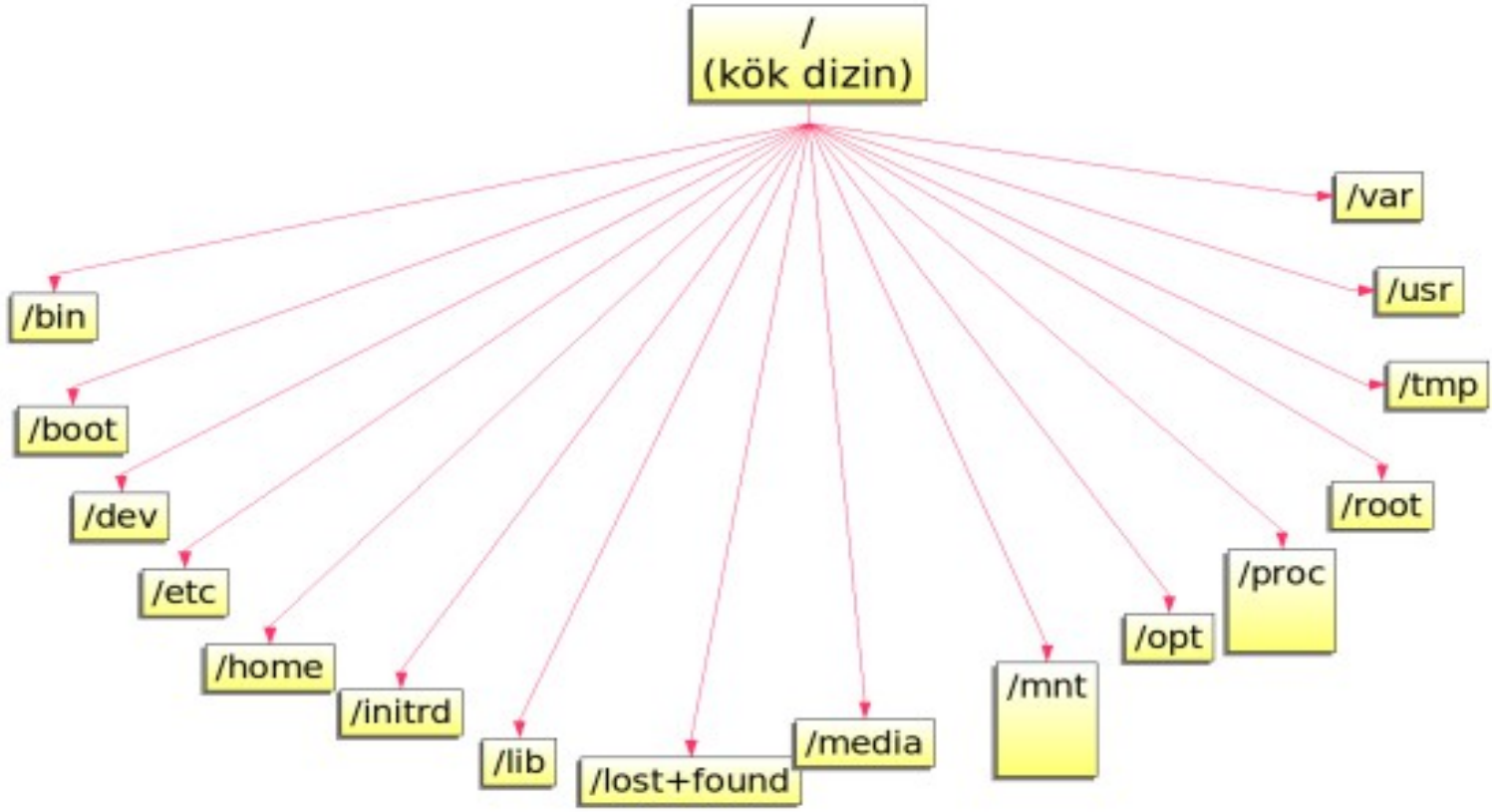
30 günde Cyber Security-1 öğren
3&4. GÜN

Linux Dizin ve Dosya Yapısı
Komut Satırı (Kabuk)
Temel Komutlar
Örnek Uygulamalar
GNU/Linux İşletim Sistemi Giriş

Linux Dizin ve Dosya Yapısı



Linux Dizin Yapısı

Linux Dizin ve Dosya Yapısı

- Linux’ta dosya ve dizin yapısı alışılmış işletim sistemlerinden oldukça farklıdır.
- Linux bir Unix türevi olduğu için Tekil Hiyerarşik klasör yapısını benimsemiştir.

