Mes stats de SSTIC'08

Jean-Philippe Gaulier
jpgaulier@point-libre.org

30 juin 2008

Sujet du support : « Réconforter » ceux qui n'ont pas pu assister à SSTIC'08. Montrer la diversité des thèmes abordés, donner une idée de l'ambiance, renvoyer vers les actes et les présentations en ligne.

Cet article est issu du blog de Jean-Philippe Gaulier[1], il accompagne la présentation faîte pour l'OSSIR Bretagne, le 17 juin 2006.

Direction Beaulieu, capitale française de la sécurité pour trois jours. Arrivée matinale afin de ne pas devoir subir la même file d'attente qu'à la poste. C'est payant, à peine cinq minutes pour récupérer le badge, les tickets du resto U, les actes et deux stickers. Je retrouve mes camarades d'INL[2] ainsi que Christophe Grenier[3]. Nous ne nous quitterons plus jusqu'à la fin du SSTIC. Belle tablée d'étudiants, s'il en est.

[1] `http://jp.gaulier.info/blog/`
[2] `http://www.inl.fr`
[3] `http://www.cgsecurity.org`

1 JOUR I

SSTIC commence officiellement, avec quelques mots du président, Philippe Biondi[4] qui paraphrase quelque peu sa préface des actes. On enchaîne[5] avec un Marcus Ranum[6] en chair et en os. C'est un grand plaisir pour moi de rencontrer un de ceux que je considère comme un "père spirituel" en matière de sécurité informatique. Je m'assieds au fond de mon siège à rabat et m'attend à en prendre plein les oreilles pendant une heure pour une conf... en français. Stupeur. Ranum nous fait l'honneur de parler entièrement dans la langue de Molière, avec l'assistance, d'après lui, de Google Translator. Je pense que l'outil a dû faire bien des progrès depuis la dernière fois que je m'en suis servi, parce Marcus n'a pas fait énormément de fautes. Par contre, pas toujours facile de suivre à jeun, un mercredi matin. Ce qu'il faut retenir, en substance, *c'est que la plupart des gens préfèrent conserver leur travail, plutôt que d'avoir raison.* De manière générale, la sécurité est une matière ingrate, on ne fait que la blâmer pour les pertes, mais on est incapable d'en retirer les bénéfices. En prenant un peu de recul, le sinistre informatique a déjà eu lieu, car on ne définit pas si une attaque sur les infrastructures va survenir, on essaye plutôt de savoir quand cela va arriver. Et tout cela n'est que la conséquence d'une seule et même entreprise : *la mauvaise idée*. En effet, c'est elle qui grandit et que l'on n'a pas su tuer assez tôt. On pourrait symboliser cette catastrophe sous la forme suivante :

Naissance de la mauvaise idée $\rightrightarrows$ partage de la mauvaise idée par mail (preuve) $\rightrightarrows$ mise au courant de la direction $\rightrightarrows$ attente de la direction vis à vis de cette idée (ROI) $\rightrightarrows$ rencontre de DSI $\rightrightarrows$ mise en place de la mauvaise idée.

Certaines étapes sont optionnelles, mais le résultat est toujours là, si vous ne tuez pas la mauvaise idée à sa naissance, une fois implémentée, vous aurez à peu près autant de chance que ce qu'est la limite de un sur x, lorsque cette variable tend vers l'infini...

On parle de sécurité, mais c'est plus une question de réalité à laquelle il faut revenir. En effet, pourquoi transportez-vous des données confidentielles sur des laptops alors même que vous vous trimballez dans un aéroport ? Il faut revenir sur terre. Les désastres informatiques vont être énormes et notre tâche relève de l'accomplissement de l'impossible. Pour employer la métaphore, on sait que les voyages dans l'espaces sont dangereux, pourtant, on continue encore et toujours la recherche dans ce domaine, tout simplement parce qu'il n'y a pas eu encore de désastres, seuls quelques "catastrophes", si vous me passez l'expression. Internet est à l'image des voyages dans l'espace, c'est un *miracle* que cela fonctionne.

En conclusion, Ranum avancera qu'avec le web, nous étions au bord du gouffre, avec le web 2.0, nous avons réussi à faire un grand pas en avant...

Du très bon, comme je le disais.

