N° d'ordre:
N° de série:

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université d'El-Oued

Faculté de Sciences et de Technologie

Mémoire fin de cycleprésenté en vue de l'obtention du diplôme de

LICENCE ACADEMIQUE

Domaine Mathématiques et Informatique

Département d'Informatique

Filière : Informatique

Thème

La protection du réseau local conter les attaques: La mise en place d'un IPS

Présenté par:

BELABEL Mohammed larbi

DEYAT Ayoub

Encadré par:

Mr.Gharbi Kaddour

Année Universitaire 2013/2014

Dédicace

Nous dédions ce modeste et humble mémoire à toute personne soit de prés ou de loin, ayant eu la bonté de nous soutenir et de nous aider tout au long de l'élaboration de cette rude tâche qui nous a pris un temps très précieux.

Nous dédions aussi notre travail à tous nos enseignants (es), à toute notre grande famille, à nos amis et à tous nos collègues de la promotion 2014.

Avec sincérité et fidélité, je vous embrasse tous très très fort.

Remerciement

En premier, je remercie le Tout Puissant ALLAH, notre créateur qui m'a donné la force d'accomplir ce travail.

Je tiens à remercier vivement, le chargé du suivi de ce travail,

Monsieur ***GHARBI KADDOUR*** pour ses encouragements, ses conseils précieux et sa disponibilité.

Je présente mes chaleureux remerciements aux enseignants et touts les étudiants du département informatique pour leurs aides et orientations durant ma formation.

Et à tous ceux qui ont participé de prés ou de loin à la réalisation de ce travail.

Résumé:

de nos jours où tout est informatisé, l'ordinateur est un outil stratégique dans tous les domaines, tant professionnels que personnels. La question que l'on se pose est de savoir comment penser à la sécurité de cet indispensable outil .

Aujourd'hui les systèmes d'information des entreprises sont de plus en plus ouverts sur le réseau des réseaux (Intenet). Ainsi la mise en place des mesures sécuritaires devient une condition nécessaire, mais pas suffisante pour se protéger des risques présents sur la toile internet.

Pour se protéger systèmes informatiques contre les attaques , le plus souvent on utilise: les pare-feu , et pour surveiller les attaques les systèmes de détection d'intrusions. Pourtant, la détection des intrus ne suffit point. Cela ne servira à rien de détecter une attaque, si l'on n'est pas capable de la faire échouer. La solution est de construire un système de prévention des attaques . ce rapport explique comment construire un tel système et comment le maintenir.

الملخص:

في الوقت الحاضر عندما يكون كل شيء على الكمبيوتر، و يصبح هذا الأخير أداة مهنية والشخصية في جميع المجالات. السؤال الذي يطرح نفسه هو كيفية التفكير بشأن سلامة هذه الأداة الأساسية.

ان شركات والأداراة اليوم أصبحت أكثر انفتاحا على شبكات ولهذا فإن تنفيذ التدابير الأمنية هو ضروري، ولكن ليس كافيا للحماية ضد المخاطر الموجودة داخل الإنترنت.

لحماية أنظمة الكمبيوتر ضد الهجمات، غالبا ما تستخدم: الجدران النارية وأنظمة كشف التسلل ورصد الهجمات ومع ذلك، فإن كشف الدخيل ليست كافية. وهذا لن يساعد على الكشف عن هجوم، إذا لم يكن قادرا على افشالها. الحل هو بناء نظام لمنع وقوع هجمات. ويصف هذا التقرير كيفية بناء مثل هذا النظام وكيفية الحفاظ عليه.

Sommaire

1-Introduction et Proplématique :

Aujourd'hui les systèmes d'information des entreprises sont de plus en plus ouverts sur le réseau des réseaux (Intenet). Ainsi la mise en place des mesures sécuritaires devient une condition nécessaire, mais pas suffisante pour se protéger des risques présents sur la toile internet.

Ainsi les entreprises commencent à prendre conscience de l'importance de la sécurité informatique et intègrent des mécanismes de sécurité dans leurs architectures réseaux. De plus la mise en place d'une politique de sécurité informatique autour de ces systèmes d'information et détecter d'éventuelles intrusions devient une nécessité pour estimer la complétude de cette politique de sécurité.

Dans cette perspective, outre la mise en place de pare-feu et des systèmes d'authentification sécurisés, les systèmes de détection d'intrusions (IDS) et les systèmes de protection d'intrusions (IPS) interviennent pour assurer une protection efficace face aux tentatives intrusives des systèmes d'information.

Pour se protéger un systèmes informatiques contre les attaques , le plus souvent on utilise: les pare-feu ; et pour surveiller les attaques les systèmes de détection d'intrusions. Pourtant, la détection des intrus ne suffit point. Cela ne servira à rien de détecter une attaque, si l'on n'est pas capable de la faire échouer. La solution est de construire un système de prévention des attaques . ce rapport explique comment construire un tel système et comment le maintenir.

2- Le système de prévention d'intrusions(IPS):[1]

2-1-Définition:

IPS (Intrusion Prevention System) est une offre logicielle qui est conçue pour identifier, référencer et bloquer le trafic malveillant avant qu'il ne compromette la continuité de votre activité.

2-2-Avantages et limites de l'IPS :

- Avantage **:**

L'IPS peut comporter plusieurs outils et méthodes pour empêcher les attaquants d'accéder au réseau, tels qu'un coupe-feu et un antivirus.

- Limite **:**

L'IPS peut faire des fausses alertes en raison des similitudes entre l'information valide et des attaques malveillantes. Le mécanisme de contrôle de sécurité lié au signalement perd ainsi de la crédibilité.

2-3-Les types d'IPS :

dans le cadre de cette présentation nous allons présenter deux type d'ips :

2-3-1- IPS cisco :

Cisco IPS 4200 Series Sensors

Rich Media Performance: 300 Mbps

Perfromance transactionnel: 250 MBPS

Figure 1 :IPS cisco

2-3-2- snort : .[2]

Les systèmes de détection d'intrusion ou IDS pour (Intrusion Détection System) sont indispensables pour la sécurité du réseau, ils permettent (comme leur nom l'indique) de détecter les tentatives d'intrusions, et ceci en se basant sur une base de signatures des différentes attaques connues, donc leur fonctionnement est semblable à celui des anti-virus

a) Définition

Snort est un système de détection d'intrusions réseau en Open Source, capable d'effectuer l'analyse du trafic en temps réel. On l'utilise en général pour détecter une variété d'attaques et de scans tels que des débordements de tampons, des scans de ports furtifs, des attaques CGI, des scans SMB, des tentatives d'identification d'OS, et bien plus.

Snort permet d'analyser le trafic réseau, il peut être configuré pour fonctionner en plusieurs modes :

- Le mode sniffer : dans ce mode, SNORT lit les paquets circulant sur le réseau et les affiche d'une façon continue sur l'écran
- Le mode « packet logger » : dans ce mode SNORT journalise le trafic réseau dans des répertoires sur le disque
- Le mode détecteur d'intrusion réseau (NIDS) : dans ce mode, SNORT analyse le trafic du réseau, compare ce trafic à des règles déjà définies par l'utilisateur et établi des actions à exécuter
- Le mode Prévention des intrusions réseau (IPS) : c'est SNOR Tinline.

b) Que permet-il de faire exactement ?

Snort capture des paquets sur un point d'un réseau IP, analyse le flux obtenu en temps réel, et compare le trafic réseau à une base de données d'attaques connues. Les attaques connues sont répertoriées dans des librairies de règles mises à jour par plusieurs communautés très actives.

Snort peut également être utilisé avec d'autres modules compatibles (tels que des interfaces graphiques, des actualisateurs de librairies d'attaques indépendants, etc.) Snort est compatible avec la plus part des OS. Windows, Mac, Linux Ubuntu, CentOS, OpenSuSE …

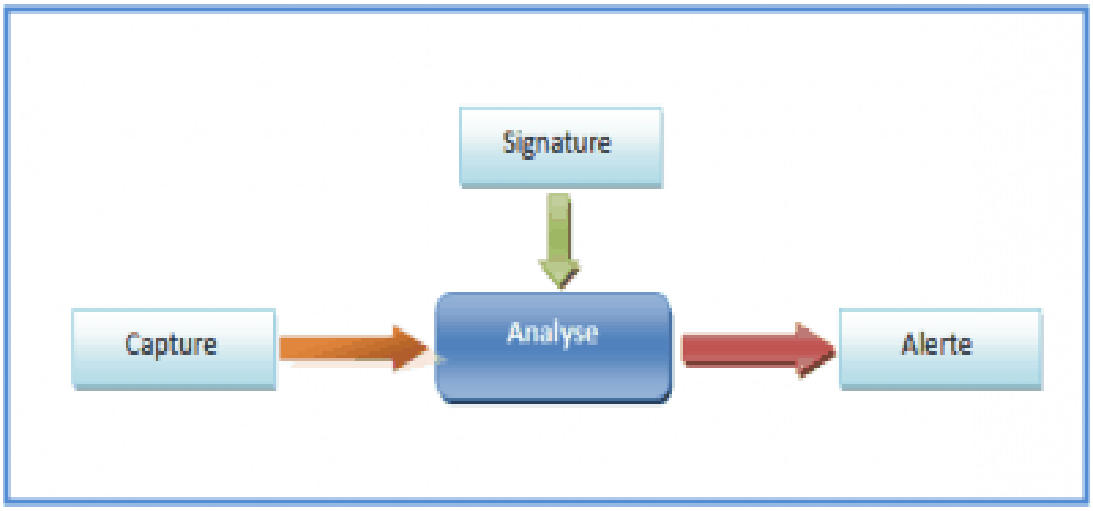


Figure 2 :Principe de l'analyse de Snort

c) Architecture du Snort :

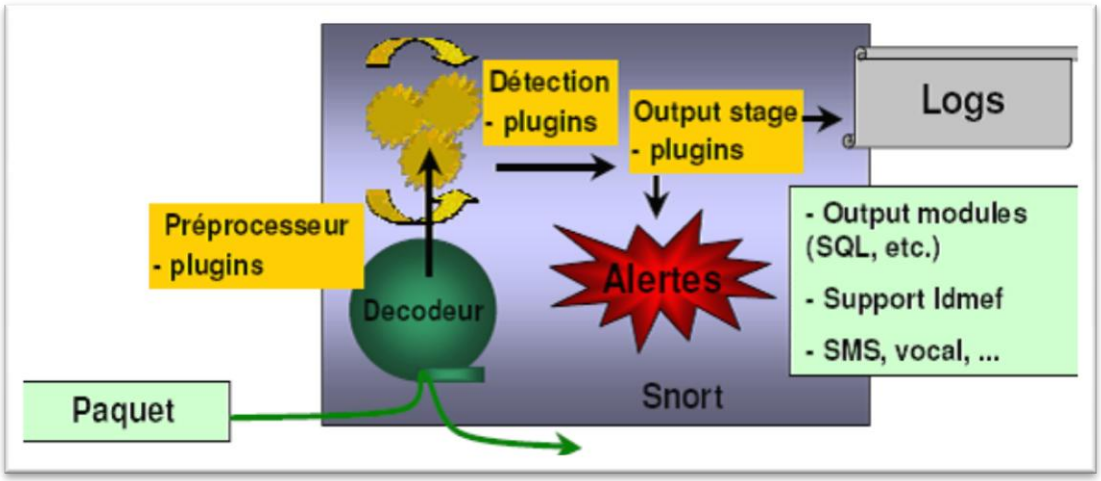


Figure 3 :Architecture du Snort

Un noyau de base :

(Packet Decoder) au démarrage, ce noyau charge un ensemble de règles, les compile, les optimise et les classe. Durant l'exécution, le rôle principal du noyau est la capture des paquets.

Une série de pré–processeurs:

(Détection Engine) ces derniers améliorent les possibilités de SNORT en matière d'analyse et de recomposition du trafic Capturé. Ils reçoivent les paquets directement capturés et décodés, les retravaillent éventuellement puis les fournissent au moteur de recherche des signatures pour les comparer avec la base des signatures.

Une série de « détection plugins »:Ces analyses se composent principalement de comparaison entre les différents champs des headers des protocoles (IP, ICMP, TCP et UDP) par rapport à des valeurs précises.

Une série de « output plugins »:

Permet de traiter cette intrusion de plusieurs manières : envoie vers un fichier log, envoie d'un message d'alerte vers un serveur syslog, stocker cette intrusion dans une base de données SQL.

d) les Positionner de Snort dans le réseau :

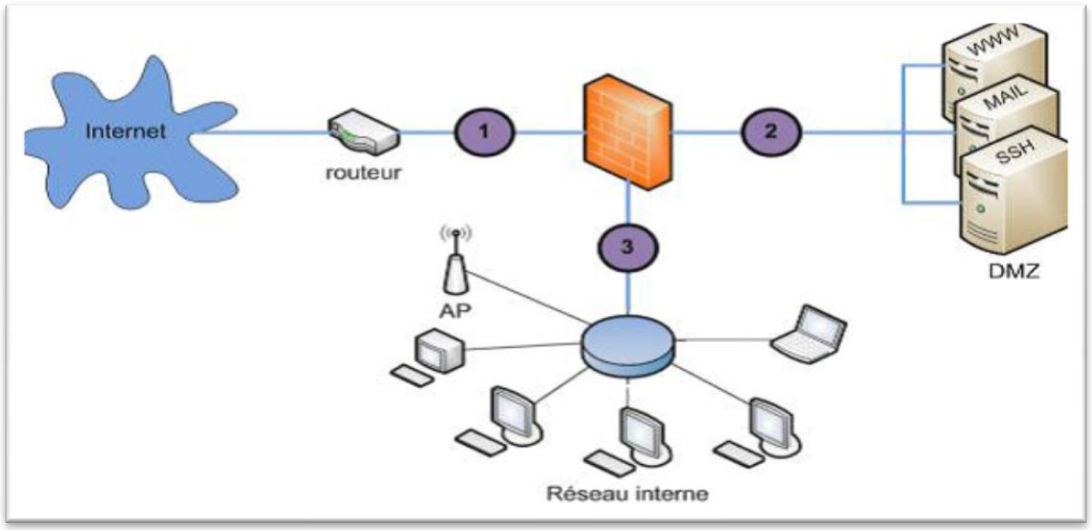


Figure 4 :positionner de Snort dansle réseau

Position 1 : Sur cette position, Snort va pouvoir détecter l'ensemble des attaques frontales, provenant de l'extérieur, en amont du firewall. Ainsi, beaucoup d'alertes seront remontées ce qui rendra les logs difficilement consultables.

Position 2: Si Snort est placé sur la DMZ, il détectera les attaques qui n'ont pas été filtrées par le firewall et qui relèvent d'un certain niveau de compétence. Les logs seront ici plus clairs à consulter puisque les attaques bénignes ne seront pas recensées.

Position 3 : Snort peut ici rendre compte des attaques internes, provenant du réseau local de l'entreprise. Il peut être judicieux d'en placer un à cet endroit étant donné le fait que 80% des attaques proviennent de l'intérieur. De plus, si des trojans ont contaminé le parc informatique (navigation peu méfiante sur internet) ils pourront être ici facilement identifiés pour être ensuite éradiqués.

Ce dernier positionnement est celui que j'ai testé pendant mon stage. Pourquoi ?

Le temps du stage n'étant pas infini, j'ai choisi de m'intéresser à la détection des intrusions qui ont réussi à entrer dans l'enceinte du réseau. Le web regorge d'activités malveillantes qui ne nous concernent pas forcément. Donc la position 3 me parait de loin la plus pertinente. De plus les failles les plus répandues proviennent généralement de l'intérieur de l'entreprise, et non de l'extérieur.