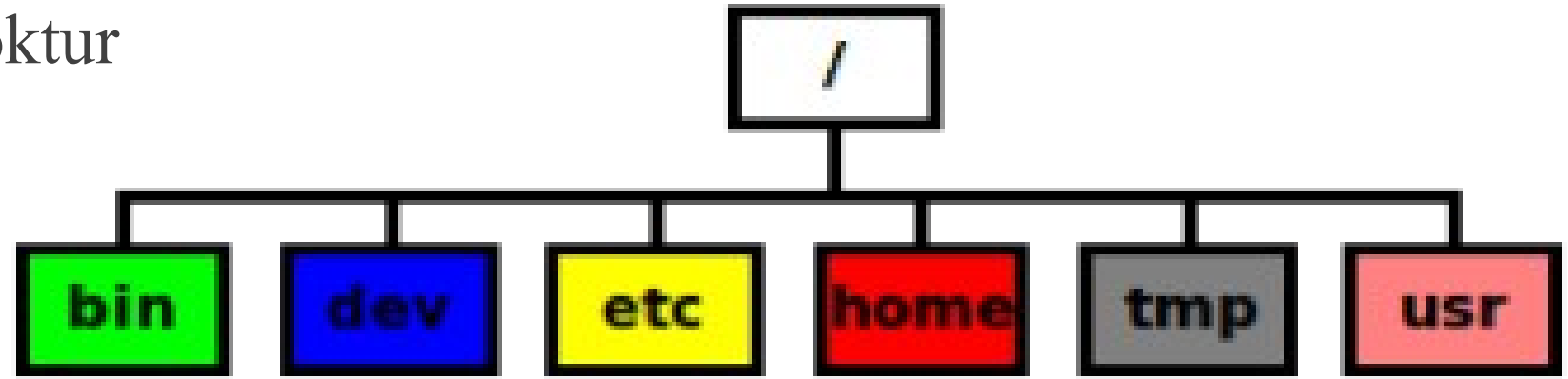
Linux Dizin ve Dosya Yapısı

- Linux dosya yapısında her şey bir dosyadır. Donanım (ram, ekran kartı ,işlemci vs.) veya bilgisayarımıza taktığımız bir harici bellek dahil dosya olarak tutulur.

Linux Temel Yapısı

Linux Dizin ve Dosya Yapısı

- En üst dizin Kök(/) dizinidir ve diğer tüm dizin ve dosyalar bu dizinin altındadır.
- Her şey " / " simgesiyle ifade edilen kök dizinden başlayarak dallanıp budaklanır
- Linux işletim sisteminde ROOT kullanıcısının yapamayacağı hiç bir şey yoktur

