Jean-Thierry EMOH ZOGO
Arnaud GALONNIER
Walter GIN
Libasse HANNE
Jean Pierre HOANG
Osnelle HOUANSOU
Thomas ISSOLAH
Frédéric JAMOIS
Sami KACHA
Aleksandar KALEV
Pooya KHADEMI
Sylvain LACOUE
Olivier LANNRETONNE
Julien LEBRETON
Dimitri LEGALLAIS
Leymarie LEYMARIE
Jérémy MACHETO
Nicolas MADELAINE

Groupe ANALYSE

M2 STRI

Sécurité Réseau

Rapport d'audit

Decembre 2008

SOMMAIRE

Introduction

Cette année et comme les années précédentes, les cours de sécurité des réseaux de M2 se déroulent selon trois approches métiers qui sont : la défense, l'analyse et l'attaque.

Le scénario est simple. Nous avons fait 3 groupes de même effectif.

- **Le groupe défense** : Il doit mettre en place une infrastructure réseau similaire à une entreprise. Il doit se protéger des attaques du groupe attaque.
- **Le groupe d'attaque** : Il doit déployer des attaques de tout genre pour perturber le réseau de l'entreprise, voire même de le faire tomber.
- **Le groupe d'analyse** : Il travaille en étroite collaboration avec la défense pour superviser leur réseau, collecter des informations, les analyser et détecter les attaques qui arrivent sur le réseau.

I- L'équipe analyse et gestion du projet

1. Nos objectifs

Voici les objectifs que nous avons fixés en début de projet :

- Travailler en équipe avec une bonne coordination
- Communiquer avec les différents groupes (Défense et Attaque)
- Découvrir le métier d'audit de réseau informatique
- Savoir prédire les failles du système de sécurité mis en place par la défense
- Superviser le réseau et conseiller le groupe Défense
- Dégager les responsabilités, les objectifs et les moyens mis en œuvre en les explicitant dans un contrat avec la Défense
- Analyser les logs pour informer la Défense de l'état de son réseau
- Faire preuve de réactivité en cas de déni de service sur le réseau

2. Présentation du groupe et diagramme organisationnel

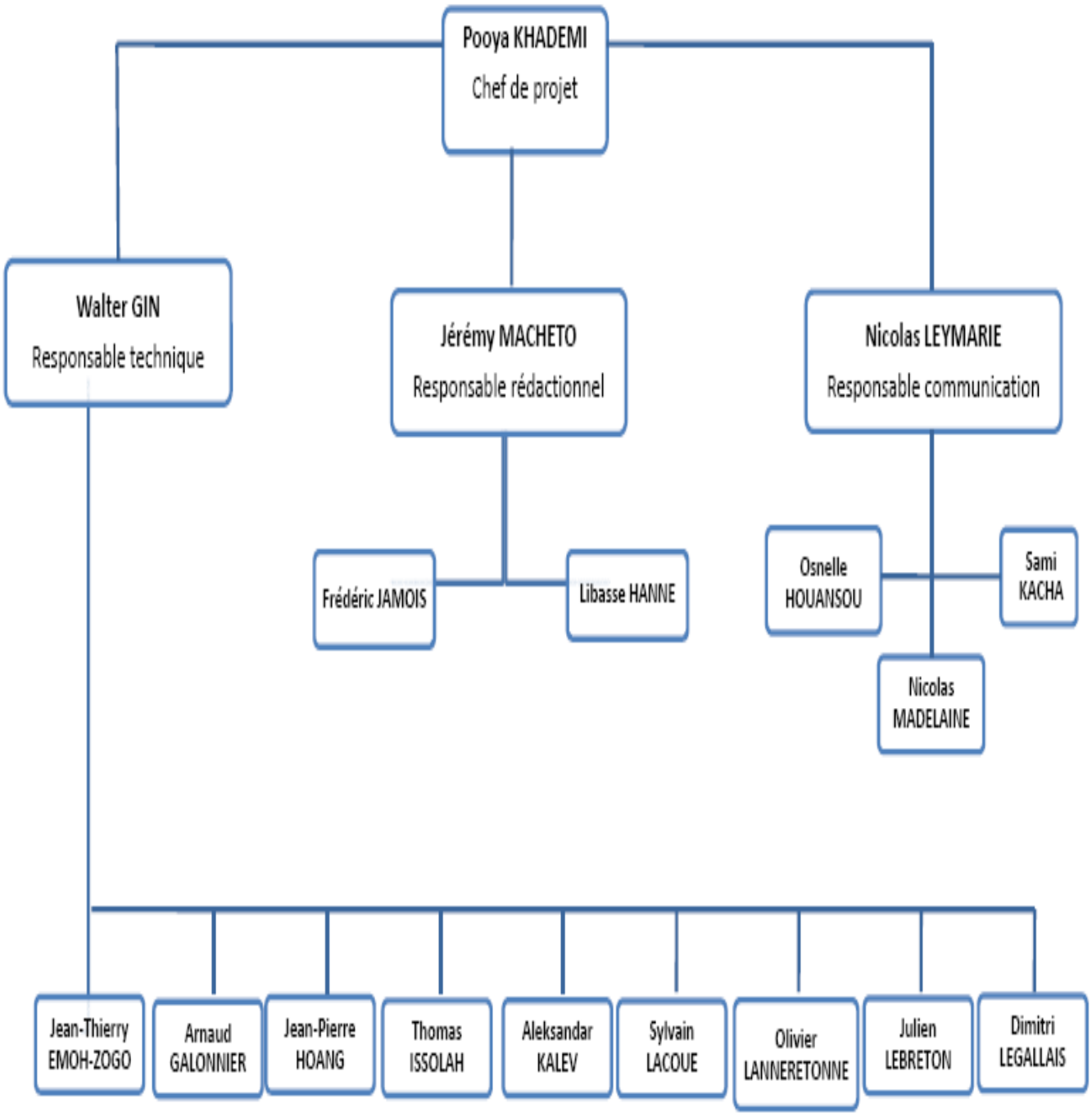
Cette année, l'effectif des groupes est particulièrement important. Nous sommes 18 dans le groupe analyse. Notre challenge commence déjà par la réussite de ce projet malgré ce nombre.
Dès notre première réunion, nous avons ressenti le besoin inévitable de se diviser en sous groupe pour gérer au mieux les activités de chacun. Nous avons également élu un responsable par groupe qui sera chargé de remonter les informations lors de nos réunions.

Voici nos 3 sous groupes :

- **Groupe communication** : chargé de la communication internet et externe (avec la Défense)
- **Groupe technique** : chargé de déployer des outils de capture de flux et analyser les logs

- **Groupe rédactionnel** : chargé de rédiger les comptes rendus de toutes les réunions, collecter les informations du groupe technique pour rédiger des rapports régulièrement. Chargé de rédiger le rapport final.

Diagramme organisationnel :



3. Outil de communication et confidentialité

i. Le wiki

La communication est un élément primordial dans ce projet vu notre effectif.
Au départ, nous échangions nos documents et compte rendus par e-mails. C'est vite devenu ingérable et ce n'était pas une solution sécurisée.
Afin de faciliter l'écriture collaborative de nos documents, nous avons mis en place un wiki sécurisé avec chacun un accès par login et mot de passe en HTTPS. Tous les documents à échanger dans le groupe étaient envoyés sur une mail-list au départ. Suite à des problèmes de sécurité et de confidentialité des boites mails et pour ne pas surcharger les boites, nous avons mis en place ce wiki.

Table des matières du wiki :

- Confrontation2
- Tools
  - Detect & analyse tools
  - Logging tools & solutions
  - Sauvegarde et restauration
  - Divers
  - Outils Maisons
- Audit Actif
- Links
- Machines
- Documents
- Rapport de projet
- Books
- Misc

Exemple des documents mis en ligne :

Documents

- CR seance 6 - cr_seance6.pdf
- CR seance 5 - compte_rendu_seance5_20081030.rar
- CR seance 3 - cr_seance3.pdf
- CR Premiere confrontation - cr_confrontation1.pdf
- CR seance 1 - cr_seance1.pdf
- CR seance 2 - cr_seance2.pdf
- CR negociation - cr_negociation.pdf
- CR analyse - cr_analyse.doc
- CR reunion technique - cr_reunion_technique_02_10_08.pdf
- Fiche technique Netflow :pole Netflow - netflow_definition.pdf
- CR technique 1 :pole Netflow - compte_rendu_netflow_20081010.rar
- CR technique 2 :pole Netflow - compte_rendu_netflow_20081013.rar
- CR technique 3 :pole Netflow - compte_rendu_netflow_20081020.rar
- Politique de Sécurité du groupe Analyse - politique_de_securite_analyse_v1_20081020.rar
- Presentation analyse traces TEAM WIRESHARK - rapport_analyse_wireshark_suite_1ere_confrontation.rar
- CR technique 4 :pole Netflow - compte_rendu_netflow_20081029.rar
- Rapport confrontation 2 :pole Netflow - rapport_conf2_netflow_20081107.rar

=> Comme nous le voyons sur cette copie écran, certains documents sont postés en dossier compressé. Ces dossiers sont cryptés selon une politique de sécurité défini à l'avance par le groupe analyse. En effet, ils contiennent des données sensibles. Malgré l'accès par authentification au wiki, si un attaquant parvenait à pénétrer dans le système, il ne pourrait pas ouvrir ces dossiers compressés et cryptés.

ii. Les rapports

Comme nous l'avons vu précédemment, notre groupe analyse a été décomposé en 3 sous groupes :

- Le groupe technique, lui-même divisé en plusieurs sous groupe.
- Le groupe communication
- Le groupe rédactionnel

La naissance du groupe rédactionnel vient d'un constat évident : il fallait trouver un moyen de centraliser toutes les informations des différents sous groupe, les synthétiser et les diffuser à tous les groupes pour donner à chacun un aperçu global de l'avancement du projet.
Le groupe rédactionnel a donc rédigé un rapport à l'issue de chaque réunion et confrontations. Des rapports plus techniques ont aussi étés rédigés par les équipes techniques pour donner plus de détails sur l'avancement de leur activité.
Afin de garder une uniformité dans les rapports, l'équipe rédactionnelle a élaboré une trame qui a ensuite été utilisées pour tous les comptes rendu.

Trame d'un compte rendu :

Séance 1

COMPTE RENDU

Lundi 20 octobre	10h15 – 10h45	Salle U2
Objectif		
Animateur		
Rédacteurs		
Absent		

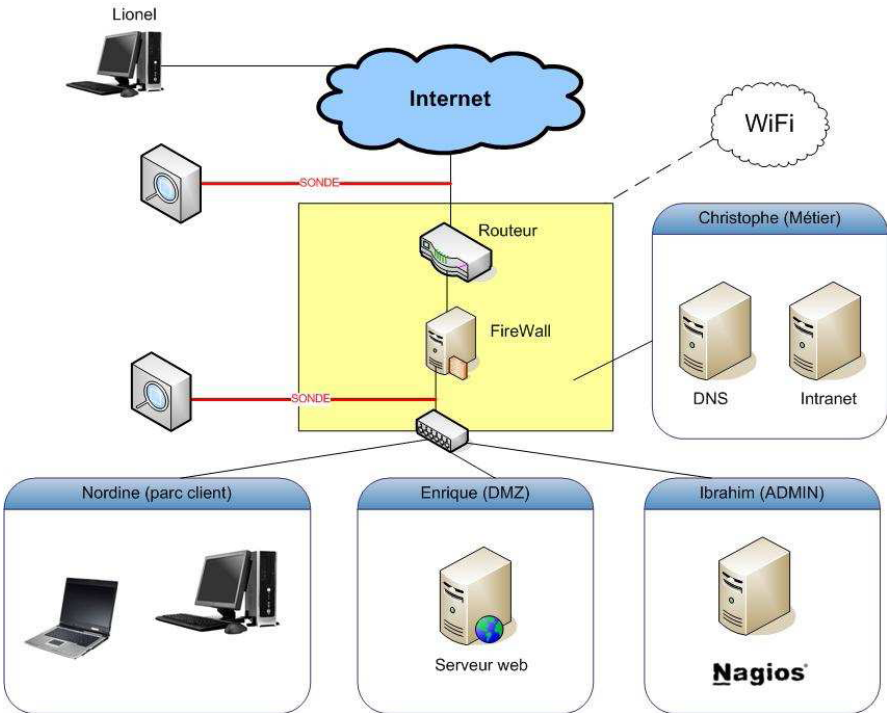
DISCUSSIONS	COMPTE RENDU
CONCLUSIONS	
POINTS D'ACTIONS	

Date de la prochaine réunion	
Objectifs de la prochaine réunion	

II- La défense

1. Architecture de la défense

L'architecture du réseau présentée par le groupe de la *Défense* nous a permis de comprendre l'organisationnel de ce dernier mais surtout d'identifier les failles d'analyse possibles :



2. Contrat

Cf. Annexe1- Contrat d'audit

Le contrat entre les deux groupes d'*Analyse* et de *Défense* a pu être signé juste à temps avant la première confrontation du lundi 13 octobre 2008. L'accord entre les deux équipes a permis ainsi de répondre suivant un certain nombre de clauses aux différents objectifs convenus :

- Délimiter un certain périmètre de confidentialité et d'action de l'audit
- Définir le cadre de communication entre les deux groupes

Assurer le bon fonctionnement de la mission d'audit de sécurité

3. Cahier des charges

Le cahier des charges transmis par l'équipe *Défense* par l'intermédiaire du sous-groupe de communication doit répondre aux différents critères suivants :

- Connaître l'organisationnel de l'équipe *Défense* définissant les responsables afin de mieux communiquer

- Comprendre l'architecture du réseau avant la première confrontation

Identifier le besoin de la *Défense* suivant les différentes évolutions de l'architecture réseau

III- Les outils utilisés

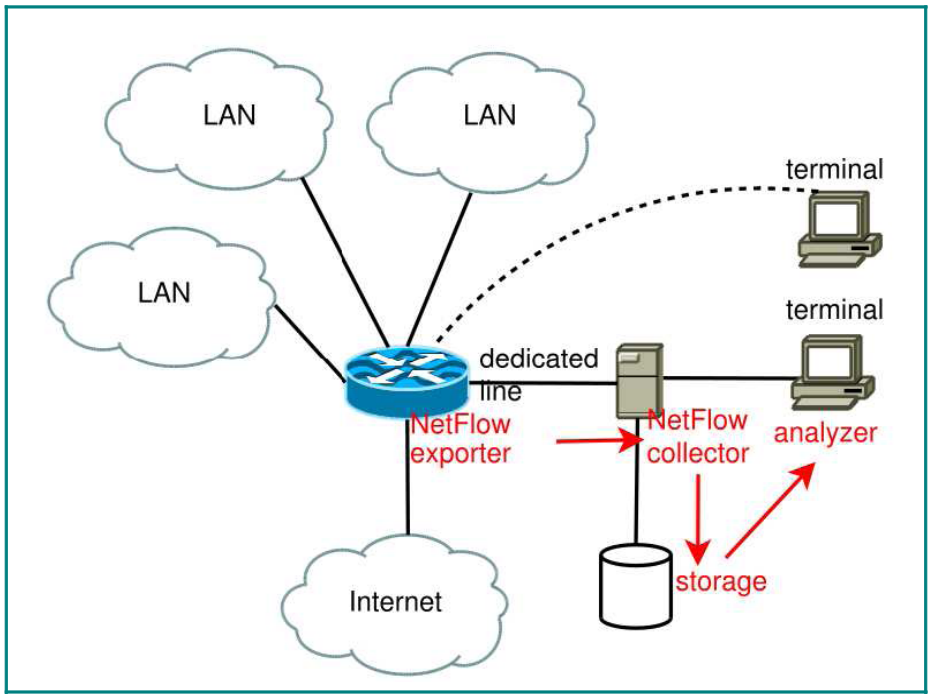
1. Netflow

a. Définition

Netflow est un protocole réseau développé par CISCO afin de collecter des informations sur le trafic IP des équipements CISCO IOS (Internetwork Operating System).
C'est un protocole propriétaire mais Open Source qui a été conçu pour être supporté par les plateformes autres, comme les routeurs Juniper ou bien FREEBSD et OpenBSD.

ii. Description du protocole

Les routeurs CISCO ayant le protocole Netflow actif génèrent des enregistrements netflow. Ils sont enregistrés dans le cache de ce routeur, et peuvent être exportés sous la forme de paquets UDP (User Datagram Protocol) ou bien SCTP (Stream Control Transmission Protocol) vers un collecteur netflow. Ce collecteur récupère les données et les stocke. Un analyseur netflow peut alors être utilisé afin d'analyser les paquets netflow et de les interpréter en effectuant des statistiques sur les paquets reçus.



En analysant le flux de données, une image du flux et du volume du trafic peut être alors dessinée. Elle peut nous aider a mieux comprendre les flux de données circulant à travers le routeur, et ainsi à voire quels sont les flux les plus utilisés au sein du réseau, ou bien à détecter toute attaque, lorsque le trafic en provenance d'une machine ou à destination d'un même serveur semble trop important, suspect.
Aussi, l'analyse de ces enregistrements devra être convenablement effectuée afin de profiter au maximum des statistiques apportées par la les flux netflow.

iii. Les outils

La fonction Netflow de supervision du réseau va être mise en place pour notre audit sécurité, sur le réseau de la Défense. Elle va nous permettre de récolter des statistiques sur le trafic passant par le routeur CISCO. Une fois cette fonction activée et configurée sur le routeur, nous avons mis en place une machine appelée « collecteur Netflow » pour récolter les statistiques réalisées par le routeur CISCO afin de les stocker et de les analyser pour déceler des attaques sur le réseau.

La suite d'outils Netflow que l'on a mis en place est la suite **NFDUMP**, contenant un collecteur et un analyseur Netflow. Celle-ci a été choisie pour sa fonctionnalité d'analyse asynchrone des flux, et pour sa précision d'analyse. De plus amples informations sur ce produit sont disponibles sur le site : http://nfdump.sourceforge.net/

Collecteur Netflow

nfcapd - netflow capture daemon. Lit les données netflow du réseau et les sauvegarde dans des fichiers. La rotation des fichiers s'effectue toutes les n minutes (autour de 5 min habituellement). nfcapd peut lire les enregistrements netflow de version 5, 7 et 9. Il faut un processus nfcapd pour chaque netflow stream.

Analyseur Netflow

nfdump - netflow dump. Il lit les données netflow à partir de fichiers stockés par nfcapd. Il utilise la même syntaxe que tcpdump. Il affiche les données netflow et peut créer des lots de statistiques par adresse IP, par port etc…

NfSen permet d'ajouter à l'analyseur nfdump (qui est en mode console) une interface graphique pour la retranscription des statistiques netflow.

2. SNORT

a. Définition

Snort est un outil IDS (Introduction Detection System) open source. Son but est d'effectuer en temps réel des analyses de trafic et de logger les paquets IP transitant sur son réseau. Cela est du à sa communauté très active qui partagent ses règles de sécurité permettant à tous utilisateurs de garder sa configuration à jours. Snort est considérer comme un des meilleurs outils de détection d'intrusions sur le marché.

Notons que Snort dispose de trois modes de fonctionnement :

- sniffer de paquets
- logger de paquets
- système de détection/prévention d'intrusions.

ii. Mise en place des sondes

Snort va nous servir à analyser les trafics inhabituels sur le réseau. Pour pouvoir analyser au mieux le trafic, son mode de fonctionnement sera en NIDS. Grâce à cela on analysera plus rapidement les échanges inhabituels.

Dans le cadre du projet, nous avons installé 2 sondes sur le réseau afin de capturer le trafic :

- Une sonde a été placée juste avant le réseau de l'entreprise : permet de capturer toutes les attaques qui sont destinées au réseau.
- Une autre sonde dans le réseau, juste après le firewall : permet de voir toutes les attaques bloquées et surtout analyser celles qui seront passées pour renforcer la sécurité du réseau.

Afin de récupérer tout le trafic arrivant sur le réseau dans la seconde sonde, il est nécessaire d'effectuer un mirroring des flux arrivant sur le commutateur d'entrée. Comme le commutateur d'entrée est un CISCO, il est possible de réaliser du SPAN, et donc dupliquer toutes les requêtes entrantes et sortantes vers une sortie reliée à la sonde.
Le SPAN (Switched Port ANalyzer) est une fonction des commutateurs Ethernet Cisco qui permet de recopier sur un port donné le trafic destiné à un ou plusieurs autres ports.
Un analyseur de réseau connecté au port SPAN peut surveiller le trafic provenant de l'un des ports du commutateur. Cette fonction permet d'effectuer des analyses de trafic sans perturber le fonctionnement.

iii. Fonctionnement du NIDS

Un NIDS fonctionne en 3 parties :

- la capture
- l'analyse des signatures des paquets
- l'envoie d'une alerte selon les règles misent en place

La capture consiste en la récupération des requêtes en temps réel. Snort utilise la bibliothèque standard de capture de paquet : libcap. Son fonctionnement est très simple : tout paquet arrivant au niveau de la couche de liaison de données est copié. Puis on lui applique un filtrage selon les paquets que l'on souhaite analyser.

On peut comparer l'analyse par signature à un antivirus. Sur chaque paquet, on va rechercher selon les règles définies, des informations non habituelles. Si un message n'est pas commun, alors une alerte est envoyée. Il est donc essentiel de bien réaliser les règles pour récupérer au mieux des alertes pertinentes.

Ecriture des règles SNORT :
Les règles de snort sont décrites dans un langage simple.
Dans un premier temps l'en-tête de règle qui contient :

- l'action de la règle (la réaction de snort)
- le protocole qui est utilisé pour la transmission des données
- les adresses IP source et destination et leur masque
- les ports source et destination sur lesquels il faudra vérifier les paquets

Dans un deuxième temps, les options de la règle (entre parenthèse) qui contiennent :

- le message d'alerte
- les conditions qui déterminent l'envoi de l'alerte en fonction du paquet inspecté. Exemple : alert tcp any any → 192.168.1.0/24 21 (content: "USER root"; nocase; msg: "Tentative d'accès au FTP pour l'utilisateur root"). Les messages en direction de 192.168.1.0/24 effectuant une tentative de login root ("USER root" contenu dans le paquet) auront pour conséquence la génération de l'alerte "Tentative d'accès au FTP pour l'utilisateur root".

Exemple d'un rapport SNORT envoyé automatiquement par e-mail :

De : root [root@casper.ups-tlse.fr] Date : mar. 25/11/2008 06:25
À : root@casper.ups-tlse.fr
Cc :
Objet : [m2-stri.analyse] [SNORT] Casper.stri daily report

```
Events between  11 24 06:26:14  and  11 25 06:24:20 Total events: 5307 Signatures
recorded: 16 Source IP recorded: 197 Destination IP recorded: 12


Events from same host to same destination using same method
=============================================================================
 # of  from             to               method
=============================================================================
 3745  130.120.84.1     224.0.0.13       BAD-TRAFFIC IP Proto 103 PIM
   98  130.120.84.96    91.121.143.114   FTP command overflow attempt
   59  63.218.69.2      130.120.84.96    ICMP PING NMAP
   53  63.216.14.130    130.120.84.96    ICMP PING NMAP
   47  130.120.84.96    71.199.101.86    FTP command overflow attempt
   36  130.120.84.96    141.115.64.16    SNMP request udp
   36  130.120.84.96    141.115.64.16    SNMP public access udp
   28  194.214.181.111  130.120.84.170   MISC MS Terminal server request
   25  202.172.101.36   130.120.84.96    ICMP PING NMAP
   23  122.152.142.14   130.120.84.96    ICMP PING NMAP
```

iv. Les outils complémentaires

Pour fonctionner au mieux, un ensemble d'outils ont été installé pour compléter Snort :

- BASE (Basic Analysis and Security Engine) : Base est une interface graphique en PHP permettant de visualiser les logs de l'IDS Snort.
- Easy PHP : c'est une plateforme de développement web permettant d'exécuter des scripts PHP. Il contient 2 serveurs : le serveur APPACHE et le serveur http.

3. Les sondes et Audit Actif

Dans le cadre des différentes confrontations, nous avons mis en place des sondes snort qui permettent de faire, entre autres, des captures de trames circulant sur le réseau. Les objectifs définis sont les suivants :

-Installer une sonde en accord avec le client

-Sécuriser la sonde

-Réaliser la capture des trames transitant sur le réseau

-Réaliser une détections d'intrusions

-Réaliser un audit actif du réseau de la défense

A. Mise en place des sondes

A1) L'installation de la sonde

Pour l'installation de la sonde, nous avons mis en place au préalable un système d'exploitation Linux debian que nous connaissons bien et que nous pouvons installé de manière rapide. Nous maîtrisons bien cet outil pour l'avoir utilisé depuis trois ans maintenant. De plus, nous avons installé un système minimal sans interface graphique de manière à limité le nombre de logiciels inutiles sur la sonde. Enfin, l'OS Debian contient un gestionnaire de paquet très pratique, "apt-get|cache|remove" en ligne de commande, qui permet d'installer rapidement les paquets à partir des sources disponibles sur les miroirs debian.

D'un point de vue services, nous avons installé sur notre sonde les services suivants :

- Apache-ssl, Php, Mysql, Acid-base, SSH

Les trois premiers servent à gérer de manière graphique les résultats que fournira la sonde snort. Acid-base est un outil utilisé pour récupérer et analyser les alertes générées par la sonde snort.

a) Sonde en détection d'intrusions

L'installation d'une sonde nécessite plusieurs outils. En effet, il faut dans un premier temps, installés les logiciels qui vont permettre de faire fonctionner la sonde :

- SNORT (l'IDS), Barnyard, Mysql

Le premier outil, SNORT est l'outil principal qui permet de détecter des alertes via les fichiers de règles définis sur le site officiel SNORT.

L'enregistrement des évènements qui se produisent sur le réseau est l'une des activités les plus coûteuses en temps que snort réalise. Les données doivent être :

-collectées

-formatées

-écrites

Dans notre cas, une base de données Mysql est utilisée. Dans ce cas, snort doit envoyer l'alerte et attendre la confirmation de l'écriture des informations. Cette situation empire lorsque le serveur de bases de données est sur un système distant.

