Master 2 SeCReTS 2020-2021
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 (13 points)

1. *(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 *ReadFileEx* de *kernel32.dll*.
2. *(3 pts)* Lors d'une tentative d'accès en lecture à un fichier , quelles informations SRM analyse dans le jeton d'accès et le descripteur de sécurité. Précisez à quelles entités le jeton d'accès et le descripteur de sécurité sont accociés dans cette situation.
3. *(2 pts)* Imaginez une façon de passer administrateur avec le privilège *SeDebugPrivilege* (ce privilège permet de lire la mémoire de tous les processus).
4. *(1.5 pt)* Quelles parties de la base de registre faut-il récupérer pour obtenir les secrets d'authentification locaux ?
5. *(3 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

6. *(0,5 pt)* À quel compte correspond ce SID : S-1-5-21-3535373721-3146749226-1307819366-1000

Deuxième partie

Domaines Windows (9 points)

1. *(1 pt)* Dans le schéma, la classe *Person* hérite de *Top*. Qu'est-ce que cela implique ?
2. *(1 pt)* Donnez deux attributs identifiant de manière unique un utilisateur d'un domaine.
3. *(2 pts)* Sur les DC, quels éléments (fichiers, bases de données, processus...) spécifiques à leur rôle dans le domaine peut-on trouver ?
4. *(1 pt)* Une GPO au niveau de l'OU contenant la machine *station-001.uvsq.fr* autorise via une règle de pare-feu la connexion vers le port 22 en TCP. Une GPO au niveau du domaine interdit via une règle de pare-feu la connexion vers le port 22 en TCP.
   Quelle règle s'applique sur la machine *station-001.uvsq.fr* ?
5. (1 pt) Où sont stockées les informations relatives aux GPO ?
6. (1 pt) Donnez un exemple de technique de persistance qui peut être trouvée à l'aide d'un outil comme *AD-Control-Paths*.
7. *(2 pts)* Quelle relation d'approbation existe-t-il entre la racine d'un arbre et un de ces sous-domaines (entre *uvsq.fr* et *ufr.uvsq.fr* par exemple) ? Qu'est-ce que cela implique pour les utilisateurs du domaine *uvsq.fr* ?

Troisième partie

Scénario d'intrusion (8 points)

1. *(2 pts)* Donnez les 3 étapes principales d'une intrusion et expliquez chacune d'elle.
2. *(1 pt)* Quelle étape d'une intrusion l'administration en silos permet-elle de bloquer ?
3. *(2 pts)* À quoi sert Applocker ? Donnez un scénario d'attaque pouvant être bloqué par la mise en place d'Applocker.
4. *(1 pt)* Donnez deux faiblesses du hash NTLM.
5. *(2 pts)* Expliquez le principe du Golden Ticket et ce qu'il permet de faire. Un schéma pourra illustrer votre réponse.

Fin de l'examen.