Linux Security

Patrick J Cush, PhD
Senior Architect
Novell, Inc.

Novell

Base Security for the Linux System

- Partitioning
- Loading Services
- User/Group Access
- Program/Service Access

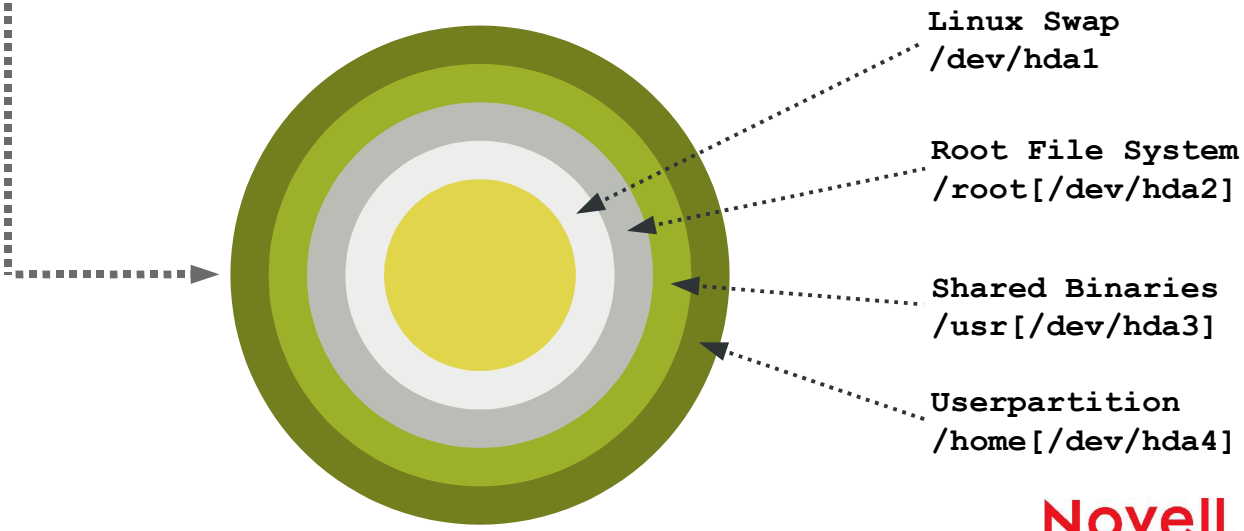
© April 25, 2005 Novell Inc.

Novell.

Loading the Linux System

Partitioning Disk

- Base Partition Scheme provided not adequate
- Partition disk to stop DOS attacks on system
- Partition each functional area based on usage of system
  - For example:



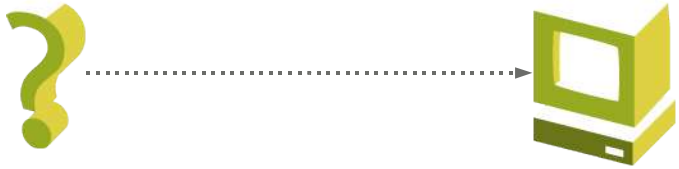
© April 25, 2005 Novell Inc.

Novell.

Loading Services for the System

What Services to Load?

- What is the system use going to be?
- More Services equal higher administrative cost
- More Services equal higher possibility of attack
- Remember Services are a privilege not a right. Only load what you will use on the system.



© April 25, 2005 Novell Inc.

Setting Up User and Group Security

Set User Accounts

- Delete unneeded default accounts
- Set user name, password and access
- Set Password Aging (change /etc/login.def)
  - PASS_MAX_DAYS & PASS_MIN_DAYS
- For system accounts lock them by assigning an invalid shell

Set Group Accounts

- Set up Groups to contain User Accounts
- Only give group enough rights as needed

