BTS SIO 2022

Support et mise à disposition de services informatiques (E4)

PAGE DE PRÉSENTATION DU DOSSIER

N° de candidat1 : |0|2|1|4|6|7|1|7|4|8||5|

NOM : Mutschler

Prénom : Sacha

Date de passage[1] : ……. / ……. /2022	**Heure de passage[1] :** ……**h**……

CATEGORIE CANDIDAT [2] (UNE CASE A COCHER)	
❑ Scolaire ☑ Apprenti ❑ Formation professionnelle continue ❑ Expérience professionnelle 3 ans	❑ Ex-scolaire ❑ Ex-apprenti ❑ Ex-formation professionnelle continue

[1]Informations communiquées sur votre convocation envoyée en mars-avril 2022

[2] Informations communiquées sur votre confirmation d'inscription

Tampon de
L'établissement

BTS SIO – Dossier Etudiant

Justificatif d'acquisition des compétences

Epreuve E4

Support et mise à disposition de

Services informatiques

SOMMAIRE

1 Introduction

L'objectif de ce document est de vous présenter les missions professionnelles que j'ai effectué dans le cadre de ma formation BTS SIO à l'école IRIS de Strasbourg.

Ces missions peuvent être de trois types :

- Effectuées en entreprise durant une alternance
- Effectuées en stage en entreprise
- Effectuées à l'école (compte-rendu de TP, projet collaboratif)

Le type de la mission sera précisé dans chaque cahier des charges.

Ce document se compose des parties suivantes :

Chapitres	Contenu
Chapitres 1 à 5	Présentation des missions, avec pour chacune : - Le cahier des charges - La solution proposée - La gestion de projet - La mise en œuvre - Le bilan du projet

2 Mission 5 : Cyber – Attaque Man In The Middle

2.1 Cahier des charges

Type de mission
Mission effectuée à l'école.
Contexte
Dans le cadre de mon apprentissage de la cybersécurité, notre groupe nommé ALLSafe doit intervenir dans une entreprise afin de les protéger de potentielles attaques ARP via la méthode du « Man in the middle » sur des postes Linux et Windows.
Demande du client
Sécuriser le réseau existant d'une attaque ARP en trouvant des solutions logicielles ou en utilisant le matériel existant.
Expression du besoin
Empêcher les attaques par la méthode Man in the middle afin protéger les données sensibles au sein de l'entreprise en utilisant ce qui est nécessaire.
Budget disponible
100€ par poste.
Outils disponibles
Switch et Routeur type cisco. Machines virtuelles Kali et ISO Windows + Linux.
Contraintes
Temps : 1 semaine. Répondre au budget du client. Disposer d'un poste permettant de faire tourner plusieurs machines virtuelles.
Confidentialité
Pas de collecte de données personnelles ou critiques.

2.2 Etude et conception de la solution

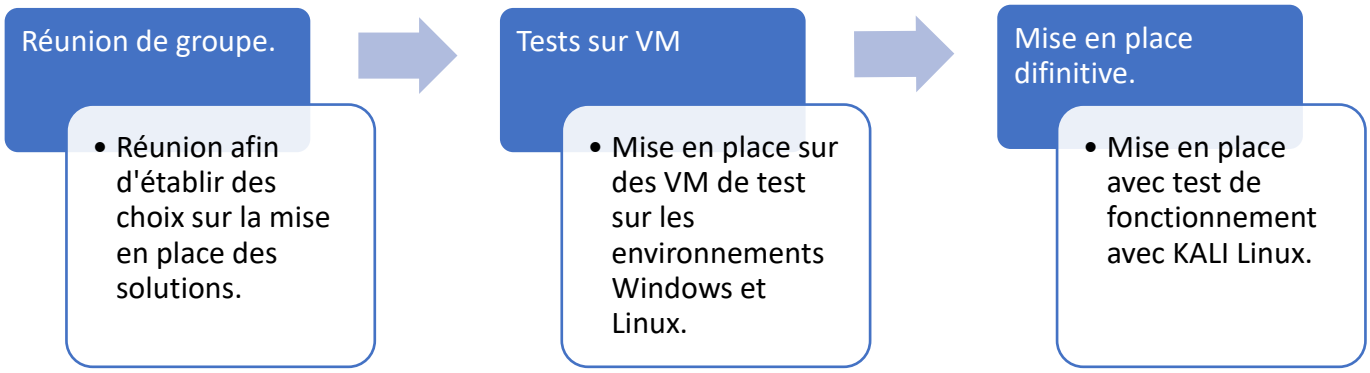
2.2.1 La solution retenue

- Windows : Express VPN, xARP
- Linux : ExpressVPN, shARP
- Communateurs : switchport port-security maximum 1 avec un mac address sticky

2.3 Gestion de projet

2.3.1 Planing de déploiement de la solution

Schéma de la réalisation de la mission :



2.3.2 Budget

Matériel : 3 poste informatique, un Switch, 2 serveurs.

Licences : Windows, Windows Server, Debian (Gratuit), Kali Linux.

Coût humain : 1 semaine de travail pour 3 personnes.

2.4 Mise en œuvre

2.4.1 Implémentation de la solution

Préambule

Tout d'abord, il nous faut mettre en œuvre une solution de contre-mesure contre le MITM.
Ce risque est présent uniquement lorsque l'attaquant se trouve dans le même réseau (cafés ou réseau interne de l'entreprise).
L'essentiel, pour l'utilisateur, est de faire en sorte de naviguer en toute sécurité. En chiffrant le trafic entre le réseau et votre appareil à l'aide d'un logiciel de chiffrement de navigation, vous pouvez repousser les éventuelles attaques dites de l'homme du milieu. Vérifiez toujours que les sites que vous visitez sont sécurisés, en https. Avant toute configuration ou installation de logiciel, il est essentiel d'adopter les bonnes pratiques en termes de sécurité.

Nous pouvons fournir un manuel des bonnes pratiques de l'utilisateur sur simple demande

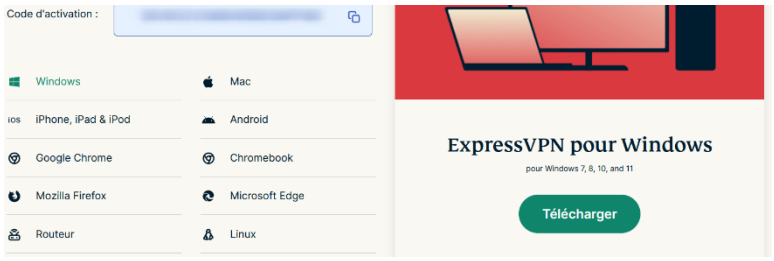
1) Amélioration de la sécurité réseau des laptops

