Utilisation de produits de simulation d'intrusions

■ Nicole DAUSQUE, dausque@urec.cnrs.fr
CNRS/UREC

Bon nombre des 1 250 unités du CNRS communiquent sur l'Internet pour l'ordinaire : messagerie électronique, recherche documentaire... mais aussi pour échanger, partager des résultats de recherche et cela en toute confiance : considérant l'Internet comme un Intranet. Cette confiance est souvent malheureusement mal fondée, et nombre de problèmes de sécurité dans les systèmes informatiques des unités le prouvent. Il est apparu nécessaire d'une part d'aider les unités à faire le point sur leur niveau de sécurité et à l'améliorer, d'autre part de poursuivre l'effort entrepris en leur offrant la possibilité d'utiliser des logiciels les aidant dans la recherche de failles de sécurité et la simulation d'intrusions. Un aperçu des particularités de certains logiciels utilisables, quelques précisions sur celui retenu et surtout des recommandations d'utilisation de ce type de produit (qui ne fournit rien d'autre, pour les matériels testés, que la liste des vulnérabilités détectées...) font l'objet de cette présentation.

■ Constat

L'internet, support des échanges culturels entre chercheurs du monde entier devient le support des échanges commerciaux internationaux. Or bon nombre des 1 250 unités du CNRS communiquent sur l'Internet pour l'ordinaire : messagerie électronique, recherche documentaire... mais aussi pour échanger, partager des résultats de recherche et cela en toute confiance : considérant l'Internet comme un Intranet. Le chercheur n'utilise plus son cahier d'expériences qu'il gardait précieusement dans un endroit protégé sous clef ; les systèmes d'informations sont les outils de travail, la mémoire de l'ensemble de la communauté recherche. Cette confiance est souvent malheureusement mal fondée, et nombre de problèmes de sécurité dans les systèmes informatiques des unités le prouvent. Les systèmes ne sont pas fiables, et les hackers voire les crackers éprouveront toujours le besoin d'en trouver les failles et de les exploiter. Les outils utilisables pour ce genre de « sport » sont disponibles sur l'Internet…

Il est donc apparu nécessaire d'une part d'aider les unités à faire le point sur leur niveau de sécurité et à l'améliorer, d'autre part de poursuivre l'effort entrepris en leur offrant la possibilité d'utiliser des logiciels les aidant dans la recherche de failles de sécurité et la simulation d'intrusions.

Cependant il n'existe pas de solution technique miracle, applicable partout. Le CNRS avec ses nombreuses unités dispersées sur des sites souvent ouverts, tous interconnectés par RENATER, réseau lui aussi ouvert, est un cas un peu atypique, auquel on ne peut pas appliquer un modèle de protection classique recommandé par les experts du sujet.

Pour le premier objectif fixé, la méthode proposée[1] à plusieurs laboratoires, regroupés par site autour de coordinateurs locaux, leur permettant de faire le point sur leur niveau de sécurité, a été considérée par ceux ci comme une bonne méthode ; elle a été bien perçue des administrateurs de systèmes et réseaux, mais nous estimons qu'elle reste cependant du « domaine artisanal » et il est donc apparu nécessaire, pour compléter le premier travail accompli, de se tourner vers des « produits finis » (ou se disant l'être…) offerts soit dans le domaine des logiciels libres soit dans le domaine commercial.

Un aperçu des particularités de certains logiciels utilisables, quelques précisions sur celui retenu et surtout des recommandations d'utilisation de ce type de produit (qui ne fournit rien d'autre, pour les matériels testés, que la liste des vulnérabilités détectées...) font l'objet de la suite de cet article.

■ Les produits

Avant de se lancer dans l'utilisation d'un produit permettant d'éprouver un système ou un réseau il est nécessaire de pouvoir le classifier c'est-à-dire savoir ce qu'il est sensé faire :

- détection de failles dans les systèmes,
- tests des vulnérabilités à travers le réseau permettant de faire de la simulation d'intrusions,
- écoute des trames sur le réseau permettant de faire de la détection d'intrusion.

