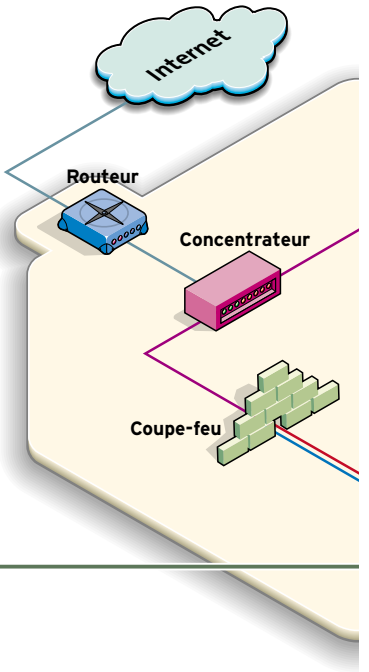
SÉCURITÉ

Détection d'intrusions : prévenir plutôt que guérir

Les sondes de détection d'intrusions sont les yeux du responsable de la sécurité. Complexes à paramétrer, elles alertent néanmoins en cas d'attaque et permettent de riposter avec les moyens appropriés.

Par **Frédéric Bordage**



SI VOUS ÊTES PRESSÉ

Les sondes de détection d'intrusions complètent les coupe-feu en alertant les administrateurs réseau de toute tentative de piratage. Contrairement aux coupe-feu, les sondes ne bloquent pas les attaques. Leur mise en œuvre nécessite de bonnes connaissances techniques mais c'est surtout un investissement difficile à justifier… tant que l'entreprise n'a pas subi de dommages. Les sondes génèrent beaucoup de fausses alertes et peuvent donc se révéler consommatrices de temps. D'autant qu'il faut remettre à jour les fichiers de signatures et reparamétrer régulièrement les règles. Des solutions hébergées apparaissent pour décharger l'entreprise de ces contraintes.

La sécurité est le sujet tabou de toutes les directions informatiques. D'abord parce qu'elles ne savent jamais avec certitude ce qui se passe réellement sur leurs serveurs et, ensuite, parce qu'une attaque peut générer des dégâts considérables pour l'entreprise.

Les sondes de détection d'intrusions, appelées également IDS (Intrusion Detection System), les aident à y voir plus clair. Commercialisées sous la forme de logiciels, de boîtiers voire de services FAH (fourniture d'applications hébergées, ces sondes ne bloquent pas les attaques. En revanche, elles les signalent aux responsables informatiques afin qu'ils puissent prendre rapidement les contre-mesures adaptées. *« Les coupe-feu ne sont pas suffisants. On oublie trop souvent que les attaques proviennent parfois du réseau interne. Un employé qui connaît bien le système d'information de l'entreprise peut générer des pertes d'exploitation importantes »*, rappelle Alain Rossi, directeur des systèmes d'information du CFCE (Centre français du commerce extérieur). C'est souvent une attaque réussie qui déclenche l'installation d'une sonde. *« C'était un projet "dormant" que le piratage de quelques serveurs sensibles a brutalement réveillé »*, illustre Guillaume Arcas, en mission d'ingénierie chez un opérateur télécoms.

Des trafics réseaux ralentis

- Les sondes de détection d'intrusions peuvent parfois pénaliser les temps de réponse du réseau si elles ne sont pas assez rapides.
- Snort n'est pas adapté à des bandes passantes supérieures à 20 Mbit/s tandis que d'autres produits tels que le boîtier Network Sensor 3000 de Sourcefire ou SecureNetPro d'Intrusion peuvent traiter jusqu'à un 1 Gbit/s.
- Les sondes les plus performantes prennent la forme de boîtiers dédiés.

