SCAP & Remediation: Lessons Learned and Path Ahead

SHAWN WELLS
DIRECTOR, INNOVATION PROGRAMS
unclass: shawn@redhat.com
(+1) 443-534-0130

RHEL5 STIG Delay: 1,988 days

RHEL5 STIG Delay:
1,988 days

RHEL6 STIG Delay:
932 days

SCAP Security Guide

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

In a Nutshell, SCAP Security Guide:

... has had 1,943 commits from 24 contributors, representing 164,355 lines of source

In a Nutshell, SCAP Security Guide:

... has had 1,943 commits from 24 contributors, representing 164,355 lines of source

... took an estimated 43 years of effort (COCOMO model)

In a Nutshell, SCAP Security Guide:

... has had 1,943 commits from 24 contributors,
representing 164,355 lines of source

... took an estimated 43 years of effort
(COCOMO model)

... has become upstream for DISA RHEL6 STIG,
NIST NVD for JBoss EAP,
NSA SNAC guide in progress

60 MINUTES, 3 GOALS

[1] Review SCAP remediation initiatives @ Red Hat

[2] Demonstrate current capabilities
(walk the code)

[3] Fedora 20 / RHEL7 Roadmap

Linking
XCCDF + OVAL + Remediation

Step 1 / 3: XCCDF Short Hand

```
<Rule id=“ ”  severity=“ ”>
    <title>  </title>
    <description>  </description>
    <ocil>  </ocil>
    <rationale>  </rationale>
    <ident cce=“ ” />
    <ref nist=“ ” disa=“ ” />
    <oval id=“ ” />
</Rule>
```

Step 1 / 3: XCCDF Short Hand

```
<Rule id=“ ”  severity=“ ”>
    <title>  </title>
    <description>  </description>
    <ocil>  </ocil>
    <rationale>  </rationale>
    <ident cce=“ ” />
    <ref nist=“ ” disa=“ ” />
    <oval id=“ ” />
</Rule>
```

Step 2 / 3: OVAL Linking

OVAL developed independently from XCCDF,
<oval id=“”> tag matches OVAL filename:

$ ls RHEL6/input/checks/ ; ls RHEL6/input/checks/ | echo "Total Checks: `wc -l`”

accounts_dangerous_path_for_root.xml
accounts_disable_post_pw_expiration.xml
accounts_max_concurrent_login_sessions.xml
accounts_maximum_age_login_defs.xml
accounts_minimum_age_login_defs.xml
accounts_no_uid_except_zero.xml
accounts_pam_no_nullok.xml
accounts_password_all_shadowed.xml
accounts_password_minclass_login_defs.xml
accounts_password_minlen_login_defs.xml
package_dovecot_removed.xml
package_hal_removed.xml
package_httpd_removed.xml
package_iptables_installed.xml
package_iptables-ipv6_installed.xml
package_iputils_removed.xml
package_irqbalance_installed.xml
package_kexec-tools_removed.xml
package_libcgroup_removed.xml
package_mdadm_removed.xml

Total Checks: 342

Step 3 / 3: Remediation Linking

- Bash first

```
<fix system="urn:xccdf:fix:script:sh">
    yum -y install screen
</fix>
```

Step 3 / 3: Remediation Linking

- Bash first

- Someday Puppet

```
<fix-group id="puppet-clip”
 system="urn:xccdf:fix:script:puppet”
 xmlns="http://checklists.nist.gov/xccdf/1.1">

    <fix rule="disable_vsftp">class vsftp</fix>
    <fix rule="package_aide_installed">class aide</fix>

</fix-group>
```

Step 3 / 3: Remediation Linking

- Bash first
- Someday Puppet
- URN’s via NIST IR 7275 Rev 4, Table 17

```
<Rule id="package_screen_installed" selected="false" severity="low”>
    <title xml:lang="en-US">Install the screen Package</title>

    <description xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US”>
        …..
    </description>

    <reference href="http://iase.disa.mil/cci/index.html">58</reference>
    <reference xmlns:dc="http://purl.org/dc/elements/1.1/" href="test_attestation”>
    </reference>

    <rationale xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US”>
        …..
    </rationale>

    <ident system="http://cce.mitre.org">CCE-26940-7</ident>

    <fix system="urn:xccdf:fix:script:sh">
        yum -y install screen
    </fix>

    <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
        <check-content-ref name="oval:ssg:def:897" href="ssg-rhel6-oval.xml"/>
    </check>

    <check system="ocil-transitional”>
        <check-export export-name="the package is not installed" value-id="conditional_clause"/>
        <check-content xmlns:xhtml="http://www.w3.org/1999/xhtml">
            …..
        </check-content>
    </check>
</Rule>
```

