Université de Guelma
Département Informatique

Chapitre 3 : Firewalls Pfsense

Cours - Sécurité Informatique

3 année LMD Système d'Information

Par : Dr. M. A. Ferrag

Plan du cours

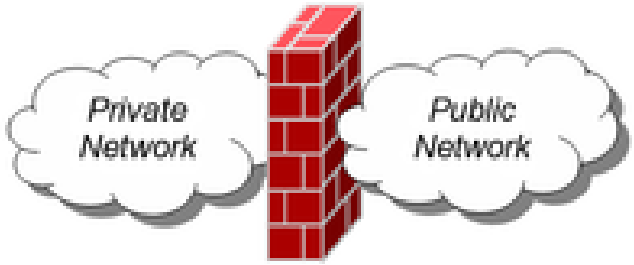
- **Firewalls**
- **Pfsense**
- **Wireshark**
- **Kali-lunix**
- **Le model réseau du TP (Exemple)**

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

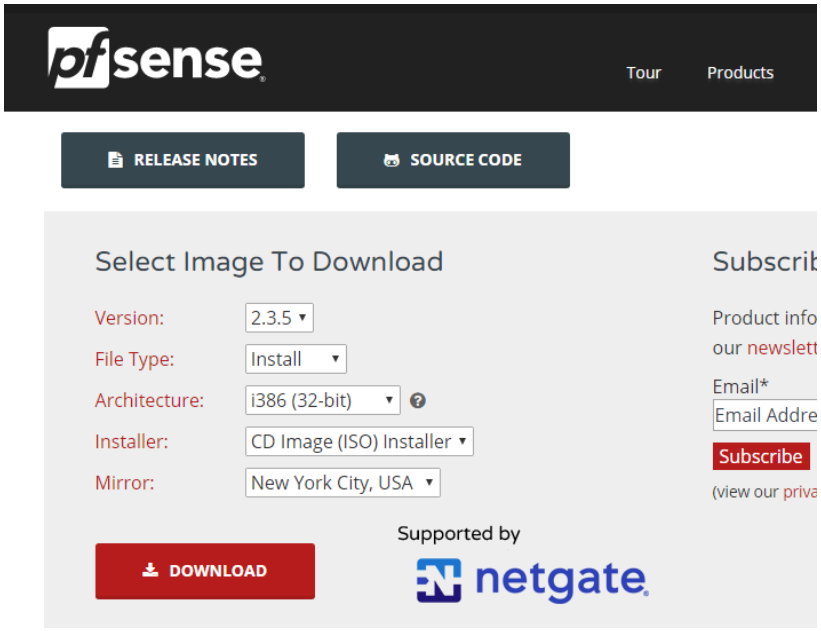
Pfsense

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

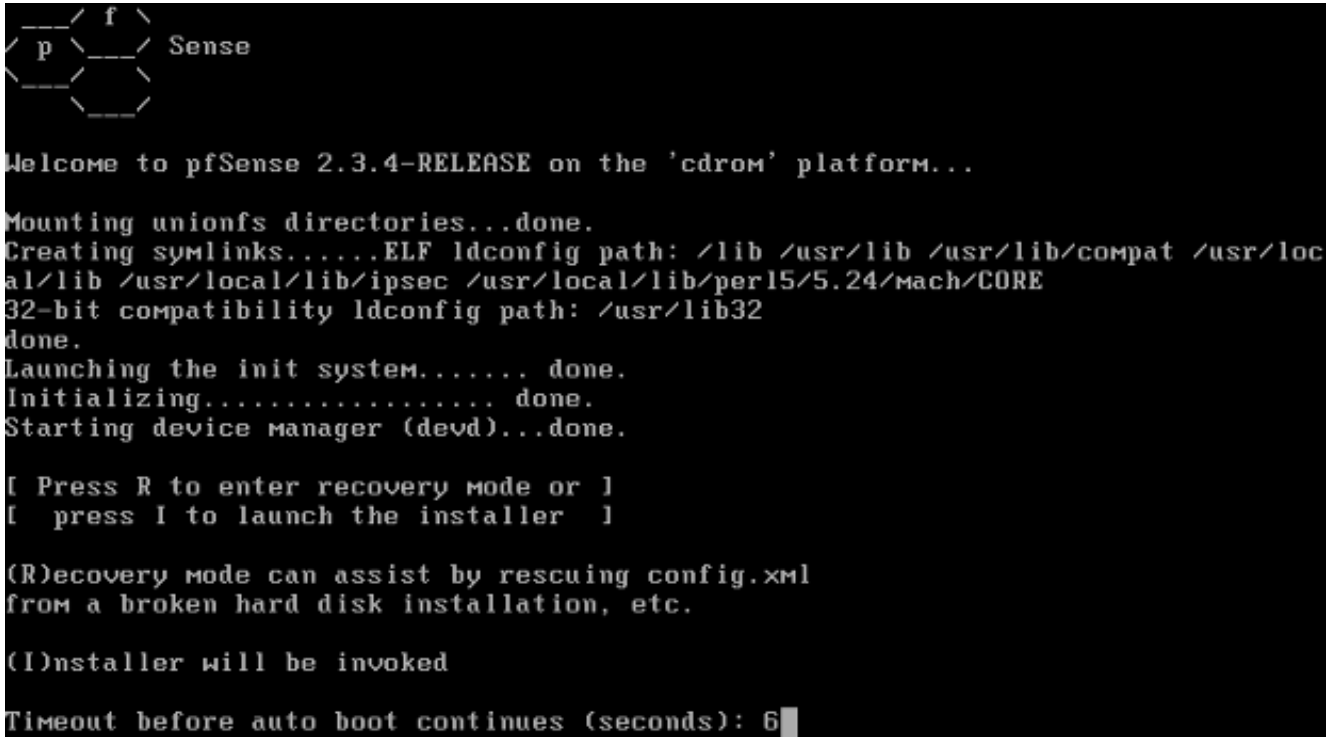
- https://www.pfsense.org/download/



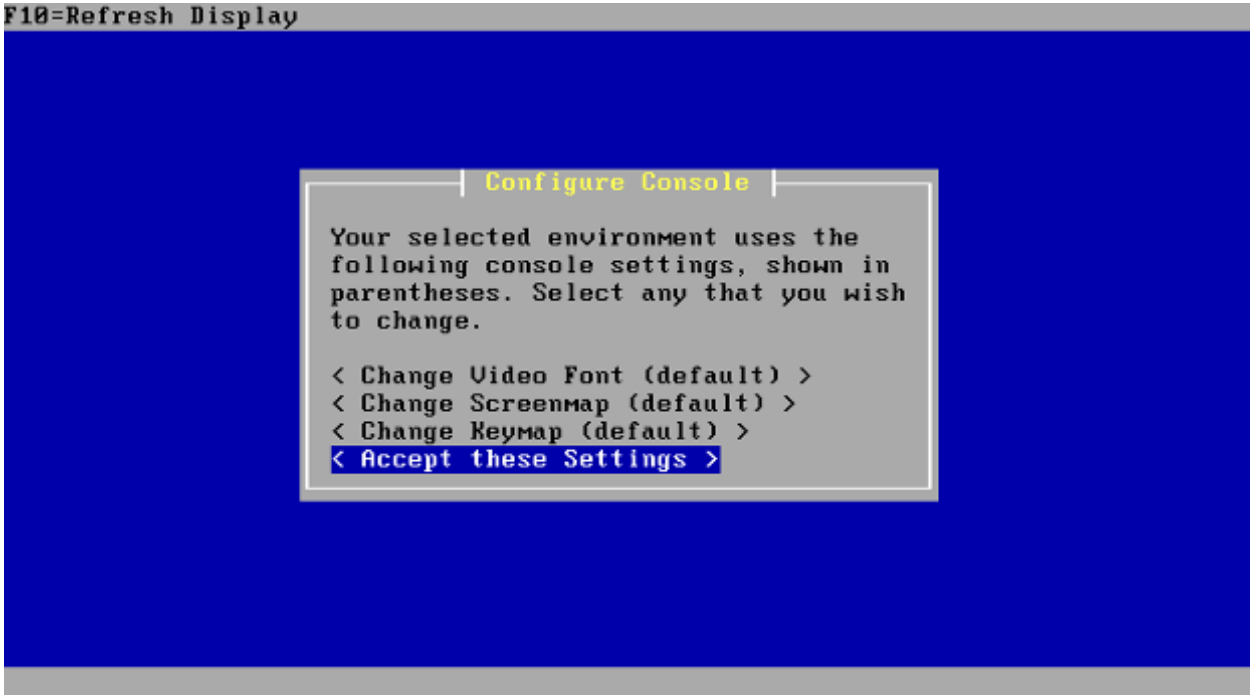
Insérez pfSense dans le lecteur de DVD ou, s'il s'agit d'une VM, sélectionnez l'image Iso

