Moving Target Defense : Software-Defined Networking

ANQUETIL Eloi - IR4
BAUDIER Bastien
BERGER Richard
BONFILS Kim
BRUN-PICARD Matéo

Tuteur ESAIP : Karim ZKIK
TUTEUR Entreprise : Kamal BENZEKKI

Semestre 8 2023

Table des matières

1 Introduction

Dans le cadre du projet d'initiative d'Activ'ESAIP, notre équipe, sous la supervision de Kamal BENZEKKI et Karim ZKIK, se concentre sur l'étude et l'implémentation de la stratégie de Moving Target Defense (MTD) dans un environnement de Software-Defined Networking (SDN). L'intérêt croissant pour la cybersécurité, motivé par la nécessité de protéger les infrastructures critiques contre des attaques de plus en plus sophistiquées, nous a guidés vers l'exploration de cette approche innovante. Le MTD, en modifiant dynamiquement les configurations du réseau, vise à déjouer les attaques en rendant les cibles moins prévisibles et plus difficiles à compromettre.

Notre projet s'articule autour de la mise en place de cette solution sur la workzone 1 du CyberRange d'ESAIP, situé à Angers. Ce choix de localisation favorise une collaboration étroite et efficace avec nos tuteurs et experts en la matière, enrichissant ainsi notre compréhension et notre capacité à implémenter des solutions de cybersécurité robustes. En explorant les facettes de la MTD dans le SDN, nous aspirons non seulement à renforcer la sécurité des réseaux informatiques mais aussi à offrir une formation pratique aux étudiants impliqués, leur permettant de se familiariser avec des technologies de pointe et de contribuer activement à la sécurité de l'information dans leurs futurs environnements professionnels.

2 CONTEXTE ET DÉFINITION DE LA PROBLÉMATIQUE DE LA STRUCTURE D'ACCUEIL

L'ESAIP, une école d'ingénierie reconnue, se trouve aujourd'hui confrontée à une menace croissante de cyberattaques, notamment les attaques de phishing qui ciblent ses étudiants et personnel. Cette vulnérabilité soulève des inquiétudes majeures car les informations compromisées pourraient non seulement affecter les individus concernés mais également la sécurité des futures entreprises où ces étudiants pourraient exercer. En réponse à cette menace, l'initiative de mettre en œuvre une stratégie de Moving Target Defense (MTD) au sein d'un réseau défini par logiciel (SDN) a été proposée par notre enseignant-chercheur, Kamal BENZEKKI.

Cette approche innovante vise à augmenter la résilience du réseau en modifiant dynamiquement ses configurations, rendant ainsi les attaques plus difficiles et coûteuses pour les cybercriminels. L'objectif principal est de transformer notre infrastructure en une cible mouvante, moins prévisible et plus difficile à exploiter. Cela est crucial non seulement pour protéger les données sensibles de l'école mais aussi pour préparer les étudiants à appliquer et à développer ces technologies dans leurs futures carrières, renforçant ainsi la sécurité informatique au sein des entreprises qu'ils rejoindront.

L'importance de cette démarche est amplifiée par la nature des données traitées par l'école, incluant des informations personnelles et professionnelles sensibles. La mise en place de la MTD dans le cadre du SDN permettrait de créer un environnement de test et d'apprentissage idéal pour les étudiants, tout en contribuant activement à la sécurité et à l'intégrité de l'écosystème numérique de l'école. Ce projet, en plus de répondre aux besoins immédiats de sécurité, servira également de pilier pour des recherches et des applications futures dans le domaine de la cybersécurité éducative et professionnelle.

3 OBJECTIFS VISES PAR LE PROJET

Les attendus pour ce projet sont de faire un état de l'art du *Moving Target Defense* (MTD) en *Software-Defined Networking* (SDN) et si possible faire une mise en place sur la workzone 1 du CyberRange.
L'objectif est de découvrir cette partie de la cybersécurité et ainsi comprendre les différentes méthodes pour protéger une entreprise.

4 PERIMETRE DU PROJET

Le projet Moving Target Defense (MTD) dans un environnement Software-Defined Networking (SDN) à l'ESAIP est défini par plusieurs dimensions clés qui encadrent son développement et son exécution. Ces dimensions incluent le site d'intervention, le domaine d'intervention, les ressources nécessaires et les contraintes et limitations. Une compréhension claire de ces aspects est essentielle pour assurer la réussite du projet.

4.1 Site d'Intervention

4.1.1 Campus d'Angers de l'ESAIP

Le projet sera principalement mené sur le campus d'Angers, qui offre un accès exclusif au CyberRange. Le CyberRange est une plateforme de simulation d'attaques et de défenses cybernétiques, équipée de technologies de pointe permettant de recréer des environnements réseau complexes et variés. Ce site centralisé facilite une collaboration étroite avec les tuteurs et les experts en la matière, optimisant ainsi les conditions de test et d'apprentissage pour les étudiants. La proximité des ressources et des infrastructures de l'ESAIP permet une mise en œuvre pratique et une intervention rapide en cas de besoin. De plus, le campus d'Angers est un lieu stratégique car il est équipé des dernières technologies en matière de cybersécurité, ce qui offre un cadre idéal pour la réalisation de ce projet.

4.1.2 Avantages du CyberRange

Le CyberRange offre des capacités avancées pour la simulation et l'analyse des cyberattaques. Il permet de créer des scénarios réalistes où les étudiants peuvent tester et évaluer différentes stratégies de défense. La flexibilité de cette plateforme permet de simuler divers types d'attaques et de configurations réseau, offrant ainsi un terrain d'apprentissage riche et diversifié. Les infrastructures du CyberRange sont conçues pour supporter des charges de travail intensives et des tests répétés, ce qui est crucial pour un projet de cette envergure.

4.1.3 Collaboration et Support

La localisation du projet sur le campus d'Angers facilite également une collaboration étroite avec les tuteurs et les experts en cybersécurité. Les interactions régulières avec ces professionnels permettent d'obtenir des conseils précieux et des feedbacks constructifs, améliorant ainsi la qualité et l'efficacité du projet. Le support technique et académique disponible sur le campus joue un rôle crucial dans la résolution rapide des problèmes et l'optimisation des processus de mise en œuvre.