Snort sait envoyer des infos collectées à propos d'une alerte vers un fichier au format binaire. Cet enregistrement est très rapide car les données n'ont pas besoin d'être formatées. Barnyard lit ce fichier, formate les données des alertes et les enregistre vers le mécanisme de sortie choisi (fichier journal snort, syslog, fichier texte ou BDD).

Pour utiliser l'enregistrement au format binaire unifié, snort est configuré comme d'habitude. La seule différence se situe au niveau du choix de greffon de sortie dans le fichier snort.conf. L'unique greffon de sortie qui devrait y être spécifié est « log_unified ».

output alert_unified: filename snort.alert, limit 128

output log_unified: filename snort.log, limit 128

Avec ces deux lignes activées dans le fichier de configuration des sondes (/etc/snort/snort.conf), nous allons récupérer des fichiers snort.log et snort.alert dans le répertoire de log de snort. Barnyard va utiliser ces fichiers pour enregistrer les données dans la base de données. Ils sont, en quelques sortes, des fichiers "intermédiaires" entre snort et la BD.

Le lancement des sondes se faisait grâce à un script shell automatisé qui était contenu dans le fichier /etc/init.d :

```
#!/bin/bash

/sbin/ifconfig eth0 up

/usr/local/bin/snort -Dq -u snort -g snort -c \

/etc/snort/snort.conf -i eth0 -z

/usr/local/bin/barnyard -c /etc/snort/barnyard.conf -g \

/etc/snort/gen-msg.map -s /etc/snort/sid-msg.map -d \

/var/log/snort -f snort.log -w /etc/snort/bylog.waldo &
```

b) Sondes avec capture de trames

La deuxième fonctionnalité des sondes était de pouvoir capturer les trames circulant sur le réseau. Pour cela, nous avons utilisé le logiciel tcpdump. Cependant, nous l'avons amélioré puisque nous avons utilisé un script de lancement comme pour que tcpdump soit lancer comme un service.

Tcpdump était lancée avec des options bien précises. En l'occurence, nous avons spécifiés, pour la seconde et troisième confrontation, la taille maximale des fichiers de capture à 50Mo (options -C). L'interface d'écoute était eth0, et nous avons mis en place un filtre de captures (FILTER='(ip or arp or rarp) and not icmp').

A2) Sécurisation de la sonde

La sécurisation des sondes est un point très important puisque c'est un point très critique. En effet, il ne faut pas que celle-ci soit compromise.

La sécurisation des sondes passent par différents points :

-La sécurisation des services mis en place

-La sécurisation de l'accès à la machine

Etant donné que nous avons mis en place un serveur web et une base de données Mysql sur les sondes, il nous fallait sécuriser ces services. Ainsi, l'accès à la base était restreint par des certificats SSL. De plus, nous avons supprimé les bannières apache et php, supprimé l'ouverture mysql sur le réseau via l'option "skip-networking" du fichier de configuration mysql (my.cnf).

La sécurisation de l'accès à la machine passait par une bonne configuration du service sshd. Nous l'avons préféré à telnetd car ce dernier ne crypte pas les données circulant sur le réseau, ce qui est critique. Au niveau du service SSH, nous avons interdit l'accès root distant, la redirection X11 et nous avons mis en place une bannière.

Au niveau adressage, nous avons mis en place une configuration ARP statiques :

// Cooper : routeur d'accès

Cooper : 172.18.4.1 00:04:23:B8:4E:2C

//candide-sa : routeur de la défense

candide-sa : 172.18.4.2 00:14:F2:75:ED:72

//première sonde extérieure

ossim : 172.18.4.202 00:10:5A:D8:89:41

//Seconde sonde extérieure

Ramada : 172.18.4.200 00:0A:5E:1D:FC:3F

Enfin, nous avons sécurisé les sondes au niveau des iptables (via un script) afin de restreindre les données pouvant arriver sur la machine. En voici quelques lignes :

//restriction au niveau des pings

$ipt -A OUTPUT -o eth1 -p icmp --icmp-type echo-request -m limit --limit 3/s -m state --state NEW -j ACCEPT

$ipt -A OUTPUT -o eth1 -p icmp --icmp-type echo-reply -m limit --limit 3/s -m state --state NEW -j ACCEPT

//on accepte les nouvelles connexions ssh (sur lastemperor) à partir de la seconde sonde topper 172.10.200.3

$ipt -A INPUT -i eth1 -s 172.10.200.3 -p tcp --dport 22 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT

$ipt -A OUTPUT -o eth1 -d 172.10.200.3 -p tcp --sport 22 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT

B. Réaliser un audit actif sur le réseau de la défense

Dans le cadre de notre contrat avec la défense, nous avions prévu de réaliser un audit actif du réseau de la défense. Pour cela, nous avons utilisé Nessus, un scanner de vulnérabilités ainsi que l'outil nmap pour le compléter.

Nessus est très utile lors de tests de pénétration et fait gagner un temps incroyable. Il se compose d'une partie serveur (qui contient une base de données regroupant différents types de vulnérabilités) et une partie cliente. Le client se connecte au serveur et après authentification, il peut scanner les différents systèmes du réseau pour récupérer les différentes vulnérabilités du système. Le client reçoit ensuite les résultats du test sous un format html (ce que nous avons choisi). Nessus a été implémenté sur ma machine et disposé sur le réseau interne de la défense (comme un poste client).

- **Test de l'outil Nessus**

Le test a été réalisé le 30 octobre 2008, et nous a permis de vérifier si les serveurs étaient ou non infaillibles. Par exemple, le test sur le serveur web/Sql 172.10.140.2 a rendu le résultat suivant :

- 3 ports ouverts.
- 21 failles qualifiées faible.
- 2 failles qualifiées moyennes.

- **Information détectée par le test :**

- La machine tourne sous linux Kernel 2.6.

Les ports ouverts :

Port 22: SSH en écoute, risque faible

Récupération du banner sur SSH

Port 443 : HTTPS Risque faible

Réponse du serveur fonctionnant sous TLSv1.

Il est possible de récupérer les Web directories : /incons.

Port 80 : HTTP risques faibles :

Détection du serveur

Détection de la version et du type de serveur : Apache/2.2.9 (Debian) PHP/5.2.6-5 with Suhosin-Patch mod_ssl/2.2.9 OpenSSL/0.9.8g

Risques moyens :

- Redirection vers des domaines de manière arbitraire par les méthodes : 303, 304 ou 307. : http://172.10.140.2/.anydomain.test redirects to location: https://www.candide-sa.com.anydomain.test
- Faiblesse : un attaquant peut se servir de la redirection pour effectuer du phishing.

Voici un exemple de résultat graphique généré par nessus : au niveau client.

List of hosts

172.10.140.2 — Medium Severity problem(s) found

[^] Bac

172.10.140.2

Scan time :

Start time :	Thu Oct 30 10:39:16 2008
End time :	Thu Oct 30 10:41:34 2008

Number of vulnerabilities :

Open ports :	3
Low :	21
Medium :	4
High :	0

Information about the remote host :

Operating system :	Linux Kernel 2.6
NetBIOS name :	(unknown)
DNS name :	(unknown)

[^] Back to 172.10.140.

Port ssh (22/tcp)

Service detection

An SSH server is running on this port.

Nessus ID : 22964

SSH Server type and version

Synopsis :

An SSH server is listening on this port.

Description :

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Risk factor :

None

Plugin output :

SSH version : SSH-2.0-OpenSSH_5.1p1 Debian-3
SSH supported authentication : publickey,password
SSH banner :
GENTOO 2008.1 - WILLKOMMEN

- **Test avec l'outil NMAP**

NMAP est un logiciel disponible sous linux sous forme de paquet debian,

il permet de scanner les ports sur le réseau (par exemple sur le réseau des serveurs de la défense) en envoyant des SYN/ACK par exemple via la commande :

nmap -sS 172.10.140.0

Le résultat sous AcidBase est le suivant, il y a un résultat sur les ports ouverts.

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#600-(2-104)	[snort] portscan: Open Port	2008-11-13 15:07:31	172.10.150.4	172.10.140.2	Raw IP
#601-(2-103)	[snort] portscan: TCP Portscan	2008-11-13 15:07:31	172.10.150.4	172.10.140.2	Raw IP
#602-(2-61)	[snort] portscan: Open Port	2008-11-13 15:05:11	172.10.150.4	172.10.140.2	Raw IP
#603-(2-59)	[snort] portscan: TCP Portscan	2008-11-13 15:05:11	172.10.150.4	172.10.140.2	Raw IP
#604-(2-58)	[snort] portscan: Open Port	2008-11-13 15:05:11	172.10.150.4	172.10.140.3	Raw IP
#605-(2-57)	[snort] portscan: TCP Portscan	2008-11-13 15:05:11	172.10.150.4	172.10.140.3	Raw IP
#606-(2-56)	[snort] portscan: Open Port	2008-11-13 15:05:11	172.10.150.4	172.10.140.1	Raw IP
#607-(2-55)	[snort] portscan: TCP Portscan	2008-11-13 15:05:11	172.10.150.4	172.10.140.1	Raw IP
#608-(2-54)	[snort] portscan: TCP Portsweep	2008-11-13 15:05:11	172.10.150.4	172.10.140.3	Raw IP
#609-(2-60)	[snort] portscan: Open Port	2008-11-13 15:05:11	172.10.150.4	172.10.140.2	Raw IP
#610-(2-62)	[snort] portscan: Open Port	2008-11-13 15:05:11	172.10.150.4	172.10.140.3	Raw IP
#611-(2-63)	[snort] portscan: Open Port	2008-11-13 15:05:11	172.10.150.4	172.10.140.3	Raw IP
#612-(2-71)	[snort] portscan: Open Port	2008-11-13 15:05:11	172.10.150.4	172.10.140.3	Raw IP
#613-(2-70)	[snort] portscan: Open Port	2008-11-13 15:05:11	172.10.150.4	172.10.140.3	Raw IP
#614-(2-69)	[snort] portscan: Open Port	2008-11-13 15:05:11	172.10.150.4	172.10.140.3	Raw IP
#615-(2-68)	[snort] portscan: Open Port	2008-11-13 15:05:11	172.10.150.4	172.10.140.3	Raw IP
#616-(2-67)	[snort] portscan: Open Port	2008-11-13 15:05:11	172.10.150.4	172.10.140.3	Raw IP
#617-(2-66)	[snort] portscan: Open Port	2008-11-13 15:05:11	172.10.150.4	172.10.140.3	Raw IP
#618-(2-65)	[snort] portscan: Open Port	2008-11-13 15:05:11	172.10.150.4	172.10.140.2	Raw IP
#619-(2-64)	[snort] portscan: Open Port	2008-11-13 15:05:11	172.10.150.4	172.10.140.2	Raw IP
#620-(2-37)	[snort] portscan: Open Port	2008-11-13 14:54:46	172.10.150.4	172.10.140.3	Raw IP
#621-(2-38)	[snort] portscan: Open Port	2008-11-13 14:54:46	172.10.150.4	172.10.140.3	Raw IP
#622-(2-34)	[snort] portscan: Open Port	2008-11-13 14:54:27	172.10.150.4	172.10.140.3	Raw IP
#623-(2-33)	[snort] portscan: Open Port	2008-11-13 14:54:27	172.10.150.4	172.10.140.3	Raw IP
#624-(2-19)	[snort] portscan: Open Port	2008-11-13 14:54:09	172.10.150.4	172.10.140.3	Raw IP
#625-(2-18)	[snort] portscan: Open Port	2008-11-13 14:54:09	172.10.150.4	172.10.140.3	Raw IP
#626-(2-17)	[snort] portscan: Open Port	2008-11-13 14:54:09	172.10.150.4	172.10.140.3	Raw IP
#627-(2-16)	[snort] portscan: TCP Portscan	2008-11-13 14:54:09	172.10.150.4	172.10.140.3	Raw IP
#628-(2-15)	[snort] portscan: Open Port	2008-11-13 14:54:09	172.10.150.4	172.10.140.3	Raw IP
#629-(2-14)	[snort] portscan: TCP Portscan	2008-11-13 14:54:09	172.10.150.4	172.10.140.2	Raw IP
#630-(2-13)	[snort] portscan: TCP Portscan	2008-11-13 14:54:09	172.10.150.4	172.10.140.1	Raw IP
#631-(2-20)	[snort] portscan: Open Port	2008-11-13 14:54:09	172.10.150.4	172.10.140.2	Raw IP
#632-(2-21)	[snort] portscan: Open Port	2008-11-13 14:54:09	172.10.150.4	172.10.140.2	Raw IP
#633-(2-22)	[snort] portscan: Open Port	2008-11-13 14:54:09	172.10.150.4	172.10.140.1	Raw IP
#634-(2-23)	[snort] portscan: Open Port	2008-11-13 14:54:09	172.10.150.4	172.10.140.1	Raw IP
#635-(2-24)	[snort] portscan: Open Port	2008-11-13 14:54:09	172.10.150.4	172.10.140.2	Raw IP
#636-(2-25)	[snort] portscan: Open Port	2008-11-13 14:54:09	172.10.150.4	172.10.140.2	Raw IP
#637-(2-12)	[snort] portscan: TCP Portsweep	2008-11-13 14:54:09	172.10.150.4	172.10.140.2	Raw IP
#638-(2-27)	[snort] portscan: Open Port	2008-11-13 14:54:09	172.10.150.4	172.10.140.3	Raw IP

IV – Les étapes du projet

1. Première confrontation

L'objectif de la première confrontation était pour nous le groupe analyse de récupérer les attaques et les moyens utilisés par le groupe attaque par des sondes que nous avons installé dans le réseau de la défense. Ainsi l'interprétation de ces sondes devrait nous conduire à étudier le système de sécurité qu'il fallait mettre en place pour la protection du réseau de la défense. Ainsi nous avons observé ces différentes actions menées par les attaquants

- Beaucoup de trafic récupéré sur la sonde frontale avec TCP dump et SNORT.
- Pas d'informations utiles sur les logs de la sonde interne.
- Récupération des logs de Cisco (échec pour les logs d'apache)
- Echec de récupération des logs netflow

Les attaquants ont ciblé notre sonde au lieu d'attaquer le serveur WEB de la défense.

Les attaques identifiées sont principalement de type ICMP flooding et ARP spoofing. Ces attaques ont entrainés un déni de service avec un taux d'utilisation du CPU du routeur à égale à 99%..

Le bilan de cette confrontation a été positif pour notre équipe puisque aucune de nos sondes est tombées .Cette phase d'analyse nous permettra de mieux conseiller la défense afin qu'il prépare au mieux la seconde confrontation.

- Bilan pour les sondes installées

Au niveau de la première confrontation, nous avons mis en place qu'une seule sonde snort. Celle-ci était configurée en SPAN sur le switch de la défense qui gérait les VLANS. Toutes les données du trunk (port G1) étaient copiées vers l'interface de capture de la sonde (port G2 du switch).

Cependant, les sondes internes n'ont remontés aucunes alertes car il ne s'est rien passé de concret sur le réseau de la défense. Toutes les attaques se sont concentrées sur le réseau extérieur de la défense.

On a cependant pu recencer des attaques suivantes :

[**] [1:1301:12] WEB-PHP admin.php access [**]

Event ID: 93 Event Reference: 93

10/24/08-09:40:06.777888 172.16.97.6:50140 -> 172.10.140.2:80[**]

Cette alerte est générée quand il y a une tentative d'exploit sur une vulnérabilité du serveur web.

[**] [1:2152:2] WEB-PHP test.php access [**]

Nombre d'alerte : 4

Cette alerte est générée lorsqu'un attaquant tente d'accéder à un script non utilisé dans un environnement de production. L'attaquant souhaitait sans doute récupérer des informations sur le serveur web afin de réaliser une attaque par la suite.

[**] [1:1852:4] WEB-MISC robots.txt access [**]

[Classification: access to a potentially vulnerable web application] [Priority: 2]

10/13/08-07:56:28.518446 172.16.64.86:3742 -> 172.10.140.2:80

Cette alerte est générée lorsqu'un attaquant tente d'accéder à des données qui ne sont pas publiques telles que des répertoires utilisateurs ou des fichiers d'administration.

2. Deuxième confrontation

Pareil que la première confrontation, le but de celle-ci est surtout d'analyser les moyens utiliser par le groupe attaque, observer la réaction des techniques de sécurité mise en place et enfin voire l'impact des solutions que nous avons conseillé à la défense sur sa protection de son réseau vis-à-vis des attaques.

• Bilan des attaques

Nous avons donc pu observer beaucoup de trafic polluant venant des attaquants, ayant pour but de noyer le réseau de trames inutiles, afin de saturer le routeur, dissimuler une attaque sous un flux de données important, et tenter de détecter des failles de sécurités (ports du routeurs ouverts…).
L'analyse des flux nous a permis de constater qu'ils ont envoyé une majorité de trames TCP, ce qui peut vouloir dire qu'ils ont essayé de s'attaquer directement au serveur web
« Candide » de la défense.
Aussi, nous avons recensé des scannages de ports, de l'IP Flooding, des tentatives de Saturation du routeur par l'envoi de trames TCP et UDP et ICMP de destinataires différents sur des ports du routeur de la défense.

• Bilan du Netflow

L'analyse netflow de la deuxième confrontation nous a permis de nous rendre compte que le netflow n'était pas efficace pour l'analyse directe des attaques. Cet outil est très utile pour donner une vision globale du trafic, des protocoles les plus utilisés, des adresses les plus génératrices de trafic, mais pas pour détecter précisément type d'attaque.

Le netflow est complémentaires à des outils d'analyse de paquets, comme Wireshark, Snort, et à des analyseurs de logs, mais ne peut pas fonctionner seul pour la détection d'attaques. Il peut donner une cartographie globale du trafic pour orienter les équipes Wireshark et Snort dans l'analyse des paquets.

Pour plus de détail se conférer à l'annexe (Rapport netflow 2° confrontation).

• Bilan des sondes

Nous avons mis en place pour cette seconde confrontation une seconde sonde (en plus de la première toujours configurée en SPAN sur le switch) qui était configuré pour écouter ce qu'il se passait sur le réseau des serveurs (172.10.140.0/29). De plus, nous avons rajouté une interface réseau sur chacune des sondes afin de pouvoir les administrer à distance. Une interface serait une interface administration et l'autre était destinée à l'écoute uniquement.

Nous avons pu observer que durant la confrontation (et même au préalable) qu'il y a eu des tentatives de découvertes de mots de passe sur le serveur web de la défense :

[**] [1:8426:6] WEB-MISC SSLv2 openssl get shared ciphers overflow attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

Event ID: 18 Event Reference: 18

11/03/08-07:38:57.403908 **172.16.80.20:38508 -> 172.10.140.2:443**

[**] [1:2436:8] WEB-CLIENT Microsoft wmf metafile access [**]

[Classification: Attempted User Privilege Gain] [Priority: 1]

Event ID: 328 Event Reference: 328

11/03/08-10:38:22.563904 172.10.150.3:1765 -> 172.16.64.86:80

TCP TTL:128 TOS:0x0 ID:12957 IpLen:20 DgmLen:478 DF

…

/1.1..Accept: im

61 67 65 2F 67 69 66 2C 20 69 6D 61 67 65 2F 78 age/gif, image/x

2D 78 62 69 74 6D 61 70 2C 20 69 6D 61 67 65 2F -xbitmap, image/

6A 70 65 67 2C 20 69 6D 61 67 65 2F 70 6A 70 65 jpeg, image/pjpe

67 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 g, application/x

2D 73 68 6F 63 6B 77 61 76 65 2D 66 6C 61 73 68 -shockwave-flash

2C 20 2A 2F 2A 0D 0A 52 65 66 65 72 65 72 3A 20 , */*..Referer:

68 74 74 70 3A 2F 2F 73 74 72 69 2D 61 74 74 61 **http://stri-atta**

71 75 65 2E 69 66 72 61 6E 63 65 2E 63 6F 6D 2F que.ifrance.com/

Cette alerte est générée quand il y a une tentative d'accès à un fichier qui peut être sujet à une vulnérabilité Internet Explorer.

La conséquence d'une telle attaque est critique puisqu'elle peut amener à une DOS de la machine. Ici, la machine client a accéder au site stri-attaque.ifrance.com.

3. Troisième confrontation

Comme les autres confrontations, celle-ci a les mêmes objectifs mais présente quelques différences par rapport à son contexte. D'abord c'était la dernière confrontation ce qui explique que les méthodes des attaquants et la nature des attaques ont évolué, d'un autre coté avec l'appui de l'équipe analyse, le système des défenseurs aussi a évolué.

• Bilan des attaques

Pour cela pendant toute la confrontation rien de particulier ne s'est passé, les attaquants n'ont pas réussi à atteindre le réseau des défenseurs.

Les attaques que l'équipe d'analyse a pu relever sont les suivantes :

- DNS Flooding
- Envoi massif de mails
- MAC Flooding
- Attaques STP
- Mail bombing

- UDP Flooding
- DNS Man in the Middle (Hijacking)
- les autres attaques relevées

L'aspect technique de ces attaques sont développées en annexe. (Annexe bilan des attaques 3° confrontation)

• Bilan du netflow

Sur le plan Netflow, nous n'avons pas enregistré de fichiers de taille maximale, on peut donc supposer que nous avons bien récupérés toutes les communications.
Pour l'analyse Netflow de la troisième confrontation, Nfsen n'était pas complètement opérationnel car la génération des graphiques n'a pas pu être débuggée. Nous avons donc Utilisé les fonctionnalités de traitement des flows mais sans les graphs. Cette nouvelle analyse de l'activité durant la confrontation nous amène donc à tirer un bilan sur la solution Netflow. Cette solution est réellement pratique pour avoir une vue globale des activités sur le réseau, Pour effectuer de rapides statistiques sur les communications. En ce qui concerne Nfsen nous n'avons pas pu tester toute sa puissance qui réside dans la génération de graphiques, et permet de visualiser l'activité générale du réseau de manière graphique, ce qui permet de mieux cibler les périodes d'activités qui méritent une analyse plus approfondie.

La technologie Netflow est certainement bien plus intéressante en exploitation réelle. En effet, durant les confrontations nous avions des quantités de données à analyser mais aucun moyen de les comparer à un trafic « normal » dans le réseau. Aussi c'est en observant des pics d'activités par rapport à une activité normale que l'on peut aussi détecter des attaques. Pour résumer la technologie peut être très utile si l'on veut avoir une vue global de l'activité sur le réseau et effectuer des statistiques. Netflow ne constitue absolument pas une solution à part entière en termes d'analyse réseau. Les résultats que peuvent apporter netflow sont à mettre en relation avec d'autres outils notamment tcpdump + wireshark pour une analyse détaillée. On notera comme principal inconvénient de la technologie netlflow : la charge CPU que cela demande au routeur, l'arrêt de ce service si le routeur est trop sollicité et la taille maximum des fichiers (108Mo) qui témoignent d'une perte d'information. Pour plus de détails se conférer à l'annexe (Rapport netflow 3° confrontation)

• Bilan des sondes

Pendant la troisième confrontation, il y a eu beaucoup de messages ICMP, c'était une procédure pour inonder les sondes et le réseau par la même occasion :

[**] [1:485:5] ICMP Destination Unreachable Communication Administratively Prohibited [**]

[Classification: Misc activity] [Priority: 3]

Event ID: 39754 Event Reference: 39754

11/17/08-08:25:27.712393 **172.10.140.1 -> 172.10.140.2**

[**] [1:485:5] ICMP Destination Unreachable Communication Administratively Prohibited [**]

[Classification: Misc activity] [Priority: 3]

Event ID: 39756 Event Reference: 39756

11/17/08-08:25:29.837332 **172.10.140.1 -> 172.10.140.3**

ICMP TTL:255 TOS:0x0 ID:49774 IpLen:20 DgmLen:56

Type:3 Code:13 DESTINATION UNREACHABLE: PACKET FILTERED

Ces alertes étaient toutes filtrées.

Tentative de récupération des privilèges administrateurs :

[**] [1:8428:6] WEB-MISC SSLv2 openssl get shared ciphers overflow attempt [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

Event ID: 39968 Event Reference: 39968

11/17/08-08:28:32.385449 **172.16.80.12:40534 -> 172.10.140.2:443**

[**] [124:7:1] smtp: Attempted header name buffer overflow [**]

[Classification: Unknown] [Priority: 3]

Event ID: 45844 Event Reference: 45844

11/17/08-10:02:36.969770 **172.18.4.102:60954 -> 172.10.140.3:25**

TCP TTL:63 TOS:0x0 ID:60730 IpLen:20 DgmLen:1500 DF

A* Seq: 0xBD2C470A Ack: 0x7C2DC20E Win: 0x16D TcpLen: 32

TCP Options (3) => NOP NOP TS: 280334335 304422742

[**] [1:3486:3**] **WEB-MISC SSLv3 invalid data version attempt [**]

[Classification: Attempted Denial of Service] [Priority: 2]

Event ID: 42169 Event Reference: 42169

11/17/08-09:08:01.448723 **172.16.97.18:3313 -> 172.10.140.2:443**

Cette alerte est générée lorsqu'il y a une tentative d'exploit sur une vulnérabilité de l'implémentation sur les système microsoft SSLv2.

Cependant, nous pensons qu'il y a une grand nombre de faux positifs qui ont été générés par la sonde snort ce qui n'a sans doute pas permis de détecter correctement l'ensemble des attaques des attaquants. La sonde a récupéré dans le fichier dump.log, généré par snort, un grand nombre d'alertes ICMP Destination Unreachable entre le routeur 172.10.140.1 et le serveur web ou DNS (140.2, 140.3). Nous pensons que l'ensemble de ces alertes ont sans doute empêché de voir d'autres attaques.

De plus sur la sonde interne lastemperor (surveillance des serveurs), il y a 161039 alertes dont le message généré est : [**] Snort Alert [1:1000002:0] [**] et 2 alertes "Snort Alert [1:8428:0]". Cependant, nous n'avons pas pu découvrir la signification de ces alertes.

