SUPERVISION

Introduction

Une fois qu'un réseau est mis en place, on peut se contenter de le laisser vivre et n'intervenir qu'au moment où survient un problème : saturation, baisse de performances, problèmes de connexion…

Mais si un administrateur est en responsabilité, l'une de ses attributions sera d'agir en amont de ces **défaillances** en mettant en place un système **d'audit régulier** ou permanent portant sur les serveurs, routeurs, commutateurs et tout système centralisé.

Les trois étapes

Lorsqu'une **défaillance** intervient dans la **disponibilité du réseau**, la première étape consiste à chercher la **source de la saturation**. Pour cela, on procèdera à des analyses en direct des trafics circulant, et l'on cherchera les anomalies possibles :

- service/activité anormale,
- machine monopolisatrice,
- etc.

De là, on pourra intervenir sur le (ou les) matériel(s) ou services incriminés (isolation, arrêt de service, mise en place de restrictions, etc). On réalise cette activité avec les **analyseurs de trames** et **scanneurs de ports**.

Pour éviter la survenue de tels défauts de fonctionnement, on devra mettre en place des outils de **supervision** qui donneront **en permanence** une vision sur l'activité du réseau, des serveurs et matériels d'interconnexion, de manière à anticiper le moment de la saturation par la détection immédiate des défaillances. Cette deuxième étape repose sur les outils de supervision décrits dans le chapitre II.

Enfin, pour ne pas laisser l'entrée possible de trafic, et ce malgré la présence éventuelle d'un **filtre pare-feu** (**firewall**) qui définit ce qui est autorisé à passer, on pourra décider la mise en place d'outils chargés de **détecter** dès le départ les **tentatives d'intrusion** ou de mise en panne de matériels, voire de les éviter : il s'agit de la détection et la prévention d'intrusion.

Aspect juridique

Sans entrer dans le détail précis des lois s'appliquant à l'étude du trafic réseau, deux précautions indispensables sont à prendre par l'administrateur :

- les utilisateurs doivent avoir connaissance de la possibilité d'étude du contenu de leurs échanges
- l'administrateur (ou les techniciens) ne peut étudier le contenu informatif (texte des messages notamment) ou exploiter les sites visités pour confondre l'utilisateur (seule une requête de la justice leur autorise à en divulguer le contenu). Il doit cependant mettre en place les outils permettant l'enregistrement de l'activité sur le réseau.

Par ailleurs, en tant que responsable de la sécurité, l'administrateur se doit légalement de mettre en œuvre toutes les techniques susceptibles de garantir l'inviolabilité des données à caractère personnel

présentes dans son système d'information.

La supervision et les outils de détection d'intrusion peuvent contribuer à cette garantie.

I Analyse instantanée

Dans une démarche de résolution de problème, de recherche de trafic illicite, d'étude de fonctionnement ou d'anticipation d'évolution, un administrateur peut avoir recours aux outils d'analyse du trafic ou de l'activité des équipements. Ceux-ci lui amèneront des statistiques/synthèses ou des informations très détaillées.

1.1 Les analyseurs de trame : étude du trafic

Les analyseurs sont des outils permettant de capturer les trames circulant dans un domaine de collision (donc limités à un réseau local). Ils offrent une analyse active du comportement d'un réseau et demandent à l'administrateur d'être présent devant sa machine pour visualiser des graphiques, des statistiques, etc.

Ils peuvent produire des analyses par protocole (TCP/ICMP/ARP/IP/Services de la couche 7), par adresse (IP, Netbios, MAC), par réseau (IP, Ethernet, Token Ring, IPX)…

Ils vont jusqu'à afficher le contenu des trames en clair, y compris les mots de passe des connexions aux sites de courrier ou aux matériels qui ne sont ni cryptés ni hachés.

On trouve quelques outils gratuits, dont le *Moniteur Réseau de Windows* (sur version Server) ou les produits libres *Ethereal/Wireshark/Packetyser*. Les produits commerciaux portent aussi le nom de *sniffer*. Des sondes matérielles (du fabricant *Fluke* notamment) permettent de capturer le trafic en se branchant sur un équipement ou en entourant simplement un câble réseau (ils servent notamment pour certifier les installations des cablo-opérateurs).