4.2 Domaine d'Intervention

4.2.1 Recherche et Développement en Cybersécurité

L'essence du projet réside dans la recherche appliquée et le développement de stratégies de cybersécurité innovantes. En se concentrant sur le MTD au sein du SDN, le projet explore de nouvelles façons de renforcer la sécurité des réseaux. Les objectifs incluent la mise en œuvre de techniques de défense dynamiques, la modification constante des configurations réseau pour déjouer les attaques, et l'utilisation de leurres pour tromper les attaquants. Le projet s'inscrit dans une démarche de recherche et développement visant à transformer les systèmes informatiques en cibles mouvantes, moins prévisibles et plus résistantes aux cyberattaques.

4.2.2 Innovations et Technologies Avancées

Le projet vise à intégrer des innovations technologiques pour améliorer la sécurité des réseaux. En utilisant les capacités du SDN, nous pouvons centraliser la gestion des politiques de sécurité et adapter rapidement les configurations en réponse aux menaces émergentes. La flexibilité du SDN permet de déployer des solutions de MTD de manière plus efficace et de manière à maximiser l'impact de ces stratégies de défense.

4.2.3 Impact sur l'Industrie et l'Éducation

Le projet ne se limite pas à une simple exploration académique. Il a un impact direct sur l'industrie en proposant des solutions applicables aux environnements professionnels. Les étudiants impliqués acquièrent des compétences précieuses en cybersécurité et en gestion de réseau, les préparant à des carrières dans ce domaine crucial. De plus, les résultats et les découvertes du projet peuvent être partagés avec la communauté académique et professionnelle, contribuant ainsi à l'avancement des connaissances et des pratiques en cybersécurité.

4.3 Ressources

4.3.1 Ressources Humaines

Notre équipe est composée de plusieurs étudiants de l'ESAIP, incluant Eloi Anquetil, Bastien Baudier, Richard Berger, Kim Bonfils, et Matéo Brun-Picard, supervisés par Karim ZKIK de l'ESAIP et Kamal BENZEKKI du secteur industriel. Cette diversité de compétences et de perspectives enrichit le projet et stimule une approche collaborative. Chaque membre de l'équipe apporte une expertise unique, qu'il s'agisse de la programmation, de la gestion de réseau, de la cybersécurité ou de l'analyse de données. Cette synergie est cruciale pour aborder les défis complexes du projet et pour développer des solutions innovantes.

4.3.2 Organisation et Collaboration

L'équipe s'organise en sous-groupes spécialisés pour aborder différents aspects du projet, tels que la recherche, le développement de code, et les tests. Des réunions régulières sont tenues pour assurer la coordination et la cohérence des efforts. La collaboration est facilitée par l'utilisation d'outils de gestion de projet et de communication, ce qui permet de suivre les progrès, de partager des ressources et de résoudre rapidement les problèmes.

4.3.3 Expertise et Formation

Les membres de l'équipe bénéficient d'une formation continue et de l'accès à des ressources éducatives pour renforcer leurs compétences. Des ateliers et des sessions de formation sont organisés pour aborder les nouvelles technologies et les meilleures pratiques en cybersécurité. L'expertise des tuteurs et des experts industriels est également mise à profit pour fournir des conseils et des orientations stratégiques.

4.3.4 Ressources Matérielles

Le CyberRange joue un rôle crucial en fournissant une plateforme pour simuler des attaques et tester des configurations de défense. Les ressources matérielles comprennent également des serveurs haute performance, des switches programmables, et divers outils logiciels nécessaires pour déployer et gérer le réseau SDN et les stratégies de MTD. Ces outils permettent de créer un environnement de test réaliste où les scénarios d'attaque peuvent être simulés et analysés en temps réel. En outre, des équipements supplémentaires tels que des routeurs, des pare-feu et des systèmes de détection d'intrusion sont également disponibles pour renforcer l'infrastructure de test.

4.3.5 Logiciels et Outils

Le projet utilise une gamme de logiciels et d'outils spécialisés pour la gestion et l'analyse des réseaux. Ces outils incluent des plateformes de simulation de réseau, des environnements de développement intégré (IDE) pour le codage et des suites logicielles pour l'analyse des performances et la détection des anomalies. L'accès à ces ressources logicielles est essentiel pour effectuer des tests approfondis et obtenir des résultats précis.

4.3.6 Maintenance et Support Technique

Un support technique continu est disponible pour garantir que toutes les ressources matérielles et logicielles fonctionnent correctement. En cas de défaillance ou de problème technique, une équipe de support dédiée intervient rapidement pour résoudre les problèmes et minimiser les interruptions. Ce support est crucial pour maintenir la continuité des travaux et assurer que les délais du projet sont respectés.

4.4 Contraintes et Limitations

4.4.1 Temps

Le projet est contraint par un délai serré de quatre semaines, imposant une gestion efficace du temps pour couvrir tous les aspects de la recherche, du développement, et de la mise en œuvre. Chaque semaine doit être planifiée de manière stratégique pour maximiser la productivité et assurer que toutes les étapes critiques du projet soient complétées dans les temps. Des jalons hebdomadaires sont définis pour suivre les progrès et ajuster les plans si nécessaire.

4.4.2 Gestion du Temps

Une planification détaillée est cruciale pour s'assurer que toutes les tâches sont accomplies dans les délais impartis. Un calendrier de projet précis est établi, avec des deadlines claires pour chaque étape. Des réunions hebdomadaires permettent de suivre les progrès, de discuter des défis rencontrés et de réajuster les priorités si nécessaire. La gestion du temps est facilitée par l'utilisation d'outils de gestion de projet qui permettent de visualiser les tâches et les échéances de manière efficace.

4.4.3 Équilibrage des Charges de Travail

Pour éviter la surcharge de travail et assurer une progression constante, les tâches sont réparties de manière équilibrée entre les membres de l'équipe. Des périodes de travail intense sont alternées avec des périodes de révision et de validation pour garantir une qualité constante du travail produit. L'équilibrage des charges de travail permet également de maintenir un niveau de motivation élevé au sein de l'équipe.

