Seth Lunders

Professor Song

CS336 HW #1

3 September 21

1. Distinguish between vulnerability, threat, and control.
    a. A vulnerability is a weakness in the system. A threat is a situation that has the potential to cause loss or harm to assets by exploiting a vulnerability in the system (maliciously or inadvertently). A control is something put in the system to prevent threats from exploiting vulnerabilities.
2. Give 3 examples of violation of availability, 3 examples of violation of confidentiality, and 3 examples of violation of integrity.
    a. Violation of availability:
        i. denial of service attack - overwhelming a server with requests
        ii. power outage
        iii. wireless signal jammer
    b. Violation of confidentiality
        i. using stolen keycard to access a building
        ii. releasing secret company data to the public
        iii. violation of something like FERPA
    c. Violation of integrity
        i. fire burns down building that houses data servers
        ii. student breaking in to grading system to change their grades
        iii. someone inserting malicious code into source code
3. Describe a situation in which you have experienced harm as a consequence of a failure of computer security. Was the failure malicious or not? Did the attack target you specifically or was it general and you were the unfortunate victim?
    a. In 2019 the website Canva had a data breach exposing emails, usernames, and names of users, as well as some hashes of passwords. I think the failure was

malicious. The target was not me specifically, but all of the users of this service.

4. Consider a program to display on your website your city’s current time and temperature.
    a. Who might want to attack your program? What types of harm might they want to cause?
        i. Not a lot is coming to mind for this. Maybe someone would try to shut it down and ask for money to get it working again.
    b. What kinds of vulnerabilities might they exploit to cause harm?
        i. Maybe a denial of service attack, sending so many requests the server can’t handle it. I imagine if I made a site like this it would probably be hosted on a small virtual server, which would probably be relatively easy to overwhelm.
5. Consider a program that allows consumers to order products from the web.
    a. Who might want to attack the program? What types of harm might they want to cause?
        i. Someone who wants money might do this, or maybe they just want to get your product without paying. They may want to make it look like they paid for products, and therefore get you to ship them things for free. They may also want to steal things such as user’s login info, shipping/billing location, or even credit card info if possible.
    b. What kinds of vulnerabilities might they exploit to cause harm?
        i. If the server is poorly secured (bad password, no multi-factor authentication) they may be able to brute-force guessing the password in a relatively short time.
        ii. They could pose as a legitimate user and get their password reset to something else. They could also make a site that looked like yours to get users’ logins.