# Séminaire Confiance Numérique

# Audit et Test de Sécurité des Systèmes d'Information

Florent Autréau -
florent@mataru.com / florent.autreau@imag.fr
7 mai 2015

# Objectives

- Introduction to Standards, Methods and Tools used to assess Security of Information System
- “CookBook”/ Recipes to conduct Security Audit

# What is a Security Audit ?
# For what Purpose ?

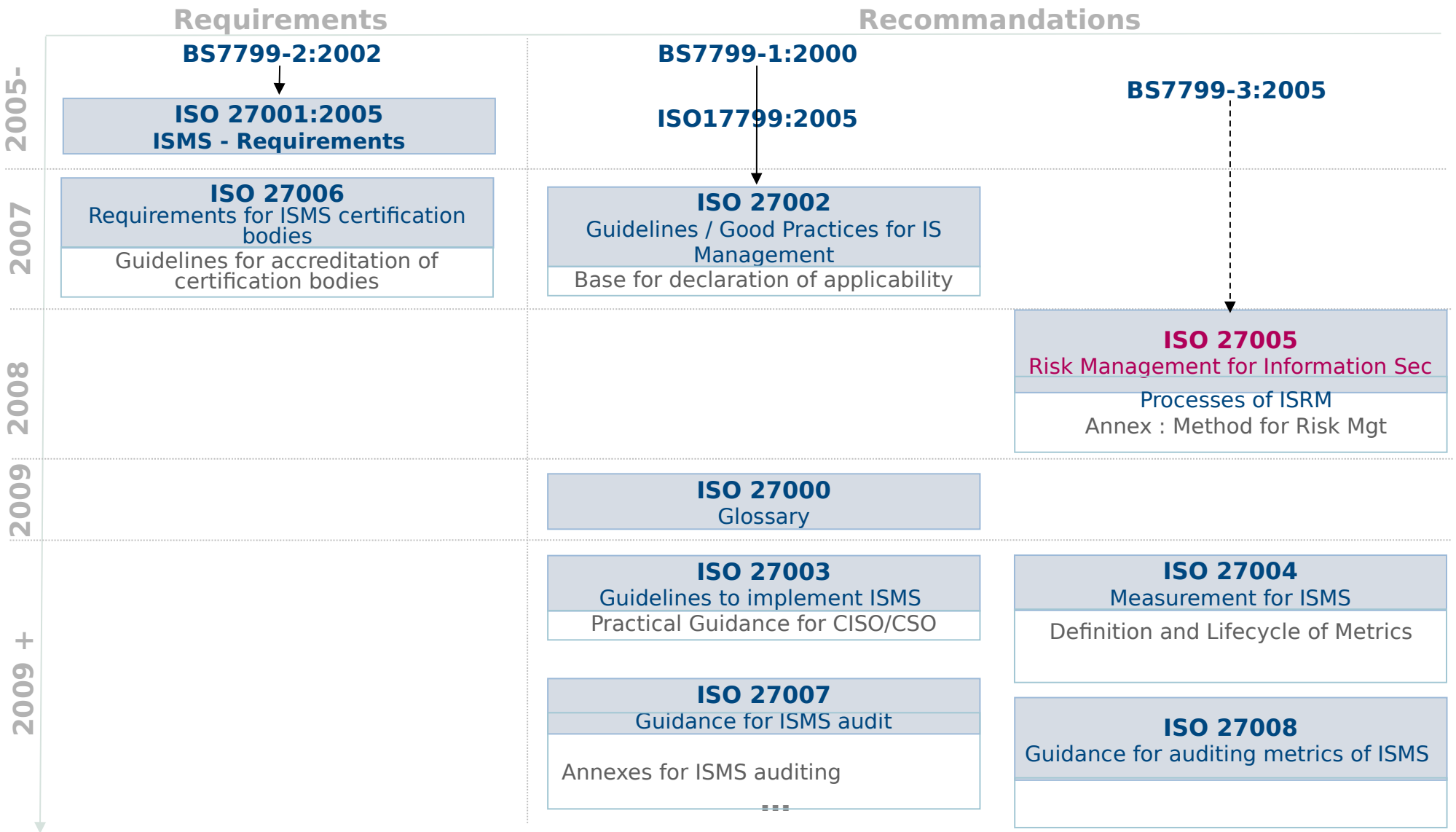
# Information Security Audit

- Audit :
  - Risk Assessment
  - Assessment and Evaluation of conformance with security policy and set of security rules.
- Reference : Set of rules defining organization, procedure and/or technology to ensure information security.

| Identification | Désignation | Source |
|---|---|---|
| EBIOS | Méthode | ANSSI |
| MEHARI | Méthode | CLUSIF |
| OCTAVE | Méthode | CERT |
| PSSI | Guide Méthodologique | ANSSI |
| TDBSSI | Guide Méthodologique | ANSSI |
| RMF | Guide Méthodologique | NIST |
| SP800-60 | Guide Méthodologique | NIST |
| ITIL | Guide de bonnes pratiques | OGC – BSI |
| COBIT | Guide de bonnes pratiques | ISACA |
| ITSEC | Norme d'exigences | UE – ANSSI |
| ISO 15408 | Norme d'exigences | ISO |
| NF Z 42-013 | Norme d'exigences | AFNOR |
| ISO 2700x | Norme de bonnes pratiques | ISO |
| PP nc / 0XX | Guide Technique | ANSSI |
| SP800-45 | Guide Technique | NIST |

