ÉCOLE EUROPÉENNE DE CYBERSÉCURITÉ

REFERENTIEL D'ACTIVITES DE COMPETENCES ET D'EVALUATION

Article L6113-1 créé par la 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. »

Intitulé de la certification

Opérateur en cybersécurité - Niveau 5

Description du métier, des activités et de la situation professionnelle à partir duquel le dispositif de formation visant la certification est initié

Contexte

La cybersécurité est un enjeu majeur pour la France. Le pays est régulièrement la cible de cyberattaques, qui peuvent entraîner des conséquences économiques, politiques et sociales importantes.

Le gouvernement français a pris des mesures qui ont permis de renforcer la cybersécurité du pays, mais il reste encore beaucoup à faire. Le risque cyber a considérablement augmenté ces dernières années, en particulier depuis la crise sanitaire et le conflit russo-ukrainien, concomitant à la numérisation des processus et modes de travail et aux avancées technologiques telles que l'IA et l'informatique quantique. L'ambition nationale dans ce domaine est régulièrement actualisée dans différents documents institutionnels, comme la Revue Nationale Stratégique 2022 publiée par le Secrétariat Général de la Défense et de la Sécurité Nationale qui vise une « résilience cyber de premier rang ».

La cyberdéfense doit donc suivre et faire face aux menaces afin de protéger l'ensemble de nos systèmes et réseaux : hôpitaux, sites industriels, OIV…

Pour se protéger, les entreprises et administrations font alors appel à un opérateur en cybersécurité.

Métier

La mission de l'opérateur en cybersécurité est de protéger les données et la fiabilité du système informatique d'une entreprise ou d'une administration en matière de prévention, détection et correction.

Pour cela, il réalise un diagnostic du système d'information dans le but de déceler les éventuels points faibles, apporte différentes solutions de protection pour sécuriser les informations et les données de l'entreprise, met en place les différents processus de sécurité, garantit la pérennité des systèmes de sécurité et actualise ces derniers en fonction des nouvelles menaces et des dernières technologies. Il est aussi responsable de rétablir dans les meilleures conditions le système d'information ayant subi une attaque.

Pré requis

- Être inscrit dans un parcours de formation menant à la certification.
- Être titulaire d'un diplôme ou titre d'un niveau 4 ou niveau bac (au minimum) avec un bon niveau d'anglais technique, ou avoir une expérience significative de 2 ans et les compétences informatiques nécessaires à l'exercice du métier d'opérateur et une bonne compréhension du fonctionnement des entreprises.

