Document Technique

TEST D'INTRUSION

Mars 2004

Commission Réseaux et Systèmes Ouverts

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS
30, Rue Pierre Semard
Téléphone : 01 53 25 08 80 Fax : 01 53 25 08 88
Mail : clusif@clusif.asso.fr Web : http://www.clusif.asso.fr

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Julien	**AIRAUD**	**ETUDIANT – UNIVERSITE DE LIMOGES**
Philippe	**BOUVIER**	**THALES SECURE SOLUTION**
Eric	**CHASSARD**	**CSC - PEAT MARWICK FRANCE**
Paul	**CONSTANT**	**PAUL CONSTANT**
Jean-François	**GONEL**	**AGENCE FRANCE PRESSE**
Xavier	**GUILLOT**	**ETUDIANT – UNIVERSITE DE LIMOGES**
Vincent	**MARET**	**ERNST & YOUNG AUDIT**
Lazaro	**PEJSACHOWICZ**	**CNAMTS**
Paul	**RICHY**	**FRANCE TELECOM**
Hervé	**SCHAUER**	**HSC**
Laurence	**SELIGMANN**	**THALES SYSTEMES AEROPORTES**

TABLE DES MATIERES

1 INTRODUCTION

L'objectif de ce document de synthèse relatif aux tests d'intrusion des accès Internet, est de fournir des éléments sur l'intérêt et les limites de cette démarche dans le cadre d'une politique de sécurité en entreprise.

La commission regroupant offreurs et utilisateurs a permis d'établir une première approche de langage commun autour du service « tests d'intrusion » afin que les attentes des utilisateurs soient correctement prises en compte par les pratiques des offreurs. Ce document vise aussi à mettre en exergue le niveau de maturité actuel d'un test d'intrusion dont la démarche s'inscrit pleinement dans les plans de sécurisation établis par les RSSI.

Le caractère contractuel, méthodique, transparent, et l'environnement législatif dans lesquels se déroulent ces tests d'intrusion pratiqués par les véritables professionnels reconnus du domaine, ont depuis longtemps maintenant, balayé l'image sulfureuse des tests pratiqués par quelques « bidouilleurs avisés » à l'insu du fonctionnement officiel du SI.

Bien qu'il existe différents types de tests d'intrusion, nous nous limiterons volontairement aux tests permettant une intrusion depuis Internet.

2 OBJECTIFS, AVANTAGES ET LIMITES DES TESTS D'INTRUSION

Les principes de réalisation des tests d'intrusion présentent, par rapport à d'autres méthodes d'analyse de la sécurité, des avantages, mais aussi des limites. Il convient donc de bien mesurer ces insuffisances, et de les mettre en perspective avec les objectifs que l'on veut atteindre.

2.1 Objectifs pouvant être satisfaits par des tests d'intrusion

2.1.1 Mettre à l'épreuve la sécurité d'un environnement et qualifier sa résistance à un certain niveau d'attaque.

Les tests d'intrusion peuvent en effet être comparés à certaines méthodes de qualification du monde industriel (résistance de coffre-forts, endurance de moteurs d'avions) où l'on vérifie que le mécanisme testé résiste pendant un certain temps à des attaques ou des agressions d'un niveau défini. Dans le cas des tests d'intrusion, le résultat se réduit à savoir si l'environnement testé a résisté aux attaques pendant le laps de temps imparti (en général quelques jours). Si tel est le cas, alors on peut supposer que la plupart des attaquants n'iront pas aussi loin.

Cette approche a l'avantage de permettre de tirer des enseignements d'un test qui échoue, c'est-à-dire pour lesquels aucune intrusion n'a pu être réalisée dans le laps de temps imparti. On peut donc supposer que la sécurité existante est adaptée au niveau de risque accepté. Il convient de définir très précisément, avant le test, la durée du test et ce qui sera considéré comme une intrusion afin de pouvoir tirer précisément des enseignements en matière de résistance à l'intrusion.

