Thorough, Safe and Secure

fedora™ Security Lab

and the OSSTMM

Joerg Simon

jsimon@fedoraproject.org

http://fedoraproject.org

[Clarification – yes i know, but ... ;)]

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

Both are part of the FOSS ECO System!

Share relationships

/me

fedora
SECURITY LAB

[what was planned @ foss.in Bangalore 2009]

- move wishlist to fedorahosted - http://fedorahosted.org/security-spin/
- get wishlist packaged – still a lot of work ahead -
- more webapplication testing tools – “we do not live in a ideal world” but!
- implement new branding – decided to use the Fedora Branding for now
- improve spin section content – went to spins.fedoraproject.org/security
- consider new menustructure along OSSTMM 4points – still in discussion

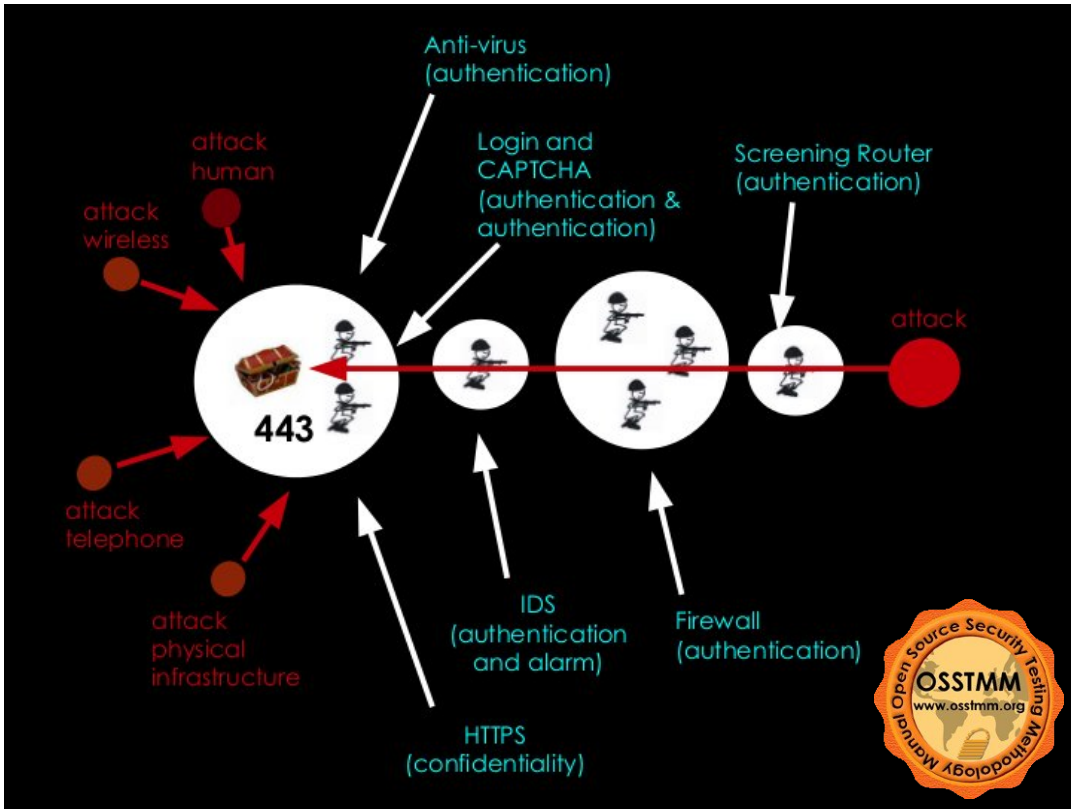
rsc helped so much!

- move to as SLiM desktop manager – moved to SLiM -> moved to LXDM
- move to LXDE as window manager – we moved to LXDE
- implement OSSTMM upstreams – we packaged SCARE, unicornscan, but ...
- become a official spin in Fedora 13 – we made it as a official spin in Fedora 13, 14, 15

and will be for 16

[Security
the Day before Yesterday]

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



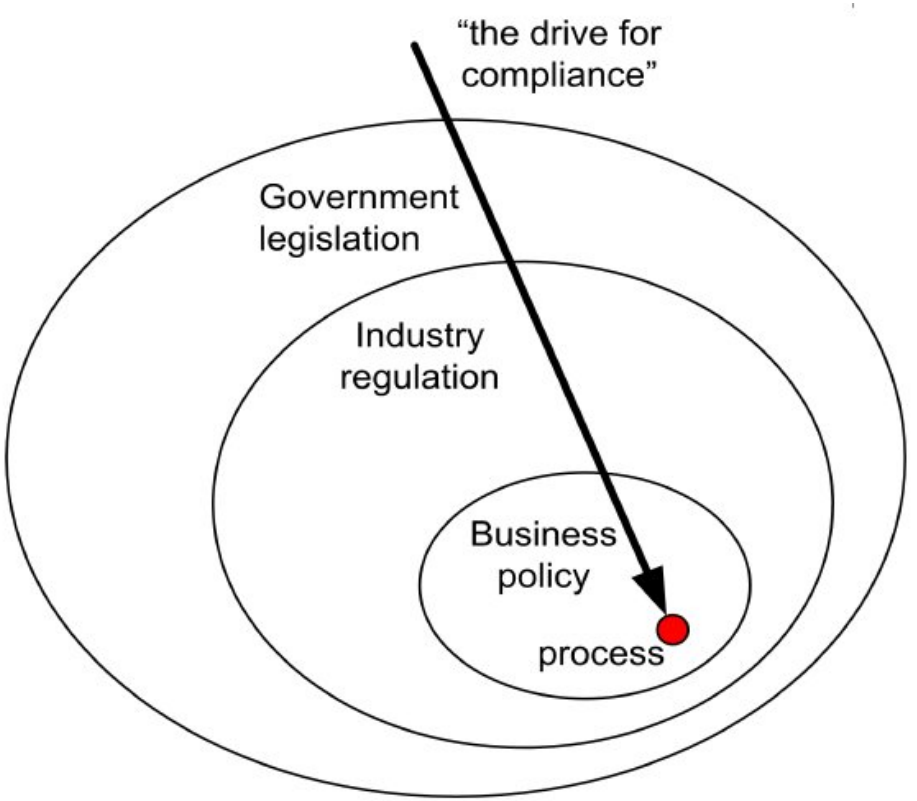
Pete Herzog ISECOM

[one truth?]

Pete Herzog ISECOM

[Compliance?]

- Comply!?
  - But not secure?
  - Blocked?
- Get the Audit Result you need?
  - But not secure?
  - Blocked?
- Secure?
  - But not compliant?
  - Blocked?



Quelle: OSSTMM ISECOM

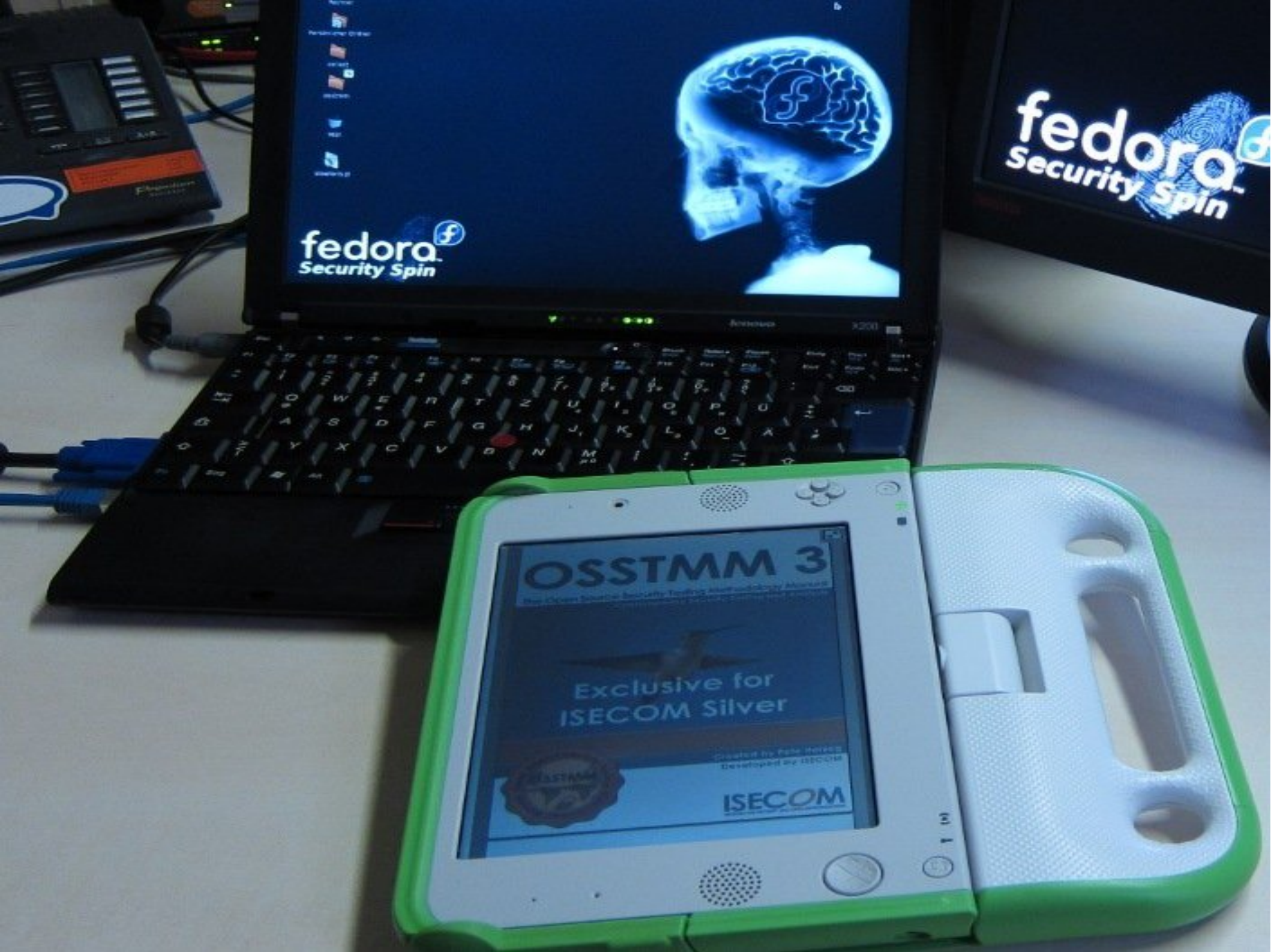
Security Today?

