WEEK 3 – TASK 3.1P

Pass Task.
Release Date: 29 March, Due Date: 15 April, End Date: 19 April.

Learning Outcomes

In this task, you will learn more about Unix/Linux Access Control. You will get hands-on experience of configuring and interpreting permissions. This will complement the theoretical discussion about Access Control in Week 3.

Instructions

An **answer sheet template** is available on OnTrack as a `**Resources**'. Please download the answer sheet and fill it with your answers. To upload on OnTrack, you need to convert the answer sheet template document to **PDF**. MS Word includes built-in PDF conversation capability.

All 5 questions and their sub-questions of this task must be attempted. If screenshots are required, please ensure that text in screenshots is readable.

Remember that troubleshooting technical problems is part of learning in this field. You must patiently work through issues and solve these. Tasks are not step-by-step guide. You need to be in the driver seat and learn concepts by doing – as you would when you start your future job (many times even your future supervisor doesn't know the answer to problems you face). After patent troubleshooting and research, if you need help:

Help is always available in SIT182. Please go to **Discussions** and ask your questions about this task in **Task 3.1P**. All students are encouraged to participate and help peers with their questions. Helping others is a great way to learn and think about aspects you may have overlooked. You can also seek help from tutors during online and face-to-face pracs. Please do not raise your questions through Teams, OnTrack, or Email.

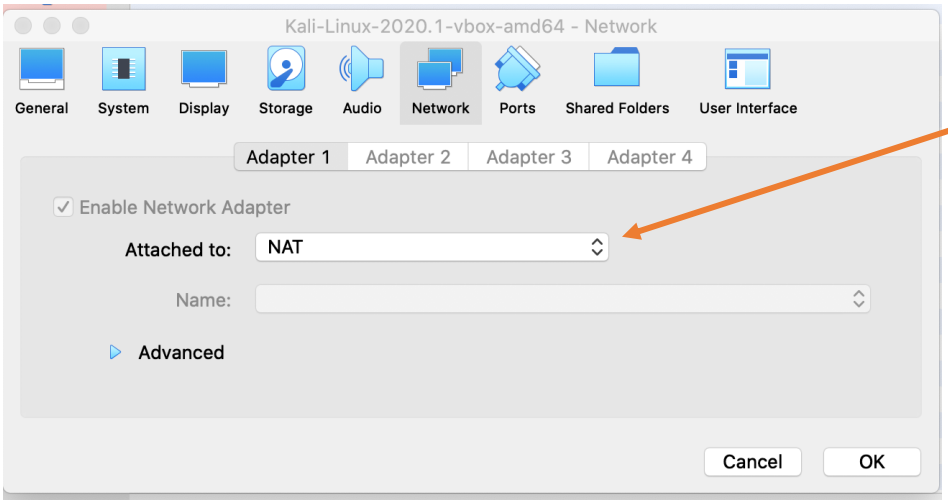
References In cyber security, our preferred referencing style is **IEEE** – however, you are allowed to use any Deakin approved referencing style in this unit. Please refer to unit site > Content > Referencing - Hints & Tips for more information.

This task involves working on a set of challenges. You will also need to answer a set of follow up questions listed in this task sheet to ensure the learning outcomes of the task are met.

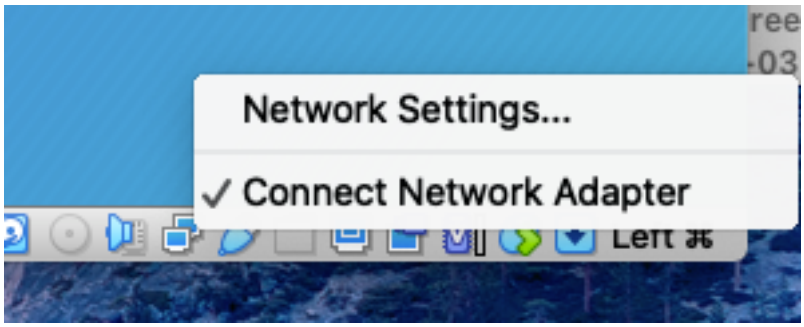
To access challenges that you need to complete open Kali VM from VirtualBox. We will use the same Kali VM that you used for Task 1.4P.

Note: If you are using cyber lab PCs, you will need to import Kali VM into VirtualBox from Drive D > SIT182 folder. Just like you did for Task 1.4P.