[4] `http://www.secdev.org`
[5] `http://actes.sstic.org/SSTIC08/Anatomy_Security_Disasters/`
[6] `http://www.ranum.com/`

On continue sur l'intervention[7] de Michel Iwochewitsch qui ne parlera de rien d'autre que de Social Engineering (aïe, pas la tête). Sujet supra sexy, surtout pour moi qui travaille depuis longtemps sur la question. Je n'ai pris que quelques notes car il est indispensable de recourir au support tellement il y a de références à des méthodes et des acronymes. Ce qu'on pouvait tout de même noter c'est qu'il y a deux angles d'attaque ; le "one shot" et le "long terme". Les cibles sont variées, telle que l'argent, l'intégrité de l'information, la confidentialité, la disponibilité, la nuisance, la valeur d'opposition... Il y a deux modes d'exploitation de l'être humain :

- exploiter une faille pour obtenir un effet,
- utiliser un outil afin de mieux appréhender l'autre.

Il y a des boutons universels qui nous font tous chavirer. La phrase à retenir semble être que

> Pour les russes, le cerveau est comme un système d'information sans pare-feu.

Je n'attendais vraiment rien du talk de gemalto[8] étant habitué à leurs obscures déviances cryptographiques. J'ai donc été plus qu'agréablement surpris de faire face à une conf qui a su me passionner. On y parle de carte sans contact, mais également la capacité de créer des tunnels pour se servir de votre carte pour acheter des tickets de métro, ouvrir votre voiture, etc. Une vidéo devrait figurer dans les actes, elle n'a pas eu le temps d'être jouée pendant la conf, *trop de pression*.

L'heure du repas, direction le RU. Je sais de manière sûre que ce n'est pas ce que je regrette de ma période de travail à l'université, encore aujourd'hui. Rendez-moi le resto de supélec ;-)

David Naccache s'est fendu d'un papier en anglais pour une conférence en français[9]. Ça aurait dû me mettre la puce à l'oreille. Je n'ai rien n'appris, rien vu d'innovant, si ce n'est que de réussir à placer un HS pendant plus de vingt minutes sur des thermo bugs, dont je serai réellement curieux de voir l'application dans le monde réel. Un covert channel par la chaleur, je suis sûr que vous voyez, vous aussi, la correspondance directe avec l'expertise judiciaire des téléphones mobiles. Pour ma part, ça ne m'a pas frappé !

C'est moutane[10] qui se coltinera l'avant-pause de l'après-midi avec une comparaison entre les outils phares du marché d'analyse de faille : CORE IMPACT, Immunity CANVAS et Metasploit Framework. Rien de bien nouveau, mais ça

[7] `http://actes.sstic.org/SSTIC08/Identification_Exploitation_Failles_Humaines/`

[8] `http://actes.sstic.org/SSTIC08/Activation_Cartes_Puce_Sans_Contact_Insu_Porteur/`

[9] `http://actes.sstic.org/SSTIC08/Law_Enforcement_Forensics_Mobile_Communications/`

[10] `http://moutane.rstack.org/`

permet de refaire un point sur l'état de l'art. Il évoquera quelques contre mesure face à ces outils : la mise à jour des systèmes (qui a dit le saint graal en prod ?), les I[PD]S, le confinement par des pots de miel (on sent l'enseignement Oudot ;)) et la contre attaque, quoi que celle-ci ne soit pas très légale en France.

Après la pause, et non, je ne parlerai ni des litres de jus d'orange, ni de la centaine de pains au chocolat (mini quand même), c'est Loïc Duflot qui entame cette dernière partie avec les bogues sur les processeurs[11]. Pas beaucoup de notes, je vous renvoie aux actes.

On continue avec l'autopsie d'un banker[12], de son doux nom Anserin. Étude forte intéressante qui vient compléter la présentation de Franck Veysset à l'OSSIR Bretagne[13], ainsi que celle qui viendra deux jours plus tard de Guillaume Arcas. Conférence intéressante, sujet passionnant. Il semble pourtant que le même sujet avait été proposé deux années auparavant, sans avoir été accepté. Serait-ce que tout cela devient moins sensible ? On en retient une chose importante en tous cas. Tout le monde est d'accord, les anti-virus en tant que tels sont inutiles. Il en résulte deux questions : comment se passer de cette industrie et quelle réponse positive apporter pour faire avancer le schmilblick.

La dernière conférence marquera le début du cycle YaFD (Yet another Fucking Debugger). Un taf intéressant[14] de la part de l'équipe du CELAR, mais qui n'est pas publié et où la documentation réside dans le *.h*. Toute similitude avec un outil en python serait complètement fortuite.

