How will we obsolete sectool?

(Script Check Engine for XCCDF)

Martin Preisler, Peter Vrabec
What is sectool?
Security Tool

Overview

Test Results

Test | Result
-----|------
shadow | PASSED
home_dirs | WARNING
home_files | ERROR
filesystem | WARNING
path | PASSED
firewall | PASSED
netserv | PASSED
openssh | PASSED
openvpn | PASSED
removedlibs | testing...

Summary

Messages: 7
Errors: 0
Warnings: 1
Hints: 1
Info messages: 5

Time the test was running: 0m 0s

Mal | Severity | Test | Description
-----|---------|------|------------------
Warning | home_dirs | Directory /home/mbarabas doesn't have matching user in /etc/passwd

Please wait, executing test 'removedlibs'
Why NOT sectool?

- Time
- Technology
- Idea
SCAP

Checklist -> XCCDF
SCAP

- Checklist
- Checking Engine
- XCCDF
- OVAL, OCIL
SCAP

● Pros
  ○ interoperability
  ○ avoids vendor lock-in
  ○ security

● Cons
  ○ authoring
  ○ maintainance
  ○ lack of experts
  ○ linux unfriendly
SCAP

● Pros
  ○ interoperability
  ○ avoids vendor lock-in
  ○ security

● Cons
  ○ authoring
  ○ maintenance
  ○ lack of experts
  ○ Linux unfriendly
SCAP

● Pros
  ○ interoperability
  ○ avoids vendor lock-in
  ○ security

● Cons
  ○ authoring
  ○ maintainance
  ○ lack of experts
  ○ linux unfriendly
SCAP

● Pros
  ○ interoperability
  ○ avoids vendor lock-in
  ○ security

● Cons
  ○ authoring
  ○ maintainance
  ○ lack of experts
  ○ linux unfriendly
SCAP

● Pros
  ○ interoperability
  ○ avoids vendor lock-in
  ○ security

● Cons
  ○ authoring
  ○ maintainance
  ○ lack of experts
  ○ linux unfriendly
Pros
  - interoperability
  - avoids vendor lock-in
  - security

Cons
  - authoring
  - maintainance
  - lack of experts
  - linux unfriendly
SCAP

- **Pros**
  - interoperability
  - avoids vendor lock-in
  - security

- **Cons**
  - authoring
  - maintainance
  - lack of experts
  - linux unfriendly
Script Check Engine

Checklist

Checking Engine

XCCDF

SCE
SCE - Overview

- works with everything executable
- exit code -> XCCDF result
- reasons via stdout/stderr
- XCCDF variables via environment variables
SCE - Overview

- works with everything executable
- exit code -> XCCDF result
- reasons via stdout/stderr
- XCCDF variables via environment variables
SCE - Overview

- works with everything executable
- exit code -> XCCDF result
- reasons via stdout/stderr
- XCCDF variables via environment variables
SCE - Overview

- works with everything executable
- exit code -> XCCDF result
- reasons via stdout/stderr
- XCCDF variables via environment variables
Evaluate and export both XCCDF results and SCE results:

```
$ oscap xccdf eval --results res.xml --sce-results /usr/share/openscap/sectool-sce/sectool-xccdf.xml
```

Generate XHTML report from previously exported data

```
$ oscap xccdf generate report --sce-template %.result.xml res.xml
```
scap-workbench demo

$ scap-workbench
SCE

- **pros**
  - content
  - flexibility
  - reuse skills
  - provides policy

- **cons**
  - security
  - interoperability
  - comparison against previous results
  - visualization
SCE

• pros
  ○ content
  ○ flexibility
  ○ reuse skills
  ○ provides policy

• cons
  ○ security
  ○ interoperability
  ○ comparison against previous results
  ○ visualization
SCE

- **pros**
  - content
  - flexibility
  - reuse skills
  - provides policy

- **cons**
  - security
  - interoperability
  - comparison against previous results
  - visualization
SCE

● pros
  ○ content
  ○ flexibility
  ○ reuse skills
  ○ provides policy

● cons
  ○ security
  ○ interoperability
  ○ comparison against previous results
  ○ visualization
SCE

• pros
  ○ content
  ○ flexibility
  ○ reuse skills
  ○ provides policy

• cons
  ○ security
  ○ interoperability
  ○ comparison against previous results
  ○ visualization
SCE

● pros
  ○ content
  ○ flexibility
  ○ reuse skills
  ○ provides policy

● cons
  ○ security
  ○ interoperability
  ○ comparison against previous results
  ○ visualization
SCE

• pros
  ○ content
  ○ flexibility
  ○ reuse skills
  ○ provides policy

• cons
  ○ security
  ○ interoperability
  ○ comparison against previous results
  ○ visualization
SCE

**pros**
- content
- flexibility
- reuse skills
- provides policy

**cons**
- security
- interoperability
- comparison against previous results
- visualization
SCE - Future

- restrict scripts
- structured stdout
- use in QA?
SCE - Future

- restrict scripts
- structured stdout
- use in QA?
SCE - Future

- restrict scripts
- structured stdout
- use in QA?
Summary

- end of the line - sectool
- OpenSCAP improvements
- call for Security Checklists
Summary

- end of the line - sectool
- OpenSCAP improvements
- call for Security Checklists
Summary

- end of the line - sectool
- OpenSCAP improvements
- call for Security Checklists
Questions?
URL

- http://www.open-scap.org/page/SCE
- https://fedorahosted.org/scap-workbench/
- http://scap.nist.gov/