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 Spin
fedora
Security Spin
OSSTMM 3
Exclusive for
ISECOM Silver
ISECOM

[Fedora Security Lab]

A open source test- and education platform for

- security-auditing

- forensics

- penetration-testing

fedora
SECURITY LAB

[features]

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

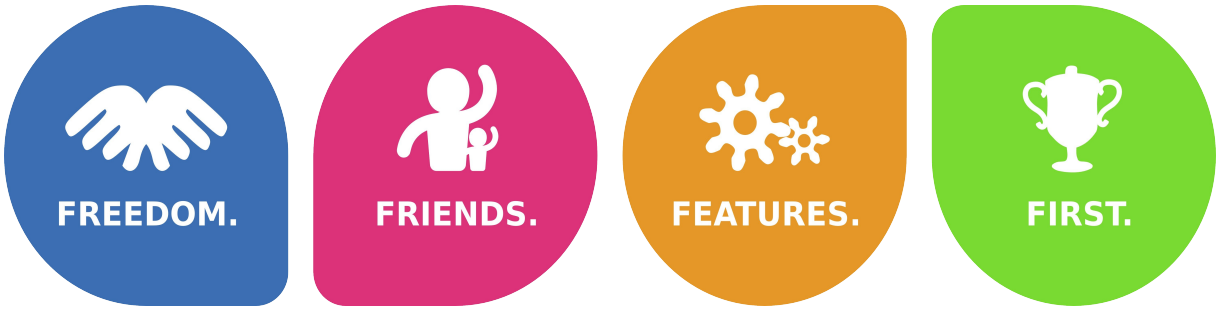
fedora

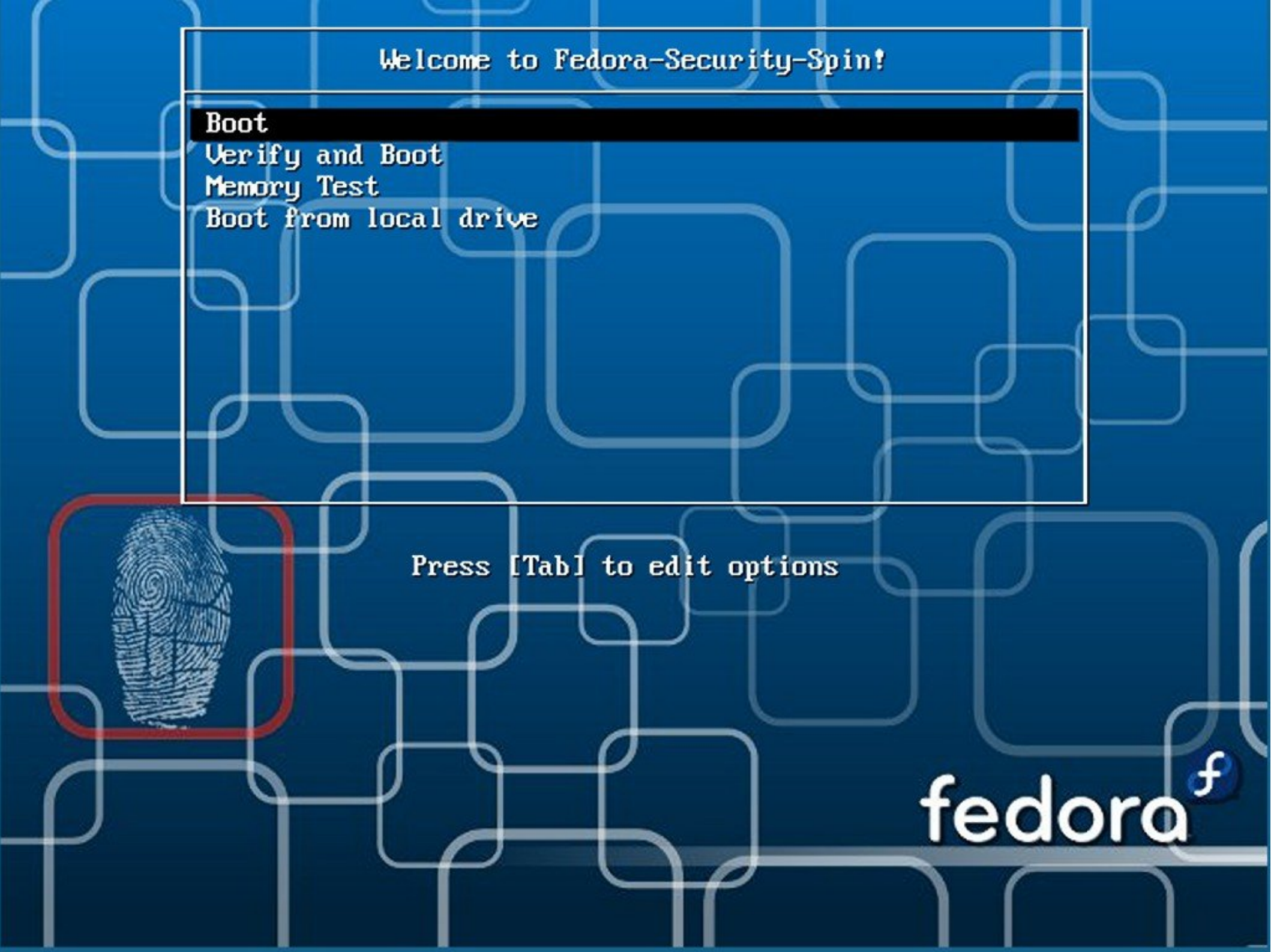
[developed by testers for testers]

