

PawnSec Security Solutions Academy

İçerik

1	Temel KaliLinux Eğitimi: Genel Kurs Bilgisi:	3
1.1	PawnSec Security Solutions Academy Kurs Materyalleri	3
1.2	PawnSec Security Solutions Academy Canlı Destek	3
1.3	PawnSec Security Solutions Academy Test Ortamı Erişimleri	3
2	Kurs Yaklaşımı için Genel Stratejiler	4
2.1	Kurs Materyalleri	4
2.2	Kurs Egzersizleri	4
2.3	Destek Sistemi	5
3	KaliLinux Dosya Sistemi ve İlgili Sözcük Havuzu	5
3.1	KaliLinux Dosya Türleri	7
3.2	Linux Terimleri	8
4	KaliLinux Shell Kullanımı ve Komutlar	9
4.1	KaliLinux Komut Çeşitleri	9
4.2	Bash, Environment ve Shell Değişkenleri	22
4.3	Dosyalarda Kullanılan Komutlar	23
4.3.1	Dosyalarda Filtreleme Komutları	24
4.3.2	Dosya Arama Komutları	28
4.3.3	Hardlink ve Softlink Kavramları	29
5	İşletim Sistemi Bağlantı Tipleri	29
5.1	Sistem Kullanıcılarıyla İlgili Komutlar	30
5.2	Servis Kontrolü	31
6	SSH Servisi	32
7	KaliLinux Dosya Sisteminde Yetki Yönetimi	35
7.1	Kullanıcıların İzinlerini Değiştirme	36
7.2	Kullanıcıların ve Grupların Yönetimi	38
7.2.1	Kullanıcıların Yönetimi	38
7.2.2	Kullanıcı Yönetim Komutları	40
7.2.3	Grupların Yönetim Komutları	43
7.2.4	Sudo Komutu ve Sudoers Dosyası	44
8	İşlemlerin Yönetimi	46
8.1	Foreground ve Backgorund İşlemler	48
8.2	İşlem Önceliğini Ayarlama ve İşlem Sonlandırma Komutları	48
9	Sistem Performansının Görüntülenmesi	49

10 KaliLinux Zaman Senkronizasyonu	55
10.1 Ntp Kavramı	55
10.2 KaliLinux Zaman Senkronizasyonu Komutları	55
10.2.1 Chrony Kullanımı	57
11 KaliLinux Yazılım Yönetimi	59
11.1 Kaynak Üzerinden Yazılım Yükleme	60
11.2 Kaynaktan Yazılım Yükleme Araçları	61
11.3 Sıkıştırılmış Dosyalarla Kurulum Yapma	62
11.4 Mirror(ayna) Terimi	63
12 Boot (Ön Yükleme) İşleminin Yönetimi	63
12.1 MBR ve GPT Nedir?	64
12.2 GRUB2 Nedir?	64
12.3 Systemd Nedir?	65
12.3.1 Service Unit	68
12.4 Recovery Mode	70
13 KaliLinux Kernel Yönetimi	71
13.1 Kernel Modüllerini Yönetme	71
13.2 Kernel Modüllerini Düzenlenmesi	74
13.3 Kernel Sürümünü Öğrenme	74
13.4 Kernel Sürümünü Güncelleme	75
13.5 Eski Kernel Sürümlerinin Kaldırılması	76
13.6 Kernel Downgrade	78
13.7 Sistem Yönetim Komutları	78

PawnSec Security Solutions Academy

TKE v1.0

1 Temel KaliLinux Eğitimi: Genel Kurs Bilgisi:

KaliLinux kullanımıyla ilgili temel bilgileri içeren (PawnSec Security Solutions Academy) kursuna hoş geldiniz!

KaliLinux işletim sisteminin kullanımına ilişkin geniş bilgi havuzuna sahip bu eğitimde sizlere terminal kullanımı, dosya-yazılım tipleri, hostlar, donanımlar ve daha birçok şey hakkında bilgilendirmede bulunacağız. Bu kurs paketimizi bitirdikten sonra KaliLinux işletim sistemini kolaylıkla kullanabilir hale gelmeniz ve aklınızdaki sorulara cevaplar bulabilmeniz en temel önceliğimizdir.

Bu kursumuzda ilk olarak kavramlara deðinerek ardından komutlar hakkında bilgi sahibi olup KaliLinux Kernel, modüller, BIOS, network, aygit yöneticileri ve dahası hakkında bilgilere kolaylıkla erişebilirsiniz.

1.1 PawnSec Security Solutions Academy Kurs Materyalleri

Kurs, çevrimiçi kitap modüllerini ve eşlik eden kurs videolarını içerir. Kitap modüllerinde ve videolarda ele alınan bilgiler örtüşmektedir, yani kitap modüllerini okuyabilir ve ardından videoları izleyerek herhangi bir boşluğu doldurabilirsiniz veya tersini yapabilirsiniz. Bazı durumlarda, kitap modülleri videolardan daha detaylıdır. Diğer durumlarda, videolar kitap modüllerindeki bazı bilgileri daha iyi iletебilir. Her ikisine de dikkatlice dikkat etmeniz önemlidir. Kitap modülleri ayrıca çeşitli egzersizler içerir.

1.2 PawnSec Security Solutions Academy Canlı Destek

PawnSec Security Solutions Academy Kütüphanesi'nin sağ üst köşesindeki "Discord'a Baðlan" düğmesine tıklayarak erişilebilir. Canlı Destek, öğrenci yöneticilerimizle doğrudan iletişim kurmanıza olanak tanır.

Öğrenci yöneticileri, teknik konularda yardımcı olmak için mevcuttur, ancak kurs materyalleri ve egzersizlerdeki maddeleri de açıklığa kavuþturabilirler. Ayrıca, bir lab makinesinde tamamen takılı kaldıysanız ve elinizden gelenin en iyisini yaptıysanız, Öğrenci Yöneticileri yolunuza yardımcı olacak küçük bir ipucu verebilirler.

1.3 PawnSec Security Solutions Academy Test Ortamı Erişimleri

Bu kısım ilgili lab'ler eklendikten sonra güncellenecektir.

2 Kurs Yaklaşımı için Genel Stratejiler

Her öğrenci benzersizdir, bu nedenle kursa ve materyallere yaklaşmak için mutlak en iyi yol yoktur. Kendi rahat hızınızda kursu tamamlamanızı teşvik etmek istiyoruz. Kendinizi takip etmek için zaman yönetimi becerilerini uygulamanız da gerekecektir.

Aşağıdaki yaklaşımı kurs materyallerine genel bir yaklaşım olarak öneriyoruz:

- Kayıt işlemi sonrasında sağlanan kaynaklarda bulunan tüm bilgileri inceleyin.
- Kurs materyallerini inceleyin.
- Tüm kurs egzersizlerini tamamlayın.

2.1 Kurs Materyalleri

Yukarıdaki bilgileri inceledikten sonra, kurs materyallerine atlayabilirsiniz. Ders videoları ile başlamayı tercih edebilirsiniz ve sonra kitap modülleri içinde verilen o konu hakkındaki bilgileri gözden geçirebilirsiniz veya tam tersi, tercih ettiğiniz öğrenme tarzına bağlı olarak. Kurs materyallerini ilerlerken, konuları tam olarak anlamak için bazı modüller tekrar izlemeniz veya okumanız gerekebilir.

Kursu bir maraton olarak ve bir sprint olarak değil ele almanızı öneririz. Zor kavramlarla daha fazla zaman geçirmekten çekinmeyin ve ardından kursa devam etmeden önce tam olarak anladığınızdan emin olun.

2.2 Kurs Egzersizleri

Bir sonraki modüle geçmeden önce, her modülün sonundaki egzersizleri tamamlamanızı öneririz. Bu, materyali anlamınızı test edecek ve ilerlemeye olan güveninizi artıracaktır.

Bu egzersizleri tamamlamak için gereken zaman ve çaba, mevcut beceri setinize bağlı olarak değişebilir. Bazı egzersizler zor olabilir ve önemli bir zaman alabilir. Özellikle daha zor egzersizlerde ısrarcı olmanızı teşvik etmek istiyoruz. Bu egzersizler, PawnSec Security Solutions "Ne kadar uykusuz kalmak o kadar bilgi zenginliği" zihniyetinin geliştirilmesinde özellikle faydalıdır.

2.3 Destek Sistemi

PawnSec Security Solutions İSK KK, sabit bir tempolu bir kurs değildir. Bu, zorlandığınız konular için ekstra zaman harcayarak kendi hızınızda ilerleyebileceğiniz anlamına gelir. Bu kursun hızından yararlanın ve yeni ve zor bir konu veya yöntemle uğraşmak için biraz daha fazla zaman harcamaktan çekinmeyin. Kendinizce bir şeyle keşfetmenin hiçbir duygusu yoktur!

Ayrıca, konuya ilgili daha derinlemesine araştırma yaparak kendinizin de öğrenme yolculuğunu sürdürdüğünüzü umuyoruz.

Sorularınızın bir kısmının cevabını alma olasılığınızın yüksek olduğu Help Center’ımıza (yardım merkezi) bakmanızı öneririz.

- <https://www.pawnsec.com/iletisim/>

İhtiyacınız olan yardım bulamazsanız, destek sayfasındaki Canlı Destek veya e-posta (info@pawnsec.com) aracılığıyla Öğrenci Yöneticilerimizle iletişime geçebilir.

3 KaliLinux Dosya Sistemi ve İlgili Sözcük Havuzu

KaliLinux eğitimimize başlamadan önce dizinler, bazı dosya türleri, bu dosyalara nasıl erişebileceğimiz ve dosya işlevleri ile ilgili biraz bilgi edinelim. Linux Filesystem Hierarchy Standard (FHS)^[1]’na göre adından da anlaşılacağı üzere root dizini altında hiyerarşik bir düzene sahiptir. Bir Linux terminalinden istediğiniz dosyaya erişmek istiyorsanız dizinleri bilmeniz gereklidir. [1] [2]

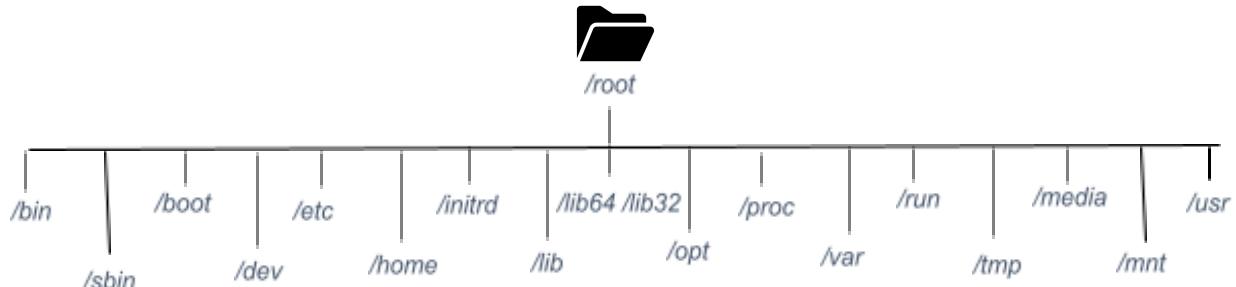
- **/bin:** Bu dizin hem sistem yönetici hem de root olmayan kullanıcılar için yararlı olan birkaç komut içerir. Bu komutlara örnek verecek olursak **cp**, **mv**, **rm**, **cat**, **ls** gibi yaygın olarak kullanılan komutları içerir. Aynı zamanda **bash**, **csh** gibi dosyaların bulunduğu dizindir. Bu dizin mevcut olması gereken temel sistem programlarını içерdiği için büyük önem arz etmektedir. Sistem önyükleme (boot) yaptığında ilk önce bu dizin çalışır.
- **/sbin:** Sistemdeki root kullanıcı tarafından kullanılan bakım ve yönetim işlemlerini gerçekleştiren **ifconfig**, **fdisk**, **iptables**, **reboot** gibi komutların dosyalarını barındırır.
- **/boot:** Bu dizin işletim sistemimizin başlatılmasını sağlar. Önyükleme yaparak sistemin başlatılması bu evrede gerçekleşir ve bilgisayar başlatılırken kullanılması gereken dosyaları barındırır.
- **/dev:** Özel sistem dosyalarını ve aygit dosyalarının bulunduğu dizindir. Örneğin; **/dev/cdrom**, **/dev/fd0**, **/dev/dsp** sırasıyla CD-ROM sürücünüzü, disket sürücünüzü ve ses aygıtlarını temsil eder. Bunlar dışında USB girişleri, portları, depolama aygıtlarını da bu dizin aracılığıyla erişim sağlayabilirsiniz.
- **/etc:** Bu dizin ve bu dizinin altındaki dizinler sistemle ilgili tüm yapılandırma dosyalarını içerir. Bir programın çalışmasını kontrol etmek için kullanılan yerel dosya olarak tanımlanan bu yapılandırma dosyalarını yedeklemek sizin sonradan oluşacak olan yeniden yapılandırma işleminden kurtaracaktır.

[1]: <https://www.debian.org/releases/stable/amd64/apcs02.en.html>

[2]: https://tldp.org/LDP/intro-linux/html/sect_03_01.html

- **/home:** Çok kullanıcılı yapıya sahip olan Linux işletim sisteminde, her kullanıcıya yalnızca kendileri ve sistem yönetici tarafından erişilebilen belirli bir dizin atanır. Bu klasörde de o işletim sistemi kullanıcılarına ait kişisel verileri, uygulama ayarları, tercihleri bu kaydedilmektedir.
- **/initrd:** Açılmı “initial ramdisk” olan bu klasör boot aşamasındaki çekirdek (Kernel) yüklenikten sonra RAM diskin yüklenmesini ve işletim sisteminin yüklenmesini sağlayan dizindir.
- **/lib:** Çekirdek modüllerini ve paylaşılan kütüphane dosyalarını içerir. Bu kütüphane dosyaları, sistemi başlatmak, /bin ve /sbin komutlarının çalışmasını sağlar. Bu kütüphane dosyaları “.so” uzantısına sahiptir.
- **/lib64 /lib32:** Günümüzde hala bazı uygulamalar 32-bit desteklediği için bazen 64-bit’ten 32 ye geçmemiz gerekebiliyor. /lib64 ve /lib32 bu tür dosyaların uyumluluğunu sağlamada bizlere yardımcı oluyor.
- **/opt:** Sistem dosyalarından bağımsız, 3. parti uygulamaları yüklerken eğer yükleneceği yeri değiştirmezseniz varsayılan olarak kurulacağı dosya dizini /opt olacaktır. Windows işletim sisteminde uygulama yüklerken sıkça karşılaşığınız “C:\Windows\Program Files\” dizini olarak da düşünülebilir.
- **/proc:** Çekirdeğin kontrol ve bilgi merkezi olarak kabul edilen “sanal” dosya sistemidir. Sistemde çalışan işlemler, bağlı aygıtlar, sistem belleği vb. gibi uygulamaların çalışması için gerekli olan bilgileri barındırır. Sistem hakkında bilgi edinebileceğiniz gibi sistem ayarlamalarını da buradan gerçekleştirebilirsiniz.
- **/root:** Bu dizin ise sistem yöneticisinin ana dizinidir. /home/kullanıcı_adı normal bir kullanıcının dizini olurken root kullanıcısının dizini /root şeklindedir. En yetkili kullanıcı olarak “kök kullanıcı (root)” olmasın
- **/var:** Sisteme ait log’ların, e-posta ve yazıcı gibi dinamik olarak boyutu değişen dosyaları içerir.
- **/run:** Bu dizin, sistemin en son yapılan boot işleminden itibaren elde edilen sistem bilgisi verilerini içerir. Bu bilgiler, boot işlemine özel olup her boot işleminin başlangıcında sıfırlanmaktadır.
- **/tmp:** Açılmı “temporary” olup adından da anlaşılacağı üzere geçici dosyaların bulunduğu yerdır. Boot sırasında bu alandaki dosyalar silinir.
- **/media:** Çıkarılabilir aygıtların (USB bellek, SD kart, CD vb.) ve sistem başlangıcında bağlanmayan sabit disk bölümlerinin bağlanma noktasıdır.
- **/mnt:** Genel donanımsal bağlantı noktasını olarak da geçmektedir. Bu dizin genellikle disketinizi (işletim sisteminin kurulu olduğu disk bölümü hariç) ve CD’nizi bağladığınız bağlama noktalarını ve alt dizinleri içerir.

- **/usr:** İşletim sistemi aracılığıyla ya da paket yönetim sistemlerini kullanarak yüklediğiniz kurmuş olduğunuz her programlara ait pek çok dosya bu dizine kaydedilir. Kurmuş olduğunuz bu programların kullanması gereken kütüphane dosyaları da bu dizin altında bulunur.



Şema SEQ Figure * ARABIC 1 KaliLinux Dizinleri

3.1 KaliLinux Dosya Türleri

KaliLinux'un dosya sisteminde birden fazla dosya tipiyle karşılaşabilirsiniz. Bu dosyalara hepsine erişmek için "ls -lah" komutunu terminalimize girebiliriz. Bunun sonucunda ortaya çıkacak olan çıktıların başındaki harf ya da simbol bize dosya tipini göstermektedir. [1] [2]

```

(kali㉿PawnSecSecuritySolutions)-[~]
$ ls -lah
total 148K
drwxr-xr-x 15 kali kali 4.0K Mar 13 06:07 .
drwxr-xr-x  3 root root 4.0K Dec  5 08:43 ..
-rw-r--r--  1 kali kali 220 Dec  5 08:43 .bash_logout
-rw-r--r--  1 kali kali 5.5K Dec  5 08:43 .bashrc
-rw-r--r--  1 kali kali 3.5K Dec  5 08:43 .bashrc.original
drwxr-xr-x  6 kali kali 4.0K Mar  9 02:18 .cache
drwxr-xr-x 11 kali kali 4.0K Mar  5 08:26 .config
drwxr-xr-x  2 kali kali 4.0K Mar  5 08:25 Desktop
-rw-r--r--  1 kali kali   35 Mar  5 08:35 .dmrc
drwxr-xr-x  2 kali kali 4.0K Mar  5 08:25 Documents
drwxr-xr-x  2 kali kali 4.0K Mar  5 08:25 Downloads
-rw-r--r--  1 kali kali 12K Dec  5 08:43 .face
lrwxrwxrwx  1 kali kali     5 Dec  5 08:43 .face.icon → .face

```

Şekil 1 "ls -lah" Komut Çıktısı

Şekil 1'de kırmızı dikdörtgen içerisinde gösterilen simbol ve harfler o dosyanın tipini açıkça belirtmektedir. Peki bu dosya tipleri nelerdir? Bu dosya tipleri:

- **-:** Regular File
Türkçe çevirisi “Normal Dosya” olup KaliLinux sisteminde en yaygın bulunan dosya tipidir. Metin dosyaları, resimler gibi birçok dosyayı yönetir.
- **d:** Directory
KaliLinux'da en çok bulunan ikinci dosya tipi olan directory bize dizinleri gösterir.

[1]: <https://www.debian.org/releases/stable/amd64/apcs02.en.html>

[2]: https://tldp.org/LDP/intro-linux/html/sect_03_01.html

- **c:** Character Device File
Bu dosya türü adından da anlaşılacığı üzere donanım aygıtlarıyla kullanıcıların ve programların birbiriyle iletişim kurmasını sağlar.
- **b:** Block Device File
Depolama aygıtları için kullanılan dosya tipidir
- **s:** Local Socket File
Syslog gibi hizmetleri kullanarak sistemde yapılan işlemler arasındaki iletişimini kurmak için kullanılır.
- **p:** Named Pipe
İki local işlem arasında iletişime olanak sağlar.
- **l:** Symbolic Link
Bir dizin veya dosyaya daha kısa şekilde ulaşmamızı sağlayan kısayolları oluşturur.

3.2 Linux Terimleri

Şimdi bazı dosya türleri ve dizinleri öğrendiğimize göre komutlara geçmeden önce Linux işletim sistemini kullanırken karşılaşabileceğiniz kelimelere göz atalım.

Background Process: Kullanıcı girişi gerektirmeyen, arka planda çalışan programlardır.

Foreground Process: Kullanıcının anlık olarak kullanmış olduğu programlardır.

Bash: Açılmış Bourne-Again Shell olan komut dili yorumlayıcısıdır.

Archive: ZIP, RAR gibi sıkıştırılmış dosyaları barındırarak depolama alanının daha verimli kullanılmasına olanak sağlayan büyük bir dosyadır.

Binaries: Programların çalışması için düzenlenmiş kaynak kodlarıdır.

Cron: Linux arka planında çalışan, belirlediğiniz görevleri belirlenen zaman aralığında gerçekleştiren programdır.

Dpkg (Debian Paket Yöneticisi): Linux dağıtımlarıyla uyumlu çalışan, internet üzerinden paket yüklemenizi sağlayan araçtır.

File System: Bir işletim sisteminin içeriğine, başka bir depolama ortamının nasıl erişip yorumlayacağını söyleyen bir dizi programdır.

Kernel: İşletim sisteminin çekirdeği olarak da bilinen Kernel, işletim sistemindeki her şeyin üzerinde denetimi olan, bütün kaynakların yönetimini sağlayan merkezi bir bileşendir.

Log: Sistemde meydana gelen hataları, sorunlar, işlemler, değişiklikler gibi bilgilerin kayıt altına alındığı yerdir.

Shell: Sisteme, komutlar ile müdahale edilmesine izin veren komut satırı yorumlayıcısıdır.

Shell Script: Otomatik olarak çalışan komutları içeren komut dosyasıdır.

SuperUser: Root kullanıcısı ile aynı yetkiye sahip kullanıcıdır.

Syslog: Standart bir günlük kaydı aracıdır. Çekirdek dahil olmak üzere çeşitli program ve servislerin mesajlarını toplar ve saklar.

Port: Cihazlar arasındaki iletişimini sağlayan başlangıç ve bitiş noktaları arasındaki sanal köprüye denir.

FTP (File Transfer Protocol): Bir cihazdan başka bir cihaza dosya aktarmak için kullanılan protokoldür.

Swap: Sistem daha fazla bellek kaynağına ihtiyaç duyarsa verileri geçici olarak RAM'dan disk'e veya disk'ten RAM'a taşımaya yarayan sanal hafızadır.

4 KaliLinux Shell Kullanımı ve Komutlar

Linux işletim sistemi çok kullanıcılı bir yapıya sahip olduğu için her bir kullanıcının sistemde bulunan kaynaklara erişmesini sağlayacak şekilde tasarlanmıştır. Bilindiği üzere Linux işletim sistemi kullanmanın temeli **shell'dır**. Herhangi bir kullanıcı sisteme giriş yaptıktan sonra sistemin açılma sırasında okuduğu dosyalara göre bir ortam oluşur. Kullanıcının kullanmış olduğu bu ortam **global** ve **personal** olmak üzere ikiye ayrılır. Tüm kullanıcılar uygulanan global yapılandırma dosyaları “/etc/profile” ve “/etc/bashrc” alt dizinleri içerisinde bulunurken belirli bir kullanıcı ortamı ise (personal) kullanıcının home dizinindeki “.profile” ve “.bashrc” dosyaları okunarak oluşturulur. [3]

Interactive ve Non-Interactive Shell nedir?

Kullanıcı sisteme giriş yaparken “/etc/passwd” içerisinde bulunan kullanıcı kimlik bilgileri doğrulanır ve ardından “/etc/profile” dosyası okunarak başlatılan shell’e **interactive shell** denir. Kullanıcı bu kabuk ile etkileşime girebilir. **Non-Interactive shell** ise kullanıcı girişini gerektirmeyen herhangi bir komut ya da script çalıştığında çağrılan kabuktur.

4.1 KaliLinux Komut Çeşitleri

Eğer kodlama hakkında bilgi sahibiyseniz bildığınız üzere bir programın çalışması için yazdığımız komutların yürütülebileceği bir ortama ihtiyaç duymaktayız. Linux işletim sisteminde shell bizim yazmış olduğumuz komutların yorumlanarak yürütülmesini sağlar. Bu işlemleri gerçekleştirmek için üç farklı komut çeşidi kullanır. Bunları sırasıyla açıklayacak olursak;

1 Alias

İşletim sisteminin mevcut kullanıcı tarafından oluşturulan komutlara denir. Örneğin; Shell kullanırken “clear” komutunu kullanmanız **Shell'in temizlenmesini** sağlayan bir komuttur. Siz “alias c=clear” komutunu Shell ekranına girerseniz artık her “c” komutunu girdiğinizde “clear” komutunun işlevi gerçekleşecektir.

Yaptığınız spesifik bir Alias atamasını kaldırmak isterseniz “**unalias [atama ismi]**” komutunu kullanabilirsiniz. Örneğin; atamış olduğumuz “c” komutunu kaldırmak istiyorsak “**unalias c**” yazmamız yeterli olacaktır. Eğer oluşturduğunuz tüm komutları kaldırmak istiyorsanız “**unalias -a**” komutunu kullanabilirsiniz.

[3]: https://wiki.debian.org/ShellCommands#Command-line_applications

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$alias c=clear
        └──(kali㉿PawnSecSecuritySolutions)-[~]
            └─$unalias -a
                └──(kali㉿PawnSecSecuritySolutions)-[~]
                    └─$c
                        c: command not found
```

Betik 1'de görüleceği üzere Alias komutu kaldırıldığı zaman karşılaşacağımız görüntü şekildeki gibi olacaktır.

Aynı zamanda sistemimizdeki paketlerin güncel versiyonlarının bulunması ve yüklenmesini sağlayan “**sudo apt update && sudo apt full-upgrade**” komutunu uzun uzun yazmak yerine “**alias upd='sudo apt update && sudo apt full-upgrade'**” yazarak işlemi daha kısa sürede gerçekleştirebilirsiniz.

2 Internal Komutlar

Shell'e ait, bash içerisinde yerleştirilmiş, işlevsel komutlara denilir.

3 External Komutlar

Sistemimizdeki alt dizinlerde bulunan, kodlar veya script'ler barındıran programlardır. Shell'e girmiş olduğumuz External Komutlar Shell tarafından PATH değişkeni üzerinde aranır. Eğer böyle bir komut mevcutsa komut çalıştırılır. Peki PATH nedir?

PATH: Her işletim sisteminin kendine özgü olarak kullandığı çevre değişkenine PATH denir. PATH sayesinde işletim sisteminde bulunan her dosyanın, komutun konumu belirlidir ve bu sayede komutlar eşsiz bir şekilde yürütülür.

type

Eğer bir komutun çeşidini öğrenmek istiyorsanız “**type [komut ismi]**” komutunu Shell'e girerek öğrenebilirsiniz.

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$ type mkdir
mkdir is /usr/bin/mkdir
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$ type alias
alias is a shell builtin
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$ type c
c is an alias for clear
```

Betik SEQ Betik * ARABIC 2 "type" Komutunun Kullanımı

Bu komut sayesinde çıkan sonuçlara baktığımızda “**mkdir**” komutunun bir External Komut olduğunu “**alias**” komutunun ise bash içerisinde yerleştirilmiş Internal komut olduğunu anlıyoruz. “**c**” komutunun ise alias komutu olarak atandığı sonucuna varabiliriz.

which

Herhangi bir komutun çalıştığı zaman PATH’e ait konumunu elde etmek istersek kullanacağımız komut “**which [komut ismi]**” şeklinde olacaktır.

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$ which sudo
/usr/bin/sudo
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$ which c
c is an alias for clear
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$ which ls
ls: aliased to ls --color=auto
```

Betik SEQ Betik * ARABIC 3 "which" Komutunun Kullanımı

Betik 3’té de belirtildiği üzere “**which sudo**” komutu ile External Komut olan “**sudo**” komutunun PATH’deki yerinin “**/usr/bin/sudo**” olduğunu görebiliyoruz. “**c**” komutunun kullanıcı tarafından oluşturulmuş Alias Komutu olduğunu, “**ls**” komutunun ise sistem tarafından oluşturulmuş bir Alias Komutu olduğu anlaşılıyor.

man

Açılımı manual olup komutlar hakkında bilgiler içeren bir çeşit kılavuzdur. “**man [komut ismi]**” komutunu kullanarak istediğimiz bir komutun kullanımı, komutla birlikte kullanabileceğiniz işlevsel değişkenleri ve bunları kullandığınızda elde edeceğiniz sonuçlar hakkında bilgi edinebiliriz.

```
clear(1)                               General Commands Manual      clear(1)
                                         Trash
NAME
  clear - clear the terminal screen

SYNOPSIS
  clear [-Ttype] [-V] [-x]

DESCRIPTION
  clear clears your terminal's screen if this is possible, including
  the terminal's scrollback buffer (if the extended "E3" capability is
  defined). clear looks in the environment for the terminal type
  given by the environment variable TERM, and then in the terminfo
  database to determine how to clear the screen.

  clear writes to the standard output. You can redirect the standard
  output to a file (which prevents clear from actually clearing the
  screen), and later cat the file to the screen, clearing it at that
  point.

OPTIONS
  -T type
    indicates the type of terminal. Normally this option is unnec-
    essary, because the default is taken from the environment vari-
    able TERM. If -T is specified, then the shell variables LINES
    and COLUMNS will also be ignored.

  -V reports the version of ncurses which was used in this program,
  and exits. The options are as follows:

  -x do not attempt to clear the terminal's scrollback buffer using
  the extended "E3" capability.

HISTORY
  A clear command appeared in 2.79BSD dated February 24, 1979. Later
  that was provided in Unix 8th edition (1985).

  AT&T adapted a different BSD program (tset) to make a new command
  (tput), and used this to replace the clear command with a shell
  script which calls tput clear, e.g.,

  /usr/bin/tput ${1:+-T$1} clear 2> /dev/null
  exit

  In 1989, when Keith Bostic revised the BSD tput command to make it
  similar to the AT&T tput, he added a shell script for the clear com-
  mand:

  exec tput clear

  The remainder of the script in each case is a copyright notice.

Manual page clear(1) line 1 (press h for help or q to quit)
```

Şekil 2 "man clear" Komut Çıktısı

info

“man” komutu gibi bu komut da size komutlar ve değişkenler hakkında bilgi verir. “man” komutunun yetersiz olduğu yerlerde bu komutu kullanarak aradığınız bilgiye ulaşabilirsiniz. “info [komut ismi]” komutunu kullanmanız bu işlem için yeterli olacaktır.

```
SUDO(8)          BSD System Manager's Manual          SUDO(8)

NAME
    sudo, sudoedit – execute a command as another user

SYNOPSIS
    sudo -h | -K | -k | -V
    sudo -v [-ABknS] [-g group] [-h host] [-p prompt] [-u user]
    sudo -l [-ABknS] [-g group] [-h host] [-p prompt] [-U user] [-u user]
        [command]
    sudo [-ABbEHnPS] [-C num] [-D directory] [-g group] [-h host]
        [-p prompt] [-R directory] [-r role] [-t type] [-T timeout]
        [-u user] [VAR=value] [-i | -s] [command]
    sudoedit [-ABknS] [-C num] [-D directory] [-g group] [-h host]
        [-p prompt] [-R directory] [-r role] [-t type] [-T timeout]
        [-u user] file ...

DESCRIPTION
    sudo allows a permitted user to execute a command as the superuser or
    another user, as specified by the security policy. The invoking
    user's real (not effective) user-ID is used to determine the user name
    with which to query the security policy.

    sudo supports a plugin architecture for security policies, auditing,
    and input/output logging. Third parties can develop and distribute
    their own plugins to work seamlessly with the sudo front-end. The de-
    fault security policy is sudoers, which is configured via the file
    /etc/sudoers, or via LDAP. See the Plugins section for more informa-
    tion.

    The security policy determines what privileges, if any, a user has to
    run sudo. The policy may require that users authenticate themselves
    with a password or another authentication mechanism. If authentica-
    tion is required, sudo will exit if the user's password is not entered
    within a configurable time limit. This limit is policy-specific; the
    default password prompt timeout for the sudoers security policy is 0
    minutes.

    Security policies may support credential caching to allow the user to
    run sudo again for a period of time without requiring authentication.
    By default, the sudoers policy caches credentials on a per-terminal
    basis for 15 minutes. See the timestamp_type and timestamp_timeout
    options in sudoers\(5\) for more information. By running sudo with the
    -v option, a user can update the cached credentials without running a
    command.

