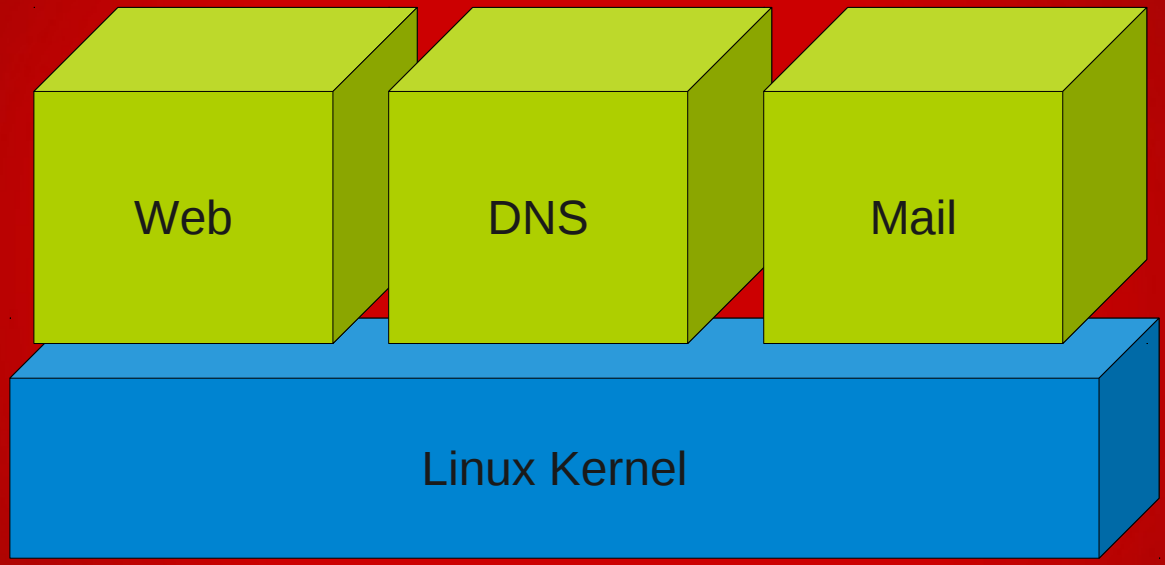
Securing Virtualization

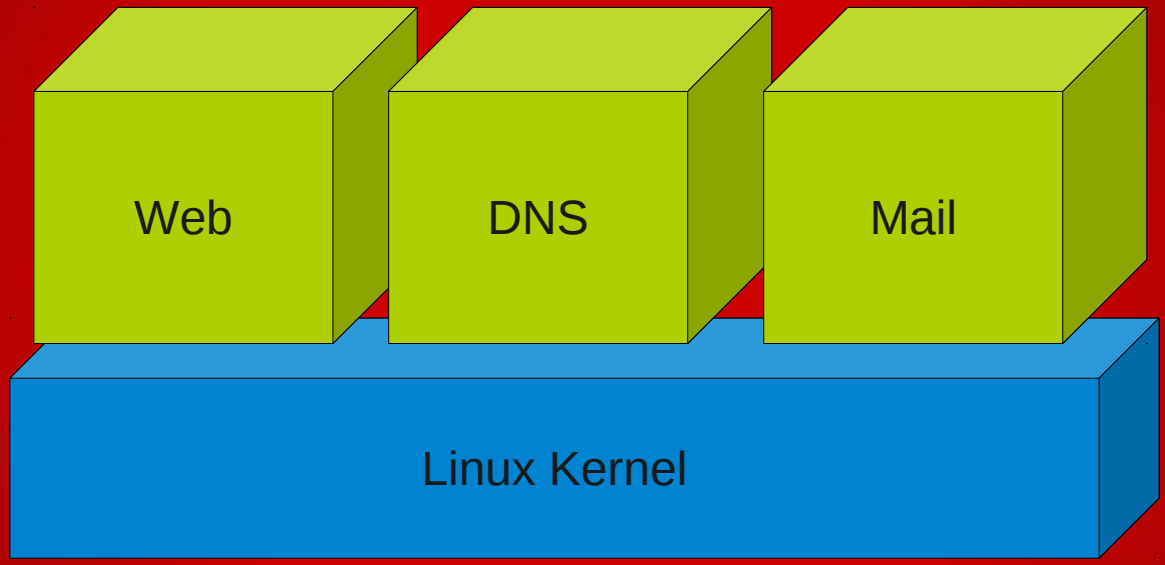
Daniel Walsh
Lead SELinux Developer
EMAIL: dwalsh@redhat.com
Twitter: RHATDAN
Blog: danwalsh.livejournal.com

