« In Your Street »

Résolution des problèmes de logistique rencontré sur le terrain.

Hacking – Lockpicking Vol 1.

Par taskforce le mardi, 29 novembre 2005.

Le titre peut être assujettit à un ou plusieurs changement dans les prochain numéro!

Page Vide

Résolution des problèmes de logistique rencontré sur le terrain.

Hacking – Lockpicking Vol 1.

Sommaire

Introduction, par taskforce, 1er décembre 2005.

L'ère de l'informatique, 1981, IBM-PC (Personnal-computer), déjà bien avant cette date des gens scientifique ou non qui par le manque d'information sur les produits existant, bidouillent par pure plaisir afin de connaître à fond cette nouvelle technologie et de publier librement des articles sur le fonctionnement, techniques de bidouillage des appareils de l'époque. Hélas nous sommes en 2005 et bientôt en 2006, les techniques et méthodologies pour le hacking-lockpicking jusqu'à présent ne sont peut-être pas encore désuète mais elles sont largement exploitées de façon exponentielle depuis les 5 dernières années. Le monde de la sécurité de l'information se développant aussi rapidement, il est essentiel de développer de nouveaux outils et techniques (qui, à mon avis, devraient rester à accès restreint) qui devanceront nos merveilleux administrateur et nos sois-disant expert en informatique.

Au cours de plusieurs années de recherche de nouvelles technique, de méthodologie et d'exploitation de celle-ci autant, dans le domaine du hacking et du lockpicking, plusieurs problèmes de logistiques se sont présenté comme des obstacles majeur ou mineur selon les cas. Ce document est dédier et a pour but de définir et de lister les problèmes en question afin d'en trouver des solutions viable dans le cadre de l'exploitation de faille physique, logique ou de logistique. Le volume 1 de cette doc a aussi pour but de voir à quel niveau d'appréciation il se situ et quel en est l'intérêt du publique cible (cour terme, long terme). Il en sera question des principaux problèmes de logistique rencontré sur le terrain et sera divisé et traité en sous-catégorie ; hacking (Hardware, Software), lockpicking (at home, in the city) et de logistique. S'il y a réel intérêt, le volume 2 sortira sous peut avec de nouveaux sujets encore plus détaillés.

À propos des fautes d'orthographe, un(e) correcteur(trice) serait bien apprécié pour aider à la correction ou pour une contribution volontaire quelconque. Email : e1130@hotmail.com.

Destroy HD Data rapido - Part 1,

par taskforce, 1er décembre 2005.

Vous détenez des informations confidentiel sensible sur votre disque dur préférer et vous croyez que la police, une organisation criminel ou n'importe qui vous tuerais seulement pour voir physiquement le contenu du disque en question et bien j'ai une solution pour vous ou plutôt trois… Je me suis penché sur ce problème il y a quelque temps, et je me suis arrêté sur une combinaison de 3 solution. La première, a été la pose de 2 tiroir à disque dur. La seconde est l'utilisation d'une carte PCI Crypto 64 bit(128 192 disponible aussi). En 3, l'utilisation d'une perceuse en EXTREME ET DERNIER RECOUR MUNIE DE LA PLUS GROSSE MÈCHE que j'ai pu trouver. 6 SECONDES POUR 3 TROUS TESTÉ…

La fonction principal de la crypto pci est de crypter toute les données qui transitent entre le contrôleur ide et un disque dur quelconque par le biais d'une chip "*Enova x-wall 64se*". Elle crypte la totalité du disque en 64bit(peut aller jusqu'a 192bit comme utiliser par certain gouvernement us ou ca) (compris boot sector) avec une security key en temps réel avec un taux de transfère de 100mb/sec (benchmark à l'appuis dans les liens). Avec ça, il y a 2 clef à id identique (connecteur firewire). Ma config. actuelle sur un poste de travail est composé de un graveur lg, d'un lecteur cd, de l'os primaire sur le premier tiroir amovible, le data backup sur le deuxième tiroir amovible, une crypto 64 brancher sur le tiroir à backup et tout fonctionne comme merveille. Au niveau des applications de la chip *Enova*, il y a du *SATA Raid*, *IDE Raid*, la biométrie, des racks amovible, pour *Notebook* quelques carte-mère Asus et j'en passe...

Une cote à donner sur 10, 8/10. 8 puisqu'elle fait seulement du 64bit et 100mb/s de taux de transfère. Un plus, la dureté de la mise en œuvre d'une attaque par brute force de clefs aléatoire du à la lenteur du processus de démarrage par le biais de la *Crypto PCI*.

Liens

http://www.enovatech.net/products.htm
http://www.enovatech.net/support/download/X-Wall_SE_Test_Report.pdf
http://www.tigerdirect.com/applications/searchtools/item-detailsInactive.asp?EdpNo=184051
http://www.tigerdirect.com/applications/searchtools/item-detailsInactive.asp?EdpNo=184052

Hide your ass from cops - Part 1,

par taskforce, 29 décembre 2005.

