



OSSIR – 12/10/2004



EdelWeb

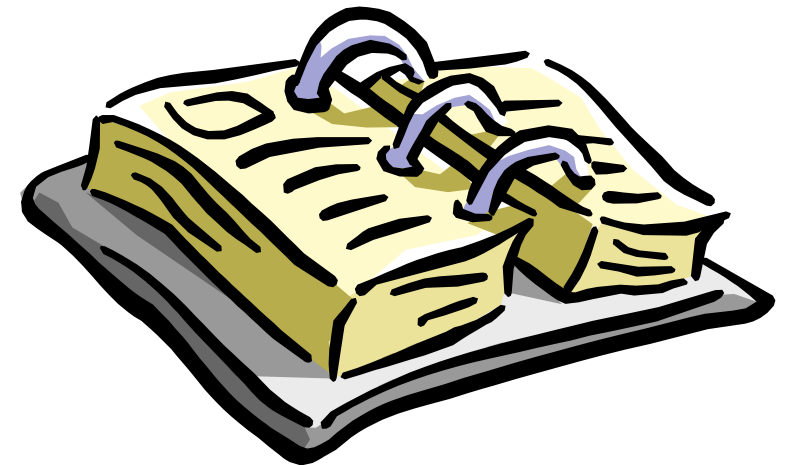
Compte-rendu BlackHat USA et DefCon 2004



Patrick CHAMBET

patrick.chambet@edelweb.fr
<http://www.chambet.com>

- **BlackHat USA**
 - Participants / ambiance
 - Présentations intéressantes
- **DefCon 12**
 - Participants / ambiance
 - Présentations intéressantes
- **Conclusion**



BlackHat USA 2004



EdelWeb

- **Environ 1500 participants**
- **Public « corporate »**
- **7 Français**
 - **Dont 2 speakers**

Ambiance



- **Plusieurs grand thèmes**
 - **Application security**
 - **Computer forensics and log analysis**
 - **Privacy & anonymity**
 - **0-day attack**
 - **0-day defense**
 - **Layer 0 (support physique / matériel)**
 - **Policy, management and the law**

Présentations remarquables



- **Metasploit**
 - La version 2.2 de l'outil est diffusée
 - Nombreux exploits et shellcodes nouveaux
 - Framework puissant permettant d'assembler les différents éléments
 - Exploits
 - Charges utiles
 - Encodeurs
 - Vecteurs
 - Injecteurs
 - Démo impressionnante
 - <http://www.metasploit.org>

- **VICE – Catch the Hookers !**
 - Hooking d'APIs Windows
 - Runtime code patching
 - Direct Kernel Object Manipulation (DKOM)
 - Diffusion d'une nouvelle version de l'outil VICE (démonstrations de techniques de rootkits): impressionnant !
 - Cache des processus
 - Ajoute des privilèges aux tokens
 - Ajoute des groupes aux tokens
 - Trompe l'Event Viewer
 - Cache des ports
 - Patche le kernel Windows

Présentations remarquables



- **Nobody's anonymous – Tracking spam and covert channels**
 - Curtis Kret analyse tout le spam qu'il a reçu depuis plusieurs années
 - Il arrive à identifier les spammeurs individuellement et à reconstruire leurs communications et leurs dialogues
 - Spam utilisé comme covert channel !
- **Cyber Jihad and the globalization of warfare**
 - Etude historique des attaques informatiques entre Israéliens et Palestiniens
 - Prétendent qu'il s'agit de la première cyber-guerre
 - Description de la stratégie et du choix des cibles des 2 camps
 - Dérive vers les attaques Chine / USA
 - Cette présentation a eu beaucoup de succès

