Superviseur de sécurité pour site Internet

Sylvain Gombault, Stéphane Ruaud

SUPERVISEUR DE SÉCURITÉ POUR SITE INTERNET

Sylvain GOMBAULT
ENST de Bretagne
Département Réseaux et Services Multimedia
BP 78, 35512 Cesson-Sévigné - France
Tél.: 99 12 70 37 - Fax: 99 12 70 30
Sylvain.Gombault@rennes.enst-bretagne.fr

Stéphane RUAUD
ENST de Bretagne
Département Réseaux et Services Multimedia
BP 78, 35512 Cesson-Sévigné - France
ruaud@supaero.fr

Résumé:

Toute politique de sécurité doit prévoir les moyens de contrôler sa mise en oeuvre. Cette surveillance est d'autant plus efficace qu'elle est réalisée par des outils indépendants. L'Analyseur de Sécurité, un outil de sécurité réseau pour site Internet, remplit ce rôle de superviseur de sécurité autonome. Après la description de ses fonctionalités, ce document présente l'étude de l'interface de surveillance développée à l'usage de l'administrateur sécurité.

SUPERVISEUR DE SÉCURITÉ POUR SITE INTERNET

Sylvain GOMBAULT
ENST de Bretagne
Département Réseaux et Services Multimedia
BP 78, 35512 Cesson-Sévigné - France
Tél.: 99 12 70 37 - Fax: 99 12 70 30
Sylvain.Gombault@rennes.enst-bretagne.fr

Stéphane RUAUD
ENST de Bretagne
Département Réseaux et Services Multimedia
BP 78, 35512 Cesson-Sévigné - France
ruaud@supaero.fr

Abstract:

Any good security policy includes procedures to verify its results. This monitoring needs to be performed by stand-alone tools. The Network Security Probe (l'Analyseur de Sécurité) designed for Internet site security, is an independant security monitor. This paper presents its functionalities and describes the monitoring interface provided to security administrators.

1 INTRODUCTION

Le raccordement mondial des sites informatiques autour d'Internet pose des problèmes en matière de sécurité. Le risque majeur vient de la standardisation des matériels et des logiciels : du fait de leur complexité les logiciels peuvent comporter des trous de sécurité , une faille trouvée sur un équipement est reproductible sur d'autres sites équipés de produits identiques. Sans verser dans le catastrophisme, cela oblige chaque entreprise à se protéger.

Chaque organisme gère de manière différente les informations qu'il considère sensibles. La politique de sécurité d'un organisme est l'ensemble des règles et pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées au sein de cet organisme [1] [2]. Vérifier que la politique de sécurité est bien appliquée fait partie intégrante de sa mise en oeuvre.

Un certain nombre d'outils d'origine commerciale ou distribués gratuitement sur Internet [3] permettent de mettre en oeuvre la politique de sécurité d'un site. Il est recommandé [2] d'en contrôler le résultat avec un outil indépendant.

L'Analyseur de Sécurité est développé à l'ENST de Bretagne, au sein du département RSM (Réseaux et Services Multimedia) de Rennes. Utilisé seul, il propose une solution pour mettre en place et contrôler la politique de sécurité au sein d'un site TCP/IP, qu'il soit raccordé ou non à Internet ; installé en complément d'autres outils, il contrôle qu'une politique de sécurité est bien appliquée grâce à des fonctions de supervision. Il intègre des innovations ayant fait l'objet de deux dépôts de brevet [4] [5].

2 L'ANALYSEUR DE SÉCURITÉ

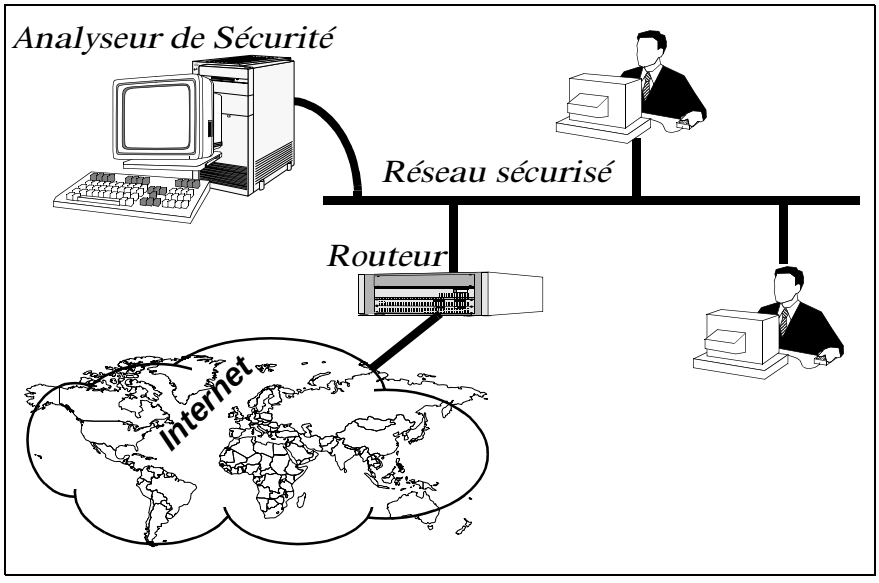

Figure 1 : *Place de l'Analyseur de Sécurité dans un réseau Ethernet*

L'Analyseur de Sécurité est un logiciel qui s'exécute sur toute station de travail munie d'une interface réseau avec laquelle il écoute le trafic. Il s'appelle alors NSP, l'acronyme de son nom anglais: Network Security Probe (cf par. 2.6). Comme tout analyseur de protocole, il est basé sur l'écoute passive et l'analyse du trafic. A partir de ces données et par rapport à une politique de sécurité prédéfinie, il y ajoute la détection des intrusions qu'il combat en alertant l'administrateur sécurité et en interrompant les communications.

2.1 Originalités et caractéristiques

L'architecture de l'Analyseur de Sécurité en fait un outil *indépendant* dont l'installation ne demande *aucune modification* des équipements de réseau ou de sécurité existants. Son fonctionnement est *transparent aux applications* et ne leur impose aucune contrainte, il ne modifie en rien leurs *performances* : il n'introduit aucune charge supplémentaire sur le réseau ni délai dans les échanges car il travaille en total parallélisme.

