Chapter 14 Network Administration

Chapter Objectives

This chapter will discuss:

- The role of an organization's network administrator from the perspective of managing user access,
- High-level issues influencing how a network administrator ensures security, and
- How network administration fits into the organization's business processes.

14.1 The Network Administrator's Role

In an organization, all the written policies and statements of senior management are worthless unless the people in charge of implementing them do not follow their direction. As was discussed in Chapter 12, a social engineer might be able to convince a network administrator to grant them access by pretending to be someone in dire need of access but who cannot get on the network. The administrator is then convinced to provide a temporary logon, which is all the attacker needs to strike. The following subsections will discuss several aspects of administering user access.

14.1.1 Usernames

This is far more involved than simply determining if the protocol for the organization's email addresses will be "first.last" or "firstinitial.last". Barman (2002) notes several considerations for usernames.

- Handling dormant usernames- If a person has not technically left an organization or is somehow still entitled to have an account with an organization even though they have for all intents and purposes moved on (a very common thing in U.S. colleges and universities), their accounts may go without being used for long periods of time. Should one of those accounts suddenly "come back to life" and begin accessing all sorts of system ad-

ministrator parts of the network, this should be noted and investigated, especially if the user is an adjunct professor in, for example, the English department.

- Procedures when an employee leaves the organization- As was discussed in the chapter on Initial Employee Communication, an employee should agree to go through a "check out" procedure before they leave. Part of that procedure should be to ensure the IT department has deactivated the separated employee's user accounts.
- Removing default user accounts- In the stories of the "phone phreaking" days, telephone company technicians would leave the default usernames and passwords, such as "field" and "manager" on their systems. This would allow enterprising hackers to access the systems once they obtained the default logon information from the equipment's technical manuals.
- Handling anonymous users- Organizations should be extremely hesitant to allow any type of anonymous access to its networks.
- Assigning all users a pre-configured "role"- A major way to help maintain network security is to define the various roles one may have in an organization and only allow users to be assigned to a role or roles. Exceptions to this practice should be kept to a minimum, as they become extremely difficult to manage.

14.1.2 Passwords

Barman (ibid) continues his analysis of managing user access by arguing that password management may be divided into two parts: what constitutes a valid password and how passwords are to be stored.

In defining a valid password, the long-running conflict between users and network administrators come to bear. Users complain about being required to have a password such as "1Lov#$pR1nger" which must be changed every three months and may not be repeated for several months or years. As discussed elsewhere, brute force methods such as "dictionary attacks," which go through every word in a dictionary, or those which try as many possible letter, number and special character combinations, simply don't work if the password is no less than eight characters, must contain at least one number, at least one special character, and at least one lower- and upper-case letter.

In deciding how to properly store passwords, network administrators realize that it is absolutely essential to keep the organization's passwords out