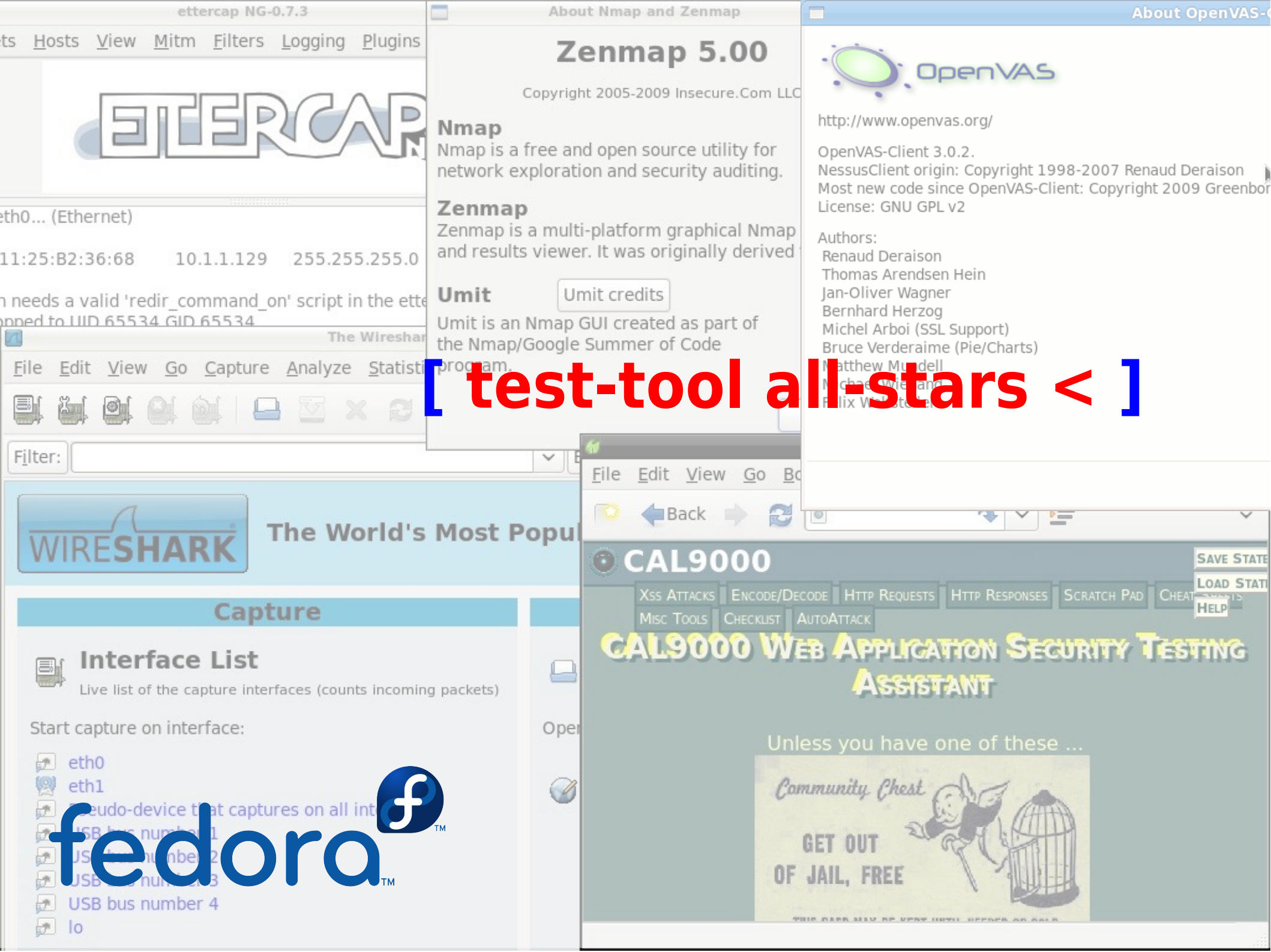
- collaborative developed

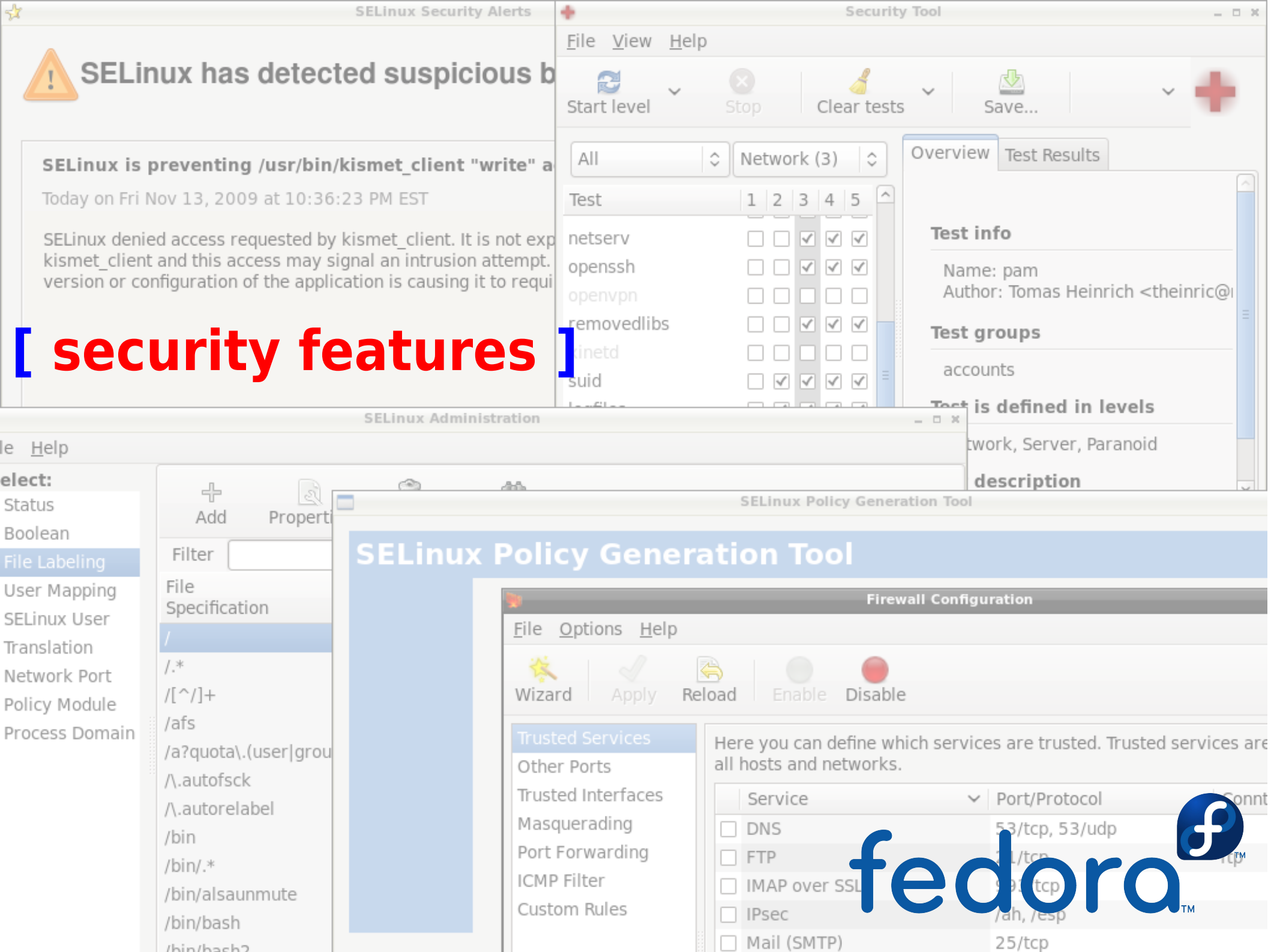
- community <> commercial benefits

- along our core values




Welcome to Fedora-Security-Spin!
Boot
Verify and Boot
Memory Test
Boot from local drive
Press [Tab] to edit options
fedora


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
needs a valid 'redir_command_on' script in the ette
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)
[test-tool all-stars <]
File Edit View Go Capture Analyze
Filter:
WIRESHARK
The World's Most Popul
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start capture on interface:
eth0
eth1
USB bus number 4
lo
fedora
File Edit View Go
Back
CAL9000
Xss Attacks
Encode/Decode
Http Requests
Http Responses
Scratch Pad
Misc Tools
Checklist
AutoAttack
Help
CAL9000 Web Application Security Testing Assistant
Unless you have one of these ...
Community Chest
GET OUT OF JAIL, FREE


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 features]
Security Tool
File View Help
Start level
Stop
Clear tests
Save...
All
Network (3)
Overview
Test Results
Test 1 2 3 4 5
netserv
openssh
openvpn
removedlibs
inetd
suid
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
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
DNS
53/tcp, 53/udp
FTP
IMAP over SSL
IPsec
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

Host	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. 192.168.1.1	0.0%	457	1.0	1.0	0.9	6.1	0.4
2. ???							
3. 172.30.1.193	0.0%	457	8.4	10.5	6.7	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 ▸
- Forensics ▸
- Wireless ▸
- Intrusion Detection ▸
- Code Analysis ▸
- Password Tools ▸
- Terminal
- Firefox
- Midori
- cNetworkManager
- MidnightCommander
- Screenshot
- Applications ▸
- Preferences ▸
- Administration ▸
- Install to Hard Drive
- Desktops ▸
- ObConf
- Reconfigure
- Exit

