Kernel Nedir?

Kernel bir çekirdektir. Bilgisayarın yönetimini sağlayan dosya giriş çıkışı, sistem yönetimi gibi davranışları sergileyen

bir işletim sisteminin merkezidir. İşletim sistemi ile hardware arasında iletişimi sağlayan software parçacığıdır.

Shell Nedir?

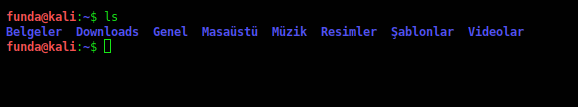
Shell kullanıcı ile çekirdek arasında iletişimi sağlayan bir yazılım programıdır.

Komutların yazıldığı, çıktıların alındığı terminal olarak düşünülebilir.

ls komutu

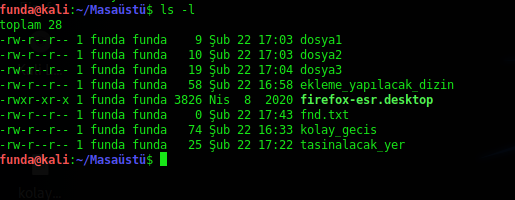
ls komutu aktif olarak girmek istediğimiz dosyanın veya dizinin listelenmesini sağlayan komuttur. Bu komut sayesinde

klasörlerin veya dizinlerin içerisinde neler var görebilmekteyiz.



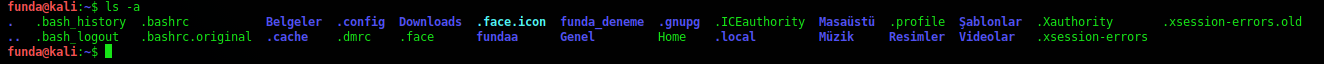
ls -l komutu

bu komut ile dizinimizde bulunan dosya ve dizinlerin bilgilerini sırasıyla dikey ve ayrıntılı olarak öznitelikleri, sahibi, grubu, boyutu, update tarihi, ve dosya isimleri olarak bilgi verilmektedir.



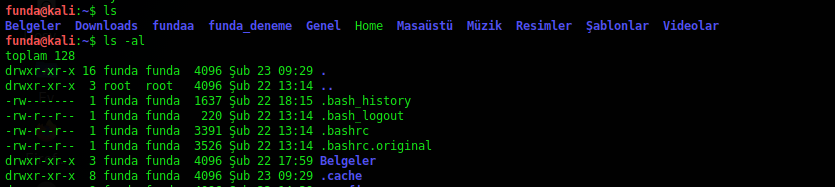
ls -a komutu

bir dosya veya dizini yatay olarak listeleyen ve ayrıntılı bilgi veren komuttur. Ve gizli olan dosya ve dizinleri de göstermektedir.ls



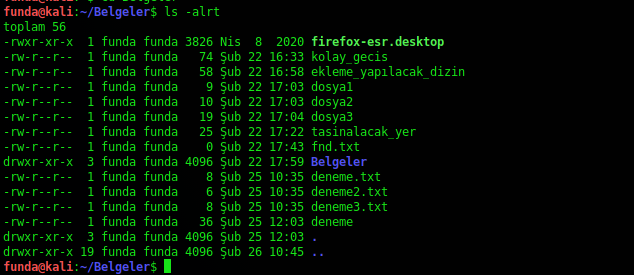
ls -al komutu

-al komutu gizli olan ve sadece ls komutu ile gösterilmeyen dosyaların listelenmesini ve yatay ve dikey olarak ayrıntılı bir bilgi vermesini sağlamaktadır. Sırasıyla öznitelikleri, sahibi, grubu, boyutu, update tarihi ve dosya isimleri hakkında bilgi vermektedir.



Ls -alrt komutu

Değiştirilme zamanlarına göre listelenmiştir.



ls -l -h komutu

hem kb,mb,gb gibi boyut değerleri ile hem de dikey ve ayrıntılı şekilde dosya veya dizin hakkında bilgi vermektedir.



ls -o komutu

-h komutu gibi dosya ve dizini listeleyen fakat boyutlarını göstermeyen aynı zamanda farklı kullanıcı grubu olduğunda onları göstermeyen parametredir.



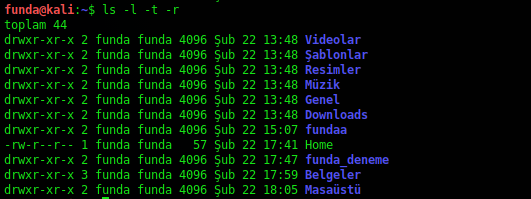
ls -l -t komutu

dosya ve dizinleri dikey olarak ve time olarak listelemektedir. Son eklenen dosya veya dizin en üst sıradadır.



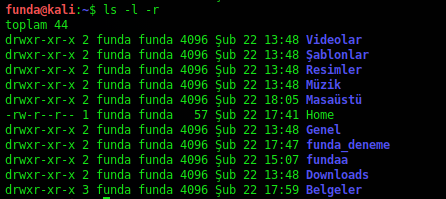
ls -l -t -r parametresi

burada zamana göre dikey ve ayrıntılı olarak listelenmektedir. Fakat reverse yani zamanı son eklenene göre değil ilk eklene göre listelenmektedir.



ls -l -r parametresi

dosya ve dizini ayrıntılı olarak dikey olarak alfabetik olarak listeler ama reserve parametresi ile tersten sıralamaktadır.



ls -l -d parametresi

sadece bulunduğumuz dizin hakkında ayrıntılı bilgi vermektedir. Biz burada belgeler dizinindeyiz içindeki dosyaları görmemekteyiz.



ls -l listelenmek\_istenen1 listelenmek\_istenen2 parametresi

iki veya daha fazla dizini aynı anda dikey ve ayrıntılı olarak listeleyebiliriz.



ls -i parametresi

dosyaların index bilgilerini küçükten büyüğe doğru sıralamaktadır.



ls --sort=? parametresi

sıralama soru işareti yazılan yere gelen parametreye göre büyükten küçüğe göre yazılır. Extension, size, time, version veya none olarak değerler yazılabilir.



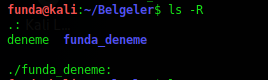
ls -I ? parametresi

soru işareti ile belirtilen alana gösterilmesini istemediğimiz klasörü yazarak ayıklayarak listeliyoruz.



ls -R parametresi

alt dizinleri listelemektedir.



ls -1 parametresi

her satıra 1 dosya yazılarak listeleyen komuttur.



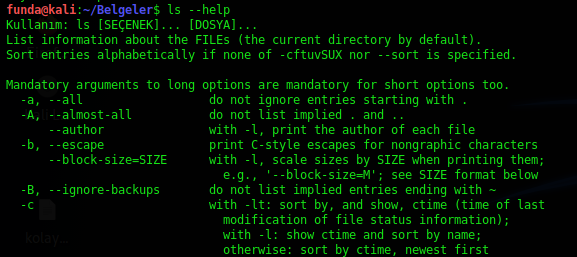
ls - -v

version bilgilerini göstermektedir.



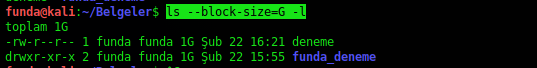
ls - -help

Daha fazla bilgi edinmek için help komutu kullanılmaktadır.



ls --block-size=G -l parametresi

burada g ile belirtilen değer gb değeridir. Kb,mb,gb,tb gibi boyutlarda 1024\*1024 şeklinde listelenir.



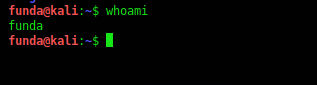
ls - -hide ?

? saklanmasını istediğimiz dosyayı yazarak listeden gizleyebiliriz.



whoami komutu

ben kimim komutudur. Who am i yani aktif user kim onu gösterir. Bu komut yerine id -un komutu da kullanılabilmektedir. Burada biz kullanıcının funda olduğunu görmekteyiz.



Tar komutu

Arşivleme yapan komuttur. Burada -c parametresi ile tar arşivi create eder. -f ile de izin verir.



-x parametresi var olan arşivi aç

-t parametresi tar arşivinin içeriğini listele

-v parametresi kullanıcıya neler olduğunu anlat

-r parametresi arşivi addle

-u parametresi arşivi updatele

-z parametresigzip/gunzip kullanarak sıkıştırma yap

-remove parametresi arşivle işin bitince sil

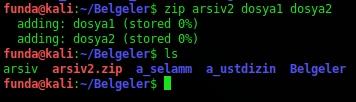
Gzip/guzip komutu

Dosyaları gziple ve guziple arşivler.



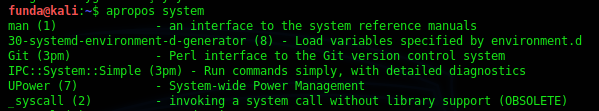
-l parametresi sıkıştırılmış dosyanın içeriğini listeleler.

-f parametresi dosyalar açılırken benzerleri varsa üstüne yazar.



apropos

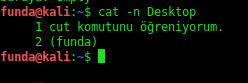
bir komutun ne işlev yaptığını bilindiği ama komutun ne olduğunu unuttuğumuzda apropos komutu kullanılır. Misal systemin ne olduğunu biliyorum ama ne işe yaradığını bilmiyorsam burada apropos komutu kullanılabilir.



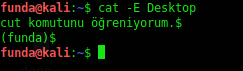
cat komutu

bir metin dosyasının içerisinde neler var onları görüntülemek için kullanılan komuttur.

-n parametresi ile her satırı yazar.



-E parametresi ile her satırın sonuna $ işareti koyar.



mkdir

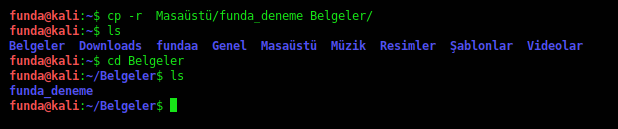
dizin yani klasör oluşturma komutudur. Biz burada fundaa isimli bi dizin oluşturduk ve -ls komutu yardımı ile görüntüledik.



cp komutu

copy paste yani bir dosyayı yada klasör kopyalanmak istediğinde kullanılan komuttur.

-r komutu ile kullanılır sebebi ise dizinin içindeki her şey gösterilen hedef dizine kopyalanır. funda\_deneme isimli dizini bulunduğu konumdan belgelere kopyaladım.



Bu parametrenin yanında başka parametreler de kullanılmaktadır.

-d paratmetresi dosyanın aslını değil linkini kopyalamaktadır.

-p parametresi ile dosyanın kullanıcı izinlerini ve passwordlarını koruyarak kopyalanmasını sağlamaktadır.

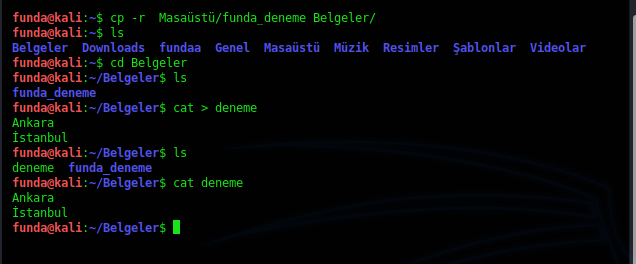
-a parametresi diğer parametrelerle aynı kullanımdadır.

-f parametresinde kullanıcıya hiçbir izin sorusu sorulmadan kabul edilmiş olarak düşünülerek varsa aynı dosyadan silinip tekrardan kopyalanmasını sağlayan değerdir.

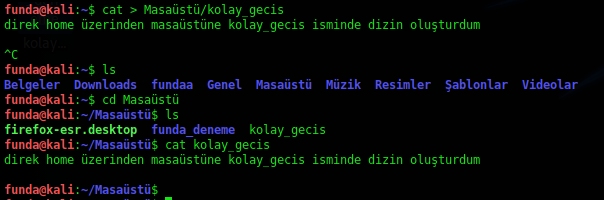
-i hedef adreste dosya mevcut ise kullanıcıya bilgi sorulur.

