|  |
| --- |
| ***Linux Dosya Sistemi Yapısı*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Web uygulama güvenliği zafiyetlerinde genellikle zafiyetini kullanmak istediğimiz sunucular Linux veya Windows tabanlıdır.Saldırı esnasında dosyalar arasında gezinti yaparken hangi dosyanın hangi dosyaları içerdiğini bilmemiz gerekir.Bu sebeple Linux dosya sistem yapısı hakkında bilgi vermek istiyorum. |

**19.07.2021**

**Linux Dosya Sistemi Yapısı**

-Dosya sistemini oluşturan dizinler,kapsadıkları dosyalar ve bunların Linux işletim sistemindeki görevlerini belirteceğim.

-Linux dizin yapısında bazı dizinlerin işlevi birbiriyle aynıdır.Bu durum,özellikle birbirini takip eden iki Linux sürümünde belirginleşir.Örnek olarak birbirin takip eden iki sürümde;bir dağıtımda “/usr/bin” dizini altında yer alan dosya,diğer sürümde “/bin” altına yerleşebiliyor.

-Dosya sistemleri ve dizinler paylaşımlı olarak da kullanılabilir.Birden fazla kişisel makinelerin bağlandığı ağda;disk alanından yer kazanmak için bir makine sunucu(ana makine) olarak tayin edilir.Ağ üzerinde ki diğer makineler de sunucu üzerindeki diski paylaşır.Buna örnek olarak kullanıcı dizinlerinin yer aldığı “/home”;çalıştırılabilir dosyaların bulunduğu “/usr” dizini örnek verilebilir.

-Kök dizini,kendisine bağlı tüm dizinleri içerdiğinden; Linux dosya sistemi önemli bir yere sahiptir.Linux açılırken önce kök dizini “/etc/fstab” dosyasına uygun bir şekilde bağlanır.Diğer dosya sistemlerin onarımı ve kontrolü için gerekli olan “fsck” programları,bu dizinde bulunmalıdır.

-Benzer bir şekilde yedekleme için gerekli olan “tar,zip,compress” gibi arşiv programlarına da kök dizin altından erişebilmeli,açılış esnasında hafızaya yüklenen çekirdek de kök dizinde yer almalıdır.

-Linux sistem yapısı hakkında basit bir bilgi verdikten sonra,Sistemdeki önemli dizinlere göz atmak istiyorum.

***“/bin”***

-Sistemin açılışı ve kontrolü için gerekli komutları barındırır.Kullanıcıların kullanabileceği dosyalar(kök dizinin çok artmaması koşuluyla) buraya depolanabilir.Sadece root kullanıcısının ihtiyaç duyacağı init,getty,updatedb gibi programlar “/sbin - /usr/sbin” de durabilir.

-Bu dizinde bulunan dosyalara örnek olarak cat,chgrp,chown,date,dd,df,ln,mkdir,mount ,ps,rm,sh,su,sync ve umount verilebilir.

***“/dev”***

-G/Ç dosyaları.Linux çekirdeğinde desteklenen her aygıta ait dosya bu dizin altında bulunur.Kurulum anında bu dosyalar yerine yerleştirilir.bu dosyaların silinmesi durumunda /dev/MAKEDEV ile tekrar yaratılabilirler.

***“/etc”***

-Bu dizinde sistem yapılandırma dosyaları vardır.Çalıştırılabilir dosyalar burada bulunmamalıdır.

**-skel :** Üzerindeki dosyalar,kullanıcı hesabı açıldığında ev dizinine kopyalanır.

**-rc.d :** Bu dizinin içinde,init sürecinin başvurduğu yapılandırma dosyaları vardır.Bunlara “rc dosyaları” da denir.

**-passwd :** Kullanıcı veritabanı olarak adlandırabiliriz.

**-fstab :** Linux’un açılışı esnasında bindirilecek dosya sistemleri burada listelenir.

**-group :** Passwd’e benzer şekilde kullanıcıların gruplarını tutar.

**-inittab :** İnit daemon için yapılandırma dosyası.

**-motd :** Kullanıcı sisteme girdikten sonra ekranına basılması istenen mesaj burada tutulur.

**-profile:** Kullanıcı sisteme girdiği zaman çalıştırılan dosya (csh ve sh türevi kabuklar için)

**-shells :** Sistemde kullanılabilecek kabuk isimleri burada tutulur.

**-login.access :** Login komutu için yapılandırma dosyası.Sisteme giriş kullanıcı bazında sınırlamak için kullanılır.

***“/home”***

-Kullanıcılara ayrılmış dizin olarak kullanılır.Açılan her hesaba ait kullanıcı burayı kullanır.Büyük sistemlerde,bu kısım alt parçalara ayrılabilir(/home/yönetici,/home/stajyer gibi).

***“/lib”***

-Sistem üzerinde kullanılan kütüphane dosyaları burada bulunur.Örneğin “python” kütüphaneleri.

***“/mnc”***

-Geçici mount edilen dosya sistemleri.Sadece bu iş için kullanıldığından sistem görevlisine zaman kazandırır.

***“/proc”***

-Süreç kontrollerini ve diğer sistem bilgilerini tutan dosya sistemi.Bu dosya sistemi aslında disk üzerinde yer kaplamaz,tüm dosyalar çekirdeğin bir uzantısı sayılabilir.

**-Cpuinfo :** İşlemci modeli,tipi ve performansı hakkında bilgi verir.

**-Devices :** Çalışan aygıt sürücülerini listeler.

**-Dma :** Hangi dma kanallarının kullanıldığını belirtir.

**-Filesystems :** Çalışan dosya sistemlerini listeler.

**-Interrupts :** Hangi kesintilerin kullanıldığını listeler.

**-İports :** Kullanılan g/ç aygıtlarını listeler.

**-Kcore :** Sistem hafızasının görüntüsü.

***“/root”***

-Sistemin dizini olarak adlandırabiliriz.Diğer kullanıcıların erişemeyeceği şekilde ayarlamak lazım.

***“/sbin”***

-Sistemi etkileyen komutlar burada tutulur.Sadece “root” kullanıcısının ihtiyacı olan komutlar, “/sbin” veya “/usr/sbin” içinde bulunur.

***“/tmp”***

-Geçici dosyaların tutulduğu dizin.

***“/usr”***

-Önemli sistem dosyalarını tutar.Linux sistemlerinde genellikle en kalabalık dizindir.Yeni kurulan tüm programlar buraya kurulur.

**-X11R6 :** X Pencere sistemi bilgileri tutulur.

**-doc :** Belge ve dökümanlar,genellikle HOWTO ve FAQ dosyaları.

**-lib :** Kullanıcının kurmuş olduğu bazı kütüphaneler burada tutulur.

**-man :** Man dosyaları burada bulunur.

**-src :** Bazı kaynak dosyaları ve Linux çekirdeğini oluşturan kodlar (/usr/src/linux) içeren dizin.

**-sbin :** Kök dosya sisteminde yer almayıp çalıştırılabilir sistem üzerinde kullanılabilen dosyalar burada tutulur.

***“/var”***

-Sürekli değişen sistem bilgileri burada tutulur.İstisnalar dışında diğer makinelerle paylaştırılmaz.

-Adm : Sistem yönetimini ilgilendiren kayıtları tutar.

-preserve : Sistem göçmesinden zarar görebilecek dosyalar burada tutulur.

-spool : Sonra işlenecek olan veriler buraya atılır.Örn : E-posta.