Topic of Presentation

Introduction

- ✓ A symbolic link is a special type of file in modern operating systems that acts as a reference or pointer to another file or directory.
- ✓ System data files are core files that hold essential configuration and information for an operating system.
- ✓ password file (/etc/passwd) is a system data file that stores essential information about the users of the system
- ✓ To improve security, modern systems use the shadow password file (/etc/shadow)

Topic of Presentation

System Data Files

System data files are essential files that store critical information required for the operating system and installed applications to function properly. These files help manage system configuration, user information, hardware settings, software installations, and various other system services.

Key Categories and example of System Data Files:

- **Configuration Files**:
  These files store settings and parameters for both the operating system and various applications. They define how the system should operate and manage its resources.
- **User Data Files**:
  These files manage user-related information, such as account credentials and settings.
- **System Logs**:
  Log files record events happening within the system, such as errors, warnings, security events, and system performance metrics.
- **System Libraries**:
  These files store shared code that multiple programs can use to execute common functions
-

Topic of Presentation

Password Files

The **password file** is a critical system data file in Unix/Linux systems, traditionally located at **/etc/passwd**. It stores essential information about user accounts, such as usernames, User IDs (UIDs), Group IDs (GIDs), home directories, and login shells. Historically, this file also contained user passwords in plain text, but for security reasons, this practice was changed.

Structure of /etc/passwd:

username:x:UID:GID:User Info:Home Directory:Shell

Example of an Entry in /etc/passwd:

- **Username**: john
- **Password placeholder**: x (password is in /etc/shadow)
- **User ID**: 1001
- **Group ID**: 1001
- **User Info**: John Doe

Topic of Presentation

Shadow Password

Shadow passwords refer to the practice of storing encrypted user passwords in a separate, more secure file called **/etc/shadow** in Unix/Linux systems. This file is accessible only by privileged users (typically the root user), which greatly enhances security compared to the older method of storing passwords in the world-readable /etc/passwd file.

Purpose of Shadow Passwords:

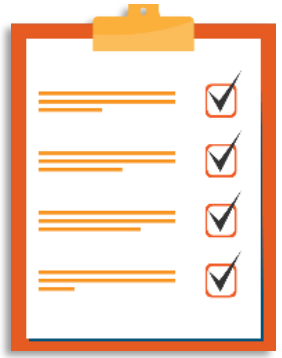
The main goal of using shadow passwords is to protect sensitive password information by restricting access to it. While /etc/passwd contains basic account information (e.g., usernames, UIDs, home directories), the actual encrypted passwords are stored in /etc/shadow, which can only be accessed by users with special permissions.

Structure of /etc/shadow:

username:password_hash:last_changed:min_days:max_days:warn_days:inactive_days:expire_date:reserved

- **Username**: john
- **Password Hash**: 6abcd1234$encryptedhash (the password is encrypted using SHA-512 with salt abcd1234)
- **Last Password Change**: 19000 days since January 1, 1970
- **Minimum Days Before Change**: 7
- **Maximum Days Before Expiration**: 90
- **Warning Before Expiration**: 7 days

Topic of Presentation



Summary

Symbolic links are special files that act as pointers to other files or directories, facilitating easier navigation within a file system. System data files contain critical configuration and operational information necessary for an operating system to function effectively. Password files store user credentials, often in a hashed format, for authentication purposes. Shadow passwords enhance security by keeping hashed passwords in a separate, restricted file, ensuring that sensitive information remains protected from unauthorized access. Together, these components play vital roles in file management and system security.