Thorough, Safe and Secure

and the OSSTMM

Joerg Simon
jsimon@fedoraproject.org
http://fedoraproject.org
Communication Security

[ Eco Systems ]
Two Security Lab Prototypes!

Fedora Security (Lab) Spin
Fedora (TM) - License Agreement

OSSTMM Lab

**All rights reserved. “Red Hat” and “Fedora” are trademarks of Red Hat, Inc. “Linux” is a registered trademark of Linus Torvalds. All other trademarks are the property of their respective owners.**
The Fedora® Project and the ISECOM – both are independent non profit entities

Both are part of the FOSS ECO System!

Share relationships

/me

This presentation incl. Fedora Artwork & all Backgrounds licensed cc-by-sa by the Fedora Project
ISECOM and OSSTMM logos and schematics licensed by Open Methodology Licence and/or cc-by-nd
[ History: started @ foss.in Bangalore 2009 ]

- pick up the Idea - give it a home - http://fedorahosted.org/security-spin/
- Contributor Wishlist - https://bugzilla.redhat.com/show_bug.cgi?id=563471
- Improve spin section content - went to spins.fedoraproject.org/security
- move to SLiM as desktop manager - moved to SLiM -> moved to LXDM ...
- move to LXDE as window manager - we moved to LXDE -> move to XFCE ?
- become an official spin in Fedora 13 - we made it as a official Fedora Security Spin in Fedora 13, 14, 15, 16, 17 and will be for 18
- LIMITS - Webapplication testing tools + implementing OSSTMM upstreams - we packaged SCARE, unicornscan also brought up limits of a large FOSS Project
- become the official OSSTMM Distro - ISECOM´s Pete Herzog announced OSSTMM Lab as the “New live linux distro for OSSTMM users” - on 12.September 2012
- new features in the current Version of the OSL (v3.8b4 (F17)) with input from the ISECOM HHS Team!
- collect input and suggestions from you for the next version - contribute!
- XFCE, OSSTMM 4 Point Menu Workflow, HHS Content?
[ legacy Security ]

- physical – technical
  - Firewall
  - IDS, HIDS
  - Antivirus
  - Security GW
  - Screening Router
  - Spamfilter
  - Multi-level Authentication
  - VPN

Pete Herzog ISECOM
Build
"Secure"
Patch
Update
Patch
Patch Again
Update
Clean
Fix
re-Build
[ one truth? ]
WARNING
slippery surfaces
when icy conditions
[ Compliance? ]

- Comply!?  
  But not secure?  
  Blocked?

- Get the Audit Result you need?  
  But not secure?  
  Blocked?

- Secure?  
  But not compliant?  
  Blocked?

Quelle: OSSTMM ISECOM
Security Today?
Cloud – Social Media – Mobile Plattform?

Oh, using these TM does not comply – i can not show you

Oh, using these Prototypes does not comply – i can not show you
[ how to find out how much security do you really need? ]
Fedora Security Lab

A open source test- and education platform for

- security-auditing
- forensics
- penetration-testing
features

- a safe livecd-place for testing
- all fedora security features
- ability to install on HD and USB
- install software anytime
- clean, functional, fast
developed by testers for testers

- collaborative developed

- community <> commercial benefits

- along our core values
possible benefits

- usecase for the FSL
- new cool upstreams
- implemented methodology
- fedora get taught along the OSSTMM
OSSTMM- Lab
Modified Version of the Fedora Security Lab

Packaging upstream Tools from the OSSTMM Team

A stable platform for teaching the curriculum For OSSTMM and HHS

Integrate the Methodology Flow Into one possible Toolset
Hacker Highschool

SECURITY AWARENESS FOR TEENS

LESSON 1

BEING A HACKER
Welcome to Fedora-Security-Spin!

Boot
Verify and Boot
Memory Test
Boot from local drive

Press [Tab] to edit options
Welcome to OSSTMM-Labv3.1b!

Boot
- Boot (Basic Video)
- Verify and Boot
- Memory Test
- Boot from local drive

Press [Tab] to edit options
[ test-tool all-stars ]
SELinux has detected suspicious behavior.

