SÉCURITÉ INFORMATIQUE

numéro 30 juin 2000

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Il n'est si bonne compagnie qui ne se sépare…

éditorial

Lorsque je suis entré au CNRS, il y a huit ans, je ne connaissais de l'informatique qu'un banal produit de traitement de texte à usage domestique. Or, dans l'héritage de mon prédécesseur se trouvait l'amorce d'une étude sur la sécurité des systèmes d'information des laboratoires dont le besoin s'était fait sentir avec la montée en puissance de RENATER.

Il me fallait donc partir à la découverte des autoroutes de l'information et des subtiles règles non écrites qui tentaient déjà d'y policer la circulation. Sans la bienveillante patience de Jean-Luc Archimbaud, de Michel Dreyfus et de Robert Longeon pour m'initier aux arcanes de l'Internet, je m'y serais sans doute perdu. L'étude eut lieu, elle intéressa les autorités du CNRS, et parmi ses retombées se situa la naissance de *Sécurité informatique* en 1994. Je pris l'habitude de venir y commenter deux ou trois fois par an les heurs et les malheurs des réseaux de la communication électronique.

Mon but n'était pas de donner des leçons aux informaticiens de la recherche qui ont amplement prouvé leur compétence et leur efficacité en développant et en mettant à la disposition des chercheurs cet incomparable outil d'échanges scientifiques. Avec mes connaissances toutes fraîches et ma vieille expérience des questions de sécurité, je voulais surtout m'adresser aux dizaines de milliers de simples utilisateurs qui, dans nos laboratoires, se connectent quotidiennement à l'Inter ou à l'Intranet. Chacun d'eux, à son niveau et avec ses moyens, a un rôle essentiel à jouer dans le maintien de la disponibilité, de l'intégrité et de la confidentialité de la somme des savoirs que nous confions aux machines et aux réseaux. Même s'il n'a pas fait de grands dégâts chez nous, ILOVEYOU vient de nous rappeler opportunément que, dans la lutte contre la malveillance informatique, il faut toujours rester vigilant.

Dans quelques semaines, je quitterai le CNRS et la vie dite « active » pour aller, sur un bout de lande bretonne, planter d'autres fleurs que celles de la rhétorique et cultiver l'art d'être grand-père. Gageons qu'il m'arrivera tout de même, par les longues soirées d'hiver, de pianoter machinalement sur un clavier pour voir apparaître la séquence http://www.cnrs.fr/Infosecu…

Philippe Schreiber
Fonctionnaire de défense du CNRS

Une page se tourne…

Qui parlait en 1992 de la sécurité des systèmes d'information ? On fêtait tout à la fois le cinquième centenaire de la découverte de l'Amérique et l'arrivée sur le marché des SUN 4 munis du fameux OS 4.1.3 qui fit le succès – et les délices – de tant de pirates en herbe. C'était les débuts de NFS et des montages de disques « pour le monde entier », l'époque où le fichier /etc/passwd était en lecture pour tous, les bandes de sauvegarde en accès libre et le mot de passe « administrateur » généreusement distribué. Certes aux États-Unis, après la panique de l'année 1988 provoquée par le « ver » de Robert Morris Junior – dont le père était responsable de la sécurité des systèmes d'information à la NSA –, la mobilisation des moyens et des esprits était déjà bien avancée. Mais en France, on en était bien loin : insouciance et bonne humeur étaient de rigueur.

Philippe Schreiber, fonctionnaire de défense tout nouvellement nommé, constata que la « protection du patrimoine scientifique » ne pouvait plus ignorer la sécurité des systèmes et des réseaux. Il fit partager sa conviction à l'ensemble de la Direction du CNRS qui accepta d'y consacrer de nouveaux moyens. Ce soutien se révéla précieux et constant depuis lors. Il organisa dès le début, avec son premier chargé de mission, Jean-Luc Archimbaud, les opérations de sensibilisation à la sécurité qui connurent très vite un grand succès. La suite est connue : Michel Dreyfus le rejoint à son tour, Jean-Luc Archimbaud crée au sein de l'UREC le groupe de sécurité, des correspondants sécurité s'organisent, tant dans les délégations régionales que dans les laboratoires…

Il reste encore beaucoup à faire. Mais quand on regarde le chemin parcouru depuis « l'époque de la joyeuse insouciance », on peut être fier du travail qui a été accompli. Cela a été réalisé grâce à tous, chacun à son poste, mais Philippe Schreiber en a été à la fois l'initiateur, l'âme et le principe organisateur. Il a fait ce travail avec cette énergie, cette foi, cette gentillesse, cette chaleur humaine que tout le monde lui reconnaît et qui lui permettait d'obtenir de chacun d'entre nous le meilleur de lui-même.