1) Installation et configuration de Express VPN,

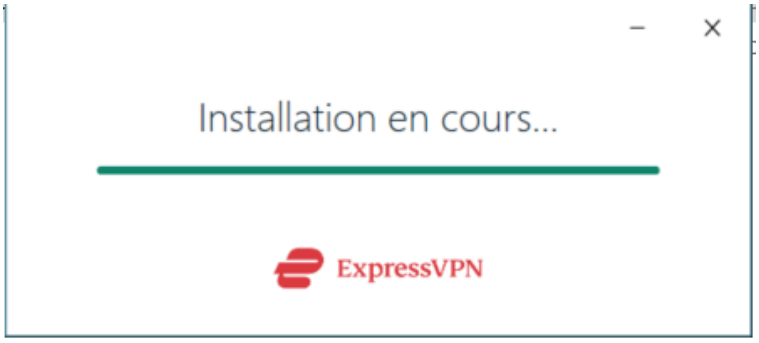
Rappel : disponible autant sur Linux que Windows, permet un chiffrement intégral des données échangées de bout en bout lors de la navigation internet et l'échange de paquets de données. Il permet une navigation et des téléchargements privés et sécurisés. Votre nouvelle IP anonyme et intraçable peut être obtenue depuis 160 localisations (dans 94 pays). Nous avons choisi ce prestataire plutôt qu'un autre en raison de son rapport qualité-prix. Ce dernier propose l''avantage d'être gratuit pendant la période d'essai puis disponible par abonnement pour seulement 5,90€/mois.

Installation sur Windows :

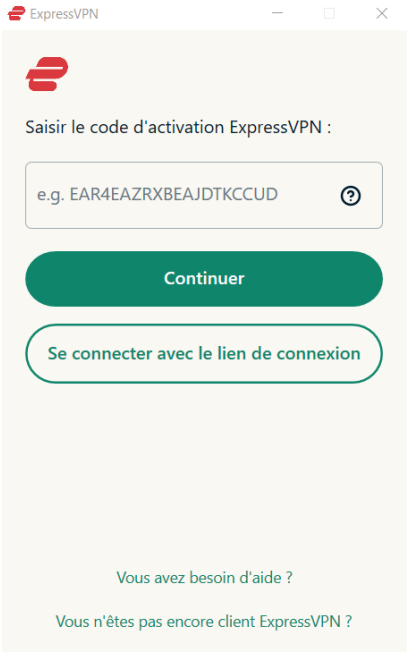
Se rendre sur le site d'expressVPN et cliquer sur abonnement, puis télécharger l'appli windows: (bien noter le code d'activation, ici flouté)



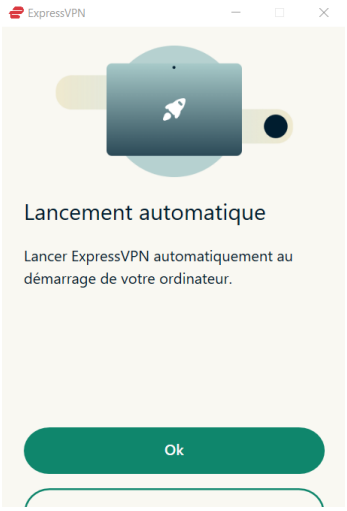
Cliquer sur l'exécutable dans /Downloads



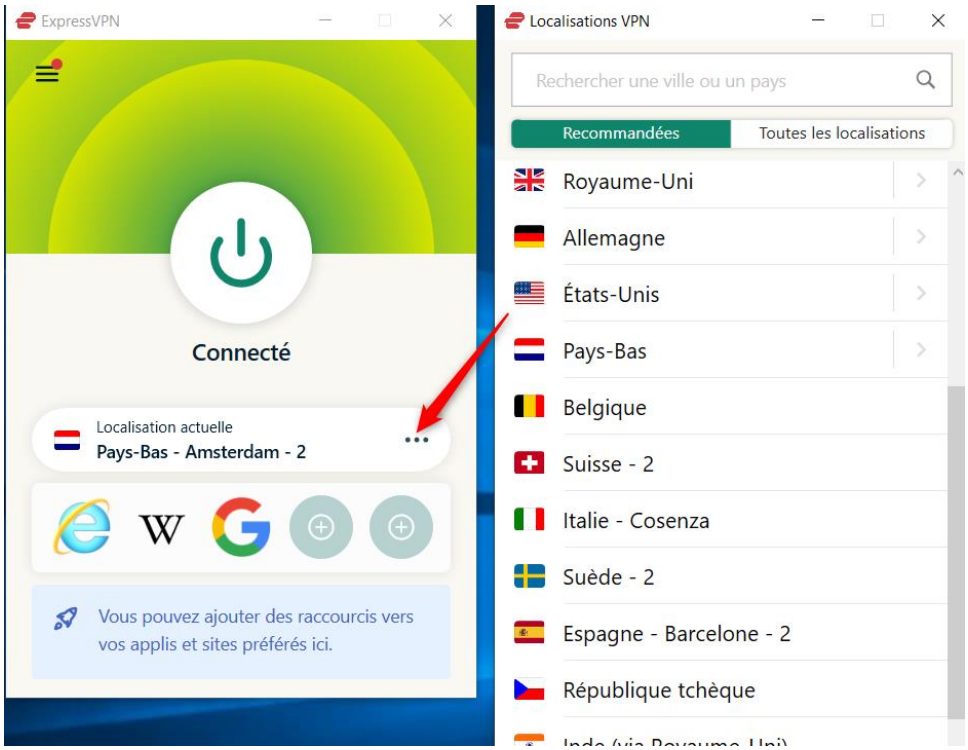
Activer à l'aide du code et continuer



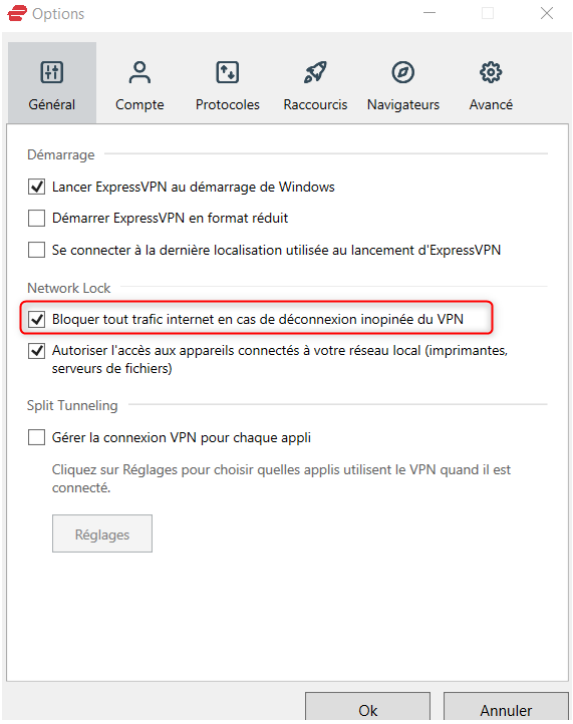
L'option lancement automatique au démarrage peut être sélectionnée en cliquant sur OK



