.0 → C class → 192.168.1.0/24 (C class demektir.) (Prefix=24'de denilebilir.)

255.255.0.0 → B class → 192.168.1.0/16 (B class demektir.) (Prefix=16)

255.0.0.0 → A class 192.168.1.0/8 (A class demektir.) (Prefix=8)

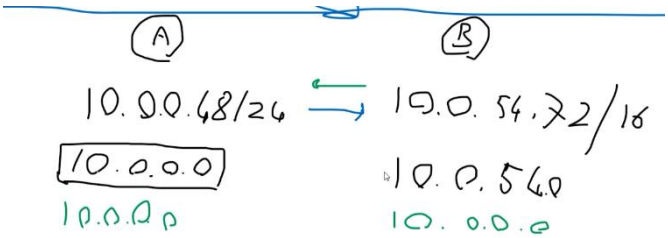
NOT: İki makinenin Network ID'si birbiri ile aynı ise herhangi bir araca kalmadan birbirlerine ulaşabilirler.



NOT

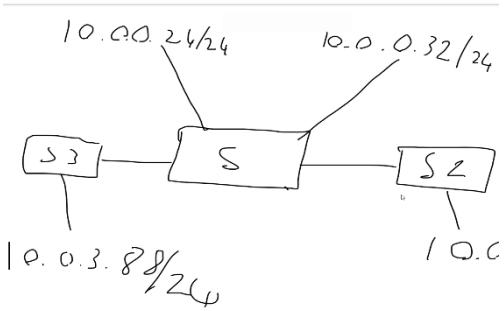
Bir makine başka bir makine ile iletişim kurarken ilk önce kendi Network ID'sini çıkarır. Sonra hedef makinedeki Network ID'sini öğrenmek ister. Bunu nasıl öğrenir?

a. **Kendi subneti ile karşı makinedeki IP adresini** "and" işlemine koyar ve sonucu karşılaştırır.



Resimde görüldüğü gibi eğer A'dan B'ye gitmek istersek Network ID eşleşmediğinden gidemez, erişemez. Kendi subneti ile karşının IP'sini "and"ledi. B'den A'ya gitmek istediği zaman görülüyor ki Network ID'ler aynıdır. Ama B, A'ya ulaştığında karşıdan cevabı alamadığından "request" hatası alacaktır. Yani böyle bir durum yanlış bir konfigürasyona örnektir.

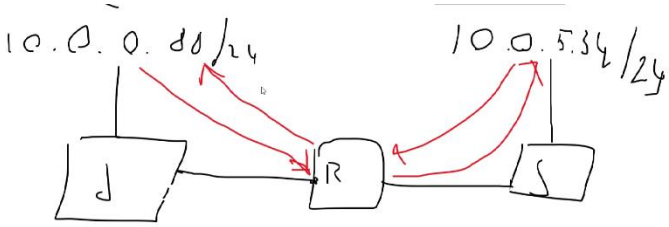
İki makinenin Network ID'leri aynı olduğunda iletişim için aynı SWİTCH'e bağlanmaları yeterlidir.



Resimde görüldüğü gibi 10.0.0.24 ile 10.0.0.32 birbirlerine erişebilirken 10.0.3.88 diğerlerine erişemiyor. Erişim sağlayabilmesi için bir yönlendirici kullanması gerekir. Bunun sonucunda da "Router" ve "Gateway" kavramları ile karşılaşıyoruz.

Router

Farklı Network ID'sine sahip cihazların birbirleriyle iletişim kurabilmeleri için TCP/IP protokollerine uygun olarak ağ geçidi denilen cihazlara denir. Birbirleriyle farklı Network ID'sine sahip cihazların iletişim sağlamasını sağlayan cihazdır.



Resimde görüldüğü gibi bir router aracılığıyla paket gönderiliyor. İşte protokollerin yönlendirilebilir olma özelliği buradan çıkıyor.

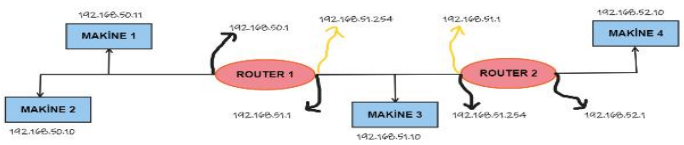
Gateway

Bir makine başka bir ağa nasıl gidileceğini gatewayden öğrenir. İletişim kuracak makinelerin çıkış kapısını oluşturur.

