commandes DNS

- Création par : lagrenouille
- Objet : du tuto Fix Me!
- Niveau requis : Fix Me!
  débutant, avisé
- Commentaires : *Contexte d'utilisation du sujet du tuto.* Fix Me!
- Débutant, à savoir : Utiliser GNU/Linux en ligne de commande, tout commence là !.

- à-tester, à-placer

Installation

```
apt install dsniff  dnstracer dnstop dnsutils  bind9-dnsutils
```

Doc trouvé sur le net et testé

Il est fortement conseillé de lire les doc et les man pour ces commandes DNS

dsniff

dsniff est un renifleur de mot de passe qui gère FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP,

```
     IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS,
SOCKS, X11, CVS,
     IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec
pcAnywhere, NAI
     Protocoles Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase et Microsoft
SQL.
```

dsniff détecte automatiquement et analyse au minimum chaque protocole d'application, en sauvegardant uniquement les bits intéressants et utilise Berkeley DB comme format de fichier de sortie, ne journalisant que tentatives d'authentification. Le réassemblage TCP/IP complet est fourni par libnids (3).

OPTIONS

1. c Effectue un réassemblage de flux TCP semi-duplex, pour gérer le trafic acheminé de manière asymétrique

(comme lors de l'utilisation de arpspoof (8) pour intercepter le trafic client à destination du

```
            passerelle).
```

1. d Activer le mode de débogage.

1. m Activer la détection automatique du protocole.

1. n Ne résout pas les adresses IP en noms d'hôte.

1. i interface

Spécifiez l'interface sur laquelle écouter.

1. p fichiercap

Plutôt que de traiter le contenu des paquets observés lors du processus réseau

```
            le fichier de capture PCAP donné.
```

1. s snaplen

Analyse au maximum les premiers octets snaplen de chaque connexion TCP, plutôt que

```
            par défaut de 1024.
```

1. f services

Charge les déclencheurs à partir d'un fichier de services .

1. t déclencheur [,...]

Charger les déclencheurs à partir d'une liste séparée par des virgules, spécifié comme port / proto = service (par exemple

```
            80/tcp=http).
```

1. r savefile

Lit les sessions reniflées à partir d'un fichier de sauvegarde créé avec l' option -w .

1. w fichier

Ecrit les sessions reniflées dans le fichier de sauvegarde plutôt que de les analyser et de les imprimer.

```
     expression
            Spécifiez une expression de filtre tcpdump (8) pour sélectionner
le trafic à renifler.
```

```
     Sur un signal de raccrochage, dsniff videra sa table de déclenchement
actuelle dans dsniff.services .
```

dnstracer

suivi des requêtes DNS jusqu'à leur source

-r retries : nombre de tentatives pour les requêtes DNS, par défaut 3

```
dnstracer -r  3 -v debian.facile.org
```

-v verbose

-4 : ne pas interroger les serveurs IPv6

-c : désactivation de la mise en cache locale, activée par défaut

-C : active la mise en cache négative, désactivée par défaut

-o : permet d'obtenir un aperçu des réponses reçues, désactivé par défaut

-q querytype : type de requête à utiliser pour les demandes DNS, par défaut A

-s server : utilisation de ce serveur pour la requête initiale, par défaut localhost

Si . est spécifié, A.ROOT-SERVERS.NET sera utilisé.

-t durée maximale : Limite du temps d'attente par tentative

-v : verbeux

-S adresse IP : utiliser cette adresse source.

dnstop

dnstop est un petit outil pour écouter sur l'appareil ou pour analyser le fichier savefile et collecter et

imprimer des statistiques sur le trafic DNS du réseau local. Vous devez avoir un accès en lecture à /dev/bpf* .

OPTIONS DE LA LIGNE DE COMMANDE

```
   Les options sont les suivantes :
```

1. 4 compte uniquement les messages avec des adresses IPv4, compte uniquement les messages avec des adresses IPv4
1. 6 compte uniquement les messages avec des adresses IPv6, compte uniquement les messages avec des adresses IPv6
1. Q ne compte que les messages de requête DNS, ne compte que les messages de requête DNS
1. R ne compte que les messages de réponse DNS, ne compte que les messages de réponse DNS
1. a anonymiser les adresses,
1. b expression

Expression de filtre BPF

```
            (par défaut : port udp 53)
```

1. j'adresse ignorer les adresses sélectionnées
1. p Ne pas mettre l'interface en mode promiscuité.
1. r Intervalle de rafraîchissement (secondes).
1. l niveau conserve le décompte des noms jusqu'au niveau des niveaux de nom de domaine.

dnsutils

Paquet : dnsutils, Clients fournis avec BIND

Ce paquet fournit divers programmes clients reliés à DNS

nslookup

nslookup est un programme informatique de recherche d'information dans le Domain Name System, qui associe nom de domaine et adresses IP. nslookup permet donc

d'interroger les serveurs DNS pour obtenir les informations définies pour un domaine déterminé.

nslookup appartient au paquet bind9-dnsutils

exemple:

```
nslookup debian-facile.org
Server:     192.168.1.1
Address:    192.168.1.1#53

Non-authoritative answer:
Name:   debian-facile.org
Address: 89.234.146.138
```

nsupdate

nsupdate est utilisé pour soumettre des demandes de mise à jour DNS

L' option -d fait fonctionner nsupdate en mode débogage. Cela fournit des informations de suivi sur les demandes de mise à jour effectuées et les réponses reçues du serveur de noms.

