Dans le cadre de

SECURIDAY 2010

Et sous le thème de

Computer Forensics Investigation

VOUS PRÉSENTE L'ATELIER :

Analyse des logs au niveaux des IDS et Firewall

Chef Atelier : Rimeh Ben Messaoud (RT4)

- **Nabiha Zanned** (RT5)
- **Ameni Hammami** (RT3)
- **Atef Bel Hadj Aleya** (RT4)

1.Présentation de l'atelier et de l'outil

Dans le cadre de « Computer Forensics », notre atelier se situe dans le processus de « Network Forensics ».Il s'agit de collecter les données à partir des différents dispositifs du réseau et d'appliquer les techniques d'investigation afin de retracer les activités se passant dans le réseau et cela dans le but d'identifier une attaque et de découvrir l'identité de l'attaquant durant et après l'attaque. Notre tâche principale consiste à vérifier et analyser la preuve informatique collectée afin d'aboutir à la preuve affirmant ou réfutant l'occurrence d'un crime informatique. Elle permet de déterminer si une attaque est survenue, la nature de l'attaque, l'auteur de l'attaque et les traces qu'il a laissées derrière lui.

La preuve informatique dépend du type d'attaque, elle peut se trouver dans trois emplacements principaux :

- ✓ Sur le composant victime du réseau.
- ✓ Sur la machine de l'attaquant.
- ✓ Sur les dispositifs du réseau situés entre le composant victime et la machine de l'attaquant.

Les données faisant objet de preuve informatique sont générées par le logging. C'est la sauvegarde de la trace des événements qui arrivent pendant leur exécution. L'enregistrement peut avoir lieu dans un hôte ou dans un système fournissant un service réseau tel qu'un serveur de messagerie, un serveur Web, un serveur de nom de domaine (DNS) ou un firewall. L'enregistrement prend la forme d'un fichier dit « fichier log ».

Tout au long de ce tutorial, on va traiter la phase d'analyse de logs au niveau des différents équipements réseaux : IDS, routeurs et Firewall

2. Environnement logiciel

2.1. Analyse des logs au niveau des IDS

Un IDS est essentiellement un sniffer couplé avec un moteur qui analyse le trafic selon des règles.

L'IDS peut analyser

- Couche Réseau (IP, ICMP)
- Couche Transport (TCP, UDP)
- Couche Application (HTTP, Telnet)

Selon le type de trafic, l'IDS accomplit certaines actions

- Journaliser l'événement : Source d'information et vision des menaces courantes
- Avertir un système avec un message: Exemple: appel SNMP
- Avertir un humain avec un message : Courrier électronique, SMS, interface web, etc.
- Amorcer certaines actions sur un réseau ou hôte : Exemple: mettre fin à une connexion réseau, ralentir le débit des connexions, etc. (rôle actif)

On distingue 2 types d'IDS:

- HIDS (Host IDS): Il est basé dans un ordinateur hôte. Il permet de surveiller le système (journaux systèmes), contrôler l'accès aux appels systèmes et vérifier l'intégrité des systèmes de fichiers. Il ne surveille qu'un seul hôte.
- NIDS (Network IDS) : Il s'agit d'une sonde placée dans le réseau. Il surveille l'ensemble de réseau, capture et analyse tout le trafic, recherche les paquets suspects (contenu des données, les adresses Mac ou IP..) et envoie les alertes.

Chacun répond à des besoins spécifiques

- HIDS particulièrement efficaces pour déterminer si un hôte est contaminé
- NIDS permet de surveiller l'ensemble d'un réseau contrairement au HIDS qui est restreint à un hôte

SNORT: IDS OPEN SOURCE :

Il permet de détecter d'éventuelles attaques en comparant le trafic réseau qu'il capture avec une base de données d'attaques connues. Il génère ensuite des logs qu'il est facile de mettre dans une base de donnée pour une exploitation facilitée.

BASE (Basic Analysis and Security Engine)

BASE est une interface graphique écrite en PHP utilisée pour afficher les logs générés par l'IDS Snort.