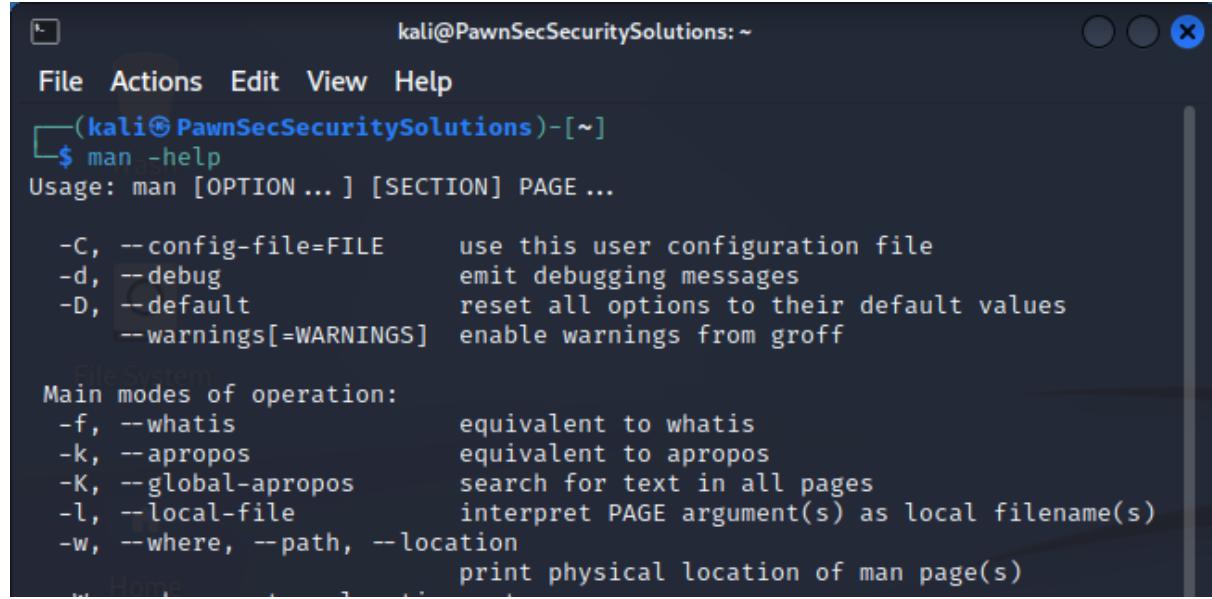
    On systems where sudo is the primary method of gaining superuser priv-
    ileges, it is imperative to avoid syntax errors in the security policy
    configuration files. For the default security policy, sudoers\(5\),
    changes to the configuration files should be made using the visudo\(8\)
    utility which will ensure that no syntax errors are introduced.

Info: (*manpages*)sudo, 794 lines --Top--
No menu item 'sudo' in node '(dir)Top'
```

Şekil 3 "info sudo" Komut Çıktısı

help

“man” ve “info” gibi uzun bilgiler içeren kılavuzlar yerine kısa bilgiler içeren “help” komutuyla da komutlarla ilgili bilgiler edinebilirsiniz. “[komut adı] -help” şeklinde kullanabilirsiniz.



A terminal window titled "kali@PawnSecSecuritySolutions: ~". The window shows the output of the "man -help" command. The output includes usage information, configuration options, and main modes of operation for the man command.

```
kali@PawnSecSecuritySolutions: ~
File Actions Edit View Help
└──(kali㉿PawnSecSecuritySolutions)-[~]
$ man -help
Usage: man [OPTION ...] [SECTION] PAGE ...
-C, --config-file=FILE      use this user configuration file
-d, --debug                 emit debugging messages
-D, --default               reset all options to their default values
--warnings[=WARNINGS]       enable warnings from groff

Main modes of operation:
-f, --whatis                equivalent to whatis
-k, --apropos                equivalent to apropos
-K, --global-apropos         search for text in all pages
-l, --local-file              interpret PAGE argument(s) as local filename(s)
-w, --where, --path, --location
                             print physical location of man page(s)
```

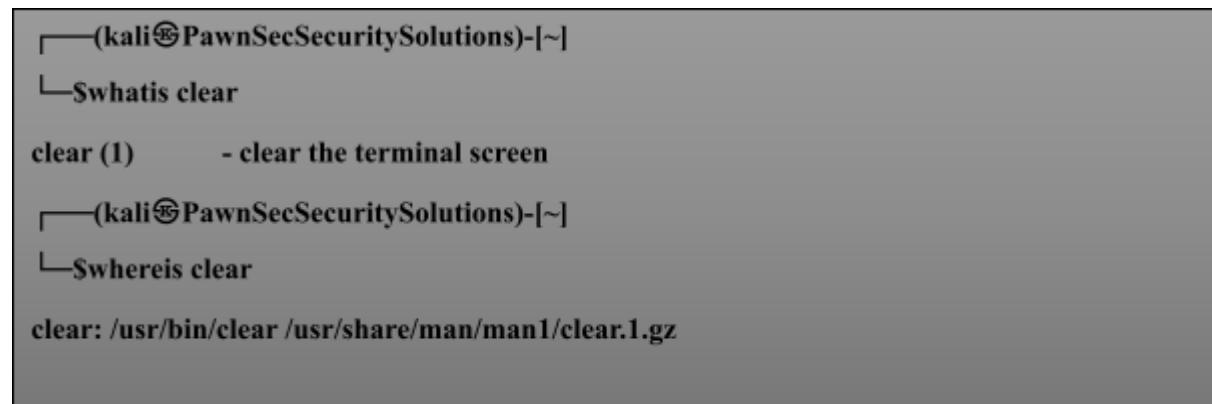
Şekil 4 "man -help" Komut Çıktısı

tab (Klavye Tuşu)

Shell kullanırken bazen kullanacağımız dizinlerin, klasörlerin veya komutların isimleri beklediğimizden uzun olabilmektedir. Bu tür durumlarda klasörün, dizinin ya da komutun ilk birkaç harfini yazdıktan sonra klavyedeki tab tuşuna basmak kullanmak istediğiniz şeyin otomatik olarak tamamlanmasını sağlayacaktır. Aynı zamanda 4 adet space tuşu yerine kullanımı da mevcuttur.

whereis/whatis

“whatis” komutu ile herhangi bir komuta ait kısa bilgi alabilirsiniz.”whereis” komutu ise komutun hangi alt dizinde bulunduğu gösterir. “whatis [komut adı]” ve “whereis [komut adı]” şeklinde kullanımını gerçekleştirebilirsiniz.



A terminal window titled "kali@PawnSecSecuritySolutions: ~". The window shows the output of the "whatis clear" and "whereis clear" commands. The "whatis" command shows the man page for "clear", and the "whereis" command shows the path to the "clear" binary.

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
$ whatis clear
clear (1)      - clear the terminal screen

└──(kali㉿PawnSecSecuritySolutions)-[~]
$ whereis clear
clear: /usr/bin/clear /usr/share/man/man1/clear.1.gz
```

pwd

Anlık olarak bulunduğuuz dizini gösterir.

```
└─(kali㉿PawnSecSecuritySolutions)-[~/Documents]
  └─$pwd
  /home/kali/Documents
```

ls

Bu komut sayesinde içerisinde bulunduğuuz dizinin içeriklerine erişebiliyoruz. Bu komutun yanına parametreler ekleyerek girdiğimiz parametreye bağlı olarak farklı sonuçlar elde edebiliyoruz.

```
└─(kali㉿PawnSecSecuritySolutions)-[~]
  └─$pwd
  /home/kali
  └─(kali㉿PawnSecSecuritySolutions)-[~]
    └─$ls
    Desktop Documents Downloads Music Pictures Public Templates Videos
```

Betik 6'da görüldüğü üzere “pwd” komutu ile “/home/kali” içerisinde bulunduğuuzu ardından yazmış olduğumuz “ls” komutuyla bu dizinin içerisinde bulunan dökümanları görebiliyoruz. Ayrıca bu komutla birlikte kullanabileceğiniz bazı parametreler;

- **ls -l:** “-l” parametresini kullanarak dizin içeriği hakkında dosya izinleri, dosya boyutu, oluşturulma tarihi gibi daha ayrıntılı bilgileri edinebiliriz. Aynı zamanda dosyaların alfabetik olarak sıralanması görevinde de rol oynar.
- **ls -a:** “-a” parametresini kullanarak dizinimizde gizli dosyalar bulunuyorsa bunları da görebilmemizi sağlar. Ayrıca “ls -la” , “ls- al” veya “ls -a -l” gibi -l ve -a parametrelerini birlikte kullanarak daha düzenli sonuçlar elde edebiliriz.
- **ls -A:** “-A” parametresini kullanarak “-a” parametresinde de olduğu gibi gizli dosyaların gösterilmesini sağlar. Farklı olarak “..” ve “.” dosyalarını göstermez. “..” dosyası “geçerli dizin”, “..” ise “ana dizin” (bir dizin yukarı) gösterir.
- **ls -h:** Dosyaların boyutları hakkında bilgileri gösterir. Böylelikle dosyanın kaç KB, MB, GB olduğuna erişebilirsiniz.
- **ls -S:** “-l” parametresi gibi sıralama işlevi görür. Dosyaların boyutlarına göre sıralanmasını sağlar.
- **ls -t:** “-l” ve “-S” parametreleri gibi sıralama işlevi görür. Dosyaların değiştirilme tarihine göre sıralanmasını sağlar.

- **ls -r:** “-l” parametresinin tersi işlevini görerek dosyaların alfabetik olarak tersten gösterilmesini sağlar. Örneğin; “ls -Sl” kullanarak dosyaları büyükten küçüğe sıralarken “ls -Slr” ile dosyaları küçükten büyüğe doğru sıralayabiliriz.

cd

Açılımı “change directory” olan bu komut sayesinde komutlar arasında gezinebiliyoruz. Komutu uygulamak için “cd [dizin adı]” yazarak bir dizinden bir başkasına geçiş yapabilirsiniz. Sadece “cd” yazarak ise giriş yapmış olduğumuz kullanıcının “/home” dizinine dönebilirsiniz.

```
(kali㉿PawnSecSecuritySolutions)-[~]
└─$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
└─(kali㉿PawnSecSecuritySolutions)-[~]
└─$ cd Documents
└─(kali㉿PawnSecSecuritySolutions)-[~/Documents]
└─$ cd
└─(kali㉿PawnSecSecuritySolutions)-[~]
└─$ pwd
/home/kali
```

Betik 7’de ifade edildiği üzere “cd Documents” komutu sayesinde “/Documents” dizinine geçiş yaptıktan sonra “cd” komutu ile “/home/kali” dizinine geçiş yapabiliyoruz.

- “cd ..”: Bu komut eğer bir dizine geçiş yaptığınız bu dizinden önceki dizine geri dönmemizi sağlar.
- “cd -“: Bu komut ise “cd ..” ile çıkışınız olduğunuz dizine geri dönmenizi sağlar.
- “cd /dizin_ismi/dizin_ismi”: Şekildeki gibi “/” kullanarak tek komut ile dizinler arasında geçiş sağlayabilirsiniz.

history

Linux işletim sisteminde her kullanıcının komut satırına girmiş olduğu komut saklanır. History sayesinde o kullanıcıya ait komut bloğuna girilmiş komutları görüntüleyebiliriz. History görüntülerken yazmış olduğunuz komutların yanında sayılar bulunmaktadır. Komut satırına “[komut numarası]” yazarsanız direkt olarak komut numarasının bulunduğu komutu çağırabilirsiniz. Örneğin; “history” yazdığında çıktı olarak 21.komutta pwd yazıyorsa “!21” yazarak pwd komutuna hızlıca erişebilirsiniz.

clear

Bu komut sayesinde kullanmış olduğunuz komut ekranını temizlemenizi sağlar.

touch

Boş bir dosya oluşturmanızı sağlayan komuttur. “touch dosya_ismi.dosya_türü” şeklinde kullanabilirsiniz. Örneğin; “touch deneme.txt” komutu ile “deneme” isimli metin dosyası oluşturabilirsiniz. Aynı anda 3 tane metin dosyası oluşturmak isterseniz “touch deneme.txt{1..3}” yazarak deneme1, deneme2 ve deneme3 isimli 3 tane dosya oluşturulmasını sağlayabilirsiniz.

cat

Dosyaların içeriği okuyarak komut satırına yazdırın komuttur.

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$ cat deneme.txt
        Merhaba Hacker
```

Betik 8’de “deneme.txt” isimli metin dosyasının “cat” komutuyla okutarak içeriğinin “Merhaba Hacker” olduğu gösterilmiştir. Aynı zamanda “cat > dosya_adi” yazarak metin dosyası da oluşturabilirsiniz.

cp

Açılımı “copy” olan bu komut isminden de anlaşıldığı üzere istediğiniz bir dosyanın kopyalanmasında rol alır.

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$ ls
        Desktop Documents Downloads Music Pictures Public Templates Videos deneme.txt
    └──(kali㉿PawnSecSecuritySolutions)-[~]
        └─$ scp deneme.txt Desktop/
    └──(kali㉿PawnSecSecuritySolutions)-[~/Desktop]
        └─$ cd Desktop
    └──(kali㉿PawnSecSecuritySolutions)-[~/Desktop]
        └─$ ls
            deneme.txt
```

Betik 9’da ”/home/kali” dizininde bulunan “deneme.txt” dosyasını ”/Desktop” dizinine kopyalama işlemi şematize edilmiştir. Aynı şekilde direk “cp deneme.txt” yazarak ”/home/kali” dizinine deneme.txt dosyasını kopyalayabilirsiniz. Bir dizinin içeriğinin tümünü başka bir yere kopyalamak isterseniz “cp - r [/kopyalamak_istediğiniz_dizin] [yeni_dizinin_ismi]” komutunu kullanabilirsiniz.

Bunların dışında dizin içerisinde bulunan birden fazla dosayı kopyalamak isterseniz “cp” komutunun ardından kopyalayacağınız dosyaların isimlerini girmeniz yeterli olacaktır.

mkdir

KaliLinux işletim sisteminde dosya oluşturabildiğimiz gibi dizin de oluşturabiliriz. İşte bunun için “mkdir [dizin_adı]” komutunu kullanmanız yeterli olacaktır. Birden fazla iç içe dizin oluşturmak

isterseniz “-p” parametresinden sonra oluşturacağınız bu dizinleri sırasıyla belirtmeniz yeterli olacaktır. Örneğin;

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$ mkdir -p Okul/Ödev/Bilişim
        └──(kali㉿PawnSecSecuritySolutions)-[~]
            └─$ cd Okul
                └──(kali㉿PawnSecSecuritySolutions)-[~/Okul]
                    └─$ ls
                    Ödev
                    └──(kali㉿PawnSecSecuritySolutions)-[~/Okul]
                        └─$ cd Ödev
                            └──(kali㉿PawnSecSecuritySolutions)-[~/Ödev]
                                └─$ ls
                                Tarih
```

rm

Açılımı “remove” olan bu komut dosyaların silinmesi işlevini yerine getirir. Silme işlemleri geri alınmadığında dikkatli kullanılması gereken bir komuttur. “rm -i” komutu ile size dosyaların silinip silinmeyeceğini soran bir işlem oluşturarak geri dönüşü olmayan durumlardan kaçınabilirsiniz. “rm -rf” komutu ile dosyalar ve dizinlerin hepsinin silinmesini sağlayabilirsiniz.

rmdir

Açılımı “remove directory” olan bu komutu ile istediğimiz dizinlerin silebilirisiniz.”mkdir” komutuyla beraber kullanılan “-p” parametresi bu komutla beraberde kullanılabildiği gibi yine aynı şekilde birden fazla dizinin silinmenizi sağlamaktadır.

mv

Açılımı “move” olup bu komut sayesinde bir dizinin ya da dosyanın yerini değiştirebilirisiniz. Bu komut “cp” komutu ile karıştırılmamalıdır. Dosya kopyalanmadan sadece taşıma işlemi gerçekleşmektedir. “mv [taşımak_istediğiniz_dosya_ya_da_dizin] [taşımak_istediğiniz_yer]” şeklinde kullanılır. Aynı zamanda dosyanın ismini değiştirmek istediğinizde de bu komuttan yararlanabilirsiniz.

The screenshot shows a terminal window with the following session:

```
kali@PawnSecSecuritySolutions: ~/Desktop/Dosyalar
File Actions Edit View Help

└─(kali㉿PawnSecSecuritySolutions)-[~/Desktop]
  └─$ cd Dosyalar

└─(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
  └─$ ls

└─(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
  └─$ cd ..
  └─(kali㉿PawnSecSecuritySolutions)-[~/Desktop]
    └─$ ls
deneme.txt  Dosyalar

└─(kali㉿PawnSecSecuritySolutions)-[~/Desktop]
  └─$ mv deneme.txt Dosyalar/
  └─(kali㉿PawnSecSecuritySolutions)-[~/Desktop]
    └─$ cd Dosyalar

└─(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
  └─$ ls
deneme.txt
```

Şekil 5 "mv" Komutunun Kullanımı

Yukarıda içerisinde “deneme.txt” metin dosyasını ve “/Dosyalar” alt dizinini bulunduran “/Desktop” dizininde “mv” komutunu kullanarak “deneme.txt” dosyasının “/Dosyalar” içerisinde taşınması sağlanmıştır.

file

Dosyaların tiplerini komut satırında gösteren komuttur.

```
└─(kali㉿PawnSecSecuritySolutions)-[~]
  └─$ file deneme.txt
deneme.txt: ASCII text
```

time

Komutların çalışma sürelerini terminale yazdırın komuttur. “time [komut_ismi]” şeklinde kullanılır.

uptime

İşletim sisteminin ne zamandan beri aktif olduğunu, başlatılma zamanını ve kullanıcı sayısını terminale yazdırın komuttur.

echo

“echo” komutu ile terminal ekranına istediğimiz yazıyı çıktı olarak alabiliriz.

stdout > ve stdin <

“>” komutu herhangi bir girdiyi bir dosyaya yazdırma yarayan komuttur. Bu işlem gerçekleştirken içerisinde yazdırma işlemi yapacağımız dosyanın içeriği silinir sonra yazdırma işlemi yapılır. Bu komut kullanılırken oldukça dikkatli olunmalıdır çünkü eğer bu işaretler beraber yanlış bir komut kullanıldığı taktirde dosya içerisindeki bilgiler silinecektir. ”set -o noclobber” komutunu kullanarak dosyanın üzerinde yazdırma işlemi yapılmasını engelleyebilirsiniz.

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─Secho Merhaba > deneme.txt
        └──(kali㉿PawnSecSecuritySolutions)-[~]
            └─$cat deneme.txt
```

Merhaba

Betik SEQ Betik * ARABIC 12 ">" İşaretinin Kullanımı

“<” komutu “cat” ile aynı işlev sahiptir. Dosya içeriğinin okutulmasını sağlayan komuttur.

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$base64 <<< kali
        a2FsaQo=
        └──(kali㉿PawnSecSecuritySolutions)-[~]
            └─$base64 -d <<< a2FsaQo=
                kali
```

Yukarıdaki ilk işlemede “kali” kelimesinin base64 ile kodlayarak görüntülenmesi sağlanırken, ikinci işlemede ise “**a2FsaQo=**” kodunun çözümlenmiş halini görüyoruz.

” ve ”

Bildiğiniz üzere KaliLinux işletim sisteminde büyük-küçük harf duyarlılığı vardır ve aynı zamanda dosya adları yazılırken boşluk (space) karakteri kullanılamaz. Bu işaretleri kullanarak dosya isimlerinde boşluk karakterinin kullanımı gerçekleşebilmektedir.

: (noktalı virgül)

Bu işaret ile birden fazla komutu tek satırda gerçekleştirebilirsiniz. Tek yapmanız gereken komutların arasına “,” işaretini koymaz olacaktır.

&

Bu işaret noktalı hem noktalı virgül ile aynı işlevi üstlenir hem de herhangi bir komut yazdıktan sonra o komutun sonuna eklenirse o komutun arka planda çalışmasını sağlamaktadır.

&&

Bu işaret “ve” anlamına gelmektedir. Art arda girilen işlemlerden biri gerçekleşmezse işlem durdurulur.

| (pipe)

Çıktı veren komutlarda kullanılması durumunda çıktıların içinden istenilen verinin yakalanmasını veya çıktı boyutunun ayarlanması için kullanılır.

||(cift pipe)

Bu işaret “veya” anlamına gelmektedir. “&&” işaretinin aksine art arda girilen işlemlerden biri gerçekleşmese bile geriye kalan işlemler yürütülmeye devam eder.

(divez)

Bu işaret ile istediğiniz komut satırının sonuna açıklama ekleyebilirsiniz. Bu açıklamalar “history” komutunu kullandığınız zaman gözükecektir.

~(tilde)

Bu simbolü kullandıkten sonra o işletim sistemini kullanan kullanıcılarından birinin ismini girerek o kullanıcıya ait “/home” dizinine erişebilirsiniz.

](köşeli parantez)

Dizinleri görüntüülerken filtreleme yapmak için kullanmak için “[]” işaretleri kullanılır. Örneğin;

```
└──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
    └─$ls
        LCA.txt  LLA.txt  LLB.txt
        └──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
            └─$ls -lah  LL[A,B].txt
                -rw-r--r-- 1 kali kali 0 Mar 19 11:27 LLA.txt
                -rw-r--r-- 1 kali kali 0 Mar 19 11:27 LLB.txt
```

? (soru işaretı)

“[]” simbolüyle benzer bir işleve sahip olan bu simbol ile belli bir karakterin yerini tutmasını sağlayabiliyorsunuz.

```
└──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
    └─$ls -lah L?A.txt
        -rw-r--r-- 1 kali kali 0 Mar 19 11:27 LCA.txt
        -rw-r--r-- 1 kali kali 0 Mar 19 11:27 LLA.txt
```

15. betikte “L?A” yazdığımız yerde soru işaretini gelebilecek değerleri yerine koyarak kontrol eder. Eğer değer dizinde bulunuyorsa bize çıktıyı verir.

***(asteriks)**

Bu işaretle yazdığınız komutun işlevini sınırlayabilirsiniz. Örneğin; “rm -rf *a” komutu ile bir dizin altındaki “a” ile başlayan her dosyanın ve dizinin silinmesini sağlarsınız.

4.2 Bash, Environment ve Shell Değişkenleri

Bash Değişkenleri

Terminal ekranında mevcut kullanıcı tarafından belli bir değerin yerini tutan, programlar tarafından kullanılmayan ve sistem kapatılınca silinen değişkenlerdir. Örneğin; [4] [5]

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$A=5

└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$B=6

└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$C= expr $A +$B

10
```

Betik SEQ Betik /* ARABIC 16 Bash Değişkeninin Kullanımı

Environment Değişkenleri

“export” komutu kullanılarak tanımlanan bu değişkenler bash değişkenlerinin aksine shell veya subshell de başlatılan programlar tarafından kullanılabilen, dinamik olarak adlandırılmış değerlerdir.

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$cat deneme.sh
      #!/bin/bash
      B=5
      C=$((A*B))
      echo $C
      └──(kali㉿PawnSecSecuritySolutions)-[~]
          └─$export A=10
          └──(kali㉿PawnSecSecuritySolutions)-[~]
              └─$bash ./deneme.sh
              50
```

Shell Değişkenleri

“\$” simbolü kullanılarak Shell değişkenlerine atanan verilerin okunarak terminale yazılmasında görev alır. Örneğin;

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$IP=10.0.7.8

    └──(kali㉿PawnSecSecuritySolutions)-[~]
        └─$echo IP
10.0.7.8
```

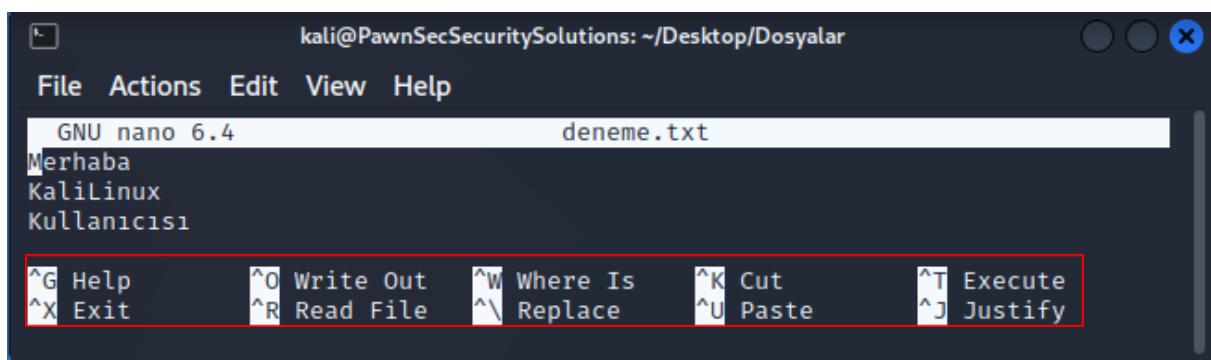
4.3 Dosyalarda Kullanılan Komutlar

Windows gibi çeşitli işletim sistemlerinde nasıl herhangi bir dosyanın içeriğini görebiliyor ve düzenleyebiliyorsak aynı şeyleri KaliLinux’da da yapmamız mümkün. Bunun için vi, vim ve nano gibi sisteme kurulu olarak gelen bazı dosya editör uygulamaları mevcuttur. Aralarında küçük farklılıklar bulunsa da hepsinin amacı aynıdır. Bu uygulamalara “[nano|vi|vim] [dosya adı]” komutu aracılığıyla erişebiliriz.

Bir dosyada herhangi bir değişiklik yaparken yaptığından deşikliğin boş gitmemesi için o dosyanın yetkilendirmesine dikkat ederek yapmanız öneririz. Aksi takdirde sadece “root” kullanıcısının erişebildiği bir dosyayı değiştirmeye çalışırsınız ve yetkiniz buna izin vermiyorsa yaptığından değişiklikler boşuna gidecektir. [6]

nano

Yukarıda da belirttiğimiz “nano” fonksiyonunu önceden hazırlamış olduğumuz “deneme.txt” metin dosyası üzerinde inceleyelim. Bunun için “nano deneme.txt” komutunu terminale giriyoruz. Hemen ardından karşımıza aşağıdaki görüntü gelecektir.



Şekil 6 "nano" Komutunun Kullanımı

İçerisinde “Merhaba KaliLinux Kullanıcı” yazan bu dosyamızın içeriğini istediğimiz gibi düzenleyebiliriz. Kırmızı dikdörtgen içerisindeki fonksiyonları gerçekleştirebilmek için Ctrl’ye basılı tutarak beyaz karelerin içerisinde bulunan harfe basmanız gerekmektedir. Dosyadan “Ctrl+X” aracılığıyla çıkış yaparken size dosyanın kaydedilip edilmeyeceği sorulacaktır.

Burada verilmiş olan fonksiyonlar dışında başka işlevsel fonksiyonlar da bulunmaktadır. Bunlardan bazıları;

- Ctrl+S Dosyadan çıkmadan dosyayı kaydeder.
- Ctrl+A Satır başı yapar.
- Ctrl+E Satır sonu yapar.
- Ctrl+Y Bir satır yukarı çıkar.
- Ctrl+V Bir satır aşağı icer.

“man” komutuyla önemli sistem dosyalarında değişiklik yapmanız gerekiğinde bu dosyaların kopyasını “cp” komutu aracılığıyla almayı ihmal etmeyiniz.

“man” komutuyla dosyaları inceleyebileceğiniz gibi aynı zamanda bu işlemi cat, less, more, head, tail komutlarını da kullanabilirsiniz. “cat” komutunu daha önce açıkladığımız için diğerlerine göz atalım.

less ve more

Bu komutların ikisi de dosyanın baştan sona kadar olan görüntülerini terminale yazdırılan komutlardır. Kullanıcıları biraz farklılık gösterse de ikisinin de temel amacı aynıdır.

head ve tail

Bu komutlar da dosyanın ilk 10 satırının okunarak terminal ekranına yazdırılmasını sağlayan komutlardır. İki kodda da terminalde gösterilecek satır sayısını ayarlayabilirsiniz.

4.3.1 Dosyalarda Filtreleme Komutları

grep

Bir ekran çıktısını veya dosya içeriğindeki istediğiniz bir filtrelemeyi bu komutla

```
└──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
```

```
└──Secho Merhaba KaliLinux Kullanıcı | grep a
```

Merhaba KaliLinux Kullanıcı

```
└──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
```

```
└──Scat deneme.txt | grep -i k
```

KaliLinux

Kullanıcı

```
└──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
```

```
└──Scat deneme.txt | grep -v -i k
```

Merhaba

gerçekleştirebilirsiniz.

Betik 19’da 1. İşlemde “echo” ile yazdırılmış olduğumuz metnin içerisinde ”a” karakterlerini filtreledik. 2.İşlemde içerisinde “Merhaba KaliLinux Kullanıcı” yazan metin dosyasında “-i” parametresiyle büyük-küçük fark etmeksizin “k” harfi içeren kelimeleri filtreleme işlemi uyguladık. Son işlemede ise “-v” parametresini de ekleyerek büyük-küçük fark etmeksizin “k” harfi bulunmayan karakterlerin yazılmasını sağladık. [7]

cut

“cut” komutu sayesinde bir dosyada sütunlarda filtreleme uygulayabilirsiniz. Ayrıca bu komutu kullanırken “tail” veya “head” komutunu da ekleyerek satır sütun aramasını birlikte sağlayabilirsiniz.

```
└──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
    └──Scut -b 1,2,3 deneme.txt
```

Mer

Kal

Kul

```
└──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
    └──Scut -b 1,2,3 deneme.txt | tail -1
```

Kul

Yukarıdaki ilk örneğimizde “cut” komutunun yanına “-b” parametresi ile dosya içerisindeki belirli byte’ları filtrelemeye çalıştık ve ilk üç sütunun alınmasını sağladık. Ardından “tail” komutunu da “|” yardımıyla ekleyerek son satırın alınmasını sağladık.

tr

“tr” komutu sayesinde dosya içeriğini değiştirmeden alacağımız çıktıya değişiklikler uygulabiliyoruz. Örneğin; “echo Merhaba KaliLinux Kullanıcı | tr ‘a-z’ ‘A-Z’” komutunu uygularsak bize çıktı olarak “MERHABA KALILINUX KULLANICISI” çıktısını dönecektir. Bu işlemi uygularken sistemimiz İngilizce kurulu olduğu için “a-z” yazdığımızda İngilizce alfabeyle göre komut uygulanacaktır. Bu yüzden “i” harfi “I” harfine dönüşecektir.

wc

“wc”, bir dosya içeriğindeki sırasıyla satır, kelime ve karakterleri saymak için kullanılır.

```
└──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
```

└──\$ wc deneme.txt

3 3 33 deneme.txt

Betik SEQ Betik * ARABIC 21 "wc" Komutunun Kullanımı

sort

Dosya içeriğini alfabetik olarak sıraya dizən komut “sort” komutudur. Ayrıca bu komutun yanına “-k” parametresini yazarak ve ardından sütun numarasını belirterek hangi sütunu sıralayacağını belirtebilirisiniz.

```
└──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
```

└──\$ sort -k1 deneme.txt

KaliLinux

Kullanıcı

Merhaba

uniq

“uniq” komutu sayesinde dosyamızda birden fazla tekrar eden kelimeleri kaldırarak bize çıktıının verilmesini sağlar. Ancak bu tekrar eden kelimeler dosya içerisinde silinmez. Sadece çıktı olarak tekrarlanan kelimeleri kaldırır. “-c” parametresini kullanarak kelimelerin kaç defa tekrar ettiğini de görebilirsiniz.

```
└──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
    └──Scat deneme.txt
        Merhaba
        Merhaba
        Merhaba
        KaliLinux
        Kullanıcısı
        Kullanıcıs
        └──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
            └──$uniq -c deneme.txt
                3 Merhaba
                1 KaliLinux
                2 Kullanıcısı
```

sed

```
└──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
    └──Secho "Merhaba KaliLinux Kullanıcısı" | sed 's/Merhaba/Hoşgeldin/;
        s/KaliLinux/Windows/'
```

Hoşgeldin Windows Kullanıcısı

Betik SEQ Betik * ARABIC 24 "sed" Komutunun Kullanımı

Bu komut “uniq” komutu gibi dosya içeriğini değiştirmeden çıktıarda değişiklik yapabilmemizi sağlar.

```
└──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
    └──Scat deneme.txt
        kalem, 15, 15 adet
        kalem, 10, 20 adet
        kitap, 40, 15 adet
        silgi, 5, 30 adet
        silgi, 3, 10 adet
        defter, 25, 25 adet
        dosya, 20, 10 adet
    └──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
        └──Scat deneme.txt | sed 's/kalem/silgi/g'
            silgi, 15, 15 adet
            silgi, 10, 20 adet
            kitap, 40, 15 adet
            silgi, 5, 30 adet
            silgi, 3, 10 adet
            defter, 25, 25 adet
            dosya, 20, 10 adet
```

Betik 24'de yazmış olduğumuz cümledeki kelimeleri sırasıyla değiştirirken Betik 25'te ise değiştirmek istediğimiz kelimeleri yazdıktan sonra "/g" fonksiyonunu ekleyerek bütün "kalem" değerlerinin "silgi" ile değiştirilmesini sağlamış oluyoruz.

awk

“awk” komutu dosya içeriğinin satır ve sütunlara ayrılarak düzenli bir çıktı verilmesini sağlayan bir komuttur.

```
└──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
    └──Scat deneme.txt
        kalem 15      15adet
        kalem 10      20adet
        kitap 40      15adet
        silgi  5       30adet
        silgi  3       10adet
        defter 25      25adet
        dosya  20      10adet
    └──(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
        └──Sawk '{print $1,$3}' deneme.txt
            kalem 15adet
            kalem 20adet
            kitap 15adet
            silgi  30adet
            silgi  10adet
            defter 25adet
            dosya  10adet
```

4.3.2 Dosya Arama Komutları

find

KaliLinux işletim sistemi kurulduğunda yüklü olarak gelen bu komut sayesinde dosyaları tiplerine, oluşturulma tarihine, izinlerine, gruplarına, boyutlarına göre arayabiliyoruz. Şimdi “find” komutu ile kullanabileceğimiz bazı parametrelerle göz atalım. [7]

- “. -name *.txt”: Bu parametre aracılığıyla bulunduğunuz dizin içerisinde bulunan metin dosyalarına erişim sağlayabilirsiniz. Ayrıca “*.txt” yazan yerdeki dosya uzantısını değiştirerek istediğiniz dosya türünü rahatlıkla bulabilirsiniz.
- “/ -name *.exe”: Bu parametre sayesinde “/root” dizi içerisindeki “exe” dosyalarına ulaşabilirsiniz.
- “. -type d -name “Dosyalar*”: Bu parametreyle bulunduğuuz dizin içerisinde “Dosyalar” ismine sahip dizin olup olmadığını bakabiliyoruz. “-type” fonksiyonundan sonra “d” yazarak

dizinleri bakmasını sağladığımız gibi “f” yazarak “Dosyalar” ismine sahip dosyaları aratabiliriz.

