Linux Komutları

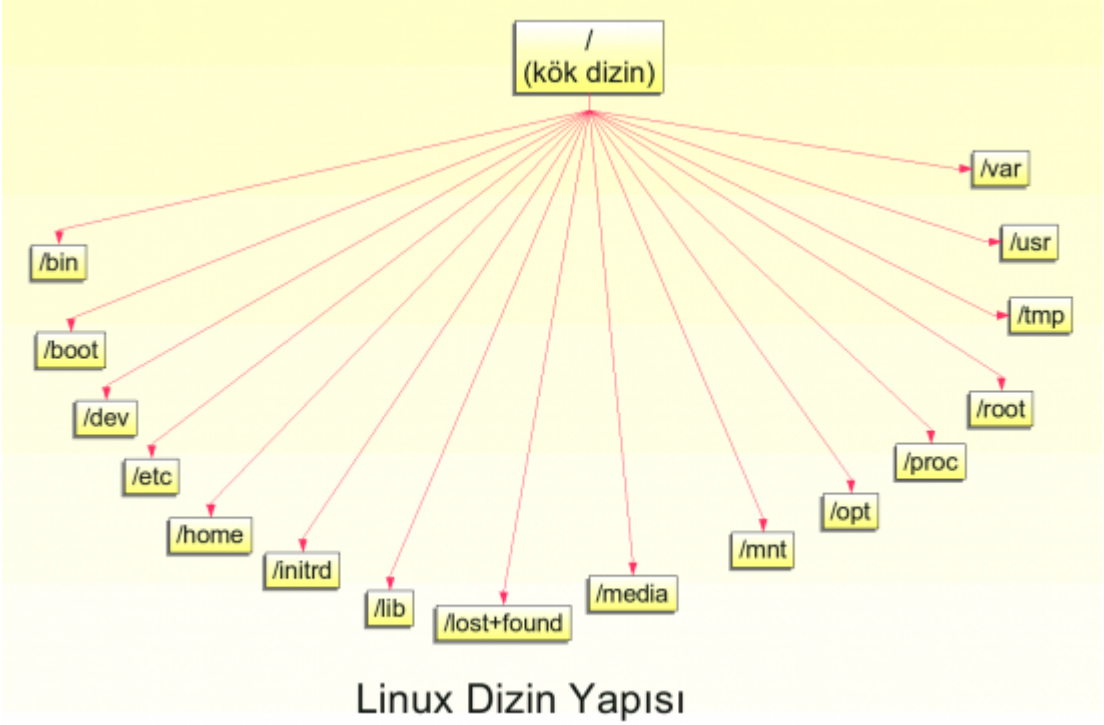
GökBörüTİM

Temel Linux Komutları

Ben profesyonel bir linux kullanıcısı değilim. Ancak linux taraftarı olduğumu söylemek mümkün. Kendimce tecrübelerimi ve arkasından komutları yazacağım. Mutlaka kişiden kişiye değişecektir yorumlar.

Linux; açık kaynaklı, herkesin geliştirebileceği, kaynak kodlarına herkesin erişebileceği ve genelde ücretsiz dağıtımları olan bir işletim sistemi. Windows'un son zamanlarda internetten satışa çıkarttığı linux versiyonu gibi istisnalar olabiliyor. Windows'a oranla daha basit donanımlarla daha hızlı çalışabilir. Windows gibi son kullanıcıya yönelik olmadığını söylemek mümkün. Terminal dediğimiz komut penceresi üzerinden işlemler yapılabilir. Linux'a geçildiğinde çoğu kişi ayak uyduramıyor ve Linux işletim sistemi o kadar da iyi değil diyor. Ancak aynı durum farklı işletim sistemine geçerken de oluyor. Dün Windows 7 kullanan insanlar Windows 10'a geçtiğinde alışamıyor, son Windows versiyonunun kötü olduğundan bahsediyor. Ancak birkaç ay sonra herkes Windows 10 kullanıyor. Bu anlamda Linux'a da şans vermek gerek sanki.
İşletim sistemini ne amaçla kullanacağımıza göre de tercihler değişiyor. Örneğin oyun oynarken veya tasarım yaparken verim almak istiyorsak Windows kullanmak yerinde olacaktır. Birçok oyun ve tasarım programları linux üzerinde çalışmıyor. Diğer yandan yazılım yazarken veya pentest işlemlerinde Linux'un çok daha iyi olduğuna inanıyorum. Çoğu linux dağıtımında pentest araçları mevcut. Ancak şöyle de bir yanılgı var: linux kurduğunuzda hacker olmuyorsunuz. Haberlerde kullanılan "Hackerların kullandığı en acayip manyak 5 işletim sistemi" gibi başlıklar vurucu olsa da o kadar realist değil.
Peki hangi dağıtımlar mevcut? En çok bilineni Kali Linux. Kali Linux, ikinci versiyonunu çıkarttı. Eskiden backtrack dağıtımı olarak bilinirken ona desteğini kesti ve daha sonra kali olarak devam etti. Pentest için oldukça iyi bir işletim sistemi. Terminal ve arayüz arasında bir denge olduğunu söylemek mümkün.
Benim sık kullandığım dağıtım ise ParrotSEC. ParrotSEC, Kali Linux'a oldukça benziyor. Ama ondan daha stabil ve arayüzünün daha hacker havasına büründüğünü söyleyebilirim. Kali