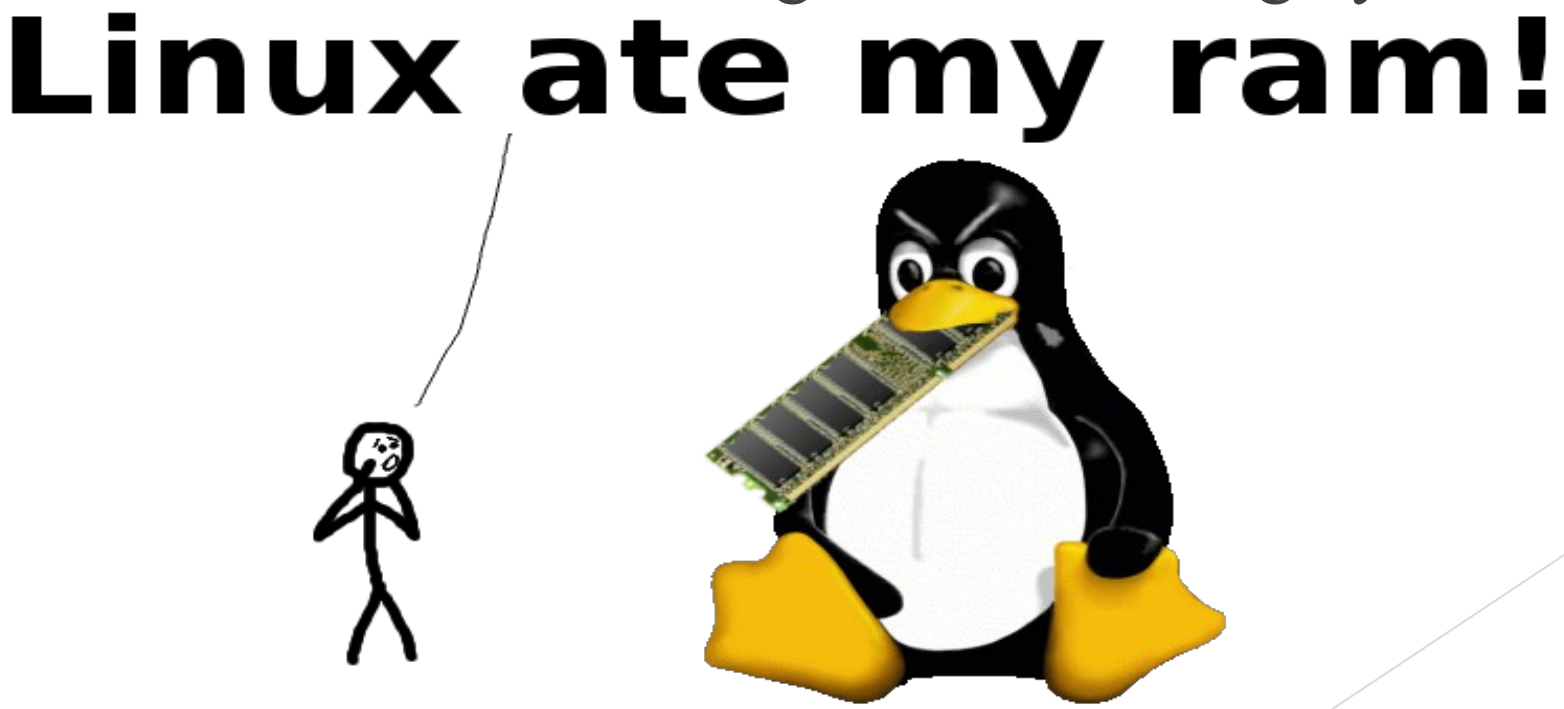


Linux Dizin ve Dosya Yapısı

- /bin: Home kullanıcısının kullanabileceği komutları içerisinde barındırır.
- /sbin: Root kullanıcısının kullanabileceği komutları içerisinde tutar.
- /boot: Sistemin booting edilebilmesi için gereken dosyaların bulunduğu dizindir.

Linux Dizin ve Dosya Yapısı

- /dev: Oluşturulan disk bölümlerinin, aygıtların bulunduğu dizindir.
- /etc: Sisteme ait yapılandırma dosyalarının tutulduğu dizindir.
- /home: Sistemdeki kullanıcı bilgilerinin tutulduğu yerdir



Linux Dizin ve Dosya Yapısı

- /tmp: Geçici dosyaların tutulduğu alandır. Bazı programlar geçici depolama alanı olarak kullanır.
- /usr/share: Diğer kullanıcılarla paylaşılan her şey bu dizinin altında yer alır.
- /media: Kaldırılabilir cihazların bulunduğu yerdir.
- /last+found: Sistem doğal yollarla sağlıklı bir şekilde kapanmadığında bulamadığı dosya var ise

genellikle bu dizinin altında yer alır.

Linux Dizin ve Dosya Yapısı

- /var: Sistem logları bu dizinin altında yer alır.
- /lib: Gerekli kütüphane dosyalarının bulunduğu yerdir.
- /opt: İşletim sistemine bağımlılığı olmayan bir uygulama program yüklediğimizde bu dizinin

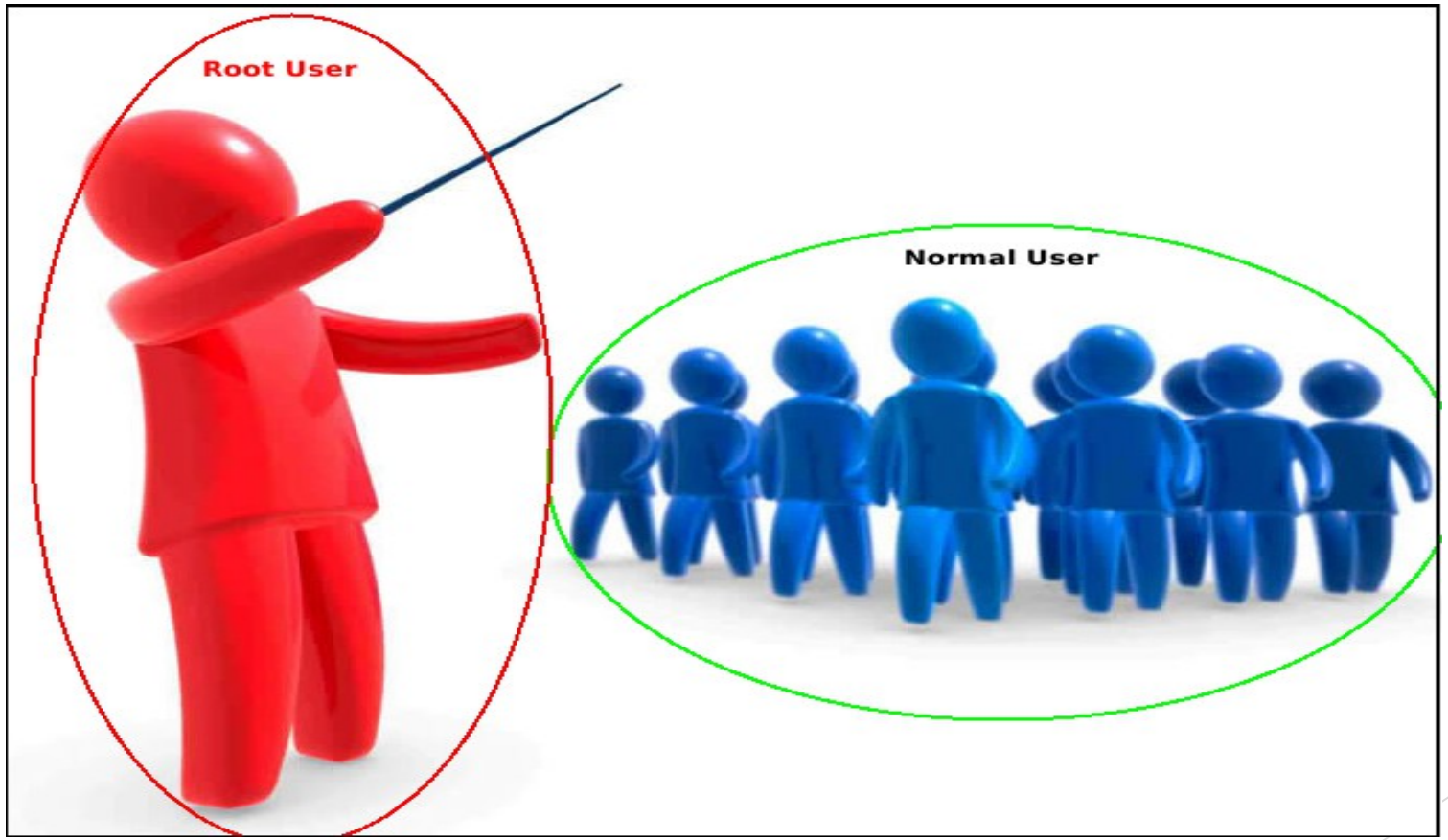
altında yer alır.

