8.6.9 Hardening Applications Facts

Application hardening is the process of preventing exploitation of vulnerabilities in software applications. Applications pose the most difficult security challenges for a security administrator because they are complex, usually developed by a third party, and designed to accept input from users.

Basic hardening guidelines for applications are as follows:

- Assume all installed applications are flawed
- Remove all unused applications from the system
- Limit administrative privileges
- Install security software, such as antivirus, anti-spyware, and anti-rootkit
- Use firewalls, content filters, and operating system user authentication features
- Restrict access to the application and provide access only to those who need it
- Update all applications with the latest patches when security bulletins are released
- Identify baselines
- Monitor log files

Additional application hardening includes the following techniques:

Technique	Description
Block Process Spawning	Process *spawning* is the creation of a new process (also called a *child* process) by an existing process (also called a *parent* process). If you take the process spawning ability from the application, threat agents will not be able to perform process spawning attacks.
Control Access to Executable Files	Executable files should be protected from modification by removing the write permissions given to applications.
Protect OS Components	Sensitive file system areas (such as Windows Registry keys) should be protected by removing write permissions given to specific applications. In most cases, applications do not need to modify sensitive areas of the system for them to properly function.
Use Exception Rules	Exception rules allow an administrator to bypass a specific hardening rule when an application has a legitimate need. Administrators should exercise caution and set parameters regarding the exception that will ensure the security of the system.
Monitor Logs	Reviewing monitor logs allows an administrator to identify potentially vulnerable applications and identify if an application is being exploited. The best way to determine exception rules is to let the application run without any exceptions and then review the monitor logs to determine what an application legitimately needs to do.
Use Data Execution Prevention	Data Execution Prevention (DEP) is a security feature that can help prevent damage to your computer from viruses and other security threats. DEP ensures that applications use computer memory safely. DEP closes an application and notifies the administrator if a program initiates run instructions from the portion of memory used for data.
Implement Third-Party Application Hardening Tools	Third-party application hardening systems are developed for specific applications. The rules used by the application hardening system can be applied to the application being hardened, including libraries and SDKs. An example of these tools is AppArmor for Linux systems.