L'UTILISATION

Analyser le trafic réseau et détecter les attaques

L'utilisation quotidienne d'une sonde obéit à un rythme immuable : mise à jour des fichiers de signatures, analyse des événements, réaction en cas d'alerte sérieuse ou affinage des paramètres en cas de fausse alerte. *« Au même titre qu'un logiciel antivirus, il faut garder ses bases de signatures à jour. Une seule signature manquante, c'est tout ce dont les pirates ont besoin pour entrer sans être détectés »*, rappelle Patrick Chevalier, analyste sécurité dans une entreprise canadienne. *« Lorsqu'une attaque est détectée, je regarde de quoi il s'agit. 90 % sont des "faux positifs", c'est-à-dire de fausses alertes. Pour les autres, j'étudie la règle qui s'est déclenchée et j'évalue le risque »*, détaille Jean-Michel Barbet, administrateur systèmes et réseaux à l'École des Mines de Nantes (Laboratoire Subatech de l'IN2P3). *« Souvent, une alerte ne nécessite aucune action particulière : par exemple, une attaque Nimda, qui n'affecte que les serveurs IIS fonctionnant avec Windows, sera pourtant détectée sur un serveur Apache fonctionnant avec Unix et sur lequel elle est inoffensive »*, précise Guillaume Arcas. Il faut alors déterminer pourquoi la sonde s'est comportée de cette façon face à un trafic normal et modifier ou désactiver la règle incriminée pour diminuer le nombre de faux positifs.

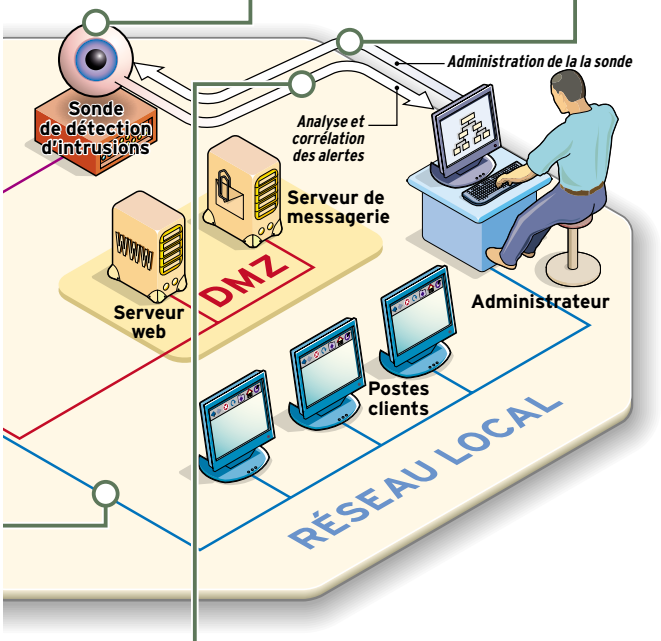
Avant de prendre les mesures qui s'imposent face à une attaque réelle, *« il faut d'abord la classifier – manœuvre d'approche, tenta-*

De nombreuses fausses alertes

- Les fausses alertes (faux positifs) constituent le problème numéro un des IDS.
- Des alertes trop nombreuses ou mal corrélées entraînent un « bruit » trop important qui ne permet pas aux équipes informatiques de se concentrer sur les attaques sensibles.
- Les faux positifs peuvent augmenter la charge (temps) nécessaire à l'administration du système de détection.

Des mises à jour automatiques

- La plupart des IDS utilisent une base de signatures d'attaques qui limite les efforts de configuration.
- Les signatures sont automatiquement téléchargées puis mises à jour au sein de l'outil.
- Les règles et les signatures sont écrites dans un langage de script tel que N-code ou Snort rule qui est vite maîtrisé par la plupart des administrateurs système et réseau.



Des outils tiers d'analyse

- L'analyse des événements enregistrés par la sonde peut s'effectuer avec des logiciels complémentaires tels qu'Acid ou PureSecure pour la sonde open source Snort.
- D'autres logiciels comme Nessus (audit de vulnérabilité) ou des scanners de port permettent de reproduire une attaque afin de tester une règle.

