

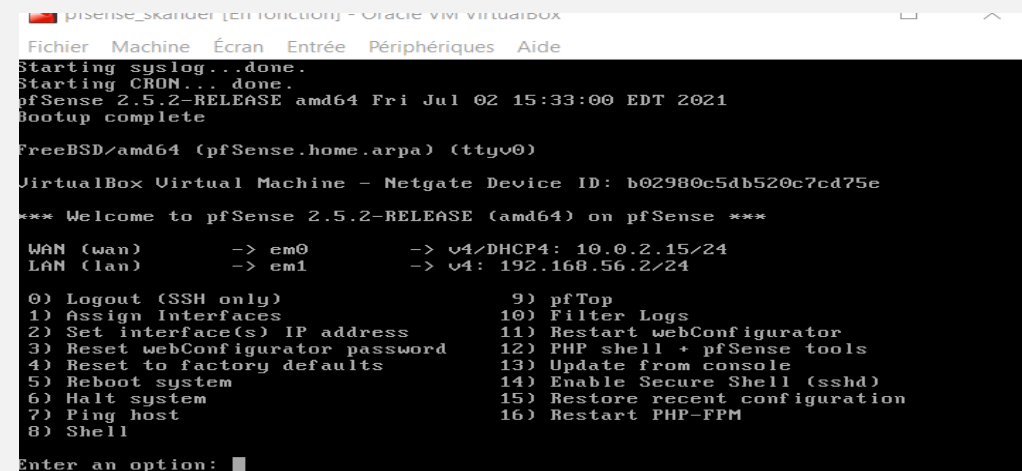
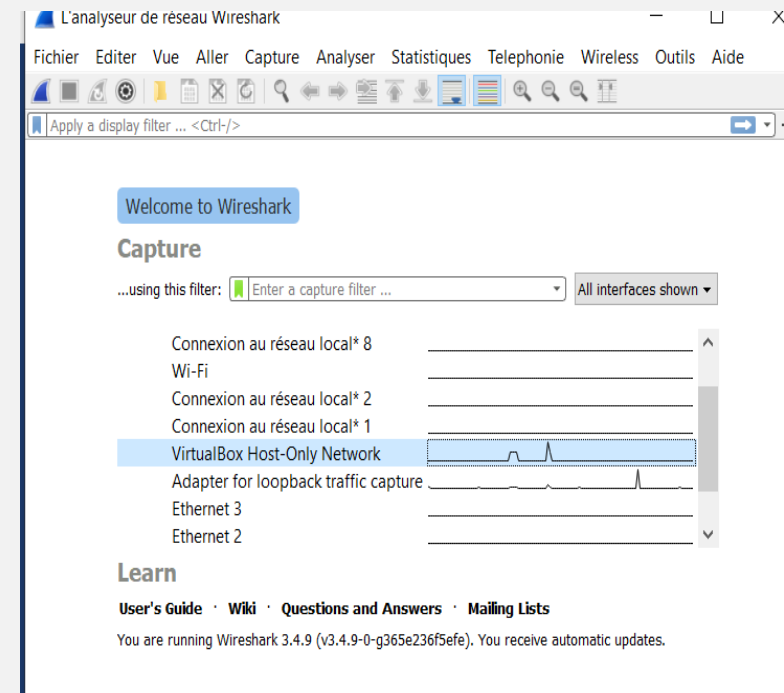
COMPTE RENDU TP2

Yasmine bettaieb- skander jmaiel-youssef hannachi l3cs02

- 1: Définir les protocoles HTTP et SSH et citer les ports utilisés:
- HTTP ou l'hypertext transfer protocol est un protocole de transfert de données sur le web qui fonctionne selon le principe "requête-réponse"
- -SSH ou secure shell est un protocole réseau cryptographique utilisé pour se connecter à un ordinateur distant pour le contrôler à l'aide de commande à distance en toute sécurité.
- 2: Quelle est l'interface qu'on doit choisir pour capturer le trafic réseau de l'interface LAN du PfSense ?