Détection de failles dans les systèmes

Les produits offrant ces possibilités, évaluent la sécurité au niveau du système, c'est-à-dire au sens configuration (système proprement dit, utilisateurs, applications). Des logiciels du domaine public correspondant à ce service, comme COPS[2] ("Computer Oracle and Password System") dont la dernière mise à jour date de 1995, sont bien connus mais ne permettent plus de tester les nouvelles vulnérabilités. Parmi les produits commerciaux, celui de chez "Internet Security Systems[3] ", S2[3] ("System Scanner") a été testé en août 1998 par une équipe du LORIA[4] ; les conclusions de ce test ont fait l'objet d'un rapport[5]. Le principal reproche fait à l'époque était que le produit ne s'adaptait pas correctement aux particularités d'implantation du système testé (implantation différente des binaires suivant les types d'unix, par exemple) et donc générait de fausses vulnérabilités. Ce n'était pas pour les administrateurs un outil fiable, il ne leur apportait pas une aide substantielle dans la configuration des systèmes.

Simulation d'intrusions

Pour ce qui est de la recherche de failles à travers le réseau, qui peut être assimilée ne l'oublions pas, à de la simulation d'intrusions, plusieurs produits existent soit dans le monde du logiciel libre, soit chez les commerciaux. SATAN[2] ("Security Analysis Tool for Auditing Networks") dont la dernière mise à jour date de 1995 n'offre donc que la possibilité de tester des failles qui " normalement " ne devraient plus être détectées sur des systèmes actuellement en exploitation. Son successeur SAINT[6] ("Security Administrator's Integrated Network Tool") annoncé en juillet 1998 gratuit au départ, est à présent tombé dans le domaine commercial (c'est le cas de beaucoup d'autres logiciels où des versions commerciales sont développées à partir des logiciels libres… logique inverse des inventions techniques ! mais c'est peut être le prix qu'il faut payer pour obtenir un produit capable de survivre aux évolutions très rapides des technologies de l'information : réseau, équipements, logiciels…). SAINT avait été en partie testé en même temps que les produits de chez ISS[11] c'est certainement un produit qui mériterait que l'on s'y intéresse à nouveau ; il semble évoluer les dernières versions datant d'août 1999 ; cependant comme tout produit scrutant un réseau certaines précautions sont à prendre et les concepteurs font quelques mises en garde[7] dans la façon d'utiliser SAINT (possibilité de sortir de son propre domaine d'adressage). Enfin NESSUS[8] développé par Renaud Deraison est disponible depuis avril 1998. NESSUS[9] est bâti sur un concept client/serveur, le serveur offre la base des signatures d'attaques (environ 120), appelés ici " plugings ", il a en charge les tests de vulnérabilités, le client (Unix ou NT) reçoit la simulation d'intrusion. Actuellement le danger réside dans la possibilité de tester des machines non prévues (si l'option choisie correspond à un réseau ou à un sous réseau) avec des attaques pouvant aller jusqu'au « déni de service ».

Dans le domaine commercial pour un environnement uniquement Solaris le produit BALLISTA[10] offre des fonctionnalités identiques aux produits IS[3] ("Internet Scanner") ; ce dernier a été testé en août 1998 par une équipe du LORIA[4] ; les conclusions de ce test ont fait l'objet d'un rapport[11]. Il en ressort qu'un des principaux avantages du produit réside dans sa base des signatures d'attaques et des remèdes à appliquer remise à jour régulièrement. Les actions correctrices à installer sont globalement bien documentées. Le produit offre plusieurs types de rapport et il est possible de faire des comparaisons entre sessions jouées à intervalle régulier.

