Université Ferhat Abbas. Sétif -1
Faculté des Sciences – Département D'informatique

Corrigé type de l'examen de sécurité informatique - LA3 -2018

Enseignant : *BOULDJADJ Samir*

Exercice 1 : 10 pts (2pts X 5)

1. C'est l'analyse heuristique. Le moteur heuristique analyse le code des fichiers exécutables pour y détecter les différents types de logiciels malveillants non détectés à l'aide de signatures antivirus. En d'autres termes, il permet de détecter des virus inconnus. Lors de l'analyse d'une application, l'analyseur émule son exécution dans un endroit sûr et enregistre toutes les actions "suspectes", telles que l'ouverture ou l'écriture dans un fichier, ou encore l'interception de vecteurs d'interruption, etc. Grâce à cet enregistrement, il est possible de se prononcer sur une éventuelle infection d'un logiciel par un code malicieux....
2. En utilisant un VPN, On constate généralement une dégradation de performance du système (connexion lente, machine moins rapide,…) et ça peut être expliquez par le fait que l'établissement du tunnel exige des calculs supplémentaires (chiffrement et déchiffrement) ainsi que l'augmentation de nombre de bits échangés.
3. L'ingénierie sociale consiste à utiliser les moyens de communication usuels (téléphone, email, socials media…) et en usurpant une identité, le pirate cherche à obtenir des renseignements confidentiels auprès du personnel d'une l'entreprise (il vise les personnes les plus faibles de l'entreprise, à savoir le personnel non technique (secrétaires, comptables...) et les personnes récemment recrutées) en vue d'une intrusion future. Seule une bonne formation du personnel permet de se protéger de cette attaque.
4. Dans ce cas-là, L'attaque par force brute n'est pas praticable vu le temps de calcul exponentiel (contrainte de temps), idem pour l'attaque par dictionnaire vu le nombre énorme de la taille du dictionnaire (contrainte de mémoire), donc la technique envisageable consiste à faire un compromis entre les deux (compromis temps-mémoire) i.e : on travaille sur un dictionnaire de taille raisonnable en faisant moins de calcul, comme exemple de cette technique on cite les Tables arc en ciel.
5. L'attaque par downgrade consiste à profiter d'une option de compatibilité de certains programmes réseau (serveur web notamment) ; l'attaquant demande au serveur d'utiliser une version d'un protocole plus ancienne afin d'exploiter les failles qu'elle comporte, elle peut s'effectuer sur toutes les applications réseau qui comportent des fonctionnalités de compatibilité avec d'anciennes versions. C'est notamment le cas de SSH1, PPTP, ou encore des protocoles de sécurité WiFi (certaines bornes permettent d'utiliser à la demande soit WPA2 soit WPA)

Exercice 2 : 10 pts (1pt X 10)

1- Cheval de Troie
2- Aucune réponse
3- DNS Spoofing
4- Algorithmes à clé secrète
5- Le chiffrement
6- Pare-feu
7- Injection SQL
8- Cheval de Troie
9- Se propage par le réseau
10- Compliquer la prédiction de N° séquence TCP