Securing Linux Systems Before Deployment

Richard Williams

Senior Support Services Specialist

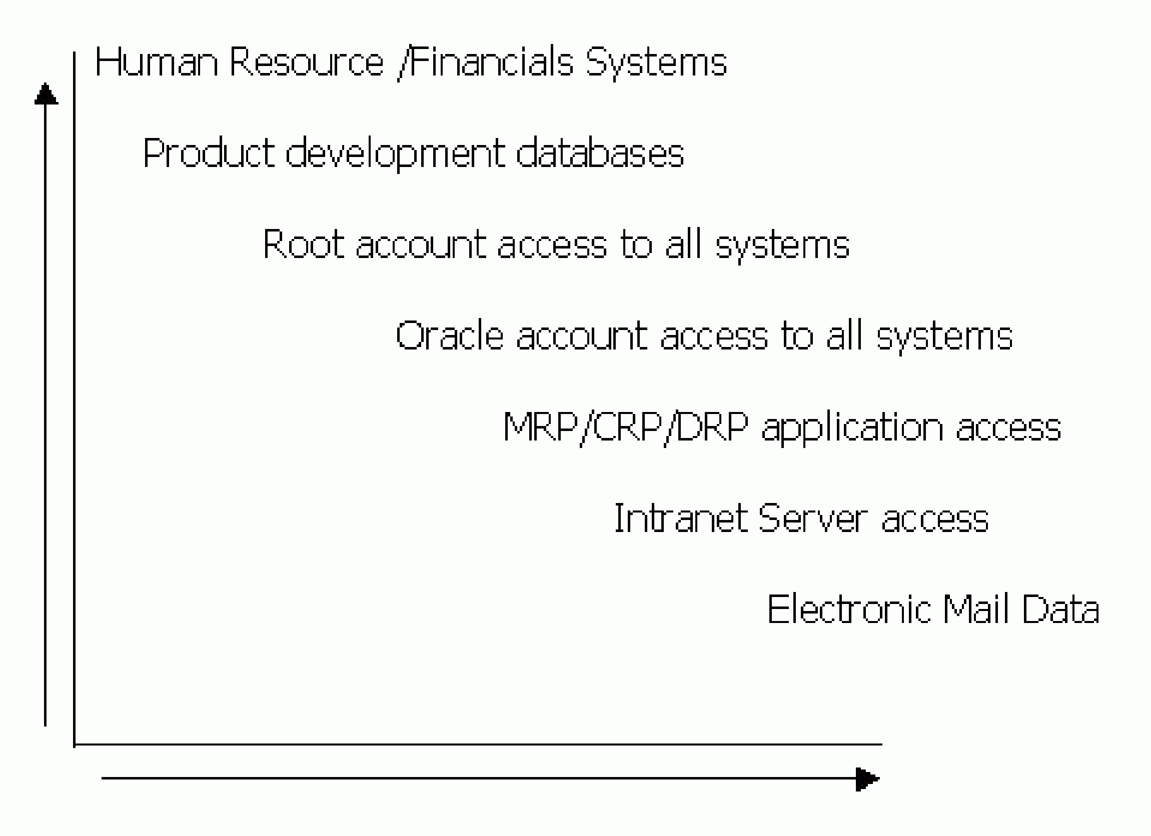
Symark

Why secure Linux systems?

- Your Linux enterprise installation is growing
- Assets on Linux systems are becoming increasingly more valuable as enterprise applications support Linux
- Current organizational security plans do not necessarily address Linux-specific concerns, although Linux may be on their IT roadmap
- Emerging financial audit requirements do not specifically address Linux
- Regulatory and legislative regulations do not specifically address Linux

The Increasing Importance of Linux Security

- What are the information assets you would least like to lose?



Human Resource /Financials Systems

Product development databases

Root account access to all systems

Oracle account access to all systems

MRP/CRP/DRP application access

Intranet Server access

Electronic Mail Data

Information Security Requires Executive Direction

- Executive Staff should establish overall direction in protecting assets
- Establish “Standards of Conduct” for maintaining information security
  - Information Management: should correspond to regulatory requirements
    - Name and description of data
    - Responsible department
    - Required length of storage
  - Information Asset Clarification: classification level and owner
  - Should identify what is and is not allowed outside of the organization
  - Should include merits as well as disciplinary actions

