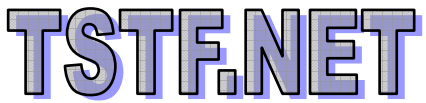
The End of Ethical Hacking

The truth about ethical hacking and penetration testing: a perspective from the OSSTMM

(a cura di **Raoul Chiesa – OPST, OPSA - @ Mediaservice.net srl**)
(e di **Fabrizio Sensibile – OPST, OPSA - @ Mediaservice.net srl**)

Raoul Chiesa

- ✓ Fondatore, Direttore Tecnico, @ **Mediaservice.net Srl**
- ✓ **O**SSTMM **P**ROFESSIONAL **S**ECURITY **T**ESTER **(OPSA)**
- ✓ **O**SSTMM **P**ROFESSIONAL **S**ECURITY **A**NALYST (**OPSA**)
- ✓ **Certified OSSTMM Trainer** (ISECOM's Train the Trainers 2002)
- ✓ OSSTMM **Key Contributor** (2.0, 2.1, 2.5, 3.0)
- ✓ ISECOM's **Director of Communications**
- ✓ Fondatore e Membro del Comitato Direttivo, **CLUSIT**
- ✓ Board of Directors Member, **OWASP Italia**
- ✓ Board of Directors Member, **ISECOM**
- ✓ Board of Directors Member, **TSTF.net**
- ✓ Referente **IDC EMEA** per eventi Security-related
- ✓ ...Ethical Hacker dal 1996



Fabrizio Sensibile

- ✓ **O**SSTMM **P**ROFESSIONAL **S**ECURITY **T**ESTER (**OPST**)
- ✓ **O**SSTMM **P**ROFESSIONAL **S**ECURITY **A**NALYST (**OPSA**)
- ✓ ISECOM Certified Trainer (ISECOM's Train the Trainers 2002, 2005)
- ✓ **H**acker **H**igh **S**chool **T**eacher – **HHST** -
- ✓ Ideatore sistemi di sicurezza ed accessi **ITN** (**I**SECOM **T**esting **N**etwork)
- ✓ **Responsabile** per i corsi di **formazione** erogati dalla @Mediaservice.net
- ✓ Security **Evaluator** and **Analyst** per @Mediaservice.net
- ✓ **Relatore** a conferenze di sensibilizzazione sul tema della **ICT security**
- ✓ Docenze **Master** sulla Sicurezza presso **Università degli Studi di Milano (DSI/CLUSIT)**
- ✓ Docenze **Master ICT Security TILS** L'Aquila
- ✓ Docenze **R**aggruppamento **O**perativo **S**peciale C.C. **(ROS)**
- ✓ Docenze **CLUSIT Educational**

Indice della Presentazione

- Breve introduzione all'Ethical Hacking
- Audit e Test, la ricerca del punto d'incontro
- The End of Ethical Hacking: insufficiente sul lungo termine
- Funzionamento di massima della metrica RAV
- Come si relazionano gli elementi del RAV
- Esempio di applicazione della metrica su un network basilare
- Riferimenti sitografici
- Q&A

Ethical Hacking, vita e morte

[Terminologie e “modi di dire” nel mercato ICT Security italiano]

- **1996 -1999**: **Test di intrusione/penetrazione, Ethical Hacking**
  In Italia si muovono i primi passi nel settore del pen-testing.
  Pochi ma buoni…

- **1999 - 2004**: **Vulnerability/Security Assessment, Test di vulnerabilità, *Security*Assessment, Super-Ethical-Hacking…di tutto un po’**
  Il chaos: nicchia di mercato a crescita esponenziale. Improvvisazione, terminologie errate nel pre-sale, mancanza di procedure ed esperienza nell’esecuzione della commesa, pen-tester “presi al volo” in esterno: falso senso di sicurezza, delusione: **processo incompleto**.

- **2001 – 2003**: **Penetration Testing, Ethical Hacking.**
  Aumenta la richiesta di chiarezza e garanzie da parte dei clienti: referenze, liberatorie, specialisti, trasparenza sui processi di security testing, riferimento a metodologie, training-on-the-job.

- **2004-2005**: **Certified Security Testing/Auditing**
  Nasce la voglia di unire gli standard e creare processi di valutazione a 360°: vengono applicate verifiche **teoriche** (ISO17799/BS7799, OCTAVE, COBIT, ISM3, CRAMM, etc..) **e pratiche** (OSSTMM, OWASP) internazionalmente riconosciute.

Perchè l'Ethical Hacking è morto ?

Durante 10 anni di professional pentesting e verifiche "sul campo" *, abbiamo osservato quanto segue:

- gli investimenti per l'ICT Security nelle aziende sono spesso erogati in maniera errata;
- le insicurezze rimangono, ma aumenta il "falso senso di sicurezza";
- le differenze tra quanto **teoricamente affermato** e quanto **verificato sul campo** sono, spesso, **abissali**;
- chi ne fa le spese è sempre **l'utilizzatore finale**;
- nonostante ciò, è sempre maggiore la richiesta di **certificazioni**, **bolli e rispetto degli standard (**nazionali ed internazionali).

❑ In una parola, "l'Ethical Hacking **muore quando è fine a sè stesso**" (Pete Herzog)

* *riferito a Penetration Testing, attacchi ad Ethical Hacking, OSSTMM Security Audit, OSSTMM Certified Security Testing verso: operatori di fonia (fissa e mobile), Banking, Finance, P.A., Sanità, Chemical, Industria, I.T. Vendor, xxSP (ISP, WISP, MSSP), System Integrator.*

In lutto, o a festa ?