-u parametresinde kopyalanacak dosyanın tarihi eski dosyadan daha yeni ise bir nevi güncel ise kopyalanmaktadır.

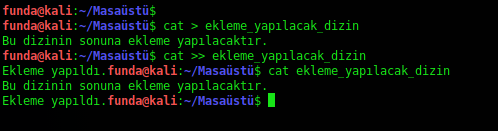
Cat komutu ile dosya oluşturulup dosya içeriği okunabilmektedir. Text ve script dosyalarını okuyabilmemizi sağlamaktadır. Burada deneme adında bir dosya oluşturduk ve dosyanın içine Ankara ve Istanbul isminde iki bilgi girdik. Cat komutu ile hem dosyayı oluşturabildik hemde içeriği görüntüleyebildik.



Cat ile dizinlerin içine girmeden direk home üzerinden istenilen hedefe dosya oluşturulabilir.

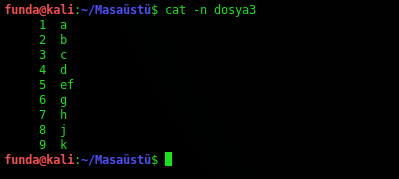


Cat ile bir dizinin sonuna ekleme yapılarak update yapılabilir.

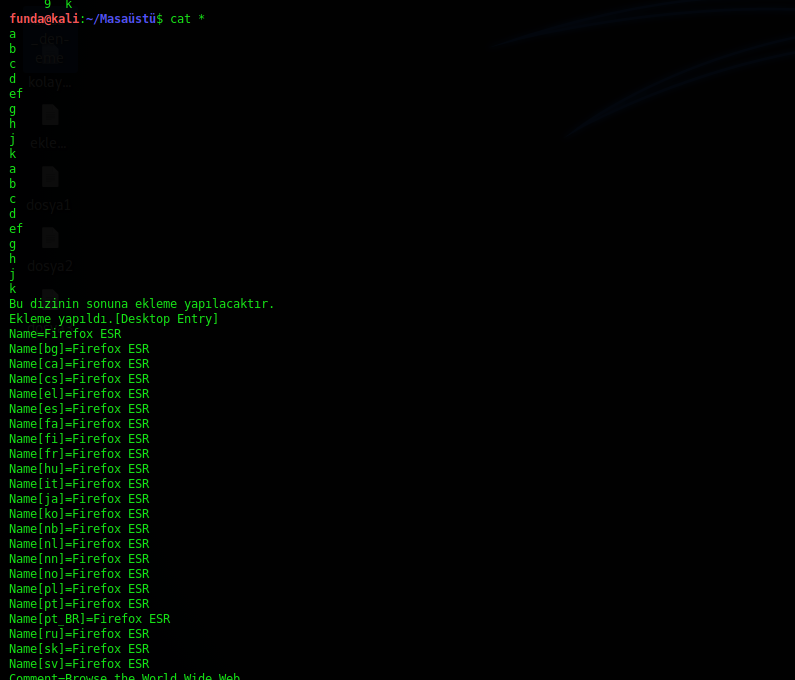


Cat komutu ile iki dosya farklı bir dosyada birleştirilme yapılabilir. Burada dosya1 ve dosya2 isminde iki tane dosya oluşturdum. Içine yazdığım bilgilerin birleştirmek için dosya3 adında dosya oluştururak görüntüledim. E harfinden sonar boşluk bırakmadığımdan dolayı f harfiyle birleşti. Burada dosya birleştirdiğimizden dolayı arka arkaya geldiğini görmekteyiz.

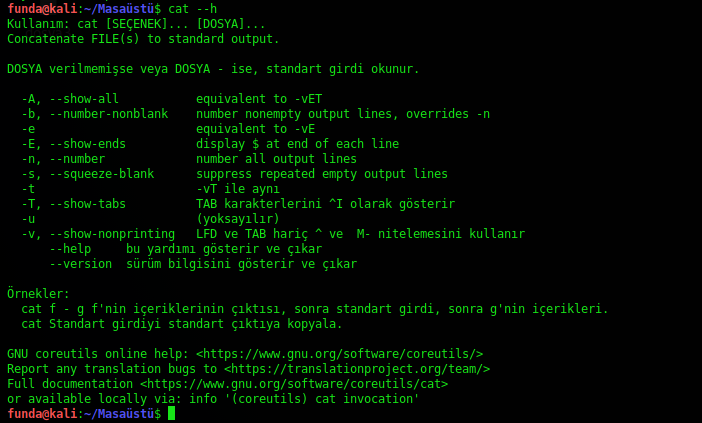
Satır numaraları ile görüntülemek için -n parametresi kullanmaktayız.



Dizinlerin içindeki tüm içerikleri görmek için “\*” kullanılmaktadır.

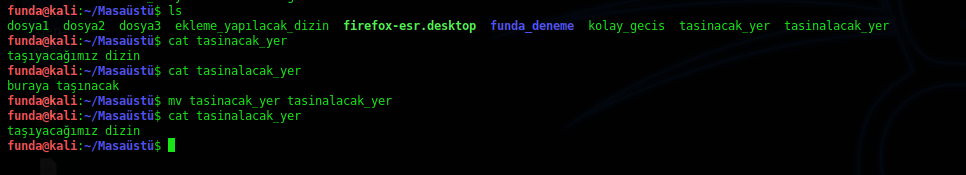


Cat hakkında daha fazla bilgi almak için - - h parametresi kullanılır.

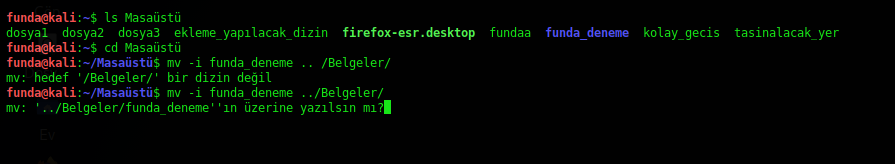


Mv komutu

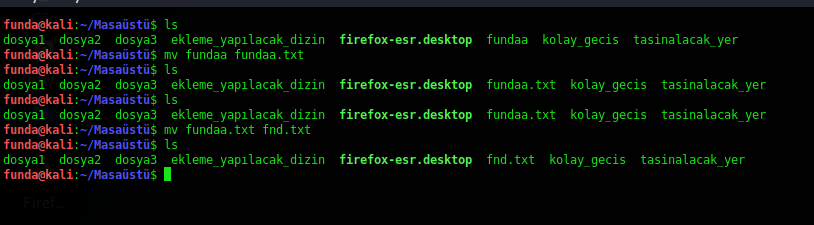
Mv komutu move yani taşıma yapmaktadır. Öncelikle taşınacak bir dosya oluşturuyoruz ki daha kolay anlayabilelim. Taşınacak yer adında bir dosya oluşturuyoruz. Dosyamızı buraya taşıyacağız sonra taşınıp taşınmadığını kontrol edelim.



Tabi bunları yaparken hedef dizinde aynı isimde dosya var mı yok mu kontrol edilmelidir. Bu kontrol -i parametresi ile yapılmaktadır. Eğer aynı isimde bir dizin mevcut ise üzerine yazılsın mı diye bizden onay beklemektedir.



Mv komutu ile bir dosyanın uzantısını değiştirebiliriz. Masaüstünde bulunan fundaa isimli klasörü fundaa.txt metin dosyasına dönüştürebiliriz. Taşıma işlemi gibi önce değiştirilecek klasör ve sonra hangi tipe dönüştüreceğimizi belirleyip uzantısını ekleyerek yapmaktayız. Bu şekilde dosyanın adını da değiştirebiliriz.



mv -n parametresi

var olan dosyanın üzerine sorulmadan yazılmasını sağlamaktadır. Dosya taşındıktan sonra eski yerinden tamamen kaybolmuştur. Burada belgeleri masaüstüne taşıdık ve tekrar listelediğimizde taşındığını görmekteyiz.



touch

touch komutu ile sıfır boyutlu dosya oluşturabiliriz. Burada kali isminde dosya oluşturduk.

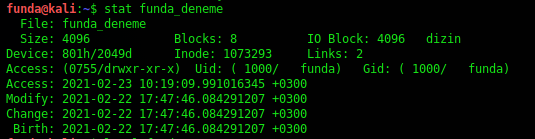


dosyaların isimlerini yan yana yazarak Birden fazla dosya da oluşturabiliriz.



Stat komutu

Bu komut sadece dosya adı ile dosyanın bilgilerini görüntülenmesini sağlamaktadır.



Alias komutu

Takma isim oluşturan komuttur. Isim = değer şeklinde syntax vardır.



Compress

Kali de zip işlemi ziplenecek yer ve dosya olarak yazılır.



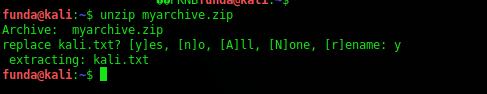
Ziplediğimiz dosyanın içine -r parametresi ile özyinelemeli olarak yeni dizin ekleyebiliriz.



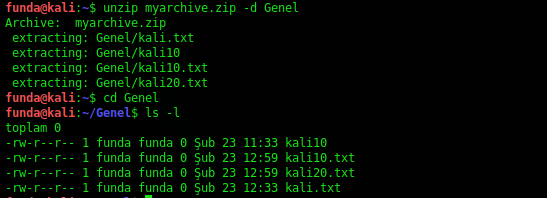
Cat komutu ile zipin içine bakalım.



Unzip komutu ile zip olan bir dosyayı çıkartabiliyoruz.



-d parametresi ile farklı lokasyona zip dosyasını çıkartabiliyoruz.



Chmod

Yetkilendirme izinleridir. Üç tip kullanıcı vardır u (user), g (group), o (other) olmak üzere bir de a (all) hepsini erişebilen bir kullanıcı vardır. Bunların yetkilendirilme tiplerine göre r (read), w (write) ve x (excute) olmak üzere 3 tür mevcuttur. Burada d dizinin de user rwx yani read,write,execute yetkisine, group xr (excute, read) yetkisine ve other x (excute) yetkisine sahiptir. ‘-’ tamamen yetkisiz olduğunu göstermektedir. D burada dizini temsil etmektedir. B özel blok sayfasını, c özel karakter dosyasını, l sembolik bağlantı dosyasını ve p ise özel isimlendirilmiş pipe dosyasını belirtmektedir.



Chmod izinleri harflerle olduğu gibi rakamlar ile de gösterilebilir. r =4, w=2, x=1 değerlerine eşittir. Binary olarak da gösterilebilmektedir. Örneğin 010 okuma yok, yazma var, çalıştırma yok anlamına gelmektedir.

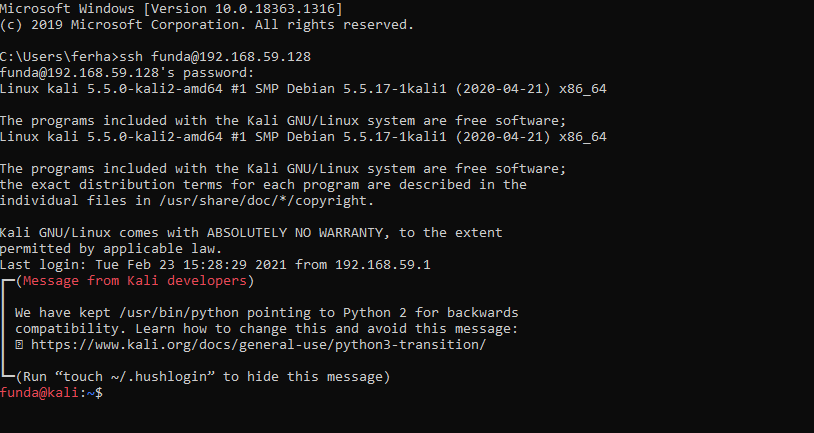
Yetkilendirme izin örneği verecek olursak masaüstü dizininde drwxr-xr-x şeklinde yetkilendirilme verilmiş. Biz burada sadece user tüm yetkilere sahip olsun istiyoruz ve diğerlerinin tüm yetkilerinin kaldırılmasını istiyoruz. Bunun için oluşturmamız gereken komut ‘ chmod u=rwx,go= Masaüstü ’ şeklindedir.