Dans un contexte « laboratoires du CNRS » l'utilisation d'un produit de ce type sera accompagnée de recommandations (cf. Méthodologie pour une mise en œuvre). L'intérêt de ces produits peut également résider dans leur utilisation après installation d'un système afin de valider celui ci et les services qu'il offre avant une mise en exploitation.

Détection d'intrusions

Il peut être intéressant de détecter des attaques en direct, en sondant les trames sur le réseau ; cependant il ne faut pas oublier que ceci peut s'apparenter à de l'écoute. De nombreux produits existent mais beaucoup sont encore au stade de prototype, des développements sont encore à faire pour qu'ils jouent pleinement leur rôle de

détecteur d'intrusions[12]. Le produit RS[3] ("Real Secure") a été testé en août 1998 par une équipe du LORIA[4] ; les conclusions de ce test ont fait l'objet d'un rapport[13].

■ Internet Scanner

C'est le produit qui a été choisi dans le cadre « d'une suite aux opérations sécurité dans les laboratoires du CNRS ». Ce produit s'appuie d'une part sur le concept de clefs d'activation construites sur les adresses IP des matériels que l'on veut éprouver, d'autre part sur une base de signatures d'attaques possibles (actuellement 600 sont offertes allant du test de configuration d'un service au « déni de service » en passant par le craquage de mots de passe triviaux). Il est alors possible de construire des scénarii ou sessions, fonction des vulnérabilités que l'on veut tester, d'une politique ou poids du test (degré de profondeur : "heavy scan", "hight scan"…) et des machines cibles que l'on veut éprouver. L'option de test sur clefs d'activation construites sur des adresses spécifiques évite de sortir de son propre domaine d'adressage. Cependant, il est possible, si le produit est mal utilisé, de saturer le réseau ou de faire tomber un serveur. Jusqu'à présent (version antérieure à 6.0) le système de mise à jour obligeait à installer entièrement le produit, sachant que bien souvent cela conduisait à réinstaller le système hôte également ! La nouvelle version, mieux structurée, offre la possibilité de mettre à jour uniquement la base de connaissances. Par contre l'abandon (ou plutôt le non maintien) de la version Unix sur la machine source des attaques est un réel handicap pour des sites purement Unix, s'investir dans un matériel et une connaissance du monde NT n'est pas forcément simple.

Pour la version 6.0 (disponible au 05-10-1999), la configuration minimale suivante est recommandée :

- Modèle : PC 200 MHz Pentium Pro (un Pentium 300 MHz est recommandé).
- Système : Windows NT 4.0 Workstation (avec Service Pack >= 4), système dédié est recommandé. Important : Internet Scanner n'est pas supporté par Windows NT Server.
- Mémoire : 80 MB.
- Espace Disque : 90 MB pour le logiciel, 40 MB pour les rapports et de préférence sur une partition NTFS.
- Privilèges : local ou domaine administrateur.
- Internet Explorer : version 4.0 pack 1.

■ Méthodologie pour une mise en œuvre

Ces recommandations pour l'utilisation de produit de simulation d'intrusions dans les laboratoires du CNRS ont été élaborées à la suite des tests du logiciel IS, effectués dans quatre laboratoires de la région toulousaine incluant la DR locale. La méthodologie est présentée aux administrateurs systèmes et réseaux en suivant une démarche un peu similaire à celle adoptée lors des premières opérations sécurité[1] , c'est-à-dire en s'appuyant sur les coordinateurs locaux et en essayant de regrouper les compétences, de sorte que les administrateurs ne se sentent pas isolés. En une demi-journée une présentation du « pourquoi », « comment », « recommandations » est faite avant de délivrer les clefs d'activation pour les matériels que les laboratoires veulent tester.

Les recommandations conseillées aux administrateurs font l'objet de la suite de ce chapitre.

Remarque préliminaire

L'utilisation de logiciel permettant de mettre en évidence les vulnérabilités des réseaux et des systèmes doit se faire avec une approche synthétique et méthodique. C'est dans ce but que le texte suivant a été écrit.