REFERENTIEL D'ACTIVITES ***décrit les situations de travail et les activités exercées, les métiers ou emplois visés***	**REFERENTIEL DE COMPETENCES** ***identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités***	**REFERENTIEL D'EVALUATION** ***définit les critères et les modalités d'évaluation des acquis***	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC 01 - REALISER DES TACHES DE PROGRAMMATION			
ACTIVITE 1 **Mise en place de tâches de contrôle et suivi de l'évolution des systèmes** **A1.1.** Automatisation de tâches répétitives en développant des scripts d'automatisation **A1.2.** Maintien de scripts déjà développés en les adaptant ou en les modifiant	**C1 . Développer des scripts d'automatisation** en utilisant les langages les plus utilisés dans le domaine de la sécurité (Python, Bash et C) **afin d'automatiser des tâches répétitives**	**ME1 – (C1-C2)** **Mise en situation professionnelle** **ME1.1.** Automatisation de 5 tâches répétitives Lecture de trois scripts d'exécution contenant des vulnérabilités et des actions qui visent à nuire aux cibles visées **ME1.2.** Etude de documents et réalisation de l'automatisation d'une tâche Analyse de scripts préexistants et recherche de vulnérabilités	**CE1.1.**Le pseudo-code de l'algorithmie nécessaire à l'automatisation de la tâche (processus du programme) correspond à la tâche attendue **CE1.2.**Le choix du langage permet de répondre au besoin
ACTIVITE 2 **Détection de fichiers corrompus avec du code malveillant** **A2.1.** Analyse des programmes du fonctionnement des antivirus **A2.2.** Analyse des programmes dans différents langages et interprétations de codes	**C2. Identifier les potentielles vulnérabilités d'un système d'information** en analysant des programmes informatiques développés en Python, Bash et C. en utilisant un outil d'IA **afin de prévenir des bugs potentiels et mauvaises pratiques de programmation**		**CE2.1.**Les points de contrôle pour gérer les exceptions sont implémentés **CE2.2.**Les logs de sortie en cas d'erreurs d'exécution du programme sont gérés **CE2.3.**Les objectifs de chaque programme sont expliqués **CE2.4.**La vulnérabilité au sein de l'un des programmes est identifiée **CE2.5.**Les exécutions des programmes contenant un risque pour les serveurs sont expliquées
BLOC 02 - CONFIGURER ET ADMINISTRER DES SYSTEMES ET APPLICATIONS DANS UN ENVIRONNEMENT VIRTUALISE			
ACTIVITE 3 **Gestion d'un parc informatique composé de plusieurs systèmes** **A3.1.** Installation, paramétrage et administration de serveurs de type MICROSOFT **A3.2.** Application des stratégies de groupe MICROSOFT	**C3. Gérer un parc informatique composé de systèmes d'exploitation propriétaires et libres** en assurant l'installation et la maintenance d'un système d'exploitation MICROSOFT & LINUX en appliquant les correctifs relatifs aux vulnérabilités découvertes par les organismes de détection et de prévention sur les systèmes concernés en vérifiant que les standards de sécurité sont appliqués	**ME2 – (C3-C4)** **Mise en situation professionnelle** **ME2.1.** Mise en place d'un serveur avec des contraintes de configuration définies	**CE3.1.**Les étapes pour installer le système d'exploitation sont détaillées **CE3.2.**Le choix des partitions et de leur allocation mémoire est adapté à la capacité de la machine **CE3.3.**La configuration des standards de sécurité est appliquée

A3.3. Administration des services centralisés d'identification à un réseau d'ordinateurs en utilisant le système WINDOWS **A3.4.** Installation, paramétrage et administration de serveurs de type LINUX **A3.6.** Supervision des serveurs des clients à distance **A3.6.** Compte-rendu à la hiérarchie en cas d'installation défaillante ou lorsqu'un système ne comporte pas l'ensemble des mises à jour requises	**afin d'appréhender l'ensemble des risques liés à une gestion potentiellement défaillante des serveurs et d'anticiper une menace**	dans le cahier des charges d'un client fictif **ME2.2.** Déploiement d'applications dans un environnement virtualisé pour répondre à une expression de besoin	**CE3.4.**La documentation de l'installation d'un serveur Activ Directory Windows et/ou Linux en intégrant les contraintes techniques est détaillée **CE3.5.**La mise en place d'un plan de test basique permet de confirmer que les points clés sont respectés
ACTIVITE 4 **Optimisation de la gestion des ressources des applications et amélioration de leur scalabilité** **A4.1.** Installation, paramétrage et administration des serveurs virtualisés (VmWare, Hyper V, XEN …) **A4.2.** Installation, paramétrage et administration des serveurs Docker **A4.3.** Détection d'anomalies **A4.4.** Administration des serveurs virtualisés déployés au sein de l'entreprise	**C4. Déployer des applications au sein d'environnements virtualisés** en installant et en configurant un serveur virtualisé (VmWare, Hyper V, XEN …) en appliquant les règles nécessaires pour limiter les risques de failles de sécurité liés à la virtualisation en utilisant une technologie de conteneurisation (Docker) pour empaqueter les applications et leurs dépendances en appliquant les procédures d'installation et de configuration nécessaires en sécurisant l'accès à un serveur virtualisé dans le cadre de la mise en place de la politique de sécurité **afin d'optimiser la gestion des ressources des applications et amélioration de leur scalabilité**		**CE4.1.**Les étapes pour installer le serveur virtualisé sont détaillées **CE4.2.** A partir du cahier des charges fourni, les choix de capacité de la machine correspondent aux besoins des applications supportées **CE4.3.**Les interconnexions entre les serveurs sont paramétrées et sécurisées **CE4.4.**Les protocoles d'échanges sécurisés sont configurés