tive non aboutie, attaque réussie, etc. – pour réagir correctement et identifier l'attaquant avant de le bloquer, même s'il est souvent difficile d'exploiter les informations recueillies », déplore Alain Rossi du CFCE. Diverses ripostes existent. *« On peut modifier des règles au niveau du coupe-feu pour bloquer l'attaquant ou prendre des mesures de protection supplémentaires* [antivirus, nouvelles règles de sécurité, etc., Ndlr] *»,* détaille Patrick Chevalier. La plus grosse difficulté reste l'analyse et la corrélation des événements car les sondes génèrent un volume important d'informations. Des outils complémentaires tels qu'Acid ou PureSecure dans le cas de Snort facilitent le travail. Le laboratoire Subatech analyse a posteriori les paquets suspects avec Ethereal. Des logiciels tels que Hoghwash peuvent aussi réagir automatiquement aux alertes en modifiant dynamiquement les règles du coupe-feu afin de bloquer l'attaquant. D'où, par conséquent, l'intérêt de réduire au maximum le nombre de faux positifs.

RETOUR D'EXPÉRIENCE


Jim Wallace

Conseil général de la Manche

- **Siège :** Saint-Lô (50).
- **Effectif :** 1 200 personnes.
- **Budget informatique 2002/2003 :** environ 4 millions d'euros.

Stéphane Riffard, chef de projet système.

Gestion des compétences

« Nous préférons externaliser l'administration de notre sonde »

Les 950 postes de travail et serveurs du Conseil général de la Manche sont connectés à Internet par une liaison spécialisée. *« Suite à des attaques du type CodeRed, nous avons constaté qu'un coupe-feu n'était pas suffisant pour garantir la sécurité de notre système d'information. Nous avons donc acquis une sonde de détection d'intrusions auprès de l'éditeur ISS »,* explique Stéphane Riffard, chef de projet système. L'administration et l'analyse des alertes prennent environ 1 h 30 par jour. En cas de doute, l'équipe informatique vérifie l'intégrité des serveurs attaqués. Mais ne disposant pas d'équipe d'astreinte, *« nous allons confier cette mission à un prestataire. Les pirates ne s'arrêtent pas après 18 heures et le week-end »,* justifie Stéphane Riffard. D'abord tenté par le logiciel open source Snort, le Conseil général a dû se rendre à l'évidence, *« la moitié des sociétés de services ne connaissent pas cet outil. Nous avons donc choisi l'un des produits leaders du marché pour en faciliter l'externalisation ».* En plus d'une licence de 12 000 euros, l'externalisation devrait représenter un budget d'un peu plus de 50 000 euros. Un budget important *« optimisé par un transfert de compétences lors de l'installation ainsi que par la mise en place des logiciels sur des serveurs Linux ».*

« Au début, nous refusions de bloquer des trames suspectes car nous avions trop de fausses alertes et ne voulions pas bloquer notre propre trafic », explique Samuel Chaboisseau. L'autoconfiguration des coupe-feu est d'ailleurs peu pratiquée. *« C'est une approche dangereuse car un pirate peut attaquer dans le seul but de bloquer des plages complètes d'adresses en faisant réagir la sonde. Il vaut certainement mieux la configurer pour qu'elle puisse couper les connexions »,* conseille Alain Rossi.

LA MISE EN ŒUVRE

Choisir le bon outil et le paramétrer finement

Il existe une grande variété de sondes. *« Snort est un logiciel libre. On peut donc l'essayer avant de se décider »,* indique Jean-Michel Barbet. *« Nous avions acheté une sonde commerciale, mais après six mois de tests, nous avons retenu Snort car il s'est révélé plus efficace »,* ajoute Samuel Chaboisseau. *« Nous exploitons Network Sensor de Sourcefire car c'est l'IDS qui remonte* **(suite p. 38)**

(suite de la p. 37) *le moins de faux positifs »,* explique Sébastien Reister, administrateur système chez Accenture. Dans ce cabinet de consultants, d'autres critères ont été pris en compte comme la facilité de maintenance et le prix *« inférieur à celui du principal concurrent ISS »*. Les critères discriminants sont l'efficacité et la capacité de traitement de la sonde. L'opérateur de télécoms chez qui travaille Guillaume Arcas utilise Prelude-IDS. Ce logiciel open source possède une architecture distribuée bien adaptée aux grands réseaux qui utilisent plusieurs sondes. *« On peut facilement l'enrichir avec un produit comme Nessus, qui apporte une vision complète des attaques et de la vulnérabilité de chaque serveur »,* précise-t-il. L'installation de la sonde ne pose généralement pas de difficulté. *« Seule la phase de paramétrage est difficile »,* résume Sébastien Reister. L'assistance d'un spécialiste est souvent indispensable au début de l'exploitation pour affiner l'analyse de certains événements ou mettre en œuvre des procédures spécifiques. *« Par défaut, Snort remonte trop d'alarmes. Nous avons donc fait appel à un prestataire – KDX Ingénierie – qui a développé un filtre qui traite les log de Snort en exploitant une base de connaissances. Le plus gros travail a été de créer cette base »,* précise Samuel Chaboisseau.

