[10289146] ORM performance tuning

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe du BuildCenter en tant que stagiaire. Cette équipe a pour mission :

- de construire et de déployer des solutions de sécurité pour les réseaux,
- de développer et industrialiser des produits permettant l'administration et la supervision de la sécurité des réseaux.

Vous serez en charge d'analyser la partie ORM (Object-Relational Mapping) d'une solution existante afin d'en optimiser les performances. Cela pourra passer à la fois par l'utilisation de cache, que par la gestion du pool de connexions ou encore des mappings objet-relationnel.

2. Déroulement et objectifs du stage

Le stage se déroulera en plusieurs phases :

1. Analyse de la solution actuelle et mise en place de benchmarks afin de mettre en évidence les parties à améliorer.
2. Etude des bonnes pratiques de l'ORM et proposition d'améliorations
3. Implémentation des solutions

L'ajout de tests à une suite de benchmarks existante sera demandé afin de visualiser l'amélioration des performances sur les parties de la solution travaillées.
Les propositions d'améliorations seront soutenues sans oublier les différents impacts possibles (cpu, ram, I/O disk).
L'implémentation de la solution sera effectuée dans le respect des bonnes pratiques de développement du BuildCenter.

Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement. Vous obtiendrez de fortes connaissances en ORM et base de données, véritable atout si vous souhaitez continuer dans le développement logiciel.

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Une bonne de connaissance de Java et SQL
- Une connaissance d'Hibernate ou de JPA est un plus.
- Un esprit de synthèse et d'excellentes capacités rédactionnelles sont attendus.
- Anglais écrit requis.

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 6 mois
- à partir de Janvier 2016
- à Elancourt (78)

[10289149] Développement Framework Tests

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrerez l'équipe du BuildCenter en tant que stagiaire. Cette équipe a pour mission de construire et de déployer :

- des solutions de sécurité pour des réseaux
- des moyens de supervision de sécurité de réseaux.

Suite à des problématiques d'efficacité dans la rédaction des tests pour du code C, l'équipe Build Center a démarré le développement d'un Framework de tests, écrit en python.

Vous serez en charge de reprendre ce framework et d'effectuer des développements de fonctionnalités innovantes et de rédiger la documentation associée.

2. Déroulement et objectifs du stage

Le stage se déroulera en plusieurs phases :

1. Faire un état de l'art des Frameworks et outils de test
2. Mettre en place les fonctionnalités manquantes
3. Faire une analyse avec un expert en test sur des innovations pouvant être réalisées
4. Faire une documentation complète sur le Framework

Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Excellente maîtrise des langages Python et C
- Bonne connaissance des processus de validation
- Un esprit de synthèse et d'excellentes capacités rédactionnelles sont attendus.
- Anglais écrit requis.

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 6 mois
- à partir de Janvier 2016
- à Elancourt (78)

[10289152] Développement Interpréteur Bash

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrerez l'équipe du BuildCenter en tant que stagiaire. Cette équipe a pour mission de construire et de déployer :

- des solutions de sécurité pour des réseaux
- des moyens de supervision de sécurité de réseaux.

Le script bash représente une grande partie des scripts systèmes. Toutefois, en termes de qualité, il existe peu d'outils ou de frameworks de test, ce qui pose de réels problèmes pour les équipes d'intégration et de validation.

L'objectif du stage est de réaliser un interpréteur de script bash, permettant de simuler un environnement d'exécution. Il serait ainsi possible de vérifier complètement le comportement des scripts.

Vous serez en charge de définir la solution à mettre en place, d'effectuer les développements et de rédiger la documentation associée.

2. Déroulement et objectifs du stage

Le stage se déroulera en plusieurs phases :

1. Faire un état de l'art sur les interpréteurs et sur le parsing de scripts bash
2. Définir les limites de la sandbox
3. Développement/Validation de l'interpréteur
4. Rédaction de la documentation

Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Excellente maîtrise des langages Bash et Python
- Bonne connaissance des processus de validation
- Un esprit de synthèse et d'excellentes capacités rédactionnelles sont attendus.
- Anglais écrit requis.

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 6 mois
- à partir de Janvier 2016
- à Elancourt (78)

[10289154] Visualisation graphique 2D/3D de données de sécurité informatique

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe du Build Center en tant que stagiaire. Cette équipe a pour mission :

- de construire et de déployer des solutions de sécurité pour les réseaux,
- de développer et industrialiser des produits permettant l'administration et la supervision de la sécurité des réseaux.

Le produit de supervision, développé par le Build Center, manipule en temps réel des données de nature diverse sur l'état de sécurité de réseaux informatiques. Ces données sont servies par un serveur REST et présentées par le biais d'une interface WEB.
L'objectif de ce stage est d'explorer des présentations 2D de ces données, dans le but améliorer l'expérience de l'opérateur. Il s'agit d'essayer et d'implémenter en JavaScript des visualisations (graphes, cartes, plans…) plus interactives, plus agréables, de meilleure ergonomie. Pour le besoin de démonstrateurs, les représentations 3D seront aussi envisagées.
Le volume important des données est un des enjeux du stage.
Les représentations les plus prometteuses seront enfin capitalisées à travers une bibliothèque JavaScript transverse utilisée pour tous les développements futurs du Build Center. L'implémentation sera réalisée avec un niveau de qualité élevé. Les pratiques d'intégration continue et TDDs seront appliquées.