4 Apr 2012

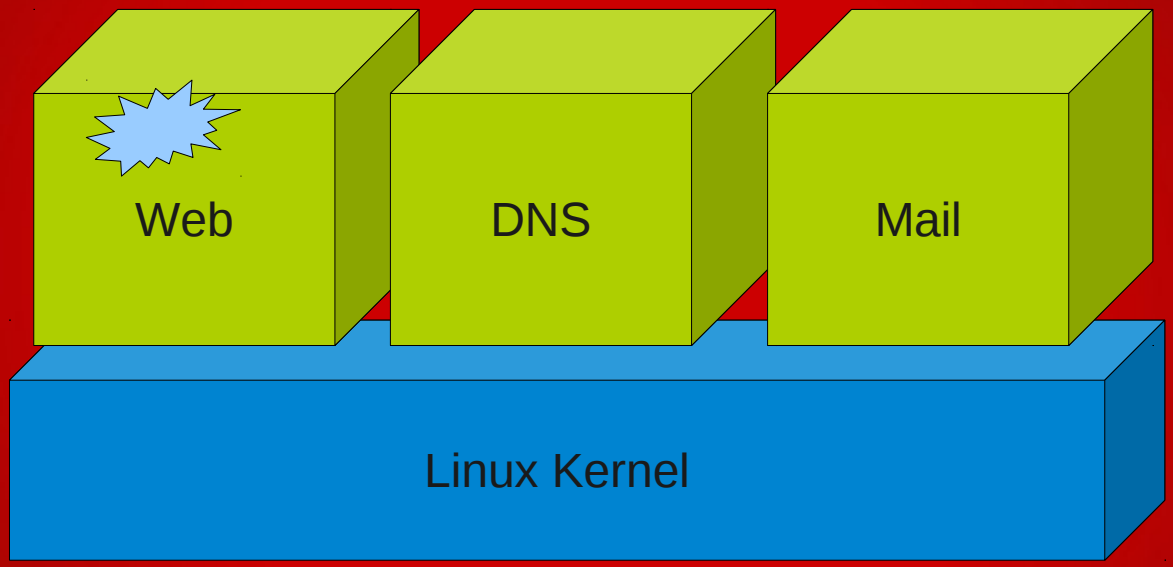
Before SELinux



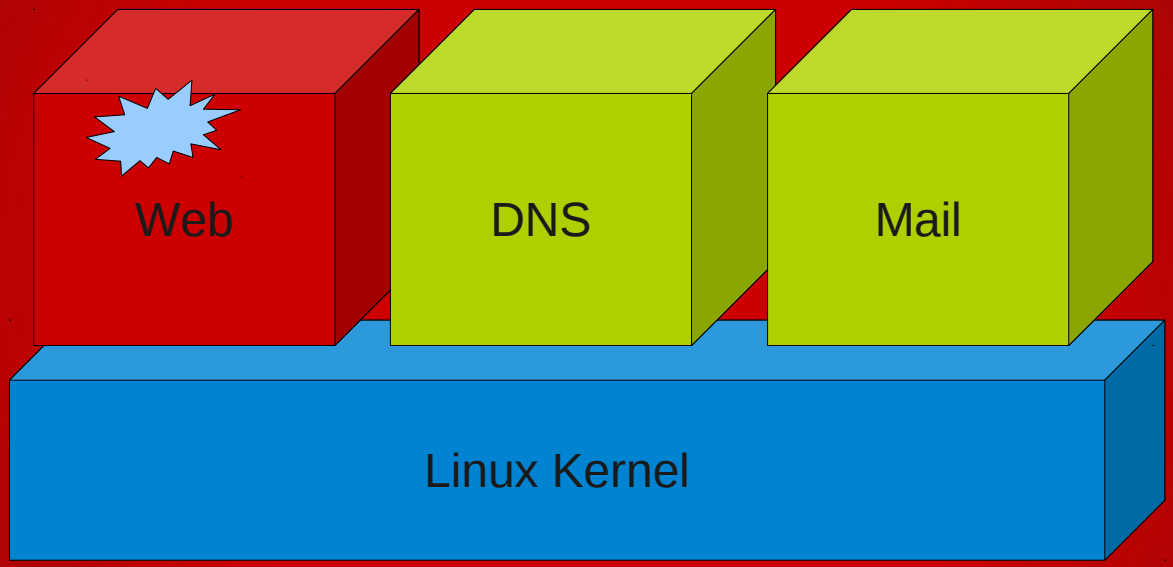
Processes all have equal access to the system...



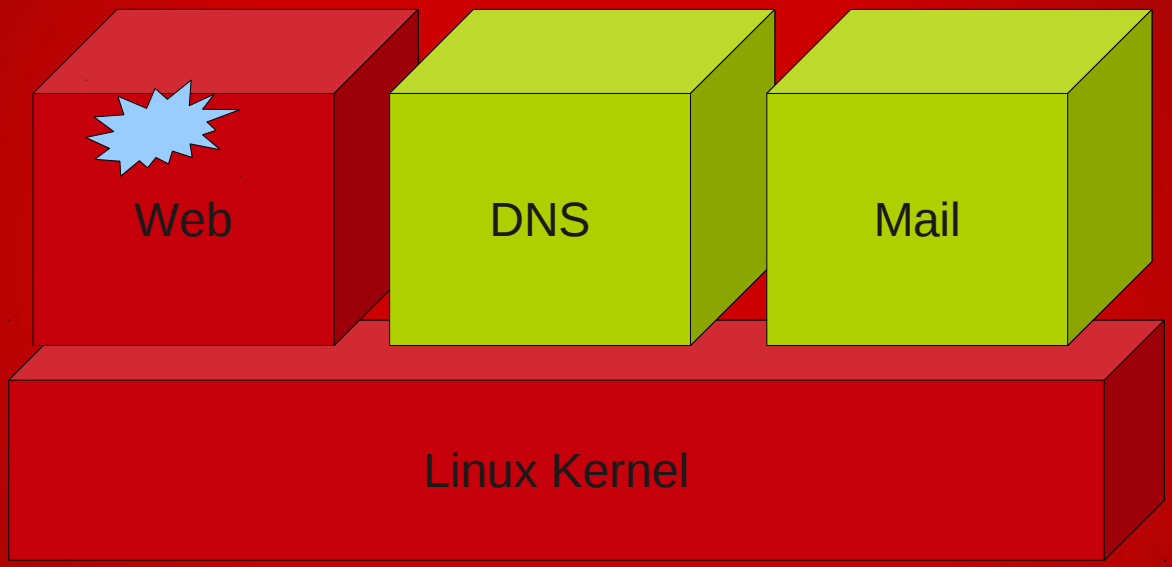
Processes all have equal access to the system...



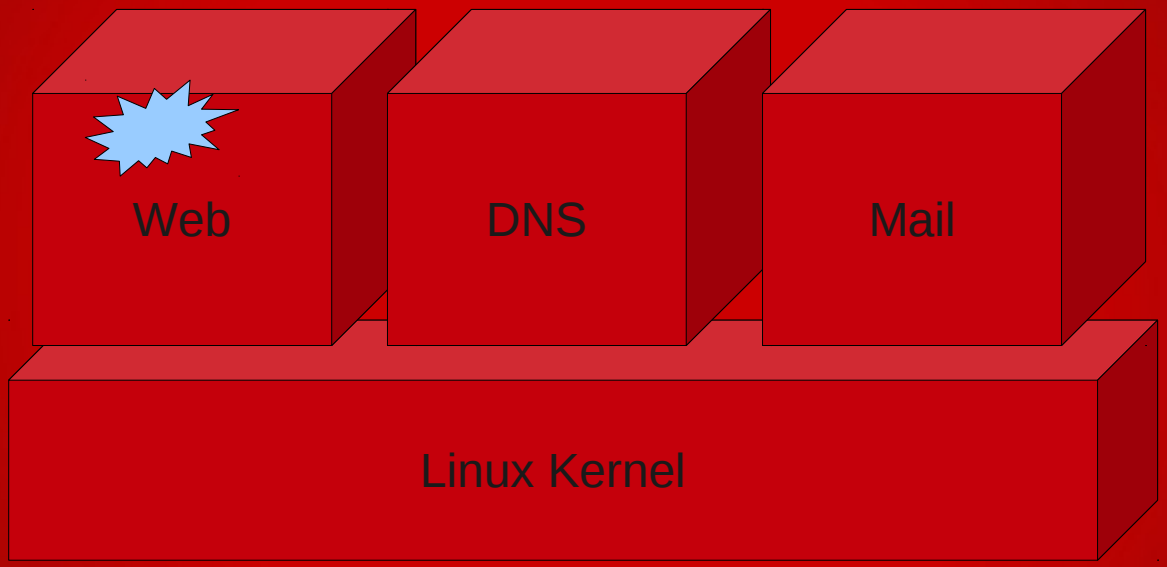
...if one is attacked...



...taken over due to vulnerability ...

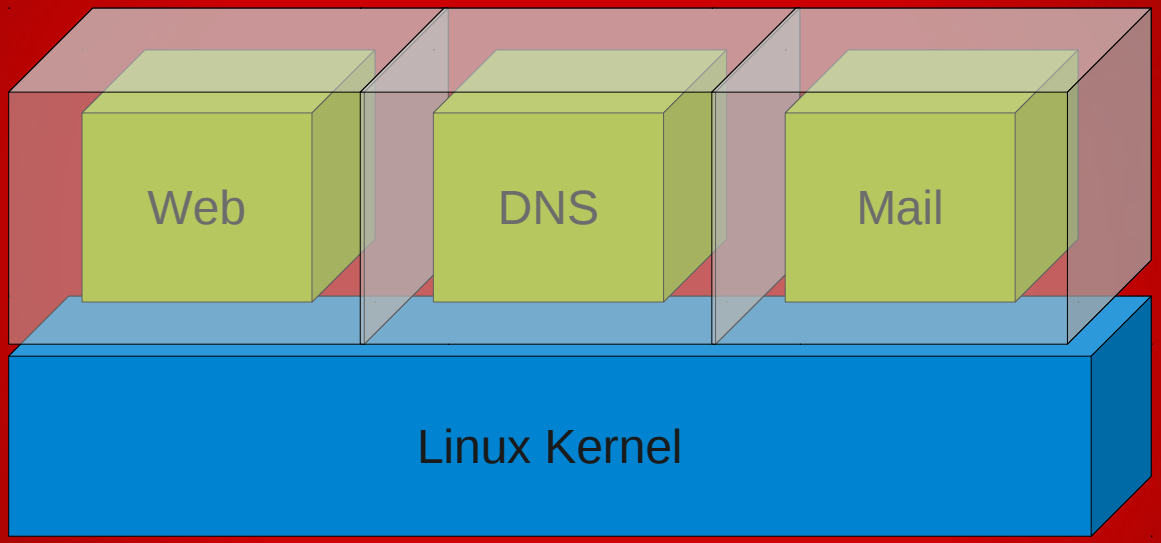


...and gets a privilege escalation...