3-Les diagrammes de fonctionnement de notre système préventive

a\ daigramme d'IPs

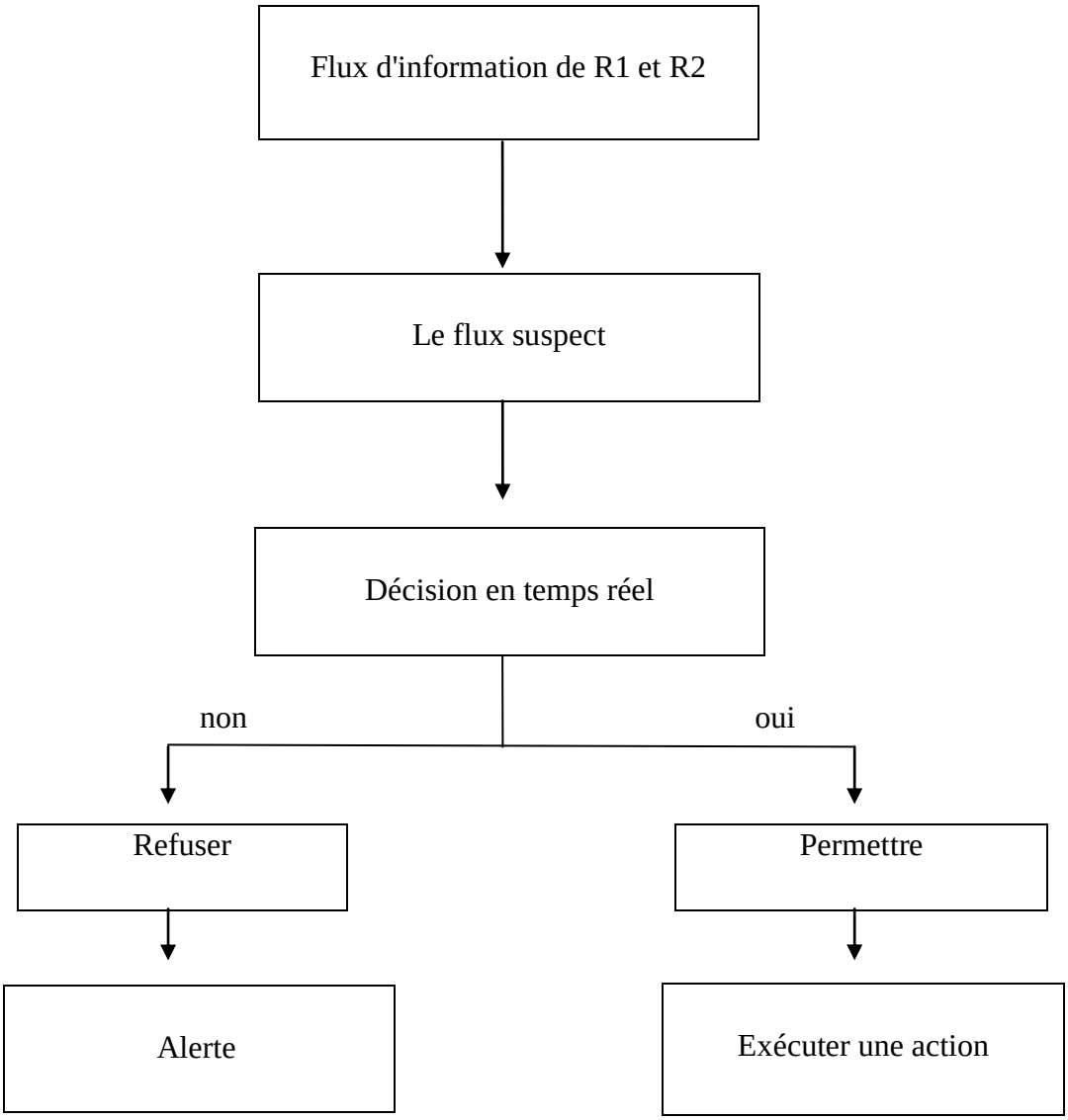


Figure 5: Fonctionnement d'IPS

b\ daigramme d'IDS snort

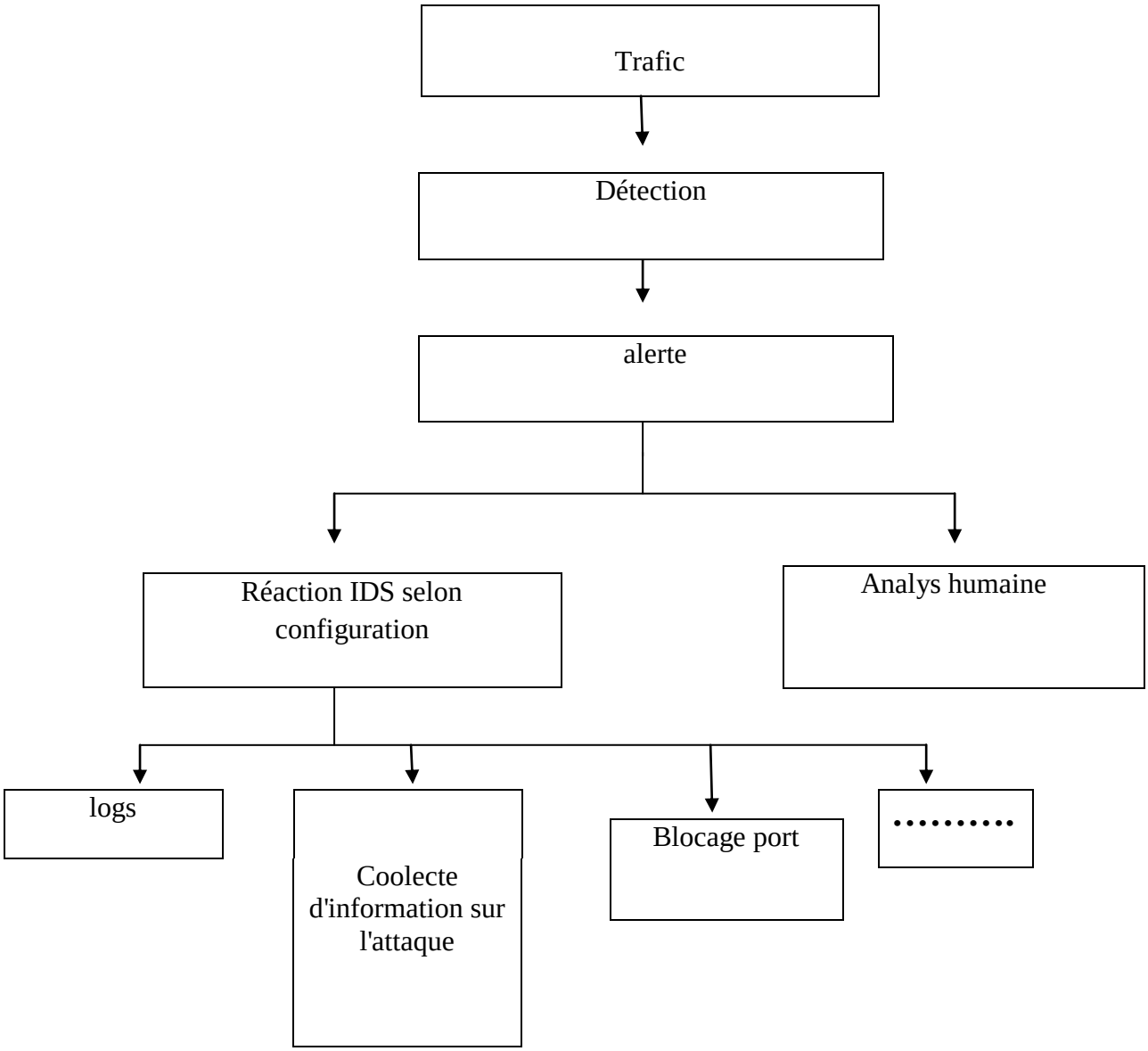


Figure 6: fonctionnement d'IDS snort

4-Implementation

3-1- Outils :

dans le cadre de cette rapport nous allons présenter deux les Outils

3-1-1-GNS3 :[3]

Définitioin :

GNS3 (Graphical Network Simulator) est un simulateur de réseau graphique qui permet l'émulation des réseaux complexes. Ces programmes vous permettent d'exécuter plusieurs systèmes d'exploitation tels que Windows ou Linux dans un environnement virtuel. GNS3 permet le même type de d'émulation à l'aide de Cisco Internetwork Operating Systems. Il vous permet d'exécuter un IOS Cisco dans un environnement virtuel sur votre ordinateur. GNS3 est une interface graphique pour un produit appelé Dynagen. Dynamips est le programme de base qui permet l'émulation d'IOS. Dynagen s'exécute au-dessus de Dynamips pour créer un environnement plus convivial, basé sur le texte environnement. Un utilisateur peut créer des topologies de réseau de Windows en utilisant de simples fichiers de type ini.

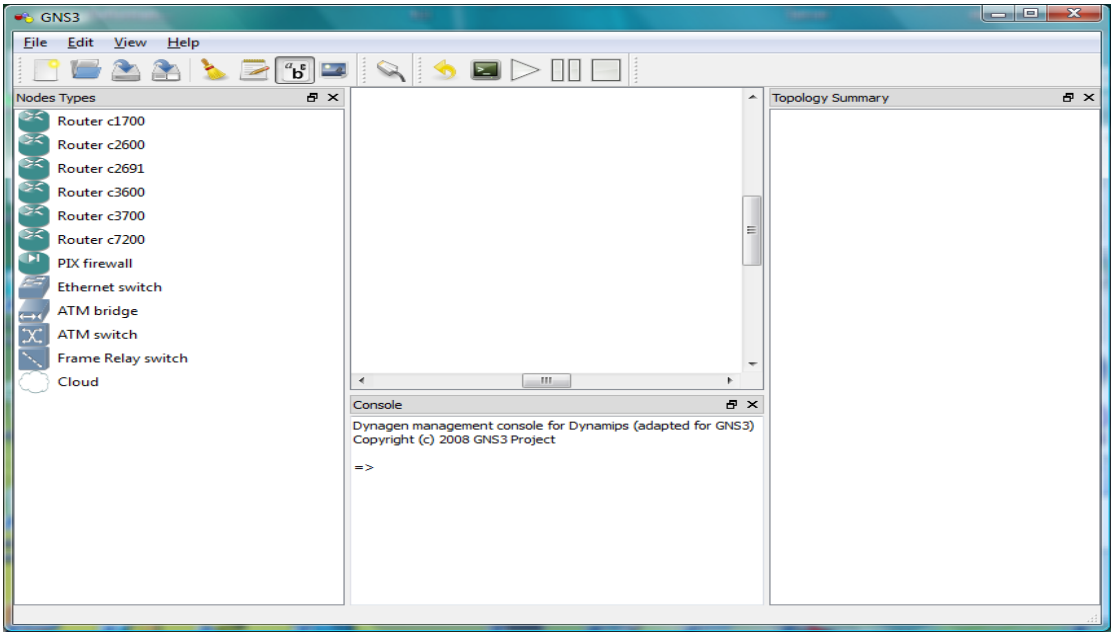


Figure 7 : l'interface principale

définition des fichiers Cisco IOS :

Comme mentionné précédemment, vous devez fournir votre propre Cisco IOS à utiliser avec GNS3 en raison de problèmes de licences. GNS3 est destiné à être utilisé

dans un environnement de laboratoire pour tester et apprendre. Une fois que vous avez obtenu votre propre copie d'un logiciel IOS de Cisco pour l'un des les plates-formes supportées, vous êtes prêt à continuer. Plates-formes actuelles pris en charge incluent:

- 1710
- 1720
- 1721
- 1750
- 1751
- 1760
- 2610
- 2610XM
- 2611
- 2611XM
- 2620
- 2620XM
- 2621
- 2621XM
- 2650XM
- 2651XM
- 2691
- 3620
- 3640
- 3660
- 3725
- 3745
- 7200

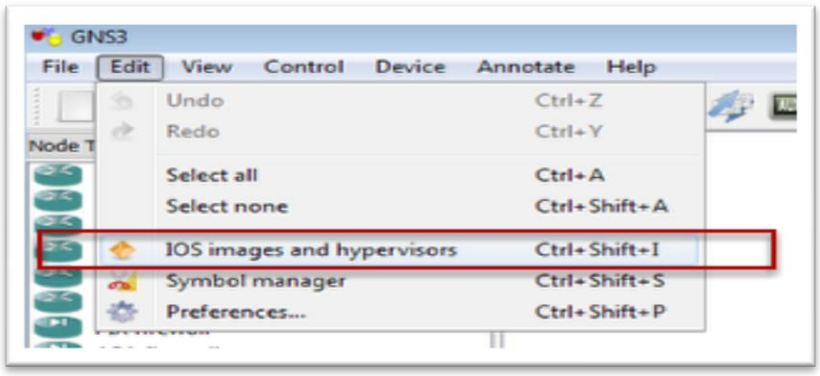


Figure 8 : menu Edit

Dans le menu Edit, choisissez se IOS image and hypervisors.

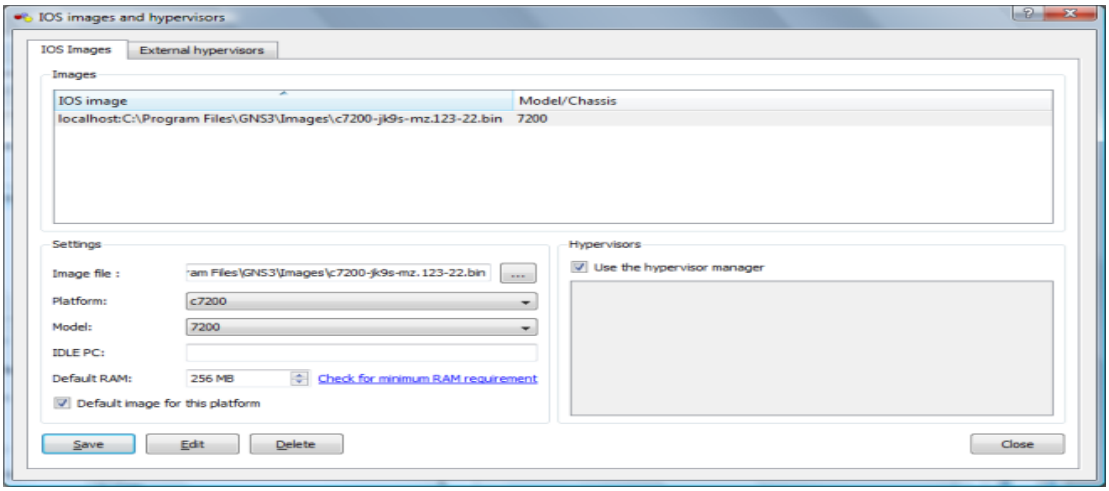


Figure 9 : Ajouter ios image

Sous l'onglet IOS Images, cliquez sur ... puis trouver votre logiciel IOS de Cisco déposer et cliquez sur Ouvrir. Le fichier apparaît sous la forme de votre fichier image

3-1-2. Machine Virtuelle :

La virtualisation consiste à faire fonctionner sur un seul ordinateur plusieurs systèmes d'exploitation comme s'ils fonctionnaient sur des ordinateurs distincts.

a) Définition **:**

Le logiciel que nous allons ici utiliser est VMware Workstation. Dans la série VMware, c'est celui qui est le mieux adapté à une utilisation « simple », càd sans gestion de dizaines de machines simultannées.

