DATAPROTECT
Security is our commitment

Bloc	Contenu	
Header	**Titre de la filière**	Pentester Junior Ss
	Logo de l'opérateur de formation	DATAPROTECT Security is our commitment
	Sous – titre	Deviens Pentester Junior en 6 mois
	Durée	6 mois
	Lieu de formation	DATAPROTECT - Casanearshore
	Prochaine session	Mars 2024
	Prérequis	• Être titulaire au minimum d'un Bac+2 en informatique • Être prédisposé et engagé à se reconvertir vers un métier de la cybersécurité
Débouchés : les postes que vous pourrez occuper après cette formation	Ce parcours de formation ouvre la porte à un métier dynamique et essentiel dans le monde de la Cybersécurité. En tant que pentester, vous serez chargé de contrôler et d'assurer la sécurité des réseaux et systèmes. Votre rôle consistera à identifier les vulnérabilités en menant des tests d'intrusion et à proposer des solutions pour les corriger. Cette formation vous prépare à devenir un professionnel indispensable dans la lutte contre les cyberattaques, vous offrant des compétences techniques pointues et une compréhension profonde des stratégies de défense en cybersécurité. En tant que pentester, vous aurez l'opportunité de travailler dans divers secteurs, contribuant activement à la sécurité et à la résilience des organisations face aux menaces numériques.	
Pourquoi devenir Pentester Junior en 2023 ?	Devenir un testeur d'intrusions en cybersécurité présente de nombreux avantages, surtout à l'heure où la sécurité numérique devient de plus en plus cruciale dans tous les secteurs.	

	Demande Croissante : Avec l'augmentation constante des cyberattaques, la demande pour des professionnels qualifiés en cybersécurité, notamment des pentesters, est en hausse. Les entreprises de toutes tailles cherchent activement des experts capables de détecter et de prévenir les failles de sécurité. **Rôle Essentiel dans la Cybersécurité :** En tant que pentester, vous jouez un rôle crucial en testant proactivement les systèmes de sécurité des organisations, en identifiant les vulnérabilités avant que les pirates ne le fassent. **Défis Stimulants et Variés :** Le travail de pentester est dynamique et en constante évolution. Vous serez confronté à des défis techniques variés et stimulants, ce qui rend ce métier passionnant et gratifiant. **Opportunités de Carrière Diversifiées :** Les compétences d'un pentester sont précieuses dans de nombreux secteurs, offrant une grande variété de possibilités d'emploi et de spécialisations. **Rémunération Attractive :** En raison de leur expertise spécialisée et de la demande croissante, les pentesters bénéficient souvent de salaires compétitifs et d'avantages intéressants. En résumé, devenir pentester est une opportunité de carrière exceptionnelle pour ceux qui sont passionnés par la résolution de problèmes, la technologie et la cybersécurité, et qui cherchent une profession à la fois stimulante, gratifiante et cruciale pour la sécurité numérique.
Compétences : ce que vous allez apprendre	▪ Maîtrise de divers systèmes d'exploitation et de leur fonctionnement interne. ▪ Compréhension des réseaux informatiques, y compris TCP/IP, et des protocoles de communication. ▪ Programmation et scripting ▪ Connaissance des vulnérabilités web courantes et des techniques d'exploitation. ▪ Capacité à utiliser et à comprendre des outils d'analyse de vulnérabilités et à interpréter leurs résultats.

	▪ Compréhension des principes de base de la cryptographie et de son application dans la sécurité des données. ▪ conduite de tests d'intrusion manuels et automatisés, ainsi que l'utilisation d'outils spécialisés. ▪ Capacité à détecter, analyser et exploiter les vulnérabilités des systèmes et des applications.
Programme de la formation	**Tronc Commun : (8 Semaines de formation et travaux pratiques)** 1. Comprendre et mettre en œuvre un réseau informatique 2. Appréhender Windows Server 3. Gérer et administrer un Système Linux 4. Méthodes et techniques de la gestion de projets 5. Conformité aux normes de cybersécurité et aux exigences règlementaires (DNSSI, Loi 09-08, ISO27001) 6. Gestion de risques 7. Introduction à la Cryptographie 8. Introduction à la programmation Python 9. Introduction aux métiers de la Cybersécurité **Spécialisation en Pentest (8 semaines de formation et Labs)** 1. Introduction au Hacking Éthique 2. Mettre en œuvre une reconnaissance active et passive 3. Déployer un Scan de vulnérabilités 4. Précéder à une contre-mesure et défense 5. Techniques d'évasion et de contournement 6. Identifier et exploiter les vulnérabilités 7. Compromettre l'active Directory 8. Réussir une Post-exploitation **Pratique intensive et professionnalisation (8 Semaines)** **Soft Skills et préparation professionnelle (En continu)** 1. Personal Branding 2. Techniques de communication en entretien d'embauche 3. Intelligence relationnelle en milieu professionnel

