Pentests : réveillez-moi, je suis en plein cauchemar !

Marie Barel

Silicomp-AQL Orange Business Services
1, rue de la Châtaigneraie CS 51766.
35517 Cesson-Sévigné Cedex
Tel. +33 2 99 12 50 00 Fax. +33 2 99 63 70 40
contact : marie.barel@aql.fr

Résumé : Les prestations d'audit et de tests d'intrusion sont utiles aux entreprises qui souhaitent mettre à l'épreuve la sécurité de leur environnement et évaluer leur résistance à un certain niveau d'attaque. Toutefois, si un test d'intrusion « réussi » (c'est-à-dire permettant de démontrer des failles dans la sécurité d'un système d'information) est un argument de poids pour la sensibilisation des acteurs et en particulier celle des décideurs, ces tests, et en particulier ceux réalisés sans la connaissance préalable de l'environnement (type boîte noire, auxquels nous limiterons la présente étude), ne sont pas sans risques. L'objectif de la présente conférence sera notamment d'examiner les « effets de bord » possibles, tant sous l'angle technique que juridique (section 1), et d'envisager les mesures à mettre en œuvre en particulier au plan contractuel ou contraire, ce qu'il convient d'éviter ou de faire pour limiter son risque, du point de vue de l'auditeur comme celui de l'audité (section 2).

1 Événements indésirables et risques de non-conformité

Vous êtes auditeur dans une SSII offrant des services de conseil et d'audit dans le domaine de la sécurité ou bien encore une organisation en charge de la défense des systèmes d'information. Vos missions consistent à détecter et exploiter des vulnérabilités d'un SI cible : après une cartographie du réseau à distance, vous avez défini votre cible, découvert les services qui y sont accessibles ainsi que les équipements et machines qui les supportent ; vous avez construit une stratégie offensive (« arbre d'attaque »), rédigé des scripts d'attaque pour exploiter les vulnérabilités que vous avez préalablement identifiées (vulnérabilités réseau, systèmes ou, le plus souvent, applicatives) et très vite, vous avez réussi à « décrocher le Graal », en laissant des traces de votre passage sur le SI de votre Client (par le dépôt d'un fichier), voire en collectant des « preuves » (par exemple un *flag* positionné sur le SI par le responsable du système ou de simples copies d'écran qui viendront illustrer votre rapport d'audit). Votre mission est un « succès » ! Je vous invite maintenant à explorer vos pires cauchemars ...

Et si tout n'avait été pour le mieux dans le « meilleur des mondes » ? Qu'aurait-il pu se produire qui transforme cette mission en « voyage en eaux troubles » ? De nombreux événements sont susceptibles de modifier le scénario de cette mission accomplie sans encombre et avec succès ...

Notre ambition ne sera pas d'en faire une liste exhaustive mais au moins d'en relever un certain nombre susceptible d'illustrer différents risques d' « écarts à la loi » ou au contrat que nous commenterons en termes de risques juridiques avant d'envisager, dans le cadre de la section 2, les enseignements à tirer de ces hypothèses multiples. Attention !, les évènements cités dans le présent article relatent des scenarii entièrement fictifs ; tout rapprochement avec des faits, des entités ou des situations réelles est fortuit :-)

1.1 Evènements liés au SI cible et au périmètre d'intervention et risques associés

- Le prestataire mène des investigations sur un système sans y être autorisé (cas des tests avant vente) ;
- Le prestataire réalise des investigations sur une ou des parties du système non prévues dans le contrat (dépassement du périmètre défini dans le contrat) ;
- Le prestataire mène des investigations sur un système qui n'appartient pas au Client (en général, un Client communique une liste d'adresses IP à tester – ou , dans le cas le plus fréquent du test « en aveugle », une adresse de sous réseau ; toutefois, les problèmes liés à l'adressage restent très communs, soit du fait même du client – l'information fournie est mauvaise – soit en raison d'une simple erreur de frappe de la part de l'auditeur) ;
- Le système audité est sous la responsabilité de plusieurs entités. Le domaine de responsabilité du Client de l'audit n'en couvre qu'une partie ;
- Le système audité est hébergé par un tiers et cet hébergement de ressources est mutualisé avec d'autres organisations ;
- La prestation de test intrusif conduit à attaquer des éléments d'un système tiers (opérateur de télécommunications, fournisseur d'accès à l'Internet, fournisseur d'hébergement, ...)
- (...)

Tous ces évènements font naître un risque de non-conformité susceptible d'engager la responsabilité du Prestataire de service[1] en charge de conduire les tests d'intrusion. Parmi les fondements envisageables figure au premier chef la responsabilité contractuelle dans la relation du Prestataire avec son Client mais aussi la responsabilité civile, notamment quasi-délictuelle (article 1383 du Code civil) vis-à-vis des tiers au contrat de tests intrusifs dont le SI aurait été audité suite par exemple à une négligence du Prestataire qui n'a pas validé avec le Client le périmètre et l'adressage du réseau à auditer. De plus, un autre fondement possible serait encore celui de l'accès et du maintien frauduleux sur un « système de traitement automatisé de données ». En particulier en cas d' « investigations » sur un système qui n'est pas celui du Client, l'article 323-1 du Code pénal n'est-il pas susceptible de s'appliquer ?

