HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

JSSI 2012

Aspects juridiques des tests d'intrusion

Frédéric Connes
<Frederic.Connes@hsc.fr>

Plan

- Typologie du test d'intrusion
- Le test d'intrusion logique technique
- Un outil d'intrusion particulier : l'ingénierie sociale

Typologie du test d'intrusion

- Selon son objet
  - Logique
    - Externe
    - Interne
  - Physique
- Selon sa méthode
  - Technique
  - Ruse (« ingénierie sociale »)
- Selon les connaissances préalables de l'auditeur
  - Boîte noire
  - Boîte grise
  - Boîte blanche

Test d'intrusion logique technique

- Cadre juridique
- Référentiel ANSSI et charte FPTI
- Convention d'audit
- Sous-traitance du test
- Passage par des intermédiaires
- Outils de test
- Absence de coopération de l'audité
- Dépôt de preuve d'intrusion
- Respect de la vie privée
- Non-respect de la convention d'audit
- Secret professionnel des auditeurs
- Infractions révélées par le test

Cadre juridique

- Systèmes de traitement automatisé de données (STAD)
  - Notion large

- Code pénal, art. 323-1
  - Le fait d'accéder ou de se maintenir, **frauduleusement**, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende
- Consentement de la victime = fait justificatif ?
  - Oui si l'existence de l'infraction suppose une **fraude**
- Donc un test d'intrusion est licite si consentement de l'audité
  - L'auditeur doit en conserver la preuve

Référentiel ANSSI et charte FPTI

- Référentiel d'exigences pour les prestataires d'audit de la SSI
  - ANSSI, version 1.0 du 31 octobre 2011
  - 24 pages
  - Plus large que les seuls tests d'intrusion
  - Labellisation possible à terme (procédure expérimentale)

- Charte de l'intrusion
  - Fédération des professionnels des tests intrusifs (FPTI)
  - Version 2.0 du 14 juin 2011
  - 10 articles
  - Moralité, transparence, confidentialité, probité

Convention d'audit

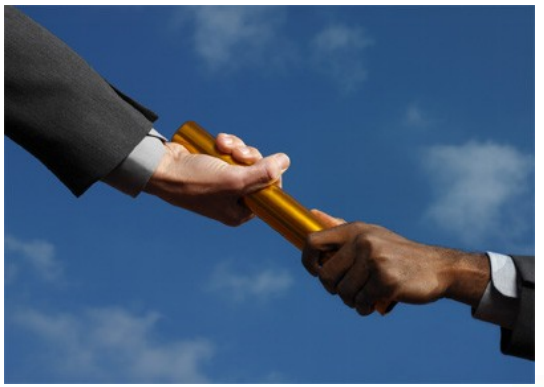
- Contenu minimum
  - Commanditaire du test, audité et auditeur
  - Autorisation de l'audité
  - Périmètre et modalités du test (IP, URL, dates, horaires...)
  - Obligation de moyens
  - Limites du test
  - Information sur les risques spécifiques au test
  - Clause d'éthique de l'auditeur
  - Clause de confidentialité imposée à l'auditeur et ses employés
  - Clause interdisant à l'auditeur de faire intervenir des personnes ayant été condamnées pour fraude informatique
  - Clause relative à la propriété intellectuelle
  - Livrables et présentation des résultats

Sous-traitance du test

- Loi du 31 décembre 1975, art. 3
- Code des marchés publics, art. 112

- Obligation de faire accepter chaque sous-traitant au moment de la conclusion et pendant toute la durée du contrat

- Conclure un contrat de sous-traitance

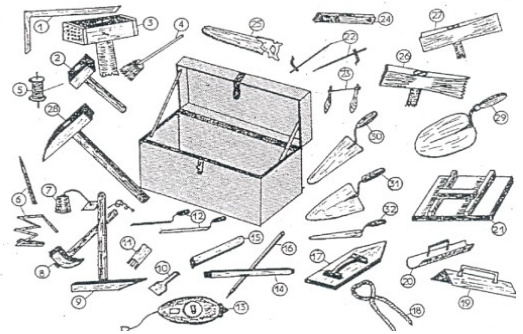


Passage par des intermédiaires

- Pour les tests externes
- CDN, hébergeurs, prestataires de *cloud computing*...
- A priori pas d'intrusion chez eux, mais risque de perturbations
  - Responsabilité civile
  - Code pénal, art. 323-2
    - Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende
- Voir leurs conditions d'utilisation du service
- Certains ont des procédures de signalement des tests d'intrusion

Outils de test

- Code pénal, art. 323-3-1
  - 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
- La réalisation de tests d'intrusion est-elle un motif légitime ?
- Faut-il être reconnu comme un professionnel de la sécurité informatique ?
  - Si oui, comment ?



Absence de coopération de l'audité

- Quand l'audité n'est pas le commanditaire
- Exemple de document rédigé par un cabinet d'avocat pour dissuader l'auditeur avant le début du test
- Exemple de comportement visant à empêcher le test
- Comment l'auditeur doit-il réagir ?

- Idéalement, prévoir le cas dans la convention d'audit

Dépôt de preuve d'intrusion

- Code pénal, art. 323-3
  - Le fait d'**introduire frauduleusement des données** dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende
- Frauduleusement = sans autorisation
- Donc mentionner explicitement le droit de déposer des preuves d'intrusion dans la convention d'audit

Respect de la vie privée

- Limite à ne pas franchir
- Code civil, art. 9
  - Chacun a droit au respect de sa vie privée
- Loi du 10 juillet 1991
  - Le secret des correspondances émises par la voie des communications électroniques est garanti par la loi
- Code pénal, art. 226-15, al. 2
  - Est puni d'un an d'emprisonnement et de 45 000 euros d'amende 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

Non-respect de la convention d'audit

- Attaque dirigée contre un tiers
  - Adresses IP/URL erronées et non vérifiées par l'auditeur
  - Faute de frappe dans les IP/URL par l'auditeur
  - Scan de ports licite ?
    - Pas d'accès à un STAD
    - Pas d'entrave si pas massif
    - Pas de tentative (acte préparatoire)

  - Erreur de fait : supprime l'élément intentionnel de l'infraction
  - Mais si manipulation du commanditaire : complicité
    - Code pénal, art. 121-7, al. 2
    - Est complice la personne qui par don, promesse, menace, ordre, abus d'autorité ou de pouvoir aura provoqué à une infraction ou donné des instructions pour la commettre
  - Responsabilité civile

Non-respect de la convention d'audit

- Dommage collatéral occasionné par le test
  - Code pénal, art. 323-2
    - Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende

  - Code pénal, art. 323-3
    - Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende
  - Responsabilité civile et assurance
  - Le recours à des outils de test automatisés ne réduit pas la responsabilité

Secret professionnel des auditeurs

- Code pénal, art. 226-13
  - La **révélation** d'une information à caractère **secret** par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende

- Responsabilité civile
  - Clause de confidentialité dans la convention d'audit
  - Clause de confidentialité dans les contrats de travail des auditeurs

Infractions révélées par le test

- L'auditeur est-il tenu de les dénoncer ?
- Cas général
  - Code pénal, art. 223-6, al. 1er
    - Quiconque pouvant empêcher par son action immédiate, sans risque pour lui ou pour les tiers, soit un **crime**, soit un **délit contre l'intégrité corporelle** de la personne s'abstient volontairement de le faire est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende
  - Code pénal, art. 434-1, al. 1er
    - Le fait, pour quiconque ayant connaissance d'un **crime** dont il est encore possible de prévenir ou de limiter les effets, ou dont les auteurs sont susceptibles de commettre de nouveaux crimes qui pourraient être empêchés, de ne pas en informer les autorités judiciaires ou administratives est puni de trois ans d'emprisonnement et de 45 000 euros d'amende

Infractions révélées par le test

- Fonctionnaires
  - Code de procédure pénale, art. 40, al. 2
    - Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un **crime** ou d'un **délit** est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs

Outil particulier : ingénierie sociale

- Usurpation d'identité
- Vol d'information
- Escroquerie
- Collecte déloyale de données personnelles

