ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

5 - RÉFÉRENTIELS

Article L6113-1 En savoir plus sur cet article... Créé par LOI n°2018-771 du 5 septembre 2018 - art. 31 (V)

« *Les certifications professionnelles enregistrées au répertoire national des certifications professionnelles permettent une validation des compétences et des connaissances acquises nécessaires à l'exercice d'activités professionnelles. Elles sont définies notamment par un* ***référentiel d'activités*** *qui décrit les situations de travail et les activités exercées, les métiers ou emplois visés, un* ***référentiel de compétences*** *qui identifie les compétences et les connaissances, y compris transversales, qui en découlent et un* ***référentiel d'évaluation*** *qui définit les critères et les modalités d'évaluation des acquis.* »

RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
Afin de mettre en place des tâches de contrôle et de suivre l'évolution des systèmes, l'opérateur doit: ❖ Automatiser des tâches répétitives en développant des scripts d'automatisation ❖ Maintenir des scripts déjà développés en les adaptant ou en les modifiant	❖ **Développer des scripts d'automatisation de tâches** ❖ Développer avec les langages les plus utilisés dans le domaine de la sécurité: **Python**, **Bash** et **Shell** afin de rédiger des scripts d'automatisation	❖ Mise en situation professionnelle de 3 heures: 5 tâches répétitives seront à automatiser afin de valider les compétences des opérateurs	❖ Le pseudo-code de l'algorithmie nécessaire à l'automatisation de la tâche (processus du programme) est pertinent et correspond à la tâche attendue ❖ Le choix du langage est approprié pour répondre au besoin. Ce choix doit être justifié par écrit.

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

			❖ Les points de contrôle afin de gérer les exceptions sont bien implémentés ❖ Les logs de sortie en cas d'erreurs d'exécution du programme sont correctement gérés
Afin de détecter des fichiers corrompus avec du code malveillant, l'opérateur doit: ❖ Analyser des programmes dans différents langages de script afin de déceler les vulnérabilités ❖ Analyser des programmes afin de détecter les potentielles menaces	❖ **Analyser un programme informatique** ❖ Analyser des programmes informatiques développés en Python, Bash et Shell afin de trouver les potentielles vulnérabilités et déceler si les tâches exécutées peuvent présenter une menace pour les systèmes visés	❖ Mise en situation professionnelle de 1 heure: lecture de trois scripts d'exécution contenant des vulnérabilités et des actions qui visent à nuire les cibles visées	❖ Les objectifs de chaque programme sont expliqués par écrit ❖ La vulnérabilité au sein de l'un des programmes a été identifiée ❖ Les exécutions des trois programmes contenant un risque pour les serveurs ont été comprises et expliquées

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

Afin d'être en mesure de gérer un parc informatique composé de plusieurs systèmes, l'opérateur doit: ❖ Installer, Paramétrer et Administrer les serveurs de type Microsoft ❖ Appliquer les stratégies de groupe Microsoft ❖ Administrer les services centralisés d'identification à un réseau d'ordinateurs en utilisant le système Windows ❖ Installer, Paramétrer et Administrer les serveurs de type Linux ❖ Administrer les distributions xBSD ❖ Superviser les serveurs des clients à distance ❖ Prévenir le responsable lorsque l'installation d'un client est défaillante	❖ **Gérer un parc informatique composé de systèmes d'exploitation propriétaires et libres** ❖ Assurer le bon fonctionnement d'un système d'exploitation Microsoft & Linux ❖ Administrer correctement un système afin d'appréhender l'ensemble des risques liés à la mauvaise gestion des serveurs ❖ Appliquer les correctifs relatifs aux dernières vulnérabilités découvertes par les organismes de détection et de prévention sur les systèmes concernés ❖ Vérifier que les standards de sécurité soient appliqués afin de prévenir une menace	❖ Mise en situation professionnelle de 4 heures: Mettre en place un serveur Windows avec des contraintes de configuration proposée dans un cahier des charges client ❖ Mise en situation professionnelle de 4 heures: Mettre en place un serveur Linux avec des contraintes de configuration proposée dans un cahier des charges client	❖ Les étapes pour installer le système d'exploitation sont correctement détaillées ❖ Le choix des partitions et de leur allocation mémoire est cohérent avec la capacité de la machine ❖ La configuration des standards de sécurité est correctement appliquée ❖ La documentation de son installation en intégrant les contraintes techniques est claires et détaillées ❖ La mise en place d'un plan de test basique afin de confirmer que les points clés sont respectés