- /initrd: İnitial ram disk kısaltmasıdır. Linux'ün yüklenip açılması için gereken bilgilerin

bulunduğu dizindir.

Linux Dizin ve Dosya Yapısı

- /root: Root kullanıcısının ev dizinidir



Linux Dizin ve Dosya Yapısı

- /bin : İşletim sisteminizi kullanmak için gereken birçok komut /bin klasörü altındadır.

-cat, mkdir, cp, ls, mv, rm vb. temel komutların hepsi buradadır.

- Sistem boot ettiğinde, ilk olarak /bin klasörü çalışır hâle getirilir.

-Sistemde ne kadar ciddi bir sorun olursa olsun /bin klasöründeki komutlar çalışmaya devam eder.

-Sisteminizde bir sorun meydana geldiğinde /bin klasörü altındaki komutları kullanarak sistemi onarabiliriz.

Linux Dizin ve Dosya Yapısı

/boot: Boot, işletim sisteminin yüklenme evresidir.

- /boot klasörü, boot işlemi için gerekli olan tümvdosyaları içerir

(çekirdek görüntüsü, sistem haritası, önyükleyici yapılandırması gibi).

- Bilgisayarın başlangıç (boot) aşamasında gerekmeyen ayar ve yapılandırma dosyaları burada bulunmaz;

Başka klasörlerden gerektiği zamanlarda yüklenir.

Linux Dizin ve Dosya Yapısı

/dev : Linux'ta her şey bir dosyadır; donanım aygıtları da öyle.

- USB girişleri, seri ve paralel portlar, diskleriniz, CD-ROM'larınız vb... Bütün aygıtlar /dev klasörü altında tutulan dosyalardan ibarettir.
- Örneğin /dev altında bulunan hda1 dosyası, sabit diskinizi temsil eder. Ya da /dev/dsp, ses aygıtınızdır. Bunları programlar vasıtasıyla kullanırız; ancak bu dosyalar üzerinden doğrudan müdahale etmek de mümkündür.
- Mesela "cat /boot/vmlinuz > /dev/dsp" yazarak Çekirdeğin sesini

duyabilirsiniz.

Linux Dizin ve Dosya Yapısı

/dev bazı önemli aygıt dosyaları:

- /dev/psaux : Mause, klavye girişidir. (PS/2 girişi)
- /dev/lp0 : Yazıcı tarayıcı gilbi cihazlar için kulanılan paralel porttur. (LPT1)
- /dev/usb : Usb portu
- /dev/sda : Flash bellek, harici disk, cd rom vs.. Cihazların tutulduğu yerdir.
- /dev/scd : CD rom'lar barındırır.

Linux Dizin ve Dosya Yapısı

- **/etc**: Sisteme ait yapılandırma dosyalarının bulunduğu dizindir.
  - /etc/passwd : Kullanıcı hakkında bilgilerin tutulduğu dizindir.
  - /etc/shadow : Kullanıcı parolalarının şifrelenmiş hali bu klasörün altında tutulur.
  - /etc/group : Kullanıcı gruplarıyla ilgili bilgiler bu klasörde yer alır.
  - /etc/resolv.conf : DNS kayıtları bu dosyanın altında bulunur.

Linux Dizin ve Dosya Yapısı

/home: home klasörü kullanıcıların kalesi olarak tabir edilir.

- home klasörü içerisinde her kullanıcının kendi adında bir alt klasörü bulunur. (örneğin /home/ahmet , /home/ayşe gibi).

- Kullanıcıların kişisel verileri, kullandığı programlarda yaptığı ayar değişiklikleri, yapılandırmaları tutulmaktadır.

- Kullanıcının çeşitli programlarda yaptığı ayarları barındıran dosyalar gizli dosya oldukları için görüntülenebilmeleri için gizli dosyaların görünür hale getirilmesi gereklidir.

Linux Dizin ve Dosya Yapısı

/**home :** dizini Windows'taki kullanıcı dizinlerine göre çok daha güvenli bir yapıya sahiptir.

- Çünkü Linux'ta bir başkasının ev klasörüne müdahale edemezken, Windows'ta çok zorlanmadan istediğinizi yapabilirsiniz.

