Je suis pleinement conscient(e) que le plagiat de documents ou d'une partie de document constitue une fraude caractérisée.
Nom, date et signature :

Étude des fichiers compressé sur les moyens de protection défensifs

Monnet-Paquet Aurélien
.
Supervised by : Lauradoux Cédric

Juin 2016

Abstract Insert your abstract here. Include keywords, PACS and mathematical subject classification numbers as needed.

Keywords Bombe de compression · IDS · Antivirus · Framework

1 Introduction

Your text comes here. Separate text sections with

Monnet-Paquet Aurelien
Université Grenoble Alpes, 38400 Saint Martin d'Hères
E-mail: monnetpa@e.ujf-grenoble.fr

Lauradoux Cedric
Inria, 38334 Montbonnot
E-mail: cedric.lauradoux@inria.fr

2 Les IDS : Sonde de détection d'intrusion

Text with citations [2] and [4].

2.1 Présentation

But : faire peter Suricata avec les bombes.

2.2 Fonctionnement

2.3 Analyse

2.4 Conclusion sur les IDS

3 Les sites web agrégateurs d'Antivirus

3.1 Présentation

Dans cette section, nous allons analyser le comportement des agrégateurs d'antivirus que l'on peut trouver sur internet.
Cette expérience portera sur 3 sites :

- VirusTotal [4]
- Jotti [5]
- Virscan [6] basé en chine

Nous allons tester chacun de ses sites en 3 étapes :

- 1. Analyse témoin : un fichier connu pour être malveillant
- 2. Analyse du même fichier dans différents formats de compression
- 3. Analyse des différentes bombes de compression

Le but de cette expérience est d'analyser le comportement de ses éléments sur les fichiers compressé.
Est-ce que tous les format de compression sont supporté ?
Le comportement des antivirus commun entre les sites sont ils similaire ?
Est-ce que les bombes sont détectées ?

3.2 Fonctionnement

VirusTotal est actuellement le site le plus populaire dans ce domaine. Il permet, à ce jour, d'analyser un fichier avec 57 antivirus différent. Il existe 3 manières pour soumettre un fichier :

- L'interface web
- L'API
- Recherche par hash (md5, sha-1, sha-256)

Remarque : pour pouvoir utilisé l'API, il faut avoir un compte actif.

3.3 Analyse

3.4 Conclusion sur les agrégateurs

4 Les Frameworks d'analyse de malwares

4.1 Présentation

4.2 Fonctionnement

4.3 Analyse

4.4 Conclusion sur les frameworks

5 Les Antivirus Linux

5.1 Présentation

5.2 Fonctionnement

5.3 Analyse

5.4 Conclusion sur les frameworks

6 Conclusion

References

1. David J. Day et Benjamin M. Burns, "A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines"
2. oisf.net, The Open Information Security Foundation, organisation à but non lucrative qui développe et met à jour Suricata.
3. redmine.openinfosecfoundation.org/projects/suricata/wiki/, la documentation pour utilisateurs et développeurs de Suricata.
4. virustotal.com, site agrégateurs d'antivirus, filière de Google.
5. virusscan.jotti.org, site agrégateurs d'antivirus, basé aux Pays-Bas.
6. www.virscan.org, site agrégateurs d'antivirus, basé en chine.
7. www.korelogic.com
8. www.viper.li
9. irma.quarkslab.com
10. www.comodo.com
11. www.clamav.net