Monsieur, vous nous quittez cet été… pour de nouvelles aventures ? Être grand-père n'est pas un art si aisé… Suivant la phraséologie des temps de guerre, « vous allez procéder à une retraite stratégique conformément à un plan préparé à l'avance ». Retraite avec les honneurs ! Une page va donc être tournée. D'autres continueront le travail que vous aviez amorcé il y a plus de huit ans et que vous avez si bien conduit au succès. Mais n'oubliez pas, dans votre nouvelle vie active, que vous avez laissé ici des amis.

Robert Longeon
Chargé de mission SSI

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

De l'utilité des logiciels de simulation d'intrusions

Cet article expose les raisons qui ont conduit à l'utilisation de logiciels de simulation d'intrusions dans les laboratoires du CNRS et quelques conclusions que l'on est susceptible d'en tirer.

Le constat

L'Internet, victime de sa popularité, rend de plus en plus vulnérables aux intrusions les laboratoires CNRS, pour qui il correspond à leur Intranet. Les panoplies du « parfait petit hacker » sont disponibles, pour tous, sur de multiples sites dont les noms sont diffusés sur des listes de messagerie. Une des techniques très utilisées actuellement consiste à scruter les réseaux. Les adresses des machines reconnues comme vulnérables sur ces réseaux scrutés, parce qu'offrant des services réseaux facilement attaquables, sont ensuite diffusées sur des sites Internet. Un bon mot clef en entrée d'un moteur de recherche vous aiguillera vers ces sites.

Pour remédier à ce problème, 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. Il est donc nécessaire pour un laboratoire du CNRS de faire, lui-même, le point sur son niveau de sécurité, et de chercher à l'améliorer.

Suite aux succès rencontrés par les opérations sécurité réalisées à ce jour sur plus de 110 laboratoires du CNRS répartis sur toute la France (*cf. Sécurité informatique* n° 21 et l'article « Opérations sécurité sur les sites » disponible à l'adresse http://www.urec.cnrs.fr/securite/articles/ope.secu.html), il a été décidé de poursuivre l'effort entrepris en offrant aux laboratoires la possibilité d'utiliser des logiciels les aidant dans la recherche de failles de sécurité en faisant de la simulation d'intrusions. Pour les opérations sécurité, la méthode était basée sur l'utilisation de listes de contrôles ; il est apparu nécessaire, pour compléter les recommandations en matière de sécurité qui y sont offertes, de se tourner vers des « produits finis » (ou se disant l'être...).

La démarche adoptée

Après une étude des fonctionnalités des logiciels permettant d'analyser les vulnérabilités des systèmes à travers le réseau (*cf.* l'article « Logiciel de simulation d'intrusions : quelques principes et généralités » dans ce numéro), et suite aux tests faits au Loria (résultats disponibles à l'adresse http://www.loria.fr/services/moyens-info/securite/), il a été décidé en mai 1999 l'achat de 2 000 licences du logiciel Internet Scanner de chez Internet Security Systems.

Cependant, pour le contexte « laboratoires du CNRS », quelle que soit l'origine des produits utilisés – monde du logiciel libre ou monde du logiciel commercial –, il est apparu important d'accompagner la mise en œuvre de ceux-ci de recommandations (*cf.* «Recommandations pour l'utilisation de produits de simulation d'intrusions dans un laboratoire CNRS » dans ce numéro). Ces recommandations font l'objet d'une présentation lors de la distribution des licences.

Bilan d'utilisation

À la date de parution de cet article, plus de 100 administrateurs systèmes et réseaux utilisent le logiciel IS, ce qui correspond à peu près à 1 500 licences distribuées, donc autant de machines explorées. La répartition d'utilisation est d'environ 80 % de simulation d'intrusions sur des systèmes UNIX et 20 % sur des systèmes NT. L'utilisation de ces produits est jugée intéressante par les administrateurs, qui les considèrent comme apportant une aide dans la maintenance des systèmes. L'intérêt réside également dans leur emploi après installation d'un système afin de valider celui-ci et les services qu'il offre avant une mise en exploitation. 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.

