December 02, from 2:15PM - 5:15PM

Question **1**

Not yet answered

Marked out of 60.00

Final Exam

INSTRUCTION:
- Type your answers into a word file (best 12pt) and convert to PDF for submission. We accept only PDF file.
- Write your name and student ID on your submission.
- Submit only ONE PDF file for all questions.

Part A: 16 questions worth 1 mark each (Total 16 Marks)

For each of the following questions you should provide a brief solution to fill in the gap or gaps. The size of gap does not generally indicate the size of an appropriate answer. In cases where the answer could be an abbreviation you need to give the full name for full marks. If you cannot think of a concise answer you can write more and still get full marks.

1) Two common authentication bases are_____and_____.

2) The common resources that can be targeted in DoS attacks are _____.

3) In multilevel access control every subject or object is given _____.

4) Canary values are used to protect against _____ by _____.

5) Lamport's one-time password scheme relies on using hash functions that are _____.

6) Two classes of intruder that an intrusion detection system may attempt to find are _____ and _____.

7) A master password is typically used to protect _____.

8) _____ is capable of distinguishing between humans and computers.

9) Data aging in the context of intrusion detection systems relates to ensuring that _____.

10) Phishing emails are typically sent in bulk because _____.

11) The Biba model is for the purpose of _____, while BLP is for the purpose of _____.

12) Inference is the derivation of _____from _____.

13) "Online" and "offline" attacks differ in that _____.

14) The term "shellcode" refers to _____ in the context of _____.

15) XSS stands for _____.

16) The purpose of sanitization in the context of auditing is to _____.

Part B: 7 questions worth 2 mark each (Total 14 Marks)

1) Describe the difference(s) between an authenticated user and an authorised user.

2) Describe three distinct types of attacks against password systems. Briefly discuss appropriate countermeasures against one of those types of attacks.

3) Explain two outcomes an attacker may aim for with a Buffer overflow attack. Sketch how and why a Buffer overflow attack works. You do not need to write code but can if it helps you to explain.

4) Explain what salting is, where we use it, and why we use it.

5) Briefly describe how an encrypted virus works.

6) Describe two primary properties used in malware classification and two distinct methods of identifying a virus.

7) Describe how honeypots can be used in an intrusion detection system.

Part C: 5 questions worth 6 marks each. (Total 30 Marks)

1. The following questions relate to authentication:

a. Explain how Unix protects user passwords. (2 marks)

b. Which of the following two methods of generating a password is better? Justify your answer. In every instance the choosing is uniformly random. (1 mark)

A: Choosing a six digit number.

B: Choosing a letter (upper or lower case), followed by two digits, followed by a lower case letter, followed by one digit then by the symbol *.

c. Name and describe the two types of error that occur in authentication systems. (1 mark)

d. Sketch an example of a one-time password system. (2 marks)

2. The following questions relate to access control:

Consider the following statements and answer the subsequent questions:

Alice can climb trees and push walls.

Bob can climb trees, push doors and jump fences.

Chris can push Alice, open doors and climb walls.

a. Draw an access control matrix for this scenario. (2 mark)

b. Name and give an example of each of the list representations corresponding to the access control matrix. (2 mark)

c. If we want to efficiently determine all the actions available to an object, which of the two list representations is appropriate and why? (1 mark)

d. Use an example to describe Attribute-based Access Control. (1 mark)

3. Consider the diagram to the right and answer the following questions:

a. What is the context of this diagram? (1 mark)

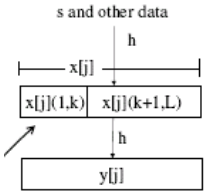
b. What is h? (1 mark)

c. What is sent to the client? (1 mark)

d. What should the client respond with? (1 mark)

e. How much work would we expect the client to do? (1 mark)

f. Is the answer from the client unique? Justify your answer.(1 mark)



4. These questions relate to intrusion detection systems and firewalls:

a. Describe the major components in an IDS and the job of each component. (1.5 marks)

b. Describe three different types of firewalls and their functionalities. (1.5 marks)

c. Describe the screened subnet firewall architecture. (2 marks)

d. Describe two types of threat a firewall cannot protect against. (1 mark)

5. These questions relate to a variety of topics:

a. In the labs for this subject various methods were used to unlock the exercises. Describe four of the methods used. (2 marks)

b. What is a statistical database? Why do we use a statistical database? (1 mark)

c. Describe two methods than can be used to provide protection against statistical inference. (1 mark)

d. Describe how Syncookie works in preventing TCP SYN Flooding attacks. (1 mark)

e. Picture-in-picture attacks and homograph attacks are two classes of phishing attack. Briefly describe each. (1 mark)

Maximum file size: 200MB, maximum number of files: 1

Files

Accepted file types

PDF document .pdf