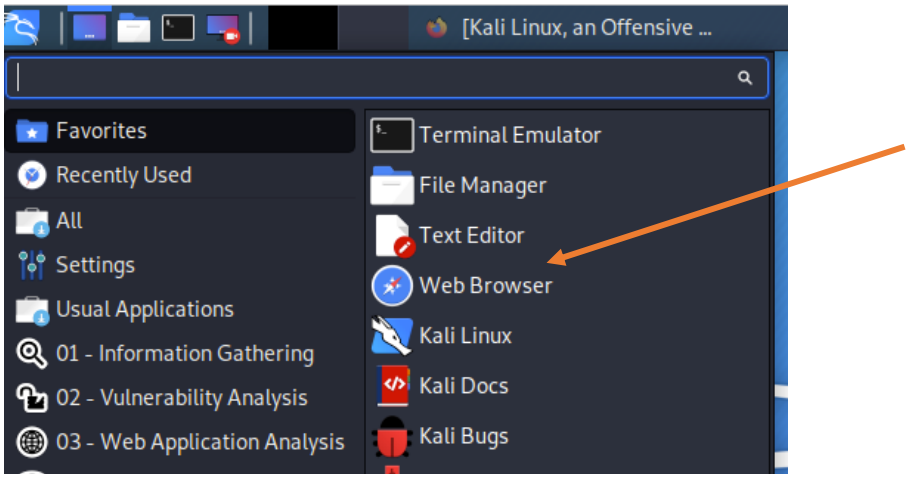
First, ensure that Kali is connected to Internet. Check the Settings of Kali VM and ensure Network Adapter is connected either through NAT or Bridged Adapter.



Run Kali VM (remember that username and password is **kali**). Ensure Network Adapter is connected using the toolbar at the bottom of VM window.



At this point you should have access to Internet from Kali. In Kali, access Web Browser.



Challenges are available for you to complete through https://cyber-challenges.com/.
[if clicking on the link didn't work, copy/paste the address to the address bar].
Enter `sit1822021' (without quotes) as password to access the website.

Question 1:

a) Include a screenshot confirming that you have managed to create the docker image, build it and get an "alice" shell (*by following the readme file in Access Control folder*).
b) List the passwords that you used to access Challenge 2, 3, and 4.

Question 2:

a. What is a Docker? How it is different from a Virtual Machine?
b. What does the "sudo" or "su" command do?
c. What does the command "ls -l" do?
d. In your own words (i.e., no direct quotes), what does `Chmod' command do in Unix/Linux?
e. In a paragraph (up to 200 words) summarize what you understood about SUID permission and capabilities as covered in Challenge 4. This needs to be in your own words (i.e., no direct quotes).

The following questions are common in interviews for cyber related positions. If you spent time going through the challenges and understanding Linux permission, then with a little extra research you should be able to answer them easily. Remember, doing your own research is an important skill for your future career in this field. If you are finding it difficult

to answer these questions, practice a bit more in the terminal and watch the help video for Linux access control. Then, try again.

Question 3:

a. **Is the following statement True or False**? `sticky bit is a special permission that can be assigned to a file'.
b. **Is the following statement True or False**? `An executable file has SUID permission set. When the file is executed on the system, the user who runs the file becomes the file's temporary owner'
c. You just created a new script file named myapp.sh. However, when you try to run it from the command prompt, the bash shell generates an error that says -bash: ./myapp.sh: Permission denied. Which command will fix this problem?
d. A file named sit182.txt has a mode of rw-r--r--. If arash is not the file's owner and is not a member of the group that owns this file, what can he do with it?
e. A file named ontrack.ppt has a mode of rw-r--r--. If chang-tsun is the file's owner, what can he do with it?

Question 4:

a) If you wanted to have a data file that you could read or write, but don't want anyone else to see, the permission would be ……. (answer using the 9-bit e.g. -r--r--r--)

b) If the file is owned by the user, the …… permission determine the access. (fill the blank either with OWNER/GROUP/OTHER)

c) If the group of the file is the same as the user's group, the ……. determine the access. (fill the blank either with OWNER/GROUP/OTHER)

d) If the user is not the file owner, and is not in the group, then the …… is used. (fill the blank either with OWNER/GROUP/OTHER)

Question 5:

Reflection point – What did you learn that was new to you? How did you manage to learn about Unix permissions to complete this task? Did you primarily use the Help Video and textbook provided or used your own resources?

(see next page)

Question 6: (optional)

As we approach the easter break, it's a good point for the teaching staff to reflect on what we can do better to support our students. I (Arash, your unit chair) am always keen to hear student feedback and committed to do what possible to improve our teaching quality. If there is anything you would like to raise with your unit chair you can use the following links – I will read each feedback and will provide report on any action, we may take to accommodate:

(see next page)

- *Lectures:* https://forms.office.com/r/R0wvNNzzsx
- *Pracs:* https://forms.office.com/r/15WRqTWsv0