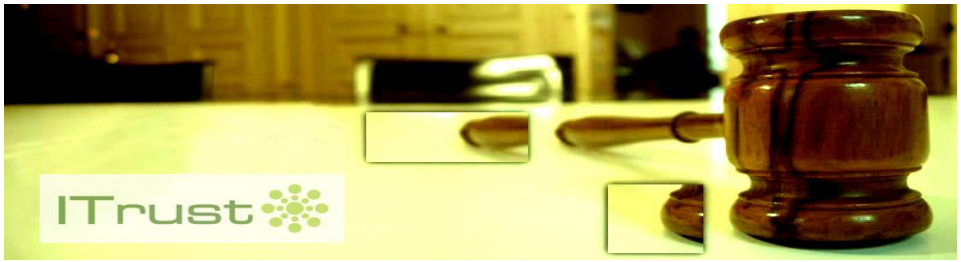
Aspects juridiques du scan et des tests intrusifs



Scan et tests intrusifs : Aspects juridiques

I/ Prolégomènes

II/ L'Audit Intrusif & Expert en Sécurité informatique

III/ L'Informatique & Le Droit

IV/ L'Audit intrusif & Le Droit

V/ De la légalité du Scan de Port

VI/ Autres Techniques de Sécurité ou de « Pirate » & Légalité

I

Prolégomènes

I/ Prolégomènes : Notions

Système d'information

« *Ensemble organisé d'éléments (organisation, acteurs, procédures, systèmes informatiques) qui permet de regrouper, de classifier et de diffuser de l'information sur un phénomène donné* ».

Information

« *Elément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement* ». Arrêté du 3 octobre 1984 du ministre de l'éducation et du ministre chargé des PTT.

Système informatique

« *Partie automatisée d'un système d'information qui regroupe l'application de gestion et ses éléments d'accompagnement, les logiciels supports et les matériels.*

STAD, Système de traitement automatisé des données

Tout équipement (de nature matérielle, logicielle, ou "firmware") permettant l'acquisition automatique, le stockage, la manipulation, le contrôle, l'affichage, la transmission, ou la réception de données.

Conception large : *« Réseau de France Telecom, réseau de Carte bancaire (Tribunal Correctionnel Paris, 25 février 2000), un disque dur (Cour d'appel de Douai, 7 octobre 1992), un radiotéléphone (Cour Appel Paris, 18 /11/1992), un ordinateur isolé, un réseau local.*

Prolégomènes : Notions

« Hacker » / Pirate Informatique

« *Hacker s'introduit dans les systèmes par des moyens illégaux sans détruire les données ni utiliser les informations données, mais dans le seul but de faire savoir qu'il existe des failles de sécurité* »

« Hacker » a l'origine : Programmeur passionné d'informatique / « *Passer tout son temps devant son ordinateur … ».*

« Hacking » : Synonyme de « Piracy » (contrefaçon) traité en droit français par CPI.

« Cracker » (casseur)

« *Appellation qui désigne le pirate qui détruit dans un but précis ou pour le plaisir ».*

L'expert en sécurité informatique

« Professionnel qui contribue à la mise en œuvre de la politique de sécurité de l'entreprise. Il fait remonter les risques en matière de sécurité informatique. Il met en place des contrôles de prévention en amont, de détection en simultané, d'explication et de consolidation en aval, pour contrer des intrusions ou des dysfonctionnements des systèmes informatiques. »

Dans l'exercice de ses fonctions il peut endosser le rôle d'un « hacker » ou d'un « cracker ».

Audit Intrusif

« *Prestation d'expert en sécurité informatique englobant plusieurs approches et méthodes dont l'objectif est d'évaluer le niveau de sécurité d'un système informatique ».*

II

L'Audit Intrusif
&
Expert en Sécurité informatique

Exemple d'ITrust : Activité Sécurité SI

- Société en sécurité des systèmes d'information, de conseil qui réalise quotidiennement des audits intrusifs.

- Diversité des profils clients :

  Banque (*BNP Paribas, LCL Crédit Lyonnais, Société Générale, La Banque Postale),* Aéronautique *(EADS, Airbus),* Automobile *(BMW),* Immobilier *(Akerys),* Grande distribution (*SA Galec),* Club sportif *(Stade Toulousain),* Institution *(AGIRC Retraite des cadres),* liste non exhaustive.