- “/home/kali/Desktop -type f -name *.txt”: Bu örneğimizde ise kali kullanıcısı içerisinde “Desktop(Masaüstü)” dizini içerisindeki metin dosyalarını aratabiliyoruz.
- “. -size -10M”: Bu örnekte ise “.” İle bulunduğuuz dizinde arama yapmasını belirterek ardından gelen “-size” fonksiyonuyla kullandığımız “-10M” 10 Megabyte altındaki dosyaları göstermesini sağlayabiliyoruz.
- “. -type f -name “.*”: Bu parametreyi kullanarak gizli olan dosyaları listeleyebilirsiniz.
- “/home/kali/Desktop -mmin +120”: “-mmin” parametresini kullanarak ardından gireceğiniz dakika süresi içerisinde değişmiş olan dosyaların bulunmasını sağlayabiliyorsunuz. Aynı şekilde “-mtime” parametresini kullanıp ardından “[gün sayısı]” belirterek o gün süresi içerisinde değiştirilen dosyaları ve dizinleri yazdırabilirsiniz.

4.3.3 Hardlink ve Softlink Kavramları

Hardlink herhangi bir dosyanın kopyasını oluşturmak olarak düşünülebilir. Herhangi bir dosyanın hardlink’ini oluşturduğunuzda ana dosyada bir değişiklik yaparsanız hardlink dosyasında da o değişiklik gerçekleşecektir. Hardlink dosyalar ana dosya silinse bile silinmez ve olduğu gibi çalışmaya devam eder.

Hardlink’ini oluşturacağınız dosyanın çalıştığı dizin dosyadan dosyaya göre önem arz etmektedir. Örneğin; “/dev/console” dizini içerisindeki bir dosyanın hardlink’ini “/dev/port” dizini içerisinde oluşturursanız bu durum bazı aksaklıklar ortaya çıkaracaktır. Bu yüzden Hardlink oluştururken dikkatli olmanızı öneririz.

Bir dosyanın Hardlink’ini oluşturmak için “ln [Kopyalanacak dosyanın adı] [Kopyanın adı]” komutunu kullanmanız yeterli olacaktır.

Softlink kavramı ise Windows işletim sistemindeki kısayol uygulamaları ile aynıdır. Nasıl ana uygulama silindiğinde kısayollar çalışmıyorsa KaliLinux’da da ana dosya silindiğinde o dosyaya ait Softlink çalışmamaktadır. Hardlink’te olduğu gibi buradaki ana dosya değiştiği zaman o değişiklik Softlink’té de gerçekleşir.

5 İşletim Sistemi Bağlantı Tipleri

Herhangi bir işletim sisteme konsol veya uzak bağlantı (terminal) ile giriş yapabiliriz. Sunucuya direk olan bağlanmak için kullandığımız konsol bağlantısı, sunucuya mouse gibi donanımlarla bağlanarak sağladığımız erişim çeşididir. Sanal sunucu tarafı da konsol bağlantısıyla aynı şekilde çalışır. Sunucuya uzaktan erişim sağlayamadığımızda sanallaştırma ortamındaki konsol bağlantısı ile sanki sunucuya donanımlar aracılığıyla bağlıyormuş gibi oluruz. Bu yöntemle sistemin boot menüsüne erişebiliriz.

KaliLinux sunucularında uzak bağlantı Telnet ve SSH bağlantı ile sağlanır. Telnet güvensiz bir ağ bağlantı şekli olup herhangi bir tehdit aktörünün ağını dinlemesi durumunda bilgilerinizi kullanarak MITM (Man In The Middle)saldırısı gerçekleştirebilir. SSH bağlantı ise sunucuya arasındaki bağlantıyı şifreleyerek güvenli bir bağlantı oluşturur. Bu sayede ağı dinleyen herhangi bir saldırgan

olsa bile elde edebileceğim tek sek anlamsız şifrelenmiş veriler olacaktır. Fakat SSH bağlantısı da tam güvenlik sağlamayıp bazı zafiyetlere sahiptir.

5.1 Sistem Kullanıcılarıyla İlgili Komutlar

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
└─$w
09:10:27 up 3:45, 1 user, load average: 0.06, 0.02, 0.00
USER   TTY   FROM      LOGIN@ IDLE  JCPU PCPU WHAT
kali    tty7  :0          05:24  3:45m 38.47s 0.22s xfce4-session
```

“w” komutu, sisteme giriş yapan kullanıcılar hakkında bilgi verir. Yukarıdaki betikte belirtildiği üzere saat 9:10’da kali kullanıcısı üzerinden konsol bağlantısının sağlandığı 3 saat 45 dakikadır oturumun açık olduğu ve 1 kullanıcının giriş yaptığı görülmüyor. Sanal bağlantıyı Telnet üzerinden kurduğumuz için “tty7” çıktısını görmekteyiz. “tty7” yerine “ttyS” çıktısı varsa bağlantınızın fiziksel olduğu anlamına gelir. Sunucuya Telnet yerine SSH ile bağlantı kursaydık “pts” çıktısını gördük.

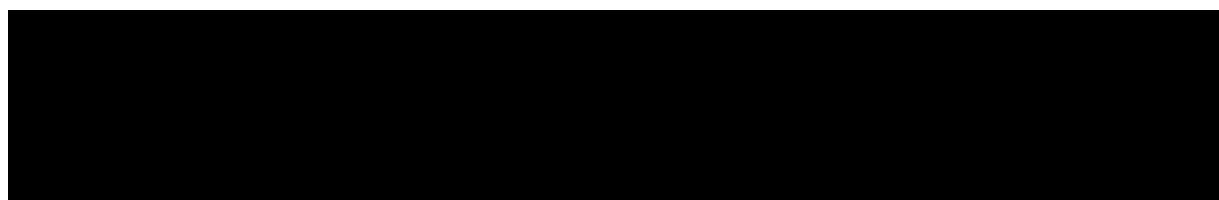
who

Sisteme giriş yapan kullanıcıları, bağlantı türünü ve bağlantının kurulduğu zamanı veren komuttur.

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
└─$who
kali  tty7    2023-03-20 05:24 (:0)
```

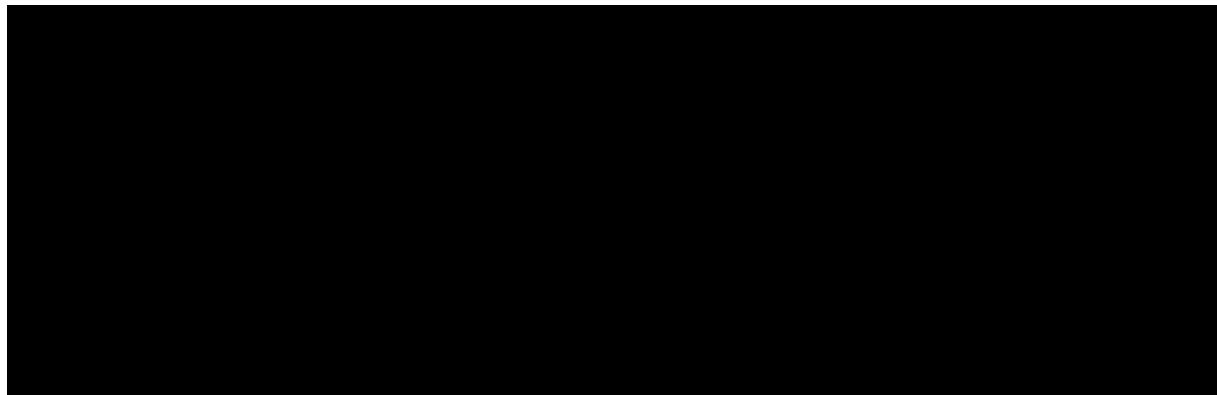
whoami

Bu komut ile sistemdeki kullanıcıların isimlerini öğrenebilirsiniz.



last

İşletim sisteminin açılma ve kapanma süresini, oturumu açan kullanıcıları, oturum süresini gösteren komuttur.



su

“su” komutu işletim sistemindeki kullanıcılar arasında geçiş yapmamızı sağlayan komuttur. “su -[kullanıcı adı]” komutu ile istediğiniz kullanıcıya geçiş yapabilirsiniz. Bu komut ile “/home/[kullanıcı adı]” dizinine ulaşırınsınız. Eğer “-“ işaretini koymazsanız kullanıcı değiştirmenize rağmen geçiş yapmadan önceki kullanıcının “/home/[kullanıcı adı]” dizininde bulunursunuz. “root” kullanıcısına geçmek isterseniz “sudo su” yazmanız gerekmektedir.

shutdown

Sistemi KaliLinux arayüzünden kapatabileceğiniz gibi terminale “shutdown” komutunu girerek de gerçekleştirebilirsiniz. Böylelikle sisteminiz 1 dakika içerisinde kapatılacaktır. Bu süre içerisinde sistemin kapatılmasını iptal etmek için “shutdown -c” yazmanız yeterli olacaktır. Aynı şekilde sistemi arayüzden yeniden başlatabileceğiniz gibi “shutdown -r” komutunu veya “reboot” komutunu kullanarak da bu işlemi gerçekleştirebilirsiniz.

Bunlar dışında “shutdown” komutuyla “-P” parametresini kullanarak bilgisayarınızın fişi çekiliyormuş gibi arkada çalışan programların kapanma işlemi tamamlanmadan kapatılmasını sağlayabilirsiniz.

5.2 Servis Kontrolü

Servisler KaliLinux sunucusu içerisindeki bazı görevlerin gerçekleşmesini sağlayan programlardır. Bu servislerin çalışıp çalışmadığını “systemctl” komutuyla sağlayabilirsiniz. Bu programların kaynak kodlarında herhangi bir değişikliği yapıldığında yapılan değişikliklerin gerçekleşmesi için “systemctl restart [servis ismi]” komutu kullanılarak servis yeniden başlatılmalıdır.

Belirli bir servisin durumunu öğrenmek için “systemctl status [servis ismi]” şeklindeki komutu terminale yazabilirsiniz. “systemctl start [servis ismi]” veya “systemctl stop [servis ismi]” kullanarak servisleri başlatılmasını veya kapatılmasını sağlayabilirsiniz. Servisleri bu kodlarla anlık durdurabileceğiniz gibi temelli olarak açılmak için “systemctl enable [servis ismi]”, kapatmak için ise “systemctl disable [servis ismi]” komutlarını kullanabilirsiniz.

6 SSH Servisi

Önceden de bahsetmiş olduğumuz SSH Kali sunucumuza uzaktan bağlantı kurmamızı sağlayan yapılandırmaya verilen addır. Bu protokol sayesinde verilerimizin şifrelenerek network bağlantısı üzerinden güvenli bir şekilde iletilir. Bu yapılandırmayı KaliLinux sisteminize indirmek için terminalinizde “sudo apt install openssh-client” komutunu kullanabilirsiniz.

Herhangi bir bilgisayara bağlanmak istiyorsanız yapmanız gereken şey terminale “ssh -l [kullanıcı_adi@IP_adresi] -p [port numarası]” komutunu yazabilirsiniz. Dosya transferi yapmak için “scp -P [port_numarası] [gönderilecek_dosya] [kullanıcı_adi@IP_adresi:hedef_dizin]” komutunu kullanabilirsiniz.

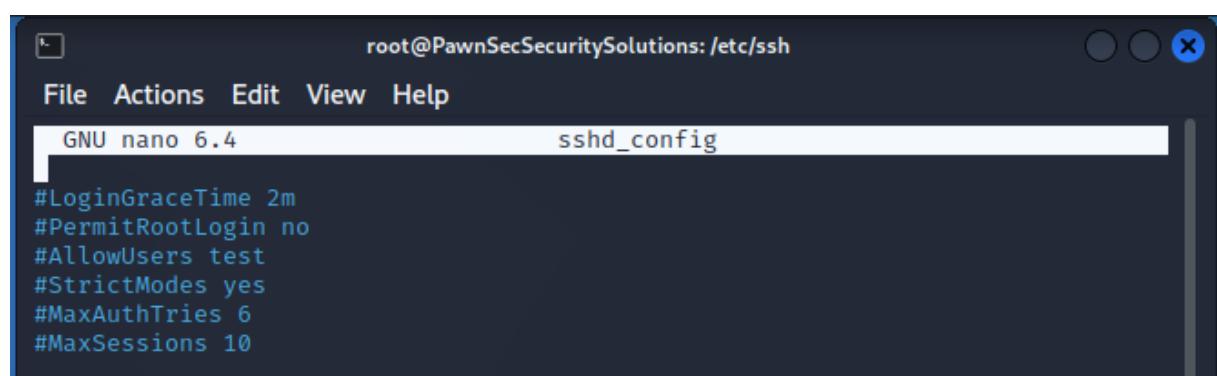
MITM saldırısının önlenmesinde büyük rol oynayan bu servis bilgisayarımız ile başka bir bilgisayar arasında veri alış-verişi gerçekleştirken veya swich ve rooter gibi cihazlarla iletişim kurulurken bağlantının şifrelenmesinde rol alır. Aynı zamanda dosyaların iletilmesini sağlayan FTP protokolüyle beraber çalışarak dosyaların güvenli bir şekilde ulaşmaktadır.

SSH servisi 22 numaralı portu kullanmaktadır ve kurulumu gerçekleştikten sonra güvenliğin gerçekten sağlanabilmesi için bazı ayarlamaların yapılması gerekmektedir. Örneğin; “/root” kullanıcısı için açık olan bu portu kapatarak veya SSH erişim portunu değiştirerek büyük bir güvenlik önlemi alabilirsiniz.

UYGULAMA

Şimdi isterseniz “/root” kullanıcısının SSH portunun kapatılması işlemine geçelim. Bu işlemi gerçekleştirmeden önce “/root” kullanıcısının yetkilileriyle aynı yetkilere sahip başka bir kullanıcı oluşturuyoruz. Kullanıcı oluşturmak için ise “useradd -m [kullanıcı adı]” komutunu kullanıyoruz. “-m” parametresi ile “/home” dizini altına bir dosya oluşturulmasını istiyoruz. “passwd [kullanıcı adı]” komutuyla kullanıcı adına ait parola koymak gerekmektedir.

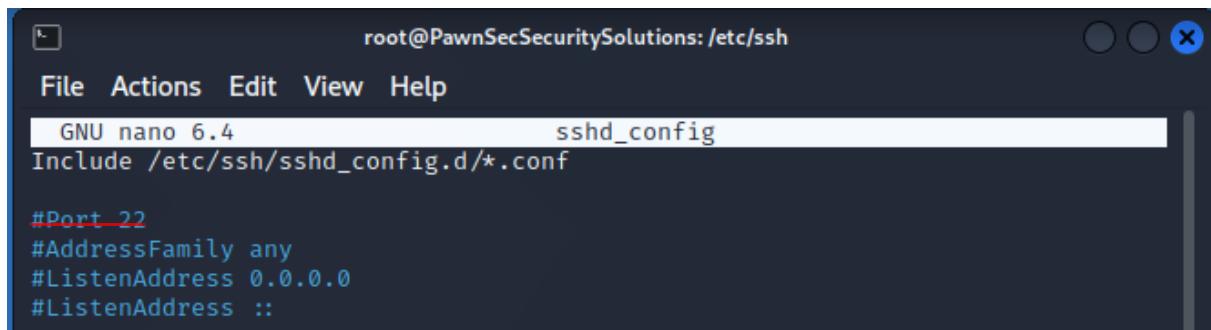
Hemen ardından “nano” komutu ile “/etc/ssh/sshd_config” dosyasını açıp “PermitRootLogin” karşısındaki değeri silerek o değer yerine “no” yazıyoruz. Sonra “Enter” ile bir alt satırda “#AllowUsers [kullanıcı adı]” yazıp dosyayı kaydederek çıkış yapıyoruz. Serviste değişiklik yaptığımız için ve bu değişikliğin gerçekleştirilebilmesi adına “systemctl restart ssh” komutunu giriyoruz. Ardından “ssh root@[kullanıcı adı]” yazmanız durumunda root parolasını girseniz bile “Connection Refused” veya “Permission Denied” yazısı alacaksınız. #AllowUsers komutu yerine “#DenyUsers” komutunu kullanarak SSH protokolüne erişimi istediğiniz kullanıcıdan kaldırabilirsiniz.



```
#LoginGraceTime 2m
#PermitRootLogin no
#AllowUsers test
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Şekil 7 SSH Yapılandırmasının Root Kullanıcısından Kapatılması

Güvenliği daha da artırmak istersek “sshd_config” dosyasından SSH’ın kullanmış olduğu 22 numaralı portu kullanılmayan başka bir port ile değiştirebilirsiniz. Dosyayı kaydettikten sonra “systemctl restart ssh” yazarak servisi yeniden başlatmayı unutmayın.



```
root@PawnSecSecuritySolutions: /etc/ssh
File Actions Edit View Help
GNU nano 6.4          sshd_config
Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

Şekil 8 SSH Portunun Değiştirilmesi

KaliLinux sunucusu kurulduğu zaman varsayılan olarak tüm SSH erişimlerini dinle. Fakat isterseniz Şekil 8'de de görünen "ListenAddress" kısmına istediğiniz IP adresini yazarak o IP adresinin dinlenmesini sağlayabilirsiniz. Bunun dışında aynı dosya içerisindeki "PermitEmptyPasswords" kısmına "no" yazarak parola kısmı boş geçilerek oluşturulan kullanıcıların erişmesine de engel olabilirsiniz. Aynı şekilde dosya içerisindeki "ClientAliveInterval" kısmına belirli bir saniye değeri girerek kullanılmayan oturumların belirtilen vakit geçtiginde kendiliğinden kapanmasını sağlayabilirsiniz.

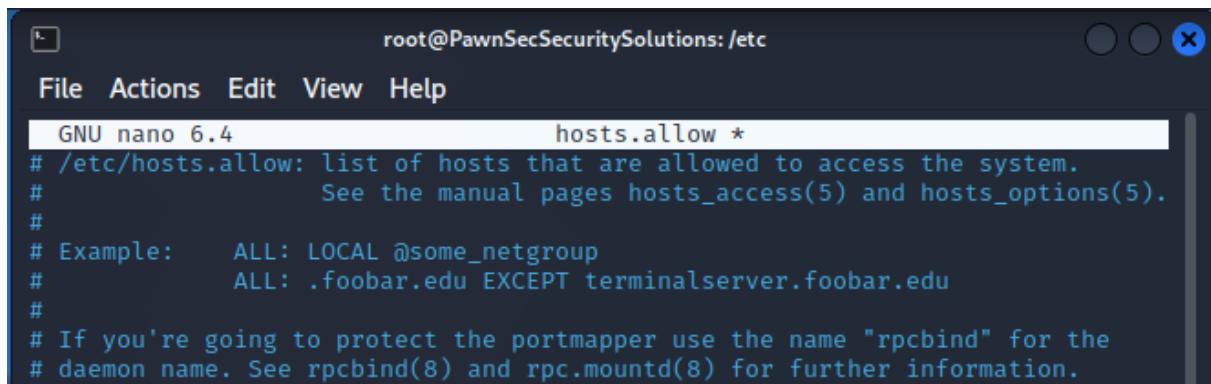
Bunlar dışında "MaxAuthTries" kısmına parola'nın kaç defa yanlış girilebileceğini ve "LoginGraceTime" ile oturum açma isteği yapıldıktan sonra parolanın ne kadar sürede girilmesi gerektiğini belirleyebiliyorsunuz. Böylelikle "Brute-Force" saldırısıyla SSH erişiminin sağlanmasına ve portların meşgul edilmesine engel olabilirsiniz. Ek olarak "sshd_config" dosyamıza "Protokol 2" parametresini ekleyerek SSH 2'nin kullanılmasını sağlayabilirsiniz.

SSH erişimini sadece belirli IP adreslerinden yapmak istiyorsanız bunu ya işletim sisteminizin güvenlik duvarıyla ya da host bazlı erişim engelleme işlemiyle gerçekleştirebilirsiniz.

UYGULAMA

Şimdi hızlı bir şekilde host bazlı erişim engelleme işlemi yapalım.

İlk olarak "/etc" dizinine girdikten sonra "nano" yardımıyla "hosts.allow" dosyasının kodlarını açıyoruz.

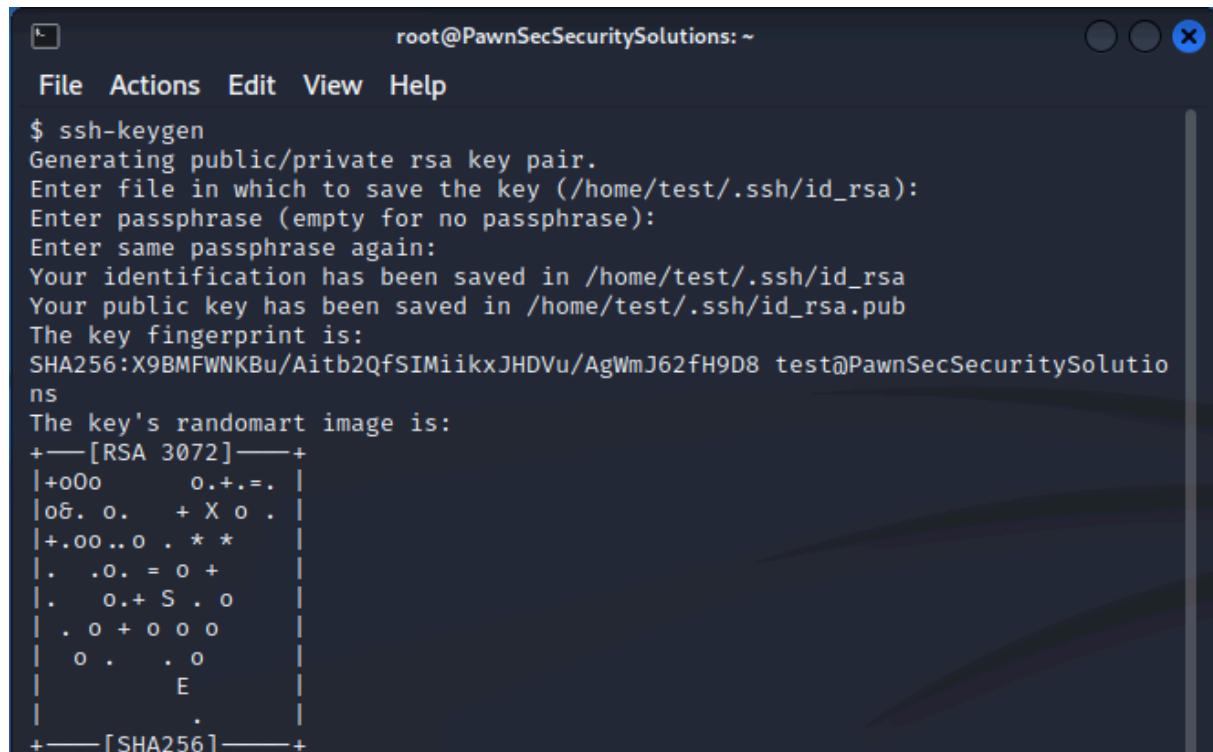


```
root@PawnSecSecuritySolutions: /etc
File Actions Edit View Help
GNU nano 6.4          hosts.allow *
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                               See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: LOCAL @some_netgroup
#              ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
```

Şekil 9 "hosts.allow" Dosyası

Şekil 9'daki dosyaya girdikten sonra en alt satırı "sshd: [izin vermek istediğimiz IP adresleri]" yazısını yazdıktan sonra kaydederek çıkıyoruz. Eğer birden fazla IP adresi girecekseniz IP adreslerinin yanına "," (virgül) koymaz yeterli olacaktır. Sonra aynı dizin içerisindeki "hosts.deny" dosyasını "nano" komutuyla açıyoruz ve yine son satırına "sshd: [engellemek istediğiniz IP adresleri]" komutunu giriyoruz. İsterseniz "sshd: * " komutunu girerek "hosts.allow" dosyası içerisinde yazan IP adreslerinin engellenmesini sağlayabilirsiniz.

Sunucuya bağlantıyı SSH parolası ve SSH key’i kullanarak yapabileceğiniz gibi “sshd-config” dosyasında ayarlamalar yaparak sadece key ile giriş de yapabilirsiniz. SSH Key oluşturduğunuzda Public ve Private olmak üzere iki key oluşur. “Public Key” bağlanmak istediğiniz sunucuya yüklenirken “Private Key” ise bağlanacağınız bilgisayarda saklanır. “ssh-keygen” komutuyla sunucumuza bağlanacağımız cihaz üzerinden bir SSH key oluşturabiliyoruz.



```
root@PawnSecSecuritySolutions:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/test/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/test/.ssh/id_rsa
Your public key has been saved in /home/test/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:X9BMFWNKBu/Aitb2QFSIMiikxJHDVu/AgWmJ62fH9D8 test@PawnSecSecuritySolutions
The key's randomart image is:
+---[RSA 3072]---+
|+o0o      o.+.=.
|o8. o.    + X o .
|+.oo .. o . * *
|.. .o. = o +
|.   o.+ S . o
| . o + o o o
|  o .   . o
|   E
|
+---[SHA256]---+
```

Şekil 10 "ssh-keygen" Komutunun Kullanımı

“Public Key” erişimini sağlamak istediğimiz sunucuya kopyalamak için “ssh-copy-id [kullanıcı_adi@IP_adresi:hedef_dizin] -p [SSH_port_numarası]” komutunu kullanabiliriz.

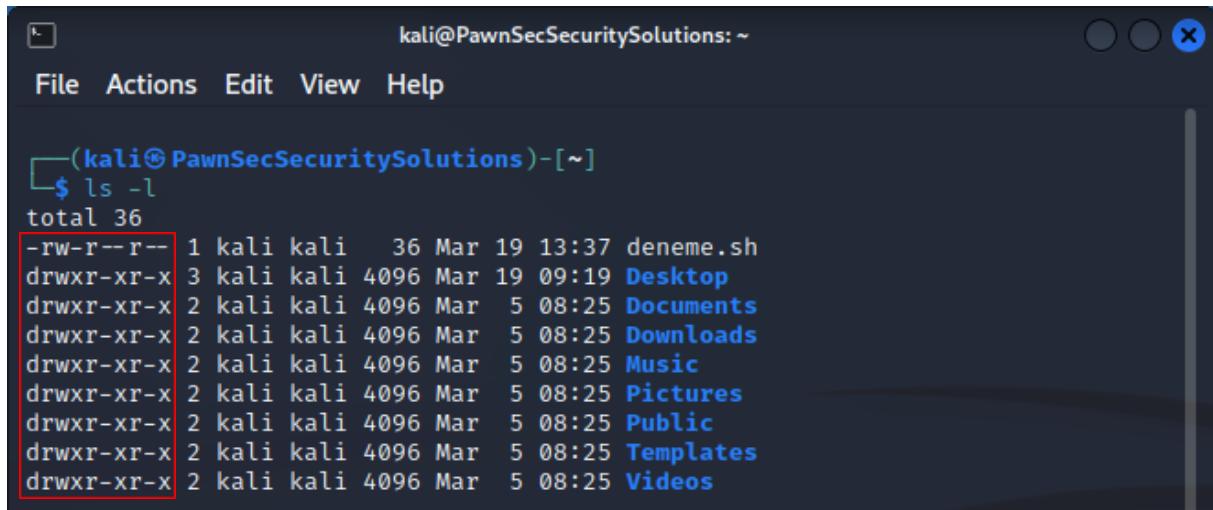
SFTP (Secure File Transfer Protocol)

Önceden de SSH protokolünün FTP protokolü ile birlikte çalışarak güvenli dosya transferi yapıldığından bahsetmiştik. Bu iki protokolün birleşmesi ile oluşan protokol çiftine SFTP ismi verilmektedir.

7 KaliLinux Dosya Sisteminde Yetki Yönetimi

Kursumuzun başında da KaliLinux işletim sisteminin hiyerarşik bir yapıya sahip olduğunu belirtmiştik. Bu yapı içerisindeki her şeyin kullanıcından kullanıcıya değişiklik gösteren okuma, yazma ve çalışma izinleri vardır. Herhangi bir kullanıcının bu yapı içerisindeki dizinlerde, dosyalarda veya aygıtlarda uygulayabileceği bu işlemlerin yetkilerini düzenleyebiliyoruz.

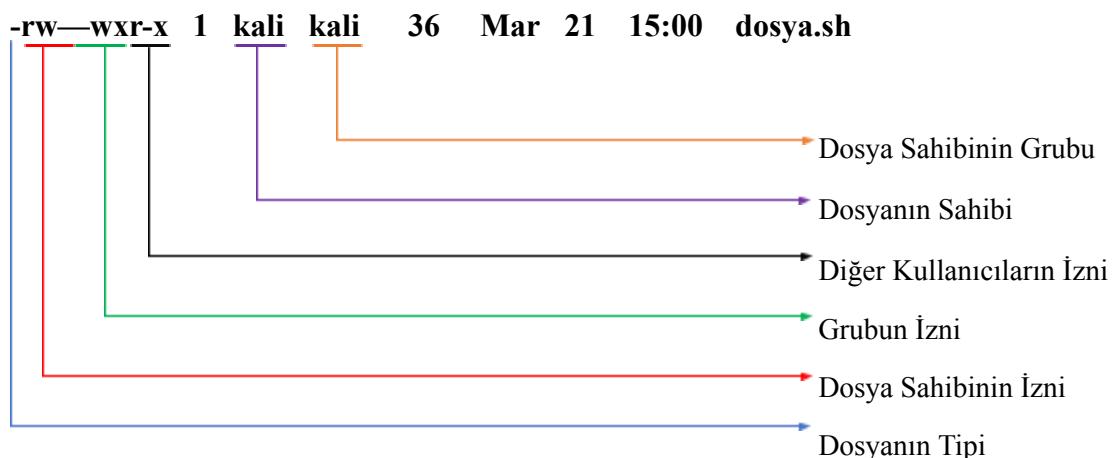
Bildiğiniz üzere terminale “ls -l” komutunu girerek dosyalar hakkında bilgi alabiliyorduk. Bu komutu çalıştırduğumızda en solda çıkan ve “d,l,r,w,x,-“ harf ve sembolleriley ifade edilen yer kullanıcıların yetkilerinin gösterildiği kısımdır.[



```
(kali㉿PawnSecSecuritySolutions)-[~]
$ ls -l
total 36
-rw-r--r-- 1 kali kali 36 Mar 19 13:37 deneme.sh
drwxr-xr-x 3 kali kali 4096 Mar 19 09:19 Desktop
drwxr-xr-x 2 kali kali 4096 Mar  5 08:25 Documents
drwxr-xr-x 2 kali kali 4096 Mar  5 08:25 Downloads
drwxr-xr-x 2 kali kali 4096 Mar  5 08:25 Music
drwxr-xr-x 2 kali kali 4096 Mar  5 08:25 Pictures
drwxr-xr-x 2 kali kali 4096 Mar  5 08:25 Public
drwxr-xr-x 2 kali kali 4096 Mar  5 08:25 Templates
drwxr-xr-x 2 kali kali 4096 Mar  5 08:25 Videos
```

Şekil 11 Dosya İzinleri

Yukarıdaki kırmızı dikdörtgen ile belirtilmiş yerde izinleri görebiliyorsunuz. Peki bu harfler ne anlama geliyor şimdi onları anlamaya çalışalım.



Yukarıdaki şemada bize verilen çıktıdaki bilgilerin ne anlama geldiği gösterilmiştir. Şemada görüldüğü üzere çıktıının başındaki karakter bize dosyanın tipini göstermektedir. “-“ dosya olduğunu, “d” dizin (directory) olduğunu ve “l” ise bu dosyanın sembolik bir bağlantı (link) olduğunu gösterir. Windows kısayoluna benzeyen bu sembolik bağlantı, sistemdeki başka bir dosyaya veya dizine işaret eden bir dosya türüdür. İlk karakterden sonra gelen kısımları üçlü parçalar halinde inceleriz. İlk üç karakterin dosya sahibinin yetkilerini, ikinci üç karakterin grubun yetkilerini, üçüncü üç karakterin ise diğer kullanıcıların iznini gösterdiğini görüyoruz. Peki bu harfler bizlere neyi ifade ediyor.

Yetkilendirme sırasında soldan sağa “r” okuma (read), “w” yazma (write), “x” çalışma (execute) izinlerinin verildiğini gösterirken “-“ (deny) işaretini ise o işlemi gerçekleştirmeye izin verilmediğini gösterir. Örneğimizi inceleyecek üçerli gruplar halinde inceleyecek olursak ilk üçlü grup bize dosya sahibinin “rw-“ yetkisinin olduğunu yani okuma ve yazma işlemine izninin olduğunu ama çalışma izninin olmadığını anlayabiliyoruz. İkinci üçlü grupta dosyanın ait olduğu grubun izinin “-wx” olduğunu yani okuma dışındaki işlemlere izninin olduğunu görüyoruz. Son grupta ise diğer kullanıcıların “r-x” işlemlerini yani yazma işlemi dışındaki işlemlere izninin olduğunu görüyoruz.