- La “sicurezza” va di **moda**
- Tutte le aziende ICT (e non) hanno visto in questo settore notevoli opportunità di “**fare soldi**” (*business-oriented ONLY*)
- E’ quindi **molto difficile** individuare il giusto fornitore/partner
- Purtroppo il pressapochismo **regna sovrano**
- Di conseguenza, **urgono** regole chiare e trasparenti nell’erogazione dei servizi di verifica
- Come prima conseguenza, sta emergendo la forte necessità di **integrare** Risk Analysis - complesse ma “teoriche” – con azioni supportate da verifiche sul campo
- L’utilizzatore finale **conosce** le metodologie ed i processi, ma anche **le loro limitazioni**

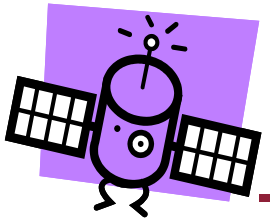
Unire la visione dell'auditor *CISA/CISM* all'approccio del tester *OPST/OPSA*

I servizi di Professional Security Analysis, oggi: alcune riflessioni

• Riuscire ad avere un **approccio a 360°** (Full Prospective View) con misurazioni dirette può **incrementare il mercato**, sposando le esigenze dei Clienti anche sul lungo periodo
• Rispondere alle richieste il cui punto focale risiede nelle parole: *Quanto sono sicuro e rispetto a cosa ?*
• OSSTMM propone un **metro di comparazione diretto** del livello di sicurezza degli asset ICT dell'azienda, da cui auditor e tester possono trarre vantaggio
• Premesse perfette per introdurre **nuovi concetti di security consulting**. (ripetibilità dei risultati di test, **valutazione oggettiva** del livello di sicurezza)
• La metrica dei R.A.V. può inoltre dar adito ad **un processo consulenziale** che preveda audit/test **periodici**, mantenendo così il livello di sicurezza **desiderato.**

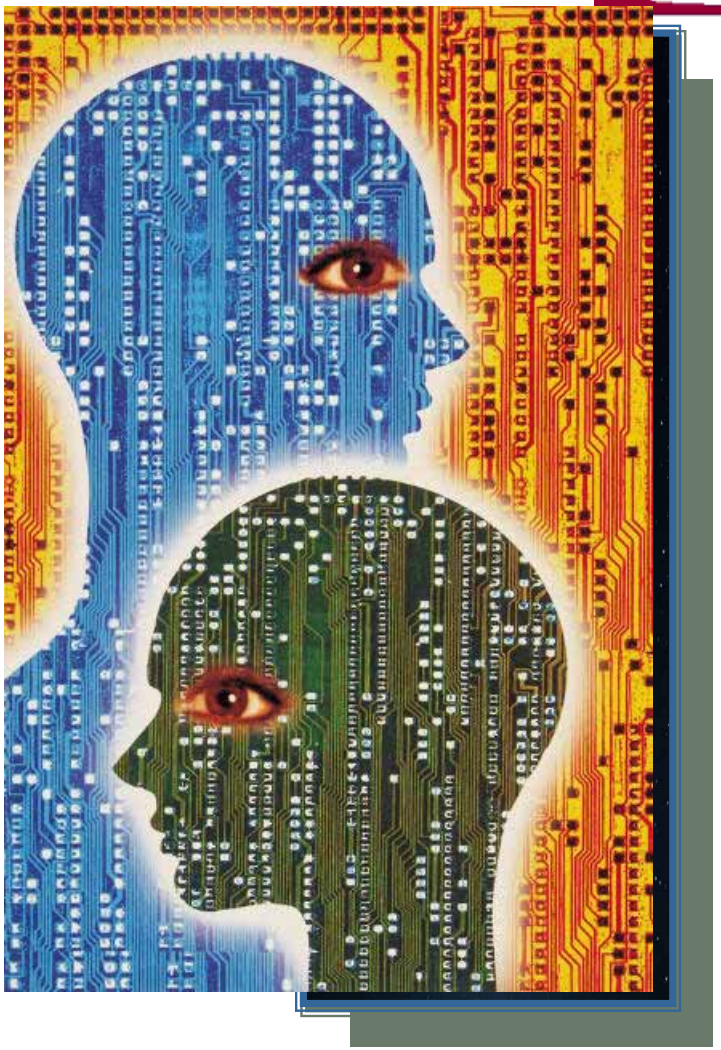
The End of Ethical Hacking

The Open Source Security Testing Methodology Manual (OSSTMM) is an **open standard methodology for performing security tests**. Since it's inception in **January 2001**, the OSSTMM has become the **most widely used, peer-reviewed, comprehensive security testing methodology in existence**. While other methodologies and best practices attack security testing from a 50,000 foot view, **the OSSTMM focuses on the technical details** of exactly **which items** need to be tested, **what to do** during a security test, and when **different types** of security tests **should be performed**. The OSSTMM provides testing methodologies for the following five security channels: **Personnel Security**, **Telecommunications Security**, **Wireless Communications Security**, **Data Networks Security**, and **Physical Security**.



or "How the OSSTMM gave me back control of my life."

HACKING IS AN ART

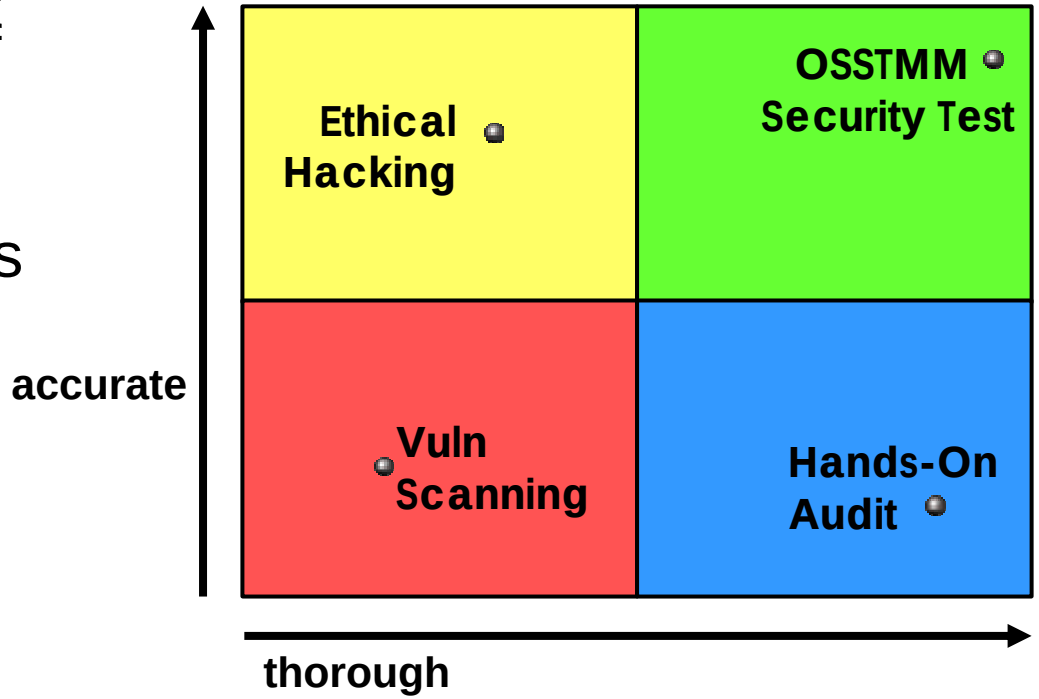


SECURITY TESTING IS A SCIENCE


ISACA
Roma
KNOWLEDGE +
PERSISTENCE =
PROFESSIONAL
SECURITY
TEST

What kinds of tests do you really need?

