

RecoNet & EvalSMSI

Outils pour la SSI

Michel Dubois

myshell.dubois@gmail.com

<http://reconet.sourceforge.net>
<http://evalsmsi.sourceforge.net>



Table des matières

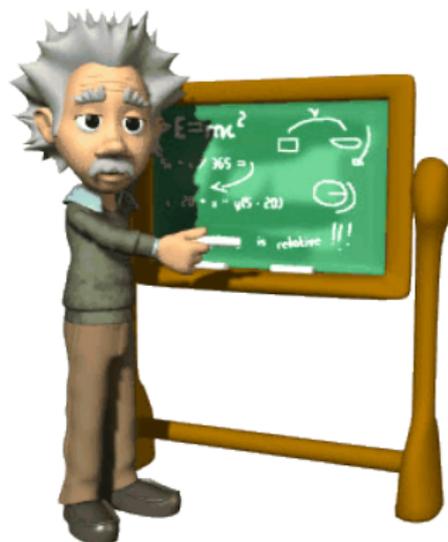
- 1 Reconet
 - Tests d'intrusions
 - Automatisation...
 - l'outil RecoNet
- 2 EvalSMSI
 - ISO 27001 & SMSI
 - l'application EvalSMSI



Reconet

1 Reconet

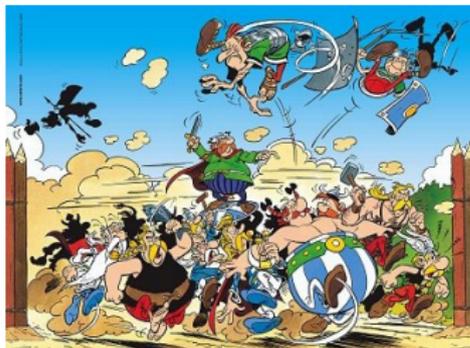
- Tests d'intrusions
- Automatisation...
- l'outil RecoNet



Définition & Objectifs

Définition

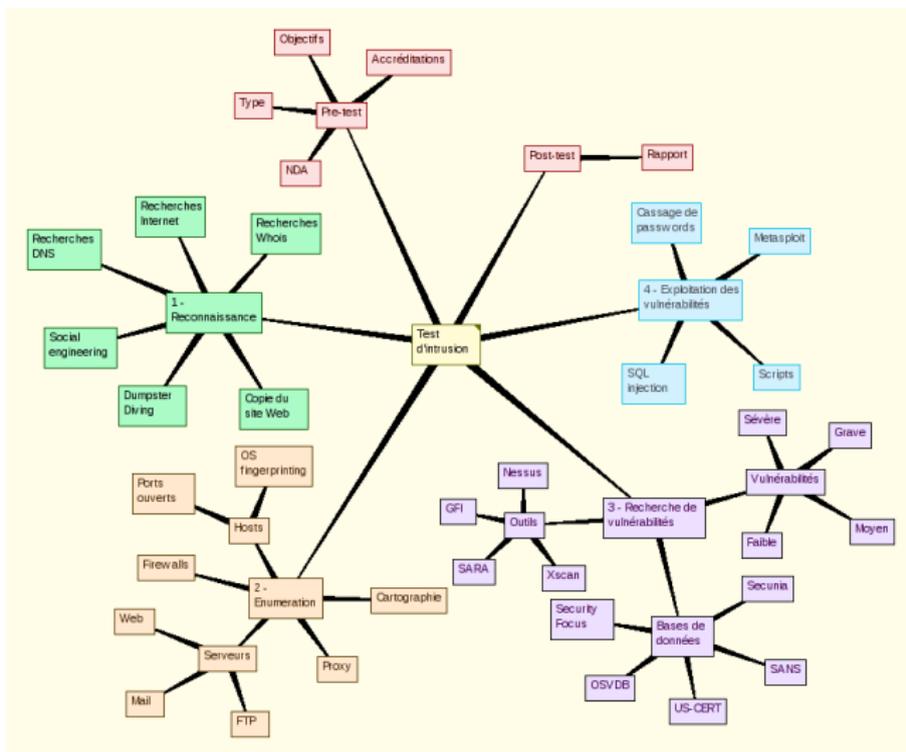
Un test d'intrusion est une méthode d'**évaluation de la sécurité d'un système d'information** basée sur la simulation d'une attaque, interne ou externe, par un cybercriminel.