Devant l'évolution constante de ce type de produit, il est apparu nécessaire de procéder à de nouvelles études comparatives dont l'essentiel des résultats vous est donné plus loin dans l'article «Comparatif des produits de simulation d'intrusions ».

Conclusion

Une utilisation récursive de ces produits est nécessaire. L'aide qu'ils apportent permet de faire un suivi de l'évolution « sécurité » des machines et du réseau du laboratoire dans la recherche de failles et dans les recommandations sur les actions à entreprendre pour les corriger. Ces produits aident à la montée graduelle du niveau de sécurité du laboratoire ; c'est pourquoi leur utilisation doit être inscrite dans la définition de la politique de sécurité du laboratoire. Il faut encourager les administrateurs à utiliser ce type de produit, ils doivent l'inclure dans les outils du quotidien au même titre que ceux liés à la maintenance du parc informatique, car ils y concourent. Il faut que ce travail soit reconnu comme une priorité dans les tâches des administrateurs systèmes et réseaux.

Nicole Dausque
nicole.dausque@urec.cnrs.fr

Comparatif des produits de simulation d'intrusions

Une première étude avait été faite en août 1998 par le LORIA portant sur les logiciels « Internet Scanner » et « Saint » (http://www.loria.fr/services/moyens-info/securite/ISS.html - ISS vs SAINT). Suite à cette étude, nous avons retenu le produit commercial « Internet Scanner » de la société « Internet Security Systems » comme outil de simulation d'intrusions à conseiller aux administrateurs systèmes et réseaux du CNRS, et nous avons acheté un certain nombre de licences que nous avons distribuées.

Actuellement, de nombreux développements sont en cours sur les produits de simulation d'intrusions, surtout dans le monde du logiciel libre. C'est pour cette raison que nous avons souhaité réactualiser notre étude, afin d'évaluer les évolutions en la matière.

Les produits étudiés

Nous avons retenu trois logiciels gratuits : Nessus, Sara (Security Auditor's Research Assistant) et Saint (Security Administrator's Integrated Network Tool). Satan (Security Administrator Tool for Analyzing Networks), précurseur dans ce domaine, n'a pas été pris en compte dans ce comparatif, car la dernière version date de 1995. Les comparaisons ont été faites avec le produit « Internet Scanner ». À noter qu'il existe des versions commerciales des logiciels Sara et Saint, il s'agit de SaraPro et WebSaint.

Les tests ont été faits avec les versions suivantes des logiciels : IS 6.0.1, Saint 2.0.1, Sara 2.1.13, et Nessus 0.99.10, à partir de deux plates-formes d'attaque : NT 4.0 Workstation et Red Hat Linux 6.1.

Les critères pour un choix

Nous avons établi une liste de critères pour étudier les produits. Ces critères sont les suivants : le type de plate-forme d'attaque (Unix, NT) ; les domaines « attaqués » (Unix, NT) ; la portée des attaques au sens adressage ; la facilité d'installation et d'utilisation du produit ; le nombre de vulnérabilités testées ; la fréquence, la régularité, la pertinence et la facilité des mises à jour des bases de connaissances ; les informations sur les attaques effectuées ; les propositions de corrections faites pour pallier les failles détectées. Nous avons aussi pris en compte le fait que le produit soit d'une exploitation aisée, sans piège, contrôlable et adaptable au site et à la politique de sécurité définie.

Quelques éléments de réponse

Dans le cadre de cet article, nous allons présenter uniquement les points les plus significatifs.

Une première constatation est que ces produits ne visent pas tout à fait le même objectif. Sara et Saint, les « descendants » de Satan, sont surtout orientés vers l'étude du réseau informatique de façon globale (étude des relations de confiance entre machines), bien qu'ils permettent aussi de tester les vulnérabilités au niveau de chaque machine. IS et Nessus sont plus orientés sur l'étude des machines prises de manière individuelle dans un contexte réseau, avec une particularité supplémentaire pour Nessus, qui ne teste que les services réseaux présents sur les machines et les découvrent même s'ils n'utilisent pas les numéros de ports standards.

De façon générale, nous notons que les développements se font dans la même direction : possibilité de tester des machines Unix et NT, intégration de plus en plus rapide de tests sur les nouvelles vulnérabilités découvertes, amélioration de la documentation sur les vulnérabilités et sur les actions à entreprendre pour pallier les failles détectées (plus particulièrement pour IS, Sara et Saint), indication des tests dangereux (par exemple, « déni de service ») à manier avec prudence.