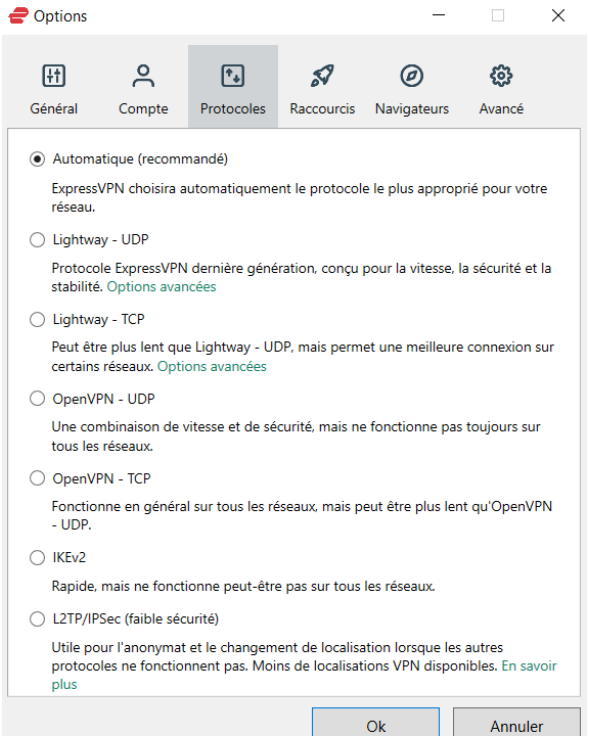
Possibilité de changer de localisation en cliquant sur les 3 points, je navigue actuellement sur le net depuis Amsterdam



Options de sécurité supplémentaires à cocher



Choisir le protocole approprié selon la situation sinon, laisser sur automatique :

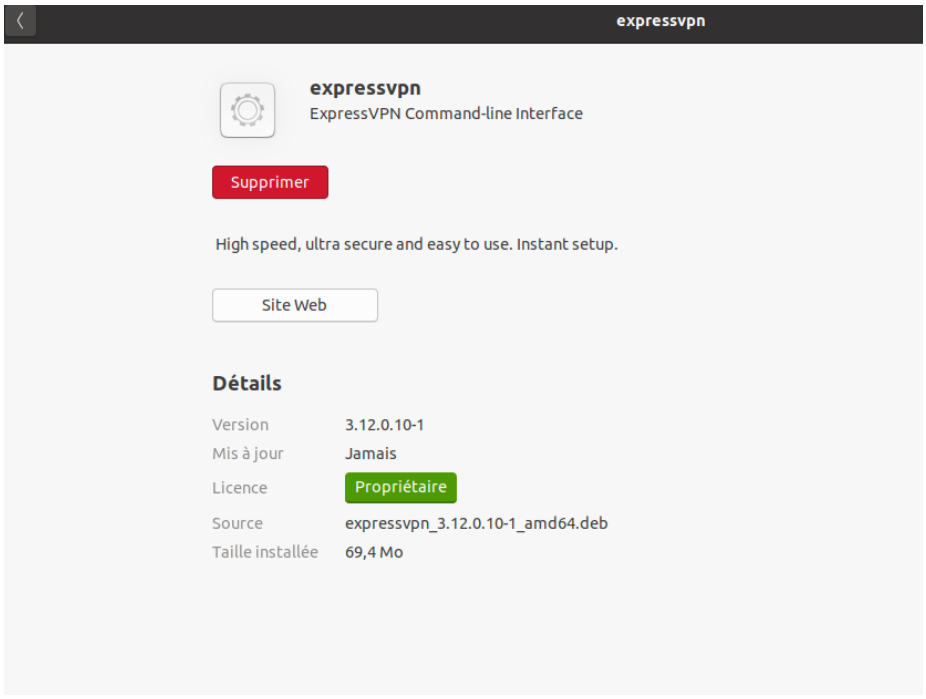


En bas à droite de mon écran je peux voir que ExpressVPN est actif et le déconnecter s'il le faut.

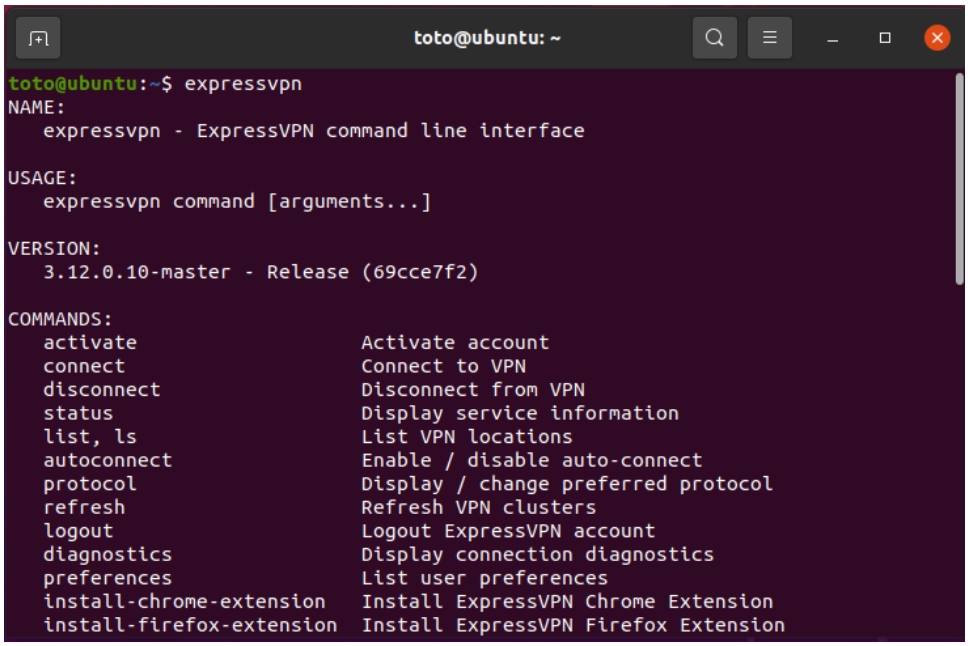
Install sur Linux :

Téléchargement du paquet via navigateur sur expressvpn.com :

Installer le paquet téléchargé dans /Downloads



Validation, exécution et paramétrage via ligne de commande possible :
La commande simple ***expressvpn*** permet d'afficher facilement toutes les commandes disponibles