Il est *dédié* uniquement à des fonctions de sécurité, ce qui permet, d'un point de vue organisationnel, de *dissocier* l'administration de la sécurité de la gestion du réseau, suivant en cela le fait qu'il est recommandé de séparer les fonctions de responsable sécurité des fonctions d'administrateur réseau [2]. L'autre avantage est que cela n'impose aucun choix en ce qui concerne les équipements (routeurs, hubs).

Il est *indétectable* du point de vue du réseau, y compris lorsqu'il génère du trafic (cf par. 2.4), même par un analyseur : cette propriété est importante pour sa sécurité mais également pour celle du site car elle n'incite pas un intrus à prendre des voies détournées ou à masquer outre-mesure son attaque.

Le trafic capturé est traité de manière *optimiste*: la majorité des communications étant légitimes, elles ne doivent pas être pénalisées par la présence d'un équipement de sécurité. L'Analyseur de sécurité laisse donc une communication s'établir normalement (a priori optimiste) pendant qu'il la compare à la politique de sécurité, il la coupe éventuellement ensuite.

Il analyse tout le trafic passant sur le réseau local et peut donc appliquer une politique de sécurité de contrôle d'accès sur des communications *locales*.

La simplification de sa configuration a fait l'objet d'une étude particulière : il se configure rapidement grâce à un outil graphique convivial qui repose sur l'utilisation de fichiers en mode texte et qui sait aller *interroger les bases* NIS ou DNS pour en extraire les listes de machines, de réseaux, d'utilisateurs ou de services.

2.2 Services de sécurité

L'ISO 7498-2 [8] définit un ensemble de services et de mécanismes de sécurité. L'Analyseur de Sécurité ne respecte pas l'architecture de sécurité OSI qui place les éléments de sécurité dans les entités d'extrémité mais les services qu'il propose peuvent être décrits avec les définitions de cette norme:

- contrôle d'accès (cf par. 2.3),
- authentification de l'entité émettrice et/ou réceptrice par délégation (cf par. 2.5),
- intégrité des données (cf par. 2.5),
- non répudiation: de par sa position, il peut certifier avoir vu ou non passer certaines informations,
- audit des communications (cf par. 3.1)

Les services que son architecture ne lui permet pas de fournir:

- confidentialité : n'étant pas sur le chemin des données, il n'a aucun moyen de les chiffrer ou de les masquer,
- disponibilité : il ne peut garantir la disponibilité du réseau,
- secret du flux : il ne peut masquer le fait qu'une communication a lieu.

2.3 Politique de sécurité et contrôle d'accès

La politique de sécurité définit les droits d'accès aux ressources. L'Analyseur de Sécurité permet uniquement de réaliser un contrôle d'accès sur les communications TCP (elles sont en mode connecté et il sait les interrompre).

Il possède sa propre description des droits d'accès voulus par la politique de sécurité : c'est un ensemble de règles décrivant le service *contrôle d'accès* qu'il fournit et qui sont élaborées à partir des critères suivants:

- adresse IP source et destination,
- service (lié au numéro de port),
- utilisateur lorsque cela a un sens (telnet, ftp, rlogin),
- heure,
- type d'audit : synthétique ou détaillé,
- action: autoriser, authentifier ou couper la communication.

Par défaut, toute communication non explicitement autorisée est coupée.

Ces critères sont plus riches que les fonctions de filtrage proposées par les routeurs. Ils permettent d'affiner le filtrage des services TCP autorisés au travers du routeur en jouant sur l'heure ou l'utilisateur.

2.4 Coupure des communications

L'Analyseur de Sécurité interrompt une communication TCP en émettant deux TCP Reset à destination des deux interlocuteurs, en se faisant passer à chaque fois pour l'autre extrémité. Sa présence n'est pas trahie par ces émissions.

2.5 Services intersites

En dialoguant avec un homologue, l'Analyseur de Sécurité peut authentifier dynamiquement par délégation l'émetteur et/ou le récepteur d'une communication, confirmer l'intégrité des documents reçus ou émis.

Ces fonctions ont fait l'objet d'une publication et sont décrites de manière plus approfondie dans [6].

2.6 Le logiciel NSP (Network Security Probe)

NSP est le nom du logiciel Analyseur de Sécurité. Il fonctionne en environnement Unix (HP-UX v10 et Solaris 2.5) et est disponible gratuitement sur le site:

- `http://www.rennes.enst-bretagne.fr`

3 SUPERVISION DE LA SÉCURITÉ

L'Analyseur de Sécurité possède une interface de supervision destinée à l'administrateur sécurité qui donne une vue complète et synthétique des événement liés à la sécurité d'un site.

Cette supervision est alimentée par les événements générés par son propre audit. Ils peuvent être enregistrés classiquement sur support magnétique: cette manière de trai-

ter l'audit est utile car elle permet des recherches à posteriori d'événements précis mais ne répond pas à toutes les attentes de l'administrateur sécurité qui souhaite également une analyse temps réel des événements.

Deux choses l'intéressent en particulier: être prévenu en immédiatement des tentatives d'intrusion mais aussi connaître à tout instant les communications autorisées établies. Pour en donner une vision synthétique, l'Analyseur de Sécurité utilise une visualisation graphique qui est décrite après la présentation de ses fonctions d'audit.

3.1 Audit

L'audit de l'Analyseur de Sécurité concerne le trafic observé, la politique de sécurité et la vie des processus.

L'audit sur le trafic a été conçu de manière à signaler tout événement réseau intéressant la sécurité, à savoir:

- le début et la fin des communications TCP: adresses IP, noms DNS, numéros de port, et heure;
- les utilisateurs des services telnet, rlogin et ftp;
- lorsque le mode détaillé est sélectionné, l'ensemble des commandes pour les seuls services ftp, smtp et http;
- le trafic ICMP autres que les messages echo et echo/reply de 64 octets ou moins [7].