- ANSSI :
  - www.ssi.gouv.fr
- CERT :
  - www.cert.org
- NIST :
  - csrc.nist.gov
- CNRS :
  - www.sg.cnrs.fr/fsd
- ISACA :
  - www.isaca.org
- ITIL :
  - www.itil.co.uk
- ISF :
  - www.securityforum.fr

# Standards for ISMS
# (Information Security Management System)




Antoine Rojat / Florent Autréau


DOGBERT IS CHAIRING THE INTERNATIONAL DATA SECURITY STANDARDS GROUP.
THE GOAL OF OUR ORGANIZATION IS TO MAKE YOUR SECURITY PROCEDURES SO INCONVENIENT THAT YOU GIVE UP HOPE AND DIE FROM BED SORES.
WE TAKE PRIDE IN BEING INDEPENDENT FROM THE COMPANIES THAT FUND US.
Dilbert.com DilbertCartoonist@gmail.com
8-1-11 © 2011 Scott Adams, Inc./Dist. by Universal Uclick

# Why assessing Information Security ?

- Evaluate and validate security practices ( control, quality processes );
- Validate procedures to alert, react and handle incident or disaster;
- Detect “forgotten/ignored” stakes or weaknesses;
- Educate users, management, employees to Information Security and Risk Management.

# The good questions

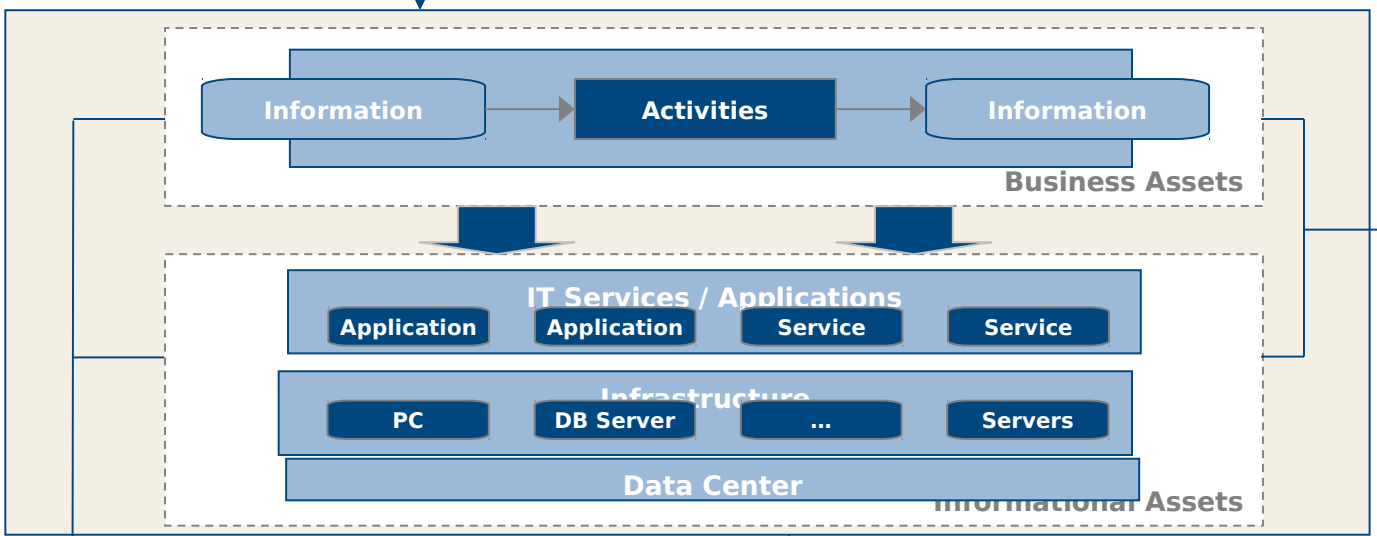
- What are the assets ?
- What are the threats ?
- What are the vulnerabilities ?
- What could be the impact/cost ?
- What are the strategies to handle the risk ?

# Risk Analysis - Terminology

- **Threat** :
  - what from you want protect valuable assets
  - anything (man made or act of nature) that has the potential to cause harm ( a.k.a Menace )
- **Vulnerability** :
  - Failure or Deviation of the Information System
  - weakness that could be used to endanger or cause harm to an informational asset
- **Risk** :
  - when Threat exploits Vulnerability against Valuable Asset
  - Probability that event will happen with a negative impact to an informational asset

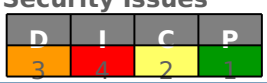
# ISO 27005 – Risk Analysis

- Definition of *evaluation criteria*
- Definition of *acceptance criteria*




- Identification of *Threats*
- Mapping of *existing measures*
- Identification of *Vulnerabilities*

