You could Use these sites for testing in some pracs :
https://scratchpads.org/explore/sites-list

Note: Turn off your Laptop's Security Settings
Practical 1 : Use Google and Whois for Reconnaissance

What is Who.is a website?
WHOIS is a query and response protocol widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system.

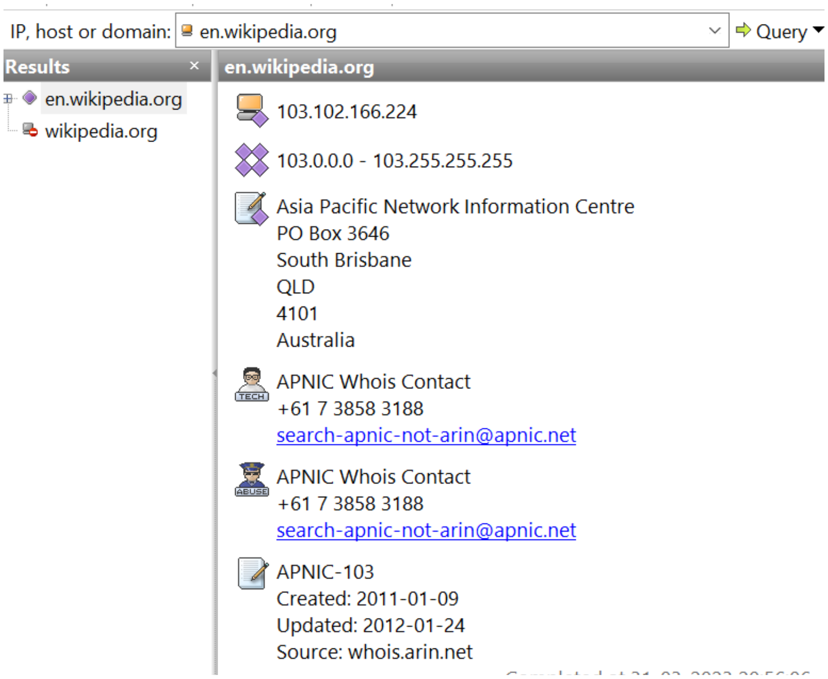
This practice uses the "Who.is" website to search any other target site to get information such as identifying who owns a domain and how to contact them.

But we will be doing it on the application/software that is smart who is

Download link :
https://en.softonic.com/download/smartwhois/windows/post-download?ex=DINS-635.3

Install the software and then open it, just enter the website you want the information about which is available on google CURRENTLY will be displayed

For Example, Open Wikipedia > English > Copy URL > Paste it in Smart Who is Tab and hit Enter



IP, host or domain: en.wikipedia.org

103.102.166.224

103.0.0.0 - 103.255.255.255

Asia Pacific Network Information Centre
PO Box 3646
South Brisbane
QLD
4101
Australia

APNIC Whois Contact
+61 7 3858 3188
search-apnic-not-arin@apnic.net

APNIC Whois Contact
+61 7 3858 3188
search-apnic-not-arin@apnic.net

APNIC-103
Created: 2011-01-09
Updated: 2012-01-24
Source: whois.arin.net

.

Practical 2: (a) Use CrypTool to encrypt and decrypt passwords using RC4 algorithm

In this practical we are signifying the use of CrypTool and RC4 algorithm for encryption and decryption , thus knowledge for both is essential.

