M2 CyberSecurity
Threat and Risk Analysis, IT Security Audit and Norms

Security Assessment of Information System
Standards, Methods and Tools

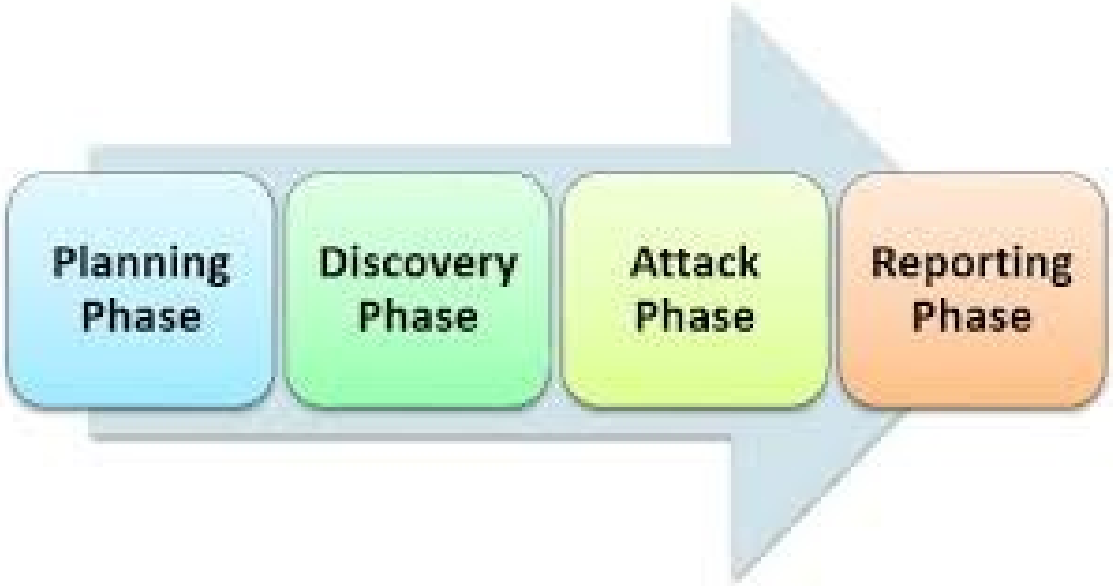
Florent Autréau - florent.autreau@imag.fr
2016 /2017

Outline

- *Introduction*
- Concepts
- Risks and Threats
- Methods and standards
  - ISO2700x, OCTAVE, Ebios, Mehari,
- Tools
  - OpenVAS, nmap, wireshark, ntop, ...
- Hand-on Labs

The Toolbox

... with a strategy




OSSTMM
Discovery:
Obtaining and analysis of the existing system documentation
Enumeration Verification:
Testing of the operating systems, the configuration and services in comparion with the system documentation
Vulnerability Research & Verification:
Vulnerability research and analysis by penetration tests
Integrity Testing:
Integrity testing of all results
Security Mapping:
Mapping of the measured security. Mapping of the results on systems and services.
Risk Assesment Value:
Calculation of the RAV and risk classification of the weaknesses found.
Reporting:
Mapping of the results and giving of recommendations

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/BackTrack) , 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, recon-ng, spiderfoot, ...
- Topology
  - IP : Traceroute, Itrace, Tctrace, ...
  - SNMP : SNMPWalk
  - SMB : LinNeighborood, NBTscan
- Network or System Administration
  - HP-Openview, N-View, Nagios
- Services :
  - Nmap, Amap

Discovery Tools (2)

- Wi-Fi
  - Kismet
- Bluetooth
  - BTScanner
- Google
- Facebook, LinkedIn, ...