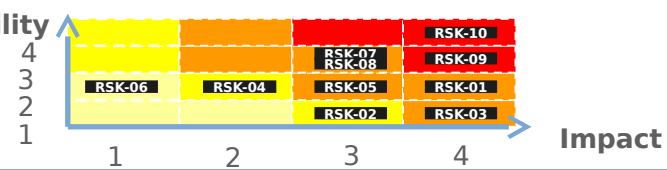
- Classification of Security Issues




- Identification of *risk scenarios*

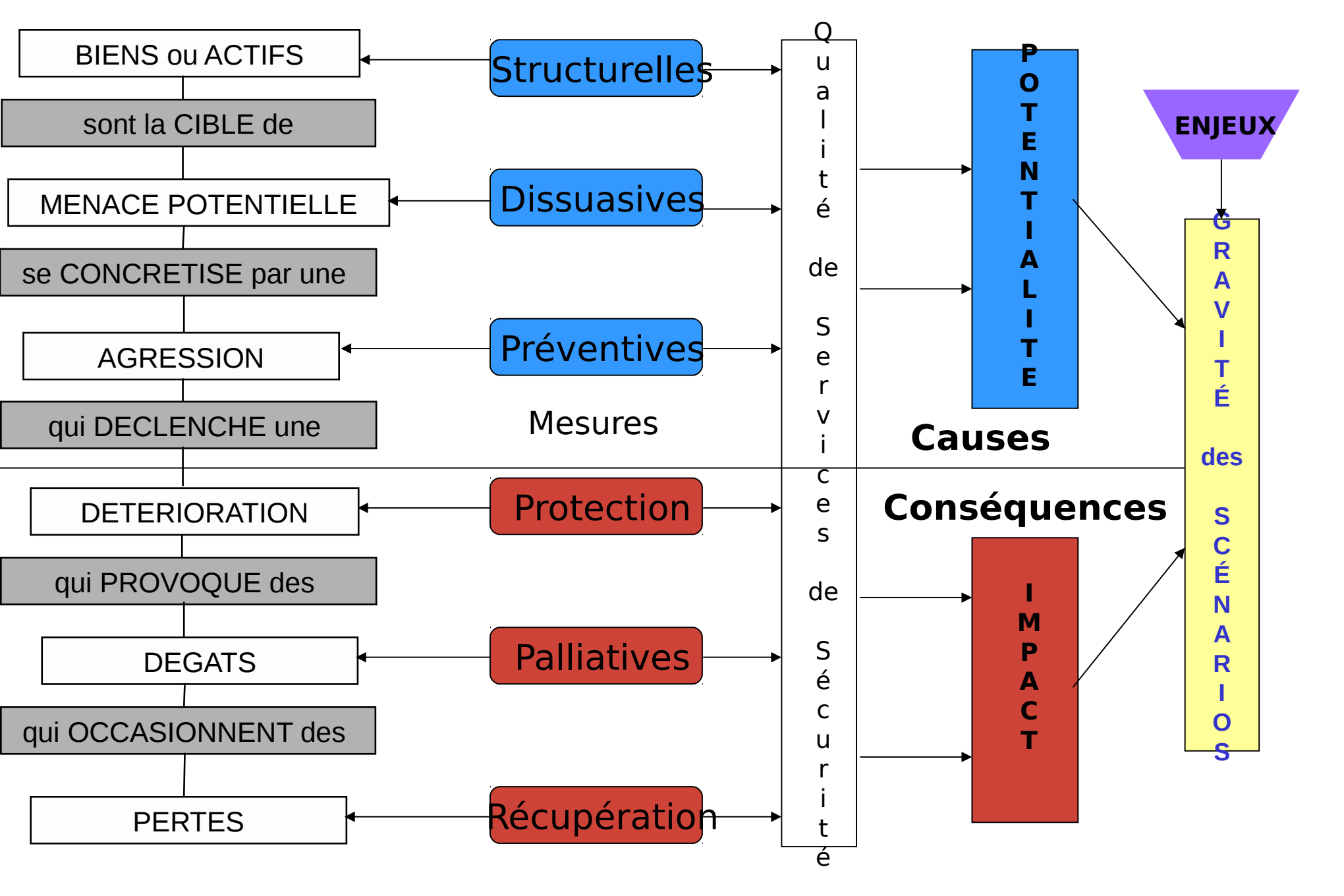
- *Classification of risk scenarios (Impact, Potentiality)*

- *Evaluation* of risk scenarios



# MEHARI

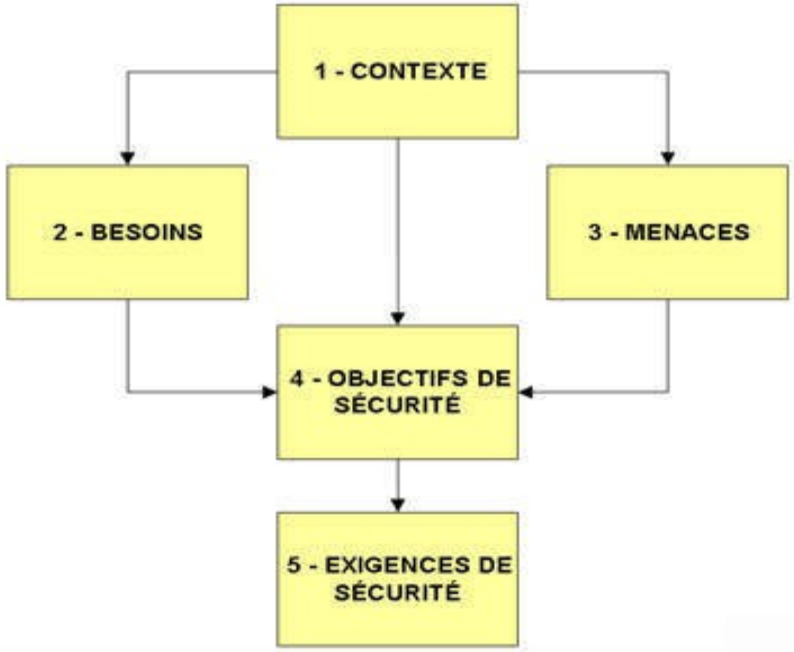
- MEthode Harmonisée d'Analyse de RIsques (MEHARI) - Commission Méthodes du CLUSIF (CLUb de la Sécurité de l'Information Français)
- 6 factors for risks :
  - 3 for potentiality and 3 for impact ;
- 6 types of security measures:
  - structural, dissuasive, prevent/protection, palliative and recovery.


