Test de connaissances (QCM)

12 octobre 2020

Ahmed Serhrouchni

1. Lequel des éléments suivants serait le meilleur exemple de contrôle dissuasif?

A. Un système d'agrégation de journaux
B. Caméras cachées sur place
C. Un gardien posté devant la porte
D. Systèmes de récupération de sauvegarde

2. Deux hackers tentent de hacker la sécurité des ressources réseau d'une entreprise. L'un est considéré comme un hacker éthique, tandis que l'autre ne l'est pas. Qu'est-ce qui distingue le hacker éthique du «cracker»?

A. Le hacker tente toujours des tests en boîte blanche.
B. Le hacker éthique tente toujours de tester la boîte noire.
C. Le hacker publie les résultats sur Internet.
D. Le hacker éthique demande toujours une autorisation écrite avant le test.

3. Quel type d'attaque est généralement menée en tant qu'attaquant interne avec des privilèges élevés sur les ressources?

A. Boîte grise
B. Boîte blanche
C. Boîte noire
D. Reconnaissance active

4. Votre entreprise a un document qui précise exactement ce que les employés sont autorisés à faire sur leurs systèmes informatiques. Il définit également ce qui est interdit et quelles conséquences attendent ceux qui enfreignent les règles. Une copie de ce document est signée par tous les employés avant leur accès au réseau. Lequel des énoncés suivants décrit le mieux cette politique?

A. Politique de sécurité de l'information
B. Politique d'accès spécial
C. Politique d'audit de l'information
D. Politique de connexion réseau

5. Julien est membre d'une équipe de pentest récemment embauchée pour tester la sécurité d'une banque. il commence à rechercher les adresses IP que la banque peut posséder en recherchant des documents publics sur Internet. Il recherche également des articles de presse et des offres d'emploi pour découvrir des informations qui peuvent être utiles. À quelle phase du pentest cela correspond?

A. Préparation
B. Évaluation
C. Conclusion
D. Reconnaissance

6. Des services de sécurité confidentialité, intégrité et disponibilité, quelle technique assure l'intégrité?

A. Chiffrement
B. Stéganographie
C. Hachage
D. Contrôle d'accès

7. Lors de l'empreinte d'un réseau, vous effectuez avec succès un transfert de zone. Quel enregistrement DNS dans le transfert de zone indique le serveur de messagerie de l'entreprise?
A. MX
B. MS
C. SOA
D. PTR

8. Un attaquant a réussi à accéder à une machine de l'organisation et à s'enfuir avec des données sensibles. Une analyse complète des vulnérabilités a été exécutée immédiatement après le vol et rien n'a été découvert. Lequel des énoncés suivants décrit le mieux ce qui a pu se produire?
A. L'attaquant a profité d'une vulnérabilité zero-day sur la machine.
B. L'attaquant a effectué une reconstruction complète de la machine après avoir terminé.
C. L'attaquant a effectué une attaque par déni de service.
D. Les mesures de sécurité sur l'appareil ont été complètement désactivées avant le début de l'attaque.

9. Quel outil ou technique d'empreinte peut-on utiliser pour trouver les noms et adresses des employés ou des points de contact techniques?
A. whois
B. nslookup
C. host
D. traceroute

9. Quel type d'enregistrement DNS mappe une adresse IP à un nom d'hôte et est le plus souvent utilisé pour les recherches DNS?
A. NS
B. MX
C. A
D. SOA

10. Vous disposez d'un service FTP et d'un site HTTP sur un seul serveur. Quel enregistrement DNS vous permet d'associer (alias) les deux services sur le même enregistrement (adresse IP)?
A. NS
B. SOA
C. CNAME
D. PTR

11. Un membre de votre équipe entre la commande suivante: nmap -sV -sC -O –traceroute IPAddress Laquelle des commandes nmap suivantes effectue la même tâche?
A. nmap -A IPAddress

B. nmap -all IPAddress
C. nmap -Os IPAddress
D. nmap -aA IPAddress

12. Vous souhaitez effectuer une capture de bannière sur une machine que vous suspectez d'être un serveur Web. En supposant que vous ayez installé les bons outils, laquelle des entrées de ligne de commande suivantes effectuera avec succès une capture de bannière? (Choisissez tout ce qui correspond.)

A. Telnet 168.15.22.4 80
B. Telnet 80 168.15.22.4
C. nc –v –n 168.15.22.4 80
D. nc –v –n 80 168.15.22.4

13. Vous avez décidé de commencer l'analyse par rapport à une organisation cible, mais vous souhaitez garder vos efforts aussi silencieux que possible. Quelle technique d'évasion IDS divise l'en-tête TCP en plusieurs paquets?

A. Fragmentation
B. Spoofing
C. Analyse du proxy
D. Anonymiseur

14. Quel (s) flag (s) sont envoyés dans le segment pendant la deuxième étape de la négociation TCP à trois voies?

A. SYN
B. RST
C. SYN / ACK
D. ACK / FIN

15. Vous analysez le port d'un système et commencez à envoyer des paquets TCP avec l'indicateur ACK défini. En examinant les paquets de retour, vous voyez qu'un paquet de retour pour un port a l'indicateur RST défini et le TTL est inférieur à 64. Lequel des énoncés suivants est vrai?

A. La réponse indique un port ouvert.
B. La réponse indique un port fermé.
C. La réponse indique une machine Windows avec une pile TCP / IP non standard.
D. ICMP est filtré sur la machine.

16. Quel flag impose une interruption des communications dans les deux sens?

A. RST
B. FIN
C. ACK
D. PSH

17. Vous examinez un hôte avec une adresse IP de 52.93.24.42/20 et souhaitez déterminer l'adresse de diffusion du sous-réseau. Lequel des éléments suivants est l'adresse de diffusion correcte pour le sous-réseau?

A. 52.93.24.255
B. 52.93.0.255
C. 52.93.32.255
D. 52.93.31.255
E. 52.93.255.255

18. Laquelle des commandes suivantes utiliseriez-vous pour identifier rapidement les cibles actives sur un sous-réseau? (Choisissez tout ce qui correspond.)
A. nmap –A 172.17.24.17
B. nmap –O 172.17.24.0/24
C. nmap –sn 172.17.24.0/24
D. nmap –PI 172.17.24.0/24

19. Vous envoyez le premier paquet TCP (SYN) à la machine cible. Ensuite vous recevez le paquet SYN / ACK est envoyé au zombie. Dans quel état se trouve le port sur la machine cible?
A. Ouvert
B. Fermé
C. Inconnu
D. Aucune de ces réponses

20. Quel type / code de message ICMP indique que le paquet n'a pas pu parvenir au destinataire en raison du dépassement de sa durée de vie?
A. Type 11
B. Type 3, code 1
C. Type 0
D. Type 8

21. Parmi les énoncés suivants, lesquels sont vrais? (Choisissez deux.)
A. WebGoat est maintenu par l'IETF.
B. WebGoat est maintenu par OWASP.
C. WebGoat peut être installé sur Windows ou Linux.
D. WebGoat est conçu uniquement pour les systèmes Apache.

22. Laquelle des commandes suivantes utiliseriez-vous pour identifier rapidement les cibles actives sur un sous-réseau? (Choisissez tout ce qui correspond.)
A. nmap –A 172.17.24.17
B. nmap –O 172.17.24.0/24
C. nmap –sn 172.17.24.0/24
D. nmap –PI 172.17.24.0/24

23. Quel numéro de port est utilisé par défaut pour syslog?
A. 21
B. 23
C. 69
D. 514

24. Quel drapeau impose une interruption des communications dans les deux sens?

A. RST
B. FIN
C. ACK
D. PSH

25. Quel(s) flags(s) sont envoyés dans le segment pendant la deuxième étape de la négociation de la connexion TCP?

A. SYN
B. ACK
C. SYN / ACK
D. ACK / FIN

26. Soit cette commande *nmap -sV -sC -O --traceroute IPAddress*
Laquelle des commandes nmap suivantes effectue la même tâche?

A. nmap -A IPAddress
B. nmap -all IPAddress
C. nmap -Os IPAddress
D. nmap -aA IPAddress

27. Vous analysez le port d'un système et commencez à envoyer des paquets TCP avec le bit ACK positioné. En examinant les paquets de retour, vous voyez qu'un paquet de retour pour un port avec le bit RST positioné et le TTL est inférieur à 64. Lequel des énoncés suivants est vrai?

A. La réponse indique un port ouvert.
B. La réponse indique un port fermé.
C. La réponse indique une machine Windows avec une pile TCP / IP non standard.
D. ICMP est filtré sur la machine.

28. Un hacker éthique envoie des paquets TCP à une machine avec le bit SYN positioné. Aucune des réponses SYN / ACK sur les ports ouverts ne reçoit de réponse. De quel type d'analyse de port s'agit-il?

A. Balayage Ping
B. XMAS
C. Furtif
D. Complet

29. Vous examinez un hôte avec une adresse IP de 52.93.24.42/20 et souhaitez déterminer l'adresse de diffusion du sous-réseau. Lequel des éléments suivants est l'adresse de diffusion correcte pour le sous-réseau?

A. 52.93.24.255
B. 52.93.0.255
C. 52.93.32.255
D. 52.93.31.255

30. Quel type de retour reçoit-on suite un à un scan de port UDP?

A. un ICMP type= 3 et code=0

B. un RST

C. un paquet IP avec le champ CRC à 0

D. un ICMP type= 3 et code=3

31. Un administrateur de sécurité définit l'indicateur HttpOnly dans les cookies. Lequel des éléments suivants tente-t-il probablement d'atténuer?

A. CSRF

B. CSSP

C. XSS

D. Débordement de tampon

32. Vous examinez les fichiers journaux et remarquez plusieurs tentatives de connexion à un serveur Web hébergé. De nombreuses tentatives apparaissent comme telles:

```
http://www.example.com/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/windows\
system32\cmd.exe
```

Quel type d'attaque est utilisé?

A. Injection SQL

B. Altération des paramètres Unicode

C. Directory traversal

D. Cross-site scripting

33. Lequel des éléments suivants serait la meilleure protection contre les attaques XSS?

A. Investissez dans des pare-feu haut de gamme.

B. Effectuez des analyses de vulnérabilité contre vos systèmes.

C. Configurez la validation des entrées sur vos systèmes.

D. Faites effectuer un test de plume sur vos systèmes.

34. Lequel des éléments suivants ne définit pas une méthode de transmission de données qui viole une politique de sécurité?

A. Canal de porte dérobée (Backdoor channel)

B. Session hijacking

C. Covert channel

D. Overt channel

35. Quel type de virus est exécuté uniquement lorsqu'une condition spécifique est remplie?

A. Sparse infector

B. Multipartite

C. Métamorphique

D. Cavité

36. Lequel des éléments suivants se propage sans interaction humaine?

A. Cheval de Troie

B. Ver

C. Virus

D. MITM

37. Lequel des éléments suivants n'utilise pas ICMP dans l'attaque? (Choisissez deux.)

A. SYN Flood

B. Ping of Death

C. Schtroumpf

D. Peer to peer

38. Lequel des éléments suivants n'est pas une étape recommandée pour se remettre d'une infection par un logiciel malveillant?

A. Supprimez les points de restauration du système.

B. Sauvegardez le disque dur.

C. Retirez le système du réseau.

D. Réinstallez à partir du support d'origine.

39. Lequel des énoncés suivants est une recommandation de protection contre le détournement de session? (Choisissez deux.)

A. Utilisez uniquement des protocoles non routables.

B. Utilisez des numéros de séquence imprévisibles.

C. Utilisez une application de vérification de fichiers, telle que Tripwire.

D. Utilisez une bonne politique de mot de passe.

40. Laquelle des options suivantes est la syntaxe appropriée sur les systèmes Windows pour générer un shell de commande sur le port 56 à l'aide de Netcat?

A. nc -r 56 -c cmd.exe

B. nc -p 56 -o cmd.exe

C. nc -L 56 -t -e cmd.exe

D. nc -port 56 -s -o cmd.exe

41. Lequel des énoncés suivants décrit le mieux un DRDoS?

A. Plusieurs machines intermédiaires envoient l'attaque à la demande de l'attaquant.

B. L'attaquant envoie des milliers et des milliers de paquets SYN à la machine avec une fausse adresse IP source.

C. L'attaquant envoie des milliers de paquets SYN à la cible mais ne répond jamais à aucun des paquets SYN / ACK renvoyés.

D. L'attaque implique l'envoi d'un grand nombre de fragments IP tronqués avec des charges utiles surdimensionnées qui se chevauchent à la machine cible.

42. Lequel des énoncés suivants décrit le mieux une attaque Teardrop?

A. L'attaquant envoie un paquet avec la même adresse source et destination.

B. L'attaquant envoie plusieurs fragments IP extrêmement volumineux qui se chevauchent.

C. L'attaquant envoie des paquets d'écho UDP avec une adresse usurpée.

D. L'attaquant utilise la diffusion ICMP vers les cibles DoS.

43. Laquelle des techniques suivantes utilise des hachages précalculés pour le craquage de mot de passe?

A. Attaque par dictionnaire

B. Attaque hybride

C. Attaque de force brute

D. Attaque de la table arc-en-ciel

44. Les chevaux de Troie utilisent un canal secret pour communiquer à distance avec l'attaquant. Vrai ou faux?

A. Vrai

b. Faux

45. Lequel des virus suivants s'est propagé aux documents Microsoft Office comme Word et Excel?

A. Virus de fichier

B. Virus polymorphe

C. Virus macro

D. Aucune de ces réponses

46. Lequel des types de logiciels malveillants suivants apporte des modifications au niveau du noyau pour masquer sa présence?

A. Spyware

B. Worm

C. Keylogger

D. Rootkit

47. Lequel des éléments suivants est une petite information envoyée d'un site Web au système client et conservée pour un suivi ultérieur?

A. HTTP

B. Cookie

C. XML

D. Aucune de ces réponses

48. Il est sûr d'utiliser le même ID de session avant et après la connexion. Vrai ou faux?

A. Vrai

B. Faux

49. Laquelle des attaques suivantes stocke un script en permanence dans les applications vulnérables?

A. Reflected cross-site scripting

B. Injection SQL

C. Persistent cross-site Scripting

D. Aucune de ces réponses

50. Lequel des éléments suivants aiderait à empêcher l'injection SQL?

A. Utilisation de HTTPS

B. Installation d'un logiciel antivirus

C. Utilisation d'une requête paramétrée

D. Tout ce qui précède