La première journée s'achève sur un petit buffet bien sympathique, avant de rentrer à la maison, manger un bout, puis sortir arpenter les –bars– rues de Rennes à la recherche de participants.

2 Jour II

Il faut être là tôt, on ne badinne pas. La première conf s'inscrit à neuf heure, autour des green datacenter et de leur sécurisation. J'ai commencé avec la ferme intention de prendre beaucoup de notes. Mon papier se résume ainsi :

- il faut une double alimentation,
- il faut une double ventilation.

Heureusement pour moi, notre speaker a introduit de superbes simulations de fluide (ventilation, aération, écoulement...) dans ses schémas. Travaillant au quotidien dans un datacenter, je n'y ai trouvé aucun intérêt, encore moins pour

[11] `http://actes.sstic.org/SSTIC08/Bogues_Piegeages_Processeurs_Consequences_Securite/`

[12] `http://actes.sstic.org/SSTIC08/Autopsie_Observations_Banker/`

[13] `http://www.ossir.org/bretagne/cr/20080408.shtml`

[14] `http://actes.sstic.org/SSTIC08/GenDbg_Debogueur_Generique/`

la partie sécurité présente dans le titre[15]. On saluera tout de même l'initiative du comité de programme de vouloir introduire de la sécurité physique dans les topics. Vivement qu'on ait un peu de lock picking[16].

Après tant d'entrain et le regret de ne pas être resté dormir quelques minutes de plus à la maison, on enchaîne sur la déprotection semi-automatique de binaire. C'est une autre bonne surprise pour moi. Je m'attendais encore à un outil qui promettait monts et merveilles et qui ne verrait jamais le jour sinon dans quelques milieux non autorisés et au final, on voit un travail concret, partant de metasm[17] et faisant de jolis graphs, tout comme le ferait IDA. Contrairement à ce dernier, d'ailleurs, l'idée est d'interpréter le code afin d'enlever une part de l'obfuscation volontairement générée (si vrai alors i=1 sinon i=0 ;). Conf intéressante, je n'ai pas encore lu le papier, mais je pense qu'il y a matière.

S'ensuit la pause avec le jus d'orange, les petits pains au chocolat, toussa... Puis la présentation d'ERESI par Anthony Desnos et Sébastien Roy. Première question qui me vient à l'esprit : mais où est Julien Vanegue alors qu'il est invité par le comité pour la présentation ? Absent ou présent, je ne saurai pas dire. Il existe deux types d'analyse : statique et dynamique. ERESI fait les deux, mais on ne nous présentera que la deuxième solution. Ce que j'en ai retenu, c'est que ça embarque du script, des bibliothèques et des API, que c'est dispo sur plusieurs architectures (IA32, Sparc, MIPS) et pour plusieurs environnements (linux, BSD, Solaris). Je suis ressorti de tout cela avec un avis plutôt mitigé. L'outil a l'air bon mais les speakers, sûrement très fort en assembleur ont quelques progrès à faire pour hypnotiser l'audience.

Énorme déception de ne pas voir Fred Raynal[18] et Éric Filiol se présenter au parloir pour le talk suivant. Ils ont collaboré à l'article, mais c'est le troisième auteur qui parlera. Trop complexe pour moi, dans un état de fatigue avancé, je n'en retiens que les deux exemples de la conf. Après une analyse d'un soft en java à partir de l'outil, un élément essentiel : sur mac, les mots de passe sont en clair dans la mémoire et dans le fichier de mise en veille (et j'obtiens par là de quoi fermer le claquos de tous les mackeus qui me fatiguent avec une soi disant faille openssl dans un paquet Debian).

Retour au Résidu Universitaire. Je découvre que le requin, c'est bon. Mais il parait que ce n'est pas éthique. Ce n'est pas grave, ça sera sûrement diététique...

On réouvre la séance de l'après-midi avec la sécurité des capteurs. C'est encore une bonne surprise. En général, tout ce qui est puce ne me passionne pas, mais

[15] http://actes.sstic.org/SSTIC08/Etat_de_l_art_et_nouveaux_enjeux_des_green_data_centers/

