WEEK 2 – TASK 2.2C

Credit Task.
Release Date: 22 March, Due Date: 5 April, End Date: 12 April.

Learning Outcomes

In this task, you will learn more about malware. This task will help you practice research in the area of cyber security. This is an important skill for security engineers and when studying at university. Further, questions covered in this task are common interview questions.

Instructions

Resources

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.

⚠ **Both** questions and their sub-questions must be attempted.

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 2.2C**. 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.

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.

The following questions are common interview questions. You are expected to do research on topics and then provide a summary in your own words. You can list references you used to learn about concepts, but we are not expecting quotes as part of your answers. Word limits are indicative, and your answer could be reasonably longer, if needed.

Question 1:

Investigate about Y2K crisis. Here is a link to an academic paper entitled as "Y2K Millennial reflections on computers as infrastructure" published in 1998:

- https://d2l.deakin.edu.au/d2l/le/content/1031803/viewContent/5554026/View

Using the above paper and your own research, answer the following questions:

a) Was Y2K a malware? Support your answer with a short answer of up to 50 words (refer to Week 2's lecture).

b) Was Y2K a computer security problem? (refer to Week 1's lecture where we define what is a computer security problem) Support your answer with a short answer of up to 100 words.

c) In your own words (up to 200 words), summaries what caused Y2K.

Question 2:

Investigate about WannaCry malware. Here are two resources for you to get started:

- https://d2l.deakin.edu.au/d2l/le/content/1031803/viewContent/5554027/View
- https://d2l.deakin.edu.au/d2l/le/content/1031803/viewContent/5554028/View

Using the above publication and your own research, answer the following questions:

a) What type of malware was WannaCry? Support your answer referring to Week 2's lecture (i.e., it's X given that …)

b) Could WannaCry move across different machines? Support your answer with up to 100 words.

c) How does WannaCry ensure persistency on a machine that has infected? (i.e., what actions does WannCry take to achieve persistency on victim machine) List the tools from Task 2.1P that you could use to detect each action. (up to 200 words)

d) Is Kali Linux vulnerable to WannaCry? Support your answer by referring to characteristics of the malware as discussed in question 2.c (up to 100 words)

e) If victims paid the ransom to hackers, could they unlock their machine? (~50 words)

f) Without paying ransom to hackers, was it possible to decrypt the encrypted content of victim's machine? If so, what made that possible? (~50 words)