Ces outils sont limités à un réseau physique (ils ne peuvent recevoir que les trames broadcast passant sur le réseau de niveau 2 où se trouve l'équipement faisant tourner l'analyseur et tout ce qui passe au niveau 1).

Souvent gourmands en ressource (processeur, mémoire, éventuellement disque), ils doivent être placés sur une machine dédiée (surtout pas sur les serveurs !).

En mode *promiscuous*, ils sont capables de récupérer des trames qui ne leur sont pas destinées.

Certains matériels d'interconnexion de niveau 2 ou 3 permettent de positionner un port en mode miroir ou en écoute générale. L'analyseur connecté sur ce port capture l'ensemble du trafic d'un autre port ou tout trafic passant par le switch.

On pourra ajouter à ces outils les fichiers de journalisation (logs) de l'ensemble des systèmes (interconnexion, serveurs, proxies, etc) qui donnent des informations utiles sur l'usage du réseau.

Que faire avec un analyseur ?

L'utilisation de ces outils est à inscrire dans une démarche d'audit et de détection de problèmes.

Grâce aux fonctions statistiques, ils peuvent permettre d'inventorier :

- Les types de trafics par protocole ayant cours sur le réseau : on pourra alors visualiser l'utilisation faite, comme le transfert de fichiers, la messagerie, le Web, et réguler l'usage de tel ou tel protocole, ou revoir les règles de filtrage d'un pare-feu… On pourra aussi détecter l'usage d'UDP, protocole moins sécurisé que TCP
- Le taux d'utilisation de la bande passante, permettant d'identifier des faiblesses sur le réseau ou, au contraire, un potentiel d'évolution avant la mise en place d'une nouvelle fonctionnalité.
- Les volumes de données échangées et leur type : on pourra ainsi repérer les taux d'erreur sur le réseau, les utilisations de broadcast toujours pénalisants, les taux de perte…
- Le trafic généré par machine de manière à identifier le bon ou mauvais fonctionnement de celles-ci, la sur-utilisation du réseau par certains équipements (soit volontaire par téléchargement de fichiers lourds, soit par une installation de services ou de logiciels réseau/virus…)

Au delà des fonctions statistiques, ces outils permettent d'effectuer des captures ponctuelles de communications qui détaillent les adresses, protocoles, contenus, utilisateurs…

Lorsque l'on a repéré un mauvais fonctionnement d'une station ou d'un équipement, il est alors intéressant de procéder à cette étude minutieuse de manière à identifier précisément les raisons du dysfonctionnement (voir copie d'écran ci-dessous).

1.2 Les scanneurs de port : étude de l'activité d'un équipement

En complément des analyseurs de trames qui se chargent des flux réseau, d'autres outils peuvent amener une information précise sur les services en exécution sur un équipement. Préambule à la sécurisation par firewall ou à la détection d'intrusion ou de portes dérobées, ces logiciels donnent une vision de l'ensemble des ports ouverts sur un serveur, un poste utilisateur ou un matériel réseau, ainsi que les connexions en cours.

Les outils libres en environnement Linux se nomment nmap, snort ou freeSwan. La commande

```
netstat -a
```

donne aussi une vision des ports en écoute (Windows/Linux)

Que faire avec un scanneur de port ?

Comme les analyseurs, ils ne peuvent être utilisés que ponctuellement dans une démarche d'inventaire occasionnelle, de recherche de faille ou dans un audit, avec des résultats détaillés et précis. Ils sont aussi utilisés par les détecteurs et protecteurs d'intrusion.

II Supervision

Seconde étape de la surveillance, la supervision consiste à mettre en place des outils permanents, en cherchant à minimiser leur impact sur le trafic (on évite l'ajout d'un trafic supplémentaire important en augmentant les intervalles d'interrogation à des seuils de tolérance supportable : on n'interroge pas un matériel en SNMP toutes les minutes mais plutôt tous les ¼ d'heure, on peut cependant

repérer la disponibilité d'un équipement par un ping très fréquent).Ils offrent une vision globale et en temps réel.