ACTIVITE 5 Prise en compte d'une situation de handicap	**C5. Favoriser l'inclusion professionnelle d'une personne en situation de handicap** en proposant par défaut des équipements et logiciels qui puissent être utilisés par toute personne, quel que soit son handicap potentiel en proposant, à défaut, des équipements et des logiciels adaptés en les réglant et en les paramétrant **afin d'aménager son poste et son environnement de travail**	**ME3 –(C5)** **Mise en situation professionnelle** **ME3.1** Identification d'équipements ou de matériels adaptés aux situations de handicap **ME3.2** Identification des adaptations et des paramétrages sur les logiciels	**CE5.1.** Les équipements proposés répondent à la gestion d'une situation de handicap **CE5.2.** Les fonctionnalités des logiciels proposés permettent un réglage ou une adaptation aux personnes en situation de handicap
BLOC 03 - INSTALLER ET GERER DES BASES DE DONNEES RELATIONNELLES			
ACTIVITE 6 **Administration d'une base de données** **A6.1.** Conception d'un schéma de base de données relationnelle **A6.2.** Application des principes de base pour protéger les accès aux bases de données **A6.3.** Installation d'une base de données en lien avec le schéma relationnel établi **A6.4.** Administration d'une base de données à partir d'outils de gestion **A6.5.** Administration d'une base de données à partir de l'outil "ligne de commande" **A6.6.** Interrogation d'une base de données en utilisant le langage approprié	**C6. Administrer des bases de données de type relationnel** en s'appuyant sur la méthode MERISE en effectuant des requêtes SQL en gérant la conception des bases de données en utilisant Oracle, MySql, PostgreSQL en utilisant les outils de gestion de SGBDR en appliquant les règles de sécurité sur une base de données relationnelle **afin de maintenir un environnement de base de données robuste et sécurisé.**	**ME4 – (C6-C7)** **Mise en situation professionnelle** **ME4.1.** Création d'un schéma de base de données relationnelle **ME4.2.** Installation et administration d'une base de données	**CE6.1.**Le schéma relationnel à partir d'un cahier des charges client est défini **CE6.2.**La base de données à partir de requêtes SQL est installée **CE6.3.**Les règles de sécurité de base sont mises en place **CE6.4.**Les outils de gestion de SGBDR sont installés et utilisés **CE6.5.**Les manipulations de données à partir de requêtes SQL sont effectuées

ACTIVITE 7 **Conception d'une architecture de bases de données pour une application** **A7.1.** Propositions de solutions techniques **A7.2.** Création des tables de la base	**C7. Concevoir une architecture de bases de données pour une application** en proposant des solutions techniques (mode projet) en préparant la création des tables de la base en s'assurant de la fonctionnalité et du bon fonctionnement de la base. **afin de préparer la mise en place d'une application de façon sécurisée.**		**CE7.1.** Le cahier des charges de l'application répond à l'expression du besoin du client **CE7.2.** Le schéma de base de données répond au cahier des charges **CE7.3.** La base et des tables correspondent au schéma
BLOC 04 - CONFIGURER ET ADMINISTRER UN RESEAU D'ENTREPRISE			
ACTIVITE 8 **Configuration et administration d'un réseau d'entreprise** **A8.1.** Calcul des adresses IP et des masques de sous-réseau selon un nombre de machines définies **A8.2.** Gestion et attribution des IP selon la répartition des architectures **A8.3.** Mise en place d'un réseau local et paramétrage d'un NAT **A8.4.** Installation et configuration d'un serveur DNS au sein d'un réseau local **A8.5.** Analyse des protocoles TCP, UDP, ICMP et des trames de données associées à chaque protocole	**C8. Administrer un réseau d'entreprise** en configurant un NAT et un DNS en calculant et gérant les adressages privés en détectant les erreurs sur un réseau en analysant le trafic par la connaissance des protocoles IPV4/IPV6, ICMP et de couche Transport: TCP, UDP en paramétrant les différentes applications à déployer au sein d'une entreprise: de la messagerie à la VOD (Skype, Zoom, etc.) **afin de gérer son architecture, son fonctionnement et son organisation**	**ME5 – (C8-C9-C10)** **Mise en situation professionnelle** **ME5.1.** Mise en place d'un réseau local interconnecté en utilisant l'outil Cisco Packet Tracer **ME5.2.** Au sein d'un réseau local préexistant, recherche, analyse et dépannage des dysfonctionnements	**CE8.1.**La définition des masques de sous-réseau en fonction du nombre de machines sur chaque réseau correspond au cahier des charges client **CE8.2.**Les attributions des IP sur chaque poste selon le nombre de réseaux sont logiques **CE8.3.**Le serveur DNS au sein de son réseau est paramétré **CE8.4.**Le NAT pour la translation d'adresses est paramétré **CE8.5.**Les anomalies au sein de trames de différents protocoles sont détectées et analysées
ACTIVITE 9 **Installation d'un réseau d'entreprise** **A9.1.** Choix des composants physiques **A9.2.** Choix du câblage nécessaire à la transmission du signal **A9.3.** Définition du débit de connexion adapté aux besoins de l'entreprise	**C9. Déployer et gérer les réseaux à accès pour la connexion des terminaux et usagers (mode projet)** en paramétrant les réseaux domiciles (WIFI et CPL) en installant un réseau en s'appuyant sur le mécanisme de la boucle locale des entreprises en paramétrant un système de VLAN respectant la structure organisationnelle de l'entreprise **afin d'installer un réseau d'entreprise**		**CE9.1.**Les caractéristiques techniques des différents câblages sont identifiées **CE9.2.** Le choix du câblage est en phase avec le besoin de l'architecture réseau **CE9.3.** Les caractéristiques techniques d'un réseau à boucle locale résidentielle sont identifiées et les explications des limites du champ d'application sont détaillées