L'audit sur la politique de sécurité trace les événement liés aux décisions prises par l'Analyseur de Sécurité:

- quelle règle de la politique de sécurité a provoqué l'autorisation, l'interruption ou une demande d'authentification pour une communication;
- la raison de la coupure: absence de règle, mauvais utilisateur, mauvaise heure...
- les demandes d'authentification et leur résultat.

Cet audit serait incomplet sans une surveillance de la vie des processus sur lesquels repose la sécurité du site, il indique donc:

- les heures de lancement et d'arrêt des processus de l'Analyseur de Sécurité.

Les messages générés par l'Analyseur de Sécurité sont répartis selon quatre niveaux de sévérité et adaptés à des outils d'audit capables d'effectuer une sélection en fonction de ce critère:

- les messages de premier niveau sont tous ceux dont la connaissance immédiate n'est pas indispensable à la sécurité, mais dont il est indispensable de conserver une trace comme par exemple les débuts et fin de communication,
- ceux de deuxième niveau permettent de suivre l'exécution des mécanismes de sécurité: vérification d'utilisateur, authentification et dont l'échec ne met pas en cause la sécurité du site mais provoque la coupure de la communication,
- les alertes au niveau sécurité sont de troisième niveau, il s'agit des messages indiquant les communications coupées,
- le changement de comportement de l'Analyseur de Sécurité est indiqué les messages de quatrième niveau signalent la mort ou le redémarrage d'un processus, passage du mode simulé au mode coupure des communications.

D'un point de vue pratique, l'audit est réalisé avec syslog, outil qui permet de rediriger les événements indifféremment sur un fichier, un écran ou une autre machine du réseau en fonction du degré de sévérité. Les quatre niveaux (level) info, notice, warning et alert de syslog correspondent à ceux décrits. Pour des raisons de performance, les messages à destination de l'interface graphique sont postés dans une file de messages Unix.

3.2 Visualisation graphique

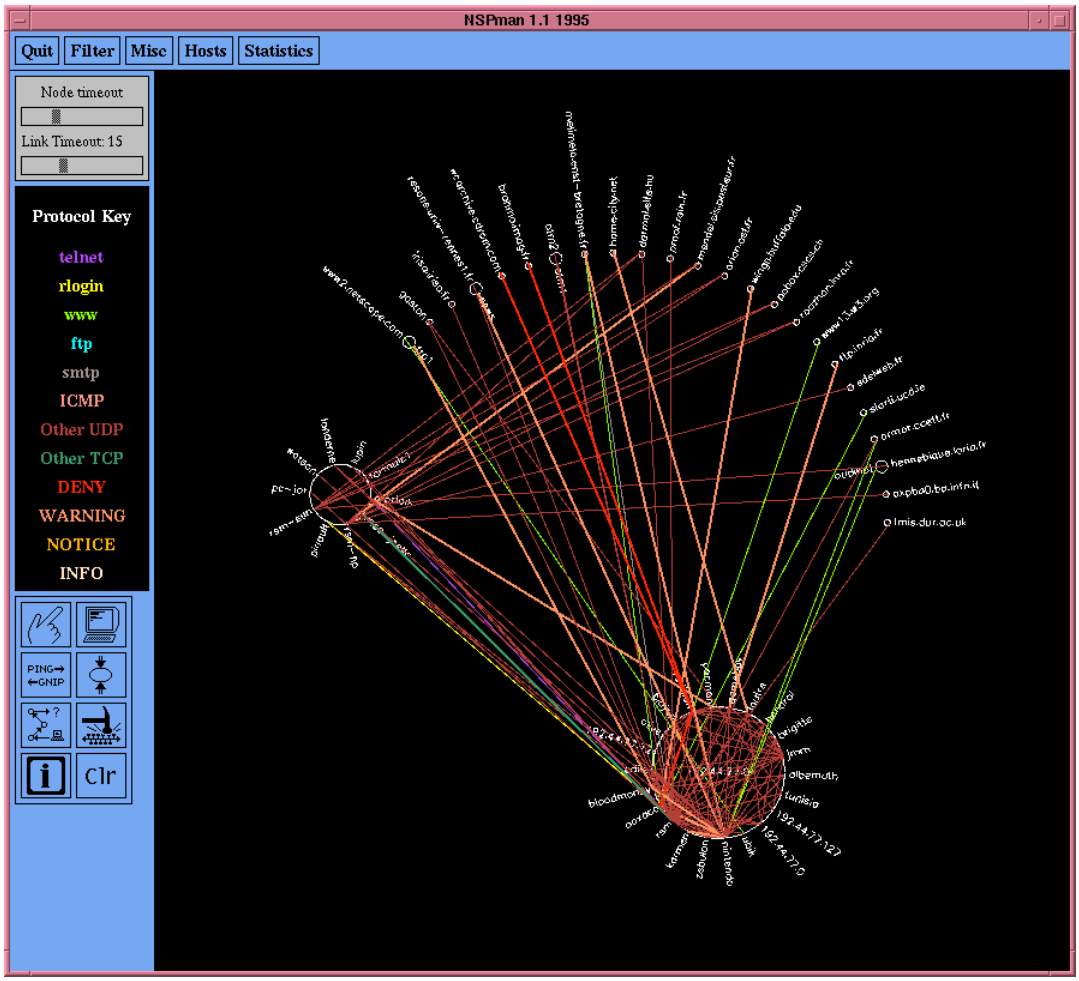

Figure 2 : *Supervision de la sécurité*

Pour donner une vision synthétique des événement d'audit, l'Analyseur de Sécurité utilise une visualisation graphique.

Il offre à l'administrateur sécurité le moyen d'observer:

- les communications TCP autorisées établies à l'instant de l'observation,
- celles qui ont été coupées car en violation avec les droits d'accès définis dans la politique de sécurité,
- les messages ICMP.

Remarque: certains services UDP pourraient y être facilement ajoutés au besoin.