4.4.4 Ressources

En l'absence d'un budget spécifique, notre projet doit optimiser l'utilisation des ressources disponibles sur le campus. Cela inclut une planification stratégique pour maximiser l'utilisation des équipements et des logiciels disponibles sans compromettre la qualité du travail. Les contraintes budgétaires nécessitent une approche innovante pour exploiter au mieux les ressources existantes, y compris la recherche de solutions open source et l'utilisation de plateformes de test collaboratives. La gestion rigoureuse des ressources humaines et matérielles est essentielle pour assurer l'efficacité du projet et minimiser les coûts.

4.4.5 Optimisation des Ressources

Une attention particulière est portée à l'optimisation des ressources disponibles. Cela inclut l'utilisation efficace des équipements existants et la recherche de solutions alternatives lorsque cela est possible. Par exemple, des logiciels open source sont utilisés pour réduire les coûts tout en offrant des fonctionnalités robustes. L'optimisation des ressources nécessite également une coordination étroite avec les départements concernés pour assurer la disponibilité des équipements nécessaires.

4.4.6 Ingéniosité et Innovation

Face aux limitations budgétaires, l'équipe adopte une approche innovante pour résoudre les problèmes. Cela inclut la recherche de solutions créatives et l'utilisation de technologies émergentes pour surmonter les défis. L'ingéniosité des membres de l'équipe est mise à profit pour développer des solutions efficaces et économiques, garantissant ainsi que le projet progresse malgré les contraintes.

4.4.7 Complexité Technique

La mise en œuvre du MTD dans un environnement SDN implique une complexité technique élevée. La gestion des configurations dynamiques, la rotation des cibles et l'intégration de leurres nécessitent une expertise avancée et une coordination minutieuse. Les défis techniques incluent la compatibilité des différents composants, la gestion des dépendances et la validation des configurations réseau dans des scénarios réalistes.

4.4.8 Gestion de la Complexité

Pour gérer la complexité technique, l'équipe adopte une approche méthodique et structurée. Cela inclut la documentation détaillée de chaque étape du processus, la création de plans de test exhaustifs et l'utilisation de méthodologies agiles pour s'adapter rapidement aux changements et aux défis imprévus. La gestion de la complexité technique nécessite également une formation continue et une collaboration étroite avec les experts du domaine.

4.4.9 Validation et Tests

Des tests rigoureux et des validations sont effectués à chaque étape pour assurer que les configurations dynamiques fonctionnent comme prévu. Cela inclut des tests de performance, des tests de sécurité et des simulations d'attaques pour évaluer l'efficacité des stratégies de MTD. Les résultats des tests sont analysés en détail pour identifier les points faibles et apporter les ajustements nécessaires.

4.4.10 Sécurité et Confidentialité

Assurer la sécurité et la confidentialité des données lors des simulations est crucial. Les tests doivent être effectués dans un environnement contrôlé pour éviter toute fuite de données sensibles. Des mesures de sécurité strictes doivent être mises en place pour protéger les informations personnelles et professionnelles des étudiants et du personnel impliqués.

4.4.11 Mesures de Sécurité

Des protocoles de sécurité stricts sont établis pour protéger les données sensibles. Cela inclut l'utilisation de systèmes de chiffrement, l'authentification multi-facteurs et des contrôles d'accès rigoureux pour limiter l'accès aux informations critiques. Les environnements de test sont isolés pour éviter toute interférence avec les réseaux de production.

4.4.12 Confidentialité des Données

La confidentialité des données est assurée par des politiques strictes de gestion des informations. Les données personnelles et professionnelles sont traitées avec le plus grand soin, et des audits réguliers sont effectués pour vérifier la conformité aux normes de sécurité. La confidentialité des données est une priorité absolue pour garantir que les tests et les simulations ne compromettent pas les informations sensibles.

En résumé, le périmètre de notre projet est défini par son emplacement stratégique, son domaine d'application focalisé sur l'innovation en cybersécurité, et ses ressources dédiées. La gestion attentive des contraintes de temps et de ressources, combinée à une approche collaborative et à une planification rigoureuse, est cruciale pour le succès du projet.

5 DESCRIPTION & GESTION DE PROJET

Le **MTD : SDN** (Moving Target Defense : Software-Defined Networking) est une stratégie de sécurité informatique innovante qui combine les principes de la défense en mouvement avec les fonctionnalités du réseau défini par logiciel (SDN). Cette approche vise à rendre les systèmes informatiques plus résistants aux attaques en introduisant une dynamique constante dans leur infrastructure réseau. La rotation des cibles, la diversification des services et l'utilisation de leurres pour tromper les attaquants sont les principaux mécanismes utilisés. En exploitant la flexibilité offerte par l'architecture SDN, le MTD SDN permet une gestion centralisée des politiques de sécurité et une adaptation rapide aux menaces émergentes, offrant ainsi une protection accrue contre les cyberattaques.

5.1 Phases du Projet

Phase 1 : Recherche et Acquisition de Connaissances

Au cours de la première semaine, nous avons entrepris plusieurs activités clés pour poser les bases de notre projet. Dans un premier temps, nous avons organisé une séance de brainstorming pour définir les grandes lignes de notre approche et identifier les axes de recherche prioritaires. Ensuite, nous avons entamé la recherche de littérature pertinente, incluant des articles académiques, des livres blancs et des études de cas sur des implémentations réussies de MTD SDN dans diverses industries. Nous avons résumé ces articles pour extraire les informations les plus pertinentes et les intégrer dans notre base de connaissances collective.

Ces activités nous ont permis de comprendre les principes fondamentaux du MTD SDN, ses applications potentielles et les meilleures pratiques pour sa mise en œuvre. Nous avons également exploré les technologies sous-jacentes, telles que les algorithmes de randomisation des cibles, les techniques de diversification des services et l'utilisation des leurres dans un environnement SDN. Cette phase nous a également permis de créer une base solide de connaissances collectives, facilitant ainsi la mise en œuvre pratique ultérieure.