- A security test should be a measurement of configurations, legal compliancy, and operational processes in action.
- **Qualitative**: A dead network is a secure network.
- **Quantitative**: A little used network is a more secure network.

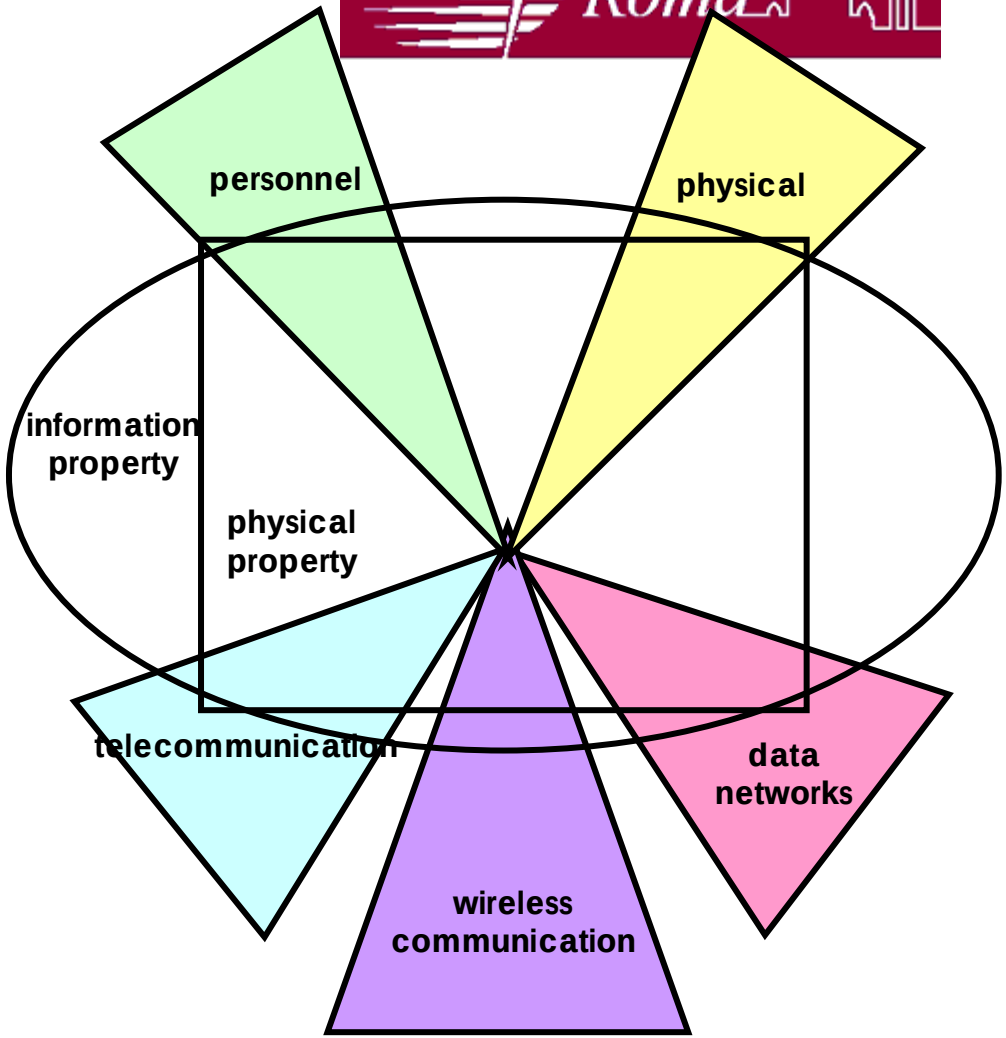


Security Is No. 2.