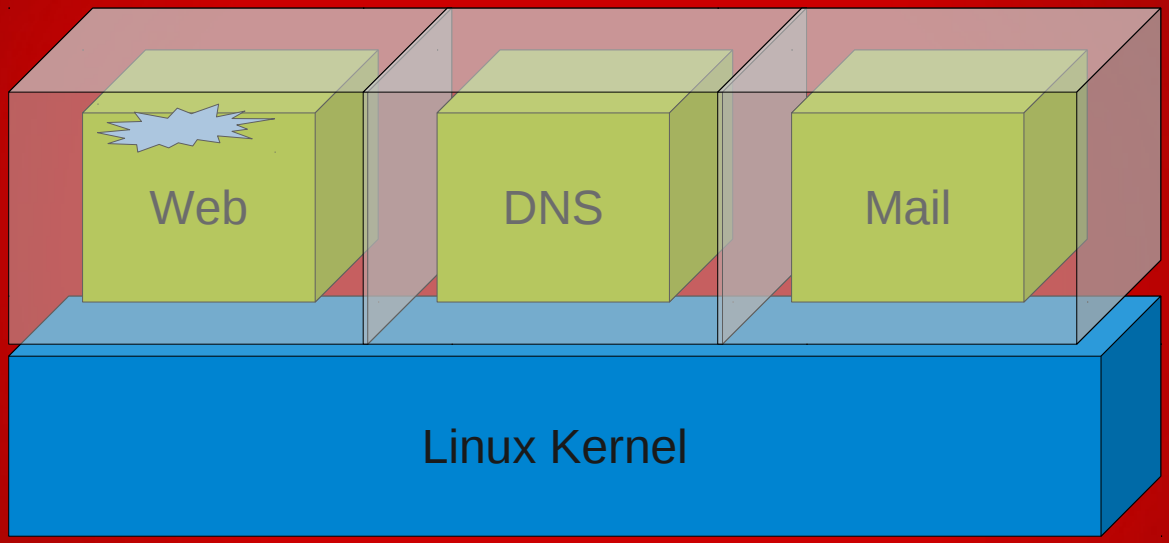


...the system is lost.

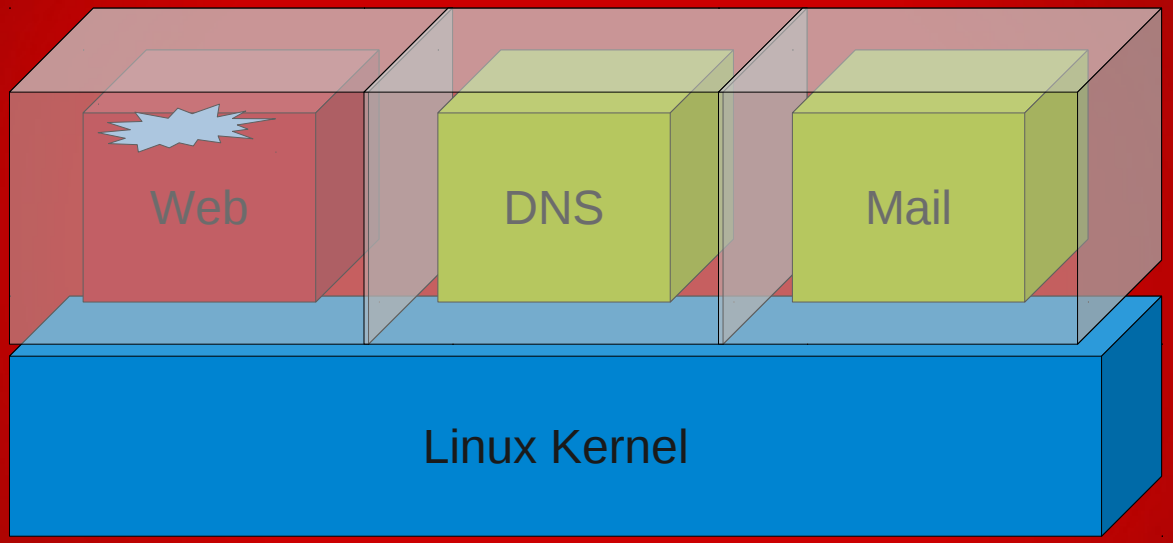
With SELinux



Each process is confined in its own sandbox, distinct from the others.

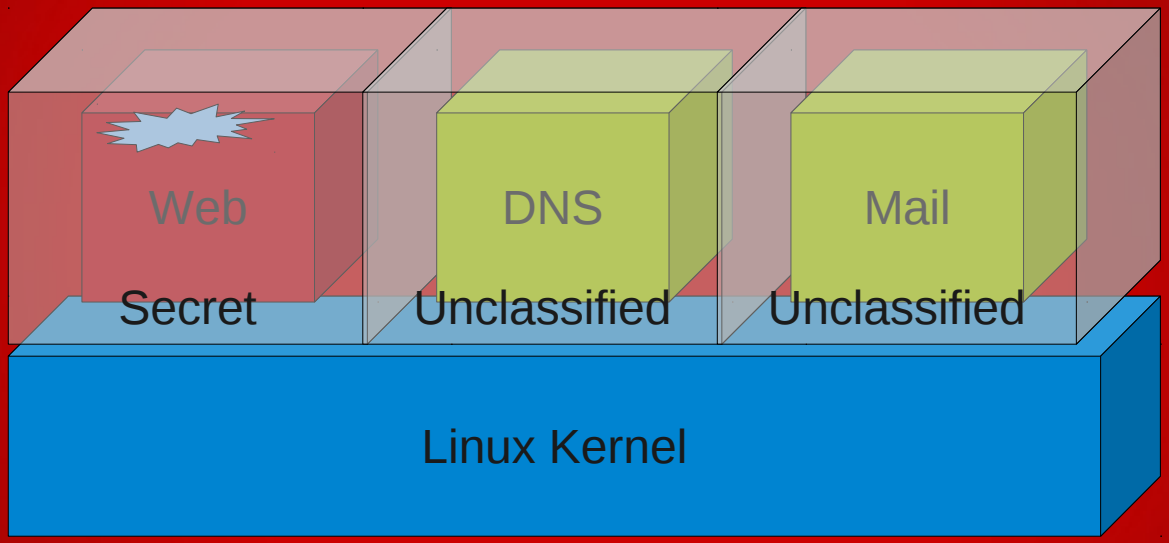


If a process is attacked...