2. Déroulement et objectifs du stage

Le stage se déroulera en plusieurs phases :

1. Etat de l'art sur les types de représentations 2D/3D et des bibliothèques JavaScript (d3.js, dc.js, three.js, cubism.js…)
2. Comparaison avec du code JavaScript existant déjà développé dans certains de nos projets
3. Prise en main de l'outil de supervision et étude de ses données de sécurité. Réflexion sur les représentations les plus adaptées.
4. Implémentation et expérimentations de plusieurs représentations sur données réelles. La première représentation montrera la topologie du réseau, enrichie par des informations concernant les incidents de sécurité.
5. Capitalisation sous forme de bibliothèque de visualisation 2D/3D dédiée à la sécurité

Durant ce stage vous serez formé aux pratiques de développement de code de qualité industriel. Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Bonne connaissance de technologies d'afficheurs Web (HTML, CSS, JavaScript, REST)
- Goût pour l'expérimentation et intérêt pour les considérations esthétiques
- Culture de représentations de données et du domaine la sécurité recommandée
- Connaissance des pratiques de tests (BDD/TDD) encouragée
- Un esprit de synthèse et d'excellentes capacités rédactionnelles sont attendus.
- Anglais écrit requis

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 6 mois
- à partir de septembre 2015
- à Elancourt (78)

[10289932] Etat de l'art des produits réseaux

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe du Build Center en tant que stagiaire. Cette équipe a pour mission de définir, de mettre en œuvre, déployer et de supporter :

- Des infrastructures de réseaux sécurisés (chiffrement, disponibilité, intégrité)
- Des passerelles d'interconnexion entre plusieurs réseaux de niveau de sensibilités différentes (filtrage, détection, blocage, journalisation)

Cette activité met en œuvre plusieurs équipements matériels, de nature différente, de constructeurs différents selon la clientèle à adresser : gouvernemental, export, privé, etc…
Compte tenu de ce grand panel de matériel permettant d'élaborer ces systèmes, vous serez en charge de constituer un référentiel de base permettant d'améliorer les choix dans la constitution de ces solutions.

2. Déroulement et objectifs du stage

Le stage se déroulera en plusieurs phases :

1. Faire un état de l'art des solutions techniques actuelles sur les switches, routeurs, parefeux et chiffreurs
2. Réaliser des fiches de synthèse comparative entre les produits par famille
3. Réaliser des mises en œuvre des produits pare-feu, chiffreurs dans un environnement virtualisé ou réel si possible.

Les livrables attendus seront :

1. Un mini catalogue réaliste et objectif des produits et technologie
2. Une architecture représentative d'une maquette permettant d'évaluer les fonctions de sécurité
3. Une documentation précise sur la mise en œuvre de l'architecture et le plan de test associé.

Ce stage vous permettra d'illustrer vos connaissances avec la mise en application dans des cas concrets. Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Excellente connaissance du monde IP, routage, cloisonnement,
- Bonne maîtrise des dispositifs de sécurité applicables aux réseaux
- Un esprit de synthèse et d'excellentes capacités rédactionnelles sont attendus.
- Anglais écrit requis.

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 6 mois
- à partir de Janvier 2016
- à Elancourt (78)

[10289935] Optimisation de configuration de passerelle

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe du Build Center en tant que stagiaire. Cette équipe a pour mission de définir, de mettre en œuvre, déployer et de supporter :

- Des infrastructures de réseaux sécurisés (chiffrement, disponibilité, intégrité)
- Des passerelles d'interconnexion entre plusieurs réseaux de niveau de sensibilités différentes (filtrage, détection, blocage, journalisation)

Cette activité met en œuvre plusieurs équipements matériels, de nature différente, de constructeurs différents selon la clientèle à adresser : gouvernemental, export, privé, etc…
Compte tenu de ce grand panel de matériel permettant d'élaborer ces systèmes, vous serez en charge de constituer un outil permettant l'optimisation des règles de configuration

2. Déroulement et objectifs du stage

Le stage se déroulera en plusieurs phases :

1. Bâtir une architecture de type passerelle avec à minima un switch, un routeur et un pare-feu
2. Définir l'infrastructure du centre gestion associé, et définir des modèles de configuration de référence
3. Identifier les moyens d'analyse et d'application de configuration

Les livrables attendus seront :

1. Une maquette répondant au besoin d'interconnexion entre les réseaux
2. Un outil à base de langage de script permettant d'optimiser la configuration de la passerelle en adressant les différents composants du réseau
3. Une documentation précise sur la mise en œuvre de l'architecture et le plan de test associé.

Ce stage vous permettra d'illustrer vos connaissances avec la mise en application dans des cas concrets. Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Excellente connaissance du monde IP, routage, cloisonnement,
- Bonne maîtrise d'environnement linux et langage de scripting
- Un esprit de synthèse et d'excellentes capacités rédactionnelles sont attendus.
- Anglais écrit requis.

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 6 mois
- à partir de Janvier 2016
- à Elancourt (78)

[10289936] Audit de sécurité et test d'instrusion sur des équipements communiquant via des technologies Zigbee

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe CSIRT (*Computer Security Incident Response Team*) en tant que stagiaire. Sa mission est de répondre aux incidents de sécurité Informatique en fournissant tous les services nécessaires pour résoudre les problèmes ou pour aider à leur résolution. Afin de diminuer les risqué et minimiser le nombre d'interventions nécessaires, l'équipe CSIRT peut être également amenée à recommander l'utilisation de méthodes préventives sur son périmètre d'intervention. Elle émet également des alertes de sécurité décrivant des vulnérabilités et des virus touchant des composants logiciels et matériels, ce qui peut permettre à ses clients de patcher et updater leurs systèmes très rapidement. L'une des activités de l'équipe CSIRT consiste à faire du pentest de protocoles radio pour la vérification de la bonne implémentation de propriétés de sécurité.

Le but de ce stage est de concevoir des outils pour auditer et tester la sécurité d'équipements **ZigBee**. L'application visée est un système de surveillance de la qualité et de la quantité d'eau potable distribuée dans un réseau. Ces outils permettront de reproduire des attaques protocolaires standards et évoluées (aussi appelés tests d'intrusion ou « **pentests** »), ce qui autorisera le test de l'architecture des capteurs déployés et les contre-mesures associées.