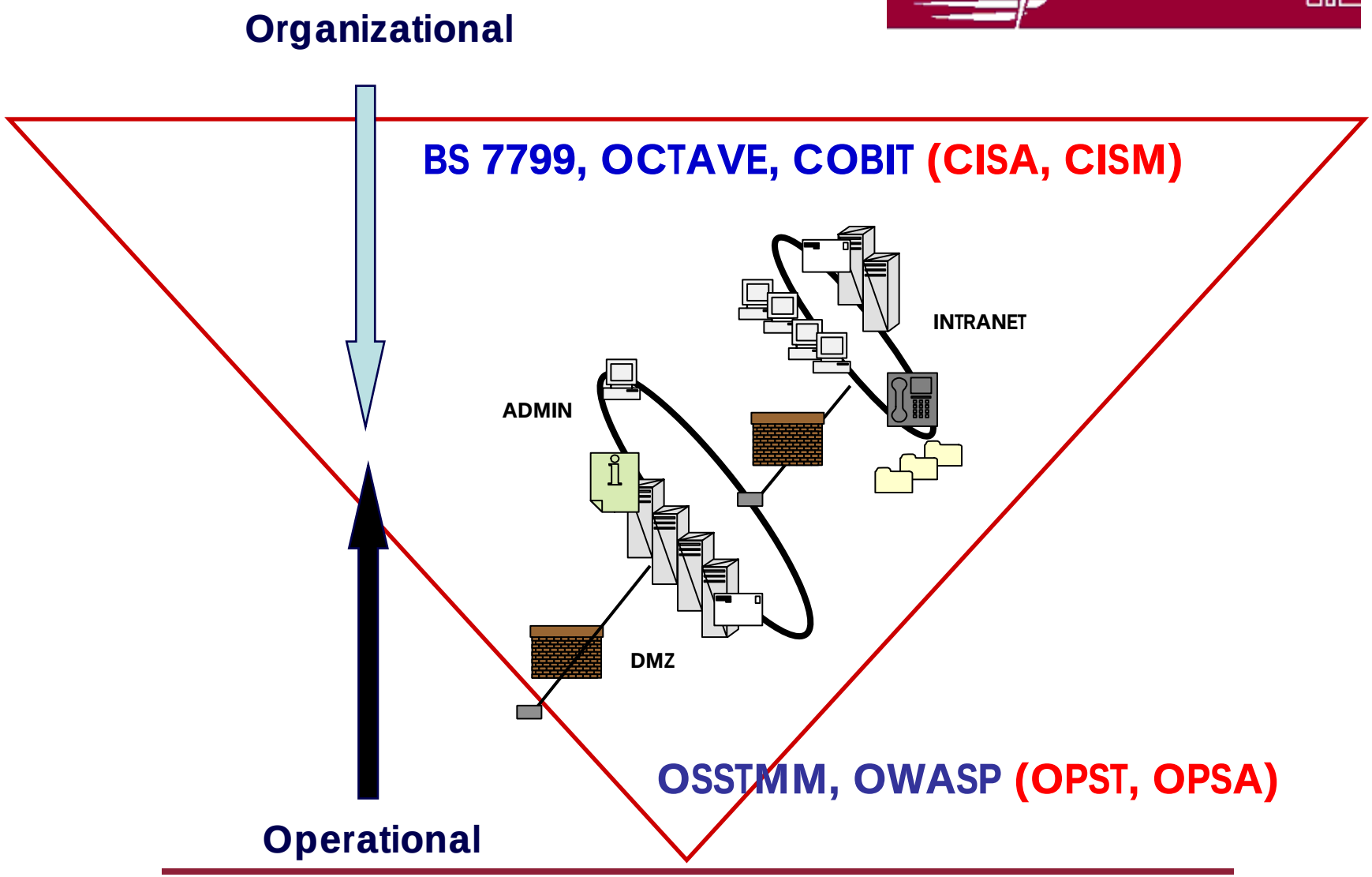
- Why are you in business?
- Is security your business?
- If not, what are you protecting?
  - Can you count it?
  - Does it have value?
- Why do you have computers at all in your shop?
  - Increase Productivity
  - Increase Efficiency
  - Lower Costs

All-Access Channels

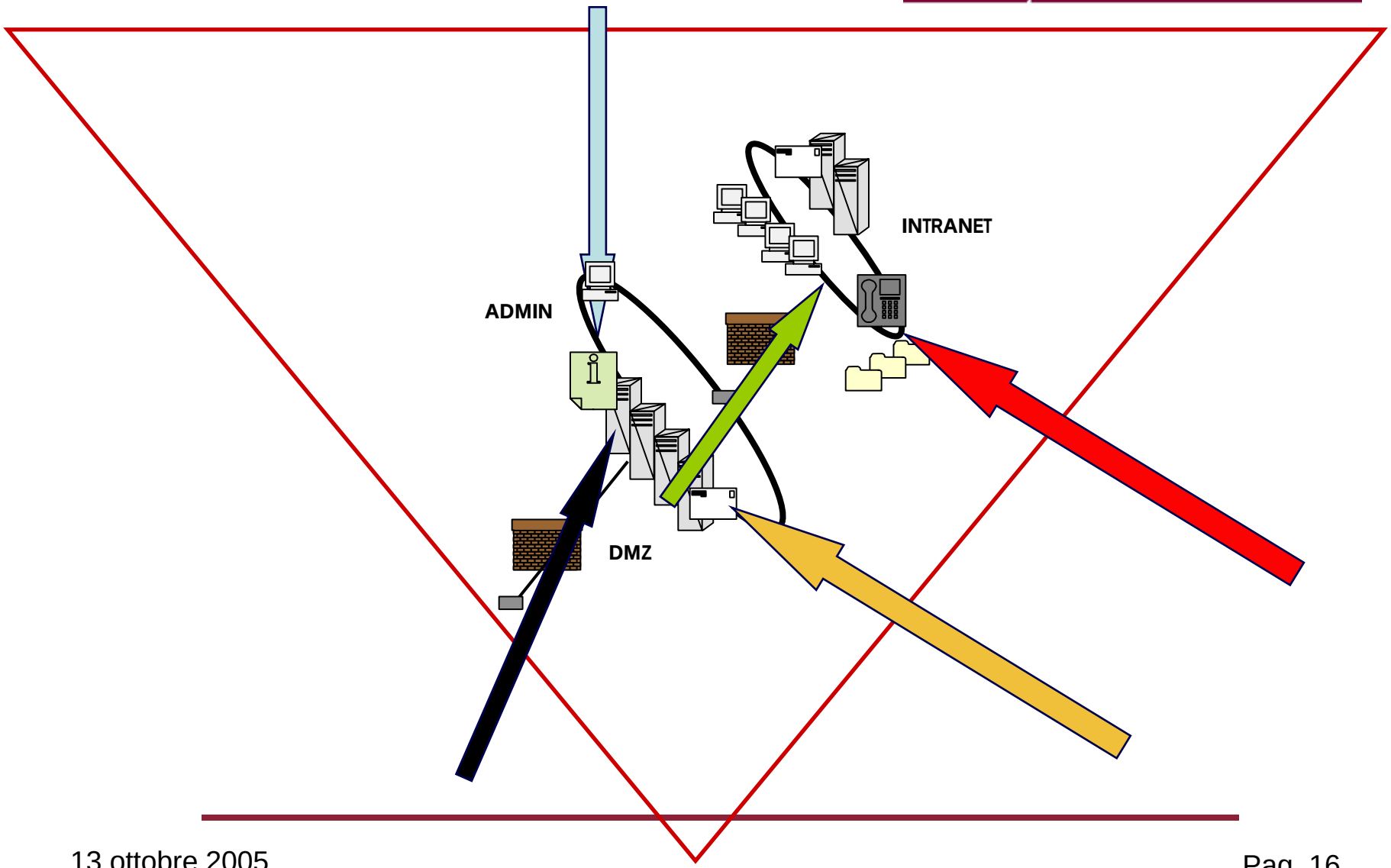
- Paths to physical or intellectual property
- Contains test methodologies for thorough security tests called MODULES
  - Guides Expected Results in the form of an “ISO” type audit report
- All make up a thorough security test from sidewalk to kernel



Combine the views



Getting Perspective



So How Does It Work?