LES RESSOURCES

Des compétences réseau et du temps

Les compétences sont le nerf de la guerre. *« Une personne qui ne connaît pas les principaux protocoles, TCP, UDP et ICMP, ne peut pas mettre en œuvre un IDS, même si l'installation est automatisée et l'interface bien faite »,* estime Jean-Michel Barbet. *« Il faut également avoir une bonne compréhension des méthodologies d'attaque des pirates. De nouvelles failles apparaissent en permanence. Un responsable sécurité doit donc tenir ses connaissances constamment à jour. Un IDS n'est pas un outil que l'on déploie et que l'on oublie. En plus d'exiger de très bonnes connaissances techniques, l'analyse des alertes et la mise à jour des règles demandent de l'organisation et de la patience »,* estime Patrick Chevalier. Sans compter que pour réagir correctement en cas d'alerte, *« il faut maîtriser le système d'information dans son ensemble pour pouvoir évaluer la gravité d'un événement »,* ajoute Guillaume Arcas.

Le Conseil de l'Europe a résolu ce problème de compétences en sous-traitant le projet au début et en bénéficiant d'un transfert de compétences tout au long de sa mise en œuvre. L'exploitation lui demande aujourd'hui environ une journée par mois. *« Nous avons décidé d'ignorer les scans de port mais nous gardons une trace pour analyse ultérieure »,* précise Samuel Chaboisseau, administrateur système et réseau du Conseil de l'Europe, avant d'ajouter que *« l'analyse des remontées prend 5 % du temps de chaque administrateur de serveur »*.
Du côté des investissements financiers, si l'on construit son IDS au-dessus de logiciels libres comme Prelude-IDS ou Snort, le coût des licences est quasi nul. *« Le principal coût d'un IDS se mesure en temps. Sa gestion peut être "chronophage" et démoralisante : 75 % des alertes remontées par les règles standards de Snort sont des faux positifs ou sont inexploitables »,* met en garde Guillaume Arcas.

LES ÉCUEILS

Avant tout des problèmes humains

Les fausses alertes restent le problème technique numéro un des sondes. Mais, bien plus que la technologie, la mise en œuvre achoppe généralement sur des problèmes humains. L'installation d'un IDS est en effet rarement vue comme une priorité : bien souvent, on considère que les coupe-feu suffisent et les sondes sont souvent assimilées à des instruments de « flicage interne ». D'autre part, *« l'administration d'un IDS peut être délicate. Ou bien on noie la hiérarchie et les équipes d'exploitation sous les alertes, et on tombe alors dans le syndrome de* "Pierre qui criait au loup", *ou bien on ne remonte rien ou trop peu et l'IDS est perçu comme inutile. Sans parler de la tentation – parfois forte – de pratiquer la politique de l'autruche : pas d'IDS, pas d'alerte. Pas d'alerte : tout va bien ! »,* constate Guillaume Arcas.

RETOUR D'EXPÉRIENCE

Déploiement : privilégier les sondes passives

« Nous sommes plus réactifs aux attaques »