BIENS ou ACTIFS
sont la CIBLE de
MENACE POTENTIELLE
se CONCRETISE par une
AGRESSION
qui DECLENCHE une
DETERIORATION
qui PROVOQUE des
DEGATS
qui OCCASIONNENT des
PERTES
Structurelles
Dissuasives
Préventives
Mesures
Protection
Palliatives
Récupération
Qualité de Services de Sécurité
POTENTIALITE
Causes
IMPACT
Conséquences
ENJEUX
GRAVITÉ des SCÉNARIOS

# EBIOS

Risk Analysis

- ANSSI
- Version 3 (2010)
- 5 modules
- ISO 27001
- *French*



# OCTAVE Allegro

- From CERT http://www.CERT.org/octave/osig.html
- Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE®)
- self-directed approach
- Required broad knowledge of business and security processes

# Conducting a Security Audit
*without wearing suit & tie*

# Phases of the Audit

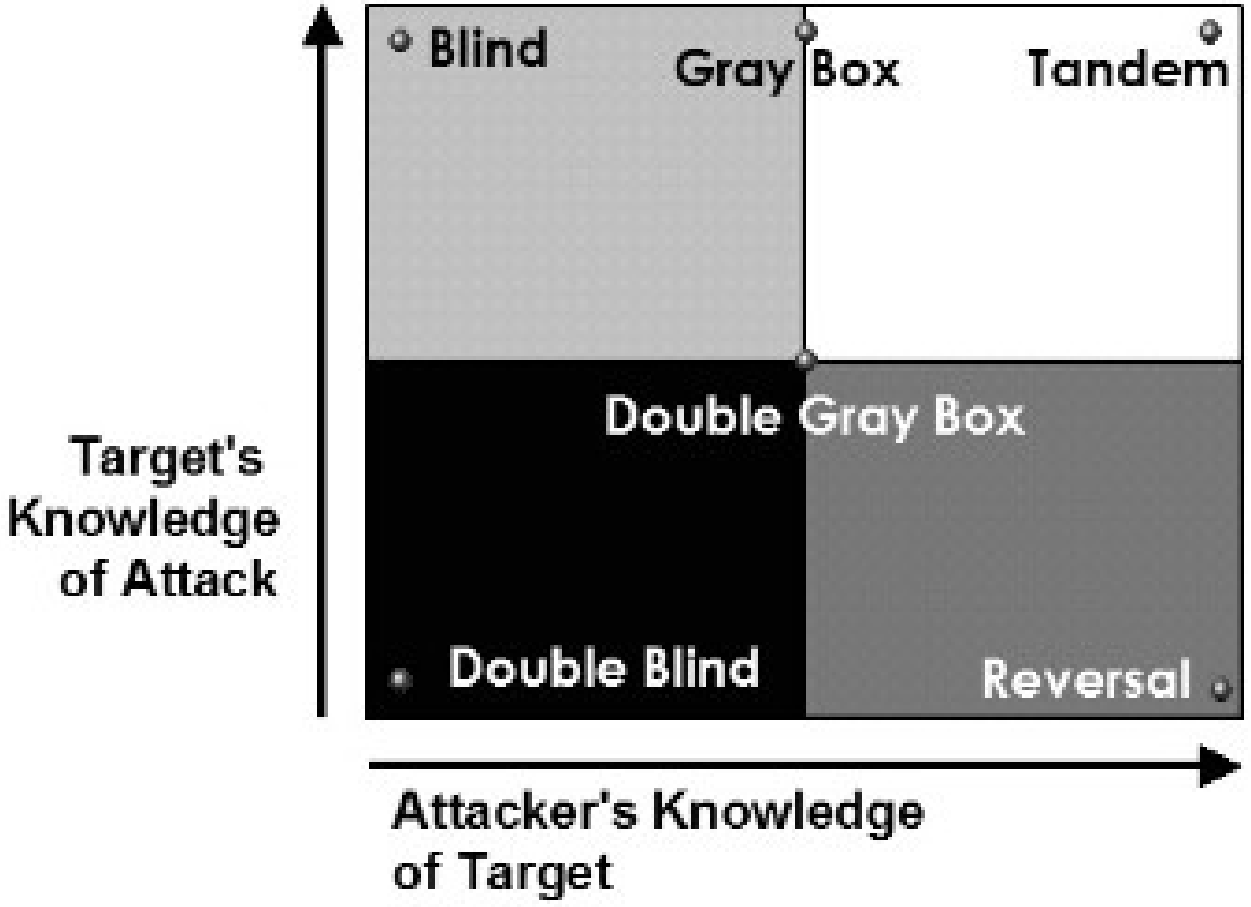
- Preparation
- Documentation Review
- Interviews, talks, visits
- Technical Investigation, Data Collection
- Data Analysis
- Synthesis and report writing
- Report Presentation
- Planning corrective actions

# InfoSec Audit (1)

- "White Box "
  - audit in situ;
  - Access to buildings, organization, data, processes, documentation and procedures;
  - Access to people with interviews of managers and people in charge of operation.