Yukarıdaki harf ve sembollerin bulunduğu izinleri vermek için o harfin veya symbolün karşılığı olan sayılar kullanılır.

- “r” okuma komutunun değeri 4’tür
- “w” yazma komutunun değeri 2’dir
- “x” işlem komutunun değeri 1’dir
- “-“ yetkisizlendirme komutunun değeri 0’dır

Bir dosya üzerinde bu değerler kullanılarak yetkilendirme yapılacaksızda değerlerin toplamı üzerinden izinler verilir.

Yetki	Toplama	Sembol
Deny	0	---
Read	4	r--
Write	2	-w-
Execute	1	--x
Read+Write	4+2+0	rw-
Read+Execute	4+0+1	r-x
Write+Execute	0+2+1	-wx
Read+Write+Execute	4+2+1	rwx

Tablo 1 İzinlerin Sayısal Değerleri

7.1 Kullanıcıların İzinlerini Değiştirme

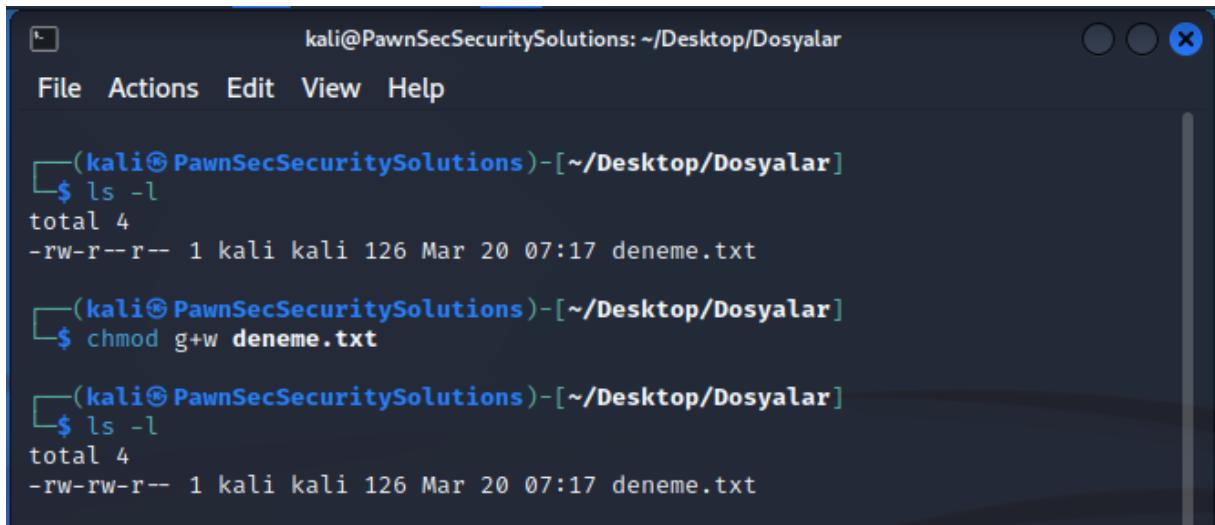
KaliLinux sisteminde izinler otomatik olarak verileceği gibi kendiniz herhangi bir kullanıcının veya grubun izinlerini değiştirebilirsınız. Bu işlemi gerçekleştirirken “chmod” komtundan yararlanabilirsiniz. Bu komut “chmod [Yetki verilecek kişiler] [Yetki ekleme çıkarma işlemi] [Yetkiler] [dosya adı]” şeklinde kullanılır. Yetki verilecek kişiler kısmında:

- “u” – dosya sahibini (user)
- “g” – dosya sahibinin grubunu (group)
- “o” – diğer kullanıcıları (others)
- “a” – tüm hakları (a)

Harflerini kullanarak işlem yapılır. Yetki ekleme çıkarma işleminin olduğu yere:

- “+” – yetki ekleme
- “=” – yetki eşitleme
- “-“ – yetki çıkarma

İşaretleri kullanılarak işlem yapılır.



A terminal window titled "kali@PawnSecSecuritySolutions: ~/Desktop/Dosyalar". The window shows a sequence of commands and their outputs:

```
(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
$ ls -l
total 4
-rw-r--r-- 1 kali kali 126 Mar 20 07:17 deneme.txt

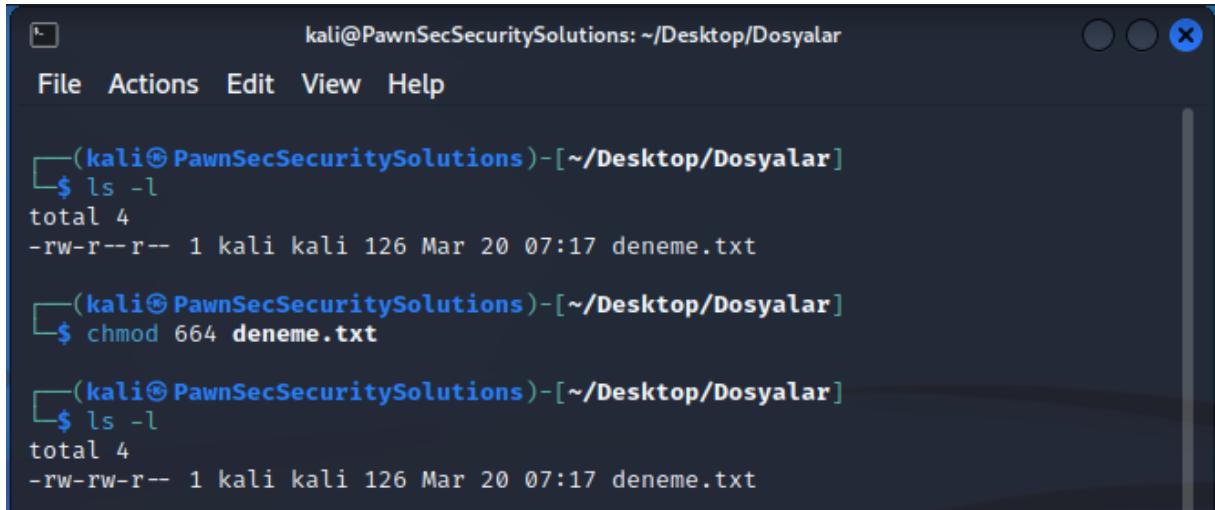
(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
$ chmod g+w deneme.txt

(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
$ ls -l
total 4
-rw-rw-r-- 1 kali kali 126 Mar 20 07:17 deneme.txt
```

Şekil 12 "chmod" Komutunun Kullanımı

Şekil 3'te "deneme.txt" isimli metin dosyamızdaki yetkinin "rw-r—r—" olduğunu görüyoruz. "chmod g+w deneme.txt" komutunu kullanarak dosyanın grup yetkilerine okuma iznini dahil etmiş oluyoruz. "chmod g=w deneme.txt" komutuyla da aynı işlemi gerçekleştirebilirdik.

Aynı şekilde Tablo 1'de verilen sayısal değerleri kullanarak ve "chmod" komutunu kullanarak da bu yetki verme/alma işlemini sağlayabiliriz.



A terminal window titled "kali@PawnSecSecuritySolutions: ~/Desktop/Dosyalar". The window shows a sequence of commands and their outputs:

```
(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
$ ls -l
total 4
-rw-r--r-- 1 kali kali 126 Mar 20 07:17 deneme.txt

(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
$ chmod 664 deneme.txt

(kali㉿PawnSecSecuritySolutions)-[~/Desktop/Dosyalar]
$ ls -l
total 4
-rw-rw-r-- 1 kali kali 126 Mar 20 07:17 deneme.txt
```

Şekil 13 "chmod" Komutunun Yetkilerin Sayısal Değerleriyle Kullanımı

Yukarıda ise "chmod 664 deneme.txt" komutunu kullanarak aynı işlemi gerçekleştirdik. Bu işlemi yaparken her sayıyı sırasıyla kullanıcının yetkisini, grup yetkisini, diğer kullanıcıların yetkisini belirtmek için kullandık. "6" sayısını "r" ve "w" yetkilerinin sayısal değerini (2+4) toplayarak gerçekleştirdik.

SUID(Set User ID)

Set User ID, herhangi bir dosyanın sahibinin full yetkiye sahip olarak diğer kullanıcılarından üstün olmasıyla sağlanan yetkilendirme türüdür. Bu yetki türünü kullanarak kullanıcı parolasını değiştirmeyi işlemeyi başka bir kullanıcıya da sağlayabilirsiniz. Bu yetkilendirmeyi "chmod 47[GrupSayıDeğeri][DiğerKullancılarınSayıDeğeri] [Dosya adı]" veya "chmod u+s [Dosya adı]" komutlarını kullanarak sağlayabiliriz. Bir dosyanın yetkileri SUID olduğunda "ls -l" yazdığınızda kullanıcı yetkilerinin olduğu üçlü kısımda "rws" değerini görebilirsiniz.

SGID(Set Group ID)

Set Group ID, herhangi bir dosyanın grubunun full yetkiye sahip olarak diğer kullanıcılarından üstün olmasıyla sağlanan yetkilendirme türüdür. SUID'den tek farkı kullanıcı yerine grubunu yetkileri en üst seviyededir. Bu yetkilendirmeyi “chmod 2[KullanıcıSayıDeğeri]7[DiğerKullanıcılarınSayıDeğeri] [Dosya adı]” veya “chmod g+s [Dosya adı]” komutlarını kullanarak sağlayabiliriz. Bir dosyanın yetkileri SGID olduğunda “ls -l” yazdığınızda grup yetkilerinin olduğu üçlü kısımda “rws” değerini görebilirsiniz.

Sticky Bit

Bu yetki türü SUID ve SGID yetkilerinden farklı olarak yetkileri diğer kullanıcılarla kısıtlamayı amaçlar. Bu yetkilendirmeyi “chmod 1[KullanıcıSayıDeğeri][GrupSayıDeğeri]7 [Dosya adı]” veya “chmod o+t [Dosya adı]” komutlarını kullanarak sağlayabiliriz. Bir dosyanın yetkileri Sticky Bit olduğunda “ls -l” yazdığınızda grup yetkilerinin olduğu üçlü kısımda “rwt” değerini görebilirsiniz. Bu işlem sayesinde diğer kullanıcıların “execute” haklarını ellerinde almış olursunuz.

Chown

Bu komutu root kullanıcısını kullanarak “chown [Kullanıcı adı]:[Grup adı] [Dosya adı]” şeklinde uygulayarak dosyamızın hangi kullanıcısını ve grubunu değiştirebiliyoruz.

Chgrp

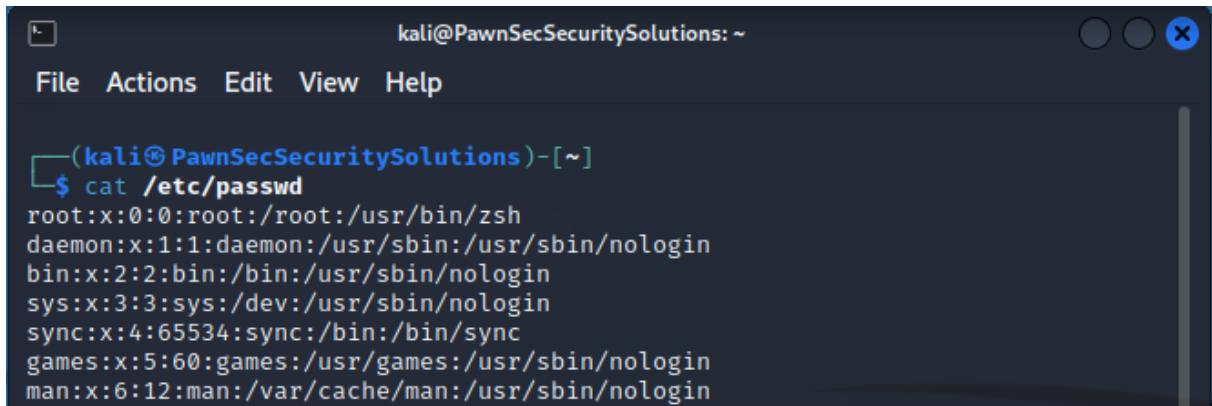
Herhangi bir dosyanın veya dizinin grup sahibini değiştirmek istersek “sudo chgrp [Grup adı] [Dosya veya dizin adı]” komutunu da kullanabilirsiniz.

7.2 Kullanıcıların ve Grupların Yönetimi

Herhangi bir sunucunun düzgün çalışması için kullanıcıları yönetmek çok önemlidir. Kullanıcı sayısı ne olursa olsun, onları etkili bir şekilde yönetmeyi öğrenmek önemlidir. Kullanıcı yönetimi, sisteme ve dizinlere erişimi, parola ilkelerini, disk kotalarını ve diğer ilkeleri yapılandırmayı içerir. Bu ilkeler, sahip olduğunuz kullanıcı sayısından bağımsız olarak aynı kalır. Kullanıcılar olmadan sunucular çalışmaz, bu da kullanıcı yönetimini sunucu yönetiminin temel bir yönü haline getirir.

7.2.1 Kullanıcıların Yönetimi

Linux sistemlerinde, üç tür kullanıcı vardır: süper kullanıcı, normal kullanıcı ve sistem kullanıcı. Her kullanıcı, sistem erişimi için bir hesaba sahiptir. Bu hesap bilgileri, “/etc/passwd” dosyasında kullanıcı türüne bakılmaksızın depolanır. Dosyada kullanıcı adı, parola, kullanıcı ve grup kimlik numaraları, tam adı, iletişim bilgileri, “/home” dizin yolu ve varsayılan komut dizini gibi bilgiler yer alır. Parolaya sahip olan kullanıcılar “x” işaretile belirtilir.



```
(kali㉿PawnSecSecuritySolutions) ~
$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
```

Şekil 14 "/etc/passwd" İçeriği

Yukarıdaki ekran görüntüsündeki "x" değerinden sonra yazılmış olan değerler UDI (User ID) ve GID (Group ID) değerlerini gösterir ve bu değerler kullanıcıların alfabetik isimlerini temsil ederler.

Linux sunucuları, birden fazla kullanıcı tarafından kullanılan çok kullanıcılı sistemlerdir. Bu nedenle, sunucuların güvenliği için kullanıcı hesapları yönetimi oldukça önemlidir. Linux'ta, üç farklı kullanıcı tipi vardır: süper/root kullanıcı, normal kullanıcı ve sistem kullanıcısı.

Süper/root kullanıcı, sistem üzerinde tüm kaynaklara sınırsız erişime sahiptir ve bu nedenle sistemi yönetmek için kullanılır. Ancak, sürekli olarak root kullanıcıyı ile işlem yapmak tehlikelidir. Yanlışlıkla bir dosya silinebilir veya bir servis durdurulabilir. Bu nedenle, güvenlik açısından daha iyi bir yaklaşım, normal bir kullanıcı hesabı oluşturmak ve bu hesaba root yetkisi atamaktır. Böylece, ihtiyaç halinde root olarak çalışıp işimiz bittiğinde normal kullanıcı hesabına geri dönebiliriz.

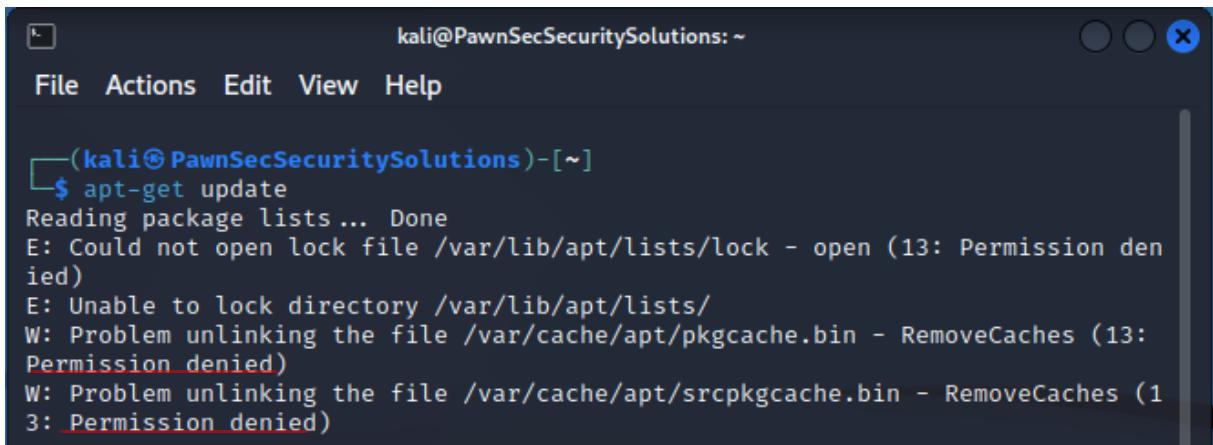
KaliLinux, Debian tabanlı bir işletim sistemi olduğu için root kullanıcıyı ilk kurulumda devre dışıdır. Ancak, kullanıcı ihtiyaçlarına göre root kullanımını aktif etmek mümkündür. Root kullanımını aktif etmek için şu adımları takip edebilirsiniz:

1. Terminali açın ve "sudo su" komutunu girin. Bu, "super user" yetkilerine sahip bir oturum açacaktır.
2. Şimdi "passwd" komutunu kullanarak root kullanıcısının parolasını ayarlayın.
3. Artık root kullanıcıyı aktif hale geldi. "exit" komutu ile super user oturumundan çıkıştırırsınız.

Root kullanıcıyı ile çalışmak, sistemi daha etkili bir şekilde yönetmenize olanak sağlar. Ancak, güvenlik açısından, root kullanıcısının yalnızca ihtiyaç duyulduğunda ve güvenli bir şekilde kullanılması önerilir. Ayrıca, yanlışlıkla bir dosya silme veya sistemi çökertme gibi risklerin de farkında olunması gerekmektedir.

Çalışması için root yetkisi gerektiren komutlara örnek verecek olursak "apt-get update" bu komutlardan birisidir. "apt-get update" komutu, Kali Linux işletim sistemindeki paket yöneticisi olan Advanced Packaging Tool (APT) tarafından kullanılan bir komuttur. Bu komut, yerel paket veritabanını güncellemek için kullanılır.

Paket yöneticisi, kullanıcının sisteme kurulu olan yazılımları güncellemesini, yeni yazılım paketlerini yüklemesini ve kaldırmasını sağlar. Ancak paket yöneticisi, sisteminizin en son paket bilgilerine sahip olmasını gerektirir. Bu nedenle "apt-get update" komutu, APT veritabanını güncellemek için kullanılır. Bu komut, Internet'teki depolardan en son yazılım paketlerinin listesini indirir ve yerel APT veritabanınızı bu bilgilerle günceller.



```
(kali㉿PawnSecSecuritySolutions)-[~]
$ apt-get update
Reading package lists... Done
E: Could not open lock file /var/lib/apt/lists/lock - open (13: Permission denied)
E: Unable to lock directory /var/lib/apt/lists/
W: Problem unlinking the file /var/cache/apt/pkgcache.bin - RemoveCaches (13: Permission denied)
W: Problem unlinking the file /var/cache/apt/srcpkgcache.bin - RemoveCaches (13: Permission denied)
```

Normal kullanıcılar “/home” dizininde kendi dosyalarını ve belgelerini saklarlar ve bu dizinlerinde kendi çalışma ortamlarını düzenleyebilirler. Bu dosyaların bir kısmı sadece kullanıcıya özeldir ve diğer kullanıcılar tarafından erişilemez, ancak bazı dosyalar diğer kullanıcılarla paylaşılabilir veya belirli gruplar tarafından okunabilir veya yazılabilir hale getirilebilir. Bu, kullanıcılara yalnızca kendi dosyalarını yönetme özgürlüğü verirken, aynı zamanda bir dizi kullanıcı hesabının etkileşimli bir şekilde çalışabilmesini sağlar.

Kullanıcılar /home dizini altında kendi klasörleri üzerinde işlem yapabilirler. Ancak, sistem çapında değişiklik yapmalarına izin verilmez. Sistem yöneticileri, izin yönetimini kullanarak kullanıcılara farklı izinler atayabilir veya mevcut izinlerini kısıtlayabilirler.

Ayrıca, Linux sistemlerinde "sistem kullanıcıı" adı verilen bir hesap türü de vardır. Bu hesap, bir şahıs tarafından kullanılan bir hesap değil, çeşitli hizmetleri çalıştıran bir yönetici hesabıdır. Sistem kullanıcılarının bir dizini veya parolası yoktur ve oturum açmalarına da izin verilmez. Sistem kullanıcıları, sistemin işleyişini sağlamak için gerekli izinlere sahiptirler ve bu nedenle, yetkilerinin düzenlenmesi tavsiye edilmez. Bu kullanıcılar, sistem yöneticileri tarafından özel olarak tanımlanırlar ve sistemde belirli bir işlevi yerine getirmek için kullanılırlar. Örneğin, Apache web sunucusu servisi genellikle "www-data" sistem kullanıcıı altında çalıştırılır.

Sistem yöneticileri, her kullanıcının izinlerini ve ayrıcalıklarını yöneterek, sistem güvenliğini korur ve istenmeyen değişikliklerin önüne geçerler. Izinler, kullanıcıların dosyalara ve dizinlere erişim düzeylerini belirler.

7.2.2 Kullanıcı Yönetim Komutları

useradd

"useradd" komutu, Kali Linux ve diğer Linux işletim sistemlerinde yeni bir kullanıcı hesabı oluşturmak için kullanılır. Bu komut, kullanıcı adı, parola, kullanıcı kimlik numarası (UID) ve grup kimlik numarası (GID) gibi kullanıcı hesabı için temel ayarları belirleyebilir. Ayrıca, kullanıcının ev dizini, kabuk seçimi, e-posta adresi gibi opsiyonel ayarlar da yapılandırılabilir. Bazı önemli parametreler şunlardır:

1. "-m" parametresi, kullanıcının ana dizinini (/home/username) oluşturur.
2. "-d" parametresi, kullanıcının ana dizinini belirlemek için kullanılır.
3. "-s" parametresi, kullanıcının varsayılan kabukunu belirler.
4. "-u" parametresi, kullanıcının kullanıcı kimliği numarasını (UID) belirler.
5. "-g" parametresi, kullanıcının birincil grubunu belirler.
6. "-G" parametresi, kullanıcının ek gruplarını belirler.
7. "-c" parametresi, kullanıcının açıklamasını belirler.

Bu parametreler, "useradd" komutu kullanılarak yeni kullanıcı hesapları oluşturulurken farklı seçenekler belirlemek için kullanılabilir.

Örneğin kullanıcı adı "test" olan ve /home dizininde "test" adında bir klasör oluşturarak yeni bir kullanıcı oluşturmak için "sudo useradd -m -s /bin/bash -c "Test" -G sudo,www-data test" komutunu kullanabilirsiniz.

Bu komutta kullanılan parametreler şu anamlara gelmektedir:

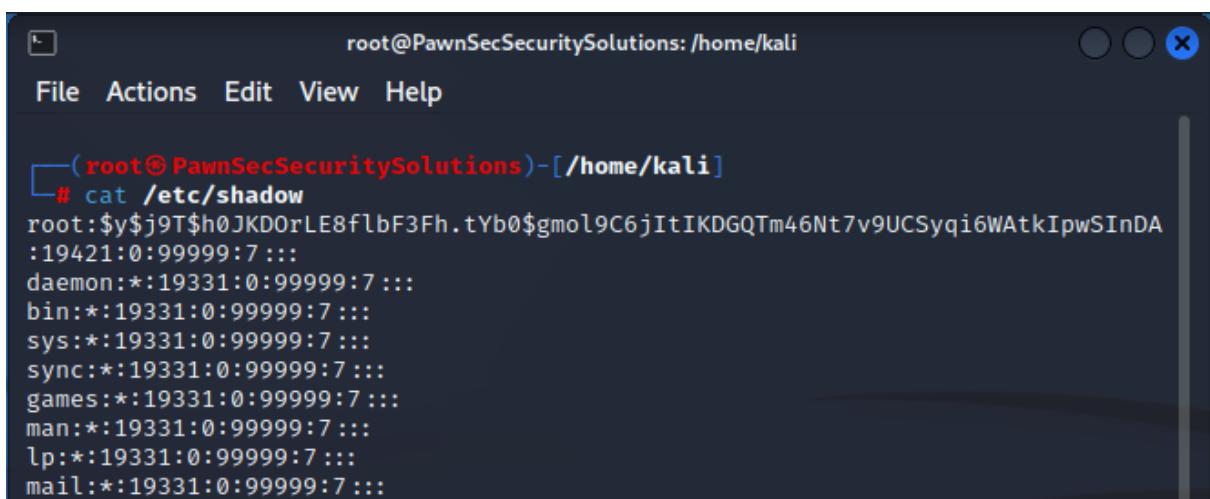
- -m: Kullanıcının ev dizininde (/home/test) varsayılan dosya ve klasörlerin oluşturulmasını sağlar.
- -s /bin/bash: Kullanıcının oturum açtığında varsayılan kabuk olarak Bash'ı kullanmasını sağlar.
- -c "Test": Kullanıcının tam adını belirtir.
- -G sudo, www-data: Kullanıcının "sudo" ve "www-data" gruplarına eklenmesini sağlar.

test: Oluşturulacak kullanıcının adıdır.

Ancak bu şekilde oluşturulan hesap için bir parola atanmadığından kullanıcı hesabı şu anda kullanılamaz.

passwd

Bu komut, Linux sistemlerinde bir kullanıcının parola değiştirmek veya yeni kullanıcıya parola atamak için kullanılır. Kullanıcı, komutu çalıştırdıktan sonra yeni bir parola girmesi istenir. Aynı zamanda kullanıcı mevcut parolasını unuttuysa, sistem yönetici parola sıfırlama işlemini gerçekleştirebilir. Bu komutun kullanımı genellikle "passwd kullanıcı_adi" şeklindedir. Bu komutu çalıştırdıktan sonra, sistem size yeni bir parola girmenizi ve ardından parolanın tekrar girilmesini isteyecektir.[



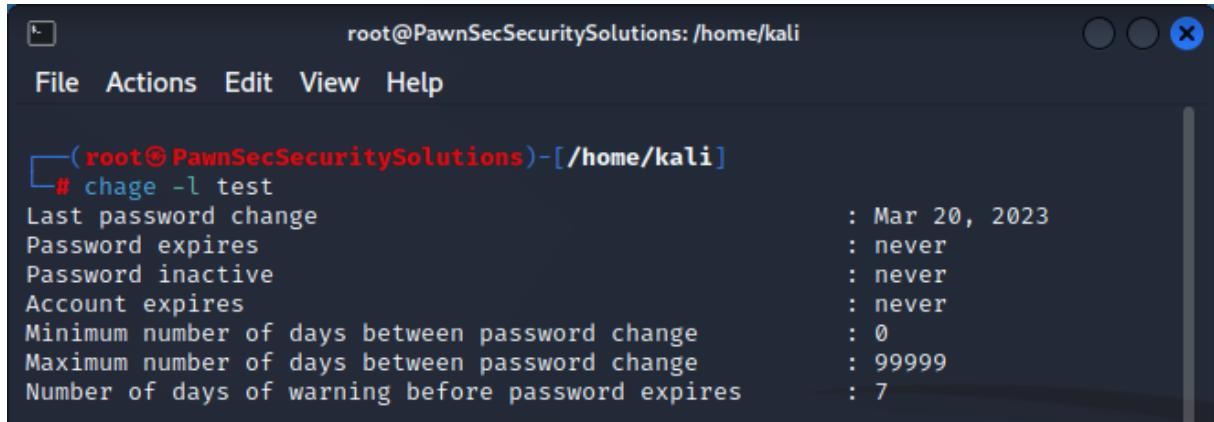
```
(root@PawnSecSecuritySolutions)-[~/home/kali]
# cat /etc/shadow
root:$y$j9T$h0JKDOrLE8flbF3Fh.tYb0$gmol9C6jItIKDGQTm46Nt7v9UCSyqi6WAtkIpwSInDA
:19421:0:99999:7 :::
daemon:*:19331:0:99999:7 :::
bin:*:19331:0:99999:7 :::
sys:*:19331:0:99999:7 :::
sync:*:19331:0:99999:7 :::
games:*:19331:0:99999:7 :::
man:*:19331:0:99999:7 :::
lp:*:19331:0:99999:7 :::
mail:*:19331:0:99999:7 :::
```

Şekil 16 root Kullanıcısının Terminalinde "cat /etc/shadow" Komutunun Çıkışı

"!" işaretini varsa o kullanıcıya parola atanmamış demektir. "*" işaretini varsa o kullanıcının sisteme erişim izni olduğunu göstermektedir. Root kullanıcısının karşısında verilmiş olan kod parolanın şifreli halidir. Bu bilgilerden sonra gelen değer 1 Ocak 1970 tarihi ile parolanızı değiştirdiğiniz tarih arasındaki gün farkıdır. Sonraki değer parolanızı kaç gün sonra değiştirebileceğinizi gösteren değerdir. Bu değer "0" olarak atanmıştır ve bu sayede istediğiniz zaman parolanızın değiştirilebilmesi sağlanmaktadır. Hemen sonraki değer parolanızın değiştirilmesinin zorunlu kılınacağı gün sayısıdır. Yani varsayılan "99999" değeri ile 99999 gün sonra parolanın değiştirilmesi gereği belirtilmiştir."7" değeri ise parola değişimine 7 gün kala kullanıcıya hatırlatma yapılacağını göstermektedir.

chage

Bu komut, Linux sistemlerinde kullanıcıların hesap bilgilerini değiştirmek için kullanılan bir komuttur. "chage" komutu, kullanıcı parolasının süresinin ne kadar geçerli olduğunu, kullanıcının son parola değiştirme tarihini, hesabın sona erme tarihini ve benzeri bilgileri ayarlamak veya görüntülemek için kullanılabilir. "chage [Kullanıcı adı]" şeklinde kullanılabilir.



```
root@PawnSecSecuritySolutions: /home/kali
File Actions Edit View Help
└─(root@PawnSecSecuritySolutions)-[/home/kali]
# chage -l test
Last password change : Mar 20, 2023
Password expires      : never
Password inactive     : never
Account expires       : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
```

Şekil 17 "chage" Komutunun Kullanımı

userdel

KaliLinux işletim sisteminde bir kullanıcı hesabını silmek için kullanılır. Kullanıcı hesabı silindiğinde, /etc/passwd, /etc/shadow, /etc/group ve diğer sistem dosyalarından kullanıcı bilgileri silinir. Ayrıca, kullanıcının ana dizini ve tüm alt dizinleri de silinir. Bununla birlikte, kullanıcının dosyalarını silmez; bu dosyalar manuel olarak silinmelidir. "userdel [Kullanıcı adı]" şeklinde kullanıma sahip olup aynı zamanda "userdel -r [Kullanıcı adı]" şeklinde "-r" parametresini de kullanarak o kullanıcıya ait her şeyin silinmesini sağlayabilirsiniz.

usermod

"usermod" komutu, Kali Linux (ve diğer Linux dağıtımları) sistemlerinde kullanıcı hesaplarını düzenlemek için kullanılan bir komuttur. Bu komut, mevcut bir kullanıcının hesap ayarlarını değiştirmek için kullanılır.

usermod komutu, aşağıdaki parametrelerden bazıları ile kullanılabilir:

- "-c": Yeni bir kullanıcı açıklaması eklemek için kullanılır.
- "-d": Kullanıcının ev dizinini değiştirmek için kullanılır.
- "-e": Kullanıcının hesap sona erme tarihini belirlemek için kullanılır.
- "-g": Kullanıcının birincil grup kimliğini değiştirmek için kullanılır.
- "-aG": Kullanıcıyı birincil grup dışında başka grplara da eklemek için kullanılır.
- "-l": Kullanıcının kullanıcı adını değiştirmek için kullanılır.
- "-s": Kullanıcının varsayılan kabuğunu değiştirmek için kullanılır.
- "-u": Kullanıcının kullanıcı kimliğini değiştirmek için kullanılır.

Örnek olarak, "usermod -aG sudo kali" komutu, "kali" kullanıcısını "sudo" grubuna ekler. Bu, "kali" kullanıcısına sudo ayrıcalıklarının verilmesine izin verir.

7.2.3 Grupların Yönetim Komutları

Linux sistemlerindeki gruplar, kullanıcı yönetimini kolaylaştırarak, her bir kullanıcıya ayrı ayrı izin atamak yerine, gruplar aracılığıyla birçok kullanıcıya aynı anda izin vermek veya iptal etmek için kullanılır. Yöneticiler, gruplar aracılığıyla kullanıcıları bir araya getirerek, ortak bir dizin altında işlemler yapmalarını sağlayabilir ve izinleri grup seviyesinde yönetebilirler. Bu sayede, kullanıcı yönetimi ve izin verme süreçlerinin daha hızlı gerçekleşmesi sağlanır.