Phase 2 : Consolidation des Recherches et Planification

Durant la deuxième semaine, nous avons poursuivi nos recherches sur les différents aspects techniques du MTD SDN. En particulier, nous avons approfondi nos connaissances sur la randomisation des adresses IP, des ports et des chemins. Nous avons également effectué une recherche sur les API nécessaires pour la mise en place du SDN. En parallèle, nous avons consolidé nos recherches individuelles en fusionnant nos résultats et en identifiant les lacunes à combler. Nous avons travaillé en étroite collaboration pour élaborer une stratégie commune et avons commencé à envisager des scénarios de tests pour évaluer la solution. En attente des accès au CyberRange de l'école, nous avons concentré nos efforts sur la planification détaillée des étapes à suivre une fois les ressources disponibles. Cette planification comprenait la conception de l'architecture réseau SDN, la configuration des politiques de sécurité dynamiques, et la préparation des environnements de test pour simuler des attaques et évaluer l'efficacité de la défense MTD.

Phase 3 : Mise en Œuvre et Tests

Lors de la troisième semaine, nous avons accédé au CyberRange et avons immédiatement commencé à mettre en œuvre la solution MTD SDN. En utilisant notre plan préalablement établi, nous avons rapidement adapté la configuration du réseau pour intégrer les mécanismes de défense MTD. Nous avons configuré les contrôleurs SDN pour gérer dynamiquement les flux réseau et utiliser des algorithmes de randomisation pour déplacer les cibles. De plus, nous avons déployé des leurres et des services diversifiés pour tromper les attaquants potentiels. Malgré les défis techniques rencontrés, notre collaboration étroite et notre répartition efficace des tâches ont permis une progression significative dans la mise en place de la solution sur le CyberRange de l'école.

5.2 Organisation et Coordination du Groupe

Notre groupe s'est organisé de manière efficace pour mener à bien ce projet. Au cours de la première semaine, nous avons pris connaissance du projet en discutant des objectifs et des attentes. Chacun d'entre nous a pu partager ses idées et perspectives initiales sur la solution MTD SDN. Cette approche collaborative a permis de rassembler une diversité de points de vue et de compétences, enrichissant ainsi notre réflexion collective.

Durant la deuxième semaine, nous avons consolidé nos recherches individuelles en fusionnant nos résultats et en identifiant les lacunes à combler. Nous avons travaillé en étroite collaboration pour élaborer une stratégie commune et avons commencé à envisager des scénarios de tests pour évaluer la solution. En attendant les accès au CyberRange de l'école, nous avons concentré nos efforts sur la planification détaillée des étapes à suivre une fois les ressources disponibles.

Enfin, lors de la troisième semaine, nous avons accédé au CyberRange et avons immédiatement commencé à mettre en œuvre la solution MTD SDN. En utilisant notre plan préalablement établi, nous avons rapidement adapté la configuration du réseau pour intégrer les mécanismes de défense MTD. Malgré les défis techniques rencontrés, notre collaboration étroite et notre répartition efficace des tâches ont permis une progression significative dans la mise en place de la solution sur le CyberRange de l'école. Durant ces trois semaines, notre groupe s'est réuni quotidiennement à l'ESAIP, l'école dirigeant ce projet.

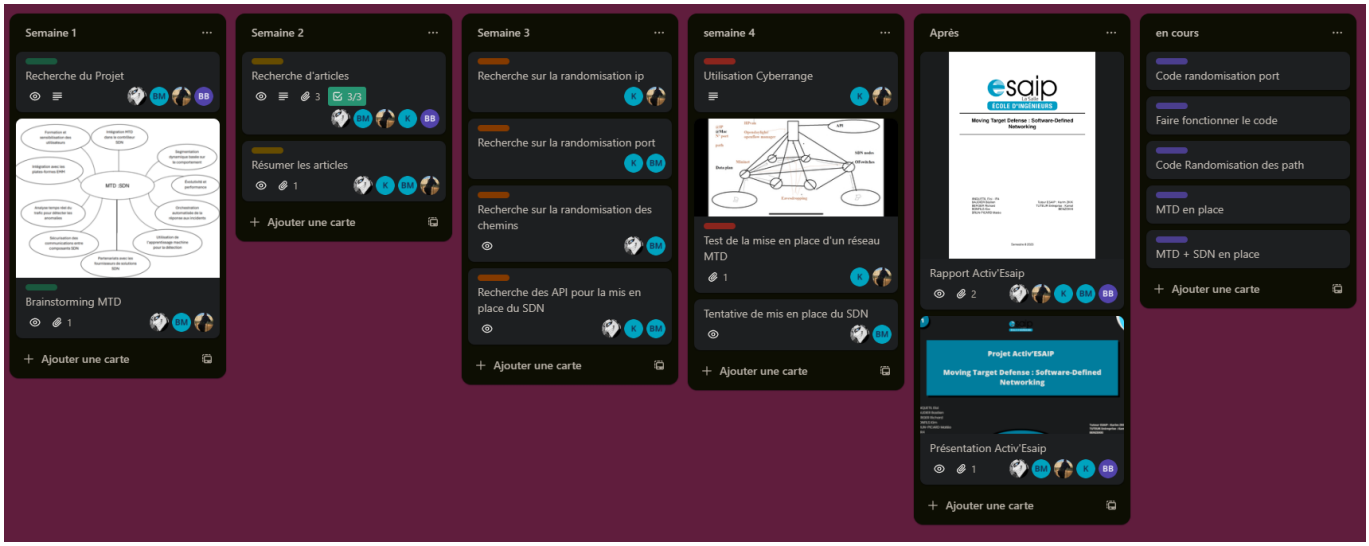

FIGURE 1 – Planification et organisation du projet sur Trello

Points Clés de la Gestion de Projet

Les principaux points clés de notre gestion de projet incluent :