Décision d'utilisation de ce type de logiciel

L'utilisation d'un logiciel de simulation d'intrusions dans un laboratoire du CNRS doit être faite avec une bonne maîtrise des équipements testés, après avoir pris conscience de l'impact de ces tests (interruption possible de certains services) et de l'importance des informations qui seront obtenues (liste des vulnérabilités pour chaque matériel).

> Il y a donc avant tout nécessité d'adhésion de la direction du laboratoire, de maîtrise de l'opération dans le laboratoire par l'administrateur réseaux et systèmes, et de coordination au niveau régional et national.

Domaine de tests

Il est intéressant de tester les vulnérabilités d'un parc de matériel d'un laboratoire depuis le réseau local du laboratoire mais aussi depuis l'extérieur. Au sein d'une région avec plusieurs laboratoires du CNRS, il est fortement conseillé de regrouper les compétences liées à l'utilisation de ce type d'outil. Il faut envisager, comme dans

le cas des premières opérations sécurité[1], une coordination locale qui assure le dialogue avec les instances nationales (UREC), l'interface avec les administrateurs locaux et l'aide aux laboratoires dépourvus d'administrateur.

Rôle du coordinateur local

Les principales tâches sont :

- Créer une liste de diffusion pour les sites utilisant le logiciel.
- Organiser la formation minimum pour utiliser ce type de logiciel.
- Recenser les moyens techniques utilisables par l'ensemble des laboratoires (matériel pour les tests depuis l'extérieur des laboratoires, par exemple) et définir la procédure d'utilisation de ces moyens.
- Etablir un planning de tests en particulier pour ceux réalisés depuis l'extérieur des sites.
- Dresser, avec les administrateurs de laboratoire, la liste des adresses IP des matériels à explorer.
- Diffuser, en concertation avec l'UREC, le logiciel et les clefs d'activation aux laboratoires.
- Prévenir les services pour qui les tests pourraient apporter des nuisances (exemple : administrateur des routeurs du réseau régional).
- Aider à effectuer les tests, à la demande d'un laboratoire et en liaison avec l'administrateur.
- Effectuer les tests, à la demande du directeur, dans les laboratoires sans administrateur.

> Le coordinateur local ne doit pas s'ingérer dans la politique d'utilisation du logiciel au sein des autres laboratoires, sauf dans le cas des laboratoires sans administrateur où il peut agir avec l'aval du directeur concerné.

Procédure d'utilisation du logiciel

La procédure d'utilisation d'un logiciel de simulation d'intrusions peut s'appuyer sur :

- Choisir et définir la liste des adresses IP à explorer (serveurs, stations personnelles, routeurs, imprimantes…). Le choix de ces équipements peut être fait sur les critères suivants : configuration particulière, machine sensible (contrats, données confidentielles…), machine à spécificité particulière (avec système type « boite noire » ou « brut de fonderie »). Pour les stations personnelles un échantillon représentatif de tous les types est recommandé.

  > La maîtrise de ces équipements est fortement recommandée.

