The University of Queensland
School of Information Technology and Electrical Engineering

COMS3000/7003
Semester 2, 2018

Assignment 3 (Weighting 10%)

This Assignment is due **12:00 NOON (MIDDAY) Thursday, 25/10/2018**

Report on the Security of the most Common Authentication Credential (Passwords)

Group Assignment

[COMS3000: 10%, 10 marks (total)]
[COMS7003: 10%, 10 marks (total)]

Tasks

Review and report on the security of the hashed passwords in /etc/shadow from Assignment 1.

Your report must include:

1. All the members of your group and THE WORK they provided to the group effort. [1 mark]

Groups must have a minimum of 1 member.

Groups may be a mix of COMS3000 and COMS7003 students, if the group desires. (This may break the assignment chute system, so you may have to submit the paper report twice, one for the COMS3000 members and one for the COMS7003 members, but identical reports.

Every member of the group must have an (identical) electronic copy of the report and submit it individually in Blackboard (the individual electronic copy is retained as your assessment record, the paper copy is returned to the group).

To prevent large cohorts claiming the same mark and to ensure sufficient opportunity to find passwords outside the group membership, group size is arbitrarily limited to 20 students. You will need a strong argument to get permission for more than 20 in a group, otherwise groups of greater than 20 will incur a 5% reduction in final marks for every member greater than 20.

Groups of more than 1 member are to select a group name.

2. You are to report on how you attempted to find the insecure passwords in the /etc/shadow file. [maximum 2 marks]

As stated in the lecture, GPUs are NOT part of this assignment. While it is impossible to ban the use of GPUs, YOUR REPORTED SOLUTION MUST WORK ON STANDARD CPUs. This section must include your selection of tools and dictionary, WHY you chose those tools and dictionary and the advantages AND DISADVANTAGES of your chosen tools and dictionary, and the description of the platforms you are running these on, including CPU, number of cores, clock speed, and amount of memory for each.

3. You must detail AND EXPLAIN the configuration you used. [maximum 4 marks]

This is where the quality of your reporting and the effort and imagination you put into your configuration and rules will affect your marks. Do not share your plans with other groups!

Your configurations will dictate your marks more than processing power. I will run up the configurations on low-end machines (e.g. VMs on one core of a MacBook Air with 2GB RAM) to compare the groups, where I need to.

NOTE – Your solution MUST work on Windows, Linux or MacOS

In this section you need to include what worked and what you needed to change AND WHY. What adjustment did you make? Did these improve the outcomes? CRITICALLY ANALYSE your outcomes and your configuration choices.

I will split the groups into five categories:

0 marks – little or no explanation, difficult or impossible to repeat the procedure

1 mark – basic configurations, weak explanations, only the easiest passwords cracked

NOTE: Any group that cracks new passwords is guaranteed minimum 5 marks overall

2 marks – some thoughtful configurations, adequate explanations, adaptation employed

3 marks – excellent configurations and not so complex as to prevent a good outcome, good explanations and adaption, must have found some passwords not found by any other team except for possibly:

4 marks – insightful efficient configurations, sound explanations and strong critical analysis, these teams have demonstrated a strong ability to develop configurations to find passwords that no other team could, except where another team at this level may have a similar high-quality configuration.

4. You must detail your results and EXPLAIN WHY each password found was insecure. [maximum 3 marks]

Again the quality of you explanations will dictate the marking.

Because the tool found it = 0 marks

Explain why the tool found each = 1 mark

Tie the explanations back to course fundamentals = 2 marks

Demonstrate significant insight into the results findings = 3 marks

REMEMBER the group's own passwords & the 3 passwords cracked in the lecture don't count.

PURELY OPTIONAL – Only because some groups wanted to do it:

You can boost some of your marks (if you fell short above) if you can successfully execute a significant break (not just passwords) into the Assignment 1 server at 35.166.144.118

Most groups will not spend time on this – it is only for those who really wanted to.

The server will **ONLY be available from 8:00 am on Saturday 13 October, for at most 12 hours** (probably significantly less if someone crashes it earlier).

I'll be watching the instance and as soon as it starts running up my bill (e.g. someone starts crypto mining on it) I'll terminate the instance. (So this may be a very short-lived option.)

If you do succeed, record evidence that you did it, and write up the vulnerabilities and your attack in a separate section of your report.

Submission Instructions

The following items need to be submitted:

- A hard-copy of the assignment is to be submitted through the Faculty of EAIT (Hawken Building 50) assignment chute and requires a **signed assignment cover sheet**.
- You also need to submit an **electronic version** of your assignment in PDF format via Blackboard.