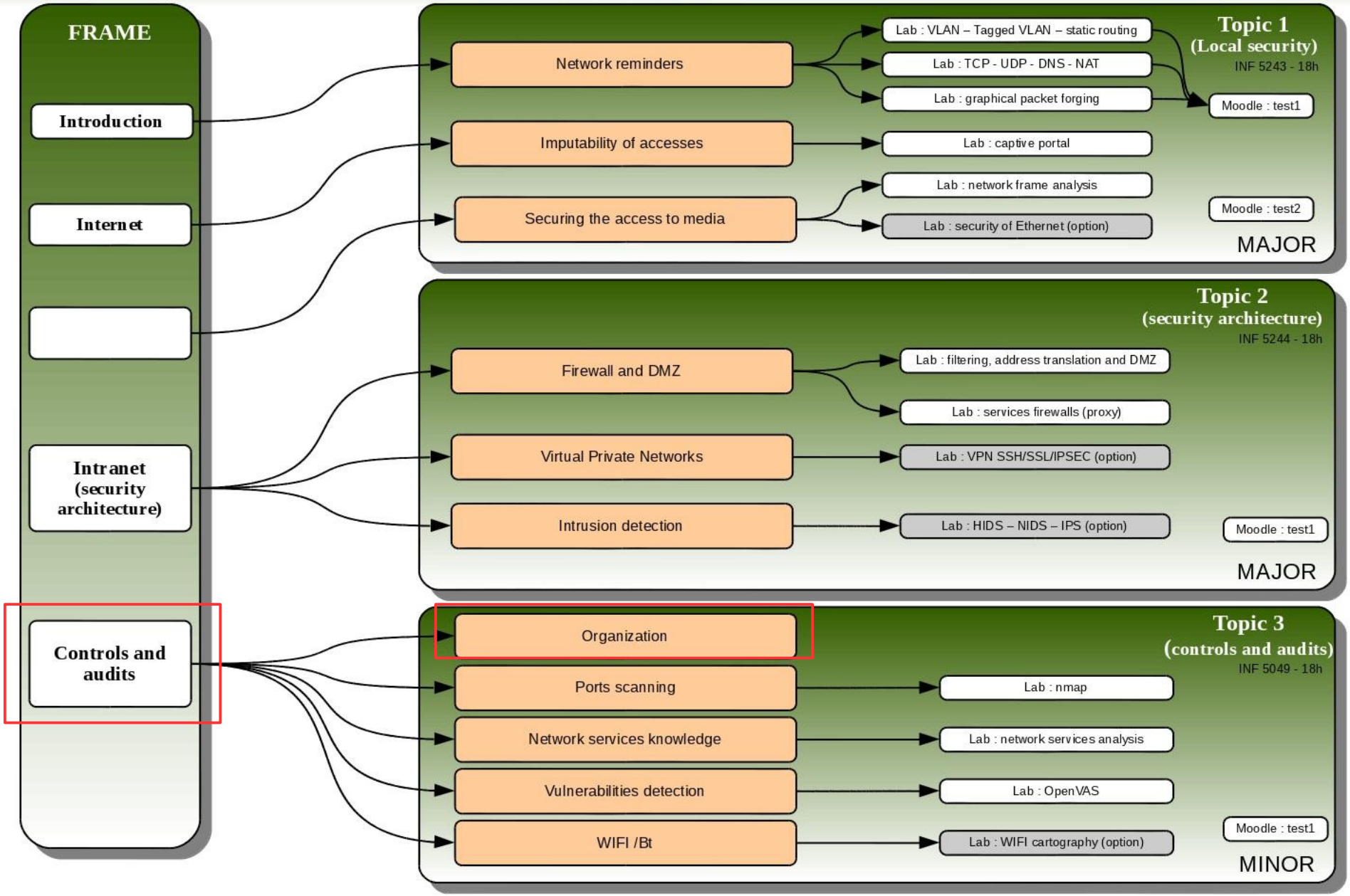
Audits, contrôles et tests d'intrusion

By Roxy

Course 5A - « network security »