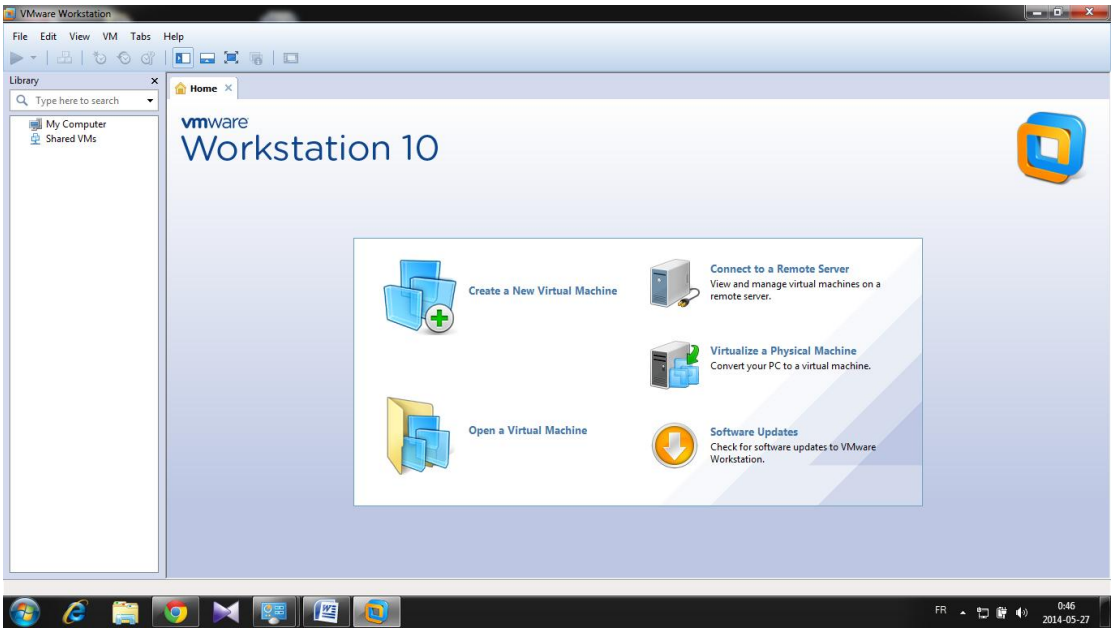


Figure 10 : interface prancipale vmware

b) Création de la machine virtuelle :

Dans notre exemple, j'ai utilisé un ISO d'un Windows Serveur 2003 R2

1. Lancez VMware Workstation. Vous vous retrouvez ici :

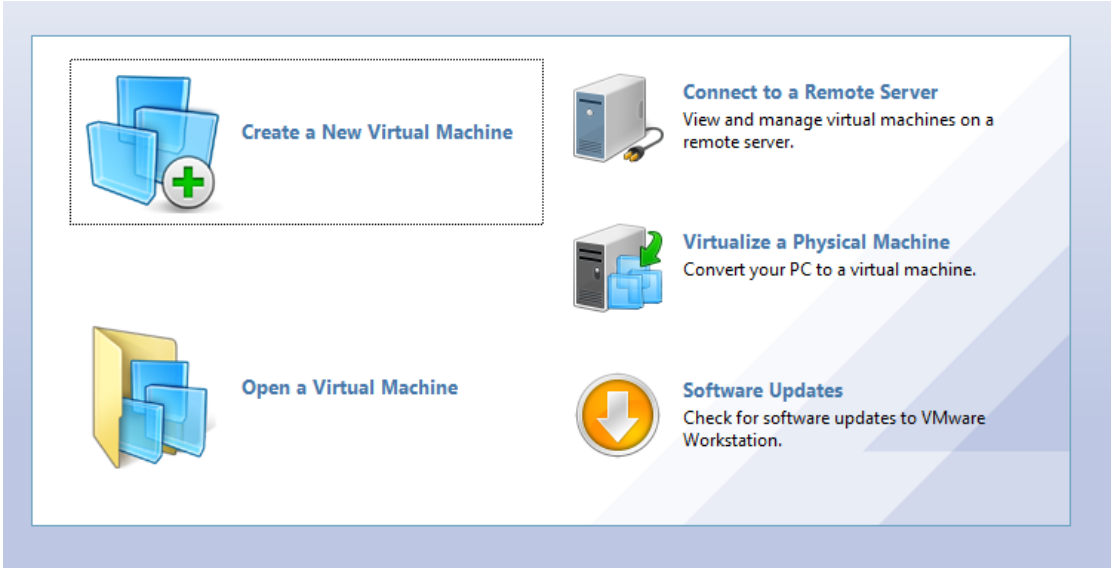


Figure 11 : l'interface prancipale

2. Cliquez sur create a new virtual machine.

3. Une fenêtre apparait, **choisissez Custom**.

4. Faites **Next**

5. Arrivé à notre troisième fenêtre, **choisissez Installer disc image file (iso)** puis faites Browse. Vous devez aller **rechercher l'iso** que vous avez stocker sur votre ordinateur et ensuite faire **Next.**

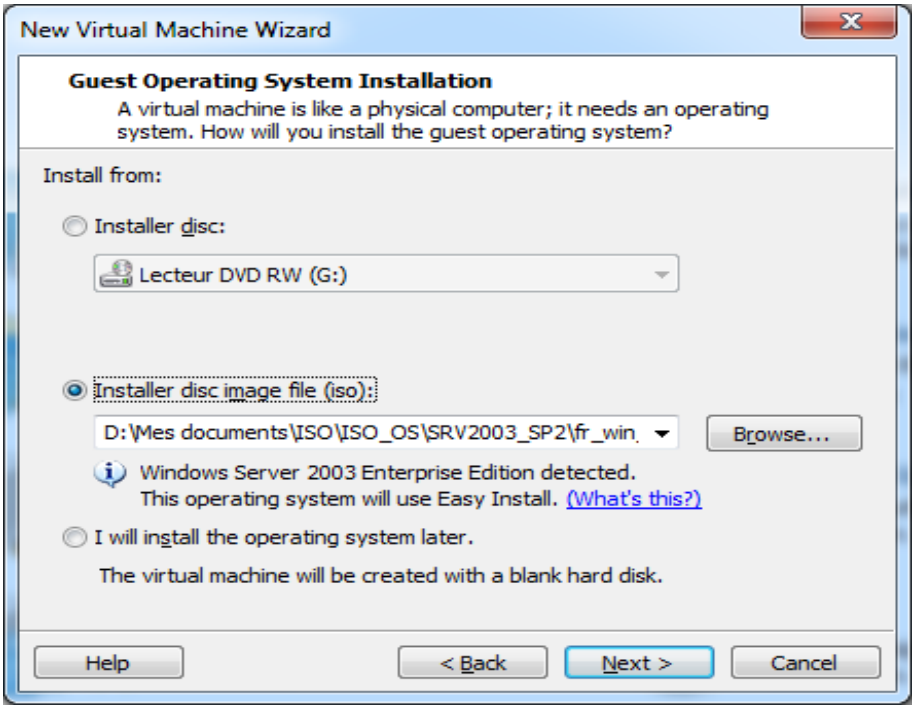


Figure 12: Ajouter iso

6. Etant donné que Windows serveur 2003 n'est pas gratuit d'utilisation, VMware vous demandera une clef de produit. Si vous possedez une clef, vous pouvez soit l'entrer immédiatement, soit attendre la procédure d'installation classique. A noté que ce n'est pas bloquant si vous n'en avez pas. Vous aurez simplement une durée d'évaluation respectable pour l'utilisation de votre serveur.

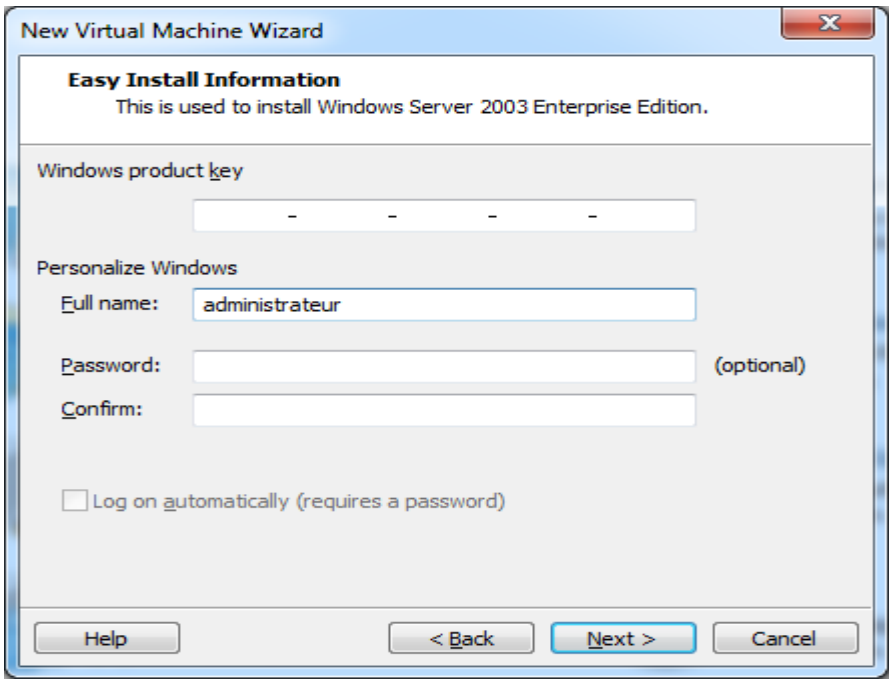


Figure 13 : insereé l'information de system

7.Nous arrivons à la feneter (Name the virtual machin).Cette étape est improtante.Le premier champs vous propose de donner un nome à votre machine (et par extension le nom du dossier propre à votre vm) et le deuxième de donner l'endroit où seront stockéés les données de votre machine. A savoir que le disque dur virtualisé de votre VM est matréialisé par un dossier consacré sur votre PC.

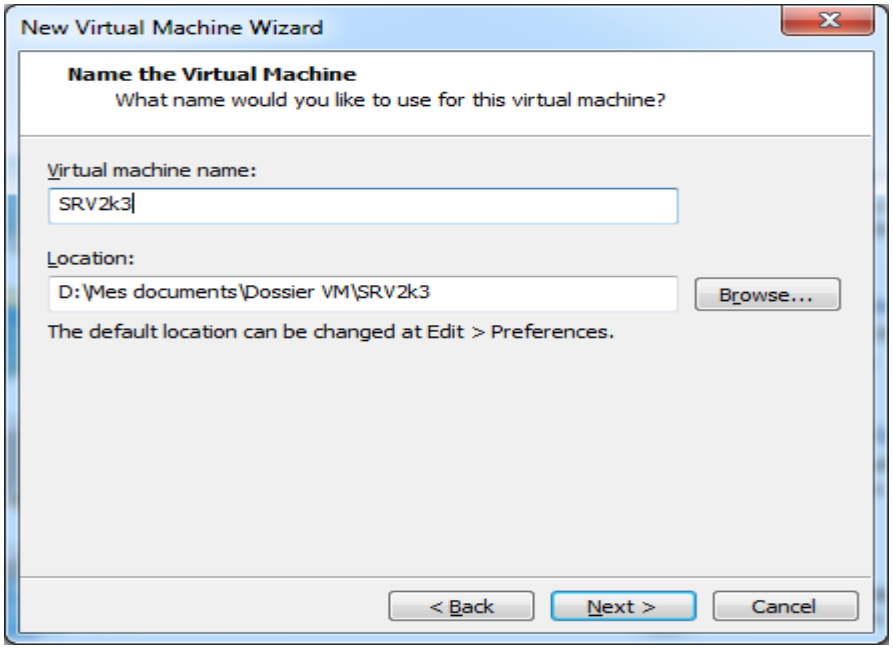


Figure 14 : Creér dossier system

8. Nous tombons sur le choix du nombre de processeur, laissez cela par défaut.

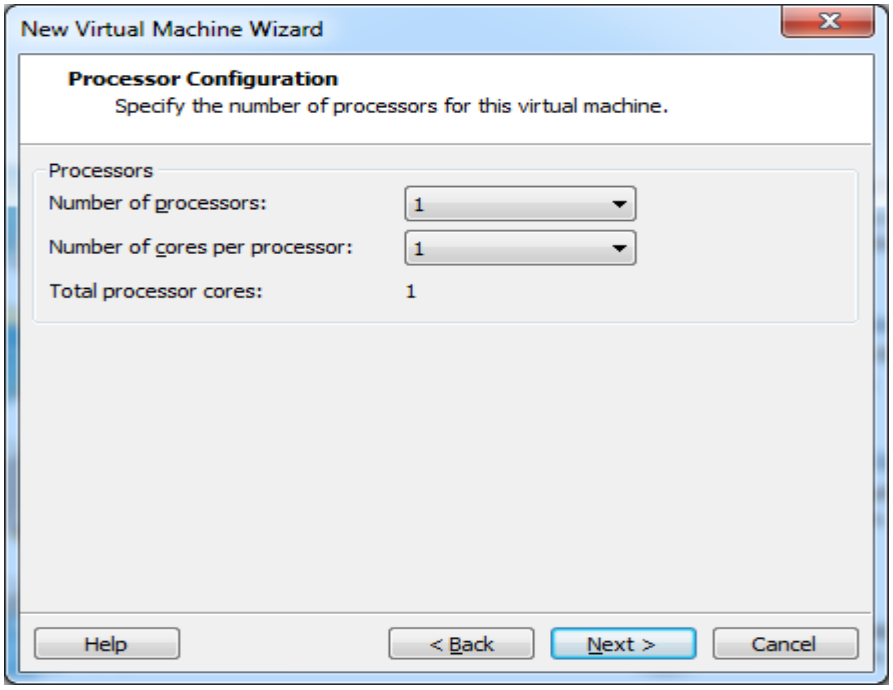


Figure 15 : configuration processor

9. Choisir nombre de ram consacrées à notre machine virtuelle.Comme je le disais dans les prérequis, il faut savoir que vous devez garder un minimum pour votre OS habituel et un minimum pour le fonctionnement de votre machine virtuelle. Dans notre exemple, j'utilise un windiws 7 64 bits. Je concidère qu'il faut un peu moins de

2go de ram pour son fonctionnement. Pour le serveur 2003 de notre TP, il faut au minimum 256 mais de préférence 512. Il faudra aussi prendre en compte qu'il y aura un serveur debian qui viendra s'ajouter à notre tp en plus d'un XP comme client.

