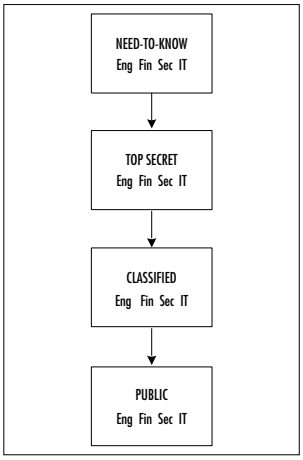
Contents

Exposing Default Solaris Security Levels

- Consider changing the umask in /etc/profile from the default value of 022 to something more restrictive, such as 027.
- Replace insecure cleartext daemons, such as FTP, Telnet, and the Berkeley r-commands, with a secure replacement like SSH or OpenSSH.
- Create Authorized Use banners in /etc/motd and /etc/issue.

An Example of Classification Hierarchy



Detecting Unusual Traffic with Network Traffic Monitoring

- Snoop, a built-in Solaris utility, is a powerful network tool for real-time monitoring of network activity for short periods of time.
- A dedicated sniffer/IDS system like Snort is the best way to get current and historically accurate information about network traffic types and patterns.

Watching Packets with Snoop

Here are a few examples of when you may want to use snoop:

- To verify that DHCP requests are being received and answered by the DHCP server
- To identify the source of denial of service (DoS) attacks
- To determine what Web sites your users are visiting
- To identify the source address of a suspected intruder
- To locate any unauthorized hosts

Answers to Your Frequently Asked Questions

Q: What is the best way to filter traffic handled by sendmail for virii?

A: There are several tools available for just this purpose. Some of them are freeware and others are commercial. You should evaluate each product based on your needs and then make the choice that best suits your environment. Certain products even integrate well with certain firewalls. Sendmail itself really should not be used as a content filter—it was never designed for this purpose.

Steps to Ensure the System Isn't Routing Traffic

1. Check for the /etc/notrouter file. If it does not exist, create it.
2. Check the value of ip_forwarding in the IP kernel module after the system has been rebooted.
3. Test the system by attempting to reach one interface of the system through the other.

Configuring Squid Services

Q: Can I force Squid to send certain requests directly to an Internet site, without using the cache? My own Web servers are local and don't need caching.

A: You can use the dstdomain acl and always_direct tag for this purpose:

```
acl localservers
dstdomain
.incoming-
traveller.com
always_direct
allow
localservers
```

Securing against Brute Force Hacks

Like other System VR4 UNIX operating systems, Solaris keeps account information in two files:

- A globally readable /etc/passwd file containing noncritical data such as the account name, default shell, user ID, and group ID.
- An /etc/shadow file for the account passwords, password expiration dates, and other critical account data.

Creating Daily Reports

There are many excellent ways to automate the process of reviewing log files. One very popular application is called *swatch*. This application gets its name from the term *simple watcher* and *filter*. It was written in Perl by Todd Adkins and can be found at www.stanford.edu/~atkins/swatch. Swatch is easy to install and configure and can be very helpful in monitoring your log files and alerting you to potential problems.