Rappel :

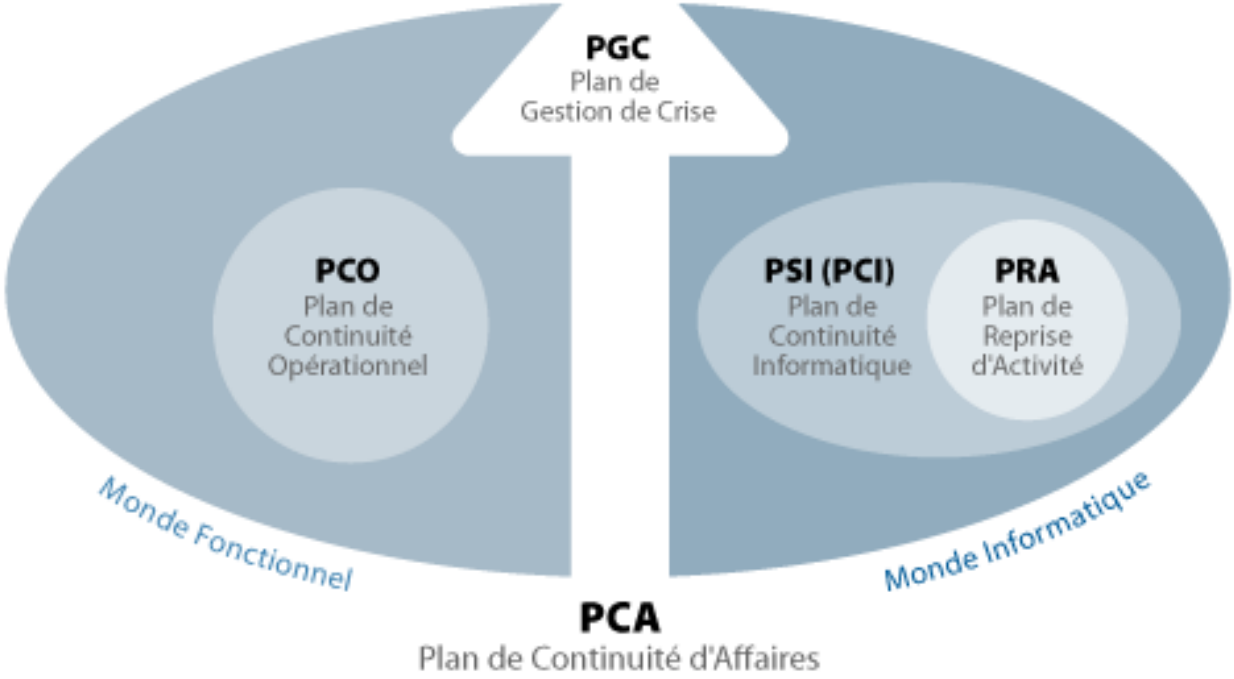
Les moyens de sécurisation déployés doivent assurer la **disponibilité**, l'**intégrité** et la **confidentialité** du système et des informations traitées. Ils doivent aussi permettre d'**imputer** les actions et en assurer la **non-répudiation**.

Évaluer l'état de protection d'un Système d'Information (SI), c'est mesurer le niveau de sécurité d'un SI face à des risques identifiés.

- Audit de sécurité d'un système d'information (Security assessments) : Rechercher les vulnérabilités d'un SI (ou d'une partie de celui-ci) sans les exploiter. L'audit est réalisé en interne, de manière collaborative avec le propriétaire qui fournit toute la documentation. Les résultats sont des recommandations classées par ordre d'importance.
- Test d'intrusion (penetration testing - pentest) : Rechercher les failles d'un système et les exploiter afin d'en prendre le contrôle et d'accéder aux données. Le périmètre de la cible est volontairement plus limité (serveur d'application, service WEB, routeur, etc.). Il est souvent réalisé de l'extérieur en « boite noire » (position du pirate).
- Contrôle de sécurité : Rechercher les défauts d'application de la politique de sécurité et des directives locales. Les résultats sont des consignes (ordres) priorisées avec échéancier.