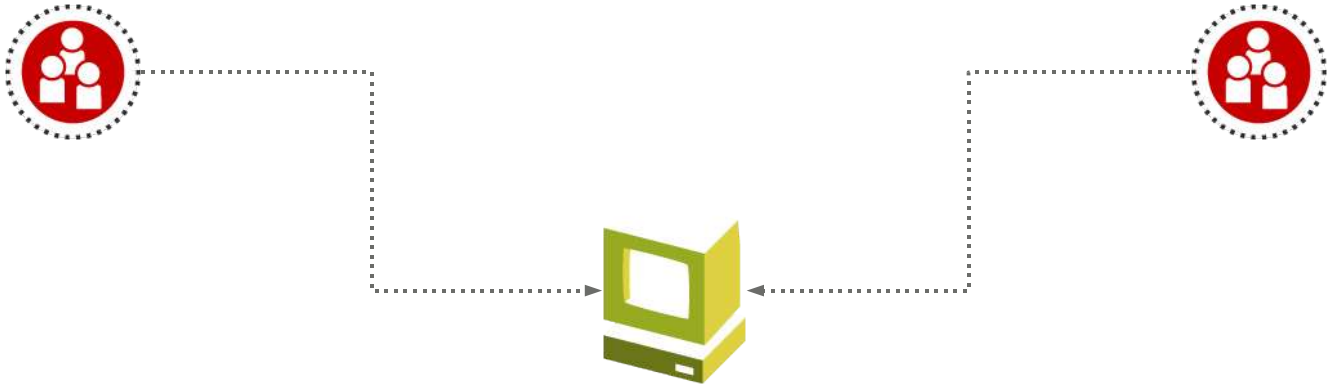
© April 25, 2005 Novell Inc.

Novell.

Designing Program and Services Access

Use Groups for access to Services and Programs

- This allows for better administration of Server
- No single account should need to be without a group
- Follows good design by establishing roles based on rules
- Easier to fit into an identity management architecture



© April 25, 2005 Novell Inc.

Novell.

Additional Security Steps

1. Modify of initial files which were loaded
2. Disable CTS-ALT-Delete
3. Disallow Remote Root Login
4. Create Security Banners
5. Apply Updates and Patches
6. System Logging

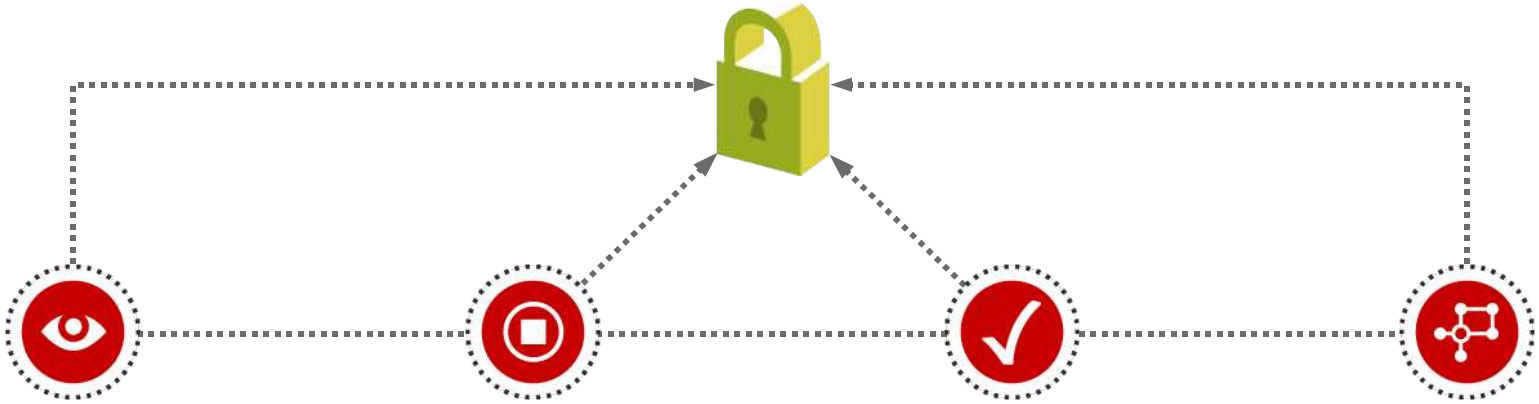
© April 25, 2005 Novell Inc.

Novell.

Web Security

Web Security steps

- Review Modules
- Harden Main Configuration Files
- Check Permissions of Files
- Encrypt Sensitive Traffic with HTTPS



© April 25, 2005 Novell Inc.

Novell.

E-Mail Security

E-Mail Security

- Disable Sendmail Daemon on Workstations
- Define SMTP Server for Mail Clients
- Define Hosts Allowed to Relay Mail
- Set Domain Name Masquerading
- Configure Sendmail to Use RBL Support
- Install an Alternative MTA
- Secure POP and IMAP daemons

© April 25, 2005 Novell Inc.

Tripwire

Open Source Integrity Checker

Tripwire works by creating a hash for all files that you have chosen to monitor on your system. These hashes are then stored in a database. Once the database is created you can schedule tripwire to run on a regular basis to compare the hashes of the files you are monitoring to the hashes stored in the database.