‘\*’ parametresi ile dosyaya tüm kullanıcıların okuma erişimi sağlanmaktadır.

cho

+++Ssh ile bağlantı kurulurken önce kurulacak bilgisayarın rootu (whoami ile bulunuyor) daha sonra ip adresi (ifconfig ile bulunuyor) ssh root@ipadress komutu kullanılarak yazılır. Burada iki makinede ssh açık olmalıdır. Uzaktan bağlantı sağlamak için bağlanmak istediğimiz makinenin password girip connection sağlayabilmekteyiz.

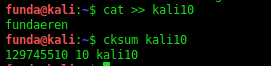


Cksum komutu

Bir dosya veya veri akışı için sağlama toplamı değerini veren komuttur. İlk sayı sağlamada toplam değerdir, ikincisi ne kadar büyüklüğe sahip olduğu ve son kısım ise dosyanın adıdır.

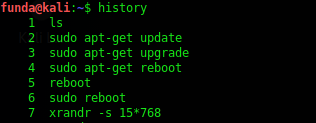


Içerisine bir yazı yazdığımda değeri değişecektir.

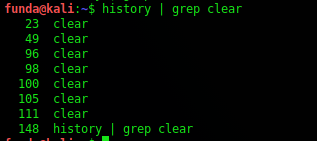


History

Daha önce kullandığımız komutları görmek istediğimizde bu komut kullanılır.



History -c ile geçmişi temizleyebilir yada son 5 kullanılmış komutları görüntülemek için history -5 gibi değerler yazılabilir. Grep komutunu kullanarak ise tüm history listelemek yerine istediğimi komutu görüntülemekteyiz.

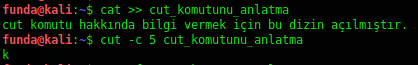


Bir komutu tekrar yazıp çalıştırmak yerine history üzerinde işlenmiş sayı numarasına göre “!” ile tekrar komutu çalıştırabiliriz. Misal olarak 74. Satırda cd Masaüstü var ve ben !74 yazarak masaüstüne geçiş yapabildim.

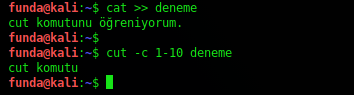


Cut

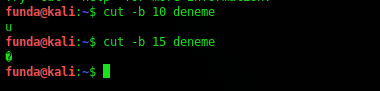
Bu komut bir dosya veya dizinde belirli bir kısmı almak istediğimizde kullanılır. Ilk olarak -c kullanımı görelim. Burada 5. Biti ekrana bastırılır.



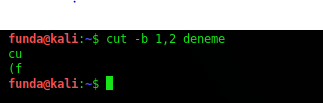
Belirli aralıktaki içerikleri de alabiliyoruz.



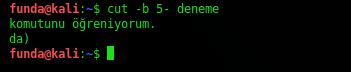
Belirli baytları göstermesi için -b parametresi kullanılır.



Satırlardaki istenilen degree kadar kesilip listelenebilir.



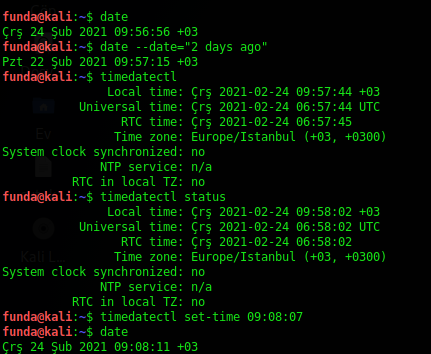
5. bitten sonrasını görmek istediğimiz de



-f parametresi uzunluğu çok fazla olan söz dizilimlerini kesmek için kullanılır.

Date

Tarih saat bilgisini ayarlamamızı, lokasyon değişikliğine göre güncellememizi yeniden yapılandırmamızı sağlayan komuttur.

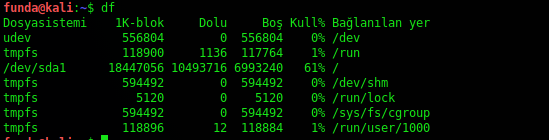


Zone değişikliğinde lokasyonu setleyebiliriz.

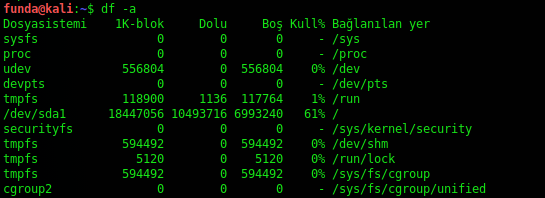


Df komutu

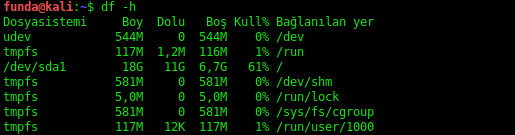
Diskteki boş alanı, ne kadar boş alan olduğunu mount (bağlanma noktasını), doluluğunu, kullanılan alanın boş alana oranı, blok sayısını gösteren komuttur.



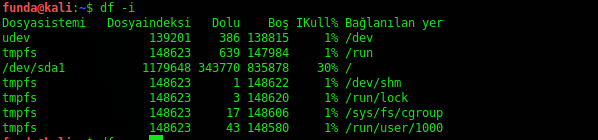
-a paremetresi ile daha ayrıntılı bilgi almaktayız.



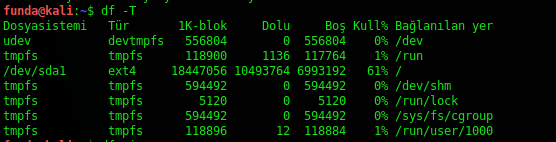
Dosyanın boyutu hakkında bilgileri gb cinsinden görmek için -h parametresi,



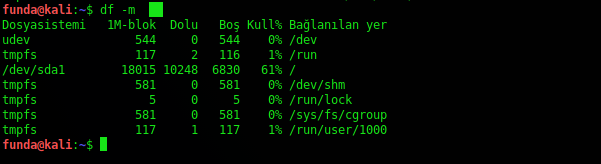
Dosyanın inodesi hakkında bilgilere ulaşmak için -i paremetresi,



Dosyanın tipleri hakkında bilgi edinmek istenilirse -T paremetresi,

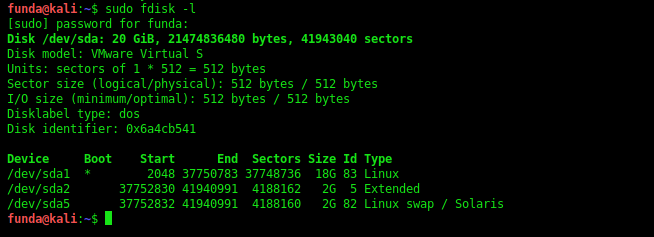


Dosyanın mb cinsinden bilgilerine ulaşılmak istenirse -m parametresi kullanılır.



Fdisk -l komutu

Sistemdeki diskleri ve bölümlerini listelemek için kullanılan komuttur.



-d parametresi ile disk üzerinde bir bölümü silmek yada biçimlendirmek için kullanılır.

-n parametresi yeni bir disk oluşturur.

Diff komutu

difference yani faklılıkları karşılaştıran bir komuttur. -a parametresi ile birlikte kullanıldığında metin dosyası olarak karşılaştırma yapmaktadır.



6c2 burada 6. Satır ile 2. Satır eşleşmesi için değiştirilmesi gerekiyor.

D ise birinci dosyadaki satır ikinci dosyadaki satırla eşleşecek şekilde silinmelidir. Burada hat 0 sekronize hale gelmesi için ilk dosyadan silinöesi gerek 2 satıra ihtiyaç vardır denilmektedir.

-r parametresi ile varsa alt dizinleri karşılaştırır.

Iki dosyanın birbirinden farklı olduğunu öğrenmek için -q parametresi kullanılır.



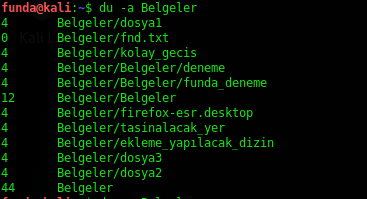
-s parametresi ile aynı olan dosyaları öğrenmek istediğimiz de kullanırız.

Du komutu

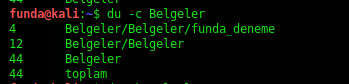
Du disk kullanımının ne kadar yer kapladığını gösterir.



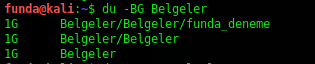
-a parametresi içindeki dizinlerin ayrıntılı olarak yer kaplamasını gösterir.



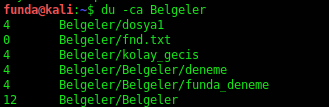
-c parametresi toplam ne kadar disk kullandığını gösterir.



-BM kullanıcıların daha açık bir şekilde anlaması için boyutu gösteren parametredir.



-ca disk kullanımını ayrıntılı gösteren parametredir.



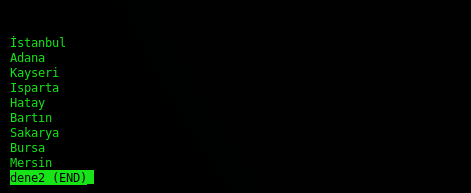
du -sh .[!.]\* \* | sort -n parametreleri ile gizli olan dosyaları boyutları ile birlikte göstermektedir.



Less komutu

Bu komut dosyanın içeriğini görüntülememizi sağlamaktadır.

Kullanımı less dosya şeklindedir.



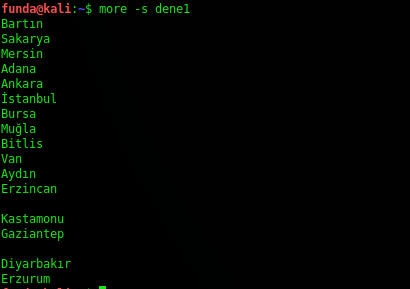
More komutu

Sayfayı görüntülememizi sağlayan komuttur. Less komutu gibidir.

More -p parametresi ile kullanıldığında önce sayfayı temizler daha sonra görüntüler.



-s parametresi birden fazla boş satırı tek boş satır olacak şekilde sıkıştırma yapar.



-n parametresi ile dosyayı satır satır yazar.

-f parametresi ile dosya ismini ve satır numarasını gösterir.

Echo komutu

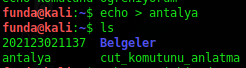
Echo ile hangi kabukta olduğunu görmek istiyorsak echo $SHELL komutunu bastırırız.



Echo ile ekrana yazı bastırabiliriz.



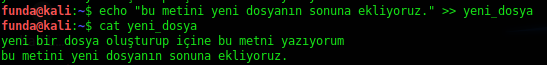
Echo ile yeni bir dosya oluşturabiliriz.



Echo ile hem yeni dosya oluşturup hem de içini doldurabiliriz.



Dosyamızı güncelleyebiliriz.

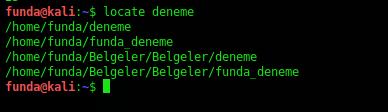


Echo kullanarak matematiksel işlemleri ekrana bastırabiliriz.



Locate komutu

Hızlı olarak arama komutudur. Bir dosyanın nerde olduğunu unuttuğumuzda locate komutu ile dosyanın adını yazarak arama yapmaktayız.



-i parametresi ile kullanıldığında büyük küçük harfleri sorun etmeden arama yapmaktadır.

