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
READEME.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'instalation 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

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
```