BLOC	COMPÉTENCES GLOBALES	SOUS COMPÉTENCES	Semestre	Num SEQ	Durée	SEQUENCE	Description de la séquence	SEANCES	SAVOIRS	FICHES Savoirs/Techno	Ressources externes	VM/Outils
BLOC 3 - Cybersécurité des services informatiques	B3.5 A - Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service (option A)	- Participer à la vérification des éléments contribuant à la sûreté d'une infrastructure informatique - Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure - Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité - Prévenir les attaques - Détecter les actions malveillantes - Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures	1	3.5 AR	8	Sécurisation de l'infrastructure réseau d'une entreprise cliente : Université Ouest	Votre mission consiste, au sein du pôle cybersécurité de l'ESN "IT Services", à participer aux activités de support, d'audit et de sécurisation de l'infrastructure réseau d'une entreprise cliente : « l'Université Ouest » afin de l'aider à prévenir les menaces en déployant les outils et les dispositifs de sécurité adaptés. Vous étudierez les règles de filtrage déjà mises en place sur l'infrastructure réseau de l'université Ouest puis en proposant de nouvelles règles pertinentes par rapport aux nouveaux services hébergés par l'université. Vous mettrez en œuvre et testerez ces règles sur un prototype de l'infrastructure cible.	À partir d'un dossier type étude de cas et de le prototype de simulation de l'infrastructure réseau : 1 - Etudier les règles de filtrage déjà mises en place et identifier les trames/paquets qui seront acceptés ou bloqués à partir d'une liste qui vous est fournie 2 - Proposer des règles de filtrage pertinentes par rapport aux nouveaux services hébergés par l'entreprise 3 - Modifier le prototype fournie pour mettre en oeuvre ces règles 4 - Proposer un plan de test et l'effectuer afin de vérifier que les règles sont bien effectives sur le prototype	Outils de sécurité : prévention et détection des attaques, gestion d'incidents. Cybersécurité : bonnes pratiques, normes et standards.	Contexte : Université Ouest Fiche savoirs Filtrage & ports courants Fiche techno Iptables/Labtainer Avertissement "piratage éthique"	Etude de cas NELL, Ruchenord, Hopital Sud, DMAT…	Maquette virtuelle Labtainer labs nmap, tcpdump, iptables
			1	3.5 BR	12	Sécurisation de l'infrastructure système pour l'entreprise cliente de 2.1AR (TiersLieux ou Cub)	Votre mission consiste, au sein du pôle cybersécurité d'IT Services, à participer aux activités d'audit et de sécurisation de l'infrastructure système de l'entreprise cliente TiersLieux. Il s'agit de prévenir les menaces externes et internes en déployant les outils et les dispositifs de sécurité adaptés. Vous commencerez par proposer des règles d'audit des comptes et des habilitations pertinentes par rapport au contexte étudié. Vous poursuivrez en mettant en œuvre des règles de sécurité centralisées (GPO) sur les postes de travail déployées au niveau du domaine.	À partir d'un dossier type étude de cas, 1 - Proposer des règles d'audit des comptes et des habilitations pertinentes par rapport à l'annuaire de l'entreprise 2 - Mettre en oeuvre ces règles sur l'infrastructure virtuelle simulant les services audités 3 - Proposer un scénario de test et l'effectuer afin de vérifier que les audits mis en place sont actifs en cas de tentative d'usurpation d'identité 4 - Mettre en oeuvre des règles de sécurité centralisées (GPO) sur les postes de travail : limiter l'accès d'un poste à un utilisateur, limiter les droits sur le poste 5 - Proposer un scénario de test et l'effectuer afin de vérifier que les GPO mises en place sont actives	Outils de sécurité : prévention et détection des attaques, gestion d'incidents. Cybersécurité : bonnes pratiques, normes et standards. Etude d'une solution de sécurisation des postes de travail au moyen de GPO	Contexte : TiersLieux ou Cub Fiche savoirs/techno 1ère année: Fiche Windows Server, GPO Fiche Windows Server Avancée Fiche Windows Server Audit Fiche Windows Server GPO Avancée Fiche CEJMA contraintes du RGPD dans la gestion des accès aux journaux Fiche CEJMA Responsabilité civile et pénale de l'administrateur	Vidéos Windows ENI Contexte : TiersLieux ou Cub	VM Windows server et client, serveur web
