Question 1

4 / 4 pts

Match the Threat Model steps with the description.

Determine which problem is most severe.	Rank threats.
Make a plan for addressing problems.	Decide how to respond.
Determine how data flows through the program.	Decompose the system.
Get access to all the necessary code and documentation.	Assemble the resources.
Find problems in critical areas.	Identify threats.
Fix the problems.	Mitigate

Question 2

3 / 3 pts

Order the steps in the threat modeling process.

Decompose the system.	2.
Rank each threat according to the risks.	4.
Determine how to respond to each threat.	5.
Identify the threats to the system.	3.
Mitigate the threats.	6.
Assemble the necessary resources.	1.

Question 3

5 / 5 pts

Match the data flow diagram symbol with its name.

A dotted line: - - - - - - -	A trust boundary.
An arrow: _____\/	Movement and format of the
A circle with text in it	Process, something that trans
Text in a box: +----------+| Text |+----------+	Interactors.
Text with a line above and below it: ---------- Text ----------	Storage.

Question 4

5 / 5 pts

Which of the following are the rules for data flow diagrams?

- [ ] All interactors must exist outside the outermost trust boundary.
- [x] Data stores connect to processes with data flow, they cannot connect together.
- [ ] There is one trust boundary for each process.
- [x] Data flow names, external entities, and data store items are nouns.
- [x] Process names are verbs with nouns.
- [x] All data flow must start and stop at a process or an interactor.
- [ ] Each process must change the composition or format of the data flow.
- [x] Processes must have at least one data flow entering and one data flow exiting.

Question 5

1 / 1 pts

How do you determine the severity of a threat?

- ( ) Ask an expert to rank the threats.
- (•) Score each threat using the DREAD system.
- ( ) Threats with the greatest damage potential are the most important.
- ( ) Rank the threats using the STRIDE system.

Question 6

1 / 1 pts

What does it mean if the E score of DREAD is a 6?

- ( ) Absolutely no effort is required to exploit this vulnerability.
- ( ) The worst case scenario is a significant disruption of service or the compromised asset does not play a key role.
- (•) The exploit requires the services of a skilled cracker or someone with inside information.
- ( ) If the exploit is known, there is only a 60% chance that it will work on a given attempt.

Question 7

5 / 5 pts

For each example threat, identify the threat type illustrated:

After having broke into my teacher's office, I wiped my fingerprints from all the surfaces.	Repudiation
I was unprepared for the in-lab test today so I disabled all the machines in the Linux lab with a hammer.	Denial of Service
I have obtained the grader's password and have logged in as him.	Spoofing
I changed the file permissions on the professor's answer key so anyone can view the contents.	Information disclosure
I have intercepted the packets leaving my teacher's computer and altered them to reflect the grade I wish I earned.	Tampering
The teacher left himself logged in on I-Learn so I changed my role from "student" to "grader."	Elevation of Privilege