2.2. Analyse des logs des routeurs :

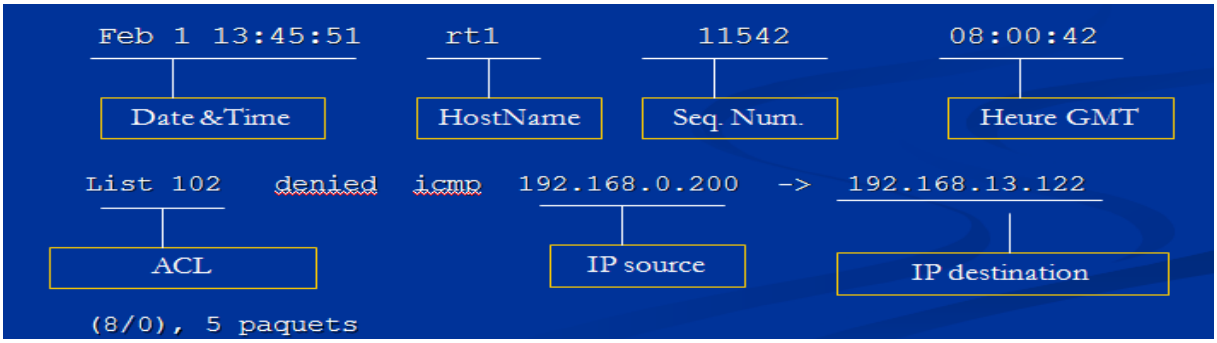
Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Il est indispensable pour transiter des paquets d'une interface réseau vers une autre, selon un ensemble de règles formant la table de routage. Quand un routeur est piraté il permet à un attaquant de :

- DoS ou désactiver le routeur et le réseau ...
- Contourner les pare-feu, les systèmes IDS, etc ...
- Surveiller et enregistrer tous les appels entrants d'un trafic ...
- Rediriger tout le trafic qu'ils désirent ...

Lorsqu'un routeur est attaqué, Les enquêteurs doivent récupérer les données en direct pour l'analyse, donc il ne faut pas l'arrêter immédiatement car ca détruit toutes ses données. C'est pour ca, suite à un incident, il ne faut pas redémarrer le routeur et on essaye de ne changer rien ni avoir un accès au routeur via le réseau.IL faut enregistrez intégralement notre console de la session et noter le temps réel et temps du routeur ainsi que les informations volatiles.

Ensuite, on essaye de récupérer les logs des routeurs qui contiennent toutes les données que les administrateurs ont besoin pour évaluer le trafic réseau et le comportement des pare-feu. En effet, on a :

- Console Logging : Ceux-ci seront capturés par l'enregistrement de votre session.
- Buffer Logging : Si la journalisation du tampon est activée, la commande de show logging nous montrera le contenu de la mémoire tampon du journal routeur, le niveau d'enregistrement effectué, et ce que les hôtes de journalisation ont envoyé.
- Terminal Logging : ca permet le non console non sessions d'afficher les messages de log.
- Syslog Logging : la journalisation des messages est envoyée à un serveur syslog lors de l'activation du Logging et la commande servername d'enregistrement est définie.
- SNMP Logging : si SNMP est en cours d'exécution, les trappes SNMP peuvent être envoyées à un serveur de Logging



-Exemple de format de log-

On trouve plusieurs outils permettant d'effectuer l'analyse des logs générés par les routeurs parmi lesquels on cite :

