Hack.lu 2007

Compte-rendu

Présentation pour le groupe SUR

08/01/2008

Jêrome Léonard et Saâd Kadhi -- HAPSIS

Agenda

★ Hack.lu? Kesako?

★ Day 1 : Defense^W Hacking-in-Depth

★ Day 2 : Deux gars, une fille, une voiture

★ Day 3 : *yawn*

Hack.lu? Kesako?

Meta-Information

★ Conférence dédiée à la sécurité

★ Durée : 3 jours

★ Lieu : Grand Duché du Luxembourg

★ 3ème édition, 150 inscriptions env.

Programme

★ Day 1 : Workshops everywhere

★ Day 2 & 3 : Présentations "classiques", un seul track

★ Un total de 5 workshops et 17 présentations

- De qualité variable

Notre ressenti

★ " Petite " conférence sympathique

★ Très bonne organisation

★ Pas de multiples tracks (sauf pour les workshops)

★ Quelques présentations réchauffées

Day 1: Defense^WHacking-in-Depth

Journée Dédiée aux Workshops ...

★ Writing exploits using Metasploit 3.0

★ Wifi protected setup workshop

★ VoIP workshop

★ Phishing workshop

★ Forensic Analysis of Botnets

Forensic Analysis of Botnets

★ En fait, ce sont 2 workshops en 1

★ 1er workshop par la FCCU (Federal Computer Crime Unit), Belgique

★ 2nd workshop par Hilar Leoste de Shadowserver.org

★ Très intéressants et didactiques

Forensic Analysis of Botnets
1er Workshop

- ★ Analyse de l'action des botnets
- ★ Nepenthes
- ★ Analyse statique
- ★ Analyse dynamique

Forensic Analysis of Botnets
2e Workshop

★ Les modes d'infection

★ Les botnets, pour quoi faire ?

★ L'avenir des botnets

Une présentation déstabilisante

★ The death of defense-in-depth? (Revisiting AV Software) par Thierry Zoller & Sergio Alvarez de nruns

★ Ou comment la multiplication des AV augmentent drastiquement votre surface d'attaque ...

The death of defense-in-depth?

