Document d’architecture :

Projet UF

* Denys Delaunay
* Yohan Stoeckle
* Bastien Bruyez

Sommaire :

I) Définition du réseau, des hosts, implantation/répartition des services

1. Présentation du projet
2. Réalisation du projet
3. Contexte du projet
4. Schéma Projet
5. Table d’adressage IP

II) Détailler la mise en œuvre des bonnes pratiques

III) Détailler les configurations à réaliser pour mettre en œuvre la solution (système, réseau, services)

1. Définition du réseau, des hosts, implantation/répartition des services
2. Présentation du projet :

Le but du projet est de mettre en place une architecture réseau avec des fonctionnalités avancées et de haute disponibilité.

Pour ce faire plusieurs éléments on était ajouté à notre réseaux :

Elément de fonctionnement :

* Deux serveurs de stockage Nas avec redondance.
* Une redondance du routeur principal.

Elément de sécurité :

* Mise en place d’un firewall.
* Un honeypot
* Une redondance du router principal.
* Une récupération de fichier.

1. Réalisation du projet :

Pour sa réalisation le projet sera avant tout fait au moyen de maquette créer sur l’outil packet tracer

Pour ce faire, nous avons voulu donner vie à notre projet en le raccordant à une entreprise fictive. Pour ce faire nous avons imaginé cette entreprise serait spécialisé dans la vente de bière et aurait donc des fichiers qu’elle souhaite garder en sûreté

Elle serait composée de 4 personnes :

* Le directeur
* Le chef de projet
* 1 employé
* 1 admin-réseau

Nous avons donc créé une GPO en relation avec cette entreprise qui nous paraissaient sensé

* Le directeur :  accès à tous les fichiers/administrateur
* Le chef de projet : accès à son secteur et à ses fichiers
* L’employé : accès aux fichiers minimum
* L’admin-réseau : administrateur/ accès à tout le réseau.

Gpo :

1 directeur / 1 laptop

1 chef de projet /1 laptop

1 employé. /1 laptop

1 admin-réseau /informatique : 1 desktop

* 1. serveurs avec des disques.

1. Contexte du projet :

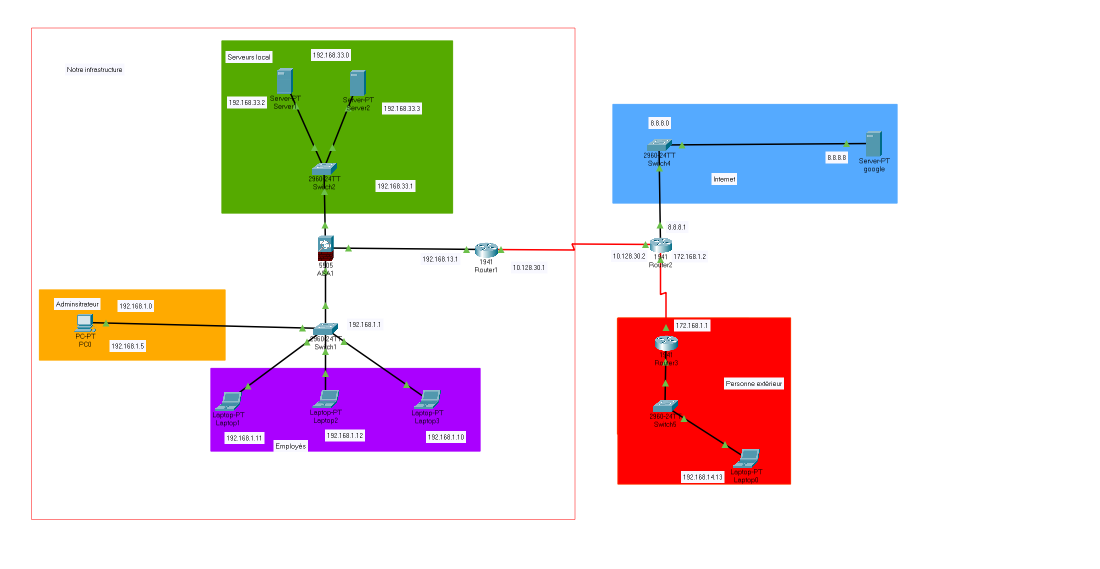
Donc ici nous sommes une entreprise de vente de bière.

Une nouvelle marque de bière là Bibli.

Nous avons besoin d’une infrastructure permettant de gérer des données sensibles sur la fabrication et la vente de bière.

