EADS

BlackHat 2008
Defcon 2008

Observatoire
de la Sécurité
des Systèmes
d'Information
& des Réseaux

Franck.veysset@orange-ftgroup.com

Cedric.blancher@eads.net

09/09/2008

orange™

La conférence

- Las Vegas, NV, USA, 6 -> 10 aout 2008

BH08 – Defcon 16

- 12 ans pour BH08 US
  - 4500 personnes (briefing), 2 jours, 5 continents représentés
  - Autour de 100 conférences, 8 tracks en //
  - Microsoft sponsor Diamond, Cisco, Nokia, Qualys sponsors Platine…
- 16 ans pour Defcon
  - > 9000 personnes, 3 jours de conférence
  - Autour de 100 conférences, 5 tracks en //
  - Et de nombreuses activités…

Ambiances…

- Pro du coté de BH
  - Plus de $1300 l'inscription
  - Salon en // : cette année, tendance AVA, conformité, NAC (!), sandboxes et A/V, audit de code…
- Du coté de Defcon
  - + underground
  - $ 120 en cash…
  - Nombreuses activités annexes…

Du coté de BlackHat

- Deux keynotes (complexité <> sécurité, ainsi que le directeur du NSCS)
- Le Wall of Sheep (nouveau cette année)
- Un salon assez garnis (>40 exposants)

- Les Pwnies awards

Du coté de Defcon

- Lockpicking, safepicking (comme d'hab…)
- Le CTF
- Guitar hero…
- Race to Zero
- Coffee Wars
- BuzzWord Survivor

- Le Wall of Sheep

- Quelques conférences communes avec BH
  - Un programme peut être meilleur qu'en 2007

Public présent

- Talks
  - Eric Filiol, (ESAT), Matthieu Suiche – BH
  - Jonathan Brossard (expat. Indien, Iviz) - Defcon
- Participants
  - DCSSI, CELAR
  - HSC, Thales
  - GlobalSecurityMag
  - RadWare France
  - PricewaterhouseCoopers
  - Président du Clusif
  - EADS
  - TenableSecurity
  - Responsable sécurité (banque française)

  Environ une douzaine de français.

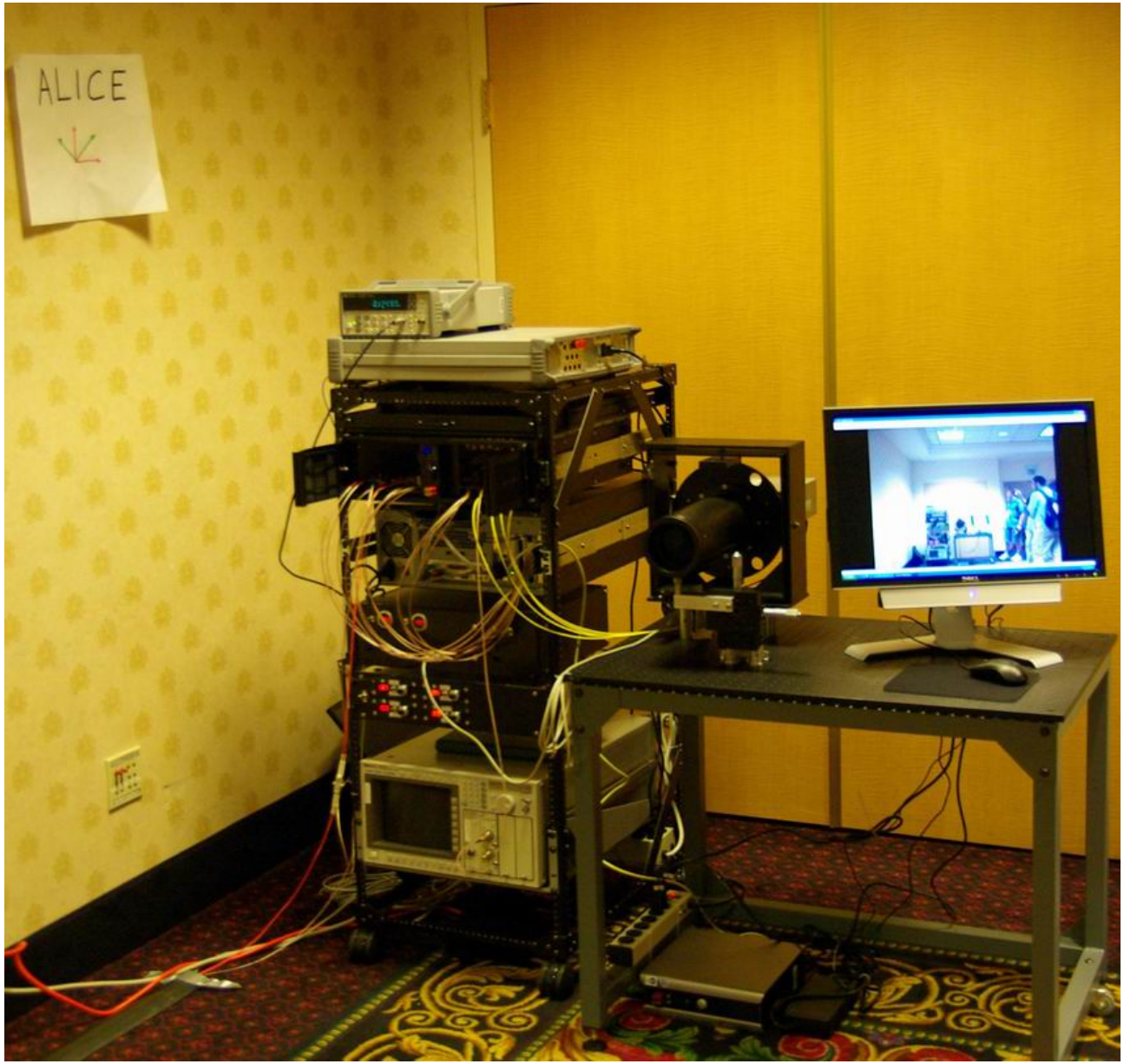
Le « Wall of Sheep »