Les différents audits

- Audit de conformité : contrôler les risques juridiques et règlementaires d'après des référentiels privés ou publics (ARJEL, ISO2700x ($0 \leq x \leq 40$), PCI-DSS (Payment Card Industry Data Security Standard), CNIL, santé, etc.)
- Audit d'architecture (réseau + système)
- Audit de sécurité d'un SI et test d'intrusion (Pentest)
- Audit de configuration
- Audit de la maîtrise de la continuité



L’audit a pour objet :

- D’évaluer la qualité, l’efficacité et la cohérence des dispositifs et des procédures de sécurité
- De mettre en évidence les vulnérabilités
- De qualifier les risques effectifs ou d’en quantifier le niveau
- De proposer les éventuelles actions correctives (recommandations)
- Dans le cadre d’une homologation : de fournir un avis à l’autorité d’homologation lui permettant d’instruire le dossier

L’audit vise un SI complet avec son environnement **physique**, **technique** et **humain**. Il s’appuie sur des documents de référence (politique de sécurité du SI). Il est réalisé **de l’intérieur** et selon une **méthodologie** approuvée.

L'audit se décompose en trois phases

Visite préparatoire à l'audit :

- Organisation d'une visite sur site pour une présentation mutuelle (auditeur / audité)
- Présentation de la méthode d'audit et de la logistique nécessaire
- Définition mutuelle du périmètre d'audit, de la charge de travail, des coûts
- Signature d'une charte de confidentialité (NDA)
- Signature d'une charte d'audit et/ou d'un protocole et/ou d'un contrat (cf. exemple)

Réalisation de l'audit sur site

- Investigations **organisationnelles , informationnelles** et **techniques**
- Analyse « à chaud » du niveau de sécurité entre auditeurs
- Préparation et présentation d'une synthèse aux responsables
- Sensibilisation et conseil SSI
- Action objective, constructive et conjointe (participation de tous les acteurs)

Analyse finale

- Analyse approfondie des relevés réalisés
- Rédaction et envoi du rapport d'audit

Rappel : Le PenTest

Investigation technique et informationnelle ciblée (un serveur / un service). Il est souvent effectué en « boite noire » et à distance.

Audit : investigation organisationnelle

- **Organisation :** Mise en œuvre du référentiel sécurité et des moyens humains

- **Personnel :** Gestion des habilitations, des compétences métiers et SSI

- **Environnement :** Gestion et mise en œuvre des moyens de protection physique (surveillance, contrôle d'accès, énergie, climatisation, incendie, etc.)

- **Matériel :** Gestion (gestion de parc informatique), procédures d'installation et de maintien en condition (serveurs, postes de travail, copieurs), procédure d'achat et de destruction

- **Logiciel :** Gestion (cartographie et licence), procédure de déploiement et de configuration, procédure d'achat et de mise à jour

- **Réseau :** Gestion (cartographie réseau), procédures de configuration (câblage et équipements actifs)

- **Support :** Procédures de gestion et de destruction (papier ou numérique)

Suivant une méthodologie validée

Audit : investigation informationnelle et technique

- **Démarche transparente :**
  - Méthodologie et traçabilité des actions.
- **Domaines traités :**
  - Analyse informationnelle (source ouverte, réseaux sociaux, ingénierie sociale, noms de domaine, etc.) ;
  - Analyse technique
    - cartographie du réseau (incluant le WIFI) ;
    - analyse de trames ;
    - analyse des services réseau ouverts ;
    - détection des vulnérabilités ;
    - contrôle de la configuration des services serveur.
- **Outils :**
  - Logiciels libres ;
  - Logiciels du commerce ;
  - Développements internes.
- **Références**
  - Dossier de sécurité du système audité ;
  - Guides ou fiches de paramétrage de serveurs ;
  - État de l'art de la SSI.