2.1.2 Sensibiliser les acteurs (management, informaticiens, utilisateurs) au sein de l'entreprise.

Les tests d'intrusions sont particulièrement efficaces pour sensibiliser les acteurs. En effet, par rapport à des méthodes d'analyse de la sécurité comme l'audit, le test d'intrusion, s'il "réussit", permet de disposer d'arguments de poids pour inciter les acteurs à prendre conscience des risques. Il peut même être envisagé de récolter des « preuves » pour convaincre les plus récalcitrants. Les tests d'intrusion permettent également d'illustrer les problèmes de sécurité issus des interactions complexes et non prévues, interactions qui sont parfois difficiles à appréhender lors d'audits de sécurité se focalisant sur des points de contrôle « atomiques ».

Toutefois, il faut considérer le risque que les tests d'intrusion n'aboutissent pas à des résultats concluants. Dans ce cas là, le pouvoir de sensibilisation des acteurs devient inexistant. Au contraire, certains peuvent croire, à la robustesse du système.

2.2 Tests de vulnérabilités

Un test de vulnérabilités est un test d'identification de failles connues. Le résultat du test de vulnérabilités est un tableau synthétique, avec pour chaque faille, la liste des machines ou équipements qui semblent vulnérables. Un test d'intrusion commence par une phase de recherche de vulnérabilités. Celle-ci ne donne généralement pas lieu à la délivrance d'un tableau des vulnérabilités, car elle sert d'entrée pour les phases suivantes du test d'intrusion. Lors d'un test d'intrusion, l'équipe de test va tenter de mettre en oeuvre les vulnérabilités trouvées, utiliser les

inter-dépendances entre ces vulnérabilités, et essayer d'aller plus loin. Ce n'est pas le cas lors d'un test de vulnérabilités. Le test de vulnérabilités est réalisable de manière automatique, et proposé en mode ASP par certains fournisseurs. Il est court et peu coûteux, donc peut être réalisé avec une fréquence plus importante que les tests d'intrusion.

Enfin, le test d'intrusion réalisé par une équipe permettra de détecter des vulnérabilités qu'un test de vulnérabilité ne verra pas.

2.3 Objectifs ne pouvant être satisfaits par des tests d'intrusion

2.3.1 Avoir l'assurance qu'un environnement informatique est sécurisé.

Un test d'intrusion ne peut constituer la preuve de la sécurité d'un environnement. Si aucune vulnérabilité significative n'est mise en évidence lors des tests, il est impossible de conclure que l'environnement testé est sécurisé. En effet, on ne peut exclure que les testeurs n'aient pas identifié certaines vulnérabilités existantes, par manque de connaissance ou de moyens, ou parce que ces vulnérabilités ne peuvent pas être mises en évidence directement dans les conditions des tests d'intrusion. On ne peut pas non plus exclure que, dans le futur, des vulnérabilités apparaissent au sein des briques logicielles constituant l'environnement ou que son paramétrage de sécurité soit modifié.

Pour obtenir un niveau d'assurance suffisant sur la sécurité d'un environnement informatique, il est plus légitime de réaliser un audit de sécurité, qui prend notamment en compte les aspects procéduraux et organisationnels, en plus des questions techniques.

2.3.2 Identifier exhaustivement les vulnérabilités de sécurité d'un environnement.

Comme les autres méthodes, un test d'intrusion ne permet pas d'être certain que toutes les vulnérabilités existantes au sein d'un environnement seront identifiées. Une fois une vulnérabilité identifiée sur un système et utilisée pour en prendre le contrôle, une personne réalisant un test d'intrusion aura tendance à s'occuper d'un autre système, sans tenter d'identifier d'autres vulnérabilités sur le système dont elle vient de prendre le contrôle. Or il est tout à fait possible que plusieurs vulnérabilités de sécurité existent sur ce système. Par ailleurs, un test d'intrusion ne permet en général pas de détecter d'éventuelles vulnérabilités dans les couches de protection au delà de la première couche présentant un niveau de sécurité suffisant.

Il faut également noter que des tests d'intrusion ne permettent pas d'identifier directement les faiblesses de sécurité d'ordre organisationnel et procédural, et se limitent aux faiblesses techniques.