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

❖ Prévenir le responsable lorsqu'un système ne comporte pas l'ensemble des mises à jour requises **Afin d'optimiser la gestion des ressources et d'améliorer la scalabilité des applications, l'opérateur doit:** ❖ Installer, paramétrer et administrer des serveurs virtualisés VmWare, Hyper V, XEN ❖ Installer, paramétrer et administrer des serveurs Docker ❖ Détecter une anomalie pour rendre-compte du problème à son responsable ❖ Administrer des serveurs virtualisés déployés au sein de l'entreprise	❖ **Déployer des applications au sein d'environnements virtualisés** ❖ Appliquer les règles nécessaires pour limiter les risques de failles de sécurité liés à la virtualisation ❖ Installer et configurer un serveur virtualisé en appliquant les procédures d'installation et de configuration nécessaires ❖ Sécuriser l'accès à un serveur virtualisé dans le cadre de la mise en place de la politique de sécurité	❖ Mise en situation professionnelle de 8 heures: Mettre en place un ensemble de serveurs virtualisés et les interconnecter	❖ Les étapes pour installer le serveur virtualisé sont correctement détaillées ❖ Le choix des partitions et de leur allocation mémoire est cohérent avec la capacité de la machine ❖ Les interconnexions entre les serveurs sont correctement paramétrées et vérifiées ❖ Les protocoles d'échanges sécurisés ont été configurés

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

Afin d'administrer une base de données, l'opérateur doit: ❖ Concevoir un schéma de base de données relationnelle ❖ Appliquer les principes de base pour protéger les accès aux bases de données ❖ Installer une base de données en lien avec le schéma relationnel établi ❖ Administrer une base de données à partir d'outils de gestion ❖ Administrer une base de données à partir de l'outil "ligne de commande" ❖ Interroger une base de données en utilisant le langage approprié	❖ **Administrer des bases de données de type relationnel** ❖ S'appuyer sur la méthode MERISE ❖ Effectuer des requêtes SQL ❖ Gérer la conception des bases de données en utilisant Oracle, SQL Server Microsoft, MySql, PostgreSQL ❖ Employer les outils de gestion de SGBDR ❖ Appliquer les règles de sécurité sur une base de données relationnelle	❖ Mise en situation professionnelle de 8 heures: installer et administrer une base de données	❖ Le schéma relationnel à partir d'un cahier des charges client est correctement défini ❖ La base de données à partir de requêtes SQL est bien installée ❖ Les règles de sécurité de base sont correctement mises en place ❖ Les outils de gestion de SGBDR sont installés et correctement utilisés ❖ Les manipulations de données à partir de requêtes SQL sont correctes

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

Afin de configurer et d'administrer un réseau d'entreprise, l'opérateur doit: ❖ Calculer les adresses IP et les masques de sous-réseau selon un nombre de machines définies ❖ Gérer et attribuer les IP selon la répartition des architectures ❖ Mettre en place un réseau local et paramétrer un NAT afin de gérer la traduction IP publique/locale ❖ Installer et configurer un serveur DNS au sein d'un réseau local ❖ Analyser les protocoles TCP, UDP, ICMP et les trames de données associées à chaque protocole en vue de détection d'anomalies	❖ **Administrer un réseau d'entreprise en gérant son architecture, son fonctionnement et son organisation** ❖ Configurer un NAT et un DNS ❖ Calculer et gérer les adressages public et privé ❖ Détecter les erreurs sur un réseau en analysant le trafic par la connaissance des protocoles IPV4/IPV6, ICMP et de couche Transport: TCP, UDP, RTP ❖ Paramétrer les différentes applications à déployer au sein d'une entreprise: de la messagerie à la VOD (Skype, Zoom, etc.)	❖ Mise en situation professionnelle de 8 heures: Mettre en place un réseau local en utilisant l'outil Cisco Packet Tracer	❖ La définition des masques de sous-réseau en fonction du nombre de machines sur chaque réseau correspond au cahier des charges client ❖ Les attributions des IP sur chaque poste selon le nombre de réseaux sont logiques ❖ Le serveur DNS au sein de son réseau est correctement paramétré ❖ Le NAT pour la translation d'adresses est correctement paramétré ❖ Les anomalies au sein de trames de différents protocoles sont analysées et détectées