Le stagiaire réalisera des bancs de test pour valider les outils développés et démontrer leurs capacités d'audit et de test. Il sera encadré par des auditeurs expérimentés pour l'aider dans la phase de spécifications de ces bancs. Il sera également amené à mettre en œuvre des démonstrations devant des publics variés.

Le stagiaire acquerra à la fin de son stage des compétences solides en radio logicielle (Software Defined Radio, **SDR**) et en langage **C++**. Il sera amené à utiliser à utiliser l'outil de développement open-source **GNURadio**, fournissant des blocs de traitement du signal permettant d'implanter des **SDRs**. Enfin, il utilisera intensivement **Scapy**, logiciel libre de manipulation de paquets réseau écrit en **Python**.

2. Déroulement et objectifs du stage

- Prise en main des outils GNURadio et Scapy
- Développement de bancs de test
- Réalisation de pentests
- Mise en place de démonstrations

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Connaissances en SDR (Software Defined Radio), GNURadio et Scapy
- Bon niveau de programmation en C(++) et en Python

4. Durée, Date et Lieu

- 6 mois
- à partir de février 2016
- à Elancourt (78)

[10289937] Implémentation de *plug-ins* IDA Pro pour la reconnaissance accélérée d'algorithmes cryptographiques

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe CSIRT (*Computer Security Incident Response Team*) en tant que stagiaire. Sa mission est de répondre aux incidents de sécurité Informatique en fournissant tous les services nécessaires pour résoudre les problèmes ou pour aider à leur résolution. Afin de diminuer les risqué et minimiser le nombre d'interventions nécessaires, l'équipe CSIRT peut être également amenée à recommander l'utilisation de méthodes préventives sur son périmètre d'intervention. Elle émet également des alertes de sécurité décrivant des vulnérabilités et des virus touchant des composants logiciels et matériels, ce qui peut permettre à ses clients de patcher et updater leurs systèmes très rapidement.

L'une des activités de l'équipe CSIRT consiste à faire de la rétro-ingénierie de logiciels, tels des malwares. De nombreux malwares utilisent des primitives cryptographiques (ex. : chiffrement des communications, du fichier de configuration, etc.). Un reverser expérimenté sait reconnaître rapidement toutes les structures « classiques » d'un code, de la boucle « for » à l'implémentation d'un algorithme cryptographique standard (ex. : DES, AES). Mais cela peut être plus difficile lorsque le malware utilise des primitives cryptographiques peu connues. On peut en effet recenser dans la littérature plusieurs dizaines de primitives de chiffrement par blocs, par flot, de fonctions de hachage, et de chiffrement authentifié, et les derniers concours cryptographiques internationaux récents participent à l'inflation de ce nombre (37 candidats pour le concours eStream, 64 pour SHA-3, 57 candidats pour CAESAR), sans parler du nombre croissant de propositions d'algorithmes cryptographiques dits « légers ». Un concepteur de malwares sait pertinemment que s'il implante de la cryptographie standard, elle va se faire détecter facilement. En revanche, l'attaquant peut compliquer la tâche du reverser en utilisant des algorithmes peu communs.

2. Déroulement et objectifs du stage

Nous proposons d'implanter des solutions pour faciliter la tâche du reverser en automatisant le plus possible la détection de ces fonctions lors de la rétro-conception d'un logiciel. Plus précisément, pour identifier la cryptographie dans les binaires, le stagiaire commencera par effectuer une recherche par patterns (constantes d'algorithmes cryptographiques, valeurs de S-Boxes, valeurs d'initialisation, etc.), puis une recherche basée sur le graphe d'appels de fonctions.

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Bonne maîtrise ou connaissances approfondies en reverse d'algorithmes (sous IDA Pro) et en cryptographie (protocoles, algorithmes de chiffrement par blocs et par flot, signature, etc.)
- Bon niveau de programmation en C(++)

4. Durée, Date et Lieu

- 6 mois
- à partir de février 2016
- à Elancourt (78)

[10290483] Capture réseau temps réel

1. Contexte du stage

Au sein d'Airbus Defence & Space CyberSecurity, vous intégrez l'équipe Cyberdéfense en tant que stagiaire. Elle a pour mission la mise en place et l'opération des capacités Cyberdéfense (analyse, construction, supervision, réponse à incident).

Le stage prend place dans la partie R&D d'un produit d'Airbus Defence and Space. Au sein du projet actif, vous réaliserez un logiciel de capture réseau temps réel, indexant le flux afin de facilité un traitement ultérieur.

2. Déroulement et objectifs du stage

Le stage se déroulera en 3 phases :

1. Un état de l'art des solutions de capture réseau
2. La spécification de l'architecture et des solutions techniques
3. Le développement de la solution spécifiée. L'implémentation sera réalisée avec un niveau de qualité élevé. Les pratiques d'intégration continue et TDDs seront appliquées.

A l'issue du stage, le logiciel doit être opérationnel, testé et documenté.

Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Excellente connaissance en C.
- Bonne maîtrise du Python, des problématiques réseaux et du format pcap est un plus.
- Un esprit de synthèse et d'excellentes capacités rédactionnelles sont attendus.
- Anglais écrit requis.

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 6 mois
- à partir de Septembre 2015
- à Elancourt (78)

[10290484] Cryptographie Hautes Performances sur FPGA

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe « cryptographie » en tant que stagiaire. Sa mission est de développer des solutions de systèmes intégrés sécurisés parfaitement conformes aux besoins de ses clients. Plus précisément, l'un de ses objectifs est de sécuriser l'exécution d'opérations (chiffrement de données, authentification, identification, etc.) en présence de personnes potentiellement mal intentionnées. Il est donc amené à implanter dans ses produits de sécurité des primitives cryptographiques.

