CHAPTER 18

Intruders

Intruders

One of the most publicized threats to security is the intruder, generally referred to as hacker or cracker. Anderson identified three classes of intruders:

1. Masquerader:

   An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.

2. Misfeasor:

   A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.

3. Clandestine user:

   An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

Intruders Continue…

- The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider.
- Intruder attacks range from benign to the serious.
- At the benign end of the scale, there are many people who simply wish to explore internets and see what is out there.
- At the serious intruders attempt to read privileged data, perform unauthorized modifications to data, or disrupt the system.

Intrusion Techniques

- The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system.
- With knowledge of some other user's password, an intruder can log in to a system and exercise all the privileges accorded to the legitimate user.
- A system must maintain a file that associates a password with each authorized user.
- If such a file is stored with no protection, then it is an easy matter to gain access to it and learn passwords.

Intrusion Techniques Continue…

The password file can be protected in one of two ways:

1. One-way encryption:

   The system stores only an encrypted form of the user's password. When the user presents a password, the system encrypts that password and compares it with the stored value. The system generally performs a one-way transformation (not reversible) in which the password is used to generate a key for the encryption function.

2. Access control:

   Access to the password file is limited to one or a very few accounts.

If one or both of these measures are in place, some effort is needed for a potential intruder to learn passwords.

Intrusion Techniques Continue…

The following techniques can be used to learn passwords:

1. Try default passwords used with standard accounts that are shipped with the system. Many administrators do not bother to change these defaults.

2. Exhaustively try all short password (those of one to three characters)
3. Try words in the system's online dictionary or a list of likely passwords.

4. Collect information about users , such as their full names, the names of their spouse and children, pictures in their office, books are in their office that are related to hobbies.

5. Try users phone numbers, social security numbers, and room numbers.
6. Try all legitimate license plate numbers for this state.

7. Use a Trojan horse to bypass restrictions on access.
8. Tap the line between a remote user and the host system.

Intrusion Techniques Continue…

- The first six methods are various ways of guessing a password. If an intruder has to verify the guess by attempting to log in, it is a tedious and easily countered means of attack.
- For example, a system can simply reject any login after three password attempts, thus requiring the intruder to reconnect to the host to try again.
- Under these circumstances, it is not practical to try more than a handful of passwords.
- The 7th method of attack can be particularly difficult to counter. A low-privilege user produced a game program and invited the system operator to use it in his or her spare time. The program did indeed play a game, but in the background it also contained code to copy the password file. Because the game was running under the operator's high-privilege mode, it was able to gain access to the password file.
- The 8th attack is a matter of physical security. It can be countered with link encryption techniques.