- /home dizini, aynı zamanda kullanıcı ayar dosyalarını barındırıyor olması nedeniyle bu dizinini, Windows'taki **Documents and Settings** ya da **Application** klasörlerine benzetebiliriz.

Linux Dizin ve Dosya Yapısı

/initrd : initrd, "initial ramdisk" kısaltmasıdır. Anlamı, yaklaşık olarak "Başlangıç Bellek Diski" şeklinde ifade edilebilir.

- Boot aşamasında ilk önce çekirdek (kernel) yüklenir. Bundan sonra bilgisayarınızın belleğinde bir Bellek Diski oluşturulur. Oluşturulan Bellek Disk üzerinde / (root) yansısı açılır ve kök dizin olarak monte edilir.

- /initrd bu işlemlerin yapılması ve Linux'un yüklenmesi için gereklidir.

Linux Dizin ve Dosya Yapısı

/lib : Çekirdek modülleri ve paylaşılan kütüphane dosyaları bu klasörde bulunur.

- Var olan çekirdek modüllerini /lib/modules/[versiyon_numarasi] içerisinde bulabilirsiniz.

- Bahsedilen kütüphane dosyalarıysa, sistemi başlatmak ve /bin ile /sbin içerisindeki komutları çalıştırmak için gereklidir.

- Paylaşılan kütüphane dosyalarını, Windows'ta DLL ile eş tutabiliriz. Linux'ta kütüphane dosyalarının sonu ".so" ile biter.

Linux Dizin ve Dosya Yapısı

/lost+found İngilizce bir terim olan “Lost and Found” kayıp eşya bürosu demektir. /lost+found klasörü de tam olarak bu işlevi görmektedir.

- Bazen sisteminizde herhangi bir problem olur; örneğin bilgisayarı resetlerseniz, elektrik gider sonrasında bilgisayarı yeniden başlatırsınız. Bu gibi durumlarda Linux'ta fsck (File System Check) komutu devreye sokulur.

Linux Dizin ve Dosya Yapısı

lost+found : Kısaca özetlersek; kötü bir sistem kapanmasından sonra, olması gereken bazı dosyaları bulamıyorsanız, kayıp eşya bürosuna bakmanızda yarar var.

- Ancak bu klasöre girmek istediğinizde erişimi engelleyen bir ileti ile karşılaşırsınız, bu klasörün içeriğine ulaşabilmek için dosya yöneticisini tam yetki ile açmanız gereklidir.

- Bunun için sudo -H nautilus komutunu kullanmalısınız.

Linux Dizin ve Dosya Yapısı

/media:

- CD-ROM, disket sürücü, flash bellek gibi çıkarılabilir aygıtlar buraya bağlanır.
- En basit tanımla, çıkarılabilir aygıtların, bağlantı noktası (mount point) olarak düşünebilirsiniz.

Linux Dizin ve Dosya Yapısı

/mnt : /media klasörünün aksine çıkarılabilir aygıtlar yerine, sistem açılışında otomatik olarak bağlanan sabit disk bölümleri ve donanım aygıtlarının bağlanması içindir.

- Bağlama (mount) işlemi, herhangi bir depolama ortamını, işletim sisteminin kullanmasını sağlar.

- Nereye bağladığınız sizin tercihinizdir, değiştirmeniz mümkündür. Yani bir diski, /media veya /mnt klasörüne ya da bir başka yere bağlamanız fark etmeyecektir.

- /media ve /mnt genel kabul görmüş bağlantı noktalarıdır.

Linux Dizin ve Dosya Yapısı

/opt : İşletim sisteminden bağımsız, sistem için zorunlu olmayan 3. parti kullanıcı programları bu dizinde bulunur.

- Örneğin; google earth programını indirip kurmak istediğinizde, 'default' olarak kurulacağı nokta, /opt/google-earth adresidir.

- Elbette üçüncü parti bir programı kurarken bu kurulum konumunu değiştirebilir, size uygun gelen bir başka konuma yükleyebilirsiniz.

- Ancak daha önce de bahsettiğimiz gibi bazı şeyler genel kabule dayanır.

Linux Dizin ve Dosya Yapısı

/proc :Süreçler, sistem belleği, bağlı aygıtlar, donanım yapılandırmalarıyla ilgili bilgileri içeren özel bir “sanal” dosya sistemidir.

- Bildiğimiz anlamda fiziksel dosyalar bulundurmaz; sistem durumuna dair

bilgi içeren sanal dosyaları vardır. Bir bilgi alma merkezi olarak görülebilir, birçok uygulama buradaki bilgilerden yararlanmaktadır.

- Örneğin "cat /proc/swaps" yazarak sisteminizdeki takas dosyalarına dair bilgi alabilir ya da "cat /proc/cpuinfo" komutuyla işlemcinizin özelliklerini görebilirsiniz.

Linux Dizin ve Dosya Yapısı

/root : Linux/Unix sistemlerde, işletim sistemine her türlü müdahalede bulunabilme yetkisine sahip, "root" adıyla tanımlanmış, süper yetkili özel bir kullanıcı hesabı vardır.

- /root dizini, bu özel kullanıcı hesabının ev dizinidir. Root kullanıcısına "kök kullanıcı" da denilir.