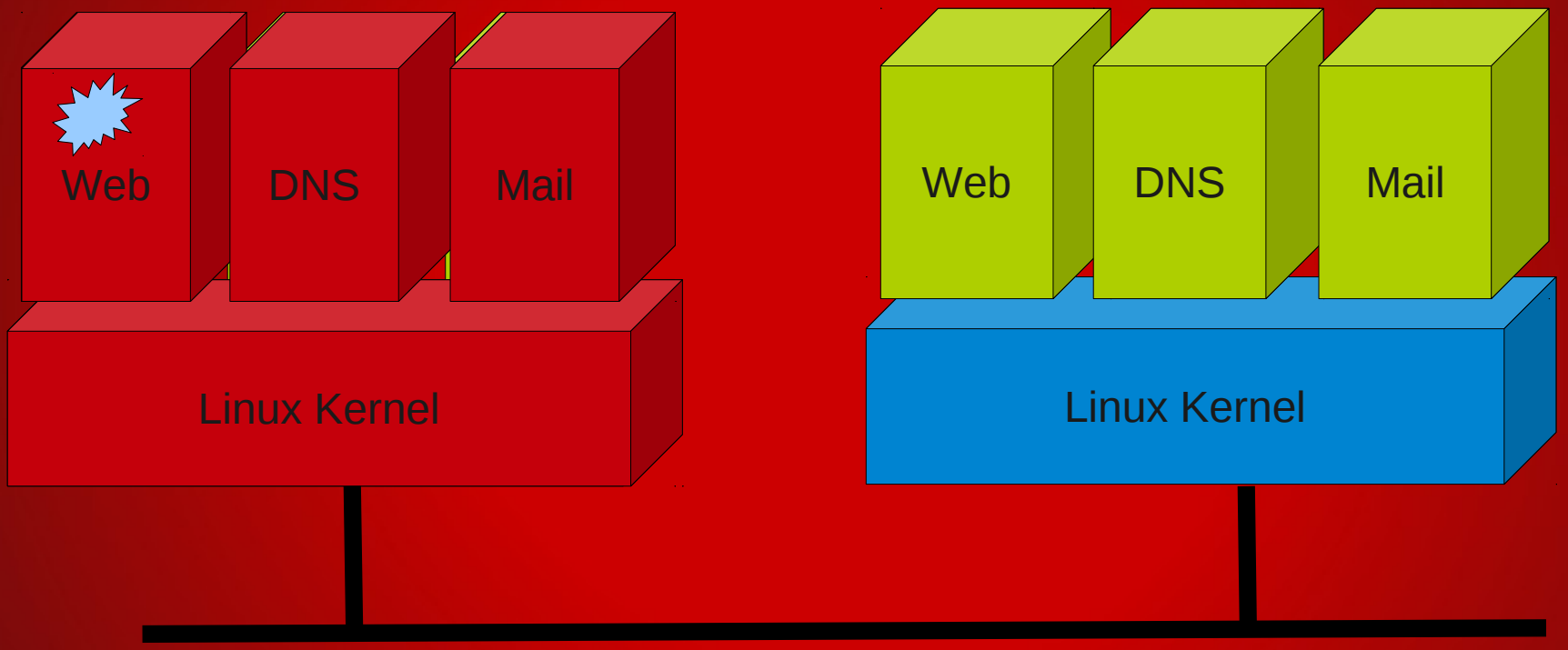
...and compromised, there is far less exposure. You lose the process, not the system.

With SELinux and MLS/MCS



We can label the sandboxes with a level of sensitivity and categories.

...now add virtualization...

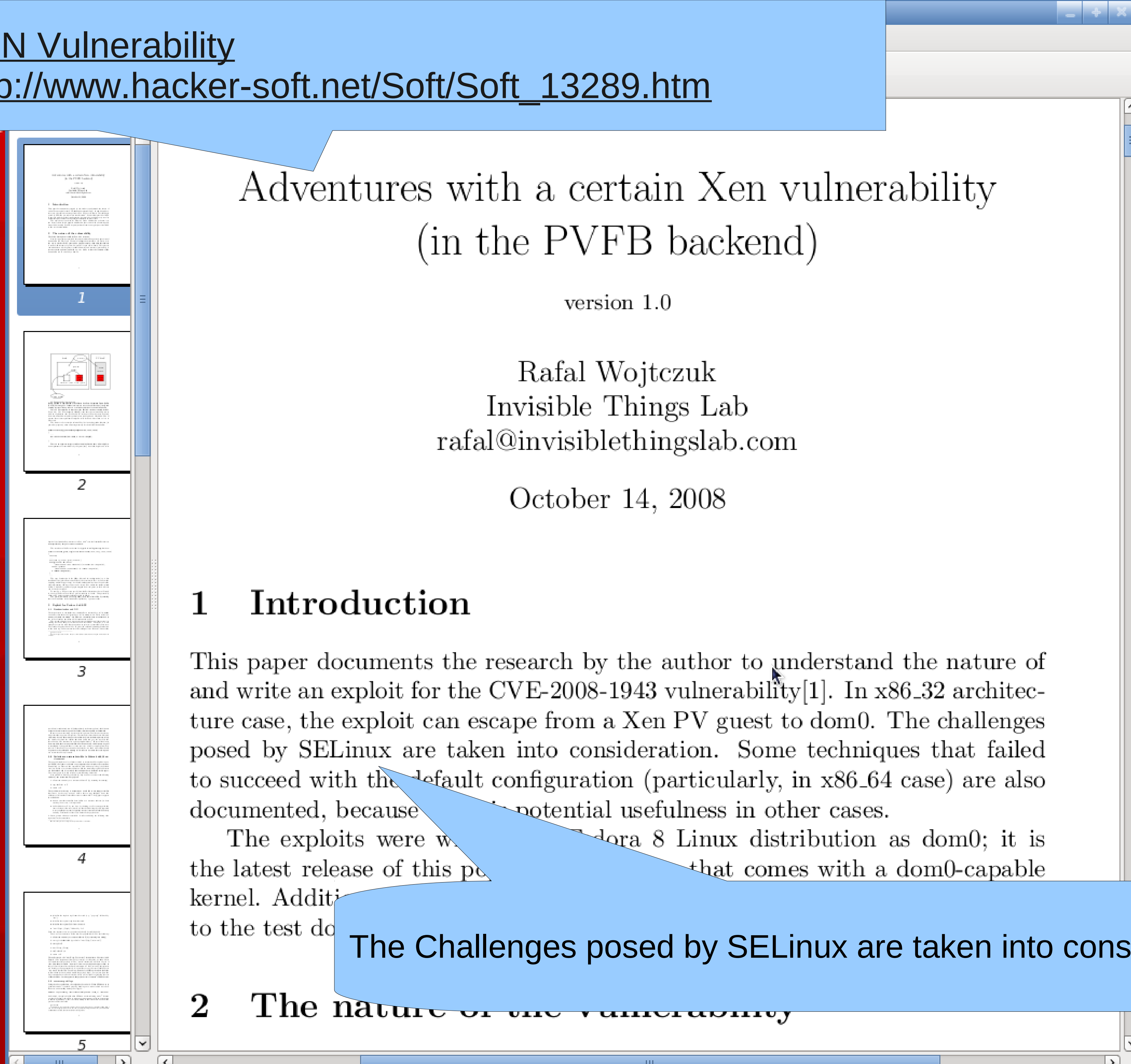


...before virtualization...