			CE9.4. Les caractéristiques techniques d'un réseau local d'entreprise sont identifiées et les explications des limites du champ d'application sont détaillées
ACTIVITE 10 **Administration d'un réseau d'entreprise et sécurisation des échanges** **A10.1.** Paramétrage d'un routeur **A10.2.** Utilisation d'un commutateur dans le cadre d'interconnexion entre plusieurs périphériques **A10.3.** Administration d'un réseau local d'entreprise avec des outils de monitoring **A10.4.** Paramétrage d'un réseau VPN (IKE, LP2P) **A10.5.** Paramétrage d'un tunnel d'échanges sécurisés entre deux serveurs en utilisant un VPN	**C10. Gérer l'articulation des réseaux de transport** en s'appuyant sur les notions d'acheminement, de commutation et de routage pour le paramétrage d'un réseau en vérifiant le bon fonctionnement d'un réseau local d'entreprise à partir d'un point de contrôle en utilisant les VPN et les solutions pour les mettre en place **afin d'interconnecter plusieurs réseaux**		**CE10.1.**L'architecture d'un réseau déjà en place est intégrée **CE10.2.**Le routeur est paramétré en fonction des contraintes définies **CE10.3.**Un commutateur est installé pour relier les différents périphériques **CE10.3.**Des tests de connectivité sont appliqués pour vérifier que les différents réseaux sont reliés **CE10.4.**Un tunnel VPN entre deux serveurs est configuré **CE10.5.**Un sniffer de réseau type Wireshark est utilisé afin de vérifier que les échanges sont chiffrés
ACTIVITE 11 **Configuration et administration des réseaux sans fil** **A11.1.** Paramétrage d'un réseau local sans fil WIFI en s'appuyant sur les standards IEEE et en prenant en compte les besoins de l'entreprise **A11.2.** Application des règles de sécurité de base sur un réseau local WIFI installé **A11.3.** Test de la connectivité du réseau local WIFI mis en place	**C11. Configurer les réseaux sans fil et mobilité** en choisissant le type de réseau sans fil approprié en s'appuyant sur les différentes typologies : WPAN, WLAN, WMAN, MRAN, Hot spot, hand over, roaming, UMTS en consultant et appliquant les référentiels des différentes technologies réseaux sans fil : IEEE 802.15, WPAN, Bluetooth, ZigBee, UWB en appliquant les principes de IEEE 802.11 (a/b/e/g/n) en réalisant une veille sur les nouvelles générations de WIFI (ac, af, ah, WiGig) en appliquant les principes de IEEE 802.22 et les futurs produits Wi-RAN en réalisant une veille sur les évolutions de l'internet ambiant: réseaux mesh, ad-hoc, réseaux de capteurs et RFID, NFC **afin de proposer des réseaux sans fil sécurisés et adaptés aux besoins de connectivité d'une entreprise**	**ME6 – (C11 - C12)** **Mise en situation professionnelle** **ME6.1.** Mise en place d'un réseau local interconnecté en utilisant l'outil Cisco Packet Tracer incluant la mise en place d'un VPN, d'un serveur Radius et d'un réseau Wifi sécurisé **ME6.2.** Etude de documents, analyse et préconisations pour la mise en place d'un réseau sécurisé hétérogène	**CE11.1.**Les standards proposés par l'IEEE 802.11 sont suivis dans le cadre d'une configuration réseau local WIFI **CE11.2.**Le réseau local WIFI est dimensionné en fonction du nombre et du type d'utilisateurs prévus **CE11.3.**Les configurations nécessaires aux bonnes pratiques en termes de sécurisation du réseau sont appliquées **CE11.4.**La connectivité est testée afin de s'assurer que le débit est suffisant pour l'ensemble des utilisateurs
ACTIVITE 12	**C12. Configurer et administrer des réseaux virtualisés** en virtualisant des serveurs		**CE12.1.**Les fonctionnements de la suite logiciel SDN et du protocole OpenFlow sont