2.1 Des outils

Les solutions sont nombreuses et vont de l'approche propriétaire pour les matériels d'interconnexion (3Com, Cisco et autres Nortell disposent de technologies implémentées sur leurs produits) aux produits complexes des éditeurs (SMS de Microsoft notamment) en passant par les offres commerciales (on citera HP Openview comme référence) ou les standards normalisés à base d'agents (SNMP : Simple Network Management Protocol ou les sondes RMON). On évoquera aussi le serveur Telnet et son équivalent sécurisé SSH.

Tous ces systèmes proposent des fonctionnalités parmi les suivantes :

- État de fonctionnement,
- Lecture des configurations,
- Mise à jour de configuration,
- Définition de seuil d'alerte (pour des débits, des capacités disques, des dysfonctionnements…),
- Renvoi d'alertes vers un appareil distant (SMS, appels, clignotant..)
- Détection

Fichiers logs On pourra aussi s'appuyer sur tous les journaux et fichiers de logs mis à disposition par les systèmes d'exploitation, les logiciels serveurs ou les matériels (routeurs, proxy, firewalls, etc) pour avoir une vision synthétique ou détaillée de ce qui se passe sur les machines et le réseau.

Ces éléments très spécifiques et propriétaires ne sont pas détaillés ici.

2.2 Le protocole SNMP : supervision des équipements

Fonctionnalité des matériels permettant une vision et une administration centralisées sur une console, le protocole SNMP est un outil d'information permettant une supervision automatisée.

Norme validée par l'IETF autour de la pile TCP/IP, SNMP (Simple Network Management Protocol), permet à tout équipement d'indiquer l'état d'un certain nombre de paramètres, de recevoir une configuration ou de déclencher des alertes lorsque des niveaux sont atteints.

Le protocole SNMP consiste en :

- Une communication client serveur grâce à une console (client) et des agents (serveurs)
- Une identification en communautés pour assurer une forme minimale de sécurité et un outil d'organisation.
- Une gestion des informations dans une base hiérarchique nommée MIB

A Agent et console

Le protocole SNMP repose sur un échange client/serveur entre une console et un agent SNMP. La console peut interagir avec plusieurs agents. MRTG, Cacti, Nagios en environnement Linux/Unix ou HP Openview sont des exemples de console. Chaque équipement administrable SNMP héberge donc un

service (l'agent SNMP) capable de répondre à des demandes ou d'émettre des alertes.

Demandes

Le premier mode d'échange consiste en une interaction à l'initiative de la console. Il correspond à une interrogation ponctuelle ou immédiate. C'est la technique de polling, dont les commandes sont snmpGet, snmpSet, snmpWalk… Il sert aussi pour la mise à jour des paramètres de l'équipement. Le serveur est l'agent, qui est en écoute sur le port UDP/161.

Alertes

Le second mode est issu d'un travail interne du service agent qui repère un élément significatif (taux d'utilisation, espace restant, type d'attaque, etc). Ce niveau d'alerte lui a été précisé dans le paramétrage. L'agent signale le problème à la console par l'envoi d'une alerte. La technique est nommée trapping, qui envoie une trame snmpTrap. La console peut alors prendre en charge l'envoi d'une alerte vers tout autre système (SMS, GPS,mail, etc). C'est alors elle qui est le serveur, sur le port UDP/162.

B Communauté

Pour pouvoir accéder à un système administrable SNMP, il faut connaître le nom de la communauté (à peu près équivalent à un domaine Windows ou un SSID Wifi). En fait, deux communautés sont proposées sur les équipements :

- Droit d'accès en lecture sur les valeurs des paramètres. On ne peut modifier le contenu. Le nom par défaut est public.
- Droit d'accès en lecture et écriture : on peut modifier le paramétrage du système, par exemple les noms de communauté, les adresses IP ou des règles de sécurité.

Sans sécurisation spécifique, ces informations sont lisibles sur le réseau par un analyseur de trame. Des améliorations au protocole visent à intégrer des fonctions de cryptage.

C Les MIB

Pour pouvoir interroger ou paramétrer un équipement SNMP selon des libellés lisibles, la norme définit une base hiérarchique standard et universelle qui décrit les données accessibles. Elle joue l'équivalent du DNS pour un réseau d'ordinateur et met en correspondance un OID numérique et un nom textuel.