			1	3.5 CR	12	Sécurisation de l'infrastructure réseau et Wifi multi-vlan d'une entreprise cliente : mise en place de l'authentification par serveur radius sur le Lan et sur le Wifi (TiersLieux ou	Votre mission, au sein du pôle cybersécurité d'IT Services, consiste à mettre en place et sécuriser l'infrastructure réseau et Wifi multi-vlan de l'entreprise cliente TiersLieux. Vous mettrez en place l'authentification par serveur radius sur le Lan et sur le Wifi sur un prototype.	À partir de le prototype de l'infrastructure réseau filaire et Wifi de l'entrprise cliente 1 - Analyser les flux wifi capturés, réaliser des tests de "hacking" de la solution wifi mise en place (WEP puis WPA) 2 - Modifier le prototype de l'infrastructure réseau filaire et Wifi, pour mettre en oeuvre l'authentification radius pour les connexions filaires et sans fil 3 - Proposer un scénario de test et l'effectuer afin de vérifier la communication entre les différents équipements réseau, les postes de travail et les serveurs	Technologies et équipements de la sécurité informatique des infrastructures réseau, systèmes et services. Etude d'une solution Radius	Fiche savoirs radius Fiche techno Wifi sécurisé	Cisco activités CCNA v7 RSW	VM Security Onion
			1	3.5 DR	24	Prévention des attaques et analyse des incidents de sécurité par la mise en oeuvre de quelques attaques typiques (MITM, Déni de service HTTP, ARP Spoofing, exploit FTP root…)	Afin de participer aux activités d'audit et de sécurisation des infrastructures réseau de ses clients, le chef de projet du pôle cybersécurité d'IT Services, vous demande de mettre en place un prototype d'infrastructure virtuelle qui servira à vous former aux attaques et vulnérabilités courantes ainsi qu'aux tests d'intrusions. Vous simuler une attaque de l'homme du milieu sur un service SSH afin de pointer différentes vulnérabilités et proposer des contre-mesures. Vous mettrez en oeuvre l'attaque de services vulnérables, constaterez les exploits, proposerez des contre-mesures et le cas échéant, utiliserez un parefeu IPS pour les bloquer.	À partir d'une infrastructure virtuelle fournie comportant un client, un serveur, un attaquant, une machine d'analyse, une machine vulnérable, un routeur Séance 1 - Implanter le prototype sur votre infrastructure virtuelle Séance 2 - Simuler une attaque de l'homme du milieu sur un service SSH afin de pointer différentes vulnérabilités et proposer des contre-mesures. Séance 3 - Mettre en oeuvre l'attaque d'un service sur la machine vulnérable (Metasploitable, ex FTP), constater l'exploit et utiliser un parefeu IPS pour la bloquer Séance 4 - Mettre en oeuvre l'attaque d'un service DHCP sur une machine vulnérable, constater l'exploit et mettre en œuvre des contre-mesures	Outils de sécurité : prévention et détection des attaques, gestion d'incidents. Cybersécurité : bonnes pratiques, normes et standards. Etude d'une solution de sécurisation des postes de travail au moyen de parefeux IDS, IPS	Fiche savoirs/techno 1ère année: Menaces, les types d'attaque et de vulnérabilité Cryptographie, protocoles sécurisés (SSH) Analyse de trames Fiche savoirs IDS/IPS Fiche Techno Labcerta MITM Fiche Techno Labcerta attaque DHCP (en cours) Fiche CEJMA - Contraintes du RGPD dans la gestion des accès aux journaux Fiche CEJMA - Les risques des cyberattaques pour l'organisation Fiche CEJMA - Réglementation en matière de lutte contre la fraude informatique Fiche CEJMA - Les organisations de lutte contre la cybercriminalité	Diaporamas Cisco Cyber Operations Cisco Cyber Operations TP Certa MITM https://www.reseaucerta.org/labo-mitm-ssh Certa attaque DHCP (à venir)	VM MITM + Stormshield et / ou Labtainer
			1	3.5 ER	4	Sécurisation d'un service web (suite séquence Bloc2 B2.2.2)	Votre mission, au sein du pôle cybersécurité d'IT Services, consiste à participer aux activités de sécurisation l'infrastructure réseau d'une entreprise cliente afin de sécuriser son service web en mettant en œuvre des certificats.	À partir de l'étude de l'infrastructure informatique d'une entreprise cliente et du serveur web (machine virtuelle Linux LAMP installée et configurée) mis en place en 2.2.2 1 - Implanter le prototype sur votre infrastructure virtuelle 2 - Vérifier que votre serveur web est accessible par un hôte du réseau interne 3 - Mettre en oeuvre l'accès sécurisé à l'application Web à l'aide de certificats	Cybersécurité : bonnes pratiques, normes et standards. Etude d'une solution de sécurisation d'un serveur web	Fiche savoirs (Bloc2) principes d'architecture d'un service web (client-serveur, protocoles HTTP...) Fiche techno (Bloc2) Serveur web LAMP Fiche techno Sécurisation d'un serveur web Apache (certificats)	https://www.reseaucerta.org/content/service-web-securise	VM Linux LAMP installée et configurée cf bloc2 2.2.2

BLOC	COMPÉTENCES GLOBALES	SOUS COMPÉTENCES	Semestre	Num SEQ	Durée	SEQUENCE	Description de la séquence	SEANCES	SAVOIRS	FICHES Savoirs/Techno	Ressources externes	VM/Outils
