

Intrusion Detection

1. Disaster Preparedness

Detecting signs of a compromise starts long before the compromise occurs. A good way to start is to create a baseline profile of your operating system. Once a compromise occurs, you can use your baseline to determine what has been modified so it may be restored.

Tools such as Tripwire® and Osiris automate the tasks of creating a baseline, discovering, and reporting changes. Osiris is available for Linux and Windows users free of charge. Older tools, such as COPS, Tiger, and TARA, are no longer maintained.

Commit resources to keeping your system, websites, and applications up-to-date. Plan on reviewing logs and run reports against your baseline often and ensure every change is approved. When an unapproved change occurs you should suspect it immediately.

Backups are another consideration. In the event of a compromise, important data for your business could become a casualty. Regular database dumps, off-site replication with Secure Copy Protocol (SCP), and tape, and SAN backups each have their own advantages.

2. Levels of Compromise

System compromises generally fit within three categories:

1. User-level compromise
2. Application-level compromise
3. Root-level compromise

User-level compromises are common on Linux systems and can be prevented by keeping applications and software up-to-date. Cleaning usually involves killing errant processes and removing affected files (or restoring them from a backup).

Application-level compromises can be described as programming or configuration errors that allow changes to your database, website, or even critical programs. SQL, XML, variable, and cross-site scripting attacks are the most common forms.

Root-level compromises can be minor or catastrophic depending on the degree of control an intruder has taken. Common infestations of viruses, worms, trojans, and other forms of malware on Windows servers are easily prevented and cleaned by most anti-virus software available today.

3. Determining the level of compromise

Without a tool such as Tripwire, a lot of detective work is required to determine the level of compromise of your server. Unless you know exactly how the system should look, you don't have any basis for comparison.

Your system's package manager may have a record of what your operating system should look like. Other tools know what certain exploits look like and can detect their signatures. However, in order for them to work they make assumptions about the way your system should look, so you need to understand your system intimately.

These tools cannot detect modifications to your database, web pages, or any custom changes

you have made to your system.

Comparing against your baseline

This is by far the easiest and most effective way to determine what, if anything, has been changed on your system. Tripwire and Osiris will list what was changed and when it was changed. If the change is something you expected and approved then your baseline will be updated.

Should you discover any unauthorized changes you may have the ability to reverse them from the utility itself (this is a feature of many commercial solutions). You will need to be careful though; package management systems may apply updates automatically and you wouldn't want to back out an important upgrade that helps maintain your system's security. Database files can change without any notice due to indexing and other processes independent of updates to your data.

Linux systems store package and update information in a database which allow for an alternate method of comparison. This information can be used informally to check package installation statuses.

Linux Package Manager

On Linux, the Red Hat Package Manager (RPM) utility stores basic information about the installation for maintenance purposes. Unfortunately this database may be corrupted by intruders or even a poorly written installation script. Typing 'rpm -Va' tells the system to verify all installed packages and print anything changed since installation (including configuration files). Refer to the rpm(8) man page on your system ('man rpm') for more information.

Root Kit Detection

Microsoft recently acquired Systemal which produced a utility called RootkitRevealer . It may be downloaded freely from Microsoft's TechNet. RootkitRevealer only detects software that tries to hide from the operating system. Other utilities (such as Microsoft's Malicious Software Removal Tool) don't appear to report anything and are normally called through Windows Update.

Linux users might try "chkrootkit" and "rkhunter" . These utilities compare the encryption signatures of system files to check for vulnerabilities and well-known Linux rootkits. None of these utilities are effective against user-level compromises. Please see the documentation on these projects' websites for more information.

If any anomalies are detected, your system is possibly root compromised. Unfortunately these tools won't give you all of the information necessary in order to clean the infection yourself (and attempts to clean the system without practice will inevitably make things worse).

Anti-Virus

On Windows systems, anti-virus software (such as McAfee Virusscan Enterprise) is the first line of defense for your operating system. Other software you may purchase (such as Tripwire or McAfee Host IPS) can help prevent or trigger early-warning errors of a major security event.

Database Inspection

If you know the contents of your database (backups, audit controls, etc.) you could possibly find entries that didn't go through proper channels. In some lucky cases an insertion might be obvious (like an administrator named "bubba", unless of course you are Bubba in which case "susan" may be suspicious).

Users of content management systems (such as PHPbb, WordPress, PHPNuke, Joomla, Mambo, and others) may find the database useful to identify files that shouldn't exist (like an article named 11643561 that looks like every other numbered filename on the system). Otherwise you may have to rely on FTP backups of the website or manual means of investigation.

Other Methods

Other Linux utilities rely on your memory and intuition to discover anomalies on your system. The "du" command may help you see disk usage anomalies. The "find" command, with appropriate options, can be used to find

- 1.files with special (non-standard) security permissions like SUID or SGID.
- 2.files owned by a specific user (or by no user whatsoever)
- 3.files and directories that are world writable (and can possibly hide exploits)

Of course the possibilities of filenames and exploits are be limitless. Intruders will encode their exploits and hide them in graphics and other media file types. Without a baseline to compare against it's trial-and-error. Your memory and knowledge of the system and applications is your only guide.

4. When all else fails

If you've found an application-level compromise you may need to reload your application. With a user-level compromise, you may need to disable the user and delete that user's files. With a root-level compromise, you may need to delete your operating system and reload everything from backups.

These are the most drastic measures you may have to take (especially if you don't already have a backup). Sometimes a compromise can be copied from system to system through backups containing copies of the exploit or vulnerability. You will need to sanitize your backups before restoring them to their proper places.

Reloading the operating system requires physical access to the machine. Some data centers offer automatic provisioning and a "rapid rebuild" solution; others will happily rebuild your system for a fee. Co-location customers are usually able to perform reloads of their operating system with little or no assistance.

5. Conclusion

Reacting to a compromise requires some preparation and the ability to effectively compare a system's state with what is known to be good. Security analysts are often able to make comparisons based on their experience and by comparative analysis (comparing an unknown system to a set of known systems).

It takes a lot of time and effort to put together a set of tools to diagnose and treat a compromised system properly. Maintaining and updating applications is still key to preventing security issues but maintaining backups and lists for comparisons also go a long way towards recovery.