ASSIGNMENT 8 Hortin

Chapter 20
15 Pts. What are the three classes of attackers that must be considered during penetration testing?

-External attacker with no knowledge of the system. - least valuable since it teaches little about the security of the system
-External attacker with access to the system. -common forms of this attack are guessing passwords, finding weaknesses in validation
-Internal attacker with access to the system. - this usually involves gaining access to files that a user should not be able to access.

15 Pts. Can penetration testing prove that a system is secure? Why?

"penetration analyses enable us to test admittedly nonsecure systems to determine whether or not they are sufficiently secure for the uses to which they are put" - This is a direct quote from the book. Already in class we have discussed that no amount of testing or any mechanism can ever prove a system is secure. It will never happen with known methods. What we can do is ensure that most security flaws are fixed by penetration testing, so this does not mean we should never do penetration testing.

Chapter 21
15 Pts. Why should secure systems have auditing systems integrated into their designs and implementations?

Secure systems should build this feature in so people can easily collect data on operation, analyze it, and finally report the results. This should be implemented so that it can collect vast amounts of useful data so if a breach does occur internally or externally, more data can be summoned to figure out exactly what happened during that breach, how it happened, what needs to be done to reverse it, and finally how to prevent it from happening in the future.

A great example is login features on websites That record an operation (someone attempting to guess a password). Analyze it (count how many times that an IP gets password/username combo wrong). Than finally reports and acts on it (bans users IP for 24 hours).

15 Pts. Why would an attacker want access to unsanitized logs?

The most obvious reason is that they would like to erase all of their tracks. It would also be possible for them to learn more about the system for any further attacks that they would like to perform. There might be many other vulnerabilities that the attacker could use in the future if their initial method fails to succeed again.