**Job 0**

Mettez en place une Machine Virtuelle et installez les services suivants :

● Un serveur SSH

● LAMPP (Apache, MariaDB, php, phpmyadmin)

● Un serveur FTP

Votre machine hôte doit pouvoir accéder à ces services.

Pour l’instant, n’installez pas de certificats SSL/TLS.

**INSTALLER SUDO ET METTRE LE USER EN SUDO :**

su -

apt-get update && apt-get install sudo

su -

useradd anne sudo

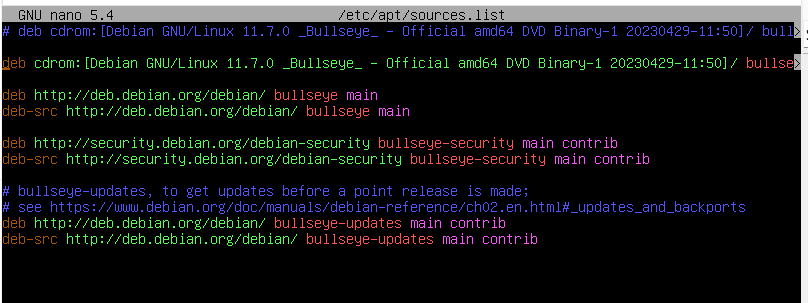
sortir de tout pour qu’il le prenne en compte

**Désactiver la lecture depuis cd-r après installation de la VM :**

supprimer la ligne deb cdrom avec # :

nano /etc/apt/sources.list

(en su -)



apt-get install -y apache2

systemctl enable apache2

apt-get install -y php

apt-get install -y mariadb-server phpMyAdmin

apt-get install -y proftpd

faire la config de proftp pour avoir les anonymous

restart le service

**Job 1**

Installez Wireshark sur votre machine hôte. Lancez la capture de paquets sur l’interface

de la VM.

Toujours depuis votre machine hôte, connectez-vous au serveur FTP, téléversez et

téléchargez des fichiers.

Connectez-vous à la VM via SSH. Connectez-vous à phpmyadmin, faites volontairement

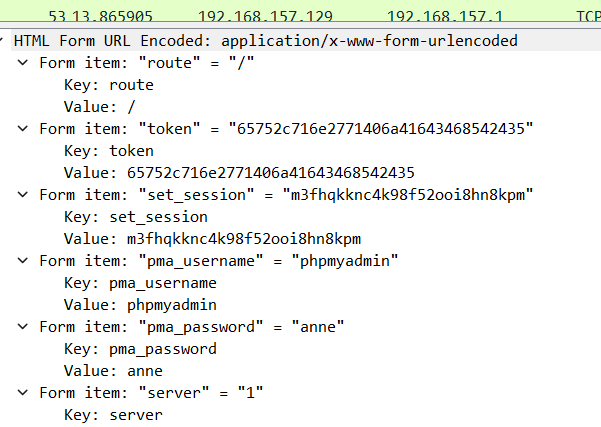
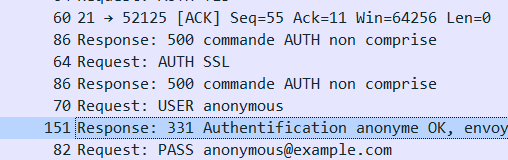
des fautes dans les usernames, password etc pour créer des logs.

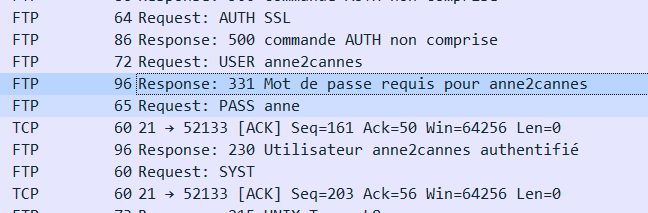
Explorez l’outil, amusez-vous avec les filtres, ses fonctionnalités.

Regardez et analysez les logs puis faites un constat.

Vous pouvez également observer et analyser votre environnement, mais attention : vos

actions doivent rester pédagogiques et éthiques.





**Job 2**

Maintenant que vous avez des traces montrant des services non sécurisés, installez des

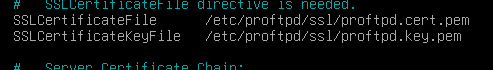
certificats de chiffrement sur vos serveurs WEB et FTP.

Réalisez des connexions aux différents services, toujours pour générer des logs.