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

Afin d'installer un réseau d'entreprise, l'opérateur doit être en mesure de choisir les composants physiques nécessaires. Pour cela, il doit: ❖ Choisir le câblage nécessaire à la bonne transmission du signal ❖ Définir le débit de connexion approprié selon les besoins de l'entreprise	❖ **Déployer et gérer les réseaux à accès pour la connexion des terminaux et usagers** ❖ Choisir les différents supports de transmission: paire torsadée (ADSL, VDSL), la boucle locale optique (FTTB, FTT, FTTdp), les solutions câblo-opérateurs, les modems câbles, la boucle locale radio, wifi, les réseaux domicile (WIFI et CPL) ❖ Choisir les solutions cellulaires appropriées au besoin des salariés (3G/4G/4G+/5G) ❖ Paramétrer les réseaux domiciles (WIFI et CPL) ❖ Installer un réseau en s'appuyant sur le mécanisme de la boucle locale des entreprises	❖ Mise en situation théorique: répondre à un QCM de 40 questions	❖ Les caractéristiques techniques des différents câblages sont connues et le choix du câblage est cohérent avec le besoin de l'architecture réseau présentée lors du QCM ❖ Les caractéristiques techniques d'un réseau à boucle locale résidentielle sont connues et les explications des limites du champ d'application sont correctement détaillées ❖ Les caractéristiques techniques d'un réseau local d'entreprise sont connues et les explications des limites du champ d'application sont correctement détaillées

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

Afin d'administrer un réseau entreprise et assurer la sécurisation des échanges, l'opérateur doit: ❖ Paramétrer un routeur afin d'interconnecter plusieurs réseaux différents ❖ Utiliser un commutateur dans le cadre d'interconnexion entre plusieurs périphériques ❖ Administrer un réseau local d'entreprise avec des outils de monitoring ❖ Paramétrer un réseau MPLS avec gestion des commutations de labels ❖ Paramétrer un tunnel d'échanges sécurisés entre deux serveurs en utilisant un VPN	❖ **Gérer l'articulation des réseaux de transport** ❖ Paramétrer son réseau en s'appuyant sur les notions d'acheminement, de commutation et de routage ❖ Vérifier le bon fonctionnement d'un réseau local d'entreprise à partir de point de contrôle ❖ Appliquer la commutation de labels et l'architecture MPLS au sein d'un réseau ❖ Utiliser les VPN et les solutions pour les mettre en place	❖ Mise en situation professionnelle de 2 heures: au sein d'un réseau local déjà monté, paramétrer un routeur et utiliser un commutateur en utilisant l'outil Cisco Packet Tracer ❖ Mise en situation professionnelle de 2 heures: au sein d'un réseau local déjà monté, mettre en place une connexion sécurisée par	❖ L'architecture d'un réseau déjà en place est correctement comprise et le routeur est paramétré en fonction des contraintes définies ❖ Un commutateur est correctement installé afin de relier les différents périphériques ❖ Des tests de connectivité sont appliqués afin de vérifier que les différents réseaux sont correctement reliés ❖ Un tunnel VPN entre deux serveurs est correctement configurés ❖ Un sniffer de réseau type Wireshark est utilisé afin