Wc komutu

Bu komut sırasıyla satır sayısı, kelime sayısı ve komut sayısını ekrana bastırmaktadır.



Karakter sayısını ekrana bastırmak için -c parametresi kullanılır.



Kelime sayısını göstermek için -w parametresi kullanılır.

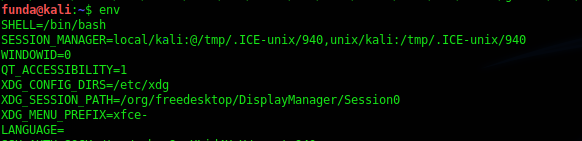


Satır sayısını göstermek için -l parametresi kullanılır.



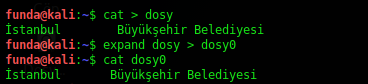
Env komutu

Environment komutu systemin propertiesi hakkında bilgi veren komuttur.



Expand komutu

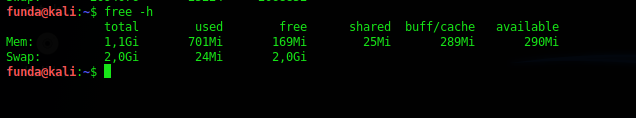
Girdi de verilen tab değerini space değerine çevirme işlemi yapmaktadır.



Free komutu

Bir işletim sisteminde belleğin ne kadarının kullanıldığı ve ne kadarının boş olduğunu göstermeye yarayan komuttur.

-h parametresi kullanarak çıktımızı daha anlamlı hale çevirebiliriz.



Burada takas ve memory kullanımını görebilmekteyiz. Ne kadarının paylaşıldığını ne kadarının meşgul olduğunu total de ne kadarlık belleğe sahip olduğumuzu görmekteyiz.

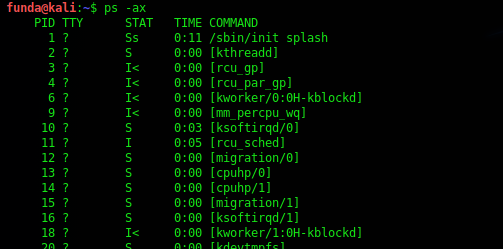
Ps komutu

Ps komutu o anda çalışan işlemleri gösteren komuttur.

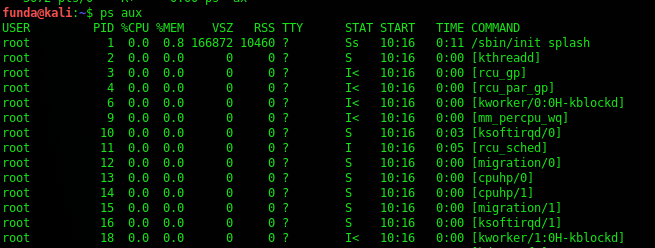
-A parametresi kullanarak çalışan tüm işlemler gösterilmektedir.



-ax parametresi kullanılarak o anda çalıştırabilir tüm işlemler gösterilmektedir.



Ps aux parametresi kullanılarak daha simple şekilde gösterilmektedir.



-L [istenilen\_satır]

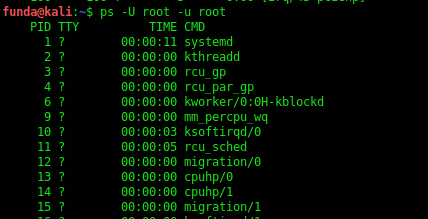
Bu parametre ile istenilen satır hakkında detaylı bilgi edinilmektedir.



-C bash parametresi çalıştırılan bash işlemleri hakkında bilgi vermektedir.



Çalıştırılmış root işlemleri hakkında bilgi almak istediğimizde -U root -u root parametresini kullanmaktayız.



-e parametresi sistemde çalışan her süreç hakkında bilgi verir.

-u kullanıcı adına göre süreç bilgilerini verir.

-p süreç numaralarına göre (PID) süreç bilgisi verir.

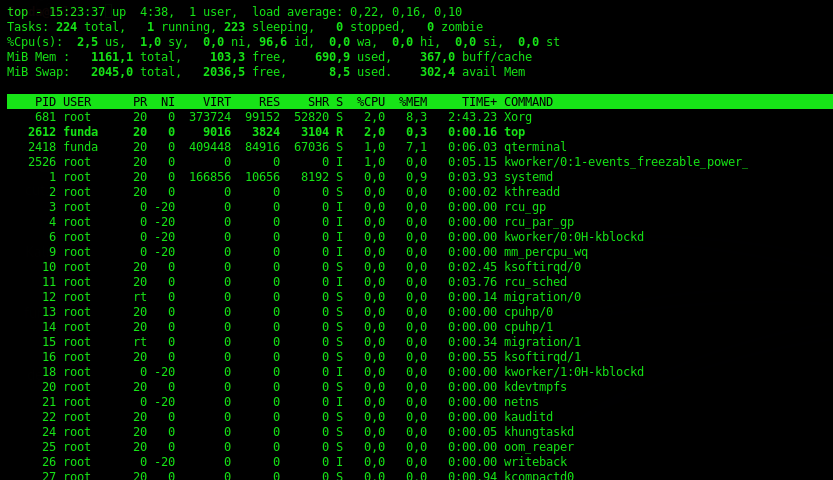
Pstree komutu

Süreci hiyerarşik olarak görüntülemek istersek bu komutu kullanırız. Bir ağaç gibi bize ayrıntılı anlatmaktadır.



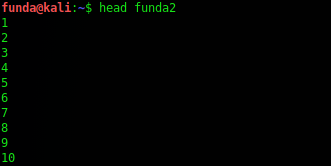
Top komutu

Bu süreci 3 saniyede bir yenilerek sistemin anlık sürecini bilgi verir. -d saniye parametresi şeklinde yazarak anlık güncellenen süreyi değiştirebiliriz. Q ile çıkış yaparız.

df

Head komutu

Head komutu listelenmiş dosyada default olarak ilk 10 komutu vermektedir. Biz istersek -n [değer]parametresi ile görmek istediğimiz kadar değeri listeleyebiliriz.



Tail komutu

Default olarak sondan 10 tane girdiyi bize çıktı olarak vermektedir. -n [değer] parametresi ile kaç değerin listelenmesini istersek çıktı olarak alabiliriz.

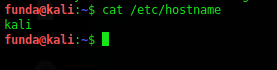


Hostname

Hostname hakkında bilgi edinmek istenirse

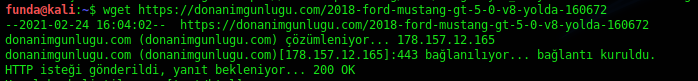


Başka bir alternative olarak şu şekilde de hostname öğrenebiliriz.



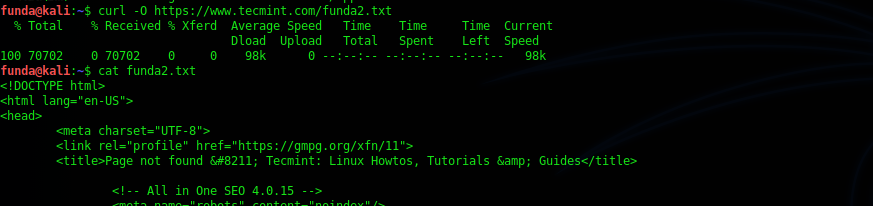
Wget komutu

Dosya indirme komutudur. Indirmek istenilen dosyanın url/dosyaadı şeklinde yazarak indirebiliriz.



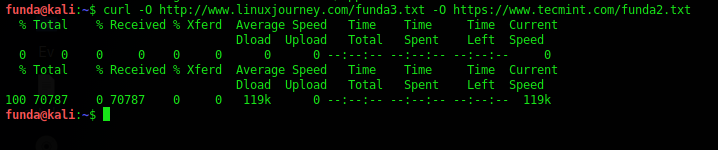
Curl komutu

Veri transferi sağlayan ve url ile verilerin bağlanılımını kontrol ettiğimiz komuttur.

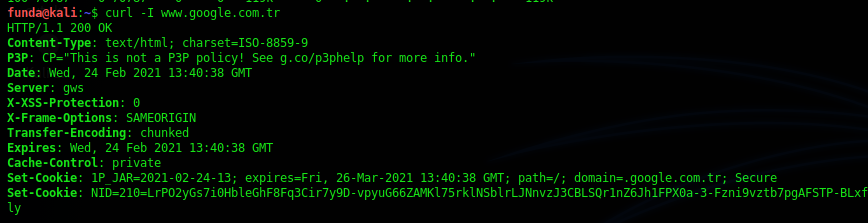


-C - parametresi ile kesilen indirmeyi devam ettirmemiz sağlanır.

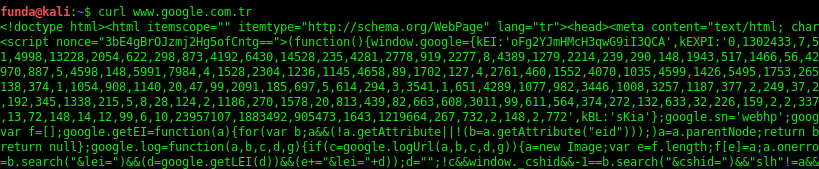
Iki dosyanın indirim işlemi yapmak istediğimizde iki url kullarak kaydetmek istediğimiz alanı da belirterek uygulayabiliriz.



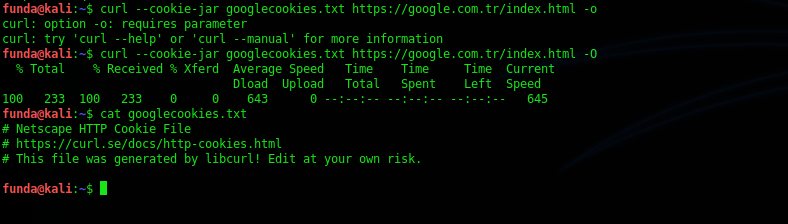
Bir web sitenin HTTP başlıklarını sorgulamak için -I parametresi kullanılır.



Curl ile bir domainin get isteğini alma



Bir web sitesine girdiğimizde hangi cookielerin indirildiğini görmek için bunu bir dosyaya kaydedip görüntüleyebiliriz.



Curl ile sunucuya bir post isteği atabiliriz.



Id komutu

Kullanıcının id bilgilerini veren komuttur.

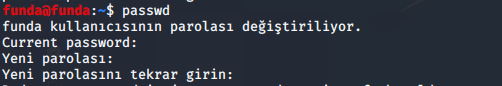


-g parametresi ile etkili kullanıcın id numarası bastırılır.



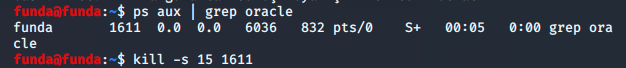
Passwd komutu

Password değişimi yapmak için kullanılır.



Kill komutu

Cevap vermeyen processleri sinyaller ile öldürmek için kill komutu kullanılır. Pid ile birlikte kullanılır. Burada PID değerini bulup kill -l ile nasıl bir kill kullanacağımızı belirlemeliyiz.



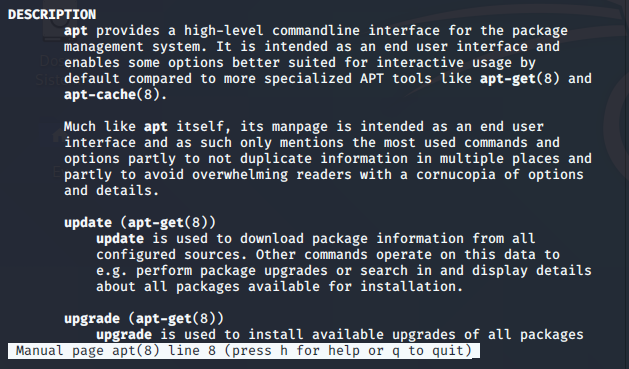
Killal komutu

Bu komut tüm ilişkili sistemi öldürmemizi sağlayan komuttur.