Network Flow Analysis

- Wireshark (formely known as Ethereal)
- Etherape
- Ntop

Checking Configuration

- HIDS – Host Based Intrusion Detection
  - MSAT – Microsoft Security Assessment Tool
  - Lynis (linux)
  - Debsecan (debian)
  - Sara (Unix)
  - JASS (Solaris)
  - 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

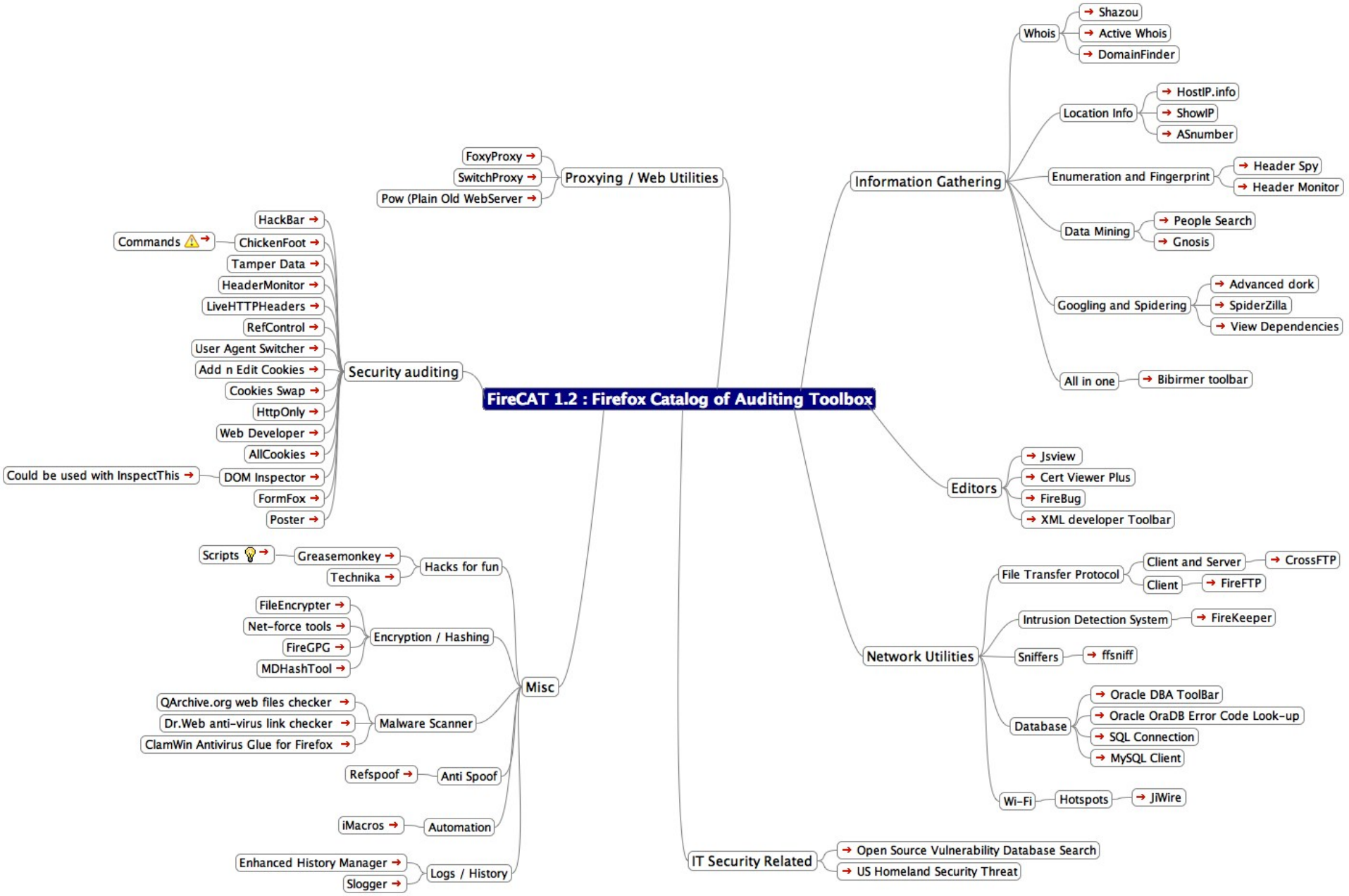
Testing based on random generation of data (either properly formatted and syntaxically correct, or not)