Notre méthode	En tant que bras éducatif de DATAPROTECT, nous tirons parti d'une connaissance terrain profonde et d'un retour d'expérience inégalé. Cette immersion directe dans le domaine nous offre une perspective unique, nous permettant d'anticiper les besoins réels des entreprises et de former nos participants en conséquence. Notre méthode de formation place les participants dans un environnement professionnel réel tout au long du parcours en mode Learning By doing.
À quoi s'attendre pendant le Bootcamp ?	**Acquisition de Connaissances :** ▪ Les participants vont acquérir des connaissances fondamentales en cybersécurité, spécifiquement centrées sur le rôle et les responsabilités d'un testeur de pénétration. Ils apprendront les dernières techniques et méthodologies en matière de tests d'intrusion. **Acquisition de Compétences Pratiques :** ▪ Le bootcamp met l'accent sur la pratique concrète. À travers des séances en laboratoire et des simulations réalistes, les participants mettront en œuvre des scénarios de tests d'intrusion. Cela leur permettra de développer des compétences opérationnelles, telles que l'identification des vulnérabilités, l'utilisation d'outils de test d'intrusion, et la mise en œuvre de techniques d'exploitation. **Professionnalisation par Projets Réels :** ▪ Les participants travailleront sur des projets réels pour acquérir une expérience concrète. ▪ Ces projets offrent une opportunité d'appliquer les compétences apprises dans un contexte professionnel, en abordant des problèmes réels de cybersécurité. **Encadrement par des Experts du métier :** ▪ Des professionnels expérimentés avec une solide expérience terrain fourniront des conseils et partageront leurs connaissances pratiques.

	Encadrement Individualisé et travaux de groupes : ▪ Chaque participant bénéficiera d'un suivi personnalisé pour garantir une progression adaptée à ses besoins et objectifs. ▪ Les participants seront encouragés à collaborer en petits groupes, favorisant l'apprentissage par les pairs et le développement de compétences en travail d'équipe. ▪ Ces sessions renforcent la résolution de problèmes collaboratifs et la communication efficace. **Outils de Pratique Avancés :** ▪ Le programme offre l'accès à des outils de cybersécurité de pointe et des plateformes de simulation pour une expérience d'apprentissage enrichissante. **Préparation à une Certification Internationale (Optionnelle) :** ▪ À la demande, une préparation spécifique pour une certification reconnue internationalement en cybersécurité peut être intégrée. ▪ Cette option ajoute une valeur significative à la formation, en offrant une reconnaissance professionnelle et en ouvrant des portes sur le marché de l'emploi. Ce Bootcamp offre une expérience d'apprentissage complète et immersive, préparant les participants à devenir des testeurs de d'intrusions juniors compétents, équipés des connaissances, des compétences pratiques, et de l'expérience nécessaire pour réussir dans le domaine de la cybersécurité.
Présentation de l'operateur	Depuis notre création en 2009, DATAPROTECT s'est imposé comme un leader incontesté dans l'écosystème de la cybersécurité, en démontrant un engagement sans faille à offrir une expertise pointue et un accompagnement 360° au profit de plus de 500 clients actifs sur 3 continents, y compris une centaine de banques. Notre approche personnalisée prend en compte les particularités de chaque client, enrichissant notre vaste bibliothèque de use-cases et renforçant notre expertise déjà solide. Notre équipe, composée de plus de 150 consultants Full Security, opère pour renforcer la sécurité des systèmes d'information de nos clients, les

	assister dans leur conformité aux normes réglementaires, et protéger leurs données sensibles et leur image de marque. Grace à notre expérience, nous avons développé le Cybersecurity Skills Lab qui se présente comme une solution chirurgicale à la problématique de la pénurie des ressources, à travers des solutions disruptives incluant des programmes UPSKILL de montée en compétences spécialisées, des certifications reconnues à l'international et des parcours RESKILL de reconversion vers les métiers d'avenir dans le domaine de la cybersécurité. Grace à une infrastructure immersive nos apprenants sont placés dans un Bootcamp de Learning By Doing permettant une professionnalisation opérationnelle rapide et efficace.
Candidature	**Pré-requis :** • Disposer au minimum d'un Bac+2 en informatique **Critères de sélection** • Étude de dossier • Motivation du participants **Candidature :** • Inscription en ligne sur la plateforme JobInTech • Présélection • Test de positionnement & Entretien • Validation et inscription au programme