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

		un tunnel VPN en utilisant l'outil Cisco Packet Tracer	de vérifier que les échanges sont chiffrés
Afin de configurer et administrer des réseaux sans fil, l'opérateur doit: ❖ Paramétrer un réseau local sans fil WIFI en s'appuyant sur les standards IEEE et en prenant en compte les besoins de l'entreprise (ratio entre nombre d'utilisateurs et débit) ❖ Appliquer les règles de sécurité de base sur un réseau local WIFI installé ❖ Tester la connectivité du réseau local WIFI mis en place	❖ **Configurer les réseaux sans fil et mobilité** ❖ Choisir le type de réseau sans fil approprié en s'appuyant sur les différentes typologies: WPAN, WLAN, WMAN, MRAN, Hot spot, hand over, roaming, GPRS, UMTS ❖ Consulter et appliquer les référentiels des différentes technologies réseaux sans fil: IEEE 802.15, WPAN, Bluetooth, ZigBee, UWB ❖ Appliquer les principes de IEEE 802.11 (a/b/e/g/n) ❖ Faire une veille sur les nouvelles générations de WIFI (ac, af, ah, WiGig) ❖ Appliquer les principes de IEEE 802.22 et les futurs produits Wi-RAN	❖ Mise en situation professionnelle de 4 heures: configurer un réseau local WIFI en utilisant l'outil Cisco Packet Tracer	❖ Les standards proposés par l'IEEE 802.11 sont suivis dans le cadre d'une configuration réseau local WIFI ❖ Son réseau local WIFI est dimensionné en fonction du nombre d'utilisateurs prévus ❖ Les configurations nécessaires au bonne pratique en terme de sécurisation du réseau sont appliquées ❖ La connectivité est testée afin de s'assurer que le débit est suffisant pour l'ensemble des utilisateurs

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

Afin de mettre en place et administrer des réseaux virtualisés, l'opérateur doit: ❖ Administrer une console d'administration de serveurs virtualisés en utilisant les différentes consoles SDN (Software-Defined Networking) ❖ Paramétrer un réseau local virtuel ❖ Paramétrer les routeurs d'un réseau virtuel ❖ Installer et connecter les commutateurs ❖ Utiliser l'algorithme de spanning tree afin de gérer les réseaux à topologie sans boucle	❖ Faire une veille sur les évolutions de l'internet ambiant: réseaux mesh, ad-hoc, réseaux de capteurs et RFID, NFC ❖ **Configurer et administrer des réseaux virtualisés** ❖ Virtualiser des serveurs et comprendre l'impact sur l'infrastructure ❖ Appliquer la centralisation du plan de contrôle et les fonctions d'un contrôleur ❖ Employer le protocole OpenFlow et l'évolution SDN (Software Defined Networking) ❖ Utiliser le principe de la technique d'accès: ISO 8802.3 (CSMA/CD) ❖ S'appuyer sur les normalisations, IEEE 802 et ISO, les couches physiques, MAC et LLC, les principaux protocoles ❖ Configurer les réseaux locaux virtuels (VLAN), les réseaux locaux Ethernet (SAN, LAN, WLAN)	❖ Mise en situation professionnelle de 4 heures: configurer un réseau local virtuel en utilisant l'outil Cisco Packet Tracer	❖ Les fonctionnements de la suite logiciel SDN et du protocole OpenFlow sont connus et explicités avec un schéma de processus ❖ Un réseau local virtuel est paramétré en fonction des consignes d'adressage ❖ Les routeurs sont paramétrés pour interconnecter les différents réseaux ❖ Les commutateurs sont utilisés de manière appropriée. Le choix doit être justifié par écrit

