Compte-rendu SSTIC 2012

Nicolas RUFF
EADS Innovation Works
nicolas.ruff(à)eads.net

SSTIC

- Conférence de sécurité
- 10ème édition

- Programme
  - https://www.sstic.org/2012/programme/

- Ce qui ne change pas
  - Toujours francophone
  - Toujours à Rennes
  - Toujours des actes papier

- Ce qui change
  - Paiement par Paypal
  - Nouveau logo

SSTIC

- Logo des actes
  - Aucune version n'est disponible en ligne

Jour 1

"20 years of PaX"

- Keynote d'un haut niveau technique

"SSL/TLS: état des lieux et recommandations"

- Intéressant tour d'horizon des implémentations
  - Microsoft ne supporte pas la PFS
- Pas d'outil publié
- Voir aussi:
  - https://www.eff.org/observatory
  - https://ssltest.offenseindepth.com/

"Netzob: un outil pour la rétroconception de protocoles"

- *NETwork protocol modeliZatiOn*
- Outil:
  - http://www.netzob.org/

Jour 1

- "Sécurité de RDP"
  - RDP est complexe
  - RDP est impossible à protéger sauf alignement ~~de planètes~~d'options
  - Pas d'outil publié

- "WinRT"
  - Aperçu de la nouvelle *sandbox* Windows 8
  - Déjà présenté

- "L'information, capital immatériel de l'entreprise"
  - Information != donnée

- "Audit des permissions en environnement Active Directory"
  - Extraction du contenu de l'AD
  - Recherche de *backdoors* extrêmement subtiles
    - SDProp, AdminSdHolder, …
  - Outil publié sur GitHub (!)
    - https://github.com/ANSSI-FR/AD-permissions

Jour 1

- "Windows 8 et la sécurité" (Microsoft France)
  - Nouveautés mises en avant:
    - *Sandbox*
    - Carte à puce virtuelle
    - Boot sécurisé (UEFI, ELAM, …)
    - TPM 2.0
    - "La tablette est le TPM"
    - Contrôle d'accès dynamique
- "10 ans de SSTIC"
  - #epic
  - Plus de 50% des participants venaient pour la 1ère fois
- Cocktail(++)

Jour 2

- "Compromission d'une application bancaire JavaCard par attaque logicielle"
  - Fonctionne
  - Seul pré-requis: pouvoir *uploader* une *applet* dans sa carte …
- "IronHide: plateforme d'attaques par E/S"
  - Réalisation d'un contrôleur d'E/S à base de FPGA
  - Permet d'analyser et/ou d'injecter toute forme de trafic PCIe
- "La qualité d'hébergeur en 2012" (OVH)
  - Juriste: conférence sans slides ☺

Jour 2

- Résultats du challenge
  - #epic

- Présentations courtes
  - "Elsim + Androguard"
    - Identification du code publicitaire dans les applications Android
      - https://code.google.com/p/elsim/wiki/Similarity
      - https://code.google.com/p/androguard/
  - "Dissecting Web Attacks Using Honeypots"
    - 500 honeypots Web à forte interaction
    - 69,000 attaques détectées
    - Encore en cours d'analyse …
  -  "SIDAN"
    - Analyse statique
    - Plugin Frama-C
      - http://www.rennes.supelec.fr/ren/rd/cidre/tools/sidan/

Jour 2

- "Contrôle d'accès mandataire pour Windows 7"
  - Tout est dans le titre …

- "Expert judiciaire en informatique" (Zythom)
  - Plein d'anecdotes
  - "Expert" est un titre, pas une qualité
  - Une activité, pas un métier
  - Pédagogie, méthode, et autres qualités humaines >>> compétences techniques
  - Il est difficile de déclarer ses revenus d'expertise ☺

- "Forensics iOS"
  - Beaucoup d'information technique
  - Déjà présenté
  - Outil:
    - https://code.google.com/p/iphone-dataprotection/
  - Voir aussi:
    - iOS Hacker's Handbook