Un graphe en deux dimensions représente l'ensemble du trafic: les communication sont représentées sous forme de trait de couleur reliant deux interlocuteurs, les interlocuteurs appartenant au même réseau au sens IP sont placés sur un même cercle et leur nom est donné de préférence sous sa forme DNS, plus «parlante» que l'adresse IP.

Pour ne pas surcharger l'écran mais garder néanmoins trace des violations de la politique de sécurité, les communications TCP autorisées restent à l'écran pour un temps égal à leur durée, le reste du trafic (communications en violation avec la politique de sécurité et messages ICMP) ne s'efface que sur demande de l'opérateur.

La signification des couleurs est indiquée sur la gauche de l'écran, il y a une couleur différente pour signaler:

- les communications interdites par la politique de sécurité,
- celles en cours d'authentification,
- les messages ICMP,
- et parmi les communications autorisées, les services ftp, smtp, www, telnet et rlogin ont chacune une couleur différente, une dernière couleur permettant de visualiser toutes les autres communications TCP autorisées.

En cliquant sur l'extrémité d'une communication qui a violé la politique de sécurité, on obtient les *raisons précises de la coupure*.

Cette interface graphique a été réalisée à partir de la licence source du logiciel netman diffusé par l'Université Curtin de Perth en Australie. Il s'appelle *nspman*.

3.3 Visualisation graphique des audits à posteriori

Un outil a été dérivé du précédent et s'appelle *nspview*.

`# nspview nsplog` lance une visualisation graphique du contenu du fichier nsplog

`# grep telnet | nspview` n'affichera que les communication telnet, celles qui ont été autorisées et celles qui ont été coupées.

3.4 Mise au point itérative du contrôle d'accès

Une utilisation de la fonction de supervision non prévue lors de sa conception mais découverte à l'usage est la capacité qu'elle donne d'affiner une politique de sécurité par itérations successives, sans aucune gêne pour les utilisateurs. C'est particulièrement utile au début d'une réflexion sur la politique de sécurité à mettre en oeuvre, lorsqu'un site ne connaît pas toutes les communications qu'il a avec l'extérieur.

Cela suppose d'invalider la fonction coupure de communications de l'Analyseur de Sécurité, ce qui est possible à partir de son panneau de contrôle . Toute communication violant la politique de sécurité est donc signalée à l'écran mais pas interrompue, L'administrateur sécurité a alors le choix entre rajouter cette communication à la liste des autorisées ou ne rien modifier. Il a dans ce dernier cas la possibilité d'informer l'utilisateur des raisons pour lesquelles ses communications seront coupées lors de la mise en oeuvre réelle et de rechercher avec lui une solution de remplacement acceptable du point de vue sécurité. L'itération se fait sur le nombre de cas à traiter.

4 CONCLUSION

Avec cette fonction de supervision proposée par l'Analyseur de Sécurité, l'administrateur sécurité dispose d'un outil indépendant pour surveiller la politique de contrôle d'accès réellement mise en oeuvre sur son réseau.

En plus de la supervision, cet outil peut intervenir sur le contrôle des accès TCP. Il est en cela complémentaire des autres équipements qui contribuent à la sécurité que sont les hubs sécurisés, les routeurs, les serveurs d'accès ou les démons sécurisés.

L'Analyseur ne travaille actuellement qu'avec les protocoles TCP/IP mais ses principes de fonctionnement peuvent facilement être étendus à d'autres familles de protocoles.

5 BIBLIOGRAPHIE

[1] *ITSEC - Information Technology Information Criteria.* Commission of the European Communities, v 1.2 edition, June 1991.

[2] *RFC 1244 - Site Security Handbook,* July 1991.

[3] D. Brent CHAPMAN and Elizabeth D. ZWICKY. *Building Internet Firewalls,* ISBN 1-56592-124-0, O'Reilly & Associates, 1995.

[4] Pierre ROLIN, Sylvain GOMBAULT et Laurent TOUTAIN. *Protection des réseaux de télécommunications.* Brevet : no 94-02963 du 11 mars 1994.

[5] P. ROLIN, Sylvain GOMBAULT et Laurent TOUTAIN. *Vérification d'intégrité de données échangées entre deux stations de réseau de télécommunications,* brevet no 94-02964 du 11 mars 1994.

[6] Christophe BIDAN et Sylvain GOMBAULT. La sécurité inter-domaines à l'aide des Analyseurs de Sécurité, *Colloque Francophone sur l'Ingénierie des Protocoles CFIP'95, Rennes,* Mai 95.

[7] William R. CHESWICK and Steven M. BELLOVIN. *Firewalls and Internet Security,* ISBN 0-201-63357-4, Addison-Wesley Professional Computing Series, 1994.

[8] *ISO 7498-2. Basic Reference Model - Part 2. Security Architecture,* Febr. 1989.

[9] P. ROLIN, L. TOUTAIN and S. GOMBAULT. An Optimistic Approch to Secure Network Acces Control. *ACM Conference on Computers and Communications Security,* November 1994

Sylvain GOMBAULT

Enseignant chercheur à l'ENST de Bretagne au sein du département Réseaux et Services Multimedia situé à Rennes, Sylvain Gombault est responsable du projet de recherche Analyseur de Sécurité. Il enseigne la sécurité des réseaux et la conception de réseaux d'entreprise aux étudiants qui sont en année de spécialisation.
Sylvain.Gombault@rennes.enst-bretagne.fr
http://www.rennes.enst-bretagne.fr

Stéphane RUAUD

Après une formation universitaire ponctuée par un DESS d'Informatique à Rennes en Juin 95, Stéphane Ruaud a participé à la finalisation graphique de la première version de NSP au cours d'un stage de 7 mois à Télécom Bretagne.
Cette année, il a développé et mis en place les applications nécessaires à la gestion des études des élèves ingénieurs de l'ENSAE sur ORACLE. Il a aussi contribué à l'apparition d'un serveur intranet dans cette école, en offrant une interface d'accès à la base de données via WWW.
Il étudie actuellement les évolutions de JAVA et de VRML.
ruaud@supaero.fr
http://www.supaero.fr/page-perso/divers/ruaud/