[16] http://hsc.fr/ressources/presentations/crochetage_2006/index.html.fr

[17] http://actes.sstic.org/SSTIC07/Metasm/

[18] http://miscmag.com

j'avoue encore une fois avoir trouvé un grand intérêt sur cette présentation. Un réseau de capteurs est un ensemble de noeuds, ce qui signifie que tout ce bazar doit communiquer ensemble. S'occuper de sécurité quant on a des ressources illimitées, le problème se trouve dans l'humain. Lorsque l'on est dans du miniature embarqué, il faut alors gérer la consommation d'énergie, l'utilisation mémoire et sa capacité, le cpu, etc. Et là, ça devient tout de suite beaucoup plus complexe ! Par exemple, vous pouvez tout de suite oublier la crypto à clef publique. Ah, beaucoup moins évident comme problème, d'un coup. On se rapproche encore plus de la réalité lorsque l'on sait qu'un pace maker est en quelque part un capteur. Le médecin doit pouvoir communiquer avec l'outil à distance, tout en garantissant la confidentialité et l'intégrité. Imaginez un déni de service sur ce genre d'outil. Encore plus quand Dick Cheney est équipé d'une occurrence de ce bazar et que l'on découvre tout un tas de truc drôle à faire avec. Dès lors, il semble que les chercheurs publient un peu moins publiquement leurs avancées sur la question. Allez savoir pourquoi !

Nous en arrivons à un moment très attendu par le lecteur (l'unique, je parle d'ulysse) et où je me dois de faire attention, car il sera sûrement lu par le speaker, à savoir Sid[19] himself. Cédric nous propose de partager quelques minutes sur la dépérimétrisation, sujet cher à son coeur, d'autant plus que ça l'oppose sur beaucoup de point au Jéricho Forum (looser[20]) et à leur idée de supprimer le pare-feu, qui est un des outils préféré de sieur Blancher. C'est un plaidoyer sur la forme avant tout, puisque le Jericho Forum se sert du buzz pour toucher les décideurs sans avoir de véritable argumentaire cohérent. Néanmoins, Cédric n'écarte pas la question du débat qui peut être intéressante sur le fond. La sécurité doit-elle résider dans des couches basses, hautes ou les données doivent-elles être sécurisées, où qu'elles se trouvent. Ma question à Sid a été de savoir comment démonter le buzz face aux décideurs. Sa réponse converge à ce que j'en savais déjà : la démonstration de la cohérence de nos architectures et de l'absurdité des propositions du Jericho Forum. Je suis un poil resté sur ma faim, connaissant la position initial de Cédric, ainsi que les dire du Jericho Forum, j'aurai bien aimé que notre speaker enfonce plus avant le clou et passe une partie de sa présentation sur des idées, même saugrenues, c'eut été sympathique. M'enfin, en une demi-heure, le temps est aussi compté, ce que je comprends largement.

On termine les conférences officielles avec Marie Barel, nouvellement bretonne, qui, pour changer, fera une présentation juridique sur le cauchemard juridique qu'est un pentest. Pour résumé le propos : contrat, contrat, contrat. Ah oui, autre chose. Si vous n'avez pas de juriste, vous n'existez pas. Vous verrez, on s'habitue à force ;)

[19] `http://sid.rstack.org`
[20] `http://www.opengroup.org/jericho/`

Un grand moment attendu par beaucoup de monde : les rumps. Une Rump session, pour ceux qui ne connaissent pas encore le principe, c'est un talk court, sur un sujet intéressant ou pas, technique ou pas, qui s'enchaîne jusqu'à épuisement des speakers. Pour le cru 2008, c'est 22 rumps qui sont présentées. Voici l'intégralité (ou pas) :

- Olivier Heen[21] se coltine le rôle d'ouvreur avec l'annonce de C&esar du 2 au 4 décembre prochain.
- Pappy et Nico enchaînent avec le SSTIC canal historique[22] et un e-mail à ne pas manquer (langue de pute)
- Ce qui aurait pu être une conf et qui s'est transformé en rump (ou pas) par Tyop ? et un copain sur les CSRF, ou comment faire un DoS à partir de cette méthode
- NF3D, par Éric Leblond, où le Netfilter Hero[23] du parefeu
- Ludovic Mé présente une nouvelle section à supélec. Ils cherchent des stages et des sujets. Je suis intéressé pour intervenir, si quelqu'un me lit :)
- Guillaume Vissia nous présente un plug-in IDA, nommé Muff'in qui ne sera pas publié (oh my god, 0-days are real ?)
- Une présentation d'un simulateur de réseau immersif nommé Hybrid Network System (hynesym) par le CELAR, peut être à croiser avec Einar
- EAP par Gabriel Campana (?) qui a fait pas mal de recherche de vulnérabilité sur les AAA
- Sid et un joli fake sur un certificat ssl des impôts de Bordeaux, suite à la soit disant vulnérabilité GNU/Debian ;)
- Exefilter && blind FTP sont maintenant des logiciels libres
- Cracker, un crypto packer par Benjamin Caillat qui permet de faire une archive chiffrée avec une clef jetable
- Monseigneur Christophe Grenier et les avancées de photorec[24]
- Pierre "Pollux" Chifflier (INL) avec Weatherwall, où comment inviter Évelyne Dheliat pour présenter votre sécurité pare-feu
- Votre serviteur proposant un état de l'art de la documentation de scapy[25] ainsi que les projets d'évolution
- Bruno Kerouanton cherche quelqu'un à recruter en Suisse, si vous êtes intéressés. Il nous a montré à quoi servait un site de PRA lorsque, comme lui, votre ville est totalement inondée :)
- Stéphane Siacco nous a présenté succinctement un socle de sécurité[26]
- Un hack du cerveau par Nikoteen, l'ancien hacker du SMTP de l'Élysée (Ce soir j'ai les pieds qui puent, d'après Scorpion, le groupe de Rock)
- Une visualisation cubique de flux, très impressionnant dans le résultat immédiat que l'on peut en tirer