PenTest

- Périmètre beaucoup plus restreint :
  - sites WEB ;
  - Serveurs ;
  - Appliances.
- Méthodologie du pirate + éthique
- Généralement réalisés de l'extérieur
- Référence : état de l'art

Audit : le livrable

Synthèse et rapport d'audit

- Des vulnérabilités et risques associés par fonction de sécurité
  - Référentiel de sécurité (critique et application de la politique et des directives internes)
  - Organisation de la sécurité de l'information (chaîne de responsabilité)
  - Gestion des biens (équipements, supports, etc.)
  - Sécurité réseau
  - Sécurité des logiciels
  - Plan de Continuité et de Reprise d'Activité (PCRA)
  - Contrôle d'accès
  - Moyens d'intégrité
  - Imputabilité
  - Supervision
- Des recommandations d'actions correctives
- Avis sur le niveau de sécurité du système
- Diffusion
  - 1 semaine pour la synthèse et 1 mois max pour le rapport
  - **Information très sensible, voire confidentielle --> marquage obligatoire**

Cas particulier : Audits CVO²

- Contraintes spécifiques
- Ligne de temps
- Méthodologie - contrat
- Présentation de la journée préparatoire
- Compte rendu

Retour d'expérience : Référentiel de sécurité

Analyse de risque

Analyses de risques partiellement ou non réalisés ne permettant pas d'identifier les besoins de sécurité

Stratégie d'homologation

Niveau d'homologation visée inadapté – habilitation inadéquate

Gestion de l'information

- Non-respect des règles de protection pour l'échange d'informations à caractère confidentiel
- Cloisonnement insuffisant des données
- Non-respect du besoin d'en connaître
- Absence de marquage (timbrage + référence) de documents contenant des informations classifiées
- Principe de non-régression non respecté (reprise des données)

Retour d'expérience : environnement

Mauvaise organisation

- Documentation d'administration incomplète ou non pertinente
- Formation insuffisante pour les taches d'administration
- Délégation de l'administration à des tiers
- Parc matériel mal ou non géré

Suivi de projet insuffisant

- Vision de l'avancement de projet éloigné de la réalité
- Absence de cellule de gestion de projet
- Processus qualité de la livraison insuffisant (livrables, échéance, pénalité, etc.)
- Délégation de tâches à une entité tierce non maîtrisée
- Réutilisation de codes ne correspondant pas aux besoins de sécurité du SI
- Développement non sécurisé

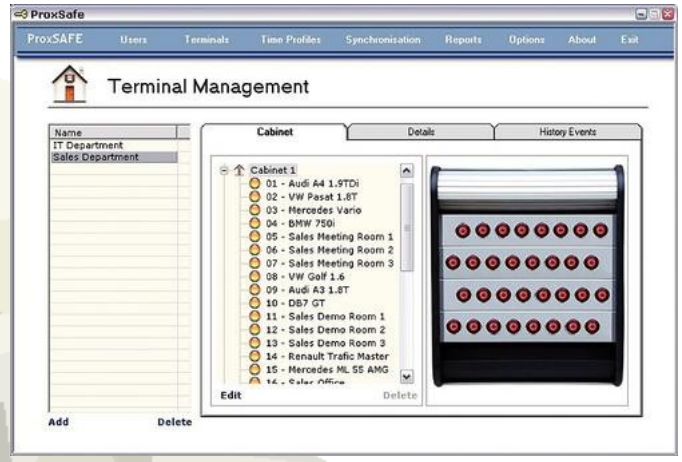
Prise en compte insuffisante de la SSI

- Procédures absentes
- sensibilisation du personnel
  - divulgation d'information sur les réseaux sociaux
  - Perte / vol de PC-portables
  - Malveillance interne
- Sécurité physique insuffisante
- Moyens énergétiques/climatiques/charges sous-dimensionnées

