



# SCAP Security Guide (SSG) RHEL 6 Kickstart DVD

Frank Caviggia  
March 12, 2015

# Overview

Government Standards & Security

Hardening Scripts

- SCAP Security Guide

SSG Kickstart

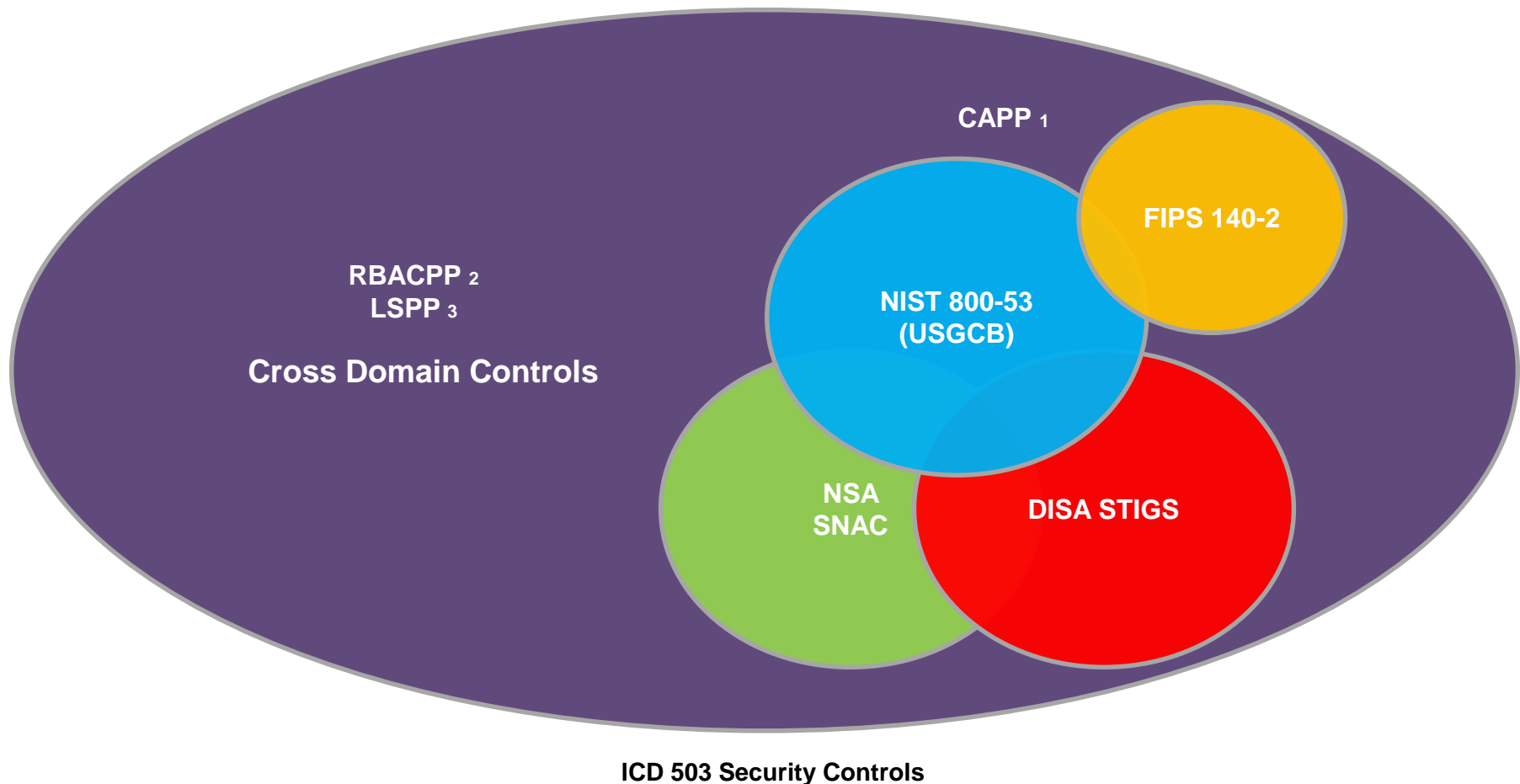
- Customize
- Re-master a RHEL 6 DVD

More Information

# Government Standards & Security

# Government Regulations

There are multiple government standards and regulations – some of which overlap:



- 1 [Controlled Access Protection Profile \(CAPP\)](#)
- 2 Role-Based Access Control Protection Profile (RBACPP)
- 3 [Labeled Security Protection Profile \(LSPP\)](#)