Killal -9 apache örnek verilebilir.

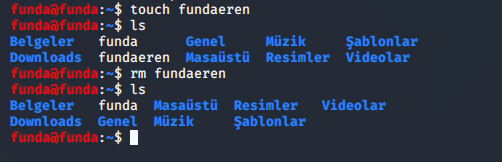
Man komutu

Bir konu hakkında detaylı bilgi almak istenildiğinde man komutu kullanılır.



Rm komutu

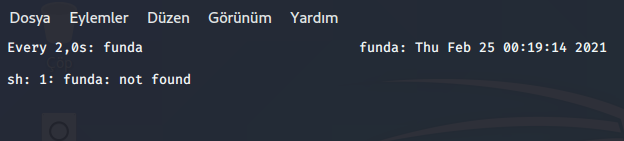
Rm komutu bir dosya yada dizin silmek için kullanılan komuttur.



Onay isteyerek silmesini -i parametresi, alt dizin yada dosyaların silinmesini -r parametresi sağlamaktadır. Yapıalan silmeyle ilgili bilgilerin elde edilmesi için de -v parametresi kullanılmaktadır.

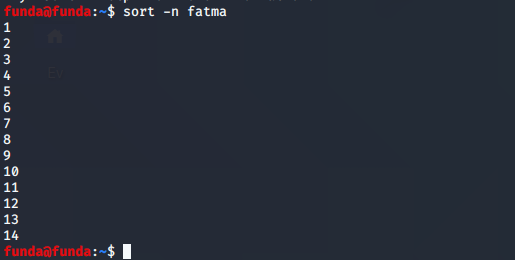
Watch komutu

Saat hakkında bilgi veren komuttur.

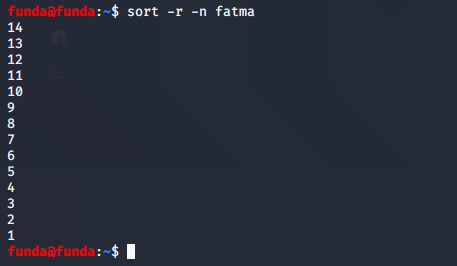


Sort komutu

Harf yada ilk bit sıralamasına göre dizen bir sıralama komutudur.



Tersten sıralama yapılmasını istiyorsak -r parametresi kullanılır.

i

Uname komutu

Makine hakkında bilgiler verir. Ilk olarak kullanılan kernel adını(linux), bilgisayarın ağ üzerindeki host adını(kali), kernel ana dağıtım bilgisini (5.5.0-kali2-amd64), yayınlandığı tarihle birlikte kernelin dağıtıma özel sürüm bilgisi, kullanılan bilgisayarın donanım adı ve kullanılanişletim sisteminin adı sırasıyla verilmektedir.



Split komutu

Boyutu çok büyük olan dosyaların daha küçük boyuttaki dosyalara bölünmesi için split komutu kullanılır.



Burada 13 satırlık funda2 dosyasını 5 satır şeklinde bölerek part1 isminin türevleri olan dosyalara atadım. Bu dosyaları wc -l \* komutu ile görüntülecek olursak şeklinde çıktı alırız.



Tee komutu

Dosyalara standart girdiği ve çıktıyı kopyalan komuta denir.

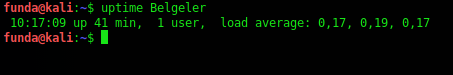
Listelediğimiz standart çıktı logunu birbirinin üzerine yazıp eski dosyayı silmesin diye -a parametresi ile filtrelemekteyiz.



Birden fazla log dosyası oluşturmak için de ls | tee file1 file2 … şeklinde yazabiliriz.

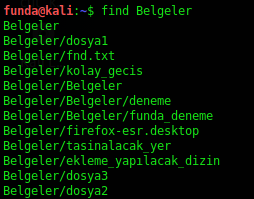
Uptime komutu

Sistemin ne kadar süredir aktif olarak çalıştığını gösteren komuttur. Geçerli zaman, çalışma süresi, kullanıcı sayısı, ortalama yük olarak sıralanmaktadır.



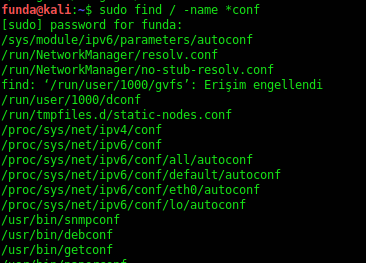
Find komutu

Bulmak istediğimiz dosyarı find komutu ile erişebiliriz.

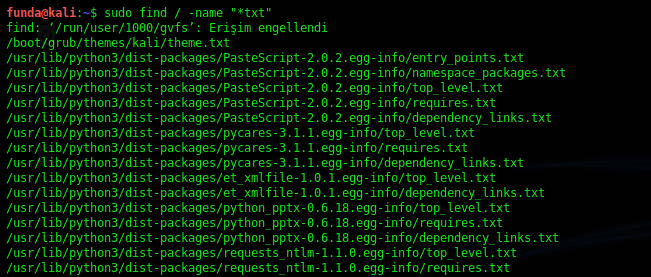
-

Içinde bazı kelimelerin geçtiği dosyaları arıyorsak \*dosya\_adı şeklinde arama yapabiliriz.

Root yetkisi vererek gizli olan dosyalar da dahil arama yapmak istiyorsak sudo su sadece tek bir defalık root yetkisine sahip olmak istiyorsak sudo araması yapabiliriz.

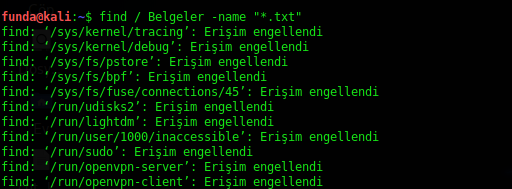


Root olarak txt tipinde arama yapmak istediğimizde kullanılan komut sudo find / -name “\*txt”

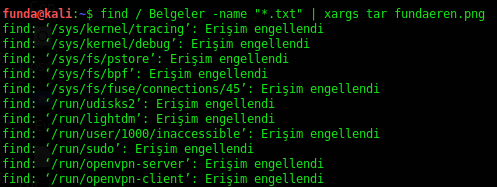


Büyük küçük harflere karşı duyarsız olmasını istiyorsak -iname parametresi kullanılmaktadır.

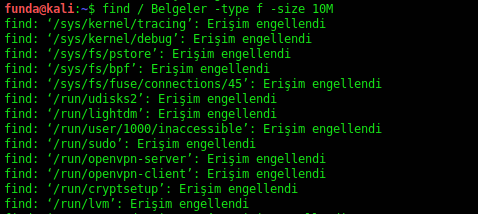
Belirli bir dizinde arama yapmak istenildiğinde ise;



Belgeler dizinin altında .txt uzantılı dosyaları fundaeren.png adında bir dosya oluşturacak ve içerisine sıkıştıracaktır.



Belgelerdeki 10M altındaki dosyaları listelemektedir.



Gizli olan dosyaları görmek için find / home -type f -name “.\*” komutu kullanılır.

Bir kullanıcı arıyorsak find / -type f -user isim -name “.log.txt”

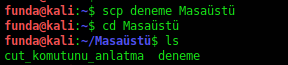
Son 2 gün içinde değiştirilmiş dosyaları arıyorsak find / -type f -mtime 2

1-7 gün arasındaki değişiklikleri görmek istiyorsak find / -type f -mtime +1 -mtime -7

30 dk içinde değiştirilmiş dosyaları görmek istediğimizde find / -type f -cmin -30 parametreleri kullanılır.

Scp komutu

Cp gibi kopyalama komutu olduğunu düşünebiliriz. Kopyalayacağımız dosyayı nereye kopyalayacağımızı gösteren komuttur.



Eğer kendi bilgisayarımızdan başka bilgisayara dosya kopyalamak istiyorsak

Scp dosya user@host:Nereye\_kopyalanacak??



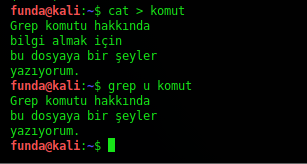
Karşı bilgisayardan kendi bilgisayarımıza dosya kopyalamak için gerekli olan komut

Scp user@host:dosya\_adı nereye\_kopyalanacağı



Grep komutu

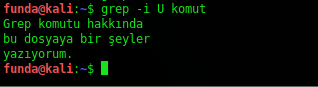
Find komutu gibi arama yapmak için kullanılır. Dosya içinde u harfi olanları ekrana bastırmaktayız.



Büyük küçük harfe duyarlıdır bundan dolayı U araması yaptığımızda sonuç vermeyecektir.



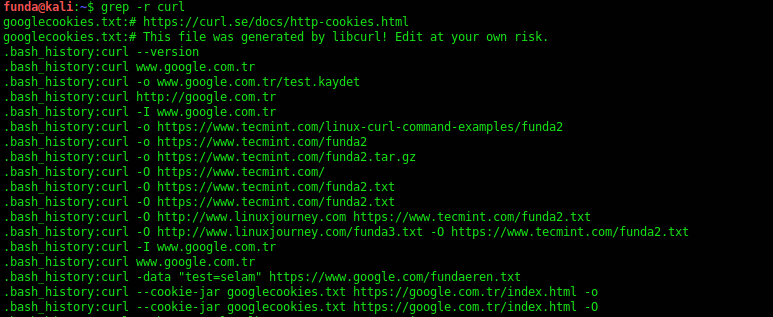
Büyük küçük harf duyarlılığını kaldırmak için -I parametresi kullanılmalıdır.



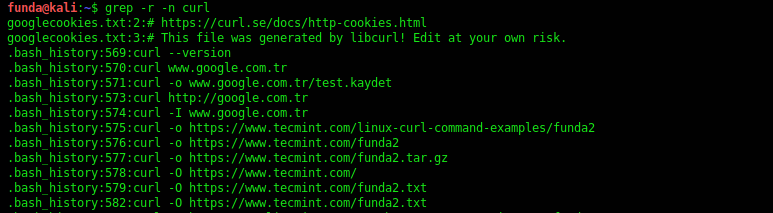
Bazı kelimeler dışında arama yapmak istediğimizde -v parametresi kullanarak arama yapabiliriz. Burada u harfi içeren satırlar gelmesin istedik.



Dizindeki tüm dosyalarda arama yapılmasını istiyorsak -r parametresi kullanmaktayız.



Satır numarası kullanarak çıktı almak istediğimizde kullanmamı gereken parametre -n dir.



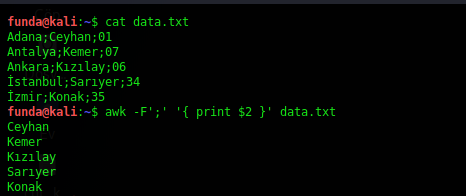
Chown komutu

Bu komut kulanıcı değiştirmektedir. Sudo olarak yetkiyi devretmekteyiz.

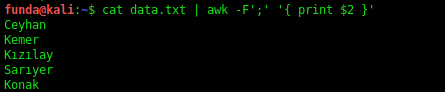
Sudo chown user dosya şeklinde yazılan komut sıralamasıdır.

Awk komutu

Awk programlama dili yazılımsal olarak ifade filtrelemektir. Burada -F alanı ayırmaya yarayan parametredir. Yani noktalı virgule ayrılmış kısımı ayırmaktadır. & ile belirtilen kısım hangi indeksleri istiyorsak o indeksleri bize verip ekrana bastırmaktadır. Biz burada 2. Indeksteki değeri ekrana bastırmak istedik.



Data.txt veri akışındaki veriyi 2. Indeksteki değeri alır ve ekrana bastırır.



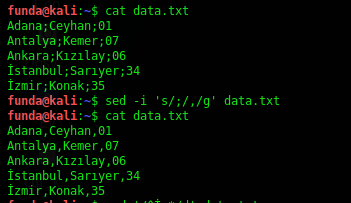
3. indekste bulunan değerlerin toplam değerini ekrana bastırır.