- ettercap
- hping3
- nc6
- nc
- ngrep
- nessus
- zenmap
- p0f
- sing
- scanssh
- scapy
- socat
- tcpdump
- tiger
- wireshark
- xprobe2
- nbtscan
- tcpxtract
- firewalk
- hunt
- halberd
- 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
```

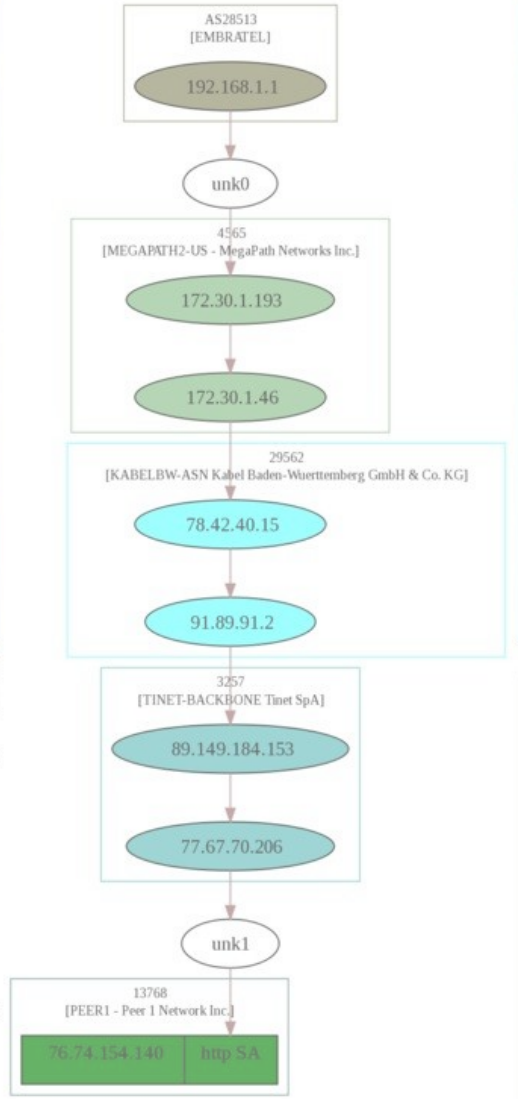
root@localhos

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: -



fedora™


[know]
- your tools
- your responsibility
- the ramification
- a way for proper testing!

[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?

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

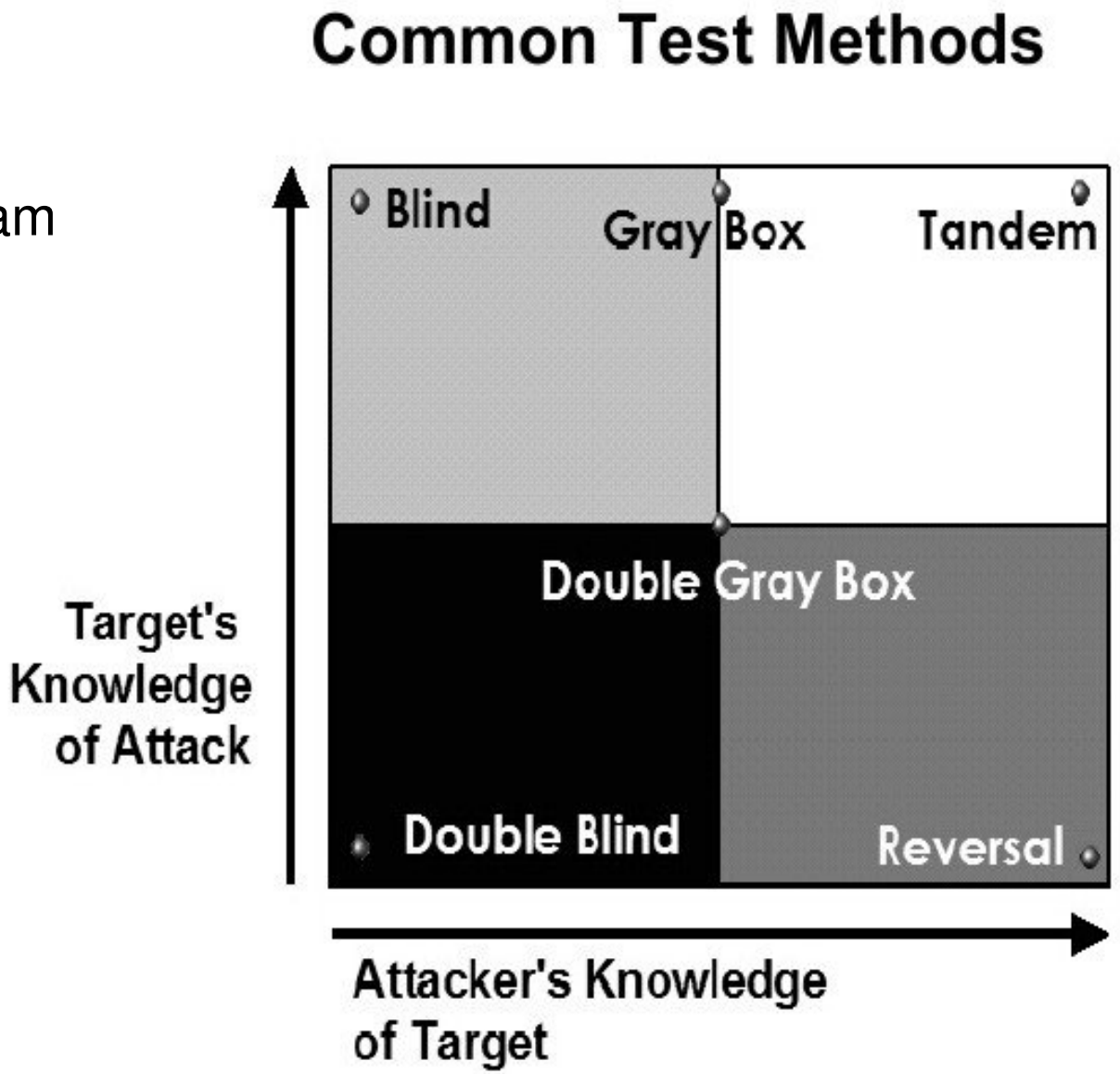
!= Checklist, solution based, best-practise

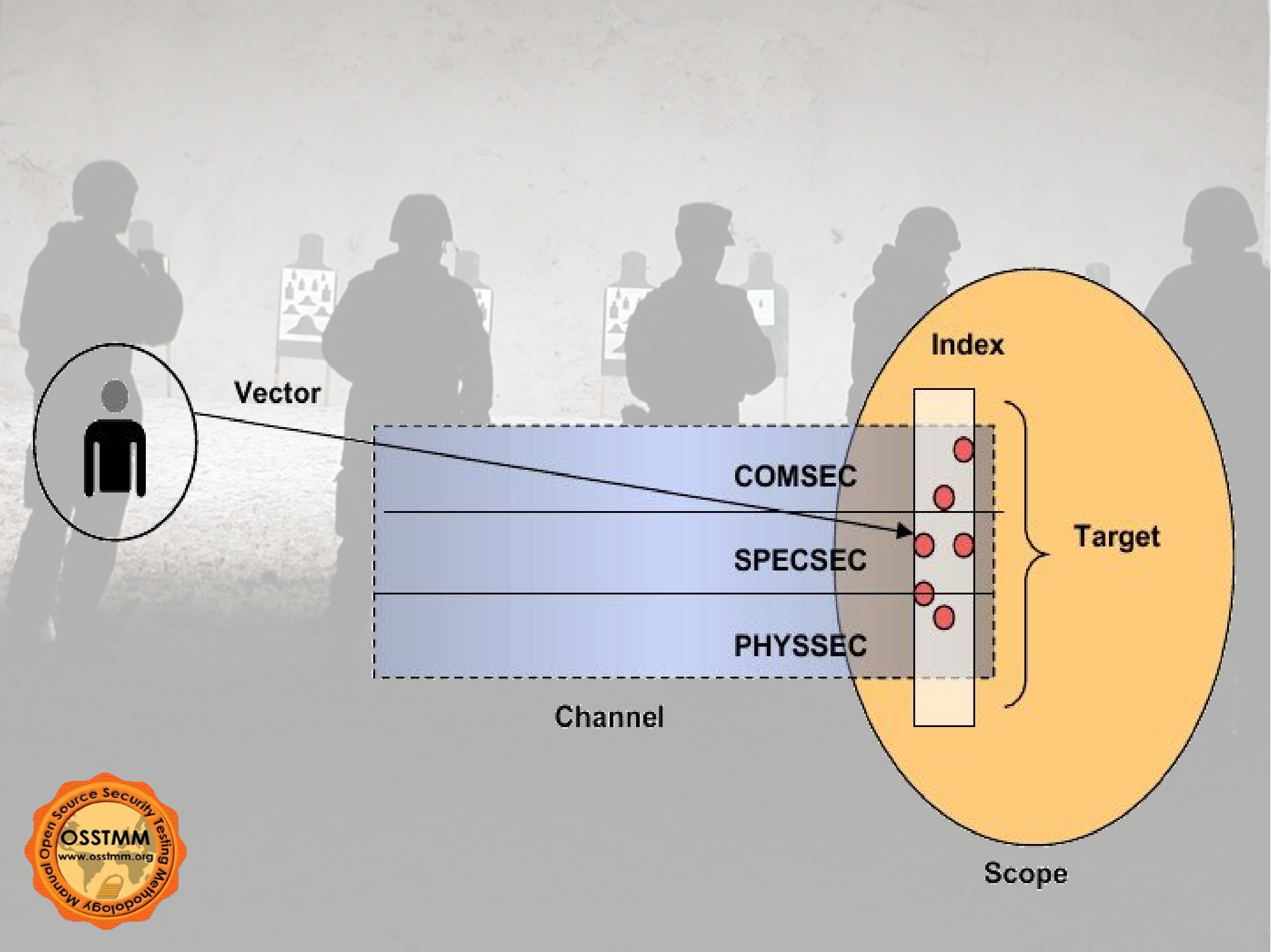
- **Measurable and comparable results**
- **Looks into operational Security and Trusts**
- **well developed Metric based on academic research**
- **„Thinking Out of the Box“**
- **ISECOM FOSS-Community - since January 2001 NPO**

[common sence]

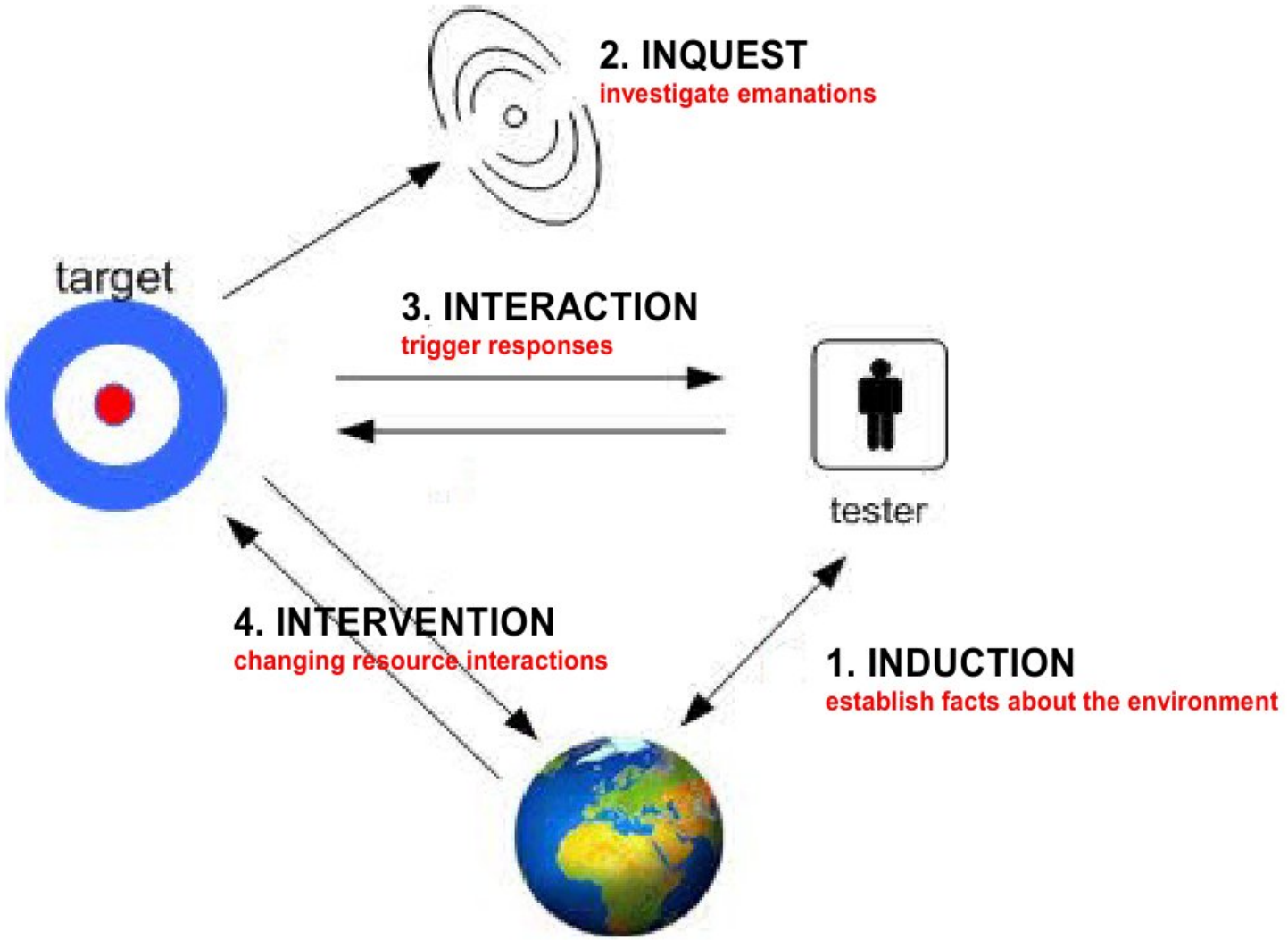
Usual testing synonyms

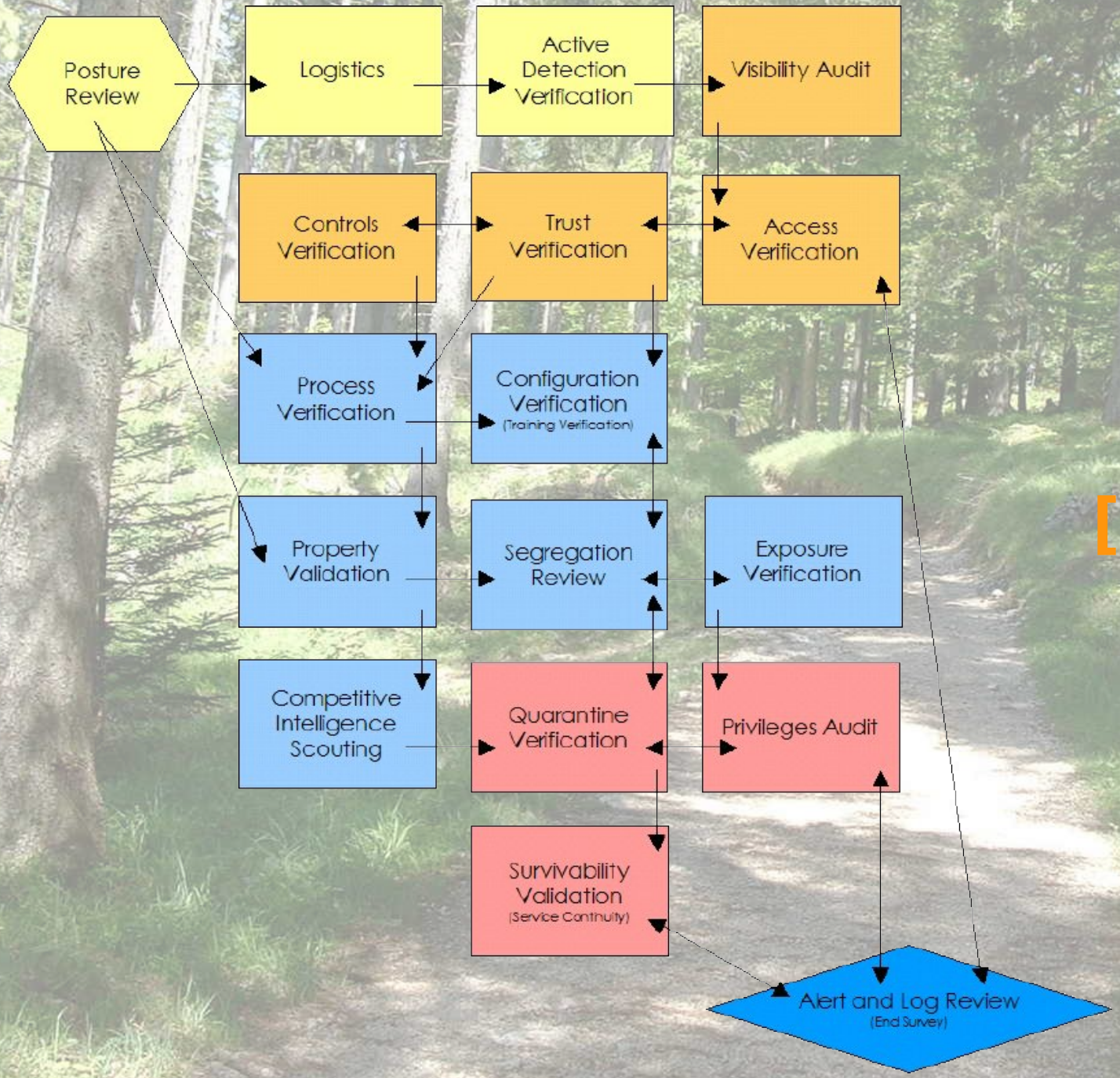
- Blind/Blackbox Pentest
- Graybox/Chrystal/RedTeam
- Social Engineering
- WarDriving
- WarDialing
- Configuration-Reviews
- Code Reviews