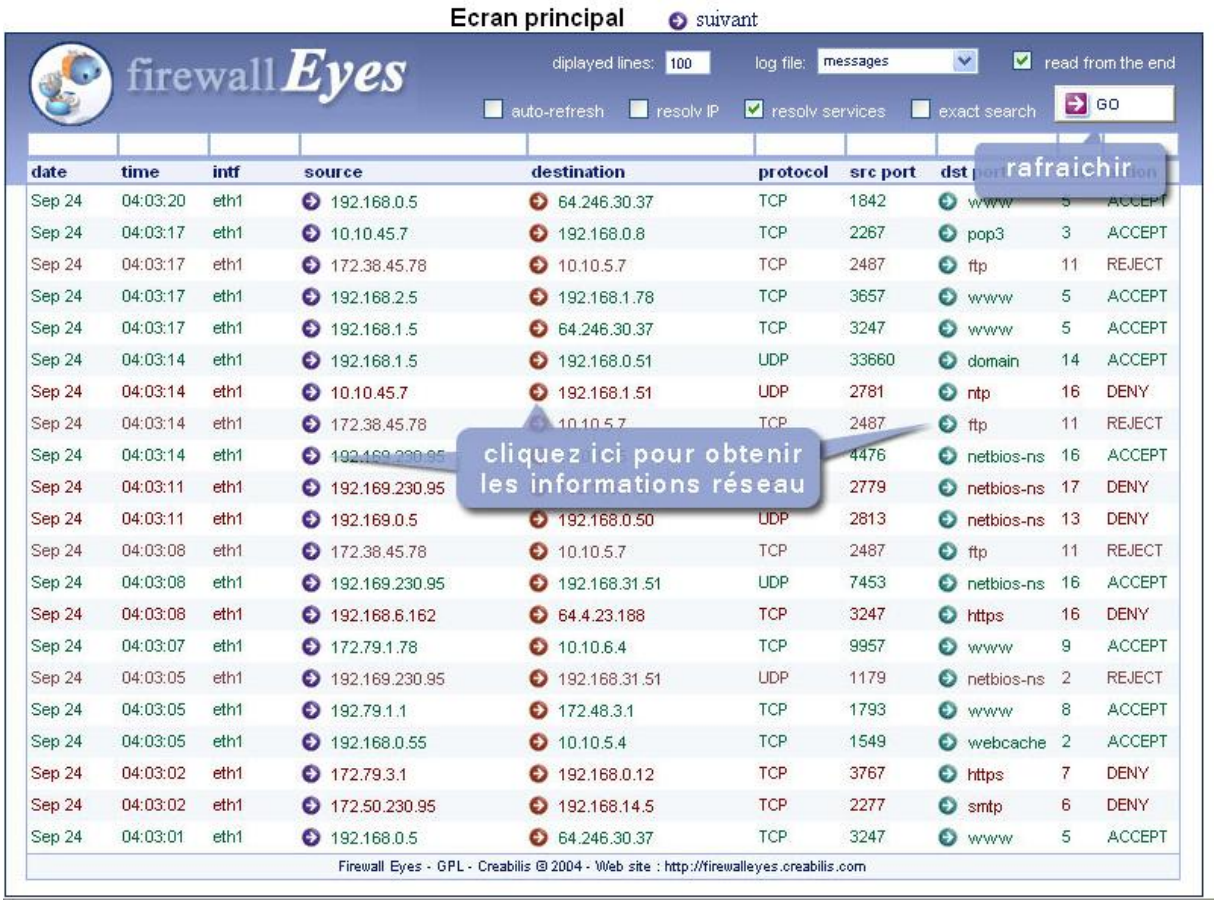
- **Anapirate** : est un script perl qui analyse les journaux émis par un ou plusieurs routeurs (Cisco pour le moment), selon un protocole défini dans le fichier de configuration. Les paquets analysés sont éliminés s'ils correspondent aux masques de paquets à ignorer. Les contacts associés aux adresses sources sont recherchés sur Internet, dans les serveurs whois et DNS, selon des modalités précisées dans le fichier de configuration et dans un fichier listant les serveurs whois par TLD (top level domain). Avec ces informations, anapirate utilise un modèle de courrier pour générer les alarmes que l'ingénieur sécurité pourra poster à chaque responsable de site d'où provient un scan.

  Un incident, au sens anapirate, rassemble tous les scans tentés par une adresse IP unique sur n'importe quelle cible : on y trouve bien entendu les machines de nos propres réseaux, mais également des machines extérieures (en cas d'attaque par rebond). Anapirate n'analyse que les paquets rejetés par les ACL cisco. Un paquet journalisé par une règle « permit... log » ne sera pas analysé.Cela signifie qu'il y aura un courrier différent par adresse IP source différente, quand bien même ces adresses appartiendraient au même fournisseur, et a fortiori à la même classe C. Parfois, un agresseur utilise plusieurs adresses d'une même classe pour la même attaque, soit qu'il ait dû se reconnecter sur un système d'allocation dynamique d'adresse, soit qu'il falsifie son adresse source depuis un fournisseur appliquant des filtres anti-spoofing en sortie. Mais il est plus facile de fusionner deux courriers correspondant manifestement au même agresseur que de séparer un courrier mixte regroupant deux scans différents. Anapirate n'est pas assez évolué pour exercer un jugement de type « ce paquet est-il associé à une attaque enregistrée sous une autre IP source ? »
  Lorsque anapirate a terminé de collecter les renseignements pour chaque adresse cible suspecte, les courriers sont générés et expédiés à l'administrateur.
  Anapirate recherche d'abord dans les DNS si la machine est connue et prépare un premier lot de contacts basés sur le nom de domaine si c'est le cas. Puis anapirate interroge les serveurs whois et tente de récupérer une adresse utilisable.