Je dispose, sur mon seven, de 8go de ram. J'ai donc choisi:

- 1024 ram pour le serveur 2003

- 256 ram pour le debian 6

- 512 ram pour l'xp

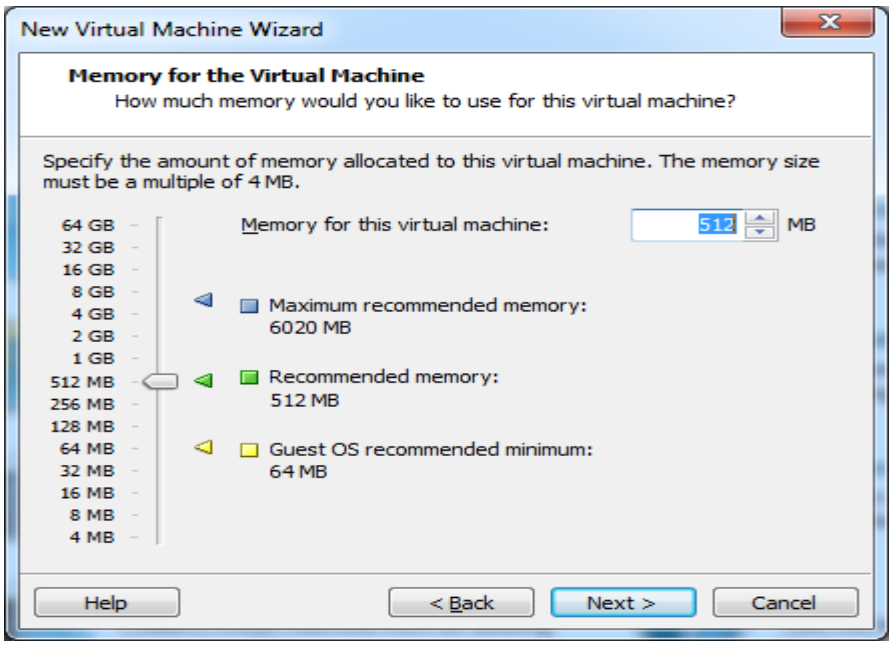


Figure 16 : Donner une valeur pour la mémoire

10. Nous tombons sur le type de réseau qui fonctionnera avec notre machine virtuelle. Je ne m'étendrai pas sur le sujet qui n'est pas celui abordé aujourd'hui, choisissez donc simplement NAT. Pour les plus curieux, je vous invite à consulter cette page qui schématise les différences entre les types de réseaux proposés.

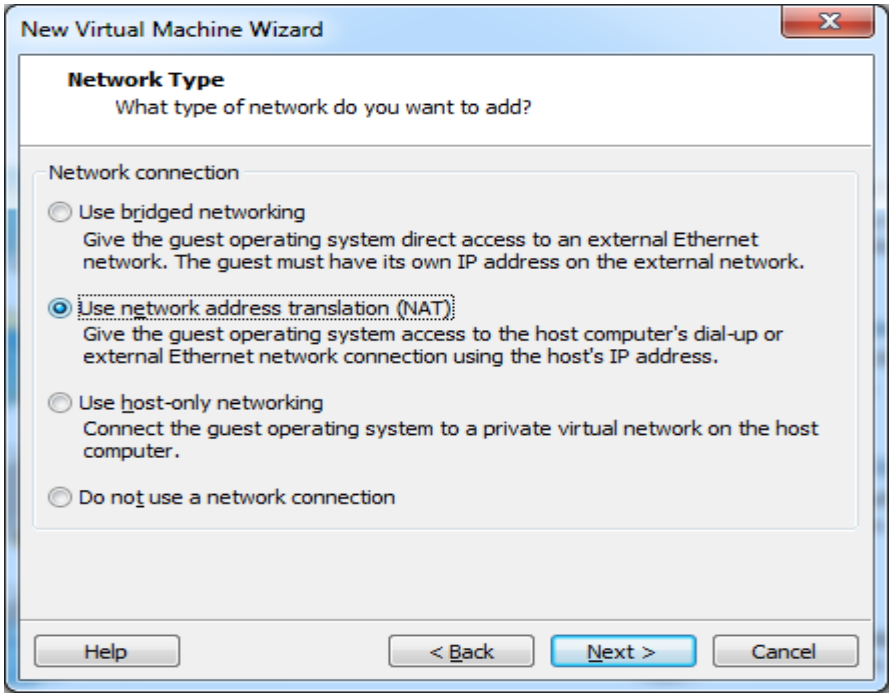


Figure 17: type network

11. La fenêtre suivante vous propose de créer un disque virtuel pour votre VM. Choisissez create a new virtual disk et faites next

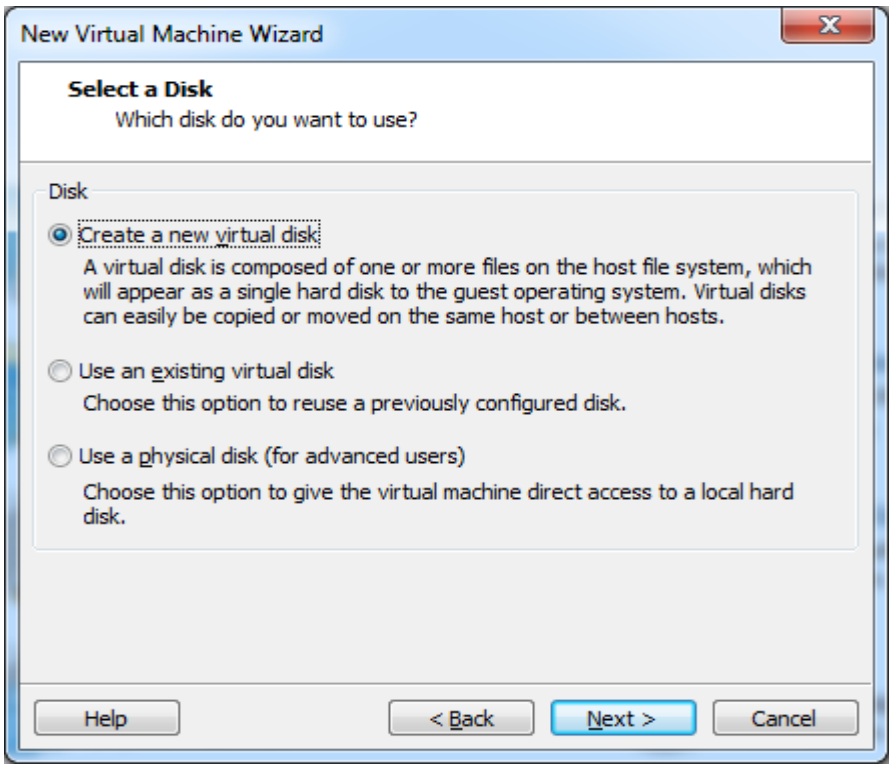


Figure 18: sélectionner disk

12. Ici, vous devez choisir l'espace disque de votre machine virtuelle. Si vous choisissez 20gb par exemple, cela n'amputera pas directement sur votre disque dur "réel", mais considérez que c'est la taille maximal du dossier de votre machine virtuelle ! Vous pouvez donc y aller sans trop d'hésitation. Vous utiliserez l'espace que vous consommez effectivement avec votre machine virtuelle. Laissez le choix par defaut "Split virtual disk into multiple files".

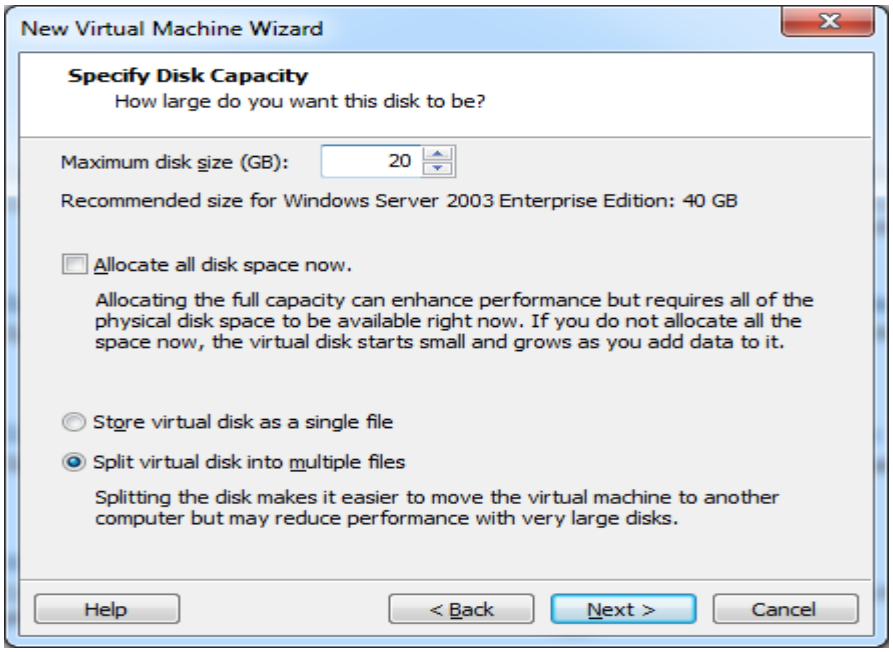


Figure 19 : spécifier capaciter disk

13. Faites Next à la fenêtre Specify disk file

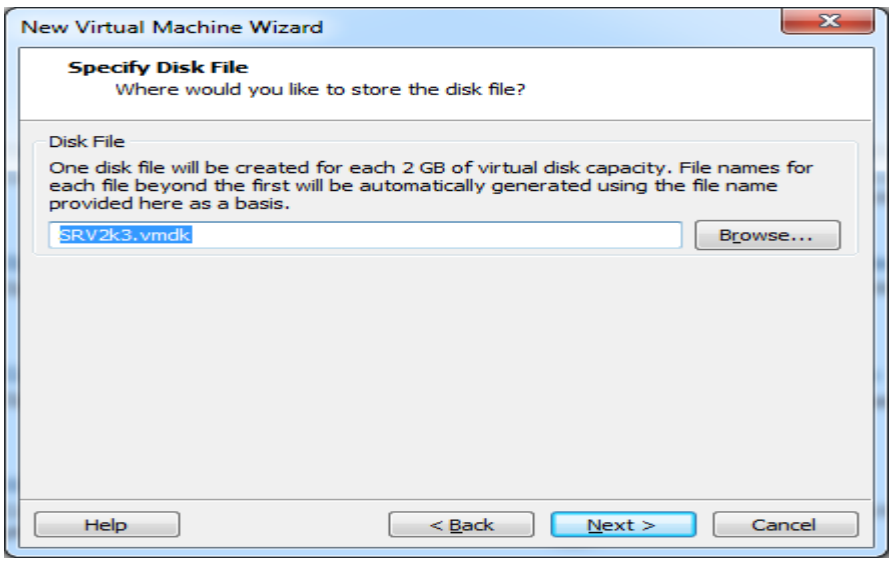


Figure 20 :spécifier dossier disk

16. Enfin, vous tombez sur le récapitulatif de notre travail. Faites finish

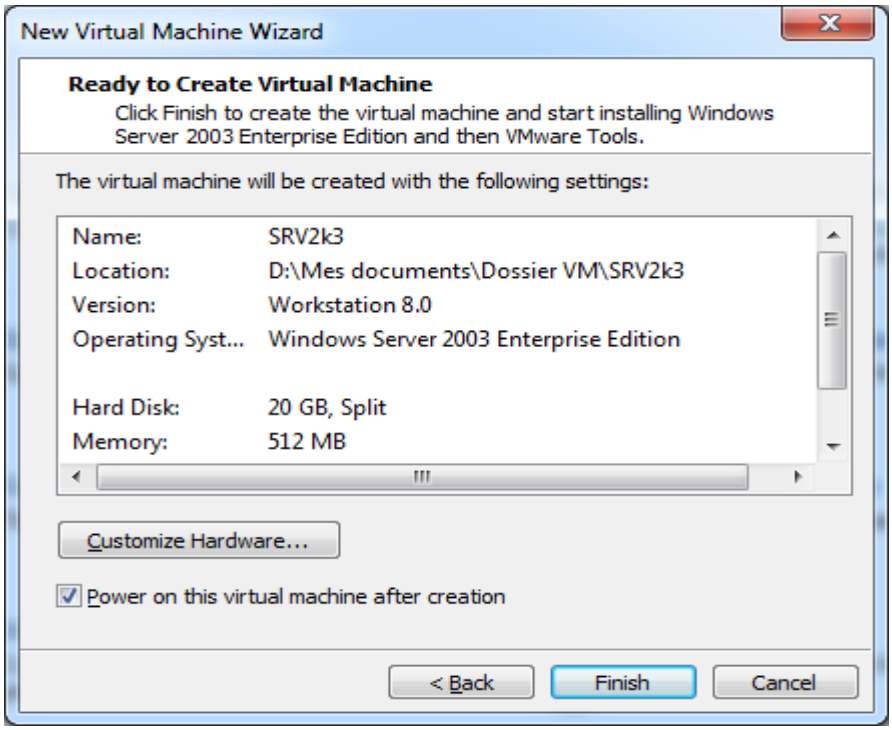


Figure 21 : fin de l'installation

5- etude de cas :

4-1 tobologie d'ips

Vue d'ensemble sur la topologie :

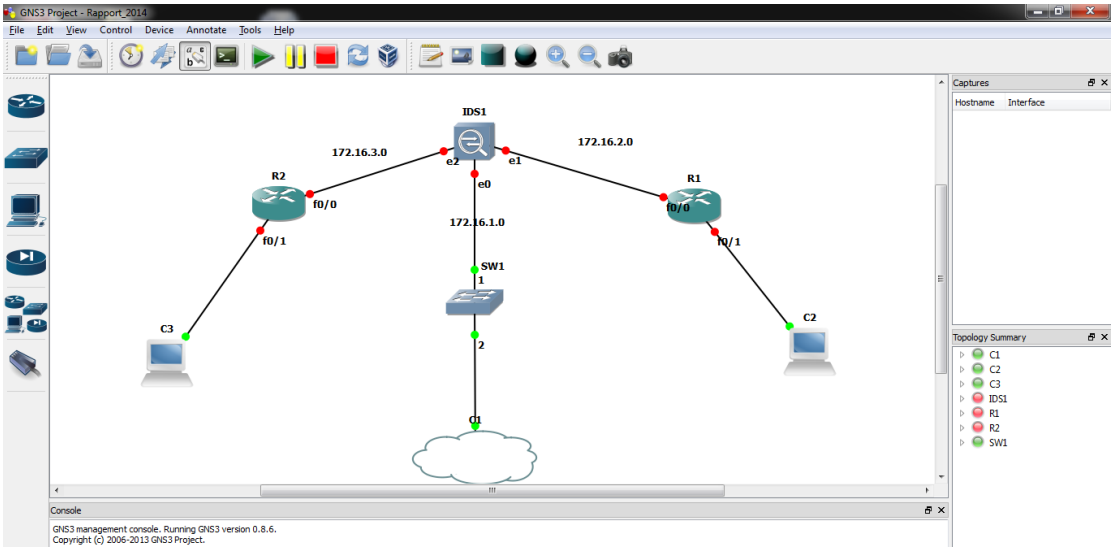


Figure 22: Topologie

- ✓ Créez deux VMS différentes en utilisant VMware
- ✓ Connecter La machine virtuelle VMware à un équipement sur GNS3

- ✓ Simuler 2 routeurs Cisco virtuels à l'aide GNS3
- ✓ Configurer les routeurs Cisco avec le routage RIP
- ✓ Configuration d'un switch Ethernet pour connecter avec le Cloud
- ✓ IPS cisco

4.2-Connecter La machine virtuelle VMware à un équipement sur GNS3:

❖ Manipulation VMware Workstation **:**

Tout d'abord, nous allons créer un nouveau VMnet sur lequel se trouvera notre machine virtuelle et notre équipement. Lancez VMware Workstation et cliquez sur Edit – Virtual Network Editor.

