LINUX Operating System Audit & Assessment
August 9, 2006

NEbraska CERT Conference 2006
Computer Security and Information Assurance

www. lsat.sourceforg net (LSAT).

www .bastille-linux.org (Jay Beale)

(today's script 8.4)

No longer completely free:
www.cisecurity.org

Standard disclaimer, "'I never said THAT, and if you did THAT, and something broke, it's your own durn fault. Also, the views expressed here are mine, not my past, present or future employer's, and not the conference sponsor, nor any quail hunting partners. When using any tool, do no harm."

Michael T Hoesing CISA, CISSP, CIA, CCP, CMA, CPA

m-hoesing@cox.net (402) 981-7747

Learning Objectives

- Define an Audit Approach/Methodology
- Determine Audit Goals, Objectives, Scope
- Individual Tests to Achieve the Goals (7)
- Other Resources
- Auditing Example – an independent assessment process (take home scripts)

Audit Approach

- Determine Key Success Criteria (objectives)
- Define System Under Review (scope, LINUX, file server, web server, both)
- Assess Risk (focus test resources where appropriate)
- Gather Standards (policy, procedures, regulation, contracts)
- Inventory the Current State (the scripts)
- Compare the Current State to Standards (analysis)
- Investigate Differences (reporting, correction)

Audit Objectives and Risks

• Authorized User Access	High
• Authorized Services, Daemons, Modules	High
• Authorized Networking/Connections	High +
• Authorized File Access	High
• Appropriate Recording/Logging	High
• Appropriate Security Parameters	High
• Authorized Applications	High

Scope

- Which Systems ? (risk based)
- How much time for each system?
- How much sys admin time for each system?
- How Long of a Duration?
- Who approves scope expansion?

Standards (if you don't have them the auditor will be happy to set them for you)

- Organization Policy, Standards, Procedures
- Regulation
- Contractual Requirements
- Industry Best Practice
  - Center for Internet Security (CIS) [Jay Beale] Linux Benchmark Standards
  - http:// **www cisecurity.org** standard is free
    assessment script is not free (version 1.6.8 on disk)
    approach = compares to specific metrics
    (8.3 password maximum days > 90 shows as negative)
  - Bastille now has an –assess option

Other Standards Resources

- More industry standards http:// www. linuxsecurity.com
- 8/05 Jay Beale contributor **LINUX Security, Audit and Control Features** http://www.isaca.org/bookstore
- Auditing Linux – Krishni Naidu http:// www.sans.org/score/checklists/AuditingLinux.doc
- SANS.ORG - Paul Santos http:// www.sans.org/rr/papers/index.php?id=81
- Raul Siles www. giac.org/practical/GCUX/Raul_Siles_GCUX.pdf/

LINUX Tests – User Access

- Who can be on the system, match to job function?
- Who is on the system right now?
- Password encryption in use?
- Who can be root?
- From where can root access the system?
- What default and group ID's are present?

LINUX Tests – Services

- What services were loaded at startup?
- What processes are currently running?
- What services are set to run?
- What modules are loaded?
- What is accessing the CPU currently?
- What jobs are scheduled to run?

LINUX Tests – Networks/Connections

- What networking devices are attached?
- What other hosts can connect to the system under review?
- What communication protocols are used?
- What routes are enabled ?
- Firewall enabled ?

LINUX Tests – File Systems

- What file systems are in use?
- Which files and directories are world writeable?
- What are the permissions on sensitive files & directories?
- What files were changed in the last day?
    1. Who changed it?
    2. Why, was that authorized?
    3. Was the change tested?

LINUX Tests – Logging

- What was recorded recently in the systems event log? /var/log/messages
- What other logs are available?
- Who can alter the log file?
- Where are logs stored?

LINUX Tests – Security Parms

- What automated password controls are in place?
  - /etc/login.defs
    - Min days password life
    - Max days password life
    - Password Length
    - Display last login time
    - Tries before lockout
    - Umask
    - motd (banner)
  - Password Strength? (suggest or force) character_class

LINUX Tests – Applications

- What applications are installed? (rpm)
- Are they running? (top)
- What malware is present? (chkrootkit)
- Are there any monitoring tools? (tripwire, FAM)

Other

- Test, test, test Before using the Script
- Flavors of LINUX (SuSE 8-9.3, 10.0, 10.1 Debian, Mandrake, SLES 8.1,9 and 10, Red Hat Enterprise 2.x, Fedora, …)
- Scripts gather information to discuss, they rarely produce reportable issues
- Portable to UNIX ?
- Time .2 – 40 minutes if not testing WW files
- CPU usage - minimal

Other Resources (cont)

- Seccheck – SuSE 9.x distros, nice password & shadow checking
- Hardening – EAL3 www.124.ibm.com/linux/pubs/ (many other LINUX topics)
- Hardening – LIDS www.lids.org
- Security Enhanced Linux – from NSA (SELinux) nsa.gov/selinux Fedora Core 4&5 install option
- Hardened Gentoo http://www.gentoo.org/main/en/about.xml
- Syslogs analysis = SNARE, Chksyslog, logwatch, router logs = mrtg-0.9.0
- Scanners = Netrecon, metasploit, chkexploit_1_13, nessus

Other Resoures (cont 2)

- Auditor Knoppix 3.8.1 Distro **w ww.remote-exploit.org/index.php/Auditor_main** June 20, 2005
- phlak.org 0.3 CD distro with tools
- http://www.linux-sec.net/Harden/harden.gwif.html
- www,linux-sec.net/distro/ variety of linux distributions
- Linux from scratch www.linuxfromscratch.org
- LSAP.ORG volunteers desk checking code
- anti-exploit-1.3 file listener
- **www.aduva.com** Soundcheck (dependancy check)
- **http://h20219.www2.hp.com/services/cache/109962-0-0-225-121.html** HP Linux Security Assessment $250/hr

Show Tool Results Here

- Show the Audit Program
- Show the Script File
  - MTH 8.4 (w chkrootkit 46a)
  - LSAT 0.9.3
  - Bastille 3.0.8-1.0
  - CIS 1.6.8 (not updated since 2005)
  - Nessus 3.0.3
- Run the Scripts
- Compare Results to Standards

Questions

- ?? (now that Bill is retiring ,who is going to demo new “blue-screens” at conferences?)
- ??
- ??