NMTUİ TOOL VE NETWORK YAPILANDIRMASI

IP yapılandırmasını sağlayan bu araç net-tools ile gelir. Bu araç sayesinde internet hostname, IP adresi, Gateway gibi birçok özelliği ayarlayabilirsiniz. İnternet isminizi de ayarlayabilirsiniz. Örneğin bir isole networke bağlı iki makine birbiriyle bağlantı kurabilir çünkü aynı isole networkteler. Fakat başka bir isole networke bağlı başka bir makine bu makinelere bağlanmak istediğinde hata ile karşılaşır. Çünkü farklı networktelerdir. İletişimi sağlamaları için bir tane gateway lazım. Eğer gateway ayarlanırsa iletişim kurabilirler.

"**nmtui**" komutu ile bu araca girebiliriz. Bu araç sayesinde isole edilmiş farklı makineleri router aracılığıyla birbirleriyle iletişime geçebilirler. Aşağıdaki şekilde de temsili bir şeması verilmiştir.



Router görevi doğru şekilde yapması için, /etc/sysctl.d dizininin içine “ip_forward.conf” dosyası oluşturup içine “net.ipv4.ip_forward = 1 “ yazmalıyız. Ardından “sysctl -p /etc/sysctl.d/ip_forward.conf “ komutunu çalışıtırırsak artık routerler yönlendirme yapacağını bilir. Aksi paketi alır ama ne yapacağını bilemez.

ROUTİNG TABLE VE STATİC ROUTE

Routing table, makinenin hangi network ID’ye hangi gateway kullanılarak gideceğini öğrendiği tablodur. Bir yol haritasıdır. Her makinede bulunur. Bir Router, bilmediği her şeyi default gateway’e yönlendirir. Genelde internet tarafına default gateway yazılır. Yani Routing table’a baktığında bulamazsa default gateway’e yönlendirir paketi.

“**ip route**” komutu ile default gateway’inizi öğrenebilirsiniz. Ya da;

“**route -n**” komutu daha detaylı bir şekilde size gösterir. Burada karşımıza çıkan 0.0.0.0 default gateway’i ifade eder. Default yazmasa bile bunun anlamı default gatewaydir. “Interface” de çıkış kapısıdır.

“**ip route add [IPadress]/subnet] via [gatewayadress] [interface(istersen)]**” komutu ile static olarak route ekleyebilirsin.

Default gateway bir adet girebildiğimizden ek olarak eklemek istediğimiz bir route varsa onu static eklemeliyiz. İşte static route’ta buradan geliyor.

Yukarı belirtilen komutları yazdıktan sonra makineyi reboot edersek yaptıklarımız kaybolur. Bunu kalıcı hale getirmek için konfigürasyon dosyasında ayarlar yapmak lazım. Route konfigürasyon dosyası “/etc/sysconfig/network-scripts/” dizini altında “route-[NetworkName]” dosyasıdır. Eğer dosya yoksa kendiniz oluşturabilirsiniz. Bu dosyanın içine de “**[IPadress]/subnet] via [gatewayadress]”** şeklinde ilgili routeları girerek kalıcı hale getirebiliriz.

Şimdi de isole network yapısındaki routerlarla bağlı makinelere bir adet NAT bağlayarak artık makineleri internete çıkaralım.

NAT KONFİGÜRASYONU

Local networkteki makinelerin dışarıya IP ile çıkmasını sağlar. Yani Localdeki IP adresini Wan IP’sine dönüştürüyor diyebiliriz. Diğer bir ifade ile de internal tarafından gelen IP’leri external tarafındaki IP’lere çevirerek internete dış networke çıkarır.