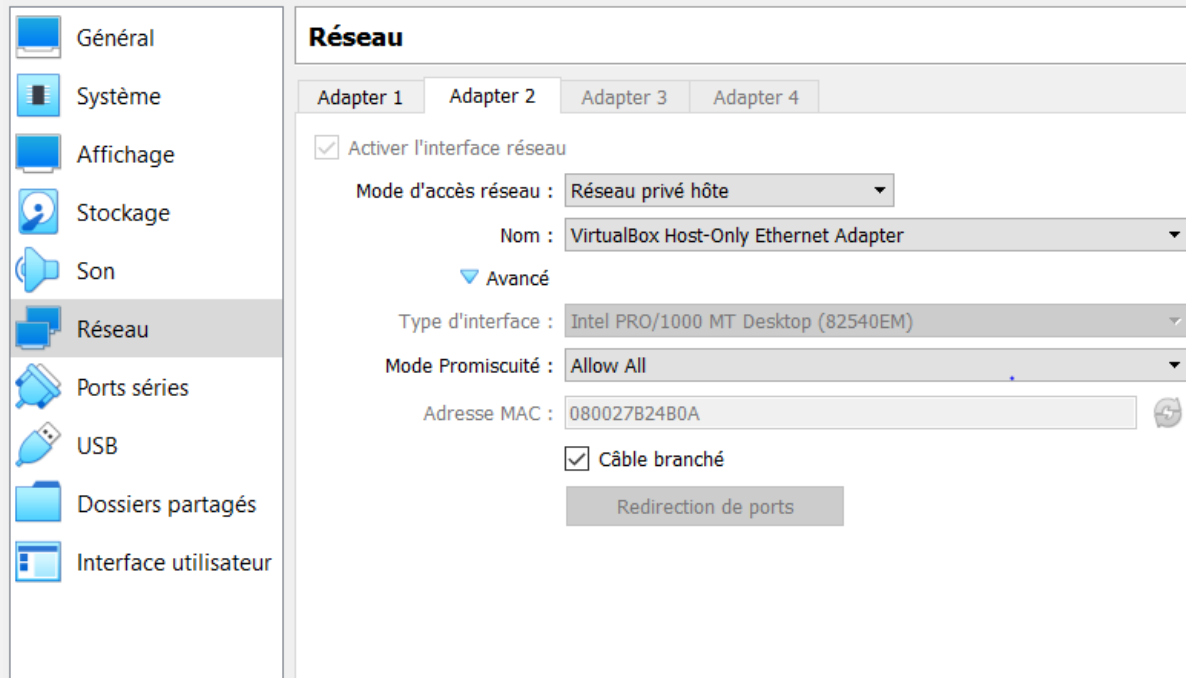
Pour capturer le trafic réseau de l'interface LAN de pfSense on choisit l'interface qui a la même adresse IP de ce dernier.

Ici l'interface concernée est "Virtual Box Host Only Network" avec l'adresse IP 192.168.56.2



- 3- Modifier l'interface réseau de la machine cliente Ubuntu pour activer le mode

« Promiscuous »



Ce mode permet est généralement utilisé pour écouter le trafic réseau il permet à la machine d'accepter tous les paquets qu'elle reçoit même si ils ne lui sont pas adressés.

- 4- Lancer Wireshark sur la bonne interface et en même temps démarrer la machine cliente.

Identifier les différents paquets DHCP échangés entre cette machine et PFSense. Interpréter ces échanges et identifier l'IP attribuée à la machine cliente. Conclure !

Capture en cours de VirtualBox Host-Only Network

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

Current filter: dhcp

No.	Time	Source	Destination	Protocol	Length	Info
3	1.984621	0.0.0.0	255.255.255.255	DHCP	344	DHCP Request - Transaction ID 0x9fdf57a2
5	1.995113	192.168.56.100	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x9fdf57a2

> Frame 5: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{B592B6B2-BF7A-403E-B33B-54F5F8E624E}, id 0

▼ Ethernet II, Src: PcsCompu_8b:99:50 (08:00:27:8b:99:50), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Destination: Broadcast (ff:ff:ff:ff:ff:ff)

▼ Source: PcsCompu_8b:99:50 (08:00:27:8b:99:50)

Address: PcsCompu_8b:99:50 (08:00:27:8b:99:50)

.... 0. = LG bit: Globally unique address (factory default)

.... 0. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 192.168.56.100, Dst: 255.255.255.255