- Activités récurrentes :

  Conseils en sécurité et administration de système d'information, formation, forensic … dont activité d'audit.

Audit intrusif … Objectifs

Face au « pirate » l'expert en sécurité

- **L'expert en sécurité informatique**
  - ✓ Méthode de « combat » devenir assaillant
  - ✓ Comment ? Audit de Sécurité / Test intrusif

Profilage, le « social engineering : art of deception (L'art de la tromperie) », le scan de port et « l'exploitation » éventuelle des vulnérabilités.

- **Finalité test d'intrusion : Eprouver la sécurité pour la renforcer**
  - *Mettre à l'épreuve la sécurité d'un environnement*
  - *Qualifier sa résistance à un certain niveau d'attaque,*
  - *Révéler des problèmes issus d'une incohérence entre différents composants*
  - *Prouver que la sécurité mise en place est insuffisante*

- **Afin de** :

Sensibiliser / Mettre en place PCA, *plan de continuité d'activité*, ou PSI, *plan de secours informatique*, de charte informatique et / ou charte d'usage de moyens de communication électronique (*salariés*)
Intégrer des gardes fous dans les contrats (*clients, fournisseurs, prestataires, partenaires*).

Audit intrusif … Différentes approches

Le Pen test :

- ✓ *A penetration test is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source, known as a Black Hat Hacker, or Cracker* (Source Wikipedia).

Trois visions différentes de réalisation des audits :

- Audit Boîte noire (Blind) / Architecture inconnue
- Audit Boîte blanche / Architecture fournie permet simulation de scénario
- Audit sur Compte utilisateur / Mesurer capacité nuisance interne : personnel malveillant ou négligence …

Audits réalisés selon les besoins en mode externe ou interne.

III

L'Informatique
&
Le Droit

III/ Informatique et Droit

- **Le respect des réglementations** exigence pour la sécurité des SI (*Critères DICPR*).

- **Réglementations / Législations** régissant système d'information / informatique :
  - *Intéressant professionnels de l'informatique (DICPR) ou praticiens novices*
  - *Multiples*
  - *Complexes*
  - *Nationales, Communautaires, Mondiales*

- **Droit Français** : Assimilation de l'Informatique dans le droit national

  ✓ Législations généralistes / Droit commun : « ***Par tout support*** », « ***Quelque que moyen que ce soit*** »

  ✓ **Législations spécifiques** : *Signature électronique, Droit du Producteur des BDD, Droit d'auteur des logiciels, Protection des données à caractère personnel « Informatique et Libertés », Loi Pour la Confiance en l'Economie Numérique, …*

  ✓ Par des **infractions spécifiques** : *Contrefaçon et P2P, Délit pénal de contournement des MTP, mesures techniques de protection, …*

  Et le <u>régime de la Fraude informatique</u>

III/ … « La Fraude Informatique »

- **But Protéger « Système informatique »**

- **Loi Godfrain du 5 janvier 1988** , n° 88-19 transposée code pénal : articles 323-1 à 323-7. « Fraudes informatiques et atteintes aux systèmes d'information »
  - ✓ Délit d'accès non autorisé (*Sanction : 2 ans / 30 000€ amende)*
  - ✓ Maintien frauduleux dans un système informatique
  - ✓ Entrave et/ou fausse le fonctionnement d'un système de traitement automatisé
  - ✓ Introduit frauduleusement des données dans un système d'information ou les modifie, ou les supprime (*Sanction : 3 ans / 45 000€ amende)*

- **Eléments constitutifs** :
  - ✓ Intrusion dans le SI : Sanctionnée qu'elle soit réalisée sur le moniteur même ou à distance, que le maintien ait eu lieu après *accès fortuit*,
  - ✓ Volonté de s'introduire ou de se maintenir : signification de « **Frauduleusement** »

- La tentative est punissable (article 323-7)
- Les personnes morales sont condamnables (article 131-39)
- Le recel après fraude informatique est condamnable (information / identifiants …)