Il s'agit de déterminer :

- ▶ la faisabilité d'une attaque
 - ▶ sur un système cible
 - ▶ à un instant donné
- ▶ la gravité de l'impact sur le SI
 - ▶ gravité d'une attaque potentielle
 - ▶ niveau technique estimé pour réaliser l'attaque

Logigramme d'un test



4 phases



- ▶ **Phase 1** : reconnaissance active et passive
- ▶ Phase 2 : énumération et cartographie
- ▶ Phase 3 : recherche de vulnérabilités
- ▶ Phase 4 : exploitation des vulnérabilités

4 phases



- ▶ **Phase 1** : reconnaissance active et passive
- ▶ **Phase 2** : énumération et cartographie
- ▶ Phase 3 : recherche de vulnérabilités
- ▶ Phase 4 : exploitation des vulnérabilités

4 phases



- ▶ **Phase 1** : reconnaissance active et passive
- ▶ **Phase 2** : énumération et cartographie
- ▶ **Phase 3** : recherche de vulnérabilités
- ▶ **Phase 4** : exploitation des vulnérabilités

4 phases



- ▶ **Phase 1** : reconnaissance active et passive
- ▶ **Phase 2** : énumération et cartographie
- ▶ **Phase 3** : recherche de vulnérabilités
- ▶ **Phase 4** : exploitation des vulnérabilités

Automatisation ?

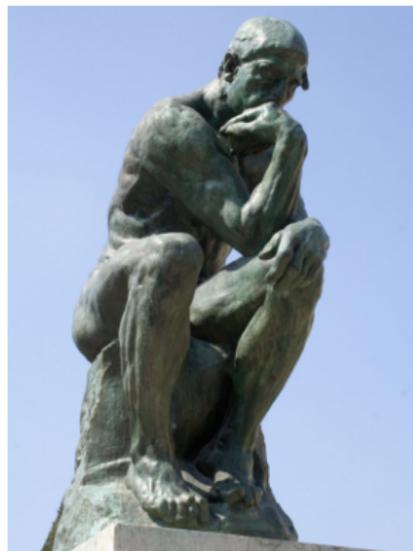
Constats

- ▶ Augmentation du nombre de demandes de tests
- ▶ Ressources en experts insuffisantes
- ▶ Durée d'un test relativement longue
- ▶ Travail sur un environnement en production
- ▶ Grande diversité des SI

Conséquence

Besoin de gagner du temps

Possibilité d'automatiser certaines parties du test ?



Automatisation ?

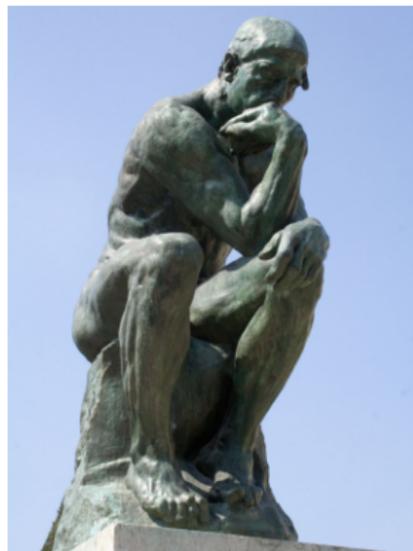
Constats

- ▶ Augmentation du nombre de demandes de tests
- ▶ Ressources en experts insuffisantes
- ▶ Durée d'un test relativement longue
- ▶ Travail sur un environnement en production
- ▶ Grande diversité des SI

Conséquence

Besoin de gagner du temps

Possibilité d'automatiser certaines parties du test ?



Automatisation ?

Constats

- ▶ Augmentation du nombre de demandes de tests
- ▶ Ressources en experts insuffisantes
- ▶ Durée d'un test relativement longue
- ▶ Travail sur un environnement en production
- ▶ Grande diversité des SI

Conséquence

Besoin de gagner du temps

Possibilité d'automatiser certaines parties du test ?



