

## Scapy : vers une documentation ?

Jean-Philippe Gaulier  
jpgaulier@point-libre.org

5 juin 2008



# Plan

- 1 Mais qu'est ce que c'est ?
- 2 L'auteur
- 3 État de l'art de la documentation
  - Avant la documentation
  - Un ouvrage, un chapitre
  - Des petits bouts
  - Un article
  - Une documentation non officielle sur le site officiel
- 4 Merci



Scapy est un outil écrit en python qui peut servir comme :

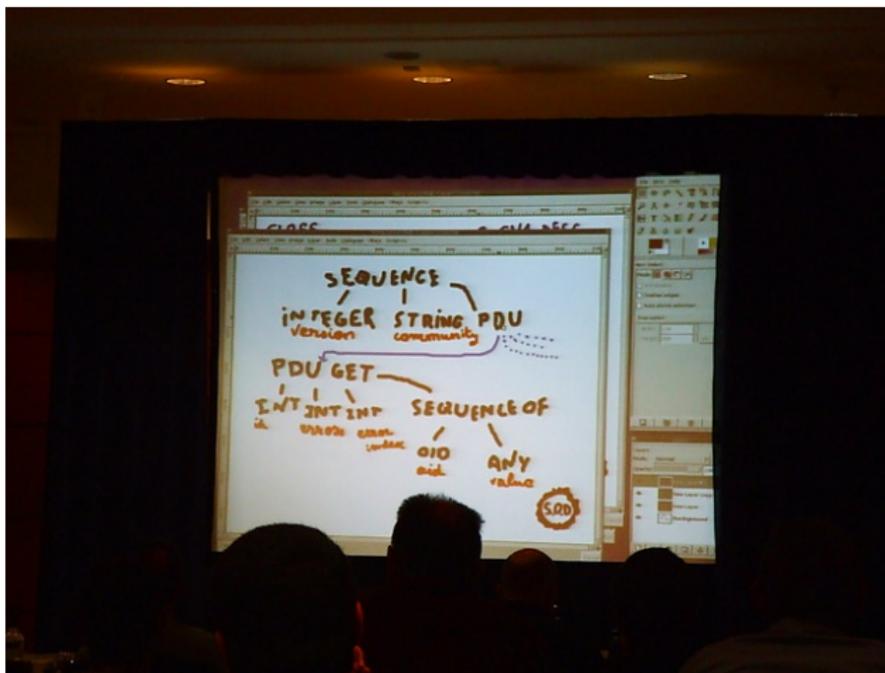
- forger de paquet,
- outil d'analyse,
- outil de test,
- scanner,
- prise d'empreinte,
- outil d'attaque. . .

Pas de feature sur le café à ce jour, mais. . .



Mais qu'est ce que c'est ?  
**L'auteur**  
État de l'art de la documentation  
Merci





©Cédric « Sid » Blancher



Mais qu'est ce que c'est ?  
L'auteur  
État de l'art de la documentation  
Merci

Avant la documentation

Un ouvrage, un chapitre

Des petits bouts

Un article

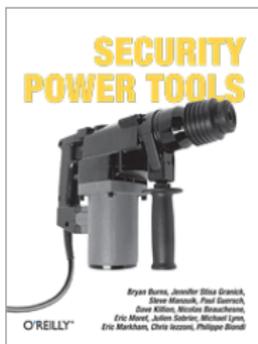
Une documentation non officielle sur le site officiel

# BOFH style



+





- Un livre de 848 pages sur les outils de sécurité,
- un chapitre complet sur scapy,
- pas de traduction française. (Pensée pour O'Reilly)

Sur le site officiel, vous trouverez :

- un début de doc en pdf,
- une session interactive à Cansec,
- comment construire sa propre application avec scapy,
- comment installer scapy sur différentes plate-formes,
- un article dans linux magazine 52.

`http://secdev.org/projects/scapy/`



## Un article complet de Xavier Poli sur SecuObs, *Trames et paquets de données avec Scapy*

- Présentation
- Installation et configuration
- Utilisation basique
- Captures de données
- Traceroute et visualisation 2D/3D
- Manipulations de paquets et de trames
- Orientation et représentation objet
- Compléments et webographie

<http://www.secuobs.com/news/01102007-scapy.shtml>



- Introduction

- Qu'est ce que Scapy ?
- À propos de l'auteur

- Concepts

- Fast packet design
- Décoder n'est pas interpréter

- Nouveautés de Scapy

- Version
- Liste des protocoles supportés

- Démarrage

- Installer scapy
- Démarrer l'interface
- Liste des commandes
- Faire ma première requête
- Faire un traceroute
- Utiliser un fichier PCAP
- Qui est présent sur mon sous-réseau ?
- Un scanner de ports en quelques lignes

- Références

- Bibliographie
- Nominations

Une documentation ouverte à tous, en perpétuelle évolution, pour permettre de mettre le pied à l'étrier et d'avoir la joie d'utiliser Scapy au quotidien.

Un wiki qui permet d'avoir différents contributeurs avec du suivi de changement.

Besoin de temps cerveau pour retransmettre de manière pédagogique l'outil vers le français.



Mais qu'est ce que c'est ?  
L'auteur  
État de l'art de la documentation  
Merci

Avant la documentation  
Un ouvrage, un chapitre  
Des petits bouts  
Un article  
Une documentation non officielle sur le site officiel

Une seule adresse à retenir :  
<http://trac.secdev.org/scapydoc-com>



- Philippe pour Scapy au quotidien et sa confiance dans le travail
- Sid pour avoir toujours de belles photos des confs dans le monde entier (plus que cinq ans pour la carte platinum...)
- les retours des utilisateurs
- Wikipedia pour le python
- Google pour les photos de manière générale

## Questions ?