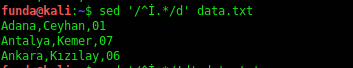
2. ve 5. Indeksler arasındaki değerleri ekrana bastırır.



Sed komutu bu komutu kullanarak dosyaların içinde değişiklikler yapabilmekteyiz. burada ; ile ayrılan kısımı , ile ayırma işlemi yaptık.



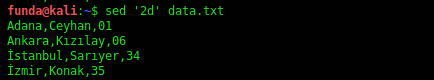
Istediğimiz satırı belirlediğimiz koşullarda silebiliriz. Biz burada I harfi ile başlayan satırları sildik.



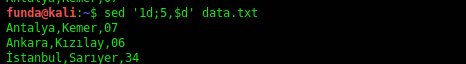
Sildiğimiz satırları geri getirebilriz.



Belirli bir indisteki satırı silebiliriz biz burada 2. Satırı sildik.

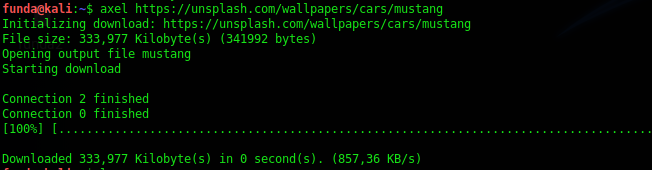


Belirli aralıktaki ifadeleri ekrana bastırabiliriz. Burada ise 1 ve 5. Satırlar arasındaki ifadeleri ekrana bastırmak istedik.



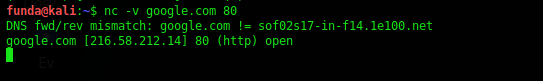
Axel komutu

Dosya indirmeyi sağlayan komuttur. Axeli öncelikle sistemimize kurup daha sonra istenilen dosyanın link adresi verilmelidir.

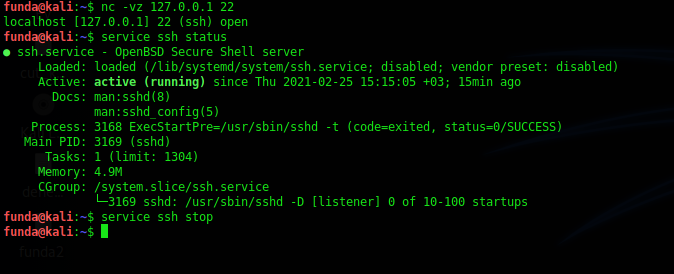


Netcad kullanımı

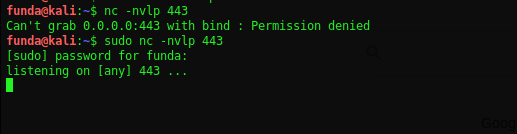
Burada google.com 80 portu üzerinden dinleme yaptık.



Hangi portların açık yada kapalı olduğunu öğrenmek için -nv parametresini kullanırız.

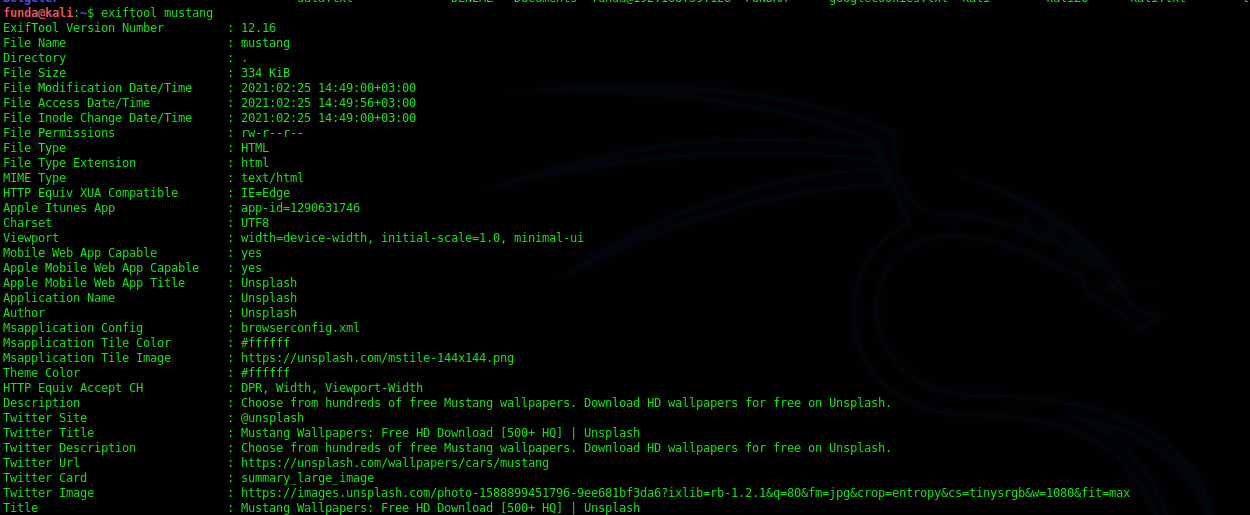


Dosya aktarımında kullanılan parametre -nvlp parametresi kullanılır. Biz burada web sitemize 443 porttan bağlandık.



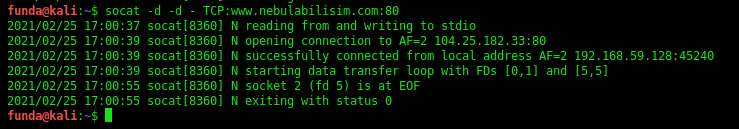
Exiftool komutu

Bu komut bir resim dosyası hakkında ayrıntılı bilgi vermektedir.



Socat komutu

Zayıf güvenlik duvarlarına saldırmak için Tcp bağlantı noktası ileticisini çift yönlü bayt akışı oluşturarak kullanılır.

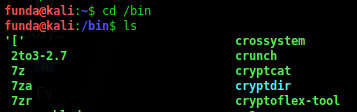


Linux Dosya Sistem Hiyerarşisi Nedir?

Dosy Sistem Hiyerarşisi linux bir kök dizin yapısına sahiptir. Öncelikle root olan kök dizinden sırasıyla alt dizinlere doğru ayrılır. Bu ayrılma / ile gösterilmektedir. Kök dizinimiz bizi en yetkili kullanıcımız anlamına gelmektedir. Onun sistemde yaptığı değişiklikler yetkili olduğu için bir soruna sebep olmamaktadır. Sistemde bir dizin yada dosyada kalıcı değişiklikler yapılması için yetki yükseltilmesi yapılıp root olunması gerekmektedir. Alt dizinlere yarılan linux dağıtık bir sistemdir. Dağıtık sistem tek bir makinede tüm özelliklerin bulunmamasıdır. Ağ üzerinden iletişim halinde olan bir çok makine farklı sunucuları farklı makinelere kullanıp ağ üzerinden iletişime geçebilir. Bu şekilde tek bir makinenin yükü azalarak performansı artmaktadır.

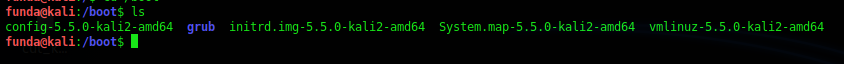
/bin dizini

Temel komutlar bu dizinde çalışmaktadır. Sistemde herhangi bir sorun olduğunda bin dizini çalışmaya devam etmektedir. Komutlar çalışmaya devam ettiğinden dolayı sistemdeki sorun /bin dizini sayesinde düzelebilmektedir.



/boot

Sistemi boot etmek işletim sitemine ulaşarak bilgisayar açılırken öncelik verdiğimiz sistemin yüklenerek sisteme güç vermesi demektir. Sistemin boot öncelik ayarlarını değiştirebilmek için BIOS a girmemiz gerekir. BIOS donanım çalışırken işletim sistemi ile aradaki iletişimi kuran yazılım işletim sisteminin nereden yükleneceğini bileni donanımsal protokolleri belirleyen ve işletim sisteminin öncelikle hangi donanımı okumasını sağlayan yazılımdır.



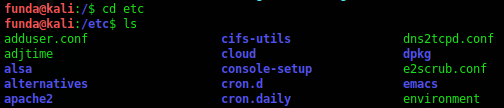
/dev

Linuxtaki herşey dosya şeklinde dizinlere ayrılmıştır bunların içine donanım aygıtları olan fare, modem gibi aygıtların bağlandığı portlar olan tty dizini, birincil ses kayıtlarının olduğu dsp aygıtlarını içerir.



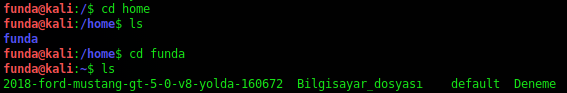
/etc

Sisteme dair tüm yapılandırmaları ve bilgisayara özel yapılandırmaları içermektedir. Çalıştırılabilir dosyalar bulunmamaktadır.



/home

Kişisel verilerinin depolandığı, başka programlara yaptığı değişiklikler burada depolanmaktadır. Ayrıca kullanıcının resim, müzik gibi dosyaları da burada tutulmaktadır.

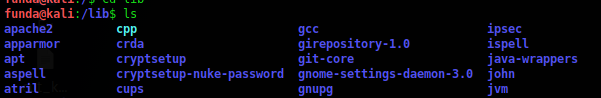


/initrd

Çekirdek yüklenmesinden sonra oluşan bellek diskin üzerinde root olarak açılmasını sağlamaktadır.

/lib

Çekirdeğe ai tolan modüller ve kütüphane dosyaları burada tutulmaktadır.



/mnt

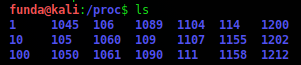
Sabit disk ve tüm donanımsal aygıtların bağlanma noktasır. İşletim sisteminin kurulu olduğu disk buna değildir.

/opt

İşletim sisteminden bağımsız, kurulumu zorunlu olmayan programların bulunduğu dizindir.

/proc

Fiziksel dosyaların bulundurulmadığı donanımsal yapılandırmalar, süreç, bağlı aygıtların bulunduğu sanal bir dosya sistemidir.

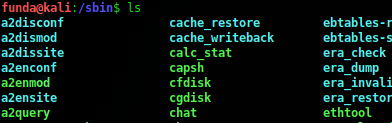


/root

Yetkilendirme olarak en üst yetkiye sahip olan kulllanıcıdır. Sistemdeki tüm değişikliklere izini bulunmaktadır. Kullanıcı olarak yapılamayacak tüm işlemleri root olarak yapılandırılabilir. Kalıcı olarak root olmamıza sistem izin vermemektedir. Geçici olarak root olma yetkisi için sudo komutu kullanılır ve sistem root olmanız için makinenin parolasını istemektedir.

/sbin

Root tarafında kullanılacak yönetimsel ve bakımsal programlar bu dizin altında tutulmaktadır. Genellikle sistem yöneticisi tarafından kullanılmaktadır.



/user

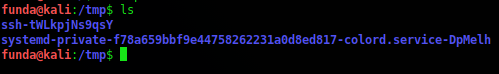
Sadece kullanılan makineye özel local klasör olan usr komutlar, programlar, kütüphaneler gibi tüm kullanıcılara paylaşılan verileri içeren dizindir.

/var

Sisteme ait güvenlik duvarını ve sisteme düşen logları görüntülemek için ve e-posta, yazıcı kuyrukları bu dizin altında tutulmaktadır.

/tmp

Geçici programların depolandığı dizindir. Belirli zaman aralıklarında temizlendiğinden dolayı önemli programları buraya kurmamalısınız. Çünkü makine yeniden başlatıldığında silinir.



Dizin işlemleri

Pwd komutu

Ben neredeyim? Bunu öğrenmek için kullanılır.



Cd komutu

Bir dizine girilmek istendiğinde kullanılır.