Usurpation d'identité

- Nouvelle infraction depuis la LOPPSI
- Code pénal, art. 226-4-1
  - Le fait d'**usurper** l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa **tranquillité** ou celle d'autrui, ou de porter atteinte à son **honneur** ou à sa **considération**, est puni d'un an d'emprisonnement et de 15 000 euros d'amende
  - Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne
- Pas d'infraction si la personne dont l'identité est usurpée est consentante
- Sinon : risque à son égard, pas à l'égard de la personne « ciblée » par l'ingénierie sociale

Vol d'information

- Code pénal, art. 311-1
  - Le vol est la soustraction frauduleuse de la chose d'autrui
- Pendant longtemps
  - Copie d'informations sans soustraction de support = pas de vol
- Tribunal correctionnel de Clermont-Ferrand, 26 septembre 2011
  - Condamnation pour vol alors que pas de soustraction de support
  - Décision isolée ou début de reconnaissance du vol d'information ?
- Si reconnaissance du vol d'information
  - Potentiellement applicable à l'ingénierie sociale
  - Il n'y a pas soustraction frauduleuse si l'audité a consenti préalablement à la soustraction de données

Escroquerie

- Code pénal, art. 313-1
  - L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de **tromper** une personne physique ou morale et de la déterminer ainsi, à son **préjudice** ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un **bien quelconque**, à fournir un service ou à consentir un acte opérant obligation ou décharge
  - L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende

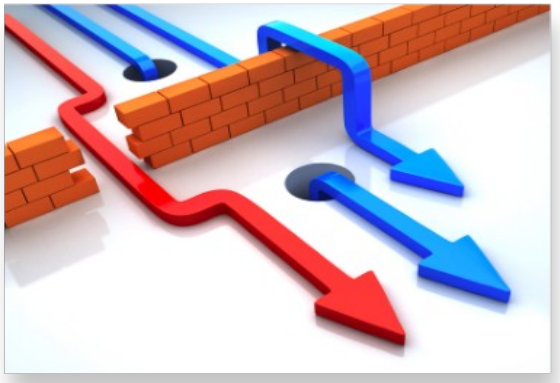
- Notion de « bien quelconque »
- Pas de préjudice de l'audité

Collecte déloyale

- Loi du 6 janvier 1978, art. 6, 1°
  - Les données sont collectées et traitées de manière loyale et licite
- Code pénal, art. 226-18
  - Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende
- Collecte de données permettant d'identifier des personnes physiques
- Déloyal = à l'insu des personnes concernées
- Or, par hypothèse, les personnes ne peuvent pas être informées

Conclusion

- Tout test d'intrusion présente des risques juridiques pour l'auditeur
- Risques souvent négligés ou ignorés
- Importance de la convention d'audit
  - Très précise sur la cible
  - Exhaustive sur les possibilités et outils de l'auditeur
    - Notamment si ingénierie sociale ou intrusion physique
  - Validée par un juriste et un technique
- Les auditeurs doivent être conscients des limites à ne pas franchir
  - Ils doivent donc être formés aux risques juridiques



Références

- Fédération des professionnels des tests intrusifs (FPTI)
  - http://www.fpti.pro/
- ANSSI, Référentiel d'exigences pour les prestataires d'audit de la sécurité des systèmes d'information
  - 31 octobre 2011
  - http://www.ssi.gouv.fr/IMG/pdf/referentiel-exigences_labellisation_prestataires-audit-teleservices_v1-0.pdf
  - La section 2.4 traite des tests d'intrusion
- Y. Garot, Les aspects juridiques du scan & des tests intrusifs
  - JSSI, 2010
  - http://www.itrust.fr/images/stories/ressources/jssi_legalite_scan_intrusif_outil_securite_y_garot_mars2010.pdf

Références

- M. Barel, Pentests : réveillez-moi, je suis en plein cauchemar !
  - SSTIC, 2008
  - http://actes.sstic.org/SSTIC08/Pentests_Cauchemar/SSTIC08-article-Barel-Pentests_Cauchemar.pdf
- CLUSIF, Test d'intrusion
  - Mars 2004
  - http://www.clusif.asso.fr/fr/production/ouvrages/pdf/TestIntrusion.pdf
  - Document de synthèse de la commission réseaux et systèmes ouverts du CLUSIF sur les objectifs du test d'intrusion, son déroulement et les mesures à prendre

Questions