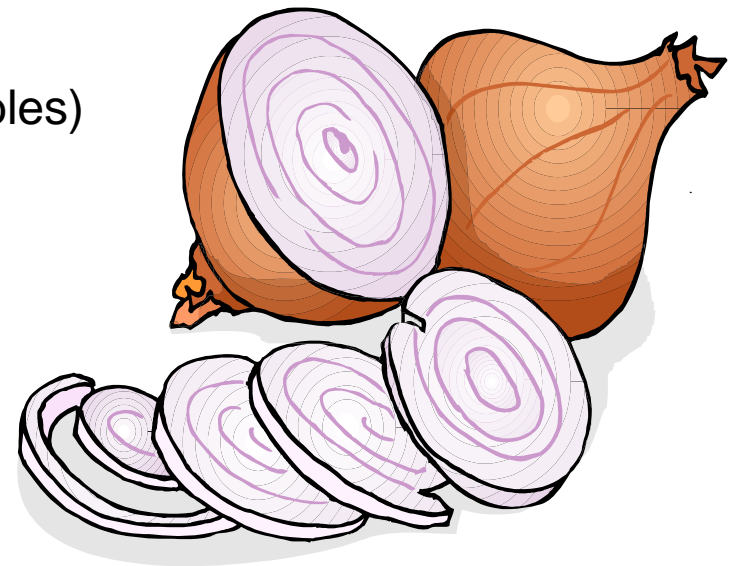
# What is System Security?

Security is like an onion – the more layers you peel the more you cry...

Goal: Create a secure virtualization environment using a standard set of packaged scripts, configurations, and policies to be deployed across systems.

Controls are implemented through the following mechanisms:

- Hardening Scripts, Kickstart Installation
- Discretionary Access Controls (DAC)
- SELinux Policies
  - Mandatory Access Controls (MAC)
- Network Controls (TCP\_WRAPPERS, iptables, ebtables)
- Process and Memory Controls (cgroups)
- Administrative Controls (physical, policies, etc.)
- Continuous Monitoring (SCAP, RHN Satellite)



# Hardening Scripts

## SCAP Security Guide (SSG)

# Security Configuration Automation Protocol (SCAP)

SCAP is implemented on Red Hat Enterprise Linux by OpenSCAP (oscap) and the SCAP Security Guide (SSG) developed with collaboration with the NSA, NIST, and DISA.

RHN Satellite can run SCAP Scans against a defined security baseline to check for configuration compliance on a schedule. This helps to maintain continuous monitoring:

```
# oscap xccdf eval --profile stig-rhel6-server-upstream --results results.xml --report  
report.html --cpe /usr/share/xml/scap/ssg/content/ssg-rhel6-cpe-dictionary.xml  
/usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml
```

OpenSCAP XCCDF System Compliance Check

```
# wget http://www.redhat.com/security/data/oval/com.redhat.rhsa-all.xml  
# wget http://www.redhat.com/security/data/metrics/com.redhat.rhsa-all.xccdf.xml  
# oscap xccdf eval --results results.xml --report report.html com.redhat.rhsa-all.xccdf.xml
```