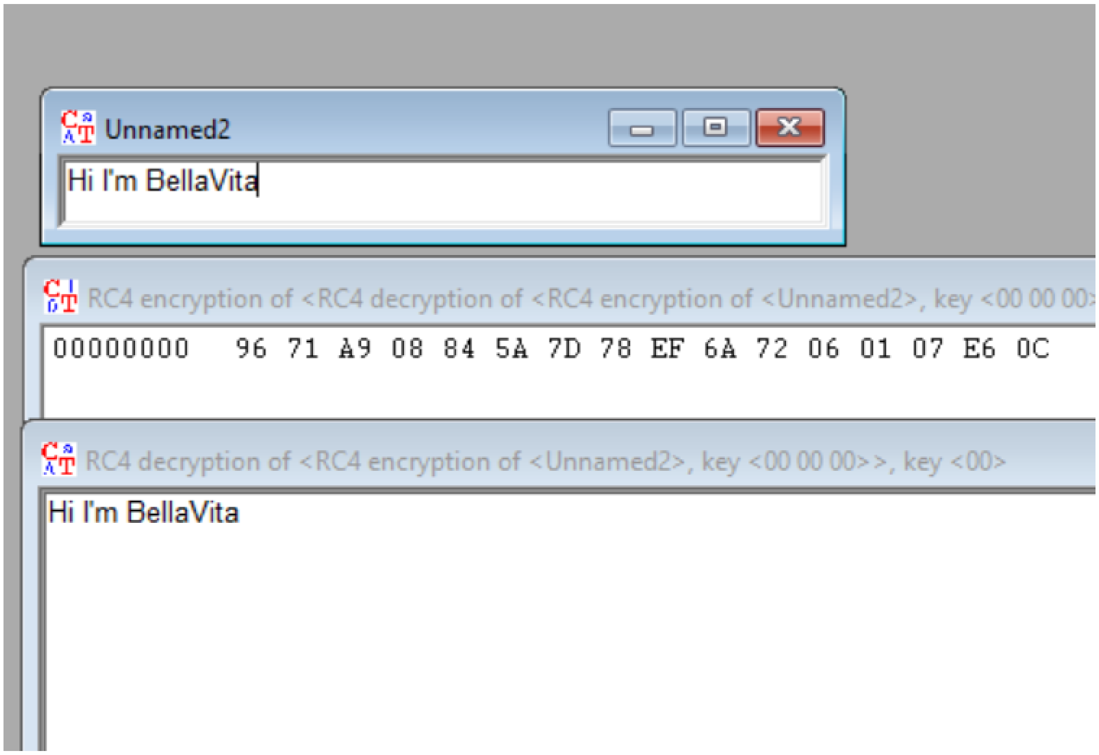
Article on RC4 : https://www.geeksforgeeks.org/what-is-rc4-encryption/
Download Link for CrypTool: https://www.cryptool.org/en/ct1/downloads

Open CrypTool after installation and close the default file.

Then click on “New” to open a new text editor page. Write Anything you want here and then click on Encrypt/Decrypt Select RC4(Symmetric)Modern.

It will ask you to select bits, again choose whatever you want and stick to it for both encryption and decryption.

Example of how your output Should Look :



Unnamed2

Hi I'm BellaVita

RC4 encryption of <RC4 decryption of <RC4 encryption of <Unnamed2>, key <00 00 00

```
00000000   96 71 A9 08 84 5A 7D 78 EF 6A 72 06 01 07 E6 0C
```

RC4 decryption of <RC4 encryption of <Unnamed2>, key <00 00 00>>, key <00>

Hi I'm BellaVita

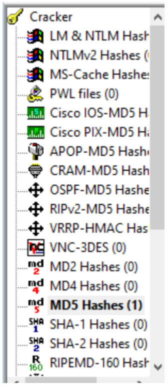
Practical 2 - (b) Use Cain and Abel for cracking Windows account passwords using Dictionary attack and to decode wireless network passwords

Cain and Abel (often abbreviated to Cain) was a password recovery tool for Microsoft Windows. It could recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks.

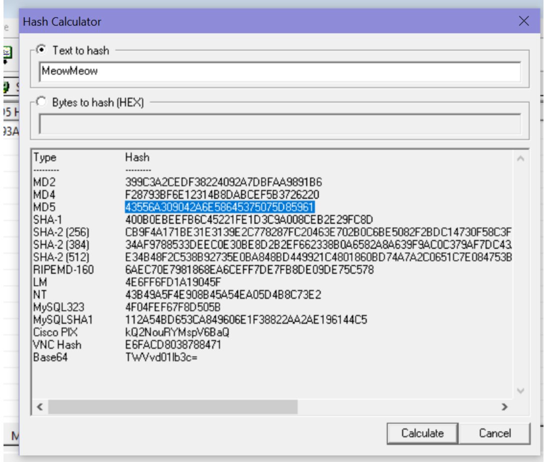
Download Link :
https://www.darknet.org.uk/2007/01/cain-and-abel-download-windows-password-cracker/

You might need to turn off your firewall in Security Settings. Anyways, After Installing follow the following steps.