III/ … Volet Jurisprudentiel

Condamnations :

- **Abus de confiance**, Stagiaire chinoise. Mais pas sur les fondements d'intrusion, d'accès STAD (*TGI de Versailles, 18 décembre 2007*)
- **Violation du secret des correspondances et accès frauduleux** à un système d'information & Recel des informations (*TGI Paris, 12ème chbre, 01/06/07, O. et Cie contre Thrinh Nghia T. et Trung T*)
- **Usurpation mot de passe / violation charte informatique** (*Cass, le 21/12/06, Monsieur P. contre société Ad 2 One SA*)
- **Maintien frauduleux** dans un SI : Neutralisation de la déconnexion automatique (*Tribunal Correct. Paris 1996 « Rafraîchissement d'écran »*)
- **Maintien illégal** après Accès régulier, pendant + 2 ans, à une BDD avec un code remis pour une simple période d'essai (*Cass. Crim 3 octobre 2007*)

Relaxes :

- Si le système n'est pas protégé et si celui qui le maîtrise n'a pas manifesté sa volonté d'en limiter l'accès : **Pas d'infraction** (*Paris 08/12/1997, Gaz Pal. 1998. 1, chron. Crim. 54*)
- **Pas de délit** de Maintien frauduleux dans un SI quand le site peut-être atteint par un logiciel grand public de navigation (*CA Paris, 11ème Chambre, 8 décembre 1997 & CA Paris, même Chbre. 30 octobre 2002 « Kitetoa »*)

III/ … Motivation politique

La Cyberdélinquance *(années 50, USA 1966, Finlande 1968)*

La protection contre l'espionnage

- ✓ Espionnage de la NSA avec le logiciel «**Promis**» vendu au monde entier *(Années 80-90)* intégration d'une puce électronique *SMART (Special Management Automate Resoning Tools) piégeant le logiciel.*

- ✓ NSA : Logiciel **ECHELON** (*1943-97 …*)
  Système mondial d'interception des communications privées et publiques (SIGINT), élaboré par les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande dans le cadre du traité UKUSA.
  Programme d'interception des e-mails, fax, télex et des communications téléphoniques via les réseaux de communications.

Réaction de l'Etat Français

- ✓ Réglementation en matière de protection des données
- ✓ Libéralisation du cryptage des informations de 40 à 128 bits en 1999 puis article 30 Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique « *I. - L'utilisation des moyens de cryptologie est libre.* »
- ✓ Lois sur le terrorisme

III/ … Législations étrangères

Elément constitutif : Présence ou violation d'un dispositif de sécurité

- Lois étrangères le retenant :

  Norvège, Finlande, Pays Bas, Suisse, Luxembourg …
- D'autres, comme la France, n'exige pas cette condition : Canada, Danemark, Royaume-Uni, Australie …

France :
« *La protection d'un système de traitement automatisé de données par un dispositif de sécurité n'est pas une condition de l'incrimination.* »
Jugement 31ème chambre correctionnelle du TGI Paris 18 septembre 2008

- **A noter**

Aux Etats-Unis : Infraction autonome du commerce des mots de passe et informations similaires permettant accès sans droit aux systèmes.

Signature de la Convention sur la cybercriminalité de Budapest *(2001)*
Objectif mener « *une* ***politique pénale commune*** *destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale* ».
42 États *dont les États-Unis, le Japon, l'Afrique et le Canada.*
France : entrée en vigueur 2006 (adoption du décret du 23 mai 2006).

IV

L'Audit intrusif
&
Le Droit

Audit intrusif : Déroulement

- Un test d'intrusion commence par une **reconnaissance** :
  - ✓ Récupération d'infos (*noms de domaines, Google, société.com, …*) :
  - ⇒ *Pas de difficulté notable, consiste en une récolte de données publiques.*

  - ✓ Scan protocolaire (*déterminer pour chaque machine les protocoles de transport fonctionnels : TCP, UDP, ICMP, …)*
  - ✓ Scan de ports TCP, UDP (*déterminer quels ports sont ouverts, fermés ou filtrés (firewall))*

- De la reconnaissance à **l'identification** :

  - ✓ Identification des systèmes d'exploitation (*LINUX, BSD, WINDOWS, …)*
  - ✓ Identification des services ainsi que de leur version (*Ex: port 80, serveur Apache, version xxx*).

