

# **RHEL5 Baseline Settings**

Steve Grubb  
Principal Engineer  
Red Hat

# RHEL5 Baseline Settings Project

- RHEL5 Workstation
- Project
- Configuration choices
- Resulting Security Profile

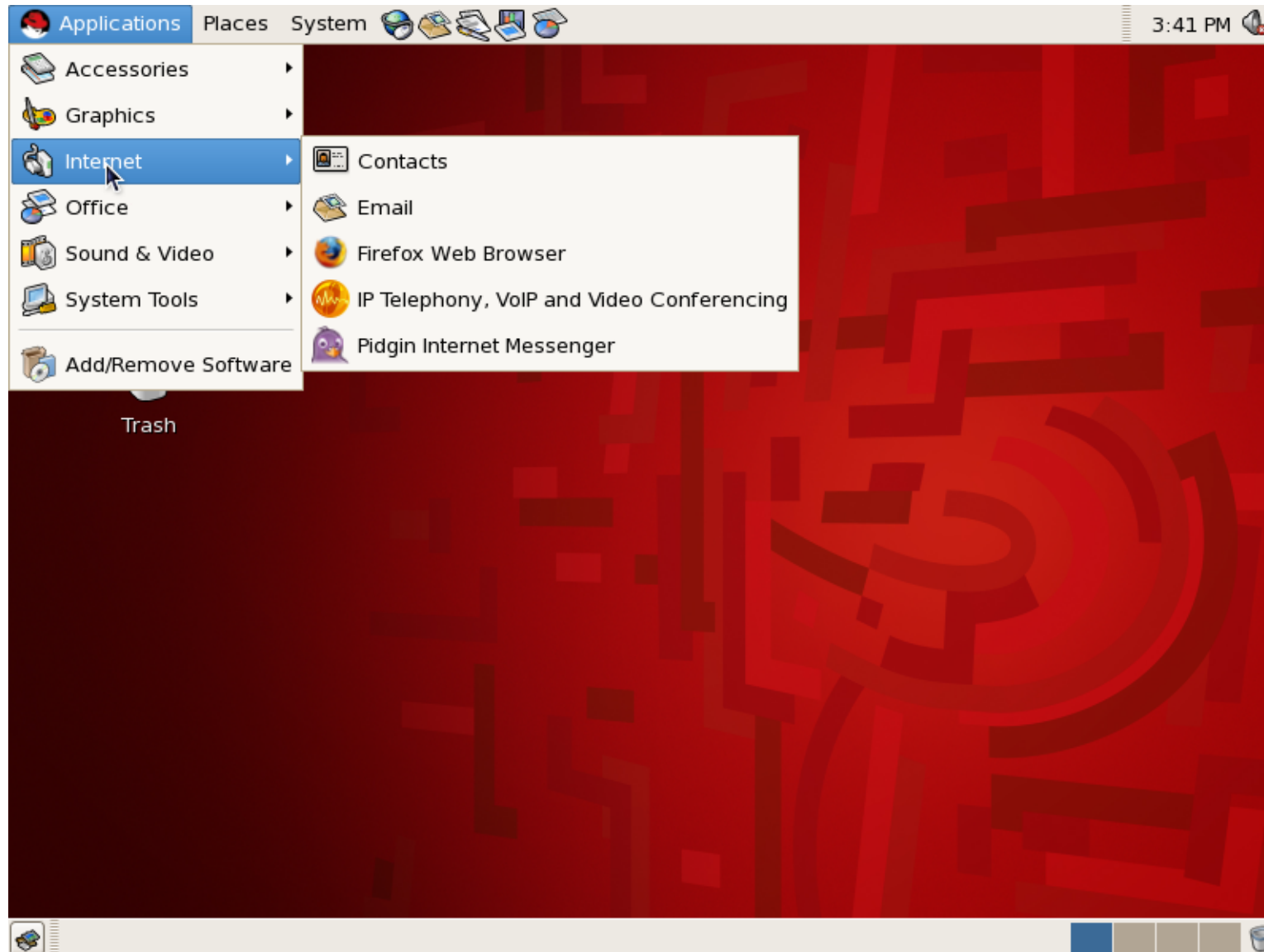
# RHEL5 Workstation

- Comprehensive Office Suite – Open Office 3.1.1
- Web Browsing – Firefox
- Mail Clients – calendar and contact management
- Messaging – IRC, VOIP, messaging applications
- Graphics – Image management, sophisticated editing
- Wireless, Networking, Cameras, printers – many devices
- Smart card login, Encrypted disks, VPN, Builtin Firewall
- Laptop and power management - ACPI
- Multi-lingual – At least 60 supported

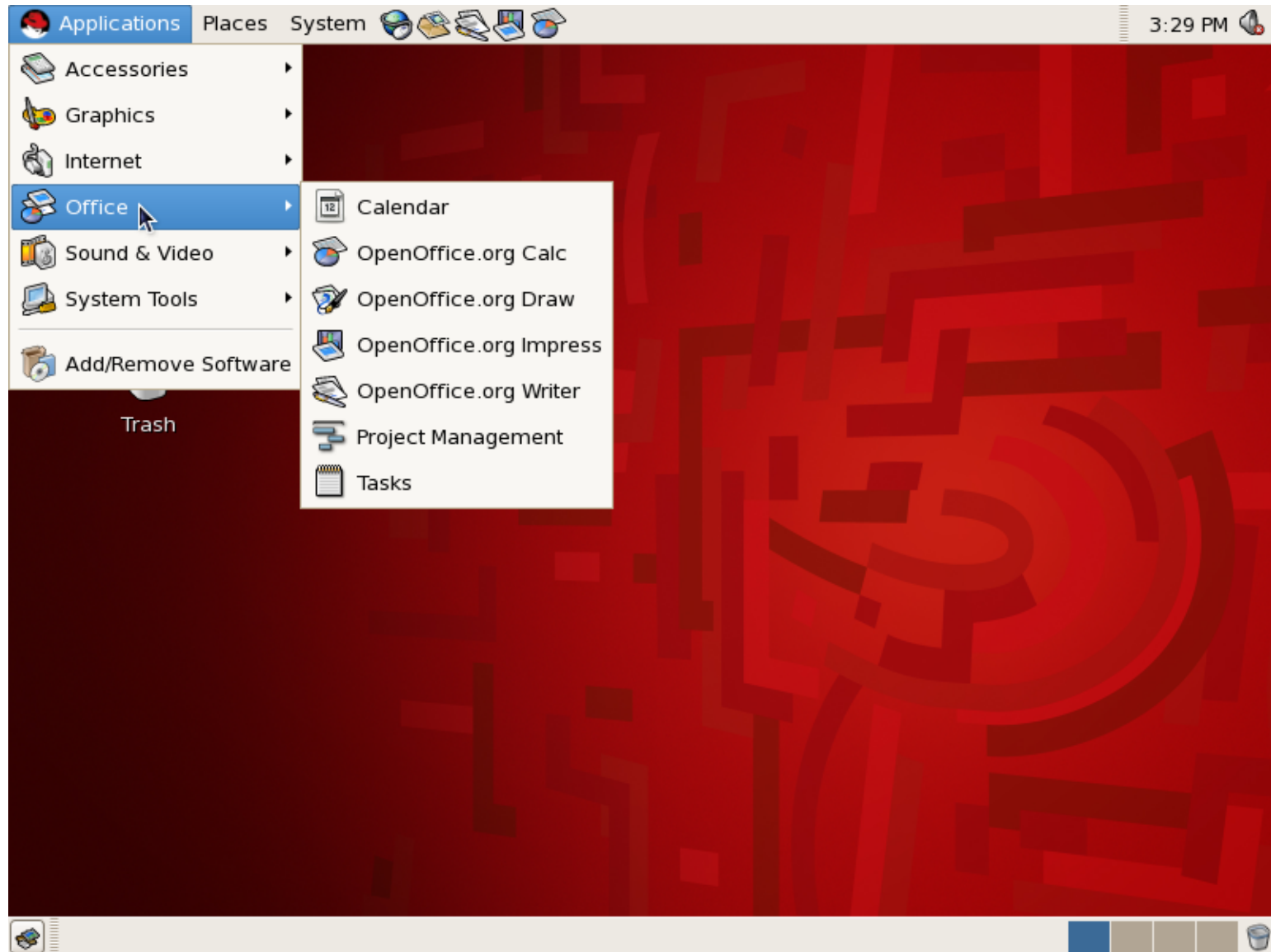
# RHEL5 Workstation

- Some options include:
  - Virtualization
  - Server apps
  - Developer tools
  - Multiprocessor and unlimited memory
  - Interoperability – Samba, NFS

# RHEL5 Workstation



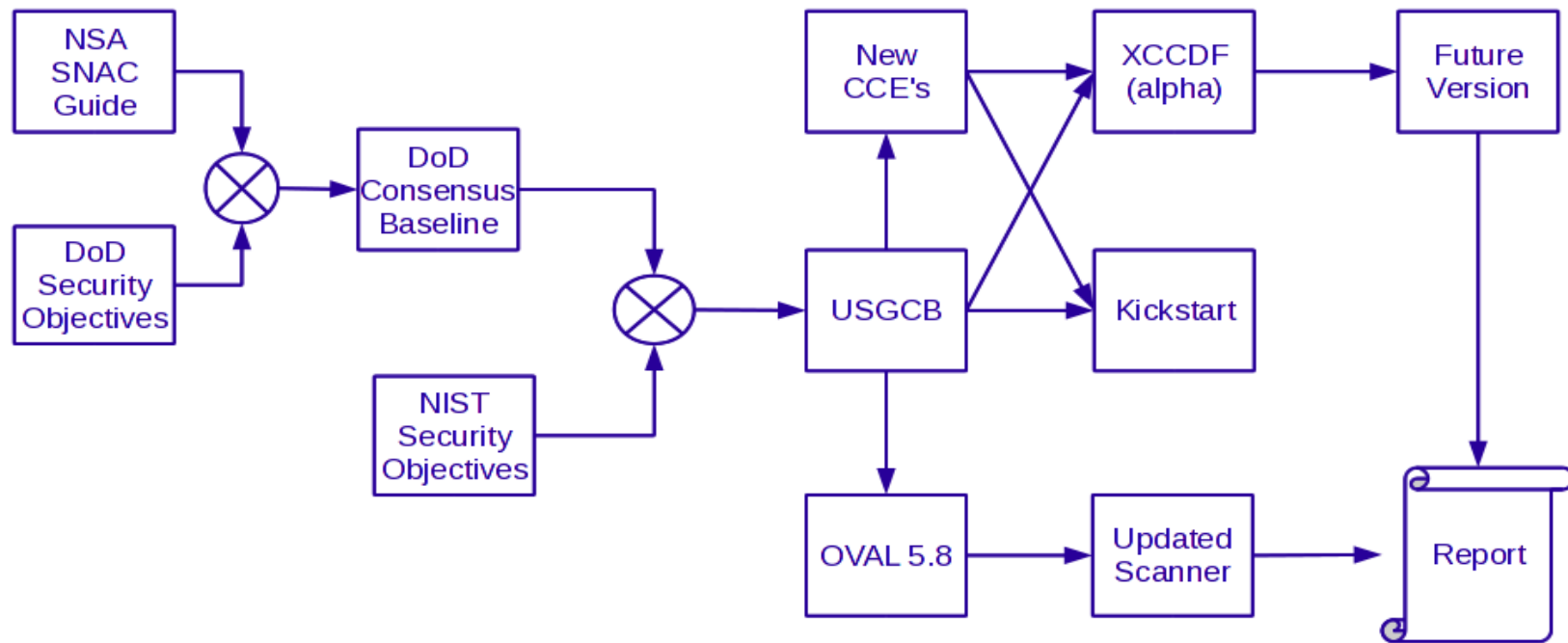
# RHEL5 Workstation



# RHEL5 Workstation



# Project





# OVAL 5.8

- Independent Schema
  - filehash58\_test
    - new hashes: SHA224, SHA256, SHA384, SHA512
  - environmentalvariable58\_test
    - Allows pid in test

# OVAL 5.8

- Linux Schema
  - iflisteners\_test
  - partition\_test
  - rpmverify\_test
  - selinuxboolean\_test
  - selinuxsecuritycontext\_test

# OVAL 5.8

- Unix Schema
  - fileextendedattributes\_test
  - gconf\_test
  - process58\_test
    - execshield, loginuid, posix capability, selinux context, login session id.
  - routingtable\_test
  - sysctl\_test

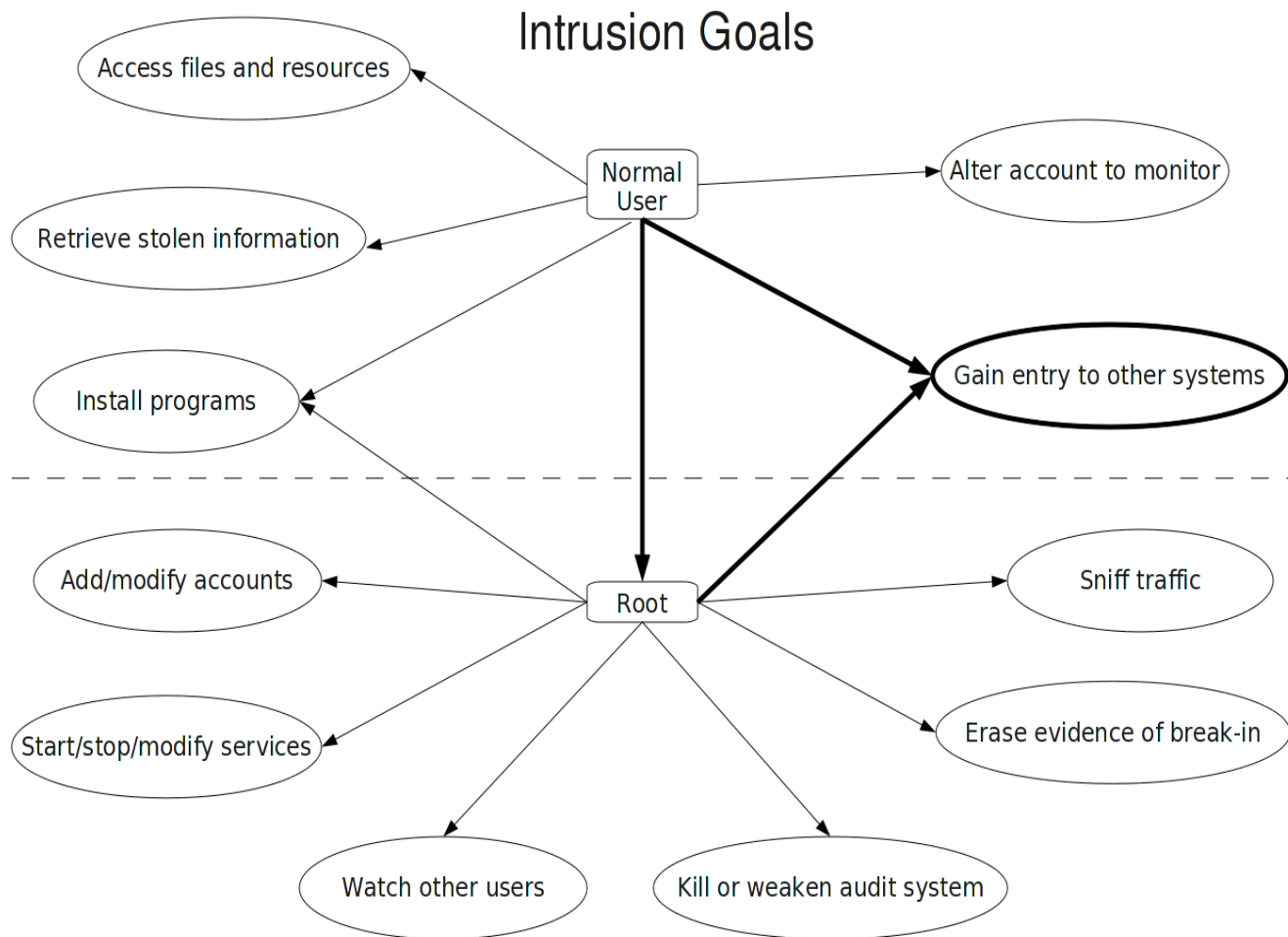
# Project

- Status
  - Is a Tier 3 DoD baseline submission
  - XCCDF will be available
  - Kickstart will be available
  - Should be on NVD web site
  - On-track to become USGCB candidate submission

# Configuration Choices

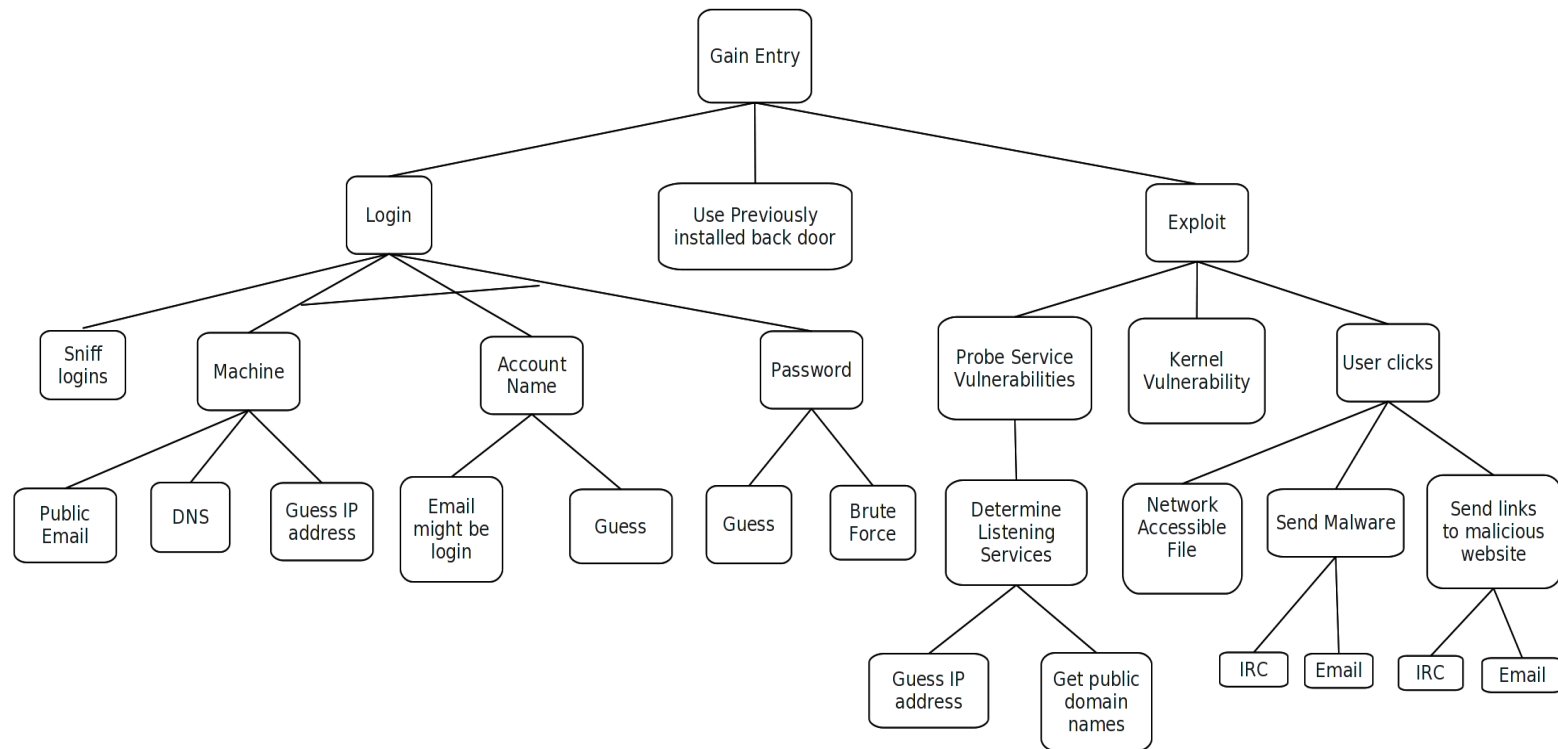
- Principles
  - Reduce attack points
  - Prefer like programs with best record
  - Prefer programs not being deprecated in RHEL 6
  - Workaround possible weaknesses by configuration options

# Configuration Choices



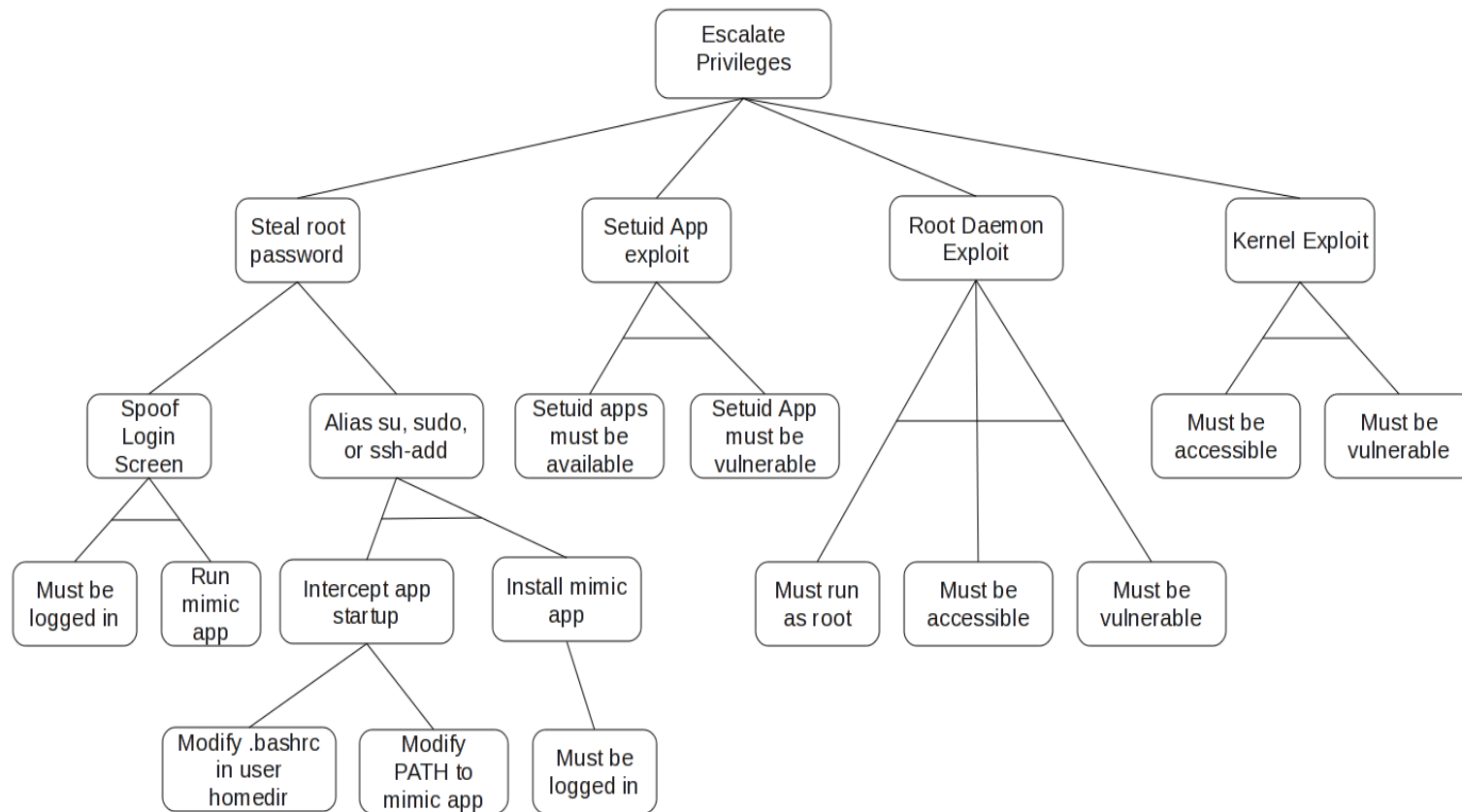
# Configuration Choices

Network Intrusion Attack Tree



# Configuration Choices

Privilege Escalation Attack Tree





# Configuration Choices

Goal	Countermeasure
Login	Require strong passwords
Use previously installed backdoor	Scan network ports and interfaces
Probe service vulnerabilities	Reduce services, select like service with best security record
Attempt Network kernel vulnerability	Reduce network related kernel modules
Setuid app exploit	Reduce setuid programs, defensive partitioning
Root daemon exploit	Reduce services
Local kernel exploit	Reduce kernel modules

# Security Profile

- Roughly 260 CCE's to check the configuration
- SE Linux is on and enforcing
- The firewall only allows IKE and sshd inbound traffic
- Server-like packages removed: xinetd, telnet, rsh, vsftpd, dhcp, httpd.
- Sshd only uses the following ciphers: aes128-ctr, aes192-ctr, aes256-ctr (to workaround the plaintext recovery attack on ssh protocol V2)
- Umask of 077 set for users, 027 for daemons

# Security Profile

- Boot sequence is not interruptable
- Lot of updates to network sysctls
  - No ip forwarding, redirects, source routed packets,
- Using su requires group wheel membership
- Passwords are stored as sha512 hashes
- Cron directory permissions are 0700 root

# Security Profile

- Some default packages were switched
  - Openswan replaces ipsec-tools for VPN
  - Postfix replaces sendmail for MTA
  - Rsyslog replaces syslogd

# Security Profile

- Requires a couple manual checks:
  - Calls out for rpm verify test to check that binaries are as expected.
  - Mount table checks (partitioning and options)
  - Generally anything mentioned as new feature in OVAL 5.8 requires a manual check

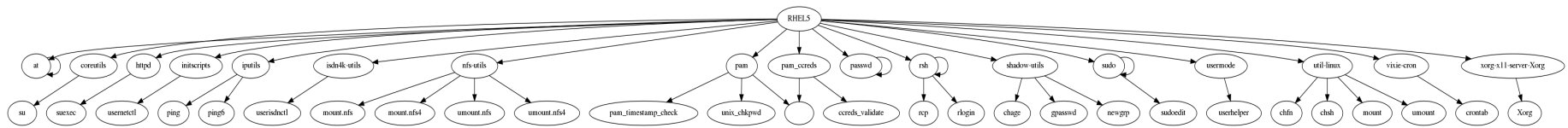
# Changes

	Plain	Baseline
Packages	947	770
Services	44	23
Listening Apps	9	5
Firewall openings	5	3
Setuid Apps	35	27
Partitions	2	7
Disk Usage	3.02 Gb	2.87 Gb

# /etc/fstab

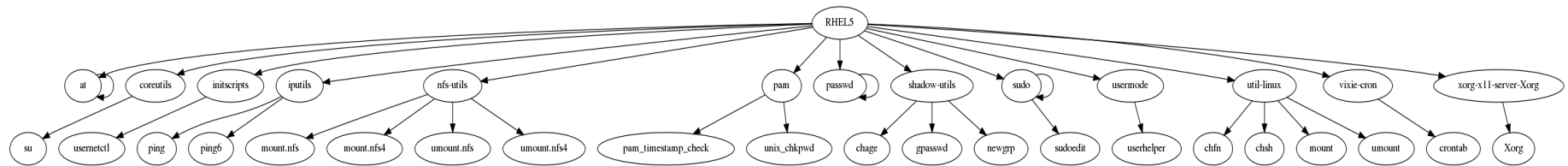
```
/dev/vgroup1/root      /          ext3      defaults          1 1
/dev/vgroup1/home      /home      ext3      defaults,nodev    1 2
/dev/vgroup1/var       /var       ext3      defaults          1 2
/dev/vgroup1/varlog    /var/log   ext3      defaults,nodev,noexec,nosuid 1 2
/dev/vgroup1/audit     /var/log/audit ext3      defaults,nodev,noexec,nosuid 1 2
/dev/vgroup1/temp      /tmp       ext3      defaults,nodev,noexec,nosuid 1 2
LABEL=/boot           /boot      ext3      defaults,nodev,noexec,nosuid 1 2
tmpfs                  /dev/shm   tmpfs     defaults,nodev,noexec,nosuid 0 0
devpts                 /dev/pts   devpts    gid=5,mode=620    0 0
sysfs                  /sys       sysfs     defaults          0 0
proc                   /proc      proc      defaults          0 0
LABEL=SWAP-vda2       swap       swap      defaults          0 0
/tmp                   /var/tmp   ext3      bind,nodev,noexec,nosuid    0 0
```

# Setuid apps (before)

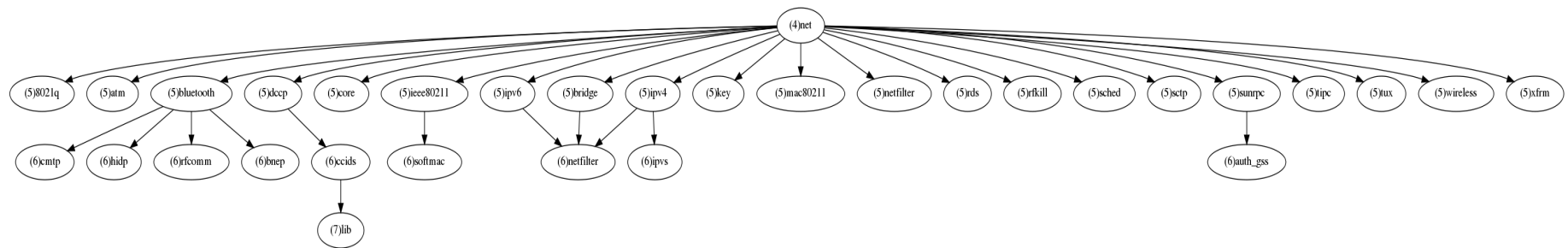




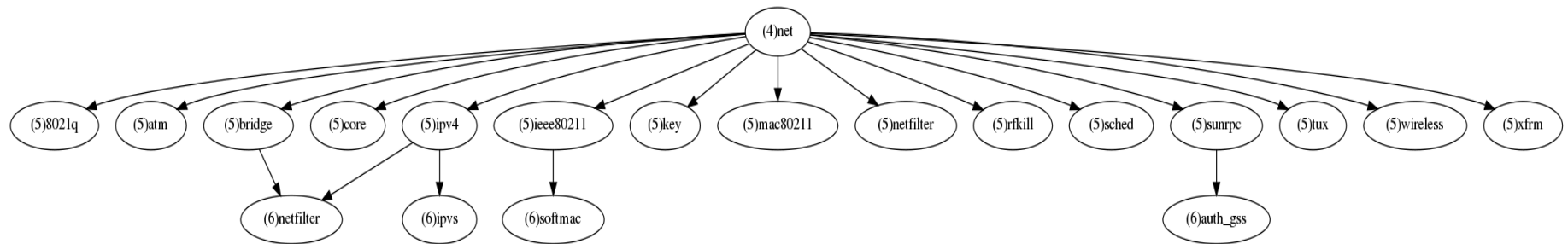
# Setuid Apps (after)



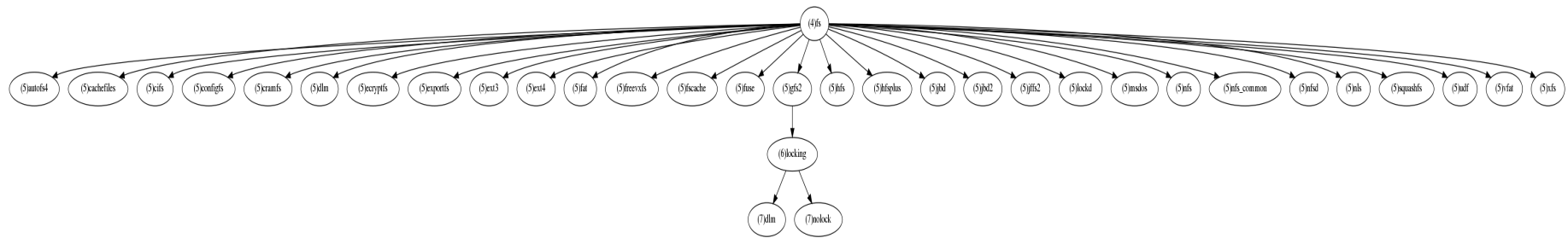
# Network modules (before)



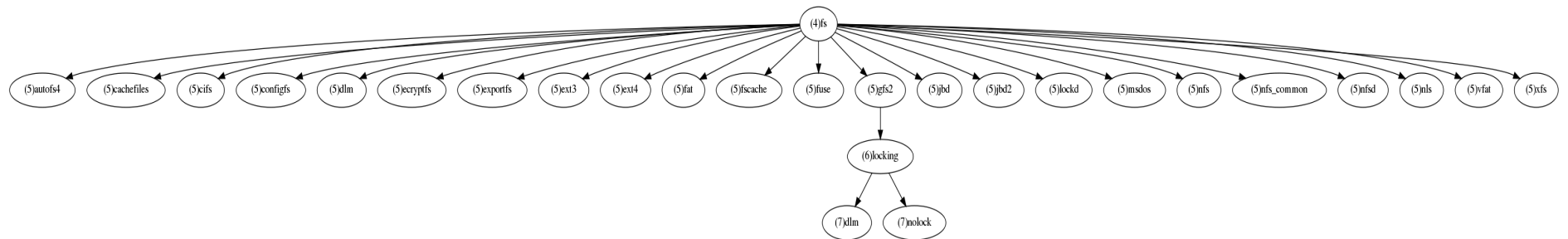
# Network modules (after)



# Filesystem modules (before)



# Filesystem modules (after)



# Using the kickstart

- Be sure to change the root password
- Be sure to change the password for the bootloader
- You need to update the `rsyslog.conf` for your log aggregator
- You also need to change the section saying where your source image is located
- May need to change the warning banner for you local policy

# Questions

sgrubb @redhat.com  
[www.openscap.org](http://www.openscap.org)

# OpenSCAP Status

- We now can do any SCAP 1.0 content
- Its a feature in F-14
  - Content be prepped
  - Content tailoring GUI
  - XSLT transforms: Docs, lockdown script
- Will be updated in RHEL 6 update 1
- Possibly added into RHEL 5 update 7



# Related Projects

- SecState – Takes XCCDF transfers to puppet for system management
- First Aid Kit – scans system to analyze what is wrong with it
- New Use Case: Release Engineering compose checks

# Future work

- Meet SCAP 1.1
- Add Java bindings
- Migrate to other platforms
- Take through certification
- Eventually meet SCAP 1.2

# Content Tailoring

The screenshot shows a software window titled "Main" with a toolbar containing icons for Main, Profiles, Tailoring, Scan, Reports, Edit, and Settings. Below the toolbar are two tabs: "XCCDF" (selected) and "OVAL". The main content area displays the following information:

**Info:**

- File: scap-fedora14-xccdf.xml
- Title: Guide to the Secure Configuration of Fedora Linux
- Version: 0.6.3
- Resolved: yes
- Status current: draft
- Language: en
- Description: This guide has been created to assist IT professionals, in effectively securing systems with Fedora Linux.
- Warnings: None
- Notices: None
- References: 1) VIVM-1 [[link](#)]  
2) PDI GEN000100 [[link](#)]
- File references: scap-fedora14-oval.xml

At the bottom of the window, there are three buttons: "Import", "Export", and "Validate".

# Content Tailoring

The screenshot shows a software application window titled "Main". The interface includes a menu bar with the following items: Main, Profiles, Tailoring, Scan, Reports, Edit, and Settings. The "Profiles" menu is currently selected. The main content area displays a list of profiles under the heading "Profile title". The list contains two entries: "(Default document)" and "Profile: Fedora 14 desktop settings", which is highlighted with a blue selection bar. To the right of the list is a vertical stack of five buttons: Add, Extend, Copy, Delete, and Save. Below the list, there is a section titled "Details:" containing the following information:

**Details:**

- ID: F14-Desktop
- Title: Fedora 14 desktop settings
- Abstract: False
- Extend:
- Version:
- Description: This profile selects security controls that conform to default Fedora 14 configuration.

# Content Tailoring

The screenshot displays the 'Content Tailoring' application window. The interface is divided into several sections:

- Toolbar:** Contains icons for Main, Profiles, Tailoring (active), Scan, Reports, Edit, and Settings.
- Tree View:** A hierarchical list of configuration groups. The 'Group: Installing and Maintaining Software' is selected. A 'Selected' column on the right of the tree shows checkboxes for each group.
- Details Panel:** Located on the right, it provides information about the selected group, including its ID, title, type, and weight. It also includes sections for References, Fixes, and a Description.
- Values Table:** A table at the bottom right of the details panel listing specific configuration values.

Rule/Group Title	Selected
Group: Introduction	<input checked="" type="checkbox"/>
Group: System-wide Configuration	<input checked="" type="checkbox"/>
Group: Installing and Maintaining Software	<input checked="" type="checkbox"/>
Group: File Permissions and Masks	<input checked="" type="checkbox"/>
Group: Account and Access Control	<input checked="" type="checkbox"/>
Group: SELinux	<input type="checkbox"/>
Group: Network Configuration and Firewalls	<input checked="" type="checkbox"/>
Group: Kernel Parameters which Affect Networking	<input checked="" type="checkbox"/>
Group: Network Parameters for Hosts Only	<input checked="" type="checkbox"/>
Rule: Disable net.ipv4.conf.default.send_redirect	<input type="checkbox"/>
Rule: Disable net.ipv4.conf.all.send_redirects for	<input type="checkbox"/>
Rule: Disable net.ipv4.ip forward for Hosts Only	<input type="checkbox"/>
Group: Network Parameters for Hosts and Routers	<input checked="" type="checkbox"/>
Group: Wireless Networking	<input checked="" type="checkbox"/>
Group: IPv6	<input checked="" type="checkbox"/>
Group: TCP Wrapper	<input checked="" type="checkbox"/>
Group: Iptables and Ip6tables	<input checked="" type="checkbox"/>
Group: Secure Sockets Layer Support	<input checked="" type="checkbox"/>
Group: Uncommon Network Protocols	<input checked="" type="checkbox"/>
Group: Logging and Auditing	<input checked="" type="checkbox"/>
Group: Configure Syslog	<input checked="" type="checkbox"/>
Group: System Accounting with auditd	<input checked="" type="checkbox"/>
Group: Services	<input checked="" type="checkbox"/>

**Details** | Refines

**Info**

ID: group-2.1  
Title: Installing and Maintaining Software  
Type: Group  
Weight: 1.0

**References**

**Fixes**

**Description**

The following sections contain information on security-relevant choices during the initial operating system installation process and the setup of software updates.

**Values**

Value Name	Values
Choose minimum size of /tmp	2G
Choose minimum size of /var	5G
Select frequency of yum update	daily
Select frequency with which to run AIDE check	daily

# Content Tailoring

The screenshot shows a software interface for content tailoring. At the top, there is a navigation bar with icons for Main, Profiles, Tailoring, Scan, Reports, Edit, and Settings. The 'Scan' icon is currently selected. Below the navigation bar is a table with three columns: Role ID, Result, and Title. The table lists 15 rules, with their results highlighted in red for 'FAIL' and green for 'PASS'. A progress bar at the bottom indicates the scanning process is at rule rule-2.2.3.2.a ... (17/75). At the very bottom, there are four buttons: Scan (with a green checkmark), Stop (with a red X), Export results (with a document icon), and Help (with a question mark icon).

Role ID	Result	Title
rule-2.1.2.1.1.a	FAIL	Ensure Fedora GPG Key is Installed
rule-2.1.2.3.3.a	PASS	Ensure gpgcheck is Globally Activated
rule-2.1.2.3.4.a	FAIL	Ensure Package Signature Checking is Not Disabled For Any Repos
rule-2.1.2.3.6.a	PASS	Ensure Repodata Signature Checking is Not Disabled For Any Repos
rule-2.2.3.1.a	PASS	Verify user who owns 'shadow' file
rule-2.2.3.1.b	PASS	Verify group who owns 'shadow' file
rule-2.2.3.1.c	PASS	Verify user who owns 'group' file
rule-2.2.3.1.d	PASS	Verify group who owns 'group' file
rule-2.2.3.1.e	PASS	Verify user who owns 'gshadow' file
rule-2.2.3.1.f	PASS	Verify group who owns 'gshadow' file
rule-2.2.3.1.g	PASS	Verify user who owns 'passwd' file
rule-2.2.3.1.h	PASS	Verify group who owns 'passwd' file
rule-2.2.3.1.i	FAIL	Verify permissions on 'shadow' file
rule-2.2.3.1.j	PASS	Verify permissions on 'group' file
rule-2.2.3.1.k	FAIL	Verify permissions on 'gshadow' file
rule-2.2.3.1.l	PASS	Verify permissions on 'passwd' file

Scanning rule rule-2.2.3.2.a ... (17/75)

Scan Stop Export results Help