TCS2251 Computer Security
Assignment (10%)
Guideline:

- The lab assignment is to be done in the registered group. Max. 3 students per group.
- **Titles selection (18 Dec 2018 – 31 Dec 2019):**
    1. Form a group of max. 3 students in respective LECTURE CLASS (either CS1 or CS2 only).
        - Select four unique hash values from different algorithms in section 1 and a website in section 2. There should be no two or more group with the same combination of hash values and a website in the same lecture class.
    2. Fill in the detail in Google Spreadsheet to register and confirmed the titles. **Ensure you choose the correct lecture class**.
        - Assignment Group registration for **CS1 (Tue)**: https://tinyurl.com/yakkctr5
        - Assignment Group registration for **CS2 (Mon)**: https://tinyurl.com/ybqh7k55
        - The selected FOUR hashes values (for section 2) and website (for section 3)
        - Note: The selection is based on first-come-first-served (FCFS). The registration will be rejected if the detail is incomplete or not fulfilled the criteria.
- You are required to submit the report in hardcopy (during lecture class) and softcopy (in MMLS). The softcopy submission of the assignment report should be made via MMLS before or on **11 February 2019 (Monday)**. Marks will be deducted for late submission. Please make sure to submit the hard copy and soft copy of the report anytime during the lecture class.
- Please prepare a cover page with the information of subject code, subject name, group nickname, group leader and member(s) names, IDs, lecture class, tutorial class, the selected pair of hash values numbers and the title.
- Attached the assessment sheet after the cover page. Ensure the report is properly formatted with Table of Content.
- The type setting for the documentation should be normal margin, Times New Roman, 12pt and 1.5 spacing.
- This assignment contains THREE sections, answer ALL questions. The total marks of the assignment are 35 and it will be translated to 10% for your coursework contribution.
- Please print screenshots to demonstrate and highlight your output and analysis result. All explanation of analysis result MUST be supported by screenshot. You may circle /highlight answers to multiple questions in one screenshot.
- Judging criteria
    - Section 1: Quality of coding, provide remarks, clear explanation of codes, the efficiency of the algorithm, output with concise explanation etc.
    - Section 2: Quality of analysis, provide screenshots and clear explanations, the accuracy of information, able to find solution effectively etc.
    - Overall quality of report and formatting
- Your solutions should be unique and depend on your chosen hash values, coding, network environment, IP address and computer configurations. A penalty will be given for those to plagiarize.

Section 1: Passwords Hackathon (25 marks)

The following table show the hash values generated using four different types of algorithms based on different combination of character sets sequence.

Set Sequence	2356	115	161	54X6
Algorithms	MD5 (A)	DES (B)	SHA-256 (C)	SHA-512 (D)
1	$1$Bvchsja2$PNIc/6FABlQsAPGZFFb7m1	J7DZMIc4lpL2g	$5$jdsAudKd0$qA/Vu5UN1zvNCCr4Ab8mPGGeqebJKWztIGxxIrIejdD	$6$va6xhJudsL$Lp.rTLL4wXAuLGwQNrSTapgnQmrwX5FeuYsDiELSUPyag9t.Pggy24DUmW7QqBncpkZ2/i3UKiOu6FP/8iE7l/
2	$1$nbcJ829X$44Ak..7EfN8rhSGvKlPV4/	n9KWHTizhHp4g	$5$sjKjs821s$JJIYxAxvixulQF0Hyq/Xx9IwAYhpKqttiRfKw2Zp4A2	$6$gbsJy832hK$xefDM8upaRhl2gO/naAZcZLCSDtkCOCTCqswY4CBZV7EEn2savdjzANMK.GFcSMoGdV0cOmVpGpSdkFU1vSl6.
3	$1$mBisdo22$.xKzt5jGz41997AM7I5MW/	ByGp49ZA87rjg	$5$KkHjbsu12d$tUEkiY6u71CbqomVBiFIXs8CZeQE/OL1VbTTXoJEMf6	$6$JhdnAY62ks$0b4ktwMnjPJxw2Ea/4FYN3qIqG58bWeSTT5Mir0VGayiwMD7XVyDYXX80gMo8Gt3aBNcIfFdjw/L8e/ISVDJ81
4	$1$ksjU92Bc$QZHCeHxpFfr5HYrUkqlU11	v7rRlq9f16/NI	$5$XncksXks91$0Xe2JRYRs6u3GLXJexK7sxjmqPUmPPsy8BYQn0Kubx4	$6$ahdKh2os0S$oSGJUKSiXV2Aa/vr7At2hvmSveMUo5sc8LOivdRVUPpWg.WYeLyWCYccAb/6fyyGZz2JPJTrSRbdos1Q6Pio8/
5	$1$dks8JJsa$pt/szIsl31N3Kzsy1XDp80	cTSx6lNBnSxG6	$5$82JHsklO29$4DCLrrO7bp349HLXD55pzNnLApr8UIYLbCdxc5JTikB	$6$kdMn79HcvA$CQunZ2AyP/5ClqWxhc5H2mhCIuN999VNCUSmf0qk49PEBZb.3Nrx5RX8zwomuKobj2YJ0WBUaqoYC0i/liazX1

The following are the six sets characters.

