

Linux Forensics



Efekan ACAR

Linux Forensics

Linux popüler olarak kullanılan açık kaynaklı bir işletim sistemidir. Sıkça sunucu işletim sistemlerinde görülse de standart kullanıcılar tarafından da kullanılıyor. Güvenlik nedeniyle birçok kişi ve kurumlar kullanmaktadır. Ancak her sistemin olduğu gibi Linux da yüzde 100 güvenli değildir. İşte burada Linux Forensics (Linux Adli Bilişim) karşımıza çıkıyor. Hukuk davalarında veya güvenlik olaylarında elektronik delillerin toplanabilmesi ve analiz edilebilmesi için Linux Forensics hakkında bilgi sahibi olmalıyız.

Linux Forensics dosya sistemleri, ağ trafiği ve diğer sistem bileşenlerini izleyerek, saldırı tarihini, saldırganların kimliğini ve diğer önemli ayrıntıları belirlemeye yardımcı olur. Bunu bazı araç ve eklentiler sayesinde yapabiliriz. Temel olarak Linux Forensics yazılım ve donanım olarak 2 kategoriye ayrılabilir.

Yazılım tabanlı Linux Forensics araçları ile kullanıcı hesapları, ağ ve uygulama bilgilerini analiz edebiliriz. Bu alanda başlıca araçlar şunlardır:

- **dd**: Disk görüntüsü olarak da bilinen bir sabit sürücünün bit bit kopyasını oluşturmak için bir araç.
- **grep**: Bir metin dosyasında belirli anahtar sözcükleri veya tümcecikleri aramak için bir araç.
- **strings**: İkili dosyalardan insan tarafından okunabilir metin çıkarmak için bir araç.
- **netstat**: Etkin ağ bağlantılarını ve açık bağlantı noktalarını görüntülemek için bir araç.
- **ps**: Çalışan işlemlerin bir listesini görüntülemek için bir araç.
- **tcpdump**: Ağ trafiğini yakalamak ve analiz etmek için bir araç.

Donanım tabanlı Linux Forensics araçları donanım bileşenleri ile ilgili analiz yapmamızı sağlar. Başlıca araçlar şunlardır:

- **lshw**: Bir sistemin donanım bileşenleri hakkında ayrıntılı bilgileri listeleyen bir araç.
- **smartctl**: Sabit sürücülerin sağlık durumunu kontrol etmek için bir araç.
- **ethtool**: Ağ arayüzü ayrıntılarını görüntülemek ve yapılandırmak için bir araç.

Temel bilgi toplama komutları şunlardır :

- **ls**: Bulunduğunuz dizindeki dosya ve klasörleri listeler.
- **pwd**: Bulunduğunuz dizinin yolunu gösterir.
- **cd**: Dizinler arasında gezinmenizi sağlar.
- **cat**: Dosyaların içeriğini görüntüler.
- **grep**: Belirli bir metin veya kelimeyi dosyalarda veya çıktılarda arar.
- **top**: Sistem kaynaklarını ve işlem bilgilerini görüntüler.
- **ps**: Çalışan tüm işlemleri görüntüler.

- **who:** Sisteme kimlerin bağlı olduğunu görüntüler.
- **w:** Sistemdeki kullanıcıların ne yaptığını görüntüler.
- **ifconfig:** Ağ ayarlarını ve arayüz bilgilerini görüntüler.
- **netstat:** Ağ bağlantıları hakkında bilgi sağlar.
- **route:** Ağ rotaları hakkında bilgi sağlar.
- **ping:** Bir ağ cihazına erişilebilirliği kontrol etmek için kullanılır.
- **traceroute:** Ağdaki rota ve iletişim yollarını görüntüler.
- **df:** Disk kullanımı hakkında bilgi sağlar.
- **du:** Dosya veya dizinlerin disk alanını ölçer.

```

root@kali: /home/kali/Desktop/juice-shop
File Actions Edit View Help

(root@kali)-[/home/kali/Desktop]
# cd juice-shop

(root@kali)-[/home/kali/Desktop/juice-shop]
# ls
app.json          docker-compose.test.yml  logs              server.ts
app.ts            Dockerfile               models            SOLUTIONS.md
build             Dockerfile.arm           monitoring         swagger.yml
CODE_OF_CONDUCT.md encryptionkeys            node_modules      test
config            frontend                 package.json      threat-model.json
config.schema.yml ftp                      README.md         tsconfig.json
CONTRIBUTING.md  Gruntfile.js             REFERENCES.md     uploads
crowdin.yaml      HALL_OF_FAME.md          routes            vagrant
ctf.key           i18n                     rsn              vapi
cypress.json      lib                      screenshots       views
data              LICENSE                  SECURITY.md

(root@kali)-[/home/kali/Desktop/juice-shop]
# pwd
/home/kali/Desktop/juice-shop

(root@kali)-[/home/kali/Desktop/juice-shop]
# cat LICENSE
Copyright (c) 2014-2022 Bjoern Kimminich & the OWASP Juice Shop contributors

Permission is hereby granted, free of charge, to any person
obtaining a copy of this software and associated documentation
files (the "Software"), to deal in the Software without
restriction, including without limitation the rights to use,
copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following
conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES
OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND

```

Uçucu Veriler

Bir makine kapatıldığında kaybolan verilere uçucu veriler denir. Bir adli soruşturma sırasında bu veriler büyük önem taşır. Tarih, saat, saat dilimi, ağ bilgileri, açık portlar, açık dosyalar, çalışan processler uçucu verilere örnektir.

Temel Bilgiler(Makine adı, tarih ve saat bilgileri)

Makine adını öğrenmek için `hostname` komutunu kullanabiliriz bunu öğrenmemiz daha sonra ağ bilgilerini öğrenirken işimize yarar. `date` komutu ile tarihi ve saati yazdırabiliriz. `timedatectl` ile saat dilimini öğrenebiliriz.

```
(root@kali)-[~]
# hostname
kali

(root@kali)-[~]
# date
Fri Feb 24 07:13:33 AM EST 2023

(root@kali)-[~]
# timedatectl
      Local time: Fri 2023-02-24 07:15:51 EST
      Universal time: Fri 2023-02-24 12:15:51 UTC
              RTC time: Fri 2023-02-24 12:15:51
      Time zone: America/New_York (EST, -0500)
System clock synchronized: yes
              NTP service: n/a
      RTC in local TZ: no

(root@kali)-[~]
#
```

Burada makinemizin isminin kali olduğu görüyoruz. 24 Şubat 2023 Cuma ve saat 7yi 13 geçiyor. Saat dilimine baktığımız zaman -05.00 olduğunu görüyoruz ve Amerika/New York saat dilimini kullanıyor.

Ağ Bilgileri

`ip addr show` komutu ile Linux sistemlerinde ağ arayüzleri, ip adresleri ve ağ yapılandırma bilgilerini görebiliriz. `ifconfig` komutu da `ip addr Show` ile aynı özelliklere sahiptir ve üstüne ek ağ yapılandırma bilgilerini değiştirebilmektedir. `ifconfig` komutunu `ifconfig <arayüz adı>` şeklinde kullanabilirsiniz.

```

(root@kali)-[~]
# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group defa
ult qlen 1000
    link/ether 00:0c:29:d8:4d:e3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.18.152/24 brd 192.168.18.255 scope global dynamic noprefixroute eth0
        valid_lft 1756sec preferred_lft 1756sec
    inet6 fe80::fdc9:d0e3:dbef:c107/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
9: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNO
WN group default qlen 500
    link/none

(root@kali)-[~]
# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.18.152 netmask 255.255.255.0 broadcast 192.168.18.255
    inet6 fe80::fdc9:d0e3:dbef:c107 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:d8:4d:e3 txqueuelen 1000 (Ethernet)
    RX packets 1817277 bytes 2204601500 (2.0 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 999575 bytes 149017082 (142.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Burada gördüğümüz gibi Ethernet bağlantısı mevcut ve ip adresi “192.168.18.152”

netstat komutu Linux sistemlerde ağ bağlantılarını görmeyi sağlar. Bazı kullanım örnekleri şunlardır:

- **netstat -a** komutu, tüm açık ağ bağlantılarını ve bağlantı noktalarını listeler.
- **netstat -t** komutu, TCP bağlantılarını listeler.
- **netstat -u** komutu, UDP bağlantılarını listeler.
- **netstat -l** komutu, dinleme modunda olan (listening) bağlantıları listeler.
- **netstat -n** komutu, IP adreslerini ve bağlantı noktalarını sayısal formatta gösterir.
- **netstat -p** komutu, bağlantılarla ilgili işlem adını (PID) gösterir.

