Outillage pour les audits de configuration

JSSI 2013

–

Maxime OLIVIER

AMOSSYS

Agenda

- **Audit de sécurité**
- Configuration, définition, extraction
- Analyse des données
- Exemples

Audit de sécurité

Organisationnel

Audit de sécurité

Code

Audit de sécurité

Test d'intrusion

Audit de sécurité

Architecture

Audit de sécurité

Configuration

L'audit de configuration

Directives non sécurisées

L'audit de configuration

Conformité avec la documentation

Exemples de résultat

- Simple : FTP anonyme
- Complexe : *secure cookie* sur un site accessible en HTTP et HTTPS

Les problématiques

Auditer hors ligne

Les problématiques

Extraire les configurations

Les problématiques

Qu'extraire et comment ?

Les problématiques

Analyser les données

Agenda

- L'audit de sécurité
- **Configuration, définition, extraction**
- Analyse des données
- Exemples

Définition

Image du serveur

Système, réseau et applications

Qu'extraire et comment ?

Version du système d'exploitation
Configuration matérielle
Configuration réseau
Utilisateurs et groupes
Paquets installés
Fichiers et droits associés

Processus en écoute
Processus actifs
Points de montage
Pare-feu local
Tâches planifiées

Qu'extraire et comment ?

Script d'extraction

Agenda

- L'audit de sécurité
- Configuration, définition, extraction
- **Analyse des données**
- Exemples

Approche

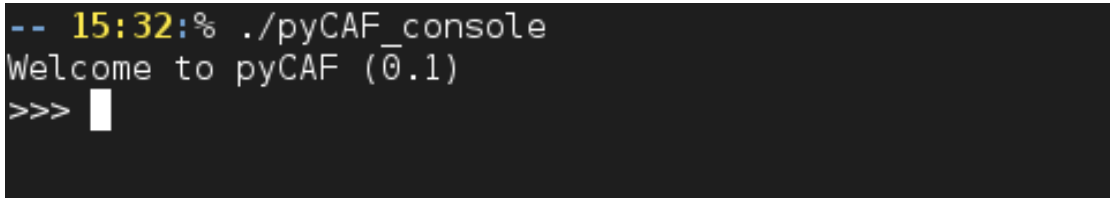
Manuelle

Automatisée

Semi-automatisée

Solution semi-automatisée

Framework



Architecture

Cœur + plugins

Cœur

Focalisé sur le système d'exploitation

Plugins

Pour gérer les applications

Agenda

- L'audit de sécurité
- Configuration, définition, extraction
- Analyse des données
- **Exemples**

Chargement d'une archive

```
-- 15:32:% ./pyCAF_console
Welcome to pyCAF (0.1)
>>> exemple = Archive("/home/maxime/Projets/pyCAF/pyCAF/test-resources/Maxime.config.11144.tar.bz2")
>>>
```

Premières manipulations

```
-- 15:32:% ./pyCAF_console
Welcome to pyCAF (0.1)
>>> exemple = Archive("/home/maxime/Projets/pyCAF/pyCAF/test-resources/Maxime.config.11144.tar.bz2")
>>> exemple.os
'debian'
>>> exemple.os_version
'wheezy'
>>> exemple.archi
'amd64'
>>>
```

Documentation

```
-- 05:35:% ./pyCAF_console
Welcome to pyCAF (0.1)
>>> exemple = Archive("/home/maxime/Projets/pyCAF/pyCAF/test-resources/Maxime.config.11144.tar.bz2")
>>> help(exemple.packages['emacs'])
```

```
 ----------------------------------------------------------------------
 Methods inherited from Package:

 __repr__(self)

 isUpToDate(self, operating_system, os_version, archi)
     Method based on rmadison in order to check if the current package is up to date.

 ----------------------------------------------------------------------
```

Manipulation des paquets

```
-- 19:01:% ./pyCAF_console
Welcome to pyCAF (0.1)
>>> exemple = Archive("/home/maxime/Projets/pyCAF/pyCAF/test-resources/Maxime.config.11144.tar.bz2")
>>> exemple.packages["emacs"].version
'45.0'
>>> exemple.packages["emacs"].isUpToDate("debian", "wheezy", "amd64")
installed version = emacs 45.0
up to date version = emacs 45.0
Package emacs in version 45.0 is up to date.
>>>
```

Merci

Olivier Tétard

Dimitri Kirchner

Merci de votre attention