AlphaNet
Solutions

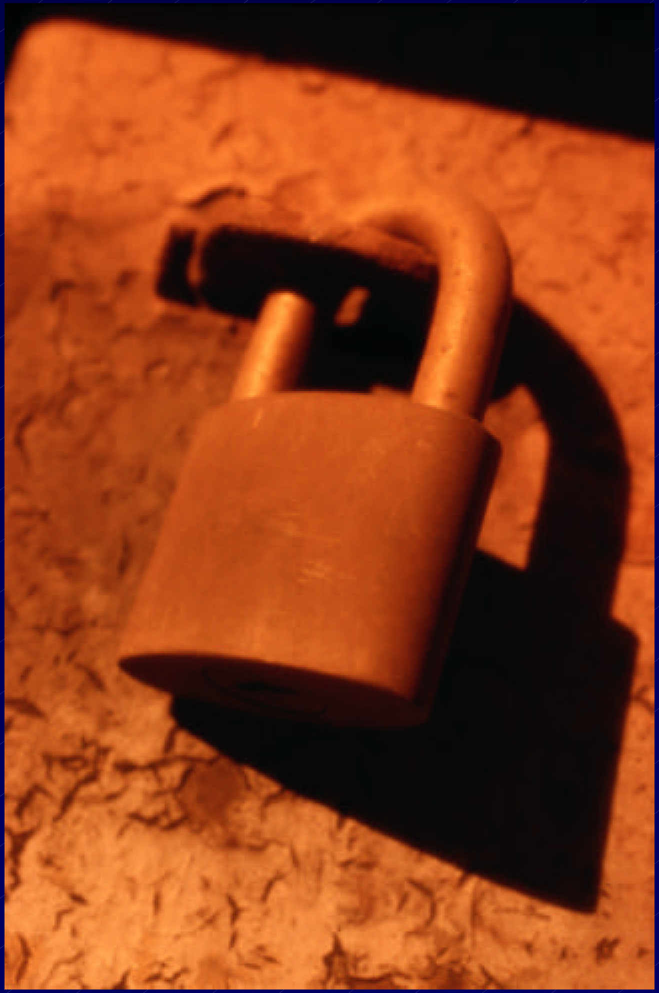
Securing (Hardening) Windows Servers

January 22, 2002

JP Vossen, CISSP
AlphaNet Solutions
800-AlphaNet
security@alphanetsolutions.com
http://www.alphanetsolutions.com/

Agenda

- What is Hardening?
- Why should I do it?
- A Generic Hardening Process.
- The Importance of Testing!
- Differences between NT 4.0 and 2000 (e.g. SCE/SCM).
- Hardening Internal Servers.
- Hardening IIS Servers.
- Hardening Windows to be a Firewall Platform.
- Q&A



What is Hardening?

- Hardening is the process of tightening the security of an operating system from the default “out of the box” configuration to an appropriately secure level.
- Sometimes known as securing or locking down.

AlphaNet Solutions

Why should I do it?

- Most modern Operating Systems are configured for ease-of-use—NOT Security—out of the box.
- One part of a “Security in Depth” approach
- “Security through Obscurity” is NO security at all!
  - See http://project.honeynet.org/papers/stats/
  - NBT Name Scans (port 139/TCP) on my iDSL link at my **house**:
    - Sep 2001: 34 (1.1/Day) Oct 2001: 160 (5.2/Day)
    - Nov 2001: 96 (3.2/Day) Dec 2001: 82 (2.6/Day)
    - Jan 2002 (to 1/21/02): 44 (2.0/Day)

Why should I do it? (Cont.)

- Hardening is a demonstration of “Due Care” and “reasonable and prudent precautions”
- CSI/FBI Computer Crime and Security Survey 2001
  - “Conventional wisdom says “80% of computer security problems are due to insiders, 20% are due to outsiders.”
  - “But for the fourth year in a row, more respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%).
  - “But is the threat from the inside actually decreasing?”
  - “It would be premature and dangerous to assume so.”

A Generic Hardening Process

- Pre-implementation: Segregation of Data
- Implementation/Installation: Install only things that are absolutely necessary
- Hardening:
  - Install all Service Packs/Hotfixes, etc.
  - Disable all unnecessary services/devices/accounts
  - Enable appropriate password settings (esp. Service Accounts!)
  - Enable appropriate logging/auditing
  - Use the concept of “Least Privilege”
    - Admin Accounts (esp. Service Accounts!)
    - User Rights (Beware the “Everyone” Group!)
  - Enable “extra” security settings (e.g. Warning Banners)
  - Tighten NTFS/Registry permissions
  - Implement Time Synchronization

AlphaNet Solutions

The Importance of Testing!

- It is **extremely easy** to corrupt a Windows system beyond recovery when hardening it.
  - NTFS Permissions
  - Registry settings/permissions
- Never attempt to establish or test hardening procedures on a production box! Ever!
- Ghost is your friend!
- Did I mention “Never attempt to establish or test hardening procedures on a production box?”
- Ever!

Differences between NT 4.0 and 2000

- In NT 4.0 SCE/SCM is not available by default. It was first made available on the SP4 CD-ROM.
- It was back-ported from 2000.
- It changes the NT 4.0 NTFS permissions DLL from the old NT 4.0 style to the new Windows 2000 style—e.g. inherited permissions. This is not always desirable.
- The un-patched version has significant bugs and issues (see resources).

Hardening Internal Servers

- Never install IIS unless the server is to be a dedicated Web Server, and then segregate data!
- Hardening:
  - Install all Service Packs/Hotfixes, etc.
  - Disable all unnecessary services/devices/accounts
  - Enable appropriate logging/auditing
  - Use the concept of "Least Privilege"
    - Admin Accounts
    - User Rights (Beware the "Everyone" Group!)
  - Consider enabling "extra" security settings
  - Consider tightening NTFS/Registry permissions

Hardening IIS Servers

- Never install IIS unless the server is to be a dedicated Web Server, and then segregate data!
- Perform all hardening as above for an internal server, except more stringently.
- Consider moving critical tools out of default locations.
- Harden IIS (see references).

Hardening Windows to be a Firewall Platform

- Firewall servers **must** be dedicated boxes that run only the firewall software!
- Never, ever, EVER run IIS on a firewall server!
- Perform all hardening as above for an internal server, except more stringently.
- Disable NBT (AKA MS Networking).
- Disable virtually all services and devices.
- Lock down NTFS permissions (easy!).
- Consider moving critical tools out of default locations.

Gartner Group on Firewalls

- “By 2003, the dominant means of deploying network security technology will be through the use of appliance technology.”

Q&A, and Resources

- See my “Windows Security Scripting” article in the February issue of *Information Security Magazine*.
- See resources list in the Handout.
- *Securing Windows NT/2000 Servers for the Internet*, by Stefan Norberg, O'Reilly & Associates