Andrew Plum

Mr. Alves-Foss

Cyb 110

9/8/21

# Ch. 4 Homework

1) Logging is one of the types of auditing. Logging gives a history of the events that have taken place in an environment. Logs are typically generated automatically in operating systems to keep track of the various activities occurring. Logging is a reactive tool meaning it allows you to see an event has taken place after it has happened. Logging is also admissible in a court of law. Logging is usually set up to record the main activities carried out but can be changed to log every action carried out. Most of the time only system administrators can review logs; and usually users of a system can't modify them.

2) Authorization is the process of determining what an authenticated party can do. Accountability is how you keep track of the activities that have taken place after you've gone through the processes of identification, authentication, and authorization. In other words, accountability is when all actions of an entity can be traced back uniquely to that entity. Authorization and accountability differ in that, authorization occurs before actions have been committed whereas accountability is attributing an action to a specific entity after they have been committed.

4) In the information security world, audit the factors that determine access to there various systems. Five items you might want to audit in this field are passwords, software licenses, and internet usage which includes websites visited, instant messaging, email, and file transfers. Auditing these resources will allow you act if you encounter misuse of them.

5) Accountability is important when dealing with sensitive date because holding someone accountable means making sure a person is responsible for their actions and if how people are accessing sensitive data stored digitally isn't tracked, business could suffer major financial losses as well as the government could experience major security issues. Accountability is important so that you can tell when various actions and policies are bad practice, and so that further you can put a stop to them. It should also be noted that businesses are held accountable when in the possession of sensitive information, and the legal repercussions could be quite severe when there is a security breach and bad practice was at play; businesses want to try to prevent this by stopping bad practice.

7) When dealing with legal or regulatory issues, you need accountability because you can keep your environment secure by enabling nonrepudiation, by entities who would otherwise misuse your resources, and by detecting and preventing intrusions. Businesses can face legal repercussions if they don't handle a situation properly. The processes that are used to ensure good accountability can assist business in preparing materials for legal proceedings. When regulating business practice, businesses want their employees to be productive and auditing them and holding them accountable for their actions is a step towards ensuring they are productive.

10) Given an environment containing servers that handle sensitive customer data, some of which are exposed to the internet, I would want to do both a vulnerability assessment and a penetration test. Because the data being handle is sensitive customer data, you would want the environment in which it is contained in to be secure as possible which is why I think it would be wise to want to do both a

vulnerability assessment and a penetration test. I would use a vulnerability scanning tool to look for weaknesses in the environment holding the data, and then I would try and patch the weaknesses in the system so that it is more secure. After this, I would engage in penetration testing with the system. If I was able to exploit a weakness in the system, I would try to fix the weakness. Ideally, I would engage in this until I ran into no more weakness in the system so that it would be very difficult for a malicious entity to break into the system through a weakness I possibly didn’t find.