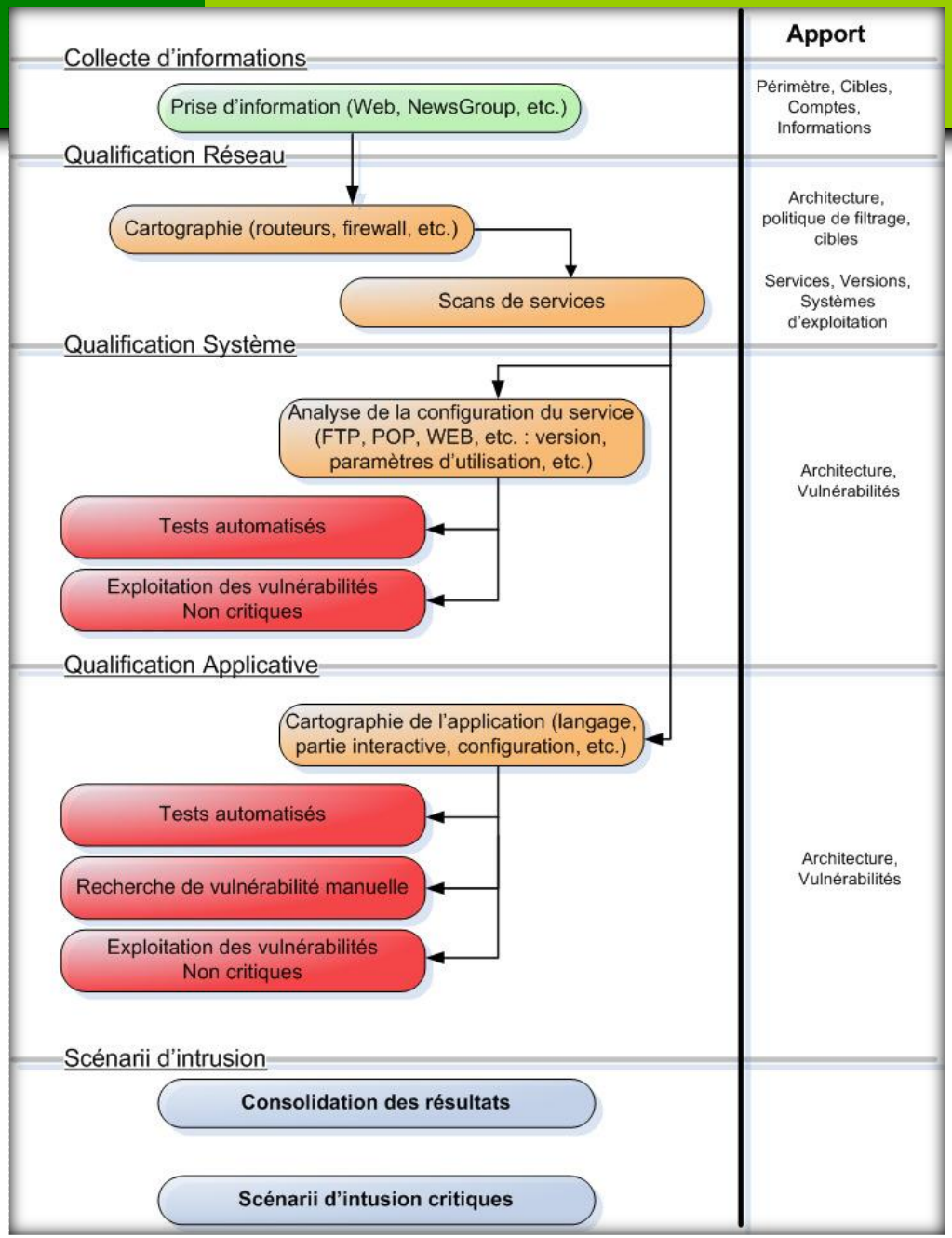
- De l'identification à la **recherche de vulnérabilité** :

  - ✓ Identification de vulnérabilités (*Ex utilisation de NESSUS.*)
  - ✓ Exploitation éventuelle des vulnérabilités

Audit intrusif :

Spécialiste
du test d'intrusion
doit savoir évoluer dans l'ensemble des couches du modèle OSI (*application, présentation, session, transport, réseau, liaison, physique*).