# InfoSec Audit (2)

- " Black Box "
  - Partial knowledge and/or access to the Information System (organization, documents procedures, sites, people);
  - Reveal/spot weaknesses :
- Ex: penetration testing.


Blind
Gray Box
Tandem
Double Gray Box
Double Blind
Reversal
Target's Knowledge of Attack
Attacker's Knowledge of Target

# Who can perform an audit ?

- *AUTHORIZED* personal
    - System/network administrator, consultant, contractor
- Technical and Business Knowledge
- Excellent Communication Skills
- Certified (ex: ISO Lead Auditor, PASSI)

*Trained and Educated people*

# Limitations

- Based on interviews with declarations and claims that can be twisted (intentionally or not);
- Context and time dependent;
- Snapshot / view.

# Where to start ?

- Define the contract : daily job, mission, contract, order, ...
- Define the type of audit ( host-based, network-based, 'white-box', 'black-box', penetration testing, ... )
- Define perimeter and schedule
- List people to be involved

# How to perform an Audit ?

- Define the type of Audit, Target, Perimeter
- Prepare the Tools
- Review Policies and Documentation
- Data Collection
- Analyze and Synthesis
- Writing the Report
- Presentation

# Collect information

- Collect information on the target :
  - Documentation : policies, “chartes”, etc ...
  - Interview
  - Research : Google, Whois, DNS, department of commerce ...

*Goal: Identify systems, processes, applications, people, organizations as well as documents*

# Cartography

- Detection of systems and services , cartography :
    - Locating and visiting sites and buildings (if possible)
    - Documentation
    - Asset Management Tools or Network Management
        - Ex: HP OpenView, Lan Manager, N-View
    - Network Topology : IP routing, SMTP ...
    - Detection of ports/services
    - Identification of systems

# Looking for Vulnerabilities

- Scan and exploitation of vulnerabilities :
  - Physical (garbage dumping, wires, access to resources)
  - Network (filtering policies, equipments)
  - Systems (patches, active services)
  - Applications
    - Web / App Server,
    - Database,
    - Mail Server,
    - Directory,
    - ...