Vector
Index
COMSEC
SPECSEC
PHYSSEC
Target
Channel
Scope
OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual

[four points]


2. INQUEST
investigate emanations
target
3. INTERACTION
trigger responses
tester
4. INTERVENTION
changing resource interactions
1. INDUCTION
establish facts about the environment



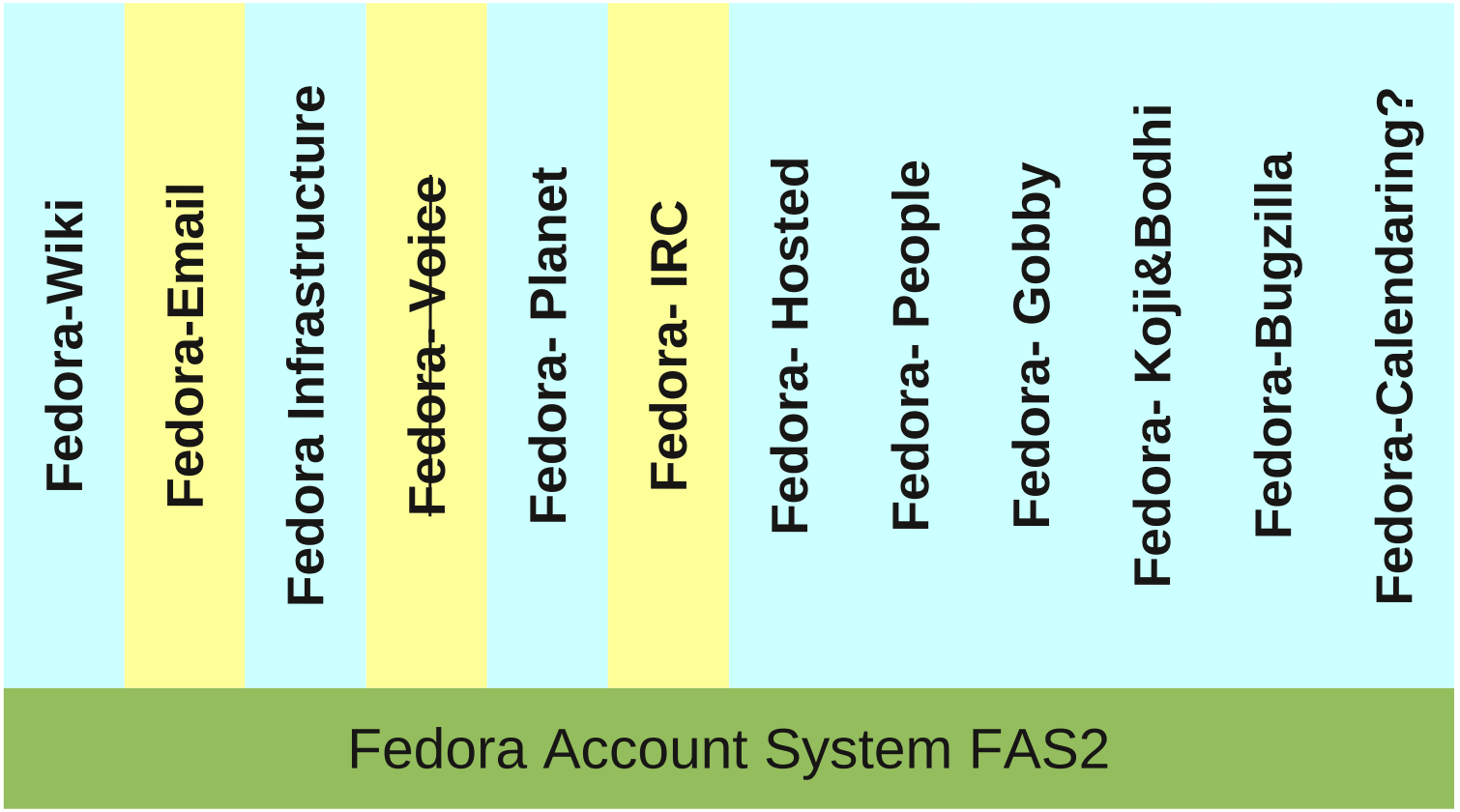
OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual

[testpath <]

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

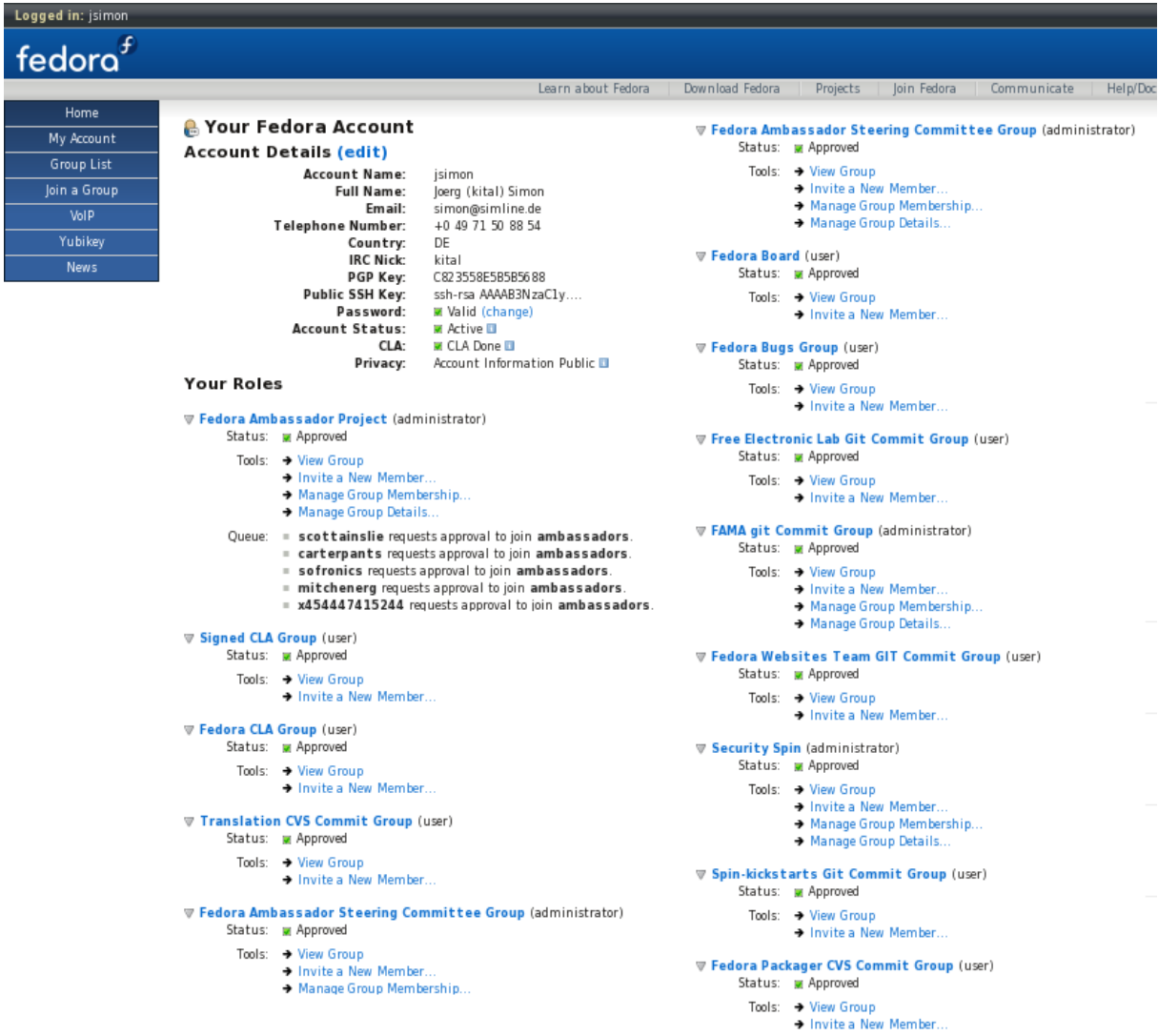
OSSTMM 3.0

broken trust has consequences



Fedora Trusts you!

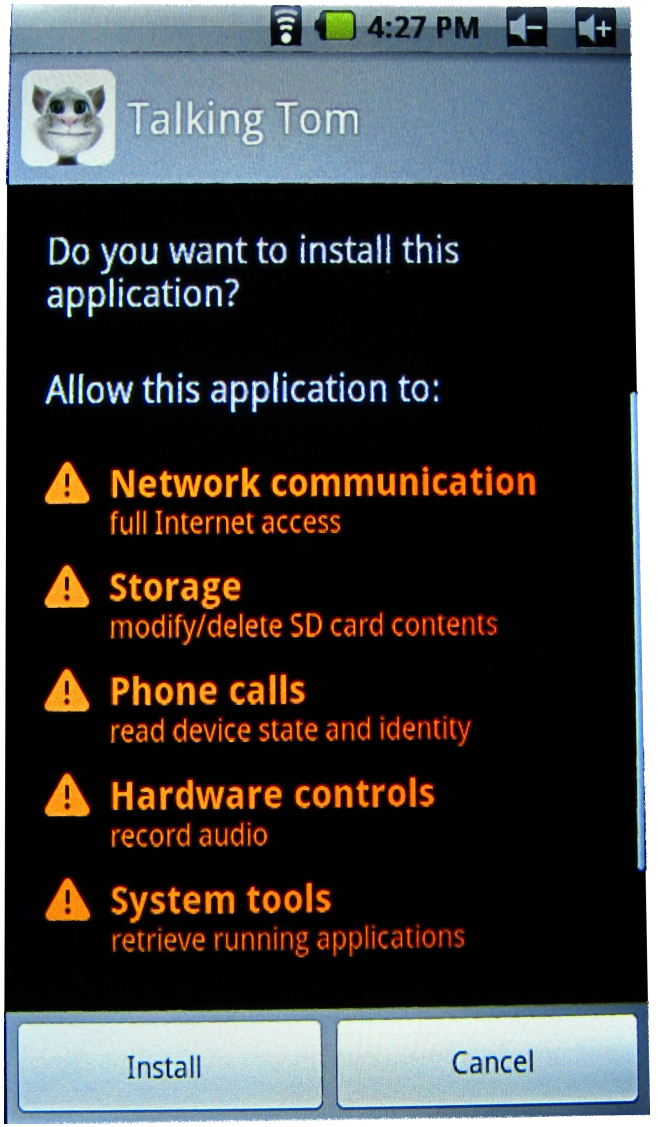
- Fedora „Code“ is used by **30 Mio.** Users!
- Contributor from
  - More than **400** commit Groups
  - **~25000** Contributors



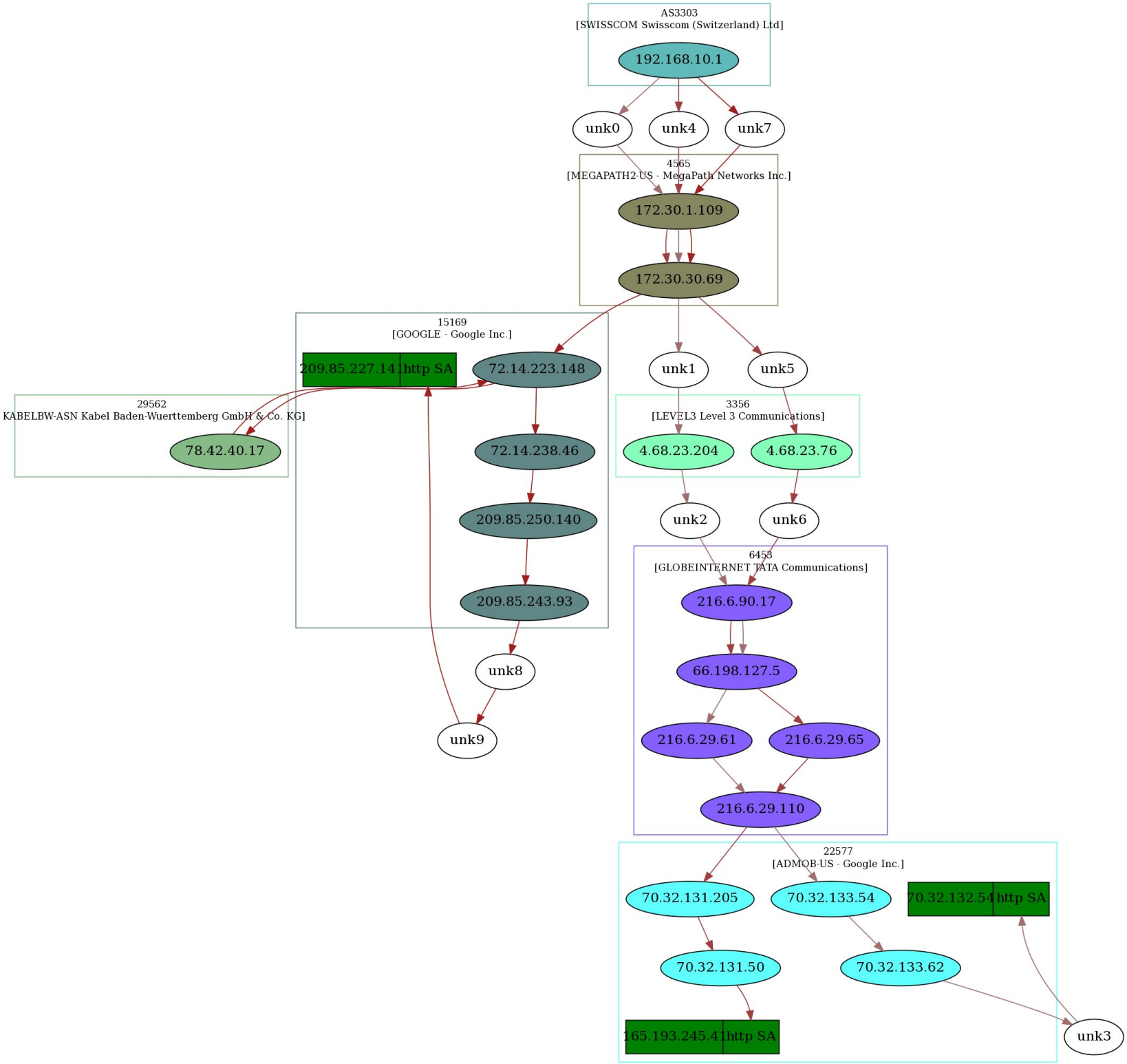
„There are only 2 ways to steal something: either you take it yourself or you have someone else take it and give it to you“

OSSTMM 3.0

Do you know your **trusts?**

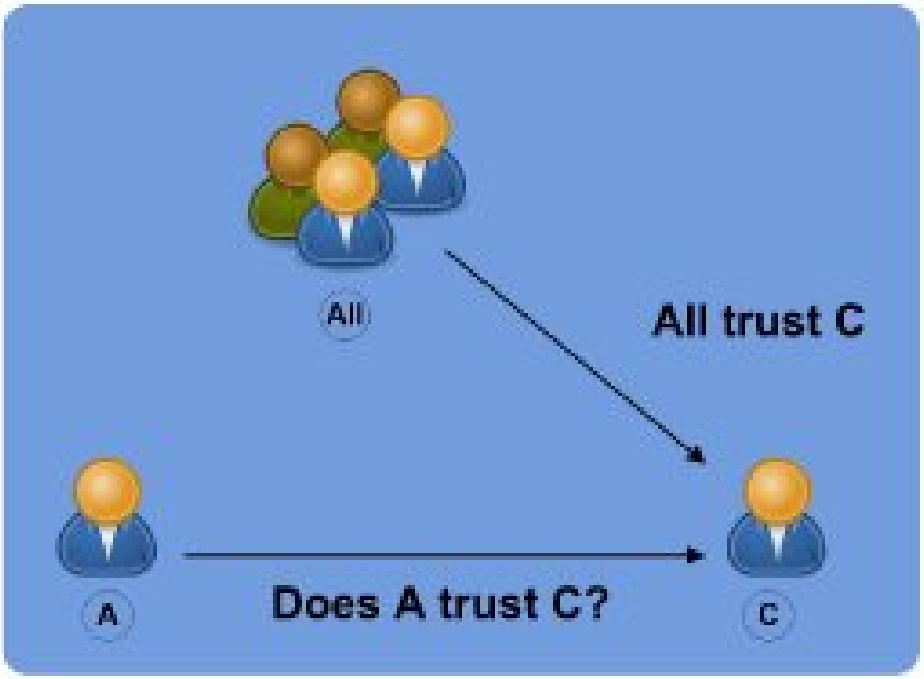


calling home?


AS3303
[SWISSCOM Swisscom (Switzerland) Ltd]
192.168.10.1
unk0
unk4
unk7
4565
[MEGAPATH2-US - MegaPath Networks Inc.]
172.30.1.109
172.30.30.69
15169