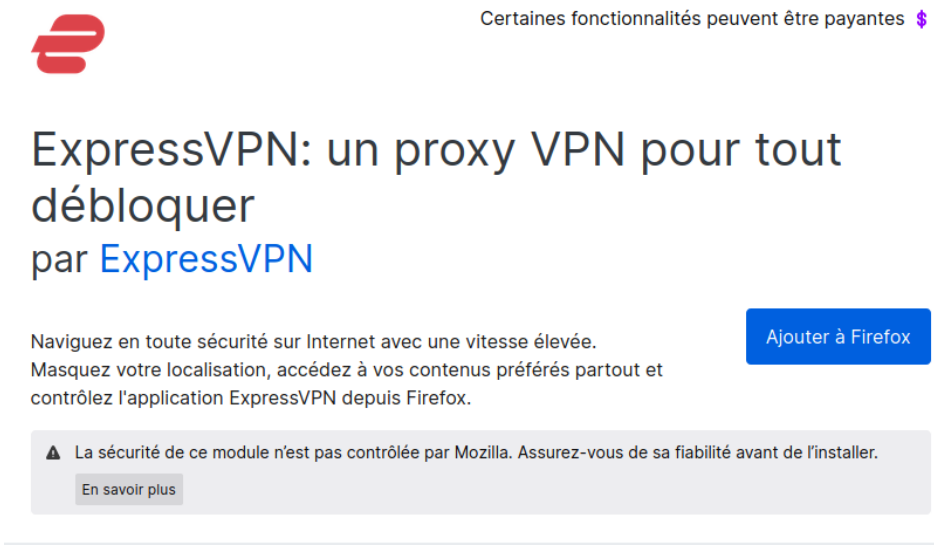
Commençons par la ligne de commande expressvpn activate:
Entrer le code reçu, et appuyer sur entrée

```
toto@ubuntu:~$ expressvpn activate
Enter activation code:
Activating...
Activated.
Help improve ExpressVPN: Share crash reports, speed tests, usability diagnostics
, and whether VPN connection attempts succeed. These reports never contain perso
nally identifiable information. (Y/n)
```

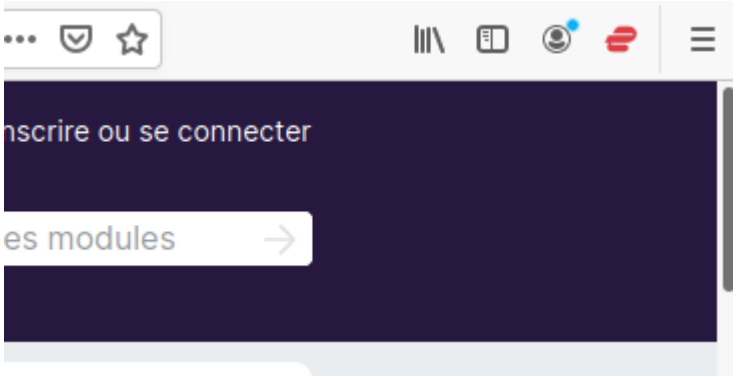
Possibilité d'installer un plugin Firefox ou Chrome, ce qui peut être pratique pour certains :

Entrer ***expressvpn install-firefox-extension***

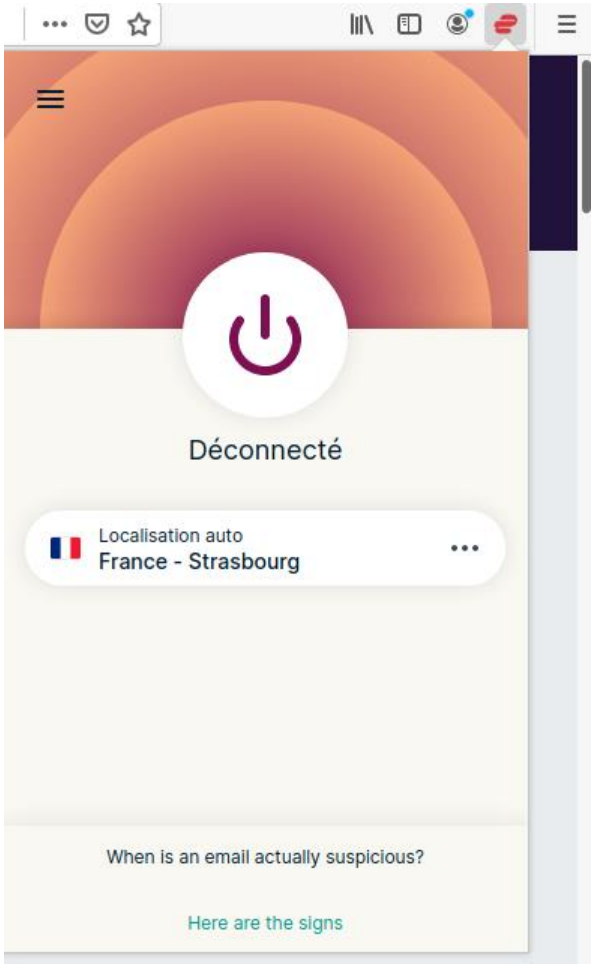
Ce qui redirige vers cette page : cliquer sur "ajouter à firefox"



L'icône d'Express VPN apparaît bien dans le coin supérieur droit de mon navigateur.



En cliquant dessus je retrouve bien l'interface similaire à celle de Windows :



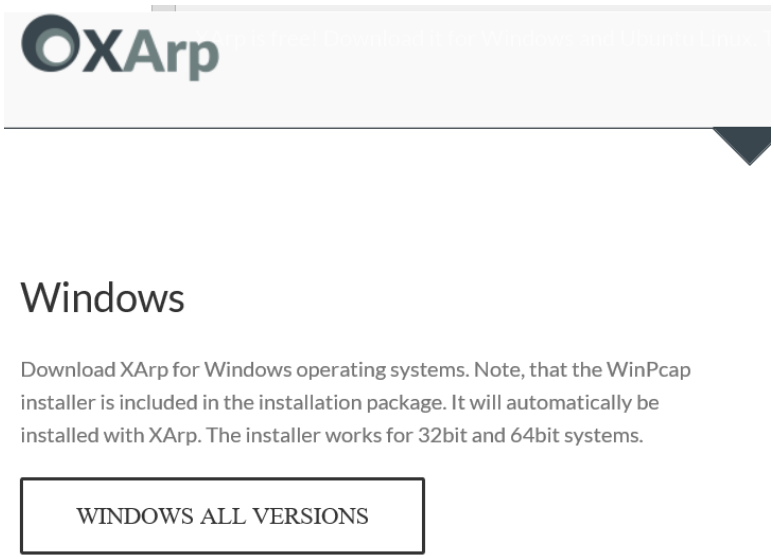
- Pour la sécurisation des postes sous Windows 10, nous installerons **XArp:**

2) XArp (Windows) :