Chaque fabricant ou éditeur peut se rattacher à cette arborescence en créant sa propre branche, précisant les paramètres spécifiques qu'il souhaite rendre interrogeable.

Cette base est appelée MIB (Management Information Base). Elle est organisée à la manière d'une arborescence DNS ou d'une structure d'annuaire LDAP. La racine est l'équivalent du point implicite des URL. A l'inverse de DNS, la lecture se fait de la racine vers les feuilles.

L'IETF définit la hiérarchie comme suit : Les organismes de normalisation sont les points d'entrée. Rappel DOD (Department Of Defense) est l'équivalent du modèle OSI pour TCP/IP.

Pour Internet (IP, en fait), la hiérarchie se poursuit comme ci-dessous. Chaque entreprise peut déposer sa propre arborescence auprès de l'IANA (Internet Assigned Numbers Authority). Chaque

feuille ou nœud de l'arbre possède une structure standard de données nommée SMI (Structure of Management Information) comportant :

- le nom du paramètre,
- le type pour les données finales (chaîne, entier, signé, réel, compteur, adresse IP, adresse MAC…)
- son mode d'accès (lecture, écriture…).

Chaque objet possède un identifiant (OID : Object identifier) correspondant à sa place dans la hiérarchie. L'OID de tcp est donc .1.3.6.1.2.1.6.

Que faire avec SNMP ?

Il s'agit ici plutôt d'un outil de supervision sur le long terme, dont le but est une analyse régulière du fonctionnement du réseau, de son utilisation.

SNMP permet aussi la détection des dysfonctionnements au moment où ils interviennent : c'est donc un outil de surveillance autorisant une réactivité immédiate et préventive (avant une panne totale).

Il peut servir pour :

- Taux d'utilisation de la bande passante sur des durées longues (ci-contre, analyse quotidienne)
- Détection d'utilisation non autorisée sur des créneaux horaires
- Définition de seuils d'alerte pour le fonctionnement des équipements (espace disque sur un serveur, niveau d'encre pour une imprimante, taux d'erreur sur un routeur…).
- Inventaires divers : répartition de charge sur les interfaces d'un routeur, sollicitations des différents serveurs, taux d'erreur par équipement…
- Répartition des frais d'utilisation du réseau : grâce aux inventaires précédents, on peut faire des statistiques par service, par réseau…

2.3 Les sondes RMON

Une des critiques du protocole SNMP est le trafic réseau lourd qu'il peut engendrer. En effet, la console est le système centralisateur des informations et l'outil de calcul statistique ou de cumul. Si l'on veut produire des informations synthétiques, il faut donc demander toutes les données détaillées, ce qui engendre autant de trames d'interrogation et de réponse qu'il y a de paramètres et de matériels à étudier. C'est pourquoi, grâce à la capacité de traitement accrue des systèmes interrogés (processeurs présents dans les routeurs, commutateurs et serveurs en particulier), une partie du travail de synthèse est intégré dans un agent (Remote MONitor) qui utilise ensuite SNMP pour envoyer les résultats calculés. Le trafic est ainsi diminué.

III Détection et protection contre les intrusions

Avec les outils de supervision, on observe l'activité et le bon fonctionnement d'un réseau. Toutefois, cela ne suffit pas à rendre un système informatique performant et efficace : en effet, dès lorsqu'il est exposé à l'extérieur, le système peut voir ses performances se dégrader de manière spontanée en cas d'attaque. La supervision ne pourra au mieux que constater cette dégradation, sans pouvoir y remédier. Les attaques susceptibles d'atteindre l'informatique sont nombreuses. Pour rappel :