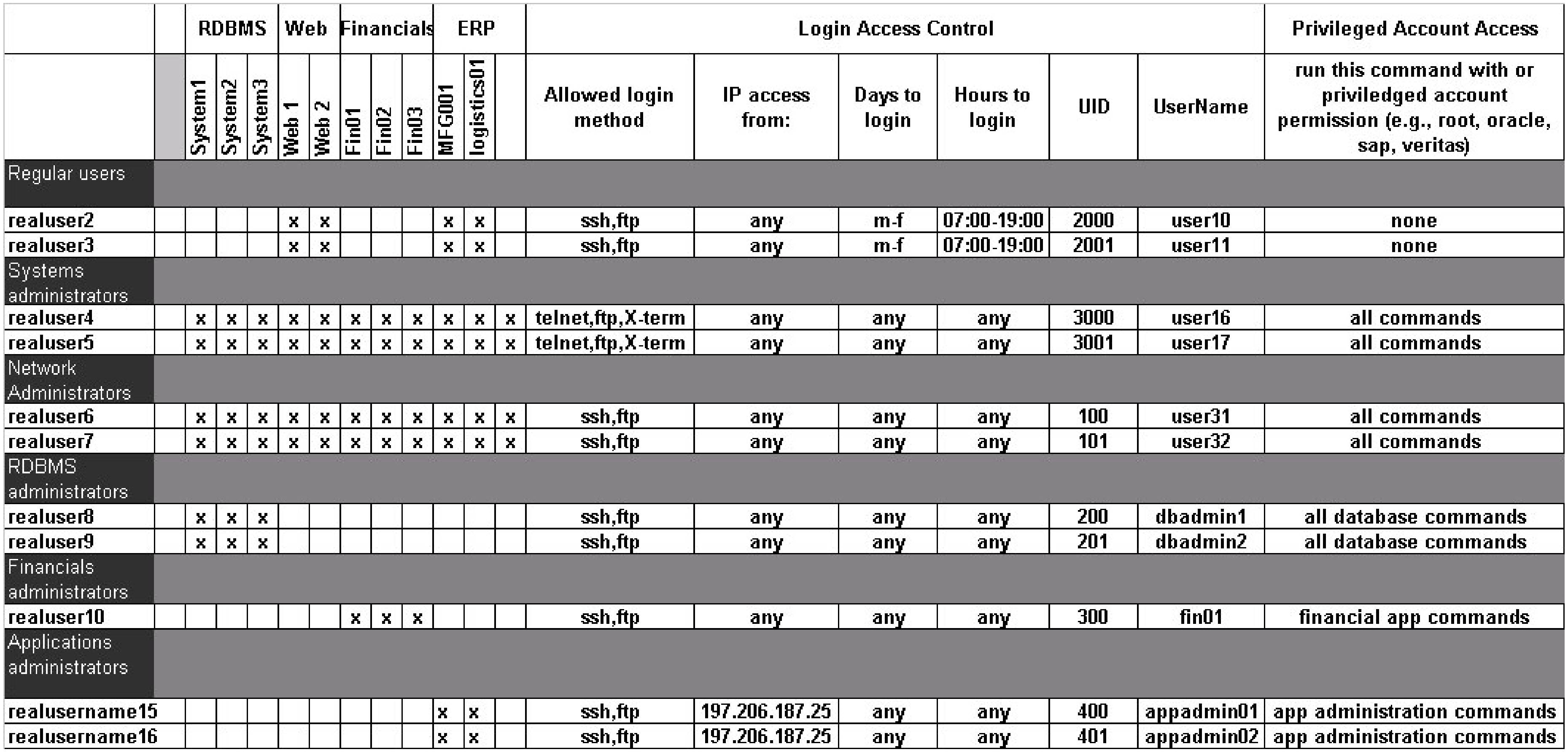
Introductory Security Planning Before Deployment

- Understand departmental needs
  - e.g., R&D needs secure remote access, legal needs to securely dispose of digital information
- Identify one internal source for policy ownership
  - Typically different departments have their own policies causing inconsistencies
  - Should always be Information Security Department
- Centralized information security training
  - Consistency is absolutely essential as the organization gets larger
  - Any department (HR) can do the training as long as IS is the publisher of the policies
- Buy in from above
  - Executive champion to give policies weight

Detailed Security Planning Efforts

- Diagram the “who, what, when, where, and why” for system access by users
- Include commands allowed per user (or group)
- Include access methods allowed per user (or group)

