PurpleBox

Linux Forensic 101

www.prplbx.com

$whoami

Ömer Faruk Çulha

PurpleBox -> Cyber Security Engineer

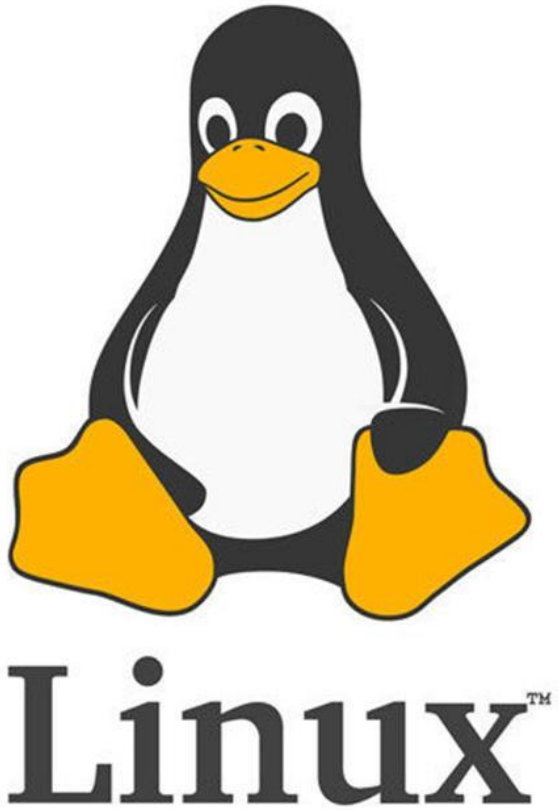
Sakarya Üniversitesi -> Makine Müh.