Eğer NAT konfigürasyonu ile internete çıkmak istersek makineyi ilk önce routing yapısını enable yaptıktan sonra aşağıdaki komutları sırayla girebiliriz;

“**firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTİNG [internete_gidecek_internet_adı] -j MASQUERADE -s [Nat_hangi_isole_makineye_bağlıysa_o_IP (Örneğin 192.168.50.0]/[subnet]**”

“firewall-cmd --change-interface=[internete_gidecek_internet_adı] --zone=external –permanent”

“firewall-cmd --set-default-zone=internal”

“firewall-cmd --complete-reload”

En son kontrol için ise şu komutları kullanabilirsin;

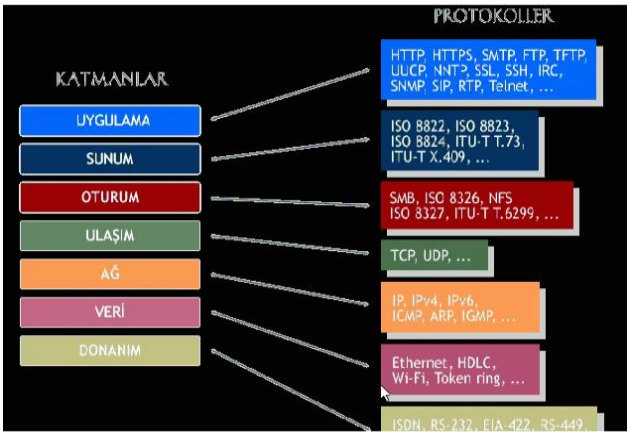
“**firewall-cmd --list all**”

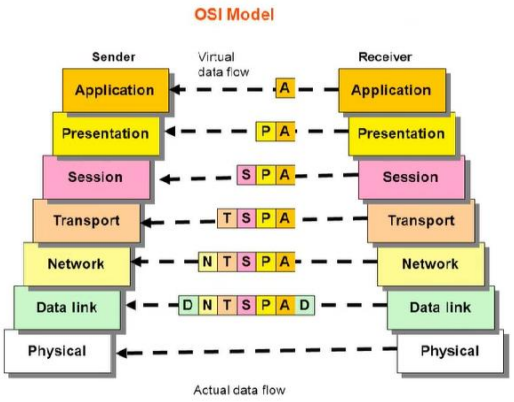
"**firewall-cmd --list-all --zone=external**" → Eğer bu komutu çalıştırdığında interface kısmında "**[internete_gidecek_internet_adı]"** yazdığın isim varsa doğru olmuştur.

"**firewall-cmd --list-all --zone=internal**"

TCP/IP OSİ KATMANLARI VE PORT KAVRAMI

OSİ 7 katmandan oluşur. Hangi makinenin hangi katmanda çalıştığını bilirsek bu katmanların çalışma mantığını bilmek, hangi işlemleri yapabileceğini bilmek ve ona göre dizayn etmek açısından önemlidir. Katmanlar ise şöyledir;





Yukarıda gösterilen katmanları akılda daha kalıcı kalması için temel de 3 bölüme ayırabiliriz:

Port bir çıkış kapısıdır. Yani sisteme giriş ve çıkış sağlar. Paketlerin girip çıktığı kapılardır. Güvenlik açısından kolaylık sağlansın ve hızlı çözümler bulmak adına port kavramı çıkmıştır. Güvenlik için o portu açmak veya kilitlemek önemlidir. TCP/IP'de ise toplam 65535 adet port bulunmaktadır. İletişim portlar üzerinden döner TCP/IP'de.

Portun hangi katmanda çalıştığını bilirsek hangi cihazların portlar üzerinde etkili olabileceğini öğrenebiliriz. Portlar 4.katman yani Transport (ulaşım) katmanında çalışır. O zaman bir firewall servisi 4.katmanda çalışır diyebiliriz. 4.katmanda çalışan cihazlar sadece portu açıp kapatır. Başka bir işleme olanak vermez.

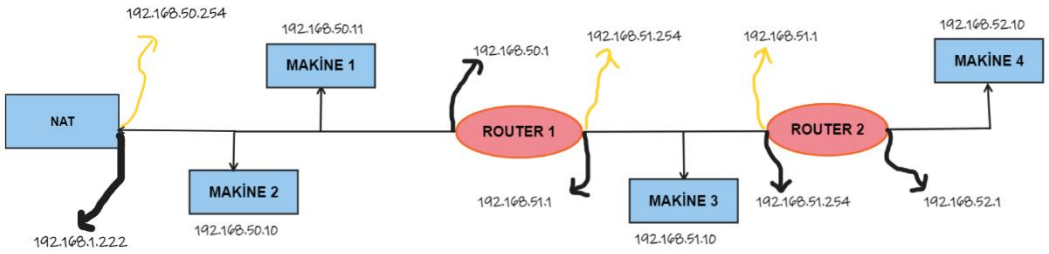
Her portun TCP ve UDP olmak üzere iki farklı yolu vardır. O yüzden port gelen pakete sorar TCP mi UDP mi diye.