SUPERVISEUR DE SÉCURITÉ POUR SITE INTERNET

Sylvain GOMBAULT
ENST de Bretagne
Département Réseaux et Services Multimedia
BP 78, 35512 Cesson-Sévigné - France
Tél.: 99 12 70 37 - Fax: 99 12 70 30
Sylvain.Gombault@rennes.enst-bretagne.fr

Stéphane RUAUD
ENST de Bretagne
Département Réseaux et Services Multimedia
BP 78, 35512 Cesson-Sévigné - France
ruaud@supaero.fr

Résumé:

Toute politique de sécurité doit prévoir les moyens de contrôler sa mise en oeuvre. Cette surveillance est d'autant plus efficace qu'elle est réalisée par des outils indépendants. L'Analyseur de Sécurité, un outil de sécurité réseau pour site Internet, remplit ce rôle de superviseur de sécurité autonome. Après la description de ses fonctionalités, ce document présente l'étude de l'interface de surveillance développée à l'usage de l'administrateur sécurité.

SUPERVISEUR DE SÉCURITÉ POUR SITE INTERNET

Sylvain GOMBAULT
ENST de Bretagne
Département Réseaux et Services Multimedia
BP 78, 35512 Cesson-Sévigné - France
Tél.: 99 12 70 37 - Fax: 99 12 70 30
Sylvain.Gombault@rennes.enst-bretagne.fr

Stéphane RUAUD
ENST de Bretagne
Département Réseaux et Services Multimedia
BP 78, 35512 Cesson-Sévigné - France
ruaud@supaero.fr

Abstract:

Any good security policy includes procedures to verify its results. This monitoring needs to be performed by stand-alone tools. The Network Security Probe (l'Analyseur de Sécurité) designed for Internet site security, is an independant security monitor. This paper presents its functionalities and describes the monitoring interface provided to security administrators.

1 INTRODUCTION

Le raccordement mondial des sites informatiques autour d'Internet pose des problèmes en matière de sécurité. Le risque majeur vient de la standardisation des matériels et des logiciels : du fait de leur complexité les logiciels peuvent comporter des trous de sécurité , une faille trouvée sur un équipement est reproductible sur d'autres sites équipés de produits identiques. Sans verser dans le catastrophisme, cela oblige chaque entreprise à se protéger.

Chaque organisme gère de manière différente les informations qu'il considère sensibles. La politique de sécurité d'un organisme est l'ensemble des règles et pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées au sein de cet organisme [1] [2]. Vérifier que la politique de sécurité est bien appliquée fait partie intégrante de sa mise en oeuvre.

Un certain nombre d'outils d'origine commerciale ou distribués gratuitement sur Internet [3] permettent de mettre en oeuvre la politique de sécurité d'un site. Il est recommandé [2] d'en contrôler le résultat avec un outil indépendant.

L'Analyseur de Sécurité est développé à l'ENST de Bretagne, au sein du département RSM (Réseaux et Services Multimedia) de Rennes. Utilisé seul, il propose une solution pour mettre en place et contrôler la politique de sécurité au sein d'un site TCP/IP, qu'il soit raccordé ou non à Internet ; installé en complément d'autres outils, il contrôle qu'une politique de sécurité est bien appliquée grâce à des fonctions de supervision. Il intègre des innovations ayant fait l'objet de deux dépôts de brevet [4] [5].

2 L'ANALYSEUR DE SÉCURITÉ

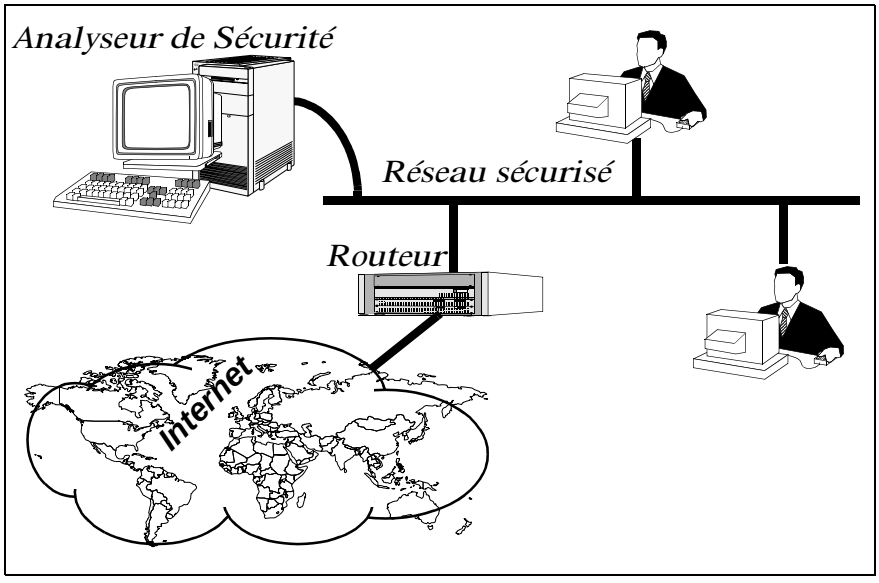

Figure 1 : *Place de l'Analyseur de Sécurité dans un réseau Ethernet*

L'Analyseur de Sécurité est un logiciel qui s'exécute sur toute station de travail munie d'une interface réseau avec laquelle il écoute le trafic. Il s'appelle alors NSP, l'acronyme de son nom anglais: Network Security Probe (cf par. 2.6). Comme tout analyseur de protocole, il est basé sur l'écoute passive et l'analyse du trafic. A partir de ces données et par rapport à une politique de sécurité prédéfinie, il y ajoute la détection des intrusions qu'il combat en alertant l'administrateur sécurité et en interrompant les communications.

2.1 Originalités et caractéristiques

L'architecture de l'Analyseur de Sécurité en fait un outil *indépendant* dont l'installation ne demande *aucune modification* des équipements de réseau ou de sécurité existants. Son fonctionnement est *transparent aux applications* et ne leur impose aucune contrainte, il ne modifie en rien leurs *performances* : il n'introduit aucune charge supplémentaire sur le réseau ni délai dans les échanges car il travaille en total parallélisme.

