Lab != Lecture

- Learning by Doing by yourself
  - We are here to assist your learning
- Read Lab manual before hand
- During Lab hour
  - Follow the lab manual. Step-by-step, Do not rush
  - Do the lab task at the end of each lab
  - More questions to check your understanding

On Completing the Tasks

- Making Notes
  - Do not just copy the output on screen
  - Try to understand, if not then ASK US
  - Then take notes of what you do/learn
    - This is for yourself!! (and for the Exam)
- Drawing Message Sequence Diagram (lab man. p2)
  - Draw only packets of the protocal you interested in
    - Use packet filter in Wireshark
- Drawing a packet content
  - Simply write down the name of the protocal for each header
  - Plus, values of important fields, e.g. IP number, port number, and etc.

Task 1

- Look in important web server directories/files:
  - /var/www/
  - /etc/apache2/ (especially sites-available/default)
  - /var/log/apache2/
- Create your own HTML web page
- Check that someone else can access your page
- Capture the HTTP messages and learn (& draw) structure of request and response

Task 1

- What is favicon.ico?
- How to capture larger packets? (Hint: -s in tcpdump)
- Can you see the TCP connection setup?
- What port number did your browser use?
- What do the status codes 200, 304 and 404 mean?
- What is returned by server if you request ”/”?

Task 2

- Use **telnet** and **nc** to request pages from web servers

Task 3

- View the web server log file and understand its format

Task 4

- Setup Basic authentication for the web server
  - Add entry to web server configuration
  - Create user and password using htpasswd
  - Test, capturing with tcpdump
  - Find someone elses password!

Questions for Web Server

- Can you tell which port number your web client/server is using?
  - Access the same web page with another tab on firefox. Does the port number of server/client change? Why? Why not?
- Create a html page with an image.
  - How many request/response when you open the page?
- What happen when you run the following command?
  - sudo apache2ctl stop
- On configuring Apache
  - Can you change the root directory for web documents?
  - Can you disable listing of files/directory when accessing a web directory that doesn't contain index.html file.
- Using Wireshark, Can you tell which version of web server www.bing.com is running on?

Questions for Server logs

- What does 200 status code mean?
- Press F5 to reload webpage, then look at access.log
  - What does 304 status code mean?
  - Clear cache in browser and reload what happen?
  - Also try Press Ctrl + F5, what the difference from F5
- Does the size shown in log same as the file size of your web document? Why not???
- Try different web browser to access the server. Can the server know that you changed the browser?
  - Which HTTP option tell about your browser?

Questions for Authentication

- Which HTTP Options contain username/password?
- What does 401 status code mean?
- At least how many requests does a browser send to server in order to retrieve the protected page?

Questions for Remote Login

- Install Telnet server and SSH server
  - telnetd and openssh-server
- Using Wireshark to investigate ...
  - Remote login using Telnet
  - Remote login using SSH
- Which one is better? Why?
- What port number does each server listening on?