7	Couche Application
6	Couche Présentation
5	Couche Session
4	Couche Transport
3	Couche Réseau
2	Couche Liaison de données
1	Couche Physique



Légalité du Pen test

Le Pen test :

- Test applicatif : Recherche de vulnérabilités et de l'exploitation de failles.
- Eventuellement test poussé jusqu'à compromission machines (direct ou par rebond).

- **Les Risques :**
  - ✓ Le Déni de Service
  - ✓ L'atteinte à la confidentialité
  - ✓ Les droits de Propriété intellectuelle et / ou Industrielle
  - ✓ Etc.

- **Consiste en un accès illégal au STAD ?**

  « Légale » : Par le biais d'une autorisation explicite
  - ✓ Le réflexe contrat et NDA
  - ✓ Le strict respect des autorisations contractuelles

  - ✓ L'autorisation et les contrats permet la Maîtrise des Risques

Protection du prestataire de Sécurité : Clause limitative ou élusive de responsabilité (*Sous couvert de Bonne foi (art. 1134 al. 3 du Code civil) et à défaut de tout dol ou faute lourde).*

Légalité du Pen test : Jurisprudence

Le Pen test est-il un accès irrégulier ?

L'autorisation le rend licite : L'infraction n'est pas constituée en présence d'une habilitation *(Grenoble 2002).*

Le **retrait d'habilitation**, après accès, rend le maintien dans le SI illégal
(Paris 5 avril 1994 : D. 1994. IR. 130 ; JCP E 1995. I. 461, obs. Vivant et Le Stanc …).

Rappel :

Le Maintien dans un STAD doit être frauduleux ce qui suppose *la conscience pour les contrevenants de l'irrégularité de leurs actes.*

(Paris 15 décembre 1999 ; D 2000 IR 44 ; Gaz Pal. 2001. 1. Somm. 268, note Prat.)

V

De la légalité du Scan de Port

Audit intrusif : Le Scan de Port

- **Scan protocolaire** (*déterminer pour chaque machine les protocoles de transport fonctionnels : TCP, UDP, ICMP, ...)*

A ce niveau : Le Scan consiste à vérifier existence des protocoles de transport et non de leur utilisation effective.

Expert en sécurité :

Niveau 4 couche OSI. Faible risque de DoS. Pas d'accès au SI. Simple envoie de paquet pour réponse.

- **Scan de ports** TCP, UDP (*déterminer quels ports sont ouverts, fermés ou filtrés (firewall))*

Scan consiste à déterminer que les ports sont ouverts mais sans confirmer que le port est dédié à l'application supposée.

Scan : Protocole TCP : OK, Port 80 ouvert mais pas identifié si HTTP.

Expert en sécurité :

Niveau 7 couche OSI. Faible risque de DoS. Pas d'accès au SI. Simple envoie de paquet pour réponse.

Audit intrusif : Le Scan de Port

- De la reconnaissance à **l'identification** :

  - ✓ **Identification des systèmes d'exploitation** (*LINUX, BSD, WINDOWS, …)*

A ce niveau : Envoie de paquet pour réponse. Paquets reçus informations plus pertinentes.

Expert en sécurité :

« Ce n'est pas une requête habituelle ». Une 10aine de paquet Nmap envoyés, les réponses reçues permettent identification des SE.

Cependant aucune action réalisée, juste information. Pas d'accès au SI.

  - ✓ **Identification des services** ainsi que de leur version (*Ex: port 80, serveur Apache, version xxx*).

Expert en sécurité :

Niveau 7. Opération opérant un transfert de données. Requête au niveau du Service donc un accès. Test des services applicatifs. Risque de DoS

Permet identifier existence et utilisation application FTP, Apache sur le protocole HTTP permettant de visualiser des pages WEB, port 80 …

Audit intrusif : Le Scan de Port

- **Le Scan de Port** : Vue d'ensemble

✓ Découvrir l'architecture / les services de la cible (*routeurs et firewalls, relais applicatifs, répartiteurs et fermes de serveurs.*
Opération de balayage des ports : de 1 à 65535.

