PRESENTED BY RED HAT

LEARN. NETWORK.
EXPERIENCE OPEN SOURCE.

www.theredhatsummit.com

Red Hat Enterprise Linux 6

Security Overview

Peter Vrabec
Dan Walsh
Jack Rieden

May 5, 2011

Agenda

- Overview
  - Standards
  - OpenSwan
- SCAP / OpenSCAP
- SELinux Sandboxes

Standards

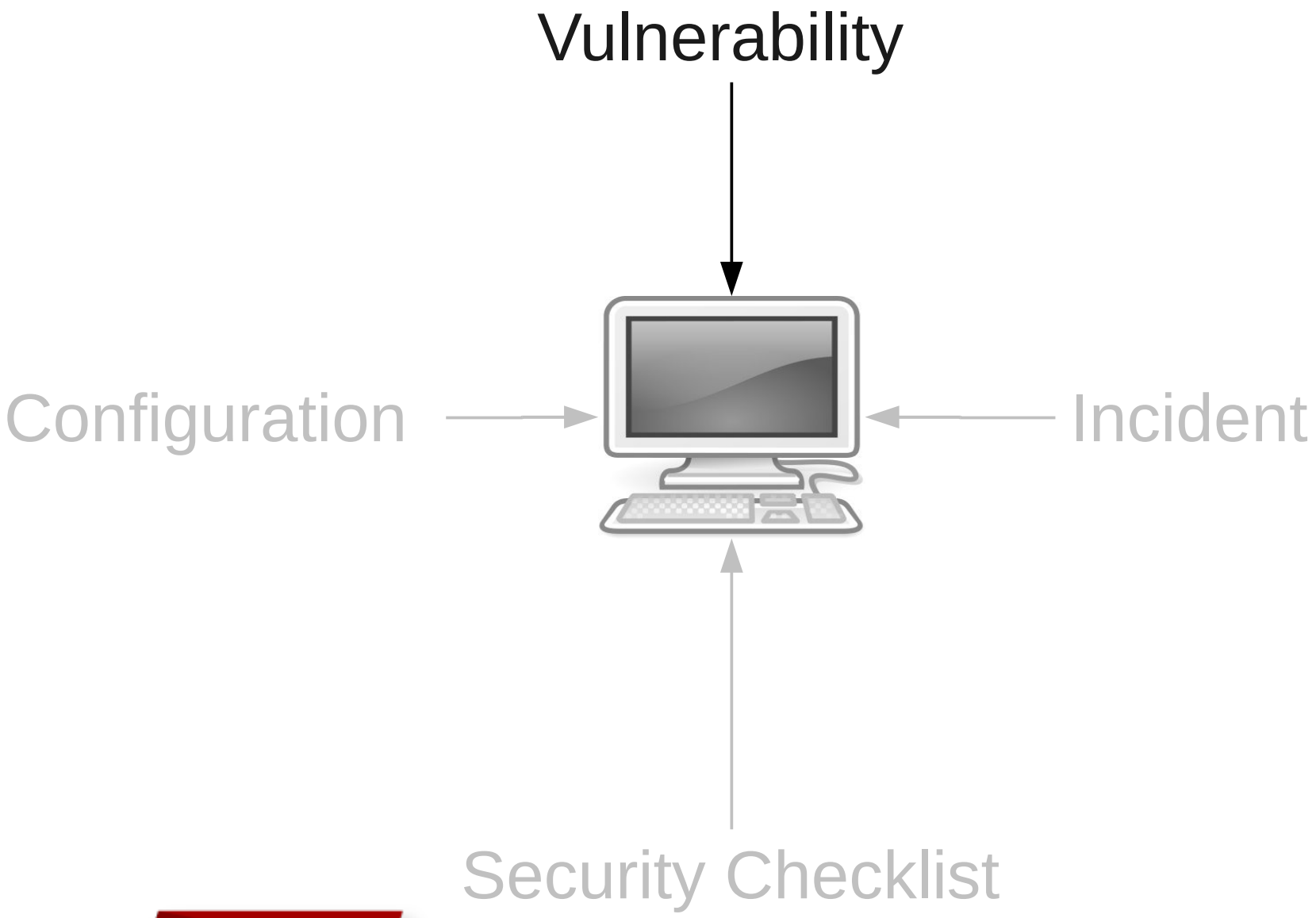
- Common Criteria
  - In Evaluation with RHEL 6
  - EAL+4
- FIPS 140-2
  - Libgcrypt, openssl, openssh, openswan, dm-crypt
  - NSS version 3.12.9
    - Support for AES-NI

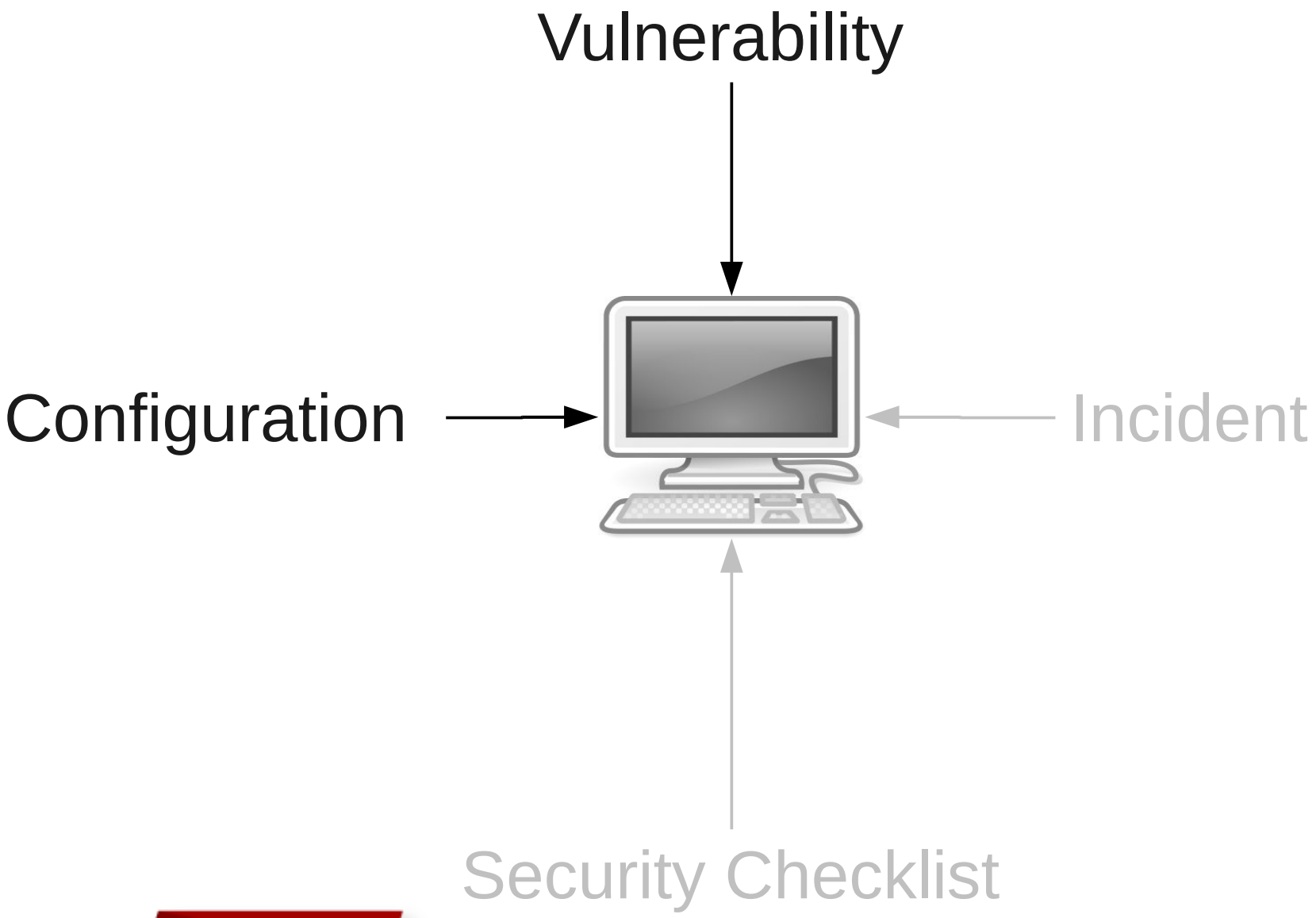
OpenSwan

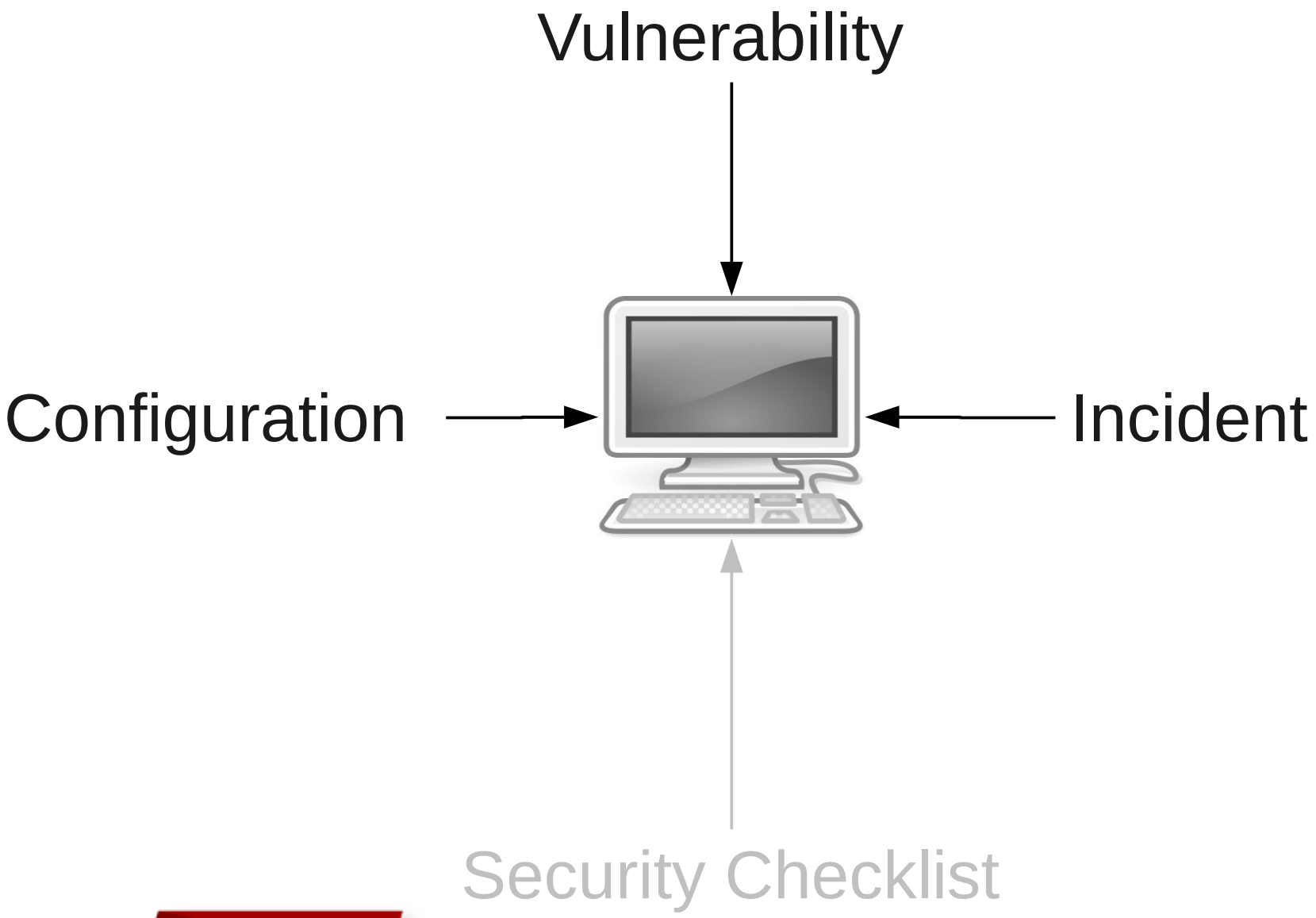
- Integrated with Network Manager
- NSS cryptographic library support
- Cisco interoperability
- Labeled Ipsec support using SELinux

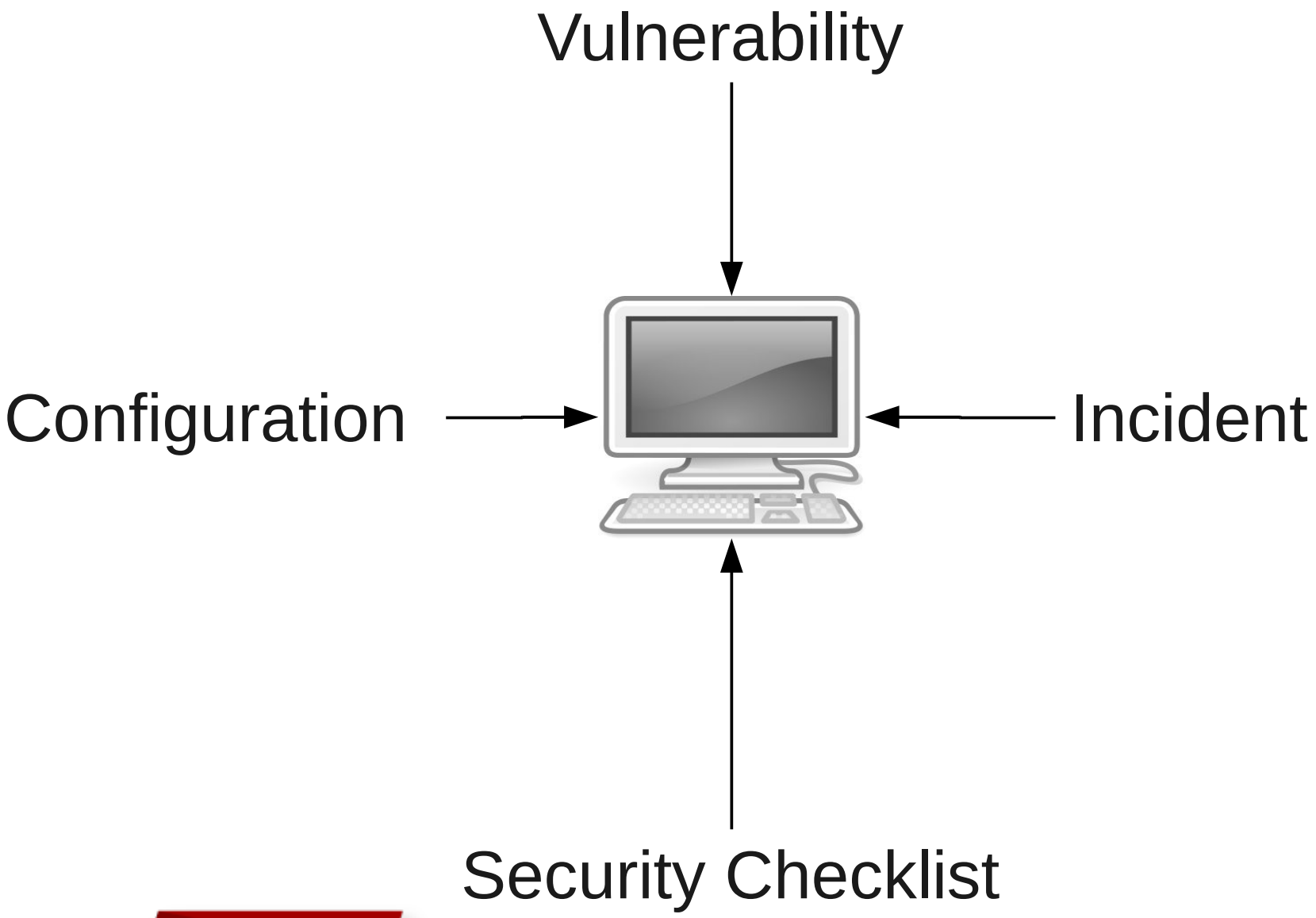
SCAP

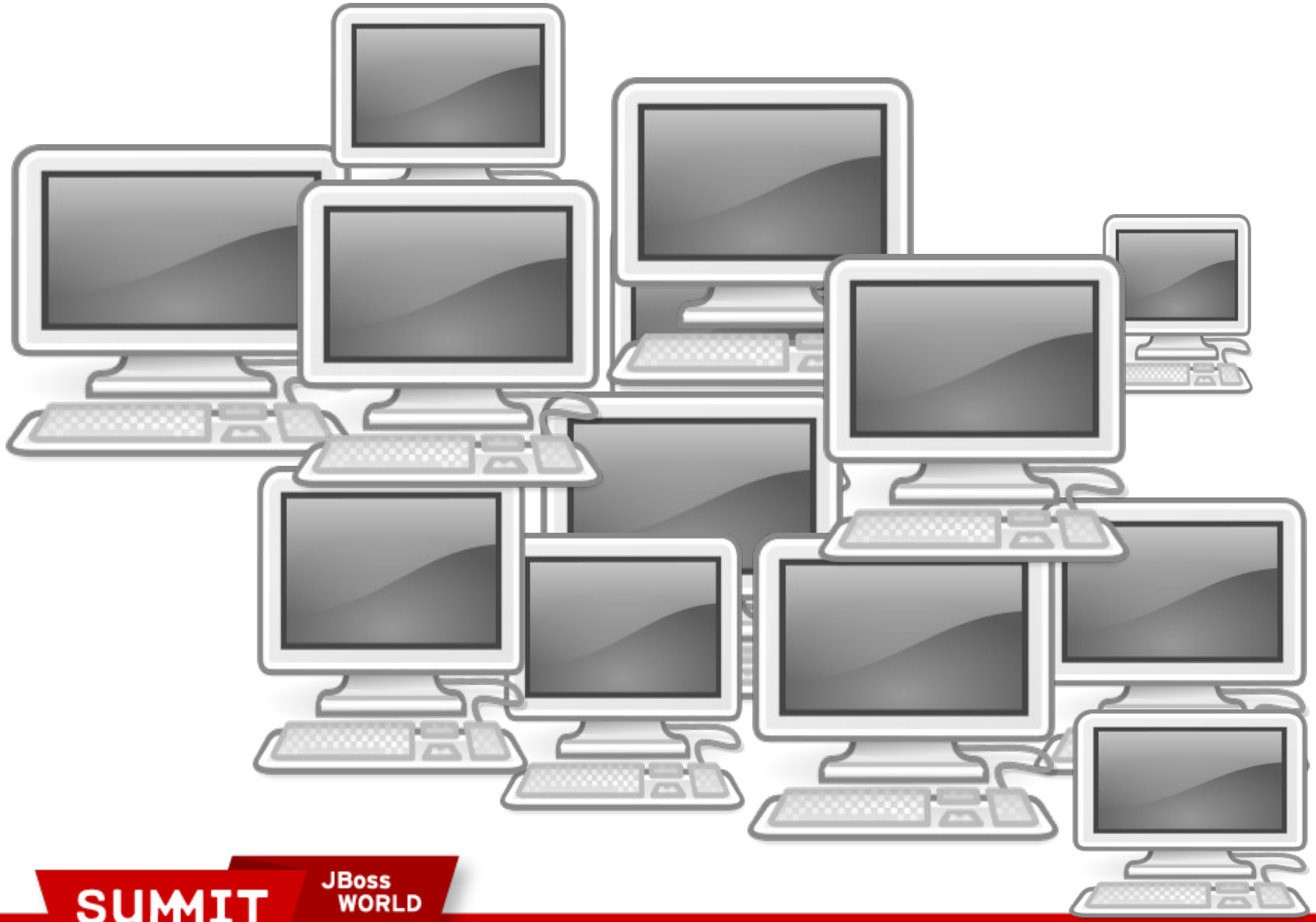
Peter Vrabec <pvrabec@redhat.com>


Vulnerability
Configuration
Incident
Security Checklist


Vulnerability
Configuration
Incident
Security Checklist


Vulnerability
Configuration
Incident
Security Checklist


Vulnerability
Configuration
Incident
Security Checklist



Content

Tools

Security
Content
Automation
Protocol

Content

- Security Response Team
- Security Technologies
- USGCB
- National Vulnerability Database

OpenSCAP

Develop

OpenSCAP

Develop

OpenSCAP

Scan

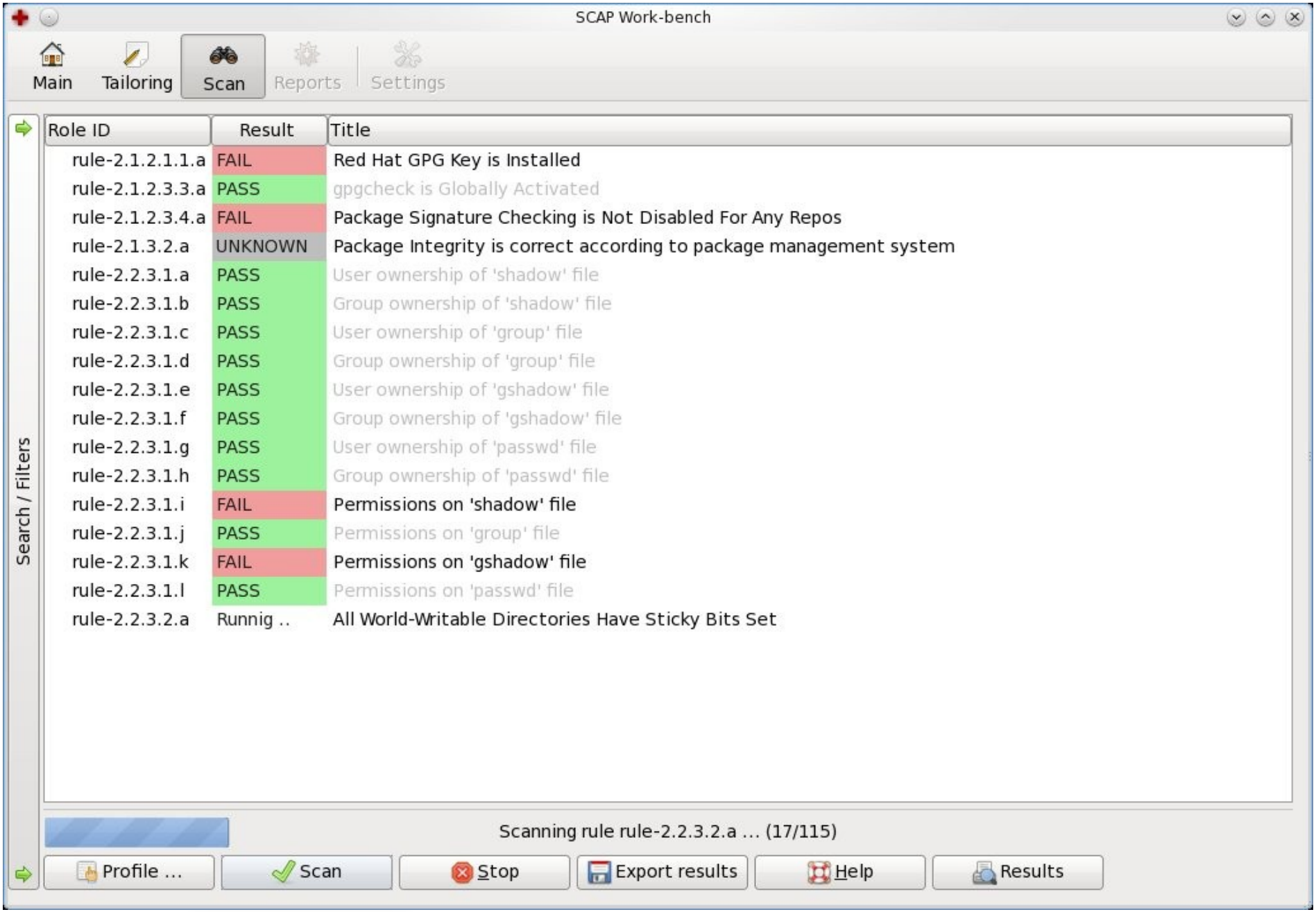
Validate

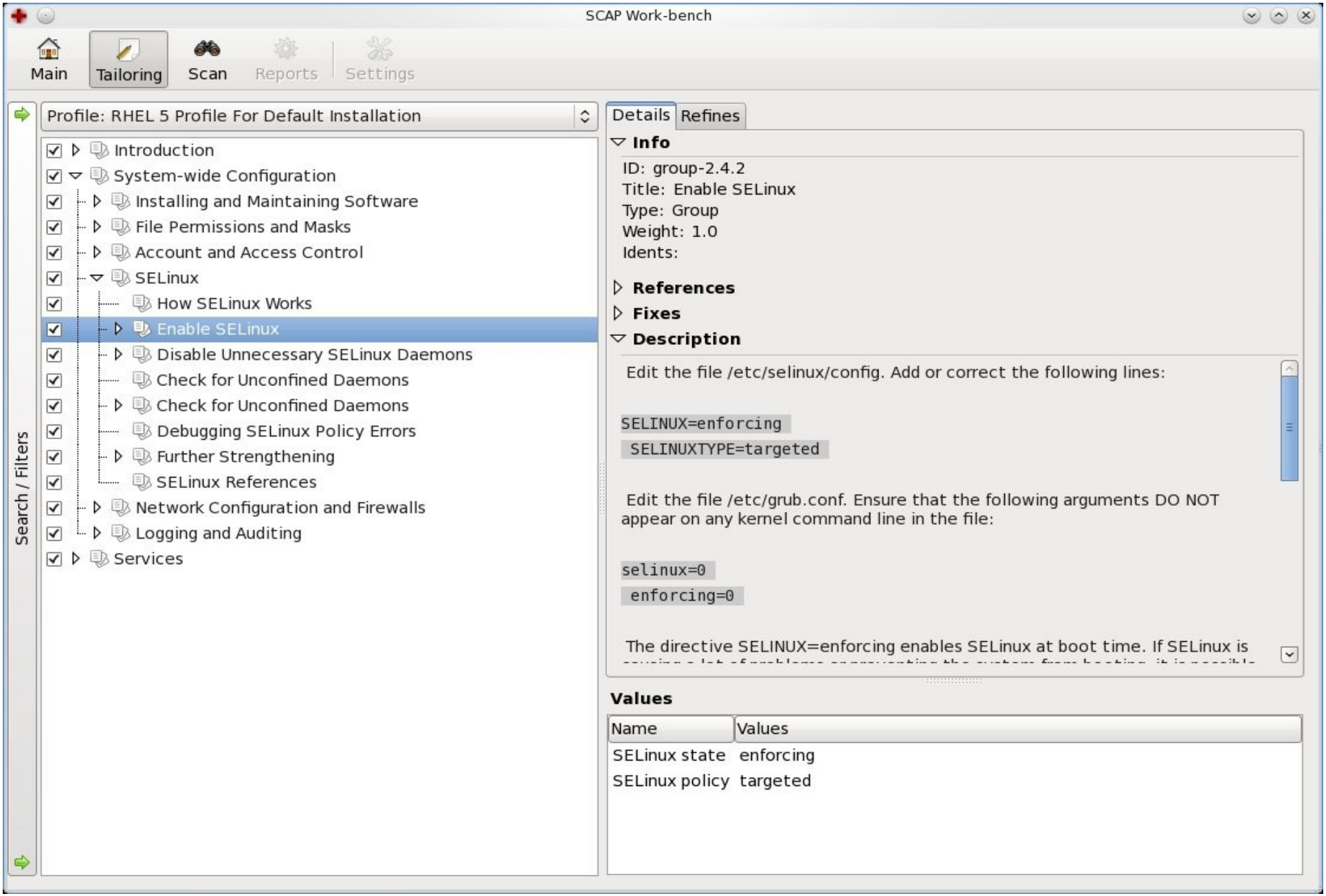
Develop

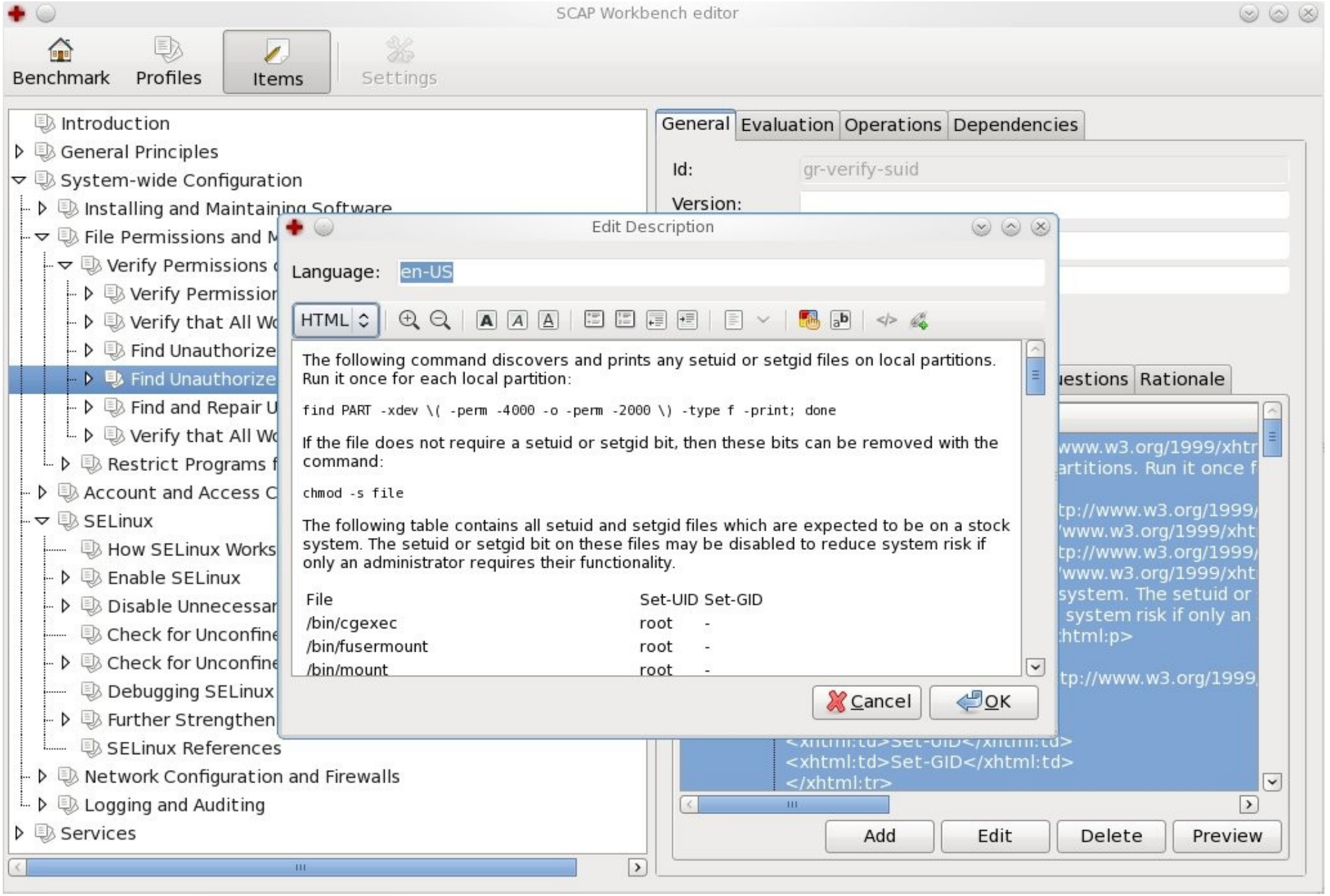
OpenSCAP

Transform

Scan







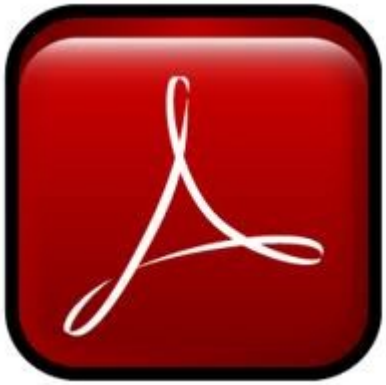
Future

- Validation Program
- Network Scans

References

- http://scap.nist.gov
- http://www.open-scap.org
- http://fedorahosted.org/scap-workbench
- http://www.redhat.com/security/data/metrics

SELinux Sandboxes



Do you trust your applications?

Do you trust your applications?

Beware the data!

What is a sandbox ?

- Run general applications in a locked down environment
  - Less privileged then other processes run by the user
  - Block Networking
  - Block Access to other Processes
  - Block Access to files, homedir?
  - Block Access to resources like X, DBUS
- Run untrusted applications or filters on untrusted data

Examples of sandboxes

- chroot
  - sftp
  - bind-chroot
- /usr/lib64/chromium-browser/chrome-sandbox
- OLPC/bitfrost – Namepacing, UID separation
- Java sandbox
- SELinux xguest – Confined users

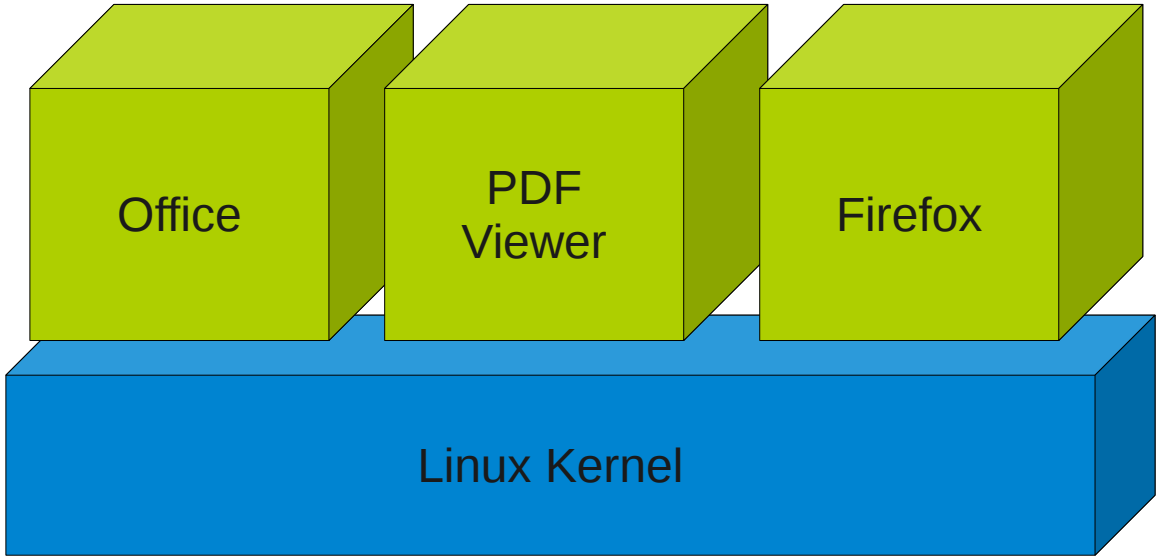
Standard SELinux Sandbox

- cat untrusted.txt | sandbox filter > trusted.txt
  - Filter gets stdin and stdout
  - Can't OPEN any files for write
  - Only OPEN system files for read

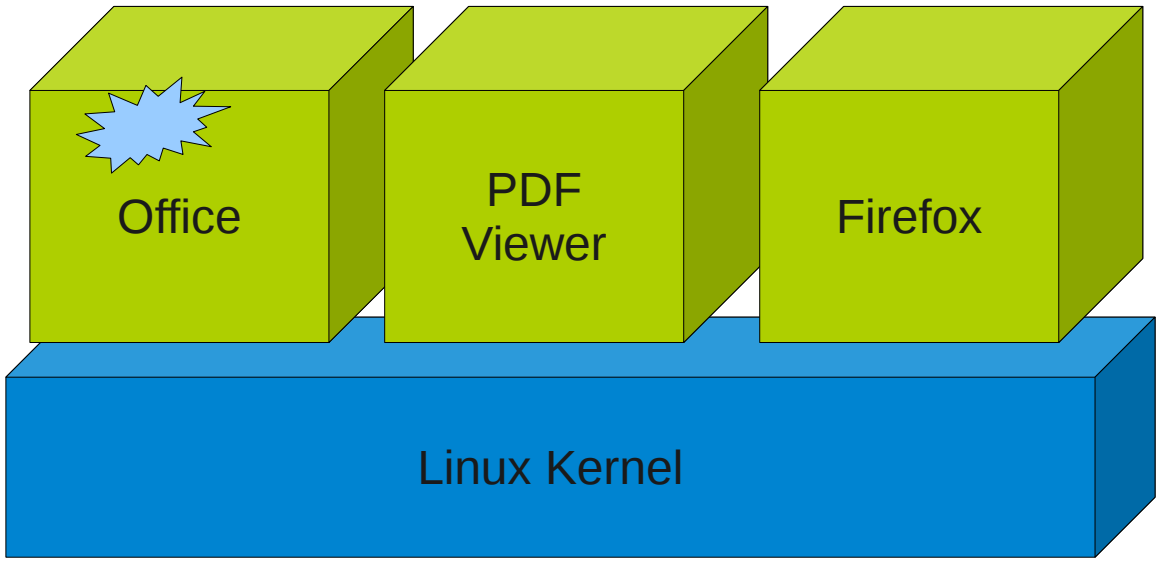
What about the desktop?

Google Chrome

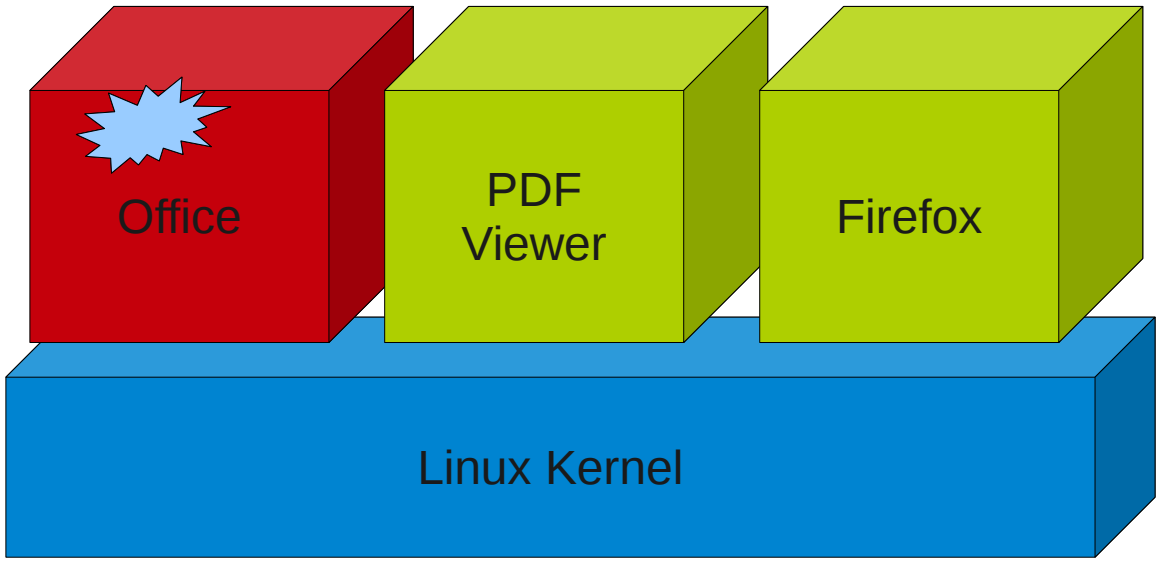
Processes all have equal access to the Desktop...



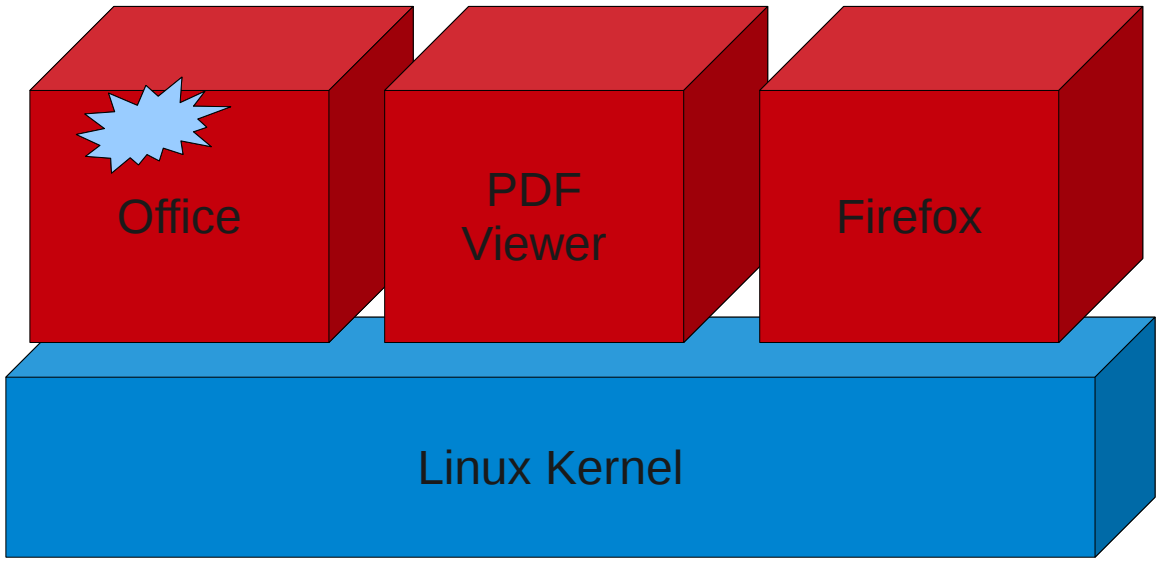
... if one is attacked via untrusted data...



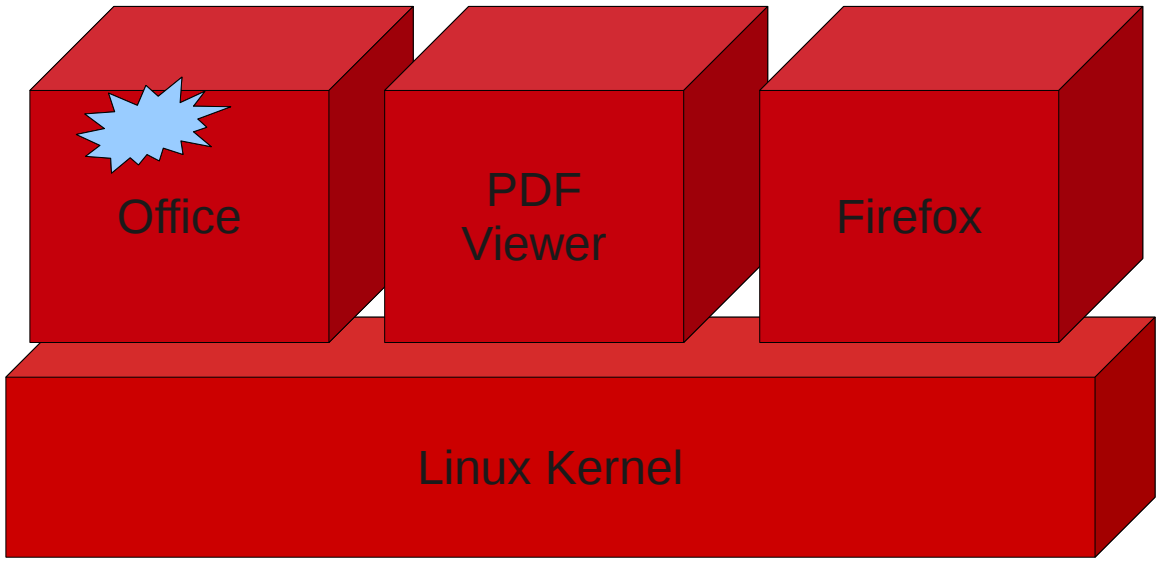
... And triggers a vulnerability ...