Cd .. o dizinden çıkılmak istendiğinde kullanılır.



Cd – ile bir önceki bulunduğumuz dizine döneriz.



Cd - - en başa döneriz.



Herhangi bir parametre kullanacak olursak kullanılan komuttan sonra -parametre şeklinde bir dizilim yaparız.

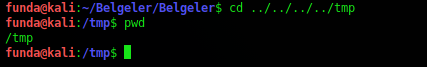
Full path

/ kullanarak çalışma dizine bağlı olmadan istediğimiz yere gidebilmemizi sağlayan araçtır.



Relative path

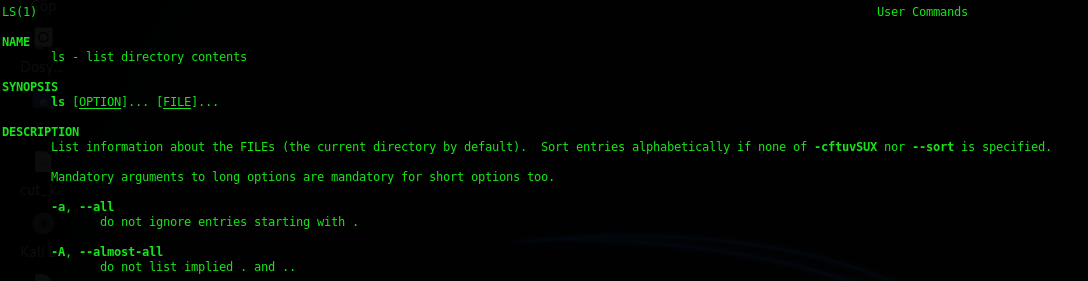
Nerede olduğumuza bağlı olarak yolumuzu belirterek istediğimiz yere o güzergahta gidebildiğimiz araçtır.



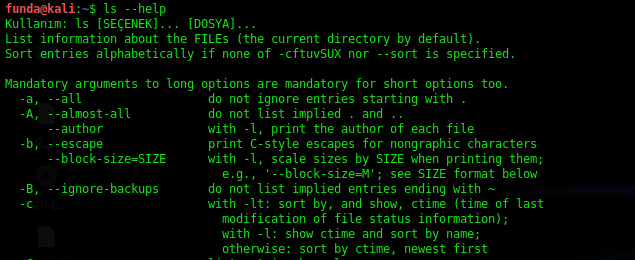
O komutlar hakkında daha fazla bilgi edinmek için man, help ve info komutları kullanılmaktadır.

Man ile ls komutu hakkında bilgi edinelim

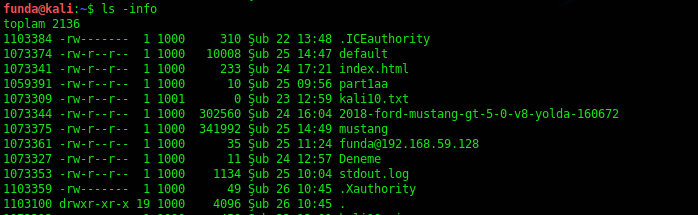
Komut man help



Help komutu ile ls hakkında bilgi edinelim.

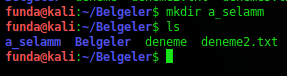


Info kumutu ile bilgi edinme

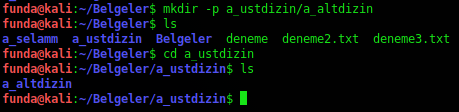


Mkdir komutu

Dizin oluşturmak için kullanılır.



Alt dizinlerde aynı anda oluşturulabilir.



Rmdir komutu

Içi boş dizinleri silmek için rm komutu kullanılır.



Rm komutu

Içi dolu dosyaları silmek için rm, dizinleri silmek için rm -r komutu kullanılır.



-i parametresi silinsin mi silinmesin mi onu sorgular.



-f parametresi sormadan siler

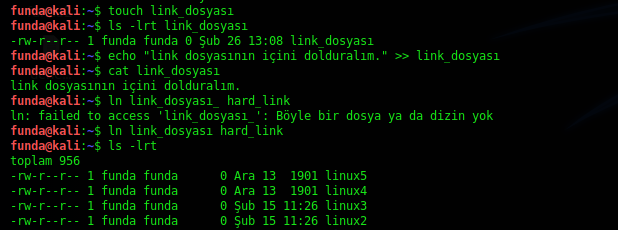
-r parametresi bulunduğu dizinin alt dizinlerini de siler

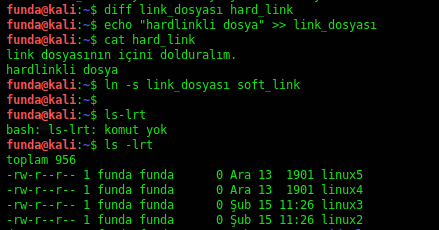
-v parametresi ne yapıldığı bilgisini alt kullanıcıya da döndürür.

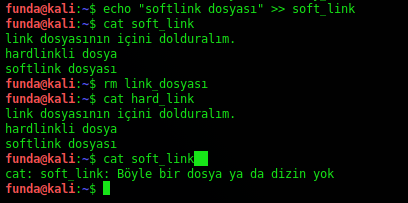


Ln komutu

Dosyalara link yapmak için kullanılır.

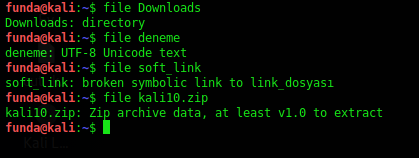






File komutu

Dosya mı dizin mi ne olduğunu bilmediğimiz zaman bu komutu kullanarak öğrenebiliriz.



‘>’ önüne 1 yazılır yada yazılmaz ise standart çıkışı ekrana verir. 2 yazılırsa komut çalışırken alınan hatalar dosyaya yönlendirilir. Yönlendirmede kullanılan tek ‘>’ eğer yönlendirilecek dosya yoksa dosya oluşturulur varsa dosya içi temizlenir ve çıktıyı yönlendirmektedir.

Yönlendirmedeki yönlendirme işaretinin çift olması “**>>**”,eğer yönlendirilecek dosya yok ise oluşturulur, dosya var ise çıktıyı dosyanın sonuna yönlendirir.

‘^’ Satır başını belirtir.

‘$’ Satır sonlarını belirtir.

‘.’ Sadece bir karakter ile eşleşir,bir karakter ifade eder

‘\*’ Kendinden önceki karakterden 0 veya daha fazla olmasını belirtir

‘[]’ Köşeli Parantez içindeki karakterlerden sadece biriyle eşleşir.

‘[^]’ Köşeli parantez içinde olmayan karakterlerle eşleşir.

+ Kendinden önceki karakter en az 1 veya daha fazla karakteri ifade eder.

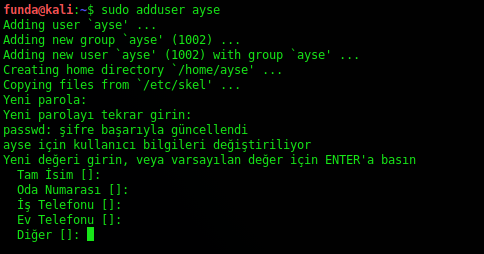
Kullanıcı işlemleri

Kullanıcı değiştirme için su komutu kullanılır.



Root olmak için sudo komutu kullanılır.

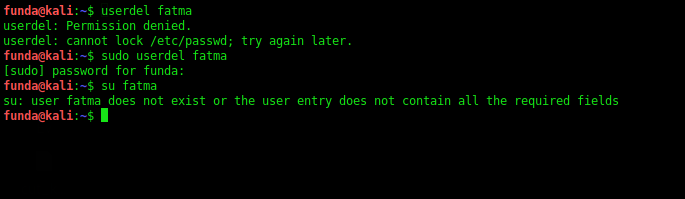
Yeni kullanıcı ekleme için sudo adduser name dizilimi kullanılır.



Kullanıcı şifresini değiştirmek için passwd parametresi kullanılır.



Kullanıcı silme



-r parametresi ile kullanıcıya ait her şeyi sileriz.

Grup oluşturma



Grup silme



Kullanıcının üye olduğu grupları gösterme



Kullanıcıyı yetkilendirme



Kullanıcıyı kilitleme



Kullanıcının kilidini kaldırma



Kullanıcı sayısı alma



Güncelleme, kurma ve kaldırma işlemleri

Güncelleme

Bu komut depolarda olan yeni sürümleri günceller

apt-get update

yeni sürümleri kontrol edilip bildirilmiş paketlerin en son versiyonlarına günceller

apt-get upgrade

hem güncelleme yapar hemde sistemdeki gereksiz paketleri siler.

apt-get dist-upgrade

depodan indirilen tüm paketlerin silinmesini sağlar sistem tertemiz olur.

apt-get clean

eski sürüm olan artık kullanılmayan paketleri siler

apt-get autoclean

silinen uygulamadan geriye kalmış ve artık kullanılmayan paketleri siler

apt-get autoremove

-y parametresi otomatik olarak yes olarak sistemi devam ettirir bizden cevap beklemeden yes diyerek sistem kesintisiz çalışır.

Kurma

Depodan kurulum ile program kurmak

Sistemimiz güncel ise ve program depoda varsa apt-get install program\_adı şeklinde programlarımızı kurarız.

Programın depoda olup olmadığını kontrol etmek için apt-cache search program\_adı komutu ile girer bakar kontrol ederiz. Tekrar konsola programın adını yazarak teyit edebiliriz.

Program kaldırma

Kurulan program kaldırmak istiyorsak apt-get remove program\_adı şeklinde girdiğimizde otomatik olarak kaldırırız.

Programın yapılandırma dosyalarını sistemden kaldırmak istiyorsak apt-get - -purge remove program\_adı ile kaldırabiliriz.

Paket yönetim sistemi ile kurulum

Debian paketleme sistemine sahip olduğu için kali uzantı olarak .deb olarak kurulum gerçekleştirebiliriz.

Dpkg -i dosya\_adı.deb ile program kurarız.

Dpkg -r dosya\_adı ile sileriz.

/etc altındaki paketlerini de silmek istersek -p parametresi kullanırız.

Paketleri tekrar yapılandırmamız gerekirse reconfigure dosya\_adı şeklinde yazarız.

-l parametresi ile tüm parametreler hakkında bilgi alırız.

Çıktıda yer alan paketlerin sol tarafındaki ifadelerin anlamı:

**ii :** paket normal olarak sisteme yüklendi.

**rc :** paket yüklendikten sonra silindi ancak konfigürasyon dosyaları halen mevcut.

**pn :** paket konfigürasyon dosyaları ile birlikte sistemden kaldırıldı.

Kurulu paketin durumu için dpkg -s program\_adı şeklinde paketin durumunu öğrenebiliriz.

Kurulu paketin içeriğini öğrenmek istersek dpkg -L parametresini kullanırız.

Indirdiğimiz paketleri kurmadan içeriğini görmek istiyorsak dpkg -c parametresi kullanırız.

Sistemden kaldırılmış paketleri dpkg - - get – selections ile görürüz.

Bu paketi daha sonraya yedeklemek istersek dpkg - - get – selections > yedeklenecek\_dosya şeklinde yazarız.

Yedeklenen dosyaları başka bir sisteme tek seferd yüklemek için

dpkg - - set – selections > yedeklenecek\_dosya

ve eksik olan bişey varsa onları güncellemek için ise

apt-get deselect-upgrade komutu ile yaparız.

Joker karakterlerin kullanımı

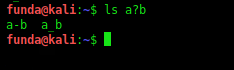
Tek seferde birden fazla dosyaya işlem yapan karakterlere joker karakterler denir.

Asterix işareti : ‘\*’ rm funda\* yaparsak funda ile ilgili her şeyi silmiş oluruz.