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

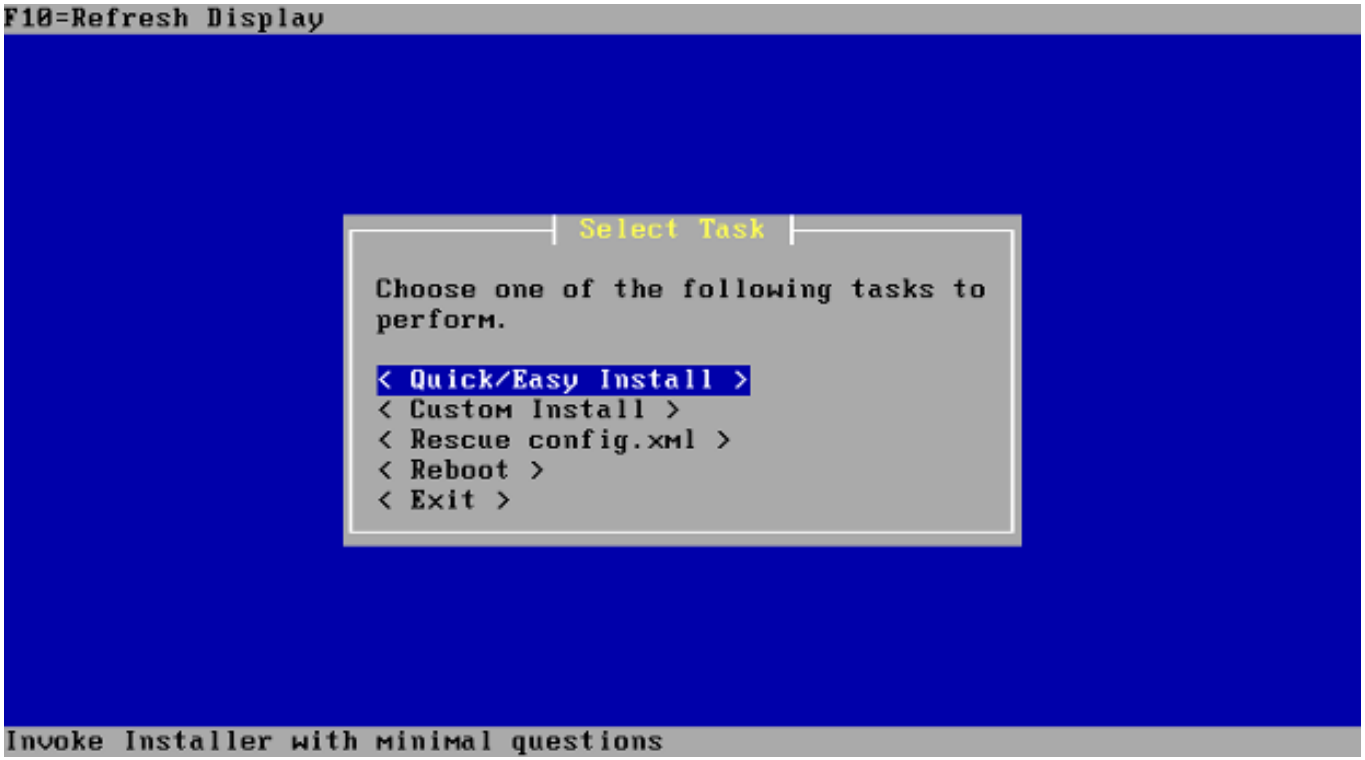
=> Appuyez sur la touche [I] - Press I to launch the installer



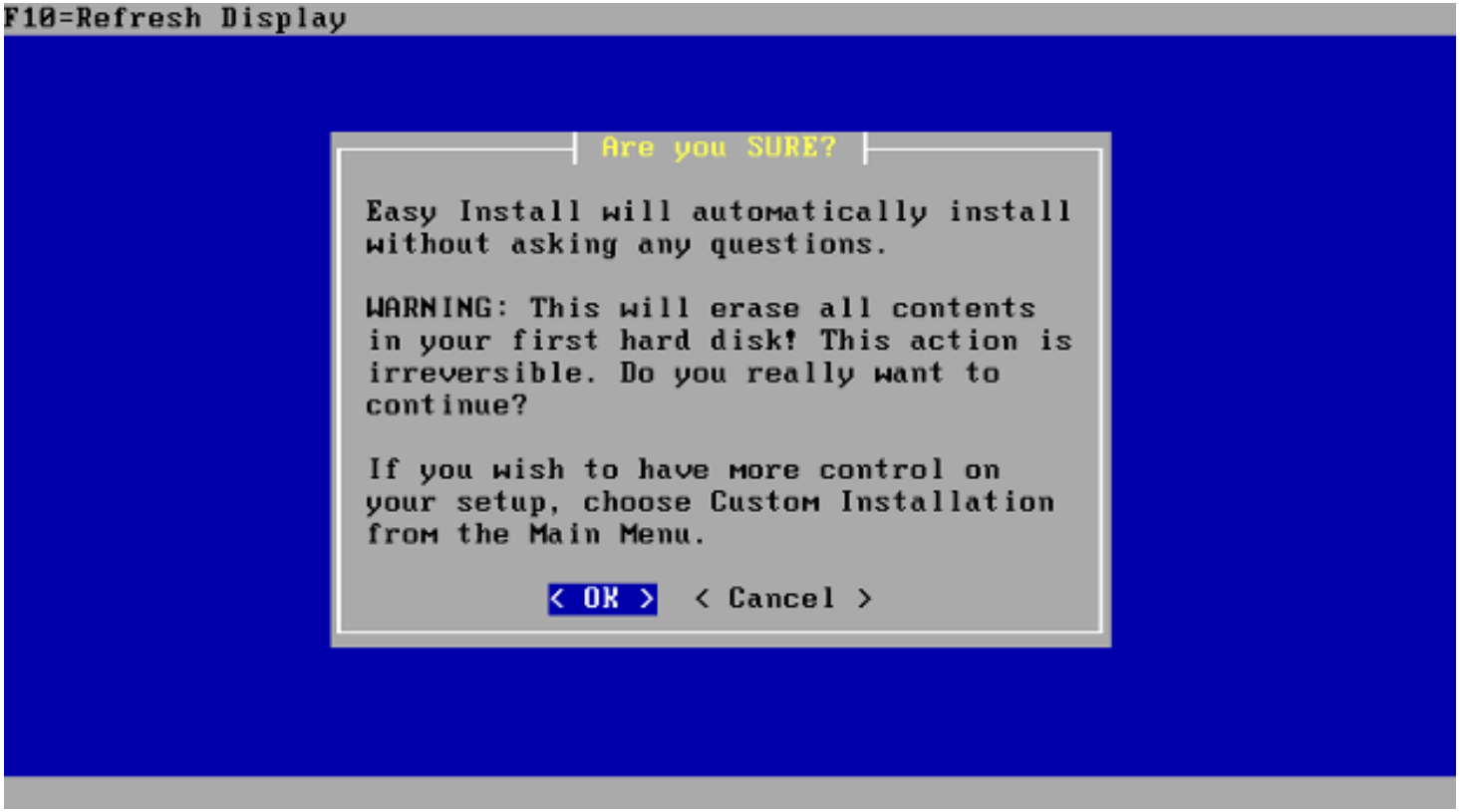
=> Sélectionnez < Accept these Settings >