Cliquez sur Add Network… et ajoutez un nouveau VMnet (j'ai personnellement choisit VMnet2). Une fois le VMnet ajouté j'ai décoché la case Use local DHCP service to distributeur IP address to VMs. Notez l'adresse IP du réseau affiché dans Subnet IP (172.16.3.2)

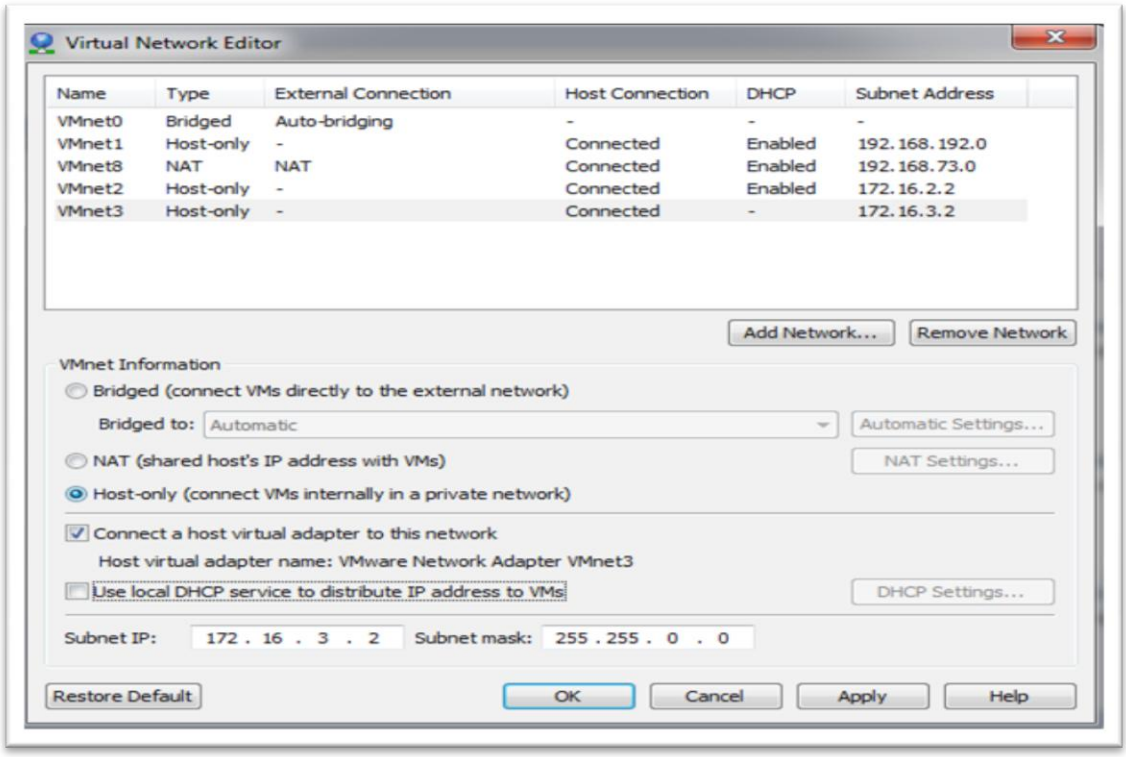


Figure 23 : Inscrivez éditeur Virtual Network

- Host-only (connect VMs internally in a private network) : limite le trafic uniquement à l'ordinateur sur lequel VMware et GNS3 installés

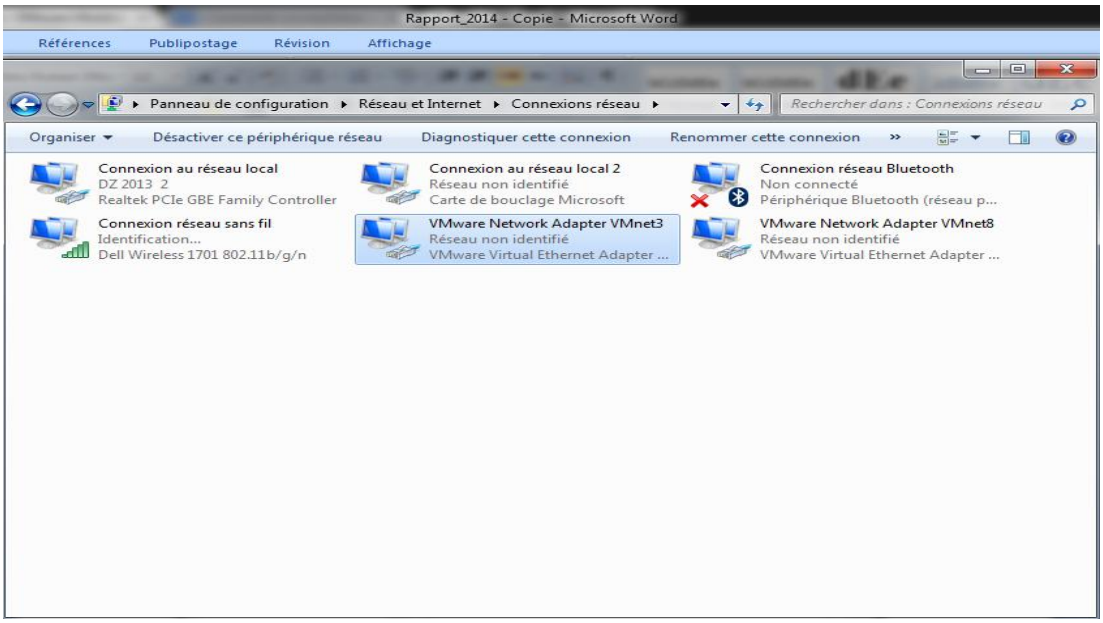


Figure 24: Center réseau

Ensuite, sur la liste des composants souligner l'adaptateur réseau et à la section de connexion réseau et cliquez sur Personnalisé de liste déroulante ramassage VMnet1 (Host-only)

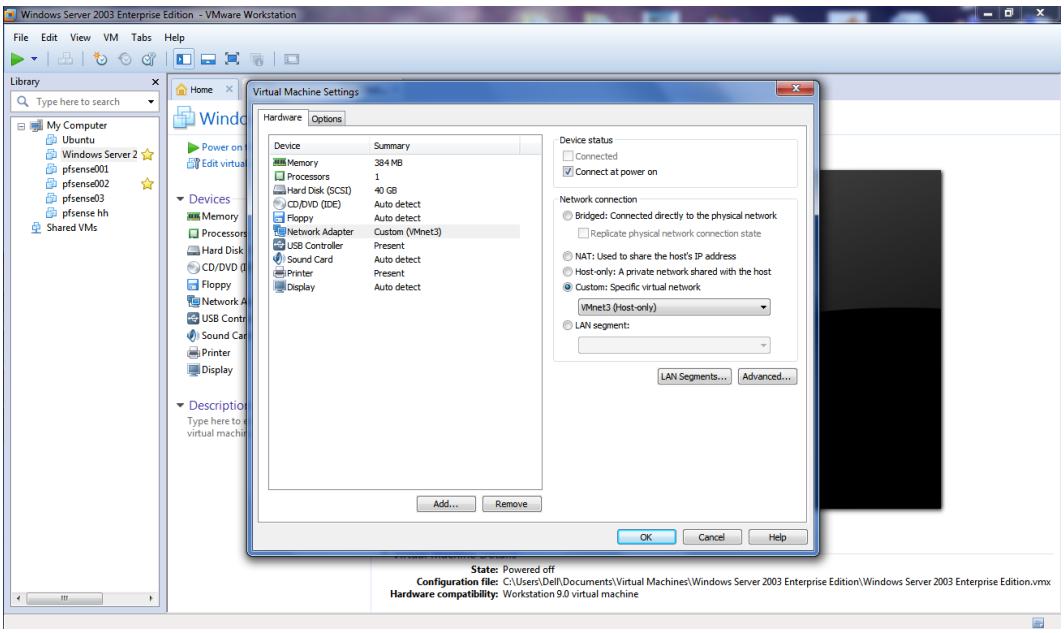


Figure 25 : connecte sous Virtual adaptateur

❖ Manipulation GNS3 :

Ouvrez GNS3, lancez votre équipement et configurez une adresse IP sur une de ses interfaces, dans l'exemple mon équipement a pour adresse IP : 172.16.3.2

Ajouter un nuage à votre topologie, en choisissant Cloud dans la liste déroulante à gauche et en plaçant le nuage dans la topologie. Faites un clic-droit sur votre nuage et cliquez sur Configure. Choisissez C1 (C1 étant le nom de notre nuage) et dans le cadre Generic Ethernet NIO (Administrator or root access required), sélectionnez l'adaptateur VMnet2 comme montré ci-dessous :

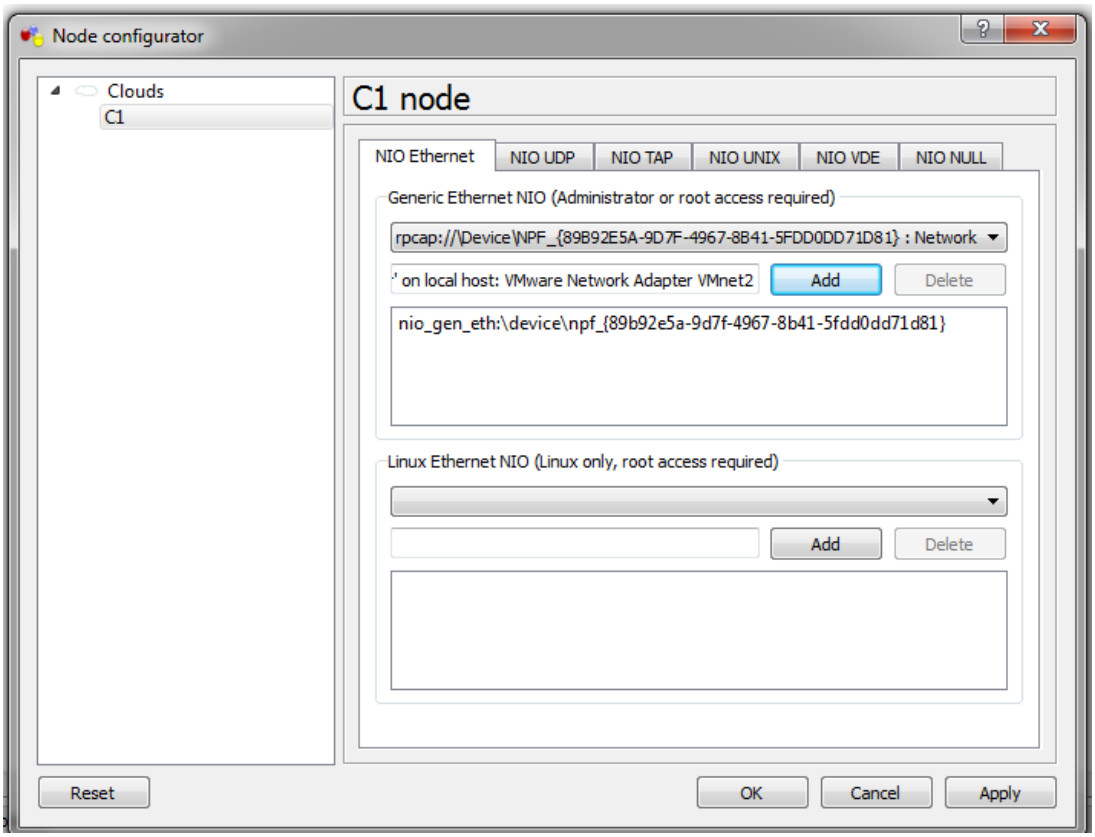


Figure 26: connecter Vmware et GNS3

Cliquez sur le bouton ajouter et click on OK en Bas. de dans la barre de boutons, Cliquez sur Choose FastEthernet et Faites la liaison Entre Votre équipement et le nuage. SAUF reglages Particulier partie de Votre (ACL, pare-feu, etc ...) la machine Windows 7 devrait Être capable de Communiquer avec l'équipement eMule

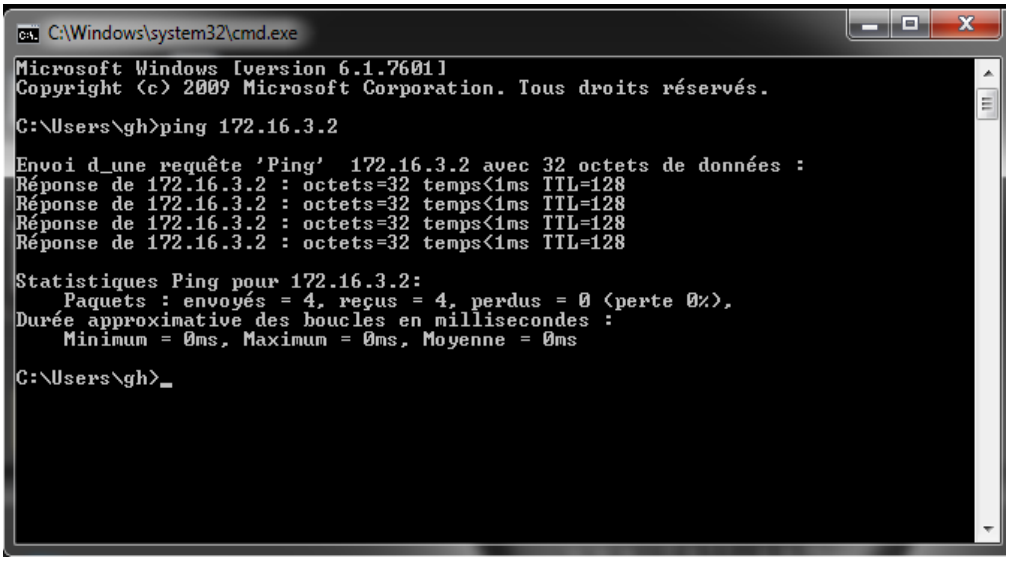


Figure27: ping loopback

4-3-Instalation et configuration de ips cisco : [4]

Télécharge IPS-K9-cd-1.1-a-6.0-6-E3.iso de puis le site web cisco

créer deux disques à utiliser pour l'opération IPS:

qemu-img.exe create ipsdisk1.img 512M

```
C:\Program Files\GNS3>qemu-img.exe create ipsdisk1.img 512M
Formatting 'ipsdisk1.img', fmt=raw size=536870912
```

qemu-img.exe create ipsdisk2.img 4000M

```
C:\Program Files\GNS3>qemu-img.exe create ipsdisk2.img 4000M
Formatting 'ipsdisk2.img', fmt=raw size=4194304000
```

qemu.exe -hda ipsdisk1.img -hdb ipsdisk2.img -m 1024 –cdrom IPS-K9-cd-1.1-a-6.0-6-E3.iso -boot d

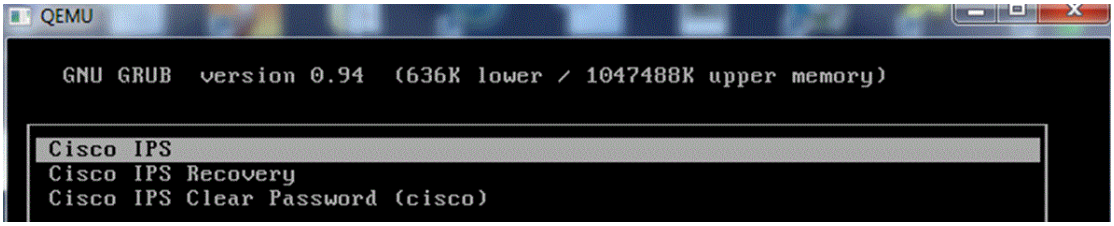
Type → k

```
Updating idsRoot/shared

Updating data device

Making filesystems on /dev/hdb2
Updating grub
Installing IPS components
```