Conclusion

Ce projet regroupais trois équipes que sont la défense, l'analyse et l'équipe attaque. Nous équipe Analyse avions pour rôle d'analyser et de proposer des solutions à l'équipe de la défense pour protéger leurs infrastructures réseaux afin d'éviter des intrusions. Nous avions eu Trois confrontations entre les différentes équipes intervenantes dans ce projet. Afin de mieux conseiller l'équipe de la défense et réussir notre mission nous avions divisé notre équipe en plusieurs sous groupes en leur octroyant chacun un rôle bien défini. Ces sous groupes ont connu différentes évolutions en fonction de la demande de la défense et la nature des attaques .Nous avons développé plusieurs technologies pour auditer le réseau de la défense tel snort , wireshark , syslog, netflow et tant d'autres nous permettant à mieux analyser la nature des attaques et à conseiller la défense .

Dans l'ensemble des confrontations nous n'avions pas trouvé des attaques pouvant nuire à l'architecture de la défense.

Ce projet nous a permis de mettre par-dessus toutes nos connaissances acquises en pratique. Selon les sous groupes aux quels nous appartenions, nous avons pu développer ces connaissances , que ca soit en management, gestion de projet, respect des délais ou les accès plus technique, mise en place des sondes, analyse des traces, politique de sécurité, architecture réseau, etc.

Pour une première réelle expérience dans le domaine des réseaux nous regrettons ce pendant, de ne pas avoir pu, tous, participer aux différentes parties techniques, notamment la configuration des routeurs. Mais nous nous réjouissions, peu importe l'appartenance des groupes, d'avoir participé à ce projet et l'avoir mené à terme et ceci avec un groupe de 18.

Annexes

1. Annexe 1 – Contrat d'audit

CONTRAT D'AUDIT

samedi 4 septembre 2010	Salle U2
Objet	Contrat avec l'équipe d'audit
Participants	Responsables groupes *analyse*/*défense*

Sommaire

Suite à la demande du client ***Candide S.A*** d'établir un **audit réseau** de son infrastructure, nous établissons le **contrat** ayant pour but de définir une **collaboration entre les équipes *défense* (Candide SA) et *analyse*.**

Cette collaboration doit **assurer le bon fonctionnement de la mission d'audit de sécurité** par la validation des moyens de protection mis en œuvre sur les plans organisationnels, procéduraux et techniques, au regard de la politique de sécurité rédigé par les soins de la *défense*.

Nous avons donc convenu après négociation avec la *défense*, les **clauses** suivantes :

Article1 - Informations sur le Réseau :

L'audité, ayant confié à l'équipe d'*analyse* le soin d'assurer un audit complet des systèmes d'information de *Candide S.A*, s'engage à fournir le recensement détaillé de l'ensemble des éléments qui constituent ce système. **L'auditeur aura accès aux informations suivantes:**

- **Réglementation interne, procédures, organigramme du personnel, charte d'utilisation des ressources.**
- **Sécurité physique :** Normes de sécurité, protection des accès (équipements, infrastructure câblée, etc.).
- **Exploitation et administration :** journalisation des logs, informations SNMP.
- **Réseaux et télécoms :** architecture réseau (topologie, plan d'adressage), matériels (routeurs, commutateurs, pare-feux), contrôle des accès logiques.
- **Systèmes :** poste de travail (gestion des droits), serveurs et les services qu'ils délivrent, applications, solutions antivirales, ainsi que le détail des versions utilisées.

Article2 - Périmètre d'actions de l'audit :

Ayant connaissance des éléments composant le système d'information, l'**auditeur** pourra **définir le périmètre de l'audit** et **planifier ses interventions et ses entretiens** avec les personnes à interviewer au sein de la *défense*. L'équipe d'***analyse*** sera **responsable de l'organisation des réunions avec l'équipe auditée** et devra, à l'issue de celles-ci, proposer des recommandations pour la mise en place de mesures organisationnelles et techniques.

Article3 - Mise en place des outils de supervision :
L'audité conviendra avec l'auditeur d'un **droit d'accès physique au système** pour la **mise en place d'outils d'analyse et de détection** (analyse des logs, scans, sondes, récupération de trafic). Sur autorisation explicite de la *défense*, l'auditeur pourra effectuer des **tests d'intrusions** selon des scénarios potentiels d'attaque, afin de déterminer les vulnérabilités et les failles de sécurité.

Article4 - Compte-rendu :
Chaque phase d'analyse et d'évaluation réalisée par les soins de l'équipe d'***analyse*** devra faire l'œuvre d'un **rapport complet** présentant de manière explicite les **vulnérabilités détectées sur le système audité**, et **proposant des améliorations techniques et organisationnelles** pouvant entraîner une revue de la politique de sécurité.

A son tour la ***défense*** devra informer l'auditeur de **toute modification ou évolution de son système de sécurité.**

Article5 - Confidentialité :
L'organisme d'audit, à savoir l'ensemble des personnes qui interviendra pour la mission d'audit de sécurité, s'engage, sous sa responsabilité exclusive, à considérer confidentielles toutes informations transmises par la *défense*, de façon orale ou écrite, et par conséquent à ne pas les divulguer à un tiers. Une **clause de confidentialité** sera établie **à l'initiative de la *défense*** et devra faire l'objet d'une **signature par l'ensemble des membres composant l'équipe d'*analyse*.**

L'organisme d'audit est entièrement responsable de la sécurisation de la sonde et de l'accès au réseau de la *défense* par celle-ci.

De la même manière, les différents droits octroyés à l'organisme d'audit sont sous leur entière responsabilité.

En cas de violation volontaire ou négligente de cette clause, la ou les personnes responsables devront répondre de sanctions négociées au préalable avec la *défense*.

Article6 - Cadre juridique :
L'organisme audité doit être conscient de la législation concernant les systèmes d'informations. Les responsables de sécurité ont une obligation de moyens pour que leur système de sécurité

rentre en conformité juridique. Ils doivent être vigilants au respect de la protection des données privées des employés. L'organisme responsable doit également sensibiliser ses employés sur le cadre d'utilisation d'internet. Un usage abusif sortant du cadre professionnel pouvant induire des problèmes de sécurité et mettre en cause la responsabilité civile ou pénale de l'entreprise et de l'employé.

A cet effet une **charte d'utilisation de l'informatique et des** télécommunications devra être établie à l'initiative de la *défense*.

Article7 - Financier :

Par ce contrat **la *défense* s'engage à prendre en charge la totalité des frais matériels** indispensables à la mise en place d'une supervision efficace. Une fois l'installation effectuée, une rémunération mensuelle sera versée à l'organisme d'audit pour le travail fourni. Une déduction sur cette rémunération pourra être effectuée en cas de responsabilité de l'organisme d'audit dans un quelconque déni de service portant atteinte aux activités de l'entreprise *Candide S.A*.

Au terme des actions entreprises par l'équipe d'attaque durant le temps imparti aux trois séances de TP, et après établissement du rapport d'analyse, un bilan organisationnel et technique de la mission accomplie par les deux équipes en collaboration permettra d'évaluer la part de responsabilité de la *défense* et de *l'audit*.

Article8 - Modification de Contrat :

Pour des éventuelles **modifications** de contrat des avenants seront produits et devront être **obligatoirement signés par les deux partis** que ce soit pour une modification mineure ou majeure afin que tout malentendu soit évité.

Article9 - Intégrité physique :

L'audit se dégage de toute responsabilité dans l'éventualité d'une attaque de niveau physique, le matériel étant hébergé dans les locaux clients ; **La *défense* prendra** donc **en charge l'intégrité physique du matériel de supervision.**

Article 10 – Accès à distance :

L'équipe *défense* s'engage à fournir un **accès sécurisé depuis l'extérieur de l'entreprise.** Cet accès permettra à l'équipe *analyse* d'accéder à ses équipements, donc à l'ensemble des machines qu'elle aura pu installer au sein de l'entreprise *Candide S.A.*

Signatures des deux parties *(précédées de la date et de la mention « lu et approuvé »)* :

Pour le groupe ***Défense***,

M. _____

Le __/10/08

Lu et Approuvé

Pour le groupe ***Analyse***,

M. _____

Le __/10/08

Lu et Approuvé

2. Rapport NetFlow : 3ème confrontation

Lors de cette confrontation, nous n'avons pas enregistré de fichiers de taille maximale, on peut donc supposer que nous avons bien récupérés toutes les communications.

1. Statistiques générales durant la confrontation du 03/11/08 :

1.1. Statistiques générales, total :

Statistics timeslot Nov 17 2008 - 07:50 - Nov 17 2008 - 12:10

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
upstream1	8.4 /s	2.7 /s	3.8 /s	2.0 /s	0 /s	672.8 /s	641.6 /s	29.1 /s	2.1 /s	0 /s	5.1 Mb/s	4.9 Mb/s	121.1 kb/s	15.9 kb/s	0 b/s

All None Display: Sum Rate

1.2. Statistiques générales : taux :

Statistics timeslot Nov 17 2008 - 07:50 - Nov 17 2008 - 12:10

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
upstream1	134.1 k	42.3 k	60.5 k	31.2 k	0	10.7 M	10.2 M	462.1 k	33.9 k	0	10.1 GB	9.8 GB	240.6 MB	31.6 MB	0 B

All None Display: Sum Rate

2. Statistiques protocole TCP :

2.1. Classement par adresse IP Source/bytes :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811170750:nfcapd.200811171210 -n 20 -s srcip/bytes
nfdump filter:
proto tcp
Top 20 Src IP Addr ordered by bytes:
Date first seen          Duration Proto      Src IP Addr    Flows   Packets    Bytes      pps      bps   bpp
2008-11-17 11:01:45.425  8185.996 any       172.18.4.102     5918     4.4 M     6.2 G      559     6.2 M  1461
2008-11-17 09:23:13.509  5159.292 any     131.246.120.27        6     1.7 M     2.4 G      338     3.9 M  1499
2008-11-17 08:54:35.874 15815.547 any        172.18.4.2    11609     3.4 M   289.9 M      226   153780    85
2008-11-17 09:10:21.398   238.296 any      213.186.33.91        6    34592    49.4 M      145     1.7 M  1498
2008-11-17 09:44:01.029 11919.752 any      172.16.80.73      113    86527    12.3 M        7     8666   149
2008-11-17 11:37:32.269  1685.984 any     205.128.69.126        3     7261    10.3 M        4    51307  1489
2008-11-17 12:01:39.977   204.756 any     198.78.208.125        4     7334    10.3 M       35   421843  1472
2008-11-17 11:50:32.921  3583.408 any      172.16.64.90    16874    76578     6.8 M       21    15917    93
2008-11-17 10:31:28.829  4702.020 any      172.16.64.77      102     3598     4.4 M        0     7887  1288
2008-11-17 10:55:43.561  4150.556 any     193.51.224.7        15     2966     4.1 M        0     8278  1448
2008-11-17 09:12:28.598 13501.439 any      172.16.80.12      712     7626     3.0 M        0     1888   417
2008-11-17 12:12:43.473   135.680 any     217.70.129.242        3     1856     2.6 M       13   161479  1475
2008-11-17 08:56:32.574 14195.291 any      72.14.221.91       30     1875     2.5 M        0     1477  1398
2008-11-17 09:33:33.861 11976.192 any      72.14.221.136       6     1606     2.2 M        0     1533  1429
2008-11-17 09:07:10.726 10715.991 any      193.51.224.9       70     1908     2.1 M        0     1644  1154
2008-11-17 09:08:51.538 11215.259 any     213.186.34.222     104     2213     1.9 M        0     1410   893
2008-11-17 11:50:30.449  1424.492 any     206.33.34.126       22     1402     1.7 M        0     9926  1260
2008-11-17 09:24:03.237  2436.324 any     209.172.41.53       26     1103     1.3 M        0     4427  1222
2008-11-17 09:21:54.726 11802.747 any      74.125.39.18      128     1698     1.2 M        0      883   767
2008-11-17 10:24:37.705  8138.224 any      172.16.64.93      158     1873   953315         0      937   508

Summary: total flows: 42283, total bytes: 9.1 G, total packets: 9.7 M, avg bps: 4.7 M, avg pps: 644, avg bpp: 958
Time window: 2008-11-17 08:54:35 - 2008-11-17 13:18:11
Total flows processed: 134065, Records skipped: 0, Bytes read: 6972064
Sys: 0.060s flows/second: 2234305.0   Wall: 0.027s flows/second: 4892526.1
```

2.2. Classement par adresse IP destination/bytes :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811170750:nfcapd.200811171210 -n 20 -s dstip/bytes
nfdump filter:
proto tcp
Top 20 Dst IP Addr ordered by bytes:
Date first seen          Duration Proto      Dst IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2008-11-17 08:54:35.870 15815.551 any        172.18.4.2    23840    6.3 M    8.8 G      418    4.6 M  1431
2008-11-17 11:01:45.429  8185.992 any      172.16.64.102     1687    2.3 M  124.5 M      294  127564    54
2008-11-17 09:44:01.029 11919.752 any      172.16.80.73       110  104572   80.5 M        8   56675   807
2008-11-17 09:23:13.509  5159.292 any     131.246.120.27        5  927284   47.3 M      179   76865    53
2008-11-17 11:50:32.929  3583.392 any      172.16.64.90     3772   40609   14.2 M       11   33254   366
2008-11-17 09:12:28.602 13501.435 any      172.16.80.12      337    5957    4.0 M        0    2499   708
2008-11-17 10:08:49.097  9246.104 any      172.16.64.95      185    3041    3.3 M        0    2951  1121
2008-11-17 09:50:12.301  5900.824 any      172.16.97.18      568    6747    3.1 M        1    4380   478
2008-11-17 10:24:37.709  8138.092 any      172.16.64.93       72    1672    1.0 M        0    1051   639
2008-11-17 09:10:21.398    74.852 any     213.186.33.91        1   17075  903496      228   96563    52
2008-11-17 12:33:56.409   547.424 any      172.16.64.65       25    1505  775164        2   11328   515
2008-11-17 11:22:12.401   133.664 any      172.16.80.13       21     623  742025        4   44411  1191
2008-11-17 09:08:51.542 11256.431 any     213.186.34.222      95    1908  653792        0     464   328
2008-11-17 09:50:17.645   577.244 any      172.16.64.88       12     477  574791        0    7966  1205
2008-11-17 10:31:28.833  4702.016 any      172.16.64.77       41    2350  507288        0     863   215
2008-11-17 11:01:45.425  8060.716 any      172.10.140.3     1681    1956  424094        0     420   216
2008-11-17 09:08:54.562 11212.275 any     91.103.136.102     158     900  344092        0     245   382
2008-11-17 12:03:34.033   136.424 any     213.186.34.205      16     733  332201        5   19480   453
2008-11-17 09:12:30.498  5222.199 any       172.16.97.6       9     296  331024        0     507  1118
2008-11-17 09:21:54.726 10907.571 any       74.125.39.18     118    1286  291462        0     213   226

Summary: total flows: 42283, total bytes: 9.1 G, total packets: 9.7 M, avg bps: 4.7 M, avg pps: 644, avg bpp: 950
Time window: 2008-11-17 08:54:35 - 2008-11-17 13:18:11
Total flows processed: 134065, Records skipped: 0, Bytes read: 6972064
Sys: 0.060s flows/second: 2234305.0  Wall: 0.027s flows/second: 4888423.0
```

3. Statistiques protocole UDP :

3.1. Classement par adresse IP source/bytes :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811170750:nfcapd.200811171210 -n 20 -s srcip/bytes
nfdump filter:
proto udp
Top 20 Src IP Addr ordered by bytes:
Date first seen          Duration Proto      Src IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2008-11-17 09:47:16.385 11495.216 any        172.18.4.2       88   213606  198.5 M       18   144855   974
2008-11-17 11:02:30.413  6870.416 any      172.16.64.89        4   184164   26.3 M       26    32131   149
2008-11-17 08:56:32.562 15336.107 any      172.16.80.1      4929     4996    1.2 M        0      663   254
2008-11-17 09:10:42.478 14687.907 any      172.10.200.3      271     2554  181935         0       99    71
2008-11-17 11:05:50.765   521.380 any      172.16.64.86        1      662   94715         1     1453   143
2008-11-17 11:03:01.529  7777.308 any           0.0.0.0      67      246   80688         0       82   328
2008-11-17 10:50:30.477   752.032 any      172.16.80.21        4      106   34760         0      369   328
2008-11-17 10:06:00.205  9320.560 any       128.8.10.90       52       52   22486         0       19   432
2008-11-17 09:09:15.954  9704.895 any        198.41.0.4       51       51   22436         0       18   439
2008-11-17 10:05:57.105  9257.384 any       192.33.4.12       50       50   21400         0       18   428
2008-11-17 10:06:08.377  9238.840 any      202.12.27.33       56       56   20849         0       18   372
2008-11-17 09:16:35.858 12812.695 any     192.228.79.201      45       45   19178         0       11   426
2008-11-17 10:06:03.257  9325.880 any     192.203.230.10      42       42   18169         0       15   432
2008-11-17 10:06:02.089  6355.564 any      193.0.14.129       42       42   17390         0       21   414
2008-11-17 09:59:42.369  9930.104 any     192.58.128.30       41       41   16570         0       13   404
2008-11-17 10:06:05.217   890.064 any       199.7.83.42       35       35   13690         0      123   391
2008-11-17 08:58:41.650 15400.555 any      172.18.4.202       25       48   11036         0        5   229
2008-11-17 10:06:01.889  9539.392 any      192.48.79.30       39       39   10198         0        8   261
2008-11-17 10:06:03.637  9260.444 any     192.52.178.30       37       37    9726         0        8   262
2008-11-17 10:06:30.297  8910.648 any      192.26.92.30       38       38    9197         0        8   242

Summary: total flows: 60549, total bytes: 229.4 M, total packets: 462110, avg bps: 123873, avg pps: 29, avg bpp: 520
Time window: 2008-11-17 08:54:35 - 2008-11-17 13:18:11
Total flows processed: 134065, Records skipped: 0, Bytes read: 6972064
Sys: 0.064s flows/second: 2094667.4  Wall: 0.031s flows/second: 4191889.2
```

3

.2. Classement par adresse IP destination/bytes :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811170750:nfcapd.200811171210 -n 20 -s dstip/bytes
nfdump filter:
proto udp
Top 20 Dst IP Addr ordered by bytes:
Date first seen          Duration Proto      Dst IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2008-11-17 11:02:30.413  6981.188 any       172.16.64.89        4   212939  198.4 M       30   238344   976
2008-11-17 08:56:32.562 15336.107 any        172.18.4.2    60012   245412   30.6 M       16    16758   130
2008-11-17 09:25:56.445 13773.940 any       172.16.80.1      291     2697   243959        0      141    90
2008-11-17 10:50:38.477  8520.360 any   255.255.255.255       71      352   115456        0      108   328
2008-11-17 11:05:50.769   634.200 any       172.16.64.86        2      462    86276        0     1088   186
2008-11-17 08:58:41.650 15400.555 any       172.18.7.255       23       46    10932        0        5   237
2008-11-17 12:52:32.477     5.016 any       172.18.4.102       21       41     5909        8     9424   144
2008-11-17 09:18:51.937  1205.352 any        192.168.1.1       39       53     3592        0       23    67
2008-11-17 12:52:00.121     5.524 any        172.18.4.1        21       42     2542        7     3615    60
2008-11-17 09:10:42.478 14344.023 any      88.191.80.132       15       15     1140        0        0    76
2008-11-17 09:11:51.486 14344.027 any      88.191.14.30        15       15     1140        0        0    76
2008-11-17 09:11:47.482 14345.027 any      81.25.192.148       15       15     1140        0        0    76
2008-11-17 09:11:13.482 14354.023 any      88.191.20.17        15       15     1140        0        0    76
2008-11-17 12:53:08.517     4.968 any       172.18.4.202        1        2      300        0      483   150
2008-11-17 10:27:40.537  7200.312 any        172.18.32.1        4        4      280        0        0    70

Summary: total flows: 60549, total bytes: 229.4 M, total packets: 462110, avg bps: 123873, avg pps: 29, avg bpp: 520
Time window: 2008-11-17 08:54:35 - 2008-11-17 13:18:11
Total flows processed: 134065, Records skipped: 0, Bytes read: 6972064
Sys: 0.060s flows/second: 2234305.0   Wall: 0.025s flows/second: 5176055.0
```

4. Statistiques protocole ICMP :

4.1. Classement par adresse IP source/bytes :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811170750:nfcapd.200811171210 -n 20 -s srcip/bytes
nfdump filter:
proto icmp
Top 20 Src IP Addr ordered by bytes:
Date first seen          Duration Proto      Src IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2008-11-17 09:47:12.385  2645.172 any       172.16.80.1       21       352   125312        0      378   356
2008-11-17 09:57:46.017 11325.044 any        172.18.4.2       24       974    82731        0       58    84
2008-11-17 10:13:58.417   442.044 any     216.239.59.104        1       443    37212        1      673    84
2008-11-17 09:57:56.881  3178.808 any     209.85.129.147       10       410    34440        0       86    84
2008-11-17 12:32:30.133  1255.484 any      172.16.64.70        3       264    22056        0      140    83
2008-11-17 08:54:46.222 14153.535 any       172.18.4.202       89       155    13943        0        7    89
2008-11-17 10:04:20.069   568.784 any     209.85.129.104        2        66     5544        0       77    84
2008-11-17 11:38:12.657  3476.248 any       172.18.0.22        3         3     3021        0        6  1007
2008-11-17 11:38:12.937  3476.352 any       172.18.0.54        3         3     3021        0        6  1007
2008-11-17 11:38:13.477  3476.956 any      172.18.0.118        3         3     3021        0        6  1007
2008-11-17 11:38:14.561  3478.388 any      172.18.0.246        3         3     3021        0        6  1007
2008-11-17 11:38:14.569  3478.380 any      172.18.0.247        3         3     3021        0        6  1007
2008-11-17 11:38:13.485  3476.948 any      172.18.0.119        3         3     3021        0        6  1007
2008-11-17 11:38:14.577  3478.372 any      172.18.0.248        3         3     3021        0        6  1007
2008-11-17 11:38:14.585  3478.364 any      172.18.0.249        3         3     3021        0        6  1007
2008-11-17 11:38:12.945  3476.348 any       172.18.0.55        3         3     3021        0        6  1007
2008-11-17 11:38:13.493  3476.940 any      172.18.0.120        3         3     3021        0        6  1007
2008-11-17 11:38:14.593  3478.356 any      172.18.0.250        3         3     3021        0        6  1007
2008-11-17 11:38:14.601  3478.348 any      172.18.0.251        3         3     3021        0        6  1007
2008-11-17 11:38:13.501  3477.028 any      172.18.0.121        3         3     3021        0        6  1007

Summary: total flows: 31233, total bytes: 30.1 M, total packets: 33851, avg bps: 16737, avg pps: 2, avg bpp: 933
Time window: 2008-11-17 08:54:35 - 2008-11-17 13:18:11
Total flows processed: 134065, Records skipped: 0, Bytes read: 6972064
Sys: 0.060s flows/second: 2234305.0   Wall: 0.026s flows/second: 5133050.0
```

4.2. Classement par adresse IP destination /bytes:

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811170750:nfcapd.200811171210 -n 20 -s dstip/bytes
nfdump filter:
proto icmp
Top 20 Dst IP Addr ordered by bytes:
Date first seen          Duration Proto      Dst IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2008-11-17 08:54:46.222 15104.091 any         172.18.4.2    31210    32870   30.1 M        2    16693   950
2008-11-17 10:13:58.381   442.040 any     216.239.59.104        1      443   37212        1      673    84
2008-11-17 09:57:56.857  3178.800 any     209.85.129.147       10      410   34440        0       86    84
2008-11-17 10:04:20.045   568.784 any     209.85.129.104        2       66    5544        0       77    84
2008-11-17 09:57:46.017  7247.140 any      209.85.129.99        5       28    2416        0        2    86
2008-11-17 11:01:34.825  4281.416 any       172.16.64.89        2       14    1152        0        2    82
2008-11-17 13:06:24.053     7.008 any      82.241.249.25        1        8     672        1      767    84
2008-11-17 10:21:22.601     1.008 any      72.14.221.104        1        2     168        1     1333    84
2008-11-17 11:02:01.833     5.472 any        172.16.64.1        1        2     120        0      175    60

Summary: total flows: 31233, total bytes: 30.1 M, total packets: 33851, avg bps: 16737, avg pps: 2, avg bpp: 933
Time window: 2008-11-17 08:54:35 - 2008-11-17 13:18:11
Total flows processed: 134065, Records skipped: 0, Bytes read: 6972064
Sys: 0.056s flows/second: 2393089.6  Wall: 0.023s flows/second: 5699800.2
```

5. Statistiques par numéro de port :

5.1. Classement par nombre de paquets :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811170800:nfcapd.200811171200 -n 20 -s port/packets
nfdump filter:
any
Top 20         Port ordered by packets:
Date first seen          Duration Proto          Port    Flows  Packets    Bytes      pps      bps   bpp
2008-11-17 11:01:45.425  7568.676 any              25     5279    6.0 M    5.7 G      833    6.2 M   976
2008-11-17 09:04:39.682 14457.435 any              80     8682    3.1 M    2.8 G      224    1.6 M   938
2008-11-17 10:22:17.713  1615.088 any           58456        5   776761  739.2 M      480    3.7 M   997
2008-11-17 09:23:13.509  1384.272 any           48716        2   773885  736.9 M      559    4.3 M   998
2008-11-17 09:46:20.689  1301.388 any           46320        2   632548  602.9 M      486    3.7 M   999
2008-11-17 10:08:04.145   852.456 any           55120        2   492662  469.3 M      577    4.4 M   998
2008-11-17 11:02:30.413  6981.188 any            1035       16   397132  224.7 M       56  269977   593
2008-11-17 09:44:01.029 11919.752 any           55555      226   191166   92.9 M       16   65348   509
2008-11-17 09:08:07.506 14159.771 any             443    25297   175636   50.3 M       12   29776   300
2008-11-17 09:44:01.029 11919.752 any           48382      113   147780   78.3 M       12   55079   555
2008-11-17 11:33:25.809  4803.228 any             520   107983   109007    5.4 M       22    9206    51
2008-11-17 11:55:37.161   247.172 any           59921        3    61926   57.3 M      250    1.9 M   969
2008-11-17 11:55:37.717   247.868 any           59922        3    59934   55.1 M      241    1.8 M   964
2008-11-17 11:55:37.157   249.428 any           59920        3    56031   53.3 M      225    1.7 M   996
2008-11-17 11:55:42.505   243.076 any           59924        3    54358   50.0 M      223    1.6 M   965
2008-11-17 11:55:42.689   242.896 any           59930        3    53610   49.4 M      220    1.6 M   965
2008-11-17 11:55:43.189   241.144 any           59937        3    53437   49.3 M      221    1.6 M   967
2008-11-17 11:55:43.401   243.176 any           59938        3    52235   47.9 M      214    1.6 M   961
2008-11-17 11:55:42.885   243.696 any           59933        3    51687   47.5 M      212    1.6 M   964
2008-11-17 09:10:21.398   238.296 any           53697        7    51667   50.3 M      216    1.7 M  1020