- Pour la 1ier fois, aussi à BH
  - réseau WiFi BH en WPA2-PSK
  - Réseau Defcon ouvert
- Nouveau : beaucoup d'iPhone et autre PDA
  - Twitter, pop, imap…
- En parlant de mot de passe, voir GlobalSecurityMag…


Wall of Sheep
login
pass
domain_ip
application
MAC ADDR
dave@davemoorecomputers.com wk0******
64.202.165.92 POP3
jdness boo******
mail.mac.com IMAP2
piotrowski 8d5******
pop3.free.fr POP3
bi0drain mir******
10.132.0.70 POP3
MuscleNerd red******
twitter.com HTTP
thumper inf******
munin.fastcoder.net HTTP
1185261 3pl******
login.icq.com ICQ
konstantinkoll@LAS 140******
dwforum.wcx-network.cc HTTP
DotNM pas******
dropshots.com HTTP
Koko E61******
iam.bmezine.com HTTP
miriku lie******
128.121.146.100 TWITTER from IPHONE
365597424 fla******
205.188.153.121 ICQ
yutsch@inbox.ru fla******
195.190.105.238 HTTP
ssmith wea******
140.198.200.70 IMAP
nokia-osso-rx-34 jos******
rickybrent.com HTTP
pa@standalone.com par******
pa.standalone.com HTTP
EAV-01475219 88e******
89.202.157.131 HTTP
81219879 alw******
icq ICQ
piotrowski 8d5******
212.27.48.3 POP
iamthedavil kee******
twitter.com/ TWITTER from IPHONE
gjong 2xo******
169.95.4.13 POP
kaizer mf9******
f-wutz.com/admin/ wordpress?
Wall of Sheep - Copyright © 2001-2008 - All rights reserved.
Analyzing Tr


JINX
GAMERS, GEEKS & HACKERS
WWW.JINX.COM
PRICES
All T-Shirts & Hats.... $20
Buttondowns..... $25
Stickers..... $1
Bracelets & Patches... $3
Any 3 T-Shirts/Hats for $50
PRICES
All T-Shirts & Hats.... $20
Buttondowns..... $25
Stickers..... $1
Bracelets & Patches... $3
Any 3 T-Shirts/Hats for $50
got root?
hacker.
iPood
STFU
JINX


GUINNESS


ALICE

Les Pwnies Awards

- Best server-side : faille IGMP.
- Best client-side : les gestionnaires d'URI buggés.
- Mass 0wnage : Wordpress.
- Most innovative research : les attaques Coldboot.
- Lamest vendor response : McAfee.
- Most overhyped bug : Dan Kaminsky et la faille DNS.
- Best song : Packin' the K.
- Most epic fail : Debian OpenSSL.
- Lifetime achievement : Tim Newsham.