SELinux is preventing /usr/bin/kismet_client "write" access.

Today on Fri Nov 13, 2009 at 10:36:23 PM EST

SELinux denied access requested by kismet_client. It is not expected for kismet_client and this access may signal an intrusion attempt. A different version or configuration of the application is causing it to request this access.

[security features]
[ little treasures ]
- your tools
- your responsibility
- the ramification
- a way for proper testing!
[reproducible]
with the right Standards & Methods!

[comparable]
real working Metrics
– based on scientific research

[neutral unbiased]
by relying on Open Standards & Open Source

[usefull Reports]
Management & Real world compatible
There is an Open Source way

- How do current operations work?
- How do they work differently from how management thinks they work?
- How do they need to work?
!= Checklist, solution based, best-practise

- Measurable and comparable results
- Looks into operational Security and Trusts
- well developed Metric based on academic research
- „Thinking Out of the Box“
- ISECOM FOSS-Community - since January 2001 NPO
Usual testing synonyms

- Blind/Blackbox Pentest
- Graybox/Chrystal/RedTeam
- Social Engineering
- WarDriving
- WarDialing
- Configuration-Reviews
- Code Reviews
[four points]

1. **INDUCTION**
   establish facts about the environment

2. **INQUEST**
   investigate emanations

3. **INTERACTION**
   trigger responses

4. **INTERVENTION**
   changing resource interactions

Target → Tester → Environment
„Trusting everyone is insecure but not trusting anyone is inefficient“
broken trust has consequences

<table>
<thead>
<tr>
<th>Fedora-Wiki</th>
<th>Fedora-Email</th>
<th>Fedora Infrastructure</th>
<th>Fedora-Voice</th>
<th>Fedora-Planet</th>
<th>Fedora-IRC</th>
<th>Fedora-Hosted</th>
<th>Fedora-People</th>
<th>Fedora-Gobby</th>
<th>Fedora-Koji&amp;Bodhi</th>
<th>Fedora-Bugzilla</th>
<th>Fedora-Calendar?</th>
</tr>
</thead>
</table>

Fedora Account System FAS2
Fedora Trusts you!

- Fedora „Code“ is used by 30 Mio. Users!
- Contributor from
  - More than 400 commit Groups
  - ~25000 Contributors
„There are only 2 ways to steal something: either you take it yourself or you have someone else take it and give it to you“
Trust Properties!

- Trust is
  - no Emotion!
  - a Decision!
  - not quantifiable between humans!

- Wrong Trust Properties

- no Control = Blind Trust!

Quelle: OSSTMM ISECOM
- Visibility
- Access
- Trust
[ controls ]
[ limitations ]
<table>
<thead>
<tr>
<th>Category</th>
<th>OPSEC</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations</td>
<td>Visibility</td>
<td>Exposure</td>
</tr>
<tr>
<td></td>
<td>Access</td>
<td>Vulnerability</td>
</tr>
<tr>
<td></td>
<td>Trust</td>
<td></td>
</tr>
<tr>
<td>Controls</td>
<td>Class A - Interactive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>Weakness</td>
</tr>
<tr>
<td></td>
<td>Indemnification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Resilience</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subjugation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continuity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-Repudiation</td>
<td>Concern</td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Privacy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alarm</td>
<td>Anomalies</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Quelle: OSSTMM ISECOM
[ done properly? ]
[Ressources]

www.osstmm.org
www.isecom.org

### Attack Surface Security Metrics

#### RAV version 3.0 - OSSTMM version 3.0

<table>
<thead>
<tr>
<th>OPSEC</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Visibility</td>
<td>0</td>
</tr>
<tr>
<td>Access</td>
<td>0</td>
</tr>
<tr>
<td>Trust</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total (Porosity)</strong></td>
<td><strong>0</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONTROLS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Class A</strong></td>
</tr>
<tr>
<td>Authentication</td>
</tr>
<tr>
<td>Indemnification</td>
</tr>
<tr>
<td>Resilience</td>
</tr>
<tr>
<td>Subjugation</td>
</tr>
<tr>
<td>Continuity</td>
</tr>
<tr>
<td><strong>Total Class A</strong></td>
</tr>
</tbody>
</table>