Hypervisor Vulnerabilities

- Not theoretical
- Evolving field
- Potentially huge payoffs
- Xen already compromised...
  - Over 200 Security Problems found in Xen?
- Vmware vulnerabilities
  - Google returns over 500,000 results

XEN Vulnerability
http://www.hacker-soft.net/Soft/Soft_13289.htm



Adventures with a certain Xen vulnerability (in the PVFB backend)

version 1.0

Rafal Wojtczuk
Invisible Things Lab
rafal@invisiblethingslab.com

October 14, 2008

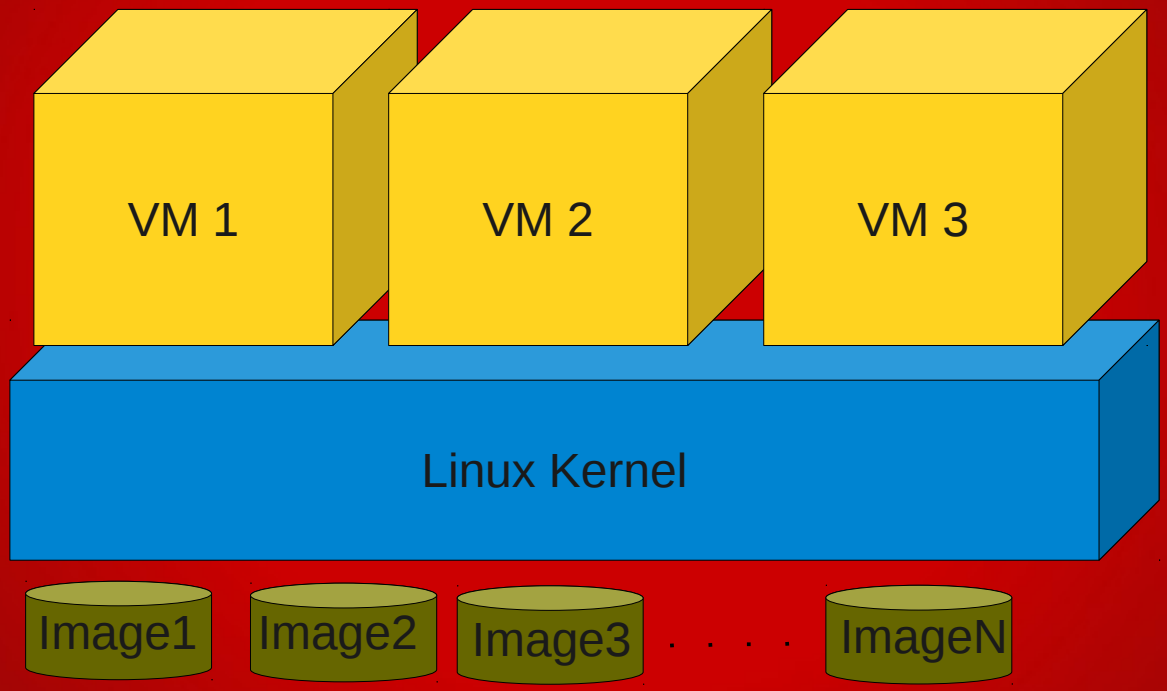
1 Introduction

This paper documents the research by the author to understand the nature of and write an exploit for the CVE-2008-1943 vulnerability[1]. In x86_32 architecture case, the exploit can escape from a Xen PV guest to dom0. The challenges posed by SELinux are taken into consideration. Some techniques that failed to succeed with th... default configuration (particularly, in x86_64 case) are also documented, because ... potential usefulness in other cases.

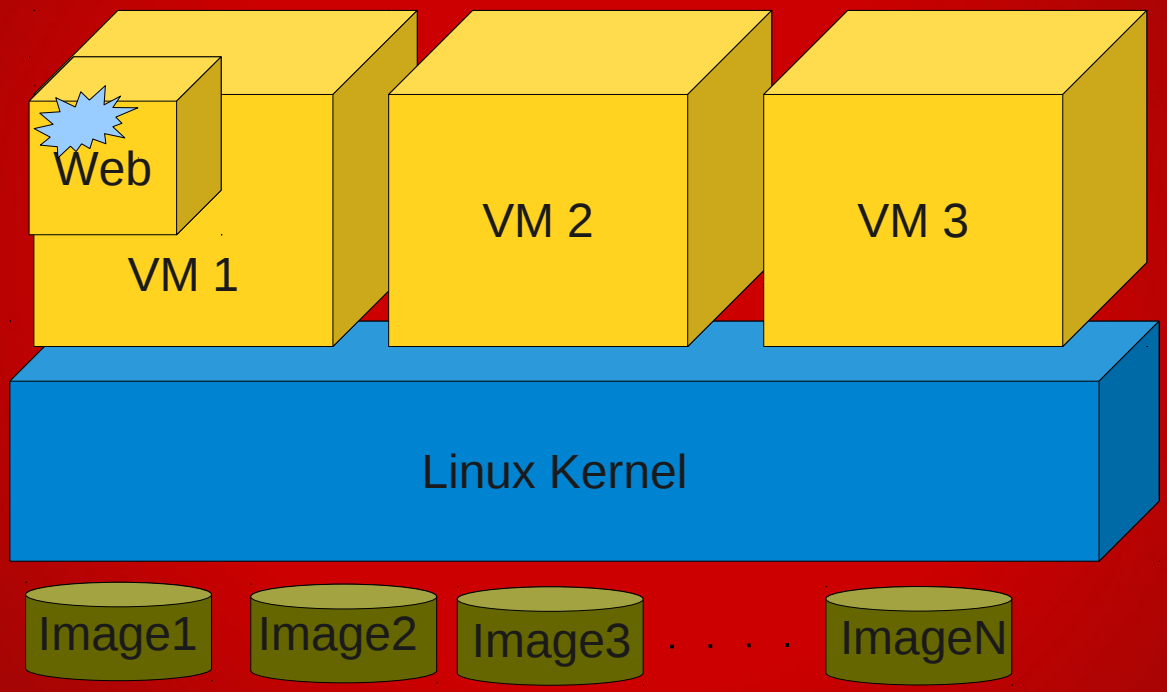
The exploits were w... ...dora 8 Linux distribution as dom0; it is the latest release of this p... ...that comes with a dom0-capable kernel. Additi...
to the test do...

2 The nat...

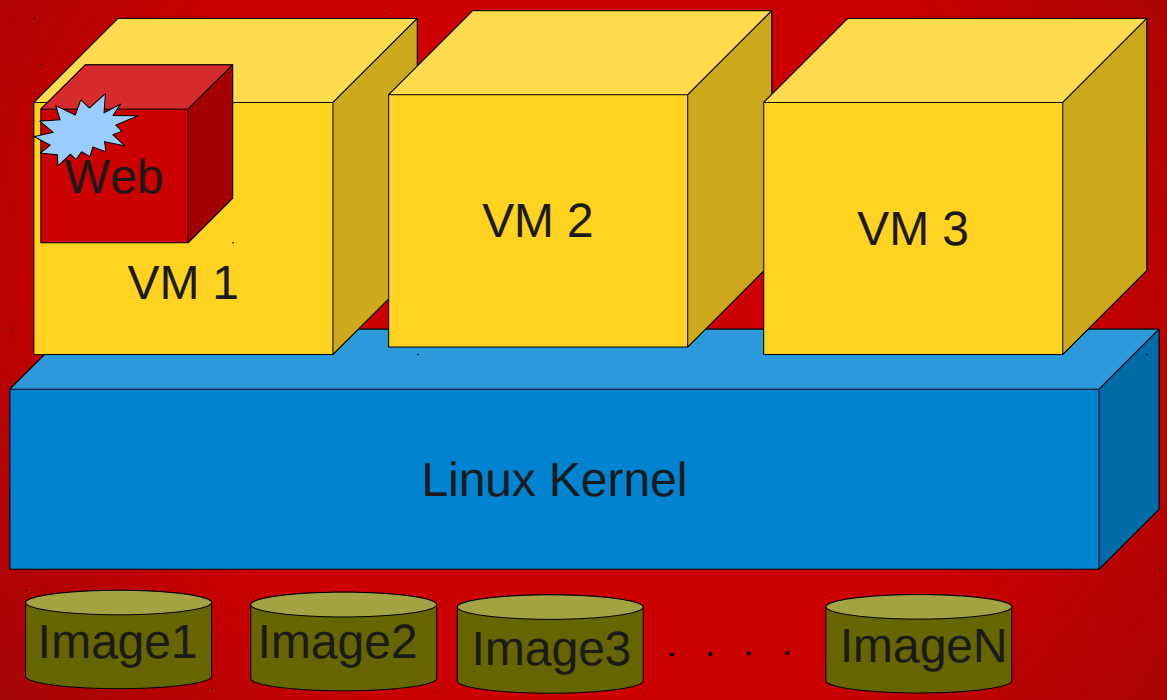
The Challenges posed by SELinux are taken into consideration.