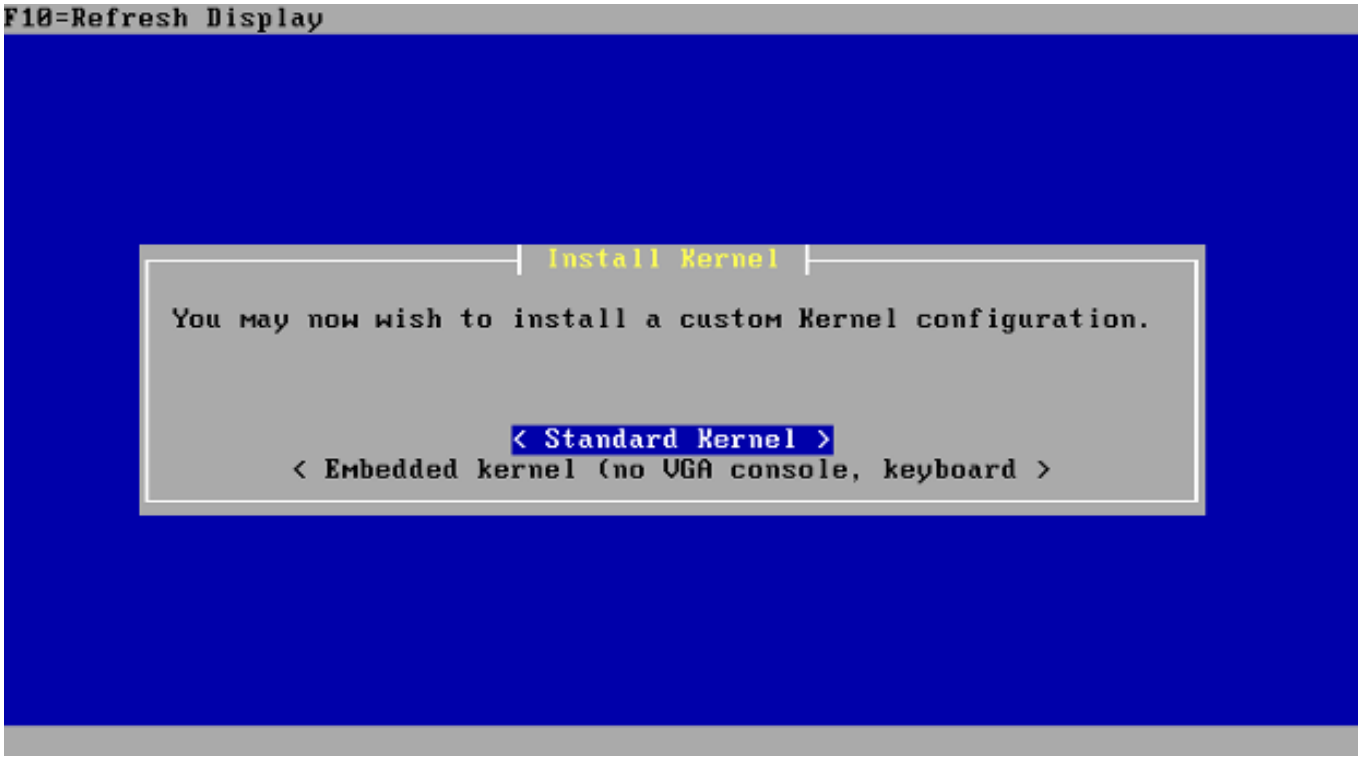
=> Sélectionnez < Quick/Easy Install >



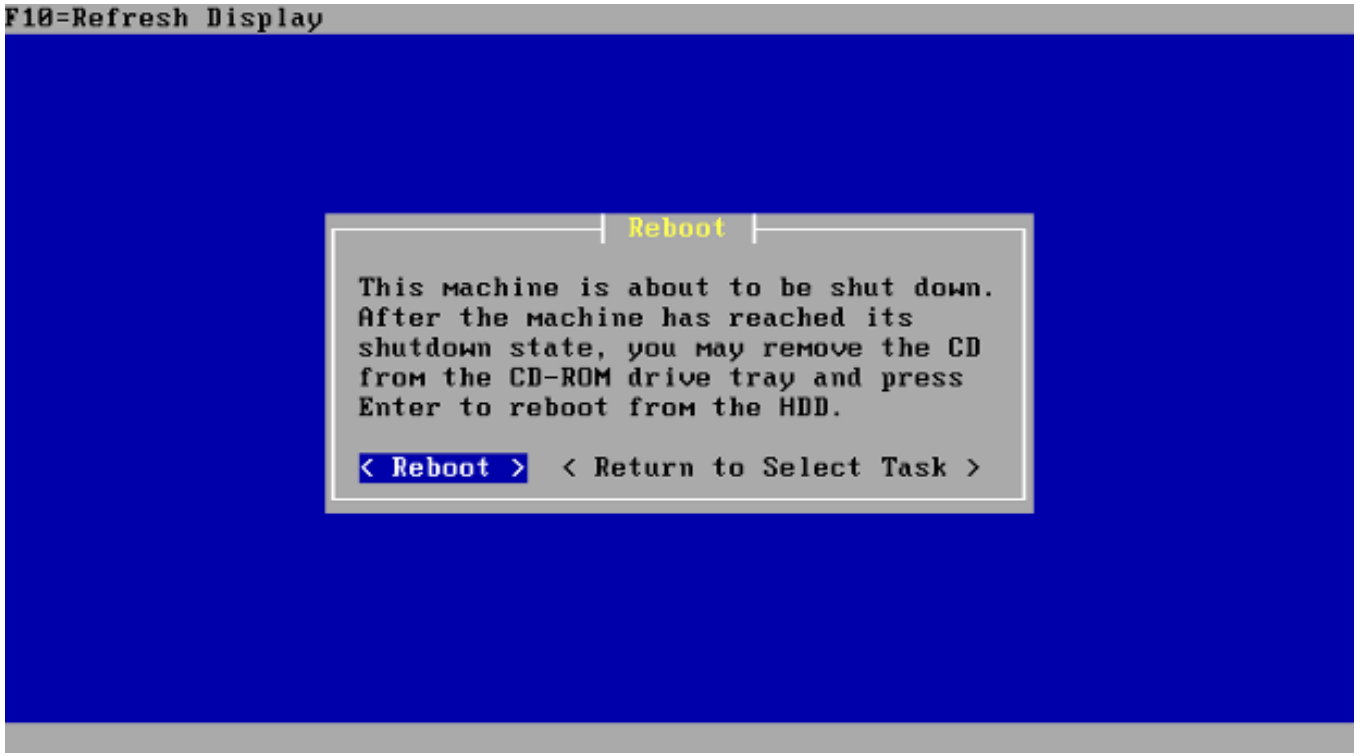
=> Sélectionnez < OK >



=> Sélectionnez < Standard Kernel >

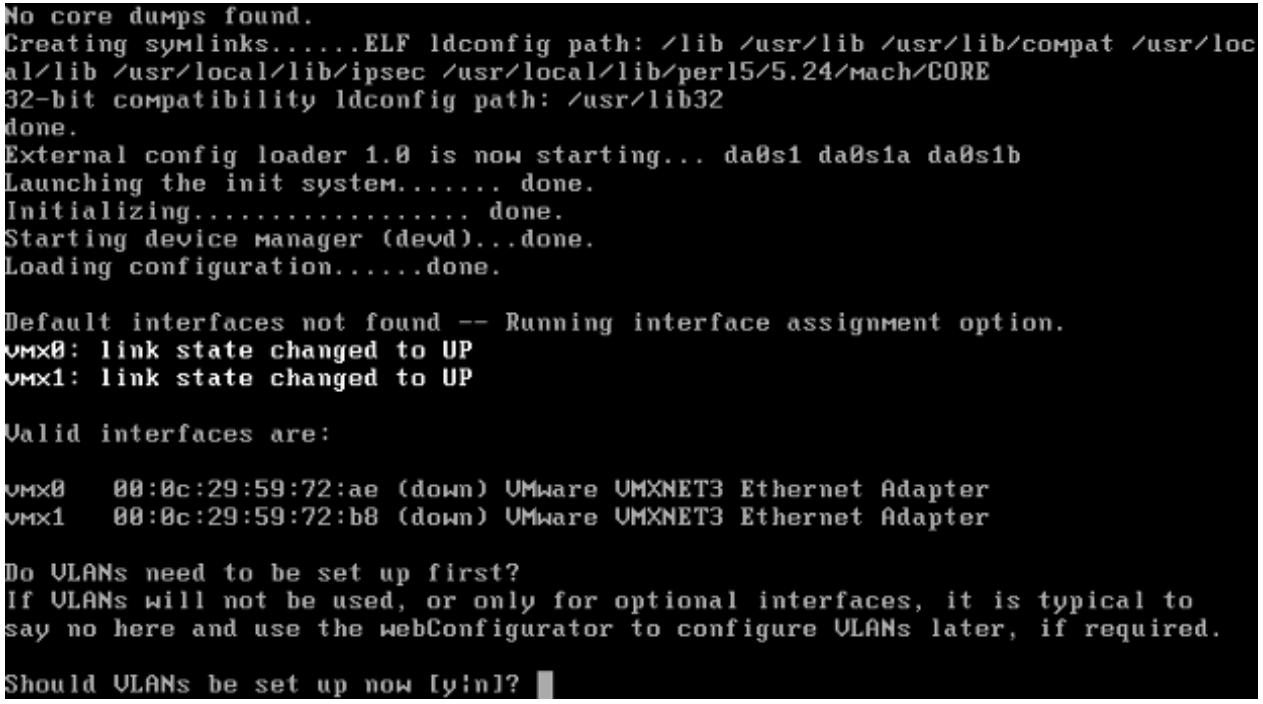


=> Sélectionnez < Reboot >