Sur cela nous devons mettre en place une infrastructure qui va permettre aux employés d’accéder à des fichiers sécurisés et d’avoir accès aux fichiers de l’extérieur.

4)Schéma Projet :



5)Table d’adressage IP :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Devices** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** | **Switch Port** |
| R1 | Gig 0/0 | 192.168.1.2 | 255.255.255.0 | N/A | Switch1 / Gig 0/1 |
| S0/0/0 | 10.128.30.1 | 255.0.0.0 | N/A | N/A |
| R2 | S0/0/0 | 10.128.30.2 | 255.0.0.0 | N/A | N/A |
| G0/0 | 8.8.8.1 | 255.0.0.0 | N/A | N/A |
| S/0/0/1 | 172.16.3.1 | 255.255.0.0 | N/A | N/A |
| R3 | S0/0/1 | 172.16.3.2 | 255.255.0.0 | N/A | N/A |
| Gig 0/0 | 192.168.2.1 | 255.255.255.0 | N/A | N/A |
| R4 | Gig 0/1 | 192.168.13.3 | 255.255.255.0 | N/A | N/A |
| S/0/0/0 | 10.128.30.1 | 255.255.255.0 | N/A | N/A |
| PC-Admin | Fa0 | 192.168.22.6 | 255.255.255.0 | 192.168.1.1 | Switch1/ Fa0/1 |
| Fa0 | 192.168.22.5 | 255.255.255.0 | 192.168.1.1 | Switch1/ Fa0/2 |
| Pc-VPN | Gig0 | 192.168.2.13 | 255.255.255.0 | 192.168.2.1 | Switch0/ Gig0/1 |
| Gig0 | 192.168.2.14 | 255.255.255.0 | 192.168.2.1 | Switch0/ Fa0/1 |
| PC-OFFICE | Fa0 | 192.168.2.2 | 255.255.255.0 | 192.168.2.1 | Switch2 / Fa0/1 |
| Fa0 | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 | Switch2 / Fa0/2 |
| Fa0 | 192.168.2.4 | 255.255.255.0 | 192.168.2.1 | Switch2 / Fa0/3 |

1. Détailler la mise en œuvre des bonnes pratiques

Pour le bon fonctionnement de l’Entreprise nous devons mettre en place des outils et des bonnes pratiques afin qu’il n’y est pas de faille de sécurité et de pertes de données.

1. Mise en place d’un Firewall :

Cet outil va nous permettre de gérer les flux entrant et sortant dans l’infrastructure, et éviter les failles de sécurités.

1. Mise en place du Honeypot :

Nous pouvons mettre en place un honeypot sur un serveur linux afin de prévenir les attaques extérieures du serveur cible et donc de perdre des données sensibles.

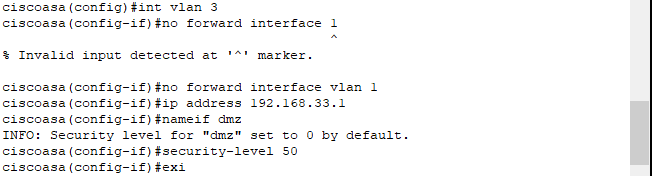
1. Mise en place du récupérateur de suppression de fichier :

Cet outil permettra à tout fichier supprimer dans un laps de temps de le récupérer et de le remettre sur le serveur, afin d’éviter les pertes de données dû à l’erreur humaine.

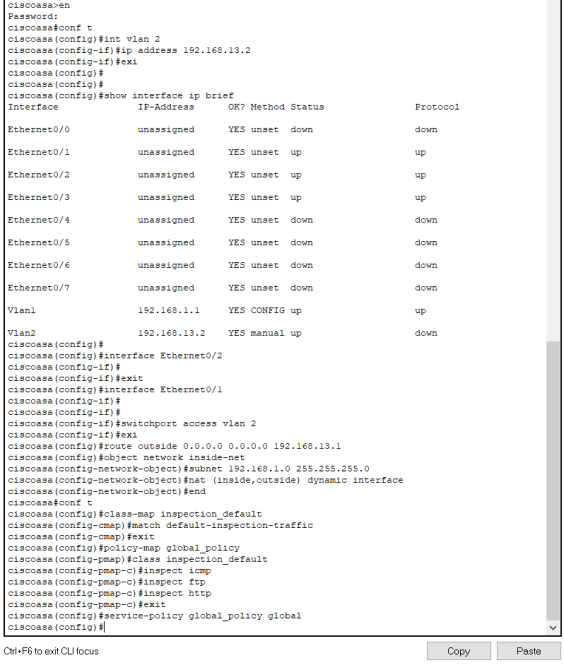
1. Mise en place d’un IDS :

Cet outil nous permettra de nous protéger et d’être averti si il y a une intrusion dans l’infrastructure.