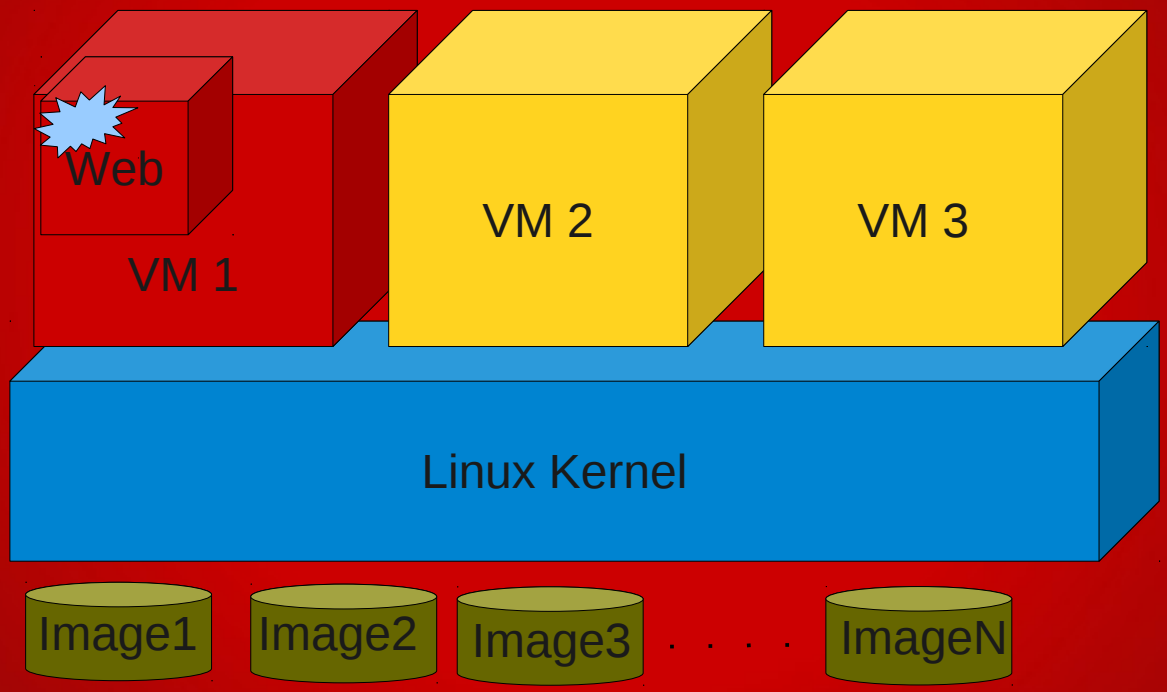
Virtual machine processes all have equal access to the system...



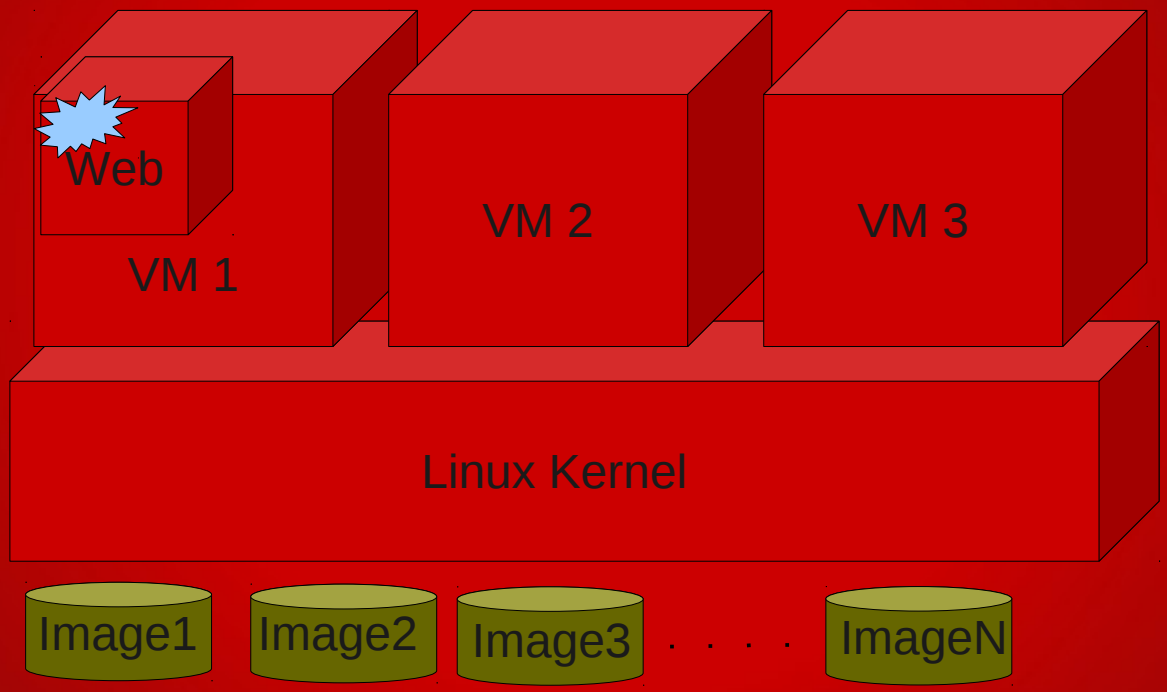
...if application on virtual machine is attacked...



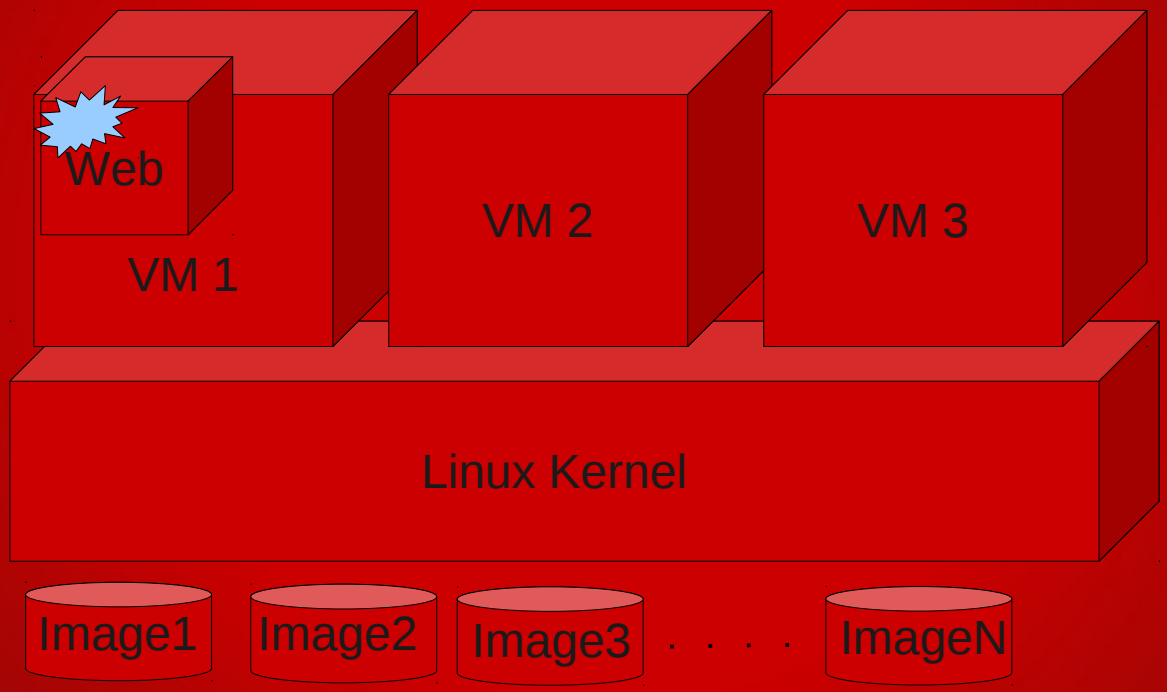
...compromised...



