fedora
SECURITY LAB

Thorough, Safe and Secure

fedora *Security Lab*

and the OSSTMM

Joerg Simon

jsimon@fedoraproject.org

http://fedoraproject.org

[Eco Systems]

[Clarification - yes i know compliance is boring ... ;) **]**

The Fedora® Project and the ISECOM – both are independent non profit entities

Both are part of the FOSS ECO System!

Share relationships
/me

[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 a 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
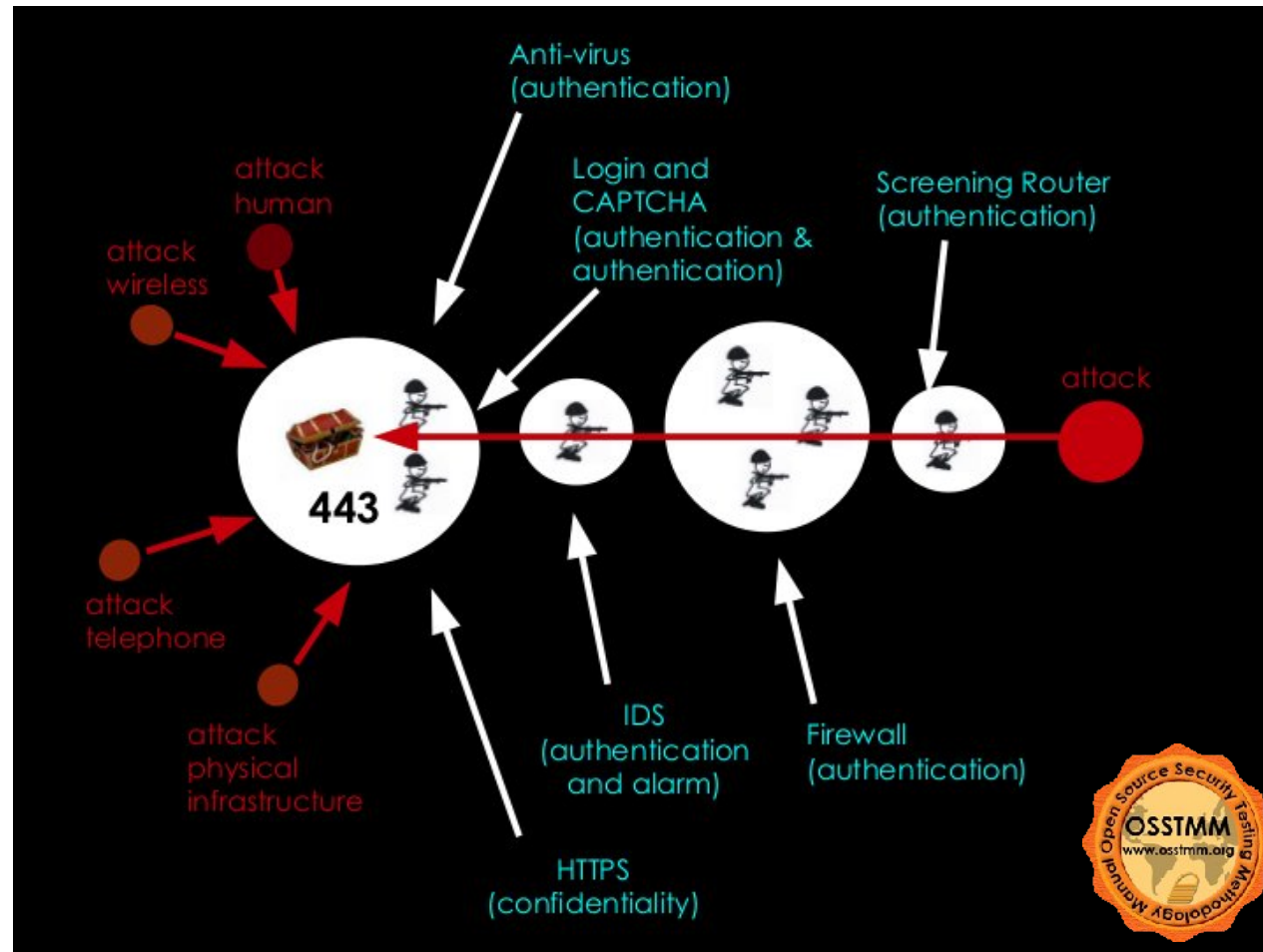
Pete Herzog ISECOM

WARNING
slippery surfaces
when icy conditions

[Compliance?]
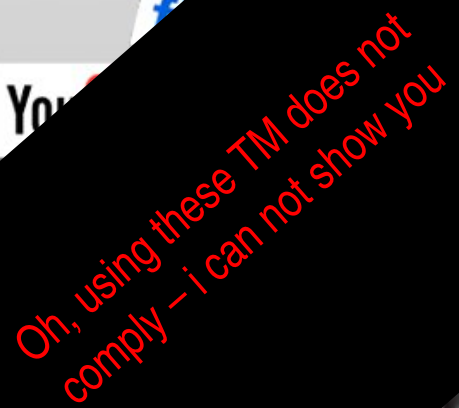
- **Comply!?**
  - But not secure?
  - Blocked?

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

- **Secure?**
  - But not compliant?
  - Blocked?
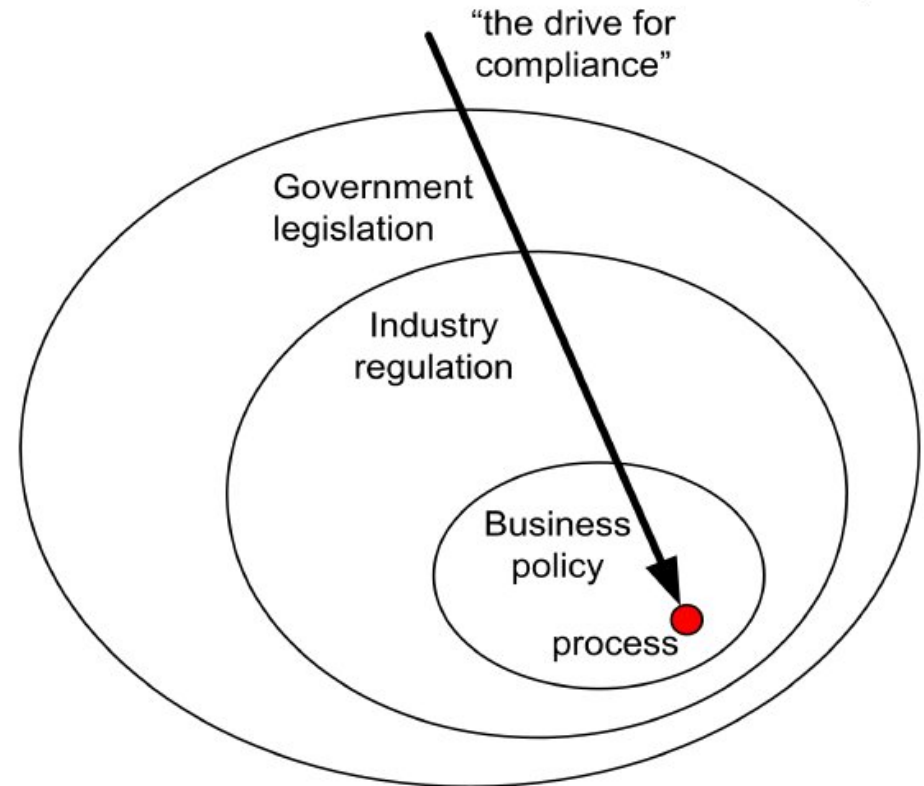
Quelle: OSSTMM ISECOM