- Porte dérobée : très en vogue actuellement, le principe est d'envoyer un message de taille trop importante entraînant un débordement en mémoire qui permet un accès au système avec des privilèges importants. Blaster et ses dérivés agissent de la sorte. Ils peuvent être le début d'un déni de service ou d'espionnage.
- Déni de service : en saturant les outils de communications (routeurs, serveurs) de requêtes (on parlera par exemple des attaques sur les serveurs de messagerie comme les virus Netsky.D ou Bagle), en envoyant des messages mal formés mettant en panne un système, en détournant les échanges vers des adresses erronées, on empêche l'accès aux services rendus par l'entreprise
- Espionnage : Chevaux de Troie ou autres outils d'analyse qui visent à observer l'activité, lire les données, intercepter les informations. On parlera notamment de spyware, mais aussi de l'espionnage interne. Les keyloggers, qui capturent les frappes au clavier, sont des outils d'espionnage très pernicieux.
- Usurpation d'identité (spoofing) : qu'il s'agisse de noms d'utilisateurs ou d'adresses de machines, l'intention est de diffuser de mauvaises informations ou, à l'opposé, de se faire communiquer des informations confidentielles
- Destruction : aussi bien des données stockées que des capacités de traitement des serveurs
- Virus : plus ou moins malveillant, ils peuvent aller d'un simple message d'infection ou d'activités anormales (affichages intempestifs, modification de l'environnement, etc) jusqu'à l'immobilisation complète du système.

Ces attaques peuvent s'appuyer sur des failles du réseau telles :

- Ports ouverts sans raison
- Services actifs présentant des dangers connus
- Machines hébergeant des chevaux de Troie
- Service Peer-to-Peer en activité
- Réponse au ping activée sur les routeurs et serveurs
- SNMP
- Failles présentes sur des services non mis à jour

Voir http://solutions.journaldunet.com/dossiers/failles/sommaire.shtml

La supervision ne donnera qu'une information par matériel, sans fournir de vision de l'ensemble (une attaque sur 10 serveurs donnera 10 messages identiques et individuels, pas un message global signalant une attaque massive), pouvant noyer l'administrateur sous des alertes difficiles à analyser.

Des logiciels ou des utilitaires permettent de travailler en amont des attaques en agissant avec les mêmes principes que les pirates : scanner le réseau à la recherche des ports ouverts et des services actifs ou non sur les serveurs et machines. On étudiera en particulier l'utilitaire nmap sous Linux. Ils sont un sous-ensemble des IDS (Intrusion Detection System) qui ont pour vocation de révéler les failles et de détecter les tentatives d'intrusions en analysant des attaques classiques. L'outil gratuit snort du monde Linux est un système très complet pour cette fonction.

On trouvera un comparatif de certains produits à l'adresse réticulaire suivante : http://solutions.journaldunet.com/0312/031212_ids_ips.shtml.

Mais ces progiciels ne permettent qu'une constatation de l'attaque. C'est pourquoi quelques règles de bonne conduite permettent de limiter les dégâts en protégeant le réseau du maximum d'attaques basiques

- ne pas tout laisser passer (Firewall ou routeurs filtrants)
- détecter les failles et tenter de les colmater

- disposer d'un antivirus à jour
- appliquer les patches de sécurité des différents services et OS en activité sur le réseau

Les IDS évoluent aujourd'hui pour prendre en charge une protection live en cas d'attaque. On parle alors d'IPS ou la détection a été remplacée par la protection. Le principe est de re-paramétrer dynamiquement les filtres, droits d'accès et autres sécurité en détectant des fonctionnements suspect (communications massives vers un service, IP récurrente sur de multiples services, etc). Il existe enfin des « attrape-hackers » qui exposent des fonctions factices sensées attirer les pirates et laissant de ce fait le réseau réel invisible : on parle de pots de miel (comme pour les mouches ou les abeilles) ou Honeypot.

IV En résumé

Action	Fréquence	Outils	(D)étection/ (P)rotection
Scanner les ports	Lors d'installations, modifications	scanners de port (par exemple snort	D
Surveiller l'activité	Régulièrement	logs, SNMP/RMON, IDS	D
Filtrer	permanent	Firewall, routeurs, proxy, Antivirus	P
Réagir aux attaques	en cours d'attaque	IPS	P
Corriger le système	Suite à une attaque, après constatation d'une infraction	Arrêter les services, corriger les failles, patches de sécurité, tromper les pirates avec les honeypots, etc	P
Maintenir le système	Veille technologique, Disponibilité de patches, etc	Patches, upgrade de BIOS, affinement de la politique de sécurité, etc	P