Click on Cracker and then Select MD5 from the list on the Left



Click on Hash Calculator and Type in any word as your password. Keep it Simple. Avoid, letters, lowercase and Uppercase along with special characters to be in the same password. Ideal Password - night, star, long, pets, 1234, HiThere etc. Then click on Calculate on the bottom right corner of the Has Calculator Tab. You'll see a bunch of Hashes , copy the hash code infront of MD5 .



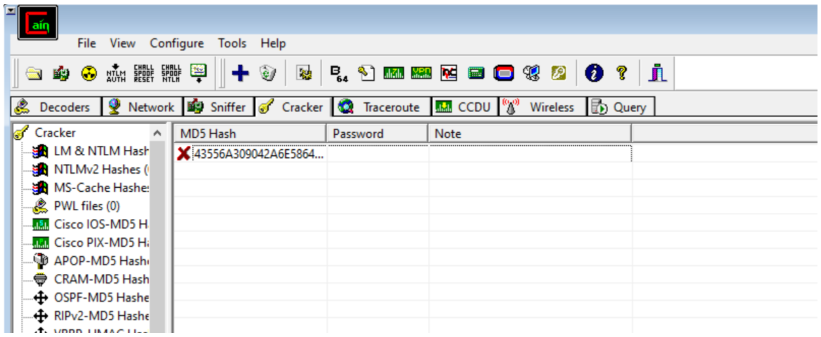
● Text to hash
MeowMeow

○ Bytes to hash (HEX)

```
Type            Hash
---------       ---------
MD2             399C3A2CEDF38224092A7DBFAA9891B6
MD4             F28793BF6E12314B8DABCEF5B3726220
MD5             43556A309042A6E58645375075D85961
SHA-1           400B0EBEEFB6C45221FE1D3C9A008CEB2E29FC8D
SHA-2 (256)     CB9F4A171BE31E3139E2C778287FC20463E702B0C6BE5082F2BDC14730F58C3F
SHA-2 (384)     34AF9788533DEEC0E30BE8D2B2EF662338B0A6582A8A639F9AC0C379AF7DC43
SHA-2 (512)     E34B48F2C538B92735E0BA848BD449921C4801860BD74A7A2C0651C7E084753B
RIPEMD-160      6AEC70E7981868EA6CEFF7DE7FB8DE09DE75C578
LM              4E6FF6FD1A19045F
NT              43B49A5F4E908B45A54EA05D4B8C73E2
MySQL323        4F04FEF67F8D505B
MySQLSHA1       112A54BD653CA849606E1F38822AA2AE196144C5
Cisco PIX       kQ2NouRYMspV6BaQ
VNC Hash        E6FACD8038788471
Base64          TWVvd01lb3c=
```

Crt + C that Hash code

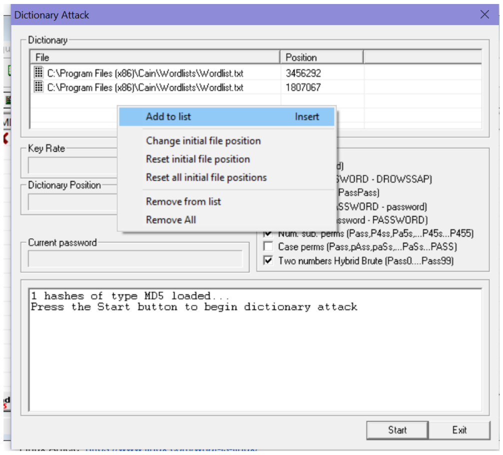
Now close this tab and then click on + Add to List, paste your hash code here, and hit Enter. You Should See that your hash code has been added.



MD5 Hash	Password	Note
✗ 43556A309042A6E5864...		

Now hover your cursor on the added hash code and right click > Dictionary Attack .

Then, In Dictionary Window right click > Add to List > WordLists > Wordlist and then click on start. If Your password is difficult then you won’t get the output so keep it simple. Maybe all lowercase and 1 single word. For me, meow and night worked.