L' option -t définit le temps maximum qu'une demande de mise à jour peut prendre avant d'être abandonnée. La valeur par défaut est de 300 secondes. Zéro peut être utilisé pour désactiver le délai d'attente.

L' option -u définit l'intervalle entre les nouvelles tentatives UDP. La valeur par défaut est de 3 secondes. Si zéro, l'intervalle sera calculé à partir de l'intervalle de temporisation et du nombre de tentatives UDP.

L' option -r définit le nombre de tentatives UDP. La valeur par défaut est 3. Si zéro, une seule demande de mise à jour sera effectuée.

dig

Dig permet de tracer le chemin de recherche DNS en utilisant l'option +trace. Cette option permet d'effectuer des requêtes itératives pour résoudre la recherche de noms. Elle interrogera les serveurs de noms à partir de la racine et parcourra ensuite l'arbre de l'espace de noms à l'aide de requêtes itératives suivant les renvois en cours de route :

la commande dig appartient au metapaquet "dnsutils"

```
apt-get install dnsutils
```

dig [serveur] [nom] [type]

```
dig debian.org
```

Pour afficher uniquement l'adresse IP associée au nom de domaine, entrez ce qui suit :

```
dig debian.org +short
```

L'option +trace répertorie chaque serveur différent que la requête passe jusqu'à sa destination finale.

```
dig debian-facile.org +trace
```

```
dig debian.org MX
```

dig La commande dig dans Linux est utilisée pour collecter des informations DNS. Il signifie Domain Information Groper et collecte des données sur les serveurs de noms de domaine

```
dig MX debian-facile.org

; <<>> DiG 9.16.37-Debian <<>> MX debian-facile.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19104
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 81bcc308b367caa0010000006481748e382ae5760456d22d (good)
;; QUESTION SECTION:
;debian-facile.org.     IN    MX

;; ANSWER SECTION:
debian-facile.org.  86400    IN    MX    10 mail.debian-facile.org.

;; Query time: 36 msec
```

```
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Thu Jun 08 08:26:22 CEST 2023
;; MSG SIZE  rcvd: 95
```

```
dig ANY debian-facile.org

; <<>> DiG 9.16.37-Debian <<>> ANY debian-facile.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22546
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 17aad4a97cf475f401000000648174d38180dd2a509ebfa0 (good)
;; QUESTION SECTION:
;debian-facile.org.     IN    ANY

;; ANSWER SECTION:
debian-facile.org.  86331    IN    RRSIG    MX 8 2 86400 20230630152546
20230531152546 52104 debian-facile.org.
nc3uj89lZCG6FTVFxpNX+Ou40FjgF62gHjhQTI3sMIZ9OOltKKM+vifZ
TllM9wYQUIQIfrH6dRTMDnGl0uVAmv+2n4ZHIhn0+36935Ela3nAelGM
VKK4GcSJ6UKQT0SwestQp2g2E/9Y2DuHs27ChF26Yt5HQl/j8g/4SMW5 U6U=
debian-facile.org.  86331    IN    MX    10 mail.debian-facile.org.
debian-facile.org.  3428    IN    RRSIG    DS 8 2 3600 20230622152518
20230601142518 33369 org.
DWJQei1TL7Pgo++yQkQcr/rwPHwyhcobJnS1z4nARghjHBVoA+MAaZhK
erl5E8kW9ZtO+9br+JQBsQOP4YH1BF8XogzRVdg/w4KoB6RKYJpydPAR
rTBdIDCJn9zxBVQqNW3H7vwiDosJ5Cy5vjixVwF2/mG19KIm29lmI5lw 3yA=
debian-facile.org.  3428    IN    DS    2656 8 2
43CB6382522A012F2CB9327C8A3C52AB0C190861C15DC1DF8D5D25F9 1AE4A547
debian-facile.org.  3428    IN    NS    dns10.ovh.net.
debian-facile.org.  3428    IN    NS    ns10.ovh.net.
debian-facile.org.  8649    IN    RRSIG    A 8 2 86400 20230630152546
20230531152546 52104 debian-facile.org.
oa9AlGyMJ3hAVZO3pQ29Tn9bgVoT5d8k69HL5OC/KqguDk4v/UtHVFzd
2oWgonAv9un692h8kgRgdnrclcX4BbJRgoVcuePGICOSn7MjqovyXO1g
VdXg8VcOlb6QHW1GRJWTZxnnaFiLEoWCIdS00oll1FpTktz1/SBtDK5Q n8Y=
debian-facile.org.  8649    IN    A    89.234.146.138

;; Query time: 44 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Thu Jun 08 08:27:31 CEST 2023
;; MSG SIZE  rcvd: 722
```