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?**]
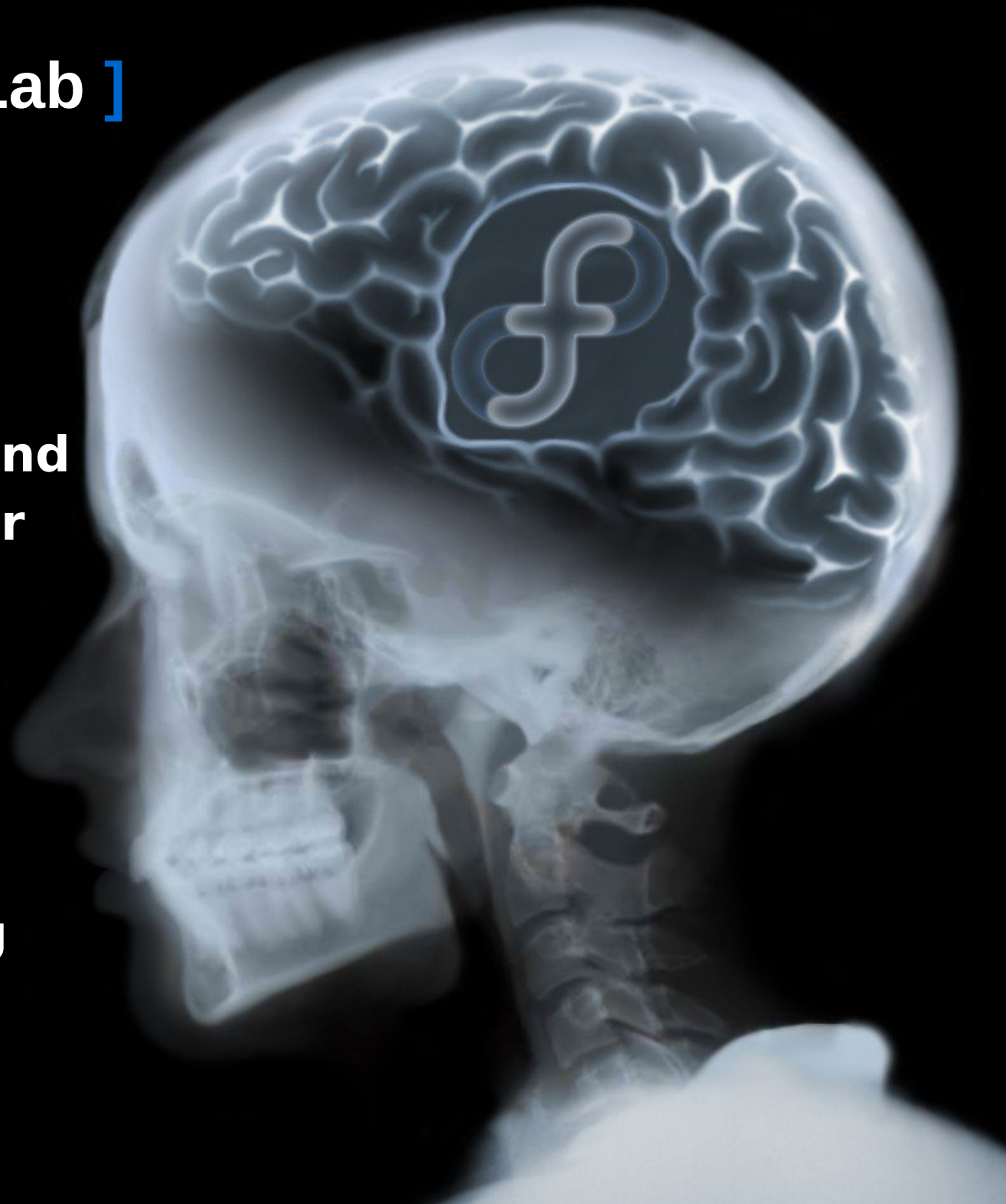
[features]

- a safe livecd-place for testing

- all fedora security features

- ability to install on HD and USB

- install software anytime

- clean, functional, fast

fedora

[developed by testers for testers]

- **collaborative developed**

- **community <> commercial benefits**

- **along our core values**

FREEDOM.   FRIENDS.   FEATURES.   FIRST.

[possible benefits]

- usecase for the FSL

- new cool upstreams

- implemented methodology

- fedora get taught along the OSSTMM

| UnicornScan | A port and protocol scanner witht he speed and power to catch a Unicorn. Actually, a truthful scanner that scales to very large networks while remaining equally fast. The scanner is truthful as it tells the tester exactly what is being returned in a clear format with no tricks to try to outsmart the auditor's experience. Results may go to an SQL DB for results you can revisit and map. A must have in any toolkit! | www.unicornscan.org |
| AFD | Active Filter Detection is one step, according to the Open Source Security Testing Methodology Manual, that security auditors should perform to identify the presence of Intrusion Prevention Systems and other technologies that would directly impact the quality of a security assessment. | www.purehacking.com/afd/ |

DNS Scan	A PERL script which supplements the DNS connect scanning task under the Port Scanning Module. Uses DNS connections on a class C to find live hosts through a firewall.	
MUTATEv2	an IDS evasion tool from Efrain Torres for assisting in system enumeration, port scanning, and vulnerability testing.	
Assessment Scanner	A JAVA tool which supplements the Document Grinding Module for electronic dumpster diving. Supports GET and POST requests.	
NWRAP	A tool developed by Simon Biles to add the Open Protocol Resource Database as an extended functionality to NMAP. This will show all known protocols for discovered ports which greatly extends the nmap_services file of one service per port. For this to work, NMAP must be installed and you should include the current version of the oprp.dump should be in the same directory.	
Metis v. 2.1.	This is a Java-based tool from Sacha Faust for finding the competitive intelligence weight of a web server and assists in satisfying the CI Scouting	

[benefits]

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

fedora

[OSSTMM Lab]

ettercap NG-0.7.3

Hosts   View   Mitm   Filters   Logging   Plugins

ETTERCAP

eth0... (Ethernet)

11:25:B2:36:68   10.1.1.129   255.255.255.0

n needs a valid 'redir_command_on' script in the ette
pped to UID 65534 GID 65534

About Nmap and Zenmap

Zenmap 5.00

Copyright 2005-2009 Insecure.Com LLC

Nmap
Nmap is a free and open source utility for network exploration and security auditing.

Zenmap
Zenmap is a multi-platform graphical Nmap and results viewer. It was originally derived

Umit   Umit credits
Umit is an Nmap GUI created as part of the Nmap/Google Summer of Code program.

About OpenVAS

OpenVAS

http://www.openvas.org/

OpenVAS-Client 3.0.2.
NessusClient origin: Copyright 1998-2007 Renaud Deraison
Most new code since OpenVAS-Client: Copyright 2009 Greenbor
License: GNU GPL v2

Authors:
Renaud Deraison
Thomas Arendsen Hein
Jan-Oliver Wagner
Bernhard Herzog
Michel Arboi (SSL Support)
Bruce Verderaime (Pie/Charts)
Matthew Mundell
Michael Wiegand
Felix Wolfstell

The Wireshar

File   Edit   View   Go   Capture   Analyze   Statisti

Filter:

[test-tool all-stars <]

File   Edit   View   Go   Bo

Back

WIRESHARK   The World's Most Popul

Capture

CAL9000

Xss Attacks | Encode/Decode | Http Requests | Http Responses | Scratch Pad | Chea

Misc Tools | Checklist | AutoAttack

SAVE STATE
LOAD STATE
HELP

CAL9000 WEB APPLICATION SECURITY TESTING ASSISTANT

Interface List
Live list of the capture interfaces (counts incoming packets)

Start capture on interface:

eth0
eth1
Pseudo-device that captures on all inte
USB bus number 1
USB bus number 2
USB bus number 3
USB bus number 4
lo

fedora

Open

Unless you have one of these ...