« Faits marquants 08 »

- Du DNS
- De la virtualisation et des hyperviseurs
- Des rootkits
- Du Cisco
- Du reverse et de-obfuscation
- Du Web 2.0 et des réseaux sociaux
- Du « client-side » attacks

- Des talks annulés (apple, RFid and Boston transport)
- Des journalistes expulsés (de BH)
- Les Pwnie awards (comme tous les ans)
- Une démonstration de crypto quantique…

Quelques déceptions…

- Pas/peu de présentation « révolutionnaire » (et une présentation DNS un peu décevante…)
- Climat « prudent » : faire attention à ce que l'on dit… conséquences juridiques importantes ? Pression ?
- Mais BH+Defcon reste un bon baromètre de la sécurité

Détail de quelques conférences

Keynote : Complexity in Computer Security – A risky Business

- Par Ian Angell, Professor Information Systems, London school of Economics

- Constat de la complexité croissante des S.I.
- Dépendance de + en + grande à la technologie

- Constat pessimiste – On court à la catastrophe !

Keynote : Natural Security

- Par Rod Beckstrom, Director of the National Cyber Security Center (NCSC) (DHS)

- Problématique actuelle :
  - la défense est beaucoup plus difficile que l'attaque
  - nous ne connaissons pas les lois qui régissent le monde numérique…
    - Physique des réseaux, tendance et évolution
    - économie des réseaux ?
    - économie de la sécurité
    - gestion de risque
- Modèle mathématique (C = S+L), minimiser C
- Passer d'un modèle Loose/Loose à du Win/Win…

Bad Sushi

- Analyse du monde des « phishers »
- Utilisation de guest book ouvert, de « drop site » non protégés…
  - Constat : code de mauvaise qualité, erreurs de débutants dans les kits de phishing
- Connexion à des places de marché « spécialisées »

- Fun : Kit de phishing « backdoorés » par les concepteurs…

Pointers and Handlers

- Deux parties distinctes :
  - NULL Pointer Dereferences
  - Protected Handle Close
- Vise l'espace noyau par la manipulation de handlers via win32k.sys
- Principalement des DoS, certains bugs peuvent conduire à l'escalade de privilèges
- Exploitation manifestement difficile

DNS Goodness (Dan Kaminsky)

- La présentation tant attendues
- Salle complètement full
- Constat assez décevant. Présentation en 3 temps
  - 1) Application du patches, beaux graphiques (10 minutes)
  - 2) Le problème technique (10 minutes)
  - 3) pourquoi c'est grave (40 minutes)

- Accent sur la dépendance au DNS
  - Récupération des mails si poisonning de MX
  - SSL n'est pas forcement une solution…

Highway to Hell

- Systèmes de paiement automatique autoroutiers de la baie de San Francisco (FasTrak)
- Analyse complète d'un transpondeur
  - Protocole de communication
  - Matériel (base MSP430)
  - Désassemblage du firmware
  - Exécution sur émulateur
- Résultats prévisible
  - Pas de crypto : clonage passif et/ou actif
  - Fonction d'écriture distante : réécriture d'ID
- Quid de la collecte de données ?...