[GOOGLE - Google Inc.]
209.85.227.141 http SA
72.14.223.148
29562
KABELBW-ASN Kabel Baden-Wuerttemberg GmbH & Co. KG]
78.42.40.17
72.14.238.46
209.85.250.140
209.85.243.93
unk8
unk9
unk1
unk5
3356
[LEVEL3 Level 3 Communications]
4.68.23.204
4.68.23.76
unk2
unk6
6453
[GLOBEINTERNET TATA Communications]
216.6.90.17
66.198.127.5
216.6.29.61
216.6.29.65
216.6.29.110
22577
[ADMOB-US - Google Inc.]
70.32.131.205
70.32.133.54
70.32.132.54 http SA
70.32.131.50
70.32.133.62
165.193.245.41 http SA
unk3

Trust Properties!

- Trust is
  - no Emotion!
  - **a Decision!**
  - not quantifiable between humans!
- Wrong Trust Properties
- no Control = Blind Trust!



Quelle: OSSTMM ISECOM

Subjugation

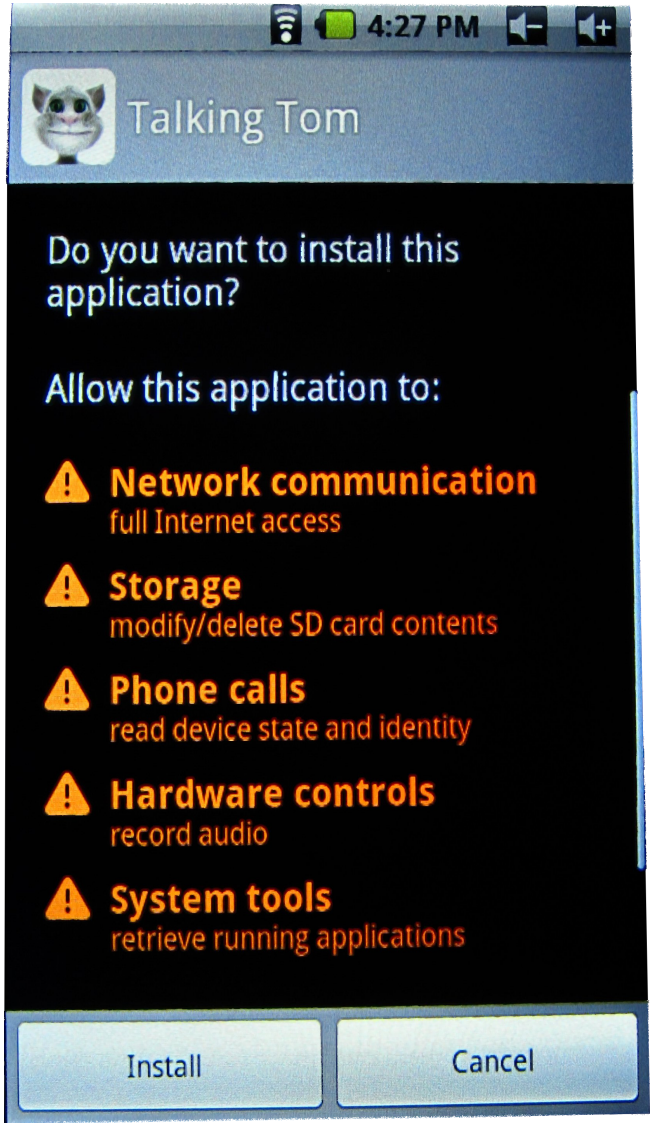
Size

Visibility

Value

Integrity

Porosity

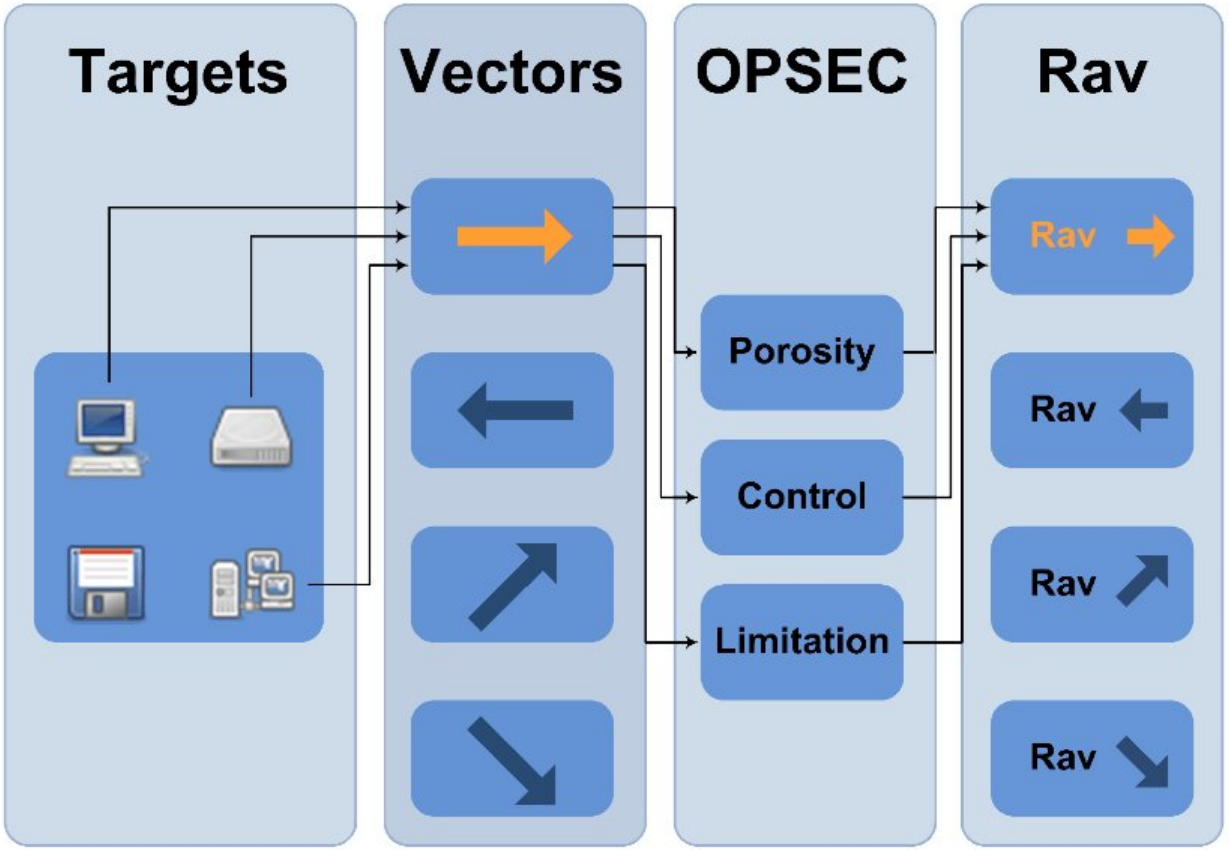


Symmetry

Offsets

Consistency

Components

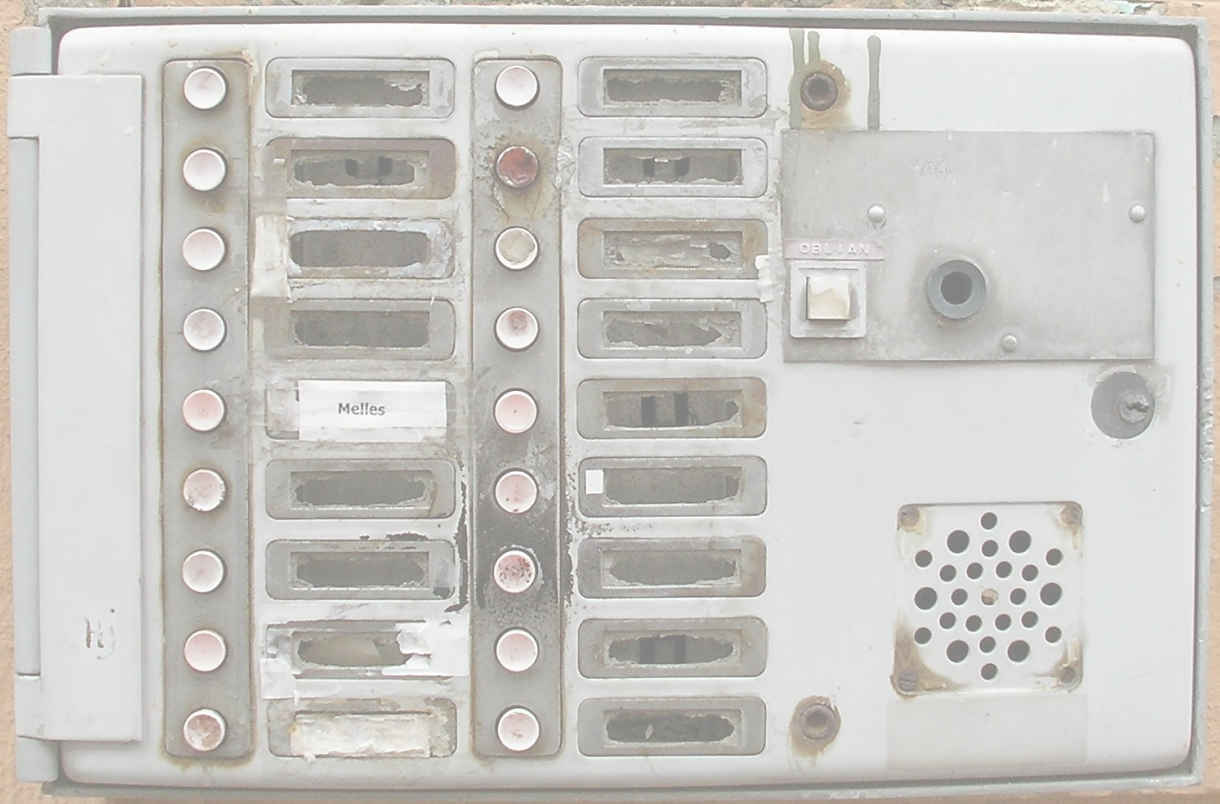


Quelle: OSSTMM ISECOM


- Visibility
- Access
- Trust
[porosity]
fedora


[controls]
CAUTION
CUIDADO
ATTENTION
Rubbermaid
Commercial Products

[limitations]

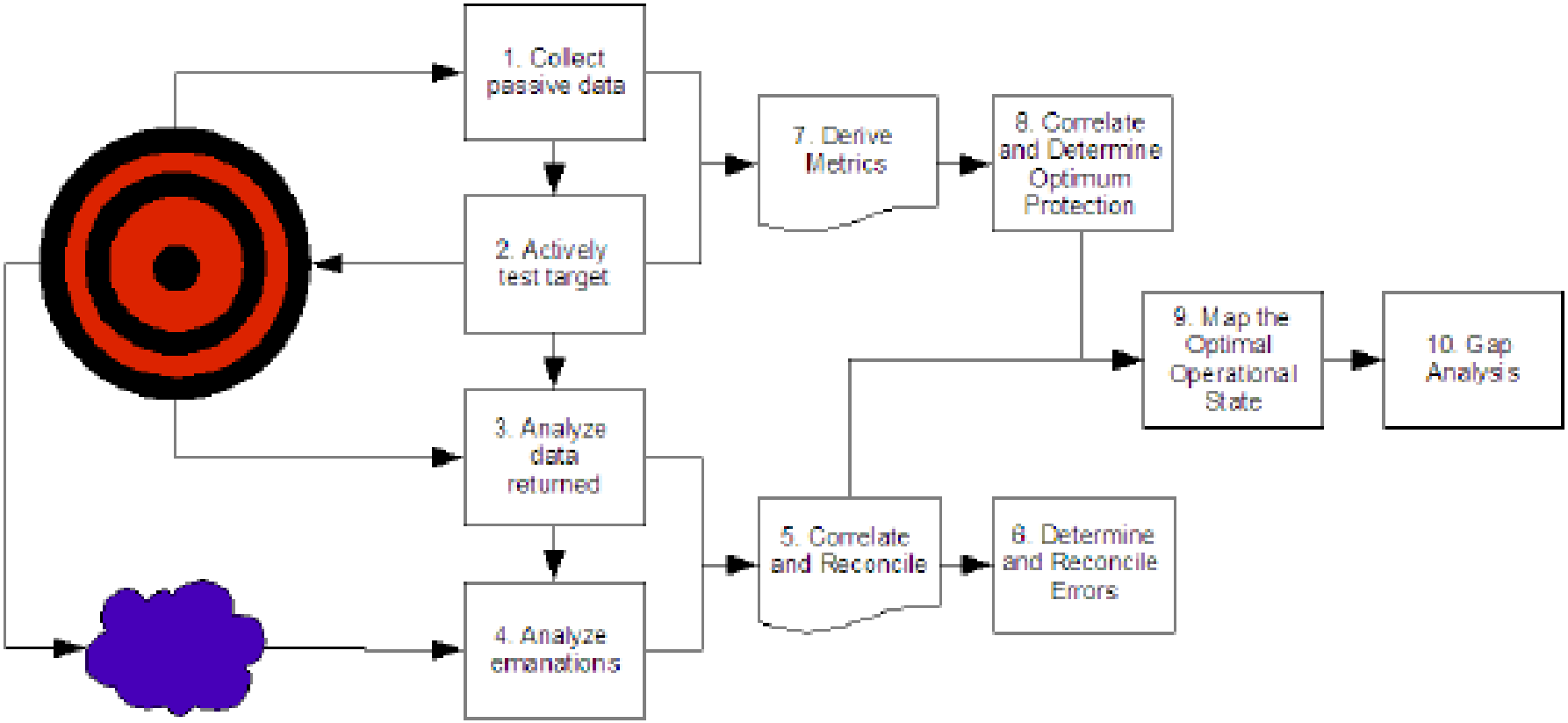


OSSTMM Risk Assessment Value

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

