

Integrating Network Security into your Site

Rich Pinder Los Angeles Cancer Surveillance Program rpinder@usc.edu

NAACCR Annual Meeting - Informatics: Methodology

June 12, 2002

Toronto

Objectives

- Big Picture thoughts on Security
- Components of organization wide security
- Rich's 'Top 10'



Big Picture thoughts on Security

■ "Security - it's TOO complicated !!!"



- Doing nothing no longer acceptable.
- Its HUGE. But why not take it piece meal ? Something BETTER than nothing!
- Little money? Few hours of the techies? Couple days time?? Hire a techie???
- YOU CAN DO IT !!!



- Start small go to the informational websites (look for .org and .gov sites) and search for 'getting started'.
- Decide which steps you can handle
- Consultants sources

 Attend local user groups _nix

 Los Angeles costs ~ 100/hr



Objectives

- Big Picture thoughts on Security
- Components of organization wide security
- Rich's 'Top 10'



Components

- User authentication and environment
- Filtering Port & Process control
- **■** Firewalls
- Encryption
- VPN & Tunneling



■ User authentication and environment

- Password protect ALL machines!
- One point login using to multiple systems can be dangerous (breach on weak machines obtains same password used on hardened machines). Long. Complex. Changing (???).
- Use password policy programs
- Biometrics promises both higher security and easier use.



■ User authentication and environment (cont)

Environment

User Training & Awareness

Part of your annual confidentiality briefings

Ramifications of bad practices

User Accountability

Commitment to compliance



■ Filtering - Port & Process control

- Control the 'doors' to your computers
- Should be done for all systems.

 Should be done for all ALL A L L major systems!
- Software to do this exists for your system
 (IPSec on WinNT/2k IPChains/IPTables on Linux)
- Rules: Incoming Outgoing Forward...

 For ALL start with DENY



■ Filtering - Port & Process control (cont)

- Limit what's running on your computer KILL Unecessary Services! (watch default installs)
- Port Scans reports tell which 'doors' open
- Threat assessment goes one better tells you what's open, and what to DO about it.
- Even some 'Automated Mitigation' software to take action on the threat assessment report
- Computer Virus considered uncontrolled processes



■ Firewalls

- There are really no flames involved!
- Firewall is Centralized Filtering typically hardware and software solution. (Same software as we discussed for Filtering)
- Two NIC's pass through design
- Not a panacea! As soon as they're in place,
 requests to bypass them come in!
 Modifications can induce error.



■ Encryption

- Why send info in 'plain text' when you can send it Encrypted ?

Pgp - public key type encryption we've heard about for a long time (GPG better alternative?)

'public' key algorithm necessary to share with others with out knowing the key.

But it's slow - for highly efficient applications, still use symmetric based keys



- Virtual Private Network (VPN) & Tunneling
 - Defines a secure interconnected conduit
 between geographically separated systems
 - Based on encryption
 - Includes Filtering concepts

Allows multiple (and future) applications to operate securely - similar in concept to using your 'server' at work

 Often implemented to allow secure email and network access for home users



Objectives

- Big Picture thoughts on Security
- Components of organization wide security
- Rich's 'Top 10'



Top 10

- Make a security commitment to do something when you get home! Start a "Security Procedures" manual document what you do.
- Do User Training & Authentication Hardening access control
- Don't use Telnet & Ftp. Get SSL enabled apps to substitute. (SSH, SCP)
- Use (and keep CURRENT) virus control software (Symantec or McAffee)
- Encrypt ALL confidential data that you send from your organization.
- OS diligence upgrade machines to at least windows NT.

 Install current patches. Document. Consider using alternatives to Brother Bill's operating systems.

Top 10

- Run vulnerability scanners (ie Nessus). Compare reports to the SANS/FBI top 20 vulnerabilities list and be SURE to mitigate the biggies
- Port filtering Cheap: Install / configure IPSec for windows servers & IPChains or IPTables for Linux servers. Expensive: Do 'Cheap' AND install dedicated Firewall machine. Router: Have your network folks be sure the routers and switches are configured properly
- Wireless? Secure the access point! (they come initially wide open). If not implemented yet, look at 802.11b spec with WEP2 security.
- DSL connections. Home lines use personal 'firewall' software', or VPN if possible.



Security Resources

■ SANS - GREAT site

http://www.sans.org/

System Administration, Networking and Security - since 1989

SANS incident site: http://www.incidents.org/

Good starting place: http://www.sans.org/newlook/publications/roadmap.htm

Top 20 security issues: http://www.sans.org/top20.htm

■ Technical Tutorials

http://www.systemexperts.com/tutorial.html

Hodgepodge tutorial..great for showing what OTHERS are looking to do to get into your site.

■ Good source of info: (not just for linux)

http://www.linuxsecurity.com/



Security Resources (cont)

■ Government / University information sources

National Security Agency

http://www.nsa.gov/isso/infosec

Windows 2000 security guidelines, including actual inf files that can be applied to deal with config / domain /admin stuff

CERT

www.cert.org

Carnegie melon Software Engineering Institute

See the 'tech tips' section - sign up for mailing list

National Infrastructure Protection Center

http://www.nipc.gov/

Computer Security Institute (CSI)

http://www.cisecurity.org

- Fee based - \$250/yr (but some good stuff for free)



Security Resources (cont)

■ Filtering - port and process control

http://www.nessus.org/ Nessus port scaner and threat assessment tool
http://www.tinysoftware.com relatively inexpensive - \$39 for new version.
Zonealarm has free version still... but 'best' versions around same price.
Deerfield, Norton (Symantec), Black Ice, Zonealarm, Tiny Personal firewall... all available

http://www.citadel.com Hercules - a threat mitigation tool

■ Locating user groups

Linux user groups: www.ssc.com/glue

Unix user groups: http://dark.wustl.ecu/~newton/othruug.html

http://www.netip.com Keith Palmgren page Check out Articles & Security
links pages

■ Virtual Private networks

http://www.vpnlabs.org see their 'Primers' section - 'how stuff works' site good one.