✓ Une « *technique consistant à balayer automatiquement, à l'aide d'un programme approprié, une série d'adresses IP spécifiques afin de trouver et d'examiner les ports ouverts sur chaque ordinateur,* (…) »

- Des outils :
Hping (*envoie de paquet vers port TCP – Réponse indique existence Port. Scan. Traceroute applicatif*). **Nmap** (*détecter port ouvert et identification service*). **Scapy** (*Scan. Traceroute applicatif. Et Pen test. Générer Paquet / Mais aussi intercepter paquet*)

- **Les ports** : « portes » / accès par lesquels une machine communique et échange des informations avec d'autres machines.

Analogie possible avec la **notion de domicile**

Le Scan de Port : Illégal ?

- **Des éléments de réponse** :

L'existant : Loi Godfrain

Art 323-3-1 Code pénal, *Loi n° 2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004* :

> « *Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.* »

Texte, initialement conçu pour lutter contre la **détention volontaire de programmes d'origine virale**.
Applicable cependant à la **simple détention de logiciels de scans** : Une présomption d'intention d'intrusion et autres infractions d'atteintes aux STAD.
Condition : « *Sans motif légitime* ». Or objectif possible : Sécurisation des réseaux.

La Pratique du Scan : Un acte préalable à une Attaque ?

Décembre 2005, **Chercheurs de l'Université du Maryland** :

✓ Un simple scan de port n'aboutit que très rarement à une attaque malveillante

✓ Seulement 5 % des attaques sont précédées d'un scan de port classique

Tendance : Scan mono-port et Worldwide (*Ex : port 21 FTP ou 25 SMTP sur un pull ip*).

Le Scan de Port : Illégal ?

- **Légalité du Scan de Port ?**
  La Réponse viendra des Juges

- **Deux approches** :
  - Le Scan est un accès à un SI :
    - ✓ L' Accès frauduleux : tous modes de pénétration irréguliers d'un STAD.
    - ✓ Induit une volonté de s'introduire ou de se maintenir
    - ✓ Induit un défaut d'autorisation lors de l'intrusion ou du maintien

  - Le Scan n'est pas un accès à un SI :
    - ✓ Pas d'Accès frauduleux
    - ✓ Pas de volonté de s'introduire ou de se maintenir
    - ✓ Pas de nécessité d'autorisation

- **Pas de précédant en droit Français** : Quelques pistes (*Décision Kitetoa et autres)*

Légalité du Scan de port … À l'étranger

USA

Scan **pas sanctionné** quand il ne permet pas d'accéder au réseau & que les données ne sont pas en danger.
US district court of Georgia, Moulton v. VC3, 2000 WL 3331091 (N.D. Ga., Nov. 7, 2000)

Droit Américain (*jurisprudence et législation*) **sanctionne** la pénétration quand :
Elle s'accompagne d'une utilisation non autorisée
ou
Inflige de dommages sur l'ordinateur et qu'il y ai intention de commettre un délit.

Israël

Relaxe de l'auteur d'un Scan du site web du Mossad poursuivi pour tentative d'accès non autorisé.
Hon. Abraham N. Tennenbaum (2004-02-29). "Verdict in the case Avi Mizrahi vs. Israeli Police Department of Prosecution.

Juge : *D'une certaine manière, les internautes qui vérifient les vulnérabilités des sites Web* ***agissent dans l'intérêt public****. Si leurs intentions ne sont pas malicieuses et ils ne causent pas de dommages, elles doivent même être félicitées.*

Légalité du Scan de port … En Europe

L'approche européenne

Plus strict : La pénétration au SI est un « crime » indépendamment de tout dommage causé. (*également adoptée par d'autres pays*)

Finlande

Cour suprême confirme verdict Cour Appel **condamnant** un JH de 17 ans pour intrusion dans le SI d'une banque finlandaise (balayage port réseau) *1 an emprisonnement et amende.*

Amende et 12000€ de dédommagements pour couvrir frais importants enquête par la banque. *Esa Halmari Attorney (2003), Retrieved 2009-05-07.*

Angleterre

Insertion nouvel article dans "the Police and Justice Act 2006" (Act of the UK Parliament).
Illégal « *fournir ou d'offrir de « l'offre » susceptible d'être utilisé pour commettre, ou pour aider à la perpétration d'une violation à la "Computer Misuse Act 1990"* ».
6 mois à 5 ans d'emprisonnement et amende.
Elément intentionnel.