```
(root@kali)-[~]
# netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.9.30.220:4444        0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:34114          0.0.0.0:*               *
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (only servers)
Proto RefCnt Flags               Type                   State                  I-Node  Path
unix   2      [ ACC ]                STREAM                LISTENING              18193   /tmp/ssh-XXXXXXIn1jvw/agent
.1141
unix   2      [ ACC ]                STREAM                LISTENING              17833   /tmp/.X11-unix/X0
unix   2      [ ACC ]                STREAM                LISTENING              18213   /tmp/.ICE-unix/1141
unix   2      [ ACC ]                STREAM                LISTENING              1637    /run/systemd/private
unix   2      [ ACC ]                STREAM                LISTENING              1639    /run/systemd/userdb/io.syst
emd.DynamicUser
unix   2      [ ACC ]                STREAM                LISTENING              1640    /run/systemd/io.system.Mana
gedOOM
unix   2      [ ACC ]                STREAM                LISTENING              1652    /run/systemd/fsck.progress
unix   2      [ ACC ]                STREAM                LISTENING              1659    /run/systemd/journal/stdout
unix   2      [ ACC ]                SEQPACKET             LISTENING              1661    /run/udev/control
unix   2      [ ACC ]                STREAM                LISTENING              18058   /run/user/1000/systemd/priv
ate
unix   2      [ ACC ]                STREAM                LISTENING              18067   /run/user/1000/bus
unix   2      [ ACC ]                STREAM                LISTENING              18069   /run/user/1000/gnupg/S.dirm
ngr
unix   2      [ ACC ]                STREAM                LISTENING              18071   /run/user/1000/gcr/ssh
unix   2      [ ACC ]                STREAM                LISTENING              18073   /run/user/1000/keyring/cont
rol
unix   2      [ ACC ]                STREAM                LISTENING              18075   /run/user/1000/gnupg/S.gpg-
agent.browser
```

Burada listening yapan bağlantıların tümünü görebiliyoruz.

Açık Port Bilgileri

nmap localhost komutu ile açık bağlantı noktalarını görebilirsiniz.

```
(root@kali)-[~]
# nmap localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-24 08:28 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000054s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

Makinede açık port bulunsaydı burada gözükecekti.

lsof komutu dosyaların işlem tarafından kullanıldığı tespit etmeye yarar.

```
(root@kali)-[~]
# lsof -i -P -n
COMMAND      PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
NetworkMa    77151 root    27u  IPv4 631476      0t0  UDP 192.168.18.152:68→192.168.18.2
54:67
tiny-http    199092 root     3u  IPv4 393779      0t0  TCP 10.9.30.220:4444 (LISTEN)
openvpn      290827 root     3u  IPv4 633292      0t0  UDP *:34114
```

Burada açık portlarda çalışan işlemleri ve ayrıntılarını görüyoruz.

Çalışan İşlemler

`ps` komutu sistemde çalışan işlemleri, bu işlemlerin durumları, bellek kullanımları vb. özellikleri gösterir. Çeşitli parametreler kullanılabilir.

```
(root@kali)-[~]
# ps aux
```

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.0	0.1	177068	13500	?	Ss	Feb23	0:31	/sbin/init splash
root	2	0.0	0.0	0	0	?	S	Feb23	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	I<	Feb23	0:00	[rcu_gp]
root	4	0.0	0.0	0	0	?	I<	Feb23	0:00	[rcu_par_gp]
root	5	0.0	0.0	0	0	?	I<	Feb23	0:00	[slub_flushwq]
root	6	0.0	0.0	0	0	?	I<	Feb23	0:00	[netns]
root	8	0.0	0.0	0	0	?	I<	Feb23	0:00	[kworker/0:0H-events_hi]
root	10	0.0	0.0	0	0	?	I<	Feb23	0:00	[mm_percpu_wq]
root	11	0.0	0.0	0	0	?	I	Feb23	0:00	[rcu_tasks_kthread]
root	12	0.0	0.0	0	0	?	I	Feb23	0:00	[rcu_tasks_rude_kthread]
root	13	0.0	0.0	0	0	?	I	Feb23	0:00	[rcu_tasks_trace_kthrea]
root	14	0.0	0.0	0	0	?	S	Feb23	0:04	[ksoftirqd/0]
root	15	0.2	0.0	0	0	?	I	Feb23	1:56	[rcu_preempt]
root	16	0.0	0.0	0	0	?	S	Feb23	0:01	[migration/0]
root	18	0.0	0.0	0	0	?	S	Feb23	0:00	[cpuhp/0]
root	19	0.0	0.0	0	0	?	S	Feb23	0:00	[cpuhp/1]
root	20	0.0	0.0	0	0	?	S	Feb23	0:01	[migration/1]
root	21	0.0	0.0	0	0	?	S	Feb23	0:04	[ksoftirqd/1]
root	23	0.0	0.0	0	0	?	I<	Feb23	0:00	[kworker/1:0H-events_hi]
root	24	0.0	0.0	0	0	?	S	Feb23	0:00	[cpuhp/2]
root	25	0.0	0.0	0	0	?	S	Feb23	0:01	[migration/2]
root	26	0.0	0.0	0	0	?	S	Feb23	0:28	[ksoftirqd/2]
root	28	0.0	0.0	0	0	?	I<	Feb23	0:00	[kworker/2:0H-events_hi]
root	29	0.0	0.0	0	0	?	S	Feb23	0:00	[cpuhp/3]
root	30	0.0	0.0	0	0	?	S	Feb23	0:01	[migration/3]
root	31	0.0	0.0	0	0	?	S	Feb23	0:03	[ksoftirqd/3]
root	33	0.0	0.0	0	0	?	I<	Feb23	0:00	[kworker/3:0H-events_hi]

`ps aux` komutu ile tüm işlemlerin detaylı bir listesini görüyoruz.