The Four Horsemen of the Virtualization Security Apocalypse

- La mode est à la virtualisation
  - utiliser de la virtualisation pour simuler de vrai réseau ne marche pas
  - Tout est encore en cours de développement, donc pas stable…
  - La virtualisation peut impacter la sécurité et les performances
  - Virtualiser la sécu coute cher, et ne fait pas faire d'économie

- Quels vont être les problèmes ?
  - Complexité, on ne va pas se reposer sur une seule solution, un seul UTM virtualisé
  - Complexité et problème de performance (très gros pb de performance à attendre)
  - Gros souci de disponibilité (les solutions de HA reposent souvent sur des équipements spéciaux, des drivers modifiés… et tout cela ne se virtualise pas bien), De plus, les solutions de sécurité virtualisées ne supporte pas la HA !
  - Tout ca va couter plus cher, car il faudra acheter des licences, du matériel, cela ajoute de la complexité…

Software Radio and the Future of Wireless Security

- Bon SDR Howto
- Présentation des différentes plate-formes
  - USRP, HPSDR
  - Logiciels, principalement GNURadio
- Utilisation pour l'évaluation de sécurité
- Démos
  - Analyse de transmissions P25
  - Rejeu de signaux RC

Xploiting Google Gadgets

- Présentation très « google bashing » !!
- Par l'auteur d'un livre sur les XSS
- Google : gros problèmes liés à la redirection
  - Google s'intéresse plus à tracer les utilisateurs qu'à la sécurité…
- Widget et gadget : encore de nouveaux pb de sécurité
  - Widget = danger car très puissant (api, accès réseau et poste de travail)
  - Peu / pas de validation de code…
- Evolution des malwares : Windows -> Web

Malware Detection Through Network Flow Analysis

- Présentation sur l'analyse de flux
  - Un peu Show-Off, ce qui permet de ne pas s'ennuyer...
- Gros focus sur Netflow
- Analyse fréquentielle plutôt que temporelle
- Logiciels
  - Softlowd (http://www.mindrot.org/projects/softflowd/)
  - Psyche (http://psyche.pontetec.com/)
- Quelques considérations de déploiement

Viral infection in CISCO IOS

- Présentation par CORE Security
- Problématique des rootkit et backdoor

- PoC : infection d'une image CISCO (rootkit persistant, resistant à l'upgrade…)
- PoC : Backdoor acces Telnet
- Conditions : avoir un bug initiale pour l'accés à l'équipement (ou infecter une image)
- Démo

New Classes of Security and Privacy Vulnerabilities for Implantable Wireless Medical Devices

- Problématiques de sécurité liées aux implants médicaux sans-fil
  - Confidentialité des données
  - Sécurité de l'implant
- Ton de la présentation : Oui-Oui découvre la sécurité...
- PoC à base d'USRP (cf. présentation SDR)
  - Écoute, analyse, rejeu, injection, etc.
  - Risque principal : épuisement de la batterie
- Approches défensives
  - Authentification «zero power»
  - Furtivité
- Gros problème de disponibilité en cas d'urgence...

Satan is on my Friends List

- (In)Sécurité et réseaux Sociaux…
  - Réseaux sociaux comme plate-forme d'attaque
  - Failles applicatives
  - Botnet
  - CSRF…
  - Openproxy pour contournement du SameOriginPolicy
- Démo Myspace : commentaires « malveillants »

- Autres attaques : attaques logiques
  - Faux profils (ca marche !)
  - Profiling

Threats to the 2008 Presidential election

- Analyse de Symantec
  - Principalement autour du Typosquatting
- Terrain de jeu : la campagne présidentielle américaine
  - Constat alarmant
  - Dépendance lourde à Internet (don, mail de campagne)
- Analyse de typosquatting (dépôt de 124 noms de domaines proche)
  - Sur 2 mois, 21000 hits
  - Test : Cybersquatting MX

Passive and Active Leakage of Secret Data from Non-Networked Computers

- Implémentation d'un canal de communication caché reposant sur les effets TEMPEST
- Définition et exemples de canaux cachés
- État de l'art TEMPEST
  - Attaque de Kuhn
  - Protections développées
  - Efficacité
- Démonstration de divers PoC maison
  - Dissimulation de données dans un son émis par la cible
  - Manipulation des périphériques (moniteur, ventilateur, disque dur, etc.)