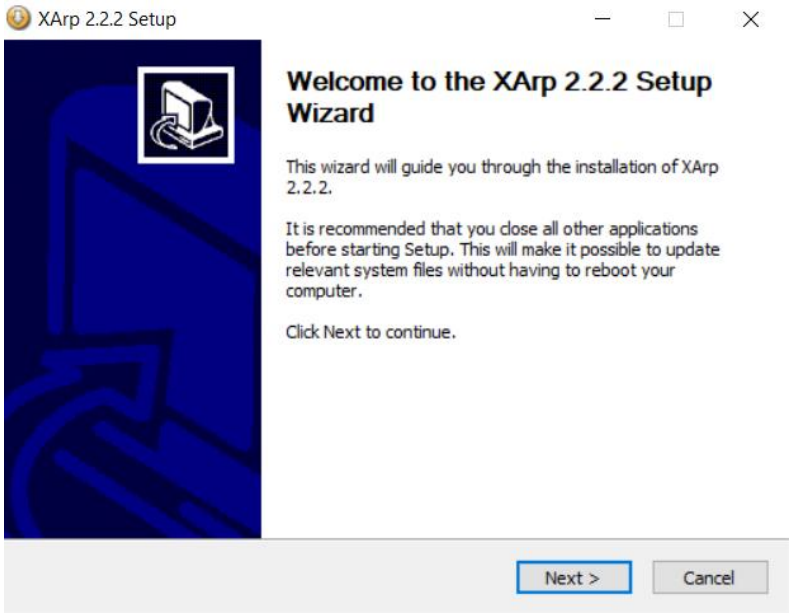
Rappel : La solution comprend des modules passifs, qui vont analyser des paquets ARP et vérifier la correspondance des adresses assignées avec les anciennes entrées. S'il y a une incohérence, l'administrateur en est immédiatement alerté. L'alerte est reçue par mail ce qui permet d'être prévenu via téléphone mobile également. Cela est pratique lorsque l'utilisateur n'est pas devant son poste, mais en pause par exemple.
Les anomalies sont identifiées sur la base d'analyses de statistiques.
Il est possible d'ajuster graduellement la sensibilité du filtre de trafic en fonction des besoins du LAN. Les modules actifs quant à eux envoient leurs propres paquets dans le réseau, de façon à valider les tables ARP des appareils accessibles, et à les compléter avec des données valides. Procéder ainsi permet de ralentir l'action du MiTM de façon significative. Notre choix s'est tourné vers cette application car celle-ci est peu onéreuse car disponible en version avancée pour seulement 27,50€/poste, et même disponible en version gratuite avec des fonctionnalités complètes tout de même.

Install et configuration de xArp:

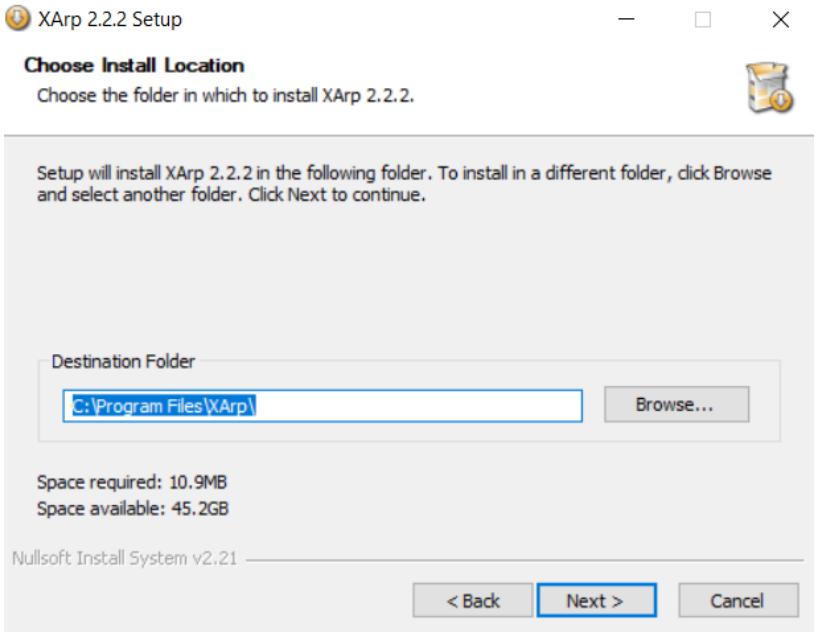
Rendez-vous sur la page de xArp et télécharger la version WINDOWS ALL VERSIONS :



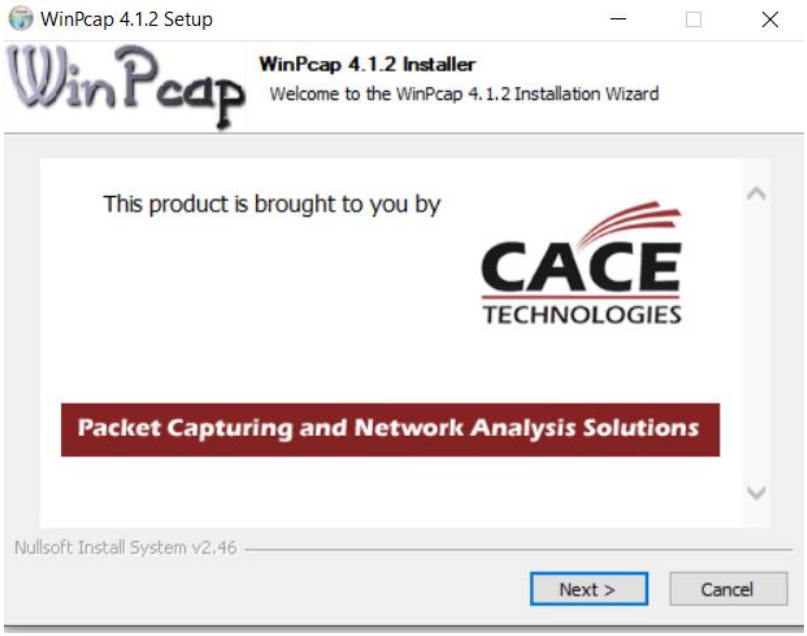
Lancer l'exécutable, cliquer sur next.



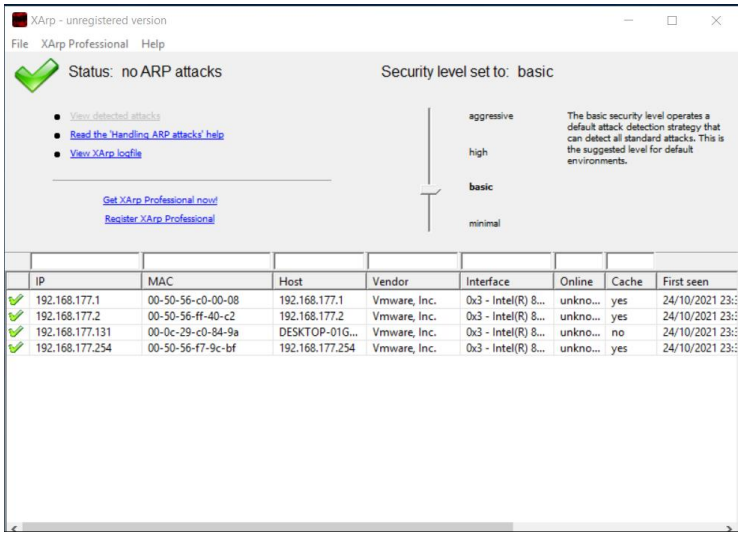
Choisir le chemin d'installation (peut rester Program Files par défaut)



