Understanding Security Policies

Lesson 3

Objectives

Lesson Skill Matrix		
Technology Skill	**Objective Domain**	**Objective Domain Number**
Using Password Policies to Enhance Security	Understand password policies.	2.3

Password

- Much of today's data protection is based on the ***password.***
- One basic component of your information security program is ensuring that all employees select and use ***strong passwords***.
- The strength of a password can be determined by looking at the password's length, complexity, and randomness.

Password Complexity

- Password complexity involves the characters used to make up a password.
- A complex password uses characters from at least three of the following categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Numeric characters (0 through 9)
  - Nonalphanumeric characters (!, @, #, $, %, ^, &, etc.)

Password Length

- The length of a password is a key component of its strength.
- Password length is the number of characters used in a password.

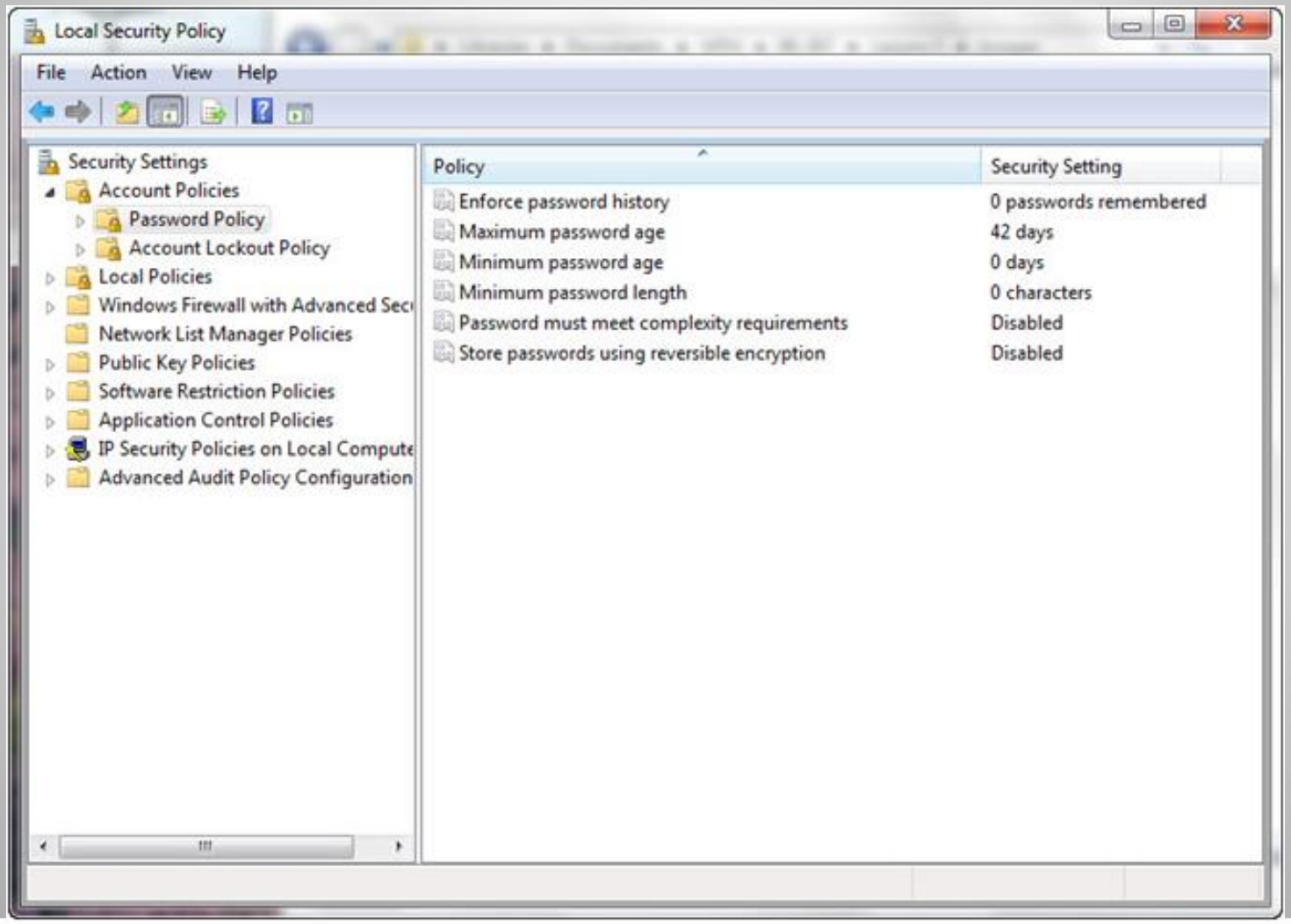
Time Between Password Changes

- Time between password changes can be defined by two settings:
  - Minimum Password Age
  - Maximum Password Age

Password History

- Password history is the setting that determines the number of unique passwords that must be used before a password can be re-used.
- This setting prevents users from recycling the same passwords through a system.