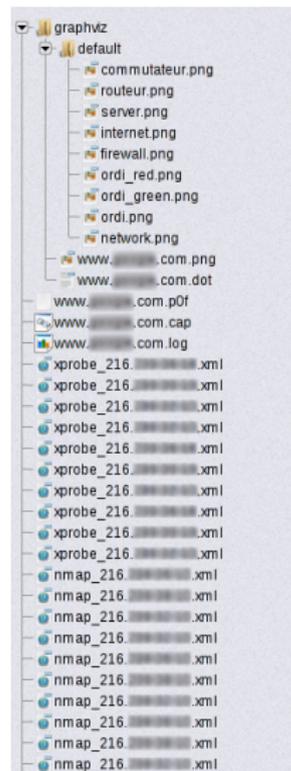
Description de reconet

RECONET

- ▶ automatisation des phases 1 et 2
- ▶ logiciel écrit en python
- ▶ cartographie du réseau étudié
- ▶ fichier de logs détaillé

Résultats obtenus

- ▶ un fichier de log
- ▶ un fichier HTML généré par netcraft
- ▶ fichiers `nmap` & `xprobe`
- ▶ un fichier généré par `p0f`
- ▶ un fichier de capture `tcpdump`
- ▶ un fichier `graphviz`



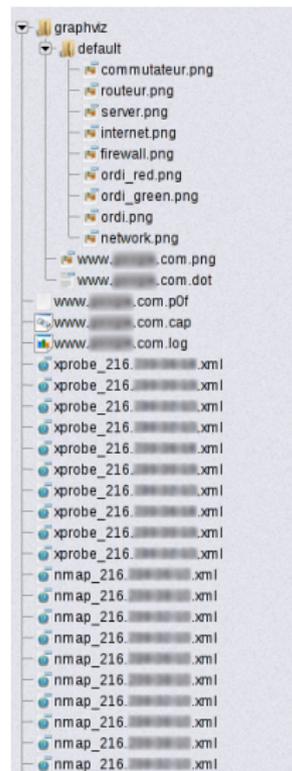
Description de reconet

RECONET

- ▶ automatisation des phases 1 et 2
- ▶ logiciel écrit en python
- ▶ cartographie du réseau étudié
- ▶ fichier de logs détaillé

Résultats obtenus

- ▶ un fichier de log
- ▶ un fichier HTML généré par netcraft
- ▶ fichiers **nmap** & **xprobe**
- ▶ un fichier généré par **p0f**
- ▶ un fichier de capture **tcpdump**
- ▶ un fichier **graphviz**



Détails...

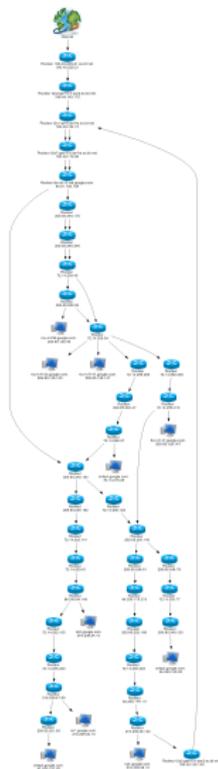
Ligne de commande :

```
# ./reconet.py
Michel Dubois -- reconet.py -- (c) 2007
Syntaxe:      reconet.py [-h -v] -s <server>
Options:     -h [--help]      affichage de l'aide
             -v [--verbose]  mode verbose
             -s [--server]   URL du site Web

# ./reconet.py -v -s www.google.com
```

- ▶ **initialisation** de l'environnement
- ▶ test de la **présence** des utilitaires
- ▶ lancement **tcpdump** & **p0f**
- ▶ énumération : DNS, **whois**, **netcraft**, transfert de zones, balayage de préfixes communs, scan plage d'adresses IP
- ▶ Fingerprinting : **nmap**, **xprobe2**
- ▶ **scan** de ports
- ▶ **traceroute** ICMP et TCP
- ▶ construction de la carte (**graphviz**)

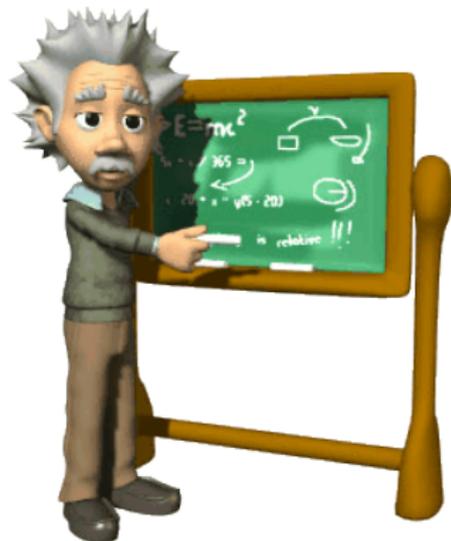
Détails...