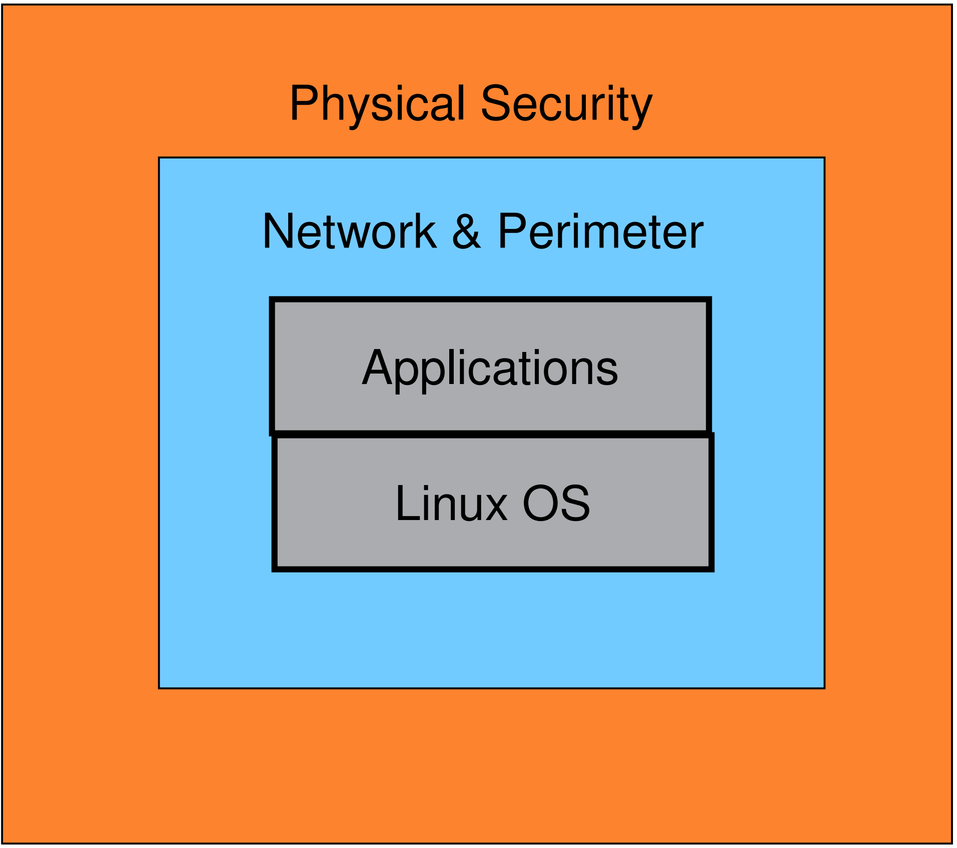
Detailed Security Planning Efforts



		RDBMS			Web		Financials			ERP			Login Access Control						Privileged Account Access
		System1	System2	System3	Web 1	Web 2	Fin01	Fin02	Fin03	MFG001	logistics01		Allowed login method	IP access from:	Days to login	Hours to login	UID	UserName	run this command with or priviledged account permission (e.g., root, oracle, sap, veritas)
Regular users																			
realuser2					x	x				x	x		ssh,ftp	any	m-f	07:00-19:00	2000	user10	none
realuser3					x	x				x	x		ssh,ftp	any	m-f	07:00-19:00	2001	user11	none
Systems administrators																			
realuser4		x	x	x	x	x	x	x	x	x	x	x	telnet,ftp,X-term	any	any	any	3000	user16	all commands
realuser5		x	x	x	x	x	x	x	x	x	x	x	telnet,ftp,X-term	any	any	any	3001	user17	all commands
Network Administrators																			
realuser6		x	x	x	x	x	x	x	x	x	x	x	ssh,ftp	any	any	any	100	user31	all commands
realuser7		x	x	x	x	x	x	x	x	x	x	x	ssh,ftp	any	any	any	101	user32	all commands
RDBMS administrators																			
realuser8		x	x	x									ssh,ftp	any	any	any	200	dbadmin1	all database commands
realuser9		x	x	x									ssh,ftp	any	any	any	201	dbadmin2	all database commands
Financials administrators																			
realuser10							x	x	x				ssh,ftp	any	any	any	300	fin01	financial app commands
Applications administrators																			
realusername15										x	x		ssh,ftp	197.206.187.25	any	any	400	appadmin01	app administration commands
realusername16										x	x		ssh,ftp	197.206.187.25	any	any	401	appadmin02	app administration commands

Layered Security Approach to Linux

- Physical Security
- Network Layer Security
- Operating System Layer Security
  - OS Configurations & Patches
  - User Accounts and Passwords
  - Access Control
- Application Security
- Complement layers with detailed Audit Trails
  - uid/processes
  - rpm/patches
  - User-specific audits for accountability