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

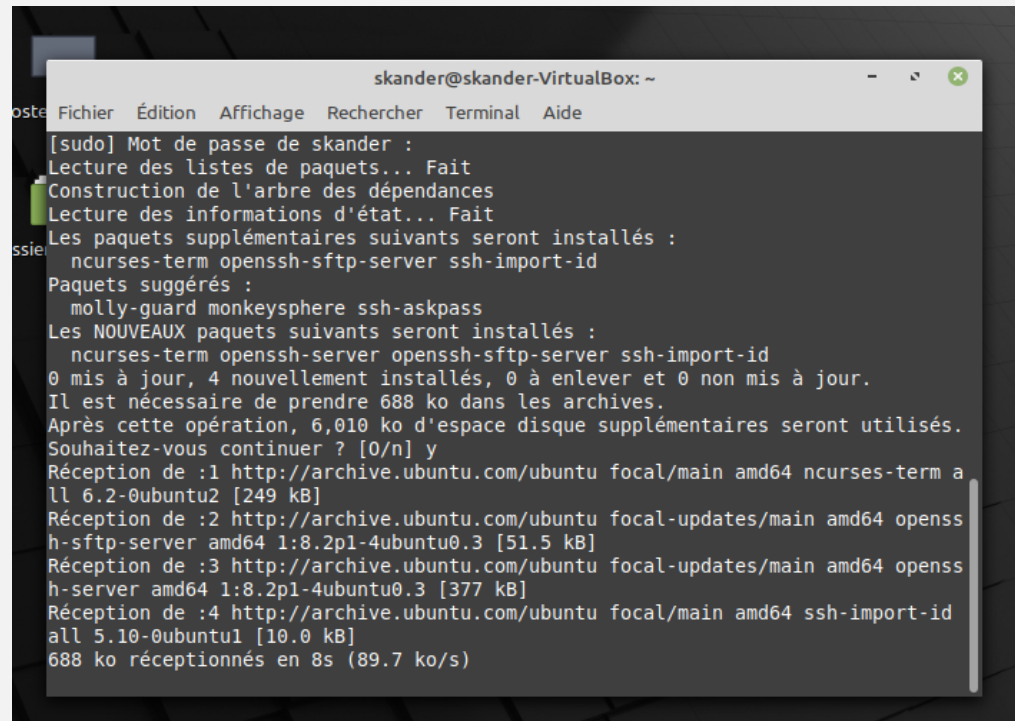
0000 00.. = Differentiated Services Codepoint: Default (0)

Wireshark a intercepté deux paquets DHCP le premier correspond à la requête DHCP envoyé par la machine mint à pfsense qui joue le rôle du serveur DHCP.

Le deuxième est un paquet DHCP Ack dans le quel le serveur DHCP (pfsense) a transféré à la machine mint les données de configuration réseau :adresse IP ,masque , gateway ,... la ligne sélectionnée en bas de l'image ci-dessous comporte l'adresse IP envoyée par pfsense et qui va être assignée à la machine mint.

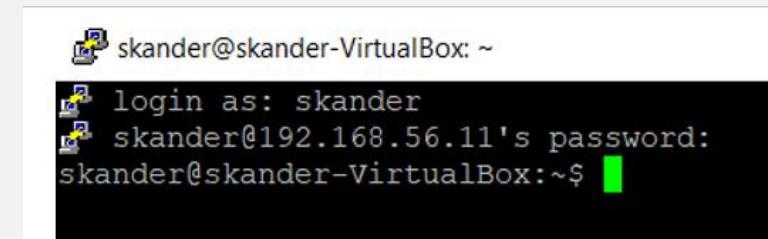
5- Avec l'outil de connexion distante [Putty](#), essayer de se connecter en SSH vers la machine cliente. Identifier les paquets échangés. Pouvez-vous récupérer les paramètres de connexion échangés ? Pourquoi ?

On doit d'abord installer le package openssh avec la commande suivante : `apt-get install openssh-server`



```
skander@skander-VirtualBox: ~  
[sudo] Mot de passe de skander :  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances  
Lecture des informations d'état... Fait  
Les paquets supplémentaires suivants seront installés :  
  ncurses-term openssh-sftp-server ssh-import-id  
Paquets suggérés :  
  molly-guard monkeysphere ssh-askpass  
Les NOUVEAUX paquets suivants seront installés :  
  ncurses-term openssh-server openssh-sftp-server ssh-import-id  
0 mis à jour, 4 nouvellement installés, 0 à enlever et 0 non mis à jour.  
Il est nécessaire de prendre 688 ko dans les archives.  
Après cette opération, 6,010 ko d'espace disque supplémentaires seront utilisés.  
Souhaitez-vous continuer ? [0/n] y  
Réception de :1 http://archive.ubuntu.com/ubuntu focal/main amd64 ncurses-term a  
ll 6.2-0ubuntu2 [249 kB]  
Réception de :2 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 opens  
h-sftp-server amd64 1:8.2p1-4ubuntu0.3 [51.5 kB]  
Réception de :3 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 opens  
h-server amd64 1:8.2p1-4ubuntu0.3 [377 kB]  
Réception de :4 http://archive.ubuntu.com/ubuntu focal/main amd64 ssh-import-id  
all 5.10-0ubuntu1 [10.0 kB]  
688 ko réceptionnés en 8s (89.7 ko/s)
```