Community Chest

GET OUT
OF JAIL, FREE

[security features]

SELinux Security Alerts

⚠ SELinux has detected suspicious b

SELinux is preventing /usr/bin/kismet_client "write" a

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

SELinux denied access requested by kismet_client. It is not exp
kismet_client and this access may signal an intrusion attempt.
version or configuration of the application is causing it to requi

Security Tool

File   View   Help

Start level   Stop   Clear tests   Save...

All   Network (3)

Test	1	2	3	4	5
netserv	☐	☐	☑	☑	☑
openssh	☐	☐	☑	☑	☑
openvpn	☐	☐	☐	☐	☐
removedlibs	☐	☐	☑	☑	☑
netd	☐	☐	☐	☐	☐
suid	☐	☑	☑	☑	☑

Overview   Test Results

Test info

Name: pam
Author: Tomas Heinrich <theinric@

Test groups

accounts

Test is defined in levels

twork, Server, Paranoid

description

SELinux Administration

le   Help

elect:

Status
Boolean
File Labeling
User Mapping
SELinux User
Translation
Network Port
Policy Module
Process Domain

Add   Properti

Filter

File Specification

/
/.*
/[^/]+
/afs
/a?quota\.(user|grou
/\.autofsck
/\.autorelabel
/bin
/bin/.*
/bin/alsaunmute
/bin/bash
/bin/bash?

SELinux Policy Generation Tool

SELinux Policy Generation Tool

Firewall Configuration

File   Options   Help

Wizard   Apply   Reload   Enable   Disable

Trusted Services
Other Ports
Trusted Interfaces
Masquerading
Port Forwarding
ICMP Filter
Custom Rules

Here you can define which services are trusted. Trusted services are
all hosts and networks.

Service	Port/Protocol	Connt
☐ DNS	53/tcp, 53/udp	
☐ FTP	21/tcp	
☐ IMAP over SSL	9/tcp	
☐ IPsec	/ah, /esp	
☐ Mail (SMTP)	25/tcp	

fedora

[little treasures]

root@localhost:~

File Edit View Terminal Help

My traceroute [v0.75]

localhost.localdomain (0.0.0.0)   Sat Nov 14 23:06:20 2009
Keys: Help   Display mode   Restart statistics   Order of fields   quit

	Packets				Pings		
Host	Loss%	Snt	Last	Avg	Bes	Wrst	StDev
1. 192.168.1.1	0.0%	457	0	0	0	6.1	0.4
2. ???							
3. 172.30.1.193	0.0%	457	8.4	10.5	0.7	28.9	3.6
4. e3-2.ST-X1.ip-bb.kabel-badenwuerttemberg.de	0.0%	457	48.5	11.8	6.6	60.1	7.8
5. ae1.FRA-M2.ip-bb.kabel-badenwuerttemberg.de	8.3%	457	12.6	15.2	9.4	115.3	11.4
6. HSI-KBW-091-089-091-002.hsi2.kabelbw.de	0.4%	456	16.5	20.8	9.7	208.4	26.2
7. xe-1-3-0.lax20.ip4.tinet.net	0.2%	456	169.7	174.3	168.0	259.5	13.4
8. peer1-gw.ip4.tinet.net	0.0%	456	165.8	170.8	165.8	322.9	16.8
9. ???							
10. foss.in	1.5%	456	171.2	225.7	166.5	490.1	101.2

Fedora Security Spin

Reconnaissance ▶   ettercap
Forensics ▶   hping3
Wireless ▶   nc6
Intrusion Detection ▶ nc
Code Analysis ▶   ngrep
Password Tools ▶   nessus

Terminal   zenmap
Firefox   p0f
Midori   sing
cNetworkManager   scanssh
MidnightCommander   scapy
Screenshot   socat

Applications ▶   tcpdump
Preferences ▶   tiger
Administration ▶   wireshark
                      xprobe2
Install to Hard Drive nbtscan

Desktops ▶   tcpxtract
                      firewalk
ObConf   hunt
Reconfigure   halberd

Exit   iptraf

Terminal

File Edit View Terminal Help

bash-4.0$ su -c "hping3 -T --ttl 3 --syn -p 80 foss.in"
Password:
HPING foss.in (eth3 76.74.154.140): S set, 40 headers +
hop=3 TTL 0 during transit from ip=172.30.1.193 name=UN
hop=3 hoprtt=19.3 ms
hop=4 TTL 0 during transit from ip=172.30.1.46 name=e3-2.ST-X1.ip-bb.kabel-badenwue
hop=4 hoprtt=60.6 ms
hop=5 TTL 0 during transit from ip=78.42.40.15 name=ae1.FRA-M2.ip-bb.kabel-badenwue
hop=5 hoprtt=12.4 ms
hop=6 TTL 0 during transit from ip=91.89.91.2 name=HSI-KBW-091-089-091-002.hsi2.kab
hop=6 hoprtt=21.3 ms
hop=7 TTL 0 during transit from ip=89.149.185.213 name=xe-1-3-0.lax20.ip4.tinet.net
hop=7 hoprtt=175.3 ms
hop=8 TTL 0 during transit from ip=77.67.70.206 name=peer1-gw.ip4.tinet.net
hop=8 hoprtt=170.4 ms
^C
--- foss.in hping statistic ---
10 packets tramitted, 6 packets received, 40% packet loss
round-trip min/avg/max = 12.4/76.6/175.3 ms

root@localhos

File Edit View Terminal Help

Welcome to Scapy (2.0.0.10 beta)
>>> res,unans = traceroute(["foss.in"],dport=[80
Begin emission:
****Finished to send 20 packets.
*************Begin emission:
Finished to send 3 packets.
*Begin emission:
Finished to send 2 packets.
Begin emission:
Finished to send 2 packets.

Received 18 packets, got 18 answers, remaining 2
      76.74.154.140:tcp80
1   192.168.1.1   11
3   172.30.1.193   11
4   172.30.1.46   11
5   78.42.40.15   11
6   91.89.91.2   11
7   89.149.184.153   11
8   77.67.70.206   11
10 76.74.154.140   SA
11 76.74.154.140   SA
12 76.74.154.140   SA
13 76.74.154.140   SA
14 76.74.154.140   SA
15 76.74.154.140   SA
16 76.74.154.140   SA
17 76.74.154.140   SA
18 76.74.154.140   SA
19 76.74.154.140   SA
20 76.74.154.140   SA
>>> res.graph()

ImageMagick:

AS28513
[EMBRATEL]
192.168.1.1

unk0

4565
[MEGAPATH2-US - MegaPath Networks Inc.]
172.30.1.193
172.30.1.46

29562
[KABELBW-ASN Kabel Baden-Wuerttemberg GmbH & Co. KG]
78.42.40.15
91.89.91.2

3257
[TINET-BACKBONE Tinet SpA]
89.149.184.153
77.67.70.206

unk1

13768
[PEER1 - Peer 1 Network Inc.]
76.74.154.140 | http SA

fedora

[know]

- your tools

- your responsibility

- the ramification

- a **way** for proper testing!

[**reproducible**

with the right
Standards
& Methods!]