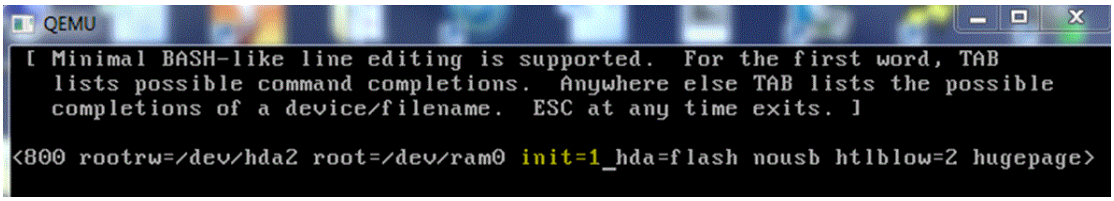
qemu.exe -hda ipsdisk1.img -hdb ipsdisk2.img -m 1024

```
C:\Program Files\GNS3>qemu.exe -hda ipsdisk1.img -hdb ipsdisk2.img -m 1024
```

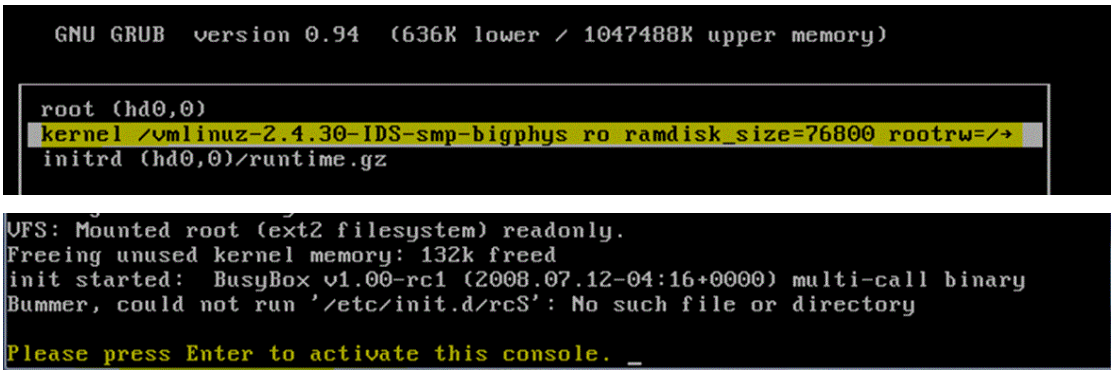
Press → e



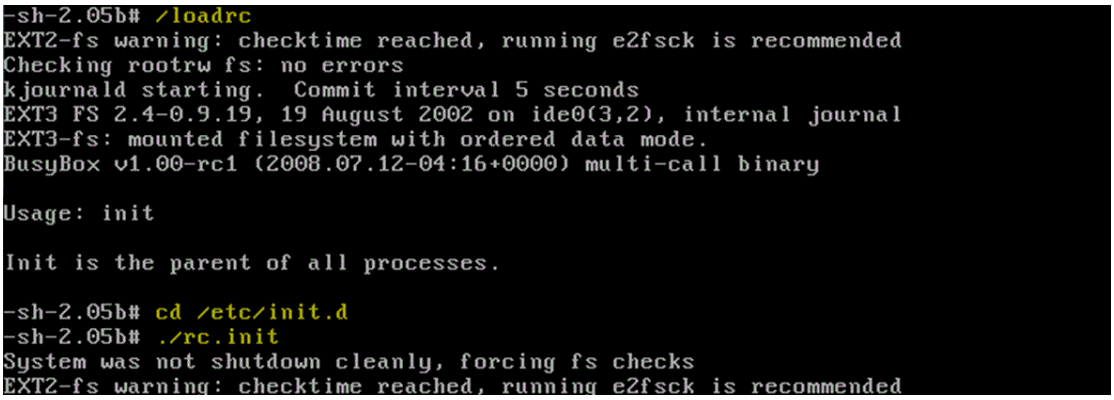
- Again Press → e
- Change à init=/loadrc to init=1
- Press → esc



Press → b



- /loadrc
- cd /etc/init.d
- ./rc.init



Ls –l

```
EXT3-fs: mounted filesystem with ordered data mode.
kjournald starting.  Commit interval 5 seconds
EXT3 FS 2.4-0.9.19, 19 August 2002 on ide0(3,66), internal journal
EXT3-fs: mounted filesystem with ordered data mode.
-sh-2.05b# ls -l
-rwxrwxr-x    1 root     root         1108 Jul 12  2008 S20urandom
lrwxrwxrwx    1 root     root            7 Feb 11 11:45 S40network -> network
-rwxrwxr-x    1 root     root         2475 Jul 12  2008 S60ssh
lrwxrwxrwx    1 906417   25             12 Feb 11 11:46 S65transfer_cfg -> trans
fer_cfg
lrwxrwxrwx    1 root     root            4 Feb 11 11:46 S80cids -> cids
-rwxr-xr-x    1 cids     cids        16263 Jul 15  2009 cids
-rwxr-xr-x    1 root     root        15692 Jul 15  2009 cntr_plane_functions
-rwxrwxr-x    1 root     root         8648 Jul 12  2008 functions
-rwxr-xr-x    1 root     root        38623 Jul 15  2009 ids_functions
```

Cp ids_functions ids_functions.orig

Vi ids_functions

```
-sh-2.05b# cp ids_functions ids_functions.orig
-sh-2.05b# vi ids_functions_
```

/845 (to find string)

Change elif ; DEFAULT_MGT_OS ; DEFAULT_MGT_CIDS ; HTLBLOW
:wq!

```
        DEFAULT_MGT_CIDS="FastEthernet0/1"
    elif [[ 1 -eq 1 ]]; then
        MODEL=$IDS4215
        HTLBLOW=32_
        MEM_PAGES=${HTLBLOW}
        DEFAULT_MGT_OS="ma0_0"
        DEFAULT_MGT_CIDS="Management0/0"
    elif [[ `isCPU 498` -eq $TRUE && $NUM_OF_PROCS -eq 1 ]]; then
        MODEL=$MOHAWK
        HTLBLOW=8
        MEM_PAGES=${HTLBLOW}
        DEFAULT_MGT_OS="fe0_0"
        DEFAULT_MGT_CIDS="FastEthernet0/0"
-- Replace --
```

cd /usr/cids/idsRoot/etc

cp interface.conf interface.conf.orig

vi interface.conf
:wq!

```
port-number=0
pci-path=
:wq!_
```

Reboot

```
port-number=0
pci-path=
-sh-2.05b# reboot_
```

Il va redémarrer plusieurs fois un login et un changement passe (cisco-cisco)

```
***LICENSE NOTICE***
There is no license key installed on the IDS-4215.
The system will continue to operate with the currently installed
signature set.  A valid license must be obtained in order to apply
signature updates.  Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
sensor# _
```

Modifier GNS3 qemu configuration:

Puis aller vers le menu edit → preferences → qemu et mettre en place la configuretion suivante

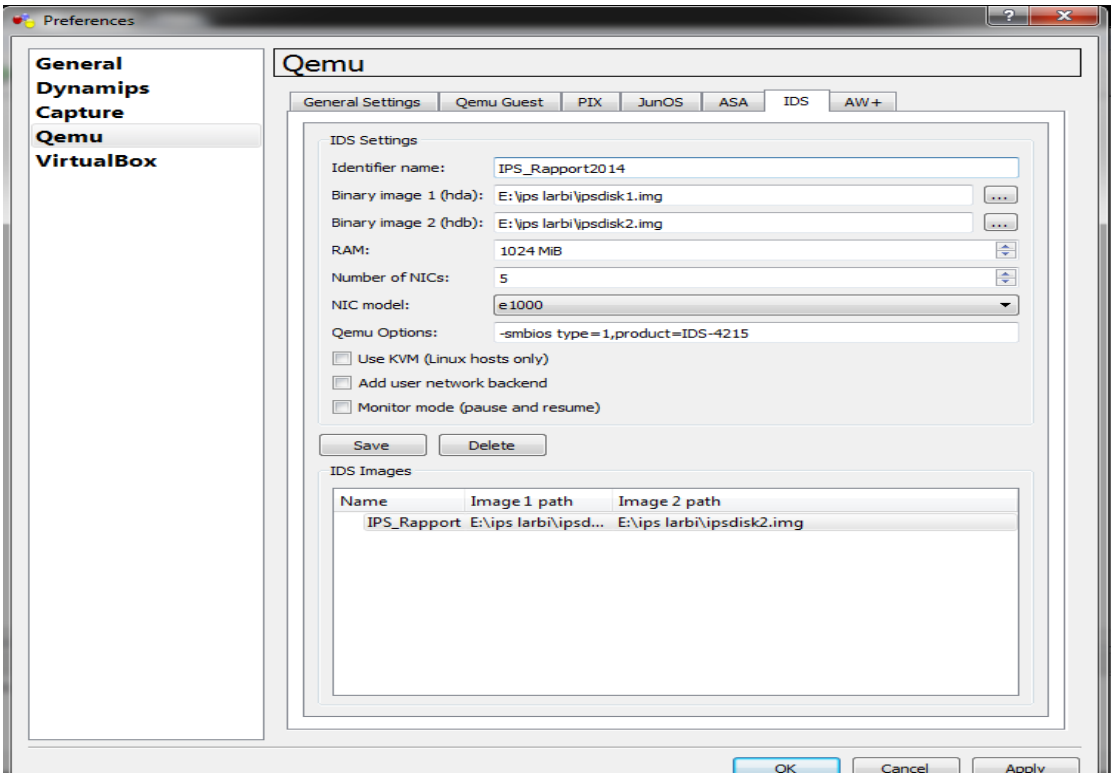


Figure28 :configuration qemu

Configure →Cloud to local loopback

IPS → console →insérer address ip

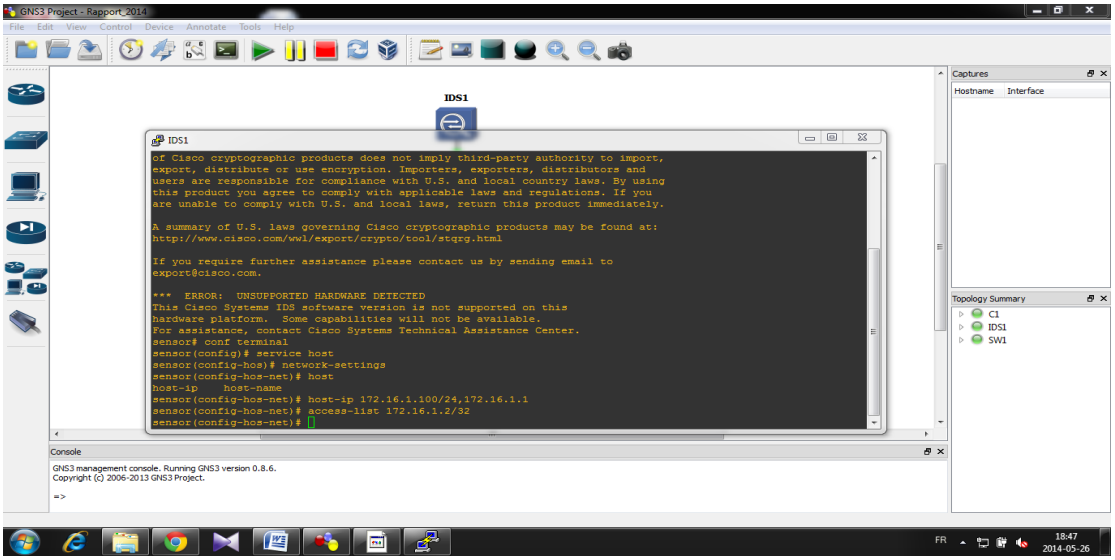


Figure 29: créer (address IP)

Pour vérifier la connectivite enter l'ips et loopack adaptateur de l'hot on à esseger de faire un ping

