TIW4 : SÉCURITÉ DES SYSTÈMES D'INFORMATION

INTRODUCTION GÉNÉRALE

romuald.thion@univ-lyon1.fr

http://liris.cnrs.fr/~rthion/dokuwiki/enseignement:tiw4

Master « Technologies de l'Information »

Outline

Page de l'UE

http://liris.cnrs.fr/~rthion/dokuwiki/doku.php?id=enseignement:tiw4

Quelques sources d'actualité

- CNIS mag http://www.cnis-mag.com
- ZATAZ https://www.zataz.com/
- Schneier on Security http://www.schneier.com/blog/
- Reflets.info : journalisme hacker-friendly https://reflets.info/
- Threat Level http://www.wired.com/threatlevel

Sites de référence :

- ANSSI
- OWASP et en particulier les cheatsheet (github)
- Offensive security, dont Exploit Database (avec HGDB) et KALI

Quelques ouvrages

Disponibles à la BU

- « Sécurité informatique – cours et exerices corrigés »
  Avoine, Gildas – Junod, Pascal – Oechslin, Philippe

Romans sérieux

- Histoire des codes secrets, Simon Singh
- Silence on the Wire et The Tangled Web, Michal Zalewski
- The Art of Deception, Kevin Mitnick

Objectifs

Bloc thématiques

1. Bases de la cryptographie et applications
2. Authentification
3. Vulnérabilités (web)
4. Contrôle d'accès et autorisation
5. Analyse de risques

Compétences

- reconnaître et réduire les vulnérabilités(web)
- mettre en place un serveur HTTPS et une authentification sûres
- définir et implémenter une politique de contrôle d'accès
- évaluer les risques de sécurité d'un système

La sécurité en chiffres

Extraits

- *The data used for this study shows that in 86% of all attacks, a weakness in a web interface was exploited* (UK Breach)
- *Vulnerability [. . .] : SQL injection (40%), Poor Server Configuration/Authentication (30%), SQLi & malware (20%), Malware (10%)* (UK Breach)
- *Websites Found With Malware : 1 in 566* (Symantec)
- *97% of attacks using exploits for vulnerabilities identified as zero-day were Java-based* (Symantec)
- *According to a survey [. . .], 91% of the organizations polled suffered a cyber-attack at least once over a 12-month period, while 9% were the victims of targeted attacks* (Kapersky)
- *In order to conduct 1 700 870 654 attacks over the Internet, cybercriminals used 10 604 273 unique hosts* (Kapersky)

Brainstorming

Donner des noms, marques, termes du jargon, acronymes, etc. de la sécurité informatique

Art. 323 du Code Pénal

- LIVRE Ier Dispositions générales.
- LIVRE II Des crimes et délits contre les personnes.
- LIVRE III Des crimes et délits contre les biens.
  - TITRE Ier Des appropriations frauduleuses.
  - TITRE II Des autres atteintes aux biens.
    - CHAPITRE Ier Du recel et des infractions assimilées ou voisines.
    - CHAPITRE II Des destructions, dégradations et détériorations.
    - CHAPITRE III Des atteintes aux systèmes de traitement automatisé de données.
    - CHAPITRE IV Du blanchiment.
- LIVRE IV Des crimes et délits contre la nation, l'Etat et la paix publique.

Article central

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)

L'article sur legifrance

Infractions « classiques »

- l'escroquerie
- l'usurpation d'identité
- la diffamation
- apologie des crimes et délits
- l'atteinte au secret des correspondances
- l'atteinte à la vie privée (c.f CNIL)

Tout ce qui est illégal *offline* est illégal offline l'est aussi *online*

Article central

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)

L'article sur legifrance

Infractions « classiques »

- l'escroquerie
- l'usurpation d'identité
- la diffamation
- apologie des crimes et délits
- l'atteinte au secret des correspondances
- l'atteinte à la vie privée (c.f CNIL)

Tout ce qui est illégal *offline* est illégal offline l'est aussi *online*

Conclusion

"*Don't rely on network safeguards and firewalls to protect your information. Look to your most vulnerable spot. You'll usually find that vulnerability lies in your people.*"

Kevin D. Mitnick – "The Art of Deception", p.79

What is the most fun to exploit ? (poll packetstormsecurity.org)

answers	votes	percent
Buffer Overflows	22917	9.9%
SQL Injection Flaws	19945	8.6%
Remote/Local File Inclusion Flaws	12437	5.4%
Cross Site Scripting Flaws	73192	31.7%
Format String Attacks	15832	6.9%
Human Stupidity	86483	37.5%

Conclusion

"*Don't rely on network safeguards and firewalls to protect your information. Look to your most vulnerable spot. You'll usually find that vulnerability lies in your people.*"

Kevin D. Mitnick – "The Art of Deception", p.79

What is the most fun to exploit ? (poll packetstormsecurity.org)

answers	**votes**	**percent**
Buffer Overflows	22917	9.9%
SQL Injection Flaws	19945	8.6%
Remote/Local File Inclusion Flaws	12437	5.4%
Cross Site Scripting Flaws	73192	31.7%
Format String Attacks	15832	6.9%
Human Stupidity	86483	37.5%