Sri Lanka Institute of Information Technology

B.Sc. Honours Degree in Information Technology

Specialized in Cyber Security

Final Examination
Year 2, Semester 1 (2019)

IE2012 – Systems Administration and Network Programming

Duration: 2 Hours

October 2019

Instructions to Candidates:

- 10 minutes reading time provided
- This paper has four questions.
- Answer all questions in the booklet given.
- The total marks for the paper is 100.
- This paper contains 05 pages, including the cover page.
- Electronic devices capable of storing and retrieving text, including calculators and mobile phones are not allowed.

Question 1 **[25 marks]**

a). Explain importance of information gathering in penetration testing process.

(5 marks)

b). Compare and contrast passive and active information gathering techniques.

(4 marks)

c). What is google hacking, Explain with few examples.

(5 marks)

d). Discuss the importance of the **Nmap** command

(2 marks)

e). Explain the following commands with a suitable example.

i). root@kali:~#nmap **-sS** 192.168.1.0/28

ii) root@kali:~#nmap **-sU** 192.168.1.1/28

iii) root@kali:~#nmap **-O** 192.168.1.1/28

(6 marks)

f). Briefly explain the usage of CVE and CVSS Systems

(3 marks)

Question 2 [25 marks]

a) Describe the importance of secure shell connection that used in bandit war game.

[5 marks]

b) Select five commands from below list and write short description.

find, du, grep, touch, file, sort, tar

[5 marks]

c) What is the correct command to identify the password that is stored in the **one of the few human-readable strings, beginning with several '=' character** in a directory?

[5 marks]

d) Explain the following commands with a suitable example.

i) find . -type f -readable ! -executable -size 1033c

ii) cat data.txt | tr [a-zA-Z] [n-za-mN-ZA-M] [5 marks]

e). Identify the correct commands to get the password from below given scenario.

The password for the next level is stored **somewhere on the server** and has all the following properties.

owned by user bandit7

owned by group bandit6

33 bytes in size

[5 marks]

Question 3 **[25 marks]**

a) What is the need of SSL certificate?

[5 marks]

b) How does SSL work? Use a diagram to explain.

[5 marks]

c) Assume you need to setup SSL on your website, explain the procedure?

[5 marks]

d) How does the web site visitor going to know that the web site is using SSL?

[5 marks]

e) Compare and contrast Self-signed certificate with CA certificate?

[5 marks]

Question 4 **[25 marks]**

a). In Linux system specific user ID numbers and ranges are used for specific reasons. Give a specific user ID number or a range of numbers for the following users?

a. Super user
b. System users
c. Regular users

[5 marks]

b). /etc/passwd is a text file that contains the attributes of (i.e., basic information about) each user or account on a computer running Linux. Name those 7 attributes that are represented by 7 colon delimited fields?

[5 marks]

c). In **/etc/shadow** file, 2nd attribute represents the password. This password section contains three pieces of information. What are those?

[5 marks]

d). Compare **/etc/passwd** file with **/etc/shadow** file?

[5 marks]

f) Why we use a salt value when hashing a password?

[5 marks]

--END OF PAPER--