- Figure out all the desired qualities you want in and about an operation.
- Count up the factual data points derived from how something works while it's working.
- Make sure that the facts are weighted only according to the scope and operational requirements.

- Compute it - it's like a hash of all the factual points of how something works.
- Now that hash can be compared in part or in whole to other hashes from other measurements based on that same methodology.
- Even a partially "same" measurement is pretty good.

Operational Security

1. Visibility
   - Opportunity. What is there?
2. Trust
   - Unauthenticated privileges for service interactions.
3. Access
   - Interactions.

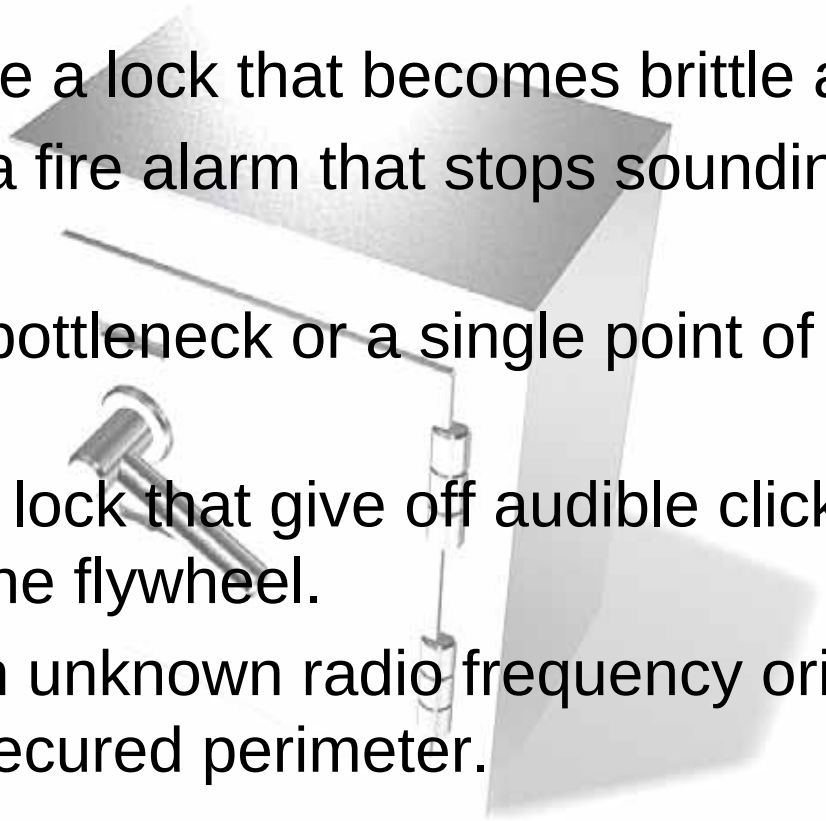
Loss Controls (1 - 5)

- **Authentication**: requirements for access
- **Repudiation**: non-deniability of access and applied interactions
- **Confidentiality**: the information communicated is protected
- **Privacy**: the process for communication is protected
- **Indemnification**: the information is protected through legal warnings and/or insurance

Loss Controls (6 - 10)

- **Integrity**: The information cannot be changed without all parties involved being aware of the change.
- **Safety**: The protection processes cannot halt interactions or deny protection upon failure.
- **Usability**: Where protection is interactive with the user, decisions of the protection process do not require the immediate action of the user.
- **Survivability**: The services do not halt interactions or deny intended services upon failure.
- **Alarm**: This is the timely and appropriate notification of activities that violate or attempt to violate any of the Loss Controls or attempt unwarranted access.

Actual Security



- **Vulnerability** like a lock that becomes brittle at -3C
- **Weakness** like a fire alarm that stops sounding after 3 seconds
- **Concern** like a bottleneck or a single point of failure in the network.
- **Exposure** like a lock that give off audible clicks when the cogs catch the flywheel.
- **Anomaly** like an unknown radio frequency originating from with your secured perimeter.

Math approach I

The **RAV** equation requires that each of the categories be assigned a base number,

OpSecbase the percentage of the scope protected by security measures
LCbase the percentage of the scope protected by loss controls
ActSecbase how much risk the problems cause

The following equations are used to calculate the first two base numbers, with all Sum variables as simple sums of constituent inputs from the table above:

$$OpSECbase = 100 - \left(\frac{OpSECsum}{Scope + OpSECsum} \right)$$

$$LCbase = Scope \times \left(\frac{LCsum \times 0{,}1}{Scope + OpSECsum} \right)$$

Math approach II

Actual Security is calculated based on values that distinguishes between:

Identified problem (through an interview, automated scan, or based on configuration)
Verified problem (one that has been manually verified by the auditor).

The following value table is used to calculate the **ActSecSum** variable, as an **intermediate step** between the **Actual Security** inputs and the **ActSecbase** variable, which is the Actual Security basic input for the RAV equation.

