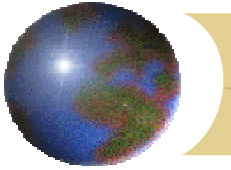


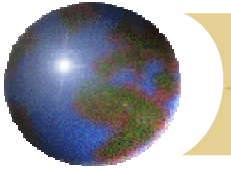
28e Conférence annuelle CSI Computer Security Institute Washington du 29 au 31 Octobre 2001

Patrick MORRISSEY
Ingénieur ESME
Ancien élève ESCP
CIA – CISA - CISSP
pmorrissey@auditware.net



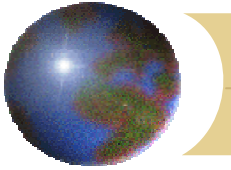
Participation à la conférence

- 1. Objectifs = apprendre, mesurer l'écart (?), appréhender l'avenir, évaluer l'impact des attentats du 11 septembre**
- 2. L'environnement de la conférence**
- 3. Méthodes d'évaluation de la sécurité des SI**
- 4. Démonstrations à sensation**
- 5. Bruits de couloir...**
- 6. Ressources**
- 7. Conclusion**



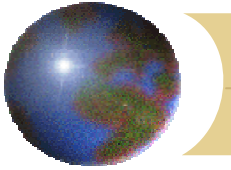
1. Les objectifs de participation

- Les américains sont ils nettement plus forts que nous ?
- De facto ils sont plus souvent attaqués que nous
- Ce qui leur arrivent aujourd'hui sera probablement chez nous demain (24H à 6 mois)
- Quelle communauté ?
 - Soixante-huitards attardés, anarchistes, Businessman ?



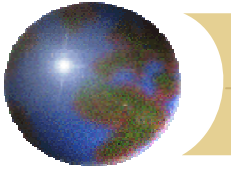
2. *L'environnement*

- MARRIOTT Washington = élimination des "pauvres"
- 2500 personnes – 175 stands (en période de post attentats !)
- Organisation américaine
- T shirts à tous les stands, loteries, (pas de pompom girls)
- Population mélangée = soixante huitards, cheveux blancs katogan & costumes cravates...
- Niveau variable des intervenants = ils ne sont pas tous top !



3. Les méthodes d'évaluation

- Les américains ne semblent pas plus avancés que nous
- Conflit marché libre vs "supervision" par l'Etat
- Obligation HIPAA (domaine médical) (Vitale en France)
- Obligation GLBA (Directive 97.02 / Ets financiers)
- Loi GRAMM-LEACH-BLILEY sur Privacy votée été 2001
- Une loi serait en cours de vote pour donner une prime (ou un avantage fiscal à toute entreprise prouvant avoir mis en place des dispositifs anti cyberterrorism.
- Ref citées dans la salle = ISO 17799, ISO 15408 (Common Criteria), SAS 70 (Experts Comptables US + CN)



4. *Démos à sensation*

🌀 Bunratty attack

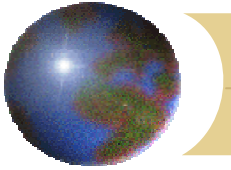
- ▣ MAPI sous Windows
- ▣ Invisible

🌀 Forensics

- ▣ Récupération de toutes traces d'enregistrement sur un support
- ▣ Démo logiciel ENCASE

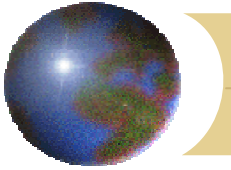
🌀 2 sessions UNIX

- ▣ Hacking UNIX
- ▣ Securing Apache



5. Bruits de couloir

- ⊕ Tripwire ou similaire
- ⊕ "Hantise" du logiciel packagé vs logiciel libre
- ⊕ Devons-nous décompiler toutes les applis et OS ?
 - ⊕ Sommes nous en fraude si nous le faisons ?
- ⊕ Un IDS sans analyste IDS = presque zéro
- ⊕ OpenSSH plutôt que SSH commercial
- ⊕ La méfiance envers notre voisin va-t-elle perdurer ?
- ⊕ Forte utilisation de l'ingénierie sociale



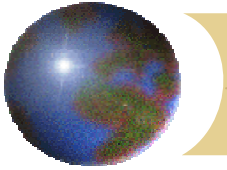
6. *Ressources*

✚ Revues papiers

- ✚ CSI journal (www.gocsi.com)
- ✚ Information security (www.infosecuritymag.com)
- ✚ International journal of information security (www.spinger.de)
- ✚ Infoscurity magazine (www.infosecnews.com)

✚ Livres

- ✚ RSA Press
- ✚ "Hacking exposed" 3e édition Mac Graw Hill ISBN 0.07.219381.6
- ✚ "Tanged Web" QUE ISBN 0-7897-2443-X



7. Conclusion

- Très riche en un espace temps court
- Beaucoup de logiciels arrivent sur le marché US
= bientôt en France... Quel marché ?
- Encore assez (trop ?) affaires de techniciens
- Partage entre expliquer les failles et à qui les expliquer
(syndrome du 11 septembre ?)

**Expérience très enrichissante à faire
au moins une fois par an ou tous les 2 ans**