University of Glasgow

DayOfWeek DayOfMonth Month 2XXX
XX.XX am/pm – XX.XX am/pm
(Duration: 1 hours 30 minutes)

DEGREES of MSci, MEng, BEng, BSc, MA and MA (Social Sciences)

Cyber Security Fundamentals (M)

Answer All Questions

This examination paper is worth a total of 60 marks

The use of a calculator is not permitted in this examination

INSTRUCTIONS TO INVIGILATORS
Please collect all exam question papers and exam answer scripts and retain for school to collect. Candidates must not remove exam question papers.

1. Identify if the following statements are True or False. If a statement is False give a brief explanation why and correct the statement in order to gain the full mark. Every statement is worth one mark. Note: Write your answers to the provided workbook and not on the question sheet. [9 marks]

1) HTTP provides secure remote login from one computer to another.
2) Point of buying; this type of attacks targets sale and payment terminals.
3) The Application layer in a network is responsible for packaging the data in a communication.
4) Network forensics focus on the communication aspect and captures traffic for further analysis.
5) Hackers might act in a positive or negative way, but they are still criminals.
6) IP address is unique for every host and does not change upon reconnection.
7) The purpose of a firewall is to do behavioural analysis on incoming traffic.
8) In cyber security the most common strategy used for building defence in a system is called Defence in Depth.
9) Cryptanalysis is the procedure of encrypting information using a cipher.

[Total: 9 marks]

2. What are the most common goals of a cyber-attack and what type of attackers can someone encounter (at least 3 goals and 3 types of attackers by mentioning examples in order to gain full marks = 3 marks)? Give one real life example of a cyber-attack and indicate what was the goal of the attack and what type the attackers might have been (2 marks).

[Total: 5 marks]

3. a. Tom is quite concerned about the level of cyber security he has employed in his work life. He is always using a secure login, but he must transfer an important document and upload it through one of his partners' website. Can you identify and describe what protocol Tom is using for authentication and which ones he can use for this transaction? [6 marks] Is there a specific information per protocol that is important from a cyber security perspective? [2 marks]

b. Tom has a big interest in cyber security, so he is thinking of taking an Ethical Hacking/Penetration Testing course. Explain to Tom the different steps that this procedure consists of with any kind of concerns that might arise for any of them. [5 marks]

c. Tom has a friend (Arthur) working in a social media company. Arthur is aware of Tom's skills and recent training attempt and is dealing with a cyber issue in his company. Arthur was tasked with making a report about the visibility of available information of the company that can be potentially be used by malicious entities

for a cyber-attack. What techniques and tools can Tom and Arthur use and how, in order to identify and report any potential issues? [2 marks]

[Total: 15 marks]

4. Artemis is working for a big networking company as a threat hunter and is tasked with providing information on the different types that exist of DDoS (Denial of Service attacks) [6 marks], giving one example per category [6 marks], alongside with existing mitigation mechanisms for each example [3 marks]. Provide Artemis with the requested information.

[Total: 15 marks]

5. Adam wants to follow the profession of a penetration tester and understand how "malicious entities" can successfully gain access to a server by experimenting in an educational created company for testing purposes. The only information he has is the IP address of one of the servers owned by the company which is 10.5.3.12 .

a. How can Adam proceed with this information? What tools can he employ to establish a connection? [7 marks]

b. Write the code that Adam will have to use in order to exploit the server and gain access. Use one sentence explanation for the code when necessary. [7 marks]

c. After gaining access how can Adam upload a malicious file named bad.exe on the C:\Documents\ directory of the targeted server? Use one sentence explanation for the code when necessary. [2 marks]

[Total: 16 marks]