OpenSCAP XCCDF Patch (CVE) Compliance Check

## SCAP Terms & Definitions

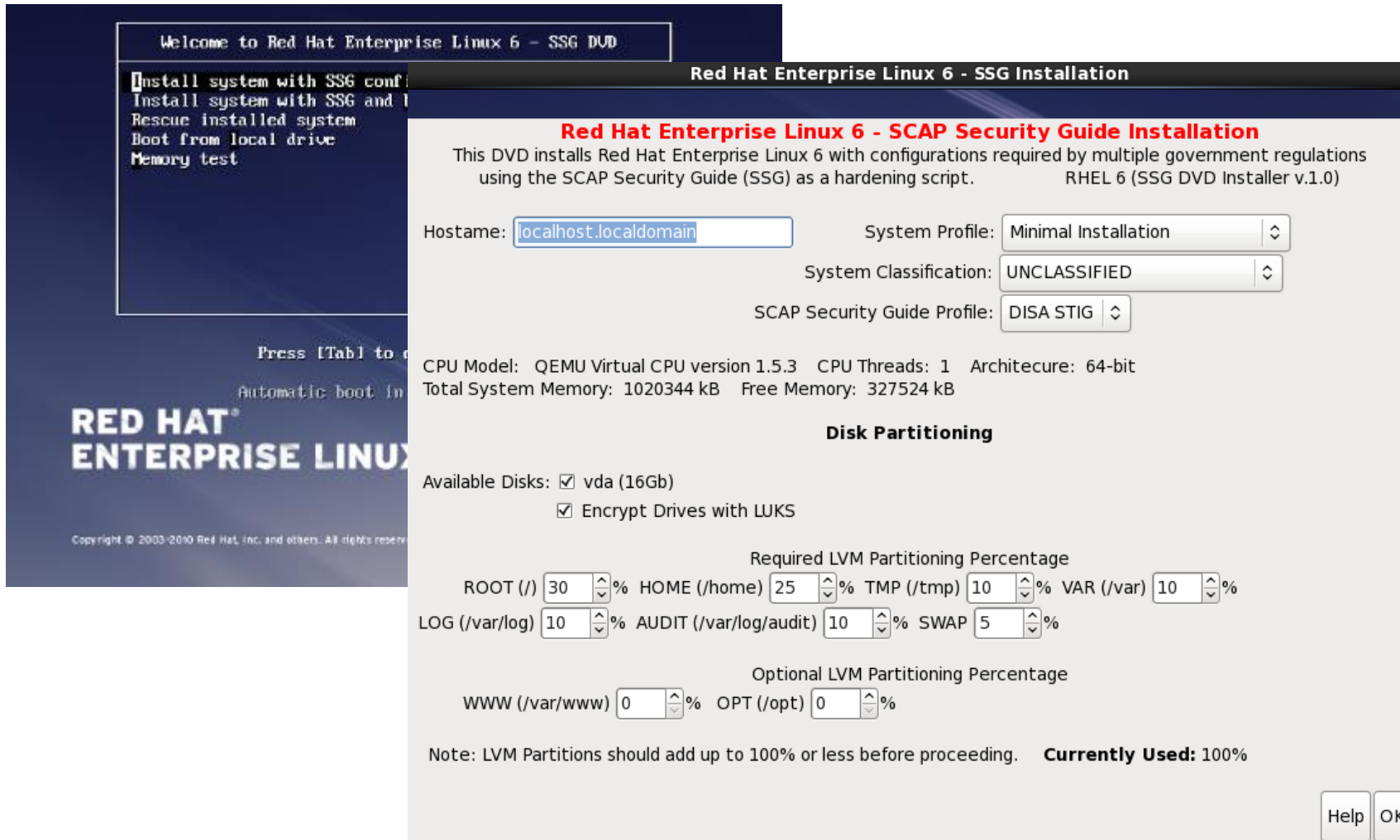
- XCCDF (eXtensible Configuration Checklist Description Format)
  - Creates checklist for security configuration on a target system
- OVAL (Open Vulnerability and Assessment Language)
  - Standardized security information content
- CPE (Common Platform Enumeration) Dictionary
  - Names and Metadata for security Evaluation
- CCE (Common Configuration Enumeration)
  - Identifies mappings between SCAP security checks and STIG/NIST 800-53 settings

# Secured Installation



# SSG RHEL 6 Kickstart DVD

The hardening script RPM was combined with a customized Kickstart to produce a standardized installation DVD to help meet security requirements right from installation.



The image shows two overlapping screenshots of the Red Hat Enterprise Linux 6 - SSG DVD installation interface. The background screenshot shows the initial boot menu with options like 'Install system with SSG conf', 'Install system with SSG and l', 'Rescue installed system', 'Boot from local drive', and 'Memory test'. The foreground screenshot shows the 'Red Hat Enterprise Linux 6 - SSG Installation' window. This window displays the title 'Red Hat Enterprise Linux 6 - SCAP Security Guide Installation' and a description: 'This DVD installs Red Hat Enterprise Linux 6 with configurations required by multiple government regulations using the SCAP Security Guide (SSG) as a hardening script. RHEL 6 (SSG DVD Installer v.1.0)'. It includes fields for 'Hostname: localhost.localdomain', 'System Profile: Minimal Installation', 'System Classification: UNCLASSIFIED', and 'SCAP Security Guide Profile: DISA STIG'. Below these, it shows system information: 'CPU Model: QEMU Virtual CPU version 1.5.3', 'CPU Threads: 1', 'Architecture: 64-bit', 'Total System Memory: 1020344 kB', and 'Free Memory: 327524 kB'. The 'Disk Partitioning' section shows 'Available Disks: [x] vda (16Gb)' and '[x] Encrypt Drives with LUKS'. It also displays 'Required LVM Partitioning Percentage' for various partitions: ROOT (/) 30%, HOME (/home) 25%, TMP (/tmp) 10%, VAR (/var) 10%, LOG (/var/log) 10%, AUDIT (/var/log/audit) 10%, and SWAP 5%. An 'Optional LVM Partitioning Percentage' section shows WWW (/var/www) 0% and OPT (/opt) 0%. A note at the bottom states: 'Note: LVM Partitions should add up to 100% or less before proceeding. Currently Used: 100%'. There are 'Help' and 'OK' buttons at the bottom right.