La SGIB a déployé soixante sondes Snort dans le monde pour compléter un dispositif de sécurité déjà bien musclé. *« Nous avons profité d'une refonte du système d'information pour compléter les coupe-feu déjà en place »,* précise Christophe Maratray. Snort a été retenu pour son adaptabilité et sa modularité, son prix et l'existence de compétences internes sur le logiciel. Utilisée en mode purement passif, la sonde a facilement été déployée sans impact majeur sur la production. Malgré une charge d'exploitation quotidienne élevée (mise à jour des signatures), le bilan est positif. La SGIB a en effet largement gagné en réactivité. *« Nous isolons et réagissons plus rapidement aux incidents tels que le ver Slammer il y a quelques semaines »,* précise Christophe Maratray.
Dès que la sonde détecte un événement suspect, celui-ci remonte au serveur de centralisation, puis au logiciel de corrélation qui génère une alerte sur la console. Le personnel de l'équipe d'exploitation enquête aussitôt sur les raisons de l'alerte. *« Nous détectons des attaques qui auparavant étaient difficiles à identifier sans corrélation avec d'autres outils – log coupe-feu et systèmes »,* explique-t-il. Au-delà d'une vision plus fine des événements réseau, les sondes mettent aussi en lumière les mauvaises configurations appliquées à des équipements de sécurité tierces.


Jim Wallace

Christophe Maratray, responsable de la sécurité du système d'information.

Société Générale Investment Banking (SGIB)
- **Siège social :** Paris (75).
- **Effectif :** 80 000 (pour le groupe Société Générale).
- **CA 2002 :** non communiqué.

Le Conseil de l'Europe a réussi à prouver l'intérêt de l'IDS par un heureux concours de circonstances. *« Nous avons mis Snort en production le jour où un audit intrusif indépendant était pratiqué à notre insu par notre direction. Snort a tout de suite détecté les tentatives d'intrusion et nous avons réussi à gérer cette attaque en moins de dix minutes. Les prestataires avaient commencé le matin sur d'autres serveurs non sondés et personne n'avait rien vu. Cet incident a été très convaincant en interne »*, se rappelle Samuel Chaboisseau.

LES GAINS

Une gestion proactive de la sécurité

Malgré ces difficultés de mise en œuvre, les sondes restent la seule approche industrielle pour découvrir les intrusions et les contrer avec des réponses automatiques et manuelles. *« C'est une gestion proactive de la sécurité »*, résume Alain Rossi. Au-delà de leur rôle de défense, elles apportent une meilleure compréhension du réseau et mettent plus facilement en évidence les maillons faibles. Le Conseil de l'Europe s'est, par exemple, aperçu qu'il subissait une dizaine d'attaques par mois dont une majorité venait du web et visait les CGI installés par défaut avec IIS, le serveur HTTP de Microsoft. *« Nous traquons donc toutes les installations IIS par défaut et surveillons particulièrement Bind, Apache et les serveurs de messageries »*, ajoute-t-il.
C'est aussi un excellent moyen d'autoformation et de paramétrage des coupe-feu. *« Nous avons récemment exploité Snort pour analyser le comportement de certains protocoles lors d'une opération de renforcement du filtrage afin d'éviter des ruptures de service. On apprend beaucoup en essayant de savoir pourquoi une règle s'est déclenchée. Une sonde est un compagnon idéal pour le réglage des filtres du coupe-feu »*, illustre Jean-Michel Barbet. ■

AVIS D'INTÉGRATEUR

Guillaume Rincé, responsable du pôle sécurité d'Easynet.

« La sonde fonctionne comme un antivirus »

Comment fonctionne une sonde ?
Une sonde fonctionne comme un antivirus. Elle analyse le trafic réseau interne et externe en fonction d'une base de signatures, corrèle les événements suspects et déclenche une alerte s'il y a lieu. Elle prend la forme d'un logiciel ou d'un service hébergé chez des prestataires. Dans ce cas, il faut absolument tester les procédures d'escalade pour s'assurer que le prestataire réagira correctement en cas d'attaque.

Quels sont les trois points-clés à examiner ?
Le premier est la performance, c'est-à-dire la capacité de la sonde à traiter tout le trafic sans pénaliser les temps de réponse. Le second est le niveau de résistance de la sonde aux techniques d'évasion. Cela limite les fausses alertes. Enfin, une sonde doit être stable car elle concentre tout le trafic. J'ajouterai la facilité d'administration qui passe par une corrélation correcte des événements et une remontée ergonomique des alertes.

