Kenneth Woodard

CS 366

Written Assignment 1

Question 1

- a website that allows consumers to order products with their credit/debit card

  A. Hackers that want to steal money from people.

  B. They could steal information from the company, such as payment information or intellectual property.

  C. If the website uses an SQL database, the hackers might try SQL injection. Another possibility could be a DDoS attack. This is when typically a smaller site is attacked by a wave of bots that overwhelms the website with traffic. Both of these can expose the business's and the customers' information.

- a social media website that allows anyone to sign-up and post content

  A. Attackers would want to steal the user's information, such as passwords, date of birth, email address, and other private information. They could also be attacks from people you know trying to ruin your reputation.

  B. Armed with this personal data, hackers could try to take over you account to spread malware or spam messages. They could also try to take over other accounts you have on other sites. Linked accounts would be more exposed.

  C. One vulnerability that hackers would explore are the linked accounts. Gaining access to one can help them gain access to others. Another vulnerability they might want to exploit is gaining access to friends' information after gaining control of one account.

- an internet-connected thermostat that allows electric utility operators to adjust temperatures to regulate power supply based on demand

    A. The Russian hackers could want to attack our electric utility system, for example.

    B. The harm they could cause is shutting down the system; and therefore, disrupting the power supply. They could also being trying to steal information about our power grid system, so that they can attack it in the future or use it for themselves.

    C. They might exploit the fact that some of these fancy thermostats run on linux. The fact that it is connected to the internet is the biggest vulnerability.

<u>Question 2</u>

The security goals for this situation should include keeping the laptop under password lock at all times as well as encrypting the file that contains this information. Reasonable attacks would include students trying to steal information such as exam answers and trying to modify their own grades in the system. We probably shouldn't worry too much about outside hackers trying to steal the students' information.

If I was the teacher, I would keep all the information regarding the course offline and encrypted, and I would make my laptop require a passcode each time it is opened. The net risk reduction would be more for keeping the files encrypted, then it would be for keeping a password on your laptop. If your laptop is stolen, hackers can and will get around your password and into your computer. I should also mention that neither of these options are very costly.

<u>Question 3</u>

A. $result = ‘last -1000 | grep $username_to_look_for’; is the vulnerable line of code here. If the attacker input “;rm -rf /” instead of a username, the program would execute that system call. The solution would be to build a list of the recent usernames and then use that to check instead of calling on the operating system.

B. Using race conditions, you can make one of the instances of the program get beyond the I-node checking if statements despite having invalid input. The first instance can get around the if statements by having the second instance run with a valid pathname while the first instance uses pathname = “what/ever”. If the second instance executes the statement stat(pathname) before the first instance checks, then it will pass through. The pathname is still “what/ever” for the first instance even though we = f. Then, this happens in the same way for the second check. The second instance switches the stat struct back to whatever the valid values were before the first instance can fail the if statement and quit running. Finally, it writes the contents from “what/ever” to the file descriptor.