Inclusion of XCCDF Variables

- Approached authored by Jeff Blank (NSA)
- "Sourcing" XCCDF variable in bash script, build process converts to proper XCCDF

- Sample source:
  (input/fixes/bash/set_system_login_banner.sh)

```
source ./templates/support.sh
populate login_banner_text
cat <<EOF >/etc/issue
$login_banner_text
EOF
```

Inclusion of XCCDF Variables

- Final XCCDF:

```
 <Value id="login_banner_text" operator="equals" type="string”>
    <title xml:lang="en-US">Login Banner Verbiage</title>
    <description xmlns:xhtml=
    "http://www.w3.org/1999/xhtml" xml:lang="en-US">
        ……
    </description>

    <value selector="dod_short">
        I\'ve read \&amp; consent to terms in IS user agreem\'t.
    </value>
</Value>

……

<fix system="urn:xccdf:fix:script:sh">login_banner_text="<sub
idref="login_banner_text"/>”
cat &lt;&lt;EOF &gt;/etc/issue
$login_banner_text
EOF
</fix>
```

Inclusion of XCCDF Variables

- **Remediation Script:**

```
cat <<EOF >/etc/issue
I’ve read and consent to the
terms in IS user agreem’t
EOF
```

Approach Limitations

- fixType data type for <xccdf:fix> elements[1] not automated (or even included)
  - complexity
  - disruption,
  - reboot
  - ……
- “undo” specification?

[1] http://scap.nist.gov/specifications/xccdf/xccdf_element_dictionary.html#fixType

Online & Offline Remediation

(reference Šimon Lukašík's blog for a great write-up:
http://isimluk.livejournal.com/3573.html)

Online Remediation

```
$ oscap xccdf eval --remediate \
  --results ~/my-results-xccdf.xml \
  ~/my-policy-xccdf.xml
```

1. OpenSCAP will perform “first pass” evaluation
2. Upon failure, executes <fix> content
3. Returns “fixed” or “error” <result>
4. Command output logged

Offline Remediation

```
$ oscap xccdf generate fix \
  --result-id xccdf_org.open-
  scap_testresult_stig-rhel6-server \
  /var/www/html/results/results.xml \
  > /tmp/remediation-script.sh
```

<result>error</result>

```
<rule-result idref="xccdf_moc.elpmaxe.www_rule_1”
   time="2013-03-22T19:15:11" weight="1.000000">

        <result>error</result>

        <message severity="info">
            Fix execution comleted and returned: 1
        </message>

        <message severity="info">
            Loaded plugins: auto-update-debuginfo, langpacks, presto,
            refresh-packagekit

            You need to be root to perform this command.
        </message>

   . . . . .

</rule-result>
```