- Kullanıcıların, sistemi root hesabıyla açma ihtiyacı bulunmaması nedeniyle ve ayrıca sistemi root olarak açmanın güvenlik zaafiyetine yol açabilecek olması nedeniyle pek çok Linux dağıtımında root hesabıyla sisteme giriş yapılması, öntanımlı olarak engellemiştir.

Linux Dizin ve Dosya Yapısı

/root:

- Linux dağıtımlarında, yetki gerektiren bir işlemin yapılabilmesi için sistem root olarak açılmaz, bunun yerine geçici olarak root hakları elde edilir.

- Bunun için, kullanmakta olduğunuz Linux dağıtımına bağlı olarak su,

su - , su root ya da sudo komutlarından biri girilir ve ardından root kullanıcısının (ya da yönetici hesabın) parolası girilir.

Linux Dizin ve Dosya Yapısı

/sbin : Linux'ta normal kullanıcının kullanabileceği komutlarla, kök kullanıcının (root) kullanabileceği komutlar ayrılmıştır.

- root tarafından kullanılacak bakım ve yönetim için kullanılan önemli programlar, /sbin altında tutulur.

- Daha az öneme sahip yönetim komutlarıysa, /usr/sbin klasöründedir.

- Eğer yerelde, yani kullandığınız makineye özgü kök kullanıcı (root) komutları bulunuyorsa, bunları da /usr/local/sbin altında bulabilirsiniz.

Linux Dizin ve Dosya Yapısı

/usr:

- daha geniş bir tanımla; tüm kullanıcılarca paylaşılan verileri (programlar, komutlar, kütüphaneler, dokümanlar gibi) içeren dizindir.
- /usr ile ilgili söylenebilecek bir başka nokta da "local" klasörüdür.

Linux Dizin ve Dosya Yapısı

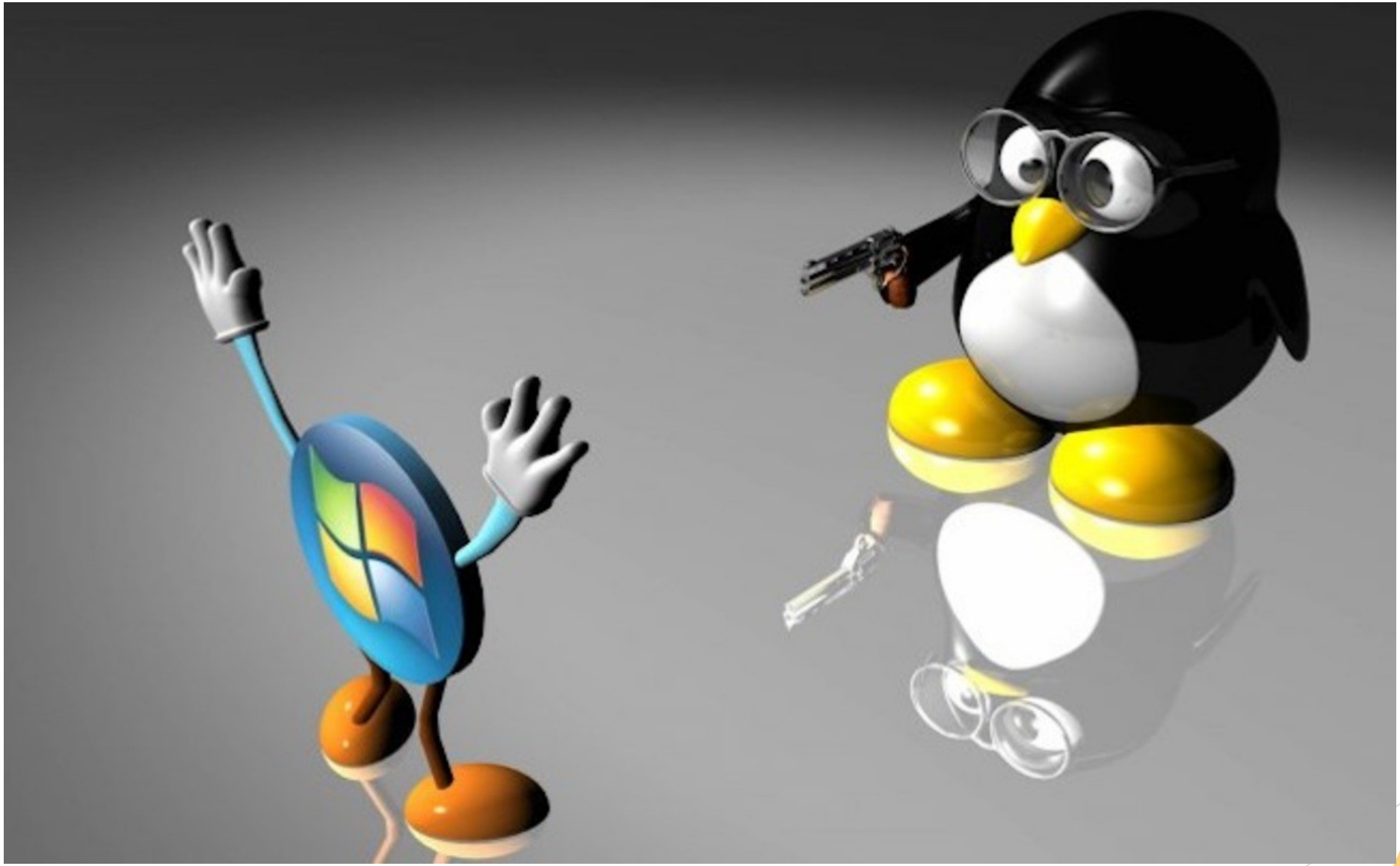
/var :