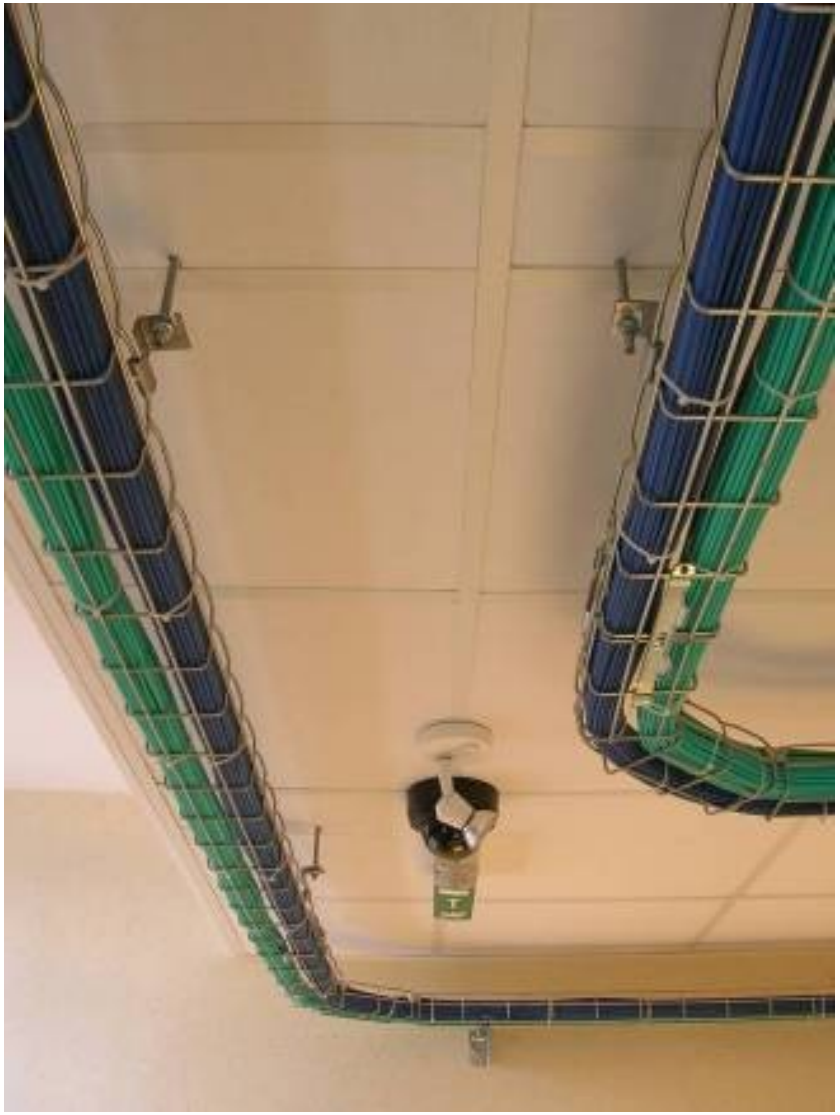
Retour d'expérience : technique

- Architecture réseau et système inadaptée
- **Utilisateurs avec pouvoir**
- Découverte de protocoles encombrants ou interdits :
  - 50% de protocoles réseau superflus (mauvaises configurations de stations, d'imprimantes réseau et des Équipements Actifs de Réseau)
  - Protocoles « domestiques » (Upnp/DLNA/mDNS)
- Prise de contrôle à distance / extérieur (sans accord écrit des usagers)
- Découverte de points d'accès extérieurs
  - Systèmes d'impression et de badgeuses tété-administrés
  - **Portables « à deux têtes »** (réseau local / 4G)
  - Points d'accès WIFI non maîtrisé
- Découverte de vulnérabilités majeures sur certains systèmes
- Journal d'authentification non vérifié (VPN + interne)