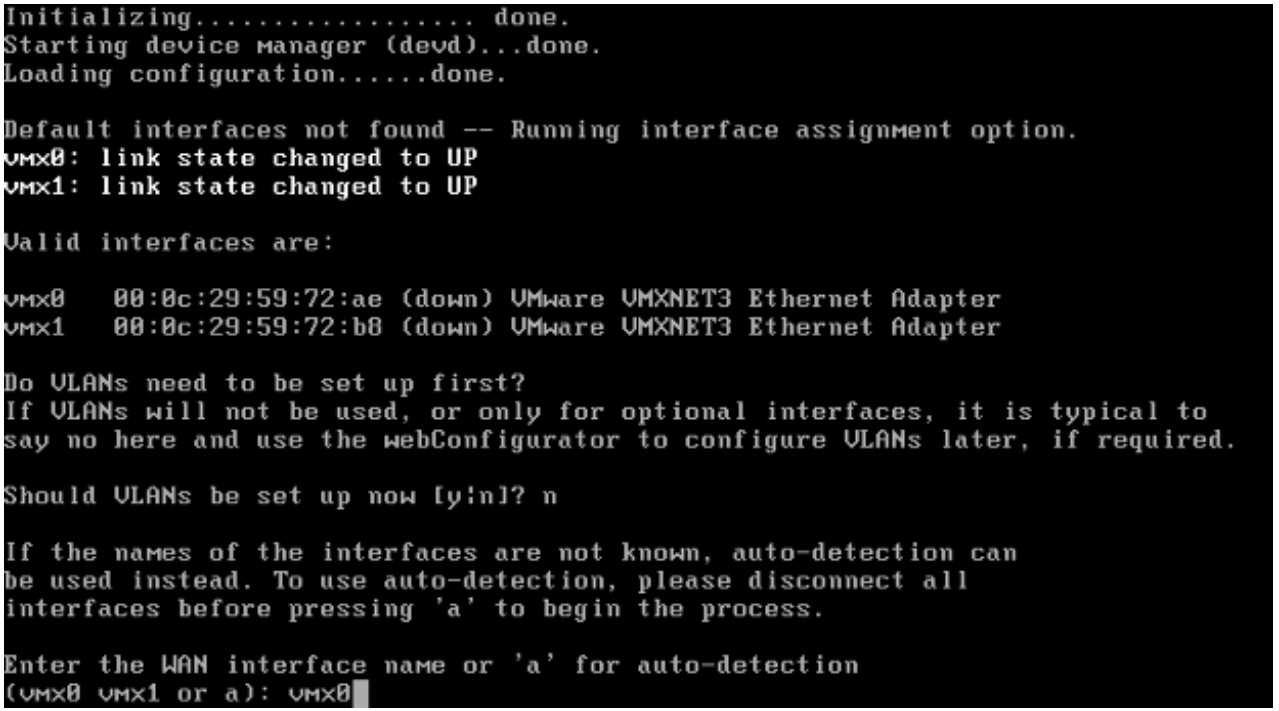


Après ce premier redémarrage, le système nécessite un paramétrage de base pour y accéder via une interface Web. Répondez aux questions suivantes :

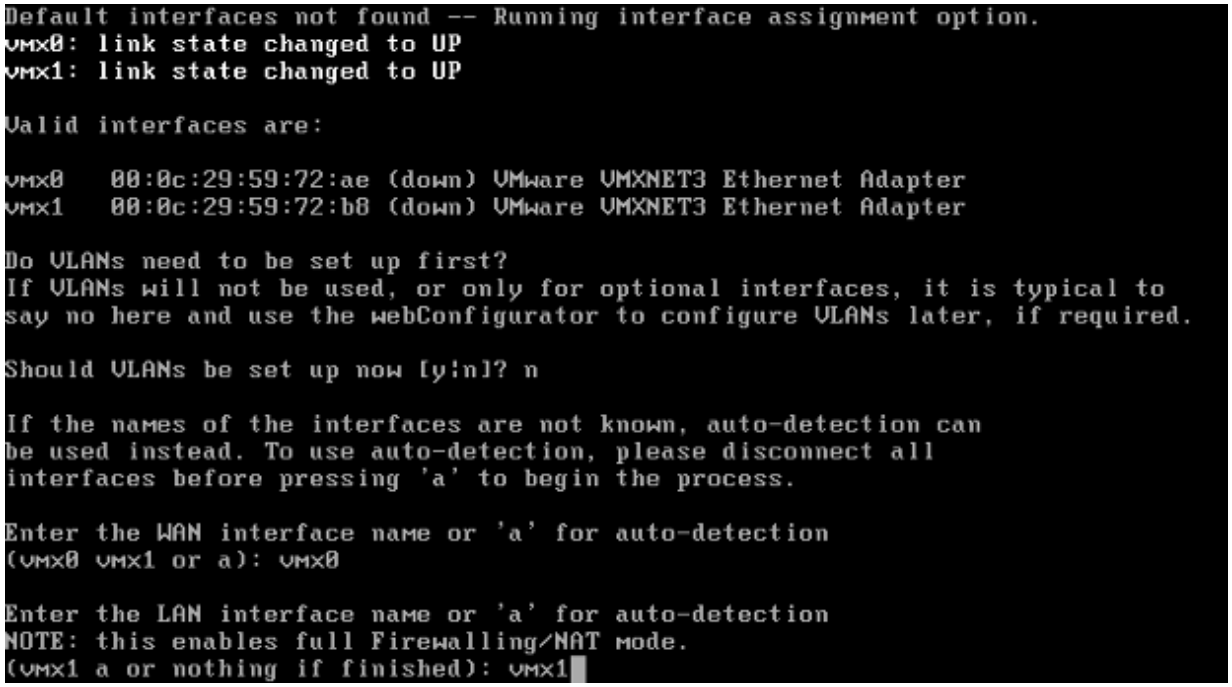
=> Should VLANs be set up now [y|n] ?
Tapez "n"



