

ANALYSE DE TRAFIC RÉSEAU - TEST PASSIF

PROTOCOLE POP

31 Décembre 2015

Egor KOCHKUROV <vint64@mail.com>

Joaquim LEFRANC <lefrancjoaquim@gmail.com>

Jérôme SKODA <contact@jeromeskoda.fr>

ARBORESCENCE DU DOSSIER

docs: Documents

res: Ressources pour le rapport

dpi-pop.py: Script d'analyse de fichier pcap dans le protocole POP

pop3-sample-X.pcap: Exemple de fichier pcap

README.md: A lire absolument avant de faire quoi que ce soit

rapport.pdf: C'est moi =')

UTILISATION DU SCRIPT

Modules

Fonctionne avec python3 avec les modules libpcap et dpkt

Memo pour l'installation des modules:

```
pip3 install libpcap
```

```
pip3 install dpkt
```

Usage

```
dpi-pop.py [-h] -i INPUT [-a] [-t] [-eth] [-ip] [-tcp]
```

arguments:

-h, --help	show this help message and exit
-i INPUT, --input INPUT	Input file name
-a, --all	Display all data
-t, --time	Display time
-eth	Display eth data
-ip	Display ip data
-data	Display tcp data

Exemple d'utilisation

1) python3 dpi-pop.py -i pop3-sample-1.pcap

Analyse de fichier pop3-sample-1.pcap

2) python3 dpi-pop.py -i pop3-sample-2.pcap -all

Analyse du fichier pop3-sample-2.pcap avec tout les détails

Détails de l'affichage

```
.../Documents/Master2/IngProt/test-passif-dpi-pop  ceee6c4 Master ?
> python3 dpi-pop.py -i pop3-sample-1.pcap -a
[POP-S] OK : Ok
[Tag]
POP-S: Réponse du Timestamp : 2009-12-09 17:04:49.494222
serveur Ether Frame: 00:1a:2b:03:8a:0c -> 00:16:e6:54:c8:97 (2048)
POP-C: Commande IP : 38.113.3.21 -> 172.26.0.4 (len=57 ttl=252 DF=1 MF=0 offset=0)
client Data : b'+OK\r\n'

[POP-C] CAPA : affiche les informations du serveur
Timestamp : 2009-12-09 17:04:49.494488 -> option: -time
Ether Frame: 00:16:e6:54:c8:97 -> 00:1a:2b:03:8a:0c (2048) -> option: -eth
IP : 172.26.0.4 -> 38.113.3.21 (len=58 ttl=64 DF=1 MF=0 offset=0) -> option: -ip
Data : b'CAPA\r\n' -> option: -data

[POP-S] ERR : Erreur
Timestamp : 2009-12-09 17:04:49.634986
Ether Frame: 00:1a:2b:03:8a:0c -> 00:16:e6:54:c8:97 (2048)
IP : 38.113.3.21 -> 172.26.0.4 (len=58 ttl=252 DF=1 MF=0 offset=0)
Data : b'-ERR\r\n'

Titre : Description Information complémentaire
[POP-C] USER : identification xplicotest@HotPOP.com
Timestamp : 2009-12-09 17:04:49.635605
Ether Frame: 00:16:e6:54:c8:97 -> 00:1a:2b:03:8a:0c (2048)
IP : 172.26.0.4 -> 38.113.3.21 (len=80 ttl=64 DF=1 MF=0 offset=0)
Data : b'USER xplicotest@HotPOP.com\r\n'
```

N'hésitez pas à tester des fichiers avec ou sans l'option -all

Exemple d'affichage

```
.../Documents/Master2/IngProt/test-passif-dpi-pop  d57ab35 Master !
> python3 dpi-pop.py -i pop3-sample-1.pcap
[POP-S] OK : Ok
[POP-C] CAPA : affiche les informations du serveur
[POP-S] ERR : Erreur
[POP-C] USER : identification xplicotest@HotPOP.com
[POP-S] OK : Ok
[POP-C] PASS : authentification kebab1
[POP-S] OK : Ok
[POP-C] STAT : indique le nombre de messages et la taille occupée par l'ensemble des messages
[POP-S] OK : Ok 4 108347
[POP-C] LIST : donne une liste des messages ainsi que la taille de chaque message : un numéro suivi de la taille en octets ;
[POP-S] OK : Ok
[DATA] : (option -data pour le contenu complet) line 1: 1 2630
[POP-C] UIDL : affiche (pour un seul ou pour tous les messages) un identifiant unique qui ne varie pas entre chaque session
[POP-S] OK : Ok
[DATA] : (option -data pour le contenu complet) line 1: 1 6ef78df6fd660391
[POP-C] QUIT : quitter la session en cours
[POP-S] OK : Ok
[POP-S] OK : Ok
[POP-C] CAPA : affiche les informations du serveur
[POP-S] ERR : Erreur
[POP-C] USER : identification xplicotest@HotPOP.com
[POP-S] OK : Ok
[POP-C] PASS : authentification kebab1
[POP-S] OK : Ok
[POP-C] STAT : indique le nombre de messages et la taille occupée par l'ensemble des messages
[POP-S] OK : Ok 4 108347
[POP-C] LIST : donne une liste des messages ainsi que la taille de chaque message : un numéro suivi de la taille en octets ;
[POP-S] OK : Ok
[DATA] : (option -data pour le contenu complet) line 1: 1 2630
[POP-C] UIDL : affiche (pour un seul ou pour tous les messages) un identifiant unique qui ne varie pas entre chaque session
[POP-S] OK : Ok
[DATA] : (option -data pour le contenu complet) line 1: 1 6ef78df6fd660391
[POP-C] QUIT : quitter la session en cours
[POP-S] OK : Ok
[POP-S] OK : Ok hello from popgate 2.45 on pop016.mail.ukl
[DATA] : (option -data pour le contenu complet) line 1: .yahoo.com
[DATA] : (option -data pour le contenu complet) line 1: AUTH
```