`uptime` komutu sistemin çalışma süresi hakkında bilgiler verir.

```
(root@kali)-[~]
# uptime
09:40:19 up 13:24, 6 users, load average: 0.03, 0.03, 0.00

(root@kali)-[~]
# uptime -s
2023-02-23 20:15:54

(root@kali)-[~]
# uptime -p
up 13 hours, 24 minutes
```

Sistemde 6 adet kullanıcı varmış, 23 şubat 20.15te sistem açılmış yani 13 saat 24 dakikadır açıktır.

top komutu Linux sistemlerde işlemlerin gerçek zamanlı izlenmesini sağlar. htop , top 'un geliştirilmiş bir türüdür. Aşağıda htop ekran görüntüsü yer almaktadır.

```
root@kali: ~  
File Actions Edit View Help  
0[ ] mem 2.0% Tasks: 102, 157 thr, 122 kthr; 1 running  
1[ ] 2.0% Load average: 0.53 0.31 0.11  
2[ ] 1.4% Uptime: 13:29:43  
3[ ] 1.3%  
Mem[ ] 1.04G/7.76G  
Swp[ ] 2.12M/1024M  
Main I/O  
PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command  
364804 kali 20 0 430M 104M 85340 S 0.0 1.3 0:02.65 /usr/bin/qterminal  
1 root 20 0 172M 13500 9036 S 0.0 0.2 0:31.55 /sbin/init splash  
403 root 20 0 49560 19320 17968 S 0.0 0.2 0:28.20 /lib/systemd/systemd-journal  
423 root 20 0 221M 2292 16 S 0.0 0.0 0:00.11 vmware-vmblock-fuse /run/vmtoolsd  
424 root 20 0 221M 2292 16 S 0.0 0.0 0:00.08 vmware-vmblock-fuse /run/vmtoolsd  
425 root 20 0 221M 2292 16 S 0.0 0.0 0:00.02 vmware-vmblock-fuse /run/vmtoolsd  
437 root 20 0 27092 7292 4508 S 0.0 0.1 0:05.82 /lib/systemd/systemd-udevd  
505 root 20 0 8260 6416 1760 S 0.0 0.1 0:16.62 /usr/sbin/haveged --For  
566 messagebus 20 0 10728 5636 3844 S 0.0 0.1 0:08.33 /usr/bin/dbus-daemon --system  
592 root 20 0 33608 8340 7104 S 0.0 0.1 0:02.77 /lib/systemd/systemd-logd  
600 root 20 0 6608 2600 2344 S 0.0 0.0 0:00.21 /usr/sbin/cron -f  
724 root 20 0 235M 10928 7212 S 0.0 0.1 0:06.57 /usr/bin/vmtoolsd  
725 root 20 0 235M 10928 7212 S 0.0 0.1 0:00.00 /usr/bin/vmtoolsd  
879 root 20 0 301M 6316 5500 S 0.0 0.1 0:00.96 /usr/sbin/lightdm  
918 root 20 0 301M 6316 5500 S 0.0 0.1 0:00.01 /usr/sbin/lightdm  
921 root 20 0 301M 6316 5500 S 0.0 0.1 0:00.18 /usr/sbin/lightdm  
934 root 20 0 5872 1064 976 S 0.0 0.0 0:00.00 /sbin/agetty -o -p -- \n  
1034 rtkit 21 1 22684 1460 1224 S 0.0 0.0 0:02.59 /usr/libexec/rtkit-daemon  
1035 rtkit 20 0 22684 1460 1224 S 0.0 0.0 0:01.11 /usr/libexec/rtkit-daemon  
1036 rtkit RT 1 22684 1460 1224 S 0.0 0.0 0:00.90 /usr/libexec/rtkit-daemon  
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice -F8Nice +F9Kill F10Quit
```


Uçucu Olmayan Veriler

Kalıcı olan; sistem bilgisi, dosya, dizin, log, çekirdek bilgisi gibi veriler uçucu olmayan veriler kategorisinde yer alır.

