Name: _____

CSci 530 Final Exam
Fall 2021

This exam is open book and open note. You may use electronic devices to consult materials stored on the devices, but you may not use them to access material through the net, or for communication during the 120 minutes in which you are completing the exam. You have **120 minutes** to complete the exam. You must submit the completed exam through the DEN drop box for CSci530 before 130 minutes from the start of the exam. (the extra 10 minutes is to provide time to logistically upload the exam and you may not use additional time to complete the answers).

Type your answers in the exam itself using word, or if you prefer a different editor using the text version of the exam that is provided. The filled-out exam document will be what you will return to me as described above. In answering the questions, please TYPE your answers rather than importing large quantities of text using cut and paste in hopes that the cut and pasted text might include an answer**. Pasted text in your responses will be ignored and you will not receive credit for words included in the pasted text.**

Be sure to include your **name in the exam document. Ideally, please rename the document to a file name that includes your name (e.g. csci530-f21-final-FIRSTNAME-LASTNAME).**

To judge the amount of time you can spend on each question, consider that you have 120 minutes and there are 100 points across the 3 questions.

There are **100 points** in all and **3 questions.**

	Q1	Q2	Q3		Total Score
Score					

Complete the following statement:

I, **(replace with your first and last name)** attest to the fact that I completed this exam within the designated time allocated (e.g. in less than 120 minutes), that I did not have knowledge of the exam or answers in advance of its start, that I did not access external material (e.g. web sites) or use the internet during completion of the exam, and that I completed the exam on my own without accepting or providing assistance to anyone else.

Signed: (type you name here). Date: 12/13/2021.

Name: _____

1. **(25 points) How do we fix that?**

   For each of the following problems listed in the lettered list below, note the solution/technique/part of the system that might be at least partially instrumental in solving the problem. To put this in other terms for the first problem: if you want to solve (problem a), which of the techniques or system components (1-8) might you apply or modify to solve the problem.

   This is not a one-to-one mapping; more than approach may apply (separately or in combination with others) in solving the lettered problem. We are looking for specific matches for which you will receive credit. If you list a match that we are not looking for, but which is still correct, while you will not lose credit, you will not get credit either. You will lose a point if you list an approach or component that would not be effective.

   1. Intrusion Detection Systems (Other than Signature Based)
   2. Strong Authentication Technologies
   3. Trusted Computing (or a trusted platform module)
   4. Access control mechanisms (Authorization)
   5. Firewalls
   6. Encryption
   7. Cryptographic Hash Functions
   8. A well thought out containment architecture.

[Type the corresponding numbers above, separated by commas following the lettered entries below]

a) Subversion (modification of installed hardware or software)

b) Disclosure of data (e.g. a Data Breach):

c) Denial of Service (attack against availability):

d) Zero Day Exploit:

e) Man in the Middle Attack:

f) Unauthorized Modification of Data:

Name: _____

2. (45 points) Short and medium length answers

a. **Trusted Platform Module (TPM)** – In what way is the TPM similar to a smartcard? Specifically, what capabilities does it have in common with a smartcard? What capabilities does the TPM have that go beyond the capabilities of a smartcard? Explain also how the storage root key (SRK) is used by the TPM to protect content on a computer. (10 points)
(type your answer here)

b. **DNS Security –** How are the ZSK and the KSK used in DNS Security. Specifically, what are the ZSK and KSK (their full names)? What is each used to protect? Specifically, are they used to protect confidentiality or integrity, and describe the data that each protects. (10 points)
(type your answer here)

c. **IPSec** – What is the difference between the SADB and the SPD in IPSec implementations? What do the records correspond to? What data is contained in each record and how is this data used when setting up a connection and/or sending and receiving application data between endpoints? (10 points)
(type your answer here)

d. Intrusion Detection – Modern intrusion detection systems (often referred to as Security Incident Event Management (SIEM) systems) are distributed in nature. What do we mean when we describe the system as distributed, and what are the advantages (and the reason for those advantages) of such systems over standalone (monolithic) host or network based intrusion detection systems. In answering this question be sure to discuss at least the nature of the data collected, false positive and negative rates, and the security of the intrusion detection system itself. (15 points)
(type your answer here)

Name: _____

3. (30 points) Impact of major vulnerabilities

Many recent security attacks involve an attack vector where a system or server in your organization downloads malicious code from a computer elsewhere on the internet and starts running that code (payload). This was the case with the SolarWinds breach, where the software was downloaded as part of a software patch. This is also the case with Apache Log4j library which can be manipulated by logged data in user provided input fields to connect to a remote server, download java modules and execute them locally, with the privileges of the server that generates the log entry.

There are many approaches covered in CSci530 that can help us limit the reach of such attacks by reducing the attack surface, by limiting the data that is reachable by the impacted system components, by reducing lateral movement by the adversary once they achieve their initial exploit, and by detecting such exploits while the attack is still in progress.

In answering the questions that follow, you may assume that you are working for a bank, and that the bank provides a website that is reachable by customers through the open internet. The bank has additional computer systems beyond those that are reachable by customers. You may state any additional assumptions you choose to make.

a. Firewall Containment – Firewalls are often used to implement a containment architecture. As typically deployed firewalls limit inbound connections to a network or system. This kind firewall policy would likely NOT be effective against this kind of initial attack vector (in either of the two examples). However, certain more strict policies might be effective. Suggest some firewall policies that could be applied in your system that might be more effective against these kinds of attacks. (10 points)
(type your answer here)

b. **Containment Architecture and least privelege –** Describe how an effective containment architecture including and as well as the implementation of least-privilege principles could potentially limit the data reachable by the impacted system components. Describe the different domains in your containment architecture. What communication might be allowed across domains, and how those rules limit lateral movement by the adversary once they achieve their initial exploit? How do these rules make it more difficult for an adversary to exfiltrate data from a system that has been compromised? What is a simple step that should be implemented on your servers to better implement the concept of least privilege? (10 points)
(type your answer here)

c. **Intrusion Detection** – What data should be collected by an intrusion detection system (or SIEM) to best detect the initial exploit, lateral movement, or exfiltration of data from the kinds of attacks just described? Where would each kind of data you described be most readily collected? For each, would this be a host based, application based, or network-based sensor? Describe several specific activities, that if detected, might be an indicator that an intrusion is in progress? (10 points)
(type your answer here)