| **Class B** | **Missing** |
| Non-Repudiation | 0 | 0 |
| Confidentiality  | 0 | 0 |
| Privacy          | 0 | 0 |
| Integrity        | 0 | 0 |
| Alarm            | 0 | 0 |
| **Total Class B** | **0** | **0** |

| All Controls Total | 0 | 0 |
| Whole Coverage     | 0,00% | 0,00% |

#### LIMITATIONS

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerabilities</td>
<td>0,000000</td>
</tr>
<tr>
<td>Weaknesses</td>
<td>0,000000</td>
</tr>
<tr>
<td>Concerns</td>
<td>0,000000</td>
</tr>
<tr>
<td>Exposures</td>
<td>0,000000</td>
</tr>
<tr>
<td>Anomalies</td>
<td>0,000000</td>
</tr>
<tr>
<td><strong>Total # Limitations</strong></td>
<td><strong>0,000000</strong></td>
</tr>
</tbody>
</table>

**Actual Security:** 100,00
- Industry 74.49%
- Military 97.16%
- Bank/Insurance 84.36%
- Software-Vendors 73.12%
- Politicians 76.58%

Compare Security
Can not show you – compliance ...

Size

Visibility

Porosity

Value

Integrity

Subjugation

Symmetry

Offsets

Consistency

Components

<table>
<thead>
<tr>
<th>Trust</th>
<th>Size (on or off)</th>
<th>Symmetry</th>
<th>Visibility (Transparency, Monitoring)</th>
<th>Subjugation/Control</th>
<th>Consistency</th>
<th>Integrity</th>
<th>Offsets (gal)</th>
<th>Broken Trust Value</th>
<th>Components</th>
<th>Porosity</th>
<th>Trustworthiness</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>40%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>4%</td>
</tr>
<tr>
<td>MDM Controlled</td>
<td>100%</td>
<td>100%</td>
<td>60%</td>
<td>100%</td>
<td>100%</td>
<td>-</td>
<td>0%</td>
<td>100%</td>
<td>0%</td>
<td>80%</td>
<td>78%</td>
</tr>
</tbody>
</table>
Welcome to Fedora Security Lab

This Trac/git instance is used for the development of the [Fedora Security Lab](https://fedora.redhat.com) also known as [Fedora Security Spin](https://fedora.redhat.com). This linked packages currently exist in Fedora and are on the Security Lab Live CD!

If you are just interested in the Spin itself, please visit the [security spin page](https://fedora.redhat.com).

Help us (aka Contribute)

There are many ways to help.

- Pick a task at the [Wishlist](https://fedora.redhat.com/wiki/Wishlist) or do a Package Review. For that just follow the [Tracker bug](https://bugzilla.redhat.com/)
- There are some packages which are in the repositories of Fedora and are waiting to get included into the Fedora Security Lab.
- Add relevant information sources to the [Documentation](https://fedora.redhat.com/wiki/Documentation) page.
- Artwork

Further Questions how to contribute? Contact Joerg Simon - jsimon <at> fedoraproject.org

Git repository access

- [git://git.fedorahosted.org/git/security-spin.git](https://git.fedorahosted.org/git/security-spin.git) (anon checkout)
- [ssh://git.fedorahosted.org/git/security-spin.git](https://git.fedorahosted.org/git/security-spin.git) (commit access)

Misc

- [Create a Live CD](https://fedora.redhat.com/wiki/Creating_a_Live_CD)
- [Security related documents](https://fedora.redhat.com/wiki/Security)
- [Competitors](https://fedora.redhat.com/wiki/Competitors)
- [Some statistics](https://fedora.redhat.com/wiki/Statistics)

Login

- Click the login link above and use your [Fedora Project](https://fedora.redhat.com) username and password.
The fedora security spin team

bug me
jsimon@fedoraproject.org

Development Home
https://fedorahosted.org/security-spin/

Help us on the Wishlist:
https://fedorahosted.org/security-spin/report/1

Your Contribution is welcome