Practical Security for UNIX

Learn how to make your UNIX machine less insecure
January 19, 2000 7–9PM Room 1–190

Presented by the MIT Network Security Team
http://web.mit.edu/net–security/www/

Kevin Fu <fubob@mit.edu>
Geoff Goodell <goodell@mit.edu>
Angie Kelic <sly@mit.edu>

Reuse, Reduce, Resecure

- Prevention
- Detection
- Recovery
- Repeat

Security is Only as Strong as Your Weakest Link

The Course of an Attack

- Probe for Vulnerabilities
- Exploit Susceptible Service
- Execute Arbitrary Commands
- Use to Compromise Other Systems (optional)
- Brag to Friends on IRC (optional)

Awareness

- man pages
- OS–specific update lists
  - (example: redhat–watch–list@redhat.com)
- bugtraq (http://web.mit.edu:8008/menelaus/bt/)
- http://www.cert.org/
- security–fyi@mit.edu

Avoid Unencrypted Connections TELNET

- sends USER and PASS in the clear
- do not use
- about SSH

Avoid Unencrypted Connections FTP

- sends USER and PASS in the clear
- about Anonymous FTP
- incoming (writable) directories

Avoid Unencrypted Connections E–Mail

- sends USER and PASS in the clear
- classic pop and kpop
- Secure Sockets Layer (SSL)
- SSH Tunneling

About NFS

- Unencrypted
- Anyone can spoof arbitrary UIDs, GIDs.
- no_root_squash, all_squash
- SUID programs

Others

- slimming down inetd.conf
- checking rc scripts
  - chkconfig
  - init.d, starting and stopping
- rsh, rhosts

Tools

- tcp wrappers
- Tripwire (Tripwire Security Systems)
- SATAN (Wietse Venema & Dan Farmer)
- COPS (COPS)
- Crack
- nmap (Fyodor)

Good Habits

- Smart Passwords (handout)
- When possible, avoid using root account
- If possible, perform backups
- Monitor Log Files

Log Files

- see one–sheets for examples
- some things to look for
  - missing logs
  - suspicious entries
  - odd time stamps
  - repeated connection attempts
- tools for automated log parsing

Suspicious Activities

- look for IRC processes, BNC, BitchX, sniffers, etc.
- system programs such as ls, ps, top, find, etc. may be trojaned!
  - tripwire may help (if you install prior to the breakin)
  - keep extra clean binaries on hand, like on a floppy
  - look for reports that do not reflect poor system performance

Suspicious Files

- things to look for
  - IRC clients and related items (e.g. BNC, ircii, epic)
  - Sniffers (linsniffer, raarpd, tcpdump, sniffit, etc.)
  - Directories with odd names (e.g. "...", ". ")
  - Suspicious directories in odd locations (e.g. /dev)
- find options (e.g. "find /usr –ctime –10 –print")
- rpm –v (in RedHat Linux)
- about "rootkits"

Intrusion Recovery

- Disconnect from network immediately
- Do NOT delete evidence. Preserve to trace the origin of the intruder.
- Notify net–security@mit.edu
- Your operating system will need to be reinstalled to eliminate stealth back doors (whenever root–level access is attained).

Useful References

- ftp://ftp.cert.org/pub/tools/
- http://ciac.llnl.gov/
- http://www.cert.org/
- http://www.first.org/
- http://l0pht.com/
- http://www.2600.com/
- http://web.mit.edu/net–security/www/