OSSTMM 3
the Open Source Security Testing Methodology Manual

Exclusive for
ISECOM Silver

ISECOM
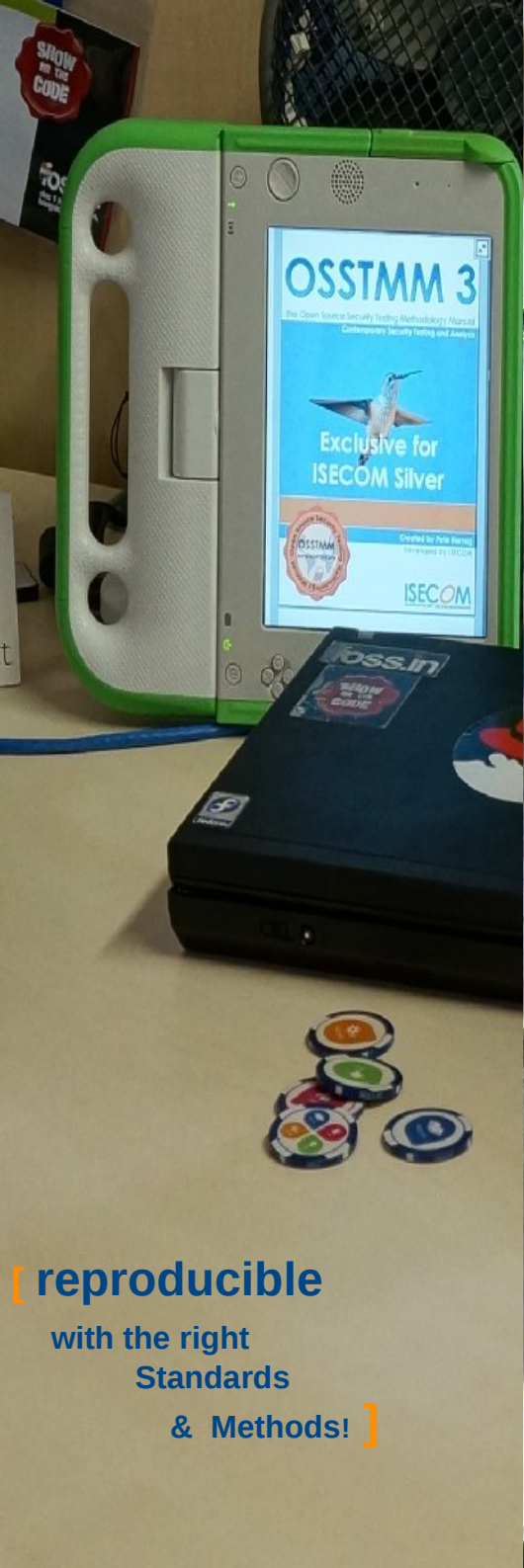
[**comparable**

real working **Metrics**

– based on scientific research]

Super
AUTO RIKSHAW METER

1 4

RUPEES **FARE** PAISE

Manufactured by:
Super METER MFG. COMPANY

59 B, MUNDHWA PUNE : 411 036
MAHARASHTRA (INDIA)

[**neutral**

unbiased

by relying on

Open Standards & Open Source]

[**usefull**
Reports
Management & Real world

compatible]

[there is a 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?

OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual

!= 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"
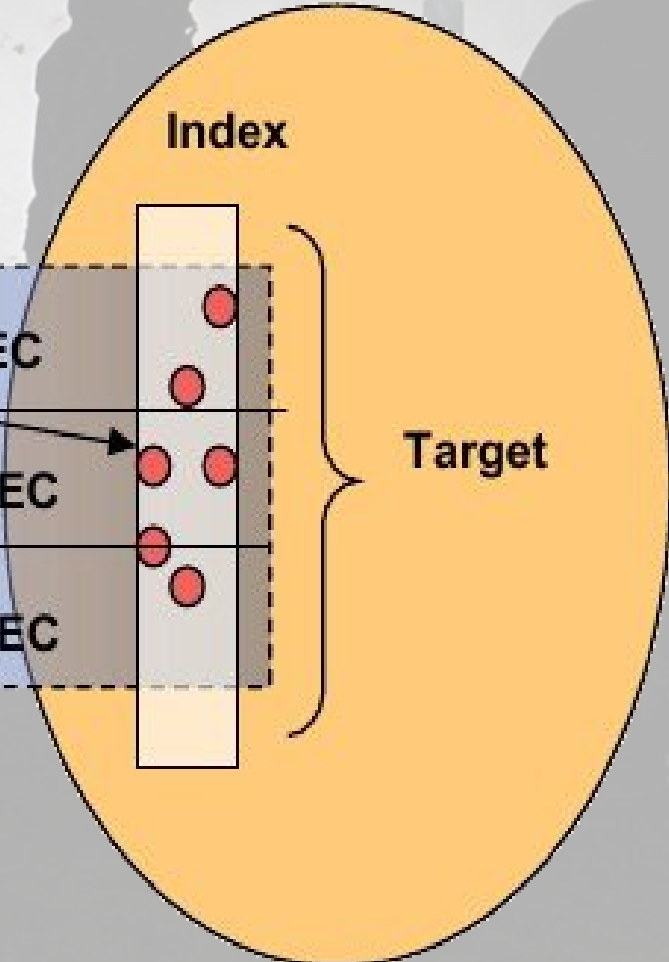
- ISECOM FOSS-Community - since January 2001 NPO

Vector

COMSEC

SPECSEC

PHYSSEC
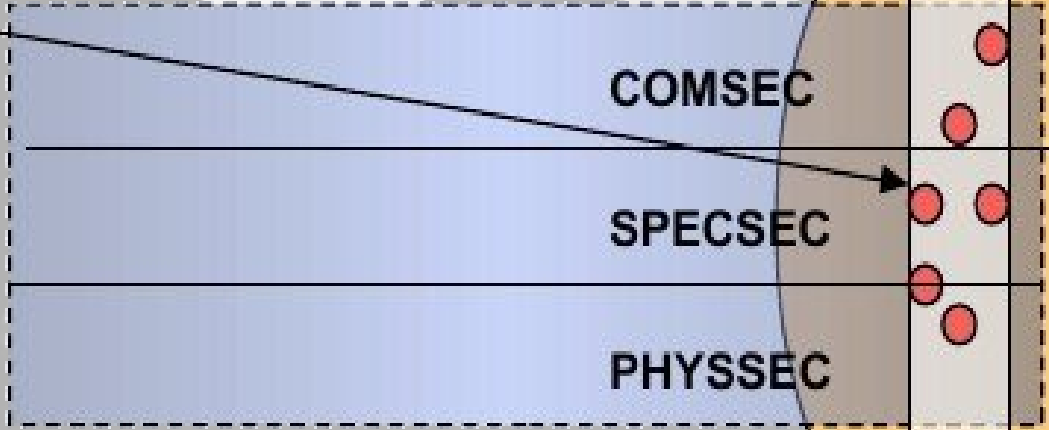
Channel

Index

Target

Scope

OSSTMM
Open Source Security Testing Methodology Manual
www.osstmm.org

[common sence]