Il est *dédié* uniquement à des fonctions de sécurité, ce qui permet, d'un point de vue organisationnel, de *dissocier* l'administration de la sécurité de la gestion du réseau, suivant en cela le fait qu'il est recommandé de séparer les fonctions de responsable sécurité des fonctions d'administrateur réseau [2]. L'autre avantage est que cela n'impose aucun choix en ce qui concerne les équipements (routeurs, hubs).

Il est *indétectable* du point de vue du réseau, y compris lorsqu'il génère du trafic (cf par. 2.4), même par un analyseur : cette propriété est importante pour sa sécurité mais également pour celle du site car elle n'incite pas un intrus à prendre des voies détournées ou à masquer outre-mesure son attaque.

Le trafic capturé est traité de manière *optimiste*: la majorité des communications étant légitimes, elles ne doivent pas être pénalisées par la présence d'un équipement de sécurité. L'Analyseur de sécurité laisse donc une communication s'établir normalement (a priori optimiste) pendant qu'il la compare à la politique de sécurité, il la coupe éventuellement ensuite.

Il analyse tout le trafic passant sur le réseau local et peut donc appliquer une politique de sécurité de contrôle d'accès sur des communications *locales*.

La simplification de sa configuration a fait l'objet d'une étude particulière : il se configure rapidement grâce à un outil graphique convivial qui repose sur l'utilisation de fichiers en mode texte et qui sait aller *interroger les bases* NIS ou DNS pour en extraire les listes de machines, de réseaux, d'utilisateurs ou de services.

2.2 Services de sécurité

L'ISO 7498-2 [8] définit un ensemble de services et de mécanismes de sécurité. L'Analyseur de Sécurité ne respecte pas l'architecture de sécurité OSI qui place les éléments de sécurité dans les entités d'extrémité mais les services qu'il propose peuvent être décrits avec les définitions de cette norme:

- contrôle d'accès (cf par. 2.3),
- authentification de l'entité émettrice et/ou réceptrice par délégation (cf par. 2.5),
- intégrité des données (cf par. 2.5),
- non répudiation: de par sa position, il peut certifier avoir vu ou non passer certaines informations,
- audit des communications (cf par. 3.1)

Les services que son architecture ne lui permet pas de fournir:

- confidentialité : n'étant pas sur le chemin des données, il n'a aucun moyen de les chiffrer ou de les masquer,
- disponibilité : il ne peut garantir la disponibilité du réseau,
- secret du flux : il ne peut masquer le fait qu'une communication a lieu.

2.3 Politique de sécurité et contrôle d'accès

La politique de sécurité définit les droits d'accès aux ressources. L'Analyseur de Sécurité permet uniquement de réaliser un contrôle d'accès sur les communications TCP (elles sont en mode connecté et il sait les interrompre).

Il possède sa propre description des droits d'accès voulus par la politique de sécurité : c'est un ensemble de règles décrivant le service *contrôle d'accès* qu'il fournit et qui sont élaborées à partir des critères suivants:

- adresse IP source et destination,
- service (lié au numéro de port),
- utilisateur lorsque cela a un sens (telnet, ftp, rlogin),
- heure,
- type d'audit : synthétique ou détaillé,
- action: autoriser, authentifier ou couper la communication.

Par défaut, toute communication non explicitement autorisée est coupée.

Ces critères sont plus riches que les fonctions de filtrage proposées par les routeurs. Ils permettent d'affiner le filtrage des services TCP autorisés au travers du routeur en jouant sur l'heure ou l'utilisateur.

2.4 Coupure des communications

L'Analyseur de Sécurité interrompt une communication TCP en émettant deux TCP Reset à destination des deux interlocuteurs, en se faisant passer à chaque fois pour l'autre extrémité. Sa présence n'est pas trahie par ces émissions.

2.5 Services intersites

En dialoguant avec un homologue, l'Analyseur de Sécurité peut authentifier dynamiquement par délégation l'émetteur et/ou le récepteur d'une communication, confirmer l'intégrité des documents reçus ou émis.

Ces fonctions ont fait l'objet d'une publication et sont décrites de manière plus approfondie dans [6].

2.6 Le logiciel NSP (Network Security Probe)

NSP est le nom du logiciel Analyseur de Sécurité. Il fonctionne en environnement Unix (HP-UX v10 et Solaris 2.5) et est disponible gratuitement sur le site:

- `http://www.rennes.enst-bretagne.fr`

3 SUPERVISION DE LA SÉCURITÉ

L'Analyseur de Sécurité possède une interface de supervision destinée à l'administrateur sécurité qui donne une vue complète et synthétique des événement liés à la sécurité d'un site.

Cette supervision est alimentée par les événements générés par son propre audit. Ils peuvent être enregistrés classiquement sur support magnétique: cette manière de trai-

ter l'audit est utile car elle permet des recherches à posteriori d'événements précis mais ne répond pas à toutes les attentes de l'administrateur sécurité qui souhaite également une analyse temps réel des événements.

Deux choses l'intéressent en particulier: être prévenu en immédiatement des tentatives d'intrusion mais aussi connaître à tout instant les communications autorisées établies. Pour en donner une vision synthétique, l'Analyseur de Sécurité utilise une visualisation graphique qui est décrite après la présentation de ses fonctions d'audit.

3.1 Audit

L'audit de l'Analyseur de Sécurité concerne le trafic observé, la politique de sécurité et la vie des processus.

L'audit sur le trafic a été conçu de manière à signaler tout événement réseau intéressant la sécurité, à savoir:

- le début et la fin des communications TCP: adresses IP, noms DNS, numéros de port, et heure;
- les utilisateurs des services telnet, rlogin et ftp;
- lorsque le mode détaillé est sélectionné, l'ensemble des commandes pour les seuls services ftp, smtp et http;
- le trafic ICMP autres que les messages echo et echo/reply de 64 octets ou moins [7].