...and gets a privilege escalation...



.. and your machine has a Hypervisor Vulnerability ...



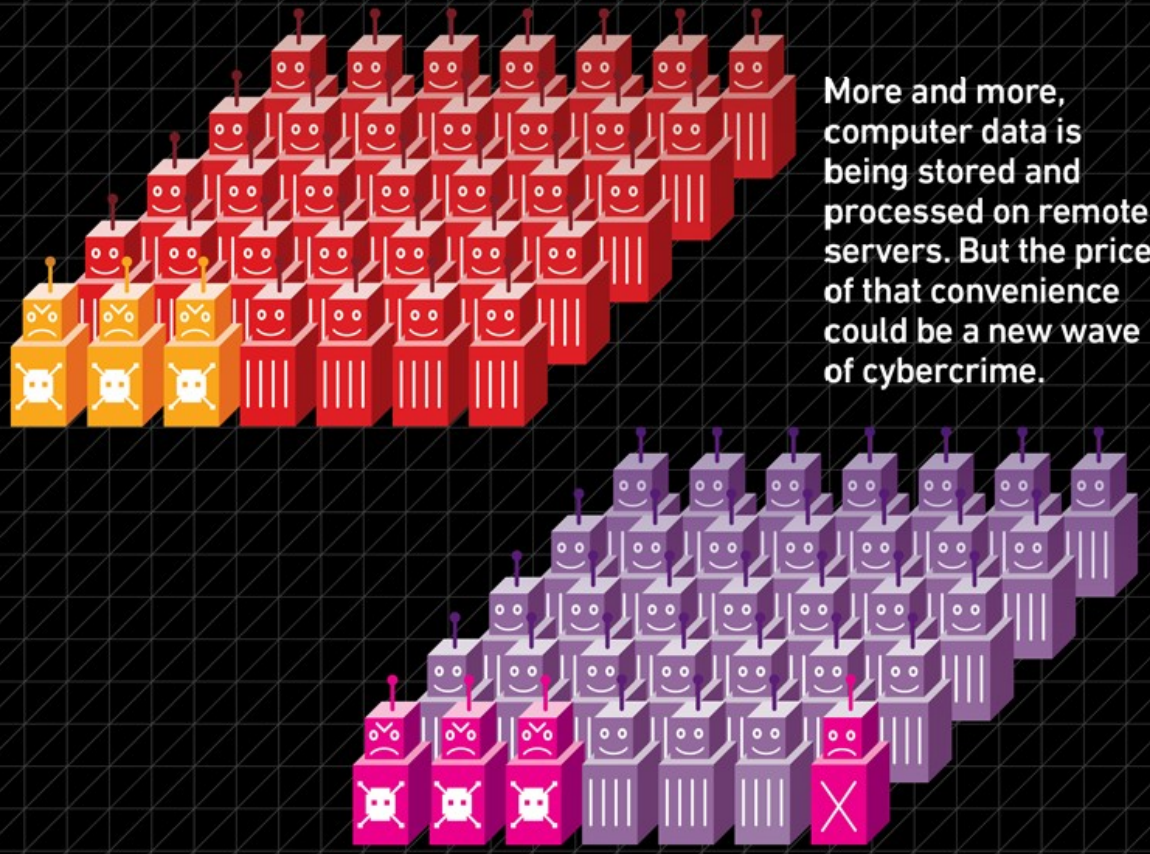
.. But not just the running VM's and host, but all images ...

redhat.

DATA SECURITY

NEXT UP: HOW 2.0

HACKING THE CLOUD



More and more, computer data is being stored and processed on remote servers. But the price of that convenience could be a new wave of cybercrime.

BY RENA MARIE PACELLA
ILLUSTRATIONS BY HYPERAKT

Popular Science April 2011

SELinux to the rescue

SELinux is all about labeling

Processes get labels

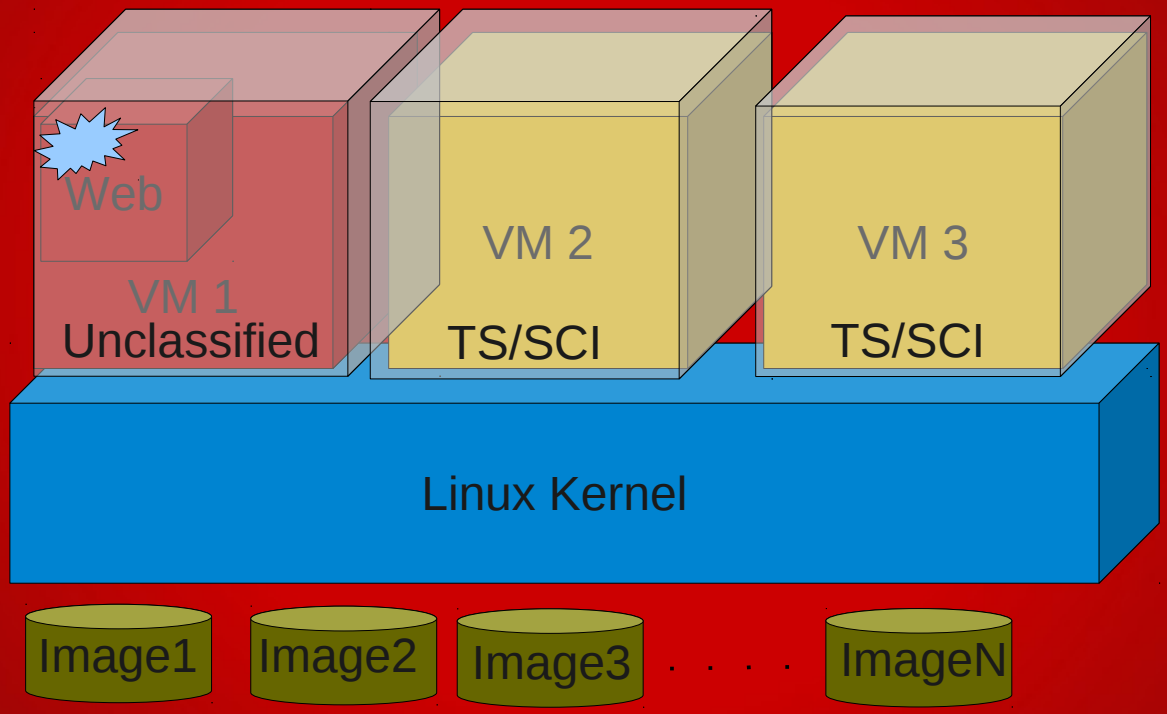
Virtual machines with kvm are processes!!!