1. Détailler les configurations à réaliser pour mettre en œuvre la solution (système, réseau, services)
   1. Configuration d’un Firewall :

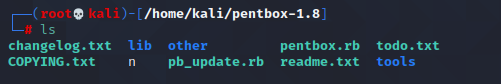


Configuration vlan 1 (inside) et 2 (outside) configuration des routes pour toute ip entrantes vers outside Configuration du network inside (192.168.1.0) pour aller vers internet + serveurs de de l'entreprise global policy -> laisse les packets icmp (ping) et http (connexion distante)

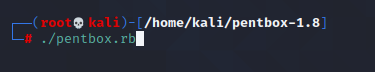


* + 1. Configuration du Honeypot :

Téléchargement de l’outil :



Lancement de l’outil :



* + 1. Configuration du récupérateur de suppression de fichier :

Au préalable, il faudrait avoir un système de fichier ext4magic sur votre machine dans le but de récupérer vos fichiers supprimés.

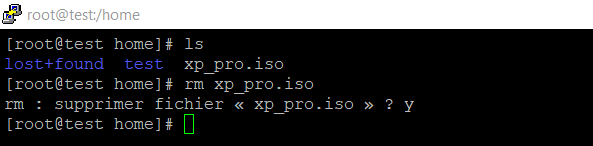
Dans cette procédure nous allons récupérer des fichiers supprimés accidentellement.

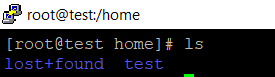
Exemple de l’accident :

On rentre dans un répertoire quelconque :



Le fichier **xp\_pro.iso** qui sera supprimé :





**/! Le fichier a été supprimé ! Récupérons-le ! !\**

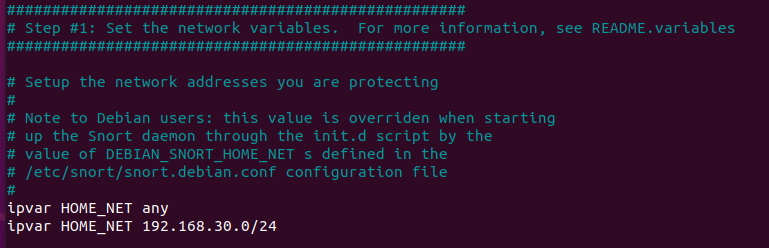
* + 1. Mise en place d’un IDS :

Après avoir téléchargé tous les paquets requis pour l’installation de Snort version 2.9.7.0. Attardons-nous sur la création de règles ainsi que les tests associés afin de visualiser le fonctionnement.

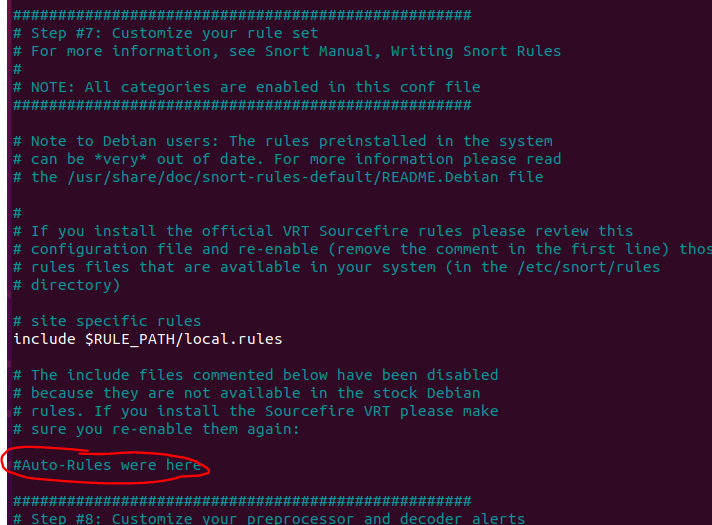
Dans un premier temps nous irons changer quelques paramètres du fichier snort.conf qui se trouve pour notre part dans le chemin /etc/snort

N’oublions pas de créer une copie de ce fichier et de la garder comme Backup (exemple : snort.conf.old)

Configurons Snort afin qu’il ne fonctionne que sur notre réseau souhaité (ici 192.168.30.0/24) notre adresse ip étant 192.168.30.129