De nombreuses différences dans les fonctionnalités sont à noter. Les plus importantes sont :
- les plates-formes d'attaque : Unix pour Nessus, Saint, Sara ; NT pour IS ;
- le nombre de vulnérabilités testées : 700 pour IS, 350 pour Nessus, 150 pour Saint et Sara. À noter qu'IS (avec 50 % des vulnérabilités testées) est beaucoup plus orienté NT que les autres produits ;
- la portée des attaques au sens adressage : libre avec Nessus, Saint, Sara ; verrouillée avec licence d'utilisation pour IS ;
- la mise à jour des vulnérabilités : simple ajout de module pour Nessus et IS ; changement de version pour Sara et Saint ;
- la sélection des vulnérabilités à tester : simple clic pour Nessus et IS ; difficilement exploitable pour Saint et Sara.

Il existe aussi une différence importante au niveau de la méthode de développement des produits ; l'accès au code source étant possible pour Saint, Sara et Nessus, le développement est en collectif.

Logiciel de simulation d'intrusions : quelques principes et généralités

MALGRÉ LES NOMBREUSES VÉRIFICATIONS, les logiciels (systèmes d'exploitation et applicatifs) sont presque tous livrés avec des erreurs. Ces erreurs sont souvent bénignes, mais parfois elles peuvent créer des trous de sécurité dans votre système, trous que des personnes mal intentionnées peuvent utiliser pour l'attaquer. De plus, certains logiciels installés dans des contextes différents ne sont pas forcément mis en place avec vigilance par rapport aux problèmes de sécurité. La surveillance manuelle des machines devient une tâche qui demande de plus en plus de temps et de compétence. C'est la raison pour laquelle des logiciels de simulation d'intrusions ont vu le jour, afin d'assister le responsable sécurité dans son travail quotidien.

LE BUT DE CES LOGICIELS est d'éprouver votre système pour identifier les vulnérabilités avant que des indélicats ne le fassent et n'en abusent. Pour cela, ils réalisent une gamme d'attaques au travers du réseau afin de détecter les points faibles de vos systèmes. Leur principe de construction repose sur une base de connaissances recensant les failles connues ; mais ces produits sont souvent sans intelligence. C'est à l'utilisateur de déterminer les machines à éprouver en fonction de leur contenu et de leur ouverture sur le réseau ; certains logiciels nécessitent des clefs d'activation afin de limiter la portée des tests.

LA QUALITÉ DE CES PRODUITS dépend de leur base de connaissances et de la fréquence des mises à jour, mais aussi de leur capacité à assister le responsable sécurité dans le choix des politiques de sécurité à tester et des remèdes à appliquer.

En conclusion

Les versions des produits testées évoluent beaucoup actuellement (environ une à trois versions par logiciel sur la période de test). Cette forte activité est sans aucun doute à corréler avec l'augmentation importante des attaques en provenance de l'extérieur, aux nombres de vulnérabilités découvertes (60 avis diffusés par le CERT RENATER depuis janvier 2000) et à l'augmentation et à la diversification des parcs informatiques.

Les outils présentés dans ce document ne sont pas tous équivalents ; ils sont plutôt complémentaires. La bonne démarche pourrait être de commencer la prise en main des problèmes de sécurité réseau avec des outils « simples », style Sara et Saint ; ensuite d'affiner et de poursuivre l'effort entrepris avec des outils plus complets, style Nessus et IS.

Suite à cette étude, le choix d'IS est toujours pertinent, malgré les efforts faits par Nessus pour développer son produit. La qualité de la documentation et la présence de politiques de sécurité prédéfinies sont des atouts importants pour l'intégration de ce type de produit dans la politique de sécurité d'un laboratoire. Le verrouillage avec licence d'utilisation des adresses IP à tester permettant de limiter d'emblée la portée des tests est aussi un atout pour le déploiement d'IS dans les laboratoires. Et en dernier lieu, le fait que ce produit soit développé par une société commerciale nous fait espérer une meilleure garantie quant à la pérennité du produit.

Dans le contexte laboratoire CNRS, IS possède donc de nombreux avantages, ce qui nous fait regretter encore plus amèrement l'abandon de la version Unix du produit, version qui existait lors des tests faits en 1998.