-On se connecte à la machine mint à l'aide de putty :



```
skander@skander-VirtualBox: ~  
login as: skander  
skander@192.168.56.11's password:  
skander@skander-VirtualBox:~$
```

-ci dessous-les paquets intercepté par wireshark :

ssh					
No.	Time	Source	Destination	Protocol	Length Info
49	43.305185	192.168.56.1	192.168.56.11	SSHv2	82 Client: Protocol (SSH-2.0-PuTTY_Release_0.76)
51	43.369760	192.168.56.11	192.168.56.1	SSHv2	95 Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.3)
52	43.382349	192.168.56.1	192.168.56.11	SSHv2	1310 Client: Key Exchange Init
53	43.382937	192.168.56.11	192.168.56.1	SSHv2	1110 Server: Key Exchange Init
54	43.388759	192.168.56.1	192.168.56.11	SSHv2	102 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
56	43.400599	192.168.56.11	192.168.56.1	SSHv2	518 Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted
62	49.865338	192.168.56.1	192.168.56.11	SSHv2	134 Client: New Keys, Encrypted packet (len=64)
64	49.868106	192.168.56.11	192.168.56.1	SSHv2	118 Server: Encrypted packet (len=64)
66	64.210990	192.168.56.1	192.168.56.11	SSHv2	134 Client: Encrypted packet (len=80)
67	64.218904	192.168.56.11	192.168.56.1	SSHv2	134 Server: Encrypted packet (len=80)
70	66.690580	192.168.56.1	192.168.56.11	SSHv2	326 Client: Encrypted packet (len=272)
71	66.720051	192.168.56.11	192.168.56.1	SSHv2	102 Server: Encrypted packet (len=48)

> Frame 49: 82 bytes on wire (656 bits). 82 bytes captured (656 bits) on interface \Device\NPF {B592B6B2-BF7A-403E-B33B-54F5F8BE624E}. id 0

on ne peut pas récupérer les paramètres de connexion échangés , les données sont cryptées(“Encrypted packet”) grâce au protocole SSH

6- Maintenant, ouvrir la page web du PfSense. Lancer une nouvelle capture Wireshark. Entrer les paramètres de connexion. Analyser le trafic capturé. Pouvez-vous récupérer les identifiants de connexion ?

*VirtualBox Host-Only Network

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.56.1	192.168.56.2	TLSv1.2	93	Application Data
2	0.000252	192.168.56.2	192.168.56.1	TCP	54	443 → 64054 [ACK] Seq=1 Ack=40 Win=514 Len=0
3	0.000361	192.168.56.2	192.168.56.1	TLSv1.2	93	Application Data
4	0.003810	192.168.56.1	192.168.56.2	TLSv1.2	154	Application Data
5	0.003847	192.168.56.1	192.168.56.2	TLSv1.2	270	Application Data
6	0.004048	192.168.56.2	192.168.56.1	TCP	54	443 → 64054 [ACK] Seq=40 Ack=140 Win=514 Len=0
7	0.004089	192.168.56.2	192.168.56.1	TCP	54	443 → 64054 [ACK] Seq=40 Ack=356 Win=513 Len=0
8	0.004269	192.168.56.2	192.168.56.1	TLSv1.2	89	Application Data
9	0.044163	192.168.56.1	192.168.56.2	TCP	54	64054 → 443 [ACK] Seq=356 Ack=75 Win=8207 Len=0
10	0.053359	192.168.56.2	192.168.56.1	TLSv1.2	415	Application Data
11	0.062486	192.168.56.1	192.168.56.2	TLSv1.2	142	Application Data
12	0.062702	192.168.56.2	192.168.56.1	TCP	54	443 → 64054 [ACK] Seq=436 Ack=444 Win=514 Len=0

[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)

Les données sont capturées par wireshark et ne sont pas protégées pour remédier à cette faille il faut activer SSH sur pfsense.

Fin tp.