1. **Compréhension approfondie des objectifs dès le départ** : Dès les premières réunions, nous avons clarifié les objectifs du projet et les attentes de chaque membre de l'équipe, ce qui a permis une direction claire et une vision partagée.
2. **Consolidation des recherches individuelles** : En partageant et en fusionnant nos résultats de recherche, nous avons formé une base solide de connaissances collectives. Cette synergie a enrichi notre compréhension globale et notre capacité à résoudre des problèmes complexes.
3. **Planification minutieuse des étapes à suivre** : Avant d'accéder au CyberRange, nous avons élaboré un plan détaillé couvrant la conception de l'architecture réseau, la configuration des politiques de sécurité dynamiques, et la préparation des scénarios de test. Cette planification rigoureuse a permis une mise en œuvre plus fluide et efficace.
4. **Utilisation efficace du temps disponible** : En maintenant des réunions régulières de suivi et des sessions de formation supplémentaires, nous avons maximisé notre productivité et notre coordina-

tion. Cette organisation a assuré que chaque membre de l'équipe restait informé des progrès et des défis, permettant des ajustements rapides et efficaces.

5. **Mise en œuvre collaborative de la solution MTD SDN** : Une fois l'accès au CyberRange obtenu, notre travail en équipe a permis une intégration rapide et efficace des mécanismes de défense MTD. Chaque membre a apporté ses compétences spécifiques, facilitant la résolution des problèmes techniques et l'optimisation des configurations réseau.

Suivi de la Performance

Pour surveiller la performance de notre projet, nous avons défini plusieurs indicateurs clés :

— **Respect des délais** : Nous avons suivi régulièrement l'avancement par rapport au planning initial, en vérifiant que chaque étape du projet respectait les délais définis. Cela nous a permis d'identifier rapidement les retards et de prendre des mesures correctives.
— **Qualité du travail** : Nous avons évalué la pertinence et l'exhaustivité de nos recherches, ainsi que la précision de notre mise en œuvre de la solution MTD SDN. Cette évaluation qualitative nous a aidés à maintenir un haut niveau de rigueur et de fiabilité dans notre travail.
— **Gestion des ressources** : Nous avons surveillé de près l'utilisation des ressources, notamment le temps et les compétences requises. Cette gestion efficace des ressources a garanti que nous tirions le meilleur parti des ressources disponibles, évitant les gaspillages et maximisant l'efficacité.
— **Surveillance des risques** : Nous avons maintenu une vigilance constante sur les risques potentiels, en identifiant les obstacles éventuels et en mettant en place des stratégies d'atténuation pour minimiser leur impact sur le projet. Cette approche proactive a permis de réduire les interruptions et de maintenir une progression continue.

6 DESCRIPTION DE LA WORKZONE

6.1 Mode d'Emploi de la Workzone

La workzone est un environnement de simulation au sein d'un cyberrange, conçu pour tester et valider des techniques avancées de sécurité informatique, telles que le Moving Target Defense (MTD). L'objectif principal est de simuler un environnement réseau dynamique et réaliste où les adresses IP, les ports, et les chemins peuvent être modifiés régulièrement pour compliquer la tâche des attaquants.

Utilisation de la Workzone :

1. **Initialisation :**
   — Vérifiez que tous les équipements (serveurs, routeur/switch, contrôleur MTD, serveur de logs) sont configurés et opérationnels.
   — Déployez les services critiques sur les serveurs cibles avec des adresses IP initiales attribuées.
2. **Déploiement des Scripts :**
   — Téléchargez et installez les scripts pour le changement d'IP, de ports, et de chemins sur le contrôleur MTD.
   — Configurez les scripts pour qu'ils se connectent aux serveurs cibles via SSH sécurisé.
3. **Configuration des Tâches Planifiées :**
   — Utilisez `crontab` pour planifier l'exécution régulière des scripts de changement d'IP, de ports, et de chemins.
   — Par exemple, configurez le script de changement d'IP pour qu'il s'exécute toutes les heures.
4. **Surveillance et Log :**
   — Configurez le serveur de logs pour collecter et stocker les journaux des changements d'IP, de ports, et de chemins.
   — Utilisez des outils de surveillance réseau pour suivre l'état des serveurs cibles et vérifier que les changements n'affectent pas la disponibilité des services.
5. **Test et Validation :**
   — Effectuez des tests de pénétration réguliers pour évaluer l'efficacité des techniques MTD.
   — Analysez les journaux et les données de surveillance pour identifier et corriger les éventuelles vulnérabilités.

6.2 Topologie Réseaux

La topologie réseau suivante décrit l'architecture de la workzone, incluant le contrôleur MTD, les serveurs cibles, le routeur/switch, et le serveur de logs.

Description Générale :

La topologie réseau est organisée de manière à permettre une gestion efficace et sécurisée des adresses IP des serveurs cibles. Chaque composant joue un rôle crucial dans l'implémentation et la gestion des techniques MTD.

Composants et Configuration :

Contrôleur MTD : Le contrôleur MTD est le cerveau de l'opération. Il gère et exécute les scripts de changement d'IP, de ports, et de chemins. C'est un serveur dédié avec une adresse IP statique, par exemple, 192.168.100.1. Il nécessite les logiciels suivants :
— **Python** pour l'exécution des scripts.
— **SSH** configuré avec des clés publiques/privées pour un accès sécurisé aux serveurs cibles.