Installer WinPcap , (la fenêtre s'ouvre automatiquement) il est nécessaire à xArp:

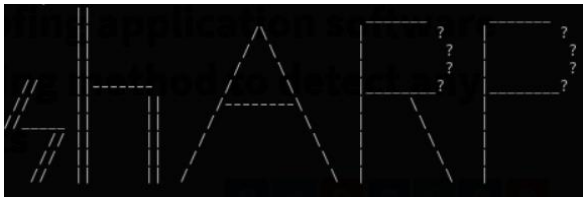


Lancer Xarp:
Il donne immédiatement des indications s'il y a une attaque ARP, en fonction du niveau de sécurité (Ici sur basic)



L'icône de xArp est bien dans mes applications actives :

Pour la sécurisation des postes sous GNU/Linux, nous utiliserons le scripte **shARP:**



3) shARP

Rappel : Sur Linux, shARP est un scripte codé en python, gratuit et open source. Il contient des modules passifs qui désactivent automatiquement la carte réseau de la machine dès la détection d'une attaque ARP spoofing, ce qui est pratique et permet de manière radicale de ne faire fuiter aucune info sensible vers l'attaquant. Le scripte contient également des modules actifs : avec ce mode d'opération, en plus de la désactivation de la carte réseau, l'outil shARP fait appel à Airmon-ng et Aircrack-ng, puis tente d'exclure l'attaquant du réseau grâce à des paquets de désauthentification.

Après les détections, shARP sauvegarde les informations de l'attaquant dans un fichier /usr/ shARP /log.txt créé par l'outil lui-même.

Installation/Configuration de shARP:

Commencer par installer le paquet **net-tools** (afin de pouvoir voir les adresses mac (protocole ARP)

```
toto@ubuntu:~/sharp$ sudo apt install net-tools
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
  libfprint-2-tod1
Veuillez utiliser « sudo apt autoremove » pour le supprimer.
Les NOUVEAUX paquets suivants seront installés :
  net-tools
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 196 ko dans les archives.
Après cette opération, 864 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://fr.archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64 1.60+git20180626.aeb
d88e-1ubuntu1 [196 kB]
196 ko réceptionnés en 1s (242 ko/s)
Sélection du paquet net-tools précédemment désélectionné.
(Lecture de la base de données... 207962 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb ...
Dépaquetage de net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Paramétrage de net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.1-1) ...
```

Installer git afin de pouvoir télécharger shARP sur le repository github: ***sudo apt get install git***

```
toto@ubuntu:~$ sudo apt install git
[sudo] Mot de passe de toto :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
  libfprint-2-tod1
Veuillez utiliser « sudo apt autoremove » pour le supprimer.
Les paquets supplémentaires suivants seront installés :
  git-man liberror-perl
Paquets suggérés :
  git-daemon-run | git-daemon-sysvinit git-doc git-el git-email git-gui gitk
  gitweb git-cvs git-mediawiki git-svn
Les NOUVEAUX paquets suivants seront installés :
  git git-man liberror-perl
0 mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 5 464 ko dans les archives.
Après cette opération, 38,4 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
```

Entre la commande : ***git clone*** *http://github.com/europa502/sharp.git*

```
toto@ubuntu:~$ git clone https://github.com/europa502/sharp.git
Clonage dans 'sharp'...
remote: Enumerating objects: 135, done.
remote: Counting objects: 100% (9/9), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 135 (delta 2), reused 8 (delta 2), pack-reused 126
Réception d'objets: 100% (135/135), 938.21 Kio | 853.00 Kio/s, fait.
Résolution des deltas: 100% (53/53), fait.
```

Le scripte est installé, positionnons-nous dans le dossier sharp:

```
toto@ubuntu:~$ cd sharp
toto@ubuntu:~/sharp$
```

On y voit le scripte en faisant un ***ls*** :

```
toto@ubuntu:~/sharp$ ls
LICENSE  mac_decoder.py  mac-vendors.txt  passive.sh  README.md  shARP.sh
```

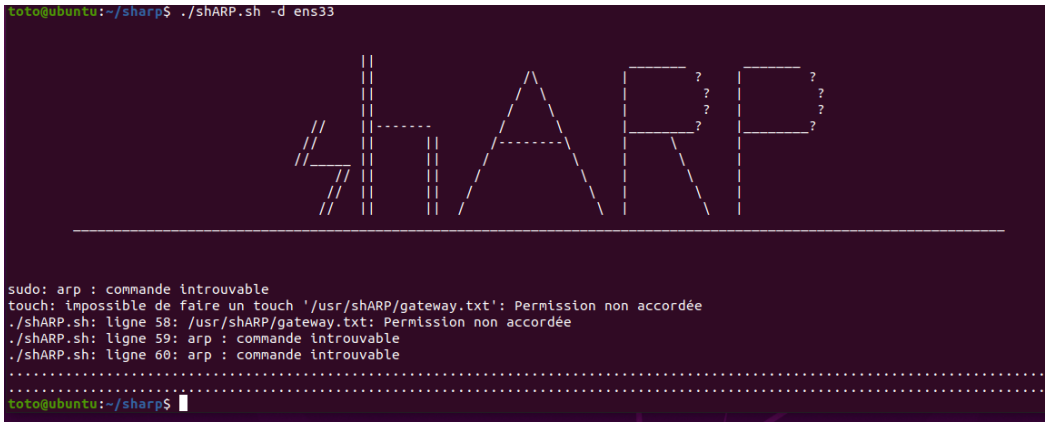
Ajoutez-lui la permission “exécuter” avec la commande ***chmod +x shARP.sh***

```
toto@ubuntu:~/sharp$ chmod +x shARP.sh
toto@ubuntu:~/sharp$
```