2.3. Analyse des logs des FW :

Le FW est le moyen d'application de la politique de sécurité à l'accès Internet. L'analyse de son log permet de détecter d'éventuelles failles/intrusions ou d'établir des statistiques. Il existe des outils d'analyse parmi lesquels on trouve :

- **Firewall Eyes** : est un outil d'analyse de logs en temps réel pour le pare-feu iptables. Grâce à une interface Web, on visualise et supervise simplement et efficacement l'activité réseau traversant notre firewall. On détecte aisément les activités suspectes et on ajuste notre politique de sécurité.
  Firewall Eyes est un logiciel open source sous licence GPL, on peut le télécharger, le distribuer et l'utiliser sans contrainte, il est entièrement gratuit. Ecrit en PHP, il fonctionne sous tout environnement Linux ou Windows. La combinaison d'iptables avec les interfaces graphiques firewall Eyes et firewall Builder constitue une réelle alternative open source aux firewalls propriétaires, élevant le pare-feu libre à la portée de tous.



date	time	intf	source	destination	protocol	src port	dst port		
Sep 24	04:03:20	eth1	192.168.0.5	64.246.30.37	TCP	1842	www	5	ACCEPT
Sep 24	04:03:17	eth1	10.10.45.7	192.168.0.8	TCP	2267	pop3	3	ACCEPT
Sep 24	04:03:17	eth1	172.38.45.78	10.10.5.7	TCP	2487	ftp	11	REJECT
Sep 24	04:03:17	eth1	192.168.2.5	192.168.1.78	TCP	3657	www	5	ACCEPT
Sep 24	04:03:17	eth1	192.168.1.5	64.246.30.37	TCP	3247	www	5	ACCEPT
Sep 24	04:03:14	eth1	192.168.1.5	192.168.0.51	UDP	33660	domain	14	ACCEPT
Sep 24	04:03:14	eth1	10.10.45.7	192.168.1.51	UDP	2781	ntp	16	DENY
Sep 24	04:03:14	eth1	172.38.45.78	10.10.5.7	TCP	2487	ftp	11	REJECT
Sep 24	04:03:14	eth1	192.169.230.95			4476	netbios-ns	16	ACCEPT
Sep 24	04:03:11	eth1	192.169.230.95			2779	netbios-ns	17	DENY
Sep 24	04:03:11	eth1	192.169.0.5	192.168.0.50	UDP	2813	netbios-ns	13	DENY
Sep 24	04:03:08	eth1	172.38.45.78	10.10.5.7	TCP	2487	ftp	11	REJECT
Sep 24	04:03:08	eth1	192.169.230.95	192.168.31.51	UDP	7453	netbios-ns	16	ACCEPT
Sep 24	04:03:08	eth1	192.168.6.162	64.4.23.188	TCP	3247	https	16	DENY
Sep 24	04:03:07	eth1	172.79.1.78	10.10.6.4	TCP	9957	www	9	ACCEPT
Sep 24	04:03:05	eth1	192.169.230.95	192.168.31.51	UDP	1179	netbios-ns	2	REJECT
Sep 24	04:03:05	eth1	192.79.1.1	172.48.3.1	TCP	1793	www	8	ACCEPT
Sep 24	04:03:05	eth1	192.168.0.55	10.10.5.4	TCP	1549	webcache	2	ACCEPT
Sep 24	04:03:02	eth1	172.79.3.1	192.168.0.12	TCP	3767	https	7	DENY
Sep 24	04:03:02	eth1	172.50.230.95	192.168.14.5	TCP	2277	smtp	6	DENY
Sep 24	04:03:01	eth1	192.168.0.5	64.246.30.37	TCP	3247	www	5	ACCEPT