[21] `http://www.irisa.fr/lande/Olivier-Heen/Olivier-Heen.htm`
[22] `http://www.sstic-canalhistorique.org/`
[23] `http://www.guitarherogame.fr/`
[24] `http://www.cgsecurity.org`
[25] `http://trac.secdev.org/scapydoc-com`
[26] `http://www.ossir.org/bretagne/supports/2008/20080214-soc_ossirb.ppt`

– Un test de QI (euh, me souviens plus de cette rump !)

Deux rumps à suivre qui deviendront probablement des conférences :

– Daniel (mad flamby) Reynaud et Philippe Beaucamps mettent en avant de grosses faiblesses de sécurité de firefox (à suivre de très près)
– Maître Es Ruff avec HP m'a tuer où la formidable équipe que forme HP et AMD (virtualisation, mot de passe et outils...)

et pour finir :

– la spirale infernale, à propos de la faille openssl GNU/Debian supposée (auto suggestion).

C'est presque la fin de la journée, il faut déjà se rendre au Social Event, qui aura lieu comme l'année dernière au centre de Rennes, ce qui est une très bonne idée. N'ayant plus de dernier métro, je rentre à la maison à pied, ça me permet de digérer le programme de la journée.

3 Jour III

On commence avec un quart d'heure de décalage par rapport à la veille, avec un universitaire, Jonathan Rouzaud-Cornabas, doctorant à l'université d'Orléans. Le sujet a l'air intéressant, mais je n'en retiendrai que l'utilisation du framework OSSIM avec un article à regarder, car la fatigue se fait encore ressentir et il est impossible de suivre de manière posée la présentation. Dommage.

On enchaîne avec un Guillaume Arcas qui présentera un Walk On the Wild Side, une présentation très proche de celle de Frank Veysset faîte à l'OSSIR Bretagne[27] quelques semaines plus tôt. Intéressant de recouper les deux points de vue.

Ce sera ensuite à Patrice Auffret, un breton de chez nous, de présenter SinFP. J'avais déjà eu l'occasion de travailler depuis un moment sur SinFP avec Patrice. J'apprécie particulièrement l'implémentation de l'outil et son rôle de prise d'empreinte active des OS. L'idée intelligente consiste à pouvoir bypasser des pare-feux en utilisant plusieurs types d'interrogation. Une base de deux cents signatures devrait suffire pour faire le tour du monde de la prise d'empreinte. Patrice a malheureusement oublié de montrer la vidéo à la fin de sa présentation, mais également de signaler que l'outil est intégré dans Nessus. On ne peut que regretter l'accueil tiède qu'à reçu la présentation malgré un intérêt grandissant de l'outil.