Mobile Phone Messaging Anti-Forensics

- Test d'outils de forensics sur GSM

- Les SMS intéressent de + en + les juges…
- Outils de forensics : Lecteurs de carte à puce (SIM) + soft

- Format de SMS : tout n'est pas supporté par les softs…
  - Exemple : SMS codés en 7 bits, 8 bits et UCS2 (UCS-2 -2-byte Universal Character Set, semblable à UTF-16)
  - En UCS2, codage big/little Endian… -> little endian crashe les outils de forensics…
- Autres tests, fuzzing du file format SMS…

A Hypervisor IPS-based on Hardware Assisted Virtualization Technologies

- Rappel : Classification des malware en 4 types (cf Rutowska)
  - Type 0 : malware standalone, pas de modification de ressources système
  - Type 1 : Changement des ressources « persistantes »
  - Type 2 : Change des ressources non persistantes
  - Type 3 : le malware fonctionne en dehors du système
- Développement de Viton, un IPS fonctionnant en dehors de l'OS guest – PoC sur Win XP SP2
  - Protection des ressources persistantes, de la base de registre, des commandes VMX (intel)…
  - Protection contre type 1 & 3

Side-Channel Timing Attacks on MSP430 Microcontroler Firmware

- Présentation sur le microcontrôleur MSP430
- Certaines fonctions du Boot Serial Loader sont protégées par une clé de 256 bits (stockée en IVT)
- Sur les 256, seuls 40 sont vraiment effectifs
  - Le canal de communication avec le MSP430 est lent
  - Attaque en force brute pas réalisable
- La version 3 du composant présente une différence de timing dans la vérification du mot de passe
  - Timing attack
  - Implémentée sur un circuit directement connecté au MSP
- Impact : récupération du firmware

The Internet is broken – extreme client side attacks

- Présentation sur les problématiques de confiance sur Internet, et le modèle de « Same Origin Policy »
- Exemple d'attaque : les GIFAR
  - GIF valide, donc upload possible sur divers sites Web
  - JAR valide, donc lancement d'une applet dans le contexte du site…
- Rebond sur serveur Web locaux
  - De plus en plus d'applications installent un web locale
    - Sous IE, « local intranet Zone », donc moins de contrôle « SOP », popup…
- Java sera-t-il la nouvelle menace ? (installé sur plus de 90% des desktops…)

Secure the Planet! New Strategic Initiatives from Microsoft to Rock Your World

- Présentation des nouvelles initiatives de Microsoft pour sauver la planète (des pirates...)
- Microsoft Vulnerability Research (MSVR)
  - Recherche de vulnérabilités sur les produits tierce partie
  - Coordination possible avec les chercheurs
- Microsoft Active Protections Program (MAPP)
  - Partage d'information sur les vulnérabilités non publiées
  - À destination de professionnels choisis, sous NDA
- Exploitability Index (XI)
  - Ajout d'un index d'exploitabilité aux alertes
  - Trois niveaux de sévérité
- Présentation très consensuelle...

Braving the Cold

- Fait suite aux « Cold boot attacks »
- Comment se protéger sans modification Hardware ?
  - Détection mise en veille / extinction, et effacement de clef (etat S5)
  - Détection refroidissement de la RAM (capteur t° board)
  - Stocker la clef en mémoire basse (0x7C00-0x7bff), écrasée lors du prochain boot
- Autre solution plus complexe : utiliser 2 clefs
  - Une clef long terme, de grosse taille (1 Mo), stockée en RAM. Elle est hashée puis utilisée pour créer la clef secrète
  - La clef à protéger, stockée dans un registre MMX

Windows Hibernation File for Fun and Profit

- Étude du fichier d'hibernation (S2D) hiberfile.sys
- Description du fichier
  - Contenu
  - Format (compressé LZ77+DIRECT2)
  - Structure interne
- Sandman (http://sandman.msuiche.net/) et applications
  - Description du framework
  - Défenses : forensics, détection et suppression de malwares
  - Attaques : vol de données, élévation de privilèges
- À mettre en perspective avec les attaques ColdBoot ou FireWire

Modscan (Scada)

- Encore une présentation sur les Systèmes de supervision et de Contrôles
- Modscada, outil de scan / audit pour protocole Modbus