Physical Security

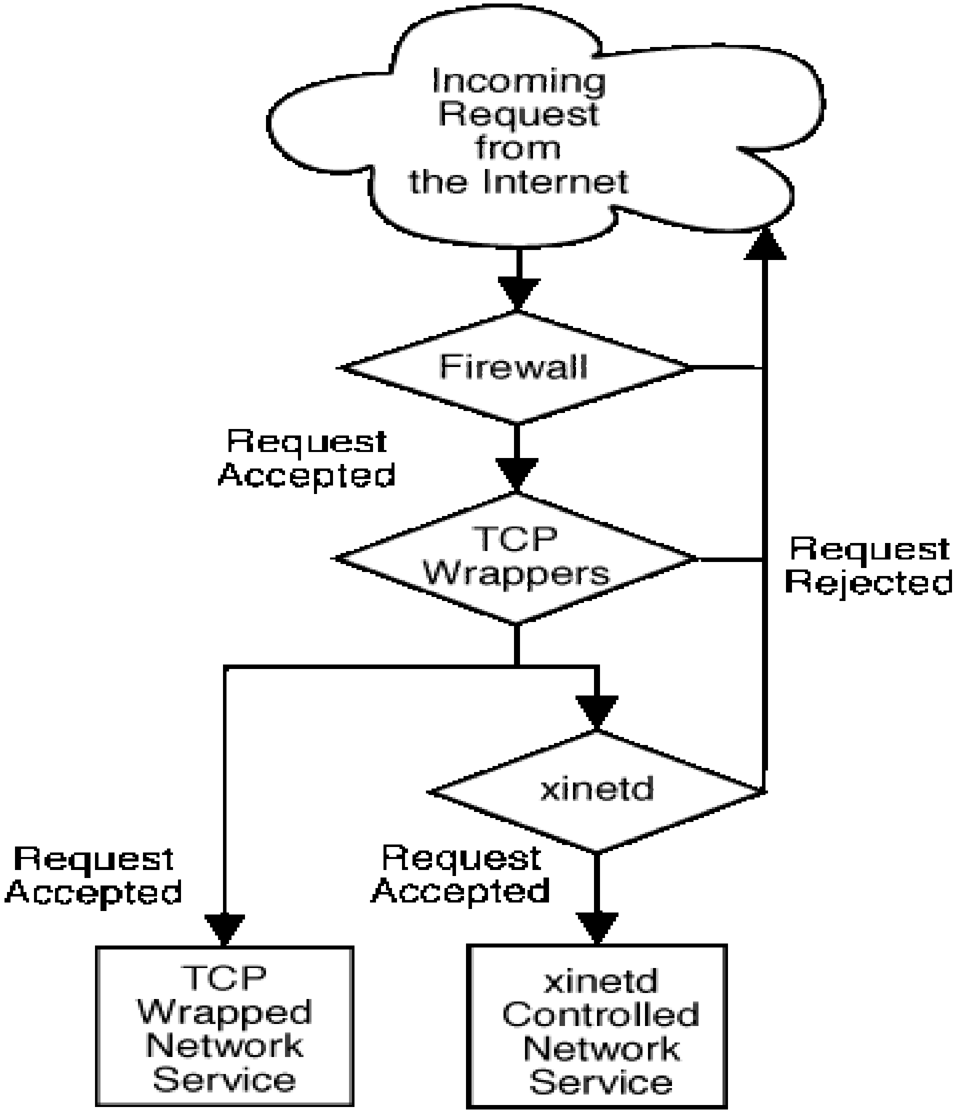
- Server rooms have limited access
- On/off keys removed from servers
- Racks closed and locked
  - Makes it more difficult to create a “denial of service” condition for a system simply by powering it off
  - Even if an intruder gains access to the server room, they cannot gain “single-user” root access by power cycling a system with a local terminal plugged into a console port
- Systems with consoles attached should be logged off, and systems with multi-console switches should be checked for any open sessions

Network Security

- Disable all unnecessary network services
  - Often inetd/xinetd.conf comes with many services enabled that are never used, or that have secure alternatives
    - Examples: echo, chargen, daytime, discard, talk
    - Can use netstat or lsof to identify other open default services
  - Disable telnet, FTP, TFTP, “r-commands”, and imap/pop
- Install SSH (www.openssh.org)
  - Configure so that both the ssh client and server are running only SSH protocol 2
  - SSH removes the need for any of the default inet services discussed above, like telnet, FTP, or r-commands

Network Security:

- Install TCP Wrappers
- ipchains and iptables
- Configure NTP


Incoming Request from the Internet
Firewall
Request Accepted
TCP Wrappers
Request Rejected
xinetd
Request Accepted
Request Accepted
TCP Wrapped Network Service
xinetd Controlled Network Service

Network Security

- ipchains and iptables
  - At first glance, ipchains and iptables appear to be quite similar. Both methods of packet filtering use chains of rules operating within the Linux kernel to decide not only which packets to let in or out, but also what to do with packets that match certain rules.
  - However, iptables offers a much more extensible way of filtering packets, giving the administrator a greater amount of control without building a great deal of complexity into the system.

