Ecole Supérieure de Gestion, d'Informatique et des Sciences

TRAVAUX DIRIGES

***Filière** : Licence 3 IRT-ESGIS Option Architecture Logicielle*

Dossier 1

Choisis la ou les bonne(s) réponse(s) qui convient (conviennent).

1. Lequel (lesquels) des programmes suivants est (sont) un (des) programme(s) malveillant(s) indépendant(s) qui ne nécessite(nt) aucun autre programme ?
   a. Porte à piège
   b. Cheval de Troie
   c. Virus
   d. Ver

2. Lequel (lesquels) des programmes malveillants suivants ne se réplique(nt) pas automatiquement?
   a. Cheval de Troie
   b. Virus
   c. Ver
   d. Zombie

3. Lequel (lesquels) des énoncés suivants décrit (décrivent) une attaque par injection de LDAP ?
   a. Manipulation des requêtes LDAP pour obtenir ou modifier les droits d'accès.
   b. Utilisation de XSS pour diriger l'utilisateur vers un serveur LDAP falsifié.
   c. Envoi de débordement de tampon pour le service de requête LDAP.
   d. Création d'une copie des informations d'identification de l'utilisateur au cours de la session d'authentification LDAP.

4. Laquelle des propositions ci-après décrit une vulnérabilité logicielle exploitant une faille de sécurité avant qu'un patch de protection ne soit disponible ?
   a. Zero day attack
   b. Buffer overflow
   c. Mystification d'adresse MAC
   d. Bluesnarfing

5. Lequel (lesquels) des termes suivants est (sont) spécifiquement conçu(s) pour leurrer et attirer les pirates ?
   a. IDS
   b. IPS
   c. Honey pot
   d. TearDrop

6. Quel type d'attaque nécessite un attaquant pour renifler un réseau ?
   a. Man-in-the-Middle
   b. MAC flooding
   c. DDoS
   d. Zero day exploit

7. Lequel des éléments suivants permet de faire un backdoor caché pour accéder aux postes de travail sur Internet ?
   a. Cheval de Troie
   b. Bombe logique
   c. Firmware
   d. Ver

8. Un _____ est un programme qui prend le contrôle d'un autre ordinateur connecté sur Internet, puis utilise cet ordinateur pour lancer des attaques.
   a. Ver
   b. Zombie
   c. Virus
   d. Trap doors

9. La sécurité informatique est
   a. l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, payer, et garantir la sécurité des systèmes informatiques.
   b. un système d'alerte physique.
   c. l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité des systèmes informatiques.
   d. l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, obéir, et garantir la sécurité des systèmes informatiques.

13. Le chiffrement et le déchiffrement des données sont de la responsabilité de quelle couche dans le modèle OSI ?
   a. Couche de session
   b. Couche réseau

c. Couche transport
d. Couche de présentation

14. Quel procédé permet d'assurer la non-répudiation des données ?
    a. Le chiffrement des données
    b. Le hachage des mots de passes
    c. Le certificat électronique
    d. La signature numérique

15. Quelle technique permet d'assurer l'intégrité des données ?
    a. La signature électronique
    b. Le certificat électronique
    c. Le chiffrement
    d. Toutes les réponses sont vraies.

16. En sécurité informatique, quelle terminologie signifie que les systèmes actifs informatiques ne peuvent être modifiés que par les personnes autorisées.
    a. La confidentialité
    b. L'intégrité
    c. La disponibilité
    d. L'authenticité

19. Lequel des services suivants doit être désactivé pour empêcher les hackers d'utiliser un serveur Web comme un relais de messagerie ?
    a. SMTP
    b. POP3
    c. SNMP
    d. IMAP
    e. Aucune des réponses n'est vraie.

20. Quels sont les types de menaces pour la sécurité d'un système informatique ou d'un réseau ?
    a. Interruption
    b. Interception
    c. Modification
    d. Création
    e. Fabrication

21. Quel est le protocole utilisé parmi ceux-ci pour sécuriser les e-mails ?
    a. POP
    b. PGP
    c. SNMP
    d. HTTP

22. Quelle terminologie représente l'art de casser des chiffres ?
    a. Cryptologie
    b. Cryptographie
    c. Cryptanalyse
    d. Cryptage

23. Quelle terminologie représente la transformation d'un message en format qui ne peut être lu par les pirates en se servant d'une clef ?
    a. Cryptage
    b. Décryptage
    c. Chiffrement
    d. Transformation
    e. Aucune réponse n'est vraie.

24. Quel est le numéro de port du protocole HTTPS ?
    a. 43
    b. 443
    c. 543
    d. 25

25. Les firewalls sont utilisés pour _____ ?
    a. le routage
    b. la sécurité
    c. le tunneling
    d. le contrôle de congestion

Dossier 2

1. Comment savoir si un site est sécurisé ?
    a. Un logo l'indique dans le bas de la page.
    b. L'URL devient verte.
    c. Un cadenas s'affiche à côté de l'adresse du site.
    d. Le certificat numérique du site d'affiche avec les clés de chiffrement.

2. Dans le domaine de la sécurité informatique, une vulnérabilité est :
    a. une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal.
    b. la caractéristique d'une faille.
    c. une faiblesse physique ou logicielle d'une machine permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à

son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

d. Aucune des définitions sus-mentionnées n'est correcte.

3. Les principaux objectifs de la sécurité informatique sont les suivants :
   a. La confidentialité – l'intégrité – la non-répudiation.
   b. La confidentialité – l'authenticité – la non-répudiation.
   c. La confidentialité – l'intégralité – la disponibilité.
   d. La confidentialité – l'intégrité – la disponibilité.

4. La norme ISO traitant des systèmes de management de la sécurité de l'information est :
   a. 27001
   b. 28001
   c. 28995
   d. 28000

5. La confidentialité a été définie par l'organisation internationale de normalisation comme :
   a. le fait de s'assurer que les clés d'accès ne sont accessibles qu'à ceux dont l'accès est autorisé, et est une des pierres angulaires de la sécurité de l'information.
   b. le fait de s'assurer que toutes les données dans un système d'information sont chiffrées, et est une des pierres angulaires de la sécurité de l'information.
   c. le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé, et est une des pierres angulaires de la sécurité de l'information.
   d. Aucune des définitions sus-mentionnées n'est correcte.

6. Quel est l'intrus dans la liste ci-après ?
   a. CIA
   b. AAA
   c. Pakerian Hexad
   d. RADIUS

7. Quel type d'accès est-il plus difficile à pirater ?
   a. Challenge-response token
   b. Mot de passe
   c. Biométrie
   d. Smart card

8. L'authentification à deux facteurs permet de :
   a. recevoir un mot de passe unique par la poste.

b. se connecter grâce à un lecteur de carte d'identité.
c. réduire les risques de piratage en ajoutant une protection supplémentaire, par SMS, une application dédiée ou la poste.
d. Aucune des réponses n'est vraie.

9. Qu'est-ce que le phishing ?
   a. Des mails sont sollicités qui envahissent une boîte de réception.
   b. Une technique de piratage d'un smartphone.
   c. Une collecte frauduleuse d'informations personnelles via une usurpation d'identité.
   d. Une technique d'attaque révolue.

10. Lequel(lesquels) des procédés suivants est(sont) utilisé(s) pour capturer des mots de passe sur un réseau ?
    a. Chiffrement
    b. Spoofing
    c. Sniffing
    d. Destruction des données

11. Une attaque d'ingénierie sociale se déroule en deux étapes. Lesquelles ?
    a. Physique et psychologique
    b. Psychologique et comportemental
    c. Comportement et physique
    d. Aucune de ses réponses n'est vraie.

12. A quoi peut-on associer le terme *WannaCry* ?
    a. Un ransonware
    b. Un spyware
    c. Un antivirus
    d. Un réseau social

13. Comment contrer l'ingénierie sociale ?
    a. Développer un esprit critique.
    b. Vérifier les renseignements fournis.
    c. Se renseigner sur l'identité de son interlocuteur.
    d. Toutes ces réponses sont vraies.

14. Lequel de ces réseaux sociaux est moins bloqué sur les lieux de travail ?
    a. LinkedIn
    b. Facebook
    c. Google+
    d. Twitter

15. Quelle est l'assertion erronée parmi les suivantes ?

a. Une injection SQL est une vulnérabilité qui consiste à forger son propre code SQL, code mélangé à du code SQL propre à l'application.
b. Les sites vulnérables à une injection SQL sont ceux qui se basent sur une base de données relationnelles SQL.
c. Une application Web déployée dans un réseau local n'est pas vulnérable à une injection SQL.
d. Toutes les assertions sont erronées.

16. Quelle est l'assertion fausse parmi les suivantes ?
    a. L'attaque XSS vise comme cible le client plutôt que le serveur.
    b. Elle se sert d'un script Javascript qui sera exécuté chez le client pour détourner le fonctionnement de son navigateur.
    c. Les pages intégrant des fichiers CSS sont celles qui sont vulnérables à une attaque XSS.
    d. L'attaque XSS est une attaque intitulée Cross Site Scripting.

17. Le niveau de sécurité dans une architecture de sécurité en parallèle est
    a. le niveau de sécurité à l'entrée.
    b. le niveau de sécurité à la sortie.
    c. le niveau de sécurité du mécanisme ayant le plus faible niveau de sécurité.
    d. Aucune des réponses sus-mentionnées n'est exacte.

18. Qui peut pratiquer la manipulation de contenu ?
    a. Les parties politiques
    b. Les Etats
    c. Les entreprises
    d. Toutes ces réponses sont vraies.

19. Vous souhaitez améliorer la sécurité d'administration à distance de plusieurs serveurs web Linux sur Internet. Les données ainsi que le processus d'authentification doivent être chiffrés. Que devriez-vous faire ?
    a. Installer Windows 2016 Remote Administration.
    b. Utiliser SSH pour se connecter au shell Linux.
    c. Installer GNOME et utiliser PC Anywhere.
    d. Utiliser le protocole Kerberos pour se connecter au Linux shell.

20. Quel(s) protocole(s) d'authentification peut être sécurisé(s) à l'aide de protocole SSL ?
    a. Kerberos
    b. LDAP
    c. Radius
    d. TACACS+

21. Lequel des éléments suivants est utilisé pour effectuer un déni de service (DoS) ?
    a. Rootkit
    b. Bombe logique
    c. Botnet
    d. Redirection de port

22. Un utilisateur est incapable de transférer des fichiers vers un serveur FTP. L'administrateur de sécurité a constaté que les ports sont ouverts sur le pare-feu. Lequel des éléments suivants devrait vérifier l'administrateur ?
    a. Les listes de contrôles d'accès ACL
    b. Antivirus
    c. Prox
    d. IDS

23. Quelle type d'attaque reflète le message d'erreur suivant : Microsoft OLE DB Provider for ODBC Drivers (0x80040E14) ?
    a. Débordement de tampon
    b. Attaque par fragmentation
    c. Attaque XSS
    d. Injection SQL