If your system is compromised and/or files replaced or changed Tripwire will know if the files are in the snapshot of changes in size, inode number, permissions, or other attributes. Even a single character change by verifying its checksum.

© April 25, 2005 Novell Inc.

Novell.

Tripwire Setup

Install Tripwire then do:

- cd /etc/tripwire
- ./twinstall.sh
- tripwire --init
- rm twcfg.txt twpol.txt

The script twinstall.sh performs the following:

- Creates site key and local key, you enter the passphrases.
- signs the default configuration file (twcfg.txt) with the site key creating tw.cfg
- Signs the default policy file twpol.txt with the site key creating tw.pol
- tripwire –init (builds the database)
- rm twcfg.txt twpol.txt (This step deletes the unencrypted policy and configuration files.)

© April 25, 2005 Novell Inc.

Novell.

Displaying the binary Policy and Configuration Files for Tripwire

Now you wish to view Tripwire's Policy and Configuration files which are encrypted:

Generate the active Configuration File:

- cd /etc/tripwire
- twadmin –print-cfgfile > twcfg.txt

Generate the Active Policy File:

- cd /etc/tripwire
- twadmin –print-polfile > twpol.txt

© April 25, 2005 Novell Inc.

Novell.

Modifying Tripwire's policy and Configuration

So you want to change the set of files and directories Tripwire examines:

1. Extract the Policy and Configuration

2. Modify the policy file, twpol.txt, and/or the configuration file, twcfg.txt, with any text editor.

3. Re-sign the modified files:
   - twadmin --create-cfgfile –cfgfile /etc/tripwire/tw.cfg \
     --site-keyfile site_key etc/tripewire/twcfg.txt
   - twadmin --create-cfgfile –cfgfile /etc/tripwire/tw.cfg \
     --site-keyfile site_key etc/tripewire/twpol.txt

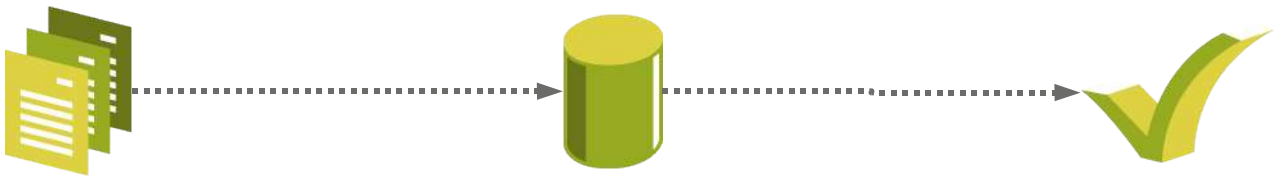
4. reinitialize the database:
   - tripwire –init
   - rm twcfg.txt twpol.txt

Tripwire Integrity Checking

Run:

- tripwire –check

This compares the filesystem against the database according to the rules of the active policy. The results are written to standard output and also stored as a timestamped signed Tripwire Report.



© April 25, 2005 Novell Inc.

Nessus

A Freeware Vulnerability Assessment Tool

- Works on a client/server based technology
- Server side contains the vulnerability database and the engine that actually performs the vulnerability assessment
- The Client connects to the server to configure the settings for the vulnerability assessment
- Nessus can provide reports in a number of different formats including its native GUI format, HTML and ASCII

© April 25, 2005 Novell Inc.

Installing and Running Nessus

1. Download the latest Distribution of Nessus
2. Four components must be installed in the order:
   - nessus-libraries
   - libnasl
   - nessus-core
   - nessus-plugins

   unarchive the source code with tar zxvf
   cd to source directory
   ./configure
   compile using make
   install make with install
3. Start the nessus server by running ./nessusd located in bin directory

© April 25, 2005 Novell Inc.

Installing and Running Nessus (cont.d)

4. Use nessus-adduser to add a new user to the system
5. Go to an X-term window type nessus and enter the password for the user you created in step 4
6. Use the Plugin Tab for the exploits you wish to check.
7. Next click the Target selection tab and enter the comma-delimited hosts to check.
8. Click Start

© April 25, 2005 Novell Inc.

Nessus

A Freeware Vulnerability Assessment Tool

- Works on a client/server based technology
- Server side contains the vulnerability database and the engine that actually performs the vulnerability assessment
- The Client connects to the server to configure the settings for the vulnerability assessment
- Nessus can provide reports in a number of different formats including its native GUI format, HTML and ASCII

© April 25, 2005 Novell Inc.

Novell®

General Disclaimer

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. Novell, Inc., makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Novell marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.

No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of Novell, Inc. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

Novell