Dans ce cadre, l'une des activités de l'équipe « cryptographie » est d'implanter de la cryptographie dans des FPGAs. Ces implémentations cryptographiques doivent être les plus performantes possibles (haut débit, surface faible). Nous proposons dans ce stage d'implanter une version d'AES à débit très élevé (l'objectif étant d'atteindre les 10GBps). Pour ce faire, nous utiliserons une implantation en « T-tables », qui n'utilisera en priorité que les Block RAMs et DSPs du FPGA pour tirer profit de leurs hautes performances. Une généralisation de cette approche à d'autres algorithmes cryptographiques peut également être envisagée.

2. Déroulement et objectifs du stage

- Etude des propriétés de l'AES et de l'architecture du FPGA utilisé (ici, un Virtex-5)
- Implantation de l'architecture de l'AES en « T-tables »
- Méthodologie de programmation des « T-tables »
- Analyse des performances
- Scénario de test et démo
- Extension de la méthodologie à d'autres blocs cryptographiques

Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Bonne maîtrise en microélectronique, FPGAs (si possible Xilinx), VHDL. Bonnes connaissances en cryptographie.
- Pour la validation, un bon niveau de programmation en langage C est également souhaitable.
- Un esprit de synthèse et d'excellentes capacités rédactionnelles sont attendus.
- Anglais écrit requis.

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 6 mois
- à partir de février 2016
- à Elancourt (78)

[10290485] Etat de l'art des solutions de détection et gestion des vulnérabilités

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe du Build Center en tant que stagiaire.

Cette équipe a pour mission de construire et de déployer :
- des solutions de sécurité pour des systèmes d'information
- des moyens de supervision de la sécurité pour des systèmes d'information

Le stagiaire devra déployer et évaluer différentes solutions de détection et gestion des vulnérabilités (Vulnerability Assessment) afin de déterminer les fonctionnalités couvertes ainsi que leurs capacités à répondre à certaines contraintes (gestion centralisée, déploiement sous forme de service (SaaS), export des rapports, intégration avec des outils SIEM…). Le stagiaire devra définir les procédures d'évaluation. Un rapport devra être rédigé pour chacun des produits.

2. Déroulement et objectifs du stage

Le stage proposé à 3 objectifs majeurs qui sont:

1. Une phase d'étude théorique sur l'état de l'art des outils de gestion de vulnérabilités acteurs dans la supervision de la sécurité des SI
2. Une évaluation technico-fonctionnelle de 2 à 3 solutions de gestion de vulnérabilités sur la plateforme R&D
3. Identification des possibilités d'intégration de ces outils dans la solution de supervision de la sécurité soutenue par Airbus Defence & Space CyberSecurity.

Un état de l'art, un bilan des tests et maquettage d'interconnexion sont attendus à l'issue de cette première partie.

Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : Formation école d'ingénieurs (4ème année ou fin d'études).
- Bonne maîtrise des environnements Windows, Linux et des technologies de virtualisation (VMware)
- Culture générale sur la sécurité informatique (firewalls, détecteurs d'intrusion, scanners de vulnérabilités,...).
- Culture générale sur les réseaux (adressage, routage,...).
- La connaissance d'un ou plusieurs solutions de scans de vulnérabilités (ex : OpenVAS, Nessus…) est fortement appréciée.
- Un esprit de synthèse et d'excellentes capacités rédactionnelles sont attendus.
- Anglais lu et écrit requis.

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 3 à 6 mois
- à partir de Janvier 2016
- à Elancourt (78)

[10290653] Etude et développement dans un outil de veille en vulnérabilités

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe du Build Center en tant que stagiaire. Au sein de cette équipe, vous travaillez dans le service de veille en vulnérabilités. Celui-ci dispose d'un outil de gestion des vulnérabilités. C'est au titre de développeur que vous travaillez sur cet outil.

L'objectif du stage est d'améliorer la base de connaissances d'un outil de veille en vulnérabilités en prenant en compte deux demandes d'améliorations principalement.
Le stagiaire devra :

- Comprendre les enjeux de la veille en vulnérabilités ;
- Ajouter une (ou des) sonde(s) parsant les bulletins de sécurité de différents éditeurs de sécurité ;
- Etudier et développer un nouveau module dans l'outil de veille ;

2. Déroulement et objectifs du stage

Le stage se déroulera en plusieurs phases :

1. Connaissance du contexte ;
2. Prise en main de l'outil et de l'environnement de travail ;
3. Attribution de tickets de faibles et moyennes importance pour se familiariser avec le processus de développement (commit, description des tickets etc.) ;
4. Attribution de tickets d'importances plus hautes ;
5. Développement d'une sonde afin de collecter des sources d'informations liées aux vulnérabilités ;
6. Etude et développement d'un nouveau module à l'outil de veille.

Le stagiaire livrera des versions du programme à travers la résolution des tickets qui lui seront attribués.
Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Excellente connaissance en langage de programmation et base de données
- Bonne maîtrise de JAVA
- Connaissance d'un ou plusieurs langages de script
- Sensibilisation à la sécurité informatique
- Un esprit de synthèse, une bonne autonomie et être force de proposition sont attendus
- Bon niveau d'anglais.

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 6 mois
- à partir de Janvier 2016
- à Elancourt (78)

[10290654] Rétro-ingénierie d'algorithmes cryptographiques par analyse de canaux auxiliaires

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe CSIRT (*Computer Security Incident Response Team*) en tant que stagiaire. Sa mission est de répondre aux incidents de sécurité informatique en fournissant tous les services nécessaires pour résoudre les problèmes ou pour aider à leur résolution. Elle émet également des alertes de sécurité décrivant des vulnérabilités et des virus touchant des composants logiciels et matériels, ce qui peut permettre à ses clients de patcher et updater leurs systèmes très rapidement.

Dans ce cadre, l'une des activités de l'équipe CSIRT consiste à faire de la rétro-ingénierie de *firmwares*. Or, lorsque CSIRT doit extraire un *firmware* dans un composant (ex. : micro-contrôleur), il se peut que des protections contre le *writeback* (fusibles) soient activées, et que donc l'extraction du *firmware* soit impossible par des moyens conventionnels. Des moyens très sophistiqués peuvent être mis en jeu (inversion de la polarité des fusibles par du rayonnement ultra-violet par exemple), mais le matériel nécessaire pour cela est coûteux, le procédé nécessite un personnel très expérimenté et le client ne voudra peut-être pas que l'on soit invasif sur le système à auditer.