Le but de cet article est de vous conscientisé aux procédure judiciaires et à quelques conseils judicieux pour ne pas en arriver à se faire prendre par la police.

Selon l'annexe 1 "Cheminement des plaintes à la police"

- Droits et lois, dans la rue et pendant les interrogatoires. Entrevue prochaine avec un avocat de l'aide juridique.

Résolution de problèmes,

par taskforce, 29 décembre 2005.

Un jour ou un autre, un problème de taille se posera sur votre chemin! Vous vous demandez comment le résoudre? Dans les prochains paragraphe qui suivent, je vais vous présenter une démarche fonctionnel en 6 étapes qui visera à développer votre sens de la logique et que si vous l'apprenez, elle sera pratique tout au long de votre vie.

Les 6 étapes importantes pour faire face à un problèmes :

Étapes 1 :
- La prise en compte du problème
  - Prise en compte et spécification du problème

Étapes 2 :
- L'analyse du problème
  - Analyse du problème et de ces contraintes

Étapes 3 :
- Formuler et vérifier des hypothèses sur les causes du problèmes
  - Exploration de solutions possibles et valables

Étapes 4 :
- Choisir une solution
  - Choix et planification d'une des solutions selon certains critères

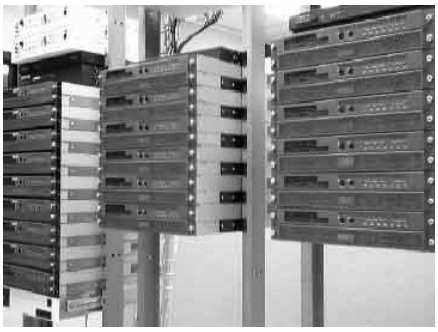
Étapes 5 :
- Application de la solution choisit
  - **Définition des opérations en tant qu'algorithme**
  - Non redondance des actions
  - Cheminement logique des données

Étapes 6 :
- Vérification de la mise en application de la solution

Obtain the accesses on network rapido,

par taskforce, 1er décembre 2005.

Le carnet de bord & Accès physique vs lockpicking

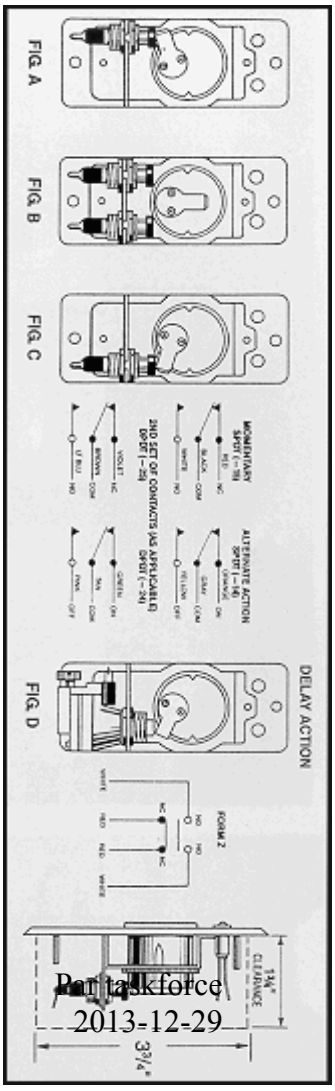


E-LaTeX Magic Trick of the month,

par taskforce, 11 mai 2006..

