Wellington Linux Users Group

Intro to Computer Security

Ed Hintz
Unix Sysadmin, IAM

Topics

- Scope/intended audience
- Why bother?
- Users in Unix
- Passwords and permissions
- Services/Daemons
- Firewalls
- Updates/mailing lists

Scope/Intended Audience

- This presentation aims to give a novice computer user, or a intermediate user new to unixish operating systems, an introduction to some basic concepts of security and management. It is not intended to be the final word; if you are securing machines for the NSA you are beyond this presentations scope. Various distributions will have their own methods of doing things, this talk intends to be a general introduction

Why bother?

- Liability/silent black helicopters/all expenses paid vacations at Guantanemo Bay
- Reliability-r00ted machines are slow/ unstable, used to the detriment of the net
- Certainty of attack-honeynet statistics
- Finance-downtime, bandwidth charges...
- Desire to be a good citizen

Users in Unix

- Root (w00t) == the LORD GOD almighty
- Mortal men/women/hamsters
- Groups
- sudo/su (sudoers/suauth)

Passwords

- Bad: favourite rugby team, wife/dog/cat/kid's names, words in the dictionary, dictionary+1337 5p34k
- Good: truly random (multitudes of generation software), randomizing stunts (phrase 1st letters, keyshifting, etc)
- Best: Disallow remote password use altogether, use only SSH pub/priv keys or one time passwords

Permissions

```
-rw-r--r--  1 kevin  users          114 Aug 28  1997 .zlogin
1st bit - directory?              (no)
 2nd bit - read by owner?          (yes, by kevin)
  3rd bit - write by owner?         (yes, by kevin)
   4th bit - execute by owner?       (no)
    5th bit - read by group?          (yes, by users)
     6th bit - write by group?         (no)
      7th bit - execute by group?       (no)
       8th bit - read by everyone?       (yes, by everyone)
        9th bit - write by everyone?      (no)
         10th bit - execute by everyone?  (no)
```

- Also-suid and sgid

(Image courtesy of the Linux HowTo)

Services/Daemons

- What are they?
- Why are they?
- Where are they?
- Are unnecessary ones on?

What/why are they?

- Software running in the background. May provide things like XWindows (the graphical user interface in linux and most unixes), login services, maintenance, hardware interfaces, etc.

Where are they?

- The daemons themselves may be in many locations, most likely /sbin, /usr/sbin, and possibly /usr/local/sbin. Control under a SysV unix (linux generally follows this model) will have start/stop scripts in /etc/rc.d/init.d, with symlinks from the various rcX.d directories for use at startup. Most distros will have a graphical management facility to simplify this, it is your friend.

Are some unnecessary?

- Once you know what's on, google it, find out what it does. If you don't need it, turn it off. Example: Apache, the unix www server. If you're not running a webserver, you don't need it, and it's a possible avenue of entry to your machine.

Huh? What's a firewall?

- Internet traffic to your box will likely use TCP/IP (Transmission Control Protocol/ Internet Protocol). A firewall can be used to block traffic to your machine. Note that many consumer broadband routers will provide some firewall functionality(usually NAT/rfc1918 solutions), but it is good practice nonetheless to use a local host based filter of some sort.

Firewalls

- Last line of defense. If you've already turned off unneeded services, theoretically you may not need the firewall, but it's a good idea to provide some redundancy. Most likely you will be using iptables to filter your network traffic, check your distros documentation for management methods. Many if not all will have a graphical utility to simplify it.

Mailing lists/updates

- Most distros have a mailing list for infosec updates. Subscribe to it. Be clued.
- Apply updates as they come available

Summary

- Moderate work and due care will make you a harder target. Kiddi3z like easy targets and will move on. This will make your life a peaceful contented existence, conducive to the consumption of alcoholic beverages (read: beer).

Questions/Resources

- Linux howto: http://www.tldp.org/HOWTO/Security-HOWTO/file-security.html
- Securing a fresh install: http://docs.linux.com/print.pl?sid=04/04/15/1913248
- SecurityFocus: http://securityfocus.com/
- Google is your friend...