Sistem Bilgileri

`cat /proc/cpuinfo` komutu ile sistem hakkındaki temel bilgilerin tümüne ulaşabiliriz. Bağlantı noktaları ve harici aygıtların bilgilerini görmek için ise : `cat /proc/self/mounts`

```
(root@kali)~[~]
# cat /proc/cpuinfo
processor       : 0
vendor_id      : GenuineIntel
cpu family     : 6
model          : 94
model name     : Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz
stepping       : 3
microcode      : 0xffffffff
cpu MHz        : 2591.998
cache size     : 6144 KB
physical id    : 0
siblings       : 2
core id        : 0
cpu cores      : 2
apicid         : 0
initial apicid : 0
fpu            : yes
fpu_exception  : yes
cpuid level    : 22
wp             : yes
flags          : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36
                clflush mmx fxsr sse sse2 ss ht syscall nx rdtscp lm constant_tsc arch_perfmon nopl tsc_re
                liable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 sse4_1 sse4_2 movbe p
                opcnt aes xsave avx hypervisor lahf_lm 3dnowprefetch pti arat
bugs           : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb
                b_multihit mmio_stale_data retbleed
bogomips       : 5183.99
clflush size   : 64
cache_alignme  : 64
```

Çekirdek Bilgileri

Linux sisteminin temel bileşenlerinden biri olan çekirdek hakkında bilgi edinmek için `uname -r` komutunu kullanabiliriz. Bunun haricinde `cat /proc/version` veya `hostnamectl | grep Kernel` komutlarını da kullanabiliriz.

```
(root@kali)~[~]
# uname -r
6.0.0-kali5-amd64

(root@kali)~[~]
# cat /proc/version
Linux version 6.0.0-kali5-amd64 (devel@kali.org) (gcc-12 (Debian 12.2.0-9) 12.2.0, GNU ld
(GNU Binutils for Debian) 2.39) #1 SMP PREEMPT_DYNAMIC Debian 6.0.10-2kali1 (2022-12-06)
```

Kullanıcı Hesabı Bilgileri

Yerel kullanıcıların bilgileri /etc/passwd dosyasında bulunur, her bir satır bir kullanıcıyı belirtir. Yalnızca kullanıcı adlarını listelemek için `cut -d: -f1 /etc/passwd` komutu kullanılabilir.

```
(root@kali)-[~]
# 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
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
tss:x:101:109:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:103:110::/nonexistent:/usr/sbin/nologin
usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
```

Geçmiş Bilgileri

`w` komutu sistemdeki kullanıcıların ne kadar süre önce sisteme giriş yaptıklarını gösterir. Bir diğer kullanım şekli de `who` 'dur. `last` ise daha detaylı bir şekilde kullanıcıların geçmişlerini gösterir.

```
(root@kali)-[~]
# w
10:06:19 up 13:50,  6 users,  load average: 0.13, 0.07, 0.05
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
kali      tty7      :0               Sun09    5days 49:16  9.96s  xfce4-session
kali      pts/1     -                Thu06    2:07m  5.98s  0.47s  sudo su
kali      pts/3     -                Sun09    0.00s  0.00s  0.12s  sudo su
kali      pts/5     -                07:12    1.00s  7.94s  0.89s  sudo su
kali      pts/7     -                07:29    2:34m  0.38s  0.14s  sudo su
kali      pts/9     -                Wed10    0.00s  0.00s  0.13s  sudo su
```

```

(root@kali)-[~]
# last -f /var/log/wtmp
kali      tty7      :0      Sun Feb 19 09:06      gone - no logout
reboot    system boot  6.0.0-kali5-amd6 Sun Feb 19 09:04      still running
kali      tty7      :0      Wed Feb 15 11:02      - crash (3+22:01)
reboot    system boot  6.0.0-kali5-amd6 Wed Feb 15 11:02      still running
reboot    system boot  6.0.0-kali5-amd6 Wed Feb 15 11:00      still running
kali      tty7      :0      Wed Feb 15 10:10      - crash (00:50)
reboot    system boot  6.0.0-kali5-amd6 Wed Feb 15 10:09      still running
kali      tty7      :0      Wed Feb 15 08:39      - crash (01:29)
reboot    system boot  6.0.0-kali5-amd6 Tue Feb 14 06:05      still running
kali      tty7      :0      Mon Feb 13 08:25      - crash (21:40)
reboot    system boot  6.0.0-kali5-amd6 Mon Feb 13 08:24      still running
kali      tty1      :0      Mon Feb 13 08:22      - crash (00:02)
reboot    system boot  6.0.0-kali5-amd6 Mon Feb 13 08:21      still running
kali      tty7      :0      Mon Feb 13 08:01      - crash (00:20)
reboot    system boot  6.0.0-kali5-amd6 Mon Feb 13 07:58      still running
kali      tty7      :0      Wed Feb 1 11:04      - crash (11+20:53)
reboot    system boot  6.0.0-kali5-amd6 Wed Feb 1 11:02      still running
kali      tty7      :0      Sat Jan 28 14:54      - crash (3+20:08)
reboot    system boot  6.0.0-kali5-amd6 Sat Jan 28 14:53      still running
kali      tty7      :0      Thu Jan 26 14:07      - 05:28 (1+15:20)
reboot    system boot  6.0.0-kali5-amd6 Thu Jan 26 14:05      still running
kali      tty7      :0      Tue Jan 24 14:50      - 07:47 (16:57)
reboot    system boot  6.0.0-kali5-amd6 Tue Jan 24 14:49      still running
kali      tty7      :0      Sun Dec 25 03:08      - crash (30+11:41)
reboot    system boot  6.0.0-kali5-amd6 Sun Dec 25 03:07      still running