- Take and Secure Position
- Progress
- Move Deeper and Deeper

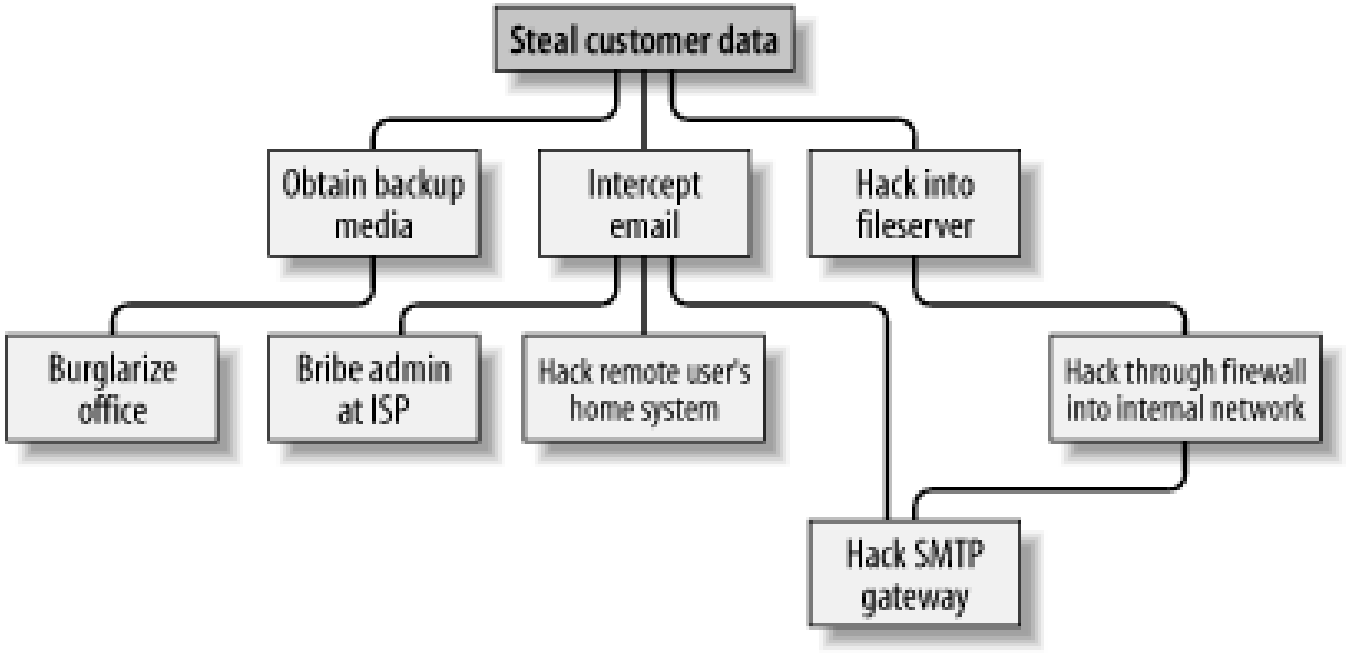
# Attack/Fault Tree Analysis

*FTA : Fault Tree Analysis*

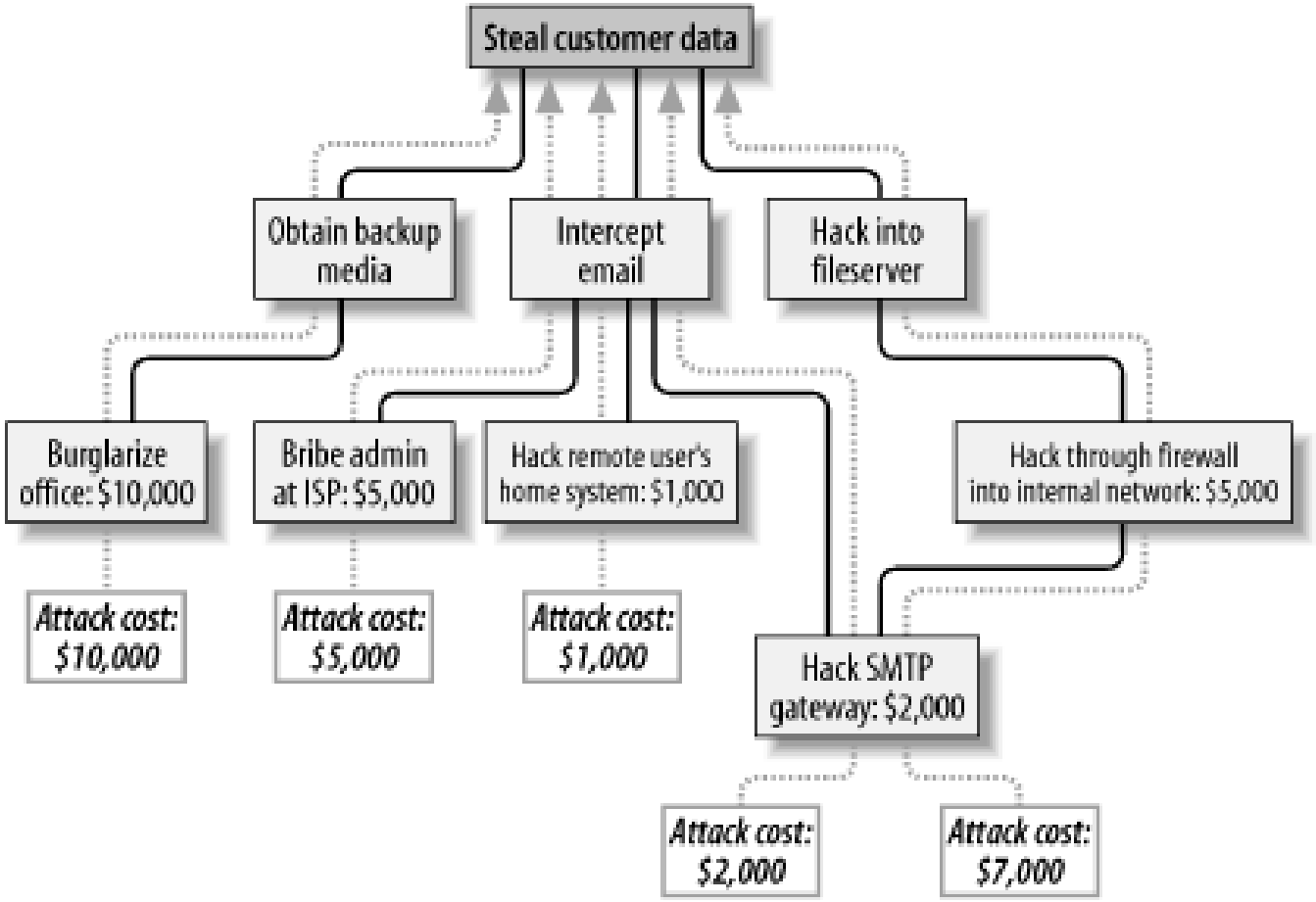
- Start with target or undesired event to study
- Identify possible attacks and conditions
- Construct and evaluate the attack/fault tree
  - By break down
  - Specify frequency/probability/costs
- Risk mitigation / hazard control