- 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


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 (see EIS – Lecture on Secure Coding)
- Design Analysis
- Protocol Validation (formal or not)
- …

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

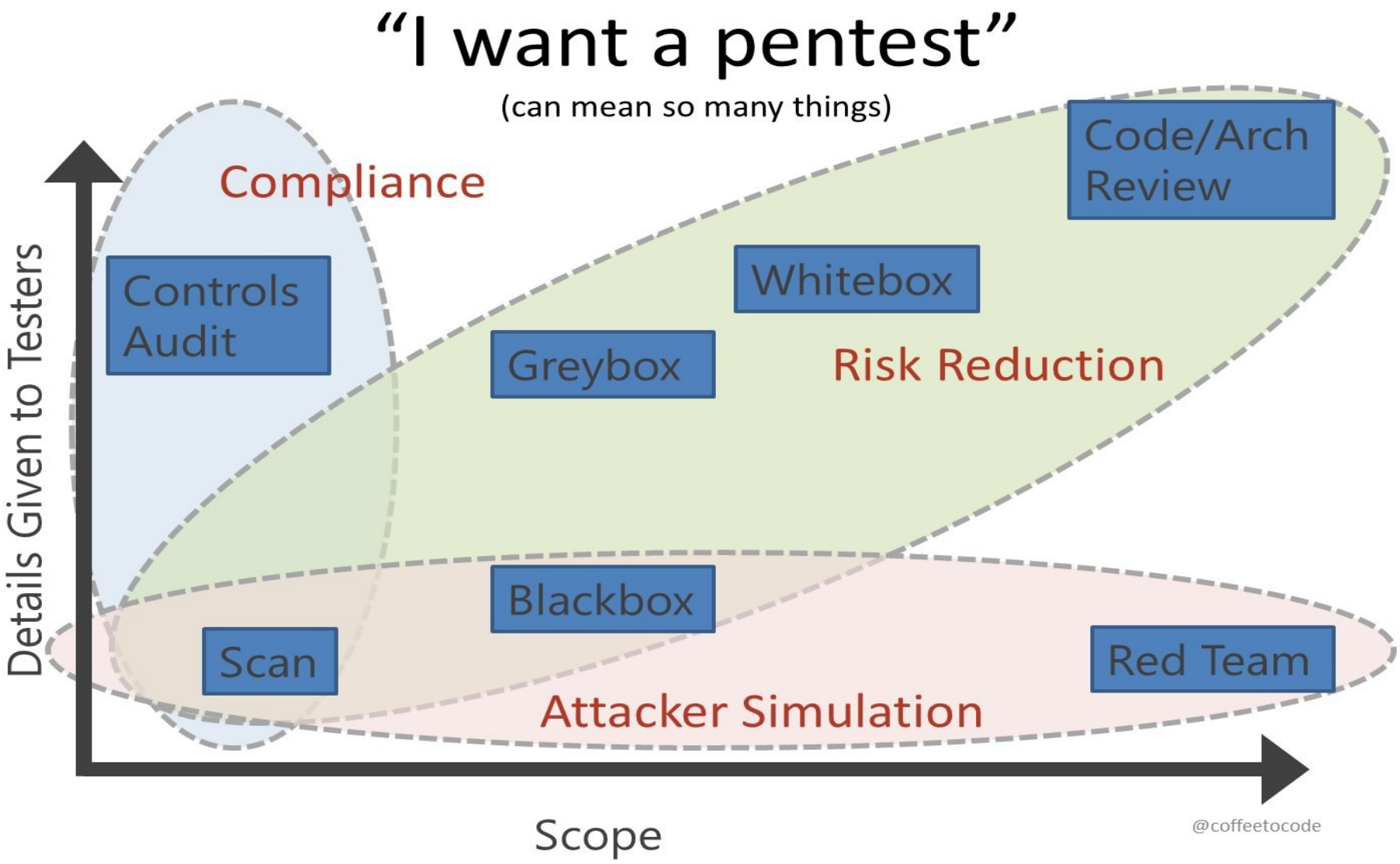
- Executive
- Stockholders
- Managers
- Operational staff
- Technical staff (techno-geek)