UYGULAMA

```
└──(root㉿PawnSecSecuritySolutions)-[]  
└─# id kali  
uid=1000(kali) gid=1000(kali) groups=1000(kali)  
└──(root㉿PawnSecSecuritySolutions)-[]  
└─# groupadd yenigrup  
└──(root㉿PawnSecSecuritySolutions)-[]  
└─# usermod -G yenigrup kali  
└──(root㉿PawnSecSecuritySolutions)-[]  
└─# id kali  
uid=1000(kali) gid=1000(kali) groups=1000(kali),1002(yenigrup)  
└──(root㉿PawnSecSecuritySolutions)-[]  
└─# deluser kali yenigrup  
Removing user 'kali' from group 'yenigrup' ...  
Done.  
└──(root㉿PawnSecSecuritySolutions)-[]  
└─# id kali  
uid=1000(kali) gid=1000(kali) groups=1000(kali)  
└──(root㉿PawnSecSecuritySolutions)-[]  
└─# groupdel yenigrup
```

31.Betikte de görüldüğü üzere “groupadd” komutu grup eklemek için kullanılır. “groupdel” komutu grup silmek için kullanılır. “deluser” komutu kullanıcıyı gruptan atmak için kullanılır. Ayrıca “gpasswd” komutunu kullanarak gruba bir parola da oluşturabilirsiniz.

```

(kali㉿PawnSecSecuritySolutions)-[~]
$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:kali
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:

```

Şekil 18 "cat /etc/group" Komutuyla Grupların Görüntülenmesi

7.2.4 Sudo Komutu ve Sudoers Dosyası

"sudo" komutu, Kali Linux (ve diğer Linux dağıtımları) sistemlerindeki kullanıcıların, yalnızca belirli işlemleri kök (root) kullanıcıyı yetkileriyle çalıştırmasını sağlayan bir araçtır. "sudo" komutu, bir kullanıcının, "sudoers file" adlı yapılandırma dosyasında tanımlı olan işlemleri yalnızca belirli koşullar altında gerçekleştirmesine izin verir. Bu sayede, tüm kullanıcılar kök kullanıcıyı yetkilerine sahip olmaz ve sistemin güvenliği artar.

"Sudoers file", "sudo" komutunun nasıl çalışacağını belirleyen yapılandırma dosyasıdır. Bu dosya, "/etc/sudoers" konumunda bulunur ve yalnızca root kullanıcı tarafından düzenlenebilir. "Sudoers file", kullanıcıların hangi komutları çalıştırabileceğini, hangi kullanıcıların belirli işlemleri çalıştırabileceğini ve hangi kullanıcıların hangi koşullar altında belirli işlemleri çalıştırabileceğini belirler.

"Passwd" komutunu anlattığımız başlığın altındaki "apt-get update" komutunu hatırlatmakta fayda var. "sudo apt-get update" komutu, "apt-get" paket yöneticisi aracılığıyla sistemdeki tüm paketlerin güncellenmesini sağlar. Ancak, bu işlem "sudoers file" dosyasında tanımlı olmadan, sadece root kullanıcısı tarafından gerçekleştirilebilir. Başka bir kullanıcı, "sudo" komutunu kullanarak yalnızca belirli koşullar altında bu işlemi gerçekleştirebilir.

Dosyayı "nano" komutuyla inceledikten sonra "User privilege specification" başlığı altına bakacak olursak herhangi bir kullanıcının hangi kullanıcılar ve gruplar üzerinde hangi yetkilere sahip olduğunu görüntüleyebiliriz.



"Sudo" komutuyla root olmayan bir kullanıcıda bir komut çalıştırduğumda bizden kullanıcı parolamızı girmemizi isteyecektir. Bu tür komutları kullanırken parola girilmesini istemiyorsak kullanıcı satırının sonundaki 'ALL' ifadesinden önce 'NOPASSWD:' argümanını eklemelisiniz.

```
GNU nano 6.4                               /etc/sudoers.tmp

#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# This fixes CVE-2005-4890 and possibly breaks some versions of kdesu
# (#1011624, https://bugs.kde.org/show_bug.cgi?id=452532)
Defaults    use_pty

# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"

# This allows running arbitrary commands, but so does ALL, and it means
# different sudoers have their choice of editor respected.
#Defaults:%sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
#Defaults:%sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_"

# Per-user preferences; root won't have sensible values for them.
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root      ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo    ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:
@includedir /etc/sudoers.d

^G Help      ^Q Write Out   ^W Where Is   ^K Cut          ^T Execute     ^C Location   M-U Undo
^X Exit      ^R Read File   ^\ Replace    ^U Paste        ^J Justify    ^/ Go To Line M-E Redo
```

Şekil 19 "nano /etc/sudoers" Komutıyla "Sudoers" Dosyasının İncelenmesi

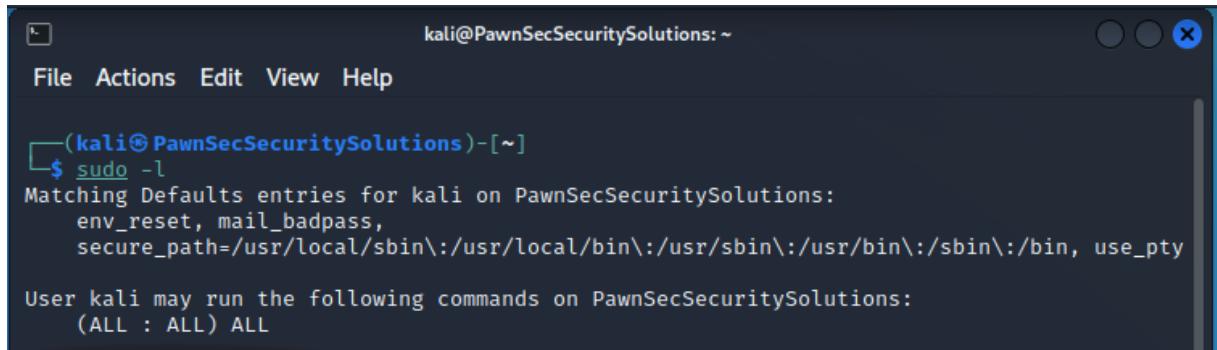
"Sudoers file" içerisinde, "aliaslar" adı verilen bir özellik bulunur. Aliaslar önceden de anlatmış olduğumuz, belirli bir komut veya grubunu temsil eden kısa bir isim veya semboldür. Aliaslar, "sudoers file" dosyasını daha okunaklı hale getirebilir ve tekrarlanan kodları azaltarak dosya boyutunu azaltabilir. Örneğin "alias ADMINUSERS = [Kullanıcı isimleri]" şeklinde kullanacağımız bir komut sayesinde "ADMINUSERS" adında bir alias tanımlayabilirsiniz. Alias, yazmış olduğunuz kullanıcıları temsil eder. Alias'ı daha sonra, "sudoers file" içinde belirli bir komut için kullanabilirsiniz.

Örneğin:

ADMINUSERS ALL=(ALL) ALL

Vermiş olduğumuz örnekte, "ALL" anahtar kelimesi, tüm komutlar için izin verildiği anlamına gelir. Böylece, girmiş olduğunuz kullanıcılar, tüm komutları "sudo" komutunu kullanarak çalıştırabilirler.

Oturumdaki kullanıcının yetkilerinin ne olduğu öğrenmek isterseniz "sudo -l" komutunu kullanmanız yeterli olacaktır.



```
kali@PawnSecSecuritySolutions: ~
File Actions Edit View Help
└─(kali㉿PawnSecSecuritySolutions)-[~]
$ sudo -l
Matching Defaults entries for kali on PawnSecSecuritySolutions:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User kali may run the following commands on PawnSecSecuritySolutions:
    (ALL : ALL) ALL
```

20.Şekilde "kali" kullanıcısının her komutu çalışma yetkisine sahip olduğunu görüyoruz.

8 İşlemlerin Yönetimi

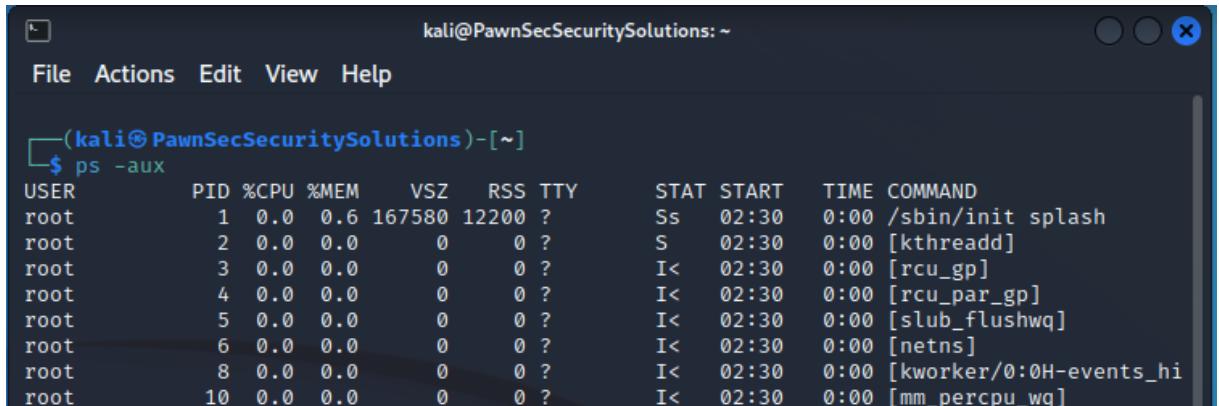
Kalilinux sistemi de diğer Linux sistemlerinde olduğu gibi işlem yönetimi konusunda çeşitli araçlar sunar. Bu araçlar sayesinde kullanıcılar sisteme çalışan işlemleri takip edebilir, yönetebilir ve gerektiğinde müdahale edebilirler.

İşlem yönetimi için kullanılan en temel araçlardan biri "**ps (process status)**" komutudur. "ps" komutu kullanılarak çalışan işlemlerin listesi ve detaylı bilgileri görüntülenebilir. Bu bilgiler arasında işlem kimliği (PID), çalışma süresi, CPU kullanımı, bellek kullanımı, komut satırı parametreleri ve daha birçok detay yer alabilir.

"ps" komutu, sistem yöneticilerinin ve kullanıcıların, sisteme çalışan işlemleri izlemelerine ve gerekirse bu işlemleri sonlandırmalarına yardımcı olur. Ancak, yanlış kullanımı veya yanlış anlaşılması, sistem hatalarına ve veri kaybına neden olabilir. Bu nedenle, "ps" komutunun kullanımı konusunda dikkatli olunmalıdır.

"ps" komutu, birçok farklı parametreye birlikte kullanılabilir. Bazı temel kullanım şekilleri şunlardır:

1. "**ps -aux**": Tüm kullanıcıların çalışan işlemlerinin ayrıntılarını gösterir.



```
kali@PawnSecSecuritySolutions: ~
File Actions Edit View Help
└─(kali㉿PawnSecSecuritySolutions)-[~]
$ ps -aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      1  0.0  0.6 167580 12200 ?        Ss   02:30   0:00 /sbin/init splash
root      2  0.0  0.0     0    0 ?        S    02:30   0:00 [kthreadd]
root      3  0.0  0.0     0    0 ?        I<   02:30   0:00 [rcu_gp]
root      4  0.0  0.0     0    0 ?        I<   02:30   0:00 [rcu_par_gp]
root      5  0.0  0.0     0    0 ?        I<   02:30   0:00 [slub_flushwq]
root      6  0.0  0.0     0    0 ?        I<   02:30   0:00 [netns]
root      8  0.0  0.0     0    0 ?        I<   02:30   0:00 [kworker/0:0H-events_hi]
root     10  0.0  0.0     0    0 ?        I<   02:30   0:00 [mm_percpu_wq]
```

Şekil 21 "ps -aux" Komutunun Çıktısı

Şekil 21'de "ps -aux" komutunun hemen altındaki satırda bazı başlıklar ve bu başlıklara ait değerler görüyoruz. Peki bu başlıklar ne anlama geliyor.

- **USER:** İşlemi çalıştan kullanıcıyı gösterir.
- **PID (Process ID):** İşlemenin ID'sidir. İşlemi durdurup, başlatmak ve takip etmek için bu ID kullanılır.
- **%CPU:** İşlemci kullanım miktarnı gösterir.
- **%MEM:** Bellek kullanım miktarnı gösterir.
- **VSZ (Virtual Memory Size):** İşlemenin erişebileceğini bellek miktarıdır.
- **RSS (Resident Set Size):** İşleme atanen bellek miktarıdır.
- **TTY:** İşlemenin gerçekleştigi terminal tipini gösterir.
- **STAT (Status):** İşlemenin durumunu gösterir.
- **TIME:** İşlemenin CPU kullanım süresini gösterir.
- **COMMAND:** İşlemenin kendisini gösterir.

STAT kolonundaki harflerin ve sembollerin anlamlarına bakacak olursak:

- **R:** İşlem, çalışıyor demektir.
 - **S:** İşlem, uyuyor (sleep) demektir.
 - **D:** İşlem, disk girdisi bekliyor (disk wait) demektir.
 - **Z:** İşlem, zombi demektir. Bu işlem çeşidini bir çocuk işlemi öldürdü, ancak ebeveyn işlem onu henüz öldürmedi şekilde özetteyebiliriz. Bu nedenle, işlem hala sistemin işlem tablosunda yer alır ancak kaynakları kullanmaz ve işlem sonlandırılamaz. Zombi işlemleri, sistem kaynakları tüketerek sistem performansını olumsuz etkileyebilirler. Zombi işlemleri, "ps -aux" komutuyla kolayca tespit edilebilirler ve sonlandırılabilirler. "kill" komutu kullanılarak, zombi işlemleri sonlandırıbilirisiniz.
 - **T:** İşlem, duraklatıldı (stopped) demektir.
 - **<:** Öncelikli işlem olduğunu gösterir.
 - **N:** Düşük öncelikli işlem olduğunu gösterir.
 - **s:** Oturum lideri olduğunu gösterir. Oturumdaki ilk süreç anlamına da gelir.
 - **I:** Çoklu işlem anlamına gelir.
 - **+: Önyüzde çalışan işlem.**
2. **"ps -ef":** Tüm işlemlerin ayrıntlarını, ana süreç kimliği (PID) dahil, ağaç yapısı olarak gösterir.
 3. **"ps -e":** Sisteminde çalışan tüm işlemleri listeler.
 4. **"ps -f":** Tüm işlemlerin ayrıntlarını, ana süreç kimliği (PID), ebeveyn süreç kimliği (PPID) ve diğer bilgiler dahil, daha ayrıntılı bir şekilde gösterir. Bahsetmiş olduğumuz PID ve PPID değerlerini takip ederek hangi işlemin hangi işlem tarafından gerçekleştirildiğinin takibini gerçekleştirebiliyoruz.
 5. **"ps -ao [Başlıklar]":** Bu komutu kullanarak çıktınızı özelleştirebilirisiniz. Bu komutta yalnızca başlıklar kısmasına girdığınız değerler hakkında bilgi edinirsiniz.

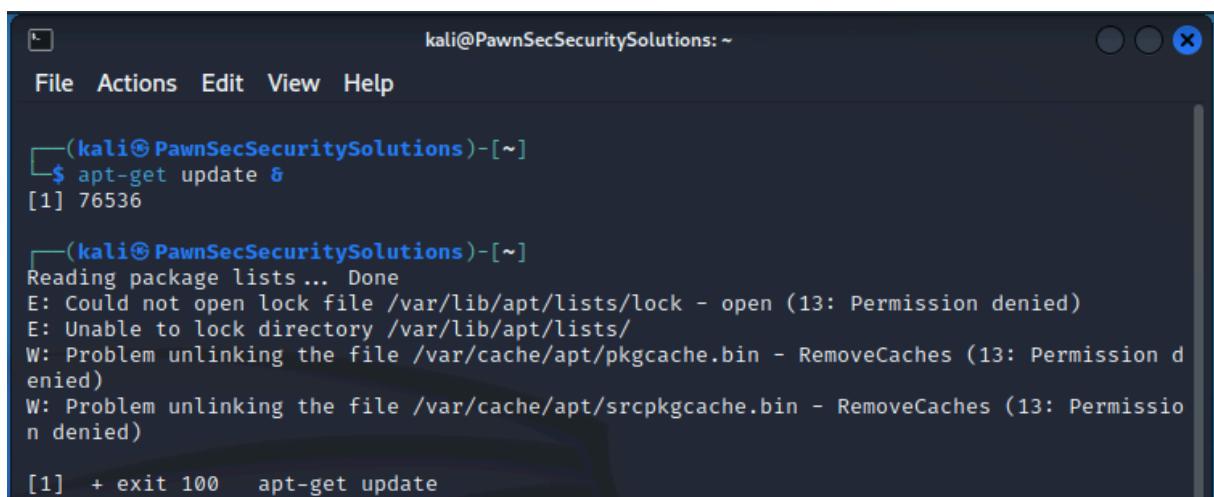
Ayrıca spesifik bir kullanıcıya ait işlemlerle ilgili bilgi edinmek istiyorsanız "ps -aux | grep [Kullanıcı adı]" şeklindeki komutunu kullanabilirisiniz.

8.1 Foreground ve Backgorund İşlemler

Linux işletim sistemi, kullanıcılarla hem ön plan (foreground) hem de arka plan (background) işlemlerini çalışma imkanı sunar.

- **Ön plan işlemleri:** Kullanıcının doğrudan etkileşimde olduğu işlemlerdir. Örneğin, bir terminal penceresinde çalışan bir program, bir ön plan işlemidir. Bu tür işlemler, terminale girilen komutların tamamlanmasını bekleyerek terminalin bloke olmasına neden olabilir. İşlemi sonlandırmak için "Ctrl+C" tuş kombinasyonunu kullanabilirsiniz.
- **Arka plan işlemleri:** Kullanıcının doğrudan etkileşimde olmadığı işlemlerdir. Örneğin, bir dosya indirme işlemi veya bir yedekleme işlemi, arka plan işlemi olarak çalıştırılabilir. Bu tür işlemler, kullanıcıların diğer işlemlerini yapmasına olanak tanır ve işlemler tamamlandığında bildirimler ile kullanıcıya haber verirler.

Kullanıcılar, bir işlemi arka plana almak veya arka plandan ön plana almak için "Ctrl + Z" tuşlarına basarak işlemi duraklatabilirler. Ardından, "bg" veya "fg" komutları kullanılarak işlem arka plana veya ön plana alınabilir.



```
(kali㉿PawnSecSecuritySolutions)-[~]
$ apt-get update &
[1] 76536

(kali㉿PawnSecSecuritySolutions)-[~]
Reading package lists ... Done
E: Could not open lock file /var/lib/apt/lists/lock - open (13: Permission denied)
E: Unable to lock directory /var/lib/apt/lists/
W: Problem unlinking the file /var/cache/apt/pkgcache.bin - RemoveCaches (13: Permission d
enied)
W: Problem unlinking the file /var/cache/apt/srcpkgcache.bin - RemoveCaches (13: Permissio
n denied)

[1] + exit 100    apt-get update
```

Şekil 22 Bir Komutu Arka Planda Çalıştırma

Yukarıdaki örnekte olduğu gibi kodlarımızın sonuna “&” işaretini koyarak o kodun arka planda çalışmasını sağlayabiliyoruz. Bu işlem başladığında bize çıktı olarak “76536” PID kodunun verildiğini görüyoruz. Bu kodun çalışmasını, kaynak tüketimi gibi bilgileri “Ctrl+Z” ile durduruktan sonra “ps -aux” komutunu kullanarak takip edebiliriz. Son satırda “exit 100” çıktılarıyla komutun işlemini çoxtan yerine getirmiş olduğunu öğreniyoruz.

8.2 İşlem Önceliğini Ayarlama ve İşlem Sonlandırma Komutları

Linux işletim sistemi, kullanıcılarla işlem önceliği ayarlama imkanı sağlar. İşlem önceliği, bir işlemin sistem kaynaklarına erişim sırasını belirler. Daha yüksek bir önceliğe sahip bir işlem, sistem kaynaklarına daha önce erişebilir ve diğer işlemlerden daha fazla kaynak kullanabilir. İşlem önceliği ayarlamak için "nice", "renice" ve "kill" komutları kullanılabilir.

- "**nice**" komutu, bir işlemin önceliğini ayarlamak için kullanılır. Komut, bir işlemi başlatırken, işlem önceliğini belirlemek için "-n" parametresi ile kullanılır. Örneğin, "nice -n 10 program" komutu, "program" adlı işlemi öncelik seviyesi 10'a ayarlayarak başlatır.
- "**renice**" komutu, bir işlemin önceliğini ayarlamak için kullanılır. Komut, bir işlem çalışırken, işlem önceliğini değiştirmek için kullanılır. Örneğin, "renice -n 5 1234" komutu, işlem kimliği 1234 olan bir işlemi öncelik seviyesi 5'e ayarlar.
- "**kill**" komutu, çalışan bir işlemi sonlandırmak için kullanılır. Komut, bir işlemi sonlandırmak için "-9" parametresi ile kullanılabilir. Örneğin, "kill -9 1234" komutu, işlem kimliği 1234 olan bir işlemi anında sonlandırır.
- "**killall**" komutu bir kullanıcıya ait tüm işlemleri sonlandırmak için kullanılır.

İşlem önceliği ayarlama ve işlem sonlandırma işlemleri, sistem yöneticilerine sistem performansını yönetmek ve gerektiğinde müdahale etmek için kullanışlı bir araç sağlar. Ancak, bu işlemlerin yanlış kullanımı, sisteme ciddi zararlar verebilir, bu nedenle dikkatli kullanılmalıdır.

9 Sistem Performansının Görüntülenmesi

Bildığınız üzere "**ps -aus**" komutunu kullanarak sistemde gerçekleşen işlemlerle ilgi bilgiler edinebiliyoruz. Bu komut sayesinde CPU kullanımı gibi sistem performansı hakkında bilgileri görebiliyoruz. Bu komutun yetersiz kaldığı zamanlarda sistem performansının görüntülenmesi ve ayarlanması için bir dizi araç mevcuttur.

top

"**top**", Linux işletim sistemlerinde, sistem performansını izlemek için kullanılan bir araçtır. Bu araç, işlemci kullanımı, bellek kullanımı, disk giriş/çıkış istatistikleri ve ağ trafiği gibi sistem kaynaklarına ilişkin bilgileri görüntüler. "**top**" foreground bir araç olduğu kullanımını gerçekleştirirken başka bir komut yazmanız mümkün değildir. Bu nedenle bu araç çalışırken herhangi bir işlem yapmak isterseniz yeni bir oturum açarak bunu gerçekleştirebilirsiniz.

```

kali@PawnSecSecuritySolutions: ~
File Actions Edit View Help
top - 07:57:11 up 5:26, 1 user, load average: 0.00, 0.01, 0.00
Tasks: 154 total, 1 running, 153 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.7 us, 0.5 sy, 0.0 ni, 98.8 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 1981.2 total, 639.8 free, 613.6 used, 727.8 buff/cache
MiB Swap: 1024.0 total, 1024.0 free, 0.0 used. 1192.3 avail Mem

      PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
      581 root      20   0  400200 150652 55336 S  1.0  7.4  0:52.24 Xorg
      1 root      20   0 167580 12204 9008 S  0.3  0.6  0:00.85 systemd
     180 root     -51   0      0      0      0 S  0.3  0.0  0:00.95 irq/18-vmwgfx
     333 root      20   0  27016  7252 4592 S  0.3  0.4  0:00.41 systemd-udevd
     468 message+  20   0  10080  5816 4296 S  0.3  0.3  0:01.43 dbus-daemon
     471 root      20   0  25376  7876 6840 S  0.3  0.4  0:00.18 systemd-logind
    50986 kali     20   0  465252 104252 85492 S  0.3  5.1  0:02.26 qterminal
      2 root      20   0      0      0      0 S  0.0  0.0  0:00.00 kthreadd
      3 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 rcu_gp
      4 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 rcu_par_gp

```

Şekil 23 "top" Aracının Terminal Görüntüsü

Ekran görüntüsündeki terminalde ilk satırda başlayacak olursak soldan sağa sırasıyla:

- Geçerli tarih bilgisi, saat bilgisi, sistem zamanı, çalışma süresi ve son 1, 5, 15 dakikadaki yüzde cinsinde yük miktarını
- Toplam işlem, çalışan işlem ve uyuyan işlem sayısı
- CPU kullanımı ve yüzdeleri
 - us:** Kullanıcıların çalıştırıldığı işlemlerin yüzdesi.
 - sy:** Kernel mode'da sistem çağrıları ve sürücü erişimleri için harcanan süre.
 - ni:** Öncelik verilen işlemler için harcanan zamanın yüzdesi.
 - id:** İşlemcinin boşta geçirdiği sürenin yüzdesi.
 - wa:** İşlemcinin disk istekleri için beklediği süredir. Yüksek değerler düşük depolama performansını işaret eder.
 - hi:** İşlemcinin donanım kesintileri için harcadığı süredir. Bu değerin yüksek olması donanım tarafında problemlerin olduğunu göstergesidir.
 - si:** İşlemcinin yazılım tarafından kesintiler için harcadığı süredir. Bu değerin yüksek olması yazılım tarafında problemlerin olduğunu gösterir.
 - st:** Eğer bir sanallaştırma ortamınız varsa buradaki değer sanal sunucuların kullanım yüzdesini gösterir.
- Bellek (Fiziksel bellek) kullanımı ve yüzdeleri
- Swap (Sanal bellek) kullanımı ve yüzdeleri

Hakkında bilgileri bize gösterdiğini anlıyoruz.

Yukarıda görüldüğü üzere “ps” komutu gibi bizlere detaylı bir grafik sunan bu komut sayesinde sistem performansını analiz edebiliriz. Ayrıca tablodaki değerlere bakılacak olursa en fazla kaynak kullanan işleminden en az kaynak kullanan işleme doğru bir sıralamanın olduğu görülüyor. Tabloda PID (işlem kimlik numarası), kullanıcı adı, CPU kullanımı yüzdesi, bellek kullanımı, komut adı gibi işlem özniteliklerine ait bilgiler bulunmaktadır.

free

Bu komutu kullanarak hem fiziksel hem sanal bellek hakkında bilgiler sunar. “free –[boyut ismi]” komutu kullanılarak hangi depolama boyutunda çıktı almak istediğiniz seçerek bellek kullanımları hakkında bilgi edinebilirsiniz.

```
└─(kali㉿PawnSecSecuritySolutions)-[~]
└─$ free --mega

      total        used        free      shared  buff/cache   available
Mem:       2077         672         640          5         764        1221
Swap:      1073           0        1073
```

Yukarıdaki çıktında, "total" RAM ve SWAP toplam bellek mictarını, "used" kullanılan bellek mictarını, "free" kullanılabilir bellek mictarını, "shared" belleği paylaşan süreçlerin sayısını, "buff/cache"

önbellek ve önbellek bellek miktarını ve "available" sistemin kullanılabilir bellek miktarını göstermektedir.

Ayrıca, "free" komutunun farklı seçenekleri de vardır. Örneğin, "free -h" komutu, bellek miktarlarını daha anlaşılır bir formatta (GB, MB, KB) gösterir. "free -s [interval]" komutu ise belirli bir süre aralığında bellek kullanımını sürekli olarak gösterir.

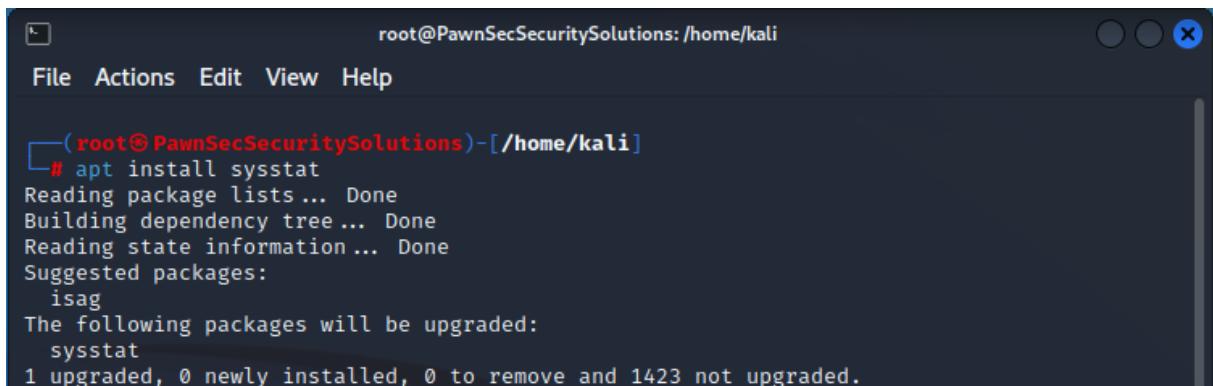
vmstat

Açılımı "Virtual Machine Stat" olan bu cihaz sayesinde makinenizi boot ettiğiniz zamandan itibaren gerçekleşen ortalama bellek kullanımı, CPU kullanımı gibi bilgiler sunar.

```
└─(kali㉿PawnSecSecuritySolutions)-[~]
  └─$ vmstat
    procs -----memory----- --swap-- ----io---- -system-- -----cpu-----
    r b swpd free buff cache si so bi bo in cs us sy id wa st
    0 0 0 645000 155868 590464 0 0 14 3 580 212 0 0 99 0 0
```

sysstat

"sysstat" aracı, Linux işletim sistemlerinde kullanılan bir sistem izleme aracıdır. Sisteme yüklü olarak gelmediği için "apt install sysstat" komutunu terminalde çalıştırarak yüklenmesini sağlıyoruz.



```
root@PawnSecSecuritySolutions:/home/kali
File Actions Edit View Help
└─(root㉿PawnSecSecuritySolutions)-[/home/kali]
# apt install sysstat
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  isag
The following packages will be upgraded:
  sysstat
1 upgraded, 0 newly installed, 0 to remove and 1423 not upgraded.
```

Şekil 24 "apt install" Komutuyla "sysstat" Aracının Kurulumu

"sysstat" aracı, CPU, bellek, disk girdi/çıktısı, ağ kullanımı ve diğer sistem kaynaklarının izlenmesi için bir dizi araç sağlar. Ayrıca, "sysstat" aracı, "sar", "mpstat", "pidstat" ve "iostat" gibi alt araçlara sahiptir. Kısacası bize daha düzenli bir şekilde daha ayrıntılı bilgiler sunan ve bir çok alt aracın birleşmesinde oluşan performans ön izleme aracıdır.

"sysstat" aracının **"sar"** komutu, sistem performansını kaydetmek için kullanılır. Bu komut, CPU, bellek ve disk kullanımını, ağ trafigini ve diğer sistem kaynaklarını belirli bir aralıkta kaydeder. Kaydedilen veriler daha sonra analiz edilebilir veya grafikler oluşturulabilir.

```

root@PawnSecSecuritySolutions: ~
File Actions Edit View Help
[(root@PawnSecSecuritySolutions)-[~]
# sar 1 3
Linux 6.0.0-kali3-amd64 (PawnSecSecuritySolutions)        03/23/2023      _x86_64_      (2 CPU)

09:05:22 AM    CPU    %user    %nice   %system   %iowait   %steal    %idle
09:05:23 AM    all    0.50     0.00    0.50     0.00     0.00    99.00
09:05:24 AM    all    0.51     0.00    0.51     0.00     0.00    98.98
09:05:25 AM    all    0.50     0.00    0.50     0.00     0.00    99.00
Average:       all    0.50     0.00    0.50     0.00     0.00    98.99

```

Şekil 25 "sysstat" ile Gelen "sar" Komutunun Kullanımı

"mpstat" komutu, CPU kullanımını izlemek için kullanılır. Bu komut, her bir işlemcinin kullanımını ayrıntılı olarak gösterir. Ayrıca, CPU kullanımı, bekleyen işler ve çalışan işler gibi diğer bilgileri de gösterir.

```

kali@PawnSecSecuritySolutions: ~/Desktop
File Actions Edit View Help
[(kali@PawnSecSecuritySolutions)-[~/Desktop]
$ mpstat 1 3
Linux 6.0.0-kali3-amd64 (PawnSecSecuritySolutions)        03/23/2023      _x86_64_      (2 CPU)

09:22:06 AM  CPU    %usr    %nice   %sys %iowait   %irq    %soft   %steal   %guest   %gnice   %idle
09:22:07 AM  all    0.00     0.00    0.51    0.00     0.00     0.00     0.00     0.00     0.00     0.00    99.49
09:22:08 AM  all    0.50     0.00    0.50    0.00     0.00     0.00     0.00     0.00     0.00     0.00    98.99
09:22:09 AM  all    0.00     0.00    0.51    0.51     0.00     0.00     0.00     0.00     0.00     0.00    98.99
Average:     all    0.17     0.00    0.51    0.17     0.00     0.00     0.00     0.00     0.00     0.00    99.16

```

Şekil 26 "sysstat" ile Gelen "mpstat" Komutunun Kullanımı

"iostat" komutu, disk kullanımını izlemek için kullanılır. Bu komut, disk okuma/yazma oranlarını, disk kullanım yüzdesini ve disk giriş/çıkış işlemlerini gösterir.

```

root@PawnSecSecuritySolutions: ~
File Actions Edit View Help
[(root@PawnSecSecuritySolutions)-[~]
# iostat
Linux 6.0.0-kali3-amd64 (PawnSecSecuritySolutions)        03/23/2023      _x86_64_      (2 CPU)

avg-cpu:  %user    %nice   %system %iowait   %steal    %idle
          0.29     0.00    0.38    0.02     0.00    99.31

Device      tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd
sda       2.27     31.80      9.78      0.00    746539    229653         0

```

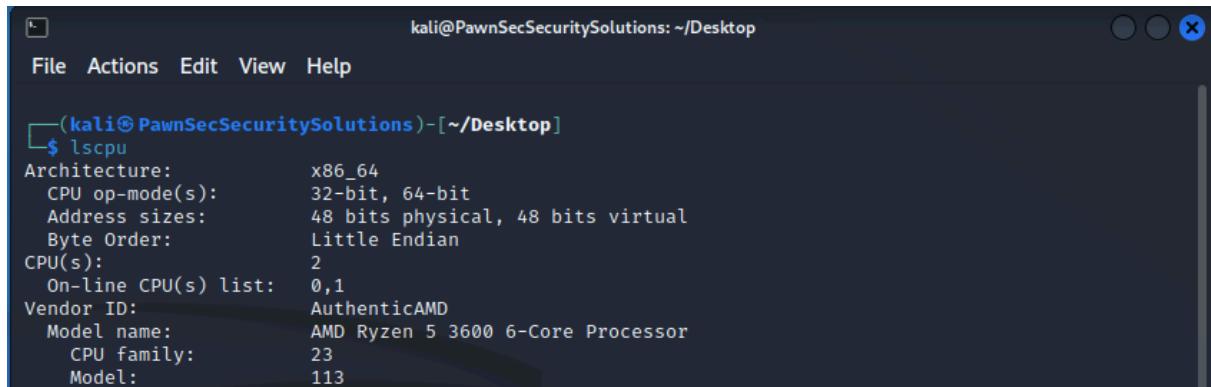
Şekil 27 "sysstat" ile Gelen "iostat" Komutunun Kullanımı

ls

Önceden anlatmış olduğumuz “ls” komutu sadece dizin içeriği hakkında bize bilgi vermekle kalmayıp aynı zamanda başka görevler de üstlenmektedir. Bu komutlara terminal satırına ls yazdıktan sonra iki kez “Tab” tuşuna basarak erişebilirsiniz. Şimdi bu komutların bazıları hakkında bilgi edinelim.

lscpu

Sistemdeki CPU (Central Processing Unit) özelliklerini görüntülemek için kullanılan bir komuttur. lscpu komutu, işlemcinin mimarisini, çekirdek sayısını, saat hızını, bellek hiyerarşisini, CPU ailesini ve diğer bilgileri görüntüler.