Cmd → ping 172.26.1.100

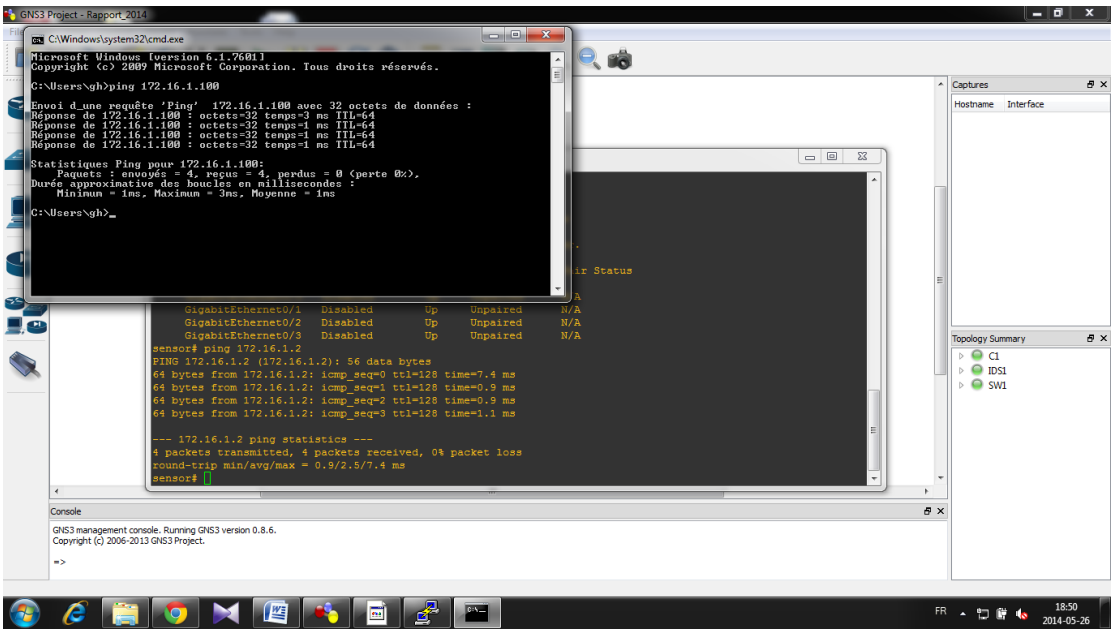


Figure 30: ping loopback et ips

Google Chrome → https:172.16.1.100

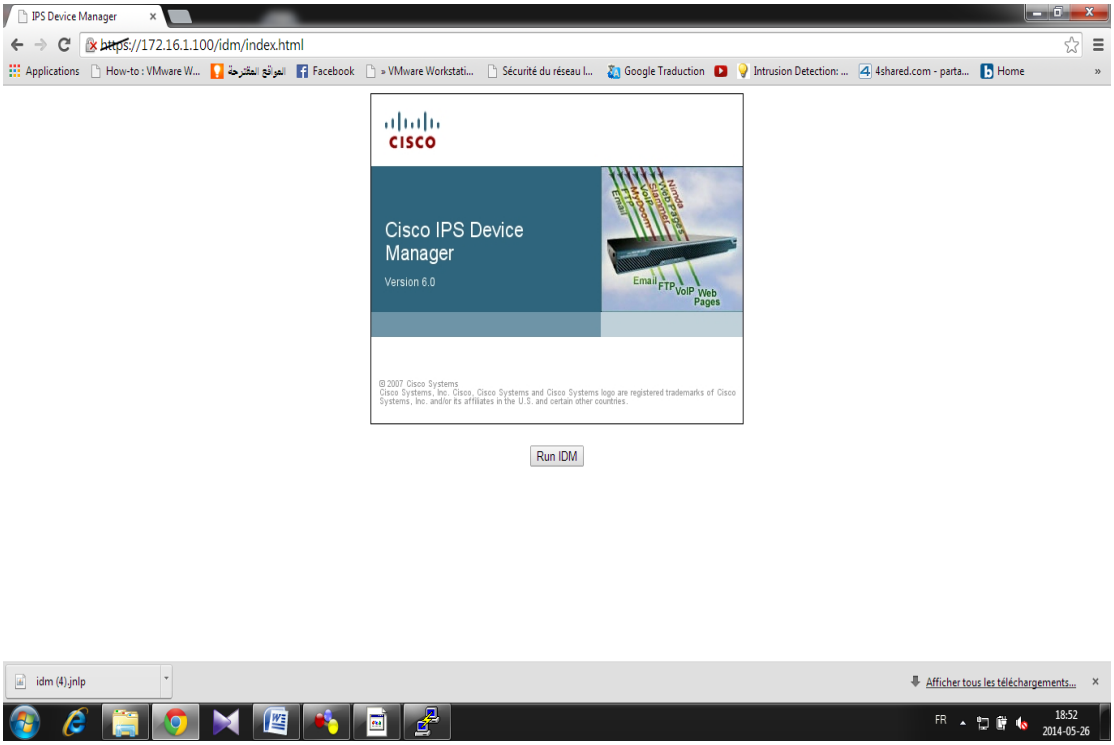


Figure 31: connecter à ips aparté de Google chrome

IDM →insérer (username and password) dans IDM

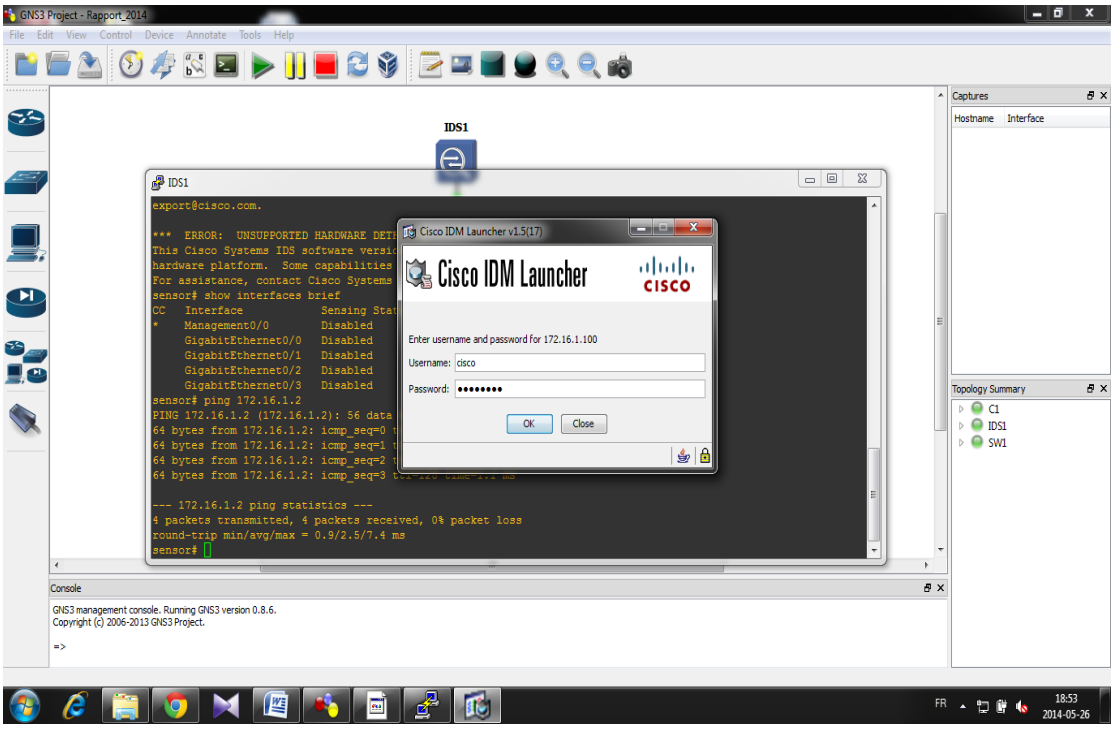


Figure 32: insurer (username and password on IDM)

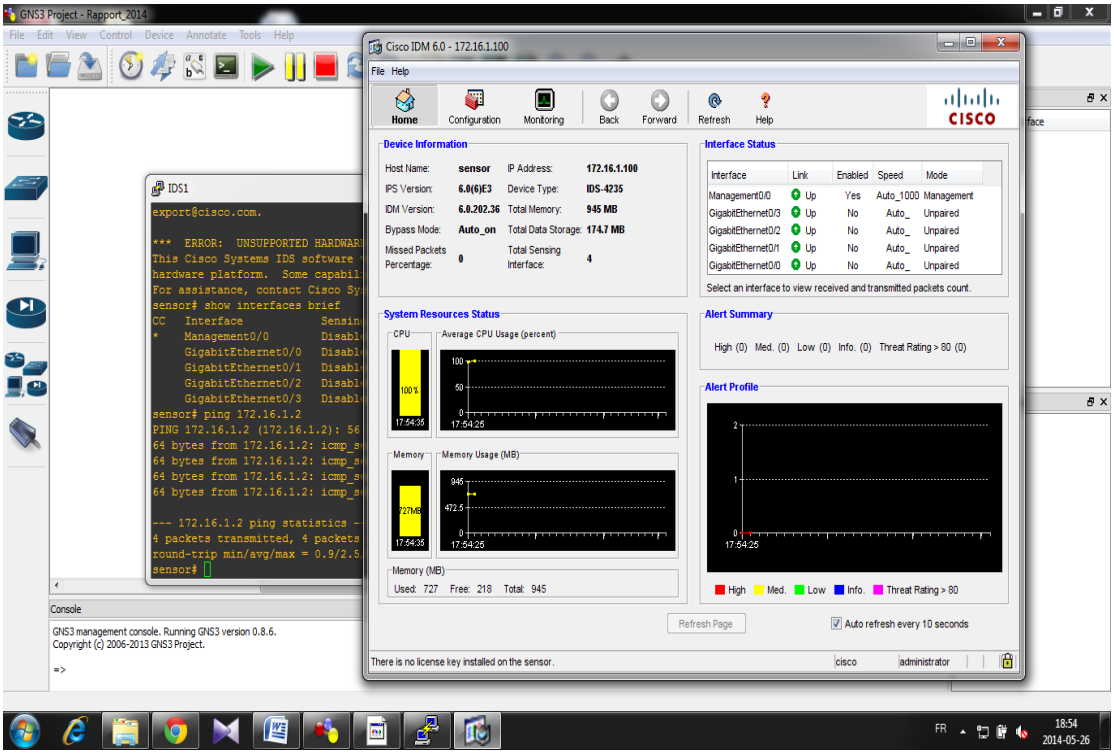


Figure 33: interface IDM

Pour configuration l'interface paries nous allons vers

IDM → configuration → interface Pairs

IDM → configuration → interface Pairs

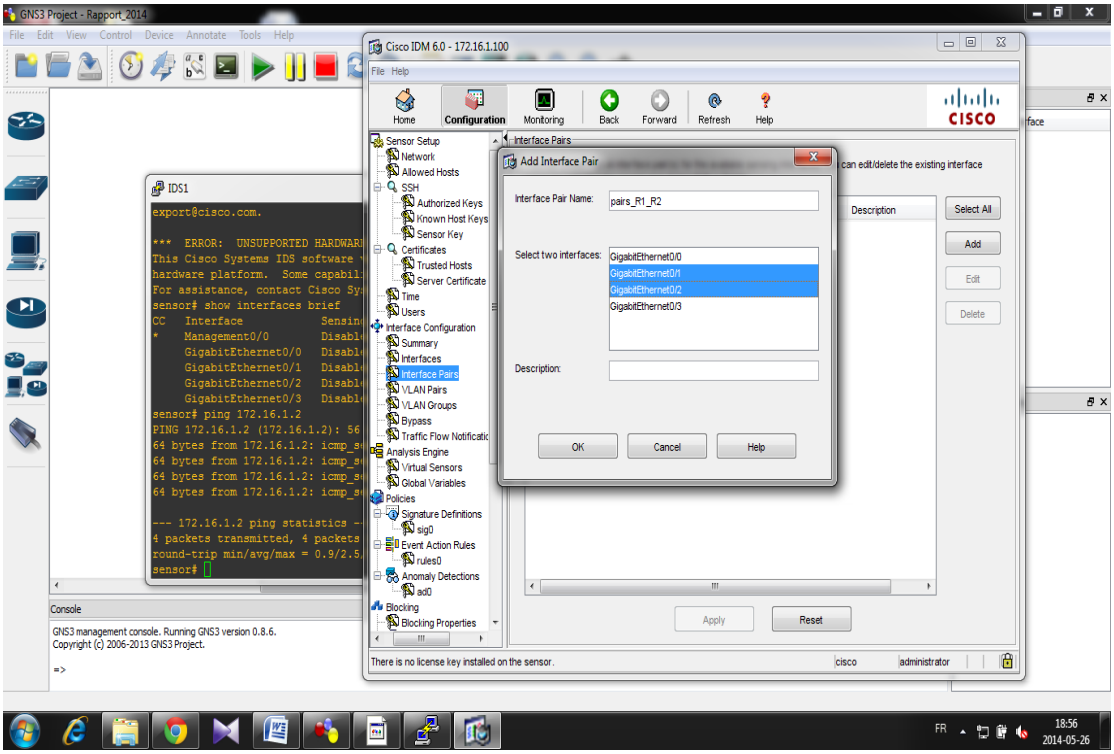


Figure 34: la configuration d'interfaces paires

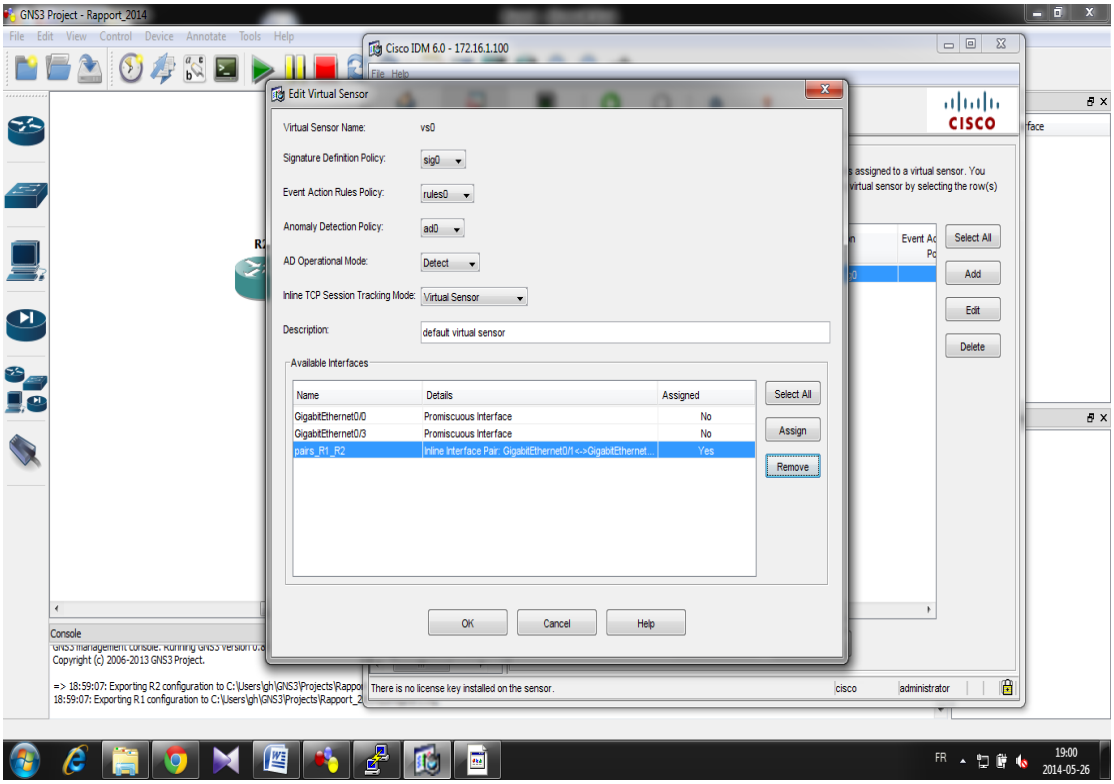


Figure 35: (Assing pairs)

Pour afficher les signatures d'attaque sous ips nous allons vers

IDM → configuration → Sg0

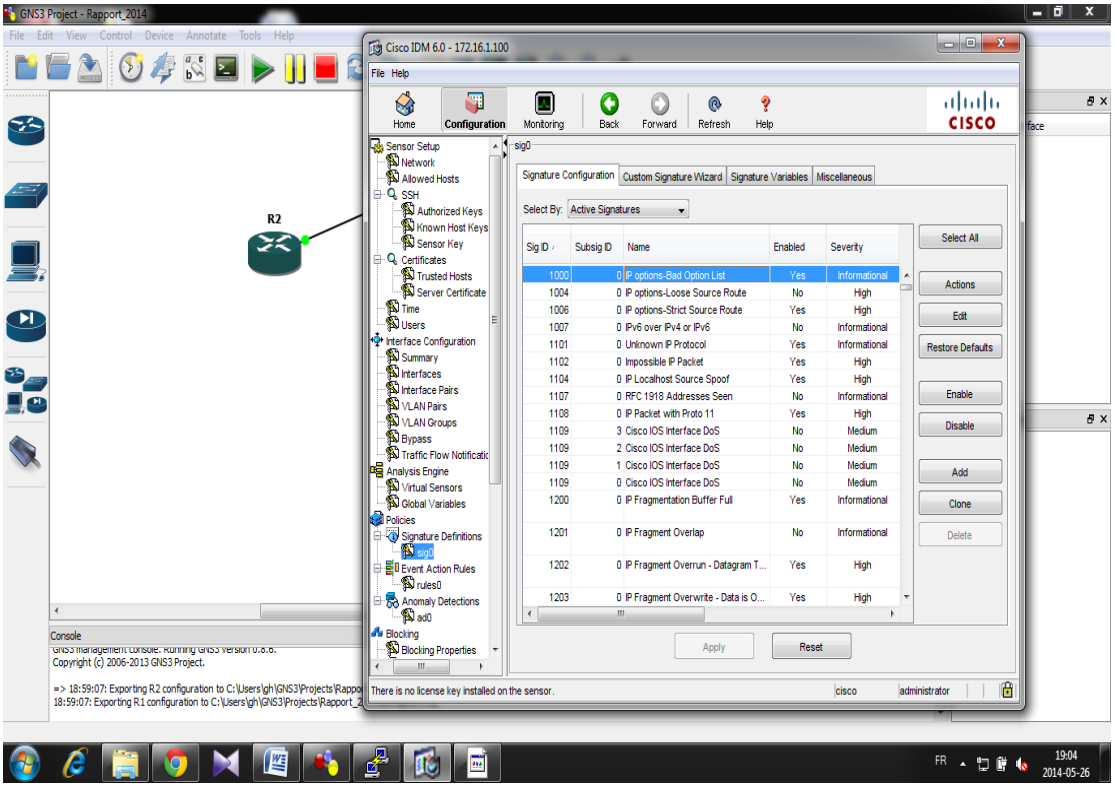
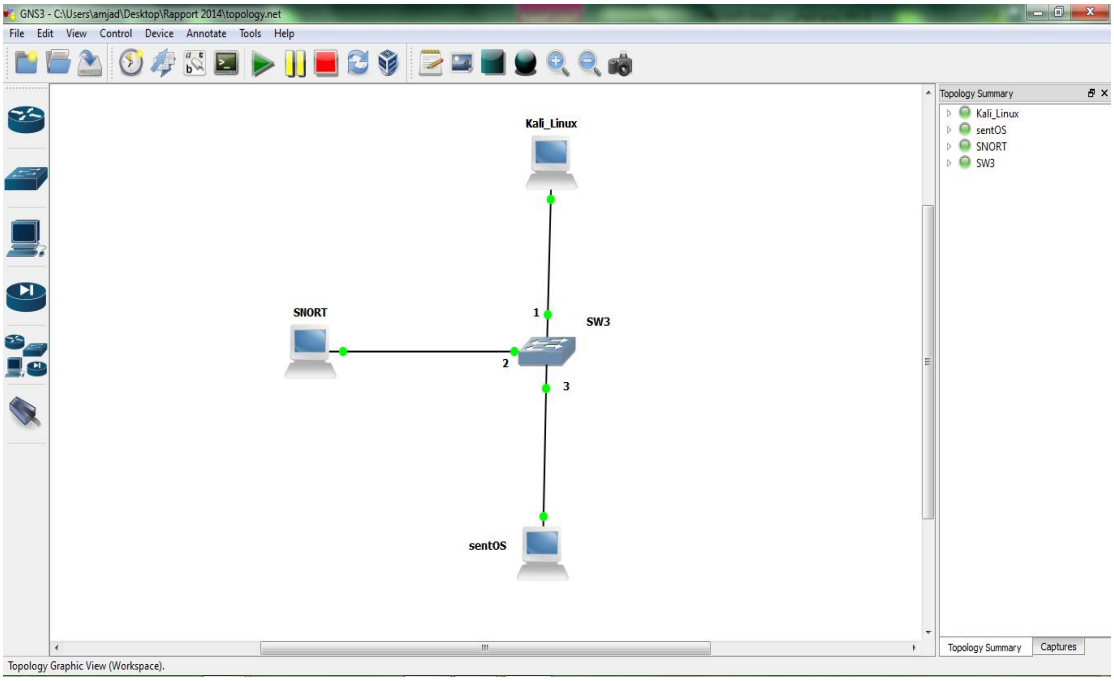