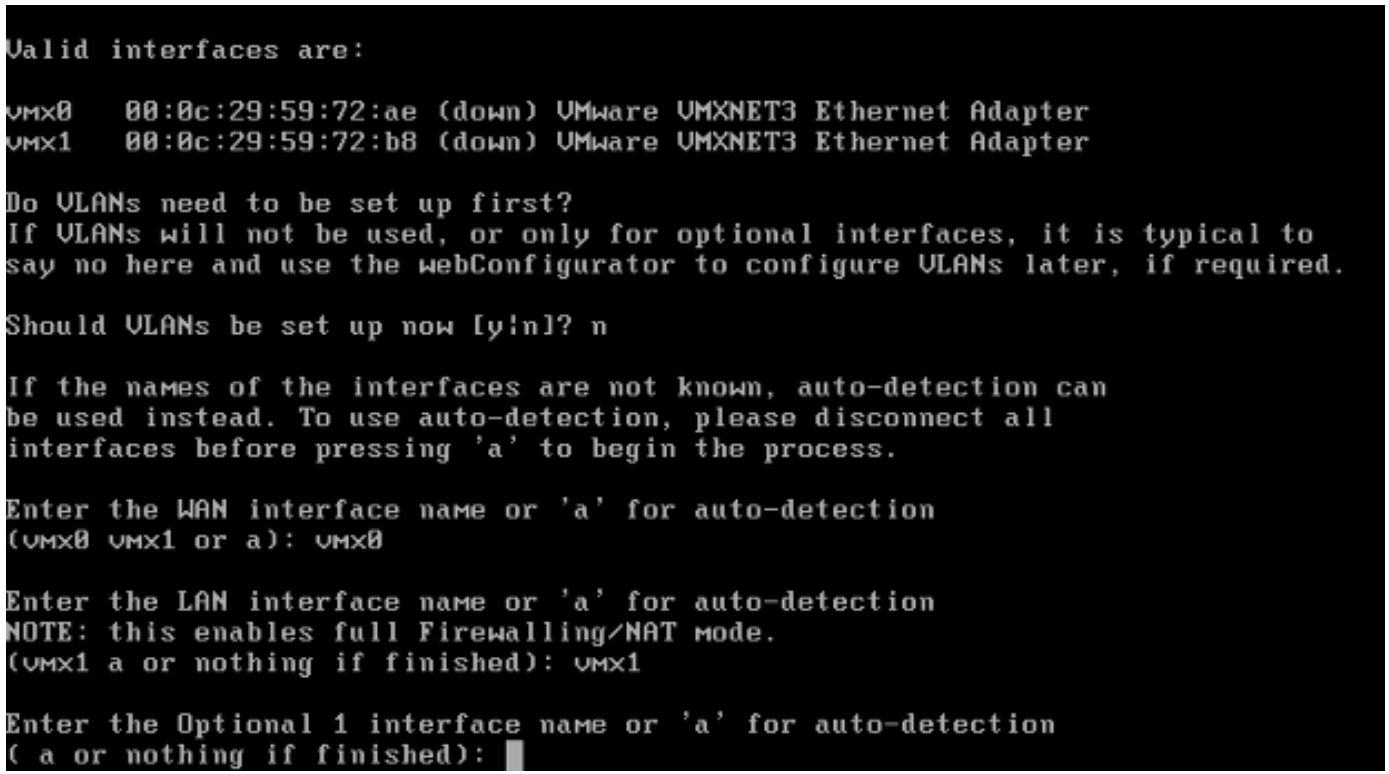
L'interface reliée à Internet est "vmx0".
=> Enter the WAN interface name or 'a' for auto-detection : Tapez "vmx0"



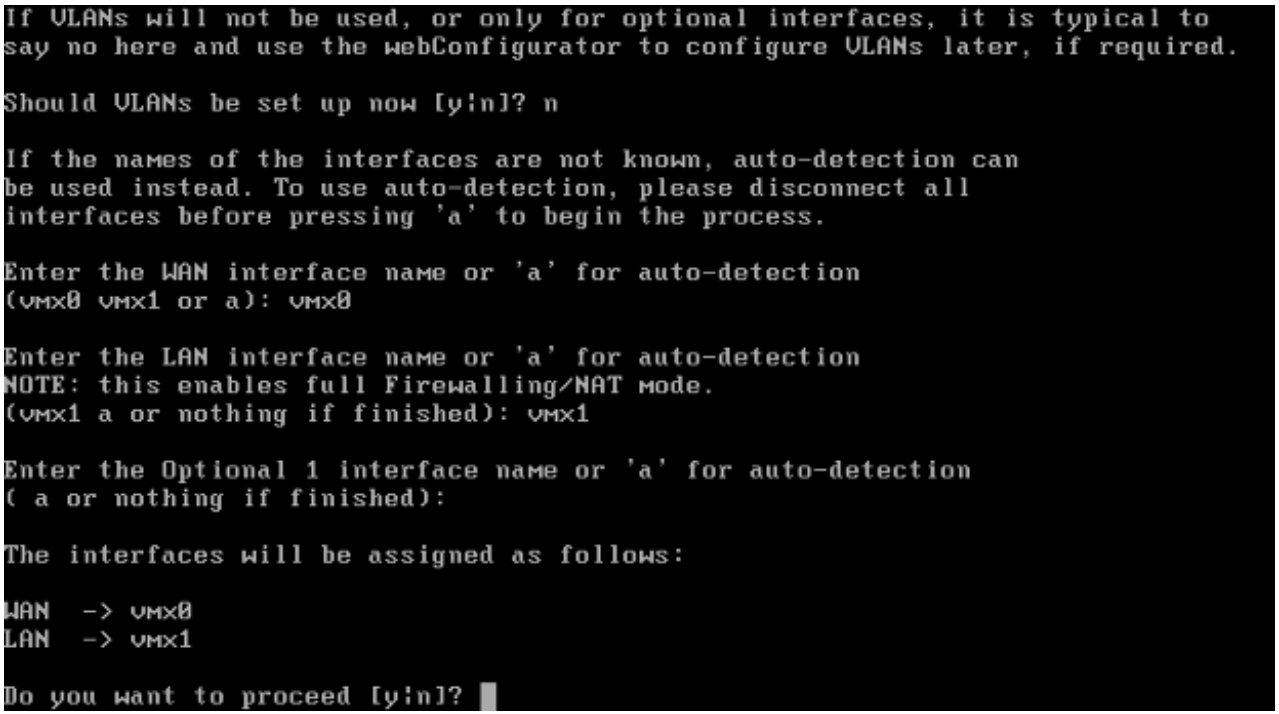
L'interface reliée au réseau local est "vmx1".
=> Enter the LAN interface name or 'a' for auto-detection : Tapez "vmx1"



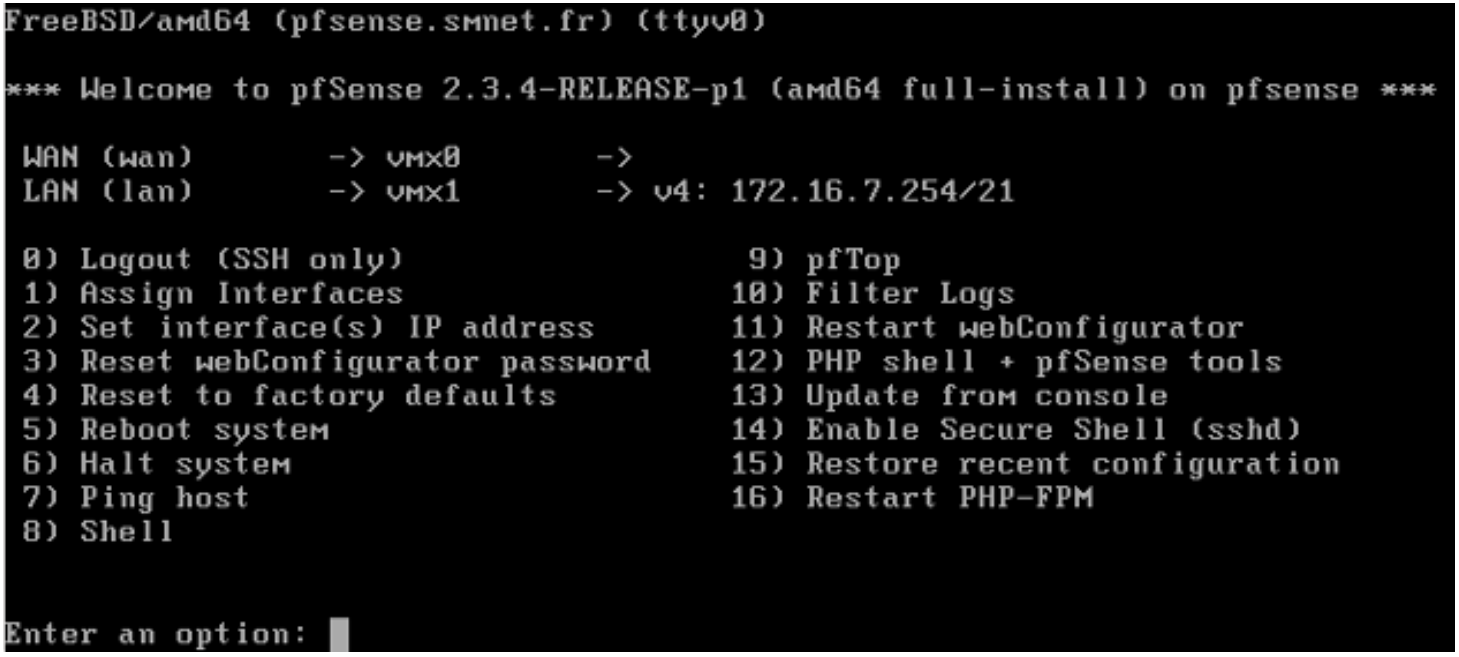
Nous n'avons pas d'autres interfaces.
=> Enter the optional 1 interface name or 'a' for auto-detection
: Appuyez sur la touche [Entrée]



