CONSTRUISONS ENSEMBLE
LA DÉFENSE DE DEMAIN

COURS
WINDOWS ET LA SÉCURITÉ

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE

TP2

TP2

TP 2.1 Mise à jour de Windows

- Lancer la VM vm1 et se connecter : admin/azerty
- Lancer le patch : Windows6.1-KB3045171-x86.msu
- Redémarrer la VM vm1 et se connecter : titi/football
- Lancer le binaire Taihou32.exe (bureau)
- Changer d'utilisateur admin/azerty (ne pas fermer la session)

TP2

TP 2.2 Signature des binaires et des drivers

- *Lancer la VM vm1 et se connecter : admin/azerty*
- **Lancer Procexp.exe (Bureau) en tant qu'administrateur (clic droit)**
- **Trouver un binaire signé par Oracle**
- **Trouver un binaire non signé et le tuer**
- **Lancer autorun.exe (Bureau) en tant qu'administrateur (clic droit)**
- **Trouver le service signé par Oracle**
- **Trouver le driver signé par Oracle**

TP2

TP 2.3 Chiffrement de volume

- *Démarrer la VM vm1*
- **Se connecter : titi/football**
- **Lancer TrueCrypt (Bureau)**
- **Créer conteneur chiffré de 10Mo c:\TPs\Secret.tc avec le mot de passe : supermot2pass**
- **Monter le conteneur sur la lettre F: (Select file)**
- **Déplacer Secret.txt dans le volume**

TP2

TP 2.4 Analyse mémoire

- Changer d'utilisateur sans fermer la session
- Se connecter admin/azerty
- Lancer RamCapturer (bureau)
- Capturer la mémoire dans c:\TPs\
- Analyser la mémoire pour retrouver la MasterKey du montage TrueCrypt :

volatility.exe –f 2015… .mem --profile=Win7SP1x86 truecryptmaster -D .

- Lancer TrueCrypt et utiliser la Masterkey pour monter le volume

TP2

TP 2.5 Désinstallation d'un patch

- *Lancer la VM vm1*
- **Se connecter admin/azerty**
- **Lancer le panneau de configuration**
- **Lancer « Désinstaller un programme »**
- **Désinstaller le patch : KB3045171**
- **Redémarrer**
- **Valider le bon fonctionnement du binaire Taihou32.exe (bureau)**