Autres thèmes abordés



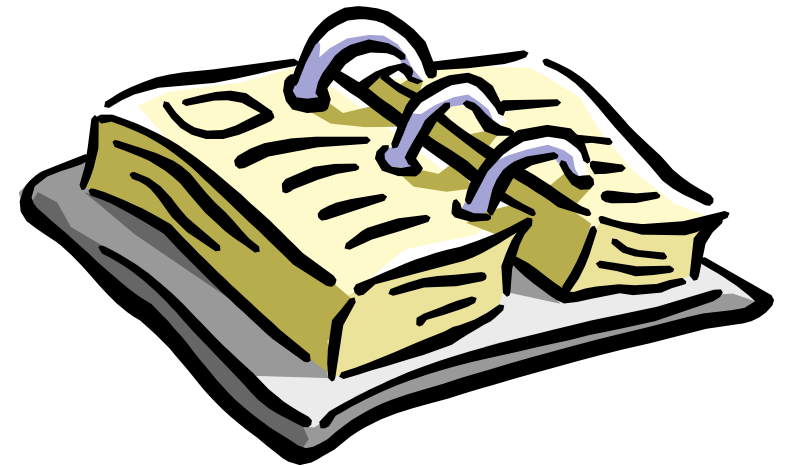
- **Honeypots (Laurent Oudot)**
 - **Contre-mesures depuis un honeypot**
- **Google hacking**
 - **Très à la mode actuellement**
- **Dé-périmétrisation**
 - **Concept fumeux de Paul Simmonds**
 - **Ne propose pas de recommandations**
- **Web applications**
 - **Sécurisation**
 - **Détection et évacion d'attaques (rien de neuf)**

- **Attaques DNS**
 - Outils amusants de Dan Kaminski (flux audio over DNS !)
 - Mais attaques anciennes, rien de nouveau
- **Sans fil**
 - Sécurisation Wifi
 - Attaques BlueTooth (« blue snarfing »)
- **RF-IDs**
 - Outil permettant de lire et d'écrire dans les RF-IDs !

