The University of Queensland
School of Information Technology and Electrical Engineering

COMS3000/7003
Semester 2, 2018

Assignment 1 (Weighting 7%)

This Assignment is due **12:00 NOON (MIDDAY) Thursday, 16/8/2018**

IT and Electrical Engineering Security Research Tasks

[COMS3000: 7%, 7 marks (total)]
[COMS7003: 7%, 7 marks (total)]

Tasks

Research, locate and download the CURRENT Institute of Electrical and Electronics Engineers ***IEEE Editorial Style Manual***.

Correctly reference (IEEE format) the current ***IEEE Editorial Style Manual*** here:

[1] DifferentBetween.net, "Difference Between Telnet and SSH," [Online]. Available: http://www.differencebetween.net/technology/internet/difference-between-telnet-and-ssh/. [Accessed 01 August 2018].

[2] Carnegie Mellon University, "Telnet Encryption," [Online]. Available: http://www.cs.cmu.edu/~droh/755/encr_telnet.html. [Accessed 01 August 2018].

[3] SSH.com, "TELNET - AND SSH AS A SECURE ALTERNATIVE," 21 February 2018. [Online]. Available: https://www.ssh.com/ssh/telnet. [Accessed 01 August 2018].

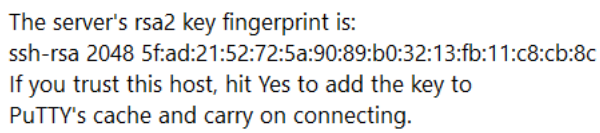
[These next tasks rely on your prerequisite (CSSE2310) knowledge of Unix shells and Unix file permissions.]

Connect to 35.166.144.118 using ssh. Do not use telnet to connect over public networks.

The key fingerprints are:

RSA 2048 MD5:5f:ad:21:52:72:5a:90:89:b0:32:13:fb:11:c8:cb:8c
RSA 2048 SHA256:s9xr+jKa8tUTop134aBs1Mxq8Jygs7WzJnAeX7h9gUs or
ECDSA SHA256:GIqgx5S6+cjtOodDgURxq/RMtR4oWiWiDmrsld0o4hs

e.g:



[If you do not already have an ssh client and want to use a Microsoft Windows device, I recommend you investigate how to use Simon Tatham's "PuTTY" at https://www.putty.org/]

Why shouldn't you use telnet to connect over public networks? : The reason not to use telnet to connect over to the public network is that telnet communicates data without an encryption. As such information that is sent over the network will then be in plaintext form [1]. This will allow the packet sniffer to do an eavesdrop attack to acquire information such as the username and password or other sensitive data on the same network as it is unencrypted [2], [3]. Therefore, attackers will gain access to information not belonging to them.

Login with your s1234567 user ID and use "COMS3000/7003" as the password.

Change your password to something secure (COMS3000/7003 is NOT a secure password).

DO NOT USE A PASSWORD YOU USE SOMEWHERE ELSE

You should **complete this task before** the second lecture, so that you have time to recover if you lock yourself out. Requests for password resets could take up to 48 hours to action.

Retrieve the file "flag1" from your home directory.

Write the contents of flag1 here: 9011473

If you can, work out how these contents were created: Using the formula, [studID + (studID - 1)] or [(2studID) - 1] where studID is the first seven numerical numbers of the student id, we could derive the contents of flag1. As such, using one of the formula above (2x4505737) -1 will give the content of "flag1"which is 9011473.

Use your knowledge of Unix shells and Unix file permissions to CHANGE the READ-ONLY file "flag2" to contain the sentence: "I know how to modify to a read-only file in Unix."

Change the permissions on "flag2" so that anyone can read it, but no-one can modify it.

End of Tasks

Do not use the services on 35.166.144.118 for any other purpose!

End of Submission

You do not need to submit this page

Assessment:

Marking Scheme:

Correctly reference (IEEE format) the current IEEE Editorial Style Manual – 1 mark

Explained why you shouldn't use telnet to connect over public networks – 1 mark

Successfully changed password on 35.166.144.118 – 1 mark

Provided the correct contents of file "flag1" – 1 mark

Method of obfuscation of contents of file "flag1" provided – 1 mark

Contents of file "flag2" changed to "I know how to modify to a read-only file in Unix." – 1 mark

Successfully changed "flag2" so that anyone can read it, but no-one can modify it – 1 mark

Further Guidelines

Academic Merit, Plagiarism, Collusion and Other Misconduct

You should read and understand the statement on academic merit, plagiarism, collusion and other misconduct contained within the course profile and the document referenced in that course profile. Work without academic merit will be awarded a mark of 0.

Unauthorised access, modification or impairment, including accessing other student's accounts, or misuse of the services, constitutes an offence under the Cybercrime Act 2001, which will be actioned both through the University statutes and the AFP.

Also, it is a **requirement for this assignment** that all students have completed the ***Academic Integrity Online Tutorial.*** The tutorial is compulsory for all UQ students, but in case you have missed it, you need to make sure you complete it before you submit your assignment.

A link to the tutorial website is displayed when you log into mySI-net.

Here is a direct link: https://www.uq.edu.au/integrity/Login.aspx?ReturnUrl=%2fintegrity

Failure to have completed the Academic Integrity Online Tutorial prior to submission will result in a mark of zero. Note most students have already completed this for previous courses. You do not need to complete it again – the system keeps the record of it.

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.

The submission deadline is 12:00 NOON (MIDDAY) Thursday, 16/8/2018 – both copies must be submitted. The hardcopy will be returned to you before the revision period at the end of semester.

Good time management is critical. Students should not expect any significant assistance from the lecturer or tutor on this assignment in the last few days before the deadline.

Requests for password resets (to dross@itee.uq.edu.au) will take 48 hours to action. Do the assignment early - **don't lock yourself out in the last week before submission!!!**