Account Types

The first step in creating secure accounts is to make certain that you have different account
types for different uses. Regardless of the type of account, which we will discuss in this sec- 1
tion, all accounts should have some of the same properties. Those properties include things
such as password complexity, age, and history. These concepts have been mentioned else- 2
where in this book ~~but bear revisiting here.~~

Password complexity refers to requiring capital letters, numbers, and symbols as part 3
of a password. This can be just as important as password length ~~in thwarting at least some~~
~~attacks. *Password age* relates to how long you can have a password before it expires and~~
~~a new password is generated.~~ *Password history* determines how many old passwords the
system will remember, thus preventing the user from simply repeating previous passwords 4
when it comes time to change his or her password.

In addition to password complexity, there will be related issues such as *password length.* 5
The rule is the longer, the better. *Passphrases* are becoming more common. ~~Beyond using a~~
~~series of words or other text to control access, passphrases are generally longer in order to~~
~~provide additional security.~~

Then there is the issue of *account lockout.* How many times can the user enter the incor- 6
rect password before the account is locked? If the account is locked, how will it be recov-
ered? ~~For example, you might have the lockout automatically recover after 24 hours, or it~~
~~might require an administrator to reset it.~~

~~There are no absolute answers to these issues.~~ What is appropriate for one organization
might not be right for another. In a low-security environment, you might have passwords 7
that are 8 characters long, expire after 6 months, don't lock out until 6 failed attempts,
and then automatically recover in 2 hours. For a high-security environment, you might 8
have 14+ character passwords that are changed every 30 days and lock out after 3 failed
attempts. Then, they can only be recovered by an administrator. ~~The specific decisions that~~
~~you make on these issues will depend on the security needs of your company.~~

The most obvious type of account is the *user account.* These will be assigned to human 9
users of your network. Each user account should have certain properties. This will include
an expiration date as well as the type of user. For example, *administrator accounts* are spe-
cial user accounts with a great deal of privileges. Administrator accounts should be granted 10
sparingly and monitored closely.

~~The topic of administrator accounts naturally leads to the broader topic of privileged~~
~~accounts. By definition, any account that has significant rights on the network is a *privi-*~~
~~*leged account.* The root account in Linux is a classic example.~~ In Windows, the admin-
istrator account and power user accounts are good examples. The main issue with such 11
accounts is that they should be given only when absolutely necessary.

~~The most important account is the *domain admin account.* A local admin account~~
~~(or root in Linux) gives the user unfettered control of a single machine.~~ But domain admin
accounts provide the user with complete and total control of your network. The ultimate 12
goal of any attacker is to get domain admin privileges. For this reason, domain admin
accounts must be very closely controlled.

In some cases, you may wish to use a shared account for several uses. This is sometimes 13
called a *generic account*. Using a generic account is usually not recommended. The pre-
ferred method is to have individual accounts for individual users. However, in some limited
situations, it may be acceptable to use very low-privileged accounts that are shared. For 14
example, for a lab on a college campus that only has access to the lab systems and no other
resources, you might have a generic account `labuser`, which can be used by any student in
the lab.

In most organizations of any significant size, you will eventually have outsiders who 15
need to access your network. This could include clients or business partners who are visit-
ing your facilities for a brief period of time. Guests in a hotel are another classic example. 16
These accounts are usually called *guest accounts*. They should have bare minimum privi-
leges. It is possible to have individual accounts for each guest. In fact, hotels often have
the guest log in by room number and last name, thus creating an individual account for an
individual guest. However, in some situations, hotels may use a shared account for guests.
For example, guest Wi-Fi often uses a single “guest” login that every guest shares.

The concept of privileged accounts and guest accounts is part of the larger topic of group-based access control. Any sizable network quickly becomes difficult to manage, and trying to administer privileges individually for a few thousand employees is a daunting task. It is often better to place users into groups based on their job roles and then to manage privileges for those groups. So rather than needing to manage privileges for all sales personnel, you can simply administer the privileges of the Sales group.

Humans are not the only entities that may require access to network resources. You might have software that needs to access your network, separately from human involvement. As one example, database services usually start when the machine they are on boots up. These services require their own accounts. One mistake that is all too common is simply to assign these services to a domain administration account. This violates the principle of least privileges that you have read about repeatedly in this book. The proper approach is to create service accounts with just enough privileges for the service to accomplish its required tasks.

General Concepts

The most important concept in account management that has been mentioned in this chapter, as well as previously in this book, is *least privileges*. This means that each account is given only the privileges that entity (user or service) needs to do their job. This is not a question of lack of trust or lack of skill of that user. The user in question may be very technically skilled and could be someone you would literally trust with your life. However, their user account is only granted just enough privileges to do their job and nothing more.

Once you have assessed the needs of each user and service and then assigned the appropriate privileges to those accounts, the next step is to audit those accounts periodically. Two types of audits are relevant to accounts: usage audits and privilege audits.