

QCM 1 – Python, Reconnaissance, Armement

1. Quel est l'avantage principal de Python pour le pentest ?
 - a) C'est un langage compilé
 - b) Il fonctionne uniquement sous Windows
 - c) Il permet d'automatiser des attaques
 - d) Il nécessite peu de mémoire
2. Qu'est-ce qu'un test d'intrusion ?
 - a) Un scan de vulnérabilités passif
 - b) Une analyse du trafic DNS
 - c) Une tentative contrôlée d'attaquer un SI
 - d) Une surveillance continue d'un réseau
3. Quelle bibliothèque est utilisée pour créer et manipuler des paquets réseau en Python ?
 - a) Requests
 - b) BeautifulSoup
 - c) Scapy
 - d) Mechanize
4. Le scan TCP SYN est aussi appelé :
 - a) Scan total
 - b) Scan semi-ouvert
 - c) Scan caché
 - d) Scan ICMP
5. Quel est l'objectif d'un scan UDP ?
 - a) Établir une connexion persistante
 - b) Envoyer des paquets ICMP
 - c) Identifier les ports TCP ouverts
 - d) Détecter des services sans handshake
6. Quel outil permet de capturer et modifier des paquets réseau ?
 - a) dpkg
 - b) dpkt
 - c) OpenSSL
 - d) bcrypt
7. Quelle technique permet de capturer des infos HTTP en HTML ?
 - a) Bruteforcing
 - b) Sniffing
 - c) Web scraping
 - d) Probing

8. Quel outil est recommandé pour l'automatisation de formulaires web ?
 - a) Mechanize
 - b) dpkt
 - c) hashlib
 - d) flask
9. Quel type d'attaque consiste à tester toutes les combinaisons possibles ?
 - a) Rainbow
 - b) Dictionnaire
 - c) Injection
 - d) Force brute
10. Quel fichier Linux contient les hash des mots de passe ?
 - a) /etc/host
 - b) /etc/passwd
 - c) /etc/shadow
 - d) /etc/login
11. Que contient le fichier `/etc/passwd` ?
 - a) Les mots de passe hachés
 - b) Les binaires système
 - c) Les comptes utilisateurs
 - d) Le fichier swap
12. Le craquage par dictionnaire est :
 - a) Une attaque aveugle
 - b) Une attaque par permutation brute
 - c) Une attaque ciblée avec des mots connus
 - d) Un scan de ports
13. Que fait une table rainbow ?
 - a) Crée des dictionnaires de mots de passe
 - b) Associe des hash précalculés à leurs valeurs
 - c) Chiffre les fichiers avec AES
 - d) Remplace les shadow passwords
14. Le chiffrement AES est :
 - a) Asymétrique
 - b) Symétrique
 - c) Basé sur des courbes elliptiques
 - d) Obsolète
15. En Python, quel module permet le chiffrement AES ?
 - a) hash
 - b) pycrypto
 - c) flask

d) subprocess

16. Quelle fonction est utilisée pour générer une clef aléatoire ?

- a) rand()
- b) open()
- c) get_random_bytes()
- d) random_str()

17. Quel est le rôle du module RSA dans un ransomware ?

- a) Générer des mots de passe
- b) Créer des adresses IP
- c) Chiffrer les clefs AES
- d) Supprimer les fichiers

18. Quel est l'intérêt d'automatiser l'armement ?

- a) Réduire l'entropie du malware
- b) Augmenter la taille du code
- c) S'adapter rapidement à la cible
- d) Éviter l'utilisation de Python

19. Quelle phase suit immédiatement la reconnaissance ?

- a) Livraison
- b) Maintien
- c) Exploitation
- d) Armement

20. Un ransomware doit :

- a) Supprimer toutes les clefs
- b) Chiffrer les fichiers sans les sauvegarder
- c) Chiffrer puis supprimer les originaux
- d) Utiliser uniquement AES-128

Correction : QCM 1 – Python, Reconnaissance, Armement

- 1 - ☒ c) Il permet d'automatiser des attaques

Python est privilégié en cybersécurité pour son accessibilité et sa capacité à automatiser des tâches complexes comme le scan de ports, la manipulation de paquets, ou la génération de phishing. Ce n'est pas un langage compilé, mais interprété.

- 2 - ☒ c) Une tentative contrôlée d'attaquer un SI

Un test d'intrusion (pentest) simule une attaque réelle pour évaluer la sécurité d'un système d'information. Il va au-delà du scan de vulnérabilité en tentant effectivement d'exploiter les failles.

- 3 - ☒ c) Scapy

scapy est une bibliothèque puissante permettant de construire, envoyer, intercepter, modifier et analyser des paquets réseau de bas niveau (IP, TCP, UDP, etc.).

- 4 - ☒ b) Scan semi-ouvert

Le TCP SYN scan, utilisé par nmap -sS, envoie un paquet SYN puis lit la réponse (SYN-ACK = port ouvert, RST = fermé) sans terminer la connexion. Il est discret et efficace.

- 5 - ☒ d) Détecter des services sans handshake

Les services UDP ne répondent que rarement à des paquets aléatoires, donc l'absence de réponse est la norme. Le scan UDP est utile pour découvrir des services "silencieux", souvent négligés.

- 6 - ☒ b) dpkt

dpkt est une autre bibliothèque Python utilisée pour l'analyse de paquets. Elle permet de parser des captures réseau comme des fichiers .pcap, très utile pour l'analyse passive.

- 7 - ☒ c) Web scraping

Le web scraping consiste à extraire des données structurées (liens, infos, emails...) depuis des pages HTML. BeautifulSoup ou requests sont souvent utilisés.

- 8 - ☒ a) Mechanize

mechanize permet d'automatiser l'interaction avec des formulaires HTML (remplissage et soumission), y compris les champs cachés. Très utilisé dans le phishing automatisé.

- 9 - ☒ d) Force brute

La force brute teste toutes les combinaisons possibles jusqu'à trouver la bonne. Elle est très lente si la complexité est élevée (longueur et caractère du mot de passe).

10 - ☒ c) /etc/shadow

Sous Linux, les hash des mots de passe sont stockés dans /etc/shadow, un fichier protégé. /etc/passwd ne contient que des infos générales sur les comptes.

11 - ☒ c) Les comptes utilisateurs

/etc/passwd liste les noms d'utilisateurs, UID, shell, etc. Historiquement, il contenait aussi les mots de passe chiffrés, mais ils sont désormais déplacés dans /etc/shadow.

12 - ☒ c) Une attaque ciblée avec des mots connus

L'attaque par dictionnaire teste un ensemble limité de mots de passe prévisibles (mots courants, prénoms, suites logiques...). Elle est plus rapide que la brute force.

13 - ☒ b) Associe des hash précalculés à leurs valeurs

Une table rainbow est un tableau qui associe à chaque mot de passe possible son hash. Cela permet d'inverser rapidement un hash sans le recalculer à chaque tentative.

14 - ☒ b) Symétrique

AES (Advanced Encryption Standard) est un algorithme de chiffrement symétrique : la même clef sert au chiffrement et au déchiffrement.

15 - ☒ b) pycrypto

pycrypto ou Crypto (via pycryptodome) est une bibliothèque qui permet d'implémenter AES, RSA, etc. en Python.

16 - ☒ c) get_random_bytes()

Cette fonction génère un flux d'octets cryptographiquement sécurisé, utile pour des clefs ou des vecteurs d'initialisation (IV) dans les algorithmes symétriques.

17 - ☒ c) Chiffrer les clefs AES


Dans les ransomwares hybrides, les fichiers sont chiffrés en AES (rapide) et la clef AES est ensuite chiffrée avec la clef publique RSA de l'attaquant.

18 - ☒ c) S'adapter rapidement à la cible

Automatiser l'armement permet de générer ou adapter un malware en fonction des cibles découvertes (ex : système d'exploitation, ports ouverts, version de logiciels).

19 - ☒ d) Armement

La séquence est : reconnaissance → armement → livraison → exploitation → maintien. Après collecte d'infos, on développe une charge utile adaptée.

20 -  c) Chiffrer puis supprimer les originaux

Un ransomware typique chiffre les fichiers utilisateurs, sauvegarde le contenu chiffré, et supprime les fichiers originaux pour forcer la victime à payer.