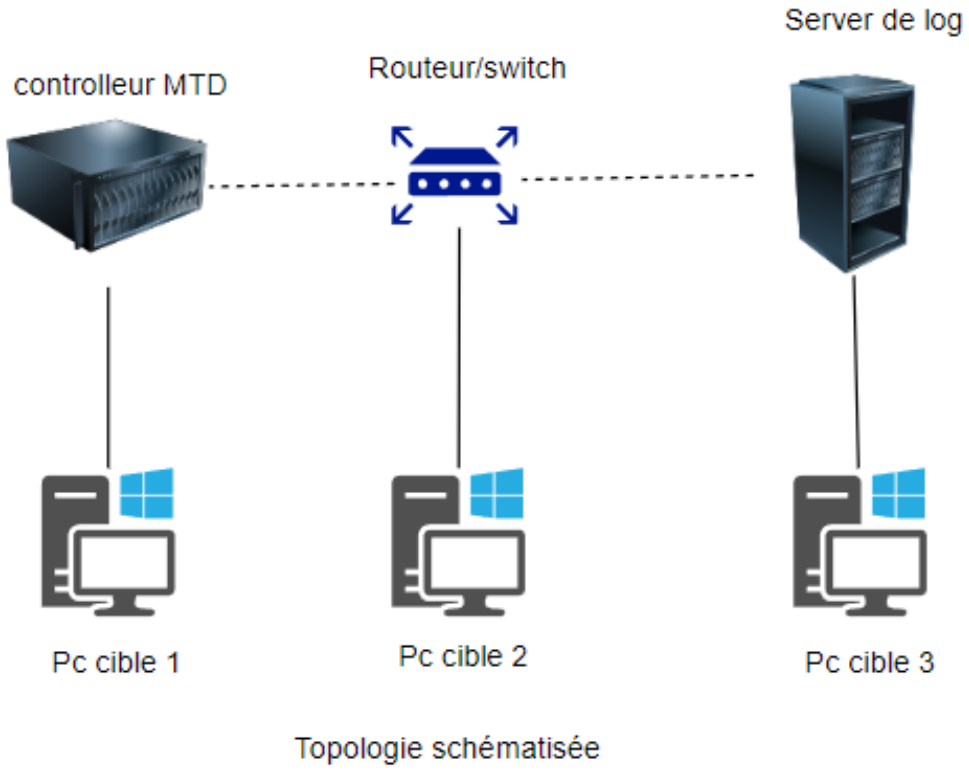

FIGURE 2 – Topologie de la Workzone

Routeur/Switch : Le routeur ou switch central assure la commutation et le routage des paquets entre les différents composants du réseau. Il est configuré pour permettre les changements dynamiques d'adresses IP des serveurs cibles. L'adresse IP de l'interface côté contrôleur MTD peut être, par exemple, 192.168.100.254.

Serveurs Cibles : Les serveurs cibles hébergent les services critiques dont les adresses IP seront modifiées régulièrement pour éviter les attaques persistantes. Chaque serveur commence avec une adresse IP initiale, par exemple, 192.168.100.10, 192.168.100.11, 192.168.100.12. Les serveurs doivent avoir SSH installé pour recevoir les commandes de changement d'IP.

Serveur de Logs : Le serveur de logs collecte et stocke les journaux des changements d'IP pour permettre des audits et des analyses. Il a une adresse IP statique, par exemple, 192.168.100.2. Il doit être configuré avec un logiciel de gestion de logs comme ELK stack ou syslog.

Pare-feu : Le pare-feu est essentiel pour sécuriser les communications entre le contrôleur MTD, les serveurs cibles, et le serveur de logs. Il doit être configuré pour autoriser uniquement le trafic SSH entre le contrôleur MTD et les serveurs cibles, empêchant ainsi tout accès non autorisé.

Fonctionnement de la Topologie :

1. **Initialisation :** Les serveurs cibles sont initialisés avec des adresses IP statiques. Le contrôleur MTD se connecte aux serveurs cibles via SSH sécurisé pour préparer l'environnement de changement d'IP.
2. **Changement d'IP Dynamique :** Le contrôleur MTD exécute des scripts à intervalles réguliers (par exemple, toutes les heures) pour changer les adresses IP des serveurs cibles. Ce processus implique

la génération d'une nouvelle adresse IP aléatoire, l'application de cette nouvelle adresse, et la mise à jour des configurations réseau.

3. **Surveillance et Logs :** Chaque changement d'IP est consigné dans le serveur de logs pour permettre une traçabilité complète. Les outils de surveillance réseau vérifient en permanence l'état des serveurs cibles pour s'assurer que les services restent disponibles malgré les changements d'IP.
4. **Sécurité :** Le pare-feu assure que seules les communications autorisées (SSH entre le contrôleur MTD et les serveurs cibles) sont permises, renforçant ainsi la sécurité de l'ensemble du réseau.
5. **Validation et Tests :** Des tests de pénétration réguliers sont effectués pour valider l'efficacité de la défense dynamique. Les journaux sont analysés pour identifier toute tentative d'intrusion ou de vulnérabilité.

Cette topologie et ces configurations permettent de créer un environnement sécurisé et dynamique où les techniques de défense par changement d'adressage peuvent être testées et évaluées de manière réaliste. L'utilisation régulière des scripts de changement d'IP, de ports, et de chemins, combinée à une surveillance et une analyse approfondies, renforce la résilience des systèmes face aux cyberattaques.

7 LES SCRIPTS DE DEFENSES DYNAMIQUE

7.1 Adressage Aléatoire IP

Dans un premier temps, nous avons réussi à trouver un code pour le changement d'adresse IP qui fonctionne de manière efficace. Le script suivant génère une nouvelle adresse IP aléatoire et l'applique aux serveurs cibles :

```
import subprocess
import random

# Fonction pour générer une nouvelle adresse IP
def generate_new_ip():
    return f"192.168.{random.randint(1, 254)}.{random.randint(1, 254)}"

# Fonction pour changer l'adresse IP d'un serveur cible
def change_ip(server):
    new_ip = generate_new_ip()
    subprocess.run(["ssh", server, f"sudo ip addr add {new_ip}/24 dev eth0"])
    subprocess.run(["ssh", server, f"sudo ip addr del {current_ip}/24 dev eth0"])
    print(f"Changed IP of {server} to {new_ip}")
    return new_ip

# Liste des serveurs cibles
servers = ["server1", "server2", "server3"]
current_ips = ["192.168.1.10", "192.168.1.11", "192.168.1.12"]  # Adresse IP actuelle des serveur

# Changer les adresses IP des serveurs cibles
for i, server in enumerate(servers):
    current_ip = current_ips[i]
    new_ip = change_ip(server)
    current_ips[i] = new_ip
```

