Titre	**Labo Windows Forensics**
Objectif	Détection de l'incident et analyse permettant de diminuer la fréquence des incidents. Etre capable d'ausculter un poste Windows suspect Retrouver des preuves d'attaques
Pré requis	Niveau de connaissance équivalent ou supérieur à Sécuriser un poste client Windows (2000 & XP) Référence = *Guidance for Securing Microsoft Windows XP Systems for IT Professionnals* http://csrc.nist.gov/itsec/guidance_WinXP.html
Public cible	Administrateur système, spécialiste sécurité, ingénieur réseau, …
Méthodologie	Mettre en œuvre une démarche forensique : *live analysis* + *post-mortem analysis* Analyser les *malwares* détectés Utiliser les outils appropriés mis à disposition dans le ***response kit*** Créer une **référence** sur un modèle comportemental *(white list)* pour faciliter la réponse d'incident
Cadre pédagogique	**La matière enseignée se répartit entre 50% de théorie et 50% de pratique** **Tous les travaux pratiques s'effectuent sur un poste Windows XP SP2** **La méthodologie enseignée convient également pour les serveurs Windows 2003**
Producteur & Intervenants	Gérald Litzistorf, professeur Nicolas Sadeg, ingénieur HES en télécommunications
Durée	2 jours
Dates	Mardi 5 & 7 juin 2007
Horaire	8h30 – 12h 13h30 – 17h
Lieu	Ecole d'ingénieurs de Genève Laboratoire de transmission de données www.td.unige.ch
Langue	Enseignement (théorique & pratique) dispensé en français Supports (cours + laboratoire) en français
Nombre de participants	Limité à 8 pour garantir un suivi optimal lors des travaux pratiques
Prix	1800.-

Programme du 1er jour

08h30	15'	**Introduction**	Présentations des objectifs et des participants
08h45	30'	**Cours 1**	Architecture Windows & Outils appropriés
09h15	75'	**Labo 1**	Approfondissement des connaissances W2k / XP Prise en main des outils du ***response kit***
10h30	30'	**Pause**	Discussion
11h00	30'	**Cours 2**	Principales données à sauver lors de *live analysis*
11h30	30'	**Labo 2**	Réponse d'incident *live* **sans référence** avec rapport
12h00		**Repas**	
13h30	45'	**Cours 3**	*Post-mortem analysis*
14h15	45'	**Labo 3**	Analyse approfondie du *malware* découvert lors du labo 2 et amélioration de la sécurité
15h00	30'	**Pause**	Discussion
15h30	30'	**Cours 4**	Création d'une référence basée sur un modèle comportemental *(white list)*
16h00	60'	**Labo 4**	Création et utilisation de la **référence** A Collecte d'informations volatiles, Création de la référence, Comparaison B Analyse *live* avec référence disponible (cas concret avec rapport)

Programme du 2ème jour

08h30	15'	**Discussion**	Synthèse du 1er jour
08h45	30'	**Cours 5**	Réponse aux incidents
09h15	60'	**Labo 5**	Réponse d'incident *live* puis analyse approfondie du *malware* dans un *sandbox*
10h15	30'	**Pause**	Discussion
10h45	45'	**Cours 6**	Système de fichiers NTFS
11h30	30'	**Labo 6**	Analyse du système de fichier NTFS Limitations de NTFS
12h00		**Repas**	
13h30	45'	**Cours 7**	Récupération de fichiers et effacement sûr
14h15	45'	**Labo 7**	Récupération de fichiers supprimés grâce à A Analyse de la MFT B *Data Carving*
15h00	30'	**Pause**	Discussion
15h30	45'	**Labo 8**	Effacement sûr de fichiers et stérilisation du disque dur
16h15	30'	**Evaluation**	
16h45	15'	**Conclusion**	

Principaux *malwares* utilisés dans les labo :

rootkit, cheval de Troie, *backdoor*, *keylogger*

Outils du *response kit* utilisés dans les labo :

auditpol, autorunsc, cmd, cryptcat, date, dd, doskey, driverquery, fport, handle, listdlls, md5deep, nc (netcat), netstat, pclip, promiscdetect, psexec, psinfo, pslist, psloggedon, systeminfo, rootkitrevealer, arm, autoruns, filemon, procexp, regmon, restoration, strings, touchpro

Outils *forensics* utilisés :

Sleuthkit, Cygwin, VMware, X-Ways Forensic

Principales références utilisées pour la partie théorique :

Foundstone : *Incident Response & Computer Forensic*, Russinovich : *Windows Internals*, Carvey : *Windows Forensics & Incident Recovery*, Skoudis : *Malware*, Carrier : *File System Forensic Analysis*