Sri Lanka Institute of Information Technology

B.Sc. Special Honours Degree in Information Technology

Final Examination
Year 3, Semester I (2019)

IE3022 – Applied Information Assurance

Duration: 3 Hours

October, 2019

Instructions to Candidates:

- This paper has **4** questions with a total of 100 marks.
- Answer all the questions in the booklet given.
- This paper contains **4 pages** including the cover page and annexure.
- This is an open book examination.

Question 1 (25 Marks)

a) Security compliance requires organizations exercise due diligence and due care in providing information security and risk management. Identify type of a **role Ethical Hacking plays** in the context? (5 marks)

b) Name and briefly explain 7 stages in the "**Cyber Kill Chain**". (7 marks)

c) Describe the following terms; (8 marks)

i. Footprinting

ii. Reconnaissance

iii. Competitive intelligence

iv. Google Hacking

d) Differentiate **5 best practices** to defend against reconnaissance. (5 marks)

Question 2 (25 Marks)

a) Briefly describe the **three types of Distributed DoS** attacks. (3 marks)

b) Analyze DDos attack **statistics and impact characterization** on Cloud environment. (9 marks)

c) Compose a **taxonomy for DDoS solutions**, which contains attack prevention, detection, mitigation and recovery. (10 marks)

d) Briefly describe the following terms. (3 marks)

i. Blacklisting / whitelisting

ii. Rate limiting

iii. Blackhole routing

Question 3 (25 Marks)

A) Discuss how digital forensics is different from data recovery. (5 marks)

B) Explain why **validation** is considered the most critical aspect of digital forensics. (5 marks)

C) Access the **IE3022** folder provided in the **Desktop** and navigate to **Q3** folder. Use the picture (**IMG_4735.JPG**) provided and using the tool (**ExifRead.exe**) extract the metadata component of the figure. Using the meta data information extracted answer the following questions.

i. Name the **Maker** and **Model** of the camera that took the photo? (2 marks)

ii. Name is the **Date** and **Time** that the picture was taken? (2 marks)

iii. Discover the following points of the picture. (7 marks)

a) Degrees

b) Minutes

c) Seconds

d) North Reference Point

e) South Reference Point

f) West Reference Point

g) East Reference Point

D) Criticize **challenges faced by the forensic investigators** in investigation process.

(4 marks)

Question 4 (25 Marks)

A) *"SQL Injection is an attack that poisons dynamic SQL statements to comment out certain parts of the statement or appending a condition that will always be true."*

i. Is the above statement true or false? (1 mark)

ii. Justify your answer in part i). (3 marks)

E) Use the instructions provided in **ANNEXURE I** and run the live-virtual machine. With the use of the machine answer the following questions.

i. Modify the URL of **Example 3** link in the **XSS** section to obtain a message box indicating a message ***"Congratulations you are the 100th winner!!!".***

(4 marks)

ii. Modify the URL of **Example 5** link in the **XSS** section to obtain a message box asking for a username and a password. (4 marks)

iii. Use the **Example 1** link in the **SQL** section to answer the following questions

a) Analyze the URL and explain how the query can be used to view all the user information. (3 marks)

b) Construct an SQL injection query calculate the number of columns in the user table. (4 marks)

c) Construct an SQL injection query to retrieve the root password.

(6 marks)

~ End of Examination Paper ~

Annexure I

Septs to configure and startup the virtual machine

1. Open **VMware Workstation**
2. Create a new virtual machine using **LINUX** type and select a **Debian-8-64-bit** operating systems.
3. Navigate to the **Virtual Machine Settings** and select the **CD/DVD** attachment option
4. Click on **Browse** and navigate to the following location
   /Desktop/IE3022/Q4
5. Select the **web_for_pentester_i386.iso** file
6. Run the virtual machine
7. Issue **ifconfig** in the command line and get the IPv4 address.
8. Use the **Chrome browser** and enter the IP address.

Optional

1. If you do not get an IP address.
2. Shutdown the virtual machine
3. Open the **Virtual Machine Settings**.
4. Navigate to **Network Adapter**
5. Select the **NAT** network option
6. Boot up the virtual machine and get the IP address.
7. Use the **Chrome browser** and enter the IP address.