Summary: total flows: 133839, total bytes: 8.7 G, total packets: 9.6 M, avg bps: 4.9 M, avg pps: 683, avg bpp: 937
Time window: 2008-11-17 09:04:02 - 2008-11-17 13:08:26
Total flows processed: 133839, Records skipped: 0, Bytes read: 5960264
Sys: 0.076s flows/second: 1760946.8  Wall: 0.043s flows/second: 3088402.3
```

5.2. Classement par quantité de données :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811170800:nfcapd.200811171200 -n 20 -s port/bytes
nfdump filter:
any
Top 20        Port ordered by bytes:
Date first seen          Duration Proto             Port    Flows  Packets    Bytes      pps      bps   bpp
2008-11-17 11:01:45.425  7560.676 any                 25     5279    6.0 M    5.7 G      803    6.2 M   976
2008-11-17 09:04:39.682 14457.435 any                 80     8682    3.1 M    2.8 G      224    1.6 M   938
2008-11-17 10:22:17.713  1615.088 any              50456        5  776761  739.2 M      480    3.7 M   997
2008-11-17 09:23:13.509  1384.272 any              48716        2  773885  736.9 M      559    4.3 M   998
2008-11-17 09:46:20.689  1301.388 any              46320        2  632548  602.9 M      486    3.7 M   999
2008-11-17 10:08:04.145   852.456 any              55128        2  492662  469.3 M      577    4.4 M   998
2008-11-17 11:02:30.413  6981.188 any               1035       16  397132  224.7 M       56  269977   593
2008-11-17 09:44:01.029 11919.752 any              55555      226  191166   92.9 M       16   65348   509
2008-11-17 09:44:01.029 11919.752 any              48382      113  147780   78.3 M       12   55079   555
2008-11-17 11:55:37.161   247.172 any              59921        3   61926   57.3 M      250    1.9 M   969
2008-11-17 11:55:37.717   247.868 any              59922        3   59034   55.1 M      241    1.8 M   964
2008-11-17 11:55:37.157   248.428 any              59920        3   56031   53.3 M      225    1.7 M   996
2008-11-17 09:10:21.398   238.296 any              53697        7   51667   50.3 M      216    1.7 M  1020
2008-11-17 09:08:07.506 14159.771 any                443    25297  175636   50.3 M       12   29776   300
2008-11-17 11:55:42.505   243.076 any              59924        3   54358   50.0 M      223    1.6 M   965
2008-11-17 11:55:42.689   242.896 any              59930        3   53610   49.4 M      220    1.6 M   965
2008-11-17 11:55:43.189   241.144 any              59937        3   53437   49.3 M      221    1.6 M   967
2008-11-17 13:05:55.365   117.736 any              52304        3   50405   48.1 M      428    3.3 M  1001
2008-11-17 11:55:43.401   243.176 any              59938        3   52235   47.9 M      214    1.6 M   961
2008-11-17 11:55:42.885   243.696 any              59933        3   51687   47.5 M      212    1.6 M   964

Summary: total flows: 133839, total bytes: 8.7 G, total packets: 9.6 M, avg bps: 4.9 M, avg pps: 683, avg bpp: 937
Time window: 2008-11-17 09:04:02 - 2008-11-17 13:08:26
Total flows processed: 133839, Records skipped: 0, Bytes read: 6960264
Sys: 0.076s flows/second: 1760946.8  Wall: 0.043s flows/second: 3057220.5
```

6. Analyse du trafic entre 7h50 et 12h10 :

6.1. Les machines ayant générées le plus de trafic :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811170750:nfcapd.200811171210 -n 10 -s srcip/bytes
nfdump filter:
any
Top 10 Src IP Addr ordered by bytes:
Date first seen          Duration Proto       Src IP Addr     Flows  Packets    Bytes      pps      bps   bpp
2008-11-17 11:01:45.425  8185.996 any       172.10.4.102      5943    4.4 M    6.2 G      559    6.2 M  1461
2008-11-17 09:23:13.509  5159.292 any     131.246.120.27         6    1.7 M    2.4 G      338    3.9 M  1499
2008-11-17 08:54:35.074 15815.547 any        172.10.4.2     11721    3.6 M  488.5 M      239  259107   135
2008-11-17 09:10:21.398   238.296 any     213.186.33.91         6   34592   49.4 M      145    1.7 M  1498
2008-11-17 09:59:30.957 10649.072 any      172.16.64.89        37  104344   26.3 M       17   20746   149
2008-11-17 09:44:01.029 11919.752 any      172.16.80.73       113   86527   12.3 M        7    8666   149
2008-11-17 11:37:32.269  1685.984 any     205.128.69.126         3    7261   10.3 M        4   51307  1489
2008-11-17 12:01:39.977   204.756 any     198.78.208.125         4    7334   10.3 M       35  421843  1472
2008-11-17 11:50:32.921  3583.408 any      172.16.64.90     16874   76578    6.0 M       21   15917    93
2008-11-17 10:31:28.829  4702.020 any      172.16.64.77       102    3598    4.4 M        0    7887  1288

Summary: total flows: 134065, total bytes: 9.4 G, total packets: 10.2 M, avg bps: 4.8 M, avg pps: 676, avg bpp: 939
Time window: 2008-11-17 08:54:35 - 2008-11-17 13:10:11
Total flows processed: 134065, Records skipped: 0, Bytes read: 6972064
Sys: 0.076s flows/second: 1763920.3  Wall: 0.041s flows/second: 3200253.0
```

6.2. Les machines ayant reçues le plus de trafic :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1 -T -R nfcapd.200811170750:nfcapd.200811171210 -n 10 -s dstip/bytes
nfdump filter:
any
Top 10 Dst IP Addr ordered by bytes:
Date first seen          Duration Proto      Dst IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2008-11-17 08:54:35.870 15815.551 any        172.18.4.2   115062     6.6 M    8.9 G      435    4.6 M  1383
2008-11-17 09:59:30.961 10760.640 any      172.16.64.89       21   213080  198.4 M       19   154700   976
2008-11-17 11:01:45.429  8185.992 any      172.18.4.102     1708    2.3 M  124.5 M      294   127569    54
2008-11-17 09:44:01.029 11919.752 any      172.16.80.73      110   104572   80.5 M        8    56675   807
2008-11-17 09:23:13.509  5159.292 any   131.246.120.27        5   927284   47.3 M      179    76865    53
2008-11-17 11:50:32.929  3583.392 any      172.16.64.90     3772    40609   14.2 M       11    33254   366
2008-11-17 09:12:28.602 13501.435 any      172.16.80.12      337     5957    4.0 M        0     2499   708
2008-11-17 10:08:49.097  9246.104 any      172.16.64.95      185     3041    3.3 M        0     2951  1121
2008-11-17 09:50:12.301  5900.824 any      172.16.97.18      568     6747    3.1 M        1     4380   478
2008-11-17 10:24:37.709  8138.092 any      172.16.64.93       72     1672    1.0 M        0     1051   639

Summary: total flows: 134065, total bytes: 9.4 G, total packets: 10.2 M, avg bps: 4.8 M, avg pps: 676, avg bpp: 939
Time window: 2008-11-17 08:54:35 - 2008-11-17 13:18:11
Total flows processed: 134065, Records skipped: 0, Bytes read: 6972064
Sys: 0.068s flows/second: 1971428.2  Wall: 0.036s flows/second: 3703146.1
```

6.3. Les ports ayant reçues le plus de trafic :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1 -T -R nfcapd.200811170750:nfcapd.200811171210 -n 20 -s dstport/bytes
nfdump filter:
any
Top 20    Dst Port ordered by bytes:
Date first seen          Duration Proto        Dst Port    Flows  Packets    Bytes      pps      bps   bpp
2008-11-17 11:01:45.425  8185.996 any              25     3749     4.4 M    6.2 G      559    6.2 M  1462
2008-11-17 10:22:17.713  1615.088 any           58456        3   507151  725.4 M      314    3.6 M  1499
2008-11-17 09:23:13.509  1384.260 any           48716        1   505569  723.2 M      365    4.2 M  1499
2008-11-17 09:46:20.689  1301.384 any           46320        1   413776  591.7 M      317    3.6 M  1499
2008-11-17 10:08:04.145   852.452 any           55128        1   322076  460.6 M      377    4.3 M  1499
2008-11-17 08:54:35.870 15661.763 any              80     4553     1.1 M  253.7 M       76  135907   220
2008-11-17 09:44:01.029 11919.752 any           48382       56    78386   67.0 M        6   47118   895
2008-11-17 09:10:21.390   230.296 any           53697        6    34592   49.4 M      145    1.7 M  1490
2008-11-17 08:54:46.222 15104.839 any            2048    31180    32483   29.9 M        2   15626   966
2008-11-17 11:02:30.413  6870.416 any            1035        7   184179   26.3 M       26   32141   149
2008-11-17 08:58:31.750 15335.563 any             443    19901   107224   18.0 M        6    9867   176
2008-11-17 09:44:01.029 11919.752 any           55555      113    86558   12.3 M        7    8669   149
2008-11-17 10:50:15.233  7933.288 any           46218       34    19175   11.5 M        2   12178   629
2008-11-17 11:25:13.505  4740.136 any            1405        4     7268   10.3 M        1   18250  1487
2008-11-17 12:02:57.125  2539.164 any            2157        2     7317   10.3 M        2   33928  1471
2008-11-17 11:33:25.809  4803.228 any             520    53992    54504    2.7 M       11    4643    51
2008-11-17 09:33:33.861   164.456 any           35527        3     1597    2.2 M        9  111632  1436
2008-11-17 10:48:39.381   140.124 any           46706        3     1562    2.1 M       11  127113  1425
2008-11-17 09:51:46.049  7179.008 any           49100       21     7012    2.1 M        0    2409   308
2008-11-17 11:50:39.237  2600.508 any            1183        3     1451    2.0 M        0    6509  1458

Summary: total flows: 134065, total bytes: 9.4 G, total packets: 10.2 M, avg bps: 4.8 M, avg pps: 676, avg bpp: 939
Time window: 2008-11-17 08:54:35 - 2008-11-17 13:18:11
Total flows processed: 134065, Records skipped: 0, Bytes read: 6972064
Sys: 0.072s flows/second: 1861910.4  Wall: 0.038s flows/second: 3483384.0
```

6.4. Un résumé des plus gros échanges de la confrontation

Les échanges les plus volumineux en termes de paquets :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811170650:nfcapd.200811171110 -n 50 -s record/byt
nfdump filter:
any
Aggregated flows 24871
Top 50 flows ordered by bytes:
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags Tos  Packets    Bytes Flows
2008-11-17 10:22:17.713  1615.088 TCP     131.246.120.27:80    ->       172.18.4.2:58456 .AP.SF   0   507151  725.4 M     3
2008-11-17 09:23:13.509  1384.260 TCP     131.246.120.27:80    ->       172.18.4.2:48716 .AP.S.   0   505569  723.2 M     1
2008-11-17 09:46:20.689  1301.384 TCP     131.246.120.27:80    ->       172.18.4.2:46320 .AP.S.   0   413776  591.7 M     1
2008-11-17 10:08:04.145   852.452 TCP     131.246.120.27:80    ->       172.18.4.2:55128 .AP.S.   0   322076  460.6 M     1
2008-11-17 11:02:30.413  3600.648 UDP        172.18.4.2:1035   ->     172.16.64.89:80     .A....   0   100128   95.0 M     2
2008-11-17 11:55:37.161   247.172 TCP      172.18.4.102:59921 ->       172.18.4.2:25     .AP.SF   0    40204   56.1 M     1
2008-11-17 11:55:37.717   247.868 TCP      172.18.4.102:59922 ->       172.18.4.2:25     .AP.SF   0    38710   54.0 M     1
2008-11-17 11:55:37.157   248.428 TCP      172.18.4.102:59920 ->       172.18.4.2:25     .AP.SF   0    37449   52.3 M     1
2008-11-17 09:10:21.398   238.296 TCP      213.186.33.91:80   ->       172.18.4.2:53697 .AP.SF   0    34592   49.4 M     6
2008-11-17 11:55:42.505   243.076 TCP      172.18.4.102:59924 ->       172.18.4.2:25     .AP.SF   0    35141   49.0 M     1
2008-11-17 11:55:42.689   242.896 TCP      172.18.4.102:59930 ->       172.18.4.2:25     .AP.SF   0    34670   48.4 M     1
2008-11-17 11:55:43.189   241.144 TCP      172.18.4.102:59937 ->       172.18.4.2:25     .AP.SF   0    34634   48.4 M     1
2008-11-17 11:55:43.401   243.176 TCP      172.18.4.102:59938 ->       172.18.4.2:25     .AP.SF   0    33608   46.9 M     1
2008-11-17 11:55:42.885   243.696 TCP      172.18.4.102:59933 ->       172.18.4.2:25     .AP.SF   0    33393   46.6 M     1
2008-11-17 11:55:42.981   243.600 TCP      172.18.4.102:59934 ->       172.18.4.2:25     .AP.SF   0    33136   46.2 M     1
2008-11-17 11:55:37.717   247.872 TCP      172.18.4.102:59923 ->       172.18.4.2:25     .AP.SF   0    33133   46.2 M     1
2008-11-17 11:55:43.153   242.432 TCP      172.18.4.102:59935 ->       172.18.4.2:25     .AP.SF   0    32832   45.8 M     1
2008-11-17 11:55:42.541   244.036 TCP      172.18.4.102:59928 ->       172.18.4.2:25     .AP.SF   0    32617   45.5 M     1
2008-11-17 11:55:43.405   240.932 TCP      172.18.4.102:59939 ->       172.18.4.2:25     .AP.SF   0    32586   45.5 M     1
2008-11-17 11:55:42.509   244.068 TCP      172.18.4.102:59927 ->       172.18.4.2:25     .AP.SF   0    32349   45.1 M     1
2008-11-17 11:55:43.153   242.432 TCP      172.18.4.102:59936 ->       172.18.4.2:25     .AP.SF   0    32086   44.8 M     1
2008-11-17 11:55:42.505   244.072 TCP      172.18.4.102:59925 ->       172.18.4.2:25     .AP.SF   0    31856   44.5 M     1
2008-11-17 11:55:42.601   243.976 TCP      172.18.4.102:59929 ->       172.18.4.2:25     .AP.SF   0    31593   44.1 M     1
2008-11-17 11:55:42.509   241.824 TCP      172.18.4.102:59926 ->       172.18.4.2:25     .AP.SF   0    31595   44.1 M     1
2008-11-17 11:55:42.689   242.896 TCP      172.18.4.102:59931 ->       172.18.4.2:25     .AP.SF   0    31343   43.7 M     1
2008-11-17 11:55:42.881   241.452 TCP      172.18.4.102:59932 ->       172.18.4.2:25     .AP.SF   0    29807   41.6 M     1
2008-11-17 09:44:01.029  8495.248 TCP        172.18.4.2:55555 ->     172.16.80.73:48382 .AP.S.   0    48749   41.1 M    52
2008-11-17 11:59:50.525   149.996 TCP      172.18.4.102:60945 ->       172.18.4.2:25     .AP.SF   0    20848   29.1 M     2
2008-11-17 11:59:50.525   151.844 TCP      172.18.4.102:60946 ->       172.18.4.2:25     .AP.SF   0    20615   28.8 M     1
2008-11-17 11:59:50.601   150.776 TCP      172.18.4.102:60948 ->       172.18.4.2:25     .AP.SF   0    19589   27.4 M     1
2008-11-17 11:59:49.933   152.436 TCP      172.18.4.102:60943 ->       172.18.4.2:25     .AP.SF   0    19344   27.0 M     1
2008-11-17 11:59:50.597   151.776 TCP      172.18.4.102:60947 ->       172.18.4.2:25     .AP.SF   0    18590   26.0 M     1
2008-11-17 11:59:58.709   142.668 TCP      172.18.4.102:60956 ->       172.18.4.2:25     .AP.SF   0    18582   25.9 M     1
2008-11-17 11:59:57.473   144.904 TCP      172.18.4.102:60954 ->       172.18.4.2:25     .AP.SF   0    17823   24.9 M     1
2008-11-17 11:59:49.993   151.440 TCP      172.18.4.102:60944 ->       172.18.4.2:25     .AP.SF   0    17312   24.2 M     1
2008-11-17 11:59:55.757   146.620 TCP      172.18.4.102:60949 ->       172.18.4.2:25     .AP.SF   0    17041   23.8 M     1
2008-11-17 12:00:00.193   141.180 TCP      172.18.4.102:60957 ->       172.18.4.2:25     .AP.SF   0    17041   23.8 M     1
2008-11-17 11:59:57.593   142.928 TCP      172.18.4.102:60955 ->       172.18.4.2:25     .AP.SF   0    17060   23.8 M     2
2008-11-17 11:45:50.489    18.620 TCP      172.18.4.102:35398 ->       172.18.4.2:25     .AP.SF   0    16715   23.4 M     1
2008-11-17 11:59:57.469   143.908 TCP      172.18.4.102:60953 ->       172.18.4.2:25     .AP.SF   0    16551   23.1 M     1
2008-11-17 11:59:57.469   143.904 TCP      172.18.4.102:60952 ->       172.18.4.2:25     .AP.SF   0    16561   23.1 M     1
2008-11-17 11:59:55.757   144.768 TCP      172.18.4.102:60950 ->       172.18.4.2:25     .AP.SF   0    16297   22.7 M     2
2008-11-17 11:59:56.977   145.392 TCP      172.18.4.102:60951 ->       172.18.4.2:25     .AP.SF   0    16027   22.4 M     1
2008-11-17 11:43:21.781    15.260 TCP      172.18.4.102:35297 ->       172.18.4.2:25     .AP.SF   0    15730   22.1 M     1
2008-11-17 12:00:02.357   140.008 TCP      172.18.4.102:60962 ->       172.18.4.2:25     .AP.SF   0    15805   22.0 M     1
2008-11-17 11:41:10.813    16.032 TCP      172.18.4.102:50950 ->       172.18.4.2:25     .AP.SF   0    15694   22.0 M     1
2008-11-17 12:00:01.677   139.692 TCP      172.18.4.102:60960 ->       172.18.4.2:25     .AP.SF   0    15271   21.3 M     1
2008-11-17 11:52:44.501    41.820 TCP      172.18.4.102:45523 ->       172.18.4.2:25     .AP.SF   0    15002   21.0 M     1
2008-11-17 11:41:32.873    18.940 TCP      172.18.4.102:50977 ->       172.18.4.2:25     .AP.SF   0    14940   20.9 M     1
2008-11-17 12:15:54.905    70.744 TCP      172.18.4.102:34856 ->       172.18.4.2:25     .AP.SF   0    14474   20.3 M     1

Summary: total flows: 30628, total bytes: 6.3 G, total packets: 6.7 M, avg bps: 3.2 M, avg pps: 443, avg bpp: 956
Time window: 2008-11-17 07:53:58 - 2008-11-17 12:18:25
Total flows processed: 30628, Records skipped: 0, Bytes read: 1593292
Sys: 0.068s flows/second: 450385.3   Wall: 0.031s flows/second: 963205.2
```

Les échanges les plus volumineux en termes de paquets :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811170650:nfcapd.200811171110 -n 20 -s record/ps
nfdump filter:
any
Aggregated flows 24871
Top 20 flows ordered by packets:
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags Tos  Packets    Bytes Flows
2008-11-17 10:22:17.713  1615.088 TCP     131.246.120.27:80     ->       172.18.4.2:58456 .AP.SF   0   507151  725.4 M     3
2008-11-17 09:23:13.509  1384.260 TCP     131.246.120.27:80     ->       172.18.4.2:48716 .AP.S.   0   505569  723.2 M     1
2008-11-17 09:46:20.689  1301.384 TCP     131.246.120.27:80     ->       172.18.4.2:46320 .AP.S.   0   413776  591.7 M     1
2008-11-17 10:08:04.145   852.452 TCP     131.246.120.27:80     ->       172.18.4.2:55128 .AP.S.   0   322076  460.6 M     1
2008-11-17 10:22:17.717  1615.084 TCP        172.18.4.2:58456 ->   131.246.120.27:80    .AP..F   0   269610   13.8 M     2
2008-11-17 09:23:13.509  1384.272 TCP        172.18.4.2:48716 ->   131.246.120.27:80    .APR..   0   268316   13.7 M     1
2008-11-17 09:46:20.693  1301.384 TCP        172.18.4.2:46320 ->   131.246.120.27:80    .APR.F   0   218772   11.1 M     1
2008-11-17 10:08:04.149   852.452 TCP        172.18.4.2:55128 ->   131.246.120.27:80    .APR..   0   170586    8.7 M     1
2008-11-17 11:02:30.413  3600.648 UDP        172.18.4.2:1035  ->     172.16.64.89:80    .A....   0   102128   95.0 M     2
2008-11-17 11:02:30.413  3600.724 UDP      172.16.64.89:80     ->       172.18.4.2:1035  .A....   0    87955   12.9 M     2
2008-11-17 09:44:01.029  8495.248 TCP        172.18.4.2:55555 ->   172.16.80.73:48382 .AP.S.   0    48749   41.1 M    52
2008-11-17 09:44:01.029  8495.248 TCP      172.16.80.73:48382 ->       172.18.4.2:55555 .AP.S.   0    42947    7.1 M    52
2008-11-17 11:55:37.161   247.172 TCP      172.18.4.102:59921 ->       172.18.4.2:25    .AP.SF   0    40204   56.1 M     1
2008-11-17 11:55:37.717   247.868 TCP      172.18.4.102:59922 ->       172.18.4.2:25    .AP.SF   0    38710   54.0 M     1
2008-11-17 11:55:37.157   248.428 TCP      172.18.4.102:59920 ->       172.18.4.2:25    .AP.SF   0    37449   52.3 M     1
2008-11-17 11:55:42.505   243.076 TCP      172.18.4.102:59924 ->       172.18.4.2:25    .AP.SF   0    35141   49.0 M     1
2008-11-17 11:55:42.689   242.896 TCP      172.18.4.102:59930 ->       172.18.4.2:25    .AP.SF   0    34670   48.4 M     1
2008-11-17 11:55:43.189   241.144 TCP      172.18.4.102:59937 ->       172.18.4.2:25    .AP.SF   0    34634   48.4 M     1
2008-11-17 09:10:21.898   238.296 TCP     213.186.33.91:80     ->       172.18.4.2:53697 .AP.SF   0    34593   49.4 M     6
2008-11-17 11:55:43.401   243.176 TCP      172.18.4.102:59938 ->       172.18.4.2:25    .AP.SF   0    33608   46.9 M     1

Summary: total flows: 30628, total bytes: 6.3 G, total packets: 6.7 M, avg bps: 3.2 M, avg pps: 443, avg bpp: 956
Time window: 2008-11-17 07:53:58 - 2008-11-17 12:18:25
Total flows processed: 30628, Records skipped: 0, Bytes read: 1593292
Sys: 0.064s flows/second: 478540.1   Wall: 0.031s flows/second: 980692.3
```

On retrouve ici les même machines que celles qui sont à l'origine de la plus grosse quantité de données transférées à quelques exceptions près :

La machine 172.16.64.89 :80 à destination du routeur sur le port 1035 , a émis beaucoup de paquets mais une quantité faibles de données 12,9Mo.

6.5. Les activités anormales :

```
2008-11-17 11:01:50.621     7.640 TCP      172.18.4.102:36362 ->      172.18.4.2:25     .AP.SF  0     767    1.1 M     1
2008-11-17 11:01:50.621     7.640 TCP      172.18.4.102:36361 ->      172.18.4.2:25     .AP.SF  0     513    744754    1
2008-11-17 11:01:50.625     7.636 TCP        172.18.4.2:25    ->   172.18.4.102:36361 .AP.SF  0     209    12565     1
2008-11-17 11:01:50.625     7.636 TCP        172.18.4.2:25    ->   172.18.4.102:36362 .AP.SF  0     364    19986     1
2008-11-17 11:01:51.157     0.000 TCP      172.18.4.102:36364 ->   172.10.140.3:25     ....S.  0     1      60        1
2008-11-17 11:01:51.157     7.104 TCP      172.18.4.102:36363 ->      172.18.4.2:25     .AP.SF  0     259    372554    1
2008-11-17 11:01:51.157    12.348 TCP      172.18.4.102:36364 ->      172.18.4.2:25     .AP.SF  0     259    372554    1
2008-11-17 11:01:51.157     0.000 TCP      172.18.4.102:36363 ->   172.10.140.3:25     ....S.  0     1      60        1
2008-11-17 11:01:51.161    12.344 TCP        172.18.4.2:25    ->   172.18.4.102:36364 .AP.SF  0     135    7228      1
2008-11-17 11:01:51.161     7.100 TCP        172.18.4.2:25    ->   172.18.4.102:36363 .AP.SF  0     134    7176      1
2008-11-17 11:01:55.801     0.000 TCP      172.18.4.102:36365 ->   172.10.140.3:25     ....S.  0     1      60        1
2008-11-17 11:01:55.801     7.704 TCP      172.18.4.102:36365 ->      172.18.4.2:25     .AP.SF  0     259    372554    1
2008-11-17 11:01:55.813     7.692 TCP        172.18.4.2:25    ->   172.18.4.102:36365 .AP.SF  0     135    7228      1
2008-11-17 11:01:55.917     0.000 TCP      172.18.4.102:36366 ->   172.10.140.3:25     ....S.  0     1      60        1
2008-11-17 11:01:55.917    12.588 TCP        172.18.4.2:25    ->   172.18.4.102:36366 .AP.SF  0     135    7228      1
2008-11-17 11:01:55.917    12.588 TCP      172.18.4.102:36366 ->      172.18.4.2:25     .AP.SF  0     259    372554    1
2008-11-17 11:01:55.925     0.000 TCP      172.18.4.102:36367 ->   172.10.140.3:25     ....S.  0     1      60        1
2008-11-17 11:01:55.925    12.580 TCP      172.18.4.102:36367 ->      172.18.4.2:25     .AP.SF  0     259    372554    1
2008-11-17 11:01:55.961     7.544 TCP      172.18.4.102:36368 ->      172.18.4.2:25     .AP.SF  0     259    372554    1
2008-11-17 11:01:55.961    12.544 TCP      172.18.4.102:36369 ->      172.18.4.2:25     .AP.SF  0     259    372554    1
2008-11-17 11:01:55.961     0.000 TCP      172.18.4.102:36368 ->   172.10.140.3:25     ....S.  0     1      60        1
2008-11-17 11:01:55.965     0.000 TCP      172.18.4.102:36369 ->   172.10.140.3:25     ....S.  0     1      60        1
2008-11-17 11:01:55.969     0.000 TCP      172.18.4.102:36370 ->   172.10.140.3:25     ....S.  0     1      60        1
2008-11-17 11:01:55.969     7.536 TCP      172.18.4.102:36370 ->      172.18.4.2:25     .AP.SF  0     259    372554    1
2008-11-17 11:01:56.025    12.480 TCP        172.18.4.2:25    ->   172.18.4.102:36367 .AP.SF  0     135    7228      1
2008-11-17 11:01:56.049     7.456 TCP        172.18.4.2:25    ->   172.18.4.102:36368 .AP.SF  0     135    7228      1
2008-11-17 11:01:56.085    12.420 TCP        172.18.4.2:25    ->   172.18.4.102:36369 .AP.SF  0     135    7228      1
2008-11-17 11:01:56.085     7.420 TCP        172.18.4.2:25    ->   172.18.4.102:36370 .AP.SF  0     135    7228      1
2008-11-17 11:01:57.193     0.000 TCP      172.18.4.202:4628  ->      172.18.4.2:22     ....S.  0     1      60        1
2008-11-17 11:02:01.833     5.472 ICMP       172.18.4.2:0     ->   172.16.64.1:8.0      .A....  0     2      120       1
2008-11-17 11:02:01.833     5.472 ICMP     172.16.64.1:0      ->      172.18.4.2:0.0    .A....  0     2      120       1
2008-11-17 11:02:01.841     0.236 TCP      74.125.39.18:80    ->      172.18.4.2:50352  .AP.SF  0     5      1613      1
2008-11-17 11:02:01.841     0.236 TCP        172.18.4.2:50352 ->   74.125.39.18:80      .AP..F  0     4      1035      1
2008-11-17 11:02:02.117     0.000 UDP      172.16.80.1:53     ->      172.18.4.2:27520  .A....  0     1      139       1
```

Nombreuses requêtes smtp depuis 172.18.4.102.