3 ACTEURS D'UN TEST D'INTRUSION

On peut considérer qu'il y a deux grandes catégories d'acteurs :

- Les acteurs internes : l'entreprise souhaitant effectuer ce test.
- Les acteurs externes : le prestataire de service proposant cette prestation, les fournisseurs d'accès, les hébergeurs. Ce prestataire pourrait être interne à l'entreprise s'il dispose des compétences et d'une indépendance suffisante.

A priori, tous les acteurs internes à l'entreprise sont concernés par le test d'intrusion, « ce n'est pas le seul problème du RSSI ! ». Afin de limiter au maximum les risques de perturbations opérationnelles, des précautions d'organisation sont à prendre vis à vis des intervenants lors du déroulement du test. Un des objectifs étant la sensibilisation du management et des utilisateurs, aussi bien aux attaques venant de l'extérieur que de l'intérieur de l'entreprise, le test d'intrusion doit faire l'objet a posteriori d'une large communication en interne. Cette communication doit être ciblée et, bien sûr, porter un message de sécurité sans pour autant informer sur les vulnérabilités non traitées..

Dans un cadre plus technique, la direction informatique dans son ensemble est concernée par ces tests ainsi que les filiales et/ou les sociétés rattachées dans le cas de réseaux WAN ou d'intranet, perspective qui peut être étendue aux clients de l'entreprise dans le cadre d'un extranet

Les principaux acteurs externes à l'entreprise sont :

- les sociétés de service proposant ce type de prestation. L'entreprise doit rechercher des acteurs fiables et professionnels. Ces acteurs externes doivent attacher un intérêt tout particulier à la confidentialité de leur acte et surtout rassurer l'entreprise désireuse de réaliser ce test qui pourrait les percevoir comme des « pirates ». Ils se doivent également d'offrir toutes les garanties nécessaires à l'entreprise ; les spécialistes de ces sociétés sont à recenser individuellement avec leurs compétences spécifiques.
- le propriétaire ou le responsable légal de la structure concernée par ce test d'intrusion dans le cas où l'entreprise aurait externalisé ses serveurs. Dans un tel cas, il convient de prévoir la possibilité de ce type de test dès le départ dans le contrat d'externalisation. Si la structure est mutualisée ou non visible directement, par exemple dans le cas d'un serveur partagé entre plusieurs entreprises, le test d'intrusion ne peut être envisagé de par cette structure particulière.

L'entreprise, le prestataire de service et l'éventuel hébergeur doivent analyser avec une attention toute particulière, le contexte organisationnel autour du système d'information objet du contrat des tests d'intrusion ; en particulier, les engagements doivent correspondre au périmètre réel de responsabilité des acteurs engagés.

4 DEROULEMENT D'UNE MISSION DE TEST D'INTRUSION TYPE DEPUIS INTERNET

L'objectif d'une telle mission est d'évaluer le risque qu'une personne malveillante puisse s'introduire dans le réseau informatique interne de l'entreprise (le demandeur) via son réseau d'interconnexion à Internet.

Une mission de ce genre est généralement réalisée par le prestataire depuis un environnement dédié, comme par exemple un laboratoire de tests d'intrusion.

Ce type de mission peut débuter sans information préalable provenant du demandeur. De manière générale, le déroulement d'une mission de test d'intrusion de type « en aveugle » ou « *zero knowledge* » depuis Internet comporte trois phases principales :

4.1 Phase 1 : Découvertes initiales

L'objectif de cette phase est de rechercher des informations significatives permettant de découvrir puis valider le périmètre de l'intrusion.

Dans un premier temps, le prestataire s'attache à cerner la connectivité Internet du demandeur. Afin de mener à bien cette recherche, il consulte diverses bases de données publiques sur Internet (notamment les enregistrements *Whois*) pour identifier les plans de nommage, d'adressage et le ou les fournisseurs d'accès utilisés par l'entreprise. Il vérifie par ailleurs l'appartenance des adresses IP concernées par le test d'intrusion. Il complète sa recherche via de nombreuses sources de données publiques, sites Web du demandeur, les forums, les serveurs de news, etc. Ces renseignements fournissent éventuellement des informations complémentaires sur les éléments réseaux et logiciels qui sont détenus par l'entreprise.