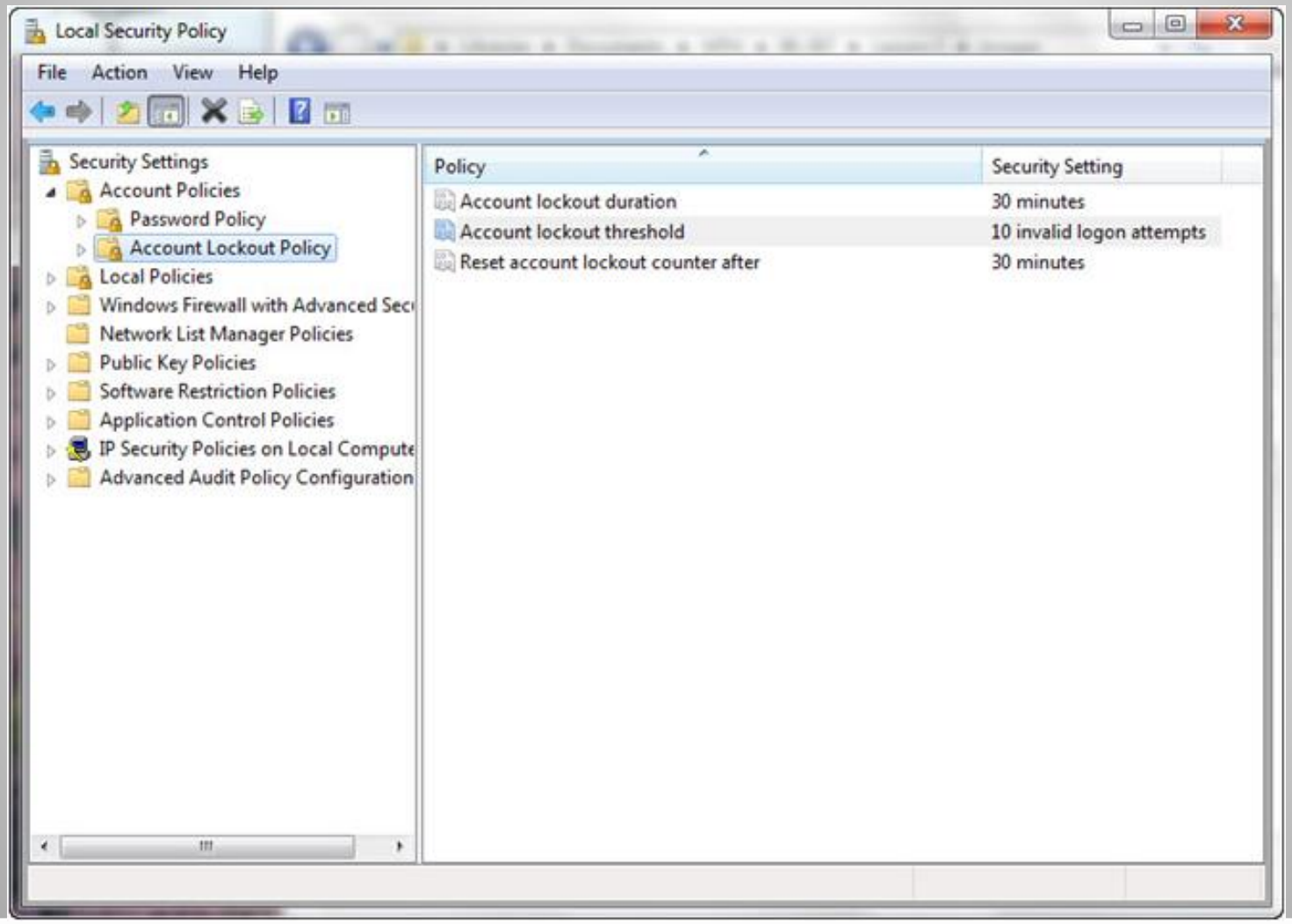
Password Policy



Account Lockout

- Account lockout refers to the number of incorrect logon attempts permitted before a system locks an account.
- Microsoft provides three separate settings with respect to account lockout:
  - Account lockout duration
  - Account lockout threshold
  - Reset account lockout counter after

Account Lockout Policy



Common Attack Methods

- Passwords have long been recognized as one of the weak links in many security programs.
  - First, you are completely reliant on users in the selection of passwords.
  - Second, even strong passwords are vulnerable to attack through a variety of different mechanisms.

Dictionary and Brute Force Attacks

- A dictionary attack uses a dictionary containing an extensive list of potential passwords that the attacker then tries in conjunction with a user ID in an attempt to guess the appropriate password.
- Another, more crude type of attack—called a brute force attack—doesn't rely on lists of passwords, but rather tries all possible combinations of permitted character types.

Physical Attacks

- Anytime your computer can be physically accessed by an attacker, that computer is at risk.
- Physical attacks on your computer can completely bypass almost all security mechanisms, such as by capturing the passwords and other critical data directly from the keyboard when a software or hardware ***keylogger*** is used.
- In fact, if your encryption key passes through a keylogger, you might find that even your encrypted data is jeopardized.

Sniffers

- Sniffers are specially designed software (and in some cases hardware) applications that capture network packets as they traverse a network, displaying them for the attacker.
- Sniffers are valid forms of test equipment, used to identify network and application issues, but the technology has been rapidly co-opted by attackers as an easy way to grab logon credentials.

Summary

- The strength of a password can be determined by looking at the password's length, complexity, and randomness.