https://twitter.com/0x1337root

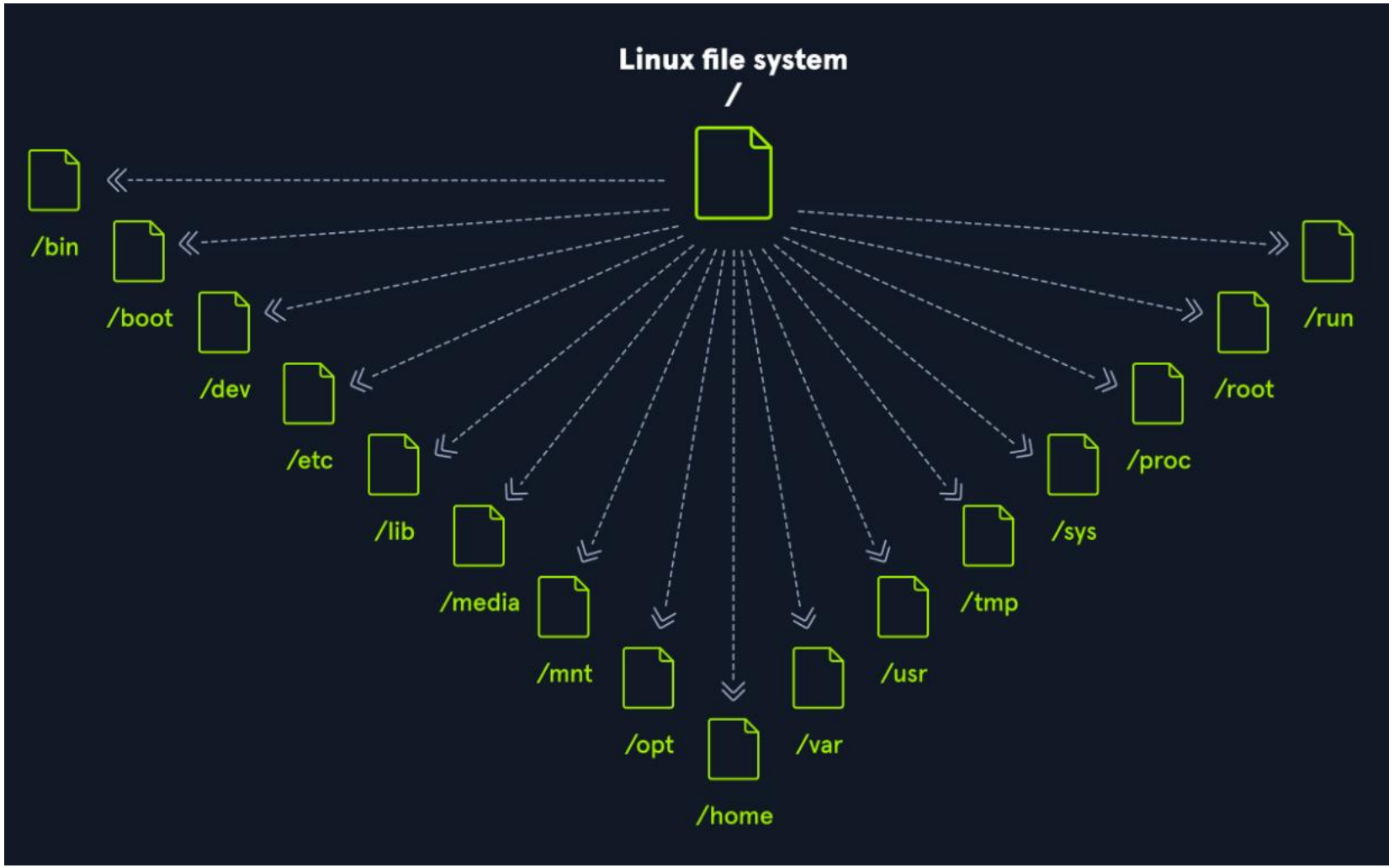
https://tryhackme.com/p/0x1337root

https://www.linkedin.com/in/ömer-faruk-çulha-b95880195

Linux Nedir ?