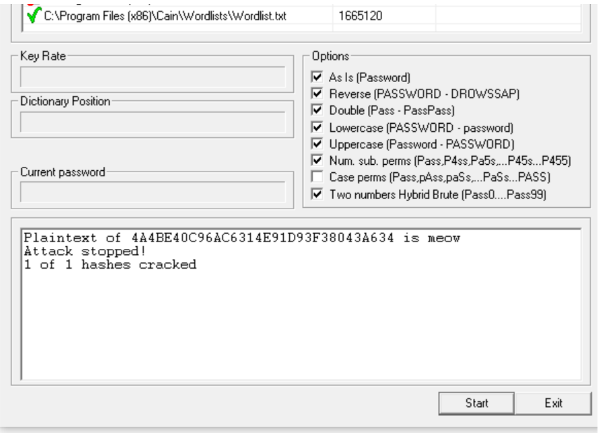


File	Position
C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt	3456292
C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt	1807067

☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
☐ Case perms (Pass,pAss,paSs,...PaSs...PASS)
☑ Two numbers Hybrid Brute (Pass0....Pass99)

```
1 hashes of type MD5 loaded...
Press the Start button to begin dictionary attack
```

Anyways, The Ouput should look something like this.



✓ C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt 1665120

☑ As Is (Password)
☑ Reverse (PASSWORD - DROWSSAP)
☑ Double (Pass - PassPass)
☑ Lowercase (PASSWORD - password)
☑ Uppercase (Password - PASSWORD)
☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
☐ Case perms (Pass,pAss,paSs,...PaSs...PASS)
☑ Two numbers Hybrid Brute (Pass0....Pass99)

```
Plaintext of 4A4BE40C96AC6314E91D93F38043A634 is meow
Attack stopped!
1 of 1 hashes cracked
```

Practical 3 - (a) Run and analyze the output of following commands in Linux – ifconfig, ping, netstat, traceroute

Kali Linux: Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Securit

Linux Article: https://www.linux.com/what-is-linux/

Basic Linux Commands : https://www.google.com/search?q=basic+linux+commands&rlz=1C1CHBF_enIN919IN919&oq=Basic+Linux+&aqs=chrome.0.0i433i512j0i512l6j69i60.3760j0j9&sourceid=chrome&ie=UTF-8

Online Kali Linux Emulator : https://www.onworks.net/os-distributions/debian-based/free-kali-linux-online

Go to Terminal and Directly Type the required commands and then you shall be done for this practical

Practical 3- (b) Perform ARP Poisoning in Windows

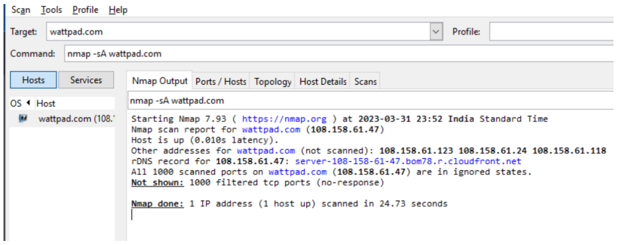
Practical 4 - Use NMap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS

Article on Nmap : https://www.mygreatlearning.com/blog/nmap-commands/#:~:text=Nmap%20is%20a%20short%20form,packets%20are%20used%20by%20Nmap.

Article on nmap Commands: https://nmap.org/book/scan-methods-null-fin-xmas-scan.html

Nmap Download: https://nmap.org/download.html

After the installation, open nmap and then set a target website after which type in the commands as , nmap-sA Target website



Target: wattpad.com

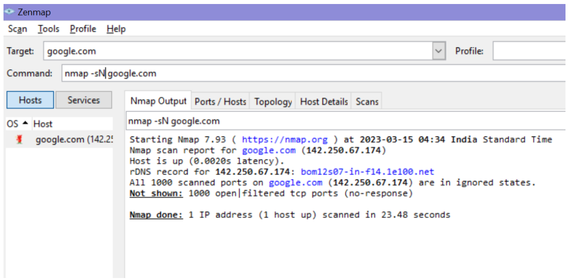
Profile:

Command: nmap -sA wattpad.com

```
nmap -sA wattpad.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-31 23:52 India Standard Time
Nmap scan report for wattpad.com (108.158.61.47)
Host is up (0.010s latency).
Other addresses for wattpad.com (not scanned): 108.158.61.123 108.158.61.24 108.158.61.118
rDNS record for 108.158.61.47: server-108-158-61-47.bom78.r.cloudfront.net
All 1000 scanned ports on wattpad.com (108.158.61.47) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 24.73 seconds
```

nmap-sN Target website



Target: google.com

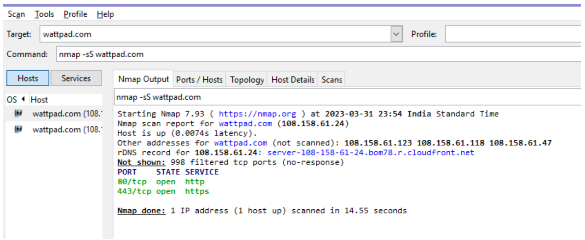
Profile:

Command: nmap -sN google.com

```
nmap -sN google.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-15 04:34 India Standard Time
Nmap scan report for google.com (142.250.67.174)
Host is up (0.0020s latency).
rDNS record for 142.250.67.174: bom12s07-in-f14.1e100.net
All 1000 scanned ports on google.com (142.250.67.174) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 23.48 seconds
```

nmap-sS Target website



Target: wattpad.com

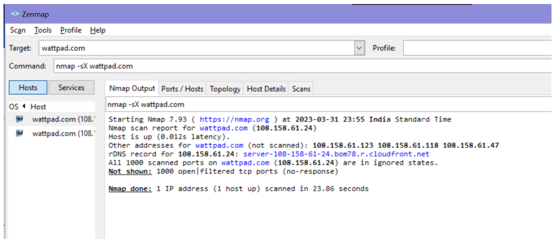
Profile:

Command: nmap -sS wattpad.com

```
nmap -sS wattpad.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-31 23:54 India Standard Time
Nmap scan report for wattpad.com (108.158.61.24)
Host is up (0.0074s latency).
Other addresses for wattpad.com (not scanned): 108.158.61.123 108.158.61.118 108.158.61.47
rDNS record for 108.158.61.24: server-108-158-61-24.bom78.r.cloudfront.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 14.55 seconds
```

nmap-sX Target Website



Target: wattpad.com

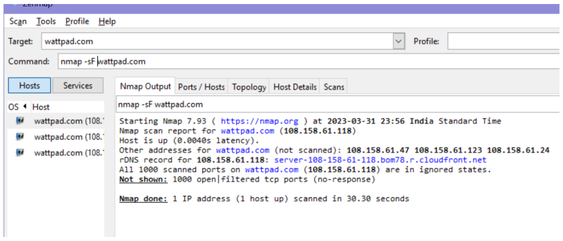
Profile:

Command: nmap -sX wattpad.com

```
nmap -sX wattpad.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-31 23:55 India Standard Time
Nmap scan report for wattpad.com (108.158.61.24)
Host is up (0.012s latency).
Other addresses for wattpad.com (not scanned): 108.158.61.123 108.158.61.118 108.158.61.47
rDNS record for 108.158.61.24: server-108-158-61-24.bom78.r.cloudfront.net
All 1000 scanned ports on wattpad.com (108.158.61.24) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 23.86 seconds
```

nmap-sF Target Website



Target: wattpad.com

Profile:

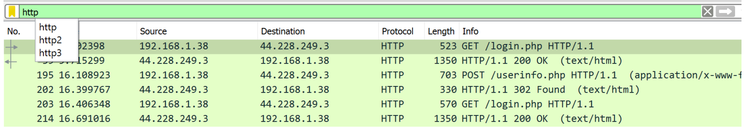
Command: nmap -sF wattpad.com

```
nmap -sF wattpad.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-31 23:56 India Standard Time
Nmap scan report for wattpad.com (108.158.61.118)
Host is up (0.0040s latency).
Other addresses for wattpad.com (not scanned): 108.158.61.47 108.158.61.123 108.158.61.24
rDNS record for 108.158.61.118: server-108-158-61-118.bom78.r.cloudfront.net
All 1000 scanned ports on wattpad.com (108.158.61.118) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 30.30 seconds
```

