ENPM695 – Secure Operating Systems

Homework – 3

Author – Syed Mohammad Ibrahim

UMD ID: iamibi

UID: 118428369

Email: iamibi@umd.edu

1. When files are deleted in an operating system the space is typically returned to the free list but the blocks are not erased. Describe how a system can be designed so that the data is not recoverable. (15 points)

A. The operating system(s) can implement a wrapper around the whole deleting process wherein, when the user deletes a file from the system, they are marked for deletion by operating system in an async manner. The user will be displayed that the file was deleted (which is the usual way), but behind the scenes, the async operation will make sure that some random garbage data (or logical operation values) is written on the marked space. This could take a little performance hit but it will grant the ability of unrecoverable blocks of memory from the disk.

2. What is the difference between a virus and a worm? How does each reproduce? (25 points)

A.

Virus	Worm
It is a malicious program that usually attaches itself with another legitimate program to perform its tasks	A malicious program that can replicate itself over a network
They are usually designed to modify or report information to the person who wrote the program	They are designed to waste the system resources
They can't be controlled remotely	They are controlled remotely
They are executed by an executable file	They are executed by a weakness in the system
A viable host like an executable, is required to replicate	It doesn't require any host necessarily to replicate itself over the network

3. Name three different protection mechanisms we discussed (5 points). For each of the following protection problems tell which of these mechanisms can be used (5 points each)

a. Michael and John want to share some secret files

b. Susan wants some of her files to be public

c. Dennis wants his files readable by everyone except his roommate

A. The three different types of protection mechanisms are:

- SSL/TLS

- VPN

- Secure Shell (SSH)

Protection mechanism that can be used for the following scenarios are:

a. Michael and John want to share some secret files – IPSec (VPN)

b. Susan wants some of her files to be public – TLS

c. Dennis wants his files readable by everyone except his roommate – SSH (using chroot jail)

4. List 5 different pathnames to the file /etc/shadow (5 points)

A. The five paths are:

- /etc/shadow

- ./shadow (If the user's present working directory is /etc)

- ../etc/shadow (If the user's present working directory is /home or any other directory in the root path)

- etc/shadow (If the user's present working directory is root /)

- ./etc/shadow (If the user's present working directory is root /)

5. The Windows file system provides a command called REN (rename). What is the difference

between this and copying the file with a new name and then deleting the old one? (15 points)

A. The renaming of a file will instruct the operating system to change the directory entry of the file in the system whereas, copying and deleting action will allocate a new memory block(s) for the file. The copying and deleting will take a performance hit as the new blocks are allocated on-the-go.

6. Describe two differences between file access control lists and file permissions. (5 points) Which

are more flexible? (5 points)

A.

File Access Control Lists	File Permissions
They are responsible for making sure that based on a user's rights, they are allowed to read, write and/or execute any given file on the file system.	The permission of an individual file for a user. This varies on where the file is located like under a restricted folder which prevents the file permission of any read/write/execute by any user other than superuser.
This involves the ownerships User, Group, Others, All	This involves access protection of read, write, and execute on any given file and folder.

The file permissions are more flexible as they don't restrict the type of user to modify a file/folder.

7. List three attacks against systems protected using full-volume encryption (10 points)

A. The three attacks available against systems protected using full-volume encryption are:

- Evil Maid Attack

This attack involves an attacker replacing the legitimate bootloader with a hacked one using a live CD/USB. Once the system is restarted, the victim's computer will load from the hacked bootloader. The victim will be required to enter their volume decryption key/password to decrypt the drive. This will be captured by the hacked bootloader for later retrieval.

- Bootkit and Rootkit Attack

Bootkit involves masking a malware as the Master Boot Record (MBR) and execute this malware before the operating system is launched. This attack bypasses the full-volume encryption as MBR can no longer be encrypted.

Rootkit involves gaining administrative privileges on a victim's computer by exploiting a vulnerability of the current operating system it's being run on and gaining access silently with persistence. They can potentially open backdoors for attackers.

- Brute-Force Sign-In Attack

This involves trying out all the possible combination of passwords or passphrases until a correct one is found for the full-volume encryption.