redhat.

RED HAT ENTERPRISE LINUX Security Tools

What's included in the package?

Ohio Linux Fest 2019
Nov 2019
Jim Wildman
wildman@redhat.com

Notes

- Some of this will seem very basic
- No demos…:-(
- I was thinking of several scenarios as I developed this
  - A server is acting “funny”
    - What has changed
    - How can I tell if something changes in the future
  - A server has been compromised
    - How do I figure out how?
    - How do I prevent a repeat, even if it is because of a bug
- How do I earn wizard status or BOFH...

Or in pictures

Agenda

- RPM - RPM Package Manager
- Rsyslog - capturing the data
- Sudo - privilege escalation
- Ssh - secure communications
- Sosreport - For when things go wrong
- LUKS- Linux Unified Key System
- NBDE - Network Bound Disk Encryption
- Selinux - Security Enhanced Linux
- Auditd - General purpose security auditting
- Aide - file monitoring and alerting
- OpenScap - Security Scanning
- Other stuff

RPM

- When/why to use: great way to verify that your vendor provided binaries have not been tampered with
- For every file delivered it stores
  - Ownership, permissions, etc
  - Date, size
  - Cryptographic hash
- Rpmdb can be compared to offline/RO copies (ie, installation media)
- Reports what has changed, not why or by whom or even what has changed

Rsylog - remote syslog server

- When/why to use: to collect all your log files into one place
- So you don’t have to run around to all the servers to find out what happened
- Particularly useful for very distributed or burstable environments
- Can be fed into Splunk or another data analysis tool w/o adding agents to every box

sudo - privilege escalation

- When/why to use: When you need to give someone rights to act as someone else (usually root)
- More than just “sudo su -”
- Can limit options passed to commands
- Can limit specific commands
- Can allow no passwords
- Can provide session logging (learned it from one of my students yesterday)

Ssh - secure shell

- When/why to use: For all remote access to servers
- Can use ssh-agent to preload keys
- Generate keys with different lengths, crypto, etc
- Keys provide “passwordless” logins
- Keys can be restricted to just run one command

Sosreport - collect all there is to know

- When/why to use: To gather all relevant, non private data on a server
- Usually used for Red Hat support cases
- Can be used to capture a snapshot of a system's config
- Xsos tool can be used to analyze
- Can be unrolled into a web directory and browsed via httpd
- Can be customized by turning off modules (for speed) or extended by writing new modules

LUKS - Linux Unified Key Setup

- When/why to use: When you need to protect data at rest
- Originally designed and written in 2004
- Well tested and proven
- https://access.redhat.com/articles/193443
- https://access.redhat.com/solutions/100463
- Portable design
- 8 key slots
- Can be used at install time or later

NBDE - Network Bound Disk Encryption

- When/why to use: Allows automatic decryption of drives based on their ability to contact the security server
- Very light weight protocol
- Passwords are NEVER transmitted over the net or stored on the security server
- Supports multiple ciphers, failover, TPM, etc, etc
- LUKS - full disk encryption
- Last year's lab on NBDE https://ohiolinux.org/wp-content/uploads/2018/10/NBDE-or-How-I-could-have-slept-better-at-night.pdf

selinux

- Not your enemy
- If you are blocked by selinux
  - Why?
  - What standard have you violated?
  - Is what you are trying to do important enough to violate standards?
  - What are the implications of the activity if we allow it?
-

selinux

- Over 400 “targetted” profiles in RHEL 7
  - File locations
  - Allowed actions
- For example, for a web server
  - All readable content must be in /var/www/html with the correct context
  - It listens on ports 80 and 443
  - It can’t write anywhere (other than logs)
  - For Apache, it gets configs from /etc/httpd

selinux

- Tools to help
- Selinux
  - /etc/selinux/settings
- policycoreutils-python-utils
  - Ausearch
  - Audit2why
  - Audit2allow
  - Semanage
  - Setsebool, getsebool
- “Selinux for mere Mortals” presentation
  - Search youtube. One of the most popular labs/demos Red Hat has ever prepared.

auditd

- When/why to use: I need to “watch” specific files for changes, or accessed or low level syscalls, etc. Configured to work with selinux by default
- Very flexible low level logger
- Files
  - Access, read, write, mode change
- Syscalls
  - Entry, exit, success, failure
- Selinux events
  - How most of us use it
- Ausearch, augen, aureport

Aide

- When/why to use: when you need to know if an entire system has been tampered with
- Minimalist Tripwire like tool
- CLI only
- Prepares a database of cryptographic hashes for specific files
- Can compare two versions of the database and generate appropriate alerts.
- Requires preparation and configuration prior to use

USB Guard

- When/why to use: to save on super glue costs!
- Restrict access via USB port
- By type
- By time of day
- Can be partial (ie, read only) or total (non-responsive)

OpenSCAP

- When/why to use: to verify that a system meets an industry standard (PCI, HIPAA, STIG). Can generate Ansible playbooks to fix
- Apply industry or government security standards (STIG) to Linux hosts
- Allow easy customization of the standards
- Can “fix” hosts by itself, but within the Red Hat sphere this is handed off to Tower or Satellite
- Can be integrated with Satellite and Tower

Other stuff: Things we discussed during the lab

- Rear - Relax and Recover, mksysb for Linux
  - Create installable images of existing systems
  - Capture image of compromised system for later analysis
- Lsof
  - What process has a file open
- Nmap
  - Analyze open ports
- Netcat
  - Create arbitrary network traffic, or lightweight listeners
- IdM/IPA
  - Centralized authentication, sudoers, ssh key manager
  - Is usually in a “cross forest trust” with the company’s AD infrastructure

Other stuff 2: Things we discussed during the lab

- Firewalld
  - Replacement for IPTables
- Lucy Kerner's talk
  - https://www.youtube.com/watch?v=xaVoONUE_xk&t=2s
- Configuration management tools
  - Ansible, Salt, Chef, Puppet, BigIP, etc, etc