Master 2 SeCReTS 2019-2020
Module Sécurité Windows

Merci de bien lire les consignes :
- une seule feuille A4 manuscrite autorisée ;
- 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 *CreateFile* 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. *(2 pts)* Quelles avantages y a-t-il à utiliser Kerberos par rapport à NTLMv2 ?
6. *(1 pt)* Pourquoi l'utilisation d'un service plutôt qu'une tâche planifiée est plus discret pour la persistance ?
7. *(0,5 pt)* À quel compte correspond ce SID : S-1-5-21-3535373721-3146749226-1307819366-500

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. *(0,5 pt)* Un utilisateur peut-il être dans plusieurs OU ?
3. *(0,5 pt)* Un utilisateur peut-il être dans plusieurs groupes ?
4. *(2 pts)* Sur les DC, quels éléments (fichiers, bases de données, processus...) spécifiques à leur rôle dans le domaine peut-on trouver ?
5. *(1 pt)* Une GPO au niveau de l'OU de la machine *station-001.uvsq.fr* autorise via une règle de pare-feu la connexion vers le port 22 en TCP. Dans les LGPO de la machine *station-001.uvsq.fr*, une règle de pare-feu interdit la connexion vers le port 22 en TCP.
   Quelle règle s'applique sur la machine ?
6. (1 pt) Où sont stockées les informations relatives aux GPO ?
7. (1 pt) Donnez un exemple de technique de persistance identifiable à l'aide d'un outil comme *AD-Control-Paths* d'un attaquant qui aurait obtenu les droits d'administrateur de domaine.

8. *(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.