- Log dosyaları, e-posta ve yazıcı kuyrukları gibi değişken sistem bilgilerini barındırır.
- Sisteminize dair tutulan log'ları buradan görebilir; güvenlik durumunu buradan kontrol edebilirsiniz.

Linux Dizin ve Dosya Yapısı

/tmp :

- Geçici dosyalar içindir. Birçok program, burayı geçici depolama alanı olarak kullanır.
- /tmp klasörünün içeriği genellikle KB'lar mertebesinde kalır ve genellikle işletim sistemi yeniden başlarken içindeki dosyalar silinir.



GNU/Linux Temel Komutlar

ve

Komut Satırı

Shell - (Kabuk)

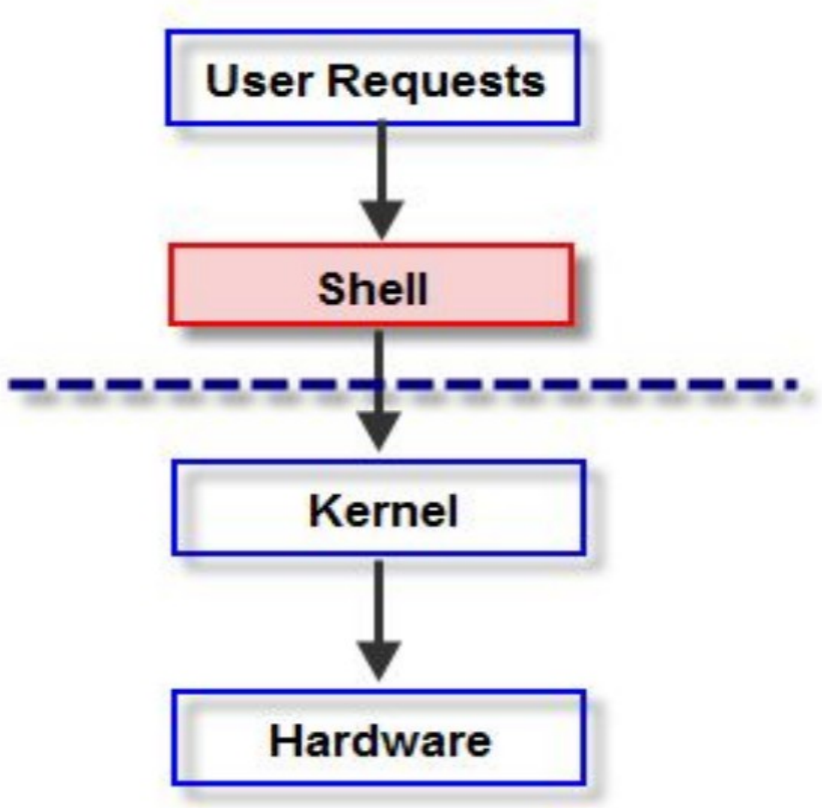
- SHELL(kabuk), KERNEL(çekirdek) ile komut satırı arasında köprü oluşturur.
- Komut satırından verdiğimiz komutları /sbin ve /bin dizinleri altında arar yorumlar ve

çekirdeğe iletir.

- Girilen komutları bilgisayara, sonuçları kullanıcıya iletir.

Shell - (Kabuk)

- Birden fazla kullanabileceğimiz SHELL (kabuk) vardır.
- echo $SHELL

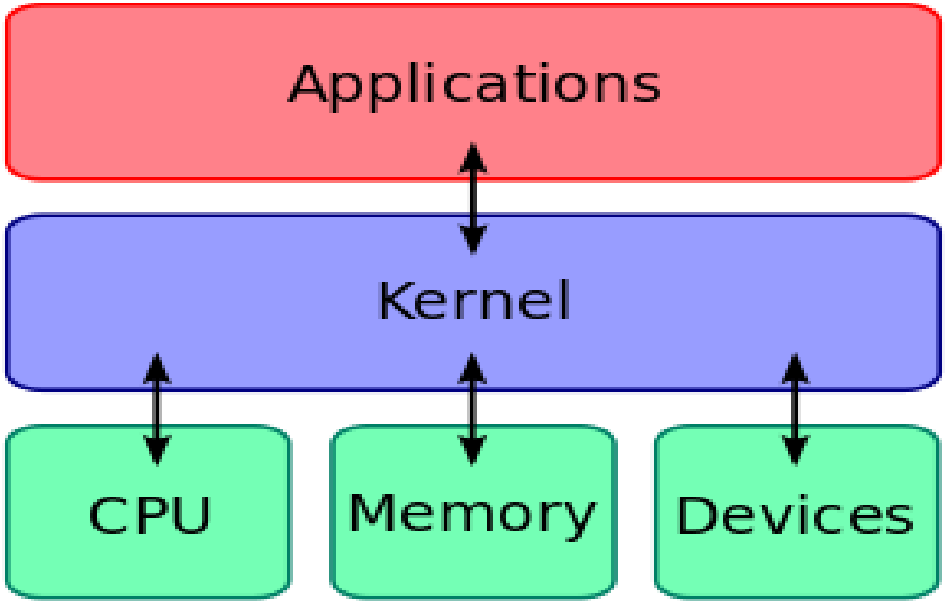


Kernel - (Çekirdek)