- Avoir à sa disposition une machine dédiée pour installer le logiciel (→ efficacité) et à partir de laquelle les tests seront faits (→ disponibilité), un portable est préférable. Configurer cette machine de manière à la rendre difficilement attaquable (→ confidentialité des résultats).
- Protéger le fichier des clefs d'activation.
- Etudier les possibilités de tests offertes par le logiciel ; le choix de politique par type d'équipements à tester est fortement recommandé.
- Définir le niveau de profondeur des tests qui seront faits (exemple : déni de service), et depuis quels équipements ils seront faits (localement, à travers un routeur propre, à partir de l'extérieur).
- Définir les périodes d'utilisation du logiciel et en avertir les utilisateurs, tout au moins ceux concernés (poste de travail autogéré, poste de travail personnel), des messages pouvant apparaître pendant les tests et les fichiers traces se remplissant plus que d'habitude il y a risque que cela soit vécu comme une intrusion.
- Choisir une période hors charge de travail, hors charge réseau importante (certains tests peuvent perturbés certaines configurations et on peut être amené à réagir très vite…). Les tests ne doivent pas être lancés en automatique, la fin de la procédure doit être attendue afin de consulter tout de suite les résultats, les sauvegarder sur support externe et effacer sur la machine de tests toutes les traces contenant des informations sur les vulnérabilités détectées.
- Prévoir un support fiable pour recevoir les résultats des tests, en aucun cas ils ne doivent rester en ligne, s'assurer de la bonne confidentialité du support choisi.
- Définir, en coordination avec le service informatique (s'il existe) et le directeur de laboratoire, quelle sera la politique adoptée pour la diffusion des résultats :
  - administrateur uniquement,
  - directeur du laboratoire,
  - coordinateur local,
  - utilisateur en étroite relation avec l'équipement exploré,
  - ensemble du laboratoire,
  - autre.

En guise de conclusion

Appliquer les corrections pour les failles mises en évidence par le logiciel et reprendre une nouvelle session de tests en suivant la même procédure…

■ Conclusion

A ce jour (date de la rédaction de cet article) environ 35 administrateurs répartis sur plusieurs sites utilisent le produit IS, avec une mise en œuvre qui suit la méthodologie décrite précédemment. Le bilan de leurs expériences n'est pas encore fait. Il semble cependant que les administrateurs, soit prêts à utiliser ce type de produit, mais qu'il est impératif de leur offrir une présentation et une démonstration de celui-ci. Ils sont parfois un peu frileux pour faire les premiers tests, déplorant que de toute façon même en ayant connaissance de toutes les vulnérabilités de leurs systèmes et les correctifs à appliquer, il ne leur sera pas possible, faute de temps, de remédier à tous les problèmes. Bien sur le peu qui sera fait sera de toute façon utile.

Actuellement le plus gros reproche fait est l'obligation d'avoir une machine sous NT pour utiliser le produit IS ; ceci est tout à fait juste car il est difficile d'obliger des administrateurs déjà très sollicités, à s'investir dans un nouveau système, bien que défini comme étant de type « cliquodrome » mais dont la logique n'a rien à voir avec celle du système Unix. Il leur est également légitime de dire : « comment faire confiance à un logiciel qui détecte les vulnérabilités des systèmes que l'on est sensé maîtriser à partir d'un autre système que l'on ne maîtrise pas ou peu ». Si cette contrainte avait existé au moment du choix du logiciel, notre choix aurait été différent. Et puis est-ce bien raisonnable de faire confiance à un fournisseur qui d'un coté averti des dernières vulnérabilités et de l'autre possède toutes les clefs d'activation permettant de les tester…

Mais ne soyons pas complètement pessimistes, l'auto-formation offerte grâce à la documentation en ligne très complète associée aux vulnérabilités testées et aux correctifs à appliquer est un des points particulièrement intéressants du produit.

Plus d'informations

[1] http://www.urec.cnrs.fr/securite/articles/ope.secu.html
[2] http://www.urec.cnrs.fr/securite/outils/index.html
[3] http://www.iss.net/
[4] http://www.loria.fr/
[5] http://www.loria.fr/services/moyens-info/securite/S3.html
[6] http://www.wwdsi.com/saint/
[7] http://www.wwdsi.com/saint/docs/dangers.html#leashing-saint
[8] http://www.nessus.org/
[9] http://www.ossir.org/ftp/supports/98/nessus/pres/
[10] http://www.idg.net/crd_ballista_15926.html
[11] http://www.loria.fr/services/moyens-info/securite/ISS.html
[12] http://www.urec.cnrs.fr/securite/articles/confRaid98.html
[13] http://www.Loria.fr/services/moyens-info/securite/RealSecure.html