Q1 :

Dans le scénario suivant :

Une cybercriminelle exploite un zero-day dans le serveur smtp d'un hôpital pour introduire un logiciel malveillant.

Que représente le zero-day ?

Question 1Veuillez choisir une réponse.

a.

La menace

b.

La contre-mesure

c.

Le risque

d.

Le danger

e.

La probabilité

f.

La vulnérabilité

Q2 :

Dans le modèle de Bell & LaPadula, quel principe empêche un attaquant de récupérer le cookie d'un administrateur grâce à un code malveillant.

Question 2Veuillez choisir une réponse.

a.

No read up

b.

No write up

c.

No write down

d.

No read down

Q3 :

Dans le modèle ABAC, quel module se charge de comparer la valeur des variables d’environnement avec les conditions d'une règle ?

Question 3Veuillez choisir une réponse.

a.

PAP

b.

PEP

c.

PDP

d.

PIP

Q4 :

Q5 :

Considérons deux générateurs de mots de passe :

G1 génère des chaînes de 6 caractères choisis aléatoirement depuis un alphabet composé de lettres minuscules (a-z), de lettres majuscules (A-Z), de chiffres (0-9) et de deux caractères spéciaux (# et $).

G2 génère des phrases de passes constituées de 4 mots choisis aléatoirement dans un dictionnaire de 4096 mots.

Quel générateur est meilleur d'un point de vue de sécurité ?

Question 5Veuillez choisir au moins une réponse.

a.

G1 est meilleur que G2

b.

G1 et G2 sont équivalents

c.

Ça dépend de la vitesse de génération

d.

G2 est meilleur que G1

Q6 :

Quelles affirmations sont vraies concernant l'algorithme de chiffrement RC4 ?

Question 6Veuillez choisir au moins une réponse.

a.

RC4 est un algorithme de chiffrement par flux

b.

RC4 est un algorithme de chiffrement par bloc

c.

RC4 est un algorithme de chiffrement asymétrique

d.

RC4 est utilisé dans l'algorithme de chiffrement des communication sans-fil WEP

e.

RC4 est utilisé dans les signatures de sites web

f.

RC4 est un algorithme de chiffrement symétrique

Q7 :

Pour authentifier Bob, Alice procède de la façon suivante :

Alice partage avec Bob un code secret de 4 chiffres.

Alice génère un nombre aléatoire de 4 chiffres et l'envoie à Bob.

Alice applique une fonction de hachage *F* sur le code secret et l'envoie à Bob.

Bob applique la fonction de hachage *F* sur le code secret et le compare avec le haché envoyé par Alice.

Si les deux sont identiques alors Alice est authentifiée.

Qu'elle est le mode d'authentification utilisé par Alice :

Question 7Veuillez choisir une réponse.

a.

Aucune de ces réponses

b.

Système défi-réponse

c.

Preuve à connaissance nulle

d.

Authentification à deux facteurs

e.

One Time Password local

f.

One Time Password distant

Q8 :

Vous utilisez le chiffrement de Vigenere avec la clé BPRQ. Votre amie Alice vous envoie le message chiffré suivant HFOBIOYVZUVFRONZ. Quel est le message en clair correspondant ?

Question 8Veuillez choisir une réponse.

a.

FNYMGWIGXCFQPWXK

b.

CASPEVMVCMIUHCMZ

c.

JHTOTDQGXVOJANGL

d.

FPWKGYGEXEDOPYVI

e.

RYXXHYEPSFJRMPRS

f.

JVGSKEQMBKNWTEFQ

Q9 :

Lorsqu'un acteur malveillant prends le contrôle d'un large réseau de botnet dans le but de lancer une attaque par déni de service sur le site web d'une entreprise, lequel des attributs suivants de l'analyse de risque est affecté ?

Question 9Veuillez choisir une réponse.

a.

Capacité

b.

Disponibilité

c.

Motivation

d.

Opportunité

Q10 :

Laquelle de ces propriété **n'est pas** une propriété de la cyber résilience ?

Question 10Veuillez choisir une réponse.

a.

L'adaptabilité

b.

Le recouvrabilité

c.

La productivité

d.

L'absorbabilité

Q11 :

Dans le chiffrement de Vernam, si la clé de chiffrement est de même taille que le message et a une entropie maximale, ...

Question 11Veuillez choisir une réponse.

a.

l'entropie du message original est négligeable.

b.

l'entropie du message original dépend de la clé de chiffrement.

c.

l'entropie du message original doit être minimale.

d.

l'entropie du message original doit être maximale.

Q12 :

Une entreprise s'inquiète du risque de l'utilisation de la capture et de la réutilisation d'une communication d'authentification par des cybercriminels.

Laquelle de ces contre-mesures est la plus adéquate ?

Question 12Veuillez choisir une réponse.

a.

Un nonce

b.

Hasher les mots de passe dans la base de donnée

c.

Du chiffrement

d.

Augmenter l'entropie des mots de passe

e.

Installer des anti-virus

f.

Un parefeu

Q13 :

Laquelle de ces méthodes d'authentification est considérée comme de la biométrie dynamique ?

Question 13Veuillez choisir une réponse.

a.

Une reconnaissance faciale

b.

Un fond de l’œil pour scanner la rétine

c.

Une montre intelligente qui reconnait les mouvement du poignet

d.

Un test ADN

e.

Un dispositif qui émet un son unique

f.

Un lecteur d'empreintes digitales sur les touches du clavier

Q14 :

QUESTION BONUS !

Dans 3DES, quel est la raison du choix de l'ordre Chiffrement-Déchiffrement-Chiffrement ?

Dans l'algorithme 3DES (Triple Data Encryption Standard), l'ordre Chiffrement-Déchiffrement-Chiffrement (EDE) a été choisi pour plusieurs raisons importantes :

Compatibilité avec DES : L'une des raisons principales est de maintenir la compatibilité avec le chiffrement simple DES. En utilisant l'ordre EDE, il est possible d'utiliser une seule clé pour les trois opérations, ce qui équivaut à une simple application de DES. Par exemple, si K1=K2=K3, alors 3DES avec l'ordre EDE devient simplement DES, ce qui assure la rétrocompatibilité avec les systèmes utilisant le chiffrement simple DES.

Renforcement de la sécurité : Le schéma EDE augmente considérablement la sécurité par rapport à l'utilisation de DES seul. En appliquant l'opération de déchiffrement intermédiaire, il

perturbe davantage le texte chiffré, ce qui rend plus difficile pour un attaquant de briser le chiffrement par des méthodes d'attaque connues, telles que les attaques par force brute ou les attaques par texte clair connu.

Prévention de certaines attaques : L'ordre EDE est également choisi pour prévenir certaines attaques spécifiques. En particulier, l'attaque meet-in-the-middle, qui est une attaque efficace contre les versions plus simples de chiffrement multiple, est beaucoup plus difficile à appliquer à 3DES en raison de la structure EDE. L'attaque meet-in-the-middle nécessite deux points de comparaison (texte clair et texte chiffré), et l'inclusion de la phase de déchiffrement au milieu complique cette attaque.

Ainsi, l'ordre Chiffrement-Déchiffrement-Chiffrement (EDE) dans 3DES assure la compatibilité descendante avec DES, renforce la sécurité du schéma de chiffrement et aide à prévenir certaines attaques cryptographiques.

Q15 :

On considère une source S1 markovienne qui génère des 0 et des 1. La probabilité d'apparition d'un 0 et de 1/5 et celle d'un 1 est de 4/5. Quelle est l'entropie d'un message de 10 chiffres généré par la source S1 ?

Rép : 7.2193

Q16 :

Laquelle de ces proposition est fausse concernant XACML ?

Question 16Veuillez choisir une réponse.

a.

Il ne permet pas d'implémenter le modèle RBAC

b.

Il utilise la notion d'attributs

c.

Il utilise des balises

d.

Il est basé sur XML

e.

Il est très verbeux

f.

Il a été standardisé par le OASIS

Q17 :

Supposant qu'un ordinateur quantique avec plusieurs milliers de Qbits soit commercialisé.

On considère un document chiffré avec une clé de chiffrement AES de 128 bits.

Comment faire pour maintenir le même niveau de sécurité ?

Question 17Veuillez choisir une réponse.

a.

Le chiffrement AES est désormais obsolète. Il faut le remplacer par un algorithme de chiffrement post-quantique.

b.

On n'a rien à faire. L'ordinateur quantique n'a pas d'effet sur le chiffrement AES

c.

Déchiffrer le document et le chiffrer avec une clé RSA de 2048 bits

d.

Déchiffrer le document et le chiffrer avec une clé RSA de 4096 bits

e.

Déchiffrer le document et le chiffrer avec une clé AES de 256 bits

f.

Déchiffrer le document et le chiffrer avec une clé AES de 512 bits

Q18 :

Basile décide d'utiliser l'algorithme RSA pour signer les messages qu'elle envoie à Anna.

Pour que Anna assure qu'un message a bien été signé par Basile, elle doit utiliser

Question 18Veuillez choisir une réponse.

a.

La clé publique de Basile

b.

La clé publique d'Anna

c.

La clé privée d'Anna

d.

La clé privée de Basile

Q19 :

Dans le fichier /etc/shadow, qu'est-ce qui fait en sorte que deux utilisateurs ayant le même mot de passe n'aient pas le même haché ?

Question 19Veuillez choisir une réponse.

a.

La clé privée de l'utilisateur

b.

La fonction de hachage

c.

La clé publique de l'utilisateur

d.

Le sel

Q20 :

Laquelle des propositions suivantes ne correspond pas à une authentification double facteur ?

Question 20Veuillez choisir une réponse.

a.

L'énoncé d'une phrase secrète et la présentation d'une carte d'identité

b.

La présentation à la fois de la paume de la main et la pause de son poignet à un lecteur de la puce qui y a été implantée sous la peau

c.

Présentation de son visage à une caméra et des empreintes digitales

d.

La saisie d'un mot de passe pris dans un dictionnaire Yiddish et la captation du rythme de frappe sur un clavier

Q21 :

Basile envoie à Anna le jour de semaine de leur prochain rendez-vous. Le message est chiffré avec du chiffrement par substitution mono-alphabétique.

Maxime intercepte le message chiffré qui est GKFMDKMV.

Quelle affirmation est vraie ?

Question 21Veuillez choisir une réponse.

a.

Anna et Basile vont se voir vendredi

b.

Maxime doit faire une attaque par analyse fréquentielle pour savoir

c.

Maxime ne peut pas déchiffrer le message

d.

Anna et Basile vont se voir mercredi

e.

Maxime doit faire une attaque par force brute pour savoir

f.

Anna et Basile vont se voir samedi

Q22 : plusieurs possible

Un générateur de mots de passe génère une chaîne de 4 lettres aléatoire.

Parmi les 4 lettres, une lettre aléatoire est en majuscule, toutes les autres sont en minuscule.

Un agent malveillant exécute une attaque par force brute sur un mot de passe générer par ce générateur.

Sachant qu'il peut tenter 100 mots de passe par seconde, de combien de temps aurait-il besoin pour tenter 60% des mots de passe possibles ?

Question 22Veuillez choisir au moins une réponse.

a.

Environ 16 jours

b.

Environ 33 ans

c.

Environ 3 heures

d.

Environ 55 ans

e.

Environ 27 jours

f.

Environ 5 heures

Q23 :

Anna décide d'utiliser le chiffrement de Vernam (masque jetable) pour communiquer avec Basile. La clé utilisée est une chaîne de caractères aléatoire de longueur égale au message.

Quelle méthode Maxime peut-il utiliser pour déchiffrer le message ?

Question 23Veuillez choisir une réponse.

a.

L'algorithme de Grover

b.

Aucune de ces réponses

c.

L'attaque par dictionnaire

d.

L'analyse fréquentielle

e.

La force brute

f.

L'agorithme de Shor

Q24 :

Basile décide d'utiliser l'algorithme RSA pour chiffrer ses communication avec Anna.

Que doit faire Anna pour déchiffrer les messages de Basile ?

Question 24Veuillez choisir une réponse.

a.

Déchiffrer avec la clé privée de Basile

b.

Déchiffrer avec la clé privée d'Anna

c.

Déchiffrer avec la clé publique d'Anna

d.

Déchiffrer avec la clé publique de Basile

Q25 :

Suite de la question : *On considère une source S1 markovienne qui génère des 0 et des 1. La probabilité d'apparition d'un 0 et de 1/5 et celle d'un 1 est de 4/5. Quelle est l'entropie d'un message de 10 chiffres généré par la source S1 ?*

On considère une seconde source S2 déterministe qui génère également des 0 et des 1. La fréquence d'apparition d'un 0 est de 1/2 et celle d'un 1 est de 1/2.

La source S est obtenue en prenant le XOR (OU exclusif) des bits générés par S1 et S2.

Quelle est l'entropie d'un message de 10 chiffres généré par la source S ?

Rép: 10bits

Q26 :

Dans le modèle AGLP (Access - Global - Local - Permission), qui est le plus qualifié pour établir la correspondance entre les groupes locaux et les ressources ?

Question 26Veuillez choisir une réponse.

a.

L'administrateur de la politique de sécurité

b.

L'ingénieur stagiaire

c.

L'auditeur de cyber-sécurité

d.

Le gestionnaire des ressources humaines

e.

L'utilisateur

f.

L'administrateur système

Q27 : plusieurs reponses

Quels modes de chiffrement permettent de chiffrer plusieurs blocs parallèlement (en même temps) ?

Question 27Veuillez choisir au moins une réponse.

a.

Cipher Feedback (CFB)

b.

Cipher Block Chaining (CBC)

c.

Output Feedback (OFB)

d.

Electronic Code Book (ECB)

Q28 :

L'algorithme cryptographique à clé publique de El-Gamal peut être défini sur un

Question 28Veuillez choisir une réponse.

a.

groupe abélien.

b.

groupe non-commutatif

c.

magma

d.

monoïde

Q29 :

Qu'est ce qui permet à un dispositif de mot de passe à usage unique (ex. RSA SecurID) qui n'est pas connecté à internet de généré le même mot de passe que le serveur d'authentification ?

Question 29Veuillez choisir une réponse.

a.

La faible entropie des mots de passe à usage unique

b.

Une autorité de certification

c.

Le réseau sans-fil GSM

d.

Une clé partagée

e.

Un dispositif de mots de passes à usage unique doit être connecté à internet

f.

Une base de donnée de mots de passe à usage unique

Q30 :

Lequel de ces aspects ne fait pas partie du contrôle d'accès ?

Question 30Veuillez choisir une réponse.

a.

L'identification

b.

L'authentification

c.

L'autorisation

d.

L'audit

e.

L'autonomie

Q31 :

Quel type de disponibilité est le plus approprié dans une infrastructure critique :

Question 31Veuillez choisir une réponse.

a.

La disponibilité en temps fini

b.

La disponibilité en temps infini

c.

Aucune de ces propositions

d.

La disponibilité en temps borné

e.

La disponibilité en temps linéaire

f.

La disponibilité en temps polynomial

Q32 :

vide

Q33 :

Dans le modèle ABAC, quelle règle permet d'autoriser un étudiant à accéder la salle où son cours est donné ?

Question 33Veuillez choisir une réponse.

a.

Permettre si Role(Sujet)=Étudiant et Type(Ressource)=Salle_de_cours et (Liste_des_cours(Sujet) ∪ Liste_des_cours(Ressources)) = 0 et Ident(Action)=Accéder

b.

Permettre si Role(Sujet)=Étudiant et Type(Ressource)=Salle_de_cours et (Liste_des_cours(Sujet) ∪ Liste_des_cours(Ressources)) > 0 et Ident(Action)=Accéder

c.

Permettre si Role(Sujet)=Étudiant et Type(Ressource)=Salle_de_cours et (Liste_des_cours(Sujet) ∩ Liste_des_cours(Ressources)) = 0 et Ident(Action)=Accéder

d.

Permettre si Role(Sujet)=Étudiant et Type(Ressource)=Salle_de_cours et (Liste_des_cours(Sujet) ∩ Liste_des_cours(Ressources)) > 0 et Ident(Action)=Accéder

Q34 :

Un utilisateur malveillant s’installe dans un cyber café et essaye d’intercepter des mots de passe et numéros de carte de crédit sur le réseau Wi-Fi du café pour réaliser de la fraude bancaire par Internet.

Est-ce qu’il s’agit :

Question 34Veuillez choisir une réponse.

a.

D'une probabilité

b.

D’une contre-mesure

c.

D’une menace

d.

D’une vulnérabilité

e.

D'un impact

f.

D’un risque

Q35 :

Laquelle de ces attaques porte atteinte à l'intégrité ?

Question 35Veuillez choisir une réponse.

a.

Les rançongiciel (ransomware)

b.

Le scan de ports

c.

L'écoute passive (sniffing)

d.

Le rejeu (replay)

e.

Le déni de service

f.

L’inondation (flooding)