```
2008-11-17 09:25:22.433     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:49148  .A....  0     1      131       1
2008-11-17 09:25:22.433     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:41812  .A....  0     1      131       1
2008-11-17 09:25:22.445     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:50675  .A....  0     1      133       1
2008-11-17 09:25:22.445     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:43231  .A....  0     1      133       1
2008-11-17 09:25:22.457     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:58808  .A....  0     1      117       1
2008-11-17 09:25:22.457     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:50042  .A....  0     1      255       1
2008-11-17 09:25:22.461     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:60909  .A....  0     1      132       1
2008-11-17 09:25:22.465     0.132 TCP      217.117.154.3:80     ->      172.18.4.2:43589  .AP.SF  0     5      792       1
2008-11-17 09:25:22.469     0.128 TCP        172.18.4.2:43589   ->   217.117.154.3:80     .AP..F  0     5      916       1
2008-11-17 09:25:22.501     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:38388  .A....  0     1      142       1
2008-11-17 09:25:22.589     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:54813  .A....  0     1      393       1
2008-11-17 09:25:22.589     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:43130  .A....  0     1      153       1
2008-11-17 09:25:22.593     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:46203  .A....  0     1      127       1
2008-11-17 09:25:22.593     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:36435  .A....  0     1      153       1
2008-11-17 09:25:22.593     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:43189  .A....  0     1      393       1
2008-11-17 09:25:22.597  6297.660 UDP        172.16.80.1:53     ->      172.18.4.2:49924  .A....  0     2      250       2
2008-11-17 09:25:22.597     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:44728  .A....  0     1      175       1
2008-11-17 09:25:22.601     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:47734  .A....  0     1      127       1
2008-11-17 09:25:22.601     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:38215  .A....  0     1      140       1
2008-11-17 09:25:22.601     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:37649  .A....  0     1      125       1
2008-11-17 09:25:26.621     0.068 TCP      172.18.4.202:3905    ->      172.18.4.2:80     .AP.SF  0     4      296       1
2008-11-17 09:25:26.621     0.068 TCP        172.18.4.2:80      ->   172.18.4.202:3905    .AP.SF  0     5      701       1
2008-11-17 09:25:26.621     0.000 TCP      172.18.4.202:3905    ->   172.18.140.2:80      ....S.  0     1      60        1
2008-11-17 09:25:27.593     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:49284  .A....  0     1      140       1
2008-11-17 09:25:27.597     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:52673  .A....  0     1      175       1
2008-11-17 09:25:27.597     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:49634  .A....  0     1      140       1
2008-11-17 09:25:27.597     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:43340  .A....  0     1      175       1
2008-11-17 09:25:27.605     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:35622  .A....  0     1      140       1
2008-11-17 09:25:27.609     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:54319  .A....  0     1      175       1
2008-11-17 09:25:27.609     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:60955  .A....  0     1      175       1
2008-11-17 09:25:27.609     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:50259  .A....  0     1      175       1
2008-11-17 09:25:27.609     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:57603  .A....  0     1      175       1
2008-11-17 09:25:27.613     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:34482  .A....  0     1      140       1
2008-11-17 09:25:27.621     0.000 UDP        172.16.80.1:53     ->      172.18.4.2:45626  .A....  0     1      393       1
2008-11-17 09:25:27.621     0.236 TCP      72.232.69.5:80       ->      172.18.4.2:56212  .AP.SF  0     6      7932      1
```

Comme lors de la confrontation précédente on observe un scan de port de puis 172.16.80.1.

2008-11-17 09:45:41.957	0.000	UDP	172.16.80.1:53	->	172.18.4.2:27056	.A....	0	1	390	1
2008-11-17 09:45:41.957	0.000	UDP	172.16.80.1:53	->	172.18.4.2:18205	.A....	0	1	166	1
2008-11-17 09:45:41.965	0.000	UDP	172.16.80.1:53	->	172.18.4.2:62666	.A....	0	1	363	1
2008-11-17 09:45:41.965	0.000	UDP	172.16.80.1:53	->	172.18.4.2:8844	.A....	0	1	139	1
2008-11-17 09:45:41.973	0.000	UDP	172.16.80.1:53	->	172.18.4.2:2292	.A....	0	1	390	1
2008-11-17 09:45:41.977	0.000	UDP	172.16.80.1:53	->	172.18.4.2:10854	.A....	0	1	363	1
2008-11-17 09:45:41.989	24.592	TCP	172.18.4.2:43989	->	209.85.129.104:80	.AP..F	0	12	1166	2
2008-11-17 09:45:41.989	24.588	TCP	209.85.129.104:80	->	172.18.4.2:43989	.AP.SF	0	11	9812	2
2008-11-17 09:45:41.993	61.088	TCP	172.18.4.2:51902	->	209.85.129.147:80	.AP..F	0	9	969	2
2008-11-17 09:45:41.993	61.088	TCP	172.18.4.2:55920	->	209.85.129.99:80	.AP..F	0	12	1166	2
2008-11-17 09:45:41.993	61.088	TCP	209.85.129.147:80	->	172.18.4.2:51902	.AP.SF	0	8	5273	2
2008-11-17 09:45:41.993	61.088	TCP	209.85.129.99:80	->	172.18.4.2:55920	.AP.SF	0	11	9812	2
2008-11-17 09:46:09.601	0.000	UDP	172.16.80.1:53	->	172.18.4.2:63186	.A....	0	1	142	1
2008-11-17 09:46:20.689	1301.384	TCP	131.246.120.27:80	->	172.18.4.2:46320	.AP.S.	0	413776	591.7 M	1
2008-11-17 09:46:20.693	1301.384	TCP	172.18.4.2:46320	->	131.246.120.27:80	.APR.F	0	218772	11.1 M	1
2008-11-17 09:46:51.253	0.000	UDP	172.16.80.1:53	->	172.18.4.2:6248	.A....	0	1	395	1
2008-11-17 09:46:51.257	0.000	UDP	172.16.80.1:53	->	172.18.4.2:60053	.A....	0	1	363	1
2008-11-17 09:46:51.273	119.768	TCP	209.85.129.104:80	->	172.18.4.2:1781	.AP.SF	0	5	944	2
2008-11-17 09:46:51.277	119.764	TCP	172.18.4.2:1781	->	209.85.129.104:80	.AP..F	0	5	685	2
2008-11-17 09:46:51.541	0.000	UDP	172.16.80.1:53	->	172.18.4.2:10402	.A....	0	1	363	1
2008-11-17 09:46:51.569	134.480	TCP	209.85.129.99:80	->	172.18.4.2:1782	.AP.SF	0	5	1030	3
2008-11-17 09:46:51.577	134.472	TCP	172.18.4.2:1782	->	209.85.129.99:80	.AP..F	0	5	678	2
2008 11 17 09:46:51.905	0.000	UDP	172.16.80.1:53	>	172.18.4.2:0000	.A....	0	1	390	1
2008-11-17 09:46:51.913	0.000	UDP	172.16.80.1:53	->	172.18.4.2:1129	.A....	0	1	363	1
2008-11-17 09:46:51.949	149.116	TCP	209.85.129.147:80	->	172.18.4.2:1783	.AP.SF	0	28	24445	4
2008-11-17 09:46:51.957	149.108	TCP	172.18.4.2:1783	->	209.85.129.147:80	.AP..F	0	21	4281	3
2008-11-17 09:46:52.037	0.000	UDP	172.16.80.1:53	->	172.18.4.2:59065	.A....	0	1	346	1
2008-11-17 09:46:53.041	0.000	UDP	172.16.80.1:53	->	172.18.4.2:49206	.A....	0	1	310	1
2008-11-17 09:46:52.077	133.968	TCP	172.18.4.2:1784	->	63.245.209.121:80	.AP..F	0	5	680	2
2008-11-17 09:46:52.077	133.968	TCP	63.245.209.121:80	->	172.18.4.2:1784	.AP.SF	0	5	933	3
2008-11-17 09:46:52.097	148.968	TCP	209.85.129.147:80	->	172.18.4.2:1785	.AP.SF	0	22	18310	4
2008 11 17 09:46:52.101	140.964	TCP	172.10.4.2:1785	>	209.05.129.147:00	.AP..F	0	16	2074	3
2008-11-17 09:46:52.461	0.000	UDP	172.16.80.1:53	->	172.18.4.2:20276	.A....	0	1	473	1
2008-11-17 09:46:52.465	0.000	UDP	172.16.80.1:53	->	172.18.4.2:8954	.A....	0	1	445	1
2008-11-17 09:46:52.469	0.000	UDP	172.16.80.1:53	->	172.18.4.2:15341	.A....	0	1	412	1

Transfert pour le moins étrange, que l'on retrouve dans le résumé des plus grosses activités de la confrontation.

Nous avons donc pu observer beaucoup de trafic polluant venant des attaquants, ayant pour but de noyer le réseau de trames inutiles, afin de saturer le routeur, dissimuler une attaque sous un flux de données important, et tenter de détecter des failles de sécurités (ports du routeurs ouverts…).

Nous avons recensé une activité anormale sur le serveur de mail notamment. Hormis le scannage de port habituel, nous avons principalement observé le transfert de grosse quantité de données, et l'envoi de nombreux paquets de faible poids.

3. Rapport NetFlow : 2ème confrontation

L'outil NetFlow permet principalement d'effectuer des statistiques à partir de données collectées par le routeur Cisco de l'équipe défense. Cet outil ne permet pas une analyse approfondie mais seulement une vue globale des communications entre le réseau de la défense et « l'extérieur ». De plus les résultats obtenus sont sous forme de fichiers d'enregistrements de 5 min, on constatera que les fichiers les plus volumineux font 108Mo au max, on peut supposer que le routeur était en surcharge et à donc chuinter une partie des flows.

1. Statistiques générales durant la confrontation du 03/11/08 :

1.1. Statistiques générales, total :

Statistics timeslot Nov 03 2008 - 07:00 - Nov 03 2008 - 11:10

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
upstream1	310.9 k	151.7 k	139.1 k	20.1 k	0	438.9 k	264.0 k	140.5 k	34.5 k	0	125.1 MB	85.2 MB	8.5 MB	31.4 MB	0 B

All None Display: Sum Rate

1.2. Statistiques générales : taux :

Statistics timeslot Nov 03 2008 - 07:00 - Nov 03 2008 - 11:10

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
upstream1	20.3 /s	9.9 /s	9.1 /s	1.3 /s	0 /s	28.7 /s	17.3 /s	9.2 /s	2.3 /s	0 /s	65.4 kb/s	44.6 kb/s	4.4 kb/s	16.4 kb/s	0 b/s

All None Display: Sum Rate

2. Statistiques protocole TCP :

2.1. Classement par adresse IP Source :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811030700:nfcapd.200811031110 -n 20 -s srcip/flows
nfdump filter:
proto TCP
Top 20 Src IP Addr ordered by flows:
Date first seen          Duration Proto      Src IP Addr    Flows  Packets    Bytes      pps      bps  bpp
2008-11-03 10:15:43.393  6399.567 any       172.16.64.96   114494   114504    4.8 M       17     6290   44
2008-11-03 11:09:47.556  3632.548 any       172.18.4.101    12927    15696    1.0 M        4     2357   68
2008-11-03 10:34:29.461  2639.579 any       172.16.64.66     6838     7392   448217        2     1358   60
2008-11-03 10:59:19.516  4604.760 any       172.18.4.103     5220     5283   246401        1      428   46
2008-11-03 08:03:21.873 15156.863 any         172.18.4.2     4130    49516    11.1 M        3     6140  234
2008-11-03 11:49:02.812  1616.184 any       172.16.64.83     2706     7197   373812        4     1850   51
2008-11-03 10:40:04.597  5663.495 any       172.16.64.92     1078     1086    48688        0       68   44
2008-11-03 09:28:56.937  9636.267 any       172.16.80.20      578     2729   653067        0      542  239
2008-11-03 10:17:45.857  7056.927 any       172.16.64.95      408     2385   341537        0      387  143
2008-11-03 08:03:21.869 15122.719 any       172.18.4.202      263      637    36868        0       19   57
2008-11-03 11:00:24.272  4280.188 any       172.16.64.67      138      608   112432        0      210  184
2008-11-03 10:34:04.053  5815.795 any       172.16.64.86       89     4609    5.8 M        0     8321 1312
2008-11-03 10:13:07.433  7371.299 any       172.16.64.78       82      480    88970        0       96  185
2008-11-03 09:09:06.789 10905.575 any      209.85.129.99       79      413   179364        0      131  434
2008-11-03 09:24:37.785  9408.599 any      193.51.224.14       70     1704    1.5 M        0     1329  917
2008-11-03 09:24:35.465  7498.543 any      209.85.129.104      64      280    77651        0       82  277
2008-11-03 09:22:22.689  8744.639 any      209.85.129.147      64      334   141716        0      129  424
2008-11-03 09:27:08.213  8344.263 any      209.62.179.182      62      676   808596        0      775 1196
2008-11-03 09:24:38.105 10166.679 any       193.51.224.8       61     1911    1.6 M        0     1315  874
2008-11-03 11:21:24.020  2459.012 any       172.16.80.22       59      265    48528        0      157  183

Summary: total flows: 151684, total bytes: 81.3 M, total packets: 263986, avg bps: 44961, avg pps: 17, avg bpp: 322
Time window: 2008-11-03 08:01:03 - 2008-11-03 12:16:04
Total flows processed: 310930, Records skipped: 0, Bytes read: 16169104
Sys: 0.076s flows/second: 4090968.9  Wall: 0.062s flows/second: 4953323.1
```

2.2. Classement par adresse IP destination :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811030700:nfcapd.200811031110 -n 20 -s dstip/flows
nfdump filter:
proto TCP
Top 20 Dst IP Addr ordered by flows:
Date first seen          Duration Proto      Dst IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2008-11-03 08:03:21.869 15162.415 any         172.18.4.2   146184   213049   70.1 M       14    38772   344
2008-11-03 08:03:21.869 15151.367 any       172.10.140.2     1068     1097    61264        0       32    55
2008-11-03 11:43:33.876  1602.600 any       172.18.4.101      368     2585   810526        1     4046   313
2008-11-03 08:50:08.069  8551.347 any       172.10.200.3      291      302    18064        0       16    59
2008-11-03 10:35:40.725  2183.623 any       172.16.64.66      286     1121    97313        0      356    86
2008-11-03 09:28:56.941  9636.263 any       172.16.80.20      226     2315    1.7 M        0     1468   764
2008-11-03 11:26:36.112  2926.672 any       172.16.64.95      211     2834    2.4 M        0     6960   898
2008-11-03 09:24:37.769  9683.843 any      193.51.224.14       83     1566   399567        0      330   255
2008-11-03 11:26:47.740  2720.788 any       172.16.64.86       79     2807   268851        1      790    95
2008-11-03 11:27:34.544  2649.916 any       172.16.64.67       77      434   211929        0      639   488
2008-11-03 09:27:08.181  8413.871 any     209.62.179.182       72      639    73532        0       69   115
2008-11-03 08:03:21.873 15122.715 any       172.18.4.202       70      248    28331        0       14   114
2008-11-03 09:33:04.437  9730.507 any       193.51.224.7       68      696    87372        0       71   125
2008-11-03 09:24:38.093 10226.851 any       193.51.224.8       62     1771   544691        0      426   307
2008-11-03 09:09:06.761 10907.531 any      209.85.129.99       55      323    47973        0       35   148
2008-11-03 11:26:30.320  2968.416 any       172.16.64.78       54      458   222475        0      599   485
2008-11-03 09:08:00.277  8933.139 any       212.27.32.66       53     5922   361131        0      323    60
2008-11-03 09:24:42.301 10257.799 any      193.51.224.17       53      776   135254        0      105   174
2008-11-03 09:24:39.813  9681.799 any      209.62.179.54       50      521    63421        0       52   121
2008-11-03 10:04:30.821  7578.403 any       82.196.5.225       50      297    40818        0       43   137

Summary: total flows: 151684, total bytes: 81.3 M, total packets: 263986, avg bps: 44961, avg pps: 17, avg bpp: 322
Time window: 2008-11-03 08:01:03 - 2008-11-03 12:16:04
Total flows processed: 310930, Records skipped: 0, Bytes read: 16169104
Sys: 0.080s flows/second: 3886430.7  Wall: 0.067s flows/second: 4614642.5
```

3. Statistiques protocole UDP :

3.1. Classement par adresse IP source :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811030700:nfcapd.200811031110 -n 20 -s srcip/flows
nfdump filter:
proto UDP
Top 20 Src IP Addr ordered by flows:
Date first seen          Duration Proto      Src IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2008-11-03 08:01:03.613 15278.791 any        172.16.80.1     4647     4742  1018633        0      533   214
2008-11-03 09:24:44.973  2136.104 any        172.16.97.6     2747     2747    76916        1      288    28
2008-11-03 09:43:23.141  9140.275 any       172.10.140.5      190      420    97165        0       85   231
2008-11-03 09:21:59.189 10186.747 any       172.10.160.3       96      247    64522        0       50   261
2008-11-03 10:40:10.741  5353.519 any         198.41.0.4       84       84    28769        0       42   342
2008-11-03 10:40:18.829  2196.011 any     192.203.230.10       82       82    26952        0       98   328
2008-11-03 10:40:12.829  5460.607 any     192.228.79.201       71       71    25906        0       37   364
2008-11-03 10:40:26.713  5369.807 any      192.36.148.17       70       70    25073        0       37   358
2008-11-03 10:40:22.801  2183.967 any      192.112.36.4       67       67    22619        0       82   337
2008-11-03 10:40:16.773  2177.959 any       128.8.10.90       67       67    22619        0       83   337
2008-11-03 10:40:24.777  4006.087 any       128.63.2.53       67       67    22913        0       45   341
2008-11-03 09:39:36.229  5488.543 any        172.18.4.2       61      212    68984        0      100   325
2008-11-03 09:49:14.049  8779.499 any       172.10.140.3       56      133    42596        0       38   320
2008-11-03 10:40:28.729  5313.499 any      192.58.128.30       49       49    15146        0       22   309
2008-11-03 10:40:14.681  2181.963 any       192.33.4.12       47       47    19276        0       70   410
2008-11-03 10:40:20.689  2196.007 any        192.5.5.241       46       46    17441        0       63   379
2008-11-03 10:40:30.717  5313.619 any       193.0.14.129       43       43    14096        0       21   327
2008-11-03 08:09:16.413 14406.855 any       172.10.170.4       31       60     4124        0        2    68
2008-11-03 08:03:19.917 15149.527 any       172.18.4.202       24       46    10554        0        5   229
2008-11-03 10:51:01.028  4916.248 any            0.0.0.0       22       80    26240        0       42   328

Summary: total flows: 139110, total bytes: 8.1 M, total packets: 140457, avg bps: 4450, avg pps: 9, avg bpp: 60
Time window: 2008-11-03 08:01:03 - 2008-11-03 12:16:04
Total flows processed: 310930, Records skipped: 0, Bytes read: 16169104
Sys: 0.084s flows/second: 3701371.4  Wall: 0.070s flows/second: 4415365.0
```

3.2. Classement par adresse IP destination :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811030700:nfcapd.200811031110 -n 20 -s dstip/flows
nfdump filter:
proto UDP
Top 20 Dst IP Addr ordered by flows:
Date first seen          Duration Proto      Dst IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2008-11-03 08:01:03.613 15278.791 any        172.18.4.2    138590   138693    7.8 M        9     4259    58
2008-11-03 08:04:51.585 15051.831 any       172.16.80.1       454     1582   314919        0      167   199
2008-11-03 10:38:37.969  5659.307 any   255.255.255.255        43      133    43624        0       61   328
2008-11-03 08:03:19.917 15149.527 any       172.18.7.255        22       44    10450        0        5   237
2008-11-03 10:39:43.089     9.536 any      172.18.15.255         1        5      260        0      218    52

Summary: total flows: 139110, total bytes: 8.1 M, total packets: 140457, avg bps: 4450, avg pps: 9, avg bpp: 60
Time window: 2008-11-03 08:01:03 - 2008-11-03 12:16:04
Total flows processed: 310930, Records skipped: 0, Bytes read: 16169104
Sys: 0.076s flows/second: 4090968.9  Wall: 0.064s flows/second: 4822115.4
```

4. Statistiques protocole ICMP :

4.1. Classement par adresse IP source :

Netflow Processing

Source: upstream1 — All Sources

Filter: `proto ICMP`

and <none>

Options: List Flows / Stat TopN

Top: 20

Stat: SRC IP Address order by flows

Limit: Packets > 0 -

Output: / IPv6 long

Clear Form | process

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811030700:nfcapd.200811031120 -n 20 -s srcip/flows
nfdump filter:
proto ICMP
Top 20 Src IP Addr ordered by flows:
Date first seen          Duration Proto      Src IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2008-11-03 10:08:10.461  8157.139 any       172.18.4.202       66       68     7429        0        7   109
2008-11-03 09:39:36.229  2766.180 any        172.16.80.1       59      210    74760        0      216   356
2008-11-03 09:16:21.017 10512.111 any         172.18.4.2       30      581    48881        0       37    84
2008-11-03 09:16:21.017 10490.251 any       193.52.8.195       19       40     2240        0        1    56
2008-11-03 10:34:02.581  6106.115 any       172.16.64.83        8       18      984        0        1    54
2008-11-03 11:19:49.372  3103.784 any      209.85.129.99        6      452    37920        0       97    83
2008-11-03 11:17:11.576  1003.196 any     209.85.129.104        5       87     6252        0       49    71
2008-11-03 10:18:00.009  3367.299 any         172.18.4.1        4        6     3072        0        7   512
2008-11-03 11:19:39.548   835.436 any     209.85.129.147        4       14     1104        0       10    78
2008-11-03 10:26:29.733  2409.435 any         172.18.0.3        3        4     3770        0       12   942
2008-11-03 10:26:29.865  2409.483 any        172.18.0.19        3        4     3770        0       12   942
2008-11-03 10:26:30.133  2409.827 any        172.18.0.51        3        4     3770        0       12   942
2008-11-03 10:26:30.141  2409.827 any        172.18.0.52        3        4     3770        0       12   942
2008-11-03 10:26:29.877  2409.483 any        172.18.0.20        3        4     3770        0       12   942
2008-11-03 10:26:30.153  2409.823 any        172.18.0.53        3        4     3770        0       12   942
2008-11-03 10:26:30.161  2409.823 any        172.18.0.54        3        4     3770        0       12   942
2008-11-03 10:26:30.169  2409.823 any        172.18.0.55        3        4     3770        0       12   942
2008-11-03 10:34:40.797  2164.523 any       172.16.64.70        3        6      360        0        1    60
2008-11-03 10:26:29.741  2409.435 any         172.18.0.4        3        4     3770        0       12   942
2008-11-03 10:26:29.885  2409.483 any        172.18.0.21        3        4     3770        0       12   942

Summary: total flows: 20138, total bytes: 29.9 M, total packets: 34477, avg bps: 22053, avg pps: 3, avg bpp: 910
Time window: 2008-11-03 08:01:03 - 2008-11-03 12:26:10
Total flows processed: 313450, Records skipped: 0, Bytes read: 16300168
Sys: 0.072s flows/second: 4353290.8   Wall: 0.059s flows/second: 5284587.1
```