★ Objectif de la présentation

★ Rappels

★ Les AVs sur une architecture

★ En pratique

Day 2: Deux gars, une fille, une voiture

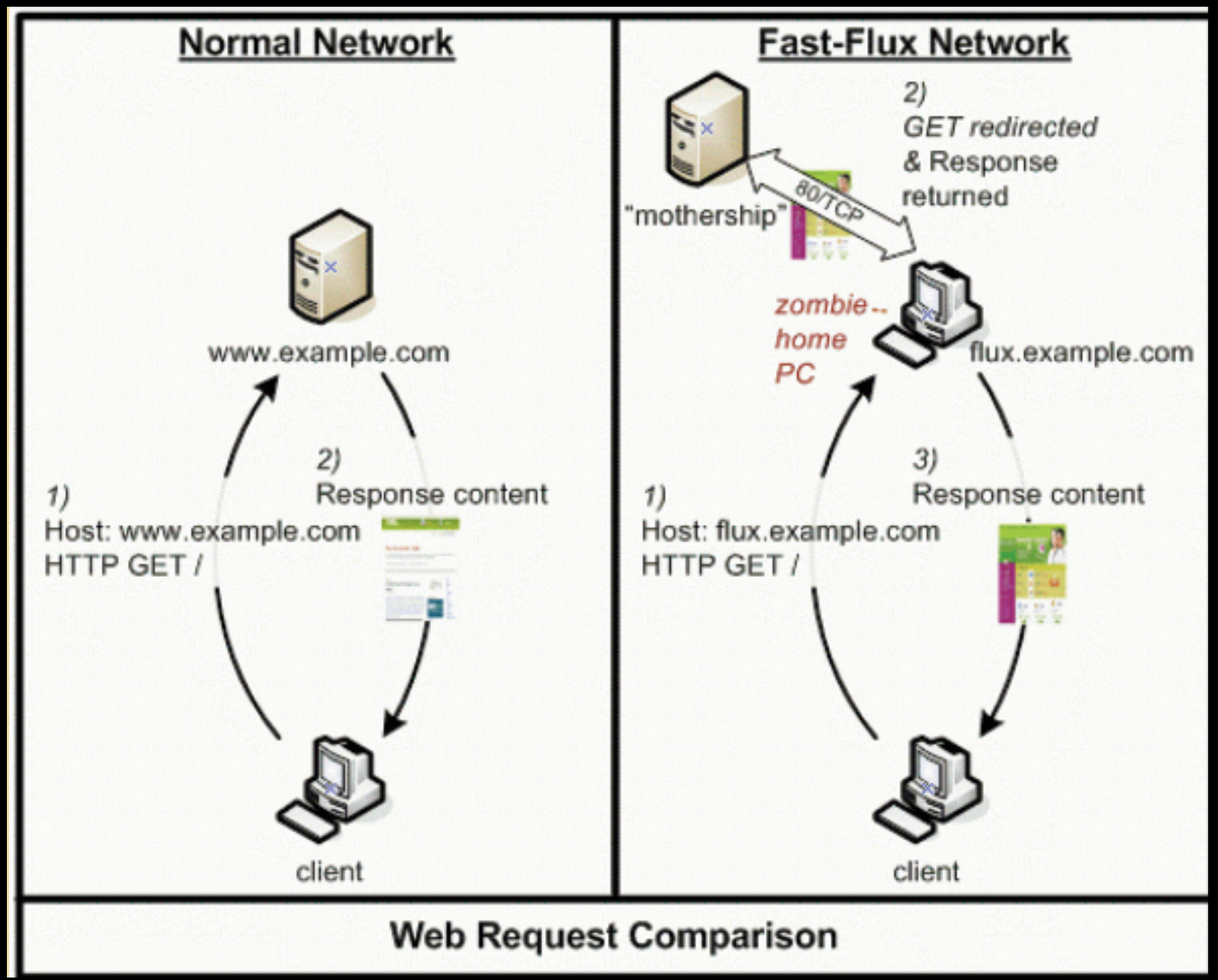
Lance Spitzner Ouvre Le Bal

★ Les présentations sont officiellement ouvertes

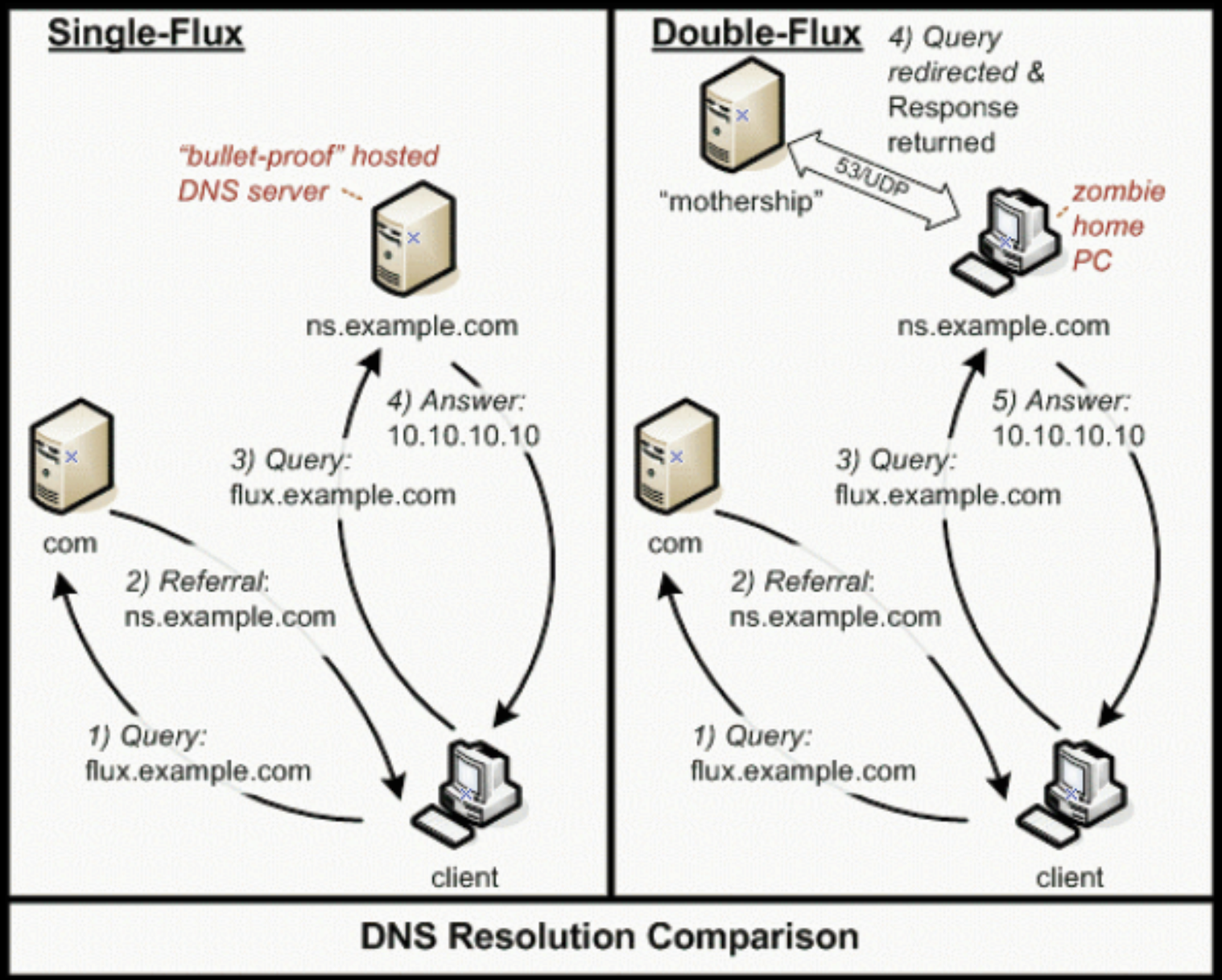
★ Lance Spitzner capte l'attention avec sa description très convaincante des réseaux Fast-Flux et Double-Flux