Rappelons ici que l'incrimination d'accès frauduleux nécessite en particulier de rapporter la preuve de la matérialité de l'infraction. En pratique, les faits retenus par les tribunaux sont souvent d'une grande simplicité et ils condamnent sur ce fondement tout accès irrégulier, entendu tant au sens actif : « *tous modes de pénétration* » (Cour d'appel de Paris, 5 avril 1994), que passif :

[1] Voire la responsabilité de l'auditeur, personne physique ayant réalisé les tests, dans le cadre notamment de la responsabilité pénale qui est, rappelons-le, une responsabilité *personnelle*. Dans le cas des délits informatiques (notamment l'infraction d'accès frauduleux à un système), le code prévoit cependant aussi la responsabilité pénale de la personne morale (article 323-6 du Code pénal) ...

notamment la mise sur écoute et la captation de paquets ou de trames circulant sur un réseau au moyen d'un *sniffer*.

Toutefois, il faut encore rapporter la preuve de l'intention frauduleuse de l'auteur de l'infraction, c'est-à-dire que s'agissant ici d'un délit dit volontaire, le prévenu doit encore avoir agi « *sans droit* » et « *en connaissance de cause* » (cf. arrêt précité de la Cour d'appel de Paris) :

- l'absence de droit résulte, selon un autre arrêt de la Cour d'appel de Toulouse (31ème chambre, 21 janvier 1999) « *de l'absence d'autorisation expresse du maître du système* » – étant observé cependant, comme le souligne la doctrine qui commente cet arrêt (Voir Lamy Informatique) que le caractère « exprès » ne s'impose vraisemblablement pas car la présence d'un dispositif de sécurité n'est pas une condition de l'incrimination (du moins, ajouterons-nous, pour les parties du SI qui n'hébergent pas de données à caractère personnel[2] : conséquences de l'obligation de sécurité prévue à l'article 34 de la loi Informatique et Libertés telle que modifiée par la loi du 6 août 2004 et du « revirement » enregistré à l'occasion de l'affaire Tati c. Kitetoa[3]). Illustration plus récente avec l'arrêt du TGI de Vannes du 13 juillet 2005 – Université de Bretagne Sud / M. A et *alii* : à propos d'étudiants ayant pénétré sur le réseau pédagogique de leur Université après avoir utilisé un logiciel de déchiffrement des mots de passe (*John the Ripper*) qu'ils avaient téléchargé sur Internet[4] pour accéder à certains comptes utilisateurs après en avoir déchiffré les identifiants et mots de passe : « *l'infraction est constituée dès lors qu'une personne, non habilitée, pénètre dans ce système en sachant être dépourvue d'autorisation, peu importe le mobile* » (en l'occurrence « le défi sous forme technologique propre à la jeunesse »- sans conséquences préjudiciables pour les comptes utilisateurs).
- En second lieu, l'agissement « en connaissance de cause » signifie que l'attaquant ne doit pas avoir agi par erreur et qu'il a conscience de l'irrégularité de son acte. A cet égard, il est important de bien distinguer la volonté du mobile qui, lui est indifférent à la qualification de l'infraction En effet, en droit pénal, l'acte conscient et volontaire est intentionnel quel qu'en soit le mobile, louable ou non (R. Merle et A. Vitu, *Traité de droit criminel*, T.1 – Ed. Cujas, 7è édition ; J. Pradel, *Traité de droit pénal*, T.1 – Ed. Cujas, 1999) ; la motivation de l'auteur (par exemple l'amélioration de la sécurité des systèmes[5] ou la critique des choix de la direction informatique) ne supprime donc pas l'intention frauduleuse. La volonté est bien ce qui détermine l'infraction, alors que le mobile tente d'en justifier la commission, d'y apporter

[2] Sur ce point, lire nos développements dans l'article *Honeypots, un pot pourri juridique* – Actes de la conférence du SSTIC 2004, pages 7 et suivantes : `http://actes.sstic.org/SSTIC04/Droit_et_honeypots/SSTIC04-article-Barel-Droit_et_honeypots.pdf`

[3] Cour d'appel de Paris, 30 octobre 2002

[4] A ce titre, l'un des étudiants était poursuivi sur le fondement de l'article 323-3-1 nouveau du Code pénal dont ce fut l'une des premières applications après son adoption dans le cadre de la loi pour la Confiance de l'économie numérique (LCEN) du 21 juin 2004 et qui incrimine notamment l'acquisition et la détention d'outils de piratage. Sur cette disposition, voir plus loin nos développements (section 1.2).

[5] TGI de Paris, 2 juin 2006 : au sujet d'un informaticien condamné pour accès frauduleux et entrave au fonctionnement d'un SI, qui avait pris le contrôle du serveur d'une société, à partir duquel il avait lancé des attaques systématiques vers 457 sites gouvernementaux et privés dans le but de dénoncer leurs failles de sécurité.

une raison, un motif[6].