Ses fonctionnalités :

- Analyse les logs iptables (netfilter linux 2.4 ou plus).
- Affichage intuitif : couleurs, icônes, résolutions.
- Recherche élaborée permettant de suivre une adresse IP, un protocole.
- Résolution DNS et services tcp/udp.
- Fourni des informations réseau sur les adresses IP et les services (DNS lookup, ping, traceroute, whois, nmap, …).
- Gère plusieurs fichiers de logs et plusieurs firewalls.
- Ecrit en PHP.
- Interface HTML testée avec Internet Explorer 6 et Firefox 0.8 en résolution minimum de 800x600.

2.4. Corrélation et analyse des logs avec OSSIM

La multiplication et la diversité des solutions de sécurité et d'administration ont conduit à l'apparition d'un nouveau problème : la gestion des logs.

OSSIM est une solution Open Source (http://www.ossim.net) offrant une infrastructure pour le monitoring temps réel de la sécurité réseau (détection d'intrusions et analyses statistiques). Ses objectifs sont :

- Fournir une plateforme centralisée
- Fournir une console d'organisation
- Améliorer la détection et l'affichage des alarmes de sécurité

3. Installation et configuration

3.1. Installation et configuration de SNORT

On a besoin d'installer les outils suivants:

- APACHE2 - serveur web : Version installée: 2.2.11
- MySQL - base de données : Version installée: 5.0.22
- PHP5 - langage de script orienté serveur : Version installée: 5.1.2
- PHP5-MySQL : Version installée: 5.1.2
- BUILD-ESSENTIAL : contenant des outils pour compiler et installer des programmes. Version installée: 11.1

A partir du fichier */etc/snort/snort.conf* on peut :

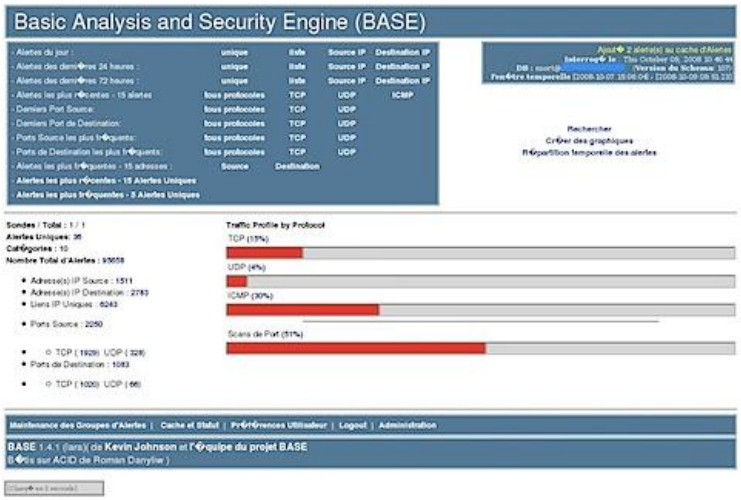
- Configurer des variables pour le réseau
    - Configurer des réseaux à écouter
    - Configurer des services à logger (http/dns/…)
- Configurer des pré-processeurs
- Configurer des plugins de sortie
- Choisir des règles à utiliser

3.2. Installation et configuration de Base

A partir du site www.sourceforge.net on peut télécharger la dernière version de Base.

Nous avons besoin d'ADOdb (Active Data Objects Data Base) pour BASE. ADOdb est en fait une librairie d'abstraction de base de données pour PHP. Des informations sur ADOdb peuvent être trouvées ici: http://adodb.sourceforge.net/

http://<adresse-ip-serveur>/base/



4. Un petit scénario de test

OSSIM récupère les logs via des agents installés sur les machines hébergeant les sondes. Les événements qui viennent d'être agrégés vont maintenant pouvoir être traités par le moteur de corrélation d'OSSIM et il fait l'analyse afin de découvrir l'origine de l'intrusion.

5. Conclusion

Au cours de notre atelier, nous avons réussi à examiner les différents formats des fichiers log générés par les équipements réseaux ainsi qu'à offrir la possibilité d'analyser ces logs afin de rendre possible l'identification d'une intrusion qui s'est produite et ceci par le biais d'une interface graphique conviviale.