CONSTRUISONS ENSEMBLE
LA DÉFENSE DE DEMAIN

COURS
WINDOWS ET LA SÉCURITÉ

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE

TP1

TP1

TP 1.1 Découverte des binaires et des DLLs

- Lancer la VM vm1 et se connecter : titi/football
- Lancer le Firefox
- Lancer Procexp.exe (Bureau)
- Trouver et cliquer sur firefox.exe et visualiser :
  - Les dépendances des DLLs du système
  - Les dépendances des DLLs l'application
  - Les différents types de handles
  - Les threads
  - Les connexions réseau
  - Le SID du propriétaire du processus, les ACL et les privilèges

TP1

TP 1.2 Exploiter une faille pour élever les privilèges

- *Lancer la VM vm1 et se connecter : titi/football*
- **Lancer cmd (bureau)**
- **Essayer de créer un répertoire : mkdir c:\windows\test**
- **Fermer cmd**
- **Lancer le binaire Taihou32.exe (bureau)**
- **Essayer de créer un répertoire : mkdir c:\windows\test**
- **Avec l'explorateur de fichier, vérifier la présence du répertoire c:\windows\test**
- **Dans la fenêtre cmd :**
  - **cd ..**
  - **rmdir test**

TP1

TP 1.3 Manipulation de la base de registre

- *Lancer la VM vm1 et se connecter : titi/football*
- **Lancer Internet Explorer pour voir la page d'accueil**
- **Lancer regedit.exe (Bureau)**
- **Dans** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\ **modifier la clé « Start page » par « http://www.hack.com »**
- **Cliquer sur l'icone de la maison (Accueil)**

TP1

TP 1.4 Manipulation d'un emplacement de démarrage auto.

- *Lancer la VM vm1 et se connecter : titi/football*
- *Lancer regedit.exe (Bureau)*
- **Dans Ajouter une « valeur chaine » nommée « lauch firefox » contenant la valeur « firefox » dans** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- **Se déconnecter et se reconnecter : titi/football**
- **Vérifier que firefox se lance bien tout seul**
- **Lancer autoruns.exe (Bureau)**
- **Désactiver « Lauch firefox »**

TP1

TP 1.5 Manipulation des services

- *Lancer la VM vm1 et se connecter : titi/football*
- **Lancer services (Bureau)**
- **Trier sur la colonne « Type de Démarrage »**
- **Chercher et essayer de désactiver le service « Pare-feu Windows »**
- **Se reconnecter à la VM : admin/azerty**
- **Lancer services (Bureau)**
- **Chercher, arrêter et désactiver le service « Pare-feu Windows » et « Centre de sécurité »**

TP1

TP 1.6 Générer un BSOD

- *Lancer la VM wm1 et se connecter : admin/azerty*
- **Lancer Procexp.exe en tant qu'administrateur (Bureau)**
- **Trouver et sélectionner sur csrss.exe**
- **Clic droit pour tuer le processus (Kill)**
- **Visualiser le BSOD**