- Donanım ile yazılımın haberleşmesini sağlar.
- Sistemin düzgün çalışmasını sağlar.
- Sistem belleğini çalışan süreçleri ve hafızayı sürekli olarak kontrol eder.

Kernel - (Çekirdek)

- Kullanıcıların görevlerinin sırasıyla yapılmasını sağlar.
- Kabuktan aldığı komutları çalıştırır



Linux Temel Komutlar ve Komut Satırı

ctrl + shift + t → yeni terminal sekmesi açar

ctrl + shift + w → yeni terminal sekmesini kapatır

ctrl + shift + c → terminal üzerinde kopyalama işlemi yapar

ctrl + shift + v → terminal üzerinde yapıştırma işlemi yapar

ctrl + a → imceli satır başına getirir

Linux Temel Komutlar ve Komut Satırı

KOMUT OPSİYON PARAMETRE

~ → /home/username demektir

/ → root yani kök olarak bilinir. Sistemin en üst seviyesidir. İçide home dizini olmak üzere sistem

dizinleri ve dosyaları bulunur.

Linux Temel Komutlar ve Komut Satırı

su →super user yani root olarak sisteme erişmemizi sağlar burada

giriş yapmak için root parolanızı girmeniz gerekir

sudo su → root olarak sisteme erişmemizi sağlar. Burada kullanıcı parolanızı girmeniz gerekir

cd gidilmekistenenyol→ cd komutundan sonra gidilmek istenen yol

girilirise o yola girer

Linux Temel Komutlar ve Komut Satırı

- Dosya ve dizinler arasında gezmek için **cd (change directory)** komutunu kullanılır.
- Sadece **cd** komutunu kullanırsak gittiğimiz adresten önce olduğumuz yere götürür.
- **cd ..** Şeklinde yazarsak bir üst dizine gideriz. 2 dizin geriye gitmek istiyorsak **cd ../../** şeklinde

yazarız.

- **cd** komutuna parametre olarak dizin adı yazarsak bizi oraya götürür.

Linux Temel Komutlar ve Komut Satırı

- Ancak yazacağımız adres **relative path** (değişken yol) veya **absolute path (kesin yol)**

olabilir buna biz karar vereceğiz.

- Gideceğimiz adresi olduğumuz yeri önemsemeden kök **(/)** üzerinden başlayarak yazarsak

absolute path olur.

- Bulunduğumuz dizinden itibaren tek tek adres yazarsak **relative path** olur

Linux Temel Komutlar ve Komut Satırı

- Bir komutun parametresi varsa komuttan hemen sonra komut -’’parametre’’ şeklinde yazılır.
- **man** ‘’komut’’ veya ‘’komut’’ --help komut ve parametreleri hakkında bilgi verir.
- **ls** komutu o an bulunduğumuz dizinin altındaki dosya ve dizinlerin listeler.

Linux Temel Komutlar ve Komut Satırı

- **ls -l** : Ayrıntılı listeler.

- **ls -R**: Bulunduğumuz dizinleri ve alt dizinleri listeler.

- **ls -h**: İnsanın okuyabileceği şekilde listeler.

- **ls -a**: Gizli dosyaları gösterir.

- **ls -F**: Listeleme yaparken dizinleri dosyalardan ayırmak için dizinlerin sonuna / koyar.

Linux Temel Komutlar ve Komut Satırı

ls komutunun çıktısını yorumlayalım.

- **1. Bölüm** dosya yapısını gösterir.
- İlk harf d ise dizin olduğunu gösterir.
- - ise basit bir dosya olduğunu belirtir.
- “l” başka bir dosyanın linki olduğunu gösterir.

Linux Temel Komutlar ve Komut Satırı

- **2. Bölüm** dosya izinlerini gösterir.
- **3. bölüm** dosya veya dizinlere bağlı olan link sayısını gösterir.
- **4. bölüm** dosyanın kime ait olduğunu
- **5. bölüm** ise hangi gruba dahil olduğunu gösterir.
- **6. bölüm** dosyanın boyutunu,
- **7. bölüm** ise dosyanın değiştirilme tarihini gösterir.
- **8. bölüm** dosya veya dizinin ismini gösterir.

Haftanın Videosu:)

1--) Hedefli Bir Siber Saldırının Hikayesi

(Targeted Cyber Attack Reality - Don't be a Victim)

https://www.youtube.com/watch?v=TB1PYwSnz2M