# Attack Tree ( start with root goal )

# Attack Tree ( with more details )

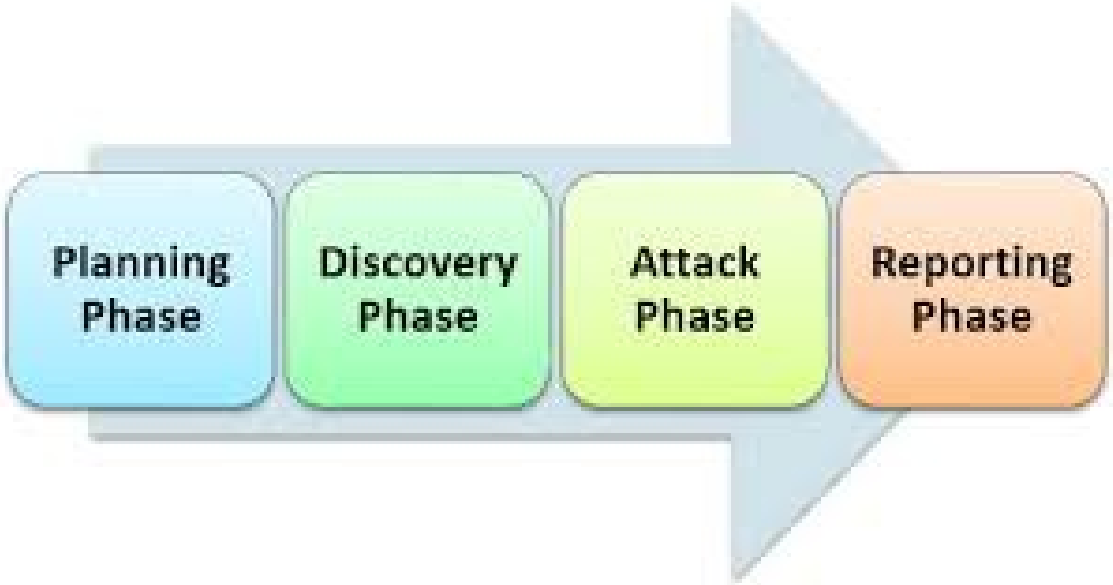


# Attack Tree ( with cost estimates )



# The Toolbox

# ... with a strategy



# Mehari – Interview Guidelines

# Prepare the Tools

- Safe, Trusted and Autonomous Platform for execution and storage of resulting data.
    - Dedicated laptop
    - USB or CD-based bootable (such as Kali) , VM
- Retrieve, install and configure necessary tools.
- Eventually development.
- Get used and trained.
- Verify ALL tools used are untampered with.

# Discovery Tools (1)

- Information : WhoIS, Dig, ...
- Topology
  - IP : Traceroute, Itrace, Tctrace, ...
  - SNMP : SNMPWalk
  - SMB : LinNeighborood, NBTscan
- Network or System Administration
  - HP-Openview, N-View
- Services :
  - Nmap, Amap

# Discovery Tools (2)

- Wi-Fi
  - Kismet
- Bluetooth
  - BTScanner
- Google

# Network Flow Analysis

- Wireshark
- Etherape
- Ntop

# Testing Configuration

- HIDS – Host Based Intrusion Detection
  - MSAT – Microsoft Security Assessment Tool
  - Sara (Unix)
  - JASS (Solaris Security Toolkit)
  - Bastille
  - Checkperms
  - Utilities from sysinternals.com

# Vulnerabilities Scanners

- Framework :
  - Nessus/OpenVAS, nexpose
  - Nikto, Wikto, W3af, wapiti
  - BlueSnarf
  - Metasploit
- Sending Virus Samples
- Code Injection, Packet Injection
- XSS (Cross Site Scripting)

# Fuzzer

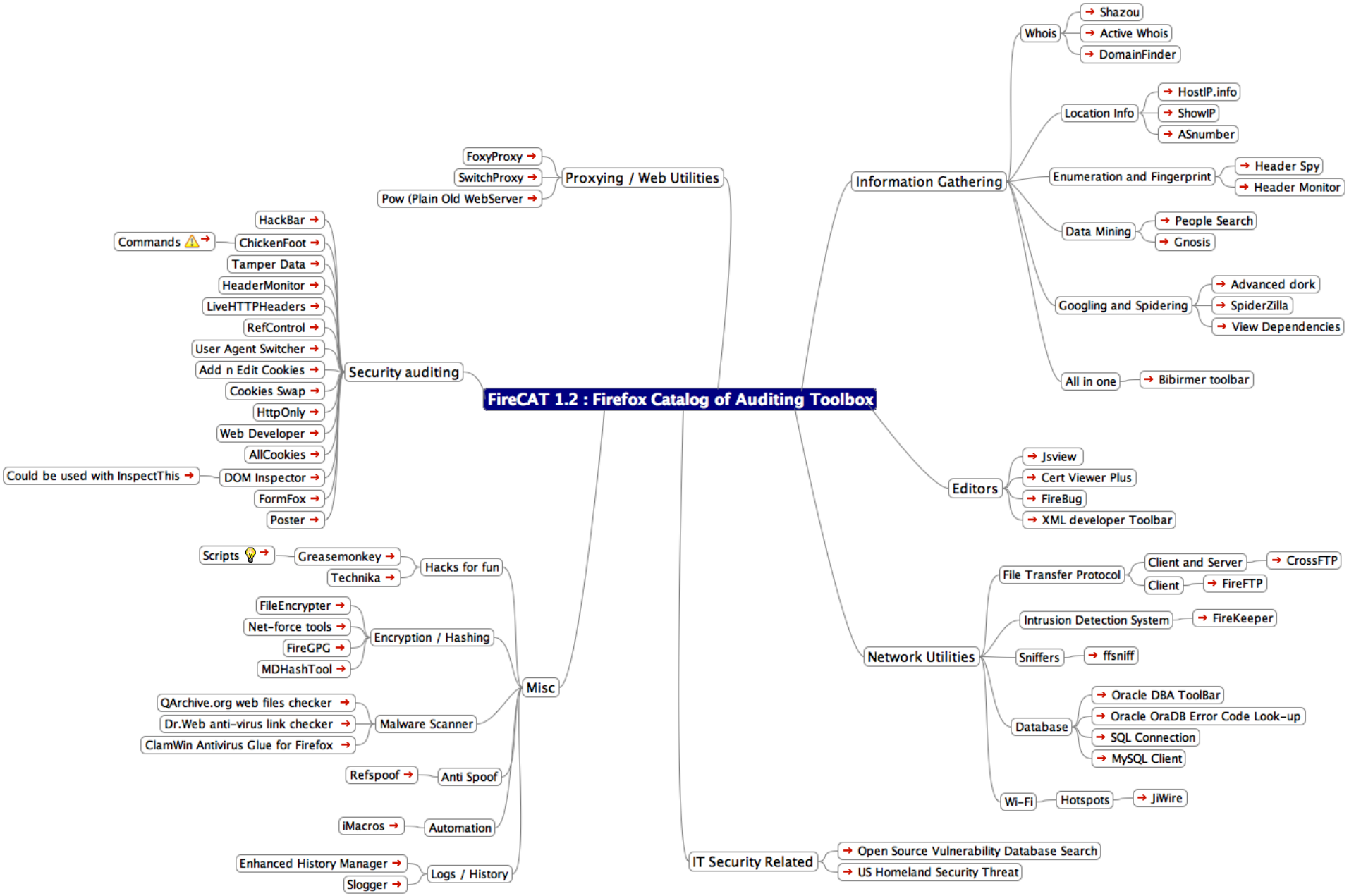
Testing based on random generation of data (either properly formatted and syntaxically correct, or not)