4.2. Classement par adresse IP destination :

Netflow Processing

Source: upstream1 — All Sources

Filter: proto ICMP — and <none>

Options: List Flows / Stat TopN — Top: 20 — Stat: DST IP Address order by flows — Limit: Packets > 0 - — Output: / IPv6 long

Clear Form | process

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811030700:nfcapd.200811031120 -n 20 -s dstip/flows
nfdump filter:
proto ICMP
Top 20 Dst IP Addr ordered by flows:
Date first seen          Duration Proto      Dst IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2008-11-03 09:14:15.929 11391.671 any         172.18.4.2    20108    33897   29.9 M        2    22020   925
2008-11-03 11:19:49.348  3103.780 any       209.85.129.99        6      452    37920        0       97    83
2008-11-03 11:17:11.552  1003.196 any      209.85.129.104        5       87     6252        0       49    71
2008-11-03 11:19:39.524   835.436 any      209.85.129.147        4       14     1104        0       10    78
2008-11-03 11:13:29.280    38.028 any         172.18.4.1        2        3      180        0       37    60
2008-11-03 11:35:01.552    92.132 any     193.252.122.103        2        5      420        0       36    84
2008-11-03 12:01:48.748     0.000 any      172.10.190.228        1        1       28        0        0    28
2008-11-03 12:01:48.748     0.000 any      172.10.190.227        1        1       28        0        0    28
2008-11-03 12:01:48.748     0.000 any      172.10.190.226        1        1       28        0        0    28
2008-11-03 12:01:50.944     0.000 any       172.10.190.23        1        1       28        0        0    28
2008-11-03 11:34:56.708     1.008 any       212.27.48.10        1        2      168        1     1333    84
2008-11-03 11:00:20.216     6.012 any       66.249.93.104        1        7      588        1      782    84
2008-11-03 10:18:00.009     0.000 any       172.18.15.255        1        1     1007        0        0  1007
2008-11-03 09:16:21.017     1.004 any       172.10.160.41        1        2      168        1     1338    84
2008-11-03 12:01:48.748     0.000 any      172.10.190.230        1        1       28        0        0    28
2008-11-03 12:01:48.748     0.000 any      172.10.190.231        1        1       28        0        0    28
2008-11-03 12:01:48.748     0.000 any      172.10.190.229        1        1       28        0        0    28

Summary: total flows: 20138, total bytes: 29.9 M, total packets: 34477, avg bps: 22053, avg pps: 3, avg bpp: 910
Time window: 2008-11-03 08:01:03 - 2008-11-03 12:26:10
Total flows processed: 313450, Records skipped: 0, Bytes read: 16300168
Sys: 0.072s flows/second: 4353230.4  Wall: 0.061s flows/second: 5097079.5
```

5. Statistiques par numéro de port :

5.1. Classement par nombre de paquets :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811030700:nfcapd.200811031110 -n 20 -s port/packets
nfdump filter:
any
Top 20        Port ordered by packets:
Date first seen          Duration Proto             Port    Flows  Packets    Bytes      pps      bps   bpp
2008-11-03 10:39:43.089  5407.687 any                520   260899   260911   12.9 M       48    20071    51
2008-11-03 08:03:21.869 15146.935 any                 80     5560    87737   62.6 M        5    34642   747
2008-11-03 10:37:15.481  5107.479 any              49153    55458    55461   2.3 M        10     3822    44
2008-11-03 10:36:38.029  5144.927 any              49154    55176    55176   2.3 M        10     3774    44
2008-11-03 08:04:54.533 15069.751 any                443    14211    37032   12.4 M        2     6884   350
2008-11-03 09:14:15.929 10892.767 any                  0    20157    35045   30.0 M        3    23098   897
2008-11-03 09:14:15.929 10892.767 any               2048    20054    33678   29.8 M        3    22973   928
2008-11-03 08:01:03.613 15294.175 any                 53     5628     6380   1.3 M         0      697   209
2008-11-03 08:50:08.069 11025.411 any              55555     3366     5728   413683        0      300    72
2008-11-03 10:13:54.565  5901.367 any              50682        4     3839   3.6 M         0     5162   991
2008-11-03 09:08:49.837  9717.099 any              43234        4     3227   3.1 M         0     2670  1005
2008-11-03 09:08:49.833 10350.443 any              51838        6     3207   3.5 M         0     2876  1160
2008-11-03 09:08:54.101  9828.535 any              43237        5     2625   2.8 M         0     2376  1112
2008-11-03 09:24:42.293  2138.784 any              50642     2614     2622   74555         1      278    28
2008-11-03 09:08:59.137  7673.627 any              43257        3     2580   2.8 M         0     3084  1146
2008-11-03 11:44:21.040  1793.924 any               1620       43     2416   1.9 M         1     8848   821
2008-11-03 09:08:56.401  9811.051 any              43241        4     2234   2.5 M         0     2110  1158
2008-11-03 09:09:00.577     0.856 any              43259        2     2142   2.3 M      2502   22.0 M  1149
2008-11-03 09:08:55.489  9886.171 any              43238        4     1155   1.2 M         0     1028  1100
2008-11-03 10:36:13.889  4535.659 any              44649     1006     1009   44412         0       78    44

Summary: total flows: 310930, total bytes: 119.3 M, total packets: 438918, avg bps: 65420, avg pps: 28, avg bpp: 285
Time window: 2008-11-03 08:01:03 - 2008-11-03 12:16:04
Total flows processed: 310930, Records skipped: 0, Bytes read: 16169104
Sys: 0.124s flows/second: 2507358.5  Wall: 0.112s flows/second: 2774179.2
```

5.2. Classement par quantité de données :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811030700:nfcapd.200811031110 -n 20 -s port/bytes
nfdump filter:
any
Top 20        Port ordered by bytes:
Date first seen          Duration Proto             Port    Flows  Packets    Bytes      pps      bps   bpp
2008-11-03 08:03:21.869 15146.935 any                80     5560    87737   62.6 M        5    34642   747
2008-11-03 09:14:15.929 10892.767 any                 0    20157    35045   30.0 M        3    23098   897
2008-11-03 09:14:15.929 10892.767 any              2048    20054    33678   29.8 M        3    22973   928
2008-11-03 10:39:43.089  5407.687 any               520   260899   260911   12.9 M       48    20071    51
2008-11-03 08:04:54.533 15069.751 any               443    14211    37032   12.4 M        2     6884   350
2008-11-03 10:13:54.565  5901.367 any             50682        4     3839    3.6 M        0     5162   991
2008-11-03 09:08:49.833 10350.443 any             51838        6     3207    3.5 M        0     2876  1160
2008-11-03 09:08:49.837  9717.099 any             43234        4     3227    3.1 M        0     2670  1005
2008-11-03 09:08:59.137  7673.627 any             43257        3     2580    2.8 M        0     3084  1146
2008-11-03 09:08:54.101  9828.535 any             43237        5     2625    2.8 M        0     2376  1112
2008-11-03 09:08:56.401  9811.051 any             43241        4     2234    2.5 M        0     2110  1158
2008-11-03 09:09:00.577     0.856 any             43259        2     2142    2.3 M     2502  22.0 M  1149
2008-11-03 10:37:15.481  5107.479 any             49153    55458    55461    2.3 M       10     3822    44
2008-11-03 10:36:38.029  5144.927 any             49154    55176    55176    2.3 M       10     3774    44
2008-11-03 11:44:21.040  1793.924 any              1620       43     2416    1.9 M        1     8848   821
2008-11-03 08:01:03.613 15294.175 any                53     5628     6380    1.3 M        0      697   209
2008-11-03 09:08:55.489  9886.171 any             43238        4     1155    1.2 M        0     1028  1100
2008-11-03 09:08:53.313     0.804 any             43236        2      981    1.0 M     1220  10.0 M  1069
2008-11-03 09:09:00.133  9879.779 any             43258        5      936  1031477        0      835  1102
2008-11-03 10:28:52.717  5115.959 any             45988        5      760   696920        0     1089   917

Summary: total flows: 310930, total bytes: 119.3 M, total packets: 438918, avg bps: 65420, avg pps: 28, avg bpp: 285
Time window: 2008-11-03 08:01:03 - 2008-11-03 12:16:04
Total flows processed: 310930, Records skipped: 0, Bytes read: 16169104
Sys: 0.124s flows/second: 2507358.5  Wall: 0.114s flows/second: 2709960.3
```

6. Analyse du trafic entre 8h et 9h20 :

6.1. Les machines ayant générées le plus de trafic :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811030700:nfcapd.200811030820 -n 10 -s srcip/bytes
nfdump filter:
any
Top 10 Src IP Addr ordered by bytes:
Date first seen          Duration Proto      Src IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2008-11-03 09:08:00.293    61.292 any       212.27.32.66       57    14204   20.0 M      231   2.6 M  1477
2008-11-03 09:08:00.325    61.264 any      91.121.86.213        3     2478    3.5 M       40  483397  1493
2008-11-03 08:03:21.873  4966.052 any        172.18.4.2      424    10457 1013721        2     1633    96
2008-11-03 09:21:45.021    24.216 any     91.121.166.153       17      465  610323       19   201626  1312
2008-11-03 09:08:24.825     7.860 any     207.46.209.124        2      267  371412       33   378027  1391
2008-11-03 09:08:18.261    36.932 any     213.199.181.20        4      260  332863        7    72102  1280
2008-11-03 09:21:36.361    17.476 any      72.233.96.253        9      204  241880       11   110725  1185
2008-11-03 09:24:37.785    66.672 any      193.51.224.14        8      289  222434        4    26689   769
2008-11-03 09:21:25.121   152.508 any       88.191.20.10       20      213  210706        1    11052   989
2008-11-03 09:22:57.785   173.692 any     209.202.161.68       15      186  194422        1     8954  1045

Summary: total flows: 2190, total bytes: 28.2 M, total packets: 32823, avg bps: 46360, avg pps: 6, avg bpp: 901
Time window: 2008-11-03 08:01:03 - 2008-11-03 09:26:08
Total flows processed: 2190, Records skipped: 0, Bytes read: 114084
Sys: 0.016s flows/second: 136875.0   Wall: 0.001s flows/second: 1502057.6
```

Infos sur l'adresse ayant transmis le plus d'octets (max :20Mo) :

212.27.32.66: debian.proxad.net

```
IP range 212.27.32.0 - 212.27.32.255
Network name FR-PROXAD
Infos Proxad
Infos Backbone
Country France (FR)
Abuse E-mail abuse@proxad.net
```

C'est cette adresse qui a généré le plus de paquets et la plus grosse quantité de trafic.

6.2. Les ports ayant reçus le plus de trafic :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811030700:nfcapd.200811030820 -n 10 -s dstport/bytes
nfdump filter:
any
Top 10    Dst Port ordered by bytes:
Date first seen          Duration Proto         Dst Port    Flows  Packets    Bytes      pps      bps  bpp
2008-11-03 09:08:49.853    11.736 any             51838        1     2457    3.5 M      209    2.4 M 1498
2008-11-03 09:08:49.853     3.020 any             43234        1     2127    3.0 M      704    8.0 M 1495
2008-11-03 09:08:59.153     0.996 any             43257        1     1953    2.8 M     1960   22.4 M 1497
2008-11-03 09:08:54.117     1.388 any             43237        1     1926    2.7 M     1387   15.8 M 1496
2008-11-03 09:08:56.413     0.968 any             43241        1     1711    2.4 M     1767   20.2 M 1495
2008-11-03 09:09:00.593     0.840 any             43259        1     1627    2.3 M     1936   22.1 M 1497
2008-11-03 09:08:55.505     0.560 any             43238        1      839    1.2 M     1498   17.1 M 1493
2008-11-03 09:08:53.329     0.788 any             43236        1      693  1032710      879   10.0 M 1490
2008-11-03 09:09:00.149     0.444 any             43258        1      682  1017694     1536   17.5 M 1492
2008-11-03 08:03:21.869  4966.056 any                80      412    10224   935110        2    1506   91

Summary: total flows: 2190, total bytes: 28.2 M, total packets: 32823, avg bps: 46360, avg pps: 6, avg bpp: 901
Time window: 2008-11-03 08:01:03 - 2008-11-03 09:26:08
Total flows processed: 2190, Records skipped: 0, Bytes read: 114004
Sys: 0.016s flows/second: 136875.0   Wall: 0.001s flows/second: 1188280.0
```

6.3. Repérage d'activités anormales :

```
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2008-11-03 09:00:53.001     0.000 TCP       172.18.4.202:4214   ->       172.18.4.2:22           1       40     1
2008-11-03 09:01:03.713     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:57785        1      119     1
2008-11-03 09:01:03.749     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:42932        1      119     1
2008-11-03 09:01:03.781     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:48112        1      119     1
2008-11-03 09:01:03.801     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:54450        1      119     1
2008-11-03 09:01:03.825     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:51518        1      119     1
2008-11-03 09:01:03.837     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:59367        1      119     1
2008-11-03 09:01:03.877  1683.728 UDP        172.16.80.1:53     ->       172.18.4.2:59096        2      246     2
2008-11-03 09:01:03.905     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:54595        1      119     1
2008-11-03 09:02:04.053     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:49973        1      119     1
2008-11-03 09:02:04.089     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:46471        1      119     1
2008-11-03 09:02:04.117     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:49219        1      119     1
2008-11-03 09:02:04.137     0.004 UDP        172.16.80.1:53     ->       172.18.4.2:47511        1      119     1
2008-11-03 09:02:04.165     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:55438        1      119     1
2008-11-03 09:02:04.181     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:56712        1      119     1
2008-11-03 09:02:04.201     0.004 UDP        172.16.80.1:53     ->       172.18.4.2:58684        1      119     1
2008-11-03 09:02:04.245  1381.460 UDP        172.16.80.1:53     ->       172.18.4.2:39319        2      482     2
2008-11-03 09:02:41.309     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:57011        1      119     1
2008-11-03 09:02:54.061     0.000 TCP       172.18.4.202:1368   ->     172.10.140.2:443          1       60     1
2008-11-03 09:02:54.061     0.004 TCP       172.18.4.202:1368   ->       172.18.4.2:443          3      156     1
2008-11-03 09:02:54.061     0.004 TCP         172.18.4.2:443    ->     172.18.4.202:1368         2      112     1
2008-11-03 09:03:03.385     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:57347        1      119     1
2008-11-03 09:03:03.425     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:37985        1      119     1
2008-11-03 09:03:03.457     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:55403        1      119     1
2008-11-03 09:03:03.477  3386.752 UDP        172.16.80.1:53     ->       172.18.4.2:34569        2      495     2
2008-11-03 09:03:03.505     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:34483        1      119     1
2008-11-03 09:03:03.517     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:48969        1      119     1
2008-11-03 09:03:03.541     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:60753        1      119     1
2008-11-03 09:03:03.585     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:36400        1      119     1
2008-11-03 09:03:07.125     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:27273        1      485     1
2008-11-03 09:03:07.229     0.000 UDP        172.16.80.1:53     ->       172.18.4.2:38733        1      379     1
2008-11-03 09:03:07.273     0.120 TCP         172.18.4.2:3556   ->      193.86.3.36:80           7      616     1
2008-11-03 09:03:07.309     0.120 TCP        193.86.3.36:80     ->       172.18.4.2:3556         8     6991     1
```

On observe des requêtes depuis l'adresse IP de Cooper vers le routeur Cisco :
Le trafic est initié par le port 53 à destination de nombreux ports. Etant donné la rapidité et la quantité de requête on peut imaginer que les attaquants ont utilisé l'adresse de Cooper pour faire du port scan sur le routeur Cisco (man in the middle). Celui-ci ne répond pas par configuration. Cet extrait de trafic est une vue non exhaustive on observe ce genre de trafic depuis 8h00.

```
2008-11-03 09:26:04.705     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:21734        1       28      1
2008-11-03 09:26:05.509     0.000 UDP       172.16.97.6:50643 ->       172.18.4.2:21734        1       28      1
2008-11-03 09:26:06.045     5.004 UDP      172.10.160.3:40350 ->      172.16.80.1:53           2       136     1
2008-11-03 09:26:06.053     5.004 UDP      172.10.160.3:35048 ->      172.16.80.1:53           2       136     1
2008-11-03 09:26:06.313     0.000 UDP       172.16.97.6:50644 ->       172.18.4.2:21734        1       28      1
2008-11-03 09:26:07.117     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:40061        1       28      1
2008-11-03 09:26:07.921     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:17572        1       28      1
2008-11-03 09:26:08.721     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:24423        1       28      1
2008-11-03 09:26:09.521     0.000 UDP       172.16.97.6:50643 ->       172.18.4.2:24423        1       28      1
2008-11-03 09:26:10.325     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:27146        1       28      1
2008-11-03 09:26:11.129     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:42729        1       28      1
2008-11-03 09:26:11.933     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:1809         1       28      1
2008-11-03 09:26:12.737     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:35551        1       28      1
2008-11-03 09:26:13.541     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:48828        1       28      1
2008-11-03 09:26:14.345     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:16660        1       28      1
2008-11-03 09:26:15.149     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:59123        1       28      1
2008-11-03 09:26:15.953     0.000 UDP       172.16.97.6:50643 ->       172.18.4.2:59123        1       28      1
2008-11-03 09:26:16.157     5.000 UDP      172.10.160.3:43640 ->      172.16.80.1:53           2       110     1
2008-11-03 09:26:16.157     5.004 UDP      172.10.160.3:35338 ->      172.16.80.1:53           2       110     1
2008-11-03 09:26:16.157     5.004 UDP      172.10.160.3:36663 ->      172.16.80.1:53           2       110     1
2008-11-03 09:26:16.157     5.000 UDP      172.10.160.3:37256 ->      172.16.80.1:53           2       110     1
2008-11-03 09:26:16.757     0.000 UDP       172.16.97.6:50644 ->       172.18.4.2:59123        1       28      1
2008-11-03 09:26:17.557     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:36302        1       28      1
2008-11-03 09:26:18.361     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:34174        1       28      1
2008-11-03 09:26:19.169     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:6117         1       28      1
2008-11-03 09:26:19.969     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:33910        1       28      1
2008-11-03 09:26:20.437     5.004 UDP      172.10.160.3:35670 ->      172.16.80.1:53           2       110     1
2008-11-03 09:26:20.437     5.004 UDP      172.10.160.3:45653 ->      172.16.80.1:53           2       110     1
2008-11-03 09:26:20.773     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:5952         1       28      1
2008-11-03 09:26:21.577     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:47801        1       28      1
2008-11-03 09:26:22.381     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:54573        1       28      1
2008-11-03 09:26:23.189     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:3730         1       28      1
2008-11-03 09:26:23.993     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:11067        1       28      1
2008-11-03 09:26:24.793     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:43485        1       28      1
2008-11-03 09:26:25.593     0.000 UDP       172.16.97.6:50642 ->       172.18.4.2:51020        1       28      1
```

Apparition d'une IP non mentionnée sur le plan d'adressage de la défense : 172.10.160.3 et qui contacte Cooper sur le port 53 (requête DNS).
On observe un scannage de port intensif de la part de 172.16.97.6 depuis le port 50642, mais une fois de plus sans réponse de la part du routeur.
On observe un scannage de port intensif de la part de 172.16.97.6 depuis le port 50642, mais une fois de plus sans réponse de la part du routeur.

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811030800:nfcapd.200811030920 -r 100 -s
nfdump filter:
any
Aggregated flows 7496
Top 100 flows ordered by flows:
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2008-11-03 09:39:36.229  2766.130 UDP         172.18.4.2:68     ->      172.16.80.1:67         210    68880    59
2008-11-03 09:39:36.229  2766.130 ICMP       172.16.80.1:0      ->       172.18.4.2:3.3        210    74760    59
2008-11-03 09:56:32.825  1743.068 UDP       172.10.140.5:68     ->      172.16.80.1:67         127    41656    41
2008-11-03 10:05:12.885  1218.072 UDP       172.10.160.3:68     ->      172.16.80.1:67          96    31488    32
2008-11-03 10:08:10.461   870.148 ICMP      172.18.4.202:0      ->       172.18.4.2:8.0         12     1008    12
2008-11-03 09:38:14.661   425.924 TCP         172.18.4.2:53247 ->   198.133.219.25:80          23     3059     8
2008-11-03 09:38:14.661   425.924 TCP         172.18.4.2:53248 ->   198.133.219.25:80          40     3769     8
2008-11-03 09:38:15.045   650.596 TCP         172.18.4.2:53250 ->   198.133.219.25:80          74     5155     8
2008-11-03 09:21:38.281   135.630 TCP         172.18.4.2:52020 ->       69.46.36.6:80          17     2356     7
2008-11-03 09:25:06.545   111.496 TCP       209.62.179.54:80     ->       172.18.4.2:39327       41    44400     7
2008-11-03 09:23:04.781   131.644 TCP         172.18.4.2:36405 ->    84.253.50.198:80          21     1567     7
2008-11-03 09:21:38.669   144.476 TCP         172.18.4.2:52022 ->       69.46.36.6:80          14     1290     7
2008-11-03 09:23:04.877   171.328 TCP         172.18.4.2:36407 ->    84.253.50.198:80          18     1859     7
2008-11-03 09:23:04.773   118.338 TCP         172.18.4.2:36403 ->    84.253.50.198:80          21     1959     7
2008-11-03 09:21:38.669   144.472 TCP         172.18.4.2:52023 ->       69.46.36.6:80          14     1290     7
2008-11-03 09:23:04.781   134.704 TCP         172.18.4.2:36406 ->    84.253.50.198:80          17     1364     7
2008-11-03 09:27:39.193   122.404 TCP         172.18.4.2:44438 ->   209.62.179.182:80          53     3523     7
2008-11-03 09:29:07.917   112.628 TCP       209.62.179.182:80    ->       172.18.4.2:44448       36    36713     7
2008-11-03 09:21:52.577   137.008 TCP         172.18.4.2:38287 ->       69.46.36.6:80          18     2756     7
2008-11-03 09:23:04.773   123.438 TCP         172.18.4.2:36404 ->    84.253.50.198:80          20     2000     7
2008-11-03 09:29:07.869   112.624 TCP       209.62.179.182:80    ->       172.18.4.2:44446       41    44400     7
2008-11-03 09:29:07.885   122.492 TCP         172.18.4.2:44447 ->   209.62.179.182:80          49     3318     7
2008-11-03 09:33:04.441   129.740 TCP         172.18.4.2:42649 ->   209.62.179.182:80          61     4725     7
2008-11-03 09:25:06.185   111.020 TCP         172.18.4.2:39322 ->    209.62.179.54:80          14     1125     7
2008-11-03 09:31:34.545   123.372 TCP         172.18.4.2:42634 ->   209.62.179.182:80          41     2892     7
2008-11-03 09:25:06.497   110.512 TCP       209.62.179.54:80     ->       172.18.4.2:39326       38    39805     7
2008-11-03 09:31:34.569   122.412 TCP         172.18.4.2:42635 ->   209.62.179.182:80          42     2951     7
```

On observe une forte activité entre le routeur cisco et Cooper entre les ports 68 et 67

Et on observe en parallèle exactement au même moment du trafic de cooper depuis le port 0 vers le routeur sur le port 3.3 ?
Autre chose étonnante on a du trafic entre 172 .10.140.5, 172.10.160.3 et cooper toujours entre les ports 68 et 67.
Ni la machine 172.10.140.5 ni la 172.10.160.3 ne sont mentionnée sur le plan d'adressage de la défense !
Cette analyse grossière des échanges entre 8h00 et 9h20 ne permet pas de mettre en relief d'autres activités anormales.

7. Analyse du trafic entre 9h20 et 10h40 :

7.1. Les machines ayant générées le plus de trafic :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811030820:nfcapd.200811030940 -n 10 -s srcip/flows
nfdump filter:
any
Top 10 Src IP Addr ordered by flows:
Date first seen          Duration Proto      Src IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2008-11-03 09:24:44.801  3218.476 any        172.16.97.6     2769     2791    79000        0      196    28
2008-11-03 09:21:01.357  5057.263 any        172.16.80.1     2753     2993   639518        0     1011   213
2008-11-03 10:14:22.073  1542.324 any       172.16.64.96     1874     1876    82572        1      428    44
2008-11-03 09:21:01.373  5078.251 any         172.18.4.2     1345    17031    3.2 M        3     5231   194
2008-11-03 09:28:56.937  4539.220 any       172.16.80.20      193     1129   303239        0      534   268
2008-11-03 10:40:04.597   299.243 any       172.16.64.92      132      132     5808        0      155    44
2008-11-03 09:43:23.141  3722.803 any       172.10.140.5      125      314    76542        0      164   243
2008-11-03 09:20:53.477  4987.332 any       172.18.4.202      116      262    18009        0       28    68
2008-11-03 09:21:59.189  5024.839 any       172.10.160.3       90      241    63546        0      101   264
2008-11-03 09:24:38.105  3605.420 any       193.51.224.8       58     1892    1.6 M        0     3667   873

Summary: total flows: 11612, total bytes: 22.5 M, total packets: 45952, avg bps: 36959, avg pps: 8, avg bpp: 513
Time window: 2008-11-03 09:20:53 - 2008-11-03 10:46:03
Total flows processed: 11612, Records skipped: 0, Bytes read: 604028
Sys: 0.024s flows/second: 483813.2   Wall: 0.266s flows/second: 43533.7
```

7.2. Les ports ayant reçus le plus de trafic :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811030820:nfcapd.200811030940 -n 10 -s dstport/flows
nfdump filter:
any
Top 10    Dst Port ordered by flows:
Date first seen          Duration Proto         Dst Port    Flows  Packets    Bytes      pps      bps   bpp
2008-11-03 09:21:01.373  5078.251 any               80     1202    15459    2.3 M        3     3835   157
2008-11-03 09:24:44.885  4755.924 any             2048      433      450   389373        0      654   865
2008-11-03 10:39:43.089   166.372 any              520      354      358    18616        2      895    52
2008-11-03 09:22:54.161  4916.148 any              443      258     1360   321275        0      522   236
2008-11-03 09:39:36.229  3967.799 any               67      220      696   220280        0      460   316
2008-11-03 09:21:59.189  4977.683 any               53      113      344    23624        0       37    68
2008-11-03 09:39:36.229  2766.180 any              771       59      210    74760        0      216   356
2008-11-03 09:20:53.477  5049.843 any               22       55      125     7748        0       12    61
2008-11-03 10:20:03.265  1496.931 any               23       16       18      852        0        4    47
2008-11-03 10:36:16.433   519.919 any              256       16       16      704        0       10    44

Summary: total flows: 11612, total bytes: 22.5 M, total packets: 45952, avg bps: 36959, avg pps: 8, avg bpp: 513
Time window: 2008-11-03 09:20:53 - 2008-11-03 10:46:03
Total flows processed: 11612, Records skipped: 0, Bytes read: 604028
Sys: 0.024s flows/second: 483833.3   Wall: 0.123s flows/second: 93908.7
```

Durant cette période, une grande quantité de trames polluantes a circulé. En effet, des IP Spoofing et des scannages de ports ont inondé le trafic, mais aucune attaque autre n'a été détectée.