Marie-Claude Quidoz
Marie-Claude.Quidoz@urec.cnrs.fr

IS : http://www.iss.net/
Nessus : http://www.nessus.org/
Sara : http://www-arc.com/sara/
Satan : http://www.porcupine.org/satan/
Saint : http://www.wwdsi.com/saint/

Recommandations pour l'utilisation de produits de simulation d'intrusions dans un laboratoire CNRS

L'utilisation de logiciels permettant de mettre en évidence les vulnérabilités des réseaux et des systèmes doit être menée avec une approche réfléchie et méthodique.

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 et de maîtrise de l'opération dans le laboratoire par l'administrateur réseaux et systèmes. Ces tests pourront être lancés à distance, il peut y avoir besoin de coordination avec les administrateurs des réseaux traversés (de campus, régionaux...).

Organisation

Au sein d'une région comptant 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, une coordination régionale qui assure le dialogue avec les instances nationales (UREC), l'interface avec les administrateurs régionaux, l'aide aux laboratoires dépourvus d'administrateur. Cette coordination facilitera la mise en œuvre de tests depuis l'extérieur. 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.

Rôle de la coordination régionale (deux personnes)

Les principales tâches sont de :
- créer une liste de diffusion pour les sites utilisant le logiciel ;
- organiser la formation minimum sur le produit ;
- recenser les moyens techniques (ordinateur portable) 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 ;
- 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 clés d'activation aux laboratoires ;
- établir un planning de tests, en particulier pour ceux depuis l'extérieur des sites ;
- prévenir les services pour qui les tests pourraient ne pas être transparents (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.

La coordination régionale doit veiller à ne pas s'ingérer dans la politique d'utilisation du logiciel au sein des autres laboratoires, sauf dans le cas des laboratoires sans administrateur où elle peut agir avec l'aval du directeur concerné.

Recommandations d'utilisation du logiciel

• Choisir comme matériels à tester : serveurs, machines sensibles (contrats et/ou données confidentielles), machines spécifiques (incluses dans des contrats, installées avec système type « boite noire » ou « brut de fonderie »...), échantillon de stations personnelles (chacune représentative d'une configuration), routeurs. *La maîtrise de ces équipements est fortement recommandée.*

• Avoir à sa disposition une machine dédiée pour installer le logiciel et à partir de laquelle les tests seront faits (un portable est préférable). Configurer cette machine de manière à la rendre difficilement attaquable (besoin de confidentialité des résultats).

• Protéger le fichier des clefs d'activation.

• Étudier les possibilités de tests offertes par le logiciel ; le choix de politique par type d'équipements à tester est fortement recommandé.

• 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. Bien choisir ces périodes, hors charge de travail, hors charge réseau importante (certains tests peuvent perturber 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 test toutes les traces contenant des informations sur les vulnérabilités détectées.*

• Définir le niveau de profondeur des tests qui seront effectués (exemple : si déni de service envisagé, bien programmer ce test à l'avance) et depuis quels équipements ils seront faits (localement, à travers un routeur propre, à partir de l'extérieur).

• Prévoir un support fiable pour recevoir les résultats des tests (en aucun cas ils ne doivent rester en ligne) et s'assurer de la bonne confidentialité du support choisi.

• Définir la politique adoptée pour la diffusion des résultats :
- administrateur uniquement,
- directeur du laboratoire,
- coordinateurs locaux,
- utilisateur en étroite relation avec l'équipement exploré,
- ensemble du laboratoire,
- autre.

Corrections et nouveaux tests

Après le premier banc de tests, il sera nécessaire de faire les corrections des trous de sécurité découverts par le logiciel. Ensuite une nouvelle session de tests sera à effectuer en suivant la même procédure que celle utilisée précédemment.

Jean-Luc Archimbaud – Nicole Dausque
CNRS/UREC

SÉCURITÉ INFORMATIQUE
numéro 30 juin 2000
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 5 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
ROBERT LONGEON
Centre national de la recherche scientifique
Service du Fonctionnaire de Défense
c/o IDRIS - BP 167. 91403 Orsay Cedex
Tél. 01 69 35 84 87
Courriel : robert.longeon@cnrs-dir.fr
http://www.cnrs.fr/Infosecu

ISSN 1257-8819
Commission paritaire n° 3105 ADEP

Conseil et coordination : CNRS - DIST - Jacqueline Leclère • Conception et réalisation : La Souris 01 45 21 09 61