- **BlackHat USA**
 - Participants / ambiance
 - Présentations intéressantes

- ✓ • **DefCon 12**
 - Participants / ambiance
 - Présentations intéressantes

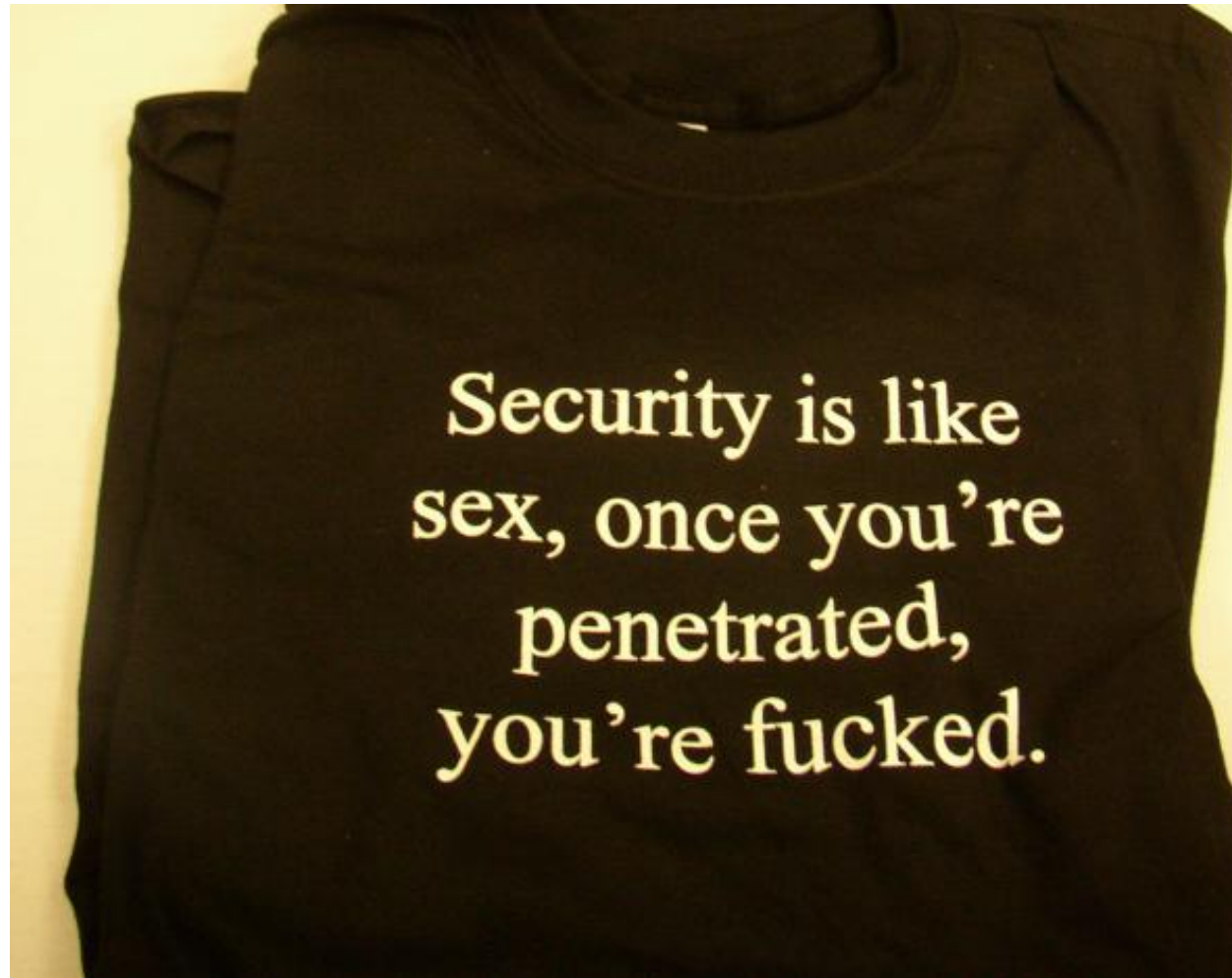
- **Conclusion**



-
- **Environ 5000 participants**
 - **Public de « geeks » mais également grand public**
 - **Plus les Feds**
 - **Environ une dizaine de Français**
 - **Dont 1 speaker**

Ambiance



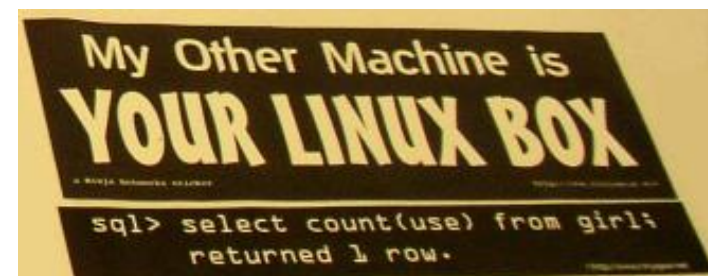


- **Beaucoup de reprises de présentations de BlackHat**
 - VICE
 - The first international cyber-war
 - Information hiding in executable libraries
 - RF-IDs
 - Etc.

- **Hardware hacking**
 - Deux présentations sur le sujet
 - Scott Fullam
 - Joe Grand



- **Présentation conjointe de FX et Halvar Flake sur la découverte de 0-days**
 - Méthode générique de découverte de bugs
 - Moins technique que prévu...
- **Wireless weaponry**
 - Le groupe Shmoo a présenté un ensemble d'outils software et hardware (« fusil » Wifi) pour le wardriving
- **Honeypots**
 - NoSEBrEaK (anti-honeypot)
 - Contre-mesures (Laurent Oudot)



- **Les réseaux automobiles embarqués**
 - Commence à être un sujet d'étude
- **Autres**
 - Attaques VoIP
 - Blind SQL injection (outil SQueal)
 - Attaques des Pocket PCs
 - Sécurité de Mac OS X Server
 - Sécurisation d'Apache
 - Présentation traditionnelle des « Feds » et... « Catch the Fed » !



- **Wifi contest**
 - **Record du monde de portée Wifi : 55 miles !
(antenne maison: 3 m de diamètre !)**
- **Catch the flag**
 - **Règles intelligentes: attaque + défense**
 - **Certainement le niveau le plus haut du DefCon !**
 - **Une équipe française l'an prochain ?**

Conclusion

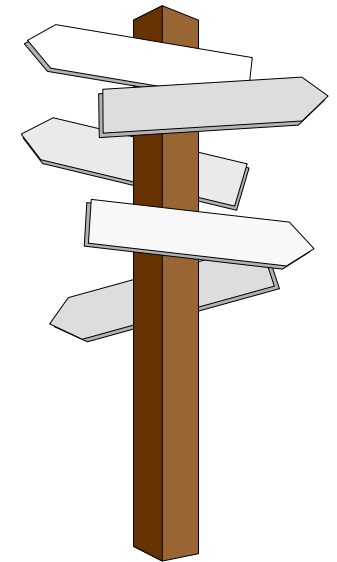
- **Niveau général**
 - **BlackHat: bon**
 - **DefCon: un peu décevant**
- **Mais excellent pour prendre la température de la « scène » et montrer que les Français ne sont pas absents**
- **Quelques perles techniques au milieu de beaucoup de bruit, qui valent le déplacement**

- **BlackHat**

- <http://www.blackhat.com>
- Archives USA 2004:
<http://www.blackhat.com/html/bh-media-archives/bh-archives-2004.html#USA-2004>

- **DefCon**

- <http://www.defcon.org>
- Archives 2004:
<http://www.defcon.org/html/links/defcon-media-archives.html#dc-12>
- <http://www.defconpics.org>



Bonus slide



Questions