Le résultat de cette phase permet d'identifier la présence de l'entreprise perçue depuis Internet. Il est recommandé de faire valider par le demandeur ces informations afin de poursuivre cette phase d'exploration. Cette validation, permet d'engager le demandeur (face au contrat) et d'informer le prestataire qui est ainsi certain que les éléments qu'il va tester par la suite sont bien des éléments appartenant au demandeur et sont bien inclus dans la couverture du contrat.

Puis le prestataire passe à l'identification de la topologie du réseau de l'entreprise vue depuis Internet. Pour cela, il identifie les machines accessibles à partir d'Internet à l'aide d'outils faiblement intrusifs (type DNS et reverse DNS, transfert de zone, traceroute, ping, etc.). Ensuite il détermine les caractéristiques et les rôles de ces machines afin de comprendre la topologie du réseau d'interconnexion à Internet. Il aura ainsi une représentation graphique de cette topologie du réseau et des éléments cibles qui sont identifiables depuis Internet.

A la fin de cette phase il est recommandé que le prestataire communique au demandeur les résultats de sa découverte du réseau (schéma de la topologie du réseau vu d'Internet). Le demandeur valide ensuite le périmètre à couvrir par le prestataire en Phase 2.

4.2 Phase 2 : Recherche d'informations et de vulnérabilités

L'objectif de cette phase est de rechercher des vulnérabilités potentielles sur les machines identifiées dans le périmètre de la phase 1.

Pour chacune des machines présentes dans la topologie de raccordement à Internet, le prestataire complète sa recherche par des techniques plus intrusives qui permettent d'identifier l'ensemble des services actifs sur ces éléments, d'analyser les configurations des éléments, etc.

Le résultat de cette recherche permet de mettre en évidence un certain nombre de vulnérabilités potentielles qui pourraient exister sur les machines cibles et qui pourraient être exploitées pour s'y introduire : version ou correctif non à jour, configuration incomplète, etc.

Etape de validation : lorsque le prestataire découvre une vulnérabilité majeure pouvant porter atteinte à la disponibilité ou à l'intégrité des données de l'entreprise, nous recommandons qu'il en fasse part à celle-ci. Sans un accord formel de cette dernière, le prestataire ne doit pas exploiter ce type de vulnérabilité.

4.3 Phase 3 : Exploitation des vulnérabilités et intrusion

L'objectif de cette phase est d'exploiter les vulnérabilités identifiées lors de la phase 2, dans le but de s'introduire sur les machines de l'entreprise à partir de l'accès Internet.

Cette phase est la plus technique. En effet, le prestataire teste et tente d'exploiter les vulnérabilités mises en évidence lors de la phase précédente. Dans le cas d'une intrusion logique sur un serveur, il doit prouver l'intrusion :

- En fournissant au demandeur des informations confidentielles sur le Système d'Information, en accord avec les objectifs et les obligations contractuelles.
- En démontrant qu'il a pu écrire ou modifier des données, par le dépôt d'un fichier particulier par exemple.

Cette phase n'aboutit pas automatiquement à la prise de contrôle total d'un ou de plusieurs éléments du système d'information. En effet, le prestataire peut simplement obtenir des privilèges lui permettant de rebondir et de poursuivre l'intrusion vers le réseau interne – à condition de ne pas sortir du périmètre défini contractuellement – en reproduisant le schéma utilisé depuis Internet : processus d'analyse du nouvel environnement, d'énumération puis d'exploitation des vulnérabilités, etc.

5 MESURES A PRENDRE DU COTE DU DEMANDEUR

Il est recommandé que le demandeur prenne en compte certaines bonnes pratiques qui permettent de s'assurer de la meilleure adéquation des résultats de la mission avec les objectifs de l'entreprise. Ces mesures ont notamment pour objectifs :

- D'analyser l'expérience professionnelle du prestataire.
- De s'assurer de la qualité du déroulement et du résultat de la prestation.
- D'obtenir une bonne intégration des résultats avec les objectifs de l'entreprise.

