Atelier pihole

starinux 25.05.2019

Travaux pratiques

TP1 :

Savoir récolter des infos sur son réseau

Sur votre pc, après vous être connecté au réseau wifi « atelier_Pihole » , relever sur votre pc les informations suivantes : (plusieurs commandes sont possibles)

Ip de votre pc :
IP de votre passerelle :
IP de votre résolveur :
@Mac de votre passerelle :
nom de votre machine :

Les ports TCP ouverts sur votre machine :
pour voir tous les ports UDP et TCP :
le nombre de machines qui sont dans le même sous réseau que la vôtre :

****

TP2 :
De Nantes à Montaigu...

Retrouver pour les sites suivants ,les @IP et serveurs de mail (s'ils existent, n'en citer qu'un seul suffira)

- www.chatons.org
- baidu.com

B/ Effectuez une requête avec Dig sur un site que vous n'avez jamais consulté. Pour être sûr laisser libre court à votre imagination.
Renouvelez exactement la même commande 3 fois d'affilée et observer les champs de la réponse.
Qu'est ce qui change ?
Que pouvez vous en déduire ?

C/ (résolution inverse)

88.191.250.166 : a quelle domaine renvoie cette @ip ?

TP3 :

Un pinocchio dans mon réseau ?

En admettant que l'on a rien touché à la config dns fournie par la BOX

A/ Essayez d'accéder au site :
sci-hub.tw

B/ Faites un :
dig sci-hub.tw

Que renvoie la réponse ?

C/ Maintenant changez l'adresse ip de votre résolveur avec celui d'un résolveur public type cloudfare en 1.1.1.1

Faites un :
dig sci-hub.tw

Puis rafraichissez la page :
https://sci-hub.tw

Qu'en déduisez-vous ?

TP 4 :

« un pihole à la rescousse »

En vous aidant du tuto « **1_HowTo_install_pihole.pdf** », installez votre pihole.
Au choix sur un raspberry ou une VM dans virtualbox.

TP 5 :

« Lespion qui m'aimait »

Votre pihole est désormais installé.

A/ configurer votre resov.conf avec l'@ip du pihole
Générer un peu de trafic web en allant sur des sites internets du type bfm.tv

B/ Analyser *Top bloked domains*
Quels sont les 3 domaines les + bloqués ?

C/ Connectez un smartphone ou une tablette
Générez du trafic en lancant vos applis préférées (réseaux sociaux,météo, télécommande etc...)
Laissez passer 5 minutes.
Observez à nouveau le *Top bloked domains*
Qu'est ce qui change ?

TP 6 :
Nommer ses bébés

- donner des petits noms à ses machines
- tester le ping d'une machine par son nom

TP 7 :
Contrôle parental
1/ ajouter une liste (antifacebook par exemple)

- tester la maj en tapant dans votre navigateur : https://facebook.com

- Désactiver cette liste sans la supprimer puis réessayer d'aller sur facebook

2/ interdire facebook et snapchat – les accès seront interdits entre 22h et 08h

indice : On passera par des regex et on match l'expression avec un wildcard

---

TP 8 :
« *On n'est jamais mieux servi que par soi même* »

- Monter un vrai résolveur avec le logiciel **unbound**
Suivre les étapes du tuto de chez pihole.net
doc :https://docs.pi-hole.net/guides/unbound/

- Customisation du fichier de conf : **/etc/unbound/unbound .conf.d/pi-hole.conf**
qui contient :

[config des logs]:
Décommenter ligne n°3
puis mettre verbosity à 3 pour notre TP

-créer le repertoire de log

- vérifier l'intégrité du fichier de conf

-Tester une requête avec dig sur le pihole :

-Reconfigurer son pihole avec l'@IP du nouveau résolveur
- Ouvrir dans un terminal tail -f /*var* / log/unbound.log

1- Aller sur pihole – query log
2- lancer Firefox et aller sur un site au pif
3- Essayer de retrouver la requête dans le log d'unbound

TP 9 :
- Monter un serveur VPN avec Openvpn (pivpn sur raspberry)
tuto dispo ici : https://tutox.fr/2017/07/20/transformer-facilement-raspberry-serveur-vpn/
- configurer le client
- l'importer sur android ou sur pc (mais faut une connexion internet différente du réseau ou est placé le pihole)
- vérifier les logs

TP 10 :
Pour aller encore plus loin

Activer le chiffrement **Dns over https** sur votre unbound **.**
Suivre le pas à pas :
https://docs.pi-hole.net/guides/dns-over-https/

à Starinux le 25.05.2019

Benjamin