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"



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



Wireshark

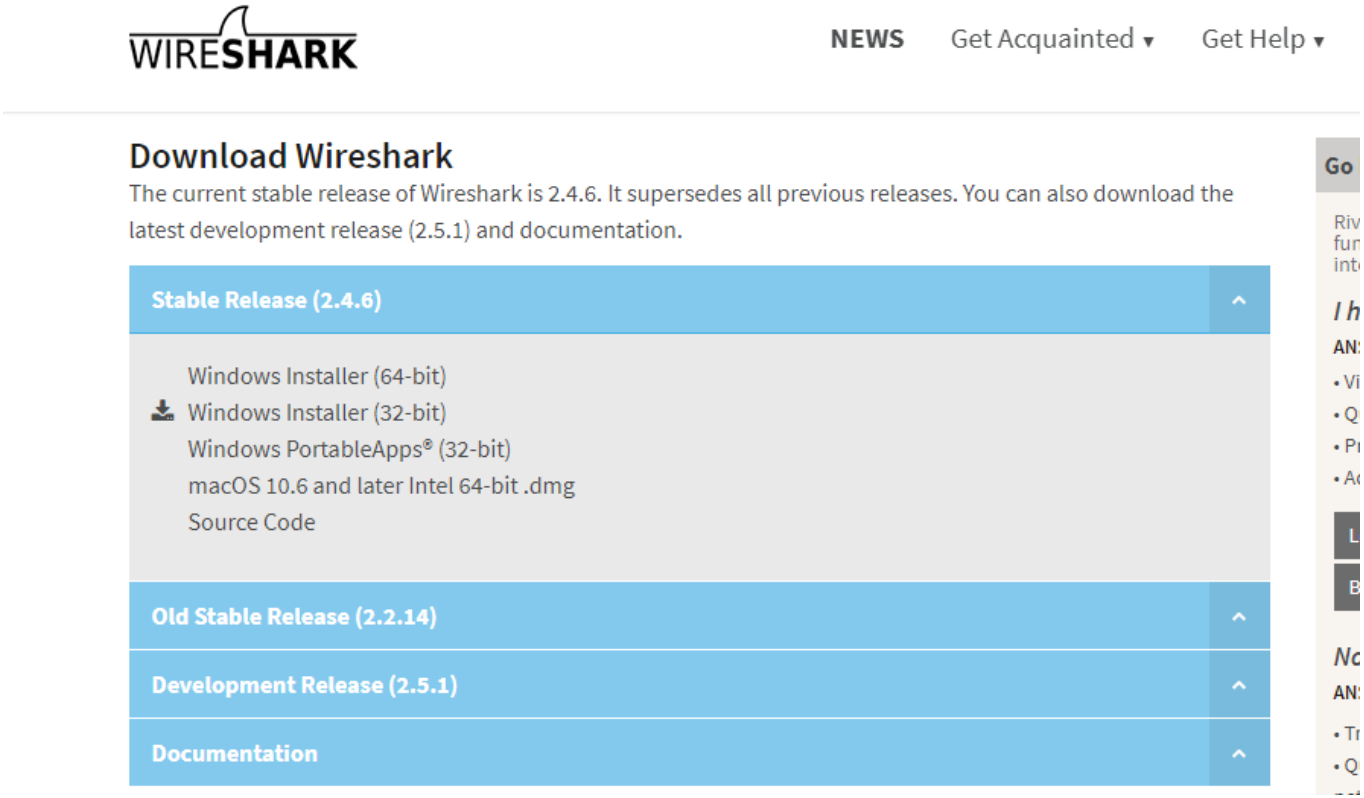
- Wireshark est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles.

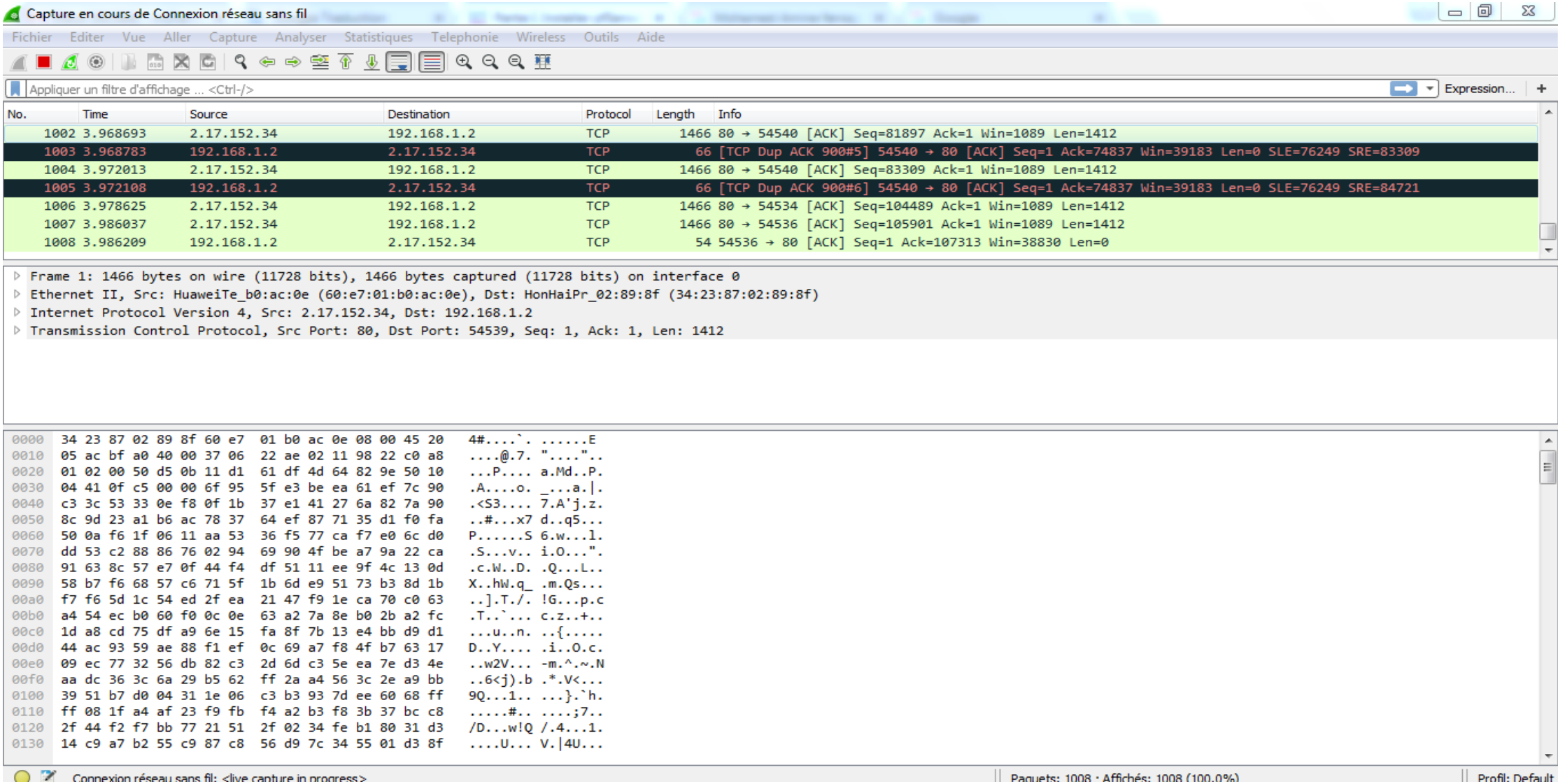
- il fonctionne sur de nombreux environnements compatibles UNIX comme GNU/Linux, FreeBSD, NetBSD, OpenBSD ou Mac OSX, mais également sur Microsoft Windows

- Il existe aussi entre autre une version en ligne de commande nommé TShark.