Usual testing synonyms

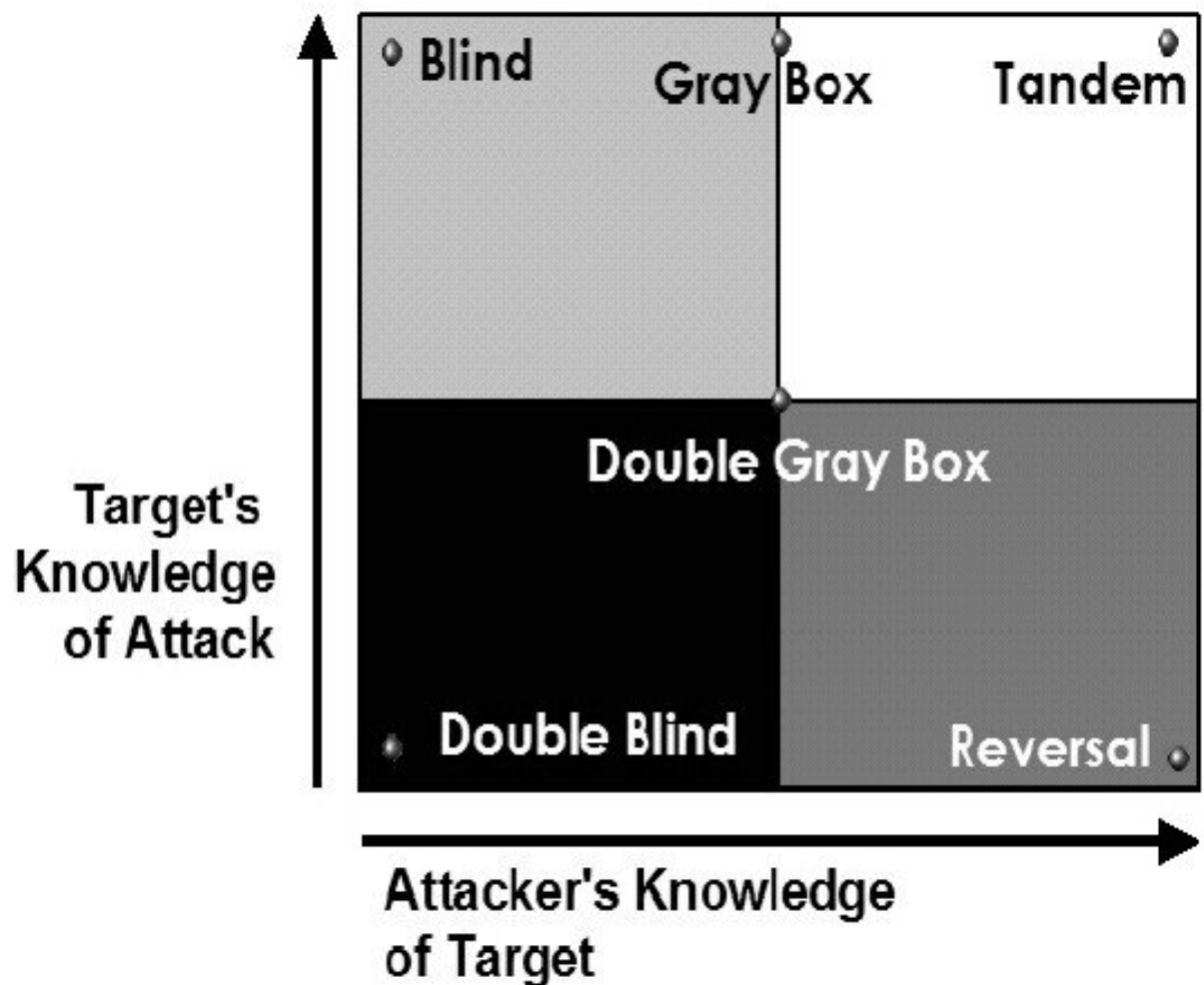Blind/Blackbox Pentest

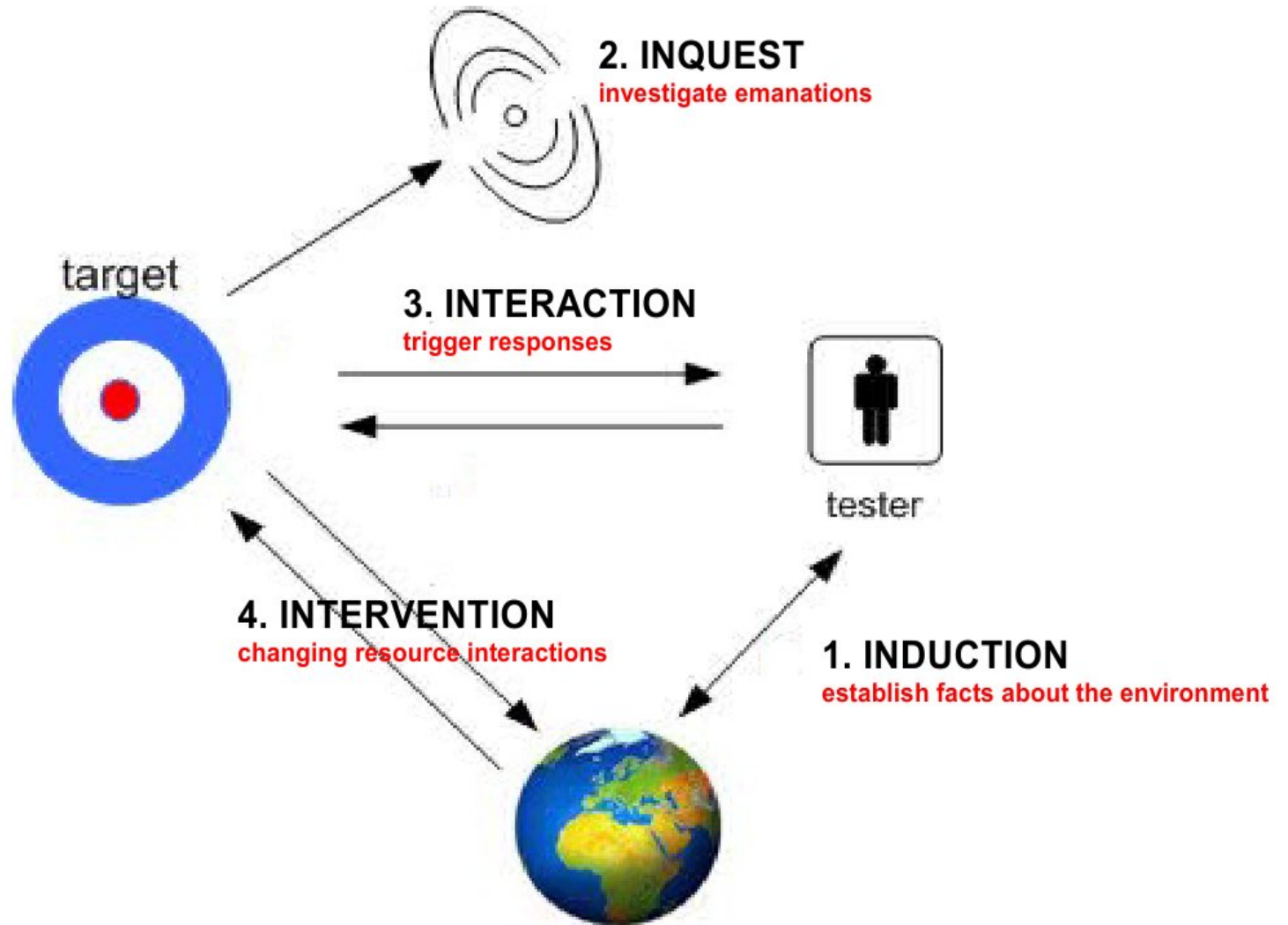Graybox/Chrystal/RedTeam

Social Engineering

WarDriving

WarDialing

Configuration-Reviews

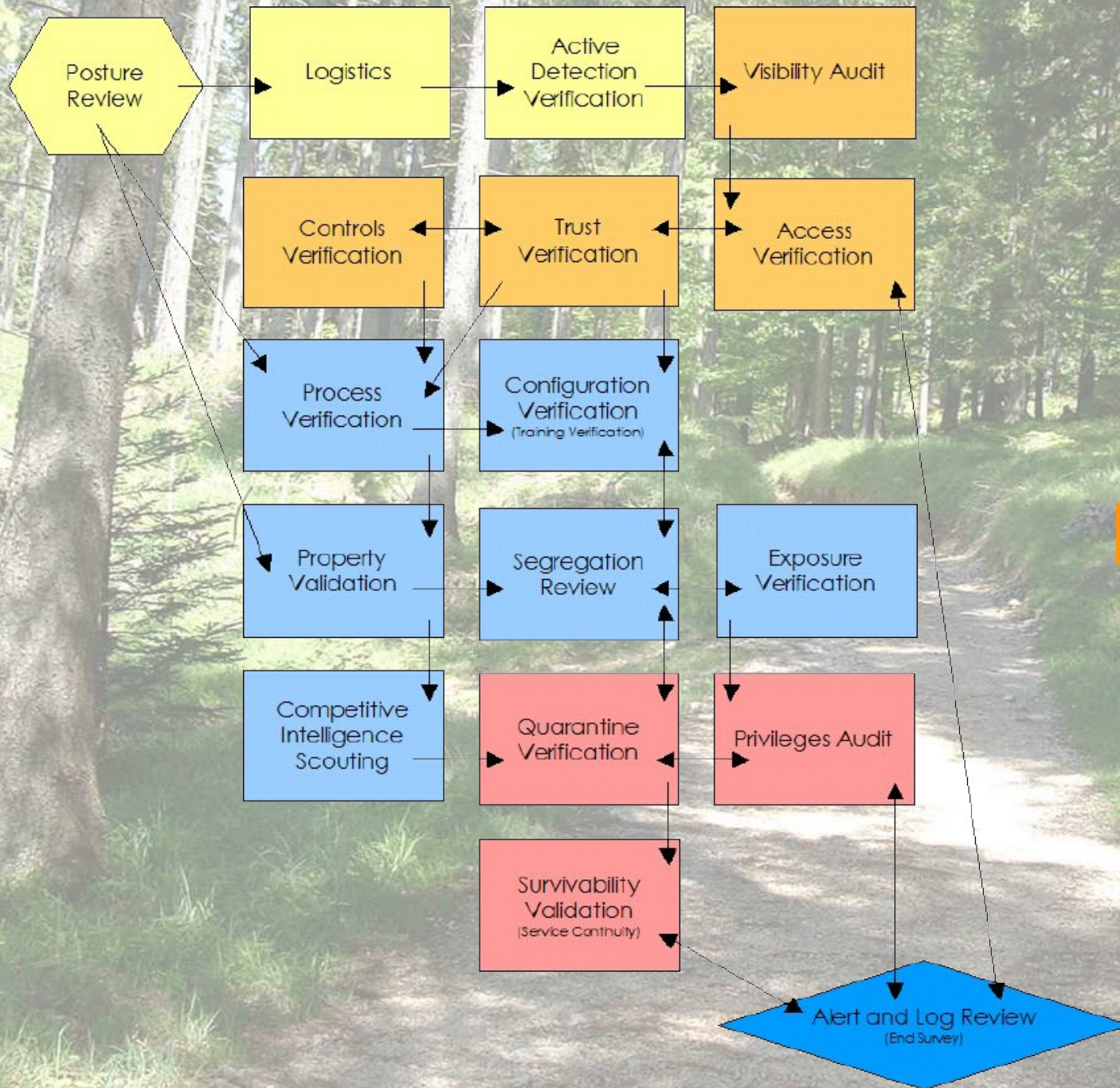Code Reviews

Common Test Methods

OSSTMM
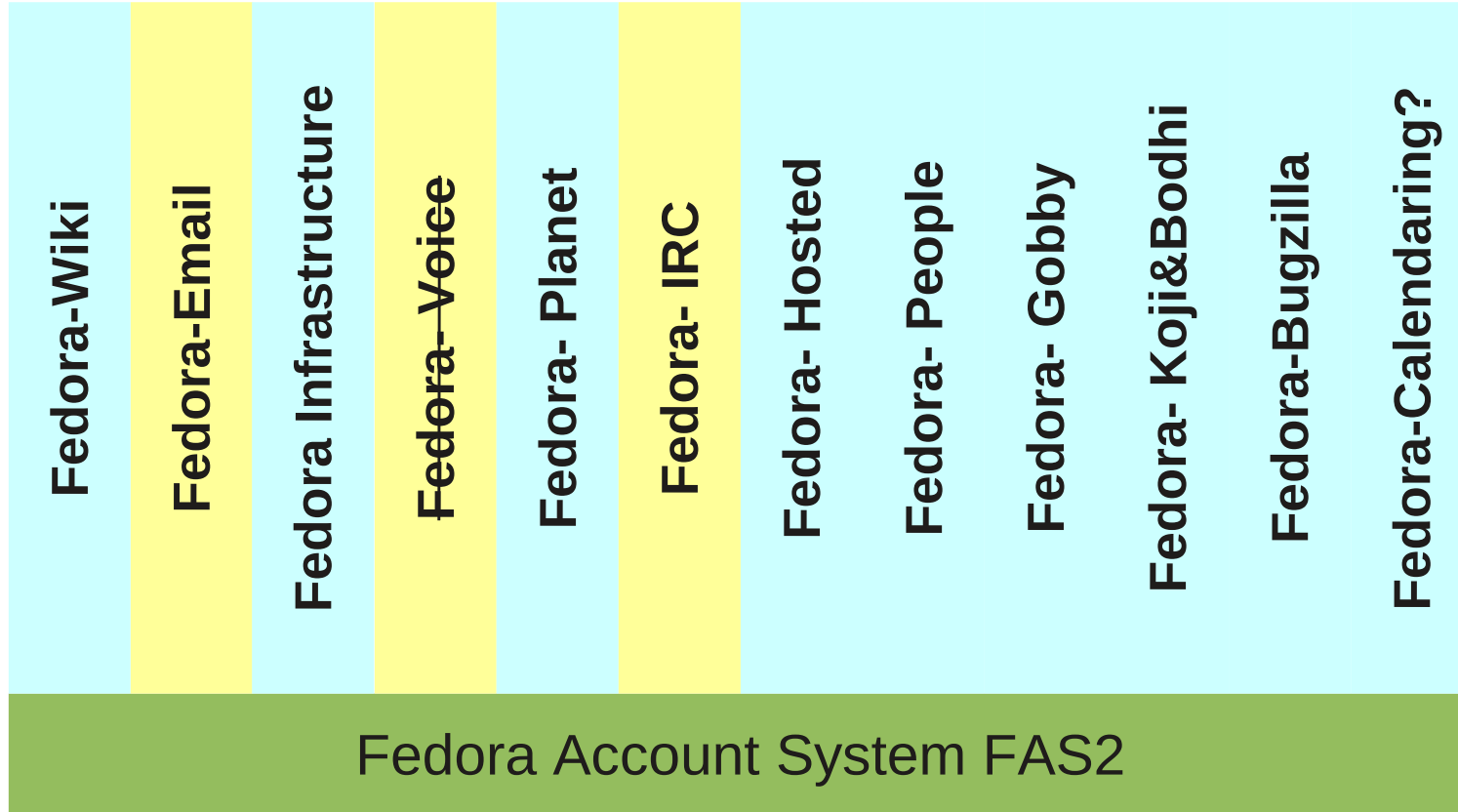www.osstmm.org
Manual Open Source Security Testing Methodology

target

2. INQUEST
investigate emanations

3. INTERACTION
trigger responses

tester

4. INTERVENTION
changing resource interactions

1. INDUCTION
establish facts about the environment

Posture Review → Logistics → Active Detection Verification → Visibility Audit

Controls Verification ← Trust Verification ← → Access Verification

Process Verification → Configuration Verification (Training Verification)

