Atelier pihole

starinux 25.05.2019

Travaux pratiques

TP1 :

Savoir récolter des infos dans 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 a**

ip publique : **curl ifconfig.me**

IP de votre passerelle : **ip r**

IP de votre résolveur : **cat /*etc*/resolv.conf**

@Mac de votre passerelle :**arp -a**

nom de votre machine : **hostname**

Les ports TCP ouverts sur votre machine : **ss -ant**
pour voir tous les ports :

ss -anut

ou
netstat -plantu

Voir les associations : nom de « programmes / socket »

lsof -i nomInterfaceReseau PROTOCOLE :port ce qui donne par exemple pour savoir quels programmes sont connectés au port 443 :

lsof -i wlan0 TCP:443

le nombre de machines qui sont dans le même sous réseau que la vôtre :

sudo nmap -sP 102.168.0.1/24

On peut aussi utiliser nmap en mode graphique/ Il faut installer le package: **zenmap**

TP2 :

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

Réponses :
A/ commandes à passer pour retrouver l'IP du domaine :
dig www.chatons.org +short

dig baidu.com +short

ou
host chatons.org

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 ?

dig popo.fr
dig popo.fr
dig popo.fr
Le champ TTL (time to live) est le seul qui varie. La première réponse affiche un TTL avec un nombre rond. Les réponses suivantes le TTL décrémente.

De plus , le QUERY TIME de la première requête est plus long que les 2 autres requêtes.

On peut en déduire que :

- la réponse à la *première requête* a été renvoyée par le **serveur faisant autorité** au résolveur puis au navigateur.

- La requête 2 et 3 ont directement été renvoyées par le **cache** du résolveur. Leur TTL et leur QUERY TIME est inférieur à la première requête.

C/ (résolution inverse)
88.191.250.166 : a quelle domaine renvoie cette @ip ?

dig -x 88.191.250.166 +short

Le reverse DNS est en général un prérequis pour utiliser son propre serveur d'envoi de mails

TP3 :

Un pinocchio dans mon réseau ?

Si vous avez un smartphone , faites un partage de connexion avec votre pc.
Ensuite allez sur le site https://dnsleaktest.com pour confirmer que vos dns sont bie ceux de votre opérateur téléphonique.

Nota : pour le test , éviter d'utiliser un navigateur ou alors vider bien le cache avant :
sous firefox cest la combinaison des touches : **shift+ctrl+r**

A/ Faites un dig du domaine :**sci-hub.tw**

La réponse renvoyée est :
status: NXDOMAIN,
autrement dit le domaine n'existe pas !

B/ Faites un :
dig sci-hub.tw

C/ Maintenant connectez vous sur le wifi de votre box
Assurez vous d'avoir mis dans le ***/etc/*resolv.conf**
nameserver 1.1.1.1

Tester sur **dnsleaktest.com** que vos dns sont bien ceux de cloudfare **:**

Faites un :
dig sci-hub.tw

la réponse a changé
STATUS= NOERROR

ANSWER SECTION:
sci-hub.tw. 1 IN A 186.2.163.90

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

Le test montre bien que les DNS de la plupart des FAI nous mentent. (testé chez moi avec Bouygues telecom comme opérateur 4G)

TP 4 :

« un pihole à la rescousse »

En vous aidant du tuto « **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 en allant sur des sites webs.

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.)
MAIS SANS UTLISER VOTRE NAVIGATEUR
Laissez passer 2/3 minutes.
Observez à nouveau le *Top bloked domains*
Qu'est ce qui change ?

Réponse :
Le test prouve qu'il n'y a pas besoin d'utiliser le navigateur pour générer des requêtes DNS.Le simple fait de lancer des applis activent un grand nombre de trackers publicitaires du style googleads.
Du coup le top block domained devrait contenir les domaines appartenant à google.

