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] IEEE Periodicals. (2016). *IEEE Editorial Style Manual v9.0.* [Online]. Available: http://ieeeauthorcenter.ieee.org/wp-content/uploads/IEEE_Style_Manual.pdf, Accessed on: Aug. 01, 2018.

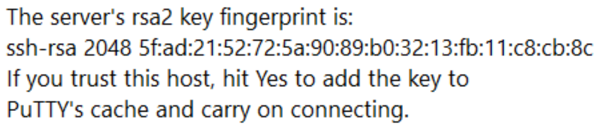
[These next tasks rely on your prerequisite (CSSE2310) knowledge of Unix shells and Unix file permissions.]

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:



```
The server's rsa2 key fingerprint is:
ssh-rsa 2048 5f:ad:21:52:72:5a:90:89:b0:32:13:fb:11:c8:cb:8c
If you trust this host, hit Yes to add the key to
PuTTY's cache and carry on connecting.
```

[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 for not using telnet to connect over the public network is because telnet communicates without using data encryption. Without data encryption, data information is transferred over in plaintext form. Packet sniffers have the potential to carry out an eavesdrop attack on a public network. An eavesdrop attack exposes the data information such as username, password and other kinds of sensitive data on the unencrypted network. Packet sniffers may gain sensitive data over unprotected networks.

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 number 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