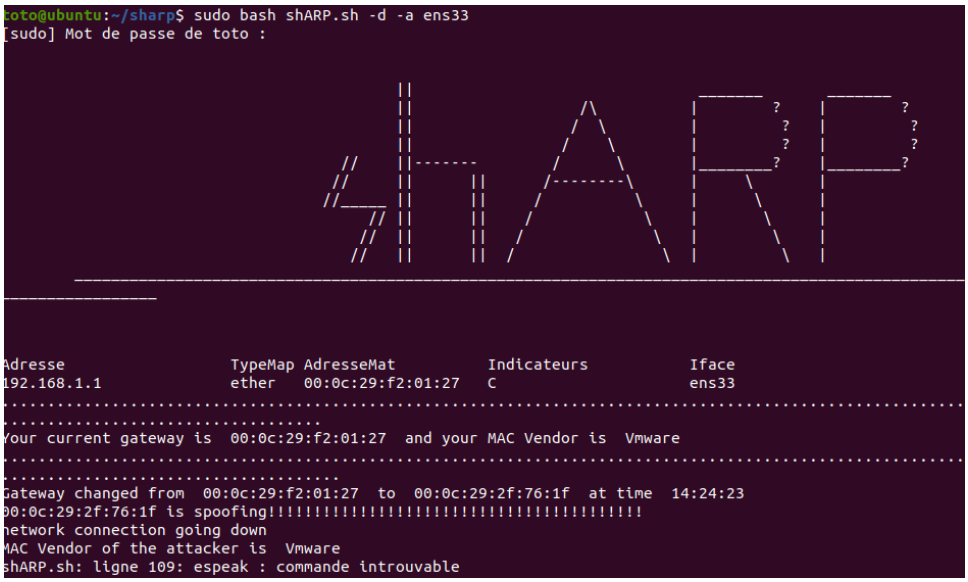
La carte réseau qui m’intéresse est 192.168.177.136, soit ens33

```
toto@ubuntu:~/sharp$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:fb:dc:a7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.177.136/24 brd 192.168.177.255 scope global dynamic ens33
       valid_lft 1231sec preferred_lft 1231sec
    inet6 fe80::20c:29ff:fefb:dca7/64 scope link
       valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
 group default qlen 1000
    link/ether 52:54:00:04:7d:4f brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
4: virbr0-nic: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel maste
r virbr0 state DOWN group default qlen 1000
    link/ether 52:54:00:04:7d:4f brd ff:ff:ff:ff:ff:ff
```

Pour lancer une analyse sur cette carte réseau, lancer la commande : ***./shARP -d ens33***



Pour passer en mode offensif :
Entrer la commande ***sudo bash shARP.sh -d –a ens33***



Pour réactiver la carte réseau après une désactivation de sécurité : ***./shARP -r***

2) Amélioration de la sécurité au niveau des commutateurs CISCO

Il nous faut trouver une solution pour éviter L'ARP SPOOFING. Nous n'opterons pas pour un enregistrement statique car il serait trop lourd de gérer manuellement 100 postes.

Sur le switch nous utiliserons une commande : ***port-security***

A) port-security

(Il faut aller dans les interfaces pour activer **port-security)**

switchport port-security
Qui permet d'activer port-security sur le port

switchport port-security mac-address sticky
Enregistre automatiquement l'adresse mac pour ce port

switchport port-security maximum 1
On définit qu'il ne peut avoir qu'une adresse MAC sur le port pour éviter qu'une personne puisse changer d'adresse MAC

switchport port-security violation shutdown
Pour finir s'il y a violation des règles imposées, le port doit alors s'éteindre

switchport port-security aging time 180
switchport port-security aging type inactivity
On définit s'il y 180 minutes d'inactivité on supprime l'adresse MAC qui est associer au port.

Pour réactiver un ou des port(s)
Il faut désactiver l'interface
En
Conf t
Interface <non du port>
Shutdown
end

Puis faire **clear port-security sticky interface <non du port>** ou **no switchport port-security mac-address sticky <mac addresse>** pour supprimer les adresse mac associer au port.

Enfin
En
Conf t
Interface <non du port>
No Shutdown
Exit

3) Amélioration de la sécurité des serveurs Windows et GNU/LINUX

Il nous faut penser à l'amélioration de la sécurité des serveurs Windows et GNU/LINUX (Proposition d'une solution pour éviter L'ARP POISONING)

Linux :

A)cron-apt

Pour maintenir les applications à jour. Et pour finir on mettra en place Cron-apt qui permettra de mettre à jour sa version Debian en cas de besoin.

Il s'installe via Git via un "Git clone"

On tapera "cron-apt" pour lancer les mises à jour.

D)Fail2Ban,

Qui est un système de surveillance des logs et bannissement par IP.

Installer fail2ban, qui est normalement présent dans les paquets officiels Debian

```
apt-get install fail2ban
```

Dont voici un extrait de la doc Fail2Ban :

Section DEFAULT

La partie *DEFAULT* qui permet de personnaliser le comportement général du service tel que les adresse IP ignorées, le temps d'un ban, le nombre maximum d'essais autorisés. Cette section est le plus souvent correctement configurée pour votre usage, vous pouvez cependant la modifier afin d'ajuster son comportement à la configuration de votre système.
Parmi les paramètres de la section *DEFAULT* voici les plus importants :

- **Ignoreip**: Ce paramètre sert à exclure une ou plusieurs adresses IP de fail2ban, ce paramètre est utile afin d'éviter de vous bannir vous-même ou un de vos utilisateurs si il vous arrivait d'oublier votre mot de passe un trop grand nombre de fois.
- **Bantime**: Ce paramètre sert à définir le temps en secondes d'un bannissement. Par défaut le bannissement dure 10 minutes.
- **Maxretry**: Ce paramètre sert à définir un nombre maximal d'essais ratés avant d'entreprendre un bannissement de l'utilisateur.

Section ACTION

La partie *ACTION* définie la réaction de **fail2ban** lorsque le nombre d'essai maximum a été atteint. Nous pouvons par exemple définir le destinataire du mail d'alerte, le service mail utilisé, le protocole par défaut de la surveillance, ainsi que l'action entreprise par **fail2ban** qui peut aller du simple ban au relevé d'informations complet sur l'origine de l'attaque et du *reporting* vers un service de blacklist choisi (Cloudfare, Badips.com, Blocklist.de, ...)
La section *ACTION* permet de définir le comportement de **fail2ban** lors d'un bannissement.

- **Banaction**: Ce paramètre sert à définir le fichier appelé lors d'un bannissement. Par défaut c'est l'appel à IPTables qui est effectué afin de bannir l'adresse IP sur tous les ports
- **Action**: Ce paramètre sert à définir l'action exécutée lors d'un bannissement. Plusieurs raccourcis sont disponibles comme par exemple l'établissement d'une règle IPTables ou l'envoi d'un mail d'alerte.

