Master 2 SeCReTS 2021-2022
Module Sécurité Windows

Merci de bien lire les consignes :

— aucune communication ;
— aucun accès à un ordinateur, une station de travail, un téléphone portable, une calculatrice, un PDA ou tout autre dispositif électronique, connectable ou non ;
— sujet à remettre en fin d'examen ;
— n'oubliez pas d'**indiquer nom et prénom sur la copie**.

Examen sur 30 points. Un point bonus est attribué au soin et à la précision dans la rédaction des réponses.

Première partie

Sécurité du système Windows (14 points)

1. *(1 pt)* Qu'est-ce qu'un PE ? Donnez 2 exemples de PE.
2. *(1.5 pt)* Donnez 3 différences entre l'exécution en mode noyau et l'exécution en mode utilisateur.
3. *(1.5 pt)* Comment limiteriez-vous l'impact de la compromission d'un service Windows ?
4. *(1 pt)* Quels éléments du jeton d'accès peuvent être utilisés pour accorder des accès ?
5. *(1 pt)* Expliquez brièvement ce qu'est un privilège. En quoi les droits d'authentification (*logon rights*) sont différents ?
6. *(3 pts)* Expliquez avec le maximum de détails possible le chemin d'éxecution, du *user mode* au *kernel mode*, d'un appel à la fonction *ReadFile* de *kernel32.dll*.
7. *(2 pts)* Imaginez une façon de passer administrateur avec le privilège *SeTakeOwnershipPrivilege* (ce privilège permet de devenir propriétaire de n'importe quel objet).
8. *(1 pt)* Quelles parties de la base de registre faut-il récupérer pour obtenir les secrets d'authentification locaux ?
9. *(2 pts)* Déterminez si le jeton d'accès suivant donne accès en écriture au fichier ayant le descripteur de sécurité suivant. Expliquez votre raisonnement :

   Jeton d'accès :

```
C:\Users\Toto>whoami /all

USER INFORMATION
----------------

User Name            SID
==================== ============================================
DOMAIN\toto S-1-5-21-735988197-2306165872-2260703477-1001


GROUP INFORMATION
-----------------

Group Name                             SID          Attributes
====================================== ============ ==============================
Everyone                               S-1-1-0      Mandatory group, Enabled group
BUILTIN\Administrators                 S-1-5-32-544 Group used for deny only
BUILTIN\Performance Log Users          S-1-5-32-559 Mandatory group, Enabled group
BUILTIN\Users                          S-1-5-32-545 Mandatory group, Enabled group
NT AUTHORITY\INTERACTIVE               S-1-5-4      Mandatory group, Enabled group
CONSOLE LOGON                          S-1-2-1      Mandatory group, Enabled group
NT AUTHORITY\Authenticated Users       S-1-5-11     Mandatory group, Enabled group
NT AUTHORITY\This Organization         S-1-5-15     Mandatory group, Enabled group
```

```
NT AUTHORITY\Local account          S-1-5-113    Mandatory group, Enabled group
LOCAL                               S-1-2-0      Mandatory group, Enabled group
NT AUTHORITY\NTLM Authentication    S-1-5-64-10  Mandatory group, Enabled group


PRIVILEGES INFORMATION
----------------------

Privilege Name                  Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```

Descripteur de sécurité au format SDDL :

```
O:S-1-5-18G:S-1-5-21-735988197-2306165872-2260703477-512D:(A;ID;FA;;;SY)
(A;ID;FA;;;BA)(A;ID;FR;;;S-1-5-11)(D;ID;FA;;;S-1-5-21-735988197-2306165872-
2260703477-1001)
```

Aide à la lecture du format SDDL :

— A : ACCESS_ALLOWED_ACE_TYPE
— D : ACCESS_DENIED_ACE_TYPE
— ID : l'ACE est héritée
— FA : FILE_ALL_ACCESS
— FR : FILE_GENERIC_READ
— BA : Groupe Administrateurs
— SY : Système local

Deuxième partie

Domaines Windows (9 points)

1. *(1 pt)* Donnez deux attributs identifiant de manière unique un utilisateur d'un domaine.
2. *((1 pt)* Si je trouve dans mon domaine un compte avec l'attribut "AdminCount" à 1, qu'est-ce que cela implique ?
3. *(2 pts)* Citez au moins 2 ports ouverts sur un contrôleur de domain. Indiquez à quoi ils sont associés.
4. *(1 pt)* À quel groupe pouvez-vous ajouter un utilisateur pour lui donner le contrôle du domaine ?
5. *(1 pt)* Où sont stockées les informations relatives aux GPO ?
6. *((1 pt)* La GPO "MA_GPO_1" est appliquée en mode "enforced" sur la racine d'un domaine. Où et dans quel mode peut-on ajouter une GPO pour modifier les paramètres définis par la GPO "MA_GPO_1" ?
7. *(1 pt)* Il y a une relation d'approbation entre les domaines Active Directory uvsq.fr et ens.fr : le domaine ens.fr approuve de manière non-transitive uvsq.fr. Qu'est-ce que cela implique pour un utilisateur ayant un compte dans le domaine uvsq.fr ? Même question pour un compte dans le domaine ens.fr.
8. *(1 pt)* Quelle partie d'une ACE permet de désigner un droit étendu ? Donnez un exemple de droit étendu.

Troisième partie

Scénario d'intrusion (7 points)

1. (1 pt) Que cherche à faire un attaquant après avoir exploité une vulnérabilité dans un service ?
2. (2 pts) Quel outil sous windows permet de restreindre les programmes exécutables par les utilisateurs ? Quelles sont ses contraintes ?
3. (2 pts) Expliquez le principe de l'attaque Pass The Hash. Quel type de hash utilise-t-on dans le cadre de cette attaque ?
4. (2 pts) Expliquer le principe de l'administration en silos et ce que ça apporte en terme de sécurité.

GLHF!