TCP'de iletişimin sağlandığına dair bir güvence söz konusu iken UDP iletişimin sağlandığına dair bir güvence vermez. Ama paketlerin doğru iletişimle gitmesinden çok hıza önem veriliyorsa UDP tercih edilmelidir.

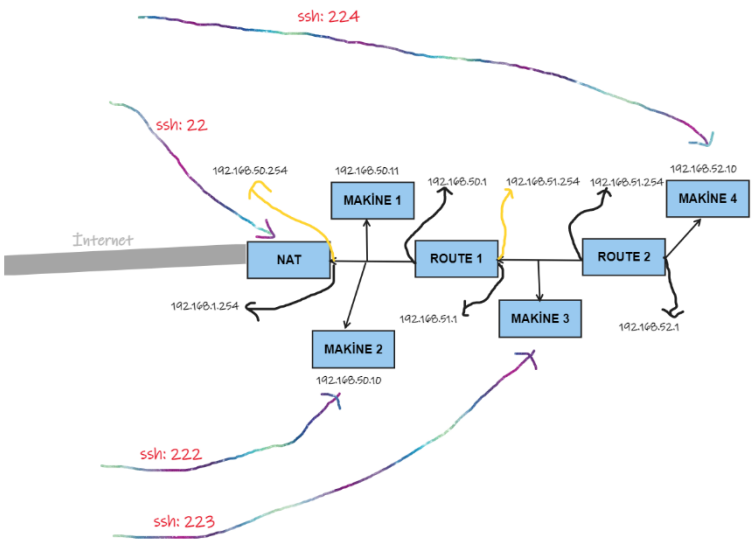
Artık güvenlik açısından portların açılıp kapatılması yeterli değildir. Çünkü port açıkken paket ayırt etmeksizin her paket gider. O yüzden zararlı bir paketinde gitme ihtimali oldukça yüksek. Buradan geçen bir paketi son katman yani 7.katman olan uygulama kısmında inceleyebiliriz. Çünkü buraya gelen paketlerin içeriği, türü, ne için kullanıldığı gibi tüm özellikleri bellidir ve bunlara bakarak ayırt etmeye çalışılır. Ancak bu katmanda hem iyiler hem kötüler birbirine girmiştir ve herkes lehine geliştirmeler yapmaya çalışır. İşte "Siber Güvenlik" denilen kavramda buradan ortaya çıkmıştır denilebilir.

PORT FORWARDİNG

Yani daha önce oluşturduğumuz isole networkleri bir NAT makineye bağlamıştık ve bu sayede internete erişim sağlanmıştı. Aşağıdaki şekilde görüldüğü gibi;



İçerden dışarı eriştik. Peki ya dışarıdan içeri nasıl erişeceğiz? İşte port forwarding burada devreye giriyor. Bunun için temelde iki farklı yol vardır. Ya NAT'a bağlı dış internete giden birden çok IP vardır. Bu IP'lere gerekli konfigürasyonlar yaparak istenilen makineye gidilir. Ya da iç makinelerin standart portu olan 22 yerine farklı portlar ekleyerek ilgili porta ait makineye erişilir. Burada erişmek için port bilinmeli. Ayrıca standart olarak 22 numaralı port olduğunu da unutmamak lazım ssh bağlantılarında. Eğer ikinci yolu izlersek şöyle bir şablon ortaya çıkabilir;



Basit düzey firewalllarda genelde out trafiğine yani içerden dışarı giden trafik açıkken dışardan içeri giden trafik her zaman kapalıdır. İleri düzeylerdeki iki tarafta kapalıdır. Kendiniz açmanız lazım. O yüzden bizimkisi basit düzey bir firewall olduğundan dışardan içeri trafiğini açmamız lazım. Bunun için şu komutu kullanabiliriz;

"**firewall-cmd --zone=external --add-forward-port=[hangi_portu_vereceksen_o_port]:proto=tcp:toport=[hangi_portu_vereceksen_o_port]:toaddr=[içerdeki_makine_IP]**"

Yukarıdaki komutta "firewall-cmd" kısmı firewall üzerinde işlem yapacağımızı, "--zone-=external" external zone üzerinden işlem yapılacağını, "--add-forward-port=[hangi_portu_vereceksen_o_port]" kısmı external zone tanımladığımız port forwardı, "toport=[hangi_portu_vereceksen_o_port]" kısmı paketi bu port üzerinden gönderi, "toaddr=" kısmı da içerdeki makine IP'sini ifade eder. Yani mesela paket [hangi_portu_vereceksen_o_port]'tan gelecek sende onu [hangi_portu_vereceksen_o_port] üzerinden içerdeki makineye gönder demek istiyoruz.