En définitive, on peut penser en conséquence de ce qui précède que la croyance légitime d'un Prestataire d'agir, moyennant autorisation et dans le périmètre réseau d'un Client, enlèverait le caractère frauduleux à un acte d'accès irrégulier commis par hypothèse (voir *supra*) sur le SI d'un tiers ou une partie du SI Client qui ne ressortirait pas en réalité de son domaine de responsabilité.

Dans tous les cas, force est de rappeler cependant que si une action en responsabilité pénale pour accès frauduleux était introduite, celle-ci étant une responsabilité personnelle (non assurable) pourrait peser directement sur les auditeurs (chargés de tests) ou bien, en vertu de l'article 323-6 du code pénal, sur le Prestataire en tant que personne morale.

S'agissant de l'hypothèse soulevée plus haut d'une action sur le fondement de la responsabilité contractuelle, le partage de responsabilité entre le Prestataire et le Client aura été préalablement aménagé entre les parties et il conviendra en conséquence de se reporter aux dispositions du contrat pour établir s'il y a eu ou non manquement à une obligation contractuelle. Concernant ensuite les « investigations » réalisées par les chargés de tests sur des parties du SI ou des réseaux relevant de la responsabilité de prestataires techniques ou d'opérateurs en relation avec le SI du Client : FAI, hébergeur dont les ressources sont mutualisées, réseau de transit ..., les risques induits par les opérations de tests devront être couverts par des autorisations expresses des maîtres de ces différents systèmes ou réseaux.

Ainsi, nous verrons à la section 2.2 quelles sont les dispositions clés des contrats de tests d'intrusion qu'il convient par conséquent de prévoir ainsi que les étapes de validation des tests à mettre en œuvre et les autorisations à obtenir pour garantir le bon déroulement des opérations d'audit.

1.2 Evènements liés aux outils et méthodes des tests d'intrusion et risques associés

Pour mener à bien des tests d'intrusion externes, l'auditeur agit généralement depuis une plateforme de tests comprenant différents environnements systèmes ainsi qu'une « boîte à outils » dans laquelle on trouvera :

- des outils dits « passifs », utilisés dans la phase de découverte du réseau, appelée cartographie ou prise d'empreintes : parmi eux, un logiciel de la famille des *sniffers* (*Wireshark* par exemple) va écouter les paquets échangés sur le réseau, permettant ainsi d'auditer et de contrôler les types de données circulant sur le réseau. Le chargé de test fera aussi appel dans cette première étape à : des scanners de ports tels que *Nmap, hping* ou *netcat*, pour identifier sur un équipement donné l'ensemble des services et ports ouverts ou bien encore la version des logiciels installés sur l'équipement (IIS ou Apache pour un serveur Web par exemple) ; des outils permettant d'analyser les résolutions des serveurs DNS (tels que *Dig ou NSlookup*) et de déterminer ainsi des erreurs de configuration ou de pressentir le rôle des différents équipements, et ; des scanners de vulnérabilités (*Nessus*, qui peut être aussi utilisé pour l'administration de réseau, est parmi les plus connus des outils de tests automatisés), pour mettre en évidence les vulnérabilités potentielles (les vulnérabilités applicatives sont aujourd'hui les plus nombreuses) ;

[6] De même, lorsque la loi prévoit un dol spécial (par exemple, les actes de terrorisme supposent, pour emporter cette qualification, le " but de troubler gravement l'ordre public, ou la terreur "), celui-ci ne se confond pas avec le mobile : le dol spécial est invariable pour une même infraction, quel que soit le ou les auteurs, tandis que le mobile, lui, reste personnel et varie suivant l'auteur.

– des outils dits « offensifs », intervenant dans une seconde étape dédiée à l'exploitation des vulnérabilités identifiées précédemment : il existe notamment des « librairies » d'*exploits* telles que *Metasploit* qui regroupe un ensemble de codes d'exploitation de vulnérabilités. On utilise aussi des bases *d'exploits* personnels et un compilateur C pour les outils « maison », et bien entendu , des casseurs de mots de passe comme *Cain & Abel* et *John The Ripper*, qui opèrent en mode dictionnaire ou force brute ...

Hormis ces outils génériques qui adressent un périmètre important, il est possible de recourir à des applications dédiées à des besoins plus spécifiques : *Kismet* et *Aircrack* pour le Wi-Fi par exemple, et d'autres pour la ToIP.

D'ores et déjà, il apparaît à l'énoncé de cette liste d'outils, que les logiciels libres sont très présents, ce qui permet souvent de couvrir des domaines délaissés par les programmes propriétaires, mais présente parfois des problèmes dans la gestion des mises à jour (plus ou moins rapprochées suivant les versions) et, contrairement à l'idée répandue, dans la gestion des licences (risque d'effet contaminant des outils sous licence GPL dont une partie du code serait intégrée dans les outils « maison » du Prestataire par exemple).