Input	Verified Value	Identified Value
Vulnerabilities	[(100 - $OPSec_{base}$) / LC_{base}] 100	(Verified Vulnerability Value) 2
Weaknesses	(Verified Vulnerability Value) 2	(Verified Vulnerability Value) 3
Concerns	(Verified Vulnerability Value) 3	(Verified Vulnerability Value) 4
Exposures	(Verified Vulnerability Value) 4	(Verified Vulnerability Value) 5
Anomalies	(Verified Vulnerability Value) 5	(Verified Vulnerability Value) 6

Math approach III

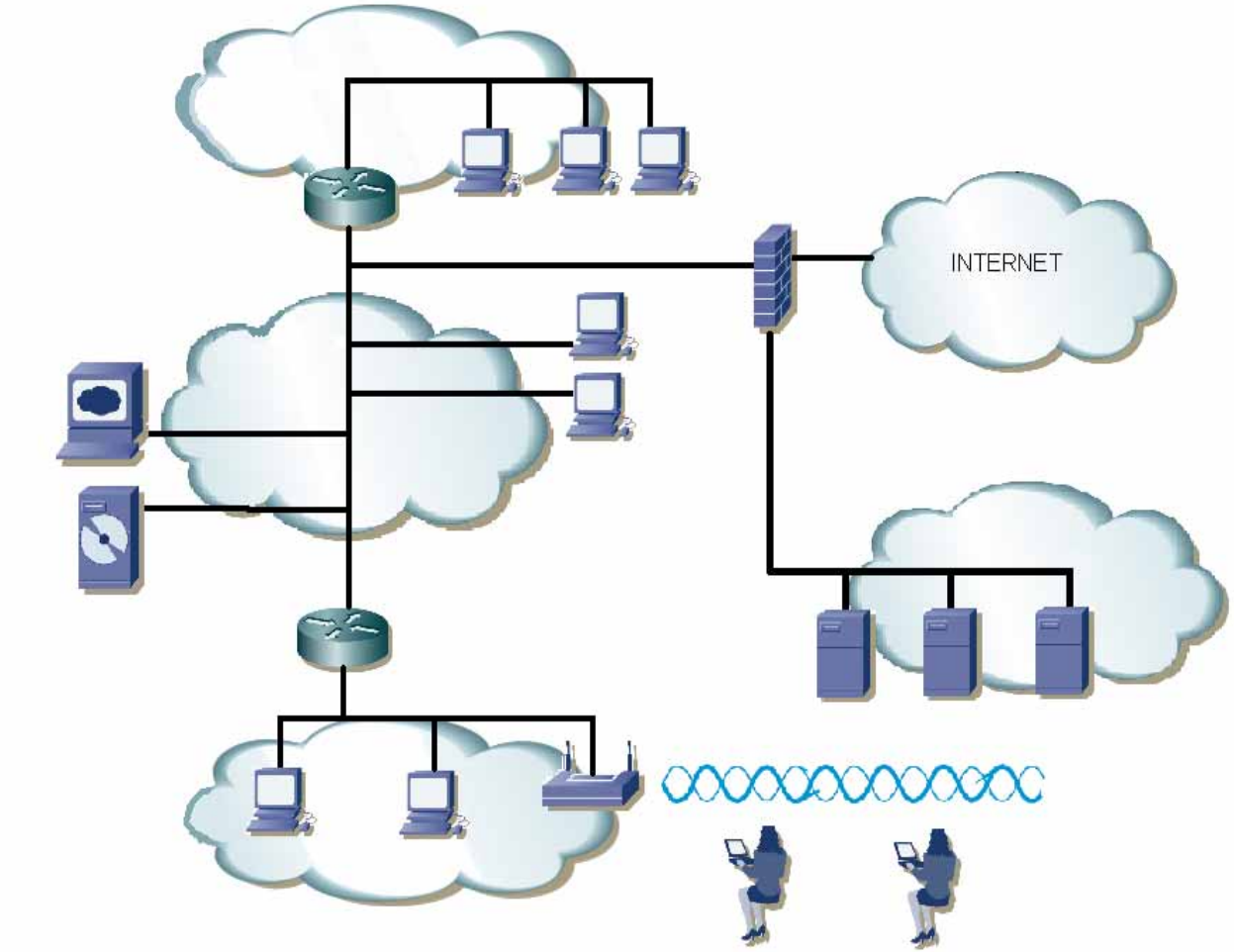
ActSecSum is then calculated as a valued average of each input multiplied by its corresponding Value. The base equation is then:

$$ActSECbase = \frac{ActSECsum}{Scope}$$

The corresponding RAV calculation is:
There is an important distinction between the base and Sum numbers, so always make sure to use the correct variable.

$$RAV = OpSECbase - \left[\frac{(ActSECbase - OpSECbase)}{100}\right] + \left[\frac{OpSECsum}{(Scope + OpSECsum)} \times \frac{LCbase}{100}\right]$$

A Network Security Story (in Pictures)



How We Found It...

Scope		Loss Controls	
Scope	15	Authentication	12
		Non-Repudiation	3
Operational Security		Confidentiality	10
Visibility	13	Privacy	0
Access	27	Indemnification	2
Trust	2	Integrity	0
Op Sec Δ	-42	Safety	0
Op Sec Total	42	Usability	4
Op Sec % of Scope	97,2	Continuity	13
		Alarm	40
		Loss Controls Δ	8,4
		Loss Controls Total	84
		Loss Controls % of Op Sec	20
		Loss Controls % of Scope	56

Security Limitations Values

	Verified	Identified
Vulnerability	0,57575758	0,58168101
Weakness	0,56983414	0,57569664
Concern	0,56397165	0,56977383
Exposure	0,55816948	0,56391196
Anomaly	0,55242699	0,55811040

Original Actual Security...

	verified	identified	total
Vulnerabilities	9	4	7,508542212
Weaknesses	4	12	9,187696197
Concerns	0	3	1,709321491
Exposures	138	0	77,02738758
Anomalies	0	0	0
		Security Limitations Δ:	95,43294748
		Security Limitations Total:	6,36219650
		Actual Delta:	-129,03294748
		Actual Security:	99,60037804

After V.S. and Patching

Security Limitations Values

	Verified	Identified
Vulnerability	0,57575758	0,58168101
Weakness	0,56983414	0,57569664
Concern	0,56397165	0,56977383
Exposure	0,55816948	0,56391196
Anomaly	0,55242699	0,55811040

	verified	identified	total
Vulnerabilities	0	0	0
Weaknesses	0	0	0
Concerns	0	0	0
Exposures	0	0	0
Anomalies	0	0	0
		Security Limitations Δ:	0,00000000
		Security Limitations Total:	0,00000000
		Actual Delta:	-33,60000000
		Actual Security:	99,66400000

Effectiveness of Patching

	verified	identified	total
Vulnerabilities	9	4	7,508542212
Weaknesses	4	12	9,187696197
Concerns	0	3	1,709321491
Exposures	138	0	77,02738758
Anomalies	0	0	0
		Security Limitations Δ:	95,43294748
		Security Limitations Total:	6,36219650
		Actual Delta:	-129,03294748
		Actual Security:	99,60037804