- Set 1: A-Za-z0-9
- Set 2: A-Z
- Set 3: a-z
- Set 4: 0-9
- Set 5: ~ ! @ # $ % ^ & * _ +
- Set 6: [ ] { } < > ( )

For example, if the password is created based on character set sequence **2356**, then the password could be "Ax@{", "{Mg&]", and "Jv*)". Where the first character is from Set 2, the second character is from Set 3 and the third and fourth characters are from Set 5 and 6 respectively. The X represent the character from set 1 to 6.

Questions:

1. What is the syntax to generate MD5, DES and SHA-512 hash using **mkpasswd**? Write down the syntax and provide **THREE (3**) sample commands and the outputs.

[3 marks]

2. Your team is required to select **FOUR** hash values from each column (A, B, C and D) shown in the table and try to find the password using BASH scripting.
   a. Each group should select **FOUR** unique hashes based on first-come-first served basis.
   b. The hash values should be placed in a file called **hackfour.pwd**, the format for place the hash values in the file is **hash_1$hash_2$hash_3$hash_4**. For example, assume A1, B4, C1 and D2 are selected then the combined hash values should be as

```
$1$Bvchsja2$PNIc/6FABlQsAPGZFFb7m1$v7rRlq9f16/NI$$5$jdsAudKd
0$qA/Vu5UN1zvNCCr4Ab8mPGGeqebJKWztIGxxIrIejdD$$6$gbsJy832hK$
xefDM8upaRhl2gO/naAZcZLCSDtkCOCTCqswY4CBZV7EEn2savdjzANMK.GF
cSMoGdV0cOmVpGpSdkFU1vSl6.
```

   c. Write codes to read the file, extract the salt and hash values and find the passwords for all the hash values.
   d. Print your codes with remarks clearly in the report. Provide the password for both hash values.

[20 marks]

3. Each member is required to write a page of report about the strategy used in solving password for the assigned hash value.

[2 marks]

Section 3: Network Analysis (10 marks)

The following is the list of banking and e-commerce websites.

1. www.google.com
2. www.youtube.com
3. mail.google.com
4. www.mmu.edu.my
5. www.celcom.com.my
6. twitter.com
7. www.facebook.com
8. www.instagram.com
9. www.wikipedia.org
10. sydney.edu.au
11. www.lazada.com.my
12. www.11street.com.my
13. www.shopee.com.my
14. www.ubuy.com.my
15. world.taobao.com
16. m.axiata.com
17. www.speedtest.com
18. www.fast.com
19. www.spectrum.net
20. www.utoronto.ca
21. www.manchester.ac.uk
22. www.ufl.edu
23. www.theguardian.com
24. www.parents.com
25. www.liverpool.ac.uk
26. www.instagram.com
27. www.apple.com
28. www.irakyat.com.my
29. www.cimbclicks.com.my
30. www.maybank2u.com.my

Select a website listed above. Each website only can be selected by at most two groups. Thus, the group is required to perform network analysis on a selected website using Wireshark or other tools. Analyze the selected website and answer the following questions and provide explanation with screen shots and circle/ highlight the information to support your answers.

Questions:

1. What is the IP address of your computer? Provide screen shot and command used.
2. What is the IP address of the selected website? Kindly describe the steps and screen shot you used to obtain the IP.
3. Ping the selected website and show how Wireshark capture the ping packets only.
4. List and show the internet layers displayed by Wireshark program.
5. Describe how you check the statistics of the number of packet lengths sent/ received using Wireshark. Accompany your answer with screen shot.
6. What is the filter command that only show the TCP packets that contain the name of the selected website?
7. What is the filter command that will highlight all the TCP packets may contain problems for analysis in Wireshark?
8. Upload a file to any website, use Wireshark to capture the packets sent and show the Stevens graph. Analyze and provide a brief explanation on the connection.

TCS2251 Computer Security
Lab Assignment – Assessment Sheet

Group Name (Section):

Section 1:

No	Requirement	Marks	Remarks
1	Provide syntax and sample command for generating MD5 hash	/ 1	
	Provide syntax and sample command for generating DES hash	/ 1	
	Provide syntax and sample command for generating SHA-512 hash	/ 1	
2	Place the FOUR hash values in hashfour.pwd	/ 1	
	Write code to read hashfour.pwd file	/ 1	
	Create six character sets	/ 1	
	Solved hash_1	/ 3	
	Solved hash_2	/ 3	
	Solved hash_3	/ 3	
	Solved hash_4	/ 5	
	Proper coding style, indentation and remarks to explain the codes	/ 3	
	Show screen shots and output	/ 1	
3	Solution strategy from each members	/ 2	
	Total	/ 25	

Section 2:

No	Requirement	Marks	Remarks
1	Show IP of own computer. Provide screen shot and command used	/ 1	
2	Show IP of selected website and steps	/ 1	
3	Show capturing ping packets only in Wireshark	/ 1	
4	List and highlight the internet layers depicted by Wireshark	/ 1	
5	Show statistics of Wireshark program with description	/ 2	
6	Show correct filter command for Q6	/ 1	
7	Show correct filter command for Q7	/ 1	
8	Show upload packets in Stevens graph, analysis and explanation	/ 2	
	Total	/ 10	

Total	/ 35