Chapter 8 - Cloud Computing

**1. Explain the differences between public, private, and community clouds. What**

**are some of the factors to consider when choosing which of the three to use?**

**2. How do cloud threats differ from traditional threats? Against what threats are**

**cloud services typically more effective than local ones?**

**3. You are opening an online store in a cloud environment. What are three**

**security controls you might use to protect customers’ credit card information?**

**Assume that the information will need to be stored.**

**4. Define TNO. Name three types of data for which one should want TNO**

**encryption.**

**5. How do cloud services make DLP more difficult? How can customers**

**wishing to enforce DLP mitigate this issue?**

**6. You run a website in an IaaS environment. You wake up to discover that your**

**website has been defaced. Assume you are running a web server and an FTP**

**server in this environment and that both an application proxy and a firewall sit**

**between those servers and the Internet. All of your VMs are running SSH**

**servers. What logs might help you determine how the website was defaced?**

**What kind of information would you look for?**

**7. Sidebar 8-2 shows that personal biographical information—addresses, phone**

**numbers, email addresses, credit card numbers, etc.—can not only be used by**

**attackers to hijack accounts but can also be collected from one hijacked account**

**to help an attacker gain access to the next. How can you protect yourself against**

**this kind of attack? What can cloud providers change to mitigate such attacks?**

**8. Describe an FIdM authentication system for which you have been a Subject.**

**What organization acted as the IdP? What service acted as the SP?**

**9. Name three security benefits of FIdM over requiring users to use a new set of**

**credentials.**

**10. Why is it important to sign SAML Assertions? Why is it not important to sign**

**OAuth Access Tokens?**

**11. In OAuth, what attack does the Client Secret mitigate? Why do you think the**

**Client Secret is optional for Public Clients?**

**12. Name four services that might allow you to control a VM in an IaaS environment.**

**What entity controls each service?**

**13. What are some characteristics of systems in which you would expect application**

**whitelisting to work well? What about systems in which you would expect it to not**

**work well?**