Screenshots of SSG RHEL6 Kickstart DVD

# Customize Kickstart DVD

Modify the kickstart with the following files:

- `config/hardening/ssg-rhel.cfg`

Kickstart Configuration (Calls `menu.py` in `%pre`). You can also add files to your installation and register with a customer's RHN Satellite by embedding the `RHN-ORG-TRUSTED-SSL-CERT`, modifying the `/etc/sysconfig/rhn/up2date` file and using ``rhnreg_ks --activationkey=<key>`` command in the `%post` section of the kickstart.

- `config/hardening/menu.py`

Python Script that presents a graphical menu to modify the kickstart. Contains the "Profiles" for configuring the system partitioning and packages.

**Profile Menu:** Starts around Line 138; **Profile Definitions:** Starts around Line 438

- `config/hardening/ssg-supplemental.sh`

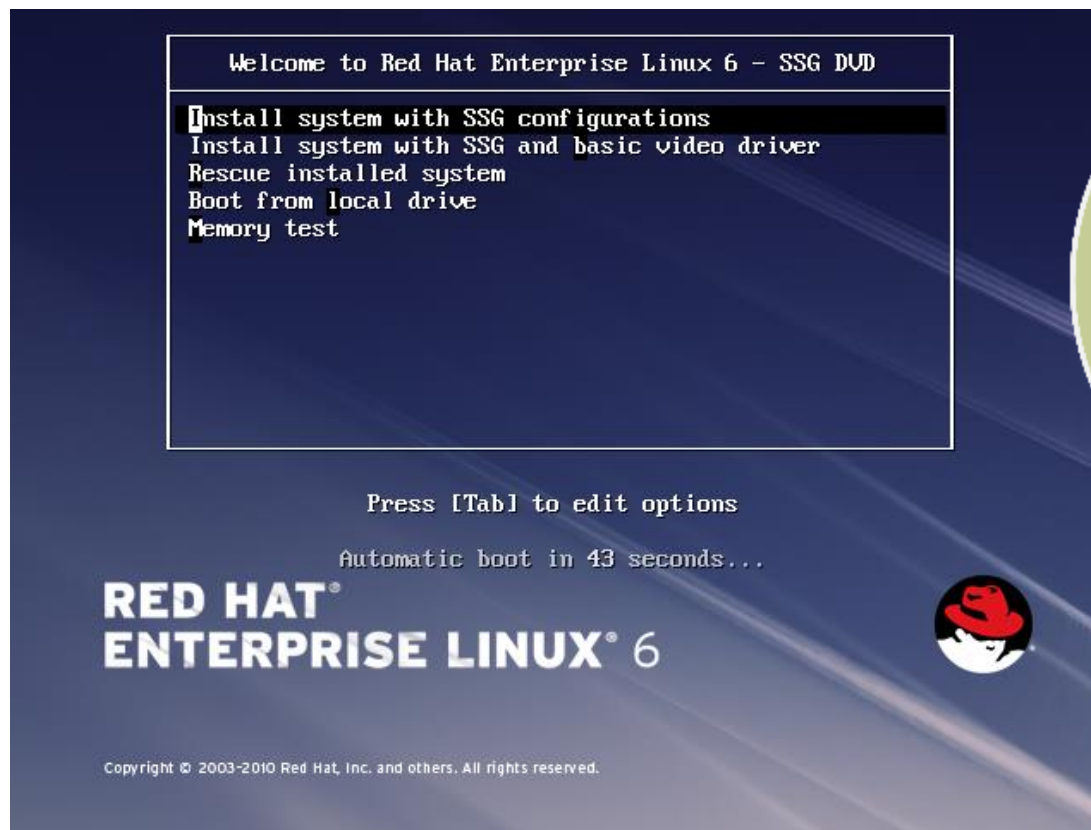
Add any additional hardening to the bash script, which is designed to allow for further customization of the SSG Hardening Scripts to tailor to specific site needs.