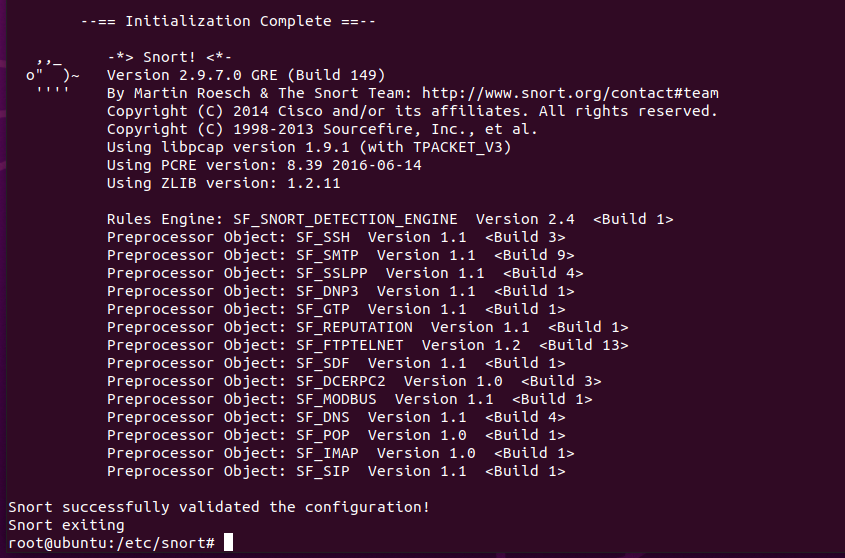
Afin de bien mettre en évidence notre compréhension du sujet, nous allons supprimer toutes les règles présentent automatiquement afin de ne pas être parasité par ces dernières et se focaliser sur la règle que nous voulons créer et mettre en évidence.



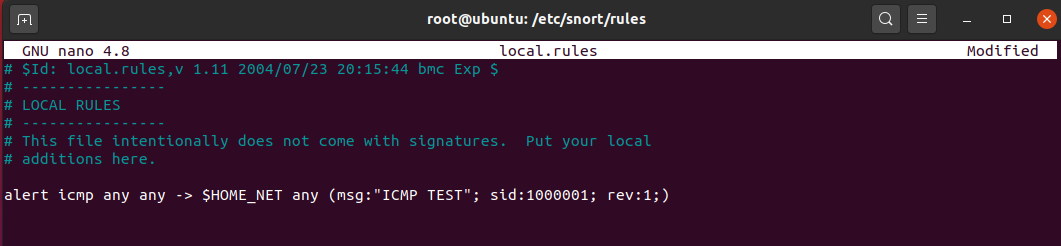
Avec cette modification nous sauvegardons le fichier et exécutons cette commande :

snort -T -i ens33 -c /etc/snort/snort.conf

Les deux dernières lignes nous confirment que le fichier de configuration n’a aucune erreur et que snort est prêt à fonctionner.



Créons maintenant notre règle qui sera une alerte dans le fichier local.rules se trouvant dans le path /etc/snort/rules



Description de la règle créée dans ce dossier->

alert icmp any any -> $HOME\_NET any (msg:"ICMP TEST"; sid:1000001; rev:1;)

Alert : Rule action

Any : Source IP -> Ici toutes

Any : Source port -> Ici tous

$HOME\_NET : Destination IP -> (variable présente dans snort.conf)

Any : Destination port -> Ici tous

msg:"ICMP TEST" : Message que snort enverra si la règle est outrepassée -> Ici ICMP TEST

sid:1000001 : Rule ID

rev:1 : Revision number

Classtype : Si on veut catégoriser les règles créées -> exemple : ICMP-event

Sauvegardons à présent le fichier et recommençons le processus de mise en fonctionnement du service Snort comme précédemment afin de vérifier si Snort est bien paramétré.

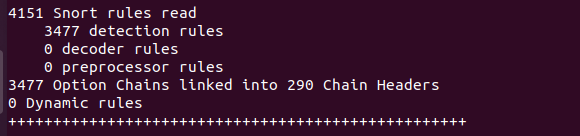
snort -T -i ens33 -c /etc/snort/snort.conf

Nous recevons donc le même message que la première fois avec Snort en succesfully validated the configuration.

Cependant attardons nous sur les lignes concernant l’Initializing rule chains

Nous constatons qu’une seule règle est prise en compte ; celle que nous venons de créer vu que nous avons supprimer toutes les autres.

Avant :



Apres :