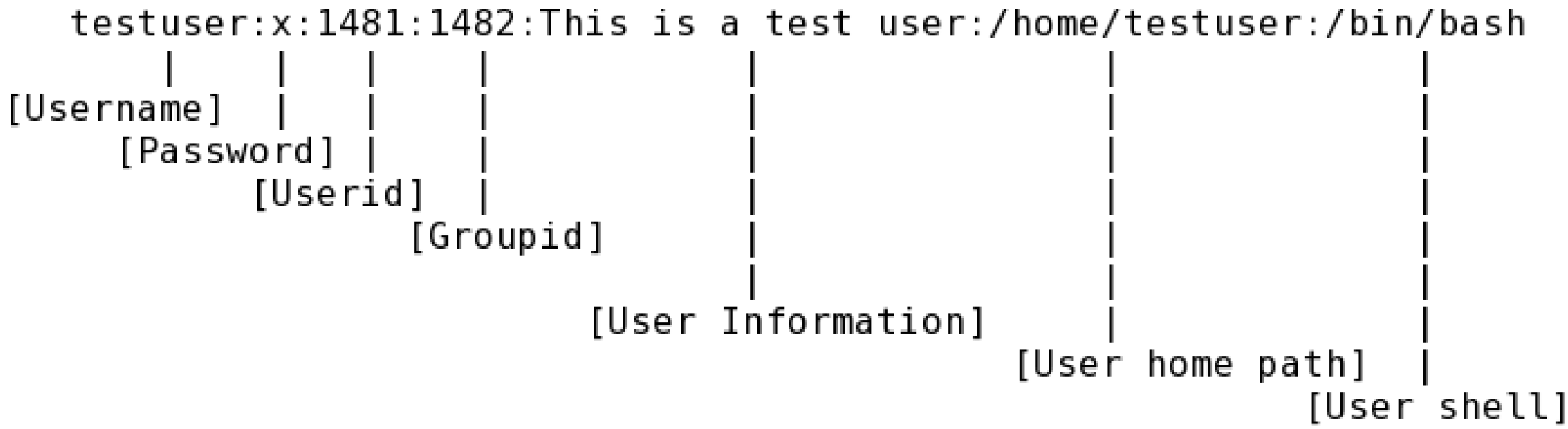
Linux Dosya Sistemi



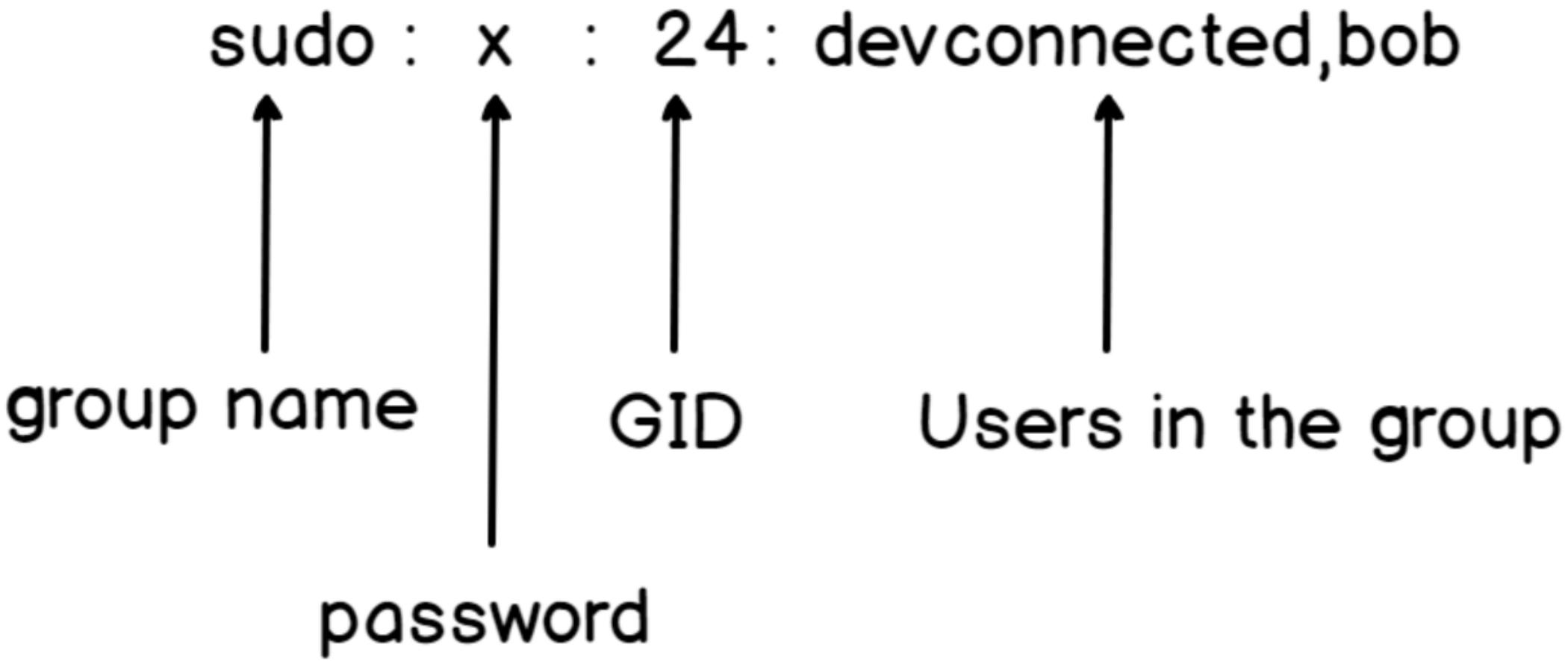
Linux Dosya Sistemi

- /
- /bin
- /boot
- /dev
- /etc
- /home
- /lib
- /media
- /mnt
- /opt
- /proc
- /root
- /run
- /sbin
- /tmp
- /usr
- /var
- /sys

Linux Kullanıcı ve Grup Analizi



Linux Kullanıcı ve Grup Analizi



Linux RAM Analizi

Linux Disk Analizi

/proc

- Bellekte yer kaplamaz
- Sanal bir dizindir
- Bilgisayar hakkında bilgiler içerir (CPU, Linux Kernel v.b.)
- Çalışan processlerin dosyaları burada bulunur.
- Dosyalar ve dizinler bilgisayar başladığında veya sistem çalışırken ve işler değiştikçe anında oluşturulur/silinir.
- cwd, exe ve root processin dizinleri hakkında bilgiler içerir.

Linux Sistem Yapısı ve Kanıtlar

- Tarih - zaman bilgisi
- İşletim sistemi ve versiyon bilgisi
- Ağ arayüzü
- İnternet bağlantıları
- Açık portlar
- Çalışan işlemler
- Bağlanan cihazlar

Tarih - Zaman Bilgisi

```
┌──(root㉿kali)-[~]
└─# date
Sun May 22 12:53:56 PM EDT 2022
```

İşletim Sistemi ve Versiyon Bilgisi

```
┌──(root㉿kali)-[~]
└─# uname -a
Linux kali 5.16.0-kali7-amd64 #1 SMP PREEMPT Debian 5.16.18-1kali1 (2022-04-01) x86_64 GNU/Linux
```

Ağ Arayüz Bilgisi

```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.112  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fedb:966a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:db:96:6a  txqueuelen 1000  (Ethernet)
        RX packets 2625  bytes 574194 (560.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1514  bytes 183722 (179.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ağ Bağlantı Bilgisi