Quelle: OSSTMM ISECOM

[done properly?]



[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	

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

[benefits]

OSSTMM- Lab
based on
Fedora Security Lab

Packaging upstream
Tools from the OSSTMM Team

A stable platform
for teaching the curriculum

Integrate the Methodology Flow
Into one possible Toolset

[OSSTMM Lab]


Welcome to OSSTMM-Labv3.1b!
Boot
Boot (Basic Video)
Verify and Boot
Memory Test
Boot from local drive
Press [Tab] to edit options
OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual
ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES
Contemporary Security Testing and Analysis

[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	

fedora SECURITY LAB

{1} Active Tickets (78 matches)

- List all active tickets by priority.
- Color each row based on priority.
- If a ticket has been accepted, a '*' is appended after the owner's name

Edit report | Copy report | Delete report

Ticket	Summary	Component	Milestone	Type	Owner	Created
#109	Disable Automount, etc, by default	Security Spin	None	Packaging Request	jsimon *	11/30/10
#103	Instructions For Joining Project	Documentation	None	task		05/22/10
#104	create comps group for the security lab tools	Security Spin		enhancement	jsimon	06/01/10
#3	Request : airsnarf	Packaging	None	Packaging Request		01/15/10
#5	Request : autopsy	Packaging	None	Packaging Request		01/20/10
#9	Request : metasploit	Packaging	None	Packaging Request	sagarun *	01/20/10
#10	Request : tct	Packaging	None	Packaging Request		01/20/10
#12	Request : sdd	Packaging	None	Packaging Request		01/20/10
#17	Request : SiLK	Packaging	None	Packaging Request	linuxthomass	01/20/10
#18	Request : Bh (Beholder)	Packaging	None	Packaging Request		01/20/10
#19	Request : Distack	Packaging	None	Packaging Request	ankursinha *	01/20/10
#20	Request : Ttyrpld	Packaging	None	Packaging Request		01/20/10
#31	Request : ssd	Packaging	None	Packaging Request		02/21/10
#32	Request : pyrit	Packaging	None	Packaging Request		02/22/10
#35	Request : guymager	Packaging	None	Packaging Request		03/12/10
#36	Request : xmount	Packaging	None	Packaging Request	fab	03/12/10
#37	Request : WIDZ	Packaging	None	Packaging Request		03/16/10
#38	Request : gspoof	Packaging	None	Packaging Request		

The fedora security spin team

every Fedora Contributor!!!!

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