<result>fixed</result>

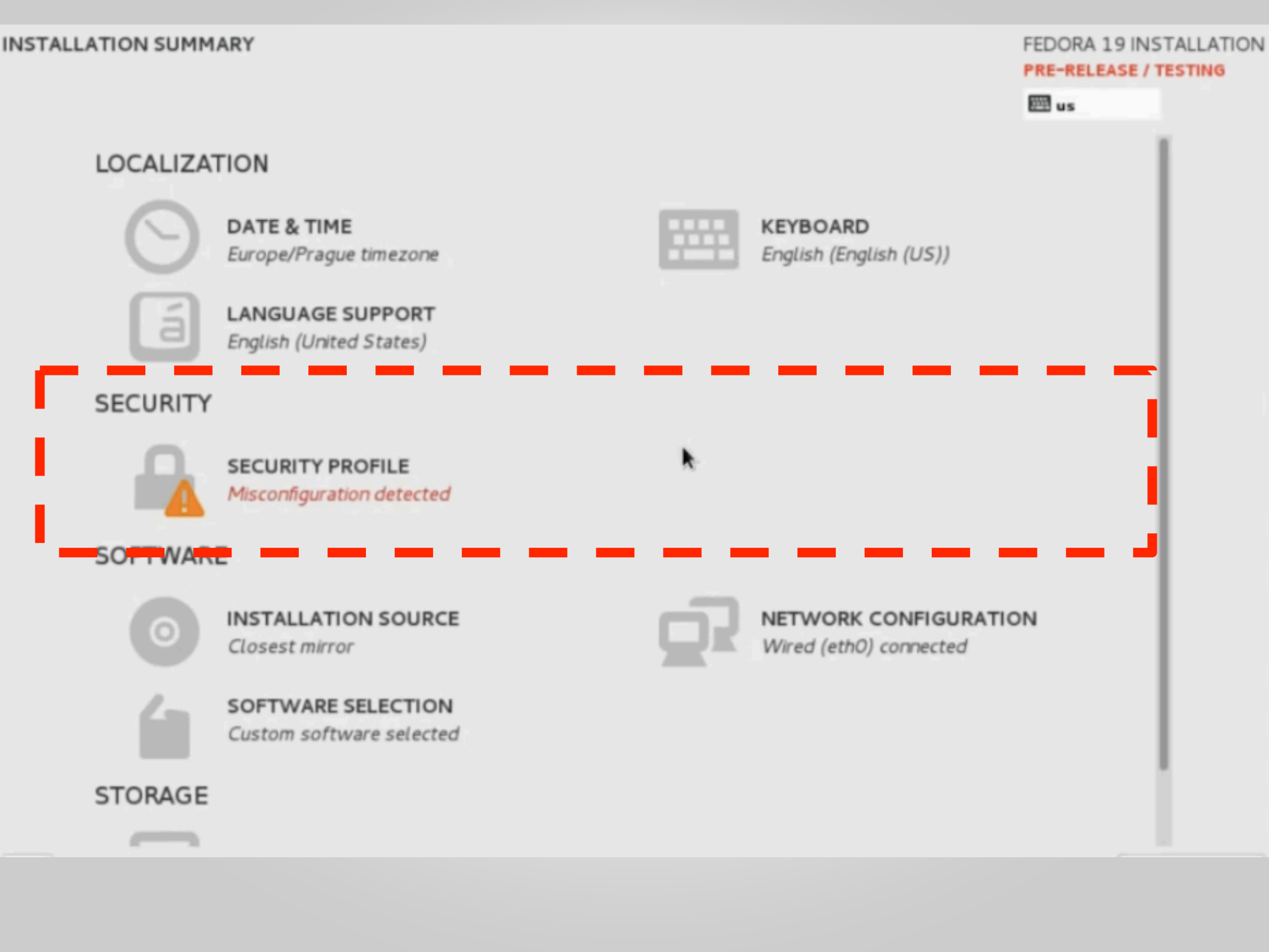
```
<rule-result idref="xccdf_moc.elpmaxe.www_rule_1"
    time="2013-03-22T19:16:03" weight="1.000000">
     <result>fixed</result>
     <message severity="info">Fix execution comleted and returned: 0</message>
     <message severity="info">
          ....
          Remove 1 Package
          Installed size: 53 k
          Downloading Packages:
          Running Transaction Check
          Running Transaction Test
          Transaction Test Succeeded
          Running Transaction
               Erasing      :    1:telnet-server-0.17-51.fc16.x86_64    1/1
               Verifying    :    1:telnet-server-0.17-51.fc16.x86_64    1/1

          Removed:
               telnet-server.x86_64 1:0.17-51.fc16
    </message>
```

Fedora 20 / RHEL7 Roadmap

(Vimeo demo by Vratislav Podzimek
@ http://vimeo.com/66085973)

Remediation During Provisioning

```
 1 this is a simple kickstart file for testing OSCAP addon's features
 2
 3 # values saving a lot of clicks in the GUI
 4 lang en US.UTF-8
 5 keyboard --xlayour=us --vckeymap=us
 6 timezone Europe/Prague
 7 rootpw aaaaa
 8 bootloader --location=mbr
 9 clearpart --initlabel --all
10 autopart --type=plain
11
12 %packages
13 vim
14 %end
15
16 %addon org_fedora_oscap
17         content-type = archive
18         content-url = http://192.168.122.1/xccdf_content.zip
19         profile = xccdf_com.stig-rhel6-server
20         xccdf-path = xccdf.xml
21 %end
```


INSTALLATION SUMMARY
FEDORA 19 INSTALLATION
PRE-RELEASE / TESTING
us
LOCALIZATION
DATE & TIME
Europe/Prague timezone
KEYBOARD
English (English (US))
LANGUAGE SUPPORT
English (United States)
SECURITY
SECURITY PROFILE
Misconfiguration detected
SOFTWARE
INSTALLATION SOURCE
Closest mirror
NETWORK CONFIGURATION
Wired (eth0) connected
SOFTWARE SELECTION
Custom software selected
STORAGE

Data stream: scap_org.open-scap_datastream_tst

Checklist: scap_org.open-scap_cref_first-xccdf.xml

Choose profile below:

My testing profile
A profile for testing purposes.

My testing profile2
Another profile for testing purposes.

Select profile

Changes that were done or need to be done:

- /tmp must be on a separate partition or logical volume
- root password was too short, a longer one with at least 10 characters will be required
- package 'iptables' has been added to the list of to be installed packages
- package 'telnet' has been added to the list of excluded packages

THANK YOU!