Property Validation → Segregation Review ← Exposure Verification

Competitive Intelligence Scouting → Quarantine Verification ← → Privileges Audit

Survivability Validation (Service Continuity)

Alert and Log Review (End Survey)

[testpath <]

OSSTMM
Open Source Security Testing Methodology Manual
www.osstmm.org

„Trusting everyone is insecure but not trusting anyone is inefficient"

OSSTMM 3.0

broken trust has consequences

Fedora-Wiki
Fedora-Email
Fedora Infrastructure
Fedora-Voice
Fedora- Planet
Fedora- IRC
Fedora- Hosted
Fedora- People
Fedora- Gobby
Fedora- Koji&Bodhi
Fedora-Bugzilla
Fedora-Calendaring?

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"

OSSTMM 3.0

Trust Properties!

- Trust is

  - no Emotion!

  - **a Decision!**

  - not quantifiable
    between humans!

- Wrong Trust Properties

- no Control = Blind Trust!

Quelle: OSSTMM ISECOM
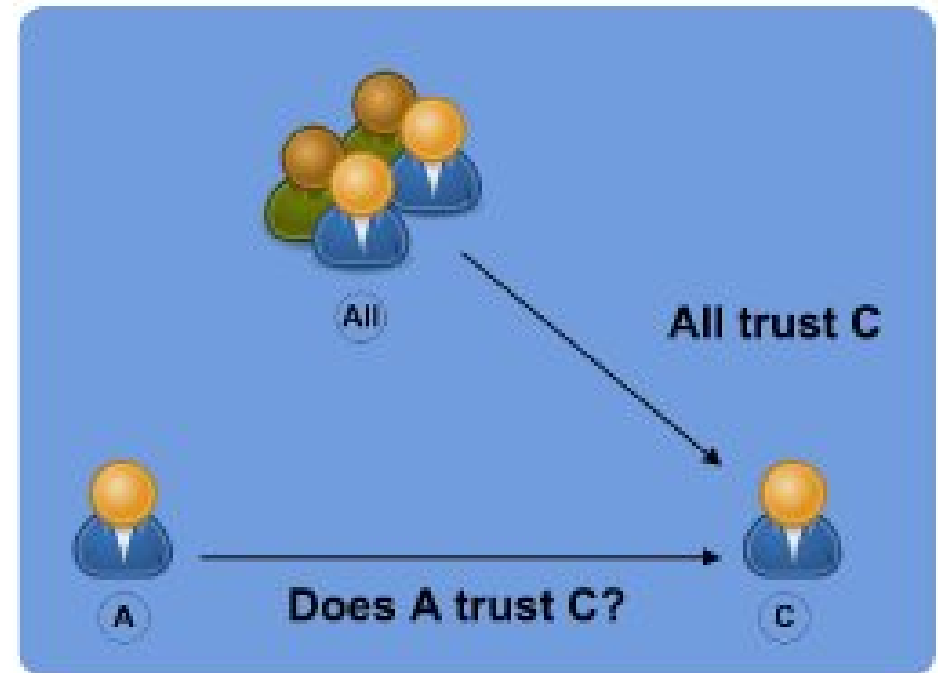
[Quantify Security]

- **Visibility**

- **Access**

- **Trust**

[porosity]

[**controls**]

[**limitations**]
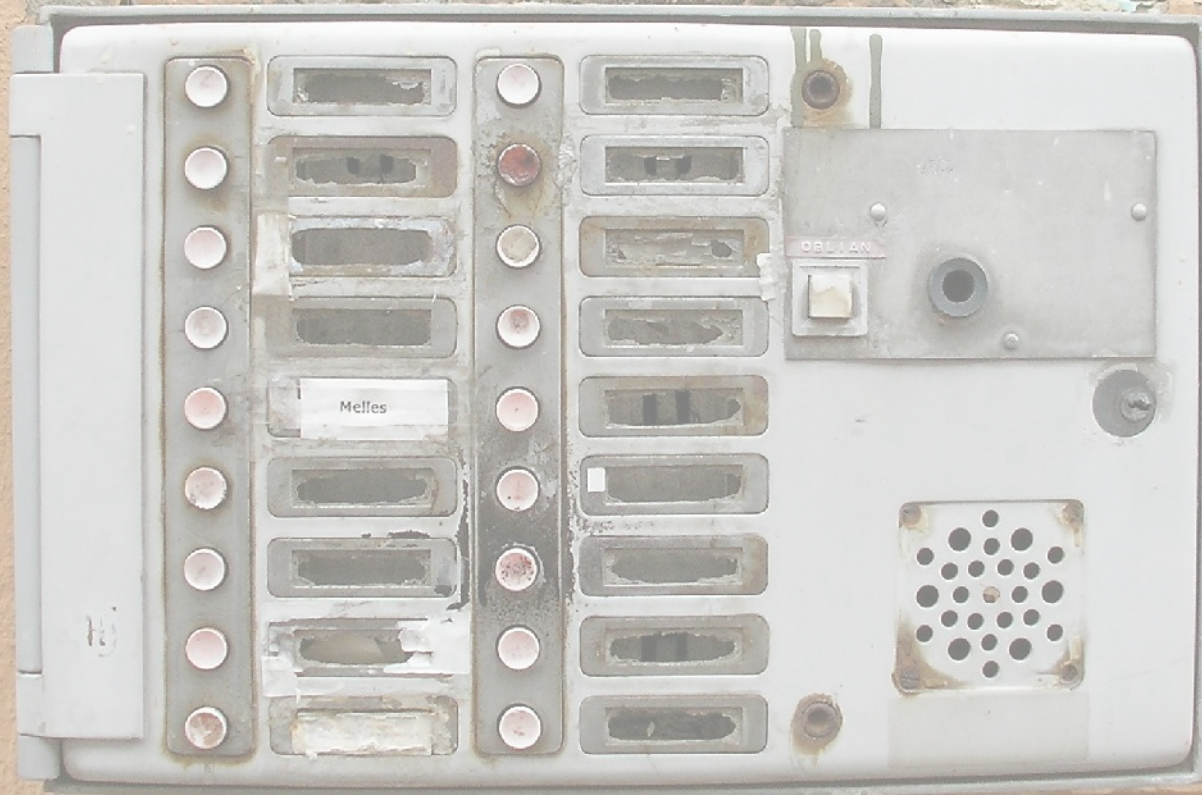
OSSTMM Risk Assessment Value