Une autre alternative possible est d'effectuer la rétro-ingénierie d'algorithmes cryptographiques par analyse de canaux auxiliaires (*Side-Channel Analysis for Reverse-Engineering*, SCARE).

2. Déroulement et objectifs du stage

Nous proposons d'effectuer du SCARE sur un composant, c'est-à-dire de monitorer les canaux auxiliaires (consommation électrique, rayonnement électromagnétique, etc.) du système audité afin de retrouver les instructions élémentaires exécutées par le système (souvent, un micro-processeur). On commence tout d'abord par « profiler » un système identique et programmable : on programme le système (ici, un processeur Leon2 implanté sur FPGA) avec une instruction particulière (par exemple une addition de deux opérandes fixes « X » et « Y », ou « ADD(X,Y) »), l'auditeur prend alors plusieurs mesures de la consommation électrique du système pendant l'exécution de cette instruction, puis reproduit le processus pour toutes les opérandes possibles, puis pour toutes les instructions restantes (« SUB », « LD », *etc*.). A la fin du processus, l'auditeur récupère un véritable « dictionnaire » qui lui servira de référence pour la deuxième phase.

La deuxième phase consiste à comparer les mesures de consommation du système audité avec le dictionnaire pour retrouver chaque instruction exécutée, puis, à la fin du processus, le *firmware* complet embarqué dans le système.

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Bonne maîtrise en instrumentation (manipulation de sondes, d'oscilloscope, *etc*.), en statistique (calcul de corrélations, *etc*.), et bonnes connaissances en architecture des processeurs.
- Bon niveau de programmation en Matlab.

4. Durée, Date et Lieu

- 6 mois
- à partir de février 2016
- à Elancourt (78)

[10290655] Etude des moyens de supervision des environnements Cloud

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe du Build Center en tant que stagiaire.

Cette équipe a pour mission de construire et de déployer :

- des solutions de sécurité pour des systèmes d'information
- des moyens de supervision de la sécurité pour des systèmes d'information

Le stagiaire devra étudier et évaluer différentes solutions de supervision de sécurité pour les environnements Cloud afin de détecter les attaques sur ces environnements. Dans un premier temps, le stagiaire devra étudier les capacités des différents environnements Cloud tels que Office 365, Microsoft Azur, Amazon AWS/EC2, … à fournir des indicateurs de sécurité (rapports, logs, API, …) et leurs intégration avec des outils SIEM ou « Analytics ». Le stagiaire devra définir les procédures d'évaluation. Un rapport devra être rédigé pour chacun des environnements étudiés.

2. Déroulement et objectifs du stage

Le stage proposé à 3 objectifs majeurs qui sont:

1. Une phase d'étude théorique sur l'état de l'art des différents environnements Cloud et des indicateurs de sécurité disponibles pour la supervision de la sécurité des SI.
2. Etude des menaces applicables sur les environnements Cloud étudiés
3. Mise en œuvre d'une ou deux solutions techniques pour la récupération des indicateurs de sécurité et l'interconnexion avec les outils supervision de la sécurité soutenue par Airbus Defence & Space CyberSecurity

Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : Formation école d'ingénieurs (4ème année ou fin d'études).
- Bonne maîtrise des environnements Windows, Linux et des technologies de virtualisation (VMware)
- Culture générale sur la sécurité informatique (firewalls, détecteurs d'intrusion, scanners de vulnérabilités,...).
- Culture générale sur les réseaux (adressage, routage,...).
- Un esprit de synthèse et d'excellentes capacités rédactionnelles sont attendus.
- Anglais lu et écrit requis.

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 6 mois
- à partir de Janvier 2016
- à Elancourt (78)

[10291152] Cryptographie légère pour la sécurisation de communications de capteurs sans fils pour le SCADA

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe « cryptographie » en tant que stagiaire. Sa mission est de développer des solutions de systèmes intégrés sécurisés parfaitement conformes aux besoins de ses clients. Plus précisément, l'un de ses objectifs est de sécuriser l'exécution d'opérations (chiffrement de données, authentification, identification, etc.) en présence de personnes potentiellement mal intentionnées. Il est donc amené à implanter dans ses produits de sécurité des primitives cryptographiques.

Dans ce cadre, l'une des activités de l'équipe « cryptographie » est d'implanter de la cryptographie dans des capteurs sans fils. Dans des environnements très contraints tels les systèmes de contrôle industriels ICS ou les systèmes d'acquisition de données SCADA, la cryptographie implantée doit être la plus transparente possible pour le système (surcoût sur le débit limité, latence faible) afin de respecter les contraintes temps réel des systèmes. Or l'utilisation d'algorithmes de chiffrement standards ne permet pas dans certains cas de respecter ces contraintes de performances. C'est dans ce cadre qu'il est souvent proposé des algorithmes dits « légers » ayant des propriétés structurelles leur permettant d'être mieux dimensionnés et adaptés aux systèmes ICS-SCADA.

Ce stage se propose d'implanter de façon logicielle des algorithmes de chiffrement légers innovants sur des microcontrôleurs de type Arduino.

2. Déroulement et objectifs du stage

- Etude d'un réseau de capteurs existant
- Prise en main des outils de développement logiciels
- Etat de l'art des algorithmes de chiffrement légers
- Implantation des algorithmes choisis
- Validation et analyse des performances

Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Bonnes connaissances en cryptographie, protocoles sans-fils de type 802.15.4 (Zigbee)
- Bonne maîtrise de la programmation en langage C et assembleur.
- Une initiation à l'outil d'analyse Scapy et au langage Python est un plus.
- Anglais écrit requis.