- Fusil
- Sulley
- Defensics (Codenomicon)

# Using Firefox as Security Tools

Testing based on use of Firefox add-ons

- FireCAT – catalog of Auditing Tools
- FoxyProxy – advanced proxy management
- Firebug – edit/debug of CSS, HTML, Javascript
- Flashbug
- Firecookie
- Modify Headers
- XSSme, RegEx Tester


FireCAT 1.2 : Firefox Catalog of Auditing Toolbox
Information Gathering
Whois
Shazou
Active Whois
DomainFinder
Location Info
HostIP.info
ShowIP
ASnumber
Enumeration and Fingerprint
Header Spy
Header Monitor
Data Mining
People Search
Gnosis
Googling and Spidering
Advanced dork
SpiderZilla
View Dependencies
All in one
Bibirmer toolbar
Editors
Jsview
Cert Viewer Plus
FireBug
XML developer Toolbar
Network Utilities
File Transfer Protocol
Client and Server
CrossFTP
Client
FireFTP
Intrusion Detection System
FireKeeper
Sniffers
ffsniff
Database
Oracle DBA ToolBar
Oracle OraDB Error Code Look-up
SQL Connection
MySQL Client
Wi-Fi
Hotspots
JiWire
IT Security Related
Open Source Vulnerability Database Search
US Homeland Security Threat
Misc
Hacks for fun
Scripts
Greasemonkey
Technika
Encryption / Hashing
FileEncrypter
Net-force tools
FireGPG
MDHashTool
Malware Scanner
QArchive.org web files checker
Dr.Web anti-virus link checker
ClamWin Antivirus Glue for Firefox
Anti Spoof
Refspoof
Automation
iMacros
Logs / History
Enhanced History Manager
Slogger
Security auditing
HackBar
Commands
ChickenFoot
Tamper Data
HeaderMonitor
LiveHTTPHeaders
RefControl
User Agent Switcher
Add n Edit Cookies
Cookies Swap
HttpOnly
Web Developer
AllCookies
Could be used with InspectThis
DOM Inspector
FormFox
Poster
Proxying / Web Utilities
FoxyProxy
SwitchProxy
Pow (Plain Old WebServer

# OWASP Top 10 Tools

| | |
|---|---|
| A1: Injection – | ZAP |
| A2: Cross-Site Scripting (XSS) - | BeEF |
| A3: Broken Authentication and Session Management | HackBar |
| A4: Insecure Direct Object References - | Burp Suite |
| A5: Cross-Site Request Forgery (CSRF) – | Tamper Data |
| A6: Security Misconfiguration – | Watobo |
| A7: Insecure Cryptographic Storage | N/A |
| A8: Failure to Restrict URL Access - | Nikto/Wikto |
| A9: Insufficient Transport Layer Protection - | Calomel |
| A10: Unvalidated Redirects and Forwards – | Watcher |

# Toolbox for analysis

- RATS
- Splint
- Flawfinder
- HP Fortify Static Code Analyzer
- Coverity SWAT
- Protocol Validation (formal or not)
  - Avispa,  ProVerif, Scyther

*More detailed information on www.dwheeler.com*

# But also

- Code Reading
- Design Analysis
- Protocol Validation (formal or not)
- Social Engineer Toolkit ...


InfoSec tools
M2 SAFE 2014-2015
incident response/reporting
contactless tools analysis
stress Testing
vulnerability assessment
maintaining access
exploitation tools
forensic
information gathering
privilege escalation
reverse engineering
mobile

# Refund

# Report

- Analysis and synthesis in report
- Achievement of audit
- Readable and adapted to audience
    - From executive summary to detailed annexes
- Adapted to the business objectives
- Definition of an action plan

# Audience

- Executive
- Stockholders
- Managers
- Operational staff
- Technical staff (techno-geek)

# Content

- Title, Introduction, legal
- Executive Summary
- Prioritized recommendations (with cost)
- Report (following the structure of MEHARI domains)
- Conclusion and detailed recommendations
- Annexes

# So What ?

- Definition of action plan for correction
  - Action
  - Who is the owner ?
  - Who is involved/concerned ?
  - When is it due ?
  - How much ?
- Require everyone's involvement

# References - Recommended readings

- Risks Digest - Forum On Risks To The Public In Computers And Related Systems

  http://catless.ncl.ac.uk/Risks

- 'Security Engineering, 2nd ed', Ross Anderson

  http://www.cl.cam.ac.uk/~rja14/book.html

- OSSTMM - Open Source Security Testing Methodology Manual

  http://www.isecom.org/osstmm/

Questions ?

# Meet you in Grenoble on Nov 20th

GREHACK

3rd panic