Mise en place et administration de réseaux virtualisés **A12.1.** Administration d'une console d'administration de serveurs virtualisés (Software-Defined Networking) **A12.2.** Paramétrage d'un réseau local virtuel **A12.3.** Paramétrage des routeurs d'un réseau virtuel **A12.4.** Installation et connexion des commutateurs **A12.5.** Analyse de trame	en intégrant l'impact de cette virtualisation sur l'infrastructure en appliquant la centralisation du plan de contrôle et les fonctions d'un contrôleur en employant GNS3 en utilisant le principe de la technique d'accès: ISO 8802.3 (CSMA/CD) en s'appuyant sur les normalisations, IEEE 802 et ISO, les couches physiques, MAC et LLC, les principaux protocoles en configurant les réseaux locaux virtuels (VLAN), les réseaux locaux Ethernet (SAN, LAN, WLAN) en configurant le paramétrage de pont, commutation de niveau 3, 4 et 7 **afin de gérer des réseaux virtualisés**		identifiés et explicités avec un schéma de processus **CE12.2.**Un réseau local virtuel est paramétré en fonction des consignes d'adressage **CE12.3.**Les routeurs sont paramétrés pour interconnecter les différents réseaux **CE12.4.**Les commutateurs sont utilisés de manière appropriée **CE12.5.** Le réseau est paramétré pour utiliser l'algorithme du spanning tree **CE12.6.**Les tests de connectivités sont présentés pour s'assurer des bons paramétrages
BLOC 05 - SUPERVISER ET SECURISER LES RESEAUX ET LES ECHANGES			
ACTIVITE 13 **Surveillance des réseaux informatiques d'une entreprise et détection des potentielles menaces** **A13.1.** Analyse et manipulation des puits de logs **A13.2.** Utilisation des outils de monitoring et de visualisation **A13.3.** Administration des outils de détection d'intrusions du marché **A13.4.** Classement des menaces selon leur niveau de criticité **A13.5.** Paramétrage des règles de base des outils de détection	**C13. Superviser les réseaux informatiques d'une entreprise, les équipements d'infrastructure actifs, systèmes d'exploitation, bases de données** en déployant une infrastructure complète et une mise en sécurisation en utilisant les outils de manipulation de fichiers de logs en analysant les logs en paramétrant les outils d'analyse et de visualisation en utilisant les outils d'administration et de détection type SIEM, IDS/IPS, pare-feu en analysant le niveau d'une menace et de la classer selon le niveau de criticité **afin de détecter des anomalies ou des comportements anormaux et d'isoler les potentielles menaces**	**ME7 – (C13)** **Mise en situation professionnelle** **ME7.1.** Mise en place d'un système de surveillance reposant sur les serveurs/agents et l'utilisation d'un IAM **ME7.2.** Analyse de logs et détection des compromissions du système d'information avec proposition de remédiations	**CE13.1.**En utilisant l'interface de visualisation de Kibana et la base de données ElasticSearch, les logs critiques sont répertoriés et analysés **CE13.2.**La menace détectée au sein des logs est classée avec le niveau de criticité approprié **CE13.3.**Une nouvelle règle sur le système IPS/IDS est mise en place en fonction de la menace détectée précédemment
ACTIVITE 14 **Gestion d'une protection des systèmes d'information**	**C14. Sécuriser des réseaux et des échanges** en utilisant les outils de gestion des identités et des accès en mettant en œuvre les différentes étapes nécessaires au durcissement d'un poste LINUX et WINDOWS en appliquant les principes de base de la cryptographie	**ME8 – (C14)** **Mise en situation professionnelle** **ME8.1.**	**CE14.1.** Les règles exposées sur le cahier des charges sont prises en compte et appliquées avec logique au sein du logiciel