Audits, contrôles et tests d'intrusion

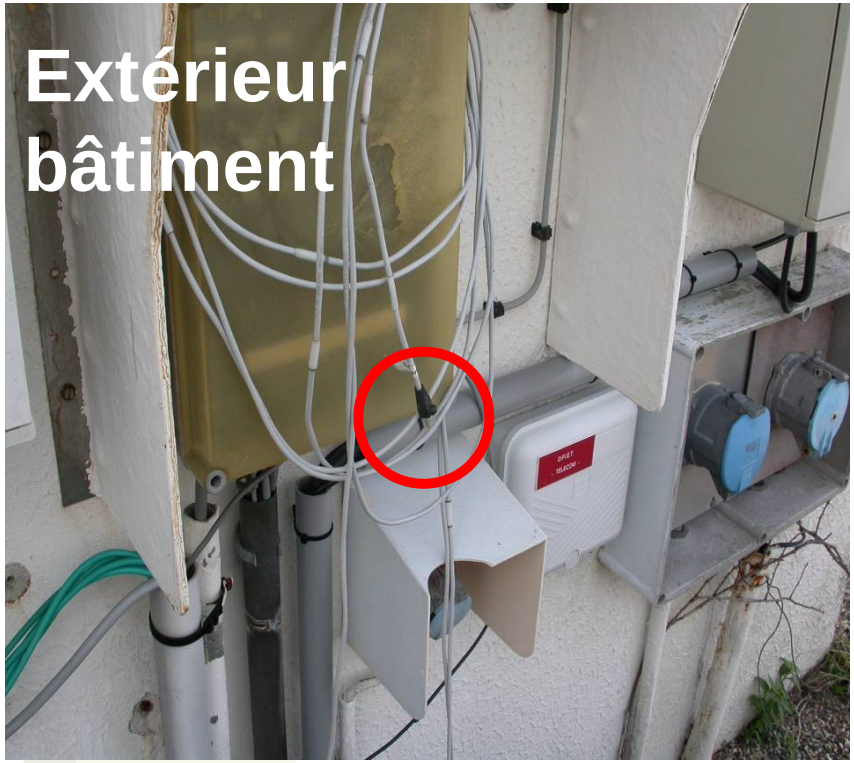



01/025/P03



Audits, contrôles et tests d'intrusion

Audits, contrôles et tests d'intrusion



- Onduleur (Off-line / On-line)
- Sauvegarde / Archivage
- Préparer un PC portable de « présentation/voyage »
- FOVI (! adresse de courriel générique)

Rappel des sanctions (code pénal)

Atteinte au secret professionnel — 226-13 → **1 an & 15 000 €**

Atteinte aux droits de la personne résultant des fichiers ou des traitements informatiques — 226-16 à 21 → **5 ans & 300 000 €**

Accès ou maintien frauduleux dans un système de traitement automatisé de données — 323-1 → **2 ans & 30 000 €**

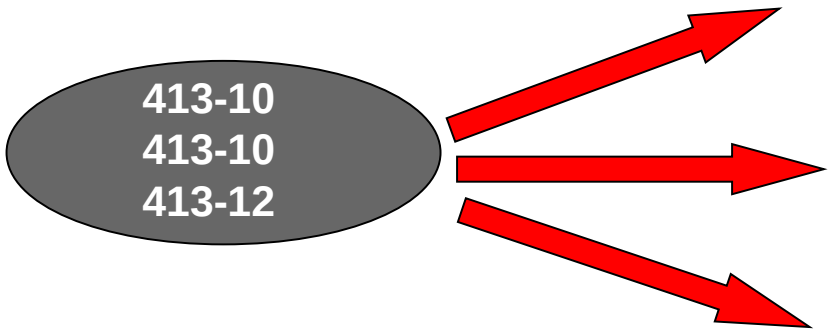
Dans le cadre d'un audit ou d'un test d'intrusion : importance