```

Linux Logs (Günlük Verileri)

Bilgisayardaki olay ve hata mesajlarının kaydedildiği belgelere log adı verilmektedir. Log dosyaları sistem ve uygulamalar tarafından oluşturulur. Log dosyalarında olayın türü, açıklaması, tarihi, saati ve hata mesajı gibi bilgiler yer alır. Sistemin çalışma durumunu anlamamızı sağlayacak olan bilgiler log dosyalarında yer alır. Bir hata alıyorsanız ancak sebebini bilmiyorsanız da log belgelerinden hata hakkında bilgi edinebilirsiniz.

Log dosyaları genellikle “/var/log” dizininde bulunur. Uygulama log dosyaları ise uygulamanın kurulu olduğu dizinde bulunur. cd komutu ile geçerli konuma gidebiliriz. ls komutu ile içeriğini görebiliriz.

```

(root@kali)-[~]
# cd /var/log

(root@kali)-[/var/log]
# ls
alternatives.log  mosquitto      vmware-network.1.log
apache2           mysql          vmware-network.2.log
apt              nginx          vmware-network.log
boot.log          notus-scanner  vmware-vmtoolsd-root.1.log
btmtp            openvpn        vmware-vmtoolsd-root.2.log
dpkg.log          postgresql     vmware-vmtoolsd-root.3.log
faillog          private        vmware-vmtoolsd-root.log
fontconfig.log   README        wtmp
gvm              redis          Xorg.0.log
inetsim          runit          Xorg.0.log.old
journal          samba          Xorg.1.log
lastlog          speech-dispatcher
lightdm          stunnel4      Xorg.1.log.old
macchanger.log   sysstat

```

Linux sistemlerindeki bazı log dosyaları ve içerikleri:

- `/var/log/messages`: Bu dosya, sistem tarafından oluşturulan genel log mesajlarını içerir. Örneğin, sistem başlangıç ve kapanış süreçleri, hata mesajları ve diğer olaylar bu dosyada saklanır.
- `/var/log/syslog`: Bu dosya, sistem ve uygulamalar tarafından oluşturulan log mesajlarını içerir. Örneğin, servislerin çalışma durumu, hata mesajları ve diğer olaylar bu dosyada saklanır.
- `/var/log/auth.log`: Bu dosya, sisteme giriş çıkış olaylarını ve yetkilendirme ile ilgili log mesajlarını içerir. Örneğin, kullanıcı girişleri ve parola hataları bu dosyada saklanır.
- `/var/log/kern.log`: Bu dosya, sistem kernel'ı tarafından oluşturulan log mesajlarını içerir. Örneğin, sistem aygıtlarının yüklenme ve çalışma durumu bu dosyada saklanır.
- `/var/log/dmesg`: Bu dosya, sistem çekirdeği tarafından oluşturulan log mesajlarını içerir. Örneğin, sistem aygıtlarının yüklenme ve çalışma durumu bu dosyada saklanır.
- `/var/log/boot.log`: Bu dosya, sistem başlangıç süreci ile ilgili log mesajlarını içerir. Örneğin, sistem aygıtlarının yüklenme sırası ve hata mesajları bu dosyada saklanır.
- `/var/log/cron`: Bu dosya, zamanlanmış görevler ile ilgili log mesajlarını içerir. Örneğin, cron servisinde oluşan bir hata veya başlatılma işlemleri bu dosyada saklanır.
- `/var/log/yum.log`: Bu dosya, yum komut günlüklerini içerir. Yum paket yöneticisi ile yüklenen yazılımlar burada yer alır.
- `/var/log/maillog`: Bu dosya, Posta sunucusu günlüklerini içerir. Sistemdeki kullanıcılara gelen ve giden maillerin header bilgileri burada yer alır.
- `/var/log/dpkg.log`: Bu dosya, dpkg günlüklerini içerir. Dpkg paket yöneticisi ile yüklenen yazılımlar burada yer alır.
- `/var/log/faillog`: Bu dosya başarısız kullanıcı oturum açma denemelerini gösterir.