Jour 2

- Rump sessions (1/2)
  - Concours de logos SSTIC
  - Fingerprinting de navigateurs Web
  - Finger-over-DNS
    - http://www.hsc.fr/ressources/presentations/sstic12_rump_dnsfinger/DnsFingerSSTICRump2012.pdf
    - http://www.hsc.fr/ressources/presentations/sstic12_rump_dnsfinger/authfinger.pdf
  - http://www.botnets.fr/
  - Fuzzing de l'outil Wireshark
  - Décompilation Python
    - https://github.com/Mysterie/uncompyle2
  - Pokémon sur GBA
  - Outil WOLFY (post-APT)
    - http://www.xmco.fr/wolfy-post-forensics.html
  - Hynesim
    - http://www.hynesim.org/
  - Une faille sur le site du SSTIC (!)
    - Découverte par la DGA/MI

Jour 2

- Rump sessions (2/2)


Méthodologie post-APT
Scapy Pipes
  - Recherche de 0day dans Android avec grep
  - Annonce pour la conférence GreHACK 2012
    - http://ensiwiki.ensimag.fr/index.php/GreHack-2012-english
  - Annonce "on recrute"
  - Annonce pour la conférence RMLL 2012
    - http://schedule2012.rmll.info/?lang=en
  - Pare-feu LibreOffice
  - DFF
    - http://www.digital-forensic.org/
  - Exploitation de Struts lorsque DevMode="true"
    - "intitle:Struts Problem Report"
  - JavaScript dans JPG dans PDF
  - Attaque par relais sur carte à puce
  - Hack matériel d'un QRCode

- Social Event

Jour 3

- "Source Address Validation Improvements" (SAVI)
  - Intéressant … pour les opérateurs
  - Invasif pour la vie privée (très utilisé en Chine)
  - Des pré-requis techniques assez contraignants
    - http://tools.ietf.org/wg/savi/

- "Utilisation malveillante des suivis de connexions"
  - Abus des "*helpers*" Netfilter pour les protocoles complexes
    - FTP, IRC/DCC, SIP …
  - Outil:
    - https://github.com/regit/opensvp

"Influence des bonnes pratiques sur les incidents BGP"
  - Une conférence sur BGP intéressante (!)
  - Illustrée de nombreux exemples

Jour 3

- Présentations courtes
  - "Netusse"
    - Un *fuzzer* de sockets qui a trouvé des vrais bugs dans FreeBSD
      - https://code.google.com/p/netusse/

"Vérification de code système par typage statique"

- Analyse statique
  - http://penjili.org/penjili.html

"Détection de domaines malveillants par analyse sémantique"

- Algorithmes de classification de noms de domaine

Jour 3

- "Successes (and limitations) of (static) binary analysis" (Halvar Flake)
  - Très bonne vulgarisation d'un domaine pourtant complexe
  - Aucun outil n'est actuellement capable d'identifier un bug sendmail de 2003
    - http://www.ouah.org/LSDsendmail.html
  - … et personne ne sait pourquoi

- "Miasm: Framework de reverse engineering"
  - #epic
  - Outil:
    - https://code.google.com/p/smiasm/

- "Rétroconception et débogage d'un baseband Qualcomm"
  - Beaucoup d'information technique
  - Déjà présenté
  - Outil:
    - https://code.google.com/p/qcombbdbg/

- "Protéger et défendre le cyberespace militaire : la démarche nationale"

A part ça …

- Zythom défacé
- Il pleut à Rennes
  - … et c'est mal famé
- > 50% de nouvelles têtes
- Mention spéciale aux T-Shirts:
  - "Guns'n'roses"
  - "Marc Dorcel"
- La concurrence de Roland-Garros …
- Le sticker ANSSI est vraiment de mauvaise qualité …

Références

- Comptes rendus en ligne
  - http://wiki.sstic.org/SSTIC2012/Presse
  - http://sid.rstack.org/blog/index.php/tag/sstic2012
  - http://vanhu.free.fr/blog/index.php?tag/SSTIC12
  - http://www.n0secure.org/search/label/SSTIC%202012
  - http://www.protocol-hacking.org/tag/SSTIC
  - http://www.ozwald.fr/index.php?post/2012/06/09/SSTIC-2012-completed
  - http://www.hsc-news.fr/