Network Security

- NTP – Network Time Protocol
  - NTP is a protocol designed to synchronize the clocks of computers over a network.
  - NTP version 3 is an internet draft standard, formalized in RFC 1305.
  - NTP version 4 is a significant revision of the NTP standard, and is the current development version, but has not been formalized in an RFC.
  - Simple NTP (SNTP) version 4 is described in RFC 2030.

Linux OS Security

- Install latest OS patches from vendor
- Minimize or disable unnecessary boot services:
  - Email server
  - GUI login (xdm, cde)
  - X Font server (xfs)
  - Any other unnecessary boot services
  - Samba services
  - NFS daemon and client
  - NIS server and client
  - RPC tools
  - netfs
  - Print daemon
  - Web server
  - SNMP
  - DNS
  - SQL
  - Webmin remote administration
  - Squid web cache services
  - Kudzu hardware detection

Linux OS Security

- Kernel Tuning
  - Disable core dumps
    - Only required for developers’ systems; protect system information that may be contained therein
  - Restrict NFS client requests to only privileged ports
    - Blocks potential attacks while maintaining normal NFS activities
  - Network Parameter Modifications
    - Re-route default IP traffic routes

Access Control:
Securing User Accounts

- Disable infrequently used and orphaned accounts
- Verify no accounts with empty password fields
- Verify no UID 0 accounts exist other than root
- Verify no legacy "+" entries exist in passwd, shadow, and group files
- User home directories should be mode 750 or more restrictive
- No user dot-files should be group/world writable
- Remove user .netrc files
- Set default umask for users
- Remove unnecessary psuedo acocunts

Access Control:
Securing Passwords & Login

- Employ shadow passwords
  - Password encryption
  - Password aging
- Set LILO/GRUB password
  - Secure single user access
- Password security using PAM modules
  - Define specific character set requirements
    - Length, alphanumeric characters, punctuations, case
  - Account lockout on 3 or more failed login attempts
  - Use Dictionary (or other list) checking
  - Password history and reuse
  - Many other PAM modules available at:
    - http://www.kernel.org/pub/linux/libs/pam/modules.html.

Access Control on Linux: Securing Login Access Control

- Banner warnings at login
- Restrict root login to local console
  - Force remote users to login as themselves before “su”
- Remove .rhosts support in /etc/pam.conf
  - Restricts remote logins via PAM

Access Control on Linux: Securing Directories and Files

- Secure configurations for root and generic accounts
  - Disallow direct logins; require su
- Find unauthorized SUID/SGID system executables
- Set sticky bit for user file access
- Disable group and outside file access permissions
- Develop and implement ACLs
  - Determine what level of access is appropriate

Securing Applications

- Patches
  - Update open source applications like Apache and SendMail to close known security holes
- Generic accounts
  - Eliminate if possible
  - Ensure no hard coded accounts/passwords in programs
- Logging
  - Create a separate, secured log server with limited access
  - Always encrypt logs

System Logging

- Capture messages sent to syslog AUTHPRIV
  - Captures su attempts, failed login attempts and root logins
- Capture detailed FTP daemon logs (when using FTP)
- Confirm permissions on system log files
  - Protect these files from persons that should not view them

About Symark

- UNIX/Linux security experts
- Founded in 1985
- Large installed customer base of Global 2000 enterprises
- Technical Alliances with HP, IBM, Sun, RedHat
- Affiliations with SANS, CSI, MISTI

SC MAGAZINE ★★★★★

SOFTWARE 500 2003

This Week | Los Angeles Business Journal®

Symark Provides Access Control Solutions Across UNIX/Linux Platforms

PowerPassword, UME®

- Centralized UNIX/Linux user account management
- Detailed host login access control
- Password security policies
  - Aging & history
  - Define character sets
  - Random and one-time passwords
- Reset & synchronization
- Manage inactive/orphan accounts
- Account lock out
- SSH integration

PowerBroker®

- Delegate root privileges
- Delegate any account (e.g. Oracle) privilege
- Restrict access to 3rd party applications (e.g. CRM, ERP)
- Control access to files & directories
- Keystroke logging

Detailed logs

No kernel modifications

Central administration of uniform security policies

“ This is a standard quote slide… type your quoted content inside the quotation marks.”

Jordan Doe

CIO, ABC Company

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP