

SUMMIT

**JBoss
WORLD**

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

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Agenda

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

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



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

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



SCAP

Peter Vrabec <pvrabec@redhat.com>

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Vulnerability



Configuration



Incident



Security Checklist

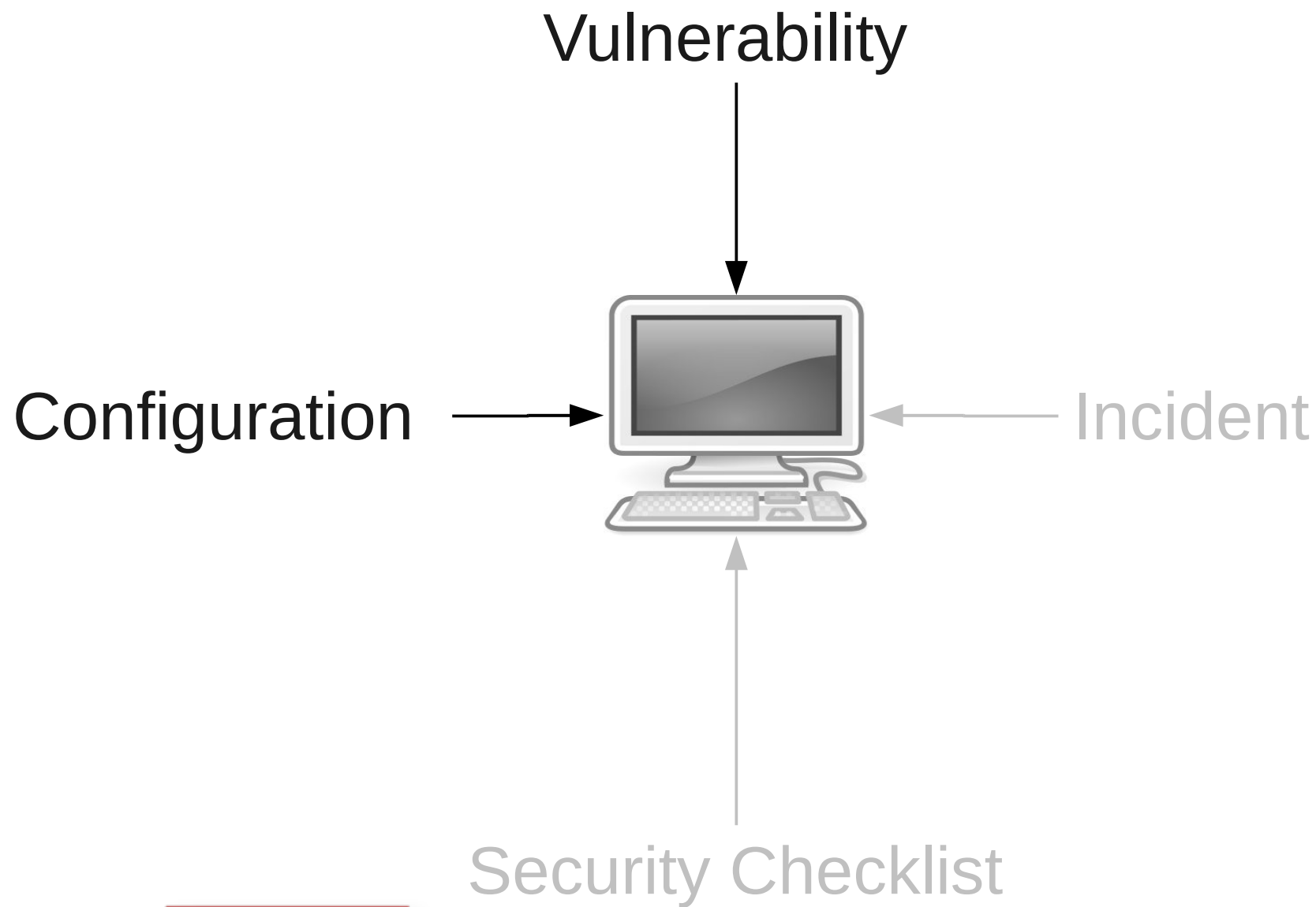


SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



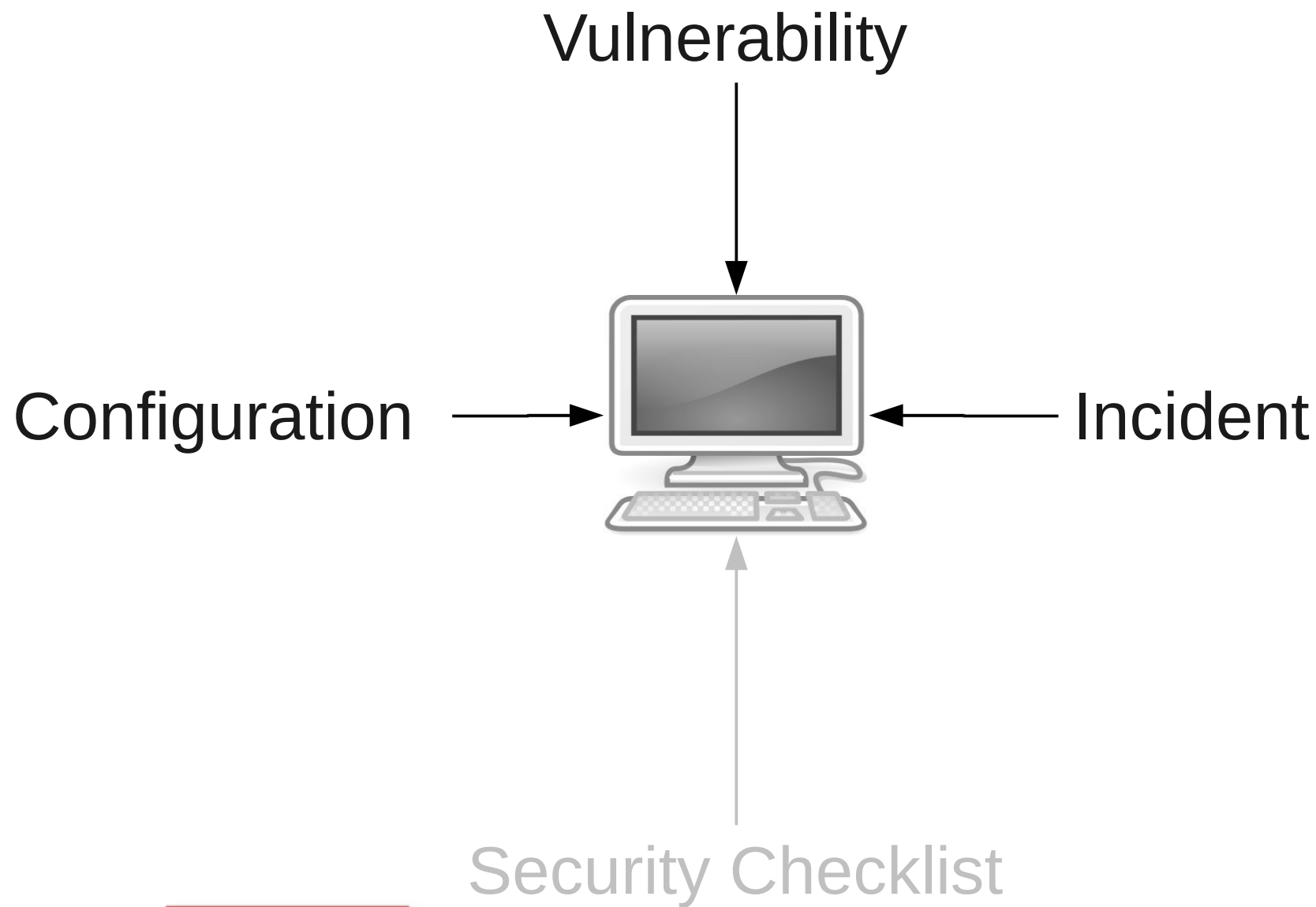


SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



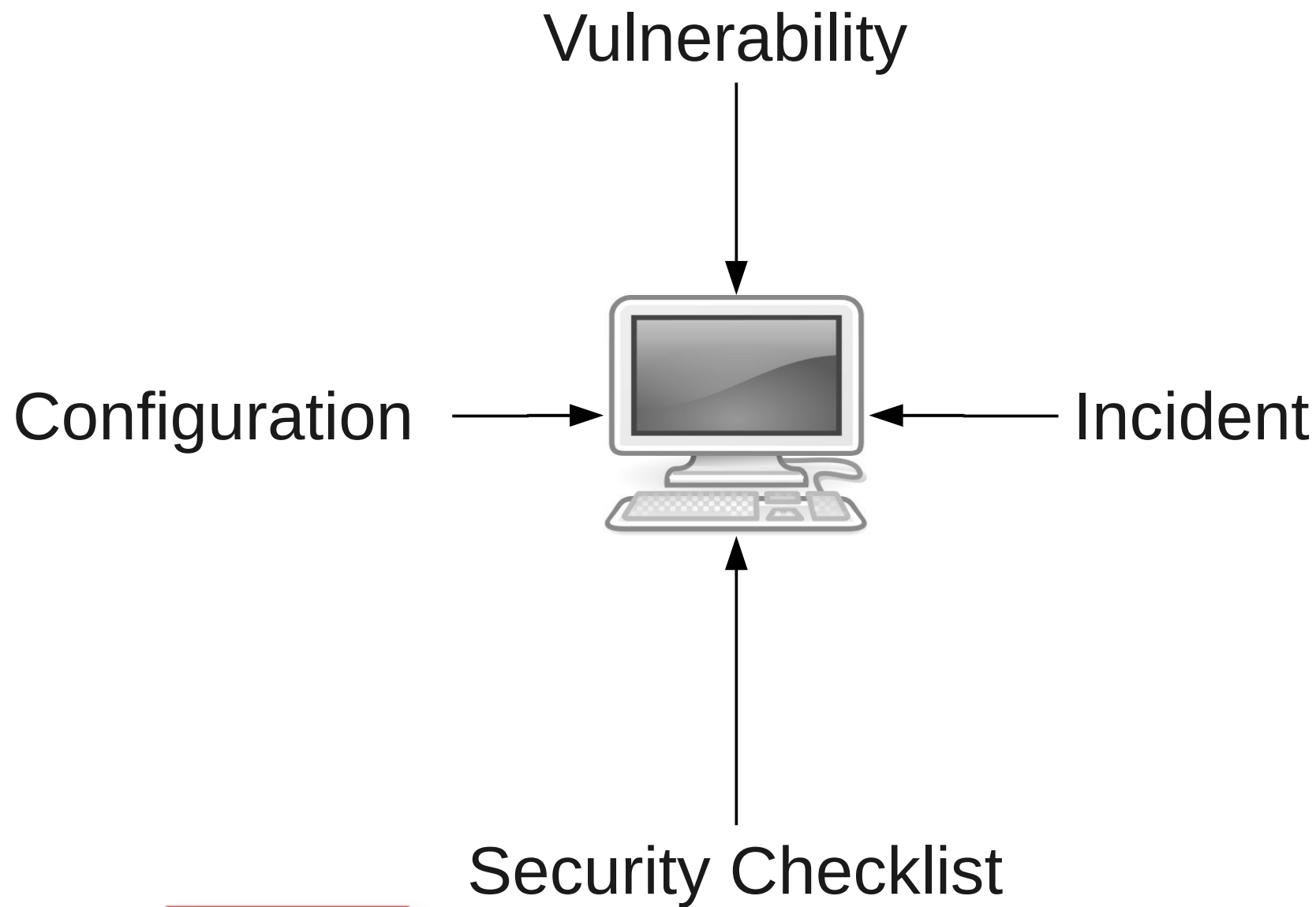


SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



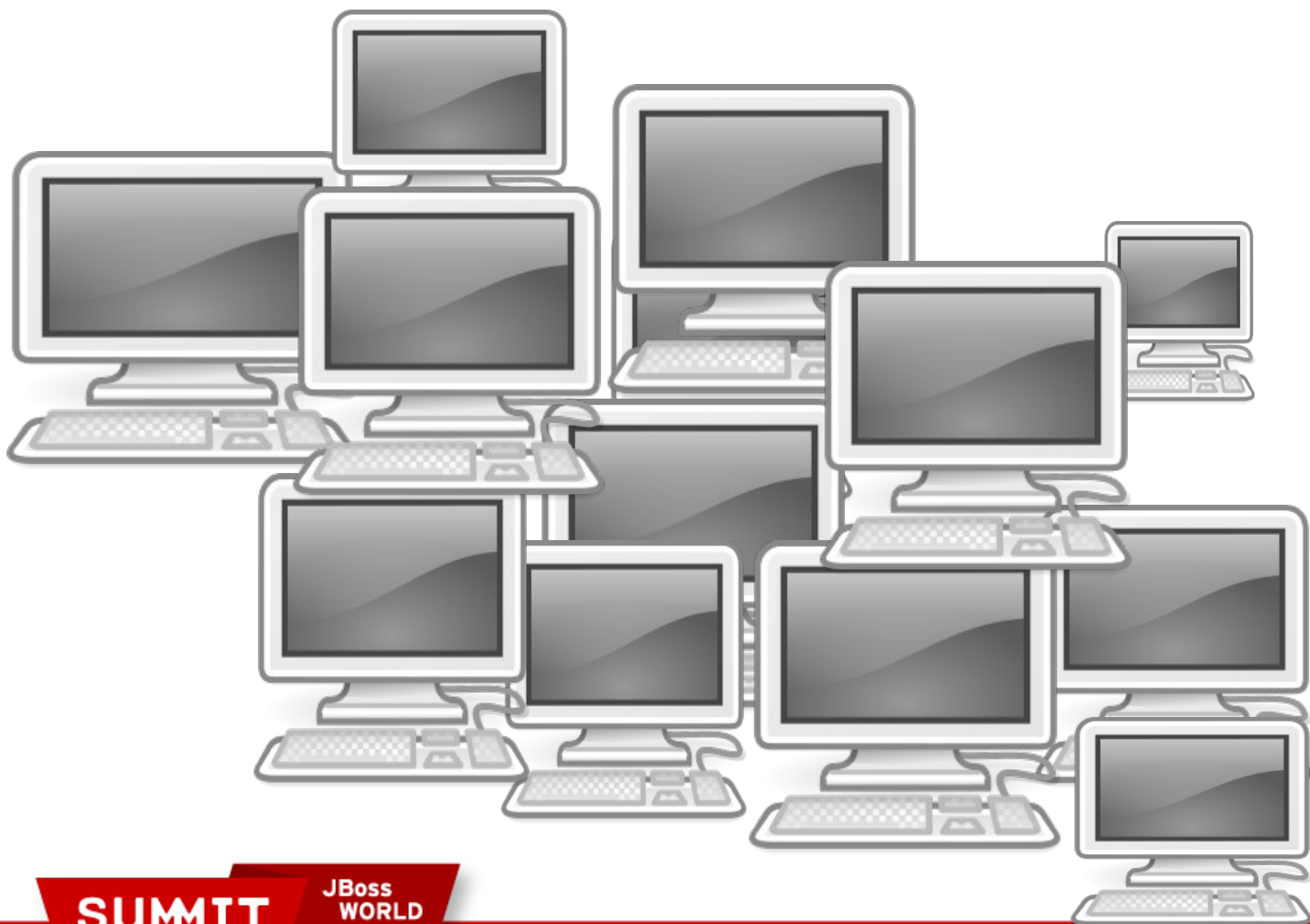


SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT





SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT





Content



Tools

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Security Content Automation Protocol

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Content

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

SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



OpenSCAP

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Develop

OpenSCAP

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Develop

OpenSCAP

Scan

SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



Validate

Develop

OpenSCAP

Transform

Scan

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



SCAP Work-bench

Main Tailoring Scan Reports Settings

Search / Filters

Role ID	Result	Title
rule-2.1.2.1.1.a	FAIL	Red Hat GPG Key is Installed
rule-2.1.2.3.3.a	PASS	gpgcheck is Globally Activated
rule-2.1.2.3.4.a	FAIL	Package Signature Checking is Not Disabled For Any Repos
rule-2.1.3.2.a	UNKNOWN	Package Integrity is correct according to package management system
rule-2.2.3.1.a	PASS	User ownership of 'shadow' file
rule-2.2.3.1.b	PASS	Group ownership of 'shadow' file
rule-2.2.3.1.c	PASS	User ownership of 'group' file
rule-2.2.3.1.d	PASS	Group ownership of 'group' file
rule-2.2.3.1.e	PASS	User ownership of 'gshadow' file
rule-2.2.3.1.f	PASS	Group ownership of 'gshadow' file
rule-2.2.3.1.g	PASS	User ownership of 'passwd' file
rule-2.2.3.1.h	PASS	Group ownership of 'passwd' file
rule-2.2.3.1.i	FAIL	Permissions on 'shadow' file
rule-2.2.3.1.j	PASS	Permissions on 'group' file
rule-2.2.3.1.k	FAIL	Permissions on 'gshadow' file
rule-2.2.3.1.l	PASS	Permissions on 'passwd' file
rule-2.2.3.2.a	Runnig ..	All World-Writable Directories Have Sticky Bits Set

Scanning rule rule-2.2.3.2.a ... (17/115)

Profile ... Scan Stop Export results Help Results

SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



SCAP Work-bench

Main Tailoring Scan Reports Settings

Profile: RHEL 5 Profile For Default Installation

- Introduction
- System-wide Configuration
 - Installing and Maintaining Software
 - File Permissions and Masks
 - Account and Access Control
 - SELinux
 - How SELinux Works
 - Enable SELinux**
 - Disable Unnecessary SELinux Daemons
 - Check for Unconfined Daemons
 - Check for Unconfined Daemons
 - Debugging SELinux Policy Errors
 - Further Strengthening
 - SELinux References
 - Network Configuration and Firewalls
 - Logging and Auditing
 - Services

Details Refines

Info

ID: group-2.4.2
Title: Enable SELinux
Type: Group
Weight: 1.0
Idents:

References

Fixes

Description

Edit the file /etc/selinux/config. Add or correct the following lines:

```
SELINUX=enforcing
SELINUXTYPE=targeted
```

Edit the file /etc/grub.conf. Ensure that the following arguments DO NOT appear on any kernel command line in the file:

```
selinux=0
enforcing=0
```

The directive SELINUX=enforcing enables SELinux at boot time. If SELinux is

Values

Name	Values
SELinux state	enforcing
SELinux policy	targeted

SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



SCAP Workbench editor

Benchmark Profiles **Items** Settings

Introduction
 General Principles
 System-wide Configuration
 Installing and Maintaining Software
 File Permissions and Management
 Verify Permissions and Management
 Verify that All Work is Done
 Find Unauthorized Files
 Find and Repair Unauthorized Files
 Restrict Programs from Running
 Account and Access Control
 SELinux
 How SELinux Works
 Enable SELinux
 Disable Unnecessary SELinux
 Check for Unconfined SELinux
 Check for Unconfined SELinux
 Debugging SELinux
 Further Strengthen SELinux
 SELinux References
 Network Configuration and Firewalls
 Logging and Auditing
 Services

General Evaluation Operations Dependencies

Id: gr-verify-suid
 Version:

Language: en-US

HTML

The following command discovers and prints any setuid or setgid files on local partitions. Run it once for each local partition:

```
find PART -xdev \( -perm -4000 -o -perm -2000 \) -type f -print; done
```

If the file does not require a setuid or setgid bit, then these bits can be removed with the command:

```
chmod -s file
```

The following table contains all setuid and setgid files which are expected to be on a stock system. The setuid or setgid bit on these files may be disabled to reduce system risk if only an administrator requires their functionality.

File	Set-UID	Set-GID
/bin/cgexec	root	-
/bin/fusemount	root	-
/bin/mount	root	-

Cancel OK

Questions Rationale

www.w3.org/1999/xhtml
 partitions. Run it once f
 tp://www.w3.org/1999/
 'www.w3.org/1999/xht
 tp://www.w3.org/1999/
 'www.w3.org/1999/xht
 system. The setuid or
 system risk if only an
 html:p>
 tp://www.w3.org/1999

<html:td>Set-UID</html:td>
 <html:td>Set-GID</html:td>
 </html:tr>

Add Edit Delete Preview

SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



Future

- Validation Program
- Network Scans

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



References

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

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



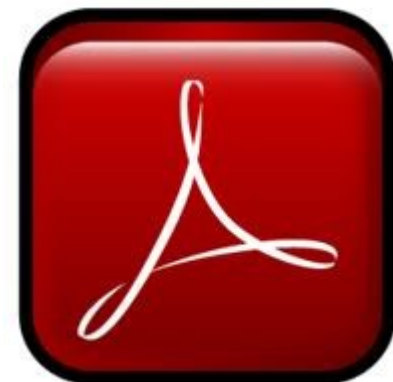
SELinux Sandboxes

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT





Do you trust your applications?



SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Do you trust your applications?



SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Beware the data!



SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



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



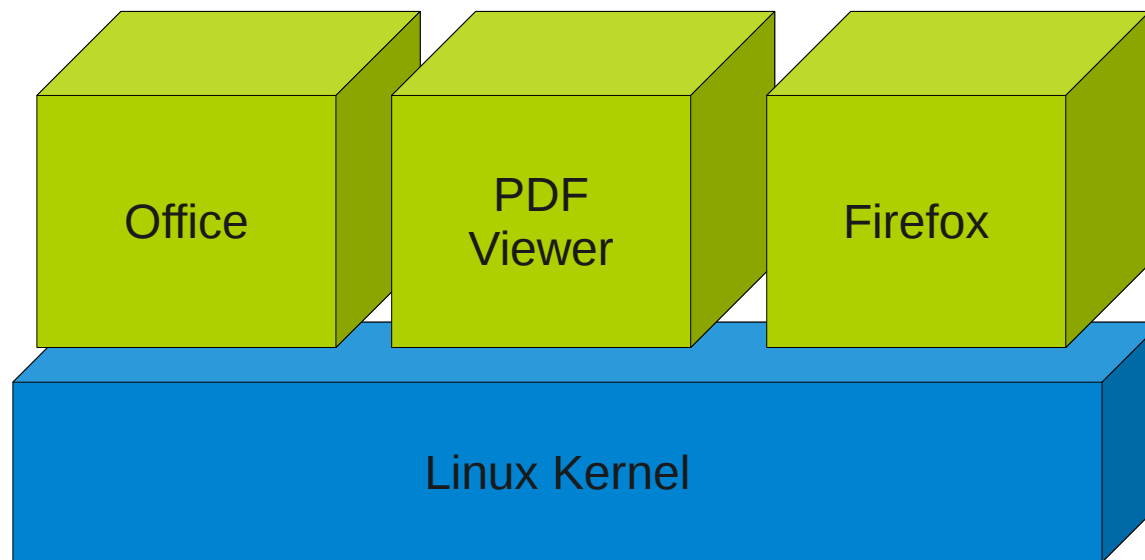
SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Processes all have equal access to the Desktop...



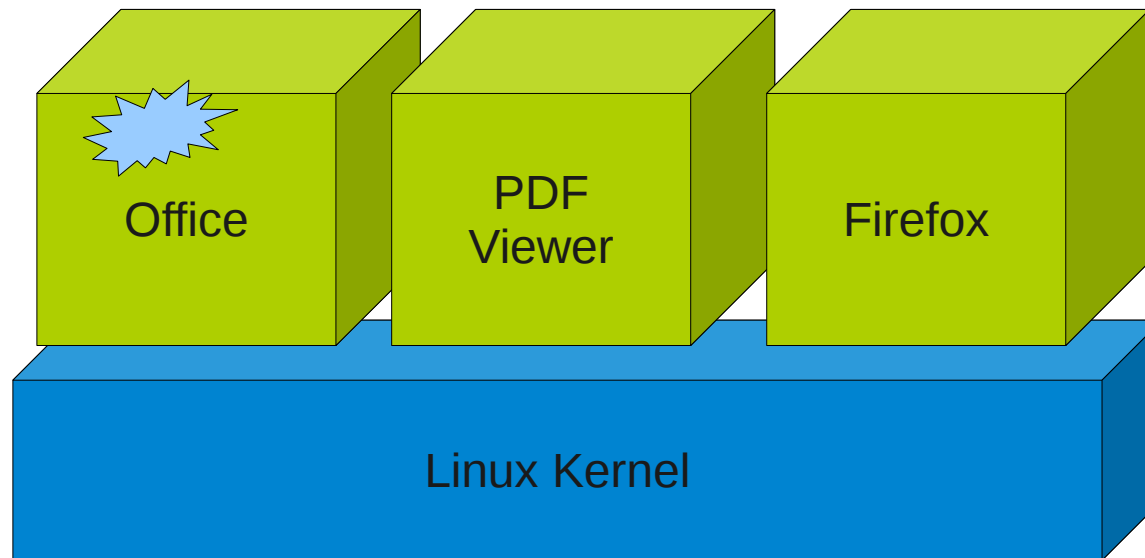
SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



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



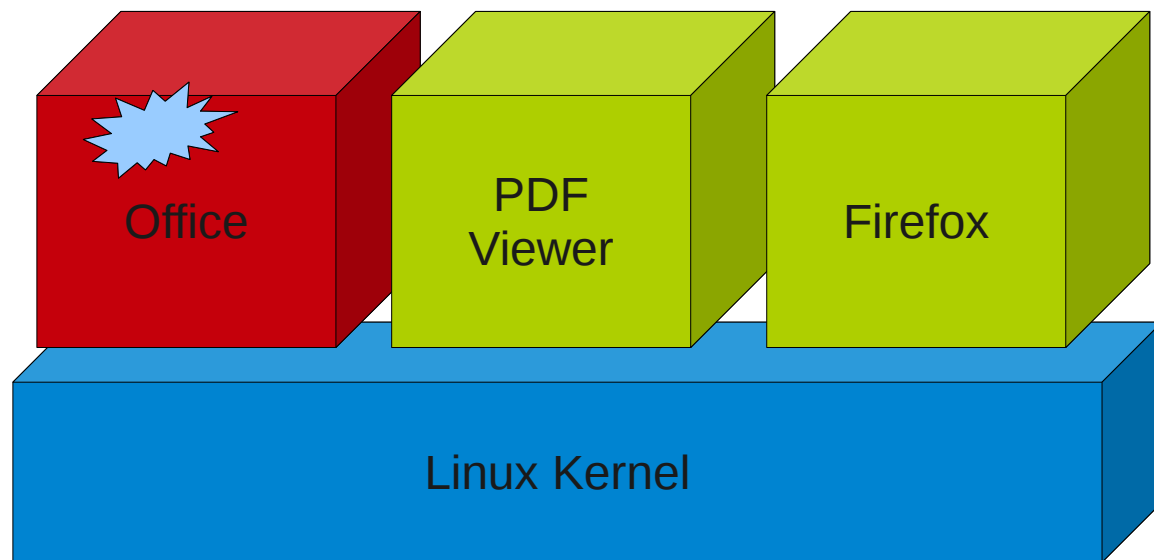
SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



... And triggers a vulnerability ...



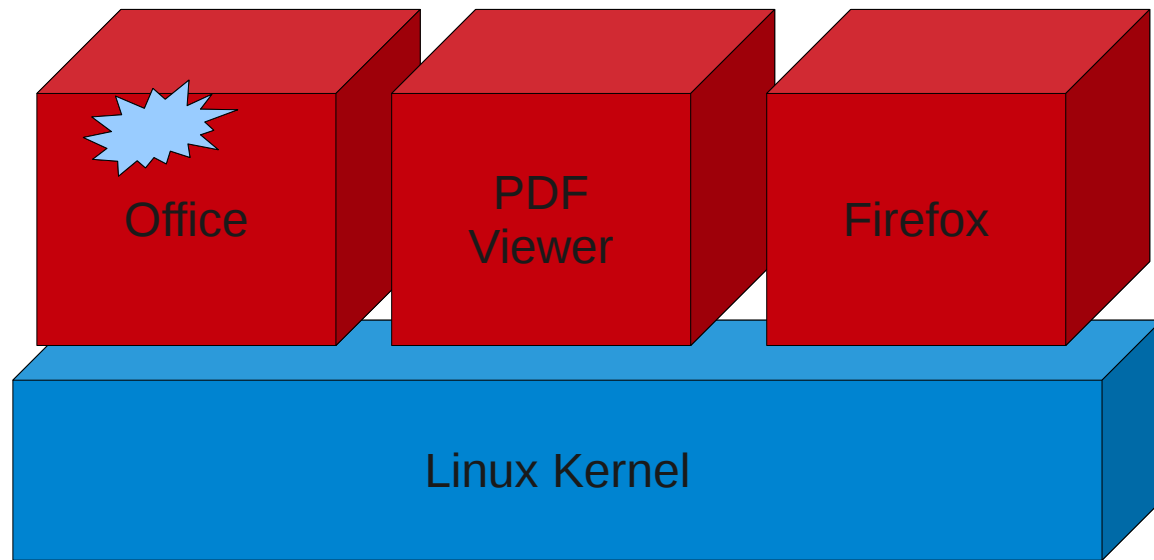
SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



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



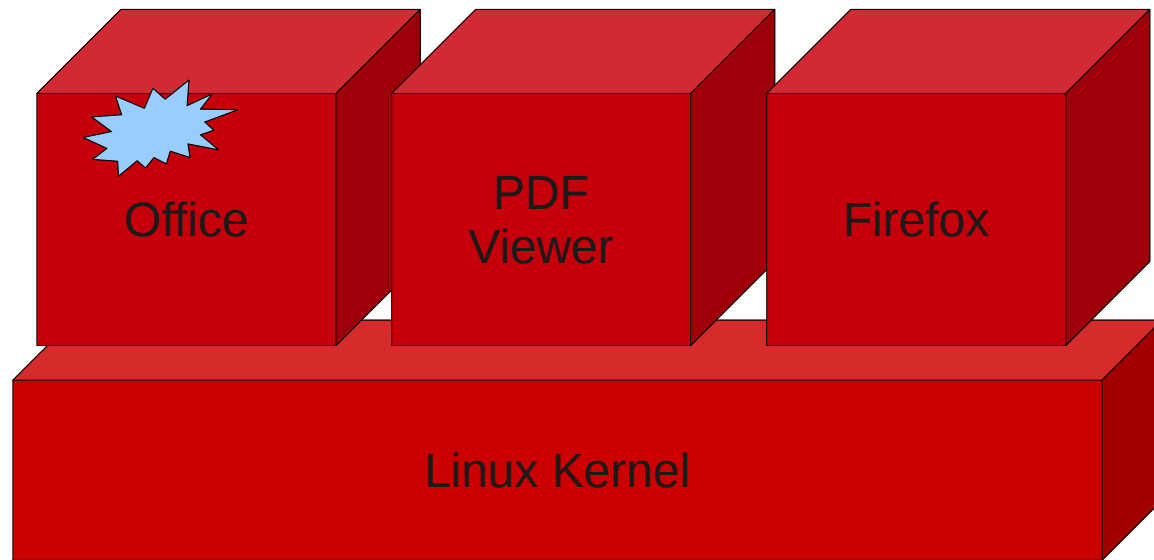
SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



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



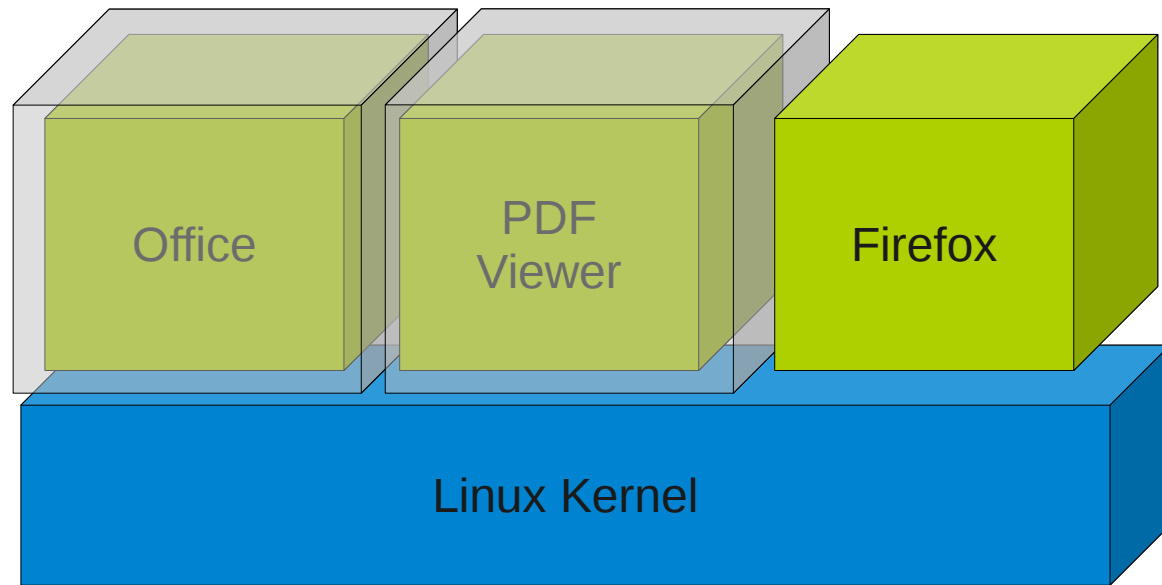
SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



