Université des Sciences et de la Technologie Houari Boumediene
FACULTE D'INFORMATIQUE

M1-SSI **Introduction à la sécurité** **2023-2024**

Nom : …… Prénom : ……

Epreuve de Moyenne Durée 15

- Documentation autorisée ;
- ***L'utilisation des téléphones est strictement interdite. L'usage des PC est autorisé ;***
- ***Les PCs ne peuvent être utilisés uniquement pour consulter la documentation et effectuer des recherches via les moteurs de recherche. Tout autre usage sera considéré comme une fraude***
- ***Tout inscription en dehors de l'espace réservé à cet effet ne sera pas prise en considération***
- ***Fournissez des réponses courtes et claires***

Exercice 01 (3pts)

- Etant un pirate informatique expérimenté, rayane lance une attaque réseau contre l'entreprise DJARRY et obtient un accès non autorisé au réseau cible. Il parvient à rester six(06) mois dans le réseau sans être détecté et obtient des informations sensibles sans saboter DJARRY. Comment s'appelle la technique d'attaque utilisée par Rayane ?

…… ***APT***…….

- Yousr souhaite collecter des informations sur des sites web similaires au site web http://www.white house.gov. Que doit-il faire ?

……***Il peut utiliser les google dork tel que related***

- Houari teste le serveur et le site Web de l'USTHB pour identifier les failles de sécurité. Au cours de ce processus, il a copié le site Web et son contenu sur sa machine pour afficher le profil complet de la structure des répertoires du site, de la structure des fichiers, des liens externes, des images, des pages Web, etc. Ces informations aident houari notamment à cartographier les répertoires du site Web. Quelle est la technique d'attaque utilisée par Houari dans le scénario ci-dessus ?

Website mirroring /web scrapping

Exercice 02

Vous venez d'obtenir votre badge "Advent of Cyber" ce qui atteste du fait que vous avez acquis les connaissances nécessaires pour effectuer certaines opérations liées à la sécurité informatique. Dans ce contexte, vous êtes recrutés par une entité pour effectuer des pentest sur certains réseaux informatiques. A cet effet, on vous avez un entretien avec votre recruteurs.

Recruteur : connaissez-vous la méthode appelée chain killer cybernetique qui permet d'identifier les étapes suivies par un attaquant ? **(0,5pts)**

Vous : ***non à moins que vous vouliez parler de la Cyber kill chain***

Recruteur : elle se compose de neuf étapes c'est bien ça ? pouvez-vous me les citer ? (**0,5 +1,5pt)**

Vous : ***je pense que vous confondez, cette approche se compose de sept étapes à savoir : la reconnaissance, l'armement, la délivrance, l'exploitation, l'installation, command & control et actions sur l'objectifs***

Recruteur : j'ai entendu parler des indicateurs de compromission mais je n'arrive pas à comprendre la différence entre les indicateurs basés host et les indicateurs basés sur le comportement **(1pt)**

Vous : ***Les indicateurs basés host sont collectées à partir d'un hôte. Ils peuvent inclure des fichiers, des processus, des connexions réseau, des modifications de registre, etc. Les indicateurs basés comportement sont collectées sur le comportement d'un hôte. Ils peuvent inclure des événements de sécurité, des anomalies dans l'utilisation des ressources, Un utilisateur qui essaie de se connecter à un compte avec un mot de passe incorrect, Un utilisateur qui essaie d'accéder à des fichiers ou à des dossiers auxquels il n'a pas le droit d'accéder***

Suite à cet entretien on décide de vous recruter pour une période d'essai et on vous demande de traiter une cible nommée téta, pour cela on vous fournit un URL et une adresse IP publique, cependant vous remarquez que l'URL ne correspond pas à l'adresse IP publique. Comment allez-vous effectuer votre reconnaissance passive **(2pts)**

Le fait que l'adresse IP ne correspond pas à l'URL est problématique. Il est nécessaire de faire les vérifications nécessaires pour s'assurer que les deux appartiennent au client. Ensuite vous devez établir le lien existant entre les deux. La réponse doit inclure les étapes permettant d'exécuter les étapes citées supra

Finalement vous découvrez que l'une de vos cibles est une entreprise située aux USA. Votre recruteur vous demande d'utiliser Edgar pour avoir un maximum d'information. Comment ferez-vous ? **(1pt)**

N'étant pas citoyen américain, je ne peux pas utiliser Edgar contre une entreprise située aux Etats-Unis

Suite aux informations obtenues, votre recruteur vous demande de ne plus vous intéressez à l'entreprise située sur le sol américain et de vous concentrer sur celle située en Afrique.

Vous avez découvert que la cible possède un serveur web qui utilise à la fois du http et du HTTPS et vous désirez faire un scan de port, vous commencer par les ports 443 et 80, pour cela vous utilisez un zombie par lequel vous envoyez un paquet P1au port 80 et un paquet P2 pour le port 443.

Pour le P1 vous recevez un premier RST avec un IPID= 45318 et un second RST avec IPID = 45320

Pour le P2 vous recevez un premier RST avec un IPID= 45605 et un second RST avec IPID = 45606

Que pouvez conclure ? **(1pt)**

Tel que vu en cours l'un est ouvert et l'autre est fermé

Comment pouvez vous expliquer cela, sachant que les protocoles http et HTTPS fonctionnent lors de la navigation web **(2pts)**

On soupçonne la présence d'un parfeu qui bloque l'accès à l'un des deux ports

Lors de votre analyse vous découvrez un fichier compressé nommé « FYE-Adminonly.rar » qui date de 2005.quand vous essayez de l'ouvrir, vous découvrez qu'il est protégé par un mot de passe. Apres quelques tentatives vous arrivez à la conclusion que le mot de passe est complexe. Veuillez décrire en détail ce que vous devez faire pour ouvrir ce fichier, sachant que vous ne disposez que de votre laptop que vous utilisez dans votre travail quotidien et que vous êtes amenés à prendre avec vous lors de vos déplacements. Evidemment vous avez accès aux ressources internet **(3pts)**

Plusieurs réponses peuvent être correctes :

L'exploitation des vulnérabilités de la méthodologie de chiffrement de 2005 (assez fastidieuse comme approche)

Utiliser des outils en ligne ou distribués pour faire des attaques de brute de force

Finalement vous décidez d'introduite un malware de type APT dans les systèmes de votre cible. Veuillez décrire dans les détails la méthodologie de conception de ce malware, sa charge utile, son type, ses techniques d'évasions, les outils et composants utilisés etc…

……***une infinité de scénario existe en se basant sur les étapes vues en cours***

Exercice 03 (03 pts)

Vous devez récupérer le mot de passe du PC de votre chargé de cours du module introduction à la sécurité en utilisant l'ingénierie sociale et plus précisément la technique MICE. Veuillez donner un scénario faisable permettant d'obtenir un résultat positif (tous les coups sont permis)

Une infinité de scénario existe