Section JAILS

La section *JAILS* permet de définir un comportement personnalisé pour les différents services surveillés tels que ssh, apache, etc...
La syntaxe générale d'une section *JAIL* est la suivante:

```
# nom de l'application ou du service
[sshd]
# le port sur lequel la surveillance doit être effectuée, ce peut être un chiffre (22) ou un mot-clé de protocole (ssh)
port = ssh
# le chemin du fichier de log sur lequel fail2ban doit aller vérifier
logpath = %(sshd_log)s

# Nous pouvons également "override" les paramètres par défauts, par exemple le nombre d'essais max
maxretry = 3 ; Abaisser le nombre d'erreurs à 3 pour le ssh
# Egalement le temps d'un bannissement
bantime = 1200 ; Doubler le temps de bannissement pour le ssh
```

Serveurs windows :

xArp

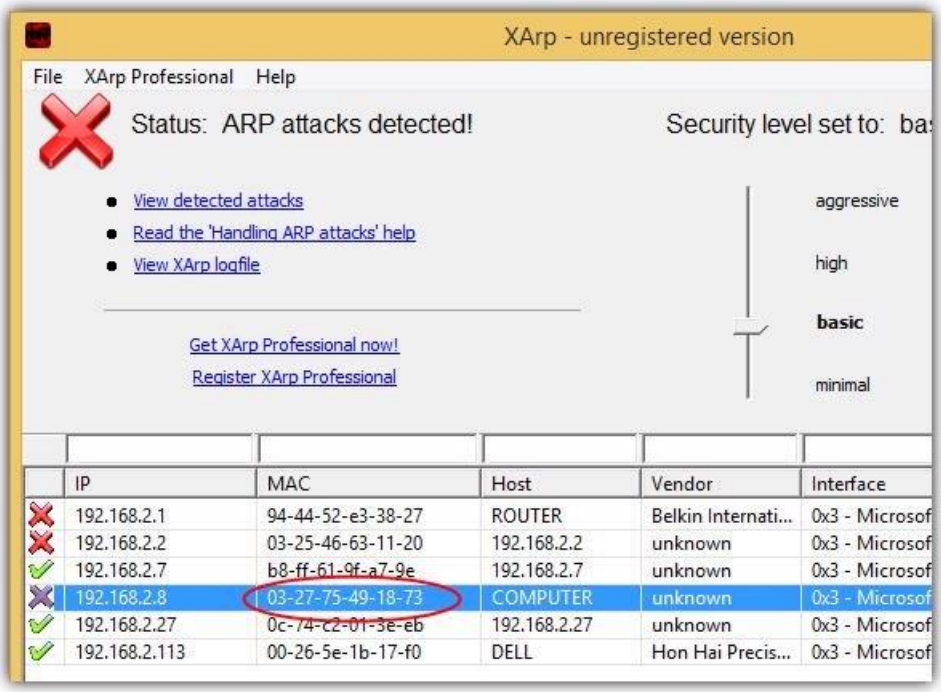
Le logiciel xArp existe sous deux versions : la version gratuite et la version prémium. Dans notre cas de figure la version gratuite est amplement suffisante.

XArp est un logiciel de détection d'Arp Spoofing, sa mise en place permettra d'éviter toutes les attaques communes à l'Arp Spoofing, comme l'attaque Man in the middle.

Le but ici est de protéger les données stockées sur le serveur afin d'empêcher toute personne mal intentionnée de les dérober ou de les corrompre.

Une fois le programme installé, nous pourrons savoir si une attaque de type ARP est en cours sur notre machine. De ce fait, nous pourrons agir en conséquence.

Lorsqu'on lance le programme xArp sur le serveur Windows (victime) et que l'on lance des requêtes depuis une autre machine sur le réseau local (attaquant), le logiciel xArp réagit automatiquement :



De ce fait, nous pouvons immédiatement réagir afin de contenir l'attaque.

Pour aller plus loin contre les attaques ARP :

Comprendre les attaques via ARP spoofing :
https://www.it-connect.fr/comprendre-les-attaques-via-arp-spoofing-mitm-dos/

A propos de l'usurpation d'identité ARP:
https://www.informatique-mania.com/linformatique/usurpation-didentite-arp/

DAI: En complément, le Dynamic ARP Inspection (DAI) permet d'éviter les attaques de type "arp spoofing", permettant notamment le Man-In-The-Middle. Le DAI utilise le DHCP Snooping pour vérifier qu'une adresse MAC à bien obtenu son IP via le serveur DHCP trusté :
https://formip.com/dai/

Sécurité au niveau des Switch :

https://cisco.goffinet.org/ccna/securite-lan/lab-securite-dans-le-lan/

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_52_se/configuration/guide/3750scg/swdynarp.html

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html

DHCP Snooping: Permet d'éviter les mauvaises surprises (par exemple, une VM windows avec le DHCP serveur activé), ainsi que les attaques de types "DHCP spoofing". Dans cette configuration, le port du serveur DHCP est explicitement "trusté", et les ports access automatiquement "untrust"**IP:**
https://community.fs.com/fr/blog/what-is-dhcp-snooping-and-how-it-works.html

Source Guard : Enfin, au niveau IP, la fonction IP Source Guard permet de valider le lien entre le port source, l'adresse IP et l'adresse MAC pour chaque requête, et évite ainsi toute usurpation au niveau 3. C'est là encore la base construite par le DHCP Snooping qui sers de référentiel.

Référentiel des commandes :

ip dhcp snooping => permettent d'activer le **« Dhcp Snooping »** en globalité

ip dhcp snooping vlan {range-ID} => surveillance vlan

No ipdhcp snooping information option => désactiver l'insertion de l'option 82 dans les paquets DHCP

ip dhcp snooping trust => dire que l'interface est de valide pour le dhcp

ip arp inspection vlan {range-ID} => vérifier l'ensemble des paquets ARP sur les interfaces non approuvées.

ip arp inspection trust => approuvée par l'inspection dynamique ARP

show ip dhcp snooping binding => voir les message dhcp

show ip arp inspection => permet de voir le nombre de paquets ARP abandonnés

Solutions logicielles:

Etherwall:
https://korben.info/etherwall.html

shARP : linux, surveillance, protection
https://homputersecurity.com/2017/04/24/cet-outil-protege-votre-machine-contre-les-attaques-arp-spoofing/
https://github.com/europa502/shARP

Arpwatch : linux, surveillance
https://www.tecmint.com/monitor-ethernet-activity-in-linux/
https://fr.linux-console.net/?p=1750

XArp : linux et w10, détection des attaques
http://www.xarp.net/

Suricata : est un logiciel open source de détection d'intrusion, de prévention d'intrusion, et de supervision de sécurité réseau.
https://suricata.io/

Snort est un système de détection d'intrusion libre publié sous licence GNU GPL
https://www.snort.org/

OSSEC est un système de détection d'intrusion gratuit et open source basée sur l'hôte.
https://www.ossec.net/

Sagan est un moteur d'analyse et de corrélation de journaux en temps réel multi-thread
https://quadrantsec.com/sagan_log_analysis_engine/

Samhain est un vérificateur d'intégrité et un système de détection d'intrusion d'hôte qui peut être utilisé sur des hôtes uniques ainsi que sur de grands réseaux UNIX

https://www.la-samhna.de/samhain/

Autre VPN gratuit:
https://openvpn.net/community-downloads/

2.5 Bilan

2.5.1 Validation des exigences point par point

- ❑ Délai respecté.
- ❑ Réseau et Postes sécurisés contre les attaques ARP.

2.5.2 Compétences acquises

- Gestion d'une demande client en groupe.
- Recherche de solution de sécurisation
- Utilisation de Kali Linux
- Configuration de ExpressVPN
- Connaissance sur les attaques ARP et Man in the Middle.