linux kurulumunda ilk aldığım hataları ParrotSEC kurarak aşmıştım. İçerisinde daha fazla araç bulunduruyor.
Arch ve Black Arch dağıtımları var. Onlar arayüzü büyük oranda grafiksel olmayan dağıtımlar. İşlerin çoğunu terminalden halletmek gerekiyor. Arayüz çok zayıf. Ancak bununla beraber donanımın gücü yapılan işlemlere kalıyor. Arayüze bir “harcama” yapmak gerekmiyor.
Ubuntu dağıtımı en popüler dağıtımlardan birisi. Daha ziyade son kullanıcıya yönelik. Arayüzü zengin. Windows’tan yeni geçecek olanlara genelde Ubuntu önerilir. Ancak siber güvenlik araçları kurulu bir şekilde gelmez. Kendiniz kurarsınız. Aynı zamanda bir mağazaya sahip.
Yavaştan dizin yapısına geçelim. Yüzeysel bahsedeceğim şimdilik.



Linux Dizin Yapısı

/bin: Temel linux komutları burada yer alır. Bunlar tüm kullanıcıların kullanabileceği komutlardır.
/sbin1: Sadece root yetkisine sahip kullanıcının kullanabileceği komutlar burada yer alır.
/boot: Sistemin boot edilmesi için gerekli değişmez veriler. Yani sistemin açılmasına yardımcı olan dosyalar burada yer alır.
/dev: Cihazların bulunduğu dosyalar.
/etc: Local sistemimiz için gerekli sistem dosyaları.
/home: Kullanıcı dizinleri.
/lib: Programların ihtiyacı olan yazılım kütüphanelerine ait dosyalar burada yer alır.
/mnt: Geçici bağlantı noktası.
/proc: Dosya sisteminin Process (işlem) bilgileri.
/root: ‘root’ kullanıcısına ait kişisel dizin. Diğeri kullanıcılar buraya erişemez.
/tmp: Geçici saklama alanı. Herkese açıktır. (Hacklenmeye çalışılan sistemlerde buraya shell atılıp çalıştırılabilir mi sanki(?))
/usr: İkincil ana hiyerarşi (Uygulama programlarını içerir.)
/var: Değişken veri bölgesi.

Komutlara geçmeden önce ufak bir şeye daha dokunmamız gerek. Linux'ta yer alan "root" kullanıcısı, Windows'ta yer alan Administrator'e denk gelir. İkisi de sistemde tam erişime sahiptir. Ancak siz, linux sistemindeki tek kullanıcı dahi olsanız, root kullanıcı olmayabilirsiniz. Eğer bu tip bir işlem yapmanız gerekirse root terminalini (genelde kırmızı renkte sembolü vardır) açmanız gerek. Veya yazacağınız komutun başına "sudo" yazarsanız root yetkisi istemiş olursunuz. Kullandığınız dağıtıma göre komut değişmektedir. İnternette arayıp temin edebilirsiniz. Daha sonra linux sizden root parolasını girmenizi ister. Daha sonrasında komutu çalıştırabilirsiniz.