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

	❖ Configurer le paramétrage de pont, commutation de niveau 3, 4 et 7		❖ Son réseau est paramétré pour utiliser l'algorithme du spanning tree ❖ Les tests de connectivités sont présentés afin de s'assurer des bons paramétrages
Afin de surveiller les réseaux informatiques d'une entreprise et détecter de potentielles menaces, l'opérateur doit: ❖ Analyser et manipuler les puits de logs ❖ Utiliser les outils de monitoring et de visualisation ❖ Administrer les outils de détection d'intrusions du marché ❖ Classer les menaces selon leur niveau de criticité ❖ Paramétrer les règles de base des outils de détection	❖ **Supervision des réseaux informatiques d'une entreprise** ❖ Utiliser les outils de manipulation de fichiers de logs ❖ Analyser les logs afin de détecter des anomalies ou des comportements anormaux ❖ Paramétrer les outils d'analyse et de visualisation de type ElasticSearch et Kibana ❖ Utiliser les outils d'administration et de détection type SIEM, IDS/IPS	❖ Mise en situation professionnelle de 2 heures: utiliser un système de visualisation et d'interprétation de logs	❖ En utilisant l'interface de visualisation de Kibana et la base de données ElasticSearch, les logs critiques sont détectées et répertoriés ❖ La menace détectée au sein des logs et correctement classée avec le niveau de criticité approprié

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

Afin d'assurer une protection des systèmes d'information, l'opérateur doit: ❖ Appliquer les politiques de gestion des accès et des identités au sein d'une entreprise ❖ Paramétrer le durcissement des postes utilisateurs sur les environnements linux et windows ❖ Mettre en place le chiffrement dans le cadre de la sécurisation des échanges entre serveurs ❖ Mettre en place le chiffrement dans le cadre d'échanges entre utilisateurs ❖ Appliquer les règles de filtrages en utilisant les outils de firewall sur	❖ Analyser le niveau d'une menace et de la classer selon le niveau de criticité ❖ **Sécurisation des réseaux et des échanges** ❖ Utiliser les outils de gestion des identités et des accès afin de mettre en place une politique de sécurité d'accès aux données au sein de l'entreprise ❖ Mettre en oeuvre les différentes étapes nécessaires au durcissement d'un poste linux et windows ❖ Appliquer les principes de base de la cryptographie afin de mettre en place une politique de chiffrement adéquat	❖ Mise en situation professionnelle de 2 heures: Appliquer des règles de gestion d'accès en utilisant un IAM ❖ Mise en situation professionnelle de 8 heures: Durcir un poste linux et windows ❖ Mise en situation professionnelle de 2 heures: Chiffrer une communication en deux	❖ Une nouvelle règle sur le système IPS/IDS est paramétrée en fonction de la menace détectée précédemment ❖ Les règles exposées sur le cahier des charges sont comprises et appliquées avec logique au sein du logiciel ❖ Toutes les étapes de configuration requises sont mises en place pour un durcissement de postes linux et windows ❖ Les technologies de chiffrement open source appropriées sont utilisées

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

les environnements linux et windows	❖ Mettre en place des règles de filtrage en utilisant les outils appropriés selon le système d'exploitation	utilisateurs en utilisant un chiffrement asymétrique ❖ Mise en situation professionnelle de 2 heures: appliquer des règles de parefeu sur un environnement linux	❖ Les clés de chiffrements sont créées en expliquant les différentes étapes ❖ Des tests entre deux postes sont effectués ❖ Un message chiffré est réceptionné, puis déchiffré ❖ Les règles de filtrage définies dans le cahier des charges sont correctement appliquées ❖ Des tests sont appliqués afin de vérifier que les règles sont effectives ❖ La bonne hiérarchie des règles est respectée afin d'éviter des conflits