# Build Kickstart DVD

Re-master a RHEL 6.5/6.6 DVD

```
# ./createiso.sh rhel-server-6.5-x86_64-dvd.iso
```

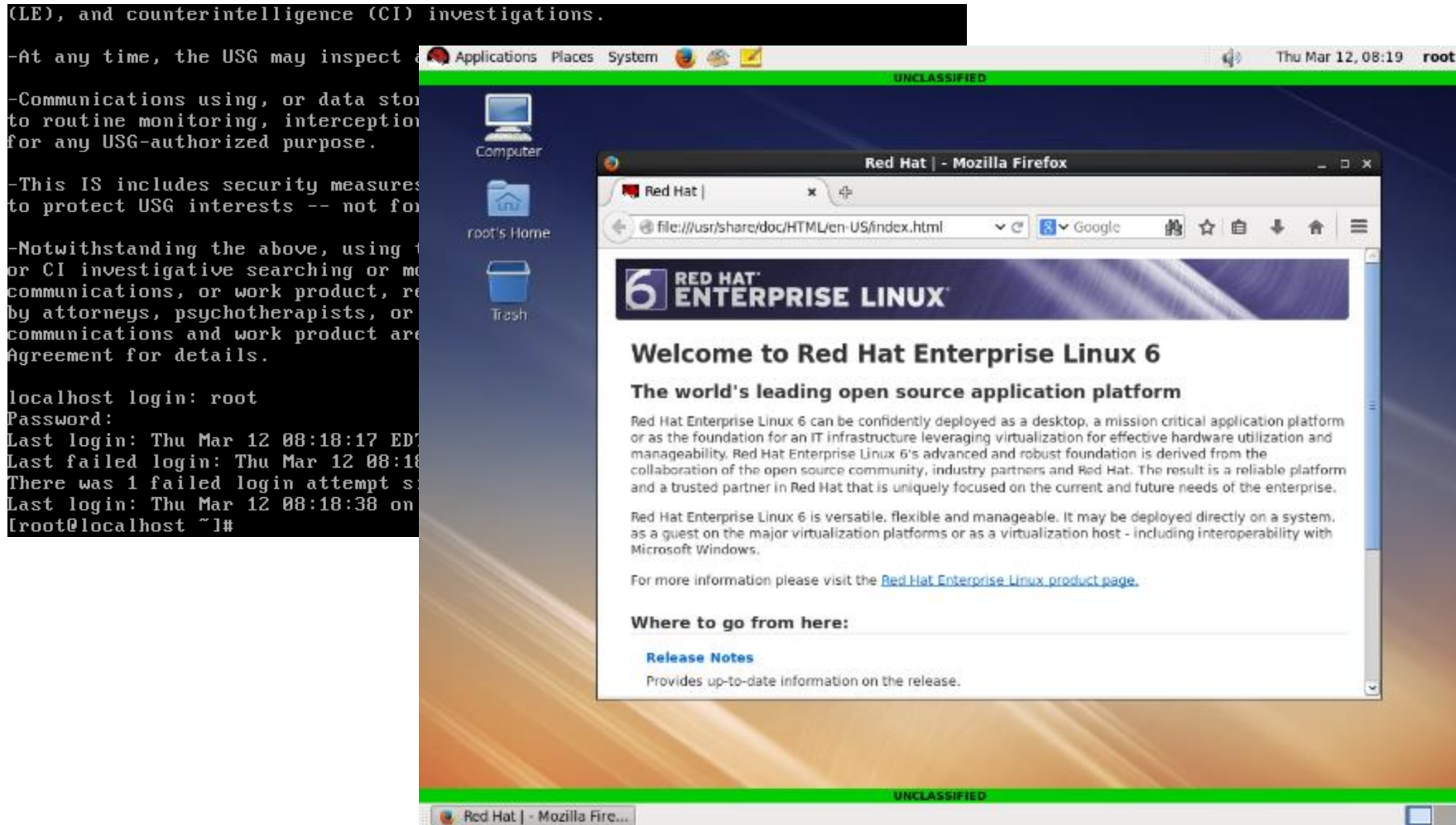
Re-master a RHEL 6.5/6.6 DVD



Grub Menu of SSG RHEL6 Kickstart DVD

# Test Installation DVD

Test your re-mastered RHEL DVD to verify configurations before deploying to your customer.



Screenshots of SSG RHEL6 Kickstart DVD

# Questions?

# More Information

DISA STIG Kickstart DVD:

<https://github.com/RedHatGov/ssg-el6-kickstart>

SCAP Security Guide:

<https://fedorahosted.org/scap-security-guide/>

Graphical Classification Banner:

<https://github.com/RedHatGov/classification-banner>