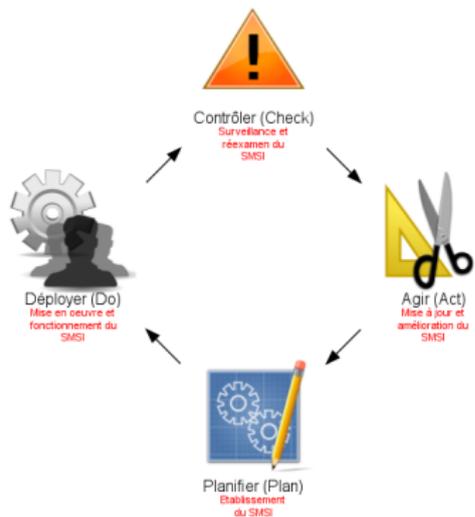
- ▶ Scan **nikto**
- ▶ Timestamp TCP, prédictibilité id IP (**hping**)
- ▶ Recherche bannière TCP, robots.txt (**netcat**)
- ▶ Recherche méthode HTTP autorisées, retour méthode GET,...

EvaSMSI

- 2 EvaSMSI
 - ISO 27001 & SMSI
 - l'application EvalSMSI



Objectifs



ISO 27001 *Source HSC*

Il s'agit de spécifier les **exigences** pour

- ▶ mettre en place
- ▶ exploiter
- ▶ améliorer

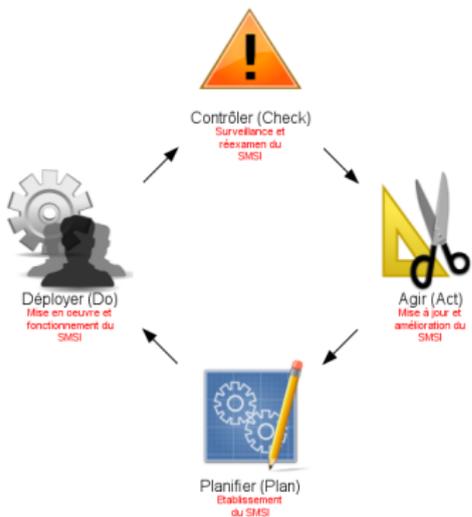
un **SMSI**

SMSI *Source HSC*

Un système de management est un système permettant

- ▶ de définir une politique
- ▶ d'établir des objectifs
- ▶ d'atteindre ces objectifs

Objectifs



ISO 27001 *Source HSC*

Il s'agit de spécifier les **exigences** pour

- ▶ mettre en place
- ▶ exploiter
- ▶ améliorer

un **SMSI**

SMSI *Source HSC*

Un système de management est un système permettant

- ▶ de définir une politique
- ▶ d'établir des objectifs
- ▶ d'atteindre ces objectifs

Justification

Faciliter les opérations d'**audit interne** et de **suivi des actions** liées au management de la sécurité de l'information.

Evaluation du Système de Management de la Sécurité de l'Information

L'objectif de ce questionnaire est d'évaluer, par rapport à un référentiel précis, le système de management de la sécurité de l'information (SMSI).

L'approche processus pour le management de la sécurité de l'information incite ses utilisateurs à souligner l'importance de:

- la compréhension des exigences relatives à la sécurité de l'information d'un organisme, et la nécessité de mettre en place une politique et des objectifs en matière de sécurité de l'information;
- la mise en oeuvre et l'exploitation des mesures de gestion des risques liés à la sécurité de l'information d'un organisme dans le contexte des risques globaux liés à l'activité de l'organisme;
- la surveillance et le réexamen des performances et de l'efficacité du SMSI;
- l'amélioration continue du système sur la base de mesures objectives.

C'est le modèle de processus Planifier - Déployer - Contrôler - Agir (PDCA) qui est appliqué à la structure des processus du SMSI.

EvalSMSI version 2.0 -- 18/02/2009



Accès établissement



Statistiques et rapports



Administration



Aides et documentations

[Accueil](#)

Fonctionnement — évaluation interne par questionnaire

Evaluation du Système de Management de la Sécurité de l'Information

[Se déconnecter \(mjeanne\)](#)

Evaluation de *Société number one - Division finance* pour l'année 2009

19%

- 1 Politique de sécurité de l'information +
- 2 Organisation de la sécurité de l'information +
- 3 Gestion des actifs +
- 4 Sécurité liée aux ressources humaines +
- 5 Sécurité physique et environnementale +
- 6 Gestion de l'exploitation et des télécommunications +
- 7 Contrôle d'accès +
- 8 Acquisition, développement et maintenance des systèmes d'information +
- 9 Gestion de la continuité de l'activité +

1: Non Applicable

La question est sans objet.