Le scan de ports du routeur 172.18.4.2 s'est effectué en provenance de multiples machines mais principalement de 172.16.80.1:53 et de 172.16.97.6:50642
Par contre il y a eu beaucoup de requêtes vers des ports 80 (en sortie). La défense a du beaucoup navigué sur des sites web.

8. Analyse du trafic entre 10h40 et 12h30 :

8.1. Les machines ayant générées le plus de trafic :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -R nfcapd.200811030940:nfcapd.200811031130 -n 10 -s srcip/flows
nfdump filter:
any
Top 10 Src IP Addr ordered by flows:
Date first seen          Duration Proto      Src IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2008-11-03 11:11:11.048  4974.032 any       172.16.64.96   112650   112706    4.8 M       22     8013    44
2008-11-03 11:04:13.068  3967.136 any       172.18.4.101    12930    15700    1.0 M        3     2162    68
2008-11-03 11:04:48.796   820.244 any       172.16.64.66     6835     7379   447481        8     4364    60
2008-11-03 10:59:19.516  5798.684 any       172.18.4.103     6488     6552   303754        1      419    46
2008-11-03 11:36:51.908  3543.344 any       172.16.64.83     4823    13540   703632        3     1588    51
2008-11-03 10:45:18.624  6640.892 any         172.18.4.2     3291    31132    9.9 M        4    12523   333
2008-11-03 10:41:04.821  6836.035 any       172.16.80.1      1492     1549   443113        0      518   286
2008-11-03 10:44:33.921  5394.171 any       172.16.64.92     1037     1045    46884        0       69    44
2008-11-03 10:43:07.053  6765.791 any       172.16.64.95      500     3375   499041        0      590   147
2008-11-03 10:43:41.525  5616.703 any       172.16.80.20      406     1680   366578        0      522   218

Summary: total flows: 303555, total bytes: 78.8 M, total packets: 386401, avg bps: 95246, avg pps: 55, avg bpp: 213
Time window: 2008-11-03 10:40:16 - 2008-11-03 12:35:59
Total flows processed: 303555, Records skipped: 0, Bytes read: 15785268
Sys: 0.096s flows/second: 3161866.6   Wall: 0.082s flows/second: 3679543.7
```

Grace aux statistiques sur les adresses IP source des flux transitant vers le routeur, nous pouvons constater que des adresses IP générant le plus de flux sont en
172.16.64 .96
.66
.83
.92
.95
Et
172.18.4 .101 et .103
Ce sont des adresses que les attaquants ont utilisé pour communiquer avec le réseau de la défense.

Le routeur CISCO (172.18.4.2) a quand à lui été gourmant en utilisation de la bande passante afin d'envoyer des flux de données.
afin d'envoyer des flux de données.

8.2. Les ports ayant reçus le plus de trafic :

```
** nfdump -M /usr/data/nfsen/profiles-data/live/upstream1  -T  -r nfcapd.200811030940 -n 10 -s dstport/flows
nfdump filter:
any
Top 10    Dst Port ordered by flows:
Date first seen          Duration Proto         Dst Port    Flows  Packets    Bytes      pps      bps   bpp
2008-11-03 10:41:39.189    50.272 any               520      353      353    18356        7     2921    52
2008-11-03 10:40:16.009   328.019 any                67       33       85    27880        0      679   328
2008-11-03 10:42:23.769   195.855 any                80       26       31     1720        0       70    55
2008-11-03 10:44:33.929    23.463 any              1723        9        9      396        0      135    44
2008-11-03 10:44:33.925    22.427 any               256        9        9      396        0      141    44
2008-11-03 10:44:33.925    22.947 any                53        9        9      396        0      138    44
2008-11-03 10:44:33.929    20.431 any               113        8        8      352        0      137    44
2008-11-03 10:44:48.069     7.771 any                25        7        7      308        0      317    44
2008-11-03 10:43:53.885    69.435 any                22        7        7      324        0       37    46
2008-11-03 10:43:07.053   103.256 any               443        7       11      524        0       40    47

Summary: total flows: 628, total bytes: 96575, total packets: 729, avg bps: 2222, avg pps: 2, avg bpp: 132
Time window: 2008-11-03 10:40:16 - 2008-11-03 10:46:03
Total flows processed: 628, Records skipped: 0, Bytes read: 32668
Sys: 0.004s flows/second: 157000.0   Wall: 0.121s flows/second: 5154.5
```

8.3. Repérage d'activités anormales :

10:40:16
IP Source : 172.10.160.3:68
Destination : 172.16.80.1:67
Protocole utilisé : UDP
Durée dialogue : 76 secondes
Paquets envoyés : 7 (2296 Bytes)
Type : Requête UDP durant 76 secondes => volonté de saturation du routeur

10:40:27
IP Source : 172.10.140.5:68
Destination : 172.16.80.1:67
Protocole utilisé : UDP
Durée dialogue : 60 secondes
Paquets envoyés : 6 (1968 Bytes)
Type : Requête UDP durant 60 secondes => volonté de saturation du routeur

10:41:08, 10 :43:52 et 10 :48 :16
IP Source : 172.10.80.13:68
Destination : 255.255.255.255 :67
Protocole utilisé : UDP
Durée dialogue : 23 secondes
Paquets envoyés : 3 (984 Bytes)
Tos : 16
Type: tentative d'envoi de trames UDP à tous les hôtes du réseau

10:41:04 à 10:41:36
IP Source : 172.16.80.1:53
Destination : 172.18.4.2 (ports 16986, 42785, 12222,…)
Protocole utilisé : UDP
Type: Scannage de ports sur le routeur CISCO 172.18.4.2

10:41:39 à 10:41:40
IP Source : de 172.18.0.0:520 à 172.18.1.7:520
Destination : 172.18.4.2
Protocole utilisé : UDP
Type : Envoi requêtes UDP avec adresses IP différentes vers le routeur => IP Spoofing, et tentative de saturation du routeur

10:41:40 à 10:41:46
IP Source : - 192.5.5.241:53
(192.5.5.241: f.root-servers.net
IP range 192.5.4.0 - 192.5.5.255
Network name ISC-NET1
Infos Internet Systems Consortium, Inc.
Infos 950 Charter Street
Infos Redwood City
Infos CA
Infos 94063
Country United States (US)
Abuse E-mail abuse@isc.org)

192.112.36.4:53
(192.112.36.4: G.ROOT-SERVERS.NET)
128.63.2.53
(128.63.2.53: h.root-servers.net
IP range 128.63.0.0 - 128.63.255.255
Network name ARL-SUBNET
Infos Headquarters, USAISC
Infos NETC-ANC CONUS TNOSC
Infos Fort Huachuca
Infos AZ
Infos 85613-5000
Country United States (US)
Abuse E-mail domain-request@aims7.army.mil)

192.36.148.17
(192.36.148.17: i.root-servers.net
IP range 192.36.148.0 - 192.36.148.255
Network name I-ROOTSERVER
Infos Special net for DNS i.root-servers.net.
Country Sweden (SE)
Abuse E-mail liman@autonomica.se)
…

Destination : 172.18.4.2 sur différents ports : (41013, 59440, 67…)
Protocole utilisé : UDP
Type : Envoi requêtes UDP de 457 Bytes avec adresses IP publiques existantes vers le routeur => IP Spoofing
Walter

10:42:23
IP Source : 172.18.4.202
Destination : 172.18.4.2 :80
Temps : 1511 secondes de connexion
Protocole utilisé : TCP
Paquets envoyés : 540 Bytes
Type : Connexion par le port 80 (HTTP) en TCP pendant 1511 secondes. Cela pourrait être traduit par la connexion à distance qu'a établi l'attaque sur un poste client en mode graphique (rapporté par les autres pôles du groupe analyse suite à l'étude Wireshark/snort).
10:43:07
IP Source : 172.16.64.95
Destination : 172.18.4.2 :443
Temps : 1632 secondes de connexion
Protocole utilisé : TCP
Paquets envoyés : 2736 Bytes
Type : Connexion par le port 443 (HTTPS) en TCP pendant 1511 secondes. Cela pourrait être traduit par la connexion à distance qu'a établie l'attaque sur un poste client en mode graphique
10:43:41
IP Source : 172.16.80.20
Destination : 172.18.4.2 :80
Temps : 1614 secondes de connexion
Protocole utilisé : TCP
Paquets envoyés : 12240 Bytes
Type : Connexion par le port 80 (HTTP) en TCP pendant 1511 secondes. Cela pourrait être traduit par la connexion à distance qu'a établie l'attaque sur un poste client en mode graphique.
La taille importante des paquets échangés peut laisser entendre dire que cela correspond bien à la connexion à distance en mode graphique à la machine cliente.
10:44:33 à 10:45:03
IP Source : 172.16.64.92 sur les ports 43840, 43841, et 46439 à 46445
Envoi paquet de 9 secondes de 172.16.64.95:49785 à 172.18.4.2:443
Destination : 172.18.4.2 sur les ports 80, 443, 113, 554, 22, …)
Protocole utilisé : TCP
Paquets envoyés : 44 Bytes
Type : Scannage de ports sur le routeur CISCO 172.18.4.2
10:44:54
IP Source : 172.10.200.3:1153
Envoi paquets pendant 155 secondes
Destination : 172.16.80.1:53
Protocole utilisé : UDP
Paquets envoyés : 32 (2352 Bytes)

Type : Envoi au routeur de grosses requêtes UDP afin de le saturer

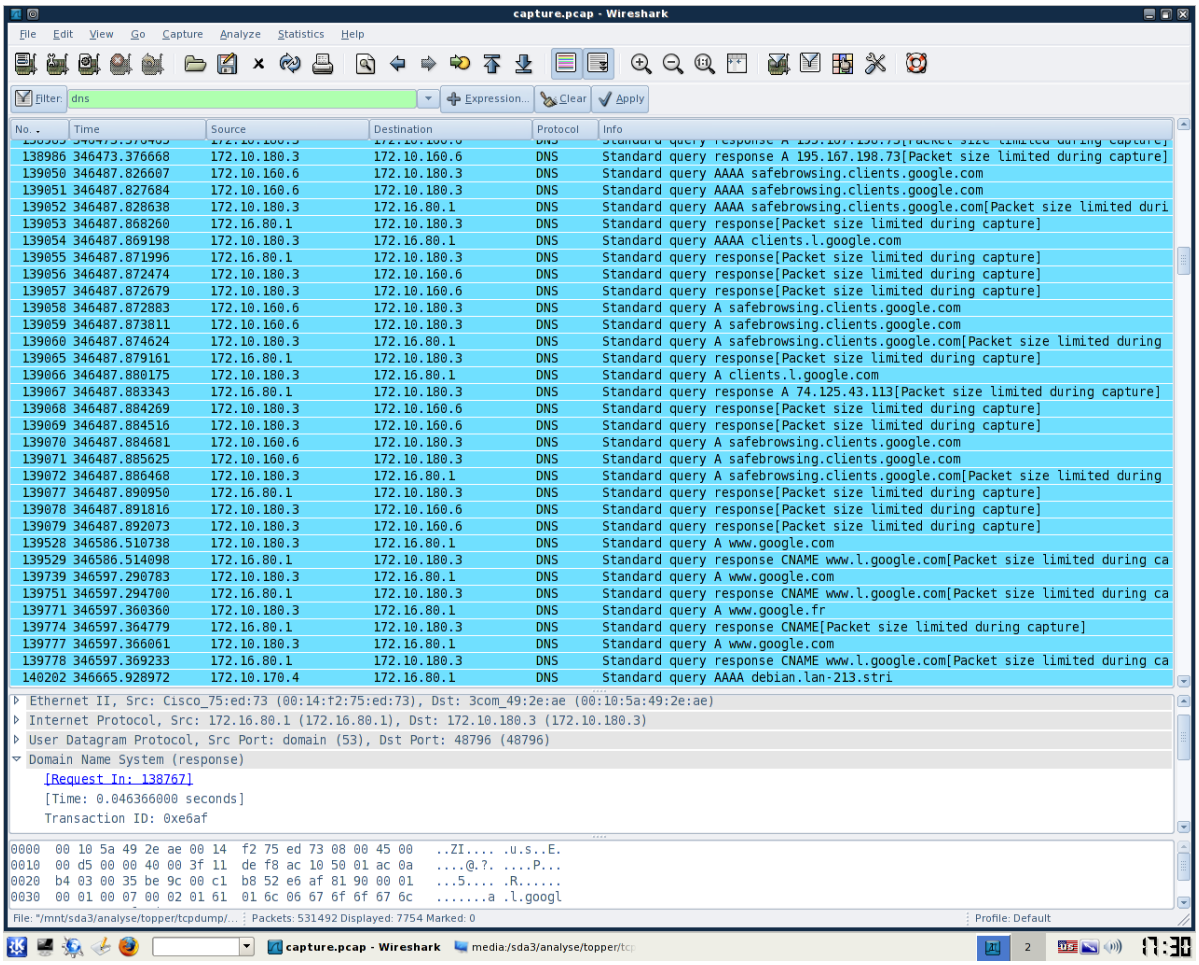
10:45:03 à 10:59:19
IP Source : 172.18.4.103
Envoi paquet de 9 secondes de 172.16.64.95:49785 à 172.18.4.2:443
Destination : 172.18.4.2 sur les ports 80, 443, 113, 554, 22, …)
Protocole utilisé : TCP
Paquets envoyés : 44 Bytes
Type : Scannage de ports sur le routeur CISCO 172.18.4.2

11 :04:07 à 11:04:48
IP Source : de 172.18.0.0:520 à 172.18.30.118:520
Destination : 172.18.4.2 :520
Protocole utilisé : UDP
Type : Envoi requêtes UDP avec adresses IP différentes vers le routeur => IP Spoofing pour saturation routeur

11 :06:28 à 11:09:16
IP Source : de 172.18.0.0:0 à 172.18.37.226:0
Destination : 172.18.4.2:8.0
Protocole utilisé : ICMP
Type : Tentative de saturation du routeur par l'envoi de requêtes ICMP provenant d'adresses IP différentes=> provoque une augmentation de temps de réponse du routeur.
Peut être utilisé pour noyer une attaque dans un flux d'informations inutiles, pour ne pas être détectée par les administrateurs de la défense ou par les analystes.

4. Annexe (Bilan des attaques 3° confrontation)

- DNS Flooding

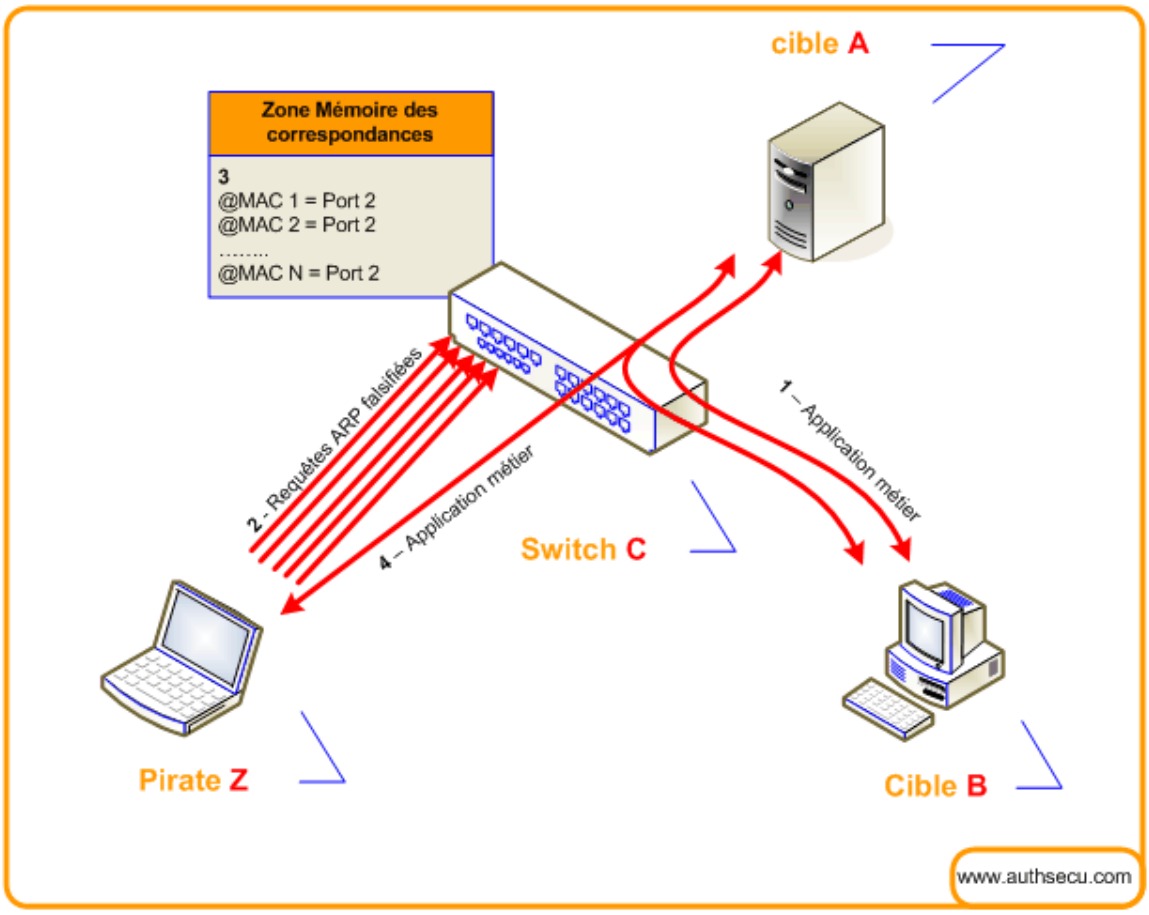


- MAC Flooding

basée sur l'envoi massif de requête et réponse ARP. Chaque requête doit avoir une adresse MAC différente, ainsi les différents Switchs du LAN vont apprendre cette correspondance entre l'adressa MAC et le port physique. Avec un envoi massif, le Switch saturera rapidement sa mémoire qui est limitée.

<u>les conséquences peuvent être multiple comme par exemple :</u>

- Buffers overflow de la mémoire gérant les correspondances (cette conséquence n'est plus réaliste de nos jours)
- Arrêt du fonctionnement du Switch ne pouvant plus commuter de trame
- Passage du Switch en mode HUB permettant ainsi à l'attaquant d'effectuer de l'écoute. Le schéma ci dessous montre le procédé :



1 - Les cibles A et B s'échangent des informations normalement
2 - Le pirate Z envoi plein de requêtes ARP avec des adresses MAC différentes
3 - Le Switch C met à jour sa table de correspondance jusqu'à saturation de la mémoire
4 - Les cibles A et B s'échangent des informations, mais le pirate les reçoit aussi du fait que le Switch fonctionne désormais en HUB

- Ils existent plusieurs possibilités afin d'éviter cette attaque.

Par exemple, il est possible :

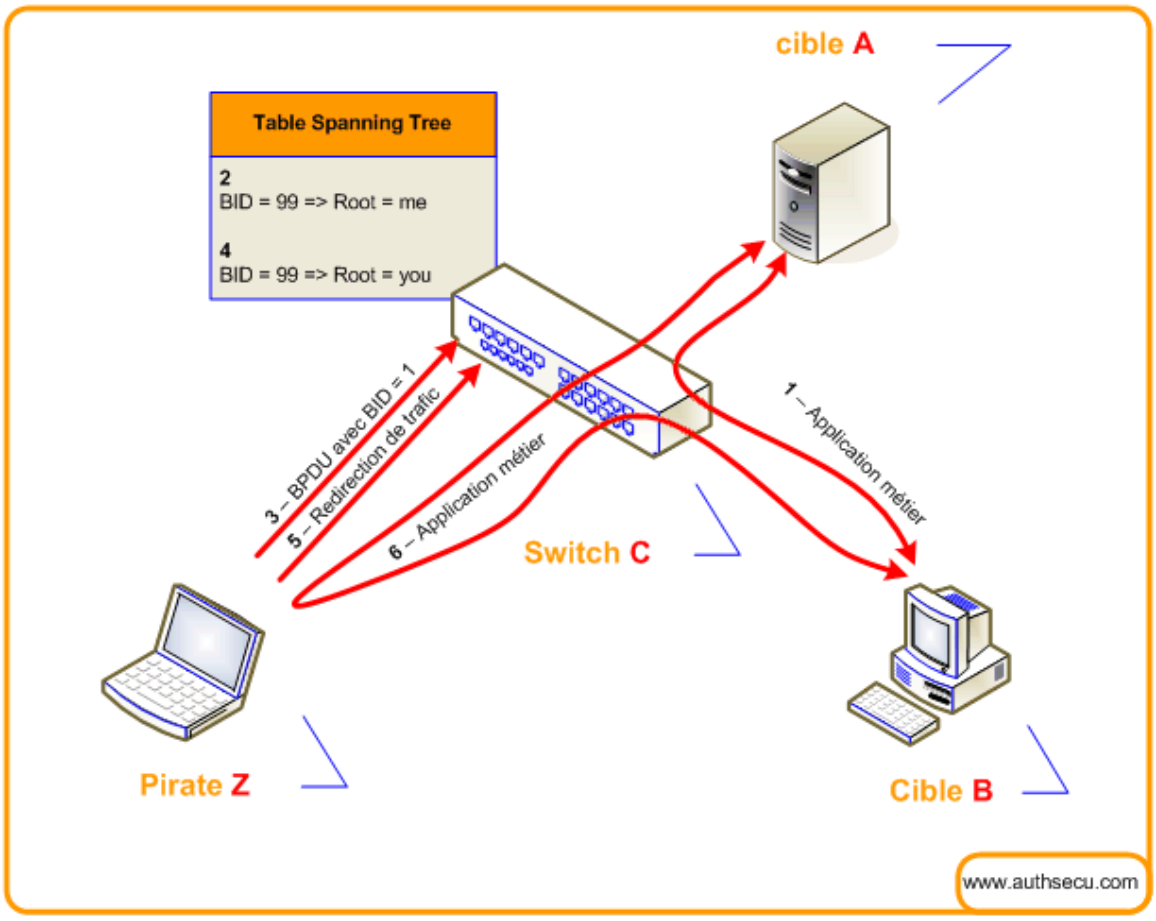
- De n'autoriser qu'une liste d'adresse MAC prédéfinie par port. Cisco propose cela via la commande "switchport port-security mac-address H.H.H"
- D'appliquer un filtre sur le nombre de correspondance maximum par port. 3 modes existent qui sont "protect", "restrict" et "shutdown"
- D'utiliser l'authentification 802.1X

• Attaques STP

Se base sur l'envoi de trames BPDU (bridge protocol data units) à destination du Switch cible. Dans un environnent Spanning-Tree, il y a un seul Switch qui est élu root (maître) servant de référence pour les coûts et les chemins. Ces trames BPDU émises avec un BID (Bridge ID) très petit, obligera les commutateurs à recalculer le nouveau root.

Cela dépend du constructeur, de l'équipement et de la version, mais les conséquences peuvent être multiple comme par exemple :

- Suite à la saturation processeur provoquée par les calculs permanents, les commutateurs ne commutent plus ou crash littéralement. Il est même possible que les Switchs basculent alors en mode HUB permettant ainsi à l'attaquant d'effectuer de l'écoute.
- Suite à l'envoi d'un BID plus petit que ceux des Switchs, l'attaquant se retrouvera alors élu comme maître de l'environnement Spanning-Tree. Ainsi, le hackeur pourra redéfinir la topologie à sa guise et ainsi intercepter tous les trafics qu'il désir.



1 - Les cibles finales A et B s'échangent des informations normalement
2 - Le Switchs est le maître du contexte Spanning Tree
3 - Le pirate Z envoi une trame BPDU avec un BID très faible
4 - Le commutateur admet que le pirate Z soit devenu le maître du contexte STP

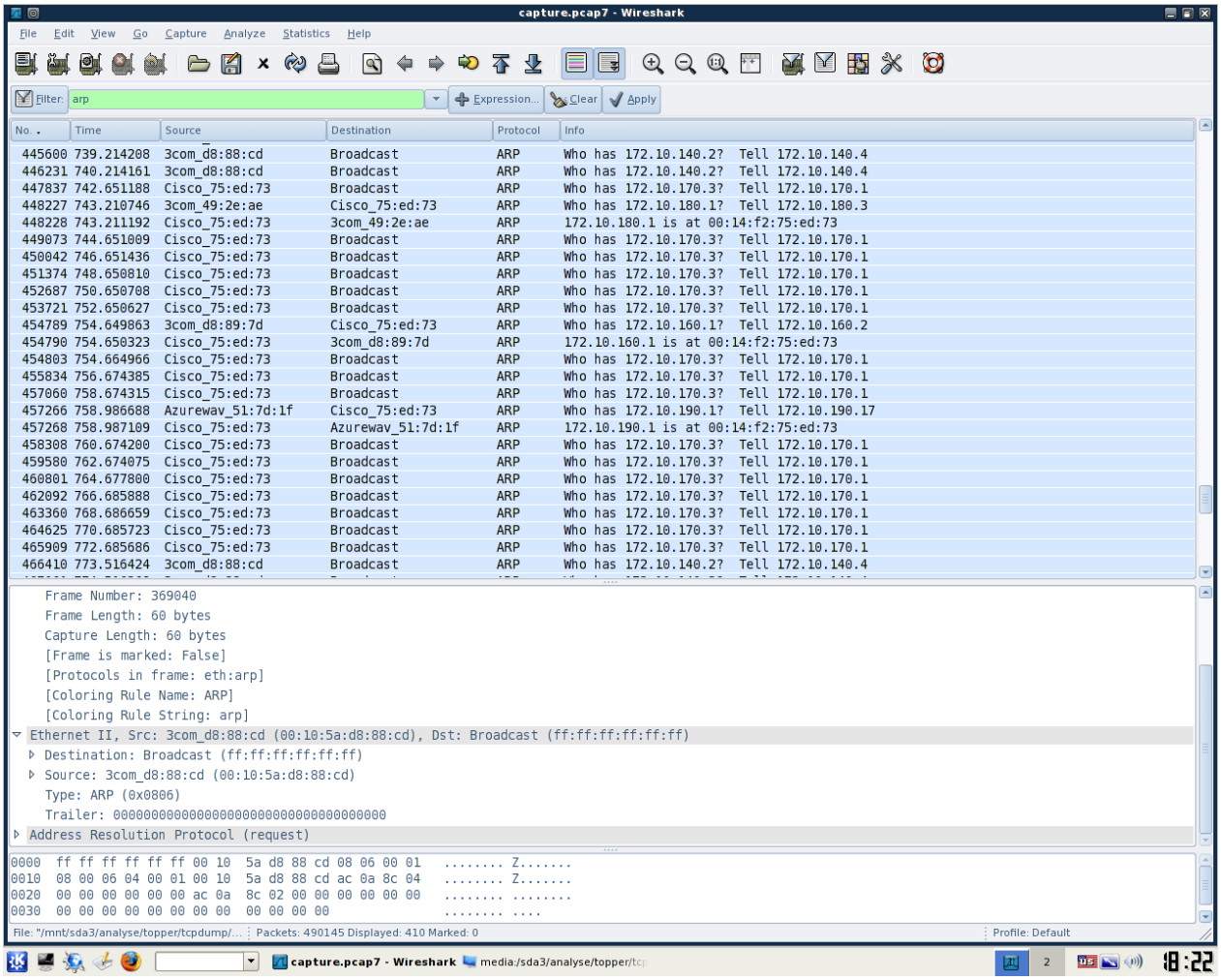
5 - Le hacker redéfinis la topologie afin de rediriger les flux vers lui
6 - Les cibles A et B s'échangent des informations, mais le pirate les reçoit aussi

Il existe plusieurs possibilités afin d'éviter cette attaque.

Par exemple, il est possible :

- D'activer STP (Spanning Tree Protocol) uniquement sur les ports interconnecté à un autre commutateur
- D'activer STRG (Spanning Tree Root Guard) sur les commutateurs permettant de laisser passer les BPDU tant que le port en question ne demande pas à devenir maître dans l'instance Spanngin Tree
- D'activer le BPDU Guard sur les Switchs afin de bloquer tous les type de message BPDU du port en question.

- ## ARP Flooding



- ## Mail Bombing

consiste à envoyer un nombre faramineux d'emails (plusieurs milliers par exemple) à un ou des destinataires. L'objectif étant de :

- saturer le serveur de mails

- saturer la bande passante du serveur et du ou des destinataires

- rendre impossible aux destinataires de continuer à utiliser l'adresse électronique.

Eviter cette attaque

Avant de prendre le risque d'avoir une adresse électronique inutilisable mieux vaut prendre ses précautions :

Si vous avez une adresse personnelle à laquelle vous tenez, ne la communiquez qu'aux personnes dignes de confiance, Créez vous un second compte de messagerie, pour tout ce qui est mailing list par exemple et groupe des discussion, ainsi, vous ne craignez pas de perdre d'informations vitales. Si ce compte est attaqué vous pourrez sans difficulté reprendre une autre adresse et vous ré-abonner. Utilisez eremove pour éviter les mail bombers.

No. .	Time	Source	Destination	Protocol	Info
6995	77.210918	172.16.80.73	172.10.200.3	SSH	Encrypted request packet len=80
6996	77.250699	172.10.200.3	172.16.80.73	TCP	ssh > 48382 [ACK] Seq=308129 Ack=55313 Win=8011 Len=0 TSV=295914713 TSER=17
6997	77.255294	172.16.80.73	172.10.200.3	SSH	Encrypted request packet len=64
6998	77.255329	172.10.200.3	172.16.80.73	TCP	ssh > 48382 [ACK] Seq=308129 Ack=55377 Win=8011 Len=0 TSV=295914714 TSER=17
6999	77.255614	172.10.200.3	172.16.80.73	SSH	Encrypted response packet len=32
7000	77.299748	172.16.80.73	172.10.200.3	TCP	48382 > ssh [ACK] Seq=55377 Ack=308161 Win=1891 Len=0 TSV=1755983 TSER=2959
7001	77.307746	172.10.140.3	172.18.4.102	SMTP	Response: 220 mx.candide-sa.com ESMTP Po
7002	77.310658	172.18.4.102	172.10.140.3	TCP	44253 > smtp [ACK] Seq=1 Ack=38 Win=5840 Len=0 TSV=279656113 TSER=303744537
7003	77.310848	172.18.4.102	172.10.140.3	SMTP	Command: XXXX tuxi.lan-211.stri
7004	77.310906	172.10.140.3	172.18.4.102	TCP	smtp > 44253 [ACK] Seq=38 Ack=25 Win=5792 Len=0 TSV=303744538 TSER=279656113
7005	77.311084	172.16.80.73	172.10.200.3	SSH	Encrypted request packet len=144
7006	77.311091	172.10.140.3	172.18.4.102	SMTP	Response: 502 5.5.2 Error: command not r
7007	77.312044	172.10.200.3	172.16.80.73	SSH	Encrypted response packet len=832
7008	77.312627	172.18.4.102	172.10.140.3	SMTP	Command: HELO tuxi.lan-211.stri
7009	77.312747	172.10.140.3	172.18.4.102	SMTP	Response: 250 mx.candide-sa.com
7010	77.314256	172.18.4.102	172.10.140.3	SMTP	Command: MAIL FROM:<root@tuxi.lan-211.s
7011	77.314485	172.16.80.73	172.10.200.3	TCP	48382 > ssh [ACK] Seq=55521 Ack=308993 Win=1891 Len=0 TSV=1755986 TSER=2959
7012	77.316578	172.10.140.3	172.18.4.102	SMTP	Response: 250 2.1.0 Ok
7013	77.320169	172.18.4.102	172.10.140.3	SMTP	Command: RCPT TO:<contact@candide-sa.co
7014	77.323657	172.10.140.3	172.18.4.102	SMTP	Response: 250 2.1.5 Ok
7015	77.326937	172.18.4.102	172.10.140.3	SMTP	Command: DATA
7016	77.327250	172.10.140.3	172.18.4.102	SMTP	Response: 354 End data with <CR><LF>.<CR
7017	77.329338	172.16.80.73	172.10.200.3	SSH	Encrypted request packet len=240
7018	77.332026	172.18.4.102	172.10.140.3	SMTP	DATA fragment, 30 bytes
7019	77.332198	172.18.4.102	172.10.140.3	SMTP	DATA fragment, 30 bytes
7020	77.332206	172.10.140.3	172.18.4.102	TCP	smtp > 44253 [ACK] Seq=167 Ack=1573 Win=8688 Len=0 TSV=303744543 TSER=279656
7021	77.332322	172.18.4.102	172.10.140.3	SMTP	DATA fragment, 30 bytes
7022	77.332389	172.10.140.3	172.18.4.102	TCP	smtp > 44253 [ACK] Seq=167 Ack=4221 Win=14480 Len=0 TSV=303744543 TSER=2796
7023	77.332531	172.18.4.102	172.10.140.3	SMTP	DATA fragment, 30 bytes
7024	77.334101	172.18.4.102	172.10.140.3	SMTP	DATA fragment, 30 bytes

- ## UDP Flooding

When a connection is established between two UDP services, each of which produces output, these two services can produce a very high number of packets that can lead to a denial of service on the machine(s) where the services are offered. Anyone with network connectivity can launch an attack; no account access is needed. For example, by connecting a host's chargen service to the echo service on the same or another machine, all affected machines may be effectively taken out of service because of the excessively high number of packets produced. In addition, if two or

more hosts are so connected, the intervening network may also become congested and deny service to all hosts whose traffic traverses that network.

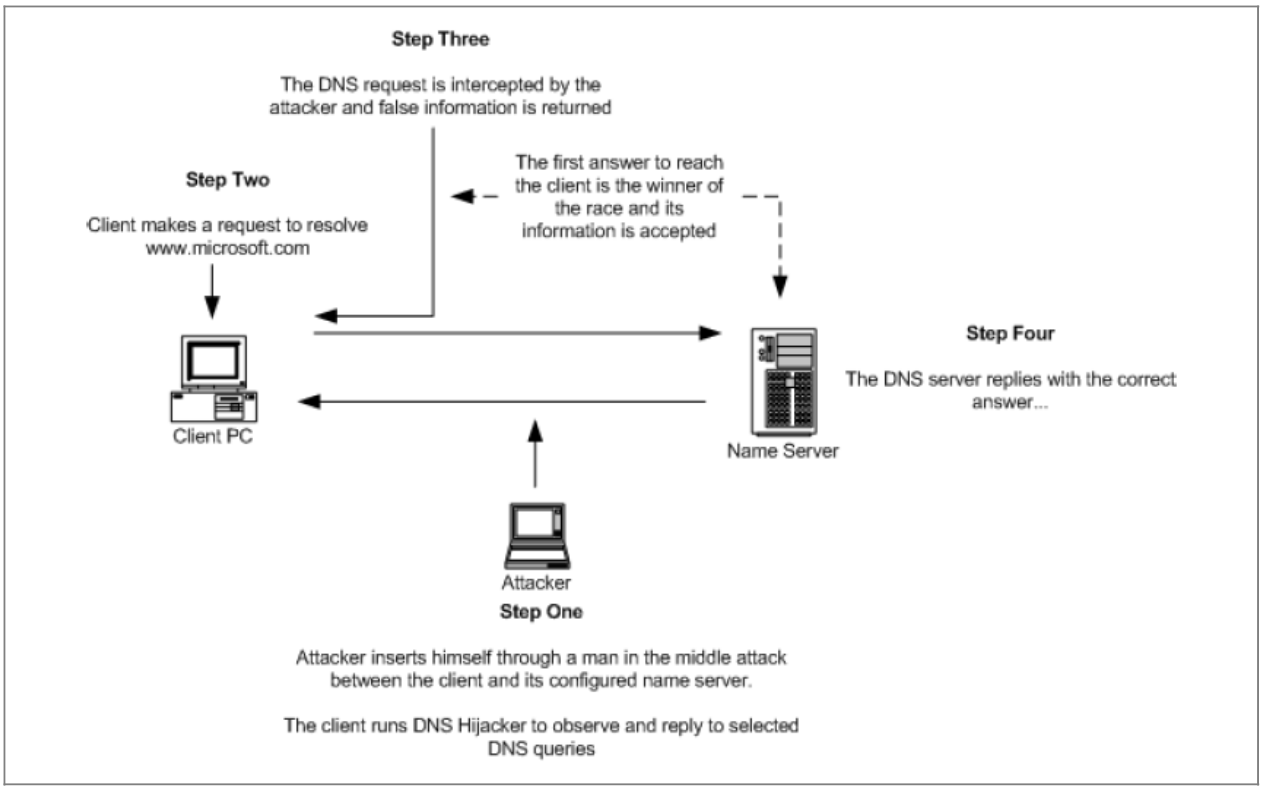
```
92592 943.863914  172.16.64.89        172.10.170.4        UDP      Source port: http  Destination port: mxxrlogin
92593 943.864063  172.16.64.89        172.10.170.4        UDP      Source port: http  Destination port: mxxrlogin
92594 943.864186  172.16.64.89        172.10.170.4        UDP      Source port: http  Destination port: mxxrlogin
92595 943.864306  172.16.64.89        172.10.170.4        UDP      Source port: http  Destination port: mxxrlogin
92600 943.964494  172.16.64.89        172.10.170.4        UDP      Source port: http  Destination port: mxxrlogin
92601 943.964619  172.16.64.89        172.10.170.4        UDP      Source port: http  Destination port: mxxrlogin
92602 943.964739  172.16.64.89        172.10.170.4        UDP      Source port: http  Destination port: mxxrlogin
92603 943.964858  172.16.64.89        172.10.170.4        UDP      Source port: http  Destination port: mxxrlogin
92608 944.283355  172.16.64.89        172.10.170.4        UDP      Source port: http  Destination port: mxxrlogin
92609 944.283477  172.16.64.89        172.10.170.4        UDP      Source port: http  Destination port: mxxrlogin
92610 944.283596  172.16.64.89        172.10.170.4        UDP      Source port: http  Destination port: mxxrlogin