À nouveau, regardez et analysez les logs puis faites un constat.

Dans default-ssl.conf mettre les adresses des chemins des clés SSL du Proftpd





Sécuriser apache : soit désactiver le port 80 soit faire le renvoi sur le port 443

Sachant que si on désactive juste le port 80 on n’a pas du tout accès a internet par http. Il vaut mieux renvoyer sur le port 443 !

Créer une clé et un certificat dans proftpd

apt install openssl

mkdir /etc/proftpd/ssl

**openssl req -new -x509 -keyout /etc/proftpd/ssl/proftpd.key.pem -days 365 -nodes -ut /etc/proftpd/ssl/proftpd.cert.pem**

Entrer les infos que l’on veut donner, rien n’est obligatoire

**nano /etc/proftpd/tls.conf**

et changer :

<IfModule mod\_tls.c>

TLSEngine on

TLSLog /var/log/proftpd/tls.log

TLSProtocol SSLv23

TLSRSACertificateFile /etc/proftpd/ssl/proftpd.cert.pem (mettre ce chemin)

TLSRSACertificateKeyFile /etc/proftpd/ssl/proftpd.key.pem (mettre ce chemin)

TLSOptions NoSessionReuseRequired

TLSVerifyClient off

TLSRequired on

**apt install proftpd-mod-crypto**

puis

**nano /etc/proftpd/modules.conf**

et changer :

Décommenter LoadModule mod\_tls.c

Et ajouter Include /etc/proftpd/tls.conf

**A présent pour aller sur le PC il faut passer par HTTPS et rien ne transparait dans le wireshark.**

**Job 3**

Installez la Suite ELK.

Exportez vos données de Wireshark : mettez en place un système permettant

d'exporter les logs sur Elasticsearch à l’aide de (Filebeat | Logstash | Curl) afin de les

analyser et de les monitorer sur Kibana.

Logstash normalise les données, Elasticsearch traite les données et Kibana permet de les visualiser.

*Pour installer la suite ELK il est préférable de suivre un tuto car c’est une usine à gaz*

*Merci Thierry 😊*

[*https://bproo.com/posts/7x3jopbrpepk9o8j/Techmology/comment-installer-elasticsearch,-logstash,-kibana-dans-windows---elk*](https://bproo.com/posts/7x3jopbrpepk9o8j/Techmology/comment-installer-elasticsearch,-logstash,-kibana-dans-windows---elk)

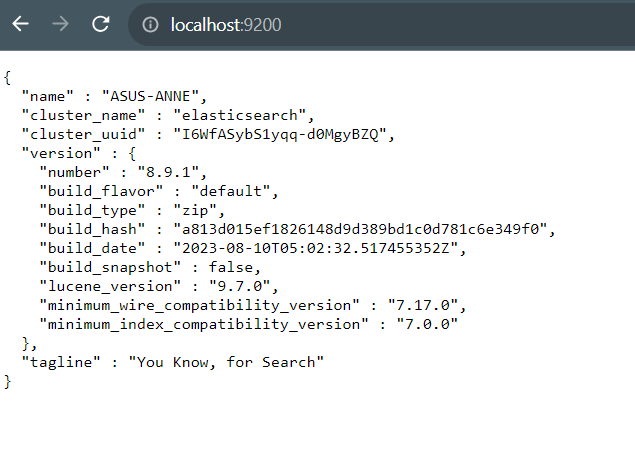
*attention avant d’aller sur* [*http://localhost:9200/*](http://localhost:9200/) *il faut créer un superuser :*

*se mettre dans elasticsearch dans le bin :*

***elasticsearch-users useradd superuser -r <nom du user>***

*ca va demander de créer et confirmer le code du superuser.*

*La connexion fonctionne sur 9200 :*

**

Installation ELK sur Debian – du coup – car ça ne marche pô sur Windows

Télécharger les paquets :

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add –

sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" > /etc/apt/sources.list.d/elastic-8.x.list'

sudo apt update

apt install elasticsearch

*The generated password for the elastic built-in superuser is : AqKlMdEt6wmv=k1TOtSJ*

wget –directory-prefix=/opt/ <https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.9.1-amd64.deb>

aller au bon endroit et faire :

sudo dpkg -i /opt/elasticsearch\*.debcd .