4. Durée, Date et Lieu

- 6 mois
- à partir de février 2016
- à Elancourt (78)

[10291154] Déchiffrement de paquets réseaux et analyses statistiques

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe « cryptographie » en tant que stagiaire. Sa mission est de développer des solutions de systèmes intégrés sécurisés parfaitement conformes aux besoins de ses clients. Plus précisément, l'un de ses objectifs est de sécuriser l'exécution d'opérations (chiffrement de données, authentification, identification, etc.) en présence de personnes potentiellement mal intentionnées. Il est donc amené à implanter dans ses produits de sécurité des primitives cryptographiques. Elle aide également la société à améliorer les performances de ses produits de CyberDéfense.

Dans ce cadre, l'une des activités de l'équipe « cryptographie » consiste à implanter efficacement des algorithmes d'analyse dans des plate-formes hautes performantes. Parmi les produits concernés, les sondes de détection d'intrusion (IDS) doivent faire face à des débits de trafic réseau de plus en plus importants et à des menaces renouvelées conduisant à des traitements sur ces paquets de plus en plus complexes. De plus, les IDS affrontent de plus en plus de trafic chiffré (souvent basiquement par OpenSSL) et anonymisé (via notamment l'utilisation de Tor), ce qui complexifie les analyses, et endommage leurs performances.

Ce stage se propose d'implanter un module software de détection de flux réseau chiffré et de déchiffrement SSL. Des analyses statistiques seront effectuées sur des paramètres du flux chiffré (par exemple la longueur moyenne et le timing des paquets réseaux) pour tenter de révéler des informations sur ces paquets et donc sur l'attaque potentiellement en cours de réalisation. Par ailleurs, suivant le protocole utilisé (ex : IPSec en mode transport), il sera possible de récupérer le header IP en clair, et donc les IPs source et destination.

Le but ultime étant de pouvoir réaliser une analyse en run-time du trafic monitoré. Par ailleurs, dans la seconde partie du stage, l'effet des contre-mesures de type « *Traffic Morphing* », ou encore « *Random Padding* » (cf. Encrypted BitTorrent et Gnuttela) devra être pris en compte.

2. Déroulement et objectifs du stage

- Etudes des solutions de l'état de l'art (SourceFire, Gigamon, etc.)
- Développement de l'outil d'analyse de flux réseau en run-time
- Interfaçage avec les produits d'Airbus Defence & Space - CyberSecurity
- Etude de l'effet des contre-mesures
- Estimation des performances dans une preuve de concept (démo)

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Bonnes connaissances en sécurité des réseaux informatiques, cryptographie, statistiques, en programmation en langage C(++) et/ou Python, et en algorithmique.

4. Durée, Date et Lieu

- 6 mois
- à partir de février 2016
- à Elancourt (78)

[10291155] Implantation d'algorithmes de *pattern-matching* dans un GPU

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe « cryptographie » en tant que stagiaire. Sa mission est de développer des solutions de systèmes intégrés sécurisés parfaitement conformes aux besoins de ses clients. Plus précisément, l'un de ses objectifs est de sécuriser l'exécution d'opérations (chiffrement de données, authentification, identification, etc.) en présence de personnes potentiellement mal intentionnées. Il est donc amené à implanter dans ses produits de sécurité des primitives cryptographiques. Elle aide également la société à améliorer les performances de ses produits de CyberDéfense.

Dans ce cadre, l'une des activités de l'équipe « cryptographie » consiste à implanter efficacement des algorithmes dans des plate-formes hautes performantes. Ce stage se propose d'implanter des algorithmes de *pattern-matching* dans des GPUs. En effet, les sondes de détection d'intrusion (IDS) doivent faire face à des débits de trafic réseau de plus en plus importants et à des menaces renouvelées conduisant à des traitements sur ces paquets de plus en plus complexes. Elles vérifient qu'un jeu de règles sur les paquets réseaux inspectés est bien respecté. Parmi toutes les étapes à réaliser, la recherche de motifs (opération également appelée *pattern-matching* qui permet de trouver le plus rapidement possible les informations utiles dans un paquet réseau) est de loin celle qui est la plus longue, occupant typiquement 75 à 80% du temps de calcul d'un IDS. Il conviendrait donc de trouver un moyen d'accélérer cette opération.

L'utilisation de cartes graphiques (GPUs) paraît une solution plus efficace et viable. Les GPUs sont utilisés depuis des années dans de nombreux champs d'applications (opérations graphiques, simulations financières, classification d'images, etc.) dont le monde de la sécurité informatique et de la cryptographie (brute forces, recherche de collisions, implantations optimisées de protocoles cryptographiques, etc.). Leur caractère intrinsèquement parallèle nous intéresse tout particulièrement car la plupart des algorithmes de *pattern-matching* sont eux-mêmes facilement parallélisables, et seraient donc adaptés aux GPUs.

2. Déroulement et objectifs du stage

- Etude des algorithmes de *pattern-matching* (Aho-Corasick, Wu-Manber, Commentz-Walter, etc.)
- Implantation de ces algorithmes sur GPU
- Extension du travail à un IDS complet (de type Snort), et estimation des performances dans une preuve de concept (démo)

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Bonnes connaissances en architecture et codage des GPUs (CUDA, etc.), en programmation en langage C(++), en algorithmique et en sécurité des réseaux informatiques en général.

4. Durée, Date et Lieu

- 6 mois
- à partir de février 2016
- à Elancourt (78)

[10291157] Utilisation de la cryptographie basée sur l'identité pour du partage sécurisé de documents

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe « cryptographie » en tant que stagiaire. Sa mission est de développer des solutions de systèmes intégrés sécurisés parfaitement conformes aux besoins de ses clients. Plus précisément, l'un de ses objectifs est de sécuriser l'exécution d'opérations (chiffrement de données, authentification, identification, etc.) en présence de personnes potentiellement mal intentionnées. Il est donc amené à implanter dans ses produits de sécurité des primitives cryptographiques.

