Kenneth Woodard

CS366

Written Assignment 4

Question 1

Checking the network logs would be a great place to start the initial scanning. It would also be wise to look into any of the newest user accounts. Anytime multiple login attempts are used should be a red flag. Looking for any recent changes in the system is another good place to start. It would be a good idea to check for changes in the systems settings/configurations specifically.

Monitoring the database itself is another good idea. Check for any connections to any external IP addresses. Check the network for any large amounts of data being accessed or sent. When it comes to cloud servers, check and analyze any connections being made to cloud servers.

Checking the Windows Registry for any recent changes could also prove fruitful. Check all processes currently running on the database system as well to be safe.

Question 2

a. Unlinkability means two different events/data do not leave observable traces that indicate a legitimate connection between. This just means that an attacker can’t figure out that two pieces of data are related/connected to one another, whether the traces are obfuscated or destroyed.

b. Unobservability means that an attacker cannot see the data in question. Obviously, not being able to observe your actions is preferred in terms of privacy.

c. Basically the Remailer system, allows communication while providing unlinkability, unobservability, and anonymity if the communication is one direction. In order to communicate back and forth, some sort of return address must be provided. This removes the anonymity from the system. It works by forcing all messages to have the same size in bytes and having everyone sending and receiving messages at once. Each user/node sends or receives each round. In between sending and receiving the messages are mixed up, so that the message cannot be traced back to the sender. A mixer accomplishes this for us. If there was no mixer, then FIFO would be nature in which the messages pass through the system. This would have poor security because the time between sent and received messages could be sorted through and linked together. This explains why messages are held by the mixer until every message as been received, so they can be sent out in a random fashion afterwards. This is also why having more messages being sent to the mixer will improve the security of the system.