

# *Network Security Using Linux*

Mike Sweeney  
Packetattack.com



# *Issues Regarding Network Security*

- Network Security is an ongoing issue.
  - Network Security can be overly complex.
  - Network Security can be very costly.
  - Network Security can have multiple solutions.
  - Network Security can be misunderstood.
- 
-

- IT departments rarely have the required budget to implement effective network security until it's too late.
  - IT staff is rarely given the proper amount of time to implement network security correctly.
  - Administrators rarely have the full skill set needed to effectively install, configure and manage network security solutions.
  - Simple and cheap solutions are often overlooked in favor of flashy and expensive solutions.
- 
-

# *Goals of Network Security*

- Easy Management
  - Provide strong ROI for budget justification battles.
  - Keep the bad guys away
  - Keep the honest folks honest on your network
  - Network stability while providing security
  - Transparency to user community
- 
-

# *Current Network Security Practices*

- Defense in depth (layers)
  - Islands of Security
  - Harden Servers
  - Effective Backups for intrusion recovery
  - Patching applications and operating systems
  - Use current networking technology and security practices
  - Effective use of tools such as Etheral and Nessus
- 
-

# *How to implement Network Security*

- ◆ OS /Application Issues and Solutions
    - YUM, APT, Up2date, Patch-o-matic for iptables
    - Use recent kernel, not bleeding edge or development
    - Build from source files, not from packages unless absolutely trusted source
    - Use signature tools such as MD5SUM to verify files
    - Lock down applications such as disabling the network listener in MySQL when it is not required
- 
-

# *How to implement Network Security*

- ◆ Effective Positioning of Security
  - Firewalls at perimeter and high-risk resources
  - IDS on each network segment
  - Log servers on their own subnet with ACLs
  - Use of out of band management if possible
  - Physically secure servers
  - Isolate dial-in access through access control
  - Isolate wireless network

# *Harden the Server*

- Install Linux as minimum or use custom install
    - This gives you less to harden or to remove.
    - Install new packages from source to maintain control over where and what is being installed.
    - Get your source files from trusted sources and use the MD5 signatures to verify file integrity.
    - Use a script engine such as Bastille Linux to harden permissions of files, directories, adjust user rights and tighten up overall security.
    - If existing Linux installation is to be hardened, audit all processes and packages installed.
- 
-

# *Harden the Server*

- Use **chkconfig –list** to show running processes
- Normally you can shut down these services but it will depend on the business needs:
  - nfs
  - nfslock
  - kudzu
  - pcmcia
  - httpd
  - telnet
  - isdn
  - rlogin
  - smb
  - sendmail
  - named
  - autofs
  - gpm

# *Inspect and Deny*

- There are some basic rules for firewalling network resources:
  - Deny all traffic unless specifically allowed.
  - Block inbound packets with private or internal IP addresses.
  - Block outbound traffic that has an external IP address.
  - Allow SMTP outbound for email but only allow specific ip addresses for inbound SMTP traffic.
  - Allow all proxy traffic out
  - Allow DNS UDP queries and answers from internet DNS servers

# *Test and Test Again*

- Never ever assume that life is good on your network without actively testing it.
  - Learn to use the various tools available to you such as nmap, nessus and ftester to help find and plug holes.
  - Scan the security boards to see how the latest attacks take place and see if they apply to your network.
  - Don't think just about the outside, the majority of intrusions take place from within the organization.
- 
-

# *Log everything*

- Configure and use NTP (network time protocol) for accurate and legal time stamps on the log files.
  - Configure a logging server that only appends the log files and uses ACLs to only receive the data to keep a secure copy of all the log files.
  - Use available tools and/or replacement syslog servers to aid in automating auditing of syslog files.
  - Log network traffic to build trends and send alerts when traffic exceeds normal trending.
- 
-

# *Actions*

- Consider setting up internal security using X.509 privately signed digital certificates.
  - Audit log files daily and have automated tools or scripts watch for tell-tale signs of intrusion or compromise.
  - Test, test and test again. Learn what is normal so you can tell when something is not normal.
  - Cruise the newsgroups for possible solutions. You are not the first one with this problem, whatever it is.
- 
-

# *Credits*

- This presentation was made using:
  - Apple OSX 10.4 Tiger
  - NeoOffice/J 1.4
  - Fedora Core 1
  - Virtual PC
  - VMware 5.0 Workstation