ORIGINAL

Security Limitations Values

	Verified	Identified
Vulnerability	0,57575758	0,58168101
Weakness	0,56983414	0,57569664
Concern	0,56397165	0,56977383
Exposure	0,55816948	0,56391196
Anomaly	0,55242699	0,55811040

	verified	identified	total
Vulnerabilities	0	0	0
Weaknesses	0	0	0
Concerns	0	0	0
Exposures	0	0	0
Anomalies	0	0	0
		Security Limitations Δ:	0,00000000
		Security Limitations Total:	0,00000000
		Actual Delta:	-33,60000000
		Actual Security:	99,66400000

PATCHED

IT Sec Budget: 50.000€

RAV Diff: 0,06362196

Patch Value: 3.181,10 €

If you spent 10% of your IT budget on patching, then you spent 5000€ on something that figuratively should have cost around 3200€ based on its value. That means you should re-analyze your security spending processes and priorities.

Now Adjust Operations...

Original:

- **Visibility: 13**
- **Access: 27**
- **Trust: 2**
- **Delta. 42**
- **Total: 42**
- **Op Sec %: 97,2**

Scope			Loss Controls
Scope	15	Authentication	5
		Non-Repudiation	5
Operational Security		Confidentiality	5
Visibility	3	Privacy	0
Access	5	Indemnification	5
Trust	0	Integrity	5
Op Sec Δ	-8	Safety	0
Op Sec Total	8	Usability	5
Op Sec % of Scope	99,46666667	Continuity	15
		Alarm	15
		Loss Controls Δ	6
		Loss Controls Total	60
		Loss Controls % of Op Sec	75
		Loss Controls % of Scope	40

Security Limitations Values

	Verified	Identified
Vulnerability	0,30666667	0,30974978
Weakness	0,30358356	0,30663567
Concern	0,30053144	0,30355287
Exposure	0,29751001	0,30050107
Anomaly	0,29451896	0,29747994

Op Sec improved

by 2,27% (1135€)

Not Vuln Scan and Patch

Original:

Actual Delta:	-129,03294748
Actual Security:	99,60037804

and with new

operational adjustments:

Differences:

Op Fix: 0,34571529

Patch: 0,06362196

Diff: 0,28209333

Security Limitations Values

	Verified	Identified
Vulnerability	0,30666667	0,30974978
Weakness	0,30358356	0,30663567
Concern	0,30053144	0,30355287
Exposure	0,29751001	0,30050107
Anomaly	0,29451896	0,29747994

	verified	identified	total
Vulnerabilities	9	4	3,998999106
Weaknesses	4	12	4,89396227
Concerns	0	3	0,910658616
Exposures	138	0	41,056382
Anomalies	0	0	0

Security Limitations Δ:	50,86000200
Security Limitations Total:	3,39066680

Actual Delta:	-52,86000200
Actual Security:	99,94609333

Now Op Fix + Patching

Original:

Actual Delta:	-129,03294748
Actual Security:	99,60037804

and with Op fix

and Patching:

Differences:

New: 99,98%

Orig: 99,6003780%

Diff: 0,37962196%

Security Limitations Values

	Verified	Identified
Vulnerability	0,30666667	0,30974978
Weakness	0,30358356	0,30663567
Concern	0,30053144	0,30355287
Exposure	0,29751001	0,30050107
Anomaly	0,29451896	0,29747994

	verified	identified	total
Vulnerabilities	0	0	0
Weaknesses	0	0	0
Concerns	0	0	0
Exposures	0	0	0
Anomalies	0	0	0
		Security Limitations Δ:	0,00000000
		Security Limitations Total:	0,00000000

Actual Delta:	-2,00000000
Actual Security:	99,98000000

And We Quantify....

Security Limitations Values

	Verified	Identified
Vulnerability	0.30666667	0.30974978
Weakness	0.30358056	0.30663567
Concern	0.30053144	0.30355287
Exposure	0.29751001	0.30050107
Anomaly	0.29451896	0.29747994

	verified	identified	total
Vulnerabilities	0	0	0
Weaknesses	0	0	0
Concerns	0	0	0
Exposures	0	0	0
Anomalies	0	0	0
		Security Limitations Δ:	0.00000000
		Security Limitations Total:	0.00000000
		Actual Delta:	-2.00000000
		Actual Security:	99.98000000