★ Bad guys win?

Simple Flux


Normal Network
www.example.com
1)
Host: www.example.com
HTTP GET /
2)
Response content
client
Fast-Flux Network
"mothership"
2)
GET redirected
& Response
returned
80/TCP
zombie --
home
PC
flux.example.com
1)
Host: flux.example.com
HTTP GET /
3)
Response content
client
Web Request Comparison

Double Flux


Single-Flux
"bullet-proof" hosted DNS server
ns.example.com
4) Answer: 10.10.10.10
3) Query: flux.example.com
com
2) Referral: ns.example.com
1) Query: flux.example.com
client
Double-Flux
4) Query redirected & Response returned
53/UDP
"mothership"
zombie home PC
ns.example.com
5) Answer: 10.10.10.10
3) Query: flux.example.com
com
2) Referral: ns.example.com
1) Query: flux.example.com
client
DNS Resolution Comparison

L'attention en chute libre

★ Franck Ackermann jette un froid dans l'audience avec une présentation sans intérêt

★ Is IT Virtualization A Security Panacea

★ Que des généralités !

Et Si On Vous Parlait De ...

★ E-Passports: The good, the bad and the ugly par Zubair Khan

★ Exploiting SAP Internals par Mariano Nunez di Croce

★ Wifi Fuzzing, Remote Kernel Exploitation par FT R&D

Mais La Palme Revient ...

★ ... à Daniele Bianco et Andrea Barisani pour une présentation très amusante et captivante

★ Injecting RDS-TMC Traffic

★ Ou comment votre système de navigation automobile peut se retourner contre vous

Day 3: *yawn*

La qualité baisse

★ Alors que les deux premiers jours étaient globalement très intéressants avec des workshops/présentations de qualité ...

★ ... Le dernier jour a enchaîné les présentations ennuyeuses

★ A l'exception de deux

Breaking And Securing Web Apps

★ Nitesh Dhanjani a démarré cette journée avec une présentation intéressante sur la sécurité des applications Web

★ Rien de nouveau mais un tour d'horizon clair et précis

★ XSS, XSRF, et leurs combinaisons

yawn

★ Et hop ! Notre intérêt retombe avec des présentations au ton monocorde et des slides généralement très chargés ...

★ Cracking Windows Access Control ...

★ Zombie 2.0 ...

Metasploit Again?

★ Yoann Guillot fait rebondir notre intérêt avec une présentation de Metasm

★ Un puissant dés(assembleur) Ruby intégré à Metasploit 3.0

Compte-rendu

★ Un compte-rendu détaillé de toutes les présentations intéressantes bientôt disponible en téléchargement sur le site de l'OSSIR

★ (Et maintenant vous savez ce qu'est l'anti-sèche que nous lisons en douce)

Remerciements

★ L'OSSIR pour nous avoir sponsorisé

★ HAPSIS pour nous avoir permis d'assister à cette conf'

★ Sharon Jones & The Dap-Kings ainsi que The Sweet Vandals ... pour la musique :-)

Informations Utiles

★ Vous pourrez (bientôt) télécharger cette présentation en ligne sur le site de l'OSSIR

★ Questions ? Commentaires ?

- jerome.leonard@hapsis.fr ||
  saad.kadhi@hapsis.fr

Intervenants

★ Jérôme Léonard, consultant sécurité,
HAPSIS (http://www.hapsis.fr/)

★ Saâd Kadhi, consultant sécurité,
HAPSIS (http://www.hapsis.fr/)

Licence

★ Creative Commons Attribution-NonCommercial 2.5

- http://creativecommons.org/licenses/by-nc/2.5/