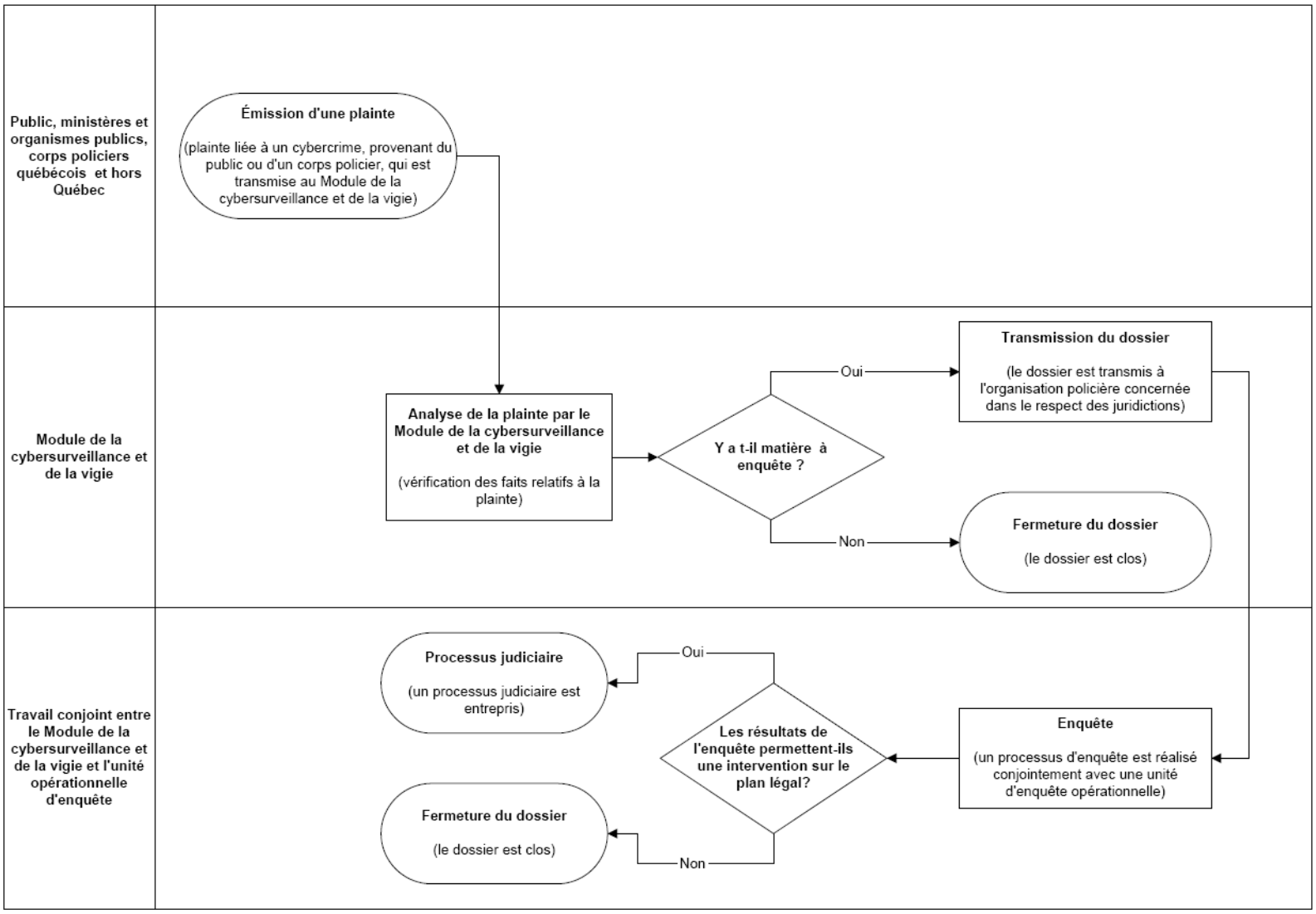
Old Skewl .inc présente une technique (imagé ci-bas) qui consiste à ouvrir les visse de sécurité `Snake eYe` (utilisé dans les ascenseurs, serrures murale, gate de parking, boîtiers de camméra) avec comme outils une brochette à épis de maïs coupé et limé afin d'entrer dans les trous et de pouvoir appliquer une torsion et ainsi dévisser la visse. Je vous laisse regarder les images.

Proximity Card Reader



Annexe 1

- Cheminement des plaintes adressées à la Sûreté du Québec.



Annexe 2

- Tableaux des autorisations d'accès (Exemple).

LISTE INFO USER

Nom	Prénom	User	Mot de passe	Département	Restriction horaire
Laval	Anie	a.laval	?l3d $/54_	Comptabilité	8 :00h à 16 :00h
Steak	Hasher	h.steak	$fs39d8o±v	Tech	8 :00h à 16 :00h
Afridi	Khurram	k.afridi	@ps3vod¤ca	Vendeur	16 :00h à 22 :00h

DROITS SUR LES RESSOURCES "Novell Netware"

RESSOURCES	GROUPE(S)		DROITS							
Appl.Office	Vendeur	Tech	L	E	C	EF	A	M	CA	S
	Comptabilité	Dir.	x				x			
Appl.Visio	Tech	Dir.	L	E	C	EF	A	M	CA	S
			x	x	x	x	x	x		x

DROITS SUR LES USERS "Novell Netware"

USER	RESSOURCES	DROITS							
User: a.laval	Appl.Office	L	E	C	EF	A	M	CA	S
		x	x	x	x	x	x		
Groupe(s)	Comptabilité	L	E	C	EF	A	M	CA	S
		x	x	x	x	x	x		
Script:		L	E	C	EF	A	M	CA	S
USER	RESSOURCES	DROITS							
User: h.steak	Appl.Office Appl.Visio	L	E	C	EF	A	M	CA	S
		x	x	x	x	x	x		
Groupe(s)	Tech	L	E	C	EF	A	M	CA	S
		x	x	x	x	x	x		
Script:		L	E	C	EF	A	M	CA	S