00057

Sri Lanka Institute of Information Technology

B.Sc. Honours Degree/Diploma

in

Information Technology

(Specialized in Cyber Security)

Final Examination

Year 3, Semester II (2022)

IE3022 – Applied Information Assurance

Duration: 2 Hours

November, 2022

Instructions to Candidates:

- This paper has 10 minutes of reading time followed by 2 hours for answering the questions
- This paper contains 4 questions
- Answer all questions in the booklet given.
- The entire exam is worth **100 marks** that contributes to **50%** of the final grade.
- This paper contains 5 pages, including the cover page.
- Electronic devices capable of storing and retrieving text, including calculators and mobile phones are not allowed
- Exam paper is to be collected back with the answer booklet.

Question 1 **(25 Marks)**

a. Define Enumeration

(1 marks)

b. Provide two examples of types of information obtained during enumeration?

(2 marks)

c. Create list of activities for profiling a Windows Host?

(7 marks)

d. Compare Enumeration and Reconnaissance.

(4 marks)

e. List and explain 3 important ports and services to Enumerate

(3 marks)

f. Recommend mitigation methods against Enumeration in a corporate environment.

(8 marks)

Question 2 **(25 Marks)**

a. Outline the objectives of penetration testing.

(4 marks)

b. Compare the approaches of Red Team vs Blue Team?

(5 marks)

c. Describe five activities in system hacking and criticize the importance of each activity?

(10 marks)

d. Google hacking is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using. Recommend the Google hacking query for the following.

(6 marks)

i. **Login Pages for the content management system (CMS) of Websites. -**
ii. **FTP logins . –**
iii. **Wikipedia Results which include the title "IoT" –**

Question 3 **(25 Marks)**

a. Recommend steps against Footprinting in an organization?

(5 marks)

b. What are the goals and objectives of scanning a network from an attacker's perspective.

(4 marks)

c. List three tools which can be used to scan a network.

(3 marks)

d. Case Study- Twitter Hack 2020

In mid-July 2020, the social media site Twitter had over 100 of its most prominent user accounts start to tweet requests to send Bitcoin to specified Bitcoin wallets. The requests promised that the Bitcoin senders would receive their money back doubled, as a gesture of charity amidst the COVID-19 pandemic.

The attack appears to have been carried out by a small group of hackers, leveraging social engineering to get access to internal Twitter support tools. These tools allowed the hackers to gain full control of the high-profile user accounts and post messages on their behalf. The attack provides many paths for investigation into the prevention, response, and impacts of cybersecurity breaches

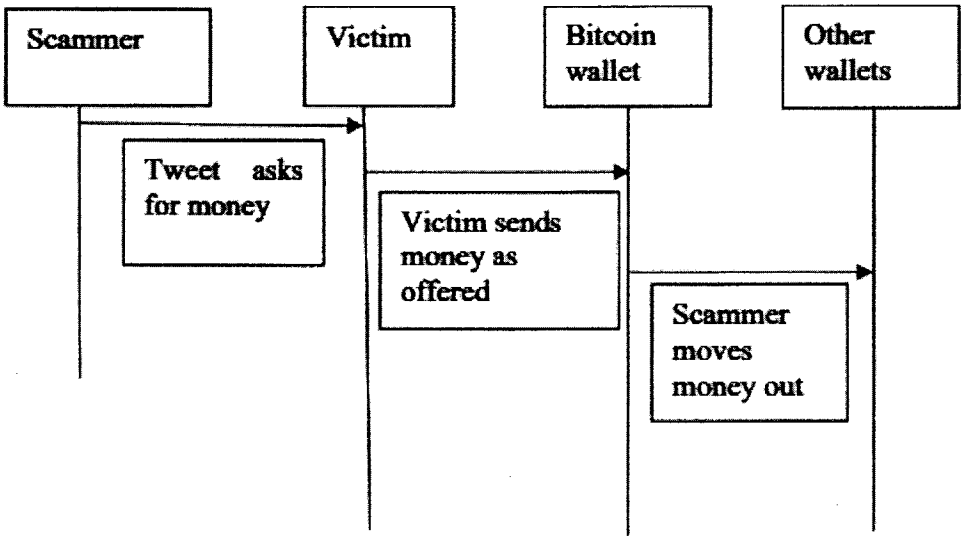

Figure 01

i. Name two assets affected by this attack.

(2 marks)

ii. What are some examples of best practices Twitter could have used to detect this problem early?

(3 marks)

iii. Was this attack a result of a people issue, a technology issue, or some of both?

(4 marks)

e. Assess the importance of obtaining necessary authorization prior to a penetration testing?

(4 marks)

Question 4 **(25 Marks)**

a) Explain what an exploit is and how it works in the context of Metasploit?

(5 marks)

b) Name an opensource scanning tool embedded in Metasploit.

(1 Marks)

c) Compile the steps in finding the right exploit module in Metasploit for your target exploitation?

(3 Marks)

d) What are the possible results of a stack overflow condition in a system?

(3 Marks)

e) Name the three types of SQL injection attacks.

(3 Marks)

f) Interpret the following SQL statements.

i. SELECT * FROM Products WHERE product_id = 20; DROP TABLE Products;
ii. SELECT * FROM Users WHERE username = "invalid_user" OR "1"="1" AND password = "invalid_pass" OR "1"="1"

(10 Marks)

End of the Question Paper