Son bir iki mesele daha…. Eğer linuxta bir komutun ne işe yaradığını veya nasıl kullanılacağını bilmiyorsanız komutun yanına -h, -help veya –help yazmanız yeterli. Linux terminalin en pratik özelliklerinden birisi de bu. Diğer yandan bir araç çalıştırdınız fakat durdurmak veya çıkmak istiyorsunuz. Büyük oranda CTRL+C kısayolu işinize yarayacaktır. Geçelim bu vırvırları ve esas meselemize gelelim.

ls: Bulunduğunuz dizindeki dosyaları listeler.

ls -a: Gizli dosyaları da gösterir. İsmi "./" ile başlayanlar örneğin.

ls -l: Dosyaların izin durumları, boyutu, tarihi vs. gibi bilgileri de beraberinde vererek listeler.

cd gokboru: gokboru ismindeki dizine geçiş yapmanızı sağlar. Bulunduğunuz dizinde böyle bir dizin varsa tabii. Veya, cd /Desktop/gokboru gibi birden fazla dizin belirterek de geçiş yapabilirsiniz.

cd ~: Home dizinine geçiş yapmanızı sağlar. cd komutu, "Change Directory"den gelir.

cd -: Bir önceki dizine döner.

cd ..: Üst dizine gider. Örneğin Desktop/gokboru dizinindesiniz. Bu komutu kullandığınızda /Desktop dizinine dönüş yaparsınız.

cp kaynak hedef: Kaynaktan hedefe dosya kopyalar. "Copy"den gelir.

cp -R kaynak hedef: Recursive kopyalar.

mv kaynak hedef: Dosyaları taşımak veya adlarını değiştirmek için kullanılır.

mkdir cumhuriyet: "cumhuriyet" isminde dizin oluşturmanızı sağlar. "Make Directory"den gelir.

rm kapitulasyon: Bulunduğunuz dizindeki "kapitulasyon" isimli dosyayı siler. "Remove Directory"den gelir.

rmdir yobaz: Bulunduğunuz dizindeki, içi boş olan "yobaz" dizinini siler.

rm -r halifelik: halifelik dizinini içindeki dosyalarla beraber siler.

rm -rf /mandavehimaye: "mandavehimaye" dizini içindeki tüm dizinleri ve dosyaları tekrar sormaksızın siler.

rm -rf / : Kök dizini tamamen siler. Kullanmadan önce tekrar düşünmek ister misiniz?

touch nutuk.txt: "nutuk.txt" isminde bir dosya yoksa yaratır, varsa tarihini değiştirir.

cat andimiz.txt: Terminal üzerinde, "andimiz.txt" isimli dosyayı gösterir.

grep Türk'üm andimiz.txt: "Türk'üm" yazısını "andimiz.txt" dosyasında arar. Bulunduğu satırı görüntüler.

less dosya adi: Dosyada ilerlemek için kullanılır. (Q ile çıkış yapar.)