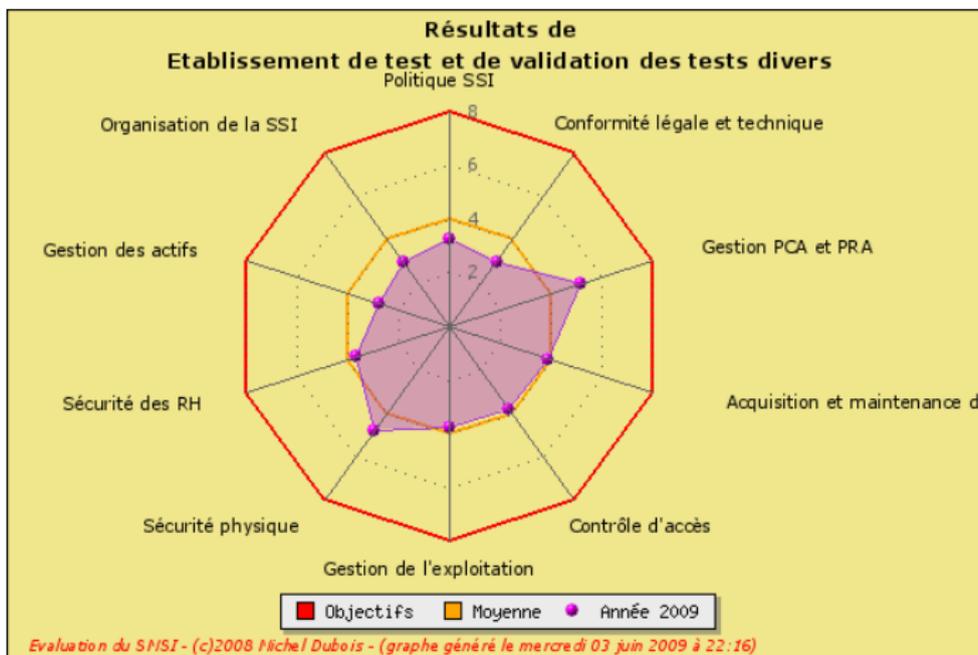
2: Inexistant et investissement important (Inexistant pour longtemps)

La disposition proposée n'est pas appliquée actuellement et ne le sera pas avant un délai important (mesure non planifiée, mesure nécessitant une étude préalable importante, mesure nécessitant un budget important, etc.).

3: Inexistant et investissement peu important (Inexistant)

La disposition proposée n'est pas appliquée actuellement, mais le sera rapidement, car sa mise en oeuvre est facile et/ou rapide.

Fonctionnement — génération de graphes



Fonctionnement — tableau de bord évaluateur

Evaluation du Système de Management de la Sécurité de l'Information - Statistiques et tableaux de bords

[Se déconnecter \(mdubois\)](#)



Graphes par établissement



Evaluation auditeur



Synthèse globale



Evaluation établissement de
regroupement



Journalisation



Rapport par établissement

[Accueil](#)

Fonctionnement — génération automatique de rapport

Rapport d'évaluation du Système de Management de la Sécurité de l'Information Etablissement de test et de validation des tests divers

Michel Dubois – RSSI

3 juin 2009



Résumé

Ce rapport décrit le résultat de l'évaluation du Système de Management de la Sécurité de l'Information (SMSI) réalisé par l'établissement de test et de validation des tests divers en 2009. L'évaluation initiale a été contrôlée le 3 juin 2009 par Michel Dubois – Responsable Sécurité des Systèmes d'Information (RSSI). Cette évaluation repose sur un questionnaire établi conformément aux normes ISO 27001 et ISO 27002.

- Directeur de l'établissement : Monsieur Jean Aymard de la si
- RSSI de l'établissement : Monsieur Louis Dupont

Fonctionnement — administration de l'application

Evaluation du Système de Management de la Sécurité de l'Information - Administration

[Se déconnecter \(mdubois\)](#)



Ajouter un paragraphe



Créer un établissement de
regroupement



Ajouter un sous paragraphe



Créer un établissement et/ou
une évaluation



Ajouter une question



Modifier un établissement



Modifications / Suppressions
Paragraphe, sous-paragraphes,
questions



Maintenance de la Base de
Données

Questions ?