Ensuite, au-delà de la compétence des chargés des tests (dont l'intuition et l'expérience seront tout aussi déterminantes dans le succès de leur mission[7]), la confiance et surtout la maîtrise des outils utilisés sont essentielles au bon déroulement des opérations de test. A défaut, on peut redouter plusieurs évènements :

– Absence de maîtrise des outils utilisés par le Prestataire causant des dommages sur le SI cible :
  – le Prestataire atteint la disponibilité du système engendrant un déni de service ;
  – le Prestataire atteint l'intégrité du système (exemple du paramétrage des systèmes d'exploitation)

Là encore, c'est la responsabilité contractuelle du Prestataire qui peut être engagée dans les limites prévues en matière de responsabilité et d'assurance[8] d'une part, et des dispositions ou annexes au contrat qui décrivent les outils et méthodes autorisés dans le cadre des opérations de test (se reporter à la section 2.2) d'autre part.

– Risques réalisés pendant la période des tests ou liés à la persistance des outils installés par le Prestataire (certains outils restent actifs après l'audit) :
  – un pirate exploite une « porte dérobée » (*backdoor*) installée par le Prestataire dans le cadre de ses tests et l'exploite pour mener une attaque contre le Client ou un tiers,
  – un pirate exploite les vulnérabilités du système permettant la réalisation d'un rebond dans le but d'attaquer un autre système sortant du domaine de responsabilité du Client et interconnecté à celui-ci,
  – Un pirate récupère un outil développé (signé) et utilisé par le Prestataire pour pénétrer le système cible et l'utilise pour attaquer un autre système.

L'un des fondements de la responsabilité susceptible d'être engagée ici (tant pour le Prestataire que pour le Client « hébergeant » lesdits outils) est celui de l'article 323-3-1 du code pénal qui incrimine, en amont, le fait notamment de détenir, offrir, céder ou mettre à disposition des outils de piratage (c'est-à-dire tout « équipement, programme informatique, instrument ou toute donnée »,

[7] En effet, les outils de tests automatisés ont leurs limites. Ainsi un outil tel que *Nessus* peut remonter de fausses alertes (faux positifs) ou, plus grave, ne pas détecter certaines vulnérabilités (faux négatifs). C'est la compétence et l'expérience du chargé de test qui permettra ici de combler les « défaillances » de l'outil ...

[8] A cet égard, l'indemnisation négociée est toujours plafonnée et ne dépasse pas généralement la limite du montant du contrat lui-même.

« conçus ou spécialement adaptés pour commettre l'une des infractions prévues aux articles 323-1 et suivants du code pénal »).[9] En effet, si le bénéfice de l'exception de « motif légitime » prévu par le législateur paraît acquise pour le Prestataire, il en va différemment concernant le Client et dans tous les cas, les faits de mise à disposition (y inclus notamment la création d'un lien hypertexte vers un site permettant de télécharger lesdits outils), doivent être appréhendés avec prudence et donner lieu à des mesures de prévention dans le cadre de bonnes pratiques (voir section 2).

D'autres situations à risque sont encore :

– L'utilisation d'outils permettant de récupérer ou d'intercepter des correspondances présentes sur le SI du Client ou échangées sur le réseau cible (mise en place d'un *snifer* sur le réseau par exemple).

Dans ce cas de figure, et dans le contexte en particulier des audits « boîte noire », c'est l'article 226-15 du code pénal[10] qui est susceptible de s'appliquer. A cet égard, rappelons que la jurisprudence considère que constitue une interception la lecture et la retranscription de messages dès lors que celles-ci ont nécessité une dérivation ou un branchement et sont effectuées moyennant un artifice ou un stratagème (sur ce point, lire la décision de la Cour d'appel de Paris du 17 décembre 2001 – Affaire du laboratoire PNMH, à propos de la mise sous surveillance et de l'accès au contenu de la boîte de courrier électronique d'un étudiant, contrôles effectués à partir du serveur de la messagerie et non pas au travers d'un dispositif installé sur le PC de l'utilisateur).

S'agissant ensuite de l'accès aux contenus, l'autorisation du maître du système n'enlèverait pas le caractère frauduleux à l'acte d'interception dans la mesure où ce dernier n'est lui-même pas autorisé à accéder au contenu des messages personnels des Utilisateurs du SI, exception faite des administrateurs de systèmes et réseaux qui ont en charge d'assurer leur fonctionnement normal ainsi que leur sécurité (jurisprudence précitée[11]). Pour plus de détails concernant ce point, lire nos développements à la section 1.3.

– Le recours aux techniques de rétro conception logicielle pour mettre à jour des vulnérabilités d'un système ou application propriétaire du SI Client.

Dans ce cas en effet, le risque de contrefaçon existe, la finalité recherchée étant étrangère aux exceptions légales prévues par le Code de Propriété intellectuelle[12], notamment le droit de décompilation à des fins d'interopérabilité. Dès lors, dans l'hypothèse d'applications développées par un presta-

---

[9] Pour un commentaire de cet article adopté dans le cadre de la Loi sur la Confiance dans l'Economie numérique (LCEN) du 21 juin 2004 et sous l'impulsion de la Convention sur la Cybercriminalité, lire notre article : *Nouvel article 323-3-1 du Code pénal, cheval de Troie du législateur ?* –MISC n°14 (2004) ; Sécurité informatique / SSI, sept. 2005 (lettre du CNRS, n°54) `http://www.sg.cnrs.fr/FSD/securite-systemes/revues-pdf/num54.pdf`

[10] Ce texte dispose que : *« 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. »

[11] Texte de la décision sur : `http://www.foruminternet.org/telechargement/documents/ca-par20011217.pdf`

[12] Lire sur ce sujet notre article paru à la revue Techniques de l'Ingénieurs / SSI : *le reverse légal existe-t-il ?* – mars 2007

taire[13], il convient que le Client signale au Prestataire l'existence de droits de propriété de tiers sur un ou plusieurs éléments du système, auquel cas, sauf accord du titulaire de droits, l'utilisation des techniques de *reverse engeneering* devrait être exclue du champ des méthodologies autorisées dans le cadre de l'audit.

1.3 Evènements liés aux résultats des tests et risques associés

Les hypothèses définies au présent paragraphe peuvent être notamment :

- Un utilisateur, non averti de l'audit en cours, constate des événements qu'il juge comme étant des infractions (accès frauduleux) et déclenche une alerte qui aboutit à un dépôt de plainte contre le Prestataire.
  A cet égard, la recommandation posée plus haut concernant la communication des adresses sources utilisées dans le cadre des opérations de test par le Prestataire présente ici l'intérêt d'éviter ces « faux positifs ».
- La perturbation du fonctionnement du système audité (fonctionnement nominal d'une machine, diminution de la bande passante du réseau)
- Le Prestataire a accès à des informations confidentielles du Client ou dévoile les résultats de l'audit à une tierce personne.

Dans ces deux derniers cas de figure, c'est la responsabilité contractuelle du Prestataire qui est en jeu. Rappelons ici en effet le principe suivant lequel, dans la jurisprudence française, la responsabilité contractuelle et la responsabilité civile délictuelle sont exclusives l'une de l'autre c'est-à-dire qu'à partir du moment où il existe un lien contractuel (fût-ce un simple ticket de transport), on ne peut invoquer la responsabilité civile délictuelle, même en cas de faute.

- L'auditeur accède à des informations personnelles traitées par le système audité.

S'agissant de l'accès à des fichiers d'un Utilisateur signalés comme « personnels », en cas de « risque ou évènement particulier » ou en la présence du titulaire de la boîte de messagerie ou bien encore celui-ci « dûment informé » (arrêt Cathnet-Science du 17 mai 2005), ou s'agissant de la présomption de caractère professionnel posée par deux décisions du 18 octobre 2006 à l'égard des « fichiers », non signalés comme personnel, présents sur le disque dur des ordinateurs mis à disposition par un employeur, on peut douter dans un premier temps de leur applicabilité en matière de correspondances. En effet, si on peut techniquement assimiler les correspondances à des fichiers, le droit pénal est soumis à un principe d'interprétation stricte et les correspondances bénéficient quant à elles d'un régime de protection spécifique qui leur donne, en tant que fichier, une nature particulière (comme les fichiers de données à caractère personnel qui sont eux aussi l'objet de droits et obligations propres).

Affinant toutefois sa jurisprudence en matière de courrier électronique sur le lieu du travail, la chambre sociale de la Cour de cassation, dans un arrêt « Phone House » du 30 mais 3007[14], a invité les juges du fond à « *rechercher si les fichiers ouverts sur le matériel mis à sa disposition par l'employeur avaient été identifiés comme personnels par le salarié* » pour définir le champ de la protection des correspondances au titre de l'atteinte à la vie privée (article 8 de la Convention européenne de Sauvegarde des Droits de l'Homme et des Libertés).

En définitive, il convient pour les chargés de tests d'adopter la même attitude que celle ainsi prescrite au juge pour prévenir tout risque de violation des droits des Utilisateurs du SI audité et

[13] Rappelons en effet que les droits afférents à des développements logiciels réalisés en interne sont automatiquement dévolus à l'employeur ...