pwd: Bulunulan dizinin ismini gösterir.
who: Makineye bağlı kullanıcıları görüntüler.
whoami: Sizin hangi kullanıcı olduğunuzu görüntüler.
uptime: Bilgisayar açıldığından beri geçen süreyi gösterir.
ifconfig: Windows'taki "ipconfig" ile aynı işi yapar. Yerel IP adresi, MAC adresi, etkin arabirim gibi bilgileri listeler.
ifconfig -a: Temel komutun yanı sıra etkin olmayan arabirimleri de sıralar.
ifconfig eth0: eth0 arabirimi ile ilgili olan bilgileri getirir.
ifconfig eth0 up/down: eth0 arabirimini aktif eder/durdurur.
ifconfig eth0 hw ether AA:BB:CC:DD:EE:FF: eth0 arabiriminin MAC adresini değiştirir.
ifconfig eth0 192.168.1.10: eth0 arabirimine IP adresi atar.
man komut ismi: komutismi yerine yazdığımız komutun detaylı biçimde nasıl kullanıldığını ve ne işe yaradığını gösterir.
useradd kobay: "kobay" isminde bir kullanıcı oluşturur.
history: Terminalde kullandığınız son komutları görüntülemenizi sağlar.
reboot: Sistemi yeniden başlatır.
shutdown -h now: Sistemi kapatır.
shutdown -h 23:59 : Sistemi, saat 23.59'da kapatır.
sudo shutdown +15: Sistemi 15 dakika sonra kapatır.
sudo shutdown -c: Kapatmaktan vazgeçerseniz bu komutu kullanabilirsiniz.
echo "Ayakta mı duramıyom?": Terminale, "Ayakta mı duramıyom? yazar.
clear: Terminali temizler.
ps: Çalışan işlemleri gösterir.
kill PID: Komuta girdiğiniz işlemi durdurur.
tar -cvf txt_dosyalar.tar *txt : Sonu txt ile biten tüm dosyaları sıkıştırır. Tamamını txt_dosyalar.tar adlı dosyada birleştirir.
tar -tf txt_dosyalar.tar: txt_dosyalar.tar dosyasının içindekileri listeler.
tar -xvf txt_dosyalar.tar: Dosyanın içeriğini çalışma alanına döker.
wget -r http://siteadi.com/wget/ : Söz konusu adreste gösterdiğiniz dizini bilgisayara indirir.
wget -c $http://siteadi.com/wget/parrotsec.iso : Belirttiğiniz iso dosyasını indirir. İndirme aniden kesilse dahi -c komutu ile indirmeye devam edebilirsiniz.
git clone URL: URL yerine girdiğiniz github adresindeki dosyaları indirir.
sudo apt-get install paket_adı: paket_adı isimli dosyanın kurulmasını sağlar.
sudo apt-get remove paket_adı: paket_adı isimli dosyanın kaldırılmasını sağlar.
sudo apt-get update: Paket listelerini günceller.
chmod komutu, dosya izinleri ile ilgilidir. Bunun için birkaç temel şeyi bilmek gerekir. Dosya izinleri üçe bölünür:

- **r**: read(okuma)

- **w**: write(yazma)
- **x**: execute(çalıştırma)

Bu izinler sıralı olarak gösterilir. “**rwx**” şeklinde. Dosya özelliklerinde hangi harf varsa o kişi, o yetkilere sahiptir. Bunun dışında bir ve sıfırlarla da gösterilebilir. Örneğin “110” yazıyorsa, okuma ve yazma izni var, çalıştırma izni yok demektir.
Devam edelim. Kullanıcılar da üçe bölünüyor:

- **u** – user (dosyanın sahibi)
- **g** – group (dosya veya dizinin ait olduğu grup)
- **o** – other (diğerleri, user ve group haricindekiler)
- **a** – all (ugo- user,group, other) (hepsi, herkes dosya ve dizinlere erişebilir.)

Şimdi hepsini bir arada inceleyeceğimiz bir örnek yazalım. Listeli şekilde giden bu izin harflerini üçer üçer böleceğiz. Diyelim ki dosta izni kısmında “drwxr-xr–” yazıyor. Bu durumda, söz konusu dizine userın okuma, yazma, çalıştırma izni var demektir. Dizinin ait olduğu grubun okuma ve çalıştırma izni var, yazma izni yok demektir. Diğer kullanıcıların ise okuma izni var, yazma ve çalıştırma izni yok demektir.
Peki buraya kadar tamam. İzinleri nasıl değiştireceğiz?

- **chmod +r dosya**: Dosyaya okuma izni verir.
- **chmod 666 dosya**: Tüm kullanıcılara okuma ve yazma yetkisi verilir.
- chmod a+rwx ve chmod 777 dosya: Dosyaya tüm kullanıcılar tarafından tam yetki verilir.
- chmod go-rw dosya: Grup ve diğer kullanıcılar üzerindeki okuma ve yazma yetkisini kaldırır.

Varyasyonları arttırmaya devam edebiliriz.
Arada bir detay var fark ettiniz mi? chmod sonrasında “rwx” yerine sayılar kullandım. Peki bunlar nasıl çalışıyor? Her yetkinin bir değeri var. Toplandığında bize yetki dağılımını veriyor.

- **Read: 4**
- **Write: 2**
- **Execute: 1**

Toplamları bize kullanıcının yetkisini verecek. Örneğin:
chmod 765 : Birinci kullanıcıya düşen sayı 7, ikinciye düşen 6, üçüncüye düşen 5. Bu durumda birinci kullanıcı “**rwx**” yetkilerine sahip. İkinci kullanıcı “**rw**-“, üçüncü kullanıcı ise “-**wx**”.