C'est la Gendarmerie Nationale qui nous présentera ses papiers pour le talk suivant. Sous le patronage de Nicolas Duvinage, chef du département informatique-électronique (INL) de l'Institut de Recherche Criminelle de la Gendarmerie Nationale, nous entrerons dans le fort de Rosny afin de savoir comment se déroule

[27] `http://www.ossir.org/bretagne/supports/2008/Cybercriminalite-OSSIRB.pdf`

les enquêtes. Il s'avère que 90% des affaires ne concernent que des machines sous windows, que peu rentrent dans le cadre d'affaires judiciaires. Ce qui m'a le plus marqué, c'est qu'il semblerait que des X, des centraux ou des gadz deviennent simple gendarme pour l'honneur de servir la nation. Et dire que l'on pointe du doigt les gens du libre :)

Damien Aumaitre nous emmène dans un voyage au coeur de la mémoire. Cet ancien du master en sécurité de l'Université de Limoges travaille actuellement chez Sogeti au sein du laboratoire de recherche de Fred "pappy" Raynal. C'est une des conférence technique des plus intéressantes du SSTIC de cette année au sens où nous verrons une intrusion en live, ce qui a pas mal fait défaut cette année. C'est donc un nouveau moyen de hacker windows[28] par l'intermédiaire d'une connexion Firewire qui nous est présenté. C'est assez bluffant. Un périphérique 1394 (linux, ipod, whatever) et vous devenez administrateur. La cerise sur le gâteau, c'est que la fenêtre de logon de Windows est toujours présente. L'outil, pour des raisons de sécurité, ne sera pas publié, du moins pour l'instant. Ça rappelle le débat sur le full-disclosure...

Le début de la dernière après-midi sera sous le signe de l'administration, avec une première intervention du sous-directeur technique et scientifique de la DCSSI, Florent Chabaud. On commence par un rappel de la souveraineté de l'état qui se doit de protéger l'autonomie de décision de l'État au delà des frontières, même numériques. Cette souveraineté ne semble cependant pas être une priorité de nos hommes politiques en matière d'informatique. Pour la suite du déroulement, Chabaud reprendra les six idées les plus stupides de la sécurité informatique[29] en adaptant celles-ci à nos besoins. Il passera également sur les points forts de la recherche française (crypto et méthode formelle) ainsi que ses faiblesses (systèmes d'exploitation, protocoles réseaux et architecture matérielle). Il lance également un appel à ce secteur en soulignant le fait qu'il ne faut pas attendre l'industrie. Je terminerai l'écoute attentive par une question à notre conférencier : Ranum, dans un point/contrepoint avec Bruce Schneier, défend le fait qu'après plus de vingt ans à essayer de sensibiliser les utilisateurs par l'éducation, il n'y a que deux moyens de retenir leur attention : les humilier ou toucher à leur porte-feuille. De plus, il semble qu'avec le projet de loi Hadopi, nos politiciens soient plus sensibilisés à des intérêts de multinationales qu'à la liberté des citoyens et la souveraineté de l'état. De ce fait, ne faudrait-il pas commencer par revoir *la sensibilisation* de nos ENArques, présents et à venir ? J'obtiens un simple *oui* de mon interloccuteur ainsi qu'une belle salutation de la part de l'auditoire. Une personne très intéressante, à suivre de prêt, qui nous aura fait l'honneur de nous faire une présentation à la MIB pour excuser son costume : port de lunettes noires tout du long de sa présentation.

[28] `http://jp.gaulier.info/photos/sstic08/DSCN3640.JPG`
[29] `http://www.ranum.com/security/computer_security/editorials/dumb/`

On terminera par un habituel Philippe Lagadec de l'OTAN. Je n'assisterai pas à sa conférence, passant une partie de mon temps à discuter avec Florent Chabaud à l'extérieur de l'amphi sur des sujets qui m'intéressaient comme la manière d'améliorer toute cette sensibilisation. Je vous renvoie donc aux actes pour tout savoir sur le Dynamic Malware Analysis for dummies.

4 Conclusion

En conclusion, ce SSTIC s'est révélé d'un bon cru, liant des sujets à la fois technique, mais également organisationnel. Un petit pincement au cœur, peu d'intrusion cette année. Mais contre mauvaise fortune, bon cœur, puisque nous avons eu quasiment droit à une session pleine d'assembleur. Les organisateurs ont bien travaillé, j'en resterai sur trois remarques :

- à quand un SSTIC d'hiver ?
- Les vidéos, c'est pas peut être, mais quand ?
- Vivement les surprises de l'année prochaine (et je peux déjà dire qu'il y en aura...)

IMPORTANT :

- les actes, vous l'aurez compris, sont en ligne depuis ce soir (wahoo)
- ma rump sur scapy[30] est disponible
- Quelques photos[31], mais mon appareil et mon emplacement n'allaient pas pour choper les speakers. Je me suis donc contenté de quelques pauses et/ou situations voisines ;)

[30] `http://jp.gaulier.info/conf/doc_scapy.pdf`
[31] `http://jp.gaulier.info/photos/sstic08/`