[14] Texte de la décision sur : `http://www.legalis.net/jurisprudence-decision.php3?id_article=1947`

de s'interdire tout accès au contenu de fichiers ou correspondances portant une indication manifeste de leur nature privée. Si on prend en considération les aboutissants de l'affaire Cathnet-Science précitée en matière de fichiers personnels et que l'on admet éventuellement sa transposition aux courriers électroniques, il conviendrait le cas échéant d' « informer dûment » ces mêmes Utilisateurs du déroulement de tests intrusifs pouvant conduire à l'accès aux contenus. En pratique, au-delà du fait que les tests portent en fait généralement sur des serveurs plutôt que les postes Clients, le risque que cette information préalable modifie les résultats du test apparaissent assez mineurs[15] dans la mesure où il supposerait que les équipes d'administration et d'exploitation aient des capacités réelles et suffisantes de réaction sur incident (existence d'une *response team* interne à l'entreprise auditée). De plus, dans tous les cas de figure et pour éviter une montée en escalade sur un incident déclenché par les opérations de test, il convient que le Prestataire communique à son Client les adresses sources utilisées par les chargés de tests afin que ceux-ci puissent être identifiés et permettre alors de qualifier un incident intervenant pendant la période de test. Reste en suspens la question de savoir si cette information préalable des Utilisateurs du SI serait vraiment suffisante car elle ne constituerait qu'un consentement implicite en l'absence de tout droit d'opposition, ce qui ne nous semble pas conforme à la nature des exceptions prévues dans le cadre de jurisprudence visée plus haut.

– La mise en évidence d'événements ou d'éléments du système pouvant être pénalement répréhensibles : cas de la découverte d'images pédophiles sur le SI du Client.

En cas d'accès à des données qui sont manifestement illicites (étant supposé par ailleurs que cet accès aux contenus litigieux ne soit pas entaché d'illégalité – cf. supra), l'attitude appropriée consiste à dénoncer les faits auprès du Client qui est celui dont la responsabilité est susceptible d'être engagée. En aucun cas le Prestataire ne devrait se substituer au Client pour décider de la façon de gérer ces situations. A l'inverse, s'abstenir de relater ce type d'incident survenu au cours d'opérations de tests intrusifs et garder le silence « en connaissance de cause » pourrait faire revêtir l'habit du complice et prendre la forme d'une aide ou d'une assistance, dans la mesure où l'absence de dénonciation permet à l'auteur du délit de poursuivre ses agissements.

2 Mesures de gestion du risque

Il convient maintenant d'examiner comment il convient de gérer les risques envisagés jusqu'ici à savoir, en particulier, au travers de la contractualisation de la prestation de test d'intrusion et aussi par différents engagements matérialisés par la référence à une Charte de déontologie (section 2.2). Mais auparavant, de même que la protection du SI dépend fortement de la sensibilisation des Utilisateurs aux risques liés à la sécurité, ce sont les Prestataires qui doivent rappeler à leurs équipes certains « fondamentaux » permettant simplement d'éviter ou de voir se réaliser les risques envisagés précédemment (section 2.1).

2.1 Connaître les situations à risque et les erreurs à éviter

Après avoir envisagé un certain nombre d'évènements indésirables et les risques de non conformité associés, il convient d'alerter sur les situations qui augmentent la probabilité d'occurrence de ces évènements et risques envisagés à la section 1.

[15] Sauf le cas bien entendu où les techniques de *social engeneering* font partie des méthodes appliquées et autorisées par le Client dans le cadre des tests, auquel cas une information préalable pourrait rendre les Utilisateurs du SI plus vigilants ...

Il s'agit par exemple de :
- plages d'adresses importantes augmentant le risque d'erreur sur la cible ;
- scans semi automatisés, qui s'exécutent pendant le week-end et en l'absence de tout personnel susceptible de détecter des « effets de bord » sur le SI Client et entraînant par exemple le verrouillage des systèmes de sécurité ;
- tests « boîte noire » sur un SI truffé d'applications propriétaires aux interactions imprévisibles
- (...)

Par ailleurs, on peut recenser également quelques unes des erreurs à éviter. Ainsi, on peut d'ores et déjà mentionner au rang des « facteurs critiques de succès » d'une mission de test d'intrusion les points suivants :

1. méconnaître les limites des outils utilisés (cas de *nmap* cité dans la revue MISC[16] [1] ...) et leurs possibles « effets collatéraux » : cas des outils qui, lorsqu'ils sont exécutés, injectent un *malware* à l'insu du chargé de test ; d'autres outils encore sont programmés pour collecter et transférer vers un point source (à l'insu de leur utilisateur) les vulnérabilités identifiées au cours des tests intrusifs dans le cadre desquels ils sont mis en œuvre.

   A la différence des attaques logiques réelles, Patrick Chambet [4] nous rappelle également que, à moins d'une autorisation expresse du Client, il faut se garder de :
2. perturber le système cible (donc pas de déni de service sans prévenir, par exemple, même pour faciliter une autre attaque) ;
3. implanter une charge utile : *rootkit*, cheval de Troie, code hostile, bombe logique, ...
4. modifier toute donnée sur la cible, et en particulier, effacer ses traces dans les *logs*. A l'inverse, comme souligné plus haut dans nos développements (cf. *supra* section 1), il convient toujours d'avancer « à visage découvert » et de préserver la traçabilité des actions effectuées sur le système.

2.2 Mesures contractuelles et bonnes pratiques

2.2.1 Le contrat de test d'intrusion .

Au premier rang des dispositions clés du contrat, le Préambule est malheureusement souvent négligé. C'est pourtant au sein de cette disposition à part entière du contrat que le contexte de la mission doit être décrit (domaine d'activité du Client, biens sensibles du SI audité, raisons du choix du Prestataire, ...), et au sein de laquelle le juge recherchera souvent « l'intention des parties » pour apprécier le reste du contrat.

L'autorisation de réaliser les tests intrusifs est bien entendu déterminante puisqu'elle conditionne d'éventuelles poursuites sur le fondement des articles 323-1 et suivants du code pénal. De même,

[16] Première limite mise en lumière dans le cadre de l'utilisation de ce scanner : tandis que l'on s'attend à ce que tous les ports, de 1 à 65535, soient passés en revue, « seuls les ports référencés dans le fichier *nmap-services* (il y en a 2276) sont utilisés. En d'autres mots, moins de 3,5 % de l'espace est couvert. » Autre limite citée : *« Les subtilités : pour obtenir une bonne vision du réseau distant, tous les détails comptent. En particulier, chaque réponse à un stimulus doit être analysée. Recevoir un* TCP Reset *en réponse à un* TCP SYN*, ne veut pas dire la même chose que de recevoir un* ICMP port unreachable*, qui est encore différent d'un* ICMP host administratively pohibited*. Des scanners comme* nmap*, qui réduisent tout à* open*,* closed *ou* filtered*, sont tout juste bons à faire le gros du travail, mais certainement pas les finitions.* »

corrélativement, la vérification de la qualité et des pouvoirs de la personne représentant le Client et portant sa signature au contrat sont essentielles pour la protection du Prestataire. Toutefois, le lancement des opérations de test doit encore être suspendu jusqu'à l'obtention des autorisations de tiers, sociétés partenaires du Client, hébergeant par exemple une partie du SI audité sur des machines mutualisées, ou bien encore détentrices de droits de propriété intellectuelle sur des applications propriétaires développées pour le compte du Client.

Le cœur des dispositions décrira ensuite les modalités de réalisation de la mission propres à garantir le bon déroulement des opérations d'audit, en particulier :

- la désignation des outils et techniques autorisés, mention le plus souvent générique, par opposition à la mention spécifique de prestations « exclues » telles que le *social engeneering* ou les opérations de déni de service conduisant à un arrêt définitif d'un équipement ;
- les délais de réalisation, qui conditionnent la période de légalité des tests ou bien, s'agissant d'une approche « boîte blanche », la période d'attribution des droits et habilitations sur le SI. Part ailleurs, le Client précisera le cas échéant le respect de certaines dates et plages horaires lors des opérations du Prestataire suivant la charge de certaines ressources du SI.
- la désignation de responsables de projet (« correspondants ») avec la fourniture de coordonnées détaillées et notamment d'un numéro de téléphone portable à contacter en cas d'urgence. Le Correspondant du Prestataire aura notamment la responsabilité d'informer le Client en cas de découverte d'une vulnérabilité critique pour laquelle il conviendrait de prendre immédiatement des mesures correctives ;
- les étapes de validation au cours de la mission. En particulier, avec le Clusif [3], on peut recommander :
  - une étape de validation du périmètre de l'intrusion (appartenance des adresses IP, données collectées au cours de la phase d'exploration et de cartographie du réseau cible) : le Prestataire fournira par exemple le schéma de topologie du réseau vu de l'extérieur et demandera au Client de valider que les éléments identifiés lui appartiennent bien et sont inclus dans la couverture du contrat ;
  - une étape de validation après la phase de recherche de vulnérabilités : lorsqu'une vulnérabilité majeure est identifiée, pouvant atteindre le fonctionnement du système ou l'intégrité des données, le Prestataire sollicite une autorisation expresse du Client pour pouvoir l'exploiter et tester plus en profondeur le SI ; de plus, en cas de découverte d'une faille critique, le Prestataire avertira immédiatement le Client pour lui permettre d'appliquer des correctifs et parer ainsi une éventuelle attaque réelle qui pourrait survenir à tout moment.
- les ressources mises à disposition par le Prestataire. A cet égard, il convient que le Client porte une attention particulière à la sélection des profils des chargés de test qui lui est soumise car le succès d'une campagne de tests repose pour une part importante sur la compétence des auditeurs. C'est pourquoi il demandera que le contrat soit signé *intuitu personae* ...

S'agissant de la présentation des résultats, le Prestataire fournira des enregistrements horodatés de l'ensemble des actions qu'il a menées. De plus, les livrables (dont la propriété intellectuelle sera classiquement cédée au Client) comporteront un rapport managérial dans lequel les faits marquants et les résultats les plus pertinents seront extraits dans la perspective d'une sensibilisation de la direction.

En dernier lieu, au-delà des dispositions classiques (mais non moins essentielles) en matière de confidentialité et d'assurances, un soin particulier sera apporté à la définition des responsabilités entre le Prestataire et son Client. A cet égard, il convient que le contrat de test intrusif sensibilise le Client aux risques auxquels il s'expose et que le Prestataire, conformément à son devoir d'infor-

mation, de conseil et d'alerte, lui donne des préconisations, notamment la consigne de réaliser une sauvegarde (*back up*) nécessaire à la sécurité de ses données, informations et programmes. Le Prestataire soulignera également les limites d'un test d'intrusion dont l'exhaustivité d'une part n'est pas garantie et qui, dès lors, n'est pas non plus la preuve de la sécurité d'un système. Ainsi, le résultat d'un test se réduit à savoir si un environnement testé a résisté aux attaques pendant le laps de temps imparti[17] et les obligations du Prestataire dans le cadre du contrat relève des obligations de moyens.