Dans ce cadre, ce stage propose d'utiliser de la cryptographie basée sur l'identité (*Identity-Based Cryptography*, IBC) pour concevoir une application de partage sécurisé de documents. L'IBC peut se servir de n'importe quelle information sur le destinataire comme clé publique (ex. : son adresse mail). Cette particularité permet de réduire drastiquement la complexité du processus cryptographique en éliminant, en particulier, la nécessité de générer et distribuer les certificats des utilisateurs. Imaginée dans les années 1980, ce type de cryptographie a commencé à émerger théoriquement dans le début des années 2000 et est maintenant utilisé dans quelques applications (chiffrement de mails, etc.). Nous nous proposons d'étudier plus particulièrement l'utilisation de l'IBC pour le chiffrement et la signature (courte) de documents sur un SharePoint utilisable par un groupe d'utilisateurs. Le stagiaire étudiera également la possibilité d'utiliser le chiffrement en *broadcast* en utilisant des rôles ou des attributs des utilisateurs (ex. : fonctions dans une entreprise).

2. Déroulement et objectifs du stage

- Etude de la théorie de l'IBC (*pairing-based cryptography*)
- Implantation sous librairie MIRACL (interfaces C++)
- Estimation des performances dans une preuve de concept (démo)

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Bonnes connaissances en cryptographie à clé publique, plus particulièrement en *pairings*, expérience en programmation en langage C(++), et en algorithmique.

4. Durée, Date et Lieu

- 6 mois
- à partir de février 2016
- à Elancourt (78)

[10291158] Etude, conception, réalisation et mise en œuvre d'une solution de validation système automatisée

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe du Build Center en tant que stagiaire.

Cette équipe a pour mission de construire et de déployer :
- des solutions de sécurité pour des systèmes d'information
- des moyens de supervision de la sécurité pour des systèmes d'information

Le stagiaire devra évaluer différentes solutions de validation système automatisées afin de déterminer leurs fonctionnalités ainsi que leur adéquation aux besoins de l'équipe. Il devra ensuite utiliser cette évaluation pour concevoir, réaliser et mettre en œuvre une solution de validation système sur une plateforme de Cybersecurité générique constituée de composants hétérogènes.

Il sera attendu du stagiaire un fort sens de l'autonomie et de la prise d'initiative, ainsi qu'une capacité à assumer la vision globale de l'ingénierie d'un projet, aussi bien sur ses aspects techniques qu'organisationnels.

2. Déroulement et objectifs du stage

Le stage proposé se déroulera suivant les phases suivantes:

1. Une phase d'étude théorique sur l'état de l'art des solutions de validation automatisées disponibles
2. Une évaluation technico-fonctionnelle de 2 à 3 solutions sur la plateforme R&D
3. Conception d'une solution adaptée aux besoins de l'organisation Cybersecurity
4. Réalisation et mise en œuvre de la solution sur une plateforme système de cybersecurité générique composée de constituants hétérogènes.
5. Amélioration de la solution par la prise en charge de la traçabilité des exigences et des campagnes de tests
6. Debrief

Description des livrables du stage :

- Un état de l'art
- Un bilan des tests
- Description de la solution retenue et de sa mise en place
- Bilan de la couverture des tests systèmes automatisés sur la plateforme cible

Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : Formation école d'ingénieurs (4ème année post-BAC ou fin d'études).
- Bonne maîtrise des environnements UNIX / Linux, Windows et des technologies de virtualisation (VMware)
- Culture générale sur la sécurité informatique (firewalls, détecteurs d'intrusion, scanners de vulnérabilités,...).
- Culture générale sur les réseaux (adressage, routage,...).
- La connaissance préalable d'outils de tests et de gestion de configuration (ex : Puppet, Chef, Jenkins, Cucumber…) est fortement appréciée.
- Un esprit de synthèse et d'excellentes capacités rédactionnelles sont attendus.
- Anglais lu et écrit requis.

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 6 mois
- à partir de Janvier 2016
- à Elancourt (78)

[10291247] Etude des mécanismes de haute disponibilité systèmes et réseaux

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe du Build Center en tant que stagiaire.
Cette équipe a pour mission de construire et de déployer :

- des solutions de sécurité pour des réseaux
- des moyens de supervision de sécurité de réseaux.

L'équipe Build Center a mis en place une solution de gestion de la sécurité des réseaux informatiques. Ce logiciel développé dispose de capacités de communication afin de récupérer des informations sur l'état de sécurité de systèmes d'information et d'offrir des services permettant de gérer les incidents de sécurité.

Le but du stage est d'étudier la faisabilité et réaliser une preuve de concept sur la mise en oeuvre de cette application en haute disponibilité tout en respectant les contraintes de sécurité.

Pour cela, le stagiaire devra étudier les solutions hardware et logicielles telles que la mise en clustering de base de données, la réplication DRDB, les solutions de « heartbeat », les mécanismes de partage de charge logiciels et réseaux.

En complément, le stagiaire pourra également évaluer les mécanismes de réplication sur réseau WAN afin de mesurer les capacités de son PoC à être mis en redondance sur un site distant.

Le stagiaire évaluera la sécurité de sa solution et les vulnérabilités potentielles induites par la mise en haute disponibilité.

2. Déroulement et objectifs du stage

Le stage se déroulera en plusieurs phases :

1. Prise de connaissance de l'application,
2. Prise de connaissance des outils et composants permettant une haute disponibilité (état de l'art des solutions logicielles et boitiers externes),
3. Présentation d'une architecture cohérente,
4. Analyse et spécifications,
5. PoC : intégration et mise en œuvre des composants techniques.
6. Evaluation de la disponibilité lors d'une mise à jour de version des composants
7. Tests et validation

Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : 4ème année ou fin d'études
- Excellente connaissance de CentOS (ou RedHat), administration Unix, réseaux, Shell et Python, sécurité informatique
- Bonne maîtrise de la gestion de configuration SVN ou GIT
- Un esprit de synthèse et d'excellentes capacités rédactionnelles sont attendus.
- Anglais écrit souhaité.