Légalité du Scan de port … En Europe

Allemagne

Cadre légal
Section 202c StGB of the computer crime laws (*Code Pénal allemand*) :

Interdiction de « *posséder, vendre, distribuer, créer, utiliser des logiciels qui pourraient être utilisés (potentiellement) comme outils de piratage ».*

« *La simple possession d'outils … permettant recueillir ou d'accéder à système d'information … est un crime* ». 12 mois d'emprisonnement et amende.

Jurisprudence
Aucune poursuite à ce jour ;
Recherche en sécurité de SI a été ébranlée : abandon de nombreux projet de recherche.

Décision de la Cour constitutionnelle fédérale allemande, la sanction légale ne s'applique que dans le cas où le logiciel a été développé avec **l'intention** illégale à l'esprit.
(*18. Mai 2009)*

VI

Autres Techniques de Sécurité ou de « Pirate » & Légalité

Légalité du Scan de vulnérabilité

- De l'identification à la **recherche de vulnérabilité** :
  - ✓ Identification de vulnérabilités
  - ⇒ Identification des vulnérabilités par la comparaison des SE et versions des applications avec BDD de vulnérabilités (type Nessus).
  - ⇒ Utilisation de BDD NESSUS pas d'illégalité : ne consiste pas en un accès à un STAD.
  - ✓ **Exploitation** éventuelle des **vulnérabilités** :
  - ⇒ Peut être illégale si dépourvue d'autorisation : L'exploitation consistant à un accès voir une modification, suppression ou altération des données et risque de DoS.

- **Vulnérabilités** : *Faiblesses de conception, de mise en œuvre ou de l'utilisation d'un composant matériel ou logiciel du système.*

- **Exemples** :
  Prise de contrôle d'un système / d'une machine par un accès Root.
  Réception URL du référenceur permettant un accès sans demande d'authentification au webmail de ce dernier.
  Exécuter des commandes sur le système hébergeant l'application

Problématique de la publication des vulnérabilités

Légalité du “ Sniffing ”

Sniffing « écoute » d’un réseau et des paquets qui transitent
(*Résolution problématiques de sécurité réseau*)

- Logiciel de Sniffing, **packet sniffers** ou « renifleurs de paquets » : TCPdump, Wireshark
  Pas intrusif ; mais récupération info confidentielle.
  Permettent consultation aisée : données non-chiffrées et **intercepter des mots de passe qui transitent en clair ou toute autre information non-chiffrée** ….
- **Ecoute passive : Article 226-15 du code pénal**

Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.
Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.

- **Ecoute active :** ajout d’information dans les paquets ou modification de certains messages => Loi Godfrain

Nécessité d’autorisation même quand passive

Merci

www.itrust.fr/

A vos questions

contact@itrust.fr

ITrust | Immeuble ACTYS/1 Avenue l'Occitane BP 67303 | 31673 LABEGE CEDEX

Fixe Sdt. 09.80.08.36.12| Fax. 09.80.08.37.23|

http://www.itrust.fr/ | Assurance intégrité | Cabinet de conseil en sécurité informatique |

Jean Nicolas Piotrowski | Dirigeant | Mel. jn.piotrowski@itrust.fr | Tel. 06.76.40.88.41|

Didier Tassin | Directeur Commercial / Sales Manager | d.tassin@itrust.fr | 06.15.41.53.35

Yoann Garot | Chef de Projet et Service Juridique / Project Manager & Lawyer |
Mel. y.garot@itrust.fr | 06.64.27.89.92

Julien Lavesque | Directeur Technique Sentinel / Technical Director | Mel. j.lavesque@itrust.fr