A14.1. Application des politiques de gestion des accès et des identités au sein d'une entreprise **A14.2.** Paramétrage du durcissement des postes utilisateurs sur les environnements LINUX et WINDOWS **A14.3.** Mise en place du chiffrement dans le cadre de la sécurisation des échanges entre serveurs **A14.4.** Mise en place du chiffrement dans le cadre d'échanges entre utilisateurs **A14.5.** Application des règles de filtrages avec les outils de firewall sur les environnements LINUX et WINDOWS A13.6. Mise en place de matériels de sécurisation	en mettant en place des règles de filtrage avec les outils appropriés selon le système d'exploitation **afin de mettre en œuvre une politique de chiffrement et de sécurité d'accès aux données au sein de l'entreprise**	Mise en place de règles de gestion des accès et identités suivant un cahier des charges **ME8.2.** Chiffrement d'une communication entre deux utilisateurs en utilisant un chiffrement asymétrique	**CE14.2.** Toutes les étapes de configuration requises sont mises en place pour un durcissement de postes LINUX et WINDOWS **CE14.3.** Les technologies de chiffrement open source appropriées sont utilisées **CE14.4.** Les clés de chiffrements sont créées avec une explication des différentes étapes **CE14.5.** Des tests entre deux postes sont effectués **CE14.6.** Un message chiffré est réceptionné, puis déchiffré **CE14.7.** Les règles de filtrage définies dans le cahier des charges sont appliquées **CE14.8.** Des tests sont appliqués pour vérifier que les règles sont effectives **CE14.9.** La hiérarchie des règles est respectée pour éviter des conflits
BLOC 06 - TESTER LA SECURITE D'UN RESEAU INFORMATIQUE AVEC LES METHODES DE HACKING			
ACTIVITE 15 **Application des mesures de sécurisation des réseaux sans fil** **A15.1.** Bypass d'une authentification sur un réseau sans fil **A15.2.** Détection des vulnérabilités pour décrypter le chiffrement sur un réseau WLAN **A15.3** Pratique d'une attaque avec l'usage de techniques avancées sur les réseaux sans fil **A15.4** Attaque d'un réseau sans fil WPA/WPA2 d'entreprise **A15.5** Attaque d'un réseau sans fil WPS d'entreprise	**C15. Attaquer un réseau sans fil** en gérant l'authentification sur un WLAN en trouvant le SSID en utilisant les filtres d'adresse MAC en utilisant le mécanisme de "Shared Key Authentication" en appliquant les techniques adéquates pour accélérer le processus de cracking du chiffrement sur un réseau WLAN en décryptant des paquets en utilisant les différents types d'attaques Deni of Service (Dos) en appliquant les attaques Evil Twin, Rogue AP. en utilisant les différents scénarios d'attaque avancée en appliquant les méthodes de MiTM, Eavesdropping, Session hijacking en mettant en place une échelle de gravité reposant sur des critères de confidentialité, intégrité, disponibilité **afin de tester la sécurité d'un réseau sans fil**	**ME9 – (C15-C16)** **Mise en situation professionnelle** **ME9.1.** Mise en place d'un réseau Wifi vulnérable, attaque d'un réseau Wifi et proposition de remédiations **ME9.2.** Attaque fictive d'un réseau sans fil WLAN Prise de contrôle fictive d'un réseau sans fil WLAN **ME9.3.**	**CE15.1.**Les routeurs sur un réseau WLAN sont détectés **CE15.2.**Les vulnérabilités sur le routeur sont identifiées **CE15.3.**L'attaque appropriée est choisie en fonction de la/les vulnérabilités identifiées **CE15.4.**Le contrôle du routeur est pris et une trace est laissée sur le serveur pour contrôler la réussite de l'intrusion **CE15.5.**Un compte-rendu détaillé est rédigé pour exposer la méthodologie utilisée et les failles détectées

