UNIVERSITY OF WOLLONGONG
SCIT-SIM

Final Examination

Subject: *CSIT302 Cybersecurity*
Exam Period: *10:00 am, 1 June 2020 – 10:00 am, 2 June 2020*

Instructions

Please read the following instructions carefully.

- There are 10 questions in this exam.
- You should type your answers using a word processor. **Create only one file** for your answers. ".doc", ".docx" format will be accepted. If your system can convert your file into a pdf, you are recommended to submit the pdf file (instead of the "doc" or "docx" file).
- Optionally, you can write your answers on white papers using a blue or black pen, scan them into one pdf file and submit it.
- Upload your answer file to the Moodle Final Examination section.
- No extension will be given. So please allow enough time to upload your file before the exam period ends.
- You must not consult any material other than lecture slides and tutorial notes.
- You must not consult anyone.
- You must not collaborate with your peers.
- Your answers may be examined further for possible violations of the above three rules. If the offence is detected, **you will get 0** for your final examination.

Question 1 [10 Marks]

Dave is working in a logistics company. He always brings his smartphone to his workplace and uses an official app developed by the company's IT department to scan items in the loading zone. Dave is supposed to use the company's exclusive tablet PC in which the app is installed, but he founds that it is possible to install the app on his smartphone, which, he thinks, is quite convenient. Recently, a computer guru of Dave's team (which consists of five people) discovered that by tweaking the source code of a similar app available in GitHub, he could develop a new app that does not trigger alarms often as the company's app. The team leader decided to use this new app, of course, without telling it to the company.

Discuss security problems that can arise from the above scenario according to the current threat landscape.

Question 2 [10 Marks]

Discribe what the Blue Team of the company should do if the real attack (breach of the security) happens in the company's system.

Question 3 [10 Marks]

A company has a group subscription for cloud-based word processor software, called "Sentence" for its employees, who can use it to produce and edit documents on the web browser. The company also subscribes to a cloud-based service called "DevCloud". Using this service, employees can launch virtual machines (VM)s on demand to develop the company's web service. Discuss how the company should conduct IR (Incident Response) differently for the two cloud-based service cases.

Question 4 [10 Marks]

A hacker managed to break into a bank's internal network, and by modifying the bank's digital ledger, he made the bank's million customers owe the bank 20 cents per month for a few years and made it to be transferred to the hacker's account. When the amount the hacker collected reached almost one million dollars, he wanted even more money, so he threatened the bank that he would reveal the incident. He asked the bank to pay him a half-million dollars if the bank does not want a lawsuit from many customers.

Here, the hacker is conducting two types of attacks. State what they are and explain why you have categorized so.

Question 5 [10 Marks]

Explain 1) how the PowerShell can be used to perform lateral movement 2) what benefits it can give to the attacker.

Question 6 [10 Marks]

Suppose that you want to design Active Directory for an international IT company based in Singapore, whose structure is as follows: There is a Head Quarter (HQ) in Singapore. Under the HQ, there are Software Development Department, Business Assistant Department and Quality Assurance Department. In Sydney, the company has a Regional Head Quarter (RHQ) commanded by HQ in Singapore. Under the RHQ, there are Business Assistant Department and Marketing Department.

Explain how you can form a domain tree and OUs based on the structure of the company; and discuss the trust relationship among the domains.

Question 7 [10 Marks]

State what IoC is. Give eight major IoCs and provide at least one example for each of them (the eight major IoCs).

Question 8 [10 Marks]

Suppose that you are designing a virtual local area network of your company. Your first approach was to divide resources according to the company's departments. But you encountered a problem that different departments want to access the shared resource like a file server. Discuss all the possible solutions to resolve this issue.

Question 9 [10 Marks]

Give an example of a Network Access Control (NAC) system when the company wants to restrict the type of access users will have when they are accessing the system remotely.

Question 10 [10 Marks]

Describe three steps of the Business Impact Analysis (BIA) by giving at least two examples for each step.

*********************The End of the Examination *********************