Category		OPSEC	Limitations
Operations		Visibility	Exposure
		Access	Vulnerability
		Trust	
Controls	Class A - Interactive	Authentication	Weakness
		Indemnification	
		Resilience	
		Subjugation	
		Continuity	
	Class B - Prozess	Non-Repudiation	Concern
		Confidentiality	
		Privacy	
		Integrity	
		Alarm	
			Anomalies
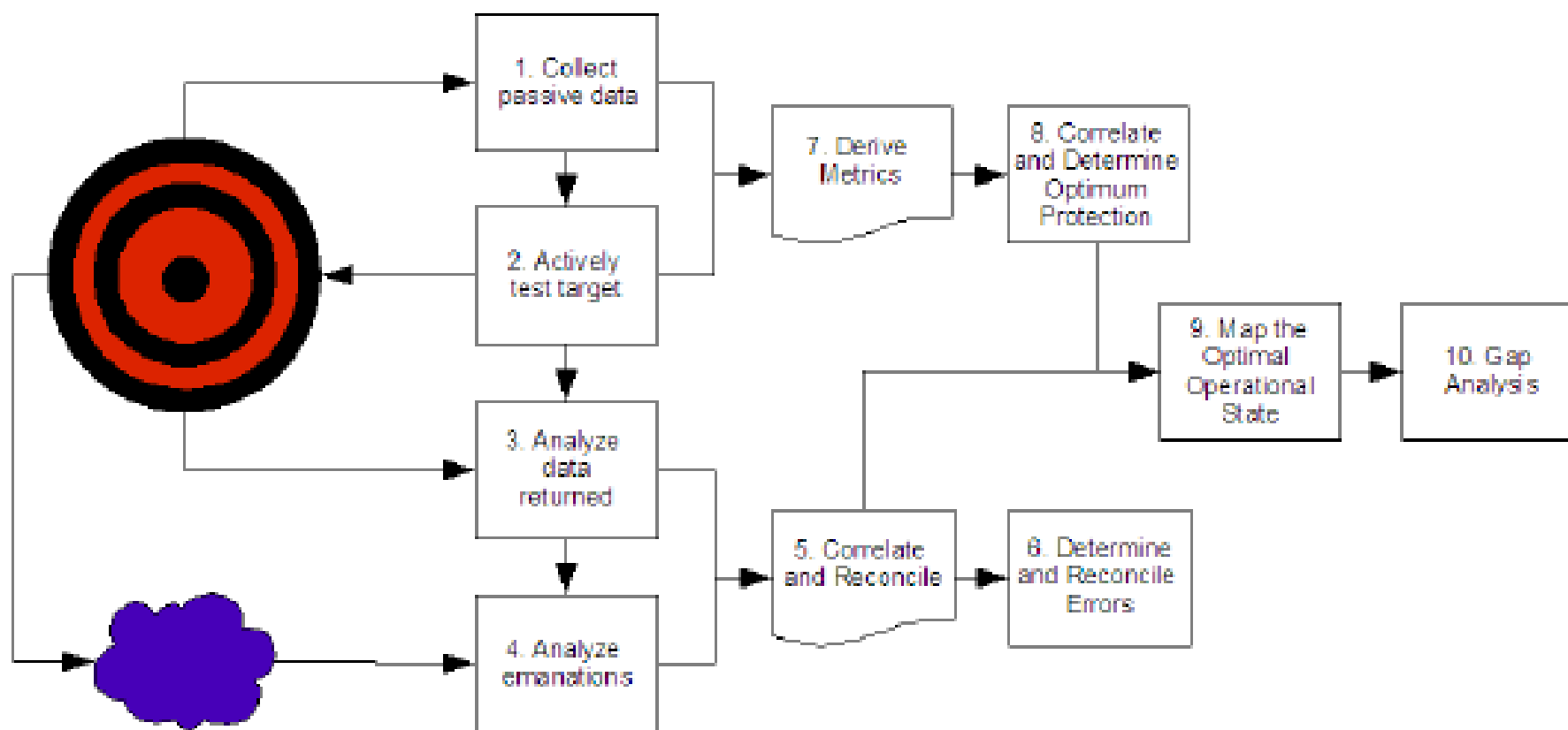
[**Ressources**]

www.osstmm.org

www.isecom.org
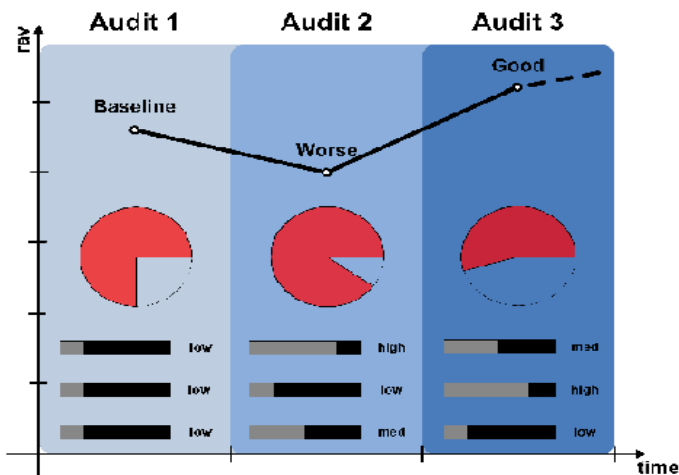
Attack Surface Security Metrics

RAV version 3.0 – OSSTMM version 3.0

OPSEC				
Visibility	0			
Access	0			
Trust	0			
Total (Porosity)	**0**			

CONTROLS				
Class A		Missing		
Authentication	0	0		
Indemnification	0	0		
Resilience	0	0		
Subjugation	0	0		
Continuity	0	0		
Total Class A	**0**	**0**		

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

		True Missing		
All Controls Total	**0**	**0**		
Whole Coverage	**0,00%**	**0,00%**		

LIMITATIONS		Item Value	Total Value	
Vulnerabilities	0	0,000000	0,000000	
Weaknesses	0	0,000000	0,000000	
Concerns	0	0,000000	0,000000	
Exposures	0	0,000000	0,000000	
Anomalies	0	0,000000	0,000000	
Total # Limitations	**0**		**0,0000**	

ISECOM — INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC
0,000000

True Controls
0,000000

Full Controls
0,000000

True Coverage A
0,00%

True Coverage B
0,00%

Total True Coverag
0,00%

Limitations
0,000000

Security Δ
0,00

True Protection
100,00

Actual Security: 100,00

- Industry   74,49%

- Military   97,16%

- Bank/Ensurance   84,36%

- Software-Vendors   73,12%

- Politicians   76,58%

Compare Security

Subjugation

[quantify Trust]

Size

Visibility

Porosity

Value

Integrity

Symmetry

Offsets

Consistency

Components

Can not show you – compliance ...

...7 PM

you want to install this application?

Allow this application to:

⚠ **Network communication**
full Internet access

⚠ **Storage**
modify/delete SD card contents

⚠ **Phone calls**
read device state and identity

⚠ **Hardware controls**
record audio

⚠ **System tools**
retrieve running applications

Install   Cancel

t allowed to show you ...

Trust	Ergänzungen, Gegenstellen	RemoveApplyCountAverage										
Mob... ...ce & App		Size (one or many)	Symmetry	Visibility (Transparency, Monitoring)	Subjugation/ Control	Consistency	Integrity	Offsets (legal)	Broken Trust Value	Components	Porosity	Trustworthyness
...verified		0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	**0%**
...ied		40%	0%	0%	0%	0%	0%	0%	0%	0%	0%	**4%**
MDM Controlled		100%	100%	60%	60%	100%	100%	-	0%	100%	80%	**78%**

Welcome to Fedora Security Lab

This Trac/git instance is used for the development of the ⇨Fedora Security Lab also known as ⇨Fedora Security Spin. 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.

Help us (aka Contribute)

There are many ways to help.

- Pick a task at the Wishlist or do a Package Review. For that just follow the ⇨Tracker bug!
- 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 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/ (anon checkout)
- ⇨ssh://git.fedorahosted.org/git/security-spin.git/ (commit access)

Misc

- ⇨Create a Live CD
- Security related documents
- Competitors
- ⇨Some statistics

Login

- Click the login link above and use your ⇨Fedora Project username and password.

The fedora security spin team

SIGNS
POINT TO
𝑓

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