Easynet
- **Références sécurité :** K-Mobile, Bouygues Telecom, ViaMichelin.
- **Siège social :** Paris (75).
- **Effectif :** 1 000 personnes.
- **Chiffre d'affaires 2002 :** 131,8 millions d'euros.

Une offre très riche

Editeur	Logiciel	Caractéristiques	Prix ht*
Cisco www.cisco.com	IDS 4210 Appliance	Boîtier. Trafic 45 Mbit/s (100 Mbit/s pour le 4230 Appliance). Cisco propose aussi une extension au switch Catalyst 6000 sous la forme d'une carte (250 Mbit/s).	8 000 €
Computer Associates www.ca.com	eTrust Intrusion Detection	Sonde logicielle. Réunit dans un même logiciel les fonctions de détection d'intrusions, de filtrage des URL, d'analyse antivirale, de déclenchement d'alertes, la journalisation d'événements et les réponses en temps réel.	2 625 €
Easynet www.easynet.fr	easynet Secure IDS	Service en FAH. Administration et supervision 24 h/24 . Reporting périodique des événements sécurité. Mise en œuvre de procédures de gestion d'incidents de sécurité. Technologie SecureNet Pro d'Intrusion.com.	15 000 €
Enterasys www.enterasys.com	Dragon Sensor	Sondes HIDS et NIDS matérielles ou logicielles. Débits jusqu'à 1 Gbit/s. Analyse de protocoles et de signatures. Compatible Snort 1 et 2. Interfaçage avec les coupe-feu Cisco, Check Point ou ipfilter.	9 450 € (IDS + Management)
Exaprobe www.exaprobe.com	Exaprotect	Sonde logicielle ou en FAH. Fondée sur des composants open source (Prelude, Snort, Nessus, etc.). La technologie iCare développée par Exaprobe assure le traitement des alertes générées par toutes les sondes.	9 500 € ou 200 €/mois en FAH
Intrusion www.intrusion.com	SecureNet Pro	Boîtier. Trafic 10/100/1 000 Mbit/s. Reconstitution des sessions en temps réel. Les connexions TCP peuvent être rejouées pour analyse ultérieure. Interruption des sessions suspectes. 1 600 signatures. 35 protocoles.	De 2 695 à 39 995 €
ISS www.iss.net	RealSecure Network Sensor	Sonde logicielle. Trafic 10 Mbit/s à 1 Gbit/s. 1 350 signatures d'attaques (gestion signatures Snort), 97 protocoles décodés, driver de capture haute performance. TCP Reset et reconfiguration de coupe-feu.	De 12 400 € (10/100 Mbit/s) à 35 700 € (1 Gbit/s)
NFR www.nfr.com	NID-310	NIDS logiciel ou boîtier. De 10 Mbit/s à 1 Gbit/s. Base de signatures et de règles. Console d'administration centralisée.	12 000 €
Open source www.prelude-ids.org	Prelude-IDS	IDS logiciel hybride. Analyse flux réseaux et des fichiers de log. Centralisation des événements par le biais d'un Manager.	Gratuit
Open source www.snort.org	Snort 2.0	Sonde logicielle. Détection dans IP, TCP, UDP et ICMP. Préprocesseur HTTP, détection de Nmap (OS fingerprint), de petits fragments, de déni de service et de débordement de buffer. Signatures régulièrement mises à jour.	Gratuit
SourceFire www.sourcefire.com	Network Sensor	Sonde logicielle. Trafic 22 Mbit/s (NS1000) à 1 Gbit/s (NS3000). Basée sur une version améliorée de Snort (par l'auteur même de Snort qui travaille chez SourceFire). Les événements et alertes sont centralisés par Intrusion Management Console, un boîtier en rack 2U.	De 5 995 € à 16 995 € (avec console)
Symantec www.symantec.com	Symantec ManHunt	Sonde réseau logicielle. Trafic 10/10/1 000 Mbit/s. Détection et blocage des attaques. Détection des anomalies de protocole, des attaques par trames fragmentées (réassemblage des paquets), des attaques dans les protocoles de routage (BGP V4/SRP), signatures Symantec et gestion native des signatures Snort.	12 000 €

*Prix à partir de : par poste/sonde