Nova Southeastern University
College of Computing and Engineering

Assignment 1

ISEC 660 Advanced Network Security

Winter 2021
Due date: 1/24/2021
Total Points: 100

Notes:
1. Please include your name in EVERY document you submit.
2. Please sign and submit the "Certification of Authorship" form (located in Canvas) along with your solutions.

Section I. Textbook Reading

Chapter 1, Chapter 3, Chapter 4, Chapter 5, Chapter 6, Chapter 7

Section II. Questions (80 points, all questions are equally weighted)

Q1. Explain the following basic security principles: fail-safe default, complete mediation, open design, separation of privilege, least privilege, isolation, defense in depth (layering). (Chapter 1)

Q2. In section 1.5, the textbook shows three areas of network attack surface: enterprise network, wide-area network, and the Internet. Show an example of each of these attack surfaces. (Chapter 1)

Q3. Describe the general concept of a challenge-response protocol. (Chapter 3)

Q4. Assume passwords are selected from four-character combinations of 26 alphabetic characters. Assume an adversary is able to attempt passwords at a rate of one per second.
a. Assuming no feedback to the adversary until each attempt has been completed, what is the expected time to discover the correct password? (Chapter 3)

b. Assuming feedback to the adversary flagging an error as each incorrect character is entered, what is the expected time to discover the correct password?

Q5. Briefly define the difference between DAC and MAC. (Chapter 4)

Q6. For the DAC model discussed in Section 4.3, an alternative representation of the protection state is a directed graph. Each subject and each object in the protection state is represented by a node (a single node is used for each entity that is both subject and object) A directed line from a subject to an object indicates an access right, and the label on the link defines the access right.
a) draw a directed graph that corresponds to the access matrix of Figure 4.2a
b) Is there a one-to-one correspondence between the directed graph representation and the access

matrix representation? Explain. (Chapter 4)

Q7. Explain the nature of the inference threat to an RDBMS. (Chapter 5)

Q8. What are the disadvantages of database encryption? (Chapter 5)

Q9. What mechanisms can a virus use to conceal itself? (Chapter 6)

Q10. What is the difference between a backdoor, a bot, a keylogger, spyware, and a rootkit? Can they all be present in the same malware? (Chapter 6)

Q11. Define a distributed denial-of-service (DDoS) attack. (Chapter 7)

Q12. What defenses are possible against TCP SYN spoofing attacks? (Chapter 7)

Section III. Article summary (20 points)

Please read the article “Security Controls for Computer Systems” at the following URL.

http://www.rand.org/pubs/reports/R609-1/index2.html

especially section " IV. AREAS OF SECURITY PROTECTION". Answer the following questions.

1. What are the categories of “leaking points” and why are they different?

2. Please give 1-2 case studies – either hypothetical or real-world cases that belong to “communication leaking point”. What are the possible ways to mitigate the leading point you choose? Elaborate your answer.

Note that your answer should not simply be a high-level review based solely on the RAND report – try to go deep into the technical details and refer to external materials. Answer to these two questions should at least be a 1-page single-spaced document. I would appreciate your critical thoughts on these questions. For external resources, please include a list of references, and use the APA format for citations and references where appropriate.

For APA formatting requirements, please refer to https://nsufl.libguides.com/writing/apa.