University of Glasgow | School of Computing Science

Lab Work Portfolio

Course Name	**Cyber Security Fundamentals (M) & (H)**			
Coursework Number	**Capture the Flag**			
Deadline	**Time:**	**12:00**	**Date:**	**See submission section**
% Contribution to final course mark	**10 %**			
Solo or Group ✓	**Solo**		**Group**	**✓**
Anticipated Hours	**x**			
Submission Instructions	**See submission section**			
Please Note: This Coursework cannot be Re-Assessed				

Code of Assessment Rules for Coursework Submission

Deadlines for the submission of coursework which is to be formally assessed will be published in course documentation, and work which is submitted later than the deadline will be subject to penalty as set out below.

The primary grade and secondary band awarded for coursework which is submitted after the published deadline will be calculated as follows:

(i) in respect of work submitted not more than five working days after the deadline
   a. the work will be assessed in the usual way;
   b. the primary grade and secondary band so determined will then be reduced by two secondary bands for each working day (or part of a working day) the work was submitted late.

(ii) work submitted more than five working days after the deadline will be awarded Grade H.

Penalties for late submission of coursework will not be imposed if good cause is established for the late submission. You should submit documents supporting good cause via MyCampus.

Penalty for non-adherence to Submission Instructions is 2 bands

You must complete an "Own Work" form via https://studentltc.dcs.gla.ac.uk/ for all coursework

Lab Work Portfolio

Overview

This Portfolio will cover 3 weeks of labs; that means a total of 3 labs will be covered by this submission. For these labs you will be asked to complete a series of activities\investigations and submit your findings.

The Portfolio should be completed in the same teams of 4 to 6 people that you used for the assessment. You should self-organise your team, details will be provided in class regarding notifying the course co-ordinator.

Your final submission of the Portfolio should be ONLY ONE per group and is worth 10% of your overall CSF grade.

Setup

You can complete the lab work on your own machine.

You will be using a series of online tools, Wireshark and Autopsy. Instructions on Autopsy is given in Lab Work Week 3 section.

Lab Work Week 1

In this lab you will need to work in your group. You will be asked to investigate three Wireshark samples. To proceed with the investigation, you will need Wireshark installed and to download the .pcap files from Moodle section Lab Material → Lab work week 1. All samples have been taken from the library of wireshark.org.

Exercise 1
Download the "sample1.pcap" file from Moodle and open it with Wireshark. Which protocols are being captured in this sample? What type of communication can you identify? Is there something noticeable in this sample? Can you identify any type of cyber-attack or similar?

Exercise 2
Download the "sample2.pcap" file from Moodle and open it with Wireshark. Which protocols are being captured in this sample? What type of communication can you identify? Is there something noticeable in this sample? Can you identify any type of cyber-attack or similar?

Exercise 3
Download the "sample3.cap" file from Moodle and open it with Wireshark. Which protocols are being captured in this sample? What type of communication can you identify? Is there something noticeable in this sample? Can you identify any type of cyber-attack or similar?

In the end you should produce a mini one-page analysis with your answers to the questions posed above and the findings of the investigation. You should explain what you have identified. This part of the Portfolio should not exceed 1 page.

Lab Work Week 2

In this lab you will need to work in your group. You will be asked to investigate a possibly suspicious email. To proceed with the investigation a list of tools is provided to you (see below). You will have to use 3 of these tools in order to extract useful information. The suspicious email can be downloaded from Moodle section Lab Material → Lab work week 2.

Questions: What is the purpose of these tools? Are there any noticeable differences between them (only for your chosen 3 tools)?

List of tools:
1) Maltego (www.threatcrowd.org)
2) IPvoid (www.ipvoid.com)
3) Checkphish (www.checkphish.ai)
4) Urlscan (www.urlscan.io)
5) Virustotal (www.virustotal.com)
6) Netcraft (www.netcraft.com)
7) CentralOps (www.centralops.net)
8) Command line approaches.

In the end you should produce a mini one-page analysis with your answers to the questions posed above and the findings of the investigation. You should explain what you have identified and the steps you have taken in order to complete your investigation. This part of the Portfolio should not exceed 2 pages.

Lab Work Week 3

In this lab you will need to work in your group. There are two things that you will need to do. You are provided with a forensic image already created with the FTK Imager for examination. This image can be downloaded from Moodle section Lab Material → Lab work week 3. You will need to load Autopsy (a tool for digital forensics) and search for evidence. We will assume that the evidence is relevant to "dogs" due to the sensitivity of the task.

If you have Windows, you can quickly download the Autopsy tool and install it. The windows tool has a nice and easy GUI to use (Autopsy - Download). If you want to use any type of Linux environment, you can access Autopsy.

Once in Autopsy you will be asked to create a case and use the keyword search functionality and identify any relevant evidence. You can also follow the material on how to use Autopsy that will be covered in week 9.

Questions: What type of keywords would you use if you are searching for dogs? Produce a relevant list. By investigating the extracted files, is there anything noticeable? What type of evidence can you gather?

In the end of the lab, you will need to produce an evidence list that could be used for the next stage of the investigation.

The Portfolio for week 3's section should include all the answers relevant to the questions posed above and, in the end, a full list of identified evidence should be presented. This part of the Portfolio should not exceed 3 pages.

The final report should not exceed 6 ½ to 7 pages excluding graphs and appendices.

Marking

The marking will depend on the description and the explanation on steps taken for completing all labs. The quality of the answers given to the posed questions and completeness. Also note that failing to adequately explain the steps taken will limit the grade you can potentially achieve.

Note that if the writing is poor in terms of coherence and grammar it could be very difficult to convey your understanding. It is advisable for all students to get others to read your work, even an uninformed reader – their feedback will help you identify where any issues might be. If you find yourself saying 'I meant this...' then it is likely you have not written it clearly enough.

Submissions

A person should be chosen per team that will ensure the successful upload of your work. One file needs to be uploaded per team: 1) the Lab Work Portfolio including a group policy document. The group policy should state what work has been achieved per person and this should be agreed between all team members. The deltas would be uploaded individually per student as they are confidential (ONLY WHEN NECESSARY, WHICH MEANS WHEN ISSUES WITHIN THE TEAM ARISE).

All submissions should be .pdf files and have the format lab_work_portfolio<team name>.pdf and the documents should have the names and student numbers of the team members. Submission slots will be available on Moodle.

A summary of submissions due is shown below:

1. Lab Work Portfolio
2. Group policy form (attached to final report)
3. Individual peer evaluation form (only when needed)

All documents should be uploaded by 12:00 14th of March.