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

Afin d'appliquer les mesures adéquats dans le cadre de la sécurisation des réseaux sans fil, l'opérateur effectue des tests. Pour cela, il doit tenter de: ❖ Bypasser une authentification sur un réseau sans fil **Afin de sécuriser les échanges au sein d'un réseau sans fil, l'opérateur doit pouvoir:** ❖ Détecter les vulnérabilités pour cracker le chiffrement sur un réseau WLAN	❖ **Attaquer un réseau sans fil** ❖ Gérer l'authentification sur un WLAN ❖ Trouver le SSID ❖ Utiliser les filtres d'adresse MAC ❖ Utiliser le mécanisme de "Shared Key Authentication" ❖ **Attaquer un réseau sans fil par les vulnérabilités de chiffrement WLAN** ❖ Appliquer les techniques adéquates pour accélérer le processus de cracking ❖ Décrypter des paquets	❖ Mise en situation professionnelle de 4 heures: Attaquer un réseau sans fil WLAN afin d'en prendre son contrôle	❖ Les routeurs sur un réseau WLAN sont détectés ❖ Des vulnérabilités sur le routeur sont identifiées ❖ L'attaque appropriée est choisie en fonction de la/les vulnérabilités identifiées ❖ Le contrôle du routeur est pris et une trace est laissée sur le serveur afin de contrôler la réussite de l'intrusion ❖ Un compte-rendu clair et détaillé est rédigé afin d'expliquer la méthodologie utilisée et les failles détectées

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

Afin de sécuriser son infrastructure réseau sans fil, l'opérateur doit pouvoir: ❖ Détecter les routeurs à attaquer au sein d'un réseau WLAN ❖ Pratiquer une attaque avec l'usage de techniques avancées sur les réseaux sans fil	❖ **Attaquer un réseau sans fil en visant l'infrastructure** ❖ Appliquer la méthodologie pour structurer son attaque ❖ Identifier un routeur sur un réseau ❖ Utiliser les différents types d'attaques Deni of Service (Dos) ❖ Appliquer les attaques Evil Twin, Rogue AP. ❖ Utiliser les différents scénarios d'attaque avancée ❖ Appliquer les méthodes de MiTM, Eavesdropping, Session hijacking ❖ Cartographier les configurations de sécurité client		

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

Afin de mieux sécuriser un réseau sans fil WPA, l'opérateur doit pouvoir: ❖ Attaquer le réseau sans fil WPA Entreprise	❖ **Attaquer un réseau sans fil type WPA-E et Radius** ❖ Appliquer les différentes attaques WPA-E et cartographier l'architecture ❖ Configurer et installer l'AP et le FreeRadius-WPE ❖ Pratiquer une attaque EAP ❖ Appliquer les best practices de sécurisation WLAN-E		
Afin de sécuriser un réseau sans fil WPS, l'opérateur doit pouvoir: ❖ Attaquer le réseau sans fil WPS	❖ **Attaquer un réseau sans fil type WPS et Probe** ❖ Appliquer les différentes attaques WPS et cartographier l'architecture ❖ Appliquer les techniques de Probe Sniffing		

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

Afin de vérifier que le réseau d'entreprise est bien sécurisé, l'opérateur doit périodiquement: ❖ Préparer une attaque en utilisant la méthodologie d'un pirate informatique	❖ **Cartographier les vulnérabilités d'un réseau** ❖ Appliquer la méthodologie pentest ❖ Utiliser les outils de scanning ❖ Utiliser Metasploit ❖ Employer les outils tels que Wireshark afin d'effectuer du sniffing ❖ Appliquer les méthodes pour effectuer du spoofing ❖ Mettre en place un MiTM ❖ Appliquer les bases de l'attaque VOIP ❖ Effectuer du flooding	❖ Mise en situation professionnelle de 8 heures: Attaquer un réseau LAN entreprise	❖ Un mapping du réseau LAN entreprise est effectué et documenté ❖ Un scanning est mis en place pour identifier les ports ouverts et les services utilisés ❖ Des vulnérabilités sur les services identifiés sont identifiées ❖ Le système est introduit (pénétré) en utilisant un exploit ❖ L'accès au système est maintenu et l'effacement de traces est géré ❖ Un compte-rendu détaillé de ses actions est rédigé afin d'expliquer la

