WEEK 5 – TASK 5.1P

Pass Task.
Release Date: 19 April, Due Date: 3 May, End Date: 10 May.

Learning Outcomes

In this task, you will learn more about a few different network security topics including network footprinting, packet inspection, and source address spoofing. This task complements the theoretical discussions in week 4 and 5.

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 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 5.1P**. 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.

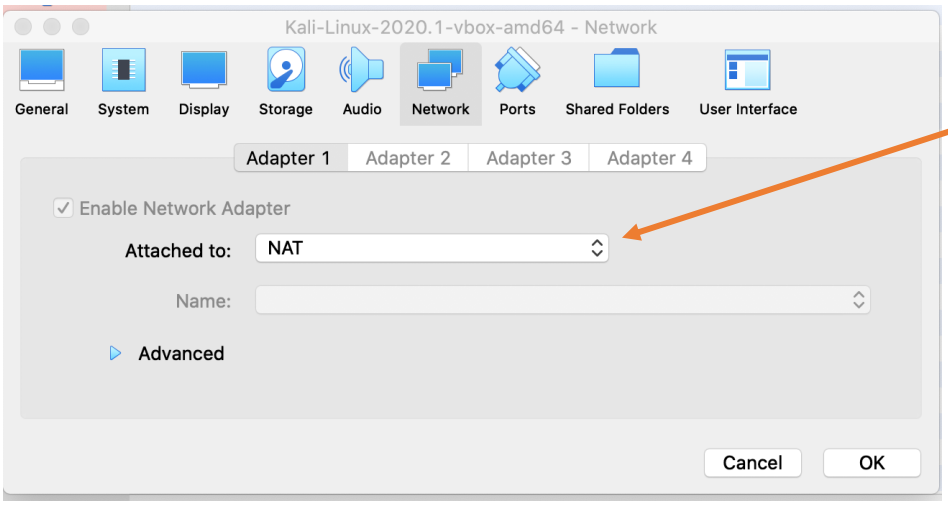
References In cyber security, our preferred referencing style is **IEEE** – however, you are allowed to use any Deakin approved referencing style in this unit. Please refer to unit site > Content > Referencing - Hints & Tips for more information.

This task involves working on a set of challenges. All questions that you need to answer are available on the website that provides you with the challenges.

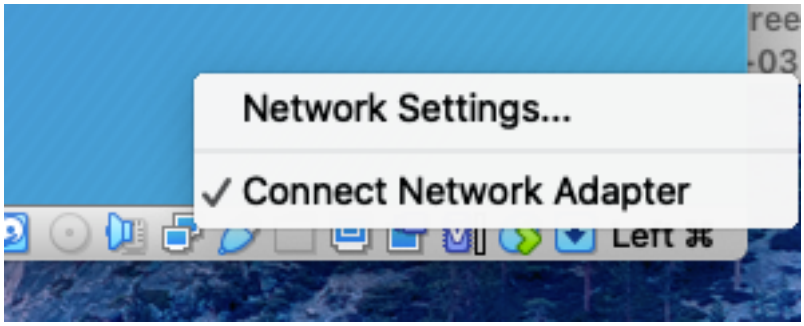
To access challenges that you need to complete open Kali VM from VirtualBox. We will use the same Kali VM that you used for Task 1.4P.

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.

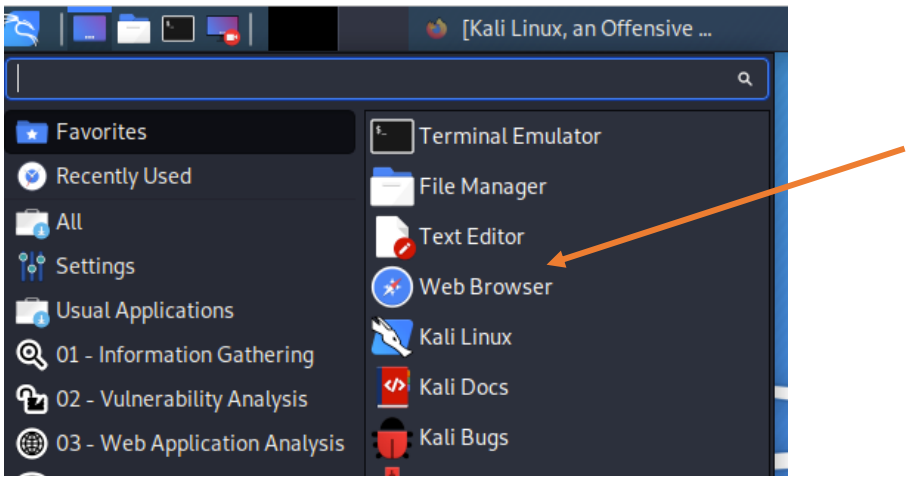
First, ensure that Kali is connected to Internet. Check the Settings of Kali VM and ensure Network Adapter is connected either through NAT or Bridged Adapter.



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. Once there, click on the link for Task 5.1P and 5.2C and provide `stuxnet' (without quotes) as password to access the tasks. You will need to complete Challenges 1, 2, and 3 for this task. All questions that you need to answer are available on the website.