Frame 92574 (135 bytes on wire, 96 bytes captured)
Ethernet II, Src: Cisco_75:ed:73 (00:14:f2:75:ed:73), Dst: 3com_d8:88:cd (00:10:5a:d8:88:cd)
Internet Protocol, Src: 172.16.64.89 (172.16.64.89), Dst: 172.10.170.4 (172.10.170.4)
User Datagram Protocol, Src Port: http (80), Dst Port: mxxrlogin (1035)
  Source port: http (80)
  Destination port: mxxrlogin (1035)
  Length: 101
⊞ Checksum: 0x9598
```

- Solutions:
  - **Disable and filter chargen and echo services**
  - **Disable and filter other unused UDP services.**
  - **If you must provide external access to some UDP services, consider using a proxy mechanism to protect that service from misuse**
  - **Monitor your network**
  - **Take steps against IP spoofing**

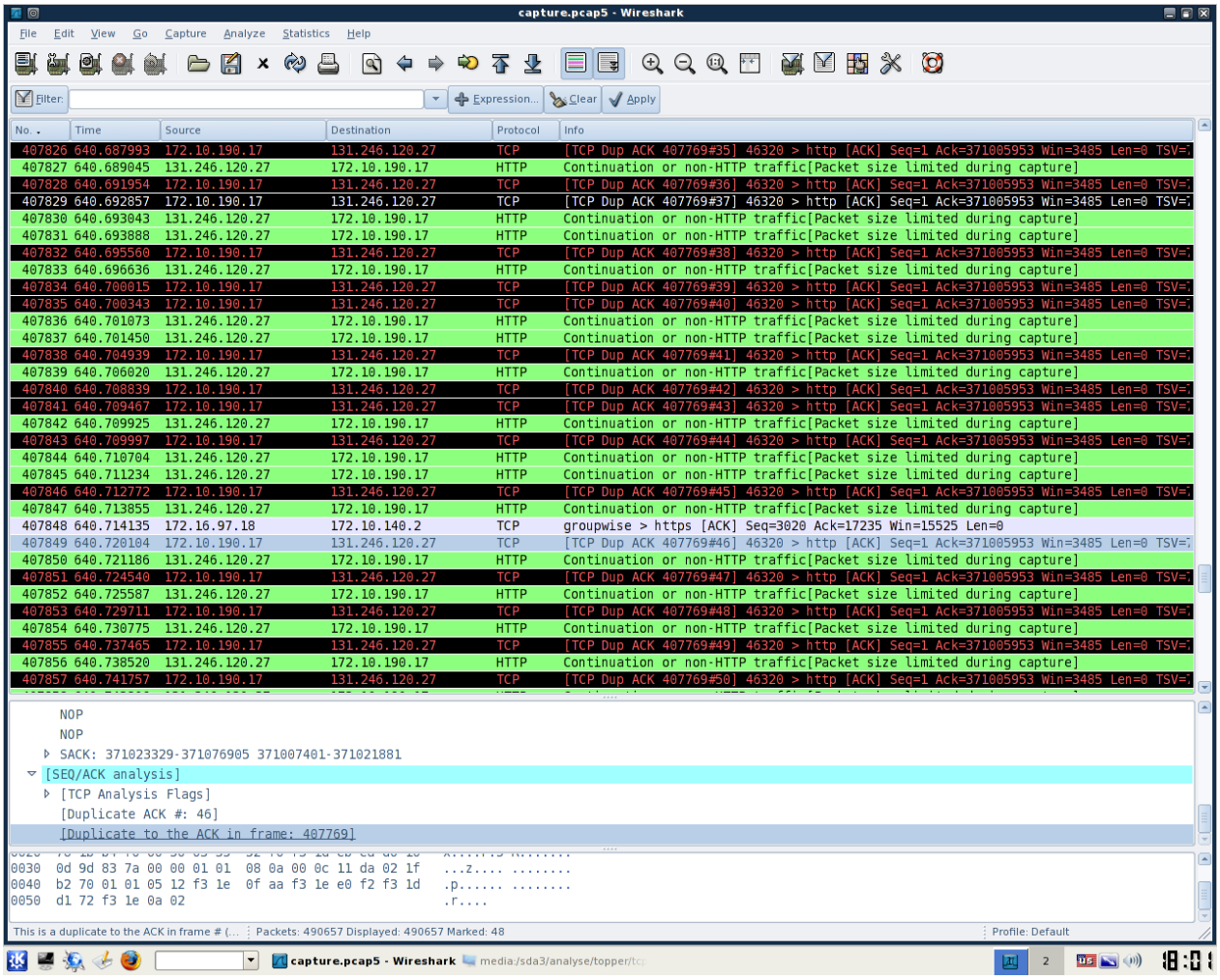
If an attacker is able to insert himself between the client and the DNS server he may be able to intercept replies to client name resolution queries and send false information mapping addresses to incorrect addresses. This type of attack is very much a race condition, in that the attacker needs to get his reply back to the client before the legitimate server does. The odds may be stacked in the favour of the client as a number of recursive queries may need to be made and the attacker may be able to slow the client's primary DNS server down by using a denial of service attack.

• DNS Hijacking

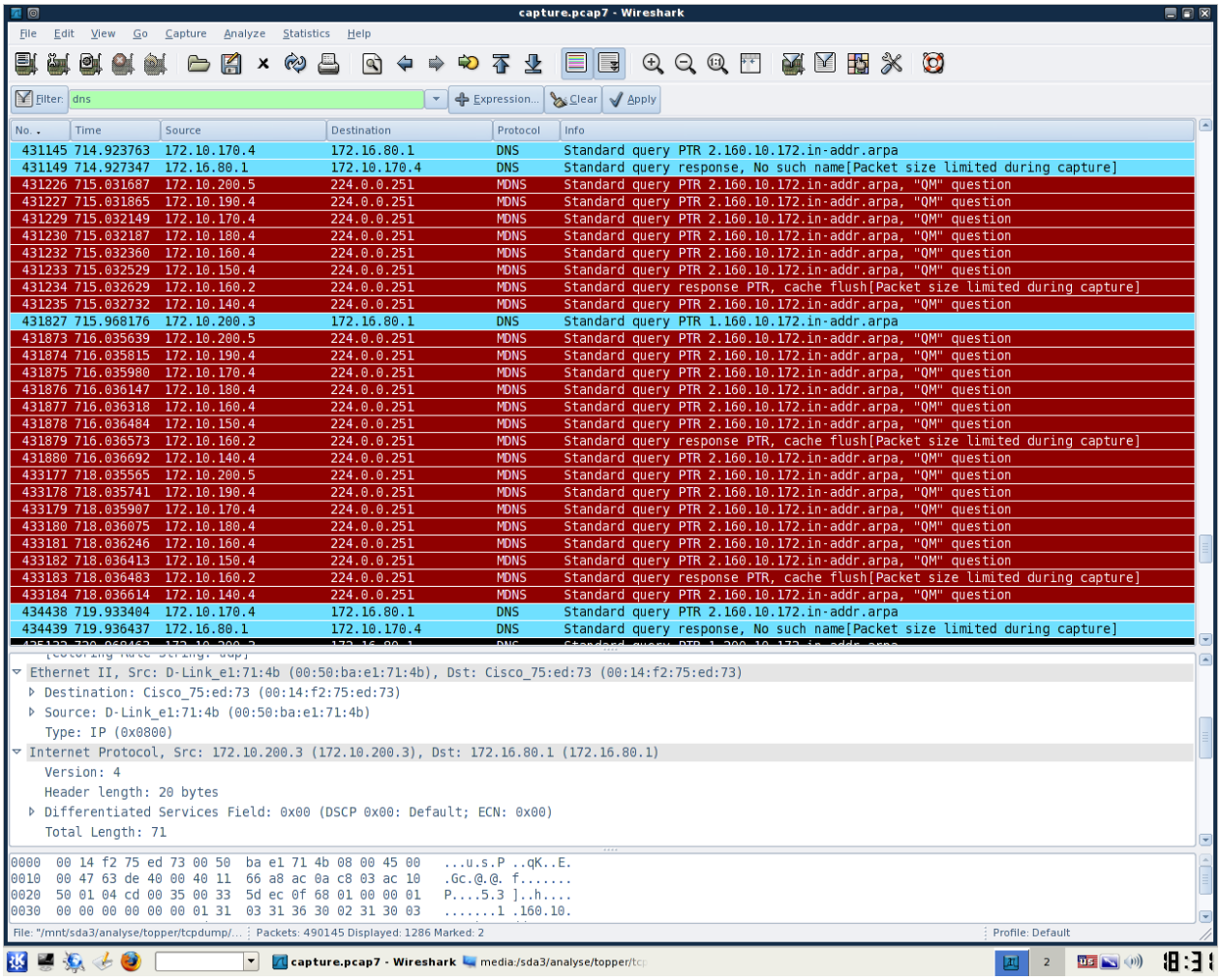
If an attacker is able to insert himself between the client and the DNS server he may be able to intercept replies to client name resolution queries and send false information mapping addresses to incorrect addresses. This type of attack is very much a race condition, in that the attacker needs to get his reply back to the client before the legitimate server does. The odds may be stacked in the favour of the client as a number of recursive queries may need to be made and the attacker may be able to slow the client's primary DNS server down by using a denial of service attack.


Step Three
The DNS request is intercepted by the attacker and false information is returned
Step Two
Client makes a request to resolve www.microsoft.com
The first answer to reach the client is the winner of the race and its information is accepted
Client PC
Name Server
Step Four
The DNS server replies with the correct answer...
Attacker
Step One
Attacker inserts himself through a man in the middle attack between the client and its configured name server.
The client runs DNS Hijacker to observe and reply to selected DNS queries

- TCP Dup Ack



- Multicast DNS


capture.pcap7 - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: dns
Expression... Clear Apply
No. Time Source Destination Protocol Info
431145 714.923763 172.10.170.4 172.16.80.1 DNS Standard query PTR 2.160.10.172.in-addr.arpa
431149 714.927347 172.16.80.1 172.10.170.4 DNS Standard query response, No such name[Packet size limited during capture]
431226 715.031687 172.10.200.5 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
431227 715.031865 172.10.190.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
431229 715.032149 172.10.170.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
431230 715.032187 172.10.180.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
431232 715.032360 172.10.160.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
431233 715.032529 172.10.150.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
431234 715.032629 172.10.160.2 224.0.0.251 MDNS Standard query response PTR, cache flush[Packet size limited during capture]
431235 715.032732 172.10.140.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
431827 715.968176 172.10.200.3 172.16.80.1 DNS Standard query PTR 1.160.10.172.in-addr.arpa
431873 716.035639 172.10.200.5 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
431874 716.035815 172.10.190.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
431875 716.035980 172.10.170.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
431876 716.036147 172.10.180.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
431877 716.036318 172.10.160.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
431878 716.036484 172.10.150.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
431879 716.036573 172.10.160.2 224.0.0.251 MDNS Standard query response PTR, cache flush[Packet size limited during capture]
431880 716.036692 172.10.140.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
433177 718.035565 172.10.200.5 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
433178 718.035741 172.10.190.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
433179 718.035907 172.10.170.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
433180 718.036075 172.10.180.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
433181 718.036246 172.10.160.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
433182 718.036413 172.10.150.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
433183 718.036483 172.10.160.2 224.0.0.251 MDNS Standard query response PTR, cache flush[Packet size limited during capture]
433184 718.036614 172.10.140.4 224.0.0.251 MDNS Standard query PTR 2.160.10.172.in-addr.arpa, "QM" question
434438 719.933404 172.10.170.4 172.16.80.1 DNS Standard query PTR 2.160.10.172.in-addr.arpa
434439 719.936437 172.16.80.1 172.10.170.4 DNS Standard query response, No such name[Packet size limited during capture]
Ethernet II, Src: D-Link_e1:71:4b (00:50:ba:e1:71:4b), Dst: Cisco_75:ed:73 (00:14:f2:75:ed:73)
Destination: Cisco_75:ed:73 (00:14:f2:75:ed:73)
Source: D-Link_e1:71:4b (00:50:ba:e1:71:4b)
Type: IP (0x0800)
Internet Protocol, Src: 172.10.200.3 (172.10.200.3), Dst: 172.16.80.1 (172.16.80.1)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 71
0000 00 14 f2 75 ed 73 00 50 ba e1 71 4b 08 00 45 00 ...u.s.P ..qK..E.
0010 00 47 63 de 40 00 40 11 66 a8 ac 0a c8 03 ac 10 .Gc.@.@. f.....
0020 50 01 04 cd 00 35 00 33 5d ec 0f 68 01 00 00 01 P....5.3]..h....
0030 00 00 00 00 00 00 01 31 03 31 36 30 02 31 30 03 ....1 .160.10.
File: "/mnt/sda3/analyse/topper/tcpdump/... Packets: 490145 Displayed: 1286 Marked: 2 Profile: Default
capture.pcap7 - Wireshark media:/sda3/analyse/topper/tc