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

Afin de vérifier que son routeur est bien sécurisé, l'opérateur doit tenter périodiquement de: ❖ Prendre le contrôle d'un routeur au sein d'un réseau informatique **Afin de vérifier que les postes utilisateurs sont bien sécurisés, l'opérateur doit tenter périodiquement de:** ❖ Introduire un poste Windows par l'exploitation d'un exploit ou d'une vulnérabilité	❖ **Utiliser les vulnérabilités d'un réseau dans le cadre de l'attaque routeur** ❖ Appliquer les différentes attaques possibles sur un routeur: SSH, SNMP, CISCO, etc. ❖ **Utiliser les vulnérabilités d'un réseau dans le cadre de l'attaque d'une machine Windows** ❖ Utiliser un exploit afin d'obtenir un accès machine ❖ Détecter et désactiver d'un firewall pour porter une attaque sur une machine windows ❖ Appliquer la technique de port forwarding ❖ Utiliser le pivoting		méthodologie utilisée et les failles détectées

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

❖ Maintenir un accès sur le système corrompu et effacer ses traces **Afin de vérifier que son réseau entreprise est bien sécurisé, l'opérateur doit périodiquement tester s'il peut:** ❖ Introduire un poste client par Social Engineering	❖ Appliquer la technique du tunneling ❖ Appliquer les techniques d'élévation de privilèges ❖ **Utiliser les vulnérabilités d'un réseau dans le cadre de la post-exploitation** ❖ Monitorer ses accès dans le but d'effacer ses traces. ❖ Utiliser les techniques de maintien de session ❖ Manipuler les outils tels que PowerShell et/ou WevTUTIL pour limiter les traces au sein des logs ❖ **Utiliser les vulnérabilités d'un réseau dans le cadre d'attaques sur les postes clients** ❖ Employer les techniques d'Anti-Virus Evasion ❖ Manipuler les techniques d'attaque sur les navigateurs		

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

Afin d'élargir le cadre de ses tests d'intrusion, l'opérateur doit périodiquement: ❖ Appliquer des techniques d'attaques avancées sur un système d'information **Afin de pouvoir s'assurer que les applications web de l'entreprise sont bien sécurisées, l'opérateur doit périodiquement:** ❖ Cartographier les services et leurs vulnérabilités lors d'une phase de reconnaissance d'une cible à attaquer	❖ Utiliser les outils et levier pour une attaque par social engineering ❖ **Utiliser les vulnérabilités d'un réseau dans le cadre d'attaques avancées** ❖ Connaître les outils et techniques avancées tels que Metasploit Loader, DLL Hijacking, DLL Main, Shell Code Exec, etc. ❖ **Utiliser les vulnérabilités Web dans le cadre de la phase de reconnaissance** ❖ S'appuyer sur les standards OWASP ❖ Utiliser les différents outils de scanning proxy et Nessus	❖ Mise en situation professionnelle de 8 heures: Attaquer un site Web afin de prendre le contrôle d'un serveur	❖ Un scan de la cible est effectué afin de déceler les vulnérabilités du site ❖ Un exploit est utilisé afin de prendre le contrôle du serveur Web ❖ Une élévation de privilèges est appliquée afin de prendre le contrôle

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

❖ Introduire un serveur Web en exploitant les différentes failles d'un système ❖ Corrompre les protocoles d'échanges sécurisés afin d'intercepter le trafic ❖ Exploiter les failles de CMS afin d'introduire un serveur Web	❖ **Utiliser les vulnérabilités Web dans le cadre de la phase exploitation** ❖ Utiliser les failles RFI & LFI ❖ Utiliser les failles Upload ❖ Effectuer du Cross Site Scripting et du Cross Site Request Forgery ❖ Utiliser les techniques de SQL Injection, Clickjacking, Injection HTML, Injection de commandes, etc. ❖ Paramétrer une Exploitation Server Side et Client Side (MiTM, Social Engineering) ❖ **Utiliser les vulnérabilités Web dans le cadre d'attaques sur authentification** ❖ Utiliser les techniques de Hijacking, Brute Force et attaque sur les protocoles sécurisés ❖ **Utiliser les vulnérabilités Web dans le cadre d'attaques sur CMS** ❖ Utiliser les techniques d'attaque sur les principaux CMS tels que WordPress, Joomla, etc.		total de la machine (niveau root) ❖ Un compte-rendu détaillé est rédigé afin d'expliquer la méthodologie utilisée et les failles détectées