- De connaître ses droits et ses devoirs (cf. diapo externe)
- du « protocole » signé incluant un accord de confidentialité / NDA (cf. exemple)
- de la traçabilité des actions menées (renseigner un cahier d'évènements)

Rappel des sanctions (code pénal)

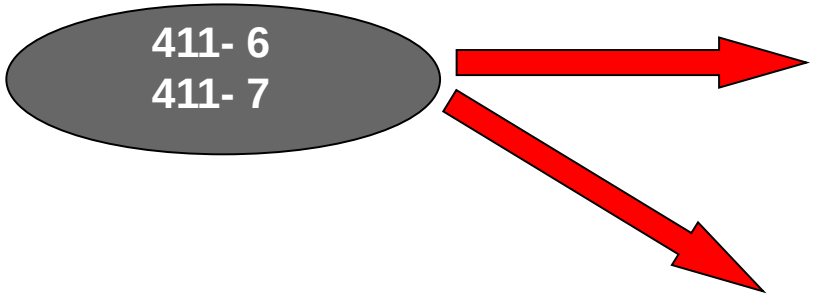
Intérêts fondamentaux de la nation

Atteinte ou tentative d'atteinte au secret de la défense nationale*



- **Dépositaire par négligence ou imprudence**
  3 ans & 45 000 €
- **Dépositaire volontaire**
  7 ans & 100 000 €
- **Non dépositaire**
  5 ans & 75 000 €

Trahison



- **Avéré**
  15 ans & 225 000 €
- **Tentative**
  10 ans & 150 000 €

*cf. cours juridique

Methodology :

- Norme ISO 27000
- OSSTMM "Open Source Testing Methodology Manual"
- NIST (computer security publications) : 800-115
- OWASP (Open Web Application Security Project) : testing guide
- Vulnerability assessment Penetration Testing Framework

Data management :

- Dradis
- MagicTree

Search stage :

Whois, Arin.net, Maltego, recon-ng, social networking, search engines, ExifTool, "strings" command (Linux & Windows Sysinternals), yougetsignal.com,

Info :

Ethicalhacker
Sectools
OWASP
Packet Storm
Security focus (tools)

Books :

RTFM (ISBN 9781494295509)
Blue team handbook (ISBN 9781500734756)

Distribution :

- KALI (previously Backtrack)
- Matriux
- BackBox
- NodEZero
- AirCrackNg

Network ports scan & analysis:

- Scapy (craft packets)
- arp-scan
- Nmap (CLI), Zenmap (GUI)
- Wireshark (GUI), Tcpdump (CLI)

Generic tools :

- Netcat/ncat (generic socket client/server)
- Metasploit (+ armitage)
- Social Engineer Toolkit
- Password Attacks
  - Hydra
  - Fgdump
  - John The Ripper
  - Cain
  - Ophcrack

Audits, contrôles et tests d'intrusion

Wifi tools :

- InSSIder
- Aircrack-ng
- Kismet
- NetStumbler
- CoWPAtty
- AirPwn
- Karma

Train, learn & challenge yourself:

honeynet project (90% network), root-me, pentesterlab, exploit-exercises, newbiecontest (french), overthewire.org (reverse/exploit), hackthissite (web pentest), crackmes.de (reverse), github.com/ctfs (CTF list).

Generic vulnerabilities scanner

- Nessus
- OpenVAS

Web Apps vulnerabilities scan :

- Act as a Proxies
  - Owasp ZAP
  - Owasp WebScarab
  - Burp Suite
- Direct scan
  - Nikto / Wikto
  - W3af
  - wapiti

The Problem of the pentesters : keep his knowledge up to date

- Analyze the tools and vulnerabilities scanners
- Keeping informed, train, learn and learn again

Audits, contrôles et tests d'intrusion

By Roxy

Course 5A - « network security »