7.2 Adressage Aléatoire des Ports

Malgré nos recherches et essais, nous n'avons pas réussi à trouver un code fonctionnel pour le changement dynamique des ports. Voici néanmoins un exemple de script que nous avons tenté d'utiliser sans succès :

```
import random
import subprocess

# Liste des services avec leurs ports par défaut
services = {
    'ssh': 22,
    'http': 80,
    'https': 443
}

# Fonction pour randomiser les ports
def randomize_ports(services):
    new_ports = {}
    for service, default_port in services.items():
        new_port = random.randint(1024, 65535)
        new_ports[service] = new_port

        # Mise à jour de la configuration des services
        if service == 'ssh':
            subprocess.run(['sudo', 'sed', '-i', f's/^#Port .*/Port {new_port}/', '/etc/ssh/sshd_
            subprocess.run(['sudo', 'systemctl', 'restart', 'ssh'])
        elif service in ['http', 'https']:
            # Mettre à jour la configuration des services web (exemple avec Nginx)
            subprocess.run(['sudo', 'sed', '-i', f's/listen .*/listen {new_port};/', f'/etc/nginx
            subprocess.run(['sudo', 'systemctl', 'restart', 'nginx'])

        print(f'{service} port changé de {default_port} à {new_port}')

    return new_ports

# Exécution de la randomisation des ports
new_ports = randomize_ports(services)
print("Nouveaux ports :", new_ports)
```

7.3 Adressage Aléatoire des Chemins

De la même manière, nous n'avons pas réussi à faire fonctionner un script pour le changement dynamique des chemins (paths). Voici un exemple de script que nous avons testé :

```
#!/bin/bash

# Liste des chemins des scripts ou exécutables
declare -A paths
paths=(
    ["/usr/local/bin/critical_script.sh"]="/usr/local/bin"
)

# Fonction pour randomiser les chemins
randomize_paths() {
    for script in "${!paths[@]}"; do
        base_dir=${paths[$script]}
        new_name=$(head /dev/urandom | tr -dc A-Za-z0-9 | head -c 13)
        new_path="$base_dir/$new_name.sh"

        # Renommer le script
```

```
        mv "$script" "$new_path"

        # Mettre à jour les configurations dépendantes
        # Exemple : mise à jour d'un cron job
        sed -i "s|$script|$new_path|g" /etc/crontab

        echo "$script déplacé à $new_path"
    done
}

# Exécution de la randomisation des chemins
randomize_paths
```

7.4 Script du Contrôleur MTD

Finalement, nous avons décidé d'adapter le code de changement d'IP au script du contrôleur MTD pour garantir son bon fonctionnement. Le script suivant est utilisé par le contrôleur MTD pour gérer les changements d'IP des serveurs cibles :

```
import subprocess
import random
import logging

# Configuration de la journalisation
logging.basicConfig(filename='/var/log/ip_change.log', level=logging.INFO)

# Fonction pour générer une nouvelle adresse IP
def generate_new_ip():
    return f"192.168.100.{random.randint(10, 254)}"

# Fonction pour changer l'adresse IP d'un serveur cible
def change_ip(pc, current_ip):
    new_ip = generate_new_ip()
    subprocess.run(["ssh", pc, f"sudo ip addr add {new_ip}/24 dev eth0"])
    subprocess.run(["ssh", pc, f"sudo ip addr del {current_ip}/24 dev eth0"])
    logging.info(f"Changed IP of {pc} from {current_ip} to {new_ip}")
    return new_ip

# Liste des pcs cibles et leurs IP initiales
pcs = ["pc1", "pc2", "pc3"]
current_ips = ["192.168.100.10", "192.168.100.11", "192.168.100.12"]

# Changer les adresses IP des pcs cibles
for i, server in enumerate(servers):
    current_ip = current_ips[i]
    new_ip = change_ip(pc, current_ip)
    current_ips[i] = new_ip
```

Cette topologie et ces configurations permettent de créer un environnement sécurisé et dynamique où les techniques de défense par changement d'adressage peuvent être testées et évaluées de manière réaliste. L'utilisation régulière des scripts de changement d'IP, combinée à une surveillance et une analyse approfondies, renforce la résilience des systèmes face aux cyberattaques.

8 FINALISATION DES IMPLEMENTATIONS

8.1 Difficultés de l'Application du Code Polymorphique

L'implémentation de la défense dynamique par changement de port et de chemin s'est avérée plus complexe que prévu. Les principales difficultés rencontrées incluent :

— **Gestion des dépendances** : De nombreux services et applications dépendent de configurations spécifiques de ports et de chemins. Modifier ces configurations dynamiquement sans interrompre les services nécessite une gestion minutieuse des dépendances. Par exemple, changer le port d'un service web nécessite de mettre à jour toutes les références à ce service, ce qui peut être complexe et sujet à des erreurs.
— **Compatibilité des systèmes** : Les systèmes et logiciels en production ne sont pas toujours conçus pour supporter des changements dynamiques de configuration. Des problèmes de compatibilité peuvent survenir lorsque les configurations sont modifiées en temps réel. Par exemple, certains services peuvent avoir des limitations sur les plages de ports qu'ils peuvent utiliser, ou des chemins d'accès statiques codés en dur.
— **Surcharge administrative** : La gestion des changements fréquents de configurations entraîne une charge administrative accrue. Cela inclut la mise à jour des scripts, la gestion des permissions et l'application des modifications de manière coordonnée. Le personnel doit également surveiller en permanence les effets de ces changements pour s'assurer qu'ils n'affectent pas la disponibilité ou la performance des services.
— **Problèmes de sécurité** : Bien que les changements dynamiques puissent améliorer la sécurité, ils introduisent également de nouveaux vecteurs d'attaque. Les scripts automatisés peuvent être ciblés par des attaquants pour introduire des modifications malveillantes. Il est essentiel de sécuriser les mécanismes de mise à jour et de surveiller les activités suspectes.
— **Complexité techniques** : Le code polymorphique est complexe a appliquer correctement et est largement en dehors du spectre de nos compétences et donc pas vraiment applicable dans notre situation.

