TD

Exercice 01

- Lequel des énoncés suivants définit le mieux la stéganographie ?
  1. La stéganographie est utilisée pour masquer les informations dans les fichiers existants.
  2. La stéganographie est utilisée pour créer des valeurs de hachage de fichiers de données.
  3. La stéganographie est utilisée pour chiffrer les communications de données, permettant les fichiers doivent être transmis sans être vus.
  4. La stéganographie est utilisée pour créer des fichiers de communication multimédia.

- Quelle norme de cryptage est utilisée par LM ?
  1. MD5
  2. SHA-1
  3. DES
  4. SHA-2
  5. 3-DES

- Lequel des éléments suivants serait considéré comme une attaque de mots de passe passive en ligne ?
  1. Deviner les mots de passe par rapport à un partage IPC$
  2. Renifler (sniffer) le trafic de sous-réseau pour intercepter un mot de passe
  3. Exécution de John the ripper sur une copie volée du SAM
  4. Envoi d'un PDF spécialement conçu à un utilisateur pour que cet utilisateur puisse l'ouvrir

- Un utilisateur du réseau de l'ANDRU n'a pas besoin de mémoriser un mot de passe long. Les utilisateurs du réseau de l'ANDRU se connectent à l'aide d'un jeton et d'un code PIN à quatre chiffres. Quelle mesure d'authentification décrit le mieux cela ?
  1. Authentification multi facteur
  2. Authentification à trois facteurs
  3. Authentification à deux facteurs
  4. Authentification par token

- Lequel des énoncés suivants définit le mieux une attaque hybride ?
  1. L'attaque utilise une liste de dictionnaires, essayant des mots provenant d'emplacements aléatoires dans le fichier jusqu'à ce que le mot de passe soit piraté.
  2. L'attaque tente des combinaisons aléatoires de caractères jusqu'à ce que le mot de passe soit déchiffré.
  3. L'attaque utilise une liste de dictionnaire, en remplaçant les lettres, les chiffres et les caractères dans les mots jusqu'à ce que le mot de passe soit déchiffré.
  4. L'attaque utilise des tables arc-en-ciel, tentant de manière aléatoire des valeurs de hachage dans la liste jusqu'à ce que le mot de passe soit déchiffré.

- En testant un client, vous découvrez que le hachage LM, sans salage, est toujours activé pour la compatibilité ascendante sur la plupart des systèmes. Un hachage de mot de passe volé indique 9FAF6B755DC38E12AAD3B435B51404EE. Cet utilisateur suit-il de bonnes procédures de mot de passe ?
  1. Oui, le hachage affiche un mot de passe complexe de 14 caractères.
  2. Non, le hachage affiche un mot de passe de 14 caractères ; cependant, il n'est pas complexe.
  3. Non, le hachage révèle qu'un mot de passe de 7 caractères ou moins a été utilisé.
  4. Il est impossible de le déterminer simplement en regardant le hachage.

- Où est stocké le fichier SAM sur un système Windows 7 ?
  1. /etc/
  2. C:\Windows\System32\etc\
  3. C:\Windows\System32\Config\
  4. C:\Windows\System32\Drivers\Config

- En examinant un serveur de base de données lors d'une maintenance de routine, vous découvrez une heure manquante dans le fichier journal, durant les heures de fonctionnement normales. Une enquête plus approfondie ne révèle aucune plainte d'utilisateur concernant l'accessibilité. Parmi les propositions suivantes, laquelle est l'explication la plus probable ?
  1. Le fichier journal est simplement corrompu.
  2. Le serveur a été compromis par un attaquant.
  3. Le serveur a été redémarré.
  4. Aucune activité ne s'est produite pendant la période d'une heure.

- Lequel des éléments suivants peut migrer le système d'exploitation actuel de la machine vers une machine virtuelle ?
  1. Rootkit au niveau de l'hyperviseur
  2. Rootkit au niveau du noyau
  3. Rootkit virtuel
  4. Rootkit au niveau de la bibliothèque

- Après avoir accédé à une machine Windows, vous voyez que la dernière commande exécutée sur la box ressemble à ceci : *net use F : \\MATTBOX\BankFiles /persistent : yes* En supposant que l'utilisateur dispose des informations d'identification appropriées, lesquels des énoncés suivants sont vrais ? (Choisissez tout ce qui correspond.)
  1. Dans l'Explorateur Windows, un dossier apparaît sous le répertoire racine nommé BankFiles.
  2. Dans l'Explorateur Windows, un lecteur apparaît désigné par BankFiles (\\MATTBOX) (F:).
  3. Le lecteur mappé restera mappé après un redémarrage.
  4. Le lecteur mappé ne restera pas mappé après un redémarrage.

- Un attaquant a caché badfile.exe dans le fichier readme.txt. Parmi les commandes suivantes, laquelle est la bonne commande pour exécuter le fichier ?
  1. start readme.txt>badfile.exe
  2. start readme.txt:badfile.exe
  3. start badfile.exe > readme.txt
  4. start badfile.exe | lisezmoi.txt

- Vous voyez la commande suivante dans un examen du fichier historique Linux : someproc & Lequel des énoncés suivants décrit le mieux le résultat de la commande ? (Choisir deux.)

1. Le processus someproc s'arrêtera lorsque l'utilisateur se déconnectera.
2. Le processus someproc continuera à s'exécuter lorsque l'utilisateur se déconnectera.
3. Le processus someproc s'exécutera en tâche de fond.
4. Le processus someproc invitera l'utilisateur à se déconnecter.

Exercice 02

- Comment s'appelle le processus permettant de masquer du texte dans une image ?
- Qu'est-ce qu'un rootkit ?
- Qu'est-ce que l'escalade de privilèges
- Citer deux méthodes utilisées pour masquer des fichiers ?
- Rai est une hackeuse éthique certifiée ainsi qu'une enquêteuse certifiée en piratage informatique travaillant en tant que consultante en sécurité informatique. Rai a été embauchée par Kiley Innovators, une grande société de marketing qui a récemment subi une série de vols et d'incidents d'espionnage industriel. Rai apprend qu'une société de marketing rivale a sorti un produit identique juste avant que le produit de Kiley Innovators ne soit lancé. L'équipe de direction estime qu'un employé divulgue des informations à l'entreprise rivale. Rai interroge tous les employés, examine les journaux du serveur et les journaux du pare-feu ; après quoi elle ne trouve rien. Rai est alors autorisée à effectuer une recherche dans le système de messagerie de l'entreprise. Elle effectue une recherche par courrier électronique reçus et envoyé par la société de marketing rivale.
  Elle trouve un employé qui semble envoyer de très gros e-mails à cette autre société de marketing, même s'il ne devrait avoir aucune raison de communiquer avec elle.
  Rai traque les e-mails réellement envoyés et, lors de leur ouverture, ne trouve que les fichiers image qui y sont joints. Ces fichiers semblent parfaitement inoffensifs et contiennent généralement une sorte de blague.
  Selon vous que dois suspecter Rai ? et que doit-elle faire exactement ?