L'audit sur la politique de sécurité trace les événement liés aux décisions prises par l'Analyseur de Sécurité:

- quelle règle de la politique de sécurité a provoqué l'autorisation, l'interruption ou une demande d'authentification pour une communication;
- la raison de la coupure: absence de règle, mauvais utilisateur, mauvaise heure...
- les demandes d'authentification et leur résultat.

Cet audit serait incomplet sans une surveillance de la vie des processus sur lesquels repose la sécurité du site, il indique donc:

- les heures de lancement et d'arrêt des processus de l'Analyseur de Sécurité.

Les messages générés par l'Analyseur de Sécurité sont répartis selon quatre niveaux de sévérité et adaptés à des outils d'audit capables d'effectuer une sélection en fonction de ce critère:

- les messages de premier niveau sont tous ceux dont la connaissance immédiate n'est pas indispensable à la sécurité, mais dont il est indispensable de conserver une trace comme par exemple les débuts et fin de communication,
- ceux de deuxième niveau permettent de suivre l'exécution des mécanismes de sécurité: vérification d'utilisateur, authentification et dont l'échec ne met pas en cause la sécurité du site mais provoque la coupure de la communication,
- les alertes au niveau sécurité sont de troisième niveau, il s'agit des messages indiquant les communications coupées,
- le changement de comportement de l'Analyseur de Sécurité est indiqué les messages de quatrième niveau signalent la mort ou le redémarrage d'un processus, passage du mode simulé au mode coupure des communications.

D'un point de vue pratique, l'audit est réalisé avec syslog, outil qui permet de rediriger les événements indifféremment sur un fichier, un écran ou une autre machine du réseau en fonction du degré de sévérité. Les quatre niveaux (level) info, notice, warning et alert de syslog correspondent à ceux décrits. Pour des raisons de performance, les messages à destination de l'interface graphique sont postés dans une file de messages Unix.

3.2 Visualisation graphique

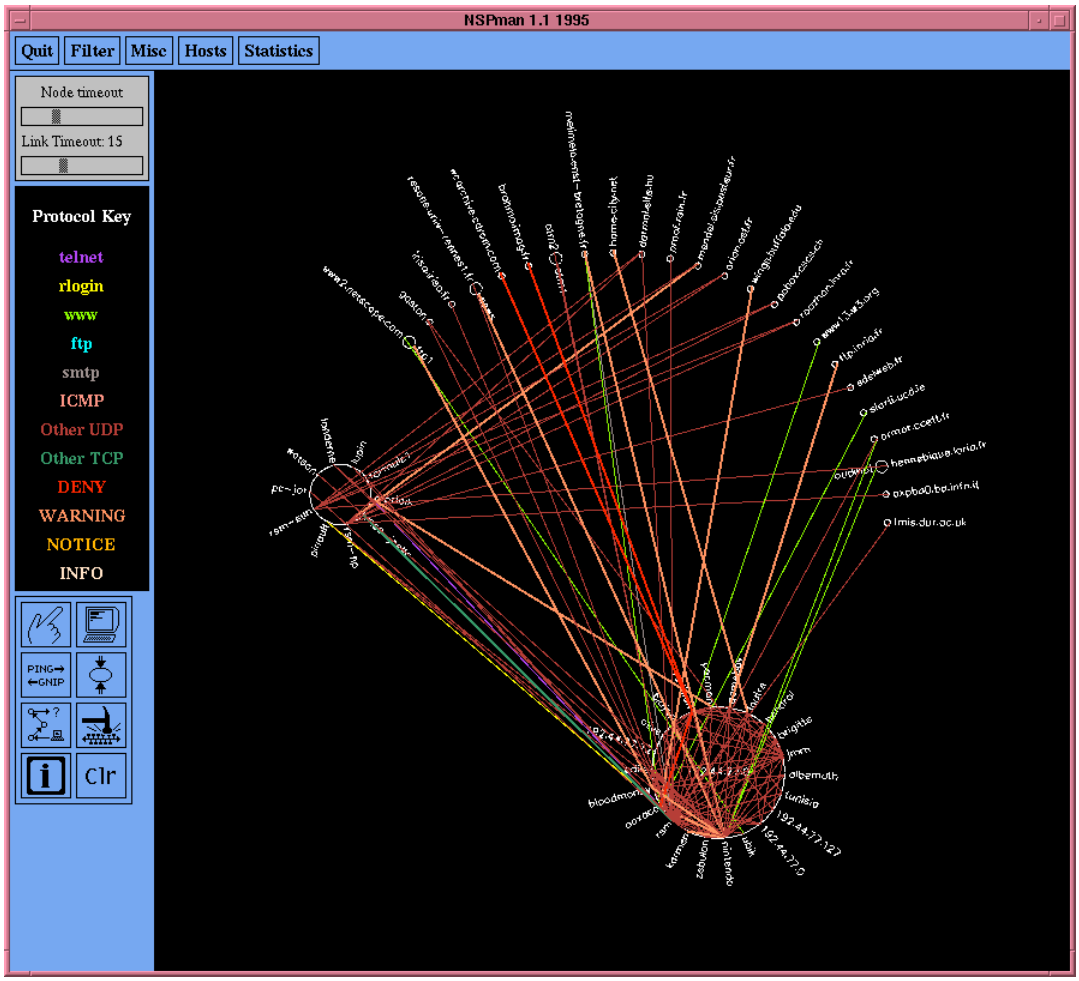

Figure 2 : *Supervision de la sécurité*

Pour donner une vision synthétique des événement d'audit, l'Analyseur de Sécurité utilise une visualisation graphique.

Il offre à l'administrateur sécurité le moyen d'observer:

- les communications TCP autorisées établies à l'instant de l'observation,
- celles qui ont été coupées car en violation avec les droits d'accès définis dans la politique de sécurité,
- les messages ICMP.

Remarque: certains services UDP pourraient y être facilement ajoutés au besoin.

