WEEK 3 – TASK 3.4HD

High-Distinction Task.
Release Date: 29 March, Due Date: 15 April, End Date: 19 April.

Learning Outcomes

In this task, you will learn about penetration testing. You will learn about Ethical Hacking, Metasploit framework, Metasploitable, and will practice basic penetration testing.

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.

We are fighting the good fight. We are on the good side of the cyber world and we are in this together. We learn together and from each other.

Help is always available in SIT182. Please go to **Discussions** and ask your questions about this task in **Task 3.4HD**. 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. However, please note that pracs are primarily aimed for Pass-level tasks and tutors will only aim to provide you with suggestions about the more advanced tasks.

Note: Distinction and HD tasks are more challenging and are less guided. The only source of support for these tasks is Discussions on the unit site. Students who achieve Distinction and HD in this unit are top performers in Bachelor of Cyber. You will need to show dedication, professionalism, and ambition to complete these challenging tasks.

References: In cyber security, one of the most common referencing styles is **IEEE** – however, you are allowed to use any referencing style in this unit. Please refer to unit site > Content > Referencing - Hints & Tips for more information.

In this task, you move one step further than what you did for Task 3.3D. You are going to use Kali VM and Metasploit to target the Windows 7 VM you were provided in Task 2.1P Hence, you will need to restore Windows 7 VM to the snapshot `ready to infect' or if you don't have this snapshot, delete the VM and re-import it to VirtualBox.

Here is a guide for you to refer on and get started:
https://resources.infosecinstitute.com/topic/how-to-attack-windows-10-machine-with-metasploit-on-kali-linux/
This guide is for Windows 10 but should help you with setting up a Meterpeter on Windows 7. You do not need to make the executable undetectable. You also don't need to setup persistent access to the victim (i.e., Windows 7 VM).

Question 1: Create a screencast/screen recording (like the one for Task 3.3D) and show the steps you followed to setup Meterpeter on Windows 7 VM. In your screencast, you will need to show the commands you executed on Kali VM, Metasploitable, and the session you establish with the victim.

Question 2: Reflection point - How difficult did you find this task? Was it more challenging compared with Task 3.3D? Are you enjoying pentest activities?

This is an HD task, so there is more flexibility for tutors when assessing your skills. If you had a Windows 10 VM or Windows XP that you wanted to exploit (instead of Windows 7), they are also fine.

One of the great merits of students aiming for D and HD is their aptitude to help others – after all, we better learn together and when helping each other. Make sure you participate to Discussions on the unit site and help peers in tasks – especially, Distinction and HD tasks. Your contributions could be claimed as `something awesome' when submitting your portfolio at the end of the trimester – i.e., includes bonus point.