Enfin, faire :

nano /etc/elasticsearch/jvm.options

mettre Xms512m au lieu de 4giga

et Xmx512m

nano /etc/elasticsearch/elasticsearch.yml

enlever le # de : node.name: node-1

mettre le network host en

network.host: 0.0.0.0

discovery.seed\_hosts: ["192.168.157.129", "10.10.1.64"] *IP de la Debian et IP du PC hôte*

cluster.initial\_master\_nodes: ["node-1"]

sortir en enregistrant

systemctl enable elasticsearch

service elasticsearch restart

apt install kibana

nano /etc/kibana/kibana.yml

Modifier :

server host mettre 0.0.0.0 (enlever le #)

Service kibana restart

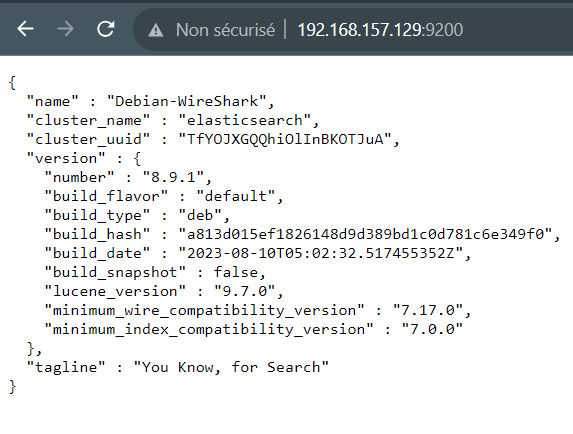
Apt install logstash

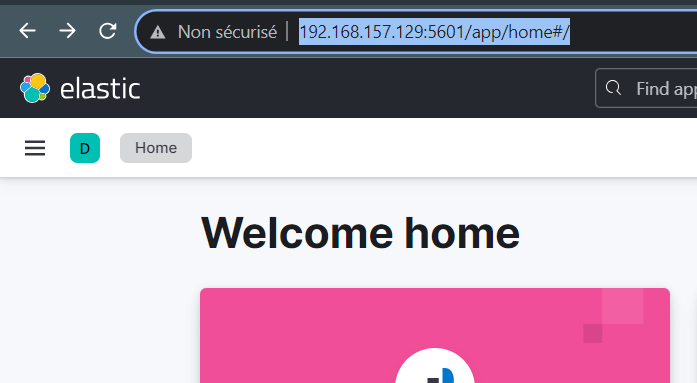
Systemctl enable logstash.service

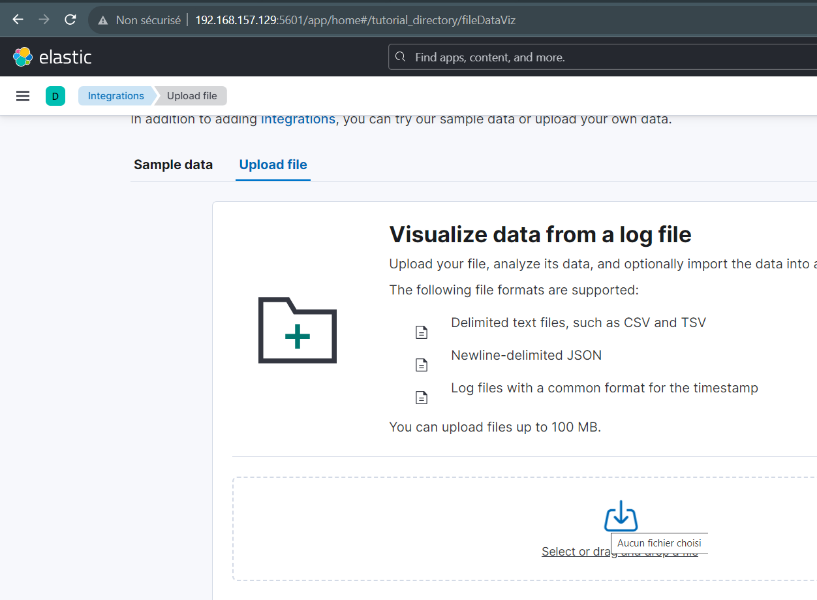
Service logstash restart

Sur l’hôte ouvrir un onglet avec l’IP de la VM :

192.168.157.129 :9200



Ouvrir un onglet avec l’adresse IP de la VM sur le port 5601



Ouvrir Wireshark, faire des logs sur la VM

Aller exporter le fichier du Wireshark et l’importer

dans elasticsearch via l’appli upload

on obtient une analyse :