Exemples des mesures à prendre avant de lancer une mission de ce type :

- Définir l'objectif et les conditions de validation de l'objectif.
- Nommer un unique coordinateur interne afin d'assurer la relation avec le prestataire. Ce coordinateur peut être accompagné par des personnes de différentes compétences techniques.
- Définir un coordinateur chez le prestataire afin de n'avoir qu'une seule personne à contacter en cas de nécessité (échanger les numéros de portable).
- Informer les acteurs internes de l'entreprise que des tests d'intrusion sont parfois réalisés au cours de l'année.
- Exiger un contrat signé avec le prestataire en incluant éventuellement la couverture des risques par une société d'assurance.
- Exiger un contrat signé entre le prestataire et les éventuels hébergeurs concernés par les tests, en incluant éventuellement la couverture des risques par une société d'assurance.
- Demander au prestataire de communiquer par écrit la liste des adresses réseaux IP sources qui seront utilisées lors des tests d'intrusion. La communication des adresses IP sources doit être perçue comme un moyen pour le demandeur de faire la différence entre le test d'intrusion et les possibles réelles intrusions.
- Communiquer au prestataire par écrit la liste des adresses réseaux IP incluses dans le périmètre de la mission. Cette communication peut être réalisée tout au long de la mission en fonction des éléments découverts par le prestataire. Par défaut, il faut convenir avec le prestataire qu'aucune adresse réseau ne peut être la cible d'un test sans accord formalisé préalable.
- Eventuellement, inclure dans le contrat la destruction par le prestataire de l'ensemble des informations recueillies dans le cadre de la mission. Notons que dans ce cas, le prestataire pourra demander au demandeur de signer un Procès Verbal de fin de prestation décrivant la taille du rapport remis, les taches qui ont été effectuées par le prestataire, le nom des personnes ayant réalisé la prestation et la durée de la prestation.
- Faire valider le contrat reçu du prestataire par le service juridique.
- Recommander aux techniciens de ne pas modifier la configuration des éléments du SI pendant les tests : d'une part cela fausse les résultats et d'autres part des modifications réalisées sans suivre les procédures internes peuvent générer des dysfonctionnements dans le SI.

- Convenir avec le prestataire d'un moyen d'échange sécurisé des informations au cours de la mission.

Exemples des mesures à prendre pour s'assurer de la compétence professionnelle du prestataire :

- Demander si le prestataire possède un Code d'Ethique formalisé et respecté.
- Demander la typologie des attaques qui seront réalisées et la liste des outils potentiellement utilisés.
- Demander une liste de références de mission précédentes dans le domaine des tests d'intrusion.
- Demander les CV des intervenants ainsi que leur rôle dans la mission et le temps qu'ils y passeront.
- Demander les moyens dont dispose le prestataire. Par exemple dans le cas d'un laboratoire de tests d'intrusion, visiter éventuellement ce laboratoire.
- Faire préciser au prestataire la manière dont sera gérée la confidentialité des résultats tout au long de la mission et après la fin de la mission.

Exemples de mesures à prendre pour cadrer la mission :

- Définir les moyens auxquels le prestataire peut recourir.
- Définir une date de début et de fin de la prestation.
- Définir les étapes intermédiaires de validation des différentes phases de la prestation afin de bien maîtriser le déroulement de la prestation.
- Préciser le respect de certaines dates et plages horaires lors des actions du prestataire suivant la charge de certaines ressources du SI.
- Assurer la traçabilité (journalisation) des actions du prestataire en s'assurant que le prestataire fournira des enregistrements horodatés de l'ensemble des actions qu'il a menées.

Exemples de mesures à prendre pour préciser la rédaction du rapport :

- Définir le contenu du rapport : par exemple la synthèse doit être compréhensible par la Direction Générale, les descriptions techniques sont reportées en annexe, le corps du rapport doit rappeler l'ensemble des vulnérabilité classées par niveau de risque, etc.
- Définir le niveau de granularité de description des tests en précisant notamment la méthode utilisée, le résultat obtenu, les risques éventuels et les recommandations à apporter.
- Exiger une qualité de la rédaction en français (ou en anglais) si la diffusion du rapport final concerne des personnes non techniques.
- Demander au prestataire de compléter éventuellement les rapports de pré-validation (échange de fichiers non modifiables pdf, etc.) afin d'expliquer certaines parties puis valider le rapport final du prestataire.