IT Sec Budget: 50.000€

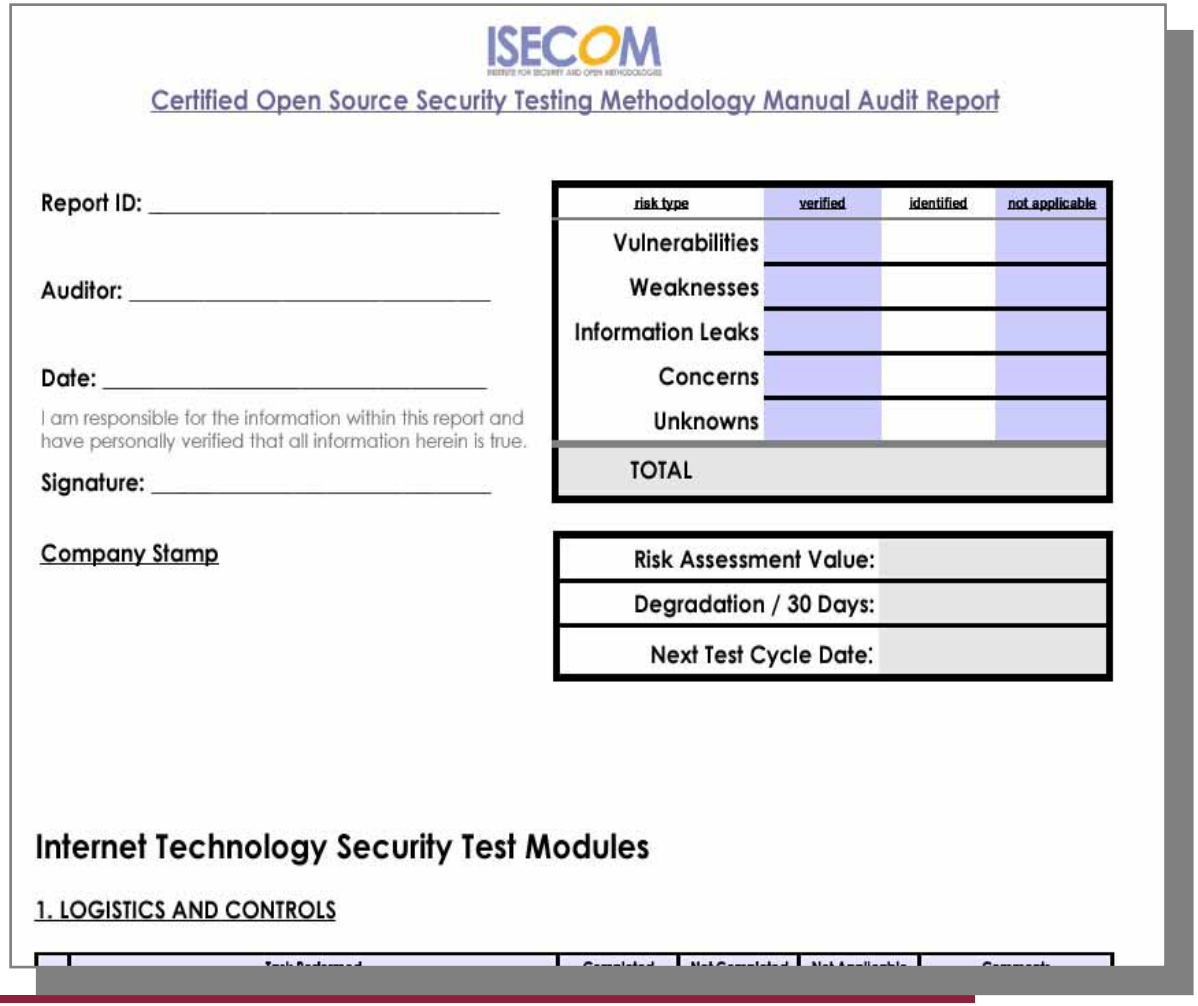
RAV Improvement: 0,37962196

Full Value: 18.981,10€

Total cost to improve the security of your infrastructure from where it was at 99,60% to the improved operational level of 99,98% should cost you about 38% of your budget at 18.981,10€.

Bye Bye E.H. and Hello OSSTMM Reports:

- The report must be:
  - Readable
  - Realistic
  - Practical
  - Accountable
  - Countable
  - Measurable
  - Schedulable



ISECOM

Certified Open Source Security Testing Methodology Manual Audit Report

Report ID: _____

Auditor: _____

Date: _____

I am responsible for the information within this report and have personally verified that all information herein is true.

Signature: _____

Company Stamp

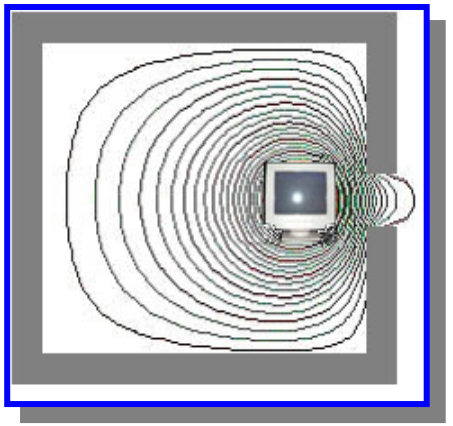
risk type	verified	identified	not applicable
Vulnerabilities			
Weaknesses			
Information Leaks			
Concerns			
Unknowns			
TOTAL			

Risk Assessment Value:	
Degradation / 30 Days:	
Next Test Cycle Date:	

Internet Technology Security Test Modules

1. LOGISTICS AND CONTROLS

Coming OSSTMM Advancements



- **SPECTRUM** - full spectrum tests
- **FACTS** - Discovering new tests with new fact points
- **PERFECT SECURITY** - further development on this as gap analysis and development of "BS7799 from OSSTMM" audits.
- **INTEGRITY** - test for fraud, money laundering, and business integrity lapses the OSSTMM way complete with metrics.
- **SAFETY** - integrating safety tests and metrics for things like EM levels and air quality.

And what do you do now?

- Operate purely on the application of security within an organization
- Provide CFOs fine-grained procurement control in-line with compliancy
- Practical Controlling Framework for CIO's to maintain a measurable level of risk
- Provide the ability to control security risk objectives with consistency and detail
- Allows for controlled security spending
- Peace through security

Get OSSTMM able

- **OSSTMM Professional Security Analysts**
  - Can analyze test reports and sum up security weaknesses.
  - Are walk-the-walk security personnel who are practical and resourceful.

- **OSSTMM Professional Security Tester**
  - Can perform OSSTMM tests and verify both positives and negatives.
  - Are go-to security personnel who learn at a packet level where even expensive scanning tools can't go.

OPST Certification

- **OSSTMM Professional Security Tester**
  - Turns operations into factual data points.
  - Maintains ethics as provided in the OSSTMM Rules of Engagement to assure no-bull security truth.
  - Knows what to test on the network, why it needs to be tested, and where it needs to be tested from.
  - Knows how to use the right tools for the job.
  - Can penetrate networks and verify vulnerabilities.
  - Is efficient and resourceful.

OPSA Certification

- **OSSTMM Professional Security Analyst**
  - Turns factual data points into intelligence.
  - Knows how to properly analyze a security presence.
  - Knows how to calculate security metrics.
  - Knows how to plan security audit and management projects.
  - Knows how to harmonize the OSSTMM with currently used methodologies such as BS 7799 or OCTAVE
  - Knows how to know if an outsourced security, penetration, or vulnerability test was done right.

Now that we have all this useful information, it would be nice to do something with it. (Actually, it can be emotionally fulfilling just to get the information. This is usually only true, however, if you have the social life of a kumquat.)

Unix Programmer's Manual.

MORE INFO:

Web resources:

www.isecom.org

www.osstmm.org

osstmm.mediaservice.net

Mail contacts:

training@mediaservice.net

raoul.chiesa@mediaservice.net

fabrizio.sensibile@mediaservice.net