

EXP 7 –

```
git clone https://github.com/foospidy/DBPwAudit.git
cd DBPwAudit
pip3 install -r requirements.txt
python3 dbpwaudit.py -h
sudo service mysql start
sudo mysql -u root
CREATE USER 'testuser'@'localhost' IDENTIFIED BY '1234';
GRANT ALL PRIVILEGES ON *.* TO 'testuser'@'localhost';
FLUSH PRIVILEGES;
exit;
cd ~/DBPwAudit
nano weakpass.txt
1234
12345
admin
password
root
test123
123456
test
qwerty
abc123
python3 dbpwaudit.py -t mysql -U testuser -H localhost -w weakpass.txt
hydra -l testuser -P weakpass.txt mysql://localhost
```

EXP 8 –

```
sudo apt update
sudo apt install apache2 php mysql-server john
sudo apt install php php-mysqli php-gd
git clone https://github.com/digininja/DVWA.git
sudo mv DVWA /var/www/html/dvwa
sudo chmod -R 777 /var/www/html/dvwa
sudo service mysql start
sudo mysql -u root -e "create database dvwa;"
sudo nano /var/www/html/dvwa/config/config.inc.php
db_user = 'root'
db_password = ''
db_database = 'dvwa'
sudo service apache2 start
http://localhost/dvwa
```

INJECT: 1' OR '1'='1

nano hashes.txt

admin:5f4dcc3b5aa765d61d8327deb882cf99

john hashes.txt

john --show hashes.txt

EXP 1 –

Ip a

Ip r

Ip addr show

Ip route show

Ss -tuln

Nmcli device show

Hostname -l

PING GOOGLE.COM

Ip neigh

Traceroute google.com

EXP 2 –

nmap 192.168.1.10

nmap 192.168.1.1-50

nmap 192.168.1.10/24

nmap -sn 192.168.1.0/24

nmap -F 192.168.1.10

nmap -sV 192.168.1.10

nmap -O 192.168.1.10

nmap -p 80,443,22 192.168.1.10

nmap -A 192.168.1.10

nmap -sC 192.168.1.10

EXP 3 –

Ip.addr == 192.168.1.10

Tcp.port == 443 || tls

Tcp.stream eq 5

http.request.method == "POST"

tcp.flags.syn == 1 && tcp.flags.ack == 0

frame contains "password"

dns

host 192.168.1.10

tls.handshake.type == 1