TP 6 :
Nommer ses bébés
- donner des petits noms à ses machines

Réponse :
Sur le pihole :
aller dans **/*etc*/pihole**
Editer le fichier local.list et mettre les infos :
@ip nomdemachine

Relancer le service :
pihole restartdns

Sur votre pc :
tester la résolution d'adresse interne par le pihole. Sur votre pc pinguer une machine de votre réseau par son nom
ping toto

si ca ne fonctionne pas : assurez vous d'avoir l@ip de votre pihole dans resolv.conf

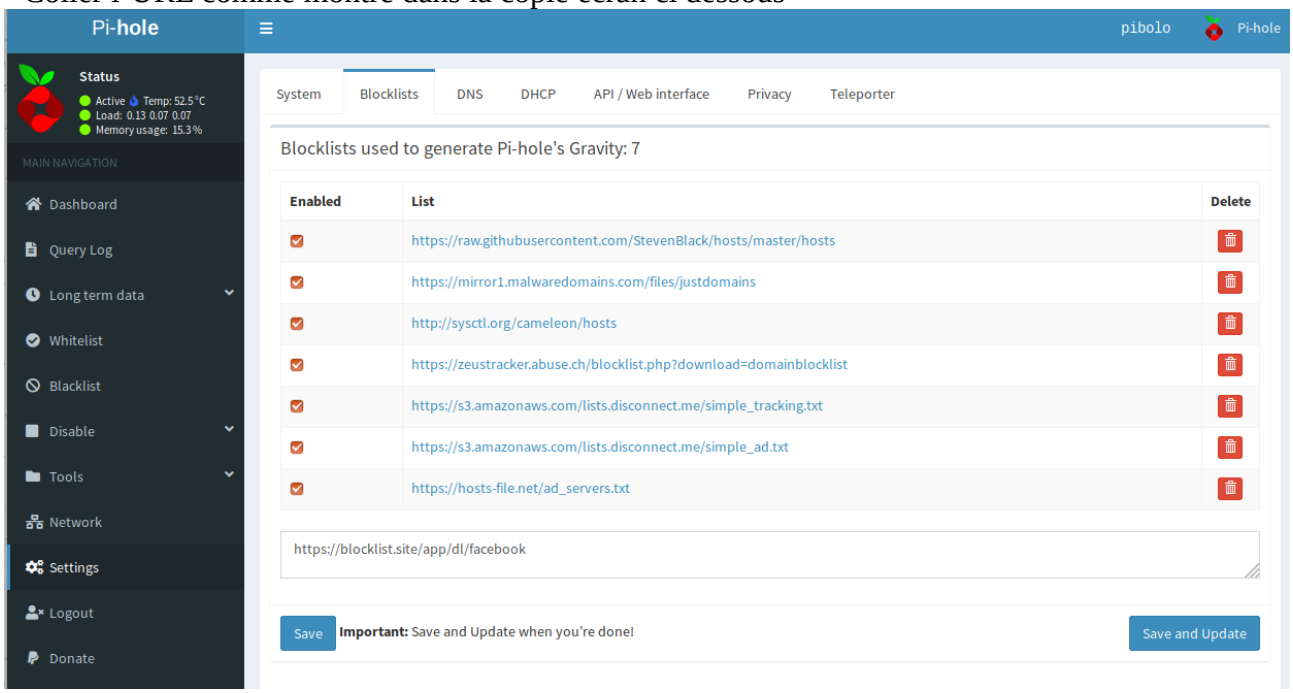
---

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

- Aller sur le site https://blocklist.site

- Copier l'URL de la liste antiFacebook
https://blocklist.site/app/list-details.php?list=facebook

- Coller l'URL comme montré dans la copie écran ci dessous



- Cliquer sur « save and update»

- 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

On passe par des regex et on match l'expression avec un « wildcard »

Editer la crontab
 # domaines bloqués
00 22 * * * /usr/local/bin/pihole --wild facebook.com snapchat.com
 # domaines à nouveau autorisés
00 07 * * * /usr/local/bin/pihole --wild -d facebook.com snapchat.com

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

1/ Monter un vrai résolveur avec le logiciel **unbound**
Pour commencer , se connecter en ssh à son pihole et s**uivre les étapes de la doc pihole :**
https://docs.pi-hole.net/guides/unbound/

2/ Customisation du fichier de conf : (étape 2 est facultatives
/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

```
server:
    # If no logfile is specified, syslog is used
    logfile: "/var/log/unbound/unbound.log"
    verbosity:3
```

créer le repertoire de log :
mkdir /var *log* /unbound
chown -R unbound /var *log* /unbound
systemctl restart unbound

