RHEL5 Baseline Settings

Steve Grubb
Principal Engineer
Red Hat

RHEL5 Baseline Settings Project

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

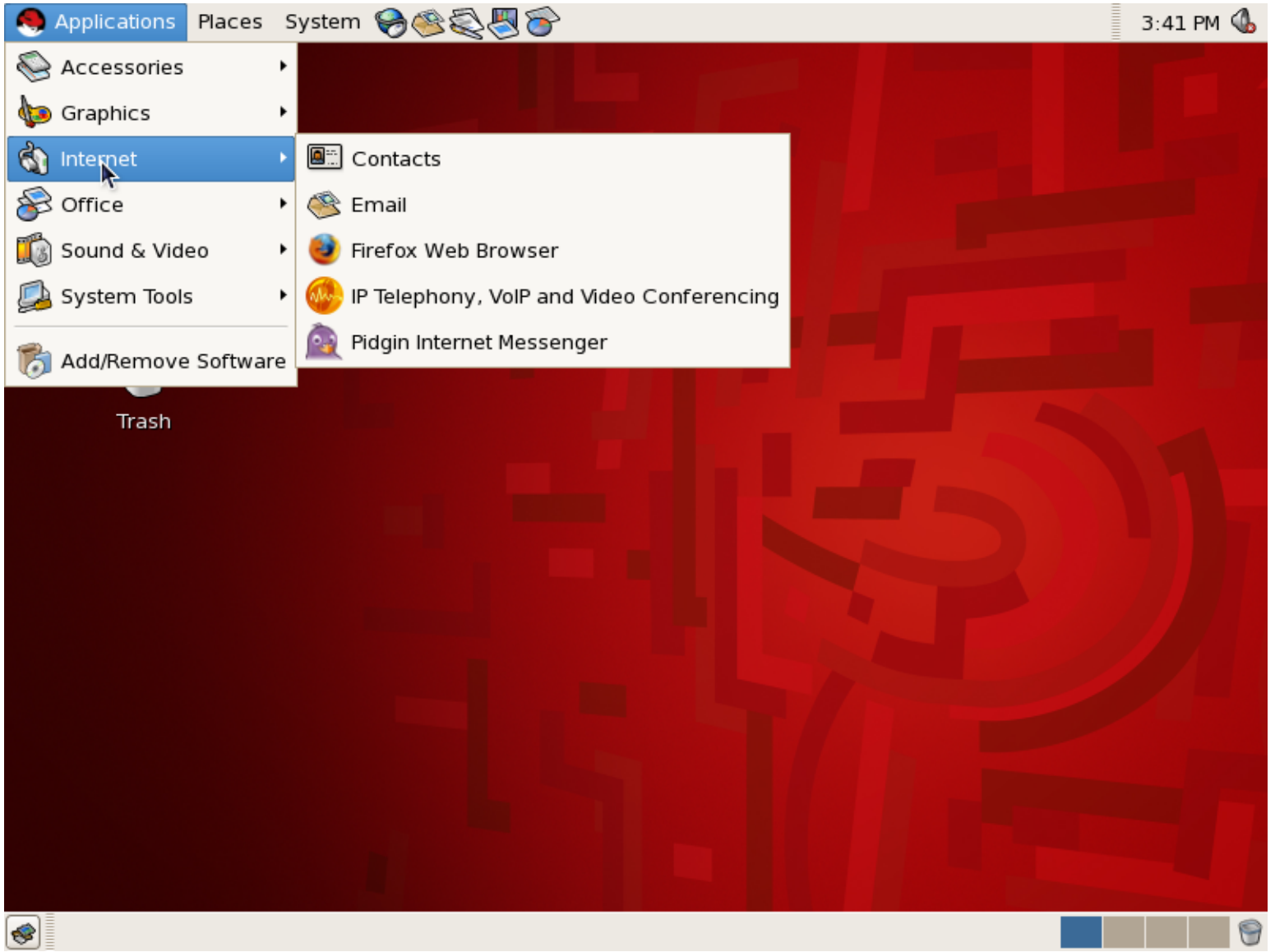
RHEL5 Workstation

- 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

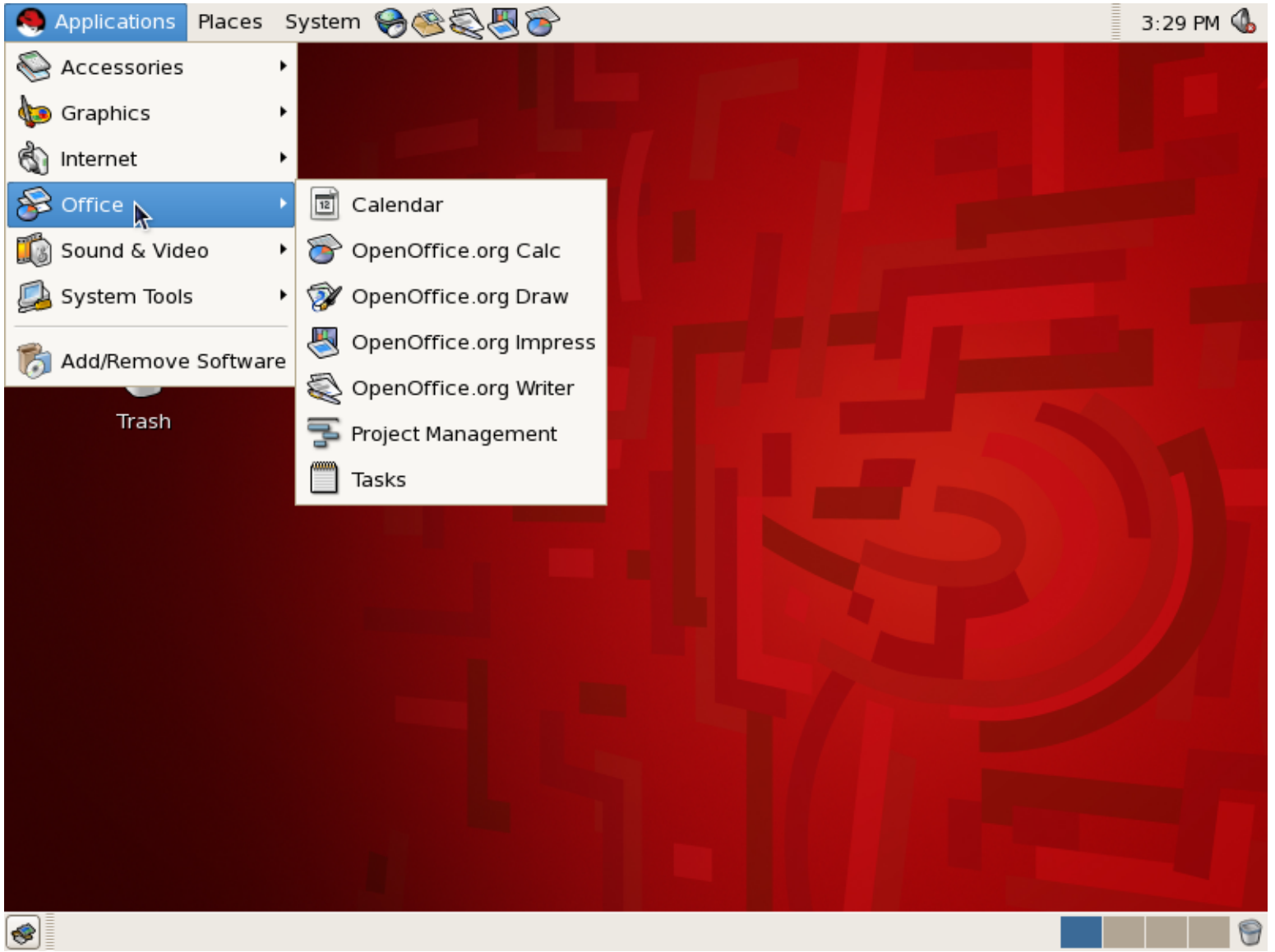
RHEL5 Workstation

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

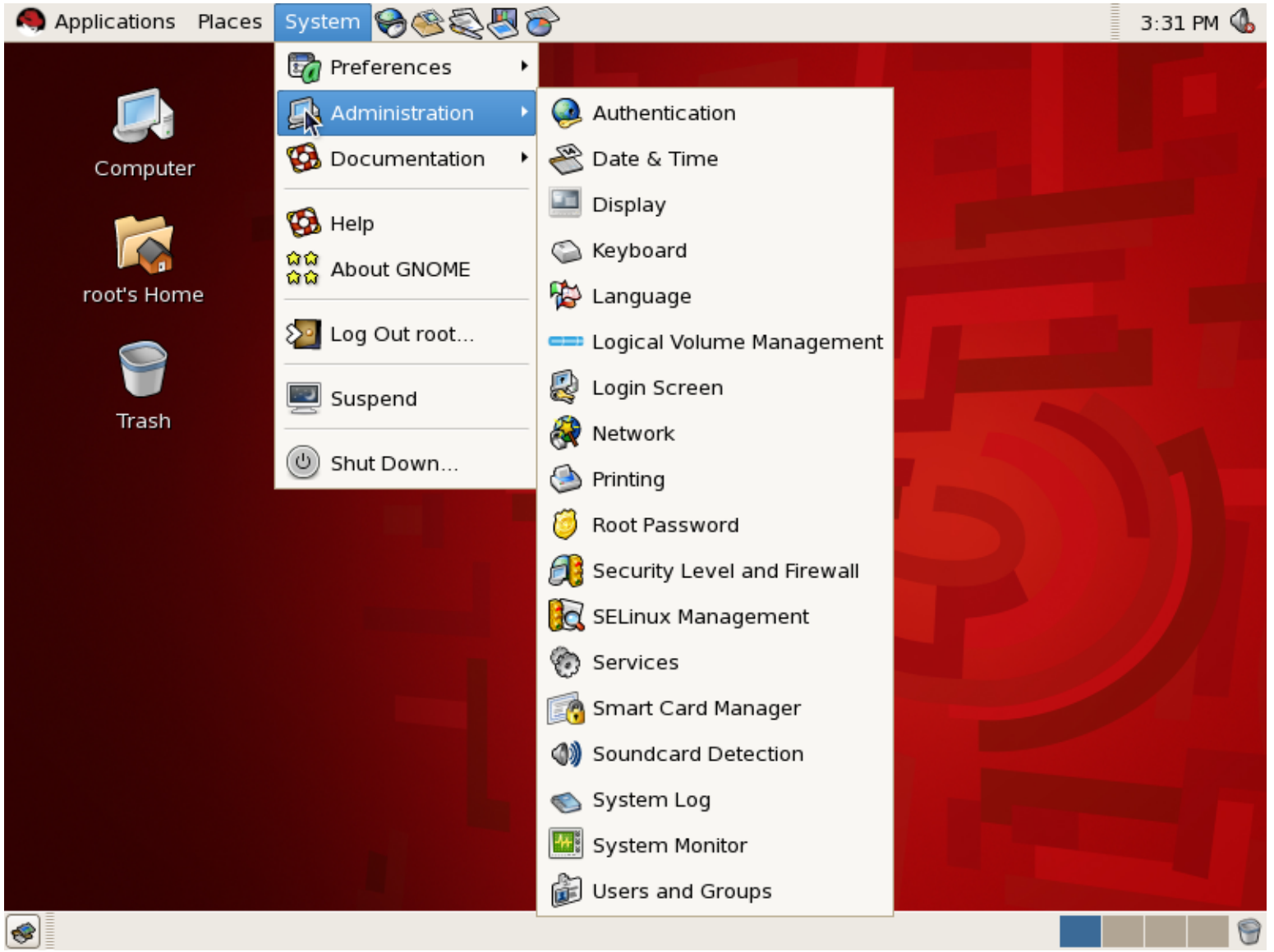
RHEL5 Workstation



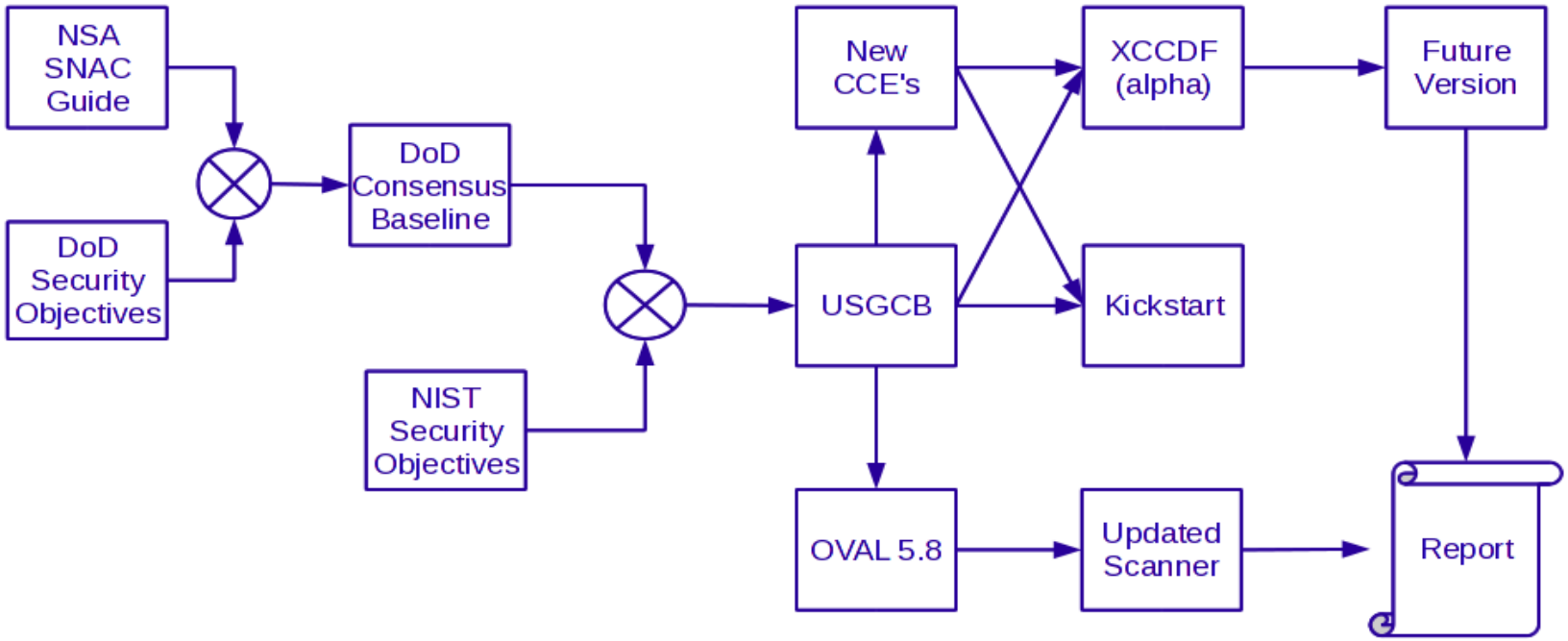
RHEL5 Workstation



RHEL5 Workstation



Project


NSA
SNAC
Guide
DoD
Security
Objectives
DoD
Consensus
Baseline
NIST
Security
Objectives
New
CCE's
USGCB
XCCDF
(alpha)
Kickstart
Future
Version
OVAL 5.8
Updated
Scanner
Report

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

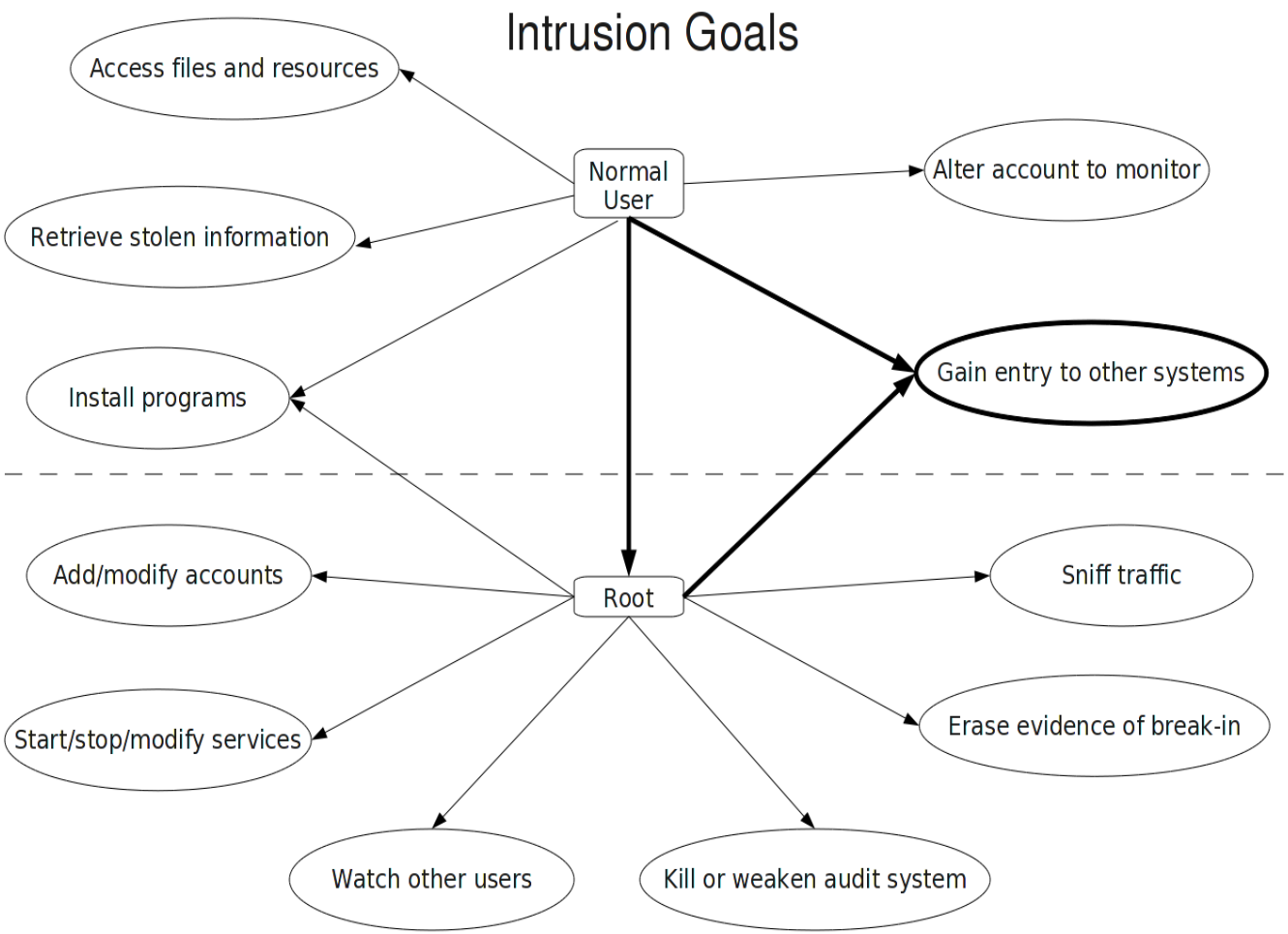
Project

- 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

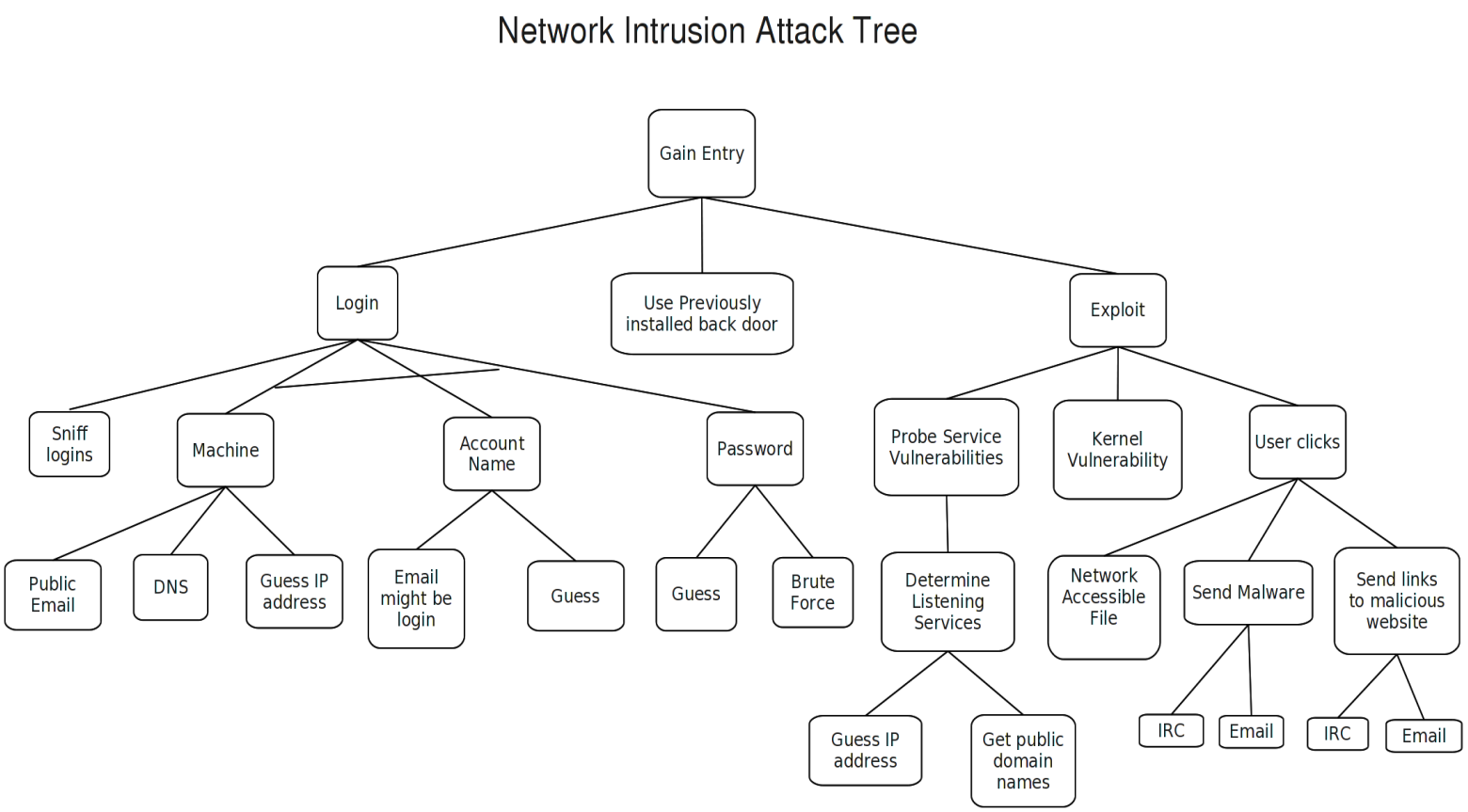
- Principles
  - Reduce attack points
  - Prefer like programs with best record
  - Prefer programs not being deprecated in RHEL 6
  - Workaround possible weaknesses by configuration options

Configuration Choices

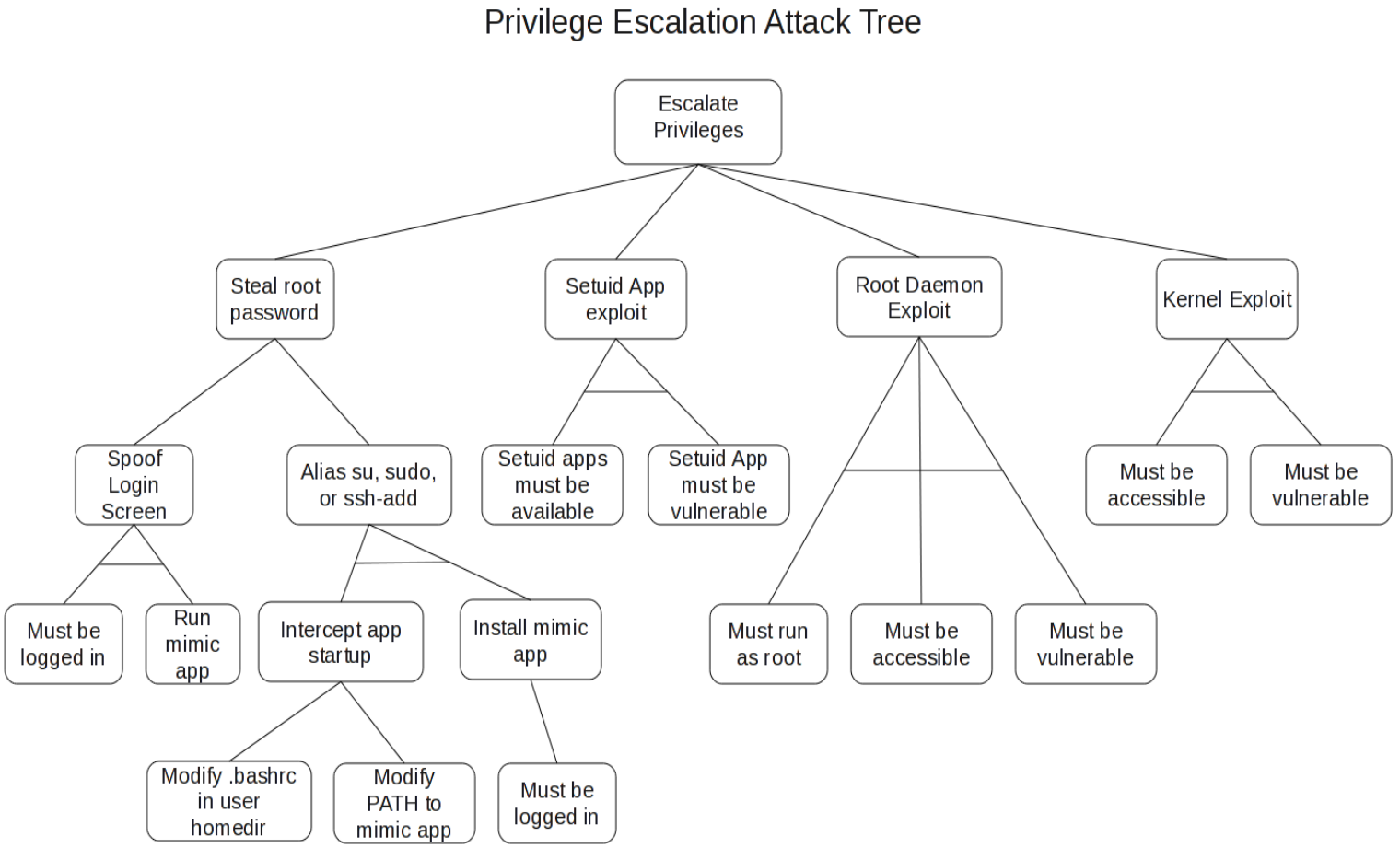


Steve Grubb, Red Hat

Configuration Choices



Configuration Choices



Steve Grubb, Red Hat

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 partioning
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 interuptable
- 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 sysklogd

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

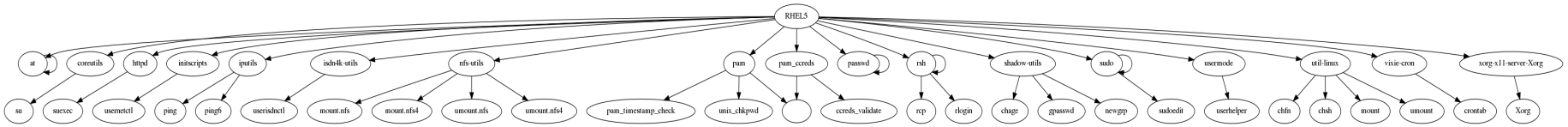
Changes

	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

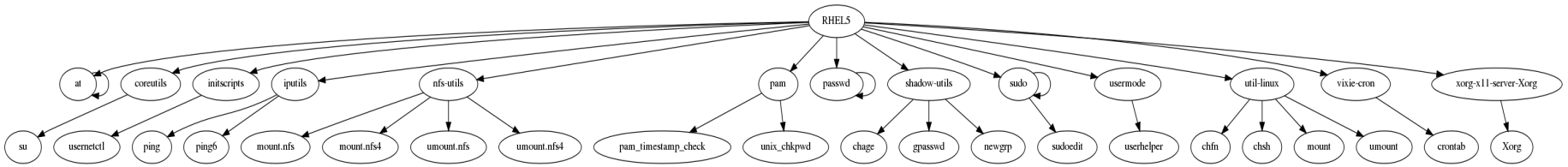
/etc/fstab

```
/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
```

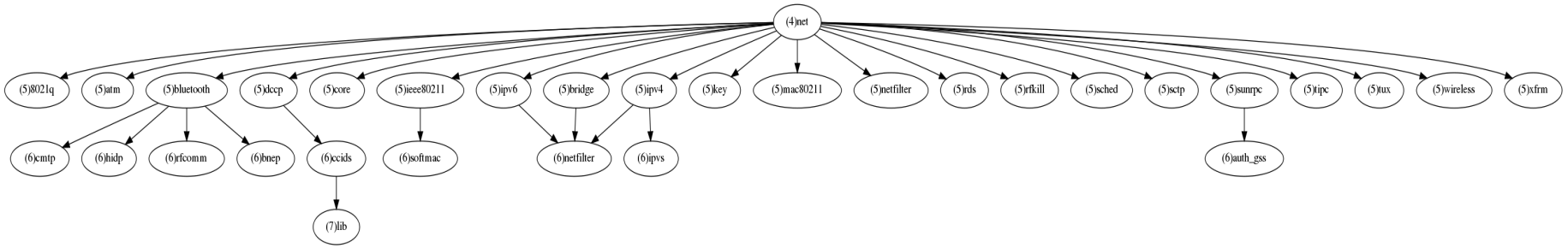
Setuid apps (before)



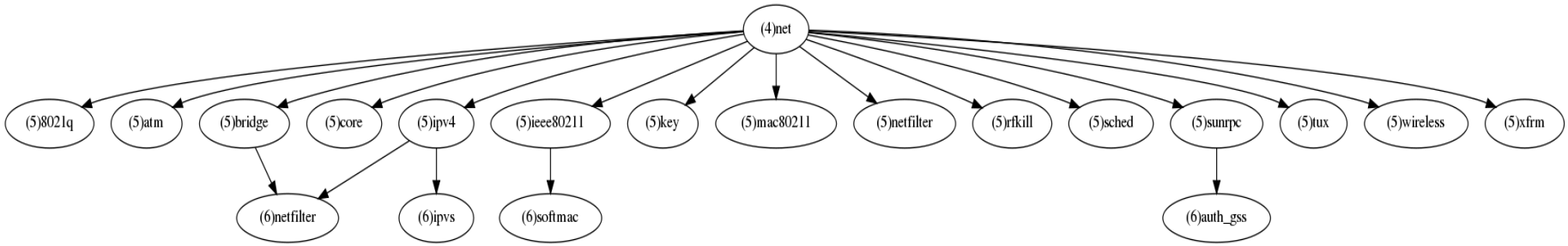
Setuid Apps (after)



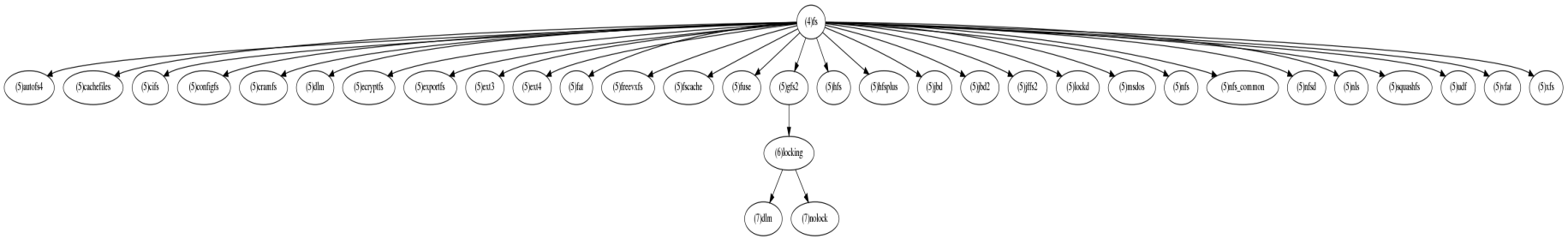
Network modules (before)



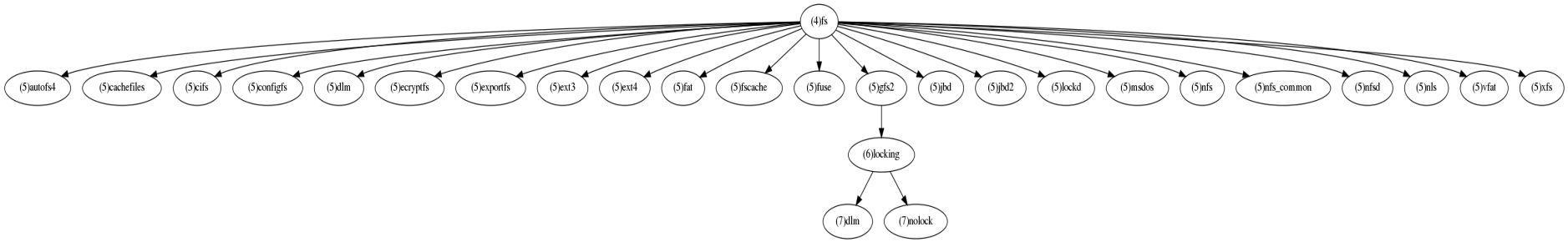
Network modules (after)



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

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

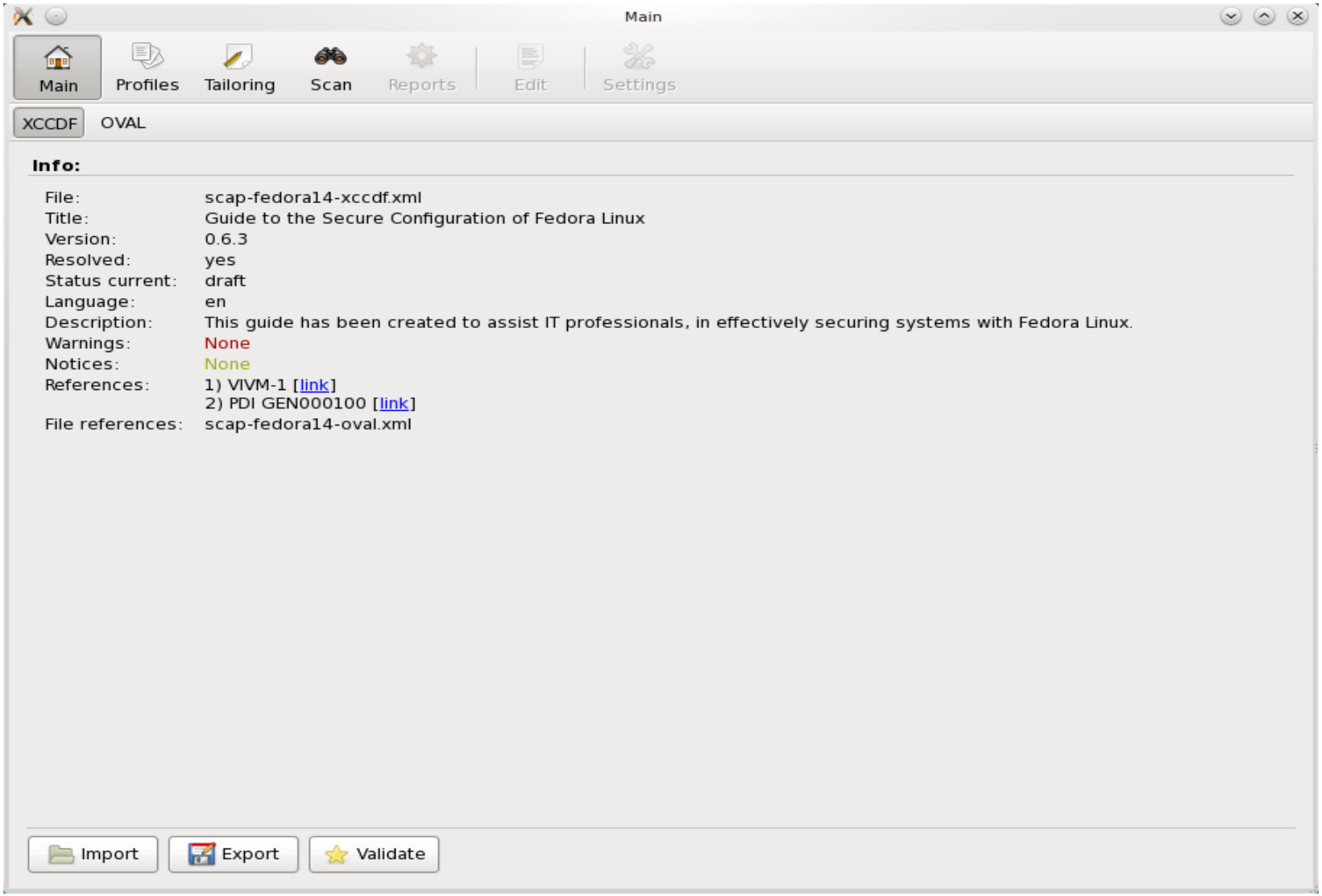
Related Projects

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

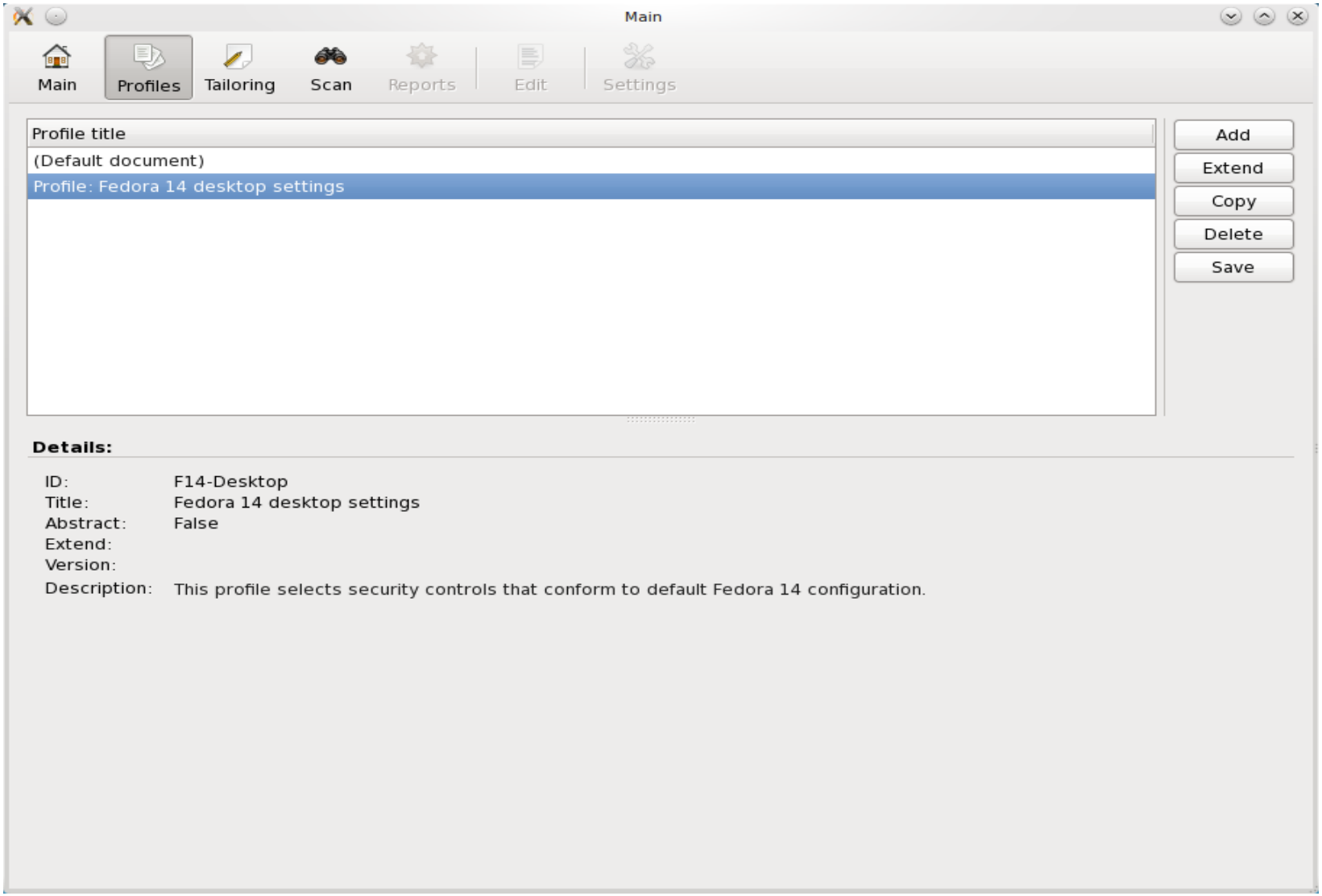
Future work

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

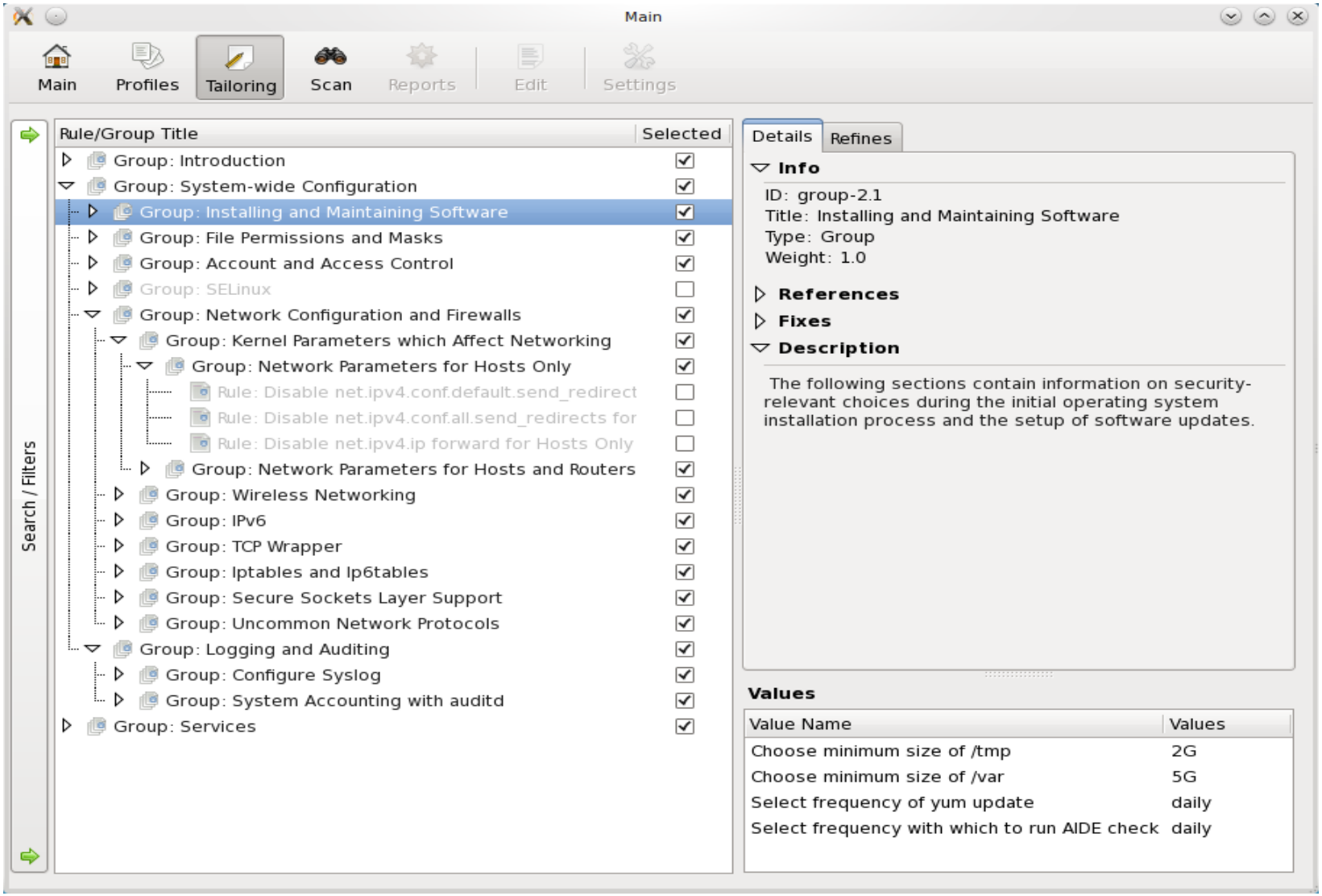
Content Tailoring



Content Tailoring



Content Tailoring



Content Tailoring