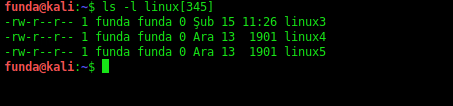
? karakteri

Birbirine yakın yazılışlara yakın dosyaları görüntülememizi sağlar.



[] karakteri

Istenilen değerler parantez içinde belirtilerek çağırılır.



[!değer] burada belirtilen değerler haricindeki değerleri basar.

[değer-değer] aralıklarını basar

Ağ bağlantı komutları

Ifconfig komutu

Ağ bağlantı kartlarını listelemek için kullanılır. Eth ethernet kartları hakkında bilgi vermektedir.

Lo localhost hakkında bilgi vermektedir.

Wlan0 ise kablosuz ağ hakkında bilgi vermektedir.

Ifconfig kart\_adı ile tüm kartları değil istediğimiz kartı listeleyebiliriz.

Eth0 ip adresini değiştirmek istiyorsak sudo ifconfig eth0 ip\_adres şeklinde yapabiliriz.

ağları kapatmak istersek ifconfig ağ\_adı down yaparız. ifconfig ağ\_adı up ile de geri açarız.

Ping komutu

Ağın ayakta olup olmadığını kontrol eden komuttur. Sınırlı sayıda pinglemek istersek -c parametresi kullanılır.

Route komutu

Sistemimizdeki ip yönlendirme tablosunun içeriğini görmemizi sağlayan komuttur.

Traceroute komutu

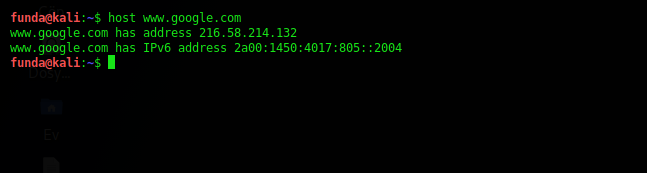
Belirli bir yere gönderilen iplerin hangi hostlar üzerinden geçtiğini gösteren komuttur.

Whois komutu

Domain hakkında bilgiler veren yani domain ne zaman kurulmuş, ne zamana kadar geçerli, kimin üzerine kayıtlı bunun gibi bilgileri verir.

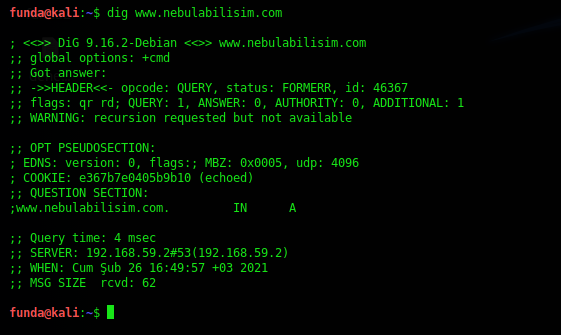
Host komutu

Host hakkında bilgi almamızı sağlar.



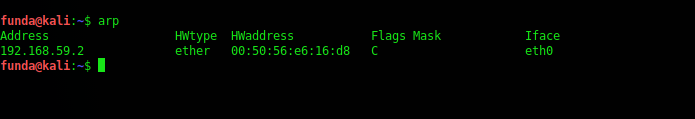
Dig komutu

Dns kayıtlarına bakmak için kullanılan komuttur.



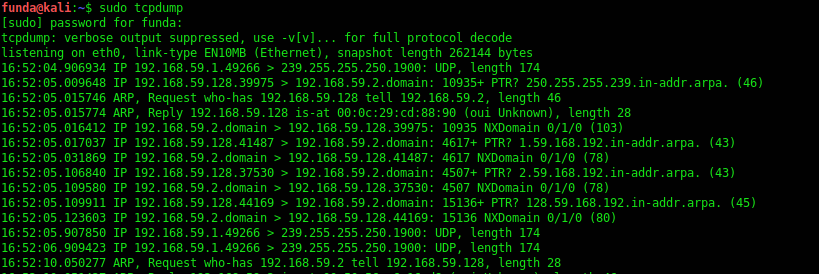
Arp komutu

Mac ve ip eşleşmesinin tablolandığı komuttur.

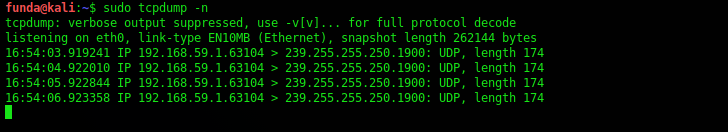


Tcpdump komutu

Sisteme yapılan ve sistemin yaptığı bağlantıları anlık olarak görüntüleyen komuttur.



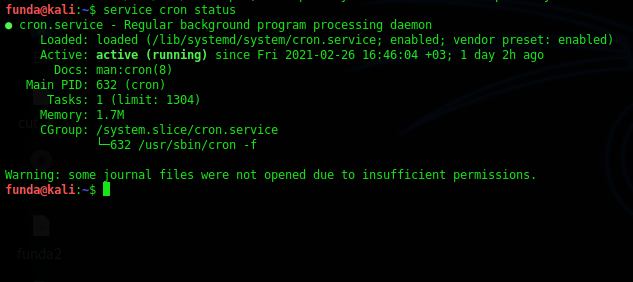
Direk olarak bağlantıları görüntülemek istersek ise -n parametresi kullanırız.



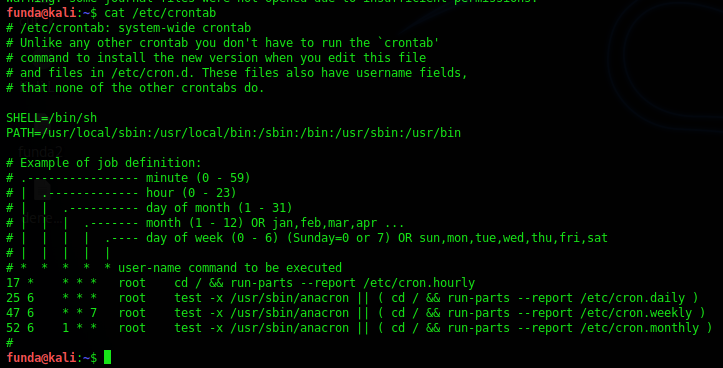
Cron komutu

Cron belirlenmiş zamanda belirlenmiş görevi yerine getiren komuttur.

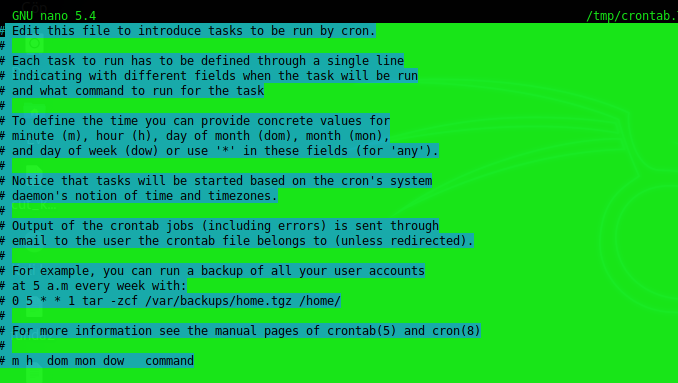
Öncelikle cron ayakta mı değil mi ona bakıyoruz. Evet cron şu anda aktif durumda.



Cron dosyasının nerede olduğunu /etc dizinin içinde bulabiliriz.



Düzenleme yapmak için -e parametresini kullanırız.



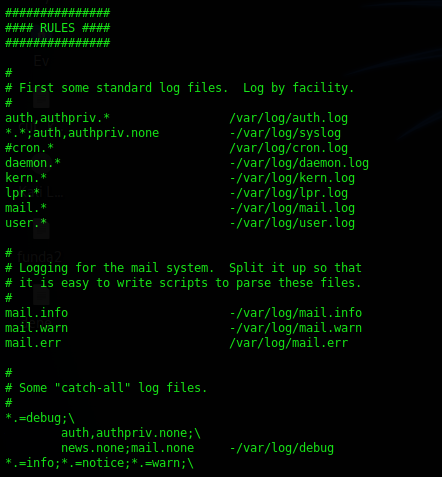
Crontabları listelemek istediğimizde -l parametresini kullanırız.



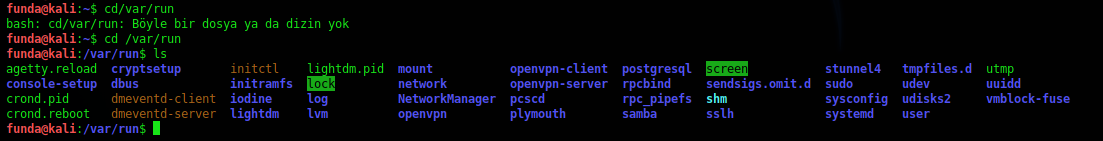
Oluşturduğumuz tüm crontabları silmek istersek -r parametresini kullanırız.

Log dosyaları

Log dosyaları kayıt dosyalarıdır. Bu dosyalarının nereden kaynaklandığını syslog konfigürasyon dosyasından bakabiliriz.



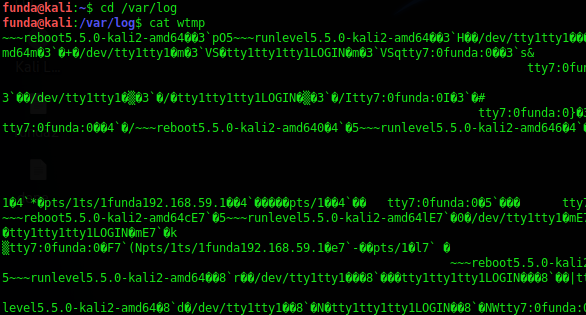
Sisteme şuanda bağlı olan kullanıcıların varlığını listeleyen log komutu /var/run ls ile bunu listelemekteyiz.



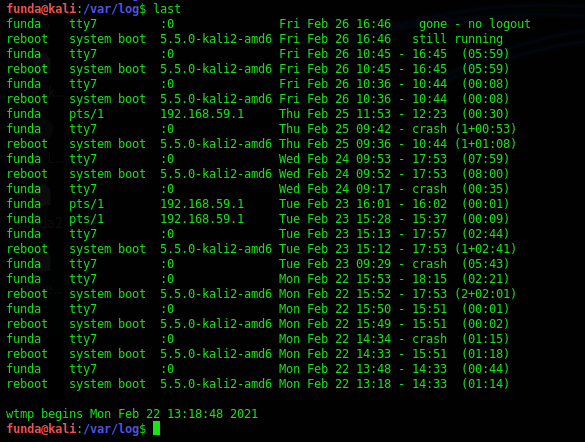
var/run içindeki who komutu sistemin son başlatılmasında hangi kullanıcının aktif olduğunu ve ne zaman aktif olduğunu görüntülemekteyiz. Ayrıca hangi id aldığını da görmekteyiz.



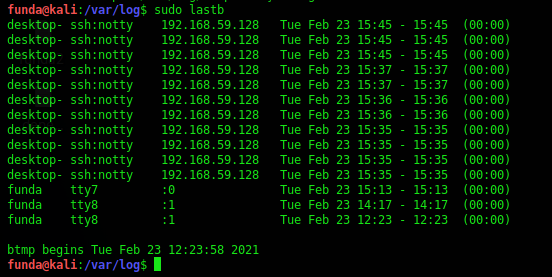
Utmp şuandaki bağlanan kullanıcılar hakkında bilgi verirken wtmp ise daha önce bağlanmış kullanıcılar hakkında bilgi vermektedir.



Last hem geçmişte hemde şuanda kayıtlı ola kullanıcıları listeler.



Bad logların listesini lastb komutu ile bakarız.



Syslog ağ üzerinden gelen TCP UDP portlarını dinleyenilen bir C kütüphanesidir.

Ryslog ise ip bazlı kısaltmalar ile herhangi bir bilgiyi log dosyasını istediğimiz bir log dosyasına yönlendirebiliriz.