Files/Devices Get Labels

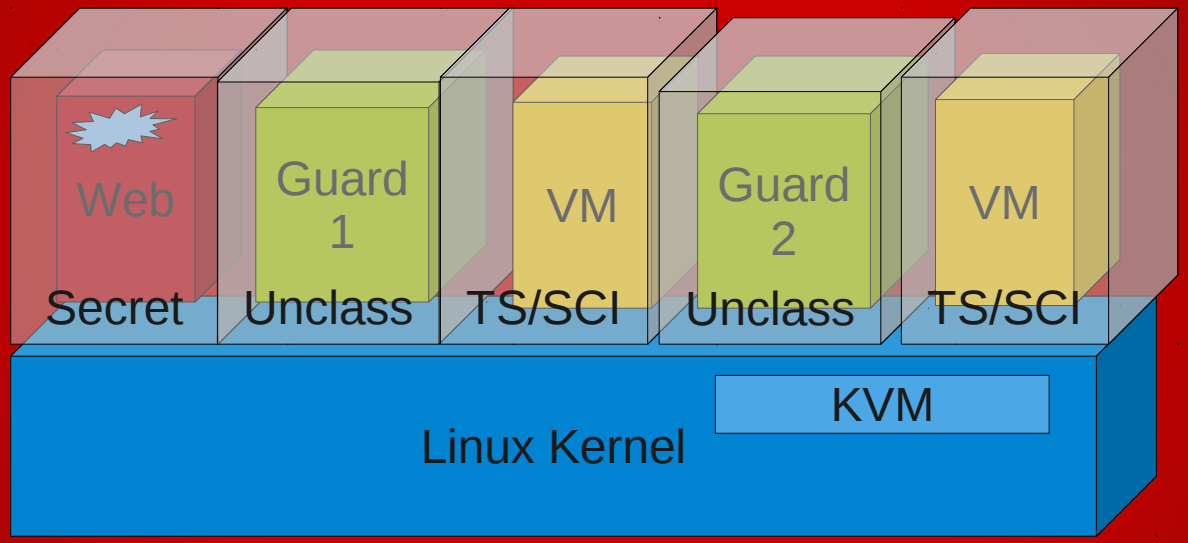
Virtual images are stored on files/devices!!!!

Rules control how Process Labels Interact with Process/File Labels.

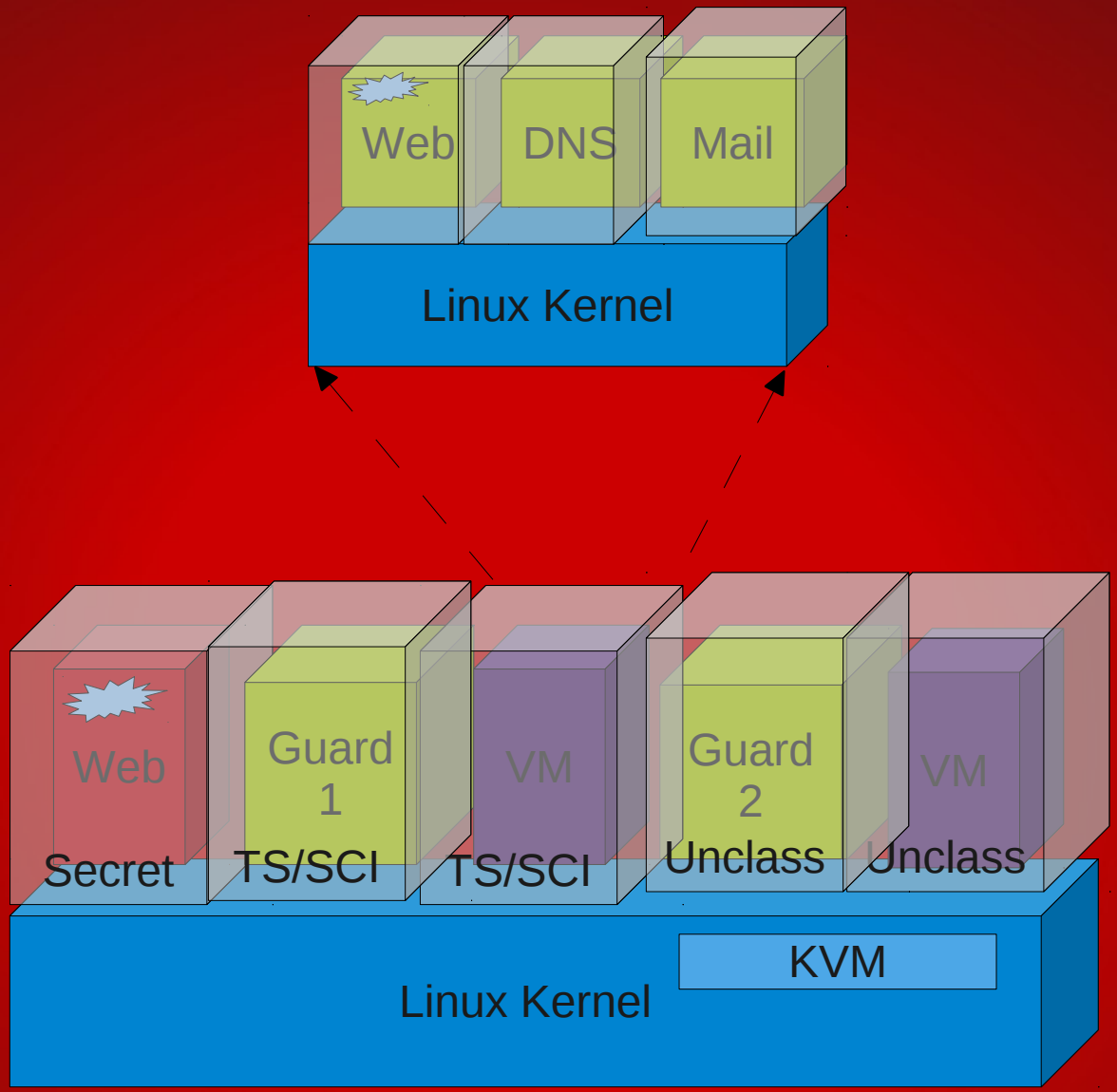
Kernel Enforces these Rules.



Compromised Virtual Machine confined despite hypervisor vulnerability



KVM guests are processes, so we can confine them like processes.



And of course the guest operating system can also run SELinux


Dan Walsh's Blog – sVirt to the Rescue – Mozilla Firefox
File Edit View History Bookmarks Tools Help
Dan Walsh's Blog - sVirt to the ...
danwalsh.livejournal.com/45194.html
svirt to the re
Most Visited Calendar Bug Red Hat Money Sports
Username Password Log in
Remember Me Forgot your password? Create an Account
You are viewing danwalsh 's
DANWALSH
RECENT ENTRIES FRIENDS ARCHIVE USER INFO RSS
Dan Walsh's Blog
Got SELinux?
sVirt to the Rescue
At the recent Black Hat conference Nelson Elhage presented:
Virtualization Under Attack: Breaking out of KVM
The exploit, CVE-2011-1751, would allow a cracker to execute code in qemu-kvm process on the host.
danwalsh
August 25th, 2011
Note: Red Hat fixed this problem back in May 2011 prior to the publication of the paper and exploit. Customers who applied our security updates are not affected by this issue. So 0 days of exposure.
In the presentation there is this bullet point:
qemu-kvm is often sandboxed using SELinux or similar, meaning that successful exploitation will often require a second privesc within the host.
(Fortunately, Linux never has any of those)

http://peoc3t.monmouth.army.mil/fbcb2/fbcb2.html