Exemples de mesures à prendre pour valoriser les résultats de la mission :

- Analyser les conclusions du rapport et réévaluer les risques en fonction des risques réels de l'entreprise : par exemple pour déclarer qu'un accès à des données doit être classé critique pour l'entreprise il faut par avance avoir réalisé une classification des données accédées et avoir défini un propriétaire des données afin de l'avertir.
- Demander au prestataire de fournir un tableau de bord des résultats des tests si ces tests couvrent de nombreux points d'accès dans le SI.
- Mettre à jour le tableau de bord de sécurité du RSSI.
- Communiquer éventuellement le rapport final au département d'audit interne
- Prévoir une (ou plusieurs) réunion de présentation des résultats par le prestataire : une réunion de synthèse pour la Direction et une réunion plus technique pour le personnel opérationnel.
- Les rapports de pré-validation et final doivent être classifiés "Confidentiel".
- Définir et formaliser au sein du rapport final, la liste des destinataires du rapport.

6 LE ROLE DES ASSURANCES DANS LE CADRE DES TESTS D'INTRUSION

Comme toute intervention externe sur un système d'information, la réalisation des tests d'intrusion peut avoir des conséquences non prévues sur l'intégrité, la disponibilité et même la confidentialité du système et des informations qui y sont gérées.

En principe, on pourrait penser que les incidents pouvant survenir dans ce cadre sont couverts soit par les assurances normales de l'entreprise propriétaire du SI soit par l'assurance « responsabilité civile » du prestataire réalisant les tests (dont il convient de vérifier l'existence et le plafond).

Pourtant, dans de nombreuses situations ce raisonnement peut se révéler inexact.

Ainsi, les assurances couvrent normalement des accidents de nature fortuite or, peut on considérer que sont fortuits des incidents comme :

- indisponibilité du Web suite à une saturation du point d'entrée réseaux conséquent à un bouclage du logiciel de test
- indisponibilité du réseau suite à une « reconfiguration sauvage et involontaire » de certains de ses éléments
- divulgation d'une information confidentielle accédée involontairement par le prestataire dans le cadre des tests

Le fait que tous ces incidents arrivent dans le cadre des actions autorisées et voulues par le propriétaire du SI, peuvent induire la compagnie d'assurance à refuser la couverture du sinistre.

Certes, les assurances (mesures de récupération selon la méthode Mehari™ du Clusif) n'interviennent qu'en dernière instance, après toutes les mesures prises par les exécutants des tests pour prévenir ce type d'incident, en s'interdisant par exemple des actions dangereuses pour le SI. L'existence de ces risques doit toutefois être prise en compte : dès lors que ces incidents peuvent produire des sinistres à fort impact pour l'entreprise, cette dernière doit s'assurer d'une couverture en terme d'assurance.

Si au niveau d'une entreprise, après avoir analysé les mesures de prévention (celles qui préviennent l'incident) et de protection (celles qui l'empêchent de devenir grave) on peut décider de « courir le risque » en considérant suffisante la « responsabilité civile » du prestataire, le cas des hébergements de sites Web est plus complexe.

En effet, les hébergeurs doivent non seulement prendre en compte les dommages pouvant être produits par un incident lors des tests d'intrusion, mais les éventuels dédommagements pouvant être demandés par les clients hébergés, autres que ceux ayant demandé le test.

En particulier, les tests d'intrusion faits vers des machines abritant plus d'un client peuvent conduire l'hébergeur à être dans l'impossibilité d'autoriser ce type de test pour un seul client. Mais, même si le serveur est dédié, des incidents comme ceux décrits ou d'autres similaires, peuvent avoir un impact sur la disponibilité ou l'image de marque d'autres clients, s'ils sont à l'origine, par exemple, d'une indisponibilité d'éléments partagés (routeurs, systèmes de sauvegarde, etc) Il convient donc de prendre en compte l'éventualité des réclamations venant d'autres clients.