8.2 Pourquoi ça n'a pas marché

Malgré nos efforts, les scripts pour le changement de port et de chemin n'ont pas fonctionné pour plusieurs raisons :

— **Limitations techniques** : Les scripts Bash et Python utilisés n'ont pas réussi à mettre à jour les configurations des services en temps réel sans provoquer d'erreurs ou d'interruptions. Les services critiques comme SSH et Nginx nécessitent des redémarrages pour appliquer les modifications, ce qui peut entraîner des temps d'arrêt non négligeables.
— **Problèmes de permissions** : L'exécution des scripts nécessitait des privilèges élevés (root), ce qui a compliqué l'automatisation sécurisée des changements. L'accès root étant nécessaire pour modifier les ports et les chemins, il devient difficile de garantir la sécurité de ces opérations sans introduire des vulnérabilités supplémentaires.
— **Complexité des dépendances** : Les configurations de services telles que SSH et Nginx sont fortement dépendantes de chemins statiques, rendant leur modification en temps réel non triviale. Par exemple, changer le chemin d'un script critique peut nécessiter la mise à jour de plusieurs fichiers de configuration, cron jobs, et services interconnectés.
— **Environnement de production** : Les environnements de production ont des contraintes strictes de disponibilité et de performance. Les tests réalisés dans des environnements simulés peuvent ne pas refléter toutes les conditions d'un environnement réel, ce qui peut conduire à des échecs lorsque les modifications sont déployées en production.

9 GESTION DES RISQUES

L'implémentation d'un Moving Target Defense (MTD) comporte plusieurs risques qu'il est important de prendre en compte :

- **Complexité accrue** : La mise en place d'un système de MTD demande une gestion des configurations dynamiques, des déplacements de cibles et des transformations qui peuvent être difficiles à gérer. Chaque changement doit être synchronisé et vérifié pour s'assurer qu'il n'introduit pas de nouvelles vulnérabilités ou de problèmes de compatibilité.
- **Impact sur la prévisibilité** : Les stratégies MTD visent à rendre les attaques plus difficiles en modifiant constamment les cibles. Cependant, cela peut également rendre le comportement du système moins prévisible. Par exemple, des changements fréquents de configuration peuvent entraîner des comportements inattendus dans les applications, rendant plus difficile le diagnostic et la résolution des problèmes.
- **Coût important** : La mise en place d'un MTD nécessite des investissements en temps, en ressources humaines, matérielles et en expertise importants. Les organisations doivent évaluer si les avantages en termes de sécurité l'emportent sur les coûts de mise en œuvre et de maintenance. Les coûts incluent non seulement le développement initial, mais aussi la gestion continue et la formation du personnel.
- **Contraintes de temps réel** : Dans les systèmes critiques tels que les véhicules autonomes, les contraintes de temps réel sont essentielles. Les stratégies MTD doivent trouver un équilibre entre sécurité et prévisibilité en temps réel. Par exemple, un changement de configuration ne doit pas entraîner de latence perceptible ou d'interruption dans des systèmes où le temps de réponse est critique.
- **Dépendance aux fournisseurs tiers** : Les systèmes modernes dépendent souvent de chaînes d'approvisionnement tierces et de logiciels hérités. Les stratégies MTD doivent tenir compte de ces dépendances pour éviter les vulnérabilités. Par exemple, un composant tiers peut ne pas supporter des changements fréquents de configuration, ce qui pourrait introduire des failles de sécurité ou des incompatibilités.
- **Gestion des incidents** : En cas d'incident, la complexité d'un système MTD peut compliquer la réponse rapide et efficace. Les équipes doivent être formées pour comprendre et gérer les dynamiques des configurations mouvantes. Une documentation exhaustive et des procédures de réponse bien définies sont essentielles pour minimiser l'impact des incidents.

10 Conclusion

En résumé, notre projet d'implémentation de la stratégie de Moving Target Defense (MTD) dans un environnement de Software-Defined Networking (SDN) a permis de développer et de tester des techniques innovantes de cybersécurité. Malgré des défis significatifs, tels que la gestion des dépendances et des limitations techniques, nous avons réussi à mettre en place une solution fonctionnelle pour le changement dynamique des adresses IP.

Points forts :

— **Approche collaborative** : Le travail d'équipe et la synergie entre les membres ont été essentiels pour surmonter les défis techniques et administratifs.
— **Utilisation efficace des ressources** : Nous avons optimisé l'utilisation des ressources disponibles au CyberRange, permettant ainsi une simulation réaliste et une évaluation approfondie des techniques MTD.
— **Apprentissage et développement** : Le projet a servi de plateforme d'apprentissage pratique, offrant une expérience précieuse en matière de sécurité des réseaux et de gestion de projet.

Défis rencontrés :

— **Complexité technique** : La mise en œuvre des changements dynamiques de ports et de chemins s'est avérée difficile en raison de la compatibilité des systèmes et des exigences de permissions élevées.
— **Surcharge administrative** : La gestion des modifications fréquentes et la nécessité de surveiller en permanence les effets des changements ont augmenté la charge de travail.

Gestion des risques :

— **Complexité accrue** : La gestion des configurations dynamiques et des transformations a été un défi constant, nécessitant une synchronisation et une vérification rigoureuses.
— **Impact sur la prévisibilité** : Les changements fréquents ont rendu le comportement du système moins prévisible, affectant la fiabilité et la performance.
— **Coût et ressources** : L'implémentation du MTD a exigé des investissements importants en termes de temps, de ressources humaines et matérielles.

En conclusion, bien que l'implémentation de MTD dans un environnement SDN soit complexe et exigeante, elle offre des avantages considérables en matière de cybersécurité. La solution développée renforce la résilience des systèmes face aux cyberattaques, tout en fournissant une expérience éducative précieuse pour les étudiants. La poursuite de ce type de projet nécessite une évaluation continue des risques et une adaptation des stratégies pour assurer leur efficacité et leur gestion optimale.

11 ANNEXES

11.1 Lien du Trello

Lien : `https://trello.com/b/Rqpn1z4y/activesaip`

11.2 Lien du Github

Lien : `https://github.com/Grimmjoow/MTD`