2.2.2 Déontologie : à propos d'éthique .

Parmi les mesures à prendre en compte du côté du Client (audité), le groupe de travail du Clusif [3] a émis un certain nombre de recommandations tendant à s'assurer notamment de la compétence professionnelle du Prestataire et des intervenants (chargés de tests). En effet, la méthodologie des tests d'intrusion techniques, qui sont nécessairement empiriques et itératifs, ne permet pas de garantir l'exhaustivité des résultats ni la maîtrise des conditions d'exécution et de réalisation. Aussi, en cas de « réussite » (c'est-à-dire comme nous l'indiquions en préambule, lorsque le test d'intrusion permet de démontrer des failles de sécurité du SI), le principal risque d'un test d'intrusion n'est-il pas en définitive le manque de connaissances et de compétence de l'auditeur et un défaut de professionnalisme du Prestataire ? Dès lors, le respect d'un Code d'éthique formalisé est un facteur de confiance dans la compétence professionnelle et le sérieux du Prestataire.

La Charte de la Fédération des Professionnels des Tests Intrusifs [2] définit par exemple un ensemble de règles d'exercice de leurs activités par les professionnels de l'Intrusion. Les quatre principes fondateurs de cette Charte sont énoncés comme suit :

- le *principe de moralité* : le Prestataire s'engage en particulier à ne pas employer de « hackers » pour l'exécution de ses activités. A noter également que le Prestataire devra être vigilant vis-à-vis d'éventuels « sous-traitants » car force est de rappeler ici que, même en l'absence de fondement textuel, la jurisprudence française a reconnu la responsabilité contractuelle du fait d'autrui [18]
- le *principe de transparence* : ce principe emporte notamment obligation pour le Prestataire de fournir à première demande du Client toutes informations relatives à son identité, son personnel, ses partenaires ou sous traitants, ses méthodologies et pratiques utilisées pour ses opérations d'intrusion, sous réserves de la protection de son savoir faire ;
- le *principe de confidentialité* : ce principe garantit le respect de la plus stricte confidentialité sur toutes les informations dont le Prestataire et les membres de son personnel pourra avoir connaissance, sur la base du besoin d'en connaître et au travers d'engagements individuels ;

[17] Pour obtenir un niveau d'assurance suffisant sur la sécurité d'un environnement informatique, un audit de sécurité prenant en compte les aspects organisationnels et procéduraux en plus des questions techniques permettra de mieux répondre à ces attentes.

[18] Voir par exemple en matière de fourniture de logiciel – Cass.1ère civ., 18 oct. 1960 : JCP 1960, II, 18446, note R. Savatier ; Cass. civ., 29 mai 1963 : *Gaz. Pal.*1963, 2ème sem., p. 290 *: « le débiteur est responsable du fait de l'inexécution de ses obligations, alors même que cette inexécution proviendrait d'un tiers qu'il se serait substitué »* ; ainsi, le débiteur qui se fait remplacer ou aider par un tiers pour l'exécution de ses obligations contractuelles doit répondre à l'égard de son cocontractant du fait de celui qu'il s'est substitué.

- le *principe de probité* : le Prestataire doit agir en toute loyauté et n'effectuer de tests intrusifs que dans le strict cadre d'un mandat préalable et express.
  Dès lors :
  - il s'interdit toute prestation d'intrusion « avant vente » ;
  - il s'astreint à n'effectuer de prestations d'intrusion qu'après vérification des pouvoirs du mandant (périmètre sous la responsabilité du Client) ;
  - toutes prestations d'ingénierie sociale ne sauraient être effectuées sans signature préalable d'un mandat explicite spécifique.

En conclusion. – Les prestations de test intrusif ne sont pas des prestations « ordinaires ». Elles comportent des risques qui doivent être correctement appréhendés et maîtrisés au travers d'un échange d'informations précis et d'engagements respectifs du Client audité et du Prestataire. A cet égard, le contrat signé constituera la clé de voûte de la confiance entre les parties et le gage d'un bon déroulement des opérations ...

3 REFERENCES

1. *Tests d'intrusion : comment évaluer la sécurité de ses systèmes et réseaux ?* – MISC, Hors-série n°1 (Oct./Nov. 2007)
2. Charte FTPI - `http://www.freesec.net/pro_charte.htm`
3. *Test d'intrusion* – Document technique du CLUSIF (mars 2004)
4. *Les tests d'intrusion externes : tests d'intrusion réseau, système, applicatifs* – Patrick Chambet (MISC 11) : `http://www.chambet.com/publications/Lestestsd'intrusion.pdf`