Securing Networks Systematically — the SKiP Method

CERT® Coordination Center

Network administrators, besides maintaining computer networks, frequently play a major role defending an organization's critical information assets. It is much easier for them to be effective if they choose a systematic approach to network security. One such method was developed at the CERT Coordination Center. Called the Security Knowledge in Practice method (or the "SKiP" method for short), it consists of steps to secure network software, "harden" a network (make it difficult to break into), detect and respond to network intrusions, and then to improve the system based on a review of events.

There are seven steps in the SKiP method, each with an associated set of security practices:

1. Select systems software from a vendor and customize it according to an organization's needs.
2. Harden and secure the system against known vulnerabilities.
3. Prepare the system so that anomalies may be noticed and analyzed for potential problems.
4. Detect those anomalies and any other system changes that could indicate evidence of an intrusion.
5. Respond to intrusions when they occur.
6. Improve practices and procedures after updating the system.
7. Repeat the SKiP process as long as the organization needs to protect the system and its information assets.

Customizing Vendor Software

The first step is to identify tasks a system must perform and configure it to fulfill essential functions while eliminating those that are unnecessary or vulnerable. Because securing a system is challenging (especially for a novice administrator) it is often neglected. In this step, network administrators do the following:

- eliminate services that are unneeded and insecurely configured
- restrict access to vulnerable files and directories
- turn off software "features" that introduce vulnerabilities
- mitigate vulnerabilities that intruders can use to break into systems

Harden and Secure the Network

In the Harden/Secure step, network administrators configure their system to meet organizational security requirements, retaining only those services and features needed to

address specific business needs. Securing a system against *known* attacks eliminates vulnerabilities and other weaknesses commonly used by intruders. The practices performed during this step may change over time to address new attacks and vulnerabilities.

Prepare

To meet the challenge of recognizing new vulnerabilities, network administrators characterize their system in the Prepare step. They work to understand and describe normal system behavior since any deviations may indicate an intrusion.

After completing a system characterization, an administrator knows what to expect in terms of

- changes in files and directories and the operating system
- normal processes, when they run, by whom, and what resources they consume
- network traffic consumed and produced
- hardware inventory on the system

Detect

In the Detect step, network administrators monitor the hardened and prepared system to detect changes. While some changes are predictable and constitute normal behavior, administrators concentrate on detecting signs of anomalous or unexpected behavior since it may indicate possible intrusions and system compromise.

Administrators also watch for early warning signs of potential intruder actions such as scanning and network mapping attempts. This step occurs as administrators monitor systems running in a production environment (such as looking at the logs produced by a firewall system or a public web server).

Respond

In the Respond step, the network administrator responds to an intrusion and contains it. A successful response means that the system is returned to its normal operational capability. There are many actions that make up this step.

For instance, if some unexpected system behavior caught the attention of the network administrator, they may choose to

- analyze the damage caused by the intrusion and respond by adding new technology or procedures to combat it
- monitor an intruder's actions in order to discover all access paths and entry points before acting to restrict intruder access.
- eliminate future intruder access
- return the system to a known, operational state while continuing to monitor and analyze

Improve the System

After completing a review of the incident, network administrators improve their system in this step. They may

- hold a post-mortem review meeting to discuss lessons learned
- update policies and procedures
- select new tools
- collect data about the resources required to deal with the intrusion and document the damage it caused

Repeat the Cycle of Steps

Finally, network administrators add any changes they made during the first six steps back into the system's characterization baseline. Now operating at a higher level of security, the system will function as designed until a new security challenge arises. Then the administrator can once again call upon the SKiP method.

Summary

Network administrators are most effective when they use a systematic approach to securing networks and responding to network intrusions. The SKiP method gives administrators a framework to select and deploy the security practices they need to combat and recover from threats to the security of the network.

References:

1. The CERT Coordination Center has authored an article that describes the SKiP's systematic, cyclical approach to securing computer networks. The full text of the article is available at http://www.cert.org/security-improvement/practices/practices.html.
2. The CERT website describes the SKiP method and associated security practices at http://www.cert.org/security-improvement/skip.html
3. Practices used in the SKiP method are described in a book entitled *The CERT Guide to System and Network Security Practices* (Addison-Wesley, 2001), by CERT author Julia Allen.