Téléchargement

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




Capture en cours de Connexion réseau sans fil
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
Appliquer un filtre d'affichage ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1002 3.968693 2.17.152.34 192.168.1.2 TCP 1466 80 → 54540 [ACK] Seq=81897 Ack=1 Win=1089 Len=1412
1003 3.968783 192.168.1.2 2.17.152.34 TCP 66 [TCP Dup ACK 900#5] 54540 → 80 [ACK] Seq=1 Ack=74837 Win=39183 Len=0 SLE=76249 SRE=83309
1004 3.972013 2.17.152.34 192.168.1.2 TCP 1466 80 → 54540 [ACK] Seq=83309 Ack=1 Win=1089 Len=1412
1005 3.972108 192.168.1.2 2.17.152.34 TCP 66 [TCP Dup ACK 900#6] 54540 → 80 [ACK] Seq=1 Ack=74837 Win=39183 Len=0 SLE=76249 SRE=84721
1006 3.978625 2.17.152.34 192.168.1.2 TCP 1466 80 → 54534 [ACK] Seq=104489 Ack=1 Win=1089 Len=1412
1007 3.986037 2.17.152.34 192.168.1.2 TCP 1466 80 → 54536 [ACK] Seq=105901 Ack=1 Win=1089 Len=1412
1008 3.986209 192.168.1.2 2.17.152.34 TCP 54 54536 → 80 [ACK] Seq=1 Ack=107313 Win=38830 Len=0
Frame 1: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface 0
Ethernet II, Src: HuaweiTe_b0:ac:0e (60:e7:01:b0:ac:0e), Dst: HonHaiPr_02:89:8f (34:23:87:02:89:8f)
Internet Protocol Version 4, Src: 2.17.152.34, Dst: 192.168.1.2
Transmission Control Protocol, Src Port: 80, Dst Port: 54539, Seq: 1, Ack: 1, Len: 1412
0000 34 23 87 02 89 8f 60 e7 01 b0 ac 0e 08 00 45 20 4#....`. ......E
0010 05 ac bf a0 40 00 37 06 22 ae 02 11 98 22 c0 a8 ....@.7. "....".
0020 01 02 00 50 d5 0b 11 d1 61 df 4d 64 82 9e 50 10 ...P.... a.Md..P.
0030 04 41 0f c5 00 00 6f 95 5f e3 be ea 61 ef 7c 90 .A....o. _...a.|.
0040 c3 3c 53 33 0e f8 0f 1b 37 e1 41 27 6a 82 7a 90 .<S3.... 7.A'j.z.
0050 8c 9d 23 a1 b6 ac 78 37 64 ef 87 71 35 d1 f0 fa ..#...x7 d..q5...
0060 50 0a f6 1f 06 11 aa 53 36 f5 77 ca f7 e0 6c d0 P......S 6.w...l.
0070 dd 53 c2 88 86 76 02 94 69 90 4f be a7 9a 22 ca .S...v.. i.O...".
0080 91 63 8c 57 e7 0f 44 f4 df 51 11 ee 9f 4c 13 0d .c.W..D. .Q...L..
0090 58 b7 f6 68 57 c6 71 5f 1b 6d e9 51 73 b3 8d 1b X..hW.q_ .m.Qs...
00a0 f7 f6 5d 1c 54 ed 2f ea 21 47 f9 1e ca 70 c0 63 ..].T./. !G...p.c
00b0 a4 54 ec b0 60 f0 0c 0e 63 a2 7a 8e b0 2b a2 fc .T..`... c.z..+..
00c0 1d a8 cd 75 df a9 6e 15 fa 8f 7b 13 e4 bb d9 d1 ...u..n. ..{.....
00d0 44 ac 93 59 ae 88 f1 ef 0c 69 a7 f8 4f b7 63 17 D..Y.... .i..O.c.
00e0 09 ec 77 32 56 db 82 c3 2d 6d c3 5e ea 7e d3 4e ..w2V... -m.^.~.N
00f0 aa dc 36 3c 6a 29 b5 62 ff 2a a4 56 3c 2e a9 bb ..6<j).b .*.V<...
0100 39 51 b7 d0 04 31 1e 06 c3 b3 93 7d ee 60 68 ff 9Q...1.. ...}.`h.
0110 ff 08 1f a4 af 23 f9 fb f4 a2 b3 f8 3b 37 bc c8 .....#.. ....;7..
0120 2f 44 f2 f7 bb 77 21 51 2f 02 34 fe b1 80 31 d3 /D...w!Q /.4...1.
0130 14 c9 a7 b2 55 c9 87 c8 56 d9 7c 34 55 01 d3 8f ....U... V.|4U...
Connexion réseau sans fil: <live capture in progress>
Paquets: 1008 · Affichés: 1008 (100.0%)
Profil: Default

Wireshark - Code couleur

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

•**Drapeaux (flags)** (6x1 bit): Les drapeaux représentent des informations supplémentaires :
•**URG**: si ce drapeau est à 1 le paquet doit être traité de façon urgente.
•**ACK**: si ce drapeau est à 1 le paquet est un accusé de réception.
•**PSH** (PUSH): si ce drapeau est à 1, le paquet fonctionne suivant la méthode PUSH.
•**RST**: si ce drapeau est à 1, la connexion est réinitialisée.
•**SYN**: Le Flag TCP SYN indique une demande d'établissement de connexion.
•**FIN**: si ce drapeau est à 1 la connexion s'interrompt.

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

Cours - Sécurité Informatique - 3 LMD Système d'Information
2018-2019

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

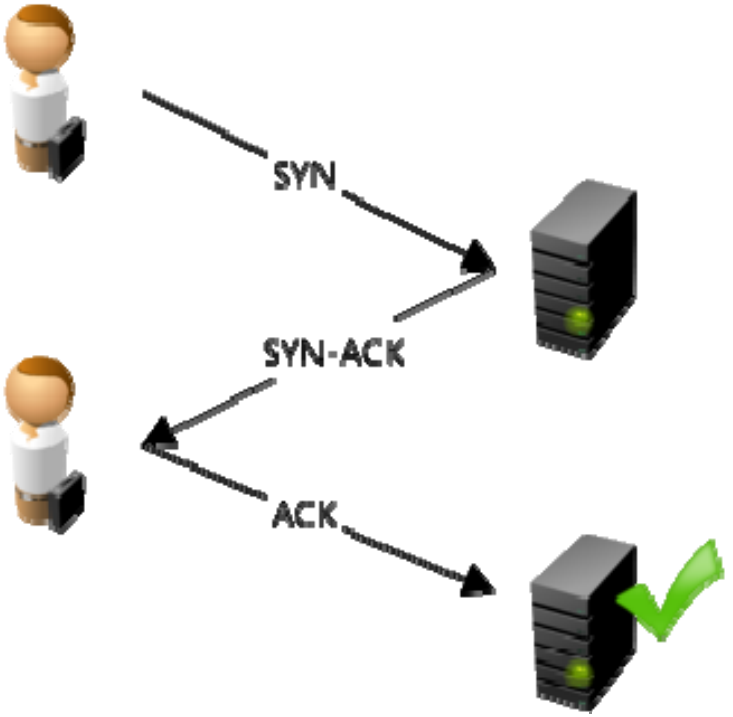
- Kali Linux propose plus de 6008 programmes d'analyse de sécurité pré-installés, dont
    - Armitage (un outil graphique de contrôle des attaques),
    - nmap (un scanneur de port),
    - Wireshark (un analyseur de paquets),
    - John the Ripper (un outil de cassage de mots de passe),
    - Aircrack-ng (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)

