Today's Meeting August 11 2005

- The game plan for today's dynamic, fast track, off site meeting is to provide etched in stone exposure to those demographically heads up elite who think outside the box regarding the best of breed and best practice techniques to drill down into the LINUX operating system metrics to provide a no brainer prototype deliverable that can add value to a scale where the recipient can be viewed as a leveraged top down virtual fault tolerant market leader in profitability.

- Do LINUX, impress someone
- No Microsoft employees were harmed during the making of these slides

LINUX Operating System Audit & Assessment CERTconf 8/10/2005

www. lsat.sourceforg net (LSAT).

www.cisecurity.org (Jay Beale)

www .bastille-linux.org (Jay Beale)

Http:// www nebraskacert com/ presentations/ 2005/ Wednesday (today's script 8.2)

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

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

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. When using any tool, do no harm."

Learning Objectives

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

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 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

- Organization Policy
- Regulation
- Contractual Conformance
- Industry Best Practice
  - Center for Internet Security (CIS) [Jay Beale]
  - Linux Benchmark Standards & Scoring Tool
  - http:// www.cisecurity.org v1.6.8
    different approach = compares to specific metrics
    (8.3 password maximum days > 90 shows as negative)
  - Bastille now has an –assess option

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 GOD (root)?
- From where can GOD (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 – Connections

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

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?

LINUX Tests – Security Parms

- What automated password controls are in place?
  - Min days
  - Max days
  - Length
- What environment controls are in place?
  - Last users
  - shells

LINUX Tests – Applications

- What applications are installed?
- What malware is present? (checkrootkit)
- Are there any monitoring tools? (tripwire)

Scripting Hints

- User Interactive
- Predict and Deal with Errors, capture errors
- Determine if a file or directory exists before executing a command

Other

- Test, test, test Before using the Script
- Flavors of LINUX (SuSE 8-9.3, Debian, Mandrake, SLES 8.1 and 9, Red Hat Enterprise 2.x, Fedora)
- Portable to UNIX ?
- Time .2 – 40 minutes if not testing WW files
- CPU usage - minimal

More Other

- More industry standards
  http:// www. linuxsecurity.com
- 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/
- C2 Secure Logging (auditing) for LINUX [SAL]
  http:// secureaudit.sourceforge.net

Other Resources (cont)

- Seccheck – SuSE 9.x distros, nice password & shadow checking
- LSAT Linux Security Audit Tool freshmeat.net/projects/lsat
- Hardening – Bastille www.batile-linux.org (Jay Beale) **(assessment now)**
- 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
- SNARE – Log Analysis sourceforge.net/project/showfiles.php?group_id=39535
- Syslogs analysis = 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
  www.remote-exploit.org/index.php/Auditor_main
  June 20, 2005
- phlak.org 0.3 CD distro with tools
- 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)

Start Script Demo Here

- Show the Audit Program
- Show the Script File
  - MTH 8.2
  - LSAT 0.9.2
  - Bastille 3.0.4-1.0
  - CIS 1.6.8
- Run the Script
- Compare Results to Standards