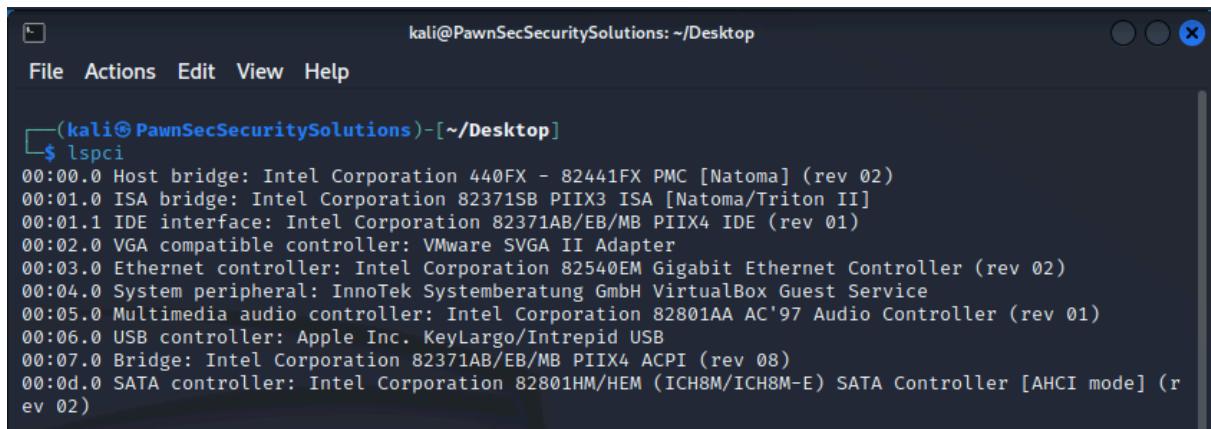


```
kali@PawnSecSecuritySolutions: ~/Desktop
File Actions Edit View Help
└─(kali㉿PawnSecSecuritySolutions)-[~/Desktop]
$ lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Address sizes:         48 bits physical, 48 bits virtual
Byte Order:            Little Endian
CPU(s):                2
On-line CPU(s) list:  0,1
Vendor ID:             AuthenticAMD
Model name:            AMD Ryzen 5 3600 6-Core Processor
CPU family:            23
Model:                 113
```

Şekil 28 "lscpu" Komutunun Çıktısı

lspci

PCI (Peripheral Component Interconnect) aygıtlarının listesini görüntülemek için kullanılan bir komuttur. “lspci” komutunu kullanarak, işlemciye takılmış tüm donanım aygıtlarını ve PCI köprülerini listelemek mümkündür.



```
kali@PawnSecSecuritySolutions: ~/Desktop
File Actions Edit View Help
└─(kali㉿PawnSecSecuritySolutions)-[~/Desktop]
$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371AB/EB/MB PIIX4 IDE (rev 01)
00:02.0 VGA compatible controller: VMware SVGA II Adapter
00:03.0 Ethernet controller: Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02)
00:04.0 System peripheral: InnoTek Systemberatung GmbH VirtualBox Guest Service
00:05.0 Multimedia audio controller: Intel Corporation 82801AA AC'97 Audio Controller (rev 01)
00:06.0 USB controller: Apple Inc. KeyLargo/Intrepid USB
00:07.0 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 08)
00:0d.0 SATA controller: Intel Corporation 82801HM/HEM (ICH8M/ICH8M-E) SATA Controller [AHCI mode] (r
ev 02)
```

Şekil 29 "lspci" Komutunun Çıktısı

lsof

"lsof" komutu, "List Open Files" kelimelerinin kısaltmasıdır ve açık dosyaları ve açık ağ bağlantılarını listelemek için kullanılır. Bu komut, sistemde çalışan tüm süreçleri görüntülemek için kullanılabilir ve bu süreçlerin her biri için açık dosyaların ve soketlerin bir listesini sağlar. Ayrıca, "lsof" komutu, sistemdeki bir dosyayı hangi sürecin kullanıyor olduğunu da belirtir.

```

kali@PawnSecSecuritySolutions: ~/Desktop
File Actions Edit View Help
└─(kali㉿PawnSecSecuritySolutions)-[~/Desktop]
$ lsof
COMMAND     PID   TID TASKCMD      USER   FD   TYPE      DEVICE SIZE/OFF NODE NA
ME
systemd      1          root cwd  unknown
roc/1/cwd (readlink: Permission denied)    root rtd  unknown
systemd      1          root rt  unknown
roc/1/root (readlink: Permission denied)
systemd      1          root txt  unknown
roc/1/exe (readlink: Permission denied)
systemd      1          root NOFD

```

Şekil 30 "lsof" Komutunun Çıktısı

Ismem

"Ismem" komutu, sistem belleği hakkında bilgi sağlar. "Ismem -a" komutu, tüm bellek bloklarını listeler. "Ismem -c" komutu, bellek bloklarını boyutlarına göre listeler. "Ismem -t" komutu, bellek bloklarını tarih ve saatlerine göre listeler.

```

kali@PawnSecSecuritySolutions: ~/Desktop
File Actions Edit View Help
└─(kali㉿PawnSecSecuritySolutions)-[~/Desktop]
$ lsmod
RANGE           SIZE  STATE REMOVABLE BLOCK
0x0000000000000000-0x000000007fffffff  2G online      yes  0-15

Memory block size:      128M
Total online memory:    2G
Total offline memory:   0B

```

Şekil 31 "Ismem" Komutunun Çıktısı

Ismod

Bu komut ise, sistemde yüklü olan kernel modüllerini listelemek için kullanılan bir komuttur. Komutun kullanımı oldukça basittir. Sadece terminalde "lsmod" yazarak çalıştırılabilir. Her bir modülün adı, kullanılan bellek miktarı, bağımlılıkları ve modülün yüklenip yüklenmediği hakkında bilgi sağlanır.

```

kali@PawnSecSecuritySolutions: ~/Desktop
File Actions Edit View Help
└─(kali㉿PawnSecSecuritySolutions)-[~/Desktop]
$ lsmod
Module           Size  Used by
rfkill          32768  2
qrtr            49152  4
vboxsf          45056  0
sunrpc          684032  1
binfmt_misc     24576  1
snd_intel8x0    49152  2
intel_rapl_msr  20480  0
snd_ac97_codec  176128  1 snd_intel8x0

```

Şekil 32 "lsmod" Komutunun Çıktısı

10 KaliLinux Zaman Senkronizasyonu

Zaman senkronizasyonu, bilgisayarların doğru zamanı göstermesini sağlamak için kullanılan bir işlevdir. Bu, bir bilgisayarın saatinin gerçek saat ile senkronize edilmesi anlamına gelir. KaliLinux, birçok siber güvenlik aracı içeren bir işletim sistemi olduğu için, doğru zamanın önemi büyüktür.

10.1 Ntp Kavramı

NTP (Network Time Protocol), agdaki cihazların birbirleriyle senkronize olmasına olanak tanıyan bir protokoldür. KaliLinux, ağ cihazlarının doğru bir şekilde senkronize edilmesini sağlamak için NTP'yi kullanır. NTP, bir NTP sunucusu veya zaman sunucusu tarafından yayınlanan zaman sinyallerini kullanarak, tüm cihazların doğru zamanı tutmasını sağlar.

NTP, doğru zamanı sağlamak için birkaç farklı yöntem kullanır. Bunlardan bazıları şunlardır:

1. NTP sunucusundan doğrudan zaman bilgileri almak: Bu yöntem, cihazların doğrudan bir NTP sunucusu ile iletişim kurmasını ve zaman bilgilerini almasını içerir. Bu yöntem, genellikle büyük ölçekli ağlarda kullanılır.
2. Yerel saat ve başvuru saatleri: Bu yöntem, yerel saati ve başvuru saatlerini kullanarak doğru zamanı hesaplar. Bu yöntem, daha küçük ağlarda kullanılabilir.
3. SNTP (Simple Network Time Protocol): Bu, daha basit bir versiyondur ve NTP sunucusundan daha az veri alır. SNTP, daha küçük ağlarda ve IoT cihazlarında yaygın olarak kullanılır.

NTP ayrıca, zaman senkronizasyonunu düzgün bir şekilde yapmak için birçok farklı faktörü dikkate alır. Bu faktörler arasında ağ gecikmesi, saat kayması, saatin doğruluğu ve diğer faktörler bulunur. Bu faktörler, NTP'nin doğru zamanı hesaplamak için kullanabileceği çeşitli algoritmaları etkiler.

10.2 KaliLinux Zaman Senkronizasyonu Komutları

date

"date" komutu, sistem saatini ve tarihini görüntülemek veya değiştirmek için kullanılır. Komutu hiçbir argüman olmadan çalıştırıldığınızda, mevcut sistem saatini ve tarihini yazdırır.

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$date
```

```
Fri Mar 24 03:17:39 AM EDT 2023
```

Ayrıca, "date" komutunu kullanarak sistem saatini ve tarihini ayarlayabilirsiniz. Örneğin:

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
    └─$sudo date --set="2022-03-24 15:20:00"
```

```
Thu Mar 24 10:20:00 AM EDT 2022
```

hwclock

"hwclock" komutu, sistem saatı ile donanım saatini (RTC - Real-time clock) senkronize etmek için kullanılır. Komutu hiçbir argüman olmadan çalıştırıldığınızda, donanım saatinin değerini yazdırır. Komutu root kullanıcısında kullanarak veya "sudo hwclock" komutuyla çalıştırabilirsiniz.

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
```

```
└─$sudo hwclock
```

```
2023-03-24 15:28:55.321687+00:00
```

Ayrıca, "hwclock" komutunu kullanarak donanım saatinin değerini ayarlayabilirsiniz. Örneğin, donanım saatinin değerini 24 Mart 2023, saat 15:30 olarak ayarlamak için şu komutu kullanabilirsiniz:

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
```

```
└─$sudo hwclock --set --date "2022-03-24 10:30:00"
```

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
```

```
└─$sudo hwclock
```

```
2022-03-24 10:30:00.249662-04:00
```

timedatectl

"timedatectl" komutu, sistem saatı ve zaman dilimini ayarlamak için kullanılır. Komutu hiçbir argüman olmadan çalıştırıldığınızda, mevcut sistem saatı, tarihi, zaman dilimi ve diğer bilgileri yazdırır.

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
```

```
└─$timedatectl
```

```
Local time: Fri 2023-03-24 03:35:56 EDT
```

```
Universal time: Fri 2023-03-24 07:35:56 UTC
```

```
RTC time: Thu 2022-03-24 14:35:13
```

```
Time zone: America/New_York (EDT, -0400)
```

```
System clock synchronized: no
```

```
NTP service: n/a
```

```
RTC in local TZ: no
```

Örneğin:

Ayrıca, "timedatectl" komutunu kullanarak sistem saatı, tarih, zaman dilimi gibi bilgileri ayarlayabilirsiniz. Örneğin, zaman dilimini Türkiye saatı olarak ayarlamak için şu komutu kullanabilirsiniz:

```
└──(kali㉿PawnSecSecuritySolutions)-[~]
```

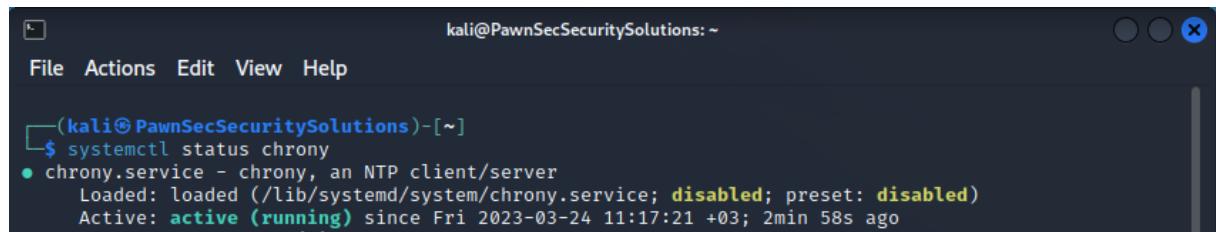
```
└─$timedatectl set-timezone Europe/Istanbul
```

```
Local time: Fri 2023-03-24 10:41:04 +03
```

10.2.1 Chrony Kullanımı

“**chrony**”, NTP sunucuları ve diğer zaman kaynaklarından senkronize olmak için kullanılan bir başka servistir. “**chrony**”, NTPv4 protokolü kullanır ve ağdaki diğer NTP sunucuları ile senkronize olmak için sistem saatini ayarlar. Ayrıca diğer NTP senkronizasyon araçlarına oranla daha düşük CPU tüketimi gerçekleştirdiği için daha çok tercih edilir. Bu araç sisteme yüklü gelmediği için “**sudo apt install chrony -y**” komutunu kullanarak kurulmasını sağlıyoruz.

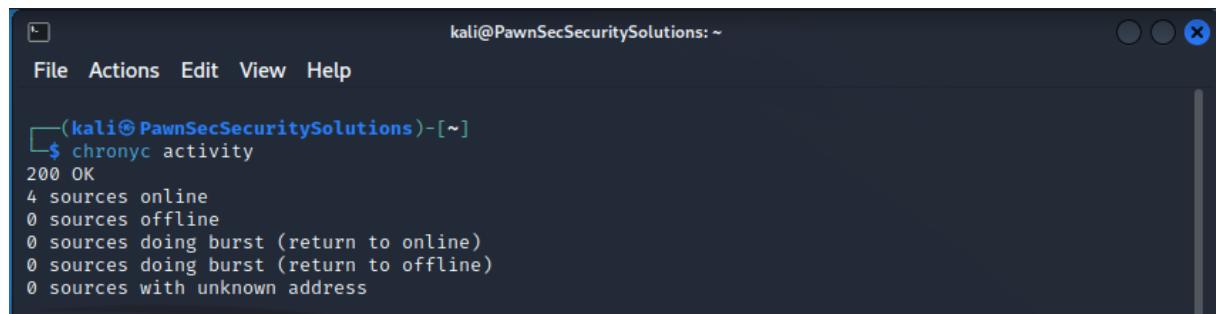
Hemen ardından servis durumunu belirlemek için “**systemctl start chrony**” komutunu kullanıyoruz. ”**systemctl status chrony**” komutuyla da sistemin çalışıp çalışmadığını öğrenebiliriz.



```
kali@PawnSecSecuritySolutions: ~
File Actions Edit View Help
└─(kali㉿PawnSecSecuritySolutions)-[~]
$ systemctl status chrony
● chrony.service - chrony, an NTP client/server
  Loaded: loaded (/lib/systemd/system/chrony.service; disabled; preset: disabled)
  Active: active (running) since Fri 2023-03-24 11:17:21 +03; 2min 58s ago
```

Şekil 33 "systemctl status chrony" Komutunun Çıktısı

”**chronyc activity**” komutunu çalıştırarak, sistem saatinin doğru şekilde senkronize edildiğini ve NTP sunucularının doğru şekilde kullanıldığını doğrulayabilirsiniz. Bu bilgiler, sistem saatinin doğruluğunu ve güvenilirliğini artırmak için chrony yapılandırması ve sorun giderme işlemlerinde kullanılabilir.



```
kali@PawnSecSecuritySolutions: ~
File Actions Edit View Help
└─(kali㉿PawnSecSecuritySolutions)-[~]
$ chronyc activity
200 OK
4 sources online
0 sources offline
0 sources doing burst (return to online)
0 sources doing burst (return to offline)
0 sources with unknown address
```

Şekil 34 "chronyc activity" Komutunun Çıktısı

”**chronyc sources**” komutunu kullanarak, chrony servisinin senkronize olduğu NTP sunucuları hakkında detaylı bilgi alabiliriz. Bu komut, her NTP sunucusunun IP adresini, erişim durumunu, zaman senkronizasyonu hakkındaki bilgileri ve diğer ayrıntıları gösterir. ”**-v**” parametresini de ekleyerek tablo başlıklarını ve değerlerin anlamlarıyla ilgili bilgileri de yazdırabiliriz.

```
kali@PawnSecSecuritySolutions:~
```

File Actions Edit View Help

```
[(kali㉿PawnSecSecuritySolutions)-[~]]$ chronyc sources -v
```

```
.-- Source mode '^' = server, '=' = peer, '#' = local clock.  
/.- Source state '*' = current best, '+' = combined, '-' = not combined,  
| | 'x' = may be in error, '=' = too variable, '?' = unusable.  
|| | | | .- xxxx [ yyyy ] +/- zzzz  
|| | | | | xxxx = adjusted offset,  
|| | | | | yyyy = measured offset,  
|| | | | | zzzz = estimated error.  
|| | | | \  
MS Name/IP address      Stratum Poll Reach LastRx Last sample  
-----  
^ time.cloudflare.com      3   6    377     31    -37us[ +58us] +/-  31ms  
^ nice.stuff.is           3   6    377     31   -6765us[-6669us] +/-  70ms  
^ 176.236.133.6           2   6    377     27   +1829us[+1924us] +/-  38ms  
^* time.ume.tubitak.gov.tr  1   6    375     27   +305us[ +400us] +/- 8348us
```

Şekil 35 "chronyc sources -v" Komutunun Çıktısı

"chronyc sourcestats" komutu, chrony servisinin zaman senkronizasyonu için kullandığı kaynakların istatistiklerini görüntülemek için kullanılır. Bu komut, NTP sunucularının saat dilimleri ve doğruluk seviyeleri gibi bilgileri içeren ayrıntılı bir liste sağlar. Aynı şekilde bu komutla da "-v" parametresini kullanabiliyoruz.

```
kali@PawnSecSecuritySolutions:~
```

File Actions Edit View Help

```
[(kali㉿PawnSecSecuritySolutions)-[~]]$ chronyc sourcestats -v
```

```
.- Number of sample points in measurement set.  
/.- Number of residual runs with same sign.  
| | | | .- Length of measurement set (time).  
| | | | | | .- Est. clock freq error (ppm).  
| | | | | | | | .- Est. error in freq.  
| | | | | | | | | | .- Est. offset.  
| | | | | | | | | | | On the -. samples. \  
Name/IP Address      NP NR Span Frequency Freq Skew Offset Std Dev  
-----  
time.cloudflare.com    25 13 32m    -0.192    1.024 -1483us  647us  
nice.stuff.is          25 15 32m    -0.194    3.192 -147us   2398us  
176.236.133.6         24 14 28m    -0.211    0.880 -826us   569us  
time.ume.tubitak.gov.tr 24 16 28m    +0.005    0.902 +1746ns  533us
```

Chrony servisine yeni bir NTP sunucusu eklemek için aşağıdaki adımları izleyebilirsiniz:

1. Yönetici (root) olarak sisteme giriş yapın.
2. Chrony konfigürasyon dosyasını açmak için terminale "sudo nano /etc/chrony/chrony.conf" komutunu yazın.
3. Dosya içinde, "# NTP serverları" altında yeni bir satır açın ve "server server-adresi iburst" komutunu girin. Burada, "server-adresi" yerine eklemek istediğiniz NTP sunucusunun IP adresini veya URL'sini girin.
4. Dosyayı kaydetmek ve çıkmak için "Ctrl+X" tuşlarına basın ve ardından "Y" ve "Enter" tuşlarına basarak değişiklikleri kaydedin.
5. Chrony servisini yeniden başlatmak için "sudo systemctl restart chrony" komutunu girin.

Bu işlem, chrony servisine yeni bir NTP sunucusu ekleyecektir. Artık sistem saatinin senkronizasyonu için bu sunucunun kullanılmasına izin verilir. Bu şekilde eklediğiniz sunucular, diğer NTP sunucuları ile kullanılabilir veya diğer sunucuları devre dışı bırakabilirsiniz.

11 KaliLinux Yazılım Yönetimi

Yazılım yönetimi, sistemdeki yazılımların güncel kalmasını sağlayarak, güvenlik açıklarının kapatılmasını, yeni özelliklerin kullanılmasını ve sistemin daha iyi çalışmasını sağlar. Bu nedenle, düzenli olarak yazılım yönetimi yapmak önemlidir.

apt

Kalinux sisteminde, yazılım yönetimi genellikle "apt (Advanced Package Tool)" komutu veya grafiksel arayüzler (örneğin Synaptic Paket Yöneticisi veya GNOME Yazılım Merkezi) kullanılarak gerçekleştirilir.

"apt" komutu, Linux dağıtımlarında en yaygın olarak kullanılan yazılım yönetim araçlarından biridir. Bu komutla, sistemde yüklü olan yazılımların güncellelemeleri, yeni yazılımların kurulumu ve mevcut yazılımların kaldırılması gibi işlemler gerçekleştirilebilir. Ayrıca, grafiksel arayüzler de kullanarak yazılım yönetimi yapılabilir. Bu arayüzler, kullanıcı dostu bir şekilde yazılım arama, yükleme, kaldırma ve güncelleme işlemlerini yapmaya olanak sağlar.

"apt" komutları tek başına çalışmıyor yanında "sudo" komutunu gerektirmektedir. Aşağıda, sık kullanılan "apt" komutları ve ne işe yaradıkları kısaca açıklanmıştır:

- "sudo apt install [paket ismi)": Belirtilen "paket ismi" adlı yazılım paketini yükler.
- "sudo apt update": Yazılım kaynaklarını günceller. Bu, sisteme yeni yazılım kaynakları eklenmişse veya mevcut kaynaklarda değişiklik yapılmışsa gereklidir.
- "sudo apt upgrade": Mevcut yazılım paketlerinin güncellenmesini sağlar. Güncelleme işlemi sırasında sistemdeki tüm yazılımların en son sürümleri indirilir ve kurulur.
- "sudo apt remove [paket ismi)": Belirtilen "paket ismi" adlı yazılım paketini kaldırır. Paket kaldırıldığında, pakete bağlı diğer paketler otomatik olarak kaldırılmaz.
- "sudo apt purge [paket ismi)": Belirtilen "paket ismi" adlı yazılım paketini kaldırır ve pakete bağlı diğer paketleri de kaldırır.
- "sudo apt search [anahtar kelime)": Verilen "anahtar kelime" ile eşleşen yazılım paketlerini arar.
- "sudo apt list": Yüklü yazılım paketlerini listeler.

apt-cache

"apt-cache" komutu, sisteme kurulu olan paketlerin bilgilerini ve arama yapmak için kullanılır. Bu komut, yazılım paketleri hakkında ayrıntılı bilgi sağlayarak, kullanıcılar aradıkları paketi bulmalarına ve paketlerin bağımlılıklarını kontrol etmelerine yardımcı olur.

"apt-cache" komutu ile yapılabilecek işlemler arasında aşağıdakiler yer alır:

- "apt-cache search [paket ismi)": Belirli bir yazılım paketinin adına göre arama yapar.
- "apt-cache show [paket ismi)": Belirtilen yazılım paketi hakkında ayrıntılı bilgi gösterir.
- "apt-cache showpkg [paket ismi)": Belirtilen yazılım paketi hakkında paket bilgisini gösterir.
- "apt-cache depends [paket ismi)": Belirtilen yazılım paketi için bağımlılıkları gösterir.
- "apt-cache rdepends [paket ismi)": Belirtilen yazılım paketini kimin kullandığını gösterir.

Bu komutlar, yazılım yönetimi ve paketlerin yönetimi açısından oldukça faydalıdır. Özellikle, sisteme yeni bir yazılım paketi kurulmadan önce, "apt-cache" komutları kullanarak paket hakkında ayrıntılı bilgi edinmek, kurulum sonrası olası sorunların önüne geçebilir.

apt-get

"apt" komutuna ek olarak "apt-get" komutu da sıkılıkla kullanılan yazılım yönetimi komutlarından biridir. Bu komutta aynı "apt" komutunda olduğu gibi Yazılım paketleri arama, yükleme, güncelleme gibi işlemler için kullanılır. İki komut arasındaki fark şunlardır:

- "apt" komutu, kullanıcı dostu bir arayüze sahiptir ve daha az yazım gerektirir. "apt" komutu, yazılım kaynaklarını güncellemeyi, bağımlılıkları otomatik olarak çözmeyi ve kurulum sırasında ilerlemeyi göstermeyi içerir. Ayrıca, "apt" komutu, "apt-cache" ve "apt-get" komutlarının işlevsellliğini birleştirir.
- "apt-get" komutu, "apt-cache" komutunu kullanarak yazılım paketleri hakkında ayrıntılı bilgi sağlar ve daha fazla işlevsellige sahiptir.

11.1 Kaynak Üzerinden Yazılım Yükleme

Kalinux sisteminde kaynaktan yazılım yükleme, yazılımı kaynak kodu şeklinde indirip, derleyerek ve yükleyerek gerçekleştirilir. Bu yöntem, kaynak kodunu düzenleme, özelleştirme veya yazılımin en son sürümünü kullanma ihtiyacı olan geliştiriciler ve ileri düzey kullanıcılar için kullanışlıdır.

Kaynaktan yazılım yükleme, aşağıdaki adımları içerir:

1. Kaynak kodunu indirme: Yazılımin resmi web sitesinden veya kaynak kodu havuzlarından (GitHub, SourceForge, vb.) indirilir.
2. Bağımlılıkların yüklenmesi: Kaynak kodu derlemeden önce gerekli olan bağımlılıkların yüklenmesi gerekebilir.
3. Derleme: Kaynak kodu derlenir ve binerler oluşturulur. Bu adım, yazılımin çalıştırılabilir dosyalarını oluşturur.
4. Kurulum: Derlenen yazılımin sistemde kurulması gerekebilir. Bu adım, yazılımı sistem dosyalarına ve diğer gerekli yerbere kopyalar.
5. Test etme: Yüklenen yazılımin doğru bir şekilde çalıştığını emin olmak için test edilir.

Bu yöntem, yazılımın bakımı ve güncellenmesiyle ilgili ek sorumlulukları da beraberinde getirir ve genellikle depodaki yazılımlardan daha az güncellenir. Bu nedenle, kaynaktan yazılım yüklemeye, yalnızca gerekli olduğunda veya belirli bir ihtiyacı karşılamak için kullanılmalıdır.

11.2 Kaynaktan Yazılım Yükleme Araçları

Kalilinux sistemi, Debian tabanlı olduğu için, kaynak kodundan yazılım yüklemek için "make" ve "make install" gibi geleneksel Unix komutları kullanılabilir. Bununla birlikte, genellikle kaynak kodu derlemek ve yüklemek oldukça karmaşık bir işlem olabilir. Bu nedenle, genellikle daha kolay bir yol olarak "**apt**" veya "**dpkg**" gibi yazılım yöneticileri kullanılır. Ancak, bazen bazı yazılımların kaynak kodu yüklenmesi gerekebilir.

Örneğin, "**wget**" yazılımını kaynak kodundan yüklemek için şu adımlar takip edilebilir:

1. İlk olarak, "wget" yazılımının kaynak kodunu indirin. Bunun için "wget" komutunu kullanabilirsiniz:

```
$ wget https://ftp.gnu.org/gnu/wget/wget-1.21.2.tar.gz
```

2. Daha sonra, "tar" komutuyla indirilen dosyayı açın:

```
$ tar -xvf wget-1.21.2.tar.gz
```

3. Açılan dizine gidin:

```
$ cd wget-1.21.2
```

4. Kaynak kodunu derleyin:

```
$ ./configure
```

```
$ make
```

5. Derleme işlemi tamamlandığında, yazılımı yüklemek için "make install" komutunu kullanabilirsiniz:

```
$ sudo make install
```

Bu işlem, "wget" yazılımını kaynak kodundan yükleyecektir. Ancak, dikkat edilmesi gereken bazı noktalar vardır. Örneğin, kaynak kodu yüklemek her zaman en iyi seçenek değildir ve bazı güvenlik riskleri taşıyabilir. Ayrıca, kaynak kodu yüklemek, bağımlılıkların elle yönetilmesini gerektirebilir. Bu nedenle, mümkünse öncelikle yazılım yöneticileri kullanılmalıdır.

"wget" kurulumunu gerçekleştirdiğimize göre şimdi birkaç parametresine ve kullanımına göz atalım.

1. "-O" parametresi: İndirilen dosyanın kaydedileceği dosya adını belirler. Örneğin:

```
$ wget -O belge.pdf https://www.ornek.com/belge.pdf
```

2. "-c" parametresi: İndirme işlemi kesilirse, sonraki çalıştırımda kaldığı yerden devam eder. Örneğin:

```
$ wget -c https://www.ornek.com/belge.pdf
```

3. "-q" parametresi: Çıktıyı sessize alır, yani sadece dosyayı indirir ve hiçbir bilgi vermez. Örneğin:

```
$ wget -q https://www.ornek.com/belge.pdf
```

4. "-r" parametresi: Verilen URL'ye ait tüm alt dizinleri ve dosyaları indirir. Örneğin:

```
$ wget -r https://www.ornek.com/dizin/
```

5. "-P" parametresi: İndirilecek dosyaların kaydedileceği dizini belirler. Örneğin:

```
$ wget -P /home/kullanici/dosyalar/ https://www.ornek.com/belge.pdf
```

6. "-t" parametresi: İndirme işlemi başarısız olursa, yeniden deneme sayısını belirler. Örneğin:

```
$ wget -t 3 https://www.ornek.com/belge.pdf
```

Bu parametrelerin yanı sıra, "wget" komutu birçok diğer parametre seçenekleri sunar ve "**man wget**" komutu ile tüm parametreler hakkında daha fazla bilgi edinilebilir.

11.3 Sıkıştırılmış Dosyalarla Kurulum Yapma

Kalilinux gibi Linux dağıtımlarında sıkıştırılmış dosyalar kullanarak yazılım kurulumu yapmak oldukça yaygın bir yöntemdir. Bu yöntem, genellikle açık kaynak kodlu yazılımların kurulumunda tercih edilir. İşte sıkıştırılmış dosyalar ile kurulum yapmak için aşağıdaki adımları takip edebilirsiniz:

İndirme

İlk olarak, sıkıştırılmış dosyayı indirin ve bir dizine kaydedin. Genellikle dosyalar web sitelerinden indirilebilir. Örneğin, "http://www.example.com/program.tar.gz" adresindeki bir dosyayı indirmek için aşağıdaki komutu kullanabilirisiniz:

```
$ wget http://www.example.com/program.tar.gz
```

Cıkartma

İndirdiğiniz dosyayı çıkartın. Bu işlem için "**tar**" komutu kullanılır. Örneğin, ".tar.gz" uzantılı bir dosyayı çıkarmak için aşağıdaki komutu kullanabilirisiniz:

```
$ tar -zxf program.tar.gz
```

Bu komut, dosyayı çıkartmak için "z" parametresini (gzip sıkıştırma) ve "x" parametresini (çıkartma) kullanır. Dosyayı çıkarttıktan sonra, dosyanın içindeki dizine gidin:

```
$ cd program/
```

Yapıllandırma

Bazı yazılımların yapılandırma ayarlarının yapılandırılması gerekebilir. Bu işlem, "**configure**" adlı bir betik dosyası ile yapılır. Betik dosyasını çalıştırmak için aşağıdaki komutu kullanabilirisiniz:

```
$ ./configure
```

Bu komut, sistemdeki gereksinimleri tespit eder ve yazılımı yapılandırır.