En tout état de cause, le test d'intrusion réalisé sur un site hébergé ne peut se faire que dans un cadre « tripartite » avec des autorisations explicites et délimitations des responsabilités prenant en compte la responsabilité civile de chaque acteur face à chaque type d'incident.

7 GLOSSAIRE

Attaque Informatique	Réalisation d'une menace sur un système d'information.
Audit de Sécurité SI	Vérification de la conformité d'un système d'information ou d'une application par rapport à sa Politique de Sécurité et à l'état de l'art.
Audit de vulnérabilité	Vérification des vulnérabilités d'un ou des systèmes par rapport aux vulnérabilités connues (par les Certs et les éditeurs). Cette vérification peut être faite directement sur le système (en « boite blanche ») ou par des automates externes (voir test de vulnérabilité). Les audits internes de vulnérabilité peuvent être automatisés par des systèmes de maîtrise de la vulnérabilité qui installent des agents de contrôle sur les différents systèmes et remontent des « états de vulnérabilité » selon les gravités et priorités établies par le propriétaire du SI. Les éditeurs de ce type de logiciel ont tendance à appeler cette « paramétrisation » une « politique de la sécurité du SI », ce qui est pour le moins abusif et réducteur.
Backdoor	Porte dérobée. Programme introduit dans un système ou une application permettant l'ouverture d'accès privilégiés au système en passant outre les systèmes d'authentification réglementaires. Les pirates utilisent ces "portes par derrière" après s'être introduit sur une machine dans le seul but d'y retourner plus facilement les fois suivantes.
CERT (Central Emergency Response Team)	Structure mutualisée qui reçoit et traite les alertes en matière de sécurité informatique. Le plus important est le Cert central américain (cert.org). En France, existent plusieurs Cert privés ou publics : CertA (Administration), CertIST , Cert Renater, etc.
Cheval de Troie	Programme introduit illicitement dans un système afin de fournir une entrée dans ce système. Nom tiré de la mythologie grecque à l'époque d'Ulysse.
Cible d'évaluation (target of evaluation, TOE)	Système d'information ou produit qui est soumis à une évaluation de la sécurité (ISO15408).
Cible de sécurité (security target)	Spécification de la sécurité qui est exigée d'une cible d'évaluation et qui sert de base pour l'évaluation. La cible de sécurité doit spécifier les fonctions dédiées à la sécurité de la cible d'évaluation, les objectifs de sécurité, les menaces qui pèsent sur ces objectifs ainsi que les mécanismes de sécurité particuliers qui seront employés.
Déni de service (DoS)	Attaque qui, par des voies diverses, vise à empêcher un serveur ou un réseau de serveurs à continuer de rendre son service.
Détection d'intrusion	Mécanisme visant à détecter les tentatives de corruption de la sécurité d'un réseau ou d'un système.
Filtrage des URL	Technique permettant l'accès ou non d'une requête HTTP à un serveur selon les caractéristiques de l'URL demandée et d'une liste des URL autorisées.
Filtrage IP	Technique permettant l'accès ou non d'une trame à un réseau selon les