Sandbox -X



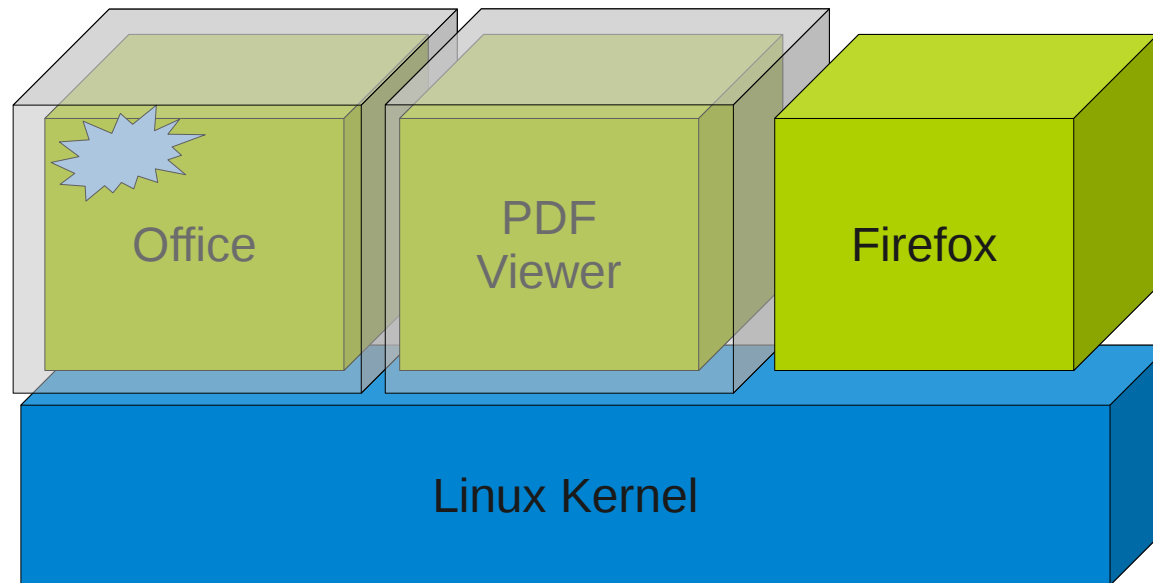
SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



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



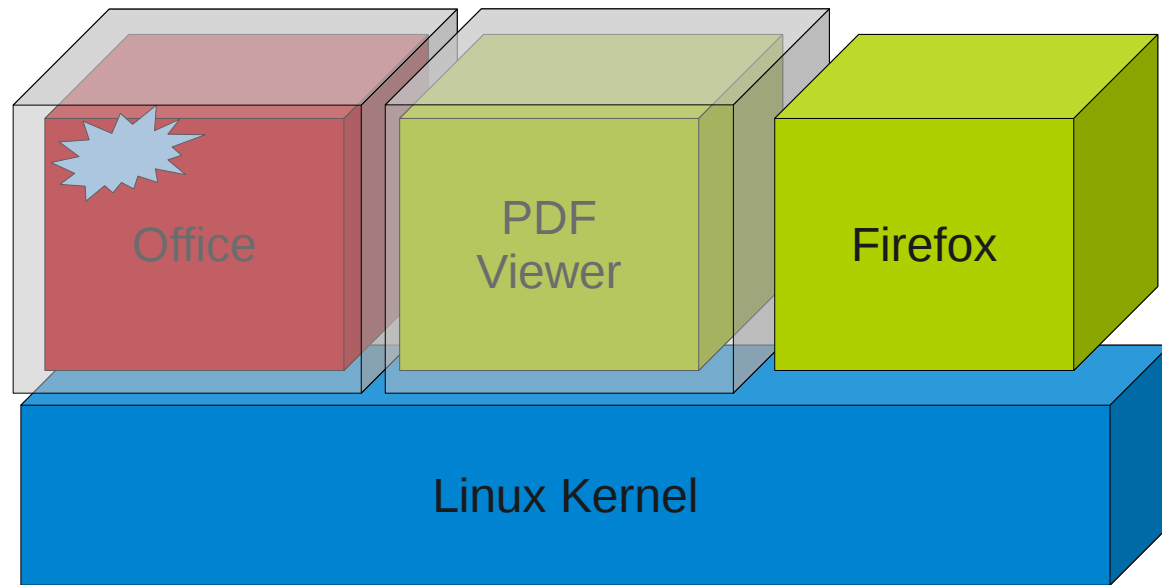
SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



... And triggers a vulnerability ...



SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



Block Communication

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

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Demo

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



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

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT

