Nom : mai 2020
Prénom :

UVSQ – M2 SeCReTs 2020 – Contrôle de connaissances
Cours sur la sécurité des réseaux Wi-Fi, introduction à l'audit, introduction à la sécurité DevOps.

NB : Pour **certaines** des questions de cette partie, il convient de cocher non pas une, mais **plusieurs réponses exactes**.
Il faudra parfois saisir ou ajouter une courte justification écrite.

1) Pour pouvoir déchiffrer les trames Wi-Fi échangées entre un terminal légitime et un point d'accès configuré en WPA2 avec une authentification WPA-PSK (utilisant une *passphrase*), de quoi l'attaquant a-t-il besoin ? Pourquoi ?

- ❑ Du SSID diffusé par le point d'accès
- ❑ De la capture des échanges d'authentification WPA-PSK préliminaires (utilisant le protocole EAP) entre le terminal et le point d'accès
- ❑ De la *passphrase* WPA-PSK configuré sur le point d'accès
- ❑ Il n'est pas possible de déchiffrer les trames Wi-Fi protégées par WPA2

Pourquoi ?

2) À quoi sert le framework EAP dans la sécurité Wi-Fi (WPA2-Entreprise) ?

- ❑ EAP propose l'authentification par d'autres moyens que la Pre-Shared Key (PSK)
- ❑ EAP garanti l'implémentation du mécanisme cryptographique CCMP (AES).
- ❑ EAP propose le mode « PushButton », après un appui sur le bouton les stations disposent de 30 secondes pour s'appairer sans mot de passe.
- ❑ EAP permet de filtrer les stations suivant leur adresse MAC.

3) Est-ce qu'être connecté à un point d'accès (AP) Wi-Fi en WPA2 (avec PSK très robuste) est un gage de sécurité pour ma connexion vers un site Internet ?

- ❑ Oui, WPA2 avec PSK robuste est incassable. Après l'AP, RADIUS assure le chiffrement.
- ❑ Non, WPA2 peut être cassé avec les mêmes vulnérabilités que WEP.
- ❑ Non, il y a de forts risques que le trafic ne soit plus chiffré ensuite sur le lien Ethernet de l'AP vers le routeur.
- ❑ Oui, WPA2-Entreprise résout les problèmes de gestion du mot de passe Wi-Fi quand il y a des départs dans l'équipe.

4) Pourquoi les réseaux Wi-Fi seront toujours faillibles sur le critère de la disponibilité ?

- ❑ Les ondes Wi-Fi traversent les murs des entreprises
- ❑ Les brouilleurs / *jammers* existent
- ❑ WPA2 est sensible aux DDoS par amplification DNS
- ❑ Le framework EAP qui gère l'authentification et autorisation, n'inclus pas l'aspect disponibilité ?

5) Est-ce qu'être connecté à un point d'accès (AP) Wi-Fi en WPA2 (avec PSK très robuste) est un gage de sécurité pour ma connexion vers un site Internet ?

- ❑ Oui, WPA2 avec PSK robuste est incassable. Après l'AP, RADIUS assure le chiffrement.
- ❑ Non, WPA2 peut être cassé avec les mêmes vulnérabilités que WEP.
- ❑ Non, il y a de forts risques que le trafic ne soit plus chiffré ensuite sur le lien Ethernet de l'AP vers le routeur.
- ❑ Oui, WPA2-Entreprise résout les problèmes de gestion du mot de passe Wi-Fi quand il y a des départs dans l'équipe.

6) L'application d'un filtrage des adresses MAC au niveau des AP (points d'accès) Wi-Fi est-t-elle une mesure efficace ? Pourquoi ?

7) Quelles sont les conditions favorables pour espérer casser une clé WEP rapidement ?

- ❑ Lorsqu'un utilisateur légitime du réseau Wi-Fi y est connecté et échange des trames de données que l'attaquant peut acquérir
- ❑ Lorsque l'attaquant dispose de tables pré-calculées (*rainbow tables*) à partir de très nombreuses clés WEP possibles
- ❑ Lorsque l'attaquant est à proximité du point d'accès, facilitant l'injection de trames Wi-Fi spécifiquement forgées

8) Quel est l'algorithme de sécurité défini dans la norme 802.11i, correspondant au profil de sécurité (et certification) WPA, et facilitant la transition avec WEP ?

- ❑ AES en mode CCMP
- ❑ TKIP
- ❑ 3DES en mode CBC-MAC
- ❑ MIC

9) Quel est l’algorithme de sécurité défini dans la norme 802.11i, correspondant au profil de sécurité (et certification) WPA2 ?

- ❑ SHA-1
- ❑ TKIP
- ❑ AES en mode CCMP
- ❑ 3DES en mode CCMP

10) Pour pouvoir déchiffrer les trames Wi-Fi échangées entre un terminal légitime et un point d’accès configuré en WPA2 avec une authentification WPA-PSK (utilisant une *passphrase*), de quoi l’attaquant a-t-il besoin ? Pourquoi ?

- ❑ Du SSID diffusé par le point d’accès
- ❑ De la capture des échanges d’authentification WPA-PSK préliminaires (utilisant le protocole EAP) entre le terminal et le point d’accès
- ❑ De la *passphrase* WPA-PSK configuré sur le point d’accès
- ❑ Il n’est pas possible de déchiffrer les trames Wi-Fi protégées par WPA2

11) Depuis plusieurs années, le protocole WPS (Wi-Fi Protected Setup) est très largement déployé sur les points d'accès Wi-Fi. À quoi sert-il ?

- ❑ Remplacer l'authentification WPA-PSK qui est trop complexe
- ❑ Permettre la configuration d'une configuration WPA-PSK sur un terminal sans nécessiter de clavier et / ou d'écran (le terminal peut être un objet connecté, par exemple une montre)
- ❑ Chiffrer la connexion Wi-Fi sans passer par une étape préalable d'authentification mutuelle entre terminal et point d’accès

12) Parmi les propositions suivantes, laquelle correspond au(x) fonction(s) de sécurité proposée(s) dans le Wi-Fi par le mode OPEN ?

- ❑ Aucune
- ❑ Authentification forte des clients
- ❑ Chiffrement du trafic
- ❑ Chiffrement du trafic et authentification forte des clients

13) Le mode par défaut consiste à saisir sur le terminal un code PIN de 8 digits inscrits au dos du point d'accès Wi-Fi. Est-ce suffisamment sécurisé, et pourquoi ? Expliquer.

14) Afin de sécuriser l'accès à votre point d'accès Wi-Fi personnel, ou plus généralement celui d'un particulier, quelle configuration simple proposeriez-vous ?

- ❑ Utiliser le protocole WEP avec une clé de 104 bits et un contrôle d'accès par adresse MAC
- ❑ Utiliser un profil WPA2 avec une authentification EAP par certificats (par exemple, EAP-TLS)
- ❑ Utiliser un profil WPA2 avec une authentification WPA-PSK utilisant une *passphrase* complexe
- ❑ Activer et utiliser WPS (*Wi-Fi Protected Setup*) avec le code PIN inscrit au dos du point d'accès Wi-Fi

15) Pour un utilisateur en itinérance étant amené à se connecter sur des réseaux Wi-Fi de type hot-spot non maîtrisés (restaurant, gare, hôtels, ...), quel(s) comportement(s) préconisez-vous ?

- ❑ Configurer le pilote (*driver*) Wi-Fi ou le système d'exploitation pour que le terminal se reconnecte automatiquement sur tous les réseaux Wi-Fi connus
- ❑ Configurer le pilote Wi-Fi ou le système d'exploitation pour que le terminal ne se reconnecte pas automatiquement sur les points d'accès et SSID connus
- ❑ Forcer l'utilisation de WPA2 dans la configuration du pilote Wi-Fi ou du système d'exploitation du terminal, pour toutes les connexions Wi-Fi
- ❑ Utiliser des mécanismes de sécurité de plus haut niveau (SSH, TLS ou VPN IPsec par exemple) pour se connecter à ses services et réseaux privés
- ❑ Systématiquement désactiver l'interface Wi-Fi lorsqu'elle n'est pas utilisée

16) Pour les employés étant en télétravail et se connectant à Internet par la box de leur domicile, quelle est la mesure que vous allez obliger du fait que les employés manipulent des données sensibles ?

- ❑ L'utilisation de clés USB pour le transfert de document à l'extérieur de l'entreprise
- ❑ Le chiffrement du disque dur des PC portables
- ❑ L'utilisation d'un VPN IPsec depuis le PC portable vers l'entreprise
- ❑ L'utilisation d'un VLAN depuis le PC portable vers l'entreprise
- ❑ L'utilisation du Wi-Fi à l'extérieur de l'entreprise
- ❑ Se connecter au travers du navigateur web en navigation privée

17) Quelle problématique touchant l'aspect « gestion de la sécurité dans l'entreprise » est induite par d'utilisation d'une PSK (clé partagée) ?

18) L’application d’un filtrage des adresses MAC au niveau des AP (points d'accès) Wi-Fi est-t-elle une mesure efficace ? Pourquoi ?

19) Dans un audit, qui est l’audité ?
- ❑ La personne qui réalise l’audit
- ❑ La personne qui demande la réalisation de l’audit
- ❑ La personne responsable du périmètre sur lequel est réalisé l’audit
- ❑ Le chef de l’équipe d’audit qui va piloter les auditeurs réalisant l’audit

20) Quel est le risque principal d’une mauvaise configuration du fichier /etc/sudoers ?

21) A quoi sert l’outil john ?

22) Quelle est la formule de calcul du risque ?

- ❑ Risque = Menace x Impact
- ❑ Risque = Probabilité x Impact
- ❑ Risque = Probabilité x Vulnérabilité
- ❑ Risque = Menace x Vulnérabilité

23) Qu’est-ce que l’Infrastructure as Code ? (1 seule réponse attendue)

- ❑ La gestion des déploiements à partir de descriptions écrites avec du code.
- ❑ Le développement (codage) des éléments d’infrastructure (développement d’un firewall par exemple).
- ❑ L’écriture de scripts Bash contenant les commandes d’installation de l’infrastructure.
- ❑ Le référentiel développé en Python de l’ensemble des ressources informatique de l’entreprise.

24) Comment la sécurité peut tirer parti de l'*Infrastructure as Code* ?

25) Comment tester l'éventuelle présence de vulnérabilités dans un container ? (1 seule réponse attendue)

- ❑ Lancer un outil de scan allant se connecter en SSH sur le container.
- ❑ Exécuter un script de scan à l'intérieur du container exécuté.
- ❑ Lancer un scan de l'image du container (non exécuté).
- ❑ Arrêter le container, lancer un scan, puis relancé le container.

26) Quelle affirmation ci-dessous est vraie ?

- ❑ Les VM apportent une meilleure isolation que les containers grâce à l'hyperviseur.
- ❑ Les containers apportent une meilleure isolation que les VM grâce l'isolation par *namespaces*.
- ❑ Les VM ont une empreinte mémoire et CPU moins importante que les containers du fait qu'elles ne multiplient pas les noyaux.
- ❑ Les processus d'un container peuvent « voir » les processus d'un autre container du fait qu'il n'y a pas d'hyperviseur pour isoler les containers.

27) Quelles sont les affirmations conseillées ? (Plusieurs réponses valides)

- ❑ Exécuter un serveur SSH dans le container pour s'y connecter.
- ❑ N'utiliser que des images sources officielles.
- ❑ Mettre à jours les package régulièrement à l'intérieur de mon container (commandes : `apt upgrade / yum update`)
- ❑ Exécuter le container en mode *priviledged*.