Derleme

Yazılımin derlenmesi, kaynak kodunun çalıştırılması ve yürütülebilir bir program oluşturulması işlemidir. Derleme işlemi "**make**" komutu ile gerçekleştirilir. Aşağıdaki komutu kullanarak derleme işlemini başlatabilirisiniz:

```
$ make
```

Kurulum

Yazılımın derlenmesinin ardından, "**make install**" komutu kullanılarak yazılım sisteme yüklenir. Yazılım, sistemde belirtilen varsayılan dizine yüklenecektir. Ancak, yükleme dizinini değiştirmek için farklı parametreler kullanabilirsiniz. Aşağıdaki komutu kullanarak yazılımı sisteme yükleyebilirsiniz:

```
$ make install
```

11.4 Mirror(ayna) Terimi

Mirror terimi, Linux ve benzeri işletim sistemlerinde kullanılan bir terimdir ve kaynak kodu, paketler, güncellemeler ve diğer dosyaların depolandığı ve sunulduğu sunucuları ifade eder. KaliLinux sistemi de çeşitli aynalar kullanır ve varsayılan olarak birkaç ayna adresi tanımlıdır.

Bir ayna, kullanıcılaraya yazılım güncellemeleri, yeni sürümler, yamalar ve diğer dosyaların hızlı bir şekilde erişilebilir olmasını sağlar. Ancak, varsayılan ayna sunucusu bazen yavaş veya dolu olabilir. Bu nedenle, ayna sunucusunu değiştirmek, dosyaları daha hızlı indirme ve güncelleme işlemlerini daha hızlı yapma şansını verir.

KaliLinux sisteminde ayna sunucusunu değiştirmek için aşağıdaki adımları izleyebilirsiniz:

- Ayna sunucuları listesini görüntülemek için "nano /etc/apt/sources.list" komutunu çalıştırın.
- Ayna sunucusu listesi, "deb" veya "deb-src" ile başlayan satırlarda tanımlanır. Bu satırlarda, "http://" veya "https://" ile başlayan bir adres görüntülenir.
- Yeni bir ayna sunucusu eklemek için, önce mevcut satırları yorum satırına çevirin veya silin. Ardından, yeni bir satır ekleyin ve ayna sunucusu adresini ekleyin. Örneğin, "deb http://mirror.lstn.net/kali kali-rolling main non-free contrib" şeklinde bir satır ekleyebilirsiniz.
- Kaydedip çıkmak için "Ctrl+X" tuşlarına basın, ardından "Y" tuşuna basın ve ENTER tuşuna basın.
- Son olarak, ayna sunucusu değişikliğini uygulamak için "apt-get update" komutunu çalıştırın.

12 Boot (Ön Yükleme) İşleminin Yönetimi

Bir bilgisayar açıldığında, ilk olarak BIOS (Basic Input/Output System) veya UEFI (Unified Extensible Firmware Interface) gibi donanım seviyesindeki programlar çalışır. Bu programlar, bilgisayarın donanımını tanır ve önyükleme işlemini gerçekleştirmek üzere işletim sistemine kontrolü devreder.

Daha sonra, işletim sistemi yükleme işlemi gerçekleştirilir. Kalilinux gibi bir Linux dağıtımını önyükleme işlemini gerçekleştirken aşağıdaki adımları izler:

1. BIOS veya UEFI, sabit sürücüdeki önyüklenen bilgisayarın sektörlere bakar ve MBR (Master Boot Record) veya GPT (GUID Partition Table) gibi bir bölüm tablosu varsa onu okur.
2. Önyüklenen bilgiyi bulduktan sonra, önyüklenen kodu yürütmek için "bootloader" olarak adlandırılan bir program yükler. GRUB (Grand Unified Bootloader) veya LILO (Linux Loader) gibi popüler boot loader'lar mevcuttur.
3. Bootloader, çekirdek dosyasını yükler. Çekirdek dosyası, işletim sisteminin en temel bileşenidir ve tüm donanımı kontrol eder.
4. Çekirdek dosyası, initramfs adı verilen bir dosya sistemini yükler. Bu dosya sistemi, disk bölümlerini, aygıtları ve sürücülerini tanır.
5. Initramfs, /sbin/init programını çalıştırır ve sistem başlatma işlemi başlar.
6. /sbin/init, tüm sistemi başlatmak için gerekli diğer bileşenleri yükler ve ardından bir oturum yöneticisi çalıştırır. Bu, kullanıcının oturum açabileceği bir giriş ekranı oluşturur.
7. Kullanıcı oturum açtıktan sonra, kullanıcının ayarları yüklenir ve masaüstü ortamı başlatılır.

Bu süreç, kullanıcının bilgisayarında bulunan donanıma, yazılıma ve diğer ayarlara göre değişebilir. Ancak, genel olarak, önyükleme işlemi sırasında bu temel adımlar gerçekleştirilir ve sonunda kullanıcı masaüstü ortamına erişebilir.

12.1 MBR ve GPT Nedir?

MBR (Master Boot Record) ve GPT (GUID Partition Table), bir sabit diskin bölümlendirmek ve bir işletim sistemini yüklemek için kullanılan iki farklı disk bölümleme tablosudur. İşletim sistemi, sabit diskteki dosyaları ve verileri depolamak için bu bölümleri kullanır.

MBR, IBM PC uyumlu bilgisayarların sabit disklerinde kullanılan geleneksel bir bölümleme yöntemidir. Bu yöntem, diskteki ilk 512 baytı kullanarak bir boot sektörü ve disk bölümleri hakkında bilgi içeren bir tablo oluşturur. Ancak, MBR sadece 2 TB'a kadar olan sabit diskleri destekler ve bu nedenle günümüzdeki daha büyük sabit diskler için yetersiz kalmaktadır.

GPT, modern bilgisayarların sabit disklerinde kullanılan bir bölümleme yöntemidir. GPT, 64-bit disk adresleme kullanarak, MBR'den daha büyük disk boyutlarına destek verir. GPT, disk bölümleri hakkında bilgiyi ayrı bir bölümde saklar ve bu sayede daha esnek bir yapı sağlar. GPT ayrıca, bir bilgisayarın UEFI (Unified Extensible Firmware Interface) firmware'ini kullanarak önyükleme yapmasını sağlayabilir.

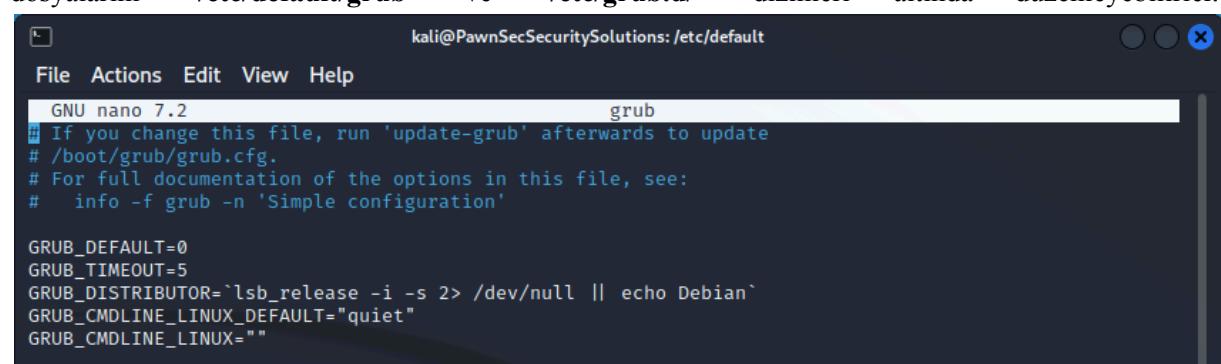
12.2 GRUB2 Nedir?

GRUB2, GNU Grand Unified Bootloader'un(GRUB) daha yeni bir sürümüdür ve KaliLinux gibi birçok Linux dağıtımında kullanılmaktadır. GRUB2, önceki sürüm olan GRUB'a benzer şekilde, bilgisayarın önyükleme yükleyicisi olarak kullanılır.

GRUB2, önceki sürümünden farklı olarak birçok yenilik ve geliştirme içermektedir. Bunlar arasında, grafik arabirim, çift önyükleme için daha iyi destek, geliştirilmiş disk şifreleme desteği ve daha fazla dosya sistemi desteği yer almaktadır.

KaliLinux'ta GRUB2, önyükleme yükleyicisi olarak kullanılan standart önyükleme yükleyicisidir ve birçok Linux dağıtımında olduğu gibi, "/boot/grub/" dizininde bulunur. GRUB2, kullanıcılarla, önyükleme seçeneklerini düzenleme, işletim sistemi seçeneklerini belirleme ve önyükleme sürecini yapılandırma imkânı sunar.

GRUB2, KaliLinux'ta genellikle varsayılan olarak yüklenir ve önyükleme işlemini yönetmek için kullanılır. Ancak, kullanıcılar özelleştirilmiş ayarlar yapmak istediklerinde, GRUB2 konfigürasyon dosyalarını "/etc/default/grub" ve "/etc/grub.d/" dizinleri altında düzenleyebilirler.

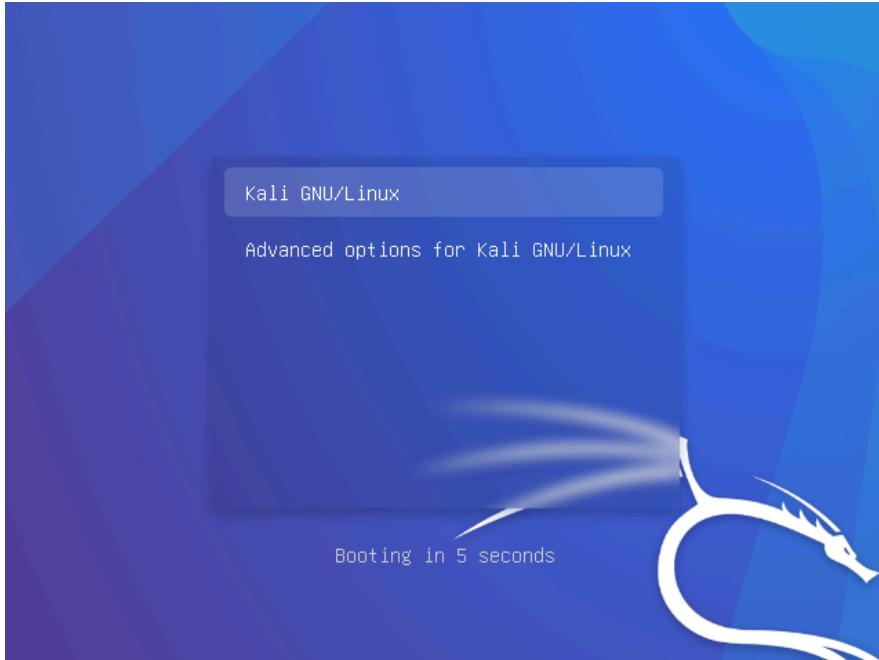


```
GNU nano 7.2                                     grub
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
#   info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="quiet"
GRUB_CMDLINE_LINUX=""
```

Şekil 37 "sudo nano grub" Komutunun Çıktısı

Yukarıdaki görselde “cd” komutu ile “/etc/default” dizinine gittikten sonra “sudo nano grub” komutunu kullanarak “GRUB” dosyasının çıktısını aldığımızı görüyoruz. **GRUB_TIMEOUT** değeri bizlere sistem boot edilirken GRUB menüsünün kaç saniye boyunca bizden seçim bekleyeceğini belirleyebiliyoruz. Yukarıda 5 saniye boyunca bize seçim ekranında bekleteceğini görüyoruz.



Şekil 38 GRUB Menüsü

Yukarıda “Booting in 5 seconds” yazısından da anlayacağınız üzere sistem bize GRUB seçimi için 5 saniye tanıyor.

12.3 Systemd Nedir?

Systemd, modern Linux dağıtımlarında kullanılan bir sistem ve hizmet yönetim aracıdır. KaliLinux da dahil olmak üzere birçok Linux dağıtımında varsayılan olarak kullanılmaktadır. Systemd, önyükleme sürecini yönetmek, hizmetleri başlatmak ve durdurmak, sistem loglarını yönetmek ve diğer sistem yönetimi görevlerini yerine getirmek için kullanılır.

Systemd, özellikle eski init sisteme kıyasla birçok avantaj sunar. Bunlar arasında hizmetlerin paralel olarak başlatılabilmesi, hizmetlerin tamamlandıktan sonra diğerlerinin başlamasına izin veren bir hizmet bağımlılık sistemi, sistem loglarının “journald” olarak adlandırılan merkezi bir yerde toplanması ve daha hızlı önyükleme süresi gibi özellikler yer alır.

Systemd, Kali Linux'ta birçok dosya ve komutla ilişkilidir. Aşağıdaki dosyalar ve komutlar, Systemd'nin kullanımı hakkında daha ayrıntılı bilgi sağlar:

- “/etc/systemd/system/”: Bu dizin, Systemd hizmetlerinin yapılandırma dosyalarını içerir. Systemd hizmetleri .service uzantılı dosyalarda tanımlanır ve bu dosyalarda hizmetin adı, açıklaması, çalıştırılacak komutlar ve diğer ayarlar tanımlanır.
- “/etc/systemd/system.conf”: Bu dosya, Systemd'nin ana yapılandırma dosyasıdır. Systemd'nin genel ayarlarını değiştirmek için bu dosya düzenlenebilir.

- “**/etc/systemd/logind.conf**”: Bu dosya, oturum yönetimi ayarlarını içerir. Örneğin, oturum açma penceresinin otomatik olarak kapanma süresi gibi ayarlar bu dosyada bulunur.

- **journalctl**: Bu komut, sistem günlüklerini yönetmek için kullanılır. journalctl ile sistemin loglarını görüntülemek, filtrelemek ve aramak mümkündür.

```
kali@PawnSecSecuritySolutions: ~
File Actions Edit View Help
└─(kali㉿PawnSecSecuritySolutions)-[~]
$ journalctl
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
Mar 05 16:25:57 kali systemd-xdg-autostart-generator[927]: /home/kali/.config/autostart/fix-duplicat>
Mar 05 16:25:57 kali systemd[913]: Queued start job for default target Main User Target.
Mar 05 16:25:57 kali systemd[913]: Created slice User Application Slice.
Mar 05 16:25:57 kali systemd[913]: Created slice User Core Session Slice.
Mar 05 16:25:57 kali systemd[913]: Reached target Paths.
Mar 05 16:25:57 kali systemd[913]: Reached target Timers.
Mar 05 16:25:57 kali systemd[913]: Starting D-Bus User Message Bus Socket ...
Mar 05 16:25:57 kali systemd[913]: Listening on GnuPG network certificate management daemon.
Mar 05 16:25:57 kali systemd[913]: Listening on GCR ssh-agent wrapper.
Mar 05 16:25:57 kali systemd[913]: Listening on GNOME Keyring daemon.
```

Şekil 39 "journalctl" Komutunun Çıktısı

- **systemd-analyze**: Bu komut, önyükleme sürecini analiz etmek için kullanılır. systemd-analyze ile önyükleme sürecinde hangi hizmetlerin ne kadar zaman aldığı gibi bilgilere erişilebilir.

```
kali@PawnSecSecuritySolutions: ~
File Actions Edit View Help
└─(kali㉿PawnSecSecuritySolutions)-[~]
$ systemd-analyze
Startup finished in 2.551s (kernel) + 1.722s (userspace) = 4.274s
graphical.target reached after 1.599s in userspace.
```

Şekil 40 "systemd-analyze" Komutunun Çıktısı

- **systemctl**: Bu komut, Systemd hizmetlerini yönetmek için kullanılır. "systemctl" ile hizmetleri başlatmak, durdurmak, yeniden başlatmak ve diğer yönetim görevlerini gerçekleştirmek mümkündür.

Komutlar	İşlevler
systemctl start servis_adi	Bu komut, belirtilen hizmeti başlatır. Örneğin, "systemctl start apache2" komutu, Apache web sunucusunu başlatır.
systemctl stop servis_adi	Bu komut, belirtilen hizmeti durdurur. Örneğin, "systemctl stop apache2" komutu, Apache web sunucusunu durdurur.
systemctl restart servis_adi	Bu komut, belirtilen hizmeti yeniden başlatır. Örneğin, "systemctl restart apache2" komutu, Apache web sunucusunu yeniden başlatır.
systemctl enable servis_adi	Bu komut, belirtilen hizmetin sistem önyükleme sırasında otomatik olarak başlatılmasını sağlar. Örneğin, "systemctl enable apache2" komutu, Apache web sunucusunun önyükleme sırasında otomatik olarak başlatılmasını sağlar.
systemctl disable servis_adi	Bu komut, belirtilen hizmetin sistem önyükleme sırasında otomatik olarak başlatılmamasını sağlar. Örneğin, "systemctl disable apache2" komutu, Apache web sunucusunun önyükleme sırasında otomatik olarak başlatılmamasını sağlar.
systemctl status servis_adi	Bu komut, belirtilen hizmetin durumunu gösterir. Örneğin, "systemctl status apache2" komutu, Apache web sunucusunun çalışıp çalışmadığını ve hangi portlarda dinleme yaptığı gösterir.

systemctl list-unit-files	Bu komut, sistemdeki tüm hizmetleri ve bunların durumunu gösterir. Örneğin, "systemctl list-unit-files" komutu, sistemdeki tüm hizmetlerin listesini ve bunların etkin veya devre dışı olup olmadığını gösterir.
systemctl reload servis_adi	Bu komut, belirtilen hizmetin yapılandırma dosyalarını yeniden yükler. Örneğin, "systemctl reload apache2" komutu, Apache web sunucusunun yapılandırma dosyalarını yeniden yükler.

Tablo 2 "systemctl" Komutları ve İşlevleri

Systemctl, Kali Linux'ta kullanılan Systemd hizmetlerinin yanı sıra socket, device, mount, swap gibi birimleri de yönetebilen bir komuttur. Aşağıda, Systemctl ile bu birimlerin yönetimi ve dosya uzantıları hakkında daha detaylı bilgi verilmiştir:

Service birimleri: Bir hizmeti temsil eder. Örneğin, Apache web sunucusu bir hizmettir. Servis dosyaları ".service" uzantılıdır ve "/etc/systemd/system" klasöründe yer alırlar.

- Socket birimleri:** Socket birimleri, bir servis tarafından dinlenen bir iletişim soketi oluşturur. ".socket" socket birimlerinin tanımlanmasını sağlar.
- Device birimleri:** Device birimleri, bir donanım aygıtı veya sanal bir dosya sistemini temsil eder. ".device" device birimlerinin tanımlanmasını sağlar.
- Mount birimleri:** Mount birimleri, bir dosya sistemi veya ağ kaynağına bağlı bir noktayı temsil eder. ".mount" mount birimlerinin tanımlanmasını sağlar.
- Swap birimleri:** Swap birimleri, bellek alanlarından birini veya bir dosyayı kullanarak sanal bellek oluşturur. ".swap" swap birimlerinin tanımlanmasını sağlar.
- Automount:** Otomatik olarak bağlanacak bir dosya sistemi ya da aygıtı temsil eder. ".automount" bu birimin tanımlanmasını sağlayan uzantıdır.
- Target:** Bir grup hizmeti temsil eder ve belirli bir hedefe ulaşmak için bir arada çalışırlar. ".target" bu birimin tanımlanmasını sağlayan uzantıdır.
- Path:** Bir dosya veya dizin değişikliklerini izleyen bir birimdir. ".path" bu birimin tanımlanmasını sağlayan uzantıdır.
- Scope:** Bir işlem grubunu temsil eder. ".scope" bu birimin tanımlanmasını sağlayan uzantıdır.
- Slice:** Bir grup hizmeti ya da işlemi birlikte yönetir. ".slice" bu birimin tanımlanmasını sağlayan uzantıdır.
- Socket:** Bir ağ soketi ya da UNIX soketi oluşturur. ".socket" bu birimin tanımlanmasını sağlayan uzantıdır.
- Snapshot:** Bir sistem görüntüsü alır. ".snapshot" bu birimin tanımlanmasını sağlayan uzantıdır.
- Timer:** Belirli bir zaman aralığında hizmetleri veya işlemleri çalıştırılmak için kullanılır. ".timer" bu birimin tanımlanmasını sağlayan uzantıdır.

"systemctl list-units --type=birim_adi" komutu, Kali Linux'ta Systemd tarafından yönetilen hizmetlerin ve diğer sistem birimlerinin bir listesini verir. "birim_adi" yerine, hizmetler, socketler, targetler, cgroups, scopes, devices, timers, paths, mounts veya slices gibi birim türleri belirtilebilir. Bu komut, belirli bir birim türündeki tüm birimlerin bir listesini görüntüler.

Örneğin, "systemctl list-units --type=service" komutu, Kali Linux'ta yüklü olan tüm hizmetlerin bir listesini görüntüler. Çıktıda, her hizmetin durumu, adı, yükleme durumu, açıklaması ve diğer ayrıntıları yer alır.

Aşağıda, örnek bir "systemctl list-units --type=service" çıktısı verilmiştir:

```
(kali㉿PawnSecSecuritySolutions)-[~]
└─$ systemctl list-units --type=service

UNIT                  LOAD ACTIVE SUB   DESCRIPTION
accounts-daemon.service loaded active running Accounts Service
apache2.service       loaded active running The Apache HTTP Server
```

Bu çıktıda, UNIT sütunu hizmetlerin adını, LOAD sütunu hizmetin yüklediğini gösterirken, ACTIVE sütunu hizmetin durumunu (örneğin, "active" hizmetin çalıştığını veya "inactive" hizmetin durduğunu) ve SUB sütunu hizmetin alt durumunu (örneğin, "running" hizmetin çalışır durumda olduğunu veya "exited" hizmetin başarılı bir şekilde sonlandığını) gösterir. DESCRIPTION sütunu ise hizmetin kısa açıklamasını verir.

12.3.1 Service Unit

Systemd, sistem hizmetleri (services) için Service Unit (servis birimi) olarak adlandırılan yapıları kullanır. Systemd, bir hizmetin tanımlanmasını ve yönetilmesini sağlamak için Service Unit yapılarını kullanır. Service Unit, hizmetin çalıştırılması için gereken tüm bilgileri içerir. Örneğin, bir hizmetin nasıl başlatılacağı, durdurulacağı veya yeniden başlatılacağı gibi aksiyonları tanımlar. "systemctl cat ssh" komutu, ssh hizmeti için tanımlı olan Service Unit'in ayrıntılarını gösterir. Dosya içeriğini "cat" aracıyla incelesek Unit, Service ve Install olarak 3 bölüm görürüz.

1. **Unit:** Bu bölümde, Service Unit'ın ismi ve tanımlayıcı bilgileri yer alır. Örneğin, hizmetin adı ve açıklaması gibi bilgiler burada yer alabilir.
2. **Service:** Service Unit içinde, hizmetin nasıl çalışacağı hakkında bilgiler yer alır. Bu bölümde hizmetin başlatılması için gerekli komutlar, hizmetin çalışması sırasında yapılandırılması gereken ayarlar ve diğer hizmet özellikleri tanımlanır.
3. **Install:** Service Unit içinde, hizmetin sistemde nasıl yüklenmesi gerekiği hakkında bilgiler yer alır. Bu bölümde, hizmetin hangi hedef (target) sistemlerde çalıştırılacağı, hangi bağımlılıklara ihtiyaç duyduğu ve hizmetin otomatik olarak başlatılıp başlatılmayacağı gibi konular ele alınır.

```
(kali㉿KaliBook)-[~/Documents]
$ systemctl cat ssh.service
# /lib/systemd/system/ssh.service
[Unit]
Description=OpenBSD Secure Shell server
Documentation=man:sshd(8) man:sshd_config(5)
After=network.target auditd.service
ConditionPathExists=!/etc/ssh/sshd_not_to_be_run

[Service]
EnvironmentFile=-/etc/default/ssh
ExecStartPre=/usr/sbin/sshd -t
ExecStart=/usr/sbin/sshd -D $SSH_OPTS
ExecReload=/usr/sbin/sshd -t
ExecReload=/bin/kill -HUP $MAINPID
KillMode=process
Restart=on-failure
RestartPreventExitStatus=255
Type=notify
RuntimeDirectory=sshd
RuntimeDirectoryMode=0755

[Install]
WantedBy=multi-user.target
Alias=sshd.service
```

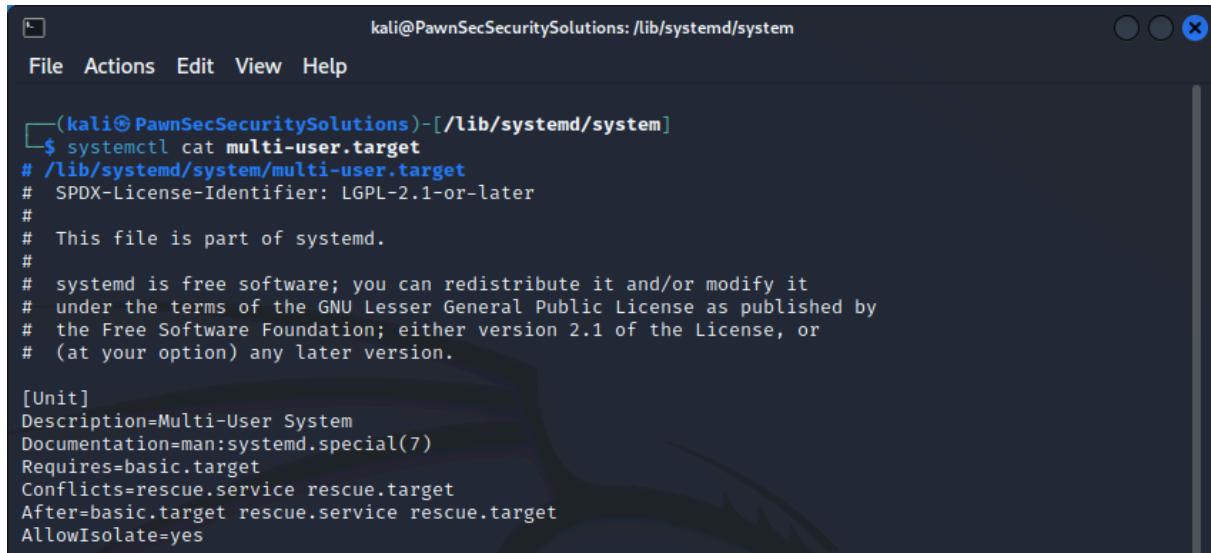
Şekil 41 "systemctl cat ssh" Komutunun Çıktısı

12.3.2 Target Unit

Target Unit, sistem yöneticilerinin hizmetleri ve diğer sistem bileşenlerini yönetmek için kullanabileceğiniz bir yapıdır. Sistemdeki farklı durumlar veya "hedefler" için önceden tanımlanmış

hedefler (targets) vardır. Örneğin, "multi-user.target" hedefi, birden fazla kullanıcının sisteme erişim sağlayabileceği bir hedefdir.

Hedeflerin tanımlanmasını ve hedefe özgü ayarların yapılandırılmasını sağlar. Her hedef, birden fazla Service Unit (servis birimi) veya diğer sistem bileşenlerinin çalışmasını etkiler. Örneğin, "multi-user.target" hedefi, ağ hizmetlerinin yanı sıra kullanıcı arabirimleri de dahil olmak üzere birçok hizmetin çalışmasını etkiler. Ayrıca sistem yöneticilerine hedeflere bağlı olan hizmetlerin durumunu kontrol etme ve gerektiğinde hedefi değiştirek sistem davranışını değiştirme imkânı sağlar. Örneğin, "rescue.target" hedefi, sistem kurtarma modunda kullanılabilir ve "poweroff.target" hedefi, sistemi kapatmak için kullanılabilir.



The screenshot shows a terminal window titled "kali@PawnSecSecuritySolutions: /lib/systemd/system". The window has a standard OS X style with a title bar, menu bar, and scroll bars. The terminal content displays the configuration of the "multi-user.target" service unit. It includes a header section with SPDX license information, a [Unit] section defining the service as a multi-user system, and a [Install] section specifying dependencies like "basic.target" and "rescue.service".

```
(kali㉿PawnSecSecuritySolutions)-[/lib/systemd/system]
└─$ systemctl cat multi-user.target
# /lib/systemd/system/multi-user.target
# SPDX-License-Identifier: LGPL-2.1-or-later
#
# This file is part of systemd.
#
# systemd is free software; you can redistribute it and/or modify it
# under the terms of the GNU Lesser General Public License as published by
# the Free Software Foundation; either version 2.1 of the License, or
# (at your option) any later version.

[Unit]
Description=Multi-User System
Documentation=man:systemd.special(7)
Requires=basic.target
Conflicts=rescue.service rescue.target
After=basic.target rescue.service rescue.target
AllowIsolate=yes
```

12.4 Recovery Mode

Kali Linux işletim sistemi, bir Recovery Mode (Kurtarma Modu) seçeneği sunar. Bu mod, sistemdeki sorunları çözmek veya diğer bakım işlemlerini gerçekleştirmek için kullanılabilir. Recovery Mode'a erişmek için bilgisayarın açılışında grub menüsünde "**recovery mode**" seçeneğini seçmeniz gerekmektedir.

Şekil 43 Recovery Moda GRUB Seçim Ekranında Giriş Yapmak

Şekil 44 Recovery Mode ile Sistemi Çalıştırma

Root Parolasını GRUB Seçim Ekranından Değiştirme

Root parolasını GRUB seçim ekranında sıfırlamak için aşağıdaki adımları izleyebilirsiniz:

1. Kali Linux'u başlatın ve GRUB seçim ekranında durun.
2. "e" tuşuna basarak seçilen önyükleme girdisini düzenlemek için grub konfigürasyonunu açın.
3. İlk satırın sonundaki "ro quiet" ifadesini "rw init=/bin/bash" ile değiştirin ve değişikliği kaydedin.
4. "ctrl+x" tuşlarına basarak değişiklikleri kaydederek önyüklemeyi başlatın.
5. Sistem, root hesabı için bir shell açarak durur.
6. Root parolasını sıfırlamak için "passwd root" komutunu girin.
7. Yeni bir parola girin ve ardından tekrar girin.
8. Parolanızı başarıyla sıfırladıktan sonra, "sync && reboot -f" komutunu kullanarak önyükleme tamamlanana kadar sistemi yeniden başlatın.

Bu işlem, root parolasını sıfırlamak için kullanışlı bir yöntemdir, ancak özellikle güvenliğin önemli olduğu ortamlarda, parolaları yönetmenin daha iyi bir yöntemi, örneğin sudo kullanımını sınırlamaktır. Ayrıca, bu işlemin doğru bir şekilde yapılması için iyi bir Linux sistem yönetimi bilgisine sahip olmak gereklidir.

13 KaliLinux Kernel Yönetimi

Kernel, bir işletim sisteminin en önemli bileşenlerinden biridir ve işletim sistemi çekirdeği olarak da adlandırılır. İşletim sistemi çekirdeği, bilgisayar donanımı ile uygulama programları arasındaki arabirimdir ve işletim sistemi kaynaklarının doğru bir şekilde kullanılmasını sağlar. Linux çekirdeği, Linux tabanlı işletim sistemlerinde kullanılan çekirdektir.

Kali Linux'da, kernel yönetimi, çeşitli nedenlerle gerekebilir. Örneğin, kullanıcılar, farklı sürücülerin veya donanım parçalarının doğru bir şekilde çalışması için kernel yapılandırmalarını değiştirebilirler. Ayrıca, güncellemeler veya güvenlik yamaları yayınlandığında, kullanıcılar bu yamaları kernel'e uygulayarak işletim sistemi güvenliğini artırabilirler.

Linux kernel, açık kaynaklı bir proje olarak geliştirilir ve sürekli olarak güncellenir. Linux kernel, birçok farklı işletim sistemi dağıtımında kullanılmaktadır ve bu nedenle, birçok kullanıcı ve geliştirici tarafından sürekli olarak incelenir ve test edilir. Çeşitli sürücüler ve protokoller destekleyen birçok özellik içerir. Bu özellikler, farklı donanım parçalarının doğru bir şekilde çalışmasını sağlar ve aynı zamanda işletim sistemi kaynaklarının doğru bir şekilde kullanılmasını da sağlar.

Kernel kaynak dosyaları ve dizinleri genellikle "/usr/src" dizininde bulunur. Bu dizinde, Linux kernel kaynak kodu bulunur ve kullanıcılar, kernel'i istedikleri şekilde yapılandırılabilir, derleyebilir ve yamalar uygulayabilir.