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


"I want a pentest"
(can mean so many things)
Compliance
Code/Arch Review
Controls Audit
Whitebox
Greybox
Risk Reduction
Blackbox
Scan
Red Team
Attacker Simulation
Details Given to Testers
Scope
@coffeetocode

References – More readings

- 'TCP/IP Illustrated', Richard Stevens
- 'Network Security Assessment', McNab
- 'The TAO of Network Security Monitoring', Bejtlich
- 'IT Auditing', Davis/Schiller/Wheeler
- 'Management de la Sécurité Informatique – Implémentation ISO 27001', Fernandez-Toro

Evaluation

- Part of evaluation for this class will be based on a report which presents :
  - the exercices of the tutoring sessions.
- Reports are due <TBD> and should be submitted electronically
- Name : M2CySecAudit-Exercices-<name>.pdf.
- 10p max. pdf format (no word or any funky format please).

Report – Exercices (reminder)

- Ex 1 - Service Availability (model / solutions)
- Ex 4 - Risk Analysis (nomadic / cloud)
- Ex 5 – Risk Analysis (student / sysadmin)
- Ex 7 – Attack Tree (student information)
- Ex 8 – MindMap (Group work)

Outline

- *Introduction*
- *Concepts*
- *Risks and Threats*
- *Methods and standards*
  - *ISO2700x, OCTAVE, Ebios, Mehari,*
- *Tools*
  - *Nessus, nmap, wireshark, ntop, ...*
- Hand-on Labs

Practical Works

- After the risk analysis conducted in Exercices 5 and 7 (student in M2 CySec), conduct a Security Audit of the working environment provided to you in Room F103 – UFRIM²AG.
- Propose and implement corrective actions.

Sec Audit – Lab 1 (1)

- Getting ready
    - Understand the scope of the exercice
    - Review Risk Analysis (Ex 5) and Attack Tree (Ex 7)
    - Prepare your toolbox (including installation)
- Organization of ISMS
    - What are your rights ? Your duties ?
    - Is the “Charte” well adapted ?
    - Who's in charge of security ?
    - How incident are being handled ?

Sec Audit – Lab 1 (2)

- Physical Security of Sites
    - How equipment are protected against theft ?
    - How access control to the building is organized ?
    - To the room itself ?
    - Protection against power failure ?
- Protection against usual risks (fire, flooding, etc.)

Sec Audit - Lab 1 (3)

- Network Architecture (Access Control, Filtering, containment, reliability)
    - Check network filtering from outside by using free on-line port scanning service
    - Or from a trusted system (run nmap on ensisun.imag.fr)
    - Check the filtering rules with nmap
        - Apt-get install zenmap
        - Run zenmap as root
    - Discover topology
        - Apt-get install mtr

Sec Audit - Lab 1(4)

- Use a network mapper
- Confidentiality and integrity of communication
  - Capture traffic with tcpdump
  - Analyze it with wireshark
  - Same with ntop

Sec Audit – Lab 1(5)

- Access Control to Logical level (systems, apps and data)
    - Analysis of BIOS settings
    - Analysis of grub.conf
    - Operating System Audit with bastille, checkperms, debsecan)
    - List of running services and configuration
    - Filtering (netfilter, tcpwrappers, …)
    - Installation of nessus/openVAS
    - Strength of passwords (using johntheripper)
- Data Security
    - Encryption ? Wiping ? Residual Data (cache, tmp files, logs) ?

Sec Audit – Lab 1(6)

- Operational Procedures
- Management of Information Support
- Rescue Plan
- Backup and Recovery Planning
- Maintenance
- Security of projects and development
- Incident Management

TP 1 – Instructions for report

- Reports are due <TBD> and should be submitted electronically
- Name : M2CySecAudit-TP1-<name>.pdf.
- 10p max. pdf format (no word or any funky format please, nor useless screen capture).