Southern Methodist University

CS7349/Data and Network Security

Exam #2

5 essay questions (20 points each)

This document contains the questions for the exam. For your answers, create a pdf document that clearly identifies every question number and your answer to that question. Name the file containing your answers 'yourLastNameCS7349Exam1.pdf'. For example, the file for Shaibal Chakrabarty would have the name ChakrabartyCS7349Exam1.pdf. Submit your pdf file.

Answer each question fully and completely. The highlighted words are your response guide – missing them will result in points deduction. Show all of your work and state your assumptions where appropriate. The questions may have 'hints' embedded within them regarding the answer. Treat these as directions. Follow these hints as appropriate for full points.

Collaboration is expected and encouraged; however, each student must hand in their own exam. To the greatest extent possible, answers should NOT be copied but, instead, should be written in your own words. Copying answers from anywhere is plagiarism, this includes copying text directly from the textbook. Any copied answers, identical answers to other students in the course (past or present) or otherwise plagiarized answers will receive a grade of zero. More than one plagiarized answer will result in a grade of 'F' for the exam with zero points earned and the procedure for academic dishonesty will be initiated. Do not copy answers. Always use your own words. Directly under each question list all persons with whom you collaborated and list all resources used in arriving at your answer. Resources include but are not limited to the textbook used for this course, papers read on the topic, class presentations and Google search results. Note that Google is not a reference. It is a tool to find references. Don't forget to place your name in the document itself.

ALWAYS provide references, your collaborators, and submit your answers in the format of the questions, in a .pdf file. Write the question and provide the answer in the same order (numbering) as the question. Font style, type and line spacing should be the same as these intructions.

1. Kerberos is an authentication service that is often used to allow a user to gain access to a computer that is connected to the network or to establish a secure communication channel. In a MINIMUM of 1 page, explain how Kerberos works, explain why Kerberos is secure, and draw a figure that illustrates the steps involved to using Kerberos to authenticate two systems to one another while establishing a secure communication channel (where the secure communication channel uses a shared secret key). Be sure to explain each step in this symmetric session key establishment protocol.

2. Kerberos provides user authentication. The broader service in Information Security is referred to as Identity and Access Management (IAM). This is a critical service for all companies and deals with (simply put) your ability to login to the corporate network and access certain services. There are trends in IAM on-going due to multiple factors.

    a. IAM Trends/services:
        i. ITDR – Identity Threat Detection and Response
        ii. CIAM and EIAM: (Customer Identity and Access Management vs EIAM - Employee Identity and Access Management)
        iii. Passwordless Authentication (Hint: please refer to FIDO and FIDO2 standards, and include in your answers)
        iv. IGA (Identity Governance and Administration) and PAM (Privileged Access Management)
        v. Zero Trust IAM

    b. In a MINIMUM of 1 page with a diagram and/or table, please discuss the following IAM services, answering the following questions, for EACH trend:
        i. Description of the service/technology/standard
        ii. How does it differentiate from existing technology? Why was it necessary? (Hint: to improve efficiency, handle new attack vector, etc; Hint: Use a table to compare the existing with the new/add-on)
        iii. Top 2 vendors and their value proposition
        iv. Loaded question: Based on your own experience, do you think SMU uses this IAM service? Explain your answer.

    c. Note/Clarification: For EACH IAM Trend/Service in 2a, write a MINIMUM of 1 page, answering the questions of 2b. (Total 5 pages MINIMUM)

3. In a MINIMUM of 1 page, explain how a public key cipher is typically used to provide a digital signature and explain how a user is able to authenticate a signature to verify that it came from a known individual. Be sure to include a description of how the user is able to determine the identity of the individual to whom the public key in the public key cipher is associated. Illustrate (Hint: picture) how a digital signature is used within a commonly used network communication protocol or security service. Be sure to identify the protocol or service.

4. The Border Gateway Protocol (BGP) is used for routing packets between Internet Service Providers (ISPs). BGP routers from each ISP communicate with one another exchanging information such as the IP addresses that are serviced within the ISP. In a MINIMUM of

1 page, explain how BGP operates, and explain how this operation may be exploited by an adversary to allow the adversary to cause all packets destined for a particular IP address that is not serviced within the ISP to flow through that ISP. Identify and discuss at least one news article published recently that discusses victims of this type of attack.

5. Understanding the threat environment is critical to protecting your IT infrastructure. There are insider and outsider threats. Insider threats can be extremely damaging for exfiltrating intellectual property and sabotaging a company. You suspect someone is stealing information within your company and causing the competition to gain market share. Please find 2 companies that provide counterintelligence services to find this 'mole' inside your company.
    a. Write 1/2 page description for the services of EACH company that will help you. Total 1-page. Hint: The companies will have case studies on their websites that you can use.

    As the heat is turned on, you suspect, that external physical/cyber threats will be used to distract you from searching for this mole. Your data center, housing your IT infrastructure will be bombed. To counter this threat, you contract IBMs (or some other company) Business Continuity and Resiliency services.

    b. Write 1-page on what services IBM/other BC and Resiliency services will provide + how long the migration will take to get your network resilient. Hint: Approximate calculations will suffice – migrate 100 servers, 1000 end points, 10 enterprise applications, etc.
    c. Create a 1-page table of mitigations for the following cyberthreats, that will be unleashed on you to prevent the mole from getting caught. Explain the threat, and provide 1 threat mitigation resource (a software package, a service, a product, a configuration):
        i. RAT (Remote Access Trojan)
        ii. BotNets (Hint: look at various mutations of Mirae botnet, or any others)
        iii. Worms
        iv. Ransomware
        v. DDoS

    Hint: Create the table, with 3 columns. In the 1st column, write each threat and describe it in 3-5 lines. In the 2nd column put down the mitigation(s) of that threat, as mentioned above (a software package, a service, a product, a configuration). In the 3rd column you may give an example, write additional notes or leave it blank. Hint: Grading is always relative.