- Modbus : protocole pouvant être encapsulé sur TCP/502
  - Modscada : scan TCP 502, brut force des ID Scada Node

Sniffing Cable modem

- Présentation du protocole DOCSIS (Data Over Cable Service Interface Specification)
  - Evidemment, pas/peu de sécurité, chiffrement pas activé…
  - Zone de diffusion potentiellement très large
- Idée : Sniffer le trafic câble
  - Simple, avec une carte DVB-C (trafic download)
- Suite logicielle adaptée : « packet-o-matic »
  - Reconstruction IP, http, mail, RTP/Voip…
- Démonstration assez percutante…

Shiffting the Focus of WiFi Security…

- Première présentation : WEP is dead
  - Sécurité des AP est en progrés
  - Prochaine cible : le client…
  - Présentation de airbase_ng, outil d'attaque simple (mitm, karma, brutforce WPA-PSK…)
- Deuxième présentation : Debridage de carte WiFi
  - .11b : 2412-2462 (US)
  - .11a 5180-5320, 5745-5825 (US) → étrange…
- Ath5k: opensource driver (source code dispo…)
  - .11a 4920-6100 (DEBUG)

Owning the Users with Agent in the Middle

- Présentation de Jay Beale
- The « midler », outil automatique de MITM
  - Interception de connexion client-server
  - Proxy / reverse proxy
  - Commutation http / https possible
  - Plugins spécialisés pour
    - GMAIL
    - Linkedin
    - Privatejournal

Feed my SAT Monkey

- Présentation fun de Adam Laurie (RFidiot…)
- Observation des feeds satellites…
  - Canaux video
  - Canaux Data
- Possible et simple aujourd'hui : DVBSnoop, outil opensource

- Des tas de choses « trainent » sur ces réseaux…

Hacking OpenVMS

- Objectif : montrer qu'un OS vieux de 30 ans, considéré comme sur, présente des failles exploitables…
- OpenVMS : multiuser, multitache, gestion de mémoire virtuelle, système très cloisonné
- Attaques :
  - Classique, username/pwd brutforce
  - Serveur web vulnérable (WASD -> directory traversal, CGI par défaut…)
  - Finger dangeureux (droit system, follow symlink…)
  - Shellcode sur VAX…, BoF…

Climbing Everest (eVoting)

- La présentation fun de la conférence
- Analyse du rapport « everest », audit de machine à voter pour le compte de l'état d'OHIO

- Résultats catastrophiques à TOUS les niveaux…
  - Sécu physique critique
  - Sécu logique aberrante
  - Pas de code validé, pas de garanties…

- Le futur sera encore plus sombre…

Race2Zero

- Concours lancé avant Defcon : Contournement des A/V
- Idée : une dizaine d'AV en série…
  - Comment bypasser tout cela…
  - Une dizaine de virus à modifier
- Résultat sans surprise…
  - 4 teams ont passé tous les tests
  - Meilleur score en 2 heures 20…
- Intéressant : Réaction des éditeurs d'A/V…

Bypassing pre-boot Authentication password

- Seule présentation faite par un Français à Defcon
  - Basé en Inde, chez iviz
- Idée : Récupération du/des mots de passes boot
  - Bios, protection HD – ATA, chiffrement disque…
- Comment : La zone mémoire utilisée par le bios n'est pas nettoyée -> elle est accessible après le boot
  - Sous linux, /dev/mem, /dev/kmem…
  - Sous windows, compatibilité 16 bits (mode MSDOS) donne accés à cette zone de mémoire remappée…

Routing: Owning the Defcon Network

- Comment 0wner un réseau ?
- Attaque « MITM » sur le trafic du réseau Defcon
- Utilisation de BGP
  - Annonce de route plus spécifique depuis un autre AS
  - Routage statique inter AS
- Pas vraiment une faille de sécurité
  - Modèle de confiance de l'Internet et de BGP
- A rapprocher du problème Youtube / Pakistan Telecom…

Questions ?

orange™

Supports disponibles

- BlackHat :
  - http://www.blackhat.com/html/bh-usa-08/bh-usa-08-archive.html
- Defcon :
  - http://www.defcon.org/html/defcon-16/dc-16-schedule.html