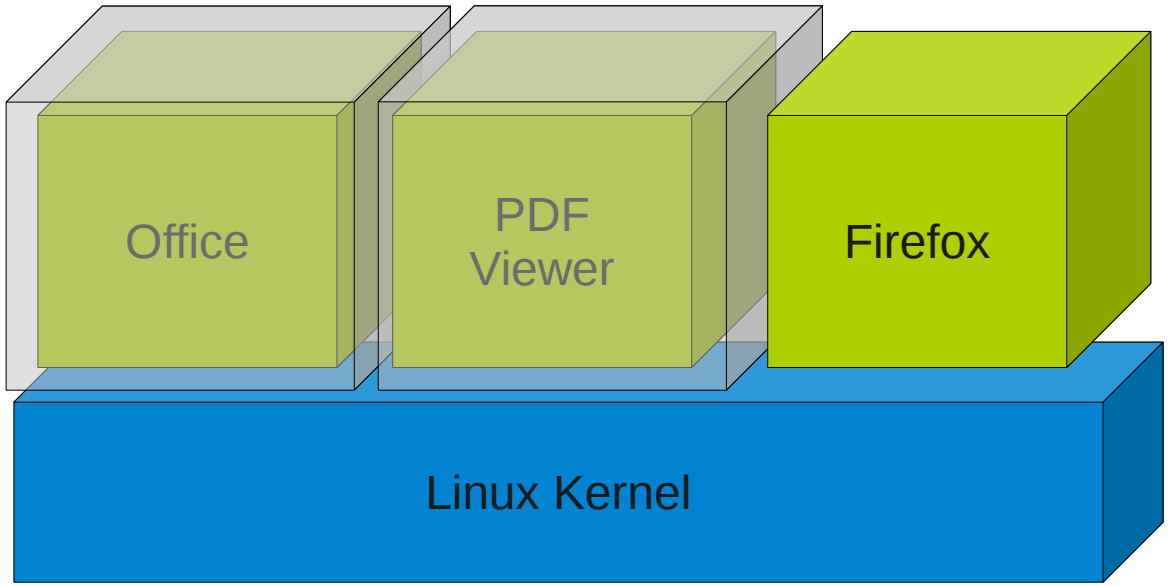
... Then that process can take over all processes ...



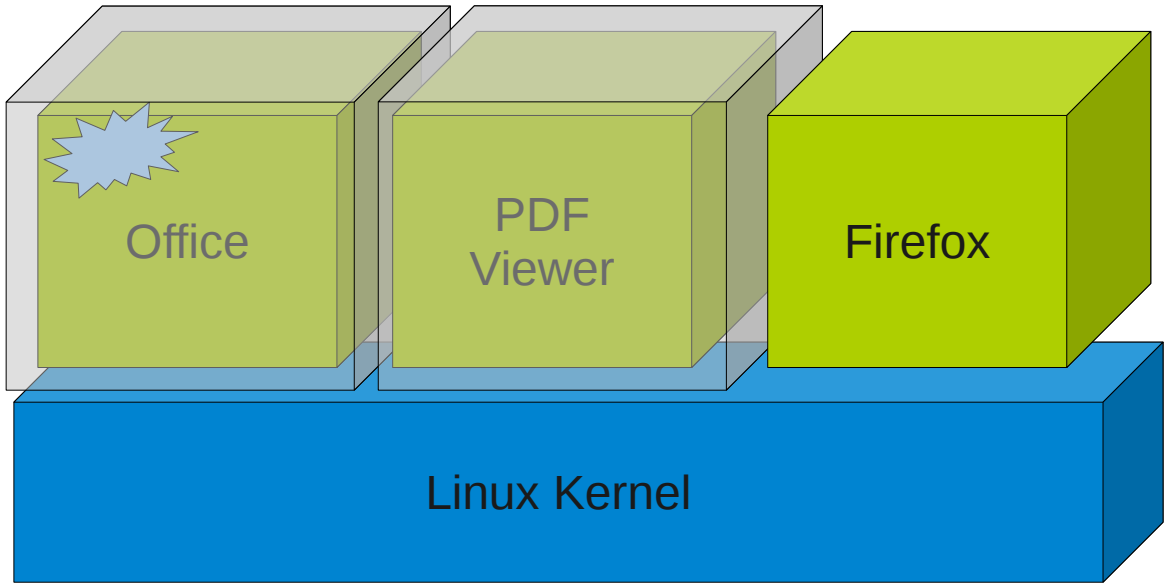
... And if you have a privilege escalation ...



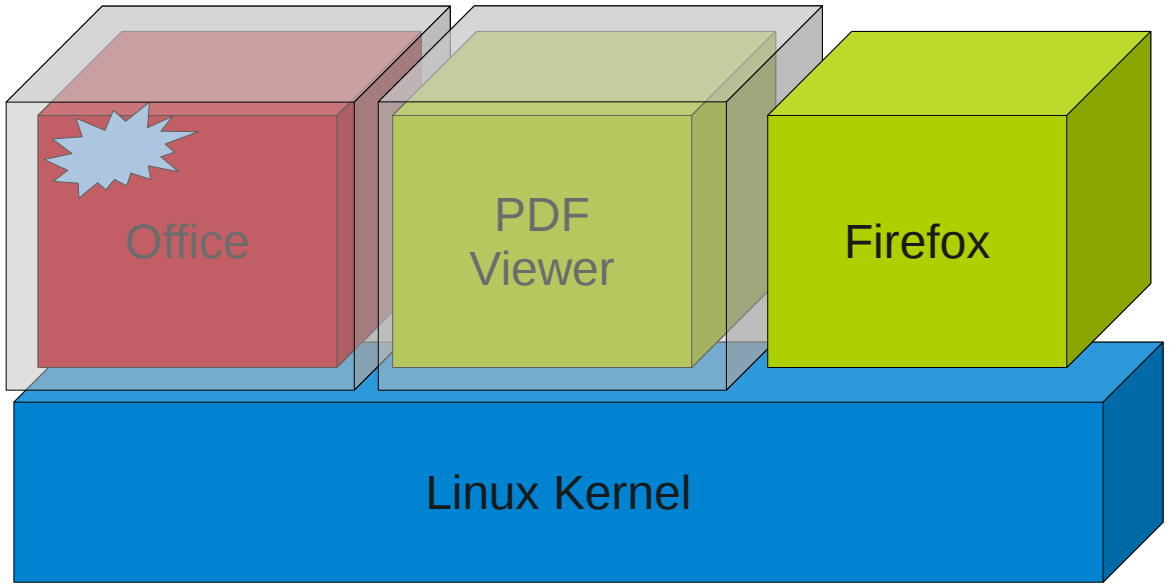
Sandbox -X



... if one is attacked via untrusted data...



... And triggers a vulnerability ...



Block Communication

- $HOMEDIR
- /tmp && /var/tmp
- DBUS
- Gconf
- X
- /proc/self
- setuid Applications
- Network

Demo

LIKE US ON FACEBOOK

www.facebook.com/redhatinc

FOLLOW US ON TWITTER

www.twitter.com/redhatsummit

TWEET ABOUT IT

#redhat

READ THE BLOG

summitblog.redhat.com

GIVE US FEEDBACK

www.redhat.com/summit/survey