13.1 Kernel Modüllerini Yönetme

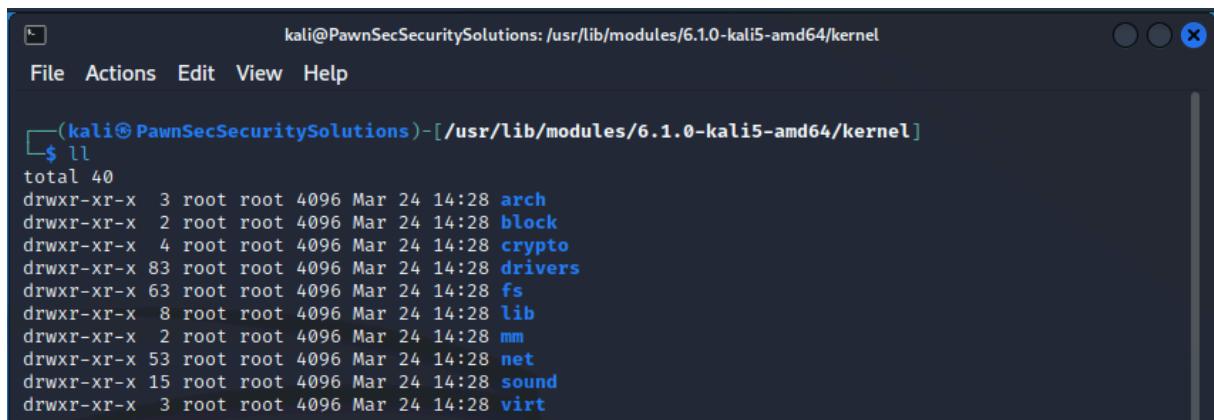
Kernel modülleri, Kali Linux ve diğer Linux tabanlı işletim sistemleri için çok önemlidir. Bu modüller, işletim sisteminin çeşitli donanım bileşenleri ve aygıtları ile etkileşim kurmasına olanak tanır. Örneğin, bir ağ kartı, bir depolama aygıtı veya bir yazıcı gibi donanım bileşenleri, ilgili kernel modüllerinin yüklenmesi ile etkinleştirilebilir.

Kali Linux'ta, kernel modüllerini yönetmek, sistemin performansını ve kullanımını optimize etmek için gereklidir. Kernel modüllerinin yönetimi, aşağıdaki görevleri içerir:

1. **Yeni modüllerin yüklenmesi:** Donanım aygıtları değiştiğinde veya yeni bir bileşen eklendiğinde, ilgili kernel modüllerinin yüklenmesi gerekebilir.
2. **Mevcut modüllerin kaldırılması:** Donanım bileşenleri değiştirildiğinde veya artık kullanılmadığında, ilgili kernel modüllerinin kaldırılması gerekebilir. Bu, sistem kaynaklarının boş harcanmasını önleyerek performansı artırabilir.
3. **Modüllerin yapılandırılması:** Kernel modülleri, yapılandırılabilen birçok özellik içerir. Bu özellikler, kullanıcıların modüllerin çalışma biçimini, hızını, bellek kullanımını ve diğer faktörleri özelleştirmesine olanak tanır.

Kernel modüllerinin yönetimi, aynı zamanda güvenlik ve sistem istikrarı açısından da önemlidir. Doğru modüllerin yüklenmesi ve yanlış modüllerin kaldırılması, sistemin çalışmasını etkileyebilir ve hatta sistem çökmesine neden olabilir.

Kernel (Çekirdek) içerisinde bulunan modüllere “**/usr/lib/modules/[Kali Çekirdek Sürümü]/kernel**” dizini ile ulaşabilirsiniz. Bu dizinde, çeşitli sürücü modülleri, sistem çağrıları ve diğer çekirdek bileşenleri yer alabilir.



```
kali@PawnSecSecuritySolutions: /usr/lib/modules/6.1.0-kali5-amd64/kernel
File Actions Edit View Help
└─(kali㉿PawnSecSecuritySolutions)-[/usr/lib/modules/6.1.0-kali5-amd64/kernel]
$ ll
total 40
drwxr-xr-x  3 root root 4096 Mar 24 14:28 arch
drwxr-xr-x  2 root root 4096 Mar 24 14:28 block
drwxr-xr-x  4 root root 4096 Mar 24 14:28 crypto
drwxr-xr-x 83 root root 4096 Mar 24 14:28 drivers
drwxr-xr-x 63 root root 4096 Mar 24 14:28 fs
drwxr-xr-x  8 root root 4096 Mar 24 14:28 lib
drwxr-xr-x  2 root root 4096 Mar 24 14:28 mm
drwxr-xr-x 53 root root 4096 Mar 24 14:28 net
drwxr-xr-x 15 root root 4096 Mar 24 14:28 sound
drwxr-xr-x  3 root root 4096 Mar 24 14:28 virt
```

Şekil 45 Modüllerin Görüntülenmesi

Yukarıdaki dizin uzantısından anlayacağınız üzere çekirdek sürümümüz “6.1.0-Kali5-amd64”dir. Bu dizin içerisindeki Kernel dosyasında “ll” komutunu kullanarak modülleri görüntüleyebiliyoruz.

Kali Linux'ta kernel modüllerini yönetmek için, birkaç farklı komut kullanılabilir. İşte bunlardan bazıları:

modprobe

Bu komut, kernel modüllerini yüklemek veya kaldırmak için kullanılır. "modprobe" komutu, modülün adını veya yolu belirtilerek kullanılır. Örneğin, "modprobe ip_tables" komutu, ip_tables modülünü yükler.

lsmod

Bu komut, yüklü olan tüm kernel modüllerini listeler. Komutun çıktısı, modüllerin adını, kullanım sayısını ve diğer bazı bilgileri içerir. Bu komutun çıktısında sırasıyla modülün ismi, bellekteki boyutu, kaç tane modül tarafından kullanıldığının sayısı ve hangi modülün kullandığını gösterir.

Module	Size	Used by
rfkill	36864	2
qrtr	49152	4
vboxsf	45056	0
sunrpc	692224	1
binfmt_misc	24576	1
snd_intel8x0	49152	2
snd_ac97_codec	176128	1 snd_intel8x0

Şekil 46 "lsmod |less" Komutuyla Modüllerin Görüntülenmesi

modinfo

Bu komut, bir kernel modülü hakkında bilgi verir. Komutun kullanımı, "modinfo modül_adi" şeklindedir.

```
(kali㉿PawnSecSecuritySolutions)-[/sys/class/net/eth0/device]
$ ll
total 0
-r--r--r-- 1 root root 4096 Apr 1 11:11 ari_enabled
-rw-r--r-- 1 root root 4096 Apr 1 12:03 broken_parity_status
-r--r--r-- 1 root root 4096 Apr 1 11:11 class
-rw-r--r-- 1 root root 256 Apr 1 11:11 config
-r--r--r-- 1 root root 4096 Apr 1 12:03 consistent_dma_mask_bits
-rw-r--r-- 1 root root 4096 Apr 1 12:03 d3cold_allowed
-r--r--r-- 1 root root 4096 Apr 1 11:11 device
-r--r--r-- 1 root root 4096 Apr 1 12:03 dma_mask_bits
lrwxrwxrwx 1 root root 0 Apr 1 11:11 driver → ../../bus/pci/drivers/e1000
```

Şekil 47 Network Adapktörünün Driver Dizini

Yukarıda sistemimizde bulunan network adaptörünün driver dizinine giriş yaptığımızı ve dosyalara ait izinlerin ve dosya boyutlarının verildiğini görüyoruz.

```
filename: /lib/modules/6.1.0-kali5-amd64/kernel/drivers/net/ethernet/intel/e1000/e1000.ko
license: GPL v2
description: Intel(R) PRO/1000 Network Driver
author: Intel Corporation, <linux.nics@intel.com>
alias: pci:v00008086d00002E6Sv*sd*bc*sc*i*
alias: pci:v00008086d000010B5sv*s*d*bc*sc*i*
alias: pci:v00008086d00001099sv*sd*bc*sc*i*
alias: pci:v00008086d0000108Asv*sd*bc*sc*i*
alias: pci:v00008086d0000107Csv*sd*bc*sc*i*
```

Şekil 48 "modinfo e1000 | less" Komutuyla Network Driver'ı Hakkında Bilgi Alma

Şekil 47'de ise "modinfo e1000 | less" komutunu kullanarak Network Driver'ı hakkında daha detaylı bilgiler edinebiliyoruz.

insmod

Bu komut, önceden derlenmiş bir kernel modülünü yüklemek için kullanılır. Komutun kullanımı, "insmod modül_adı" şeklindedir.

rmmod

Bu komut, yüklü olan bir kernel modülünü kaldırmak için kullanılır. Komutun kullanımı, "rmmod modül_adı" şeklindedir.

depmod

Bu komut, sisteme yüklenen modüllerin bağımlılıklarını belirlemek ve bir veri tabanında depolamak için kullanılır. Bu veri tabanı, modüllerin birbirleriyle olan bağımlılıklarını takip etmek için kullanılır. "/lib/modules/" altındaki modül dosyalarını tarar ve modüllerin birbirine bağlayan ilişkileri belirler. Bu ilişkiler, modüllerin sıralanması ve yüklenmesi sırasında kullanılır. Modül bağımlılıklarını belirlemek için kullanılan diğer araçlara (örneğin, modprobe) veritabanından bilgi alır.

13.2 Kernel Modüllerini Düzenlenmesi

Kali Linux işletim sisteminde, kernel modülleri bazen özel donanım veya yazılım gereksinimlerini karşılamak için düzenlenmesi gerekebilir. Bu tür durumlarda, modüllerde değişiklik yapmak gerekebilir. Modül düzenlenmesi, modülün işlevsellliğini değiştirebilir veya mevcut bir modülü yeni bir donanım parçası veya yazılım bileşeniyle uyumlu hale getirebilir.

Modüllerde değişiklik yapmak için, öncelikle modülün kaynak koduna veya derlenmiş modül dosyasına erişmek gerekir. Kaynak koduna erişmek için, genellikle modülün kaynak kodu depolarına gitmek gerektir. Derlenmiş bir modül dosyasını değiştirmek için, dosyanın bulunduğu dizine gitmek yeterlidir.

Örneğin:

Ağ kartı sürücüsü modülü ile ilgili bir değişiklik yapmayı ele alalım. Örneğin, ağ kartı sürücüsü modülü, ağ kartı donanımını desteklemediği için çalışmıyor, modülün kaynak koduna erişmek gerekebilir. Kaynak kodunu düzenleyerek, modülün donanımı desteklemesini sağlayacak değişiklikler yapılabilir. Daha sonra, modül yeniden derlenir ve kurulur.

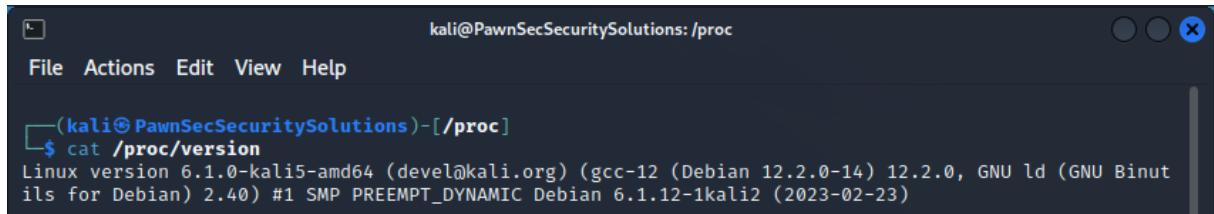
Benzer şekilde, bir modülü yeni bir donanım veya yazılım bileşeniyle uyumlu hale getirmek de gerekebilir. Bu durumda, modülün kaynak kodunu veya derlenmiş dosyasını düzenlemek gerekebilir.

Modül düzenlenmesi, doğru şekilde yapılmazsa sisteminizin stabilitesini etkileyebilir veya sisteminizin düzgün çalışmasını önleyebilir. Bu nedenle, modül düzenlenmesi yapmadan önce yedekleme yapmak ve işlemleri dikkatle takip etmek önemlidir. Ayrıca, modülün uyumlu olması için doğru derleme parametreleri kullanmak ve modülü doğru bir şekilde yeniden yüklemek gerekebilir.

13.3 Kernel Sürümünü Öğrenme

Çekirdek sürümü, işletim sisteminizin en temel bileşenidir ve donanımınızla iletişim kurarak diğer yazılımların çalışmasına izin verir. Çekirdek sürümü, donanım sürücülerini, ağ protokollerini, dosya sistemleri ve diğer temel sistem bileşenlerinin birleşimidir. Yeni bir çekirdek sürümü, önceki sürümü göre daha iyi performans, daha iyi donanım desteği ve yeni özellikler sağlayabilir. Güncel bir çekirdek sürümü, güvenlik yamaları ve hata düzeltmeleri de içerebilir. Bu nedenle, işletim sisteminizi güncel tutmak ve en son çekirdek sürümünü kullanmak önemlidir.

Kali Linux'da çekirdek sürümünü öğrenmek için “**uname -r**” veya “**cat /proc/version**” komutunu kullanabilirsiniz.



A terminal window titled "kali@PawnSecSecuritySolutions: /proc". The window has a standard OS X-style title bar with icons for close, minimize, and maximize. The menu bar includes "File", "Actions", "Edit", "View", and "Help". Below the menu is a command-line interface. The command entered is "cat /proc/version". The output shows the kernel version: "Linux version 6.1.0-kali5-amd64 (devel@kali.org) (gcc-12 (Debian 12.2.0-14) 12.2.0, GNU ld (GNU Binutils for Debian) 2.40) #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali2 (2023-02-23)".

Şekil 49 Kernel Versiyonunu Öğrenme

Genellikle, bir çekirdek versiyon numarası üç parçaya ayrılır:

“**x.y.z**”

Burada “**x**” ana sürüm numarasıdır ve genellikle büyük bir değişikliği ifade eder. Örneğin, 2.x serisi, 3.x serisinden önemli ölçüde farklıdır.

“**y**” alt sürüm numarasıdır ve genellikle yeni özellikler veya performans iyileştirmeleri gibi küçük değişiklikleri ifade eder.

“**z**” yama sürüm numarasıdır ve genellikle hata düzeltmeleri ve güvenlik yamaları gibi küçük değişiklikleri ifade eder.

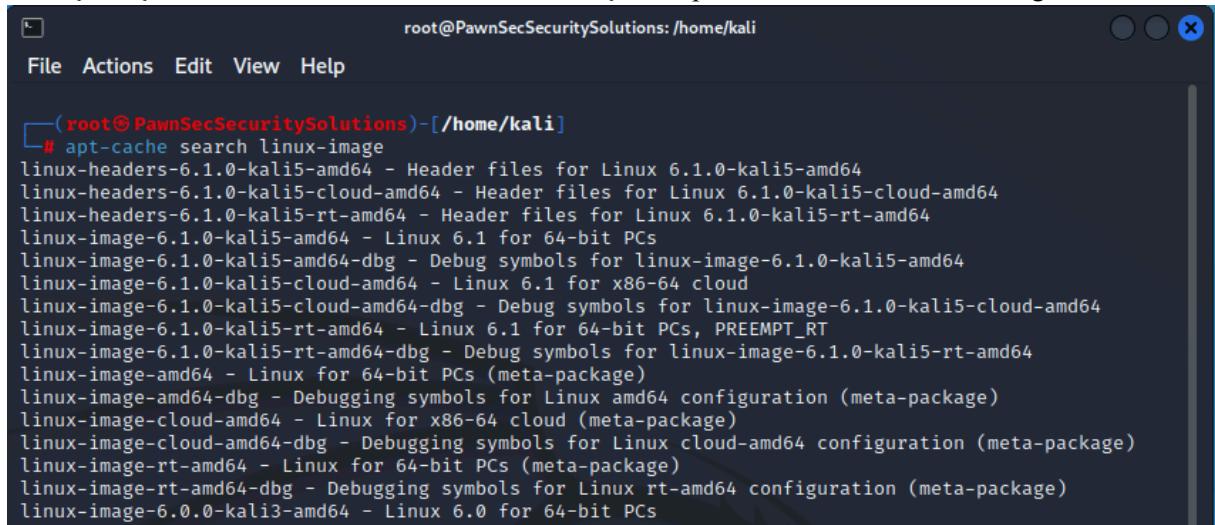
Örneğin, “6.1.0-kali5-amd64” çekirdek versiyonu, 6.x ana sürüm numarasını, 1.x alt sürüm numarasını ve 0 yama sürüm numarasını ifade eder. Bu sürüm, 6.x serisinin birinci alt sürümü ve 0 yama sürümüdür.

13.4 Kernel Sürümünü Güncelleme

KaliLinux'ta kernel güncellemek oldukça önemli bir işlemidir ve bu işlemi yaparken dikkatli olmak gereklidir. Bazı donanım sürücülerleri ve modülleri yalnızca belirli kernel sürümleriyle uyumlu olabilir. Bu nedenle, yeni bir kernel sürümü yükledikten sonra, mevcut donanımınızın uyumlu olup olmadığını kontrol etmeniz önerilir.

Ayrıca, kernel güncellemeleri önemli sistem değişiklikleri olduğundan, işletim sisteminizin istikrarını etkileyebilir. Bu nedenle, kernel güncellemesi yapmadan önce sisteminizi yedeklemeyi veya güncelleme sonrasında sisteme herhangi bir hata olup olmadığını kontrol etmeyi düşünebilirsiniz.

Zaten kernel sürümünü nasıl öğreneceğimizi söylemişik. Kernel sürümünüzü öğrendikten sonra en son çıkışlı olan sürümleri kontrol etmek için “apt-cache search linux-image” komutunu



```
root@PawnSecSecuritySolutions: /home/kali
File Actions Edit View Help
( root@PawnSecSecuritySolutions ) - [ /home/kali ]
# apt-cache search linux-image
linux-headers-6.1.0-kali5-amd64 - Header files for Linux 6.1.0-kali5-amd64
linux-headers-6.1.0-kali5-cloud-amd64 - Header files for Linux 6.1.0-kali5-cloud-amd64
linux-headers-6.1.0-kali5-rt-amd64 - Header files for Linux 6.1.0-kali5-rt-amd64
linux-image-6.1.0-kali5-amd64 - Linux 6.1 for 64-bit PCs
linux-image-6.1.0-kali5-amd64-dbg - Debug symbols for linux-image-6.1.0-kali5-amd64
linux-image-6.1.0-kali5-cloud-amd64 - Linux 6.1 for x86-64 cloud
linux-image-6.1.0-kali5-cloud-amd64-dbg - Debug symbols for linux-image-6.1.0-kali5-cloud-amd64
linux-image-6.1.0-kali5-rt-amd64 - Linux 6.1 for 64-bit PCs, PREEMPT_RT
linux-image-6.1.0-kali5-rt-amd64-dbg - Debug symbols for linux-image-6.1.0-kali5-rt-amd64
linux-image-amd64 - Linux for 64-bit PCs (meta-package)
linux-image-amd64-dbg - Debugging symbols for Linux amd64 configuration (meta-package)
linux-image-cloud-amd64 - Linux for x86-64 cloud (meta-package)
linux-image-cloud-amd64-dbg - Debugging symbols for Linux cloud-amd64 configuration (meta-package)
linux-image-rt-amd64 - Linux for 64-bit PCs (meta-package)
linux-image-rt-amd64-dbg - Debugging symbols for Linux rt-amd64 configuration (meta-package)
linux-image-6.0.0-kali3-amd64 - Linux 6.0 for 64-bit PCs
```

kullanabilirsiniz.

Bu komut, depolardaki tüm linux-image paketlerini listeleyecektir. En son sürümü arayın ve sürüm numarasını not edin. Şimdi, istediğiniz kernel sürümünü yüklemek için “sudo apt-get install linux-image-<sürüm numarası>-amd64” komutunu kullanabilir ya da “sudo apt-get update” komutunu kullanarak en son çıkışlı olan kernel sürümünü yükleyebilirsiniz.

Yeni kernel sürümünü etkinleştirmek için, bilgisayarınızı yeniden başlatmanız gerekebilir. Yeniden başlattıktan sonra, yeni kernel sürümünü doğrulamak için tekrar “uname -r” komutunu kullanabilirsiniz.

13.5 Eski Kernel Sürümlerinin Kaldırılması

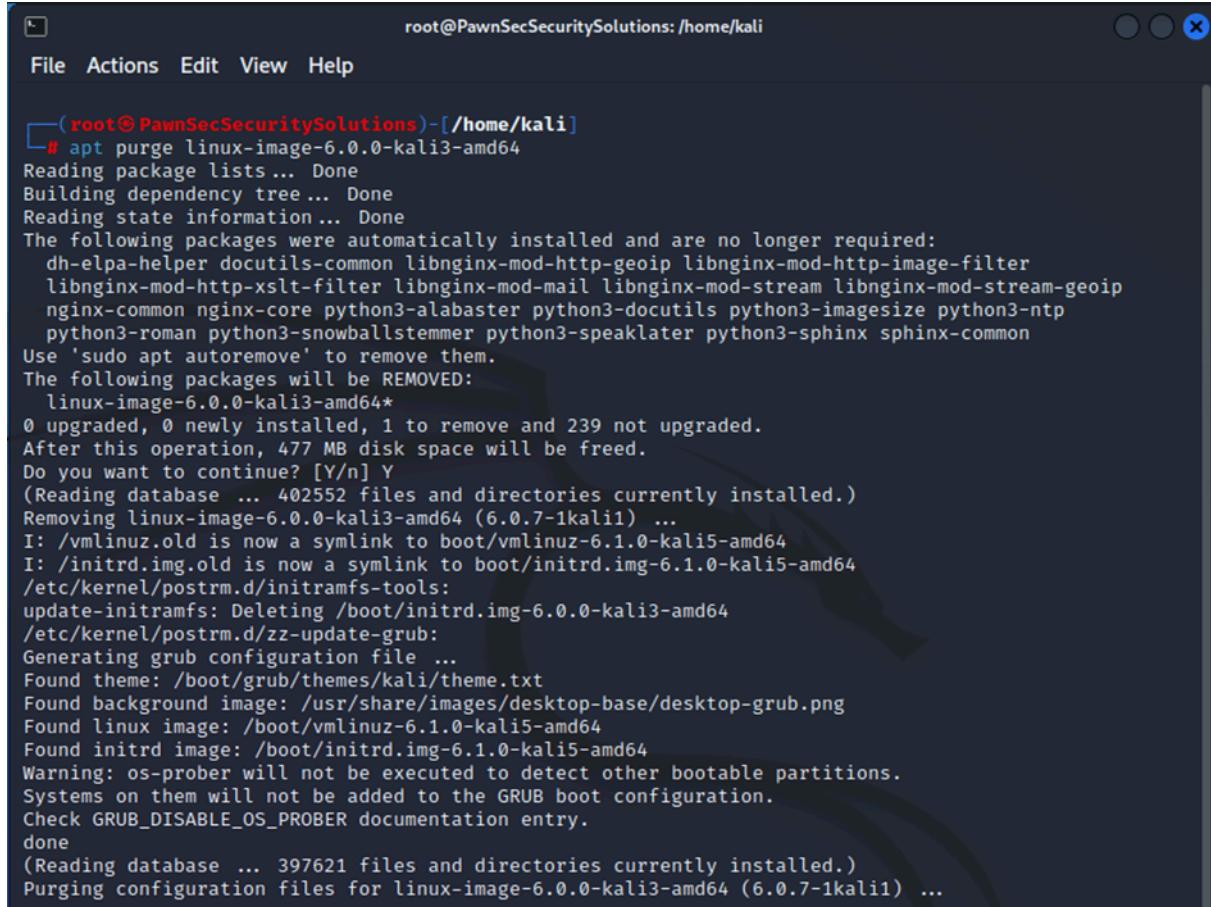
Kullanmak istemediğiniz eski kernel sürümlerini silmek ve sisteminizde kullanılmayan sürümleri kaldırarak depolama alanı açmak da mümkündür. Bu işlem için ilk önce “dpkg --list | grep linux-image” komutunu kullanarak sisteminizde yüklü olan tüm kernel sürümlerinin görüntülenmesini sağlayın.



```
root@PawnSecSecuritySolutions: /home/kali
File Actions Edit View Help
( root@PawnSecSecuritySolutions ) - [ /home/kali ]
# dpkg --list | grep linux-image
ii  linux-image-6.0.0-kali3-amd64      6.0.7-1kali1          amd64      Linux 6.
0 for 64-bit PCs
ii  linux-image-6.1.0-kali5-amd64      6.1.12-1kali2         amd64      Linux 6.
1 for 64-bit PCs
ii  linux-image-amd64                 6.1.12-1kali2         amd64      Linux fo
r 64-bit PCs (meta-package)
```

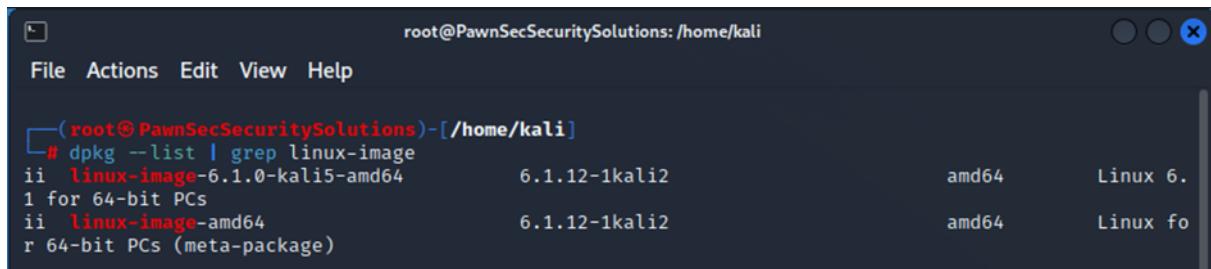
Şekil 51 "dpkg --list | grep linux-image" Komutuyla Sistemde Bulunan Kernel Versyonlarının Öğrenilmesi

Kullanmadığınız eski kernel sürümlerini kaldırmak için “**apt purge linux-image-<sürüm numarası>**” komutunu kullanabilirsiniz. Biz zaten Şekil 49’da kendi kernel versiyonumuzu öğrenmiştık. Şimdi buna göre kullanmadığımız “**6.0.0-kali3-amd64**” kernel sürümünün kaldırmasını sağlayalım.



```
root@PawnSecSecuritySolutions:/home/kali
File Actions Edit View Help
└──(root@PawnSecSecuritySolutions)-[/home/kali]
# apt purge linux-image-6.0.0-kali3-amd64
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  dh-elpa-helper docutils-common libnginx-mod-http-geoip libnginx-mod-http-image-filter
  libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip
  nginx-common nginx-core python3-alabaster python3-docutils python3-imagesize python3-ntp
  python3-roman python3-snowballstemmer python3-speaklater python3-sphinx sphinx-common
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  linux-image-6.0.0-kali3-amd64*
0 upgraded, 0 newly installed, 1 to remove and 239 not upgraded.
After this operation, 477 MB disk space will be freed.
Do you want to continue? [Y/n] Y
(Reading database ... 402552 files and directories currently installed.)
Removing linux-image-6.0.0-kali3-amd64 (6.0.7-1kali1) ...
I: /vmlinuz.old is now a symlink to boot/vmlinuz-6.1.0-kali5-amd64
I: /initrd.img.old is now a symlink to boot/initrd.img-6.1.0-kali5-amd64
/etc/kernel/postrm.d/initramfs-tools:
update-initramfs: Deleting /boot/initrd.img-6.0.0-kali3-amd64
/etc/kernel/postrm.d/zz-update-grub:
Generating grub configuration file ...
Found theme: /boot/grub/themes/kali/theme.txt
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-6.1.0-kali5-amd64
Found initrd image: /boot/initrd.img-6.1.0-kali5-amd64
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
done
(Reading database ... 397621 files and directories currently installed.)
Purging configuration files for linux-image-6.0.0-kali3-amd64 (6.0.7-1kali1) ...
```

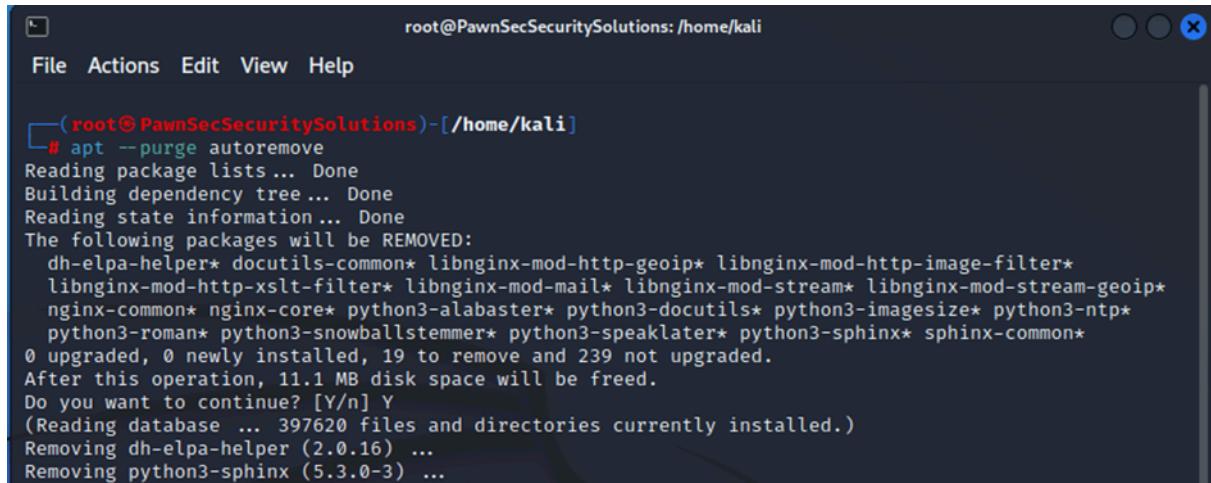
Şekil 52 Kullanılmayan Kernel Sürümünün Kaldırılması



```
root@PawnSecSecuritySolutions:/home/kali
File Actions Edit View Help
└──(root@PawnSecSecuritySolutions)-[/home/kali]
# dpkg --list | grep linux-image
ii  linux-image-6.1.0-kali5-amd64      6.1.12-1kali2          amd64      Linux 6.
1 for 64-bit PCs
ii  linux-image-amd64                 6.1.12-1kali2          amd64      Linux fo
r 64-bit PCs (meta-package)
```

Şekil 53 Kalan Sürümlerin Görüntülenmesi

Kaldırma işlemi tamamlandıktan sonra, gereksiz dosya ve paketleri temizlemek için “**apt –purge autoremove**” komutunu kullanabilirsiniz.



```
root@PawnSecSecuritySolutions:/home/kali
File Actions Edit View Help
└─(root@PawnSecSecuritySolutions)-[/home/kali]
  # apt --purge autoremove
  Reading package lists... Done
  Building dependency tree... Done
  Reading state information... Done
  The following packages will be REMOVED:
    dh-elpa-helper* docutils-common* libnginx-mod-http-geoip* libnginx-mod-http-image-filter*
    libnginx-mod-http-xslt-filter* libnginx-mod-mail* libnginx-mod-stream* libnginx-mod-stream-geoip*
    nginx-common* nginx-core* python3-alabaster* python3-docutils* python3-imagesize* python3-ntp*
    python3-roman* python3-snowballstemmer* python3-speaklater* python3-sphinx* sphinx-common*
  0 upgraded, 0 newly installed, 19 to remove and 239 not upgraded.
  After this operation, 11.1 MB disk space will be freed.
  Do you want to continue? [Y/n] Y
  (Reading database ... 397620 files and directories currently installed.)
  Removing dh-elpa-helper (2.0.16) ...
  Removing python3-sphinx (5.3.0-3) ...
```

Şekil 54 Gereksiz Dosya ve Paketlerin Temizlenmesi

13.6 Kernel Downgrade

Kernel downgrade, işletim sistemi üzerinde yüklü olan mevcut Linux kernel sürümünün daha eski bir sürümüne geri dönüş yapmak anlamına gelir. Bazen, yeni bir kernel sürümü yükseltilmesi sonrasında sistemde kararlılık veya uyumluluk sorunları yaşanabilir. Bu tür sorunlarla karşılaşılması durumunda, kullanıcılar sistemi daha önce kullanılan bir kernel sürümüne geri döndürmek için kernel downgrade işlemi yapabilirler.

Örneğin, “6.0.0-kali3-amd64” sürümüne geri dönmek istiyorsanız root kullanıcısı olarak “**apt install linux-image-6.0.0-kali3-amd64**” komutunu kullanın. Ardından, indirilen kernel sürümünü kurmak için “**dpkg -i /var/cache/apt/archives/linux-image-6.0.0-kali3-amd64.deb**” komutunu kullanarak dosyasının tam yolunu belirtin. Kurulum tamamlandıktan sonra, yeni kurulan kernel sürümünü grub menüsünde eklemek için “**sudo update-grub**” komutunu kullanın. Son olarak sistemi yeniden başlatın ve yeni kurulan kernel sürümüne geçiş yapın.

13.7 Sistem Yönetim Komutları

Sistem yönetimi işlemlerini gerçekleştirmek için kullanılan bazı önemli komutlar şunlardır:

uname: Sistem çekirdeği hakkında bilgi veren bir komuttur. Kullanabileceğiniz bazı parametreler:

-a: Tüm sistem bilgilerini gösterir

-r: Çekirdek sürümünü gösterir

-s: İşletim sistemi adını gösterir

-m: İşlemci mimarisini gösterir

hostnamectl: Sistem ana bilgisayar adı hakkında bilgi verir ve değiştirmeye izin verir. Kullanabileceğiniz bazı parametreler:

status: Mevcut bilgisayar adını ve bağlı olduğu ağ bağlantılarını gösterir

set-hostname: Yeni bir bilgisayar adı ayarlar

dmesg: Sistemdeki kernel mesajlarına erişmenizi sağlayan bir komuttur. Bu mesajlar sistem üzerindeki servis ve donanım sürücülerinin durumlarını ve hatalarını gösterir. Kullanabileceğiniz bazı parametreler:

- T: Tarih ve saatleri insan okunabilir biçimde gösterir
- H: Mesajları HTML biçiminde gösterir