Practical 5-(a) Use Wireshark (Sniffer) to capture network traffic and analyze

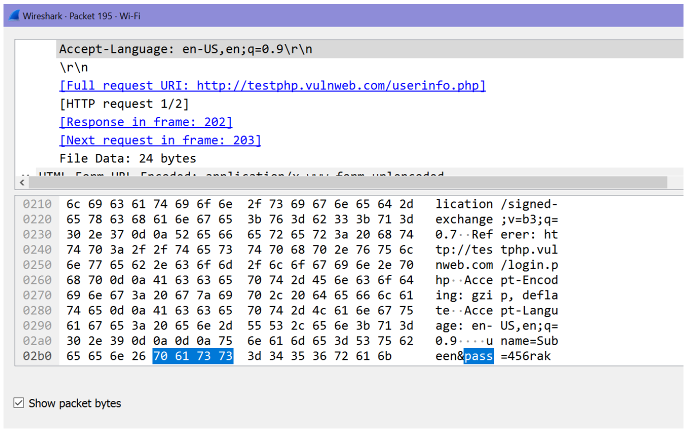
Download wireshark : https://www.wireshark.org/download.html and install it.
After the installation click on capture and select wifi.
Click on start and then you'll see a bunch of network traffic being shown.
Now goto http://testphp.vulnweb.com/login.php and enter username and password.
Comeback on Wireshark and Pause the capturing.
Apply "http" in filter bar.



http

```
No.              Source          Destination     Protocol  Length Info
      92398      192.168.1.38    44.228.249.3    HTTP        523 GET /login.php HTTP/1.1
      .715299    44.228.249.3    192.168.1.38    HTTP       1350 HTTP/1.1 200 OK  (text/html)
  195 16.108923  192.168.1.38    44.228.249.3    HTTP        703 POST /userinfo.php HTTP/1.1  (application/x-www-f
  202 16.399767  44.228.249.3    192.168.1.38    HTTP        330 HTTP/1.1 302 Found  (text/html)
  203 16.406348  192.168.1.38    44.228.249.3    HTTP        570 GET /login.php HTTP/1.1
  214 16.691016  44.228.249.3    192.168.1.38    HTTP       1350 HTTP/1.1 200 OK  (text/html)
```

Nice! Now double click on userinfo.php
Scroll down at the very end and you'll see your username and Password



```
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://testphp.vulnweb.com/userinfo.php]
[HTTP request 1/2]
[Response in frame: 202]
[Next request in frame: 203]
File Data: 24 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded

0210  6c 69 63 61 74 69 6f 6e  2f 73 69 67 6e 65 64 2d   lication /signed-
0220  65 78 63 68 61 6e 67 65  3b 76 3d 62 33 3b 71 3d   exchange ;v=b3;q=
0230  30 2e 37 0d 0a 52 65 66  65 72 65 72 3a 20 68 74   0.7··Ref erer: ht
0240  74 70 3a 2f 2f 74 65 73  74 70 68 70 2e 76 75 6c   tp://tes tphp.vul
0250  6e 77 65 62 2e 63 6f 6d  2f 6c 6f 67 69 6e 2e 70   nweb.com /login.p
0260  68 70 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   hp··Acce pt-Encod
0270  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
0280  74 65 0d 0a 41 63 63 65  70 74 2d 4c 61 6e 67 75   te··Acce pt-Langu
0290  61 67 65 3a 20 65 6e 2d  55 53 2c 65 6e 3b 71 3d   age: en- US,en;q=
02a0  30 2e 39 0d 0a 0d 0a 75  6e 61 6d 65 3d 53 75 62   0.9····u name=Sub
02b0  65 65 6e 26 70 61 73 73  3d 34 35 36 72 61 6b      een&pass =456rak
```

☑ Show packet bytes

Practical 5 -(b) Use Nemesy to launch DoS attack

Practical 6- Simulate persistent cross-site scripting attack

https://www.youtube.com/watch?v=owCMjIOMcPQ&t=22s&ab_channel=AnuragKurmi

7. Session impersonation using Firefox and Tamper Data add-on

Part 1: https://www.youtube.com/watch?v=jc90bCIk4RA&t=22s&ab_channel=Simplilearn
Part2:https://www.youtube.com/watch?v=dvdksevKyHs&t=39s&ab_channel=TecHRC

8. Perform SQL injection attack

https://www.youtube.com/watch?v=_78qDihrsTI&list=PLZb2y_zBp9oC5HBdMQ6u3NI8vpifG6Te0&index=7&ab_channel=AnuragKurmi

9. Create a simple keylogger using python

https://www.askpython.com/python/examples/python-keylogger

10. Using Metasploit to exploit (Kali Linux)

https://www.youtube.com/watch?v=hJXYCc-Lank&list=PLHI1FGtCuvyaua5mwkZ-5evSjxVNvdbgR&index=12&ab_channel=TecHRC