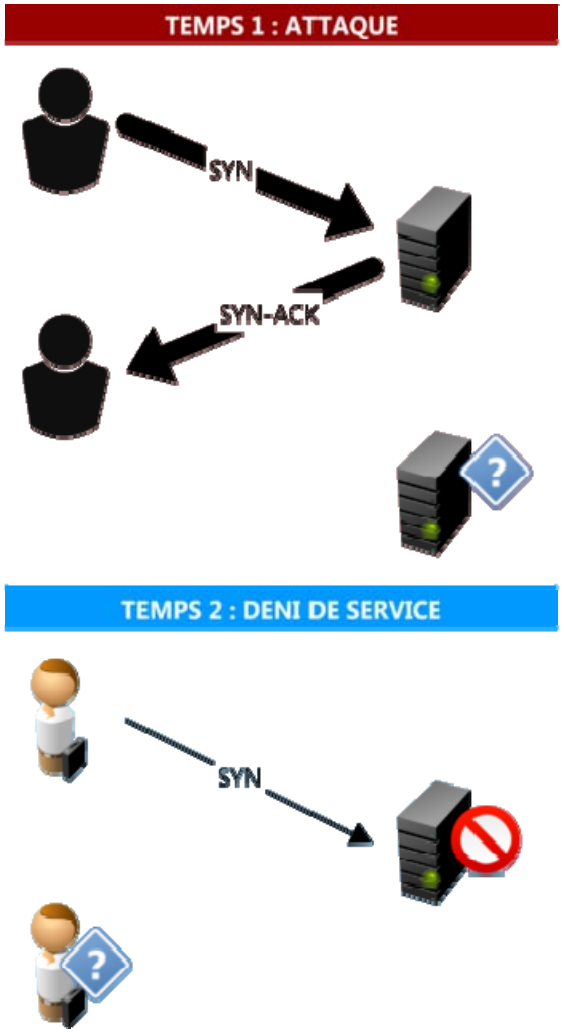
- Le SYN flood est une attaque informatique visant à atteindre un déni de service. Elle s'applique dans le cadre du protocole TCP et consiste à envoyer une succession de requêtes SYN vers la cible.
- Lors de l'initialisation d'une connexion TCP entre un client et un serveur, un échange de messages a 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.**

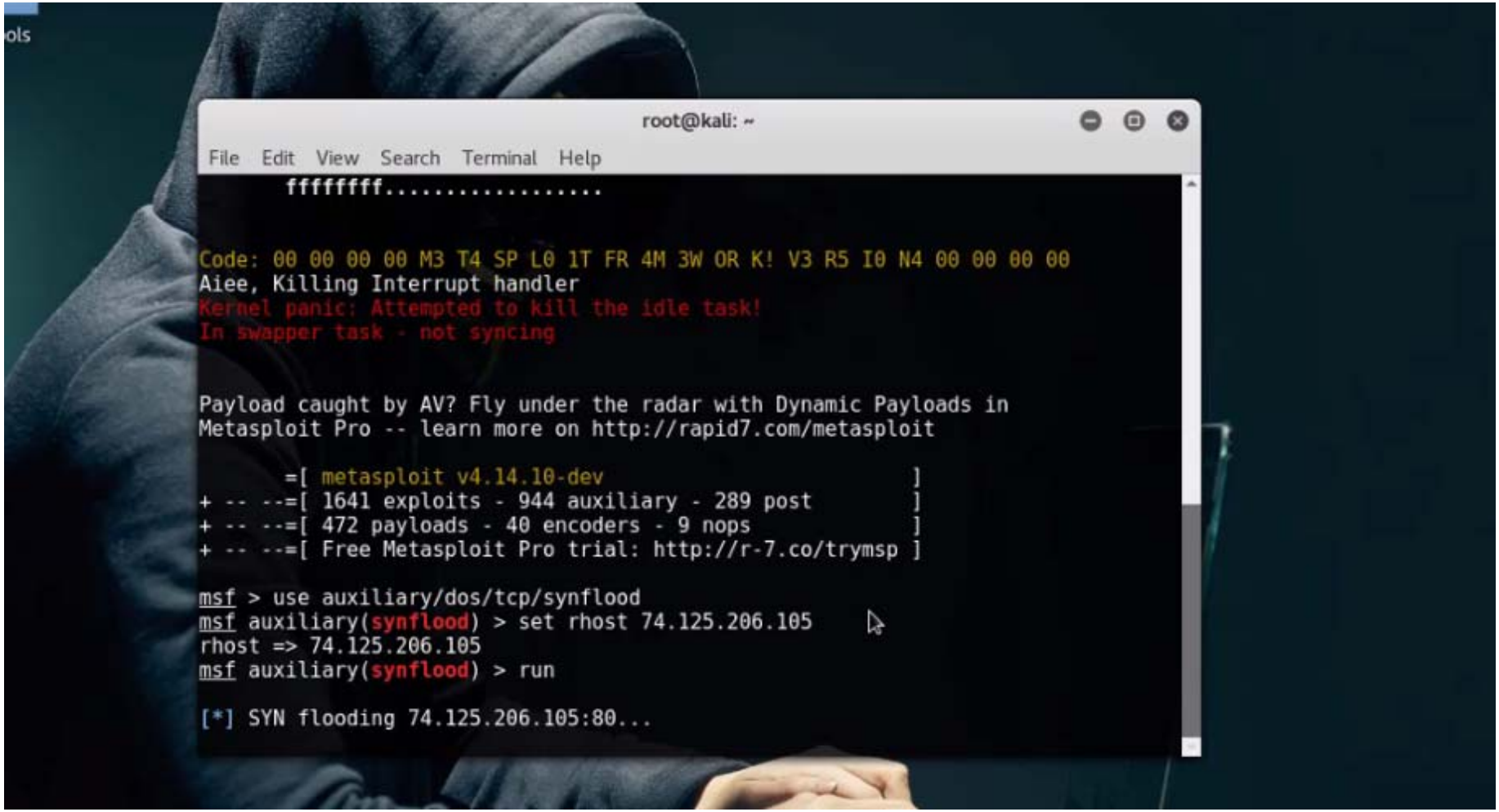


Attaque SYN flood (2)

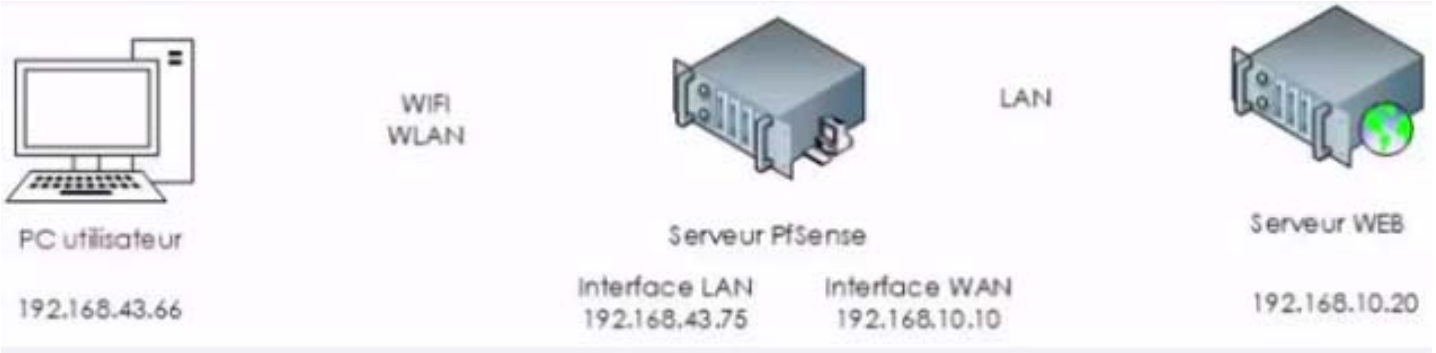
- Un client malveillant peut supprimer la dernière étape et ne pas répondre avec le message ACK. Le serveur attend un certain temps avant de libérer les ressources qui ont été réservées pour le client, car le retard du message ACK pourrait être causé par la latence du réseau. Cette période d'attente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



Attaque SYN flood avec metasploit



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

- Ross Anderson " Security Engineering "

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