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 6 mois
- à partir de Janvier 2016
- à Elancourt (78)

[10294601] Sécurité des *Internet of Things* (IoT)

1. Contexte du stage

Au sein de la société Airbus Defence & Space CyberSecurity, vous intégrez l'équipe du Build Center en tant que stagiaire.
Cette équipe a pour mission de construire et de déployer :

- des solutions de sécurité pour des réseaux ;
- des moyens de supervision de sécurité de réseaux.

Dans ce contexte, vous serez en charge de développer et intégrer de nouveaux composants sur une plateforme liée à la sécurité des objets connectés mise en place par l'équipe du Build Center dans le cadre d'une solution innovante.

2. Déroulement et objectifs du stage

Le stage se déroulera en plusieurs phases :

1. Prise en main de la plateforme
2. Rédaction de spécifications techniques pour les nouveaux composants
3. Implémentation des évolutions
4. Présentation des nouvelles capacités du démonstrateur

Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : BAC+5 ;
- Bonne connaissance des langages de programmation C, Python, JavaScript et HTML ;
- Bonne maîtrise des environnements Linux (Shell, …) ;
- Une connaissance du langage de programmation Java serait un plus ;
- Un esprit de synthèse et de bonnes capacités rédactionnelles sont attendus ;
- Anglais écrit requis.

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 6 mois
- à partir de Janvier 2016
- à Elancourt (78)

[10295437] Développement d'un relais de communication à travers une diode

1. Contexte du stage

Au sein de la société Airbus Defence&Space CyberSecurity, vous intégrez l'équipe du Build Center en tant que stagiaire. Cette équipe a pour mission:

- de construire et de déployer des solutions de sécurité pour les réseaux,
- de définir et de mettre en œuvre des passerelles d'interconnexion entre plusieurs réseaux de niveaux de sensibilité différents.

Afin d'interconnecter des réseaux de niveau de sensibilité différents via un flux unidirectionnel, l'équipe Project Design & Integration a mis en place des diodes optiques entre ces réseaux.
Le but du stage est de capitaliser le travail qui a déjà été réalisé sur différents projets et de réaliser une solution générique couvrant les besoins de ces différents projets.
Vous serez en charge d'étudier les différents développements en langage C qui ont été mis en œuvre, de proposer un protocole de communication garantissant la bonne livraison des datagrammes, de développer la solution en y ajoutant les besoins de l'équipe du Project Design & Integration, de réaliser une démonstration et de présenter vos travaux à l'équipe.

2. Déroulement et objectifs du stage

Le stage se déroulera en plusieurs phases :

1. Etude de ce qui a déjà été développé au sein de Project Design & Integration,
2. Etude de conception en fonction des nouveaux besoins de l'équipe,
3. Définition du protocole de communication et de l'architecture logicielle de la solution,
4. Rédaction des spécifications techniques,
5. Implémentation en langage C de cette solution,
6. Tests et mesures de performance de la solution réalisée,
7. Rédaction de la documentation d'utilisation,
8. Présentation des travaux réalisés et démonstration.

Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Excellente connaissance en langage C, en réseau.
- Bonne maîtrise de la gestion de configuration SVN ou GIT, des notions de sécurité, des environnements Linux (Shell, …).
- Un esprit de synthèse et d'excellentes capacités rédactionnelles sont attendus.
- Anglais écrit requis.

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 6 mois
- à partir de janvier 2016
- à Elancourt (78)

[10296076] Améliorations d'outils de Tests en Sécurité

1. Contexte du stage

Au sein d'Airbus Defence & Space CyberSecurity, vous intégrez l'équipe Cyberdéfense en tant que stagiaire. Elle a pour mission la mise en place et l'opération des capacités Cyberdéfense (analyse, construction, supervision, réponse à incident).

Le stage se déroule dans un environnement d'une plateforme technique R&D représentative de réseaux d'entreprises multi-sites (Linux, Windows, AD, serveurs applicatifs, Firewalls, Routeurs, NAS, Proxy, Outils de supervision...).

L'implémentation des travaux du stage s'articulera autour de cette plateforme technique qui centralise des outils de tests basés sur des scénarios d'attaques qui permettent entre autre d'assurer la configuration des équipements de supervision mais également de proposer des formations.

Vous travaillerez dans une équipe d'industrialisation logicielle et utiliserez les méthodes agiles.

2. Déroulement et objectifs du stage

Le stage proposé a 2 objectifs majeurs qui sont:

1. Participation à l'amélioration de l'outil via l'ajout de nouvelles fonctionnalités comme la possibilité d'ajouter facilement de nouvelles attaques et de scénarios type APT ainsi que permettre la visualisation graphique de ces attaques et scénarios à travers de vues topologiques animées.
2. Amélioration et implémentation de nouvelles attaques et scénarios type APT via la réalisation de scripts Python et en utilisant le framework Metasploit.

Ce stage vous permettra d'avoir une bonne connaissance de l'entreprise et de ses processus et par conséquent, une meilleure compréhension favorisant votre futur développement.

3. Compétences souhaitées

- Niveau d'étude : BAC+5
- Culture générale sur les systèmes, les réseaux et la sécurité
- Connaissance des systèmes Linux et Windows
- Bonne connaissance des standards et technologies web modernes
- Bonne connaissance des architectures REST
- JavaScript, Python, HTML5, CSS3, PHP
- Un esprit de synthèse et d'excellentes capacités rédactionnelles sont attendus.
- Anglais écrit requis.

Dynamique, doté d'un excellent relationnel, passionné(e) par votre métier et avec le goût du service.

4. Durée, Date et Lieu

- 6 mois
- à partir de Janvier 2016
- à Elancourt (78)