- A complex password uses characters from at least three of the following categories: uppercase, lowercase, numeric characters, and nonalphanumeric characters.
- Account lockout refers to the number of incorrect logon attempts permitted before a system will lock an account.

Summary

- The Minimum Password Age setting controls how many days users must wait before they can reset their password.
- The Maximum Password Age setting controls the maximum period of time that can elapse before users are forced to reset their password.
- A Group Policy Object (GPO) is a set of rules that allow an administrator granular control over the configuration of objects in Active Directory (AD), including user accounts, operating systems, applications, and other AD objects.

Summary

- Passwords have long been recognized as one of the weak links in many security programs.
- During a dictionary attack, the attacker tries an extensive list of potential passwords in conjunction with a user ID to try to guess the appropriate password.
- Brute force attacks try all possible combinations of permitted character types in an attempt to determine a user's password.

Summary

- Physical attacks on a computer can completely bypass almost all security mechanisms, such as by capturing passwords and other critical data directly from a keyboard when a software or hardware keylogger is used.
- In a password crack attack, attackers get access to an encrypted password file from a workstation or server. Once they have access to this file, attackers start running password cracking tools against it.

Summary

- Physical attacks on a computer can completely bypass almost all security mechanisms, such as by capturing passwords and other critical data directly from a keyboard when a software or hardware keylogger is used.
- In a password crack attack, attackers get access to an encrypted password file from a workstation or server. Once they have access to this file, attackers start running password cracking tools against it.