-Activer la qname-minimisation

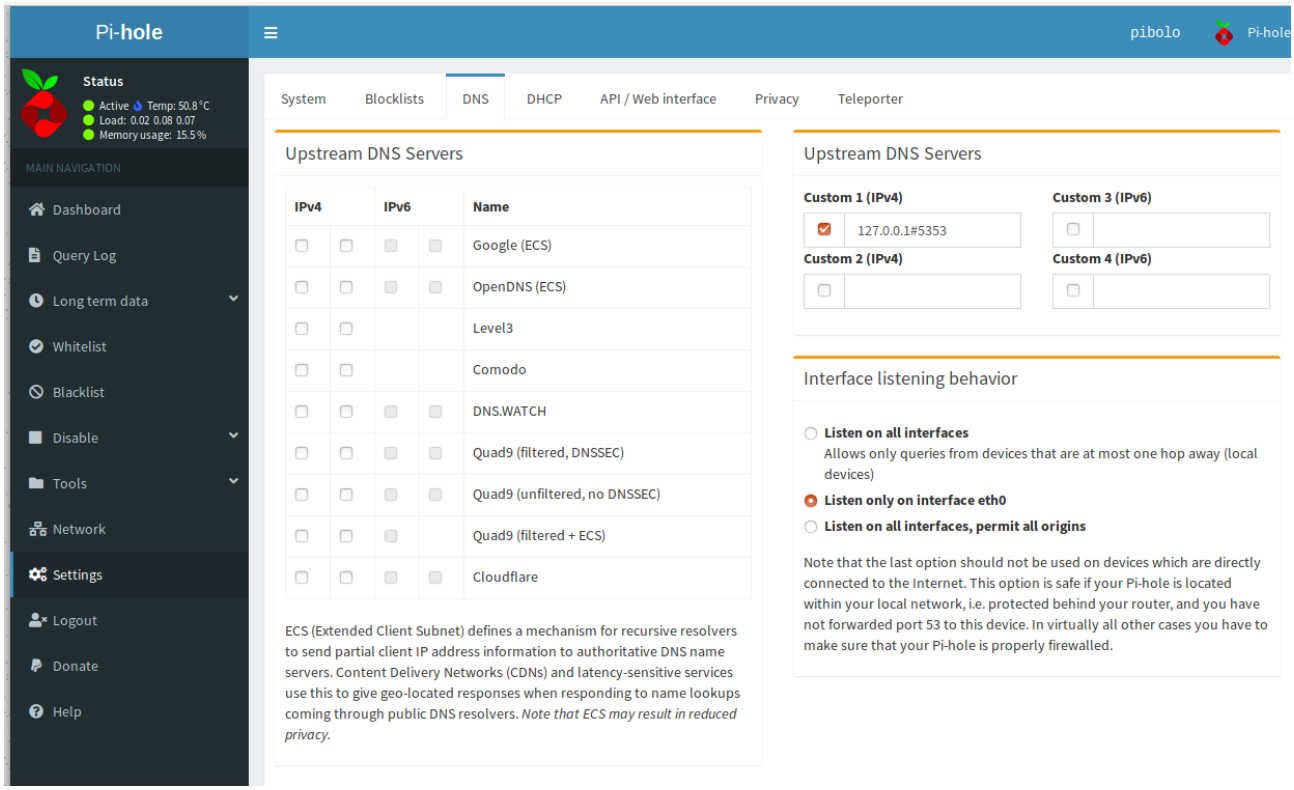
```
qname-minimisation: yes
```

- vérifier l'intégrité du fichier de conf
unbound-checkconf pi-hole.conf

Tester une requête avec dig sur le pihole :

dig joe.com -p 5353

3/ Reconfigurer son pihole avec l'@IP du nouveau résolveur unbound (va remplacer Cloudfare)



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

cat */var/* log/unbound/unbound.log | grep -i « nom du site »

nota : les premières requêtes peuvent être un peu plus longues que d'habitude car unbound contacte les serveurs racines pour les sites qu'il ne connaît pas . Ensuite la mise en cache accélèrera considérablement les requêtes.

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 : (à venir)
Pour les plus impatients , me contacter par mail :-)
Pour aller encore plus loin

Activer le chiffrement **Dns over https** sur votre unbound **.**

TP atelier Pihole
à Starinux 25.05.2019
par Benzo