Figure 36: les signatures d'ips

4-2-Topologie de snort :



Figoure 37: interface tobology

1-outile

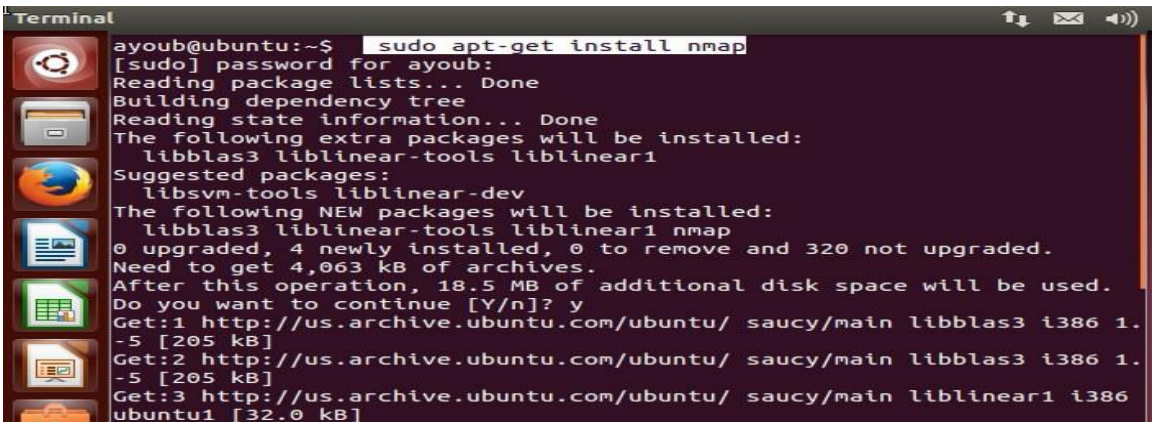
✓ Créez trois boîtes différentes en utilisant VMware

1) kali linux
2) ubuntu
3) centOS

2 -Installation de snort sous ubuntu :

- Installation des fonctionnalités nécessaires :

- sudo apt-get install nmap



- sudo apt-get install nbtscan
- sudo apt-get install apache2
- sudo apt-get install php5
- sudo apt-get install php5-mysql
- sudo apt-get install php5-gd
- sudo apt-get install libpcap0.8-dev
- sudo apt-get install libpcre3-dev
- sudo apt-get install g++
- sudo apt-get install bison
- sudo apt-get install flex
- sudo apt-get install libpcap-ruby
- sudo apt-get install mysql-server
- sudo apt-get install libmysqlclient16-dev

1. Composants pour Snort NIDS :

1) JpGraph

- sudo wget http://hem.bredband.net/jpgraph/jpgraph-1.27.1.tar.gz

2) Data acquisition API

Indispensable pour les versions de Snort après la 2.9.0. Ce composant permet d'acquérir des paquets sur le réseau.Télécharger

daq-0.6.2.tar.gz http://www.snort.org/downloads/1339

- sudo tar zxvf daq-0.6.2.tar.gz cd daq-0.6.2 sudo ./configure sudo make sudo make install

3) Libnet

Libnet, est une bibliothèque opensource. Elle permet de fabriquer et d'injecter facilement des paquets sur un réseau. Télécharger

libnet-1.12 http://libnet.google.com/files/libnet-1.12.tgz

- sudo tar zxvf libnet-1.12 cd libnet-1.12/ sudo make sudo make install sudo ln –s /usr/local/lib/libnet.1.0.1 /usr/lib/ libnet.1 14

2. Installation de Snort NIDS :

Télécharger la dernière version stable, sur http://www.snort.org/snort-downloads (j'utilise la version 2.9.2).

Une fois le fichier téléchargé, ouvrir un terminal et exécuter les commandes suivantes:

- sudo tar zxvf snort-2.9.2.tar.gz
- cd snort-2.9.2
- sudo ./configure --prefix=/usr/local/snort --enable-sourcefire
- sudo make
- sudo make install
- sudo mkdir /var/log/snort
- sudo mkdir /var/snort
- sudo groupadd snort
- sudo useradd -g snort snort
- sudo chown snort:snort /var/log/snort

1) Création de la base de données :

L'installation de Snort nécessite la mise en place d'un serveur Mysql afin de permettre au NIDS de stocker les alertes qu'il génère mais aussi à la console BASE ou Snort report de se connecter et récupérer ces alertes.

echo "create database snort;" | mysql -u root -p

mysql -u root -p -D snort < ./schemas/create_mysql

Transférer les droits root de la base de donné sur l'utilisateur snort :

echo "grant create, insert, select, delete, update on snort.* to snort@localhost identified by 'mon-mdp'" | mysql -u root -p

2) Snort rules :

Afin de donner à Snort une bonne acquittée dans son observation, il faut intégrer des règles de détection, et les mises à jour de ces règles. Les règles « *ruleset* » officielles sont proposées par Snort à l'adresse suivante :

http://www.snort.org/snort-rules/ Le principal inconvénient : ils sont payants. Il y a toute fois un « *ruleset* » disponible pour test lorsque l'on s'inscrit sur le site de Snort.

3) Barnyard2 :

Barnyard est une couche applicative qui exploite les événements générés par Snort. Barnyard permet de prendre en charge l'inscription des événements en base de données et libère donc des ressources à Snort qui peut davantage se concentrer sur la détection des intrusions.

Installation de la version courante:

- sudo tar zxvf barnyard2-1.9.tar.gz
- cd barnyard2-1.9
- sudo ./configure --with-mysql
- sudo make
- sudo make install
- sudo cp etc/barnyard2.conf /etc/snort
- sudo mkdir /var/log/barnyard2
- sudo chmod 666 /var/log/barnyard2
- sudo touch /var/log/snort/barnyard2.waldo
- sudo chown snort.snort /var/log/snort/barnyard2.waldo

Modifions le fichier /etc/snort/ barnyard2.conf Remplacer **:**

#config hostname: snort

#config interface: eth1

#output database: log, mysql, user=root password=azerty dbname=db host=localhost

Par :

config hostname : localhost

config interface: eth1

output database: log, mysql, user=root password=azerty dbname=snort host=localhost

Test snort:

- Démarrer la VM kali linux sous VMware
- Ouvrir le terminal
- Créer le commende " nmap –V –A 192.168.10.2/31 "

pour Nmap c'est outil que scane un hote et detecte les ports ouvrerts

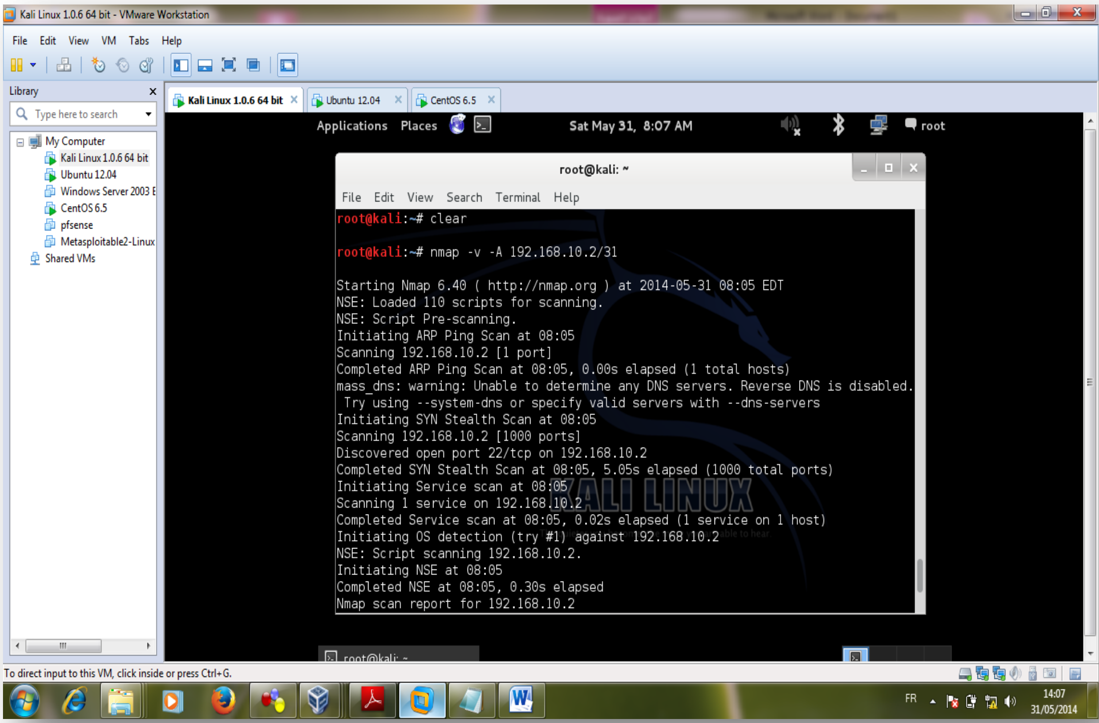


Figure 38: code les 'attaques

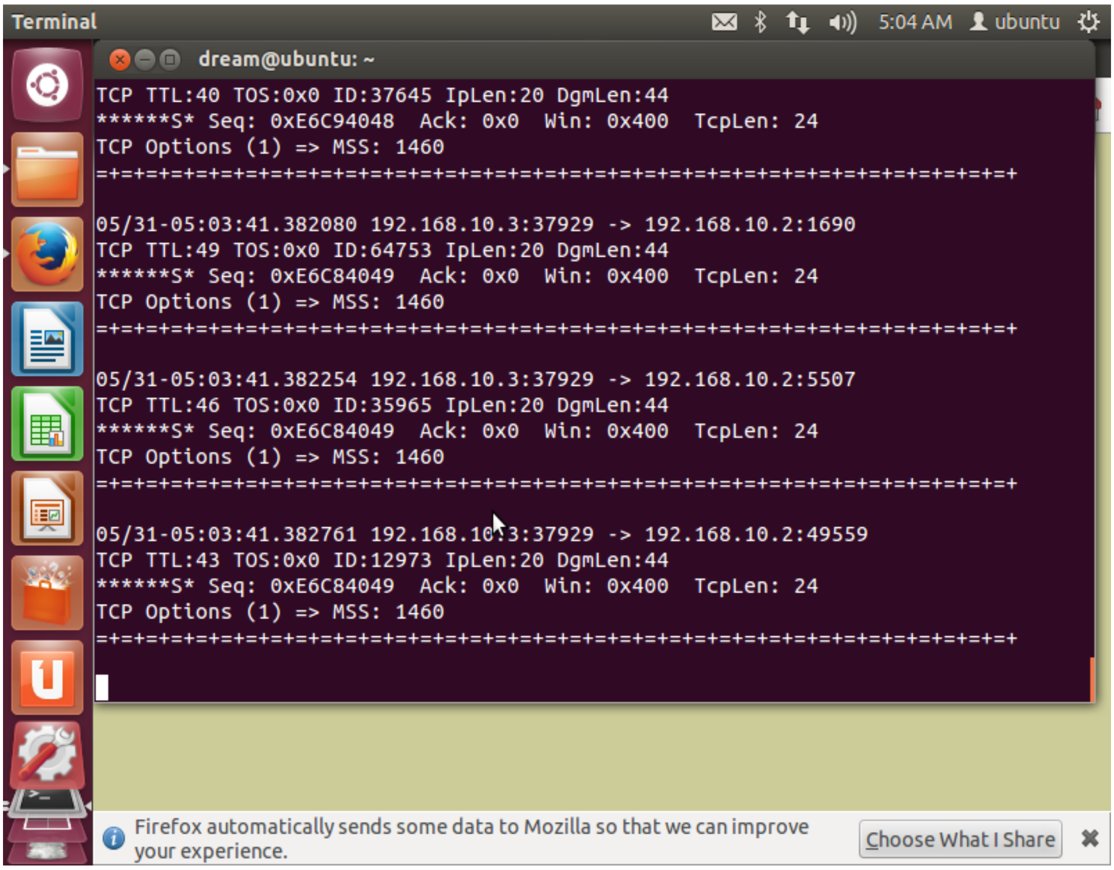


Figure 39: la détection d'intrusion

Conclusion:

Ces études nous ont permis d'avoir une idée claire des applications dans le domaine de la sécurité informatique. Et améliorer notre capacité à utiliser les produits Cisco et open sourse

Cependant, nous avons rencontré de nombreux problèmes lors de l'élaboration de ce travail. Il s'agit principalement de la difficulté à installer Snort et IPS

Il convient de noter que ce projet est une excellente introduction à la vie professionnelle, car il offre un aperçu de ce qui va travailler dans une équipe de la sécurité informatique. Il a été une expérience enrichissante en termes de théorie et de pratique.

Reference:

[1] IPS (Intrusion Prevention System):

PDF: Beyond the Perimeter "Enterprise-wideIntrusion Prevention"

Copyright © 2004, Q1 Labs Inc.

Line:

http://wp.bitpipe.com/resource/org_1046366622_812/IPS_Whitepaper.pdf

[2] Snort

Definition:

http://fr.wikipedia.org/wiki/Snort

[3] l'outil GNS3

http://www.gns3.net/

[4] instalation et configuration ips:

http://www.brainbump.net/how-to-emulate-cisco-ips/