A15.6 Attaque d'un réseau sans fil par désauthentification		Mise en place d'un réseau filaire vulnérable, attaque et proposition de remédiations **ME9.4.** Attaque fictive d'un réseau filaire Prise de contrôle fictive d'un réseau	
ACTIVITE 16 **Vérification périodique de la sécurisation du réseau filaire d'entreprise (blue,red et purple teams)** **A16.1.** Préparation d'une attaque avec la méthodologie d'un piratage informatique **A16.2.** Prise du contrôle d'un routeur au sein d'un réseau informatique **A16.3.** Analyse des trames et recherche des failles de protocoles	**C16. Cartographier les vulnérabilités d'un réseau d'entreprise** en appliquant la méthodologie Pentest en utilisant les outils de scanning en utilisant Metasploit en utilisant les outils tels que Wireshark afin d'effectuer du sniffing en appliquant les différentes attaques possibles sur un routeur: SSH, SNMP, SMTP, etc. en utilisant un exploit afin d'obtenir un accès machine en détectant et contournant un firewall pour porter une attaque sur une machine WINDOWS en appliquant la technique de port forwarding en utilisant le pivoting en appliquant les techniques d'élévation de privilèges **afin de recréer les conditions d'un piratage informatique**		**CE16.1.** L'inventaire des ressources de tests d'intrusion du système d'information est exact et complet **CE16.2.** Des vulnérabilités sont identifiées **CE16.3.** Des outils d'exploitation des vulnérabilités sont proposés **CE16.4.** Des scenarii d'attaques correspondant aux vulnérabilités découvertes sont proposés. **CE16.5.** L'intrusion dans le système est réussie. **CE16.6.** L'exploitation permet de démontrer l'existence des vulnérabilités **CE16.7.** Une attaque par Buffer over flow est mise en œuvre **CE16.8.** Des techniques d'attaque par Shell code sont mises en œuvre
ACTIVITE 17 **Vérification périodique de la sécurisation des postes utilisateurs** **A17.1.** Introduction dans un poste WINDOWS par l'exploitation d'un exploit ou d'une vulnérabilité **A17.2.** Maintien d'un accès sur un système corrompu **A17.3.** Suppression des traces d'un système corrompu **A17.4.** Application des techniques d'attaques avancées **A17.5.** Utilisation des techniques de Social Engineering **A17.6.** Introduction aux techniques de gestion des mises à jour et aux contremesures	**C17. Utiliser les vulnérabilités d'un réseau d'entreprise dans le cadre de l'attaque d'une machine Windows** en utilisant un exploit afin d'obtenir un accès machine en détectant et contournant un firewall pour porter une attaque sur une machine WINDOWS en appliquant la technique de port forwarding en utilisant le pivoting en appliquant les techniques d'élévation de privilèges en employant les techniques d'Anti-Virus Evasion en manipulant les techniques d'attaque sur les navigateurs en utilisant les outils et levier pour une attaque par social engineering en utilisant les méthodes de gestion de patch et de mises à jour **afin de de sécuriser les postes des utilisateurs d'un réseau d'entreprise**	**ME10 – (C17, 18, 19, 20, 21)** **Mise en situation professionnelle** **ME10.1.** Utilisation d'outils de tests d'intrusion pour détecter les failles réseaux et systèmes **ME10.2.** Cartographie de l'ensemble des vulnérabilités découvertes sur un réseau et proposition de remédiation **ME10.3.**	**CE17.1.** Des scenarii d'attaques correspondant aux vulnérabilités découvertes précédemment établis sont exploités. **CE17.2.** Les vulnérabilités découvertes sont analysées. **CE17.3.** La criticité des vulnérabilités découvertes est priorisée.