```
┌──(root㉿kali)-[~]
└─# netstat tulpn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.1.112:49944     ec2-52-33-84-190.:https ESTABLISHED
tcp        0      0 192.168.1.112:58558     server-52-84-119-:https ESTABLISHED
tcp        0      0 192.168.1.112:47962     93.184.220.29:http      ESTABLISHED
tcp        0      0 192.168.1.112:58554     server-52-84-119-:https TIME_WAIT
tcp        0      0 192.168.1.112:58556     server-52-84-119-:https ESTABLISHED
udp        0      0 192.168.1.112:bootpc    192.168.1.1:bootps      ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         DGRAM      CONNECTED     12586    /run/systemd/notify
unix  2      [ ]         DGRAM                    12602    /run/systemd/journal/syslog
unix  14     [ ]         DGRAM      CONNECTED     12608    /run/systemd/journal/dev-log
unix  6      [ ]         DGRAM      CONNECTED     12610    /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    15879    /run/user/1000/systemd/notify
unix  3      [ ]         STREAM     CONNECTED     18672
unix  3      [ ]         STREAM     CONNECTED     16800    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     18228
unix  3      [ ]         STREAM     CONNECTED     18068    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     17580
unix  3      [ ]         STREAM     CONNECTED     41864
unix  3      [ ]         STREAM     CONNECTED     16668
unix  3      [ ]         STREAM     CONNECTED     17528
unix  3      [ ]         STREAM     CONNECTED     16096    @/tmp/.X11-unix/X0
```

İncelenmesi Gereken Önemli Dizinler

KANIT	AÇIKLAMA
/etc/localtime /usr/share/zoneinfo	Time Zone bilgisi elde edilir.
/etc/passwd	Temel kullanıcı bilgileri elde edilir.
/etc/shadow	Parola hashleri elde edilir.
/etc/sudoers	Admin yetkisine sahip kullanıcıların listesi.

İncelenmesi Gereken Önemli Dizinler

KANIT	AÇIKLAMA
/etc/hostname	Bilgisayar adı.
/etc/cron/* /var/spool/cron/*	Zamanlanmış görevler görüntülenir.
/etc/inittab /etc/init.d /etc/rc.d /etc/init.conf	Hizmet başlangıç komut dosyaları incelenebilir.

İncelenmesi Gereken Önemli Dizinler

KANIT	AÇIKLAMA
/etc/hosts	Statik IP atamaları bilgisi.
/var/lib/dhclient	DHCP ile atanmış IP adresi bilgisi.
/var/log/*	Çeşitli log kayıtları.
$home/.ssh	Uzaktan sağlanmış erişimler hakkında bilgiler.
$home/.bash_history	Komut geçmişi elde edilir.
$home/.recent-used.xbel	Son görüntülenen dosyalar elde edilir.

Linux Log Analizi

KANIT	AÇIKLAMA
/var/log/messages	Sistem başlangıcı gibi global sistem logları tutulur.
/var/log/lastlog	Son kullanıcı girişlerini ve zaman bilgisini içerir.
/var/log/cron	Zamanlanmış görevlere ait loglar.
/var/log/secure	Kimlik doğrulama, yetkiler ve güvenlik ile alakalı loglar.
/var/log/dmesg	Sistem boot edildikten sonra aygıtlar ile ilgili tüm mesajların logları.
/var/log/maillog	Sistem üzerinde çalışan mail sunucusuna ait loglar.
/var/log/cups	Sistemdeki tüm yazıcı ve bu yazıcılardan alınmış çıktıların logları.

Linux Log Analizi

KANIT	AÇIKLAMA
/var/log/dpkg.log	Yüklenen, güncellenen, silinen tüm paketlerin logları.
/var/log/kern.log	Kernel logları.
/var/log/daemon.log	Aktif, durmuş, başarısız tüm daemonlara ait logları içerir.
/var/log/boot.log	Sistem boot sürecine ait tüm loglar.
/var/log/user.log	Kullanıcı seviyesine ait loglar.
/var/log/auth.log	Sisteme yapılan giriş denemelerine ait loglar.
/var/log/syslog	İşletim sistemine ait hata ve uyarı logları.
/var/log/wtmp	Hangi tarihte, hangi kullanıcı tarafından başarılı giriş yapıldığını içeren log dosyası.
/var/log/btmp	En son hangi tarihte, hangi kullanıcı tarafından başarısız giriş denemesini içeren log dosyası.

Linux Browser Analizi

BROWSER	AÇIKLAMA
firefox	$home/.mozilla/firefox/*.default
chrome	$home/.config/chromium/Default

Linux Resim Metadata Analizi

```
ExifTool Version Number         : 12.41
File Name                       : index.jpeg
Directory                       : /root/Downloads
File Size                       : 6.7 KiB
File Modification Date/Time     : 2022:05:22 19:11:10+00:00
File Access Date/Time           : 2022:05:22 19:11:10+00:00
File Inode Change Date/Time     : 2022:05:22 19:11:10+00:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
```

```
X Resolution                    : 1
Y Resolution                    : 1
Resolution Unit                 : None
Artist                          : F0R3N51C_M45T3R
Y Cb Cr Positioning             : Centered
Image Width                     : 194
Image Height                    : 259
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 194x259
Megapixels                      : 0.050
```

Referanslar

- https://academy.hackthebox.com/module/details/18
- https://nostarch.com/practical-linux-forensics

Thank you!
Any Questions?