Bu dosyaları incelemek için `cat` , `nano` veya `vi` komutları kullanılabilir.

nano boot.log komutu ile boot.log dosyasının içeriğine giriyorum. Örneğin burada sistemin başlatma süresinin 1dakika 39saniye olduğunu gözüküyor.

```
root@kali: /var/log
File Actions Edit View Help
GNU nano 7.1 boot.log
Thu Dec 22 03:59:15 EST 2022
root: clean, 445447/5251072 files, 3912518/20995837 blocks
[[0;32m OK [[0m Finished [[0;1;39mLoad/Save Random Seed[[0m.
[[0;32m OK [[0m Finished [[0;1;39mCreate Volatile Files and Directories[[0m.
[[0;32m OK [[0m Started [[0;1;39mEntropy Daemon based on the HAVEGE algorithm[[0m.
Starting [[0;1;39mService for virtual machines hosted on VMware[[0m...
Starting [[0;1;39mRecord System Boot/Shutdown in UTMP[[0m...
[[0;32m OK [[0m Started [[0;1;39mRule-based Manager for Device Events and Files[[0m.
[[0;32m OK [[0m Started [[0;1;39mService for virtual machines hosted on VMware[[0m.
[[0;32m OK [[0m Finished [[0;1;39mRecord System Boot/Shutdown in UTMP[[0m.
Starting [[0;1;39mShow Plymouth Boot Screen[[0m...
Mounting [[0;1;39mArbitrary Executable File Formats File System[[0m...
Mounting [[0;1;39mRPC Pipe File System[[0m...
[[0;32m OK [[0m Started [[0;1;39mShow Plymouth Boot Screen[[0m.
[[0;32m OK [[0m Started [[0;1;39mForward Password Requests to Plymouth Directory Watch[[0m.
[[0;32m OK [[0m Reached target [[0;1;39mLocal Encrypted Volumes[[0m.
[[0;32m OK [[0m Reached target [[0;1;39mPath Units[[0m.
[[0;32m OK [[0m Mounted [[0;1;39mArbitrary Executable File Formats File System[[0m.
[[0;32m OK [[0m Finished [[0;1;39mSet Up Additional Binary Formats[[0m.
[[0;32m OK [[0m Reached target [[0;1;39mSystem Initialization[[0m.
[[0;32m OK [[0m Started [[0;1;39mDaily apt download activities[[0m.
[[0;32m OK [[0m Started [[0;1;39mDaily apt upgrade and clean activities[[0m.
[[0;32m OK [[0m Started [[0;1;39mDaily dpkg database backup timer[[0m.
[[0;32m OK [[0m Started [[0;1;39mPeriodic ext4 Online Metadata Check for All Filesystems[[0m.
[[0;32m OK [[0m Started [[0;1;39mDiscard unused blocks once a week[[0m.
[[0;32m OK [[0m Started [[0;1;39mDaily rotation of log files[[0m.
[[0;32m OK [[0m Started [[0;1;39mDaily man-db regeneration[[0m.
[[0;32m OK [[0m Started [[0;1;39mRotate ntpd stats daily[[0m.
[[0;32m OK [[0m Started [[0;1;39mClean PHP session files every 30 mins[[0m.
[[0;32m OK [[0m Started [[0;1;39mUpdate the plocate database daily[[0m.
[[0;32m OK [[0m Started [[0;1;39mDaily Cleanup of Temporary Directories[[0m.
^G Help ^O 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
```

Apt indirmelerinin, dpkg veritabanı yedeklemesinin ve geçici dizin temizlemesinin başlatıldığını gözüküyor. Bu olayların tümü 22 aralık 2022’de saat3:59da gerçekleşmiş. “Ctrl+X” ile buradan çıkış yapabiliriz.