	valeurs des adresses IP source et destination.
Gravité du risque	« La gravité du risque exprime et la potentialité qu'il a de se réaliser et l'importance de ses conséquences » (Méthode MEHARI™).
IDS (Intrusion Detection System)	Outil ou programme réalisant la détection des intrusions informatiques.
Imputabilité/Traçabilité	Qualité d'un système d'information permettant de retrouver le responsable d'une action sur une information. On retrouve cette qualité aussi sous le nom de « traçabilité des actions » puisqu'elle s'appuie sur des traces informatiques.
Ingénierie Sociale (Social Engineering)	Risque d'intrusion à partir d'un ensemble d'informations obtenues sur la victime potentielle puis à partir d'elle.
Mascarade d'adresse (address spoofing)	Usurpation d'une adresse autorisée dans les accès à un système du réseau de la part d'un dispositif ou d'un utilisateur ne devant pas avoir cette adresse.
Mécanismes de sécurité (security mechanism)	Logique ou algorithme qui implémente par matériel ou logiciel une fonction particulière dédiée ou contribuant à la sécurité.
Menace (threat)	Action ou événement susceptible de porter préjudice à la sécurité.
Mesures dissuasives	« Mesures qui ont pour objet de décourager les agresseurs humains de mettre à exécution une menace potentielle. Pour être efficaces, elles doivent reposer sur une bonne connaissance des techniques et capacités des agresseurs humains redoutés » (Méthode MEHARI™).
Mesures palliatives	« Mesures destinées à minimiser les conséquences, au niveau de l'activité ou de l'entreprise, des détériorations dues à un sinistre » (Méthode MEHARI™).
Mesures préventives	« Mesures dont le rôle de barrière est d'empêcher qu'une menace n'atteigne des ressources du système d'information » (Méthode MEHARI™).
Mesures de protection	« Mesures dont l'objet est de limiter l'ampleur des détériorations éventuelles conséquences de l'exécution d'une menace » (Méthode MEHARI™).
Mesures structurelles	« Mesures dont l'objectif est de minimiser les vulnérabilités du système d'information en agissant sur sa structure même, au niveau de ses composants (matériels, immatériels, humains) comme sur l'organisation et les méthodes qui les régissent. A ces mesures pourront être ajoutées, à titre de complément si ce n'est de validation, des actions de *sensibilisation*, *information* et *formation* » (Méthode MEHARI™).
Mesures de récupération	« Mesures visant à réduire le préjudice subi par transfert des pertes sur des tiers, *assurances* ou par attribution de dommages et intérêts consécutifs à des *actions de justice* » (Méthode MEHARI™).
Potentialité du risque	« La capacité pour un tel événement adverse de se produire se traduit par la notion de potentialité du risque » (Méthode MEHARI™).
Répudiation	Fait pour une personne ou une entité engagée dans une communication de nier avoir participé à tout ou partie des échanges.

Risque	« Le risque exprime le fait qu'une entité, action ou événement, puisse empêcher de maintenir une situation ou d'atteindre un objectif dans les conditions fixées, ou de satisfaire une finalité programmée » (Méthode MEHARI™).
Sinistre Informatique	Conséquence d'une attaque réussie sur un système d'information produisant des pertes importantes (concept large incluant l'accident).
Sniffer	Outil d'écoute et visualisation de la structure des trames Ethernet qui circulent sur un réseau. C'est un programme capable de lire les paquets transitant sur un réseau et permettant de récupérer login et mot de passe. Cet outil, aussi appelé analyseur de réseau, fait également l'objet d'utilisation malveillante par les pirates afin de récupérer toutes les informations confidentielles pouvant circuler en clair sur leur brin Ethernet (exemple: mot de passe POP3).
Test d'intrusion	Batterie de tests, automatisés ou pas, exécutés depuis l'extérieur d'un Système d'Information afin de détecter la présence de failles permettant la pénétration d'un utilisateur ou agent non habilité dans le SI.
Test de vulnérabilité	Batterie de tests, automatisés au pas, exécutés depuis l'extérieur d'un Système d'Information afin de détecter la présence de vulnérabilités dans les composants techniques du SI
Ver	Programme qui peut s'auto-reproduire et se déplacer à travers un réseau en utilisant les mécanismes réseau, ils n'ont pas réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier ...) pour se propager ; un ver est donc un virus réseau.
Virus	Programmes qui se propagent de façon autonome par le biais de fichiers exécutables, de secteurs de démarrage, ou de macro commandes. Un virus est un petit programme, situé dans le corps d'un autre, qui, lorsqu'on l'exécute, se met dans la mémoire et exécute les instructions que son auteur lui a données. La définition d'un virus est: "tout programme d'ordinateur capable d'infecter un autre programme d'ordinateur en le modifiant de façon à ce qu'il puisse à son tour se reproduire".
Vulnérabilité (vulnerability)	Faiblesse de la sécurité d'un système.