CORPORATE COMPUTER SECURITY

408217, Lab Session 10 (Chapter 7, Host Hardening)

"FileVerifier$^{++®}$ is a tool that will compute hashes on any single file, or all of your files at once. These hashes are then used to check to see if there have been any changes to those files. FileVerifier^{++} can quickly check the integrity of a large number of files. FileVerifier^{++} is useful if you need to verify that a given set of files has not been changed or altered in any way. FileVerifier^{++} can be downloaded from http://www.programmingunlimited.net. It can work of flash drive, or a CD"

Questions

1. How could a hacker keep you from knowing which files were changed?

2. From the hash could you tell what was changed in the file?

3. Should you use the longest hash possible? How long is good enough? [search information on hash algorithms that you know about, e.g., MD5, SHA-1, SHA-2].

FURTHER QUESTIONS

1. Why do you think companies often fail to harden their servers adequately? Give two reasons.

2. Why do you think companies often fail to harden their clients adequately? Give two reasons.

3. How is the diversity of UNIX offerings both bad and good ? Give one reasons for each.

4. *"Directory LongFiles has several subdirectories. Each of these subdirectories has very sensitive information that should only be accessible to a single user. "*

   What permissions would you give in the top-level LongFiles directory to the group *all logged-in users* if you do not want to change the *Allow inheritable permissions from parent to propagate to this object* box default in subdirectories? What permissions would you assign in each subdirectory?

4. In their purest form, netbooks are PCs designed to have little or no software stored on them. Instead, they are designed to use cloud computing, in which the software and data are both stored on Internet servers. Netbooks in this pure form can only work when they have an Internet connection. **Based on what you learned in this chapter, discuss security implications for netbooks, both pro and con? Give one of each.**

7. What password cracking method would be suitable to be used for each of the following passwords? Explain why

a) *swordfish*

b) *Lt6^*

c) *Processing1*

d) *nitt4aGm^*

8. Critique the safety of each of the following passwords, giving your specific reasoning.

a) *swordfish*

b) *Lt6^*

c) *Processing1*

d) *nitt4aGm^*