Nitin Nagavel

CPRE 431

M03 HW

Assignments will be submitted in PDF format via Canvas.

Please submit your homework online through Canvas. Late homework will not be accepted.
Important: Your submission must be in .pdf format ONLY!
Please ensure that you support all your answers with the correct screenshots showing your solutions.

1. Briefly state the differences between DAC and MAC access control mechanisms.

   DAC requires the owner of the resources to determine the access while MAC provides the resources depending on the clearance level of the user.

2. The inclusion of the salt in the UNIX password scheme increases the difficulty of guessing by a factor of 4096. But the salt is stored in plaintext in the same entry as the corresponding ciphertext password. Therefore, salt is known to the attacker. Based on that, why is it asserted that the salt increases security?

   Salt increases security through the amount of computational power required. The More salts/ variaties of salts used, the amount of computing power increases by a factor of 10 and takes muchlonger to brute force. Also if the salt is independently located from the password, its harder for an attacker to reverse engineer the password.

3. In the traditional UNIX file access model, UNIX systems provide a default setting for newly created files and directories, which the owner may later change. The default is typically full access for the owner combined with one of the following: no access for group and other, read/execute access for group and none for other, or read/execute access for both group and other. Briefly discuss the advantages and disadvantages of each of these cases, including an example of a type of organization where each would be appropriate.

   An Advantage where an owner is given full access means that manageability of multiple computer systems is easier. An example where this can be used is with schools. A majority of users are students and a small number of admins it can be easy to restrict access to certain files and executables over a large organization.

A disadvantage of full control for the owner is the security risk. If the owner's main computer gets compromised by attackers, then its easy to obtain information from other users in the same group. For this, a solution is to provide read/execute access to other system admins. Then if an attack were to occur, then other system admins will be able to prevent that easily.

4. Provide short answers to the following questions:
   a. Why should system administrators remove unnecessary services, applications, and protocols?

By removing any unnecessary services and applications running in the background, this not only helps with ram management but it also frees up the badwidth these sericeses use. Also depending on the circumstances system admins may restrict access to certain applications due to the ability to modify the contents when running.

b. Where is application and service configuration information stored on Unix and Linux systems?

So linux treats each device as a special file that is located in a /dev ./etc. Most of the installation files are located in /etc/rc

c. How does "chroot jail" used to improve application security? And what are its limitations?

Chroot jail is basically a way to separate a [rpcess from its sub processes. It should only be applied to processes that don't run for root users because they can escape very easily. The only Limitation to Chroot Jail is its dependance of an external security source. Chroot jail itself doesn't give any practical security and this makes it very easy to escap a chroot.

5. Logging is a very important control for operating system and network security, explain the following:
   a. Why is logging important?
   Logging is important because it acts like an indicatior when the network detects unsafe events and reports back the information to the user.
   b. What are its limitations as a security control?
   Logging requires effective detection setup and needs constant monitoring. Logging by itself does not do these tasks however, and requires external sources to be properly working.
   c. What are the pros and cons of remote logging?
   Some pros include daily testing and faster reports to a user's phones. Also it cuts the costs of logging admins to travel back and forth the the physical server location. Cons include constant security patches and updates. Due to the lack of a physical admin in site, its vulnerable to various attackers.

Why is it important to rotate log files (overwrite old log files)?

Rotating log files are important because, most recent log files can provide admins information on how to improve the security functionality of the system. They are also stored in large file sizes which occupy enormous amounts of space and constant rotating ensures that the server doesn't run out of space.

6. Consider an automated audit log analysis tool (e.g., swatch). Can you propose some generic rules which could be used to distinguish "suspicious activities" from normal user behavior on a system for some organization, for the following activities:
   a. User Authentication
   Location of login, new phone number, FaceID are all ways to authenticate users from other suspicious activities.

b. Website Access
   Location of Access, and the computer IP address are used to determine suspicious activities. If the Website access is different from the previous Website Access Location, it will trigger an alert.