Session QCM : sécurité des applications web

Nom : ……..

Prénom : ……..

Date: ……..

Note : les supports de cours et les ordinateurs portables ne sont **PAS** autorisés.

Durée : 60 minutes

ATTENTION :

- Une (*) en début de question signifie que plusieurs réponses sont possibles
- 4 réponses fausses provoquent le retrait d'1 point

1) Quelle est l'une des utilisations de CVE (Common Vulnerabilities and Exposures)?

- ○ Communauté ouverte d'experts, d'industriels, de représentants d'organisation, de définition et de préconisation: de bonnes pratiques, de normes, d'outils, pour la sécurité du WEB
- ○ Centre d'expertise gouvernemental de Réponse et de Traitement des Attaques informatiques
- ○ Notation pour identifier d'une manière unique ou convergente les vulnérabilités et leurs expositions
- ○ Langage de requêtes permettant d'extraire des informations d'un document XML

2) Que signifie « CSRF »?
- ○ Common Script Request Function
- ◉ Cross Site Request Forgery
- ○ Cross Site Response Form
- ○ Complete Strategy Request Forgery

3) Quelle est la méthode d'authentification HTTP la plus faible, parmi les méthodes ci-dessous?
- ○ Form Based Authentication
- ○ HTTP Digest Authentication
- ○ HTTP Basic Authentication
- ○ HTTPS Client Authentication

4) Quelle est l'organisme non commercial en charge de la sécurité des applications web?
- ◉ OWASP
- ○ SecurityFocus
- ○ CSI
- ○ Sophos

5) Quel type de faille permet à un attaquant d'injecter des scripts « côté-client » dans des pages web lues par d'autres utilisateurs?
- ○ SQL Injection
- ○ CSRF
- ◉ XSS
- ○ Buffer overflow

6) Quel outil permet de lutter contre les failles de type XSS ou CSRF?
- ○ HTTPS-Everywhere
- ◉ NoScript
- ○ Firebug
- ○ Proxyswitch

7) Quelle méthode en HTTPS permet de sécuriser le mieux les données transmises par l'utilisateur?
- ○ Méthode HEAD
- ○ Méthode PUT
- ○ Méthode GET
- ◉ Méthode POST

8) Les phases habituelles d'une attaque APT sont réalisées dans l'ordre suivant ?
- Utilisation d'une porte dérobée, phishing, attaque 0-day, mouvement latéral, récupération d'informations, exfiltration de données
- Phishing, attaque 0-day, utilisation d'une porte dérobée, mouvement latéral, récupération d'informations, exfiltration de données
- Phishing, attaque 0-day, utilisation d'une porte dérobée, récupération d'informations, exfiltration de données, mouvement latéral
- Phishing, attaque 0-day, mouvement latéral, récupération d'informations, exfiltration de données, utilisation d'une porte dérobée

9) Pourquoi doit-on éviter une référence directe à un objet non sécurisée ?
- Un attaquant peut forcer l'utilisateur à invoquer certaines fonctions telles que la page de déconnexion de l'application
- Un attaquant peut alors manipuler directement la référence à l'objet pour accéder à d'autres objets sans autorisation, même avec des vérifications de contrôle d'accès en place
- Les applications autorisent souvent des accès à des fichiers « cachés » comme des rapports système générés
- Si le code autorise l'utilisateur à donner un nom de fichier alors il ne permet pas à un attaquant de sortir de la structure de l'application et d'accéder à d'autres ressources

10) Quel est l'organisme, créé en 2009, qui assure la mission d'autorité nationale en matière de sécurité des systèmes d'information ?
- CERTA
- CERT-RENATER
- ANSI
- ANSSI

11) Que signifie APT?
- Advanced Persistent Trend
- Advanced Polymorphic Threat
- Advanced Persistent Threat
- Anonymous Persistent Threat

12) Qu'est-ce qu'une faille « 0-day » ?
- Une faille inconnue et donc « sans correctif » offrant la possibilité de réaliser une attaque
- Une faille inconnue nécessitant peu de temps à l'éditeur pour réaliser son correctif
- Une faille connue obtenue par «reverse engineering » du correctif de l'éditeur
- Une faille connue utilisée lors d'une intrusion sur un serveur « non patché »

13) Parmi les affirmations ci-dessous laquelle est fausse ?
- Un « keylogger » permet d'enregistrer les caractères saisis par un utilisateur sur son clavier
- Une autorité de certification ne peut pas être corrompue
- Le « typosquatting » consiste à réserver des noms de domaine proches de noms de domaines réels
- « ce que je sais », « ce que je suis » et « ce que je possède » représentent différents facteurs d'authentification

14) (*) Le « Social engineering » est permis par
- Un attaquant se faisant passer pour un utilisateur légitime
- Un attaquant se faisant passer pour une personne importante
- Un attaquant se faisant passer pour un membre de l'équipe de support technique
- Un attaquant écoutant les conversations de ses collègues

15) Une faille de type « XSS Stored » consiste :
- A injecter un script malveillant de manière permanente dans un site web
- A exécuter un script malveillant de manière temporaire dans un site web au travers d'une URL forgée à cet effet
- A injecter un script malveillant au travers d'un document de type « PDF »
- A exécuter un script malveillant au travers d'une vulnérabilité de type CSRF

16) Une faille de type « XSS Reflected » consiste :
- A injecter un script malveillant de manière permanente dans un site web
- A exécuter un script malveillant de manière temporaire dans un site web au travers d'une URL forgée à cet effet
- A injecter un script malveillant au travers d'un document de type « PDF »
- A exécuter un script malveillant au travers d'une vulnérabilité de type CSRF

17) (*) L'attaque appelée « session fixation » se base sur
- La définition par l'attaquant de l'identifiant de session utilisé par la victime
- La possibilité pour un utilisateur d'avoir plusieurs sessions actives en même temps
- La validité d'un identifiant de session sans limite dans le temps
- Le caractère prédictif d'un identifiant de session

18) L'outil « Dirbuster » permet de :
- Chercher les répertoires et fichiers contenant une chaîne de caractères donnée
- Chercher les répertoires et fichiers cachés sur un site web
- Chercher les répertoires et fichiers stockés dans un disque dur
- Chercher les répertoires et fichiers supprimés

19) Le mode d'attaque « Battering Ram » dans Burp Suite permet de :
- Faire varier une variable selon une liste de valeurs prédéfinies
- Faire varier deux variables, chacune ayant sa propre liste de valeurs prédéfinies
- Faire varier une même variable présente plusieurs fois dans la page selon une liste de valeurs prédéfinies
- Faire varier une variable selon une liste de valeurs aléatoires

20) Quelle est la définition qui se rapproche le plus d'un CERT
- Centre d'Expertise gouvernemental de Réponse et de Traitement des attaques informatiques
- Centre d'Expertise gouvernemental de Régulation et de Traitement des données privées
- Centre d'Expertise gouvernemental de Renouvellement et de Traitement des solutions virtualisées
- Cabinet d'Expertise en Reclassement des Travailleurs

21) (*) Parmi les outils ci-dessous lesquels peuvent être utilisés comme « proxy » ?
- Burp Suite
- Zap
- Nmap
- Nikto

22) www.archive.org permet
- D'archiver ses données
- De consulter les archives officielles de services gouvernementaux
- De retrouver des pages supprimées des sites web
- De sécuriser ses données dans le « cloud »

23) (*) A quoi sert le site www.exploit-db.com ?
- Pour le Google Hacking
- Pour trouver une liste des dernières vulnérabilités
- Pour télécharger des outils de « hacking »
- Pour scanner les vulnérabilités des sites web

24) L'outil « nmap » est le plus souvent utilisé dans le cadre d'une phase de
- Reconnaissance active
- Maintien d'un accès
- Scanning du réseau de la cible
- Obtention d'un accès

25) Parmi les outils ci-dessous lequel n'est pas un outil de reconnaissance passive ?
- Maltego
- Google
- Facebook
- Nmap

26) (*) Qu'est-ce la reconnaissance active ?
- Obtenir des informations sur une personne sans entrer en contact avec elle directement
- Obtenir des informations sur une personne en interagissant avec elle
- Utiliser le « social engineering »
- Effectuer un scan du réseau de l'entreprise où travaille notre cible

27) (*) Qu'est-ce que « Metasploit » ?
- Il fournit des informations sur les vulnérabilités de systèmes informatiques
- C'est un outil pour le développement et l'exécution d'exploits
- C'est un scanner de vulnérabilités dynamique
- C'est l'équivalent de Nessus

28) (*) Que permet le Google Hacking ?
- Il utilise un langage de création de requêtes complexes
- Il détecte les sites web vulnérables à certains exploits
- Il utilise le langage de Google
- Il permet de trouver les hackeurs via internet

29) Quel est l'ordre des phases d'une attaque ?
- Reconnaitre, scanner, obtenir un accès, maintenir un accès, couvrir ses traces
- Obtenir un accès, reconnaitre, scanner, maintenir un accès, couvrir ses traces
- Obtenir un accès, scanner, reconnaitre, maintenir un accès, couvrir ses traces
- Reconnaitre, obtenir un accès, scanner, maintenir un accès, couvrir ses traces

30) Si l'attaquant utilise un faux badge pour pénétrer dans une entreprise on parle de
- piggybacking
- tailgating
- reverse social engineering
- typosquating

31) Qu'est-ce que le « piggybacking » ?
- utiliser un faux badge pour pénétrer dans une entreprise
- demander à une personne autorisée (ayant un badge) d'entrer avec elle
- effectuer un « rollback » après une attaque
- augmenter la sécurité périmétrique de l'entreprise pour éviter les intrusions

32) Comment réalise-t-on généralement une injection SQL dans un champ de type « texte » ?
- 1 or 1=1
- 1' or '1'='1'
- 1 or '1'='1'
- 1' or '1'='1

33) Comment réalise-t-on généralement une injection SQL dans un champ de type « numérique » ?
- 1' or '1'='1'
- 1 or '1'='1'
- 1 or 1=1
- 1' or '1'='1

34) Lorsqu'une injection SQL de type « numérique » est présente dans une page web, comment peut-on généralement vérifier que la table, sur laquelle se base la requête SQL, contient au moins 2 colonnes ?
- 1 order by 1
- 1 and column like '%2%'
- 1 union select 2
- 1 order by 2

35) Lorsqu'une injection SQL de type « numérique » est présente dans une page web, si la table sur laquelle se base la requête SQL contient 2 colonnes, comment peut-on retourner à la fois la version de la base de données et le nombre de lignes dans la table ?
- 1 and @@version and count(*)
- 1 and concat(select @@version, count(*))
- 1 union select 1, 2
- 1 union select @@version, count(*)

36) Laquelle des URLs ci-dessous correspond exactement à une attaque de type XSS ?
- http://192.168.4.18/peruggia/index.php?action=learn&type=XSS&paper=http://www.prox-ia.com
- http://192.168.4.18/peruggia/index.php?action=learn&type=XSS&account=111%27%3Escriptalert%28%27XSS!%27%29%3bscript
- http://192.168.4.18/peruggia/index.php?action=learn&type=XSS&account=111%27%3E%3Cscript%3Ealert%28%27XSS!%27%29%3b%3C%2fscript%3E
- http://192.168.4.18/peruggia/index.php?action=learn&type=XSS&account=111%27%20or%20%271%27%3d%271

37) (*) Que peut permettre une attaque XSS ?
- Permet de défigurer un site web
- Permet de forger une URL de phishing pour récupérer les mots de passe des utilisateurs du site
- Permet de voler un identifiant de session
- Permet de faire un déni de service sur le site web

38) Que signifie le terme XXE ?
- XML eXternal Entity
- eXternal XSS Execution
- Cross eXternal Execution
- XML eXperienced Element

39) (*) Que peut permettre une attaque XXE ?
- Permet d'exfiltrer des données sensibles
- Permet d'importer à un fichier DTD stocké sur une URL contrôlée par l'attaquant
- Permet d'injecter du code XML malveillant
- Permet de convertir les données à exfiltrer en « base64 »

40) Que signifie le terme RFI ?
- Remote Folder Interception
- Remote File Inclusion
- Recursive File Interception
- Remote Filter Inclusion

41) Parmi les URLs suivantes, laquelle décrit le mieux un RFI ?
- http://192.168.4.18/peruggia/index.php?action=../../../../../../etc/passwd%00
- http://192.168.4.18/peruggia/index.php?action=learn&type=XSS&paper=http://www.prox-ia.com
- http://192.168.4.18/peruggia/index.php?action=learn&type=<script>document.cookie</script>
- http://192.168.4.18/WackoPicko/users/sample.php?userid=1

42) Que signifie le terme LFI ?
- Local Folder Interception
- Lateral File Interception
- Local File Inclusion
- Local Filter Inclusion

43) Parmi les URLs suivantes, laquelle décrit le mieux un LFI ?

- http://192.168.4.18/peruggia/index.php?action=../../../../../../etc/passwd%00
- http://192.168.4.18/peruggia/index.php?action=learn&type=XSS&paper=http://www.prox-ia.com
- http://192.168.4.18/peruggia/index.php?action=learn&type=<script>document.cookie</script>
- http://192.168.4.18/WackoPicko/users/sample.php?userid=1

44) Qu'est-ce qu'un "stored webshell"?

- Un fichier devant être stocké sur le serveur pour permettre de prendre la main sur le serveur
- Du code passé dans le paramètre d'une URL permettant de prendre la main sur le serveur
- Un fichier passé directement dans le paramètre d'une URL permettant de prendre la main sur le serveur sans avoir à stocker le fichier sur le serveur
- Une page web affichée en réponse à une requête de l'attaquant

45) Qu'est-ce qu'un "reflected webshell"?

- Un fichier devant être stocké sur le serveur pour permettre de prendre la main sur le serveur
- Du code passé dans le paramètre d'une URL permettant de prendre la main sur le serveur
- Un fichier passé directement dans le paramètre d'une URL permettant de prendre la main sur le serveur sans avoir à stocker le fichier sur le serveur
- Une page web affichée en réponse à une requête de l'attaquant

46) Que fait le «googledork» suivant: inurl:"tiki-index.php" filetype:php "This is TikiWiki 1.9" ?

- Il permet de rechercher les pages web contenant "tiki-index.php" ainsi que les mots clefs "This is TikiWiki 1.9"pour des fichiers de type « php » seulement
- Il permet de rechercher les URLs contenant "tiki-index.php" pour tous les fichiers excepté ceux de type « php » et dont la page correspondante contient les mots clefs "This is TikiWiki 1.9"
- Il permet de rechercher les URLs contenant "tiki-index.php" pour des fichiers de type « php » seulement et dont la page correspondante contient les mots clefs "This is TikiWiki 1.9"
- Il permet de rechercher les paramètres « inurl » et « filetype » contenant respectivement "tiki-index.php" et "This is TikiWiki 1.9" pour des fichiers de type « php »

47) Que signifie CVSS ?

- Common Vulnerability Scoring System
- Critical Vulnerability Secondary Score
- Critical Vulnerability Scoring Suite
- Common Vulnerability Securing System

48) Quelles sont les paramètres utilisés dans le calcul d'un CVSS Base Score ?
- Exploitability, Remediation Level, Report Confidence
- Access Vector, Access Complexity, Authentication, Impact on Confidentiality Integrity Availability
- Collateral Damage Potential, Target Distribution, Requirement on Confidentiality Integrity Availability
- Access Vector, Access Complexity, Authentication

49) Que signifie BeEF ?
- Browser Exploitation Framework project
- Browser Encryption Framework project
- Banner Exploitation Framework project
- Browser Exfiltration Framework project

50) (*) Que permet BeEF ?
- Permet de prendre le contrôle d'un browser hameçonné
- Permet d'augmenter la prise de conscience des utilisateurs aux risques liés à internet
- Fournit les outils permettant d'installer un malware sur le poste d'un utilisateur dont le browser est hameçonné
- Fournit des APIs pour automatiser la détection d'un browser hameçonné et les actions à mener sur ce browser

51) (*) Selon l'OWASP, parmi les interpréteurs ci-dessous lesquels peuvent donner lieu à des attaques de type « injection » ?
- LDAP
- XPATH
- Les commandes d'un OS
- XML

52) Heartbleed aurait pu être évité si
- Les systèmes d'exploitation étaient durcis
- La cohérence des données transmises entre un client et un serveur étaient contrôlées en entrée et en sortie
- La cohérence des données transmises entre un client et un serveur étaient contrôlées en entrée
- Une politique efficace de mise à jour des patchs était en place

53) Quel est le cycle de vie des vulnérabilités correspondant à une approche « white hat » ?

- Correctif de l'éditeur / Application du correctif / Découverte d'une faille / Publication de l'exploit
- Découverte d'une faille / Correctif de l'éditeur / Publication de l'exploit / Application du correctif
- Découverte d'une faille / Publication de l'exploit / Correctif de l'éditeur / Application du correctif
- Découverte d'une faille / Correctif de l'éditeur / Application du correctif / Publication de l'exploit

54) Quel est le cycle de vie des vulnérabilités correspondant à une approche « black hat » ?

- Correctif de l'éditeur / Application du correctif / Découverte d'une faille / Publication de l'exploit
- Découverte d'une faille / Correctif de l'éditeur / Publication de l'exploit / Application du correctif
- Découverte d'une faille / Publication de l'exploit / Correctif de l'éditeur / Application du correctif
- Découverte d'une faille / Correctif de l'éditeur / Application du correctif / Publication de l'exploit

55) Parmi les requêtes ci-dessous, quelle est celle qui permet de savoir si votre serveur est vulnérable à « Shellshock » ?

- env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
- wget -U "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/cat /etc/passwd" http://192.168.4.23/cgi-bin/test.cgi
- GET /cgi-bin/test.cgi
- env x='() { :;}; echo vulnerable' nmap -c "echo this is a test"

56) (*) Quelles motivations peuvent transformer l'employé d'une entreprise en attaquant ?

- Aucune
- La colère
- Le manque de reconnaissance
- Une pression extérieure (chantage)

57) Qu'est-ce que le « dumpster diving » ?

- La découverte de dossiers cachés dans l'entreprise
- La fouille des poubelles de l'entreprise
- La découverte d'informations confidentielles dans le « web profond »
- La fouille systématique des bureaux des employés

58) (*) Parmi les affirmations ci-dessous lesquelles sont fausses ?
- « testssl.sh » et www.ssllabs.com permettent de détecter les configurations TLS faibles
- Il est conseillé d'utiliser SSL 3.0
- Aucune vulnérabilité SSL n'a été découverte depuis 2013
- Il est conseillé de ne plus utiliser RC4

59) (*) Que peut être une « propriété de sécurité » ?
- La contre-mesure appliquée à une vulnérabilité
- La disponibilité
- La confidentialité
- La non-répudiation

60) (*) Qu'appelle t'on « données sensibles » ?
- Certaines « metadata »
- Les numéros des cartes de crédit
- Les résultats d'examen médicaux anonymisés (sans lien avec les patients)
- Une dizaine de noms et prénoms

61) (*) De quoi dépend la sensibilité d'une donnée ?
- Son type
- Sa quantité
- Sa combinaison avec d'autres données
- Sa localisation

62) Que désigne-t'on par « business assets » ou « biens primordiaux »?
- Les données seules
- Les logiciels
- Les données et les services
- Le personnel

63) (*) Que désigne-t'on par « supporting assets » ou « biens en support » ?
- Les logiciels
- Le personnel
- Le site
- Le réseau

64) (*) Parmi les affirmations ci-dessous lesquelles sont fausses?
- Tous les agents de menace disposent des mêmes ressources ou compétences
- L'agent de menace peut faire partie des employés de l'entreprise
- Une agence gouvernementale ne peut être considérée comme un agent de menace
- La motivation de l'agent de menace n'est pas un critère à prendre en compte lors d'une analyse de risques

65) Un chemin d'attaque est ?
- Un ensemble de risques sur des biens en support qui, pris l'un après l'autre, permettent à l'attaquant d'atteindre les biens de l'entreprise
- Un ensemble de menaces sur des biens en support qui, prises l'une après l'autre, permettent à l'attaquant d'atteindre les biens de l'entreprise
- Un ensemble de vulnérabilités sur des biens en support qui, prises l'une après l'autre, permettent à l'attaquant d'atteindre les biens de l'entreprise
- Un ensemble de vulnérabilités sur des biens en support qui, prises indépendamment l'une de l'autre permettent à l'attaquant d'atteindre les biens de l'entreprise

66) (*) Les vulnérabilités peuvent appartenir aux catégories suivantes :
- Architecture
- Conception
- Implémentation
- Déploiement

67) (*) Pour réaliser une attaque un agent de menace a besoin:
- D'une opportunité
- De ressources
- De compétences
- D'une motivation

68) (*) Quelles sont les **principales** sources de motivation d'un agent de menace ?
- L' « ego »
- L'argent
- L'idéologie
- La difficulté technique

69) Selon le cours, la vraisemblance ou « likelihood » d'une attaque est **principalement** liée :
- Au fait que l'attaquant connaît un employé de l'entreprise ciblée
- A la valeur que représente le bien primordial pour l'attaquant
- Au fait que l'attaquant connaît le type et la version de la base de données utilisée
- A l'attention que portent les médias aux cyber-attaques

70) (*) Dans la liste ci-dessous, quelles sont les fonctions de sécurité (ou contrôles de sécurité)?
- L'utilisation d'une suite cryptographique forte
- L'intégration d'un WAF pour protéger le portail web
- La formation des développeurs aux bonnes pratiques « sécurité »
- La mise en place de tests de pénétration périodiques

71) Parmi les affirmations ci-dessous laquelle est fausse ?
- L'impact correspond uniquement à la valeur de fabrication des biens primordiaux
- L'impact peut être financier
- L'impact peut être contre la réputation de l'entreprise
- L'impact peut être légal

72) Qu'est-ce que le risque résiduel ou « residual risk »?
- C'est le risque calculé sans tenir compte de l'impact et de la vraisemblance
- C'est le risque brut ou « inherent risk » avant que les contrôles de sécurité aient été pris en compte
- C'est le risque brut ou « inherent risk » après que les contrôles de sécurité aient été pris en compte
- C'est le risque dont le score est trop petit pour devoir être pris en compte dans l'analyse de risques

73) Les 4 traitements possibles d'un risque sont ?
- Eviter (« avoid ») / Transférer (« transfer ») / Annuler (« cancel ») / Accepter (« accept »)
- Eviter (« avoid ») / Transférer (« transfer ») / Réduire (« mitigate ») / Accepter (« accept »)
- Eviter (« avoid ») / Oublier (« forget ») / Réduire (« mitigate ») / Accepter (« accept »)
- Supprimer (« suppress ») / Transférer (« transfer ») / Réduire (« mitigate ») / Vérifier (« check »)

74) (*) Les contrôles de sécurité sont principalement :
- Administratifs
- Sociaux
- Logiques
- Physiques

75) Quelle propriété de sécurité est mise en œuvre lorsque l'on signe un « email » ?
- Intégrité
- Autorisation
- Non répudiation
- Disponibilité

76) Quelle propriété de sécurité est mise en œuvre lorsque l'on met en place un « audit log » pour l'accès à un service?
- Intégrité
- Autorisation
- Non répudiation
- Disponibilité

77) Quelle propriété de sécurité est mise en œuvre lorsque l'on valide les droits d'accès à un service?
- Intégrité
- Autorisation
- Non répudiation
- Disponibilité

78) Quelle propriété de sécurité est mise en défaut lorsque notre site web est défiguré (« defaced »)?
- Intégrité
- Autorisation
- Non répudiation
- Disponibilité

79) Quelle est généralement la principale propriété de sécurité mise en défaut lorsque l'on ne peut pas tenir notre engagement sur le « Service Level Agreement » proposé contractuellement à notre client?
- Intégrité
- Autorisation
- Non répudiation
- Disponibilité

80) Dans la phase de gestion des risques, quelle définition de « éviter un risque » est la plus vraie ?
- C'est transmettre le risque sur un tiers
- C'est supprimer la fonctionnalité
- C'est considérer que le risque ne nécessite pas de traitement
- Cette action ne fait pas partie des actions possibles lors de la gestion des risques

81) Dans la phase de gestion des risques, quelle définition de « transférer un risque » est la plus vraie ?
- C'est transmettre le risque sur un tiers
- C'est supprimer la fonctionnalité
- C'est considérer que le risque ne nécessite pas de traitement
- Cette action ne fait pas partie des actions possibles lors de la gestion des risques

82) Dans la phase de gestion des risques, quelle définition de « accepter un risque » est la plus vraie ?
- C'est transmettre le risque sur un tiers
- C'est supprimer la fonctionnalité
- C'est considérer que le risque ne nécessite pas de traitement
- Cette action ne fait pas partie des actions possibles lors de la gestion des risques

83) (*) Parmi les affirmations ci-dessous lesquelles sont vraies ?

- Le « cloud privé dédié » propose des composants « hardware » et « software » communs à tous les clients
- Le « cloud privé partagé » propose des composants « hardware » et « software » communs à tous les clients
- Le « cloud privé dédié » propose des composants « hardware » et « software » spécifiques pour chaque client
- Le « cloud privé partagé » propose des composants « hardware » et « software » spécifiques pour chaque client

84) Le fichier « APK » d'une application mobile sous Android contient

- Des fichiers JAR (Java compilé)
- Des fichiers chiffrés avec la clef publique du certificat OHA (Open Handset Alliance)
- Des fichiers exécutables « Dalvik » (code interprété)
- Des fichiers XML et XSLT

85) Parmi les affirmations ci-dessous laquelle est vraie ?

- Le code Dalvik étant chiffré, il est nécessaire de connaître la clef privée pour pouvoir décompiler, modifier et recompiler l'application
- Le code Dalvik peut être décompilé, modifié et recompilé pour générer une nouvelle application
- Le code Dalvik peut être décompilé, mais une fois modifié il ne peut être recompilé pour générer une nouvelle application
- Le code Dalvik ne peut pas être décompilé

86) Parmi les affirmations ci-dessous laquelle est vraie ?

- Les fichiers JAR de l'application mobile obtenus avec l'outil « dex2jar », peuvent être décompilés, modifiés mais ne peuvent pas être recompilés pour générer une nouvelle application
- Les fichiers JAR de l'application mobile obtenus avec l'outil « dex2jar », peuvent être décompilés, modifiés et recompilés pour générer une nouvelle application
- Les fichiers JAR de l'application mobile obtenus avec l'outil « apktool », peuvent être décompilés, modifiés et recompilés pour générer une nouvelle application
- Les fichiers JAR de l'application mobile obtenus avec l'outil « apktool », peuvent être décompilés, modifiés mais ne peuvent pas être recompilés pour générer une nouvelle application

87) Parmi les affirmations ci-dessous laquelle est vraie ?

- Une application mobile Android ne peut être déployée dans « Play Store » qu'au travers d'un MDM (Mobile Device Manager)
- Une application mobile Android doit être signée pour pouvoir être installée et exécutée. Le certificat de signature peut être auto-signé
- Une application mobile Android doit être signée pour pouvoir être installée et exécutée. Le certificat de signature doit être généré par l'Open Handset Alliance
- Il n'est pas nécessaire de signer une application mobile Android pour pouvoir l'installer et l'exécuter.

88) Qu'est « Dirty C0w » ?

- Une vulnérabilité présente dans « openssl » découverte en 2012 permettant à un attaquant de lire la mémoire d'un serveur
- Une vulnérabilité présente dans le shell Unix « bash » découverte en 2014 permettant à un attaquant d'exécuter des commandes arbitraires
- Une vulnérabilité découverte en 2016 permettant de réaliser une élévation de privilèges sous Linux mais qui ne fonctionne pas pour les systèmes d'exploitation d'Android
- Une vulnérabilité découverte en 2016 permettant de réaliser une élévation de privilèges sous Linux et sous certains systèmes d'exploitation d'Android

89) En quoi consiste l'ARP spoofing ?

- Il permet de réaliser un MITM. Tout le trafic de la cible transite par l'attaquant. L'attaquant peut écouter les paquets réseau mais il ne peut pas les modifier
- Il permet de réaliser un MITM. Tout le trafic de la cible transite par l'attaquant. L'attaquant peut écouter ou modifier les paquets réseau
- Il permet de créer un faux point d'accès Wifi pour que l'attaquant écoute ou modifie les paquets réseau de la cible
- Il permet de créer un faux point d'accès Wifi pour que l'attaquant écoute les paquets réseau de la cible (toute modification reste cependant impossible)

90) (*) La conséquence principale de la fragmentation du marché des téléphones Android (différents fabricants, différents opérateurs mobiles, différents téléphones supportés) est que

- la part de marché des concurrents d'Android diminue
- les prix des téléphones et des forfaits ne cessent d'augmenter
- les patchs ne seront jamais disponibles pour de nombreux téléphones qui resteront vulnérables
- le temps nécessaire au déploiement des patchs de sécurité peut être très long

Fin du QCM -