ACTIVITE 18 **Sécurisation des serveurs et applications web de l'entreprise** **A18.1.** Cartographie des services et leurs vulnérabilités lors d'une phase de reconnaissance d'une cible à attaquer **A18.2.** Introduction dans un serveur Web **A18.3.** Corruption des protocoles d'échanges sécurisés **A18.4.** Exploitation des failles de CMS **A18.5.** Utilisation avancée des outils NMAP, BURPSUITE, WIRESHARK, BETTERCAP	**C18. Utiliser les vulnérabilités d'un réseau d'entreprise dans le cadre d'attaques avancées** en utilisant les outils et techniques avancées tels que Metasploit Loader, DLL Hijacking, DLL Main, Shell Code Exec, etc. en s'appuyant sur les standards OWASP en utilisant les différents outils de scanning proxy et Nessus en utilisant les failles RFI & LFI en utilisant les failles Upload en effectuant du Cross Site Scripting et du Cross Site Request Forgery en utilisant les techniques de SQL Injection, Clickjacking, Injection HTML, Injection de commandes, etc. en paramétrant une Exploitation Server Side et Client Side (MiTM, Social Engineering) **afin de garantir la sécurisation des applications web de l'entreprise**	Explication et utilisation des techniques de hacking pour améliorer la résilience du système d'information **ME10.4.** Etude des référentiels de sécurisation d'un système d'information (famille ISO27000-Nist800-53 ; RGPD)	**CE18.1.** Une attaque par Buffer over flow est mise en œuvre **CE18.2.** Des techniques d'attaque par Shell code sont mises en œuvre **CE18.3.** Un rapport écrit confirme l'existence de menaces
ACTIVITE 19 **Recherche et évaluation de la surface d'attaque** **A19.1.** Cartographie des services et vulnérabilités associées **A19.2.** Interprétation des résultats et recherche des attaques possibles **A19.3.** Analyse des trames et recherche des failles de protocoles	**C19. Utiliser les vulnérabilités Web dans le cadre de la phase de reconnaissance de serveurs** en s'appuyant sur les standards OWASP en utilisant les différents outils de scanning proxy et Nessus **afin de repérer les failles existantes et de les corriger**		**CE19.1.**La cartographie d'un site internet est réalisée **CE19.2.**Une reconnaissance de serveur est effectuée en exploitant le standard OWASPCE18.3 **CE19.3.**Des remédiations sont mises en place
ACTIVITE 20 **Sécurisation des échanges** **A20.1.** Vérification de la mise en place des cookies **A20.2.** Sécurisation des formulaires d'authentification **A20.3.** Schématisation de l'architecture logique d'un serveur web	**C20. Utiliser les vulnérabilités Web dans le cadre d'attaques sur authentification** en utilisant les techniques de Hijacking, Brute Force et attaque sur les protocoles sécurisés en utilisant les techniques d'injection SQL et d'utilisation de formulaires non sécurisés **afin de vérifier le respect des politiques et procédures de gestion des accès.**		**CE20.1.**Des techniques d'ingénierie sociale sont mises en œuvre **CE20.2.**Une attaque par phishing est mise en œuvre **CE20.3.**La récolte d'informations permet l'utilisation d'une technique de vol de session

ACTIVITE 21 **Gestion des données** **A21.1.**Analyse de l'architecture de CMS **A21.2.**Identification et exploitation de failles possibles	**C21. Utiliser les vulnérabilités Web dans le cadre d'attaques sur CMS** en utilisant les techniques d'attaque sur les principaux CMS tels que WordPress, Joomla, Drupal **afin de protéger l'entreprise de la fuite de données personnelles ou sensibles**		**CE21.1.**Un scan de la cible est effectué **CE21.2.**Une prise de contrôle du serveur Web est effectuée en utilisant un exploit référencé **CE21.3.**Une élévation de privilèges est appliquée **CE21.4.**La méthodologie utilisée et les failles détectées lors de la reconnaissance sont exposées dans un compte-rendu détaillé