Komutu yazıp çalıştırdıktan sonra kontrol etmek için;

"**firewall-cmd --list-all --zone=external"** komutunu kullanarak yazdığınız portun eklendiğini görürsünüz. Eğer bu yazdığınız portu silmek isterseniz;

"**firewall-cmd --zone=external --remove-forward-port=[hangi_portu_vereceksen_o_port]:proto=tcp:toport=[hangi_portu_vereceksen_o_port]:toaddr=[içerdeki_makine_IP]**"

kullanabilirsiniz. Bu işlemleri yaptıktan sonra işimiz daha bitmedi çünkü bağlanmak istediğimiz içerdeki makinenin de portunu ayarlamamız lazım. Bunun için "/etc/ssh" dizininde "sshd.config" dosyasındaki port kısmını eklemek istediğiniz port numarasını girip kaydedip çıkmamız lazım. Ardından firewall kapatmamız lazım. Bunun için "systemctl stop firewalld" komutunu kullanmamız lazım. Ardından selinux disable hale gelmesi lazım. Bunun için de gerekli konfigürasyon dosyasında düzenleme yapılır. Artık tüm işlemler bittiğine göre uzaktan, içerdeki makineye erişmemiz lazım.

Eğer bu port işlemini kalıcı hale getirmek istiyorsak

"**firewall-cmd --zone=external --add-forward-port=[hangi_portu_vereceksen_o_port]:proto=tcp:toport=[hangi_portu_vereceksen_o_port]:toaddr=[içerdeki_makine_IP]**" komutuna **"--permanent**" parametresini girmek olur. Bu sayede kalıcı hale gelmiş olur.

PAT: Port Adress Translation, sunucu üzerine gelen mesela 222 numaralı portu hedef makineye gitmesi için 22 numaralı porta dönüştürmek ve makineye 22 numaralı porttan ulaşmak PAT işlemidir. Yani portu değiştirip başka bir portla bağlanıyoruz.

İşte ya port forwarding yaparak ya da PAT yaparak port işlemlerini ayarlayabiliriz. PAT içerde herhangi bir değişiklik yapmadan sadece dışardaki port üzerinde değişiklik yaparak bağlantı kurmayı sağlarken, port forwarding içeride de değişiklik yapmanızı gerektirir.

BROADCAST, MULTİCAST VE UNİCAST

Bir paketin bir swicthe bağlı makinelerin hepsine, eğer network ID'lere sahip iseler, gönderilmesi "broadcast"tir. Yani broadcast, bir swicthe bağlı makineden paket gönderildiği zaman switche gelen paket bağlı olduğu tüm makinelere dağıtır. Bu trafiği yavaşlatır ve o yüzden çok sevilmez. Ayrıca broadcast trafik rooterlardan geçmez.

Unicast ise bir paket eğer A makinesinden B makinesine gidecekse, başka makineye gitmiyorsa, sadece B'ye gidiyorsa bu unicasttir. Bu güvenlidir ve ağı kirletmez. Daha çokk tercih edilir.

Multicast ise paket gönderme işini belli bir gruba yapmaktır. Mesela IP TV yayınları buna örnektir. Çünkü sadece satın alanlar izleyebilir.

DHCP PROTOKOLÜ

Bir makinenin otomatik IP alabilmesi için geliştirilen protokoldür. Açılımı "**Dynamic Hosts Configuration Protokol**"dür. Amacı network iletişimi kurabilmeleri için gerekli parametreleri düzenlemektir.

KAYNAKÇA

Cem Bayraktaroğlu, 2020, Red Hat Hazırlık Kursu | Tam Paket, CB Academy Pro, https://www.udemy.com/course/red-hat-linux-hazrlk-kursu/learn/lecture