Un graphe en deux dimensions représente l'ensemble du trafic: les communication sont représentées sous forme de trait de couleur reliant deux interlocuteurs, les interlocuteurs appartenant au même réseau au sens IP sont placés sur un même cercle et leur nom est donné de préférence sous sa forme DNS, plus «parlante» que l'adresse IP.

Pour ne pas surcharger l'écran mais garder néanmoins trace des violations de la politique de sécurité, les communications TCP autorisées restent à l'écran pour un temps égal à leur durée, le reste du trafic (communications en violation avec la politique de sécurité et messages ICMP) ne s'efface que sur demande de l'opérateur.

La signification des couleurs est indiquée sur la gauche de l'écran, il y a une couleur différente pour signaler:

- les communications interdites par la politique de sécurité,
- celles en cours d'authentification,
- les messages ICMP,
- et parmi les communications autorisées, les services ftp, smtp, www, telnet et rlogin ont chacune une couleur différente, une dernière couleur permettant de visualiser toutes les autres communications TCP autorisées.

En cliquant sur l'extrémité d'une communication qui a violé la politique de sécurité, on obtient les *raisons précises de la coupure*.

Cette interface graphique a été réalisée à partir de la licence source du logiciel netman diffusé par l'Université Curtin de Perth en Australie. Il s'appelle *nspman*.

3.3 Visualisation graphique des audits à posteriori

Un outil a été dérivé du précédent et s'appelle *nspview*.

`# nspview nsplog` lance une visualisation graphique du contenu du fichier nsplog

`# grep telnet | nspview` n'affichera que les communication telnet, celles qui ont été autorisées et celles qui ont été coupées.

3.4 Mise au point itérative du contrôle d'accès

Une utilisation de la fonction de supervision non prévue lors de sa conception mais découverte à l'usage est la capacité qu'elle donne d'affiner une politique de sécurité par itérations successives, sans aucune gêne pour les utilisateurs. C'est particulièrement utile au début d'une réflexion sur la politique de sécurité à mettre en oeuvre, lorsqu'un site ne connaît pas toutes les communications qu'il a avec l'extérieur.

Cela suppose d'invalider la fonction coupure de communications de l'Analyseur de Sécurité, ce qui est possible à partir de son panneau de contrôle . Toute communication violant la politique de sécurité est donc signalée à l'écran mais pas interrompue, L'administrateur sécurité a alors le choix entre rajouter cette communication à la liste des autorisées ou ne rien modifier. Il a dans ce dernier cas la possibilité d'informer l'utilisateur des raisons pour lesquelles ses communications seront coupées lors de la mise en oeuvre réelle et de rechercher avec lui une solution de remplacement acceptable du point de vue sécurité. L'itération se fait sur le nombre de cas à traiter.

4 CONCLUSION

Avec cette fonction de supervision proposée par l'Analyseur de Sécurité, l'administrateur sécurité dispose d'un outil indépendant pour surveiller la politique de contrôle d'accès réellement mise en oeuvre sur son réseau.

En plus de la supervision, cet outil peut intervenir sur le contrôle des accès TCP. Il est en cela complémentaire des autres équipements qui contribuent à la sécurité que sont les hubs sécurisés, les routeurs, les serveurs d'accès ou les démons sécurisés.

L'Analyseur ne travaille actuellement qu'avec les protocoles TCP/IP mais ses principes de fonctionnement peuvent facilement être étendus à d'autres familles de protocoles.

5 BIBLIOGRAPHIE

[1] *ITSEC - Information Technology Information Criteria.* Commission of the European Communities, v 1.2 edition, June 1991.

[2] *RFC 1244 - Site Security Handbook,* July 1991.

[3] D. Brent CHAPMAN and Elizabeth D. ZWICKY. *Building Internet Firewalls,* ISBN 1-56592-124-0, O'Reilly & Associates, 1995.

[4] Pierre ROLIN, Sylvain GOMBAULT et Laurent TOUTAIN. *Protection des réseaux de télécommunications.* Brevet : no 94-02963 du 11 mars 1994.

[5] P. ROLIN, Sylvain GOMBAULT et Laurent TOUTAIN. *Vérification d'intégrité de données échangées entre deux stations de réseau de télécommunications,* brevet no 94-02964 du 11 mars 1994.

[6] Christophe BIDAN et Sylvain GOMBAULT. La sécurité inter-domaines à l'aide des Analyseurs de Sécurité, *Colloque Francophone sur l'Ingénierie des Protocoles CFIP'95, Rennes,* Mai 95.

[7] William R. CHESWICK and Steven M. BELLOVIN. *Firewalls and Internet Security,* ISBN 0-201-63357-4, Addison-Wesley Professional Computing Series, 1994.

[8] *ISO 7498-2. Basic Reference Model - Part 2. Security Architecture,* Febr. 1989.

[9] P. ROLIN, L. TOUTAIN and S. GOMBAULT. An Optimistic Approch to Secure Network Acces Control. *ACM Conference on Computers and Communications Security,* November 1994

Sylvain GOMBAULT

Enseignant chercheur à l'ENST de Bretagne au sein du département Réseaux et Services Multimedia situé à Rennes, Sylvain Gombault est responsable du projet de recherche Analyseur de Sécurité. Il enseigne la sécurité des réseaux et la conception de réseaux d'entreprise aux étudiants qui sont en année de spécialisation.
Sylvain.Gombault@rennes.enst-bretagne.fr
http://www.rennes.enst-bretagne.fr

Stéphane RUAUD

Après une formation universitaire ponctuée par un DESS d'Informatique à Rennes en Juin 95, Stéphane Ruaud a participé à la finalisation graphique de la première version de NSP au cours d'un stage de 7 mois à Télécom Bretagne.
Cette année, il a développé et mis en place les applications nécessaires à la gestion des études des élèves ingénieurs de l'ENSAE sur ORACLE. Il a aussi contribué à l'apparition d'un serveur intranet dans cette école, en offrant une interface d'accès à la base de données via WWW.
Il étudie actuellement les évolutions de JAVA et de VRML.
ruaud@supaero.fr
http://www.supaero.fr/page-perso/divers/ruaud/