cat komutunun yardımı ile dpkg.log dosyasının içeriğini görebiliriz.

```
(root@kali)~[~] Edit View Help
# cat /var/log/dpkg.log
2023-02-01 11:06:23 startup archives unpack
2023-02-01 11:06:35 upgrade python3-pytest:all 7.1.2-4 7.2.1-1
2023-02-01 11:06:35 status half-configured python3-pytest:all 7.1.2-4
2023-02-01 11:06:36 status unpacked python3-pytest:all 7.1.2-4
2023-02-01 11:06:36 status half-installed python3-pytest:all 7.1.2-4
2023-02-01 11:06:36 status triggers-pending kali-menu:all 2022.4.1
2023-02-01 11:06:36 status triggers-pending man-db:amd64 2.11.2-1
2023-02-01 11:06:36 status unpacked python3-pytest:all 7.2.1-1
2023-02-01 11:06:36 startup packages configure
2023-02-01 11:06:36 configure python3-pytest:all 7.2.1-1 <none>
2023-02-01 11:06:36 status unpacked python3-pytest:all 7.2.1-1
2023-02-01 11:06:36 status half-configured python3-pytest:all 7.2.1-1
2023-02-01 11:06:37 status installed python3-pytest:all 7.2.1-1
2023-02-01 11:06:37 trigproc kali-menu:all 2022.4.1 <none>
2023-02-01 11:06:37 status half-configured kali-menu:all 2022.4.1
2023-02-01 11:06:38 status installed kali-menu:all 2022.4.1
2023-02-01 11:06:38 trigproc man-db:amd64 2.11.2-1 <none>
2023-02-01 11:06:38 status half-configured man-db:amd64 2.11.2-1
2023-02-01 11:06:44 status installed man-db:amd64 2.11.2-1
2023-02-13 07:43:40 startup archives unpack
2023-02-13 07:43:41 upgrade diffutils:amd64 1:3.8-3 1:3.8-4
2023-02-13 07:43:41 status half-configured diffutils:amd64 1:3.8-3
2023-02-13 07:43:41 status unpacked diffutils:amd64 1:3.8-3
2023-02-13 07:43:41 status half-installed diffutils:amd64 1:3.8-3
2023-02-13 07:43:42 status triggers-pending kali-menu:all 2022.4.1
2023-02-13 07:43:42 status triggers-pending man-db:amd64 2.11.2-1
2023-02-13 07:43:42 status unpacked diffutils:amd64 1:3.8-4
2023-02-13 07:43:43 startup packages configure
2023-02-13 07:43:43 configure diffutils:amd64 1:3.8-4 <none>
2023-02-13 07:43:43 status unpacked diffutils:amd64 1:3.8-4
2023-02-13 07:43:43 status half-configured diffutils:amd64 1:3.8-4
2023-02-13 07:43:43 status installed diffutils:amd64 1:3.8-4
2023-02-13 07:43:43 startup archives unpack
2023-02-13 07:43:43 upgrade dpkg:amd64 1.21.17+kali1 1.21.19+kali1
2023-02-13 07:43:43 status half-configured dpkg:amd64 1.21.17+kali1
```

Eğer log dosyası çok büyükse veya çok fazla mesaj içeriyorsa, arama özelliğini kullanarak belirli bir olayı veya hata mesajını bulmaya çalışabilirsiniz. Bu sayede, log dosyasını daha rahat inceleyebilirsiniz. Grep bir arama aracıdır, uzun metinlerde kelime arama yapma imkanı sunar. Grep aracı ile arama yapmak için “-E” parametresi kullanılır. Grep aracı yüklü değil ise `apt-get install grep` komutu ile indirebilirsiniz.

```
root@kali: /var/log
File Actions Edit View Help

(root@kali)-[/var/log]
# apt-get install grep
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
grep is already the newest version (3.8-3).
The following packages were automatically installed and are no longer required:
  catfish docutils-common gir1.2-xfconf-0 python3-alabaster python3-docutils python3-imagesize python3-roman
  python3-snowballstemmer python3-sphinx sphinx-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 15 not upgraded.

(root@kali)-[/var/log]
# grep -E "installed" dpkg.log
2022-12-18 01:02:46 status half-installed base-passwd:amd64 3.6.1
2022-12-18 01:02:46 status installed base-passwd:amd64 3.6.1
2022-12-18 01:02:46 status half-installed base-files:amd64 1:2022.4.0
2022-12-18 01:02:46 status installed base-files:amd64 1:2022.4.0
2022-12-18 01:02:46 status half-installed dpkg 1.21.9kali1
2022-12-18 01:02:47 status installed dpkg:amd64 1.21.9kali1
2022-12-18 01:02:47 status half-installed libc6:amd64 2.36-4
2022-12-18 01:02:47 status installed libc6:amd64 2.36-4
2022-12-18 01:02:47 status half-installed perl-base:amd64 5.36.0-4
2022-12-18 01:02:47 status installed perl-base:amd64 5.36.0-4
2022-12-18 01:02:47 status half-installed mawk:amd64 1.3.4.20200120-3.1
2022-12-18 01:02:47 status installed mawk:amd64 1.3.4.20200120-3.1
2022-12-18 01:02:47 status half-installed debconf:all 1.5.80
2022-12-18 01:02:47 status installed debconf:all 1.5.80
2022-12-18 01:02:47 status half-installed apt:amd64 2.5.4
2022-12-18 01:02:48 status half-installed base-files:amd64 1:2022.4.0
2022-12-18 01:02:48 status half-installed base-passwd:amd64 3.6.1
2022-12-18 01:02:48 status half-installed bash:amd64 5.2-2+b1
2022-12-18 01:02:48 status half-installed bsdutils:amd64 1:2.38.1-1.1+b1
2022-12-18 01:02:48 status half-installed coreutils:amd64 9.1-1
```

“installed” kelimesini filtreleyerek sadece belirli log kayıtlarının gözükmesini sağladım.