BLOC 3 - Cybersécurité des services informatiques	**B3.5 A - Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service (option A)**	- Participer à la vérification des éléments contribuant à la sûreté d'une infrastructure informatique - Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure - Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité - Prévenir les attaques - Détecter les actions malveillantes - Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures	**2**	3.5 FR	**12**	Mise en place d'une solution de centralisation et d'analyse de logs pour un espace de coworking et d'accueil de startup (TiersLieux ou Cub) - Suite séquence B2.3 ER	Votre mission, au sein du pôle cybersécurité d'IT Services, consiste à vous familiariser avec une solution de centralisation des journaux d'équipements et de serveurs. Vous devrez configurer une machine virtuelle d'analyse afin qu'elle accède aux fichiers de logs fournis que vous mettrez sous un format homogène et importerez dans la solution de centralisation. Vous apprendrez également à configurer l'accès aux fichiers de logs de vos serveurs et de vos équipements réseau le cas échéant depuis la machine d'analyse. Vous réaliserez ensuite le scénario de test proposé et définirez des filtres afin d'analyser les événements apparus dans les journaux fournis.	À partir de la plateforme virtuelle mise en place en 2.1 BR comportant une solution de centralisation des logs des équipements et des serveurs, et d'une machine virtuelle d'analyse 1 - Configurer la machine virtuelle d'analyse afin qu'elle accède aux fichiers de logs centralisés 2 - Réaliser le scénario de test proposé et définir des filtres afin d'analyser les événements apparus dans les journaux	Outils de sécurité : prévention et détection des attaques, gestion d'incidents. Cybersécurité : bonnes pratiques, normes et standards. Etude d'une solution de sécurisation des postes de travail au moyen de parefeux IDS, IPS	Fiche techno Centralisation des Logs - Bloc 2 (GG) Fiche techno Expressions régulières (GG/VM) Fiche techno Exploitation des Logs - Bloc 3 (GG) Fiche CEJMA contraintes du RGPD dans la gestion des accès aux journaux (GG) Fiche CEJMA Responsabilité administrateur (GG)	Diaporamas Cisco Cyber Operations Cisco Cyber Operations TP	VM Security Onion
			2	3.5 GR	**12**	Sécurisation des flux d'une entreprise cliente : filtrage protocolaire, filtrage d'URL, proxy SSL…	Votre mission, au sein du pôle cybersécurité d'IT Services, consiste à participer aux activités de sécurisation des flux externes d'une entreprise cliente. Vous serez chargé de proposer des règles de filtrage protocolaire, de filtrage d'URL, de redirection de ports pertinentes par rapport aux demandes émises par l'entreprise et de les mettre en œuvre sur un prototype comportant un pare-feu SNS Stormshield.	À partir d'un dossier type étude de cas et d'une infrastructure virtuelle fournie comportant un client, un serveur, un attaquant, un pare-feu 1 - Implanter le prototype sur votre infrastructure virtuelle 2 - Proposer des règles de filtrage d'URL, de redirection de ports, de proxy SLL pertinentes par rapport aux demandes émises par l'entreprise 3 - Modifier la configuration du pare-feu pour mettre en oeuvre ces règles 4 - Proposer un plan de test et l'effectuer afin de vérifier que les règles sont bien effectives sur le prototype virtuel	Outils de sécurité : prévention et détection des attaques, gestion d'incidents. Cybersécurité : bonnes pratiques, normes et standards. Etude d'une solution de sécurisation des postes de travail au moyen de parefeux IDS, IPS	Fiches 1 à 6 certa Stormshield (routage, filtrage, filtrage protocolaire, filtrage d'URL, proxy SSL…)	Fiches 1 à 6 certa Stormshield Lab 7 Stormshield CSNE Proxy SSL	VM Stormshield
			2	3.5 HR	**12**	Mise en place d'une interconnexion sécurisée des infrastructures de deux sites (Université de Nantes). Prototypage d'un VPN Site-à-Site et d'un VPN d'accès nomade	Votre mission, au sein du pôle cybersécurité d'ITS 86, consiste à mettre en place une interconnexion sécurisée des infrastructures de deux sites distants (FuzLan) à l'aide d'un VPN Site-à-Site et d'un VPN d'accès nomade.	À partir de l'étude de l'infrastructure informatique, système et réseau de l'entreprises cliente (Université de Nantes), mettre en place une interconnexion sécurisée entre deux sites : 1 - Réaliser le prototype virtuel de l'interconnexion des deux infrastructures réseau par un VPN site-à-site IPSec et nomade avec PSK 2 - Effectuer des tests afin de vérifier la communication entre les différents équipements réseau, les postes de travail et les serveurs 3 -. Etudier la mise en place d'une PKI pour la gestion du VPN avec certificats 4 - Modifier le prototype virtuel de l'interconnexion des deux infrastructures réseau par un VPN site-à-site IPSec avec certificats 5 - Effectuer des tests afin de vérifier la communication entre les différents équipements réseau, les postes de travail et les serveurs.	Technologies et équipements de la sécurité informatique des infrastructures réseau, systèmes et services. Etude d'une solution VPN site-à-site et nomade.	Fiches 7 à 8 certa Stormshield = VPN Site-à-Site IpSec, VPN d'accès nomade Fiche savoir Certificats et PKI	étude de cas DMAT, CUB, GSB, Université Ouest Lab 8 Stormshield CSNA VPN IPSec Site-à-Site	VM Stormshield
Total heures SISR					**96**							