RAPPORT DE FIN DE PROJET

HYDRA

Informations sur le projet :

Nom du projet : Hydra
Domaine : Cybersécurité
Objet du projet : Entrer et prendre le contrôle (root) de plusieurs ordinateurs, afin de comprendre les enjeux de la cybersécurité dans le monde professionnel.
Commanditaire du projet : Epitech (Strasbourg)
Utilisateurs finaux : Les acteurs de ce projet.
Délais impartis et durée du projet : Deux semaines. Le projet s'est terminé en une semaine et demie, ce qui nous a permis d'aller plus loin et d'explorer d'autres types de failles.
Date du bilan : 31/05/2025
Votre rôle dans ce projet : Chef de projet
Votre rôle ou fonction au moment de l'écriture de ce bilan : Élève

Caractéristiques du projet :

Contraintes : Le projet est à réaliser sur des machines Linux, sous des distributions variées. La principale difficulté réside dans le fait de prendre le contrôle total de la machine cible, avec pour seule piste une adresse IP. La complexité du projet est assez élevée, car les acteurs n'ont pas reçu de formation préalable en cybersécurité et ne possèdent pas toujours les connaissances adéquates pour mener à bien le projet. Ce projet n'est pas à réaliser simultanément avec d'autres projets, les acteurs ont donc tout le temps nécessaire pour répondre aux problèmes posés.

Technologies utilisées : Les principales technologies employées pour réaliser les attaques sont des machines virtuelles Linux, sous la distribution Kali Linux. En effet, cette distribution permet d'accéder rapidement à des outils de cybersécurité comme *ffuf*, *Gobuster*, *John the Ripper*, etc., offrant ainsi un environnement de travail idéal.

Équipe : Le projet ne compte que deux acteurs : Noé CARABIN et Jason KOENIG.

Volume de l'application : N/A *(le projet n'est pas une application)*

Objectifs et résultats

Le principal objectif de ce projet était de rechercher, sur 7 machines virtuelles différentes, des failles permettant d'en devenir le propriétaire. Cela permet aux acteurs du projet de développer des compétences en cybersécurité, qui renforceront par la suite la sécurité des futures infrastructures sur lesquelles ils travailleront. En outre, cela leur permet également de perfectionner leur maîtrise de Linux, un système d'exploitation aujourd'hui indispensable dans le monde de la technologie.

Les résultats de ce projet sont concluants, puisque non seulement la totalité des failles sur les machines ont été découvertes, mais elles ont aussi été exploitées correctement pour en prendre le contrôle. Les deux acteurs du projet ont donc acquis les connaissances nécessaires à la réalisation de projets sérieux et sécurisés sur des environnements tels que Linux, et savent repérer et exploiter des failles de sécurité, aussi infimes soient-elles. Ces objectifs ont été dépassés, car le projet a été réalisé avant la fin du temps imparti, laissant ainsi à l'équipe le temps de poursuivre sa formation sur de nouvelles machines virtuelles.

Difficultés et solutions

Dans ce projet, divers aspects ont été problématiques et ont nécessité de l'adaptation de la part des collaborateurs :

- **Analyse d'une grande quantité de données** : En effet, une fois connecté à la machine cible, une très grande quantité de données doit être analysée pour espérer trouver les failles permettant d'accéder au compte propriétaire de la machine : *root*. Cela ralentit considérablement les acteurs du projet et aurait pu retarder son avancement.
  Solution : Utilisation d'intelligence artificielle pour traiter les grandes quantités de données, repérer ce qui est attendu (et donc insignifiant) et ce qui diffère.
- **Découverte de failles** : La découverte de failles a également été problématique, notamment sur des machines spécifiques telles que *Tatakae*. Après des heures de recherche, les failles n'étaient toujours pas identifiées.
  Solution : Utilisation de bases de données spécifiques liées à l'exploitation de bugs, comme *Searchsploit*.
- **Découverte de sous-processus automatisés** : Nombreux sont les serveurs qui utilisent de petits scripts au lancement automatique. Ces scripts, souvent écrits à la main, sont fréquemment la clé pour atteindre l'objectif du projet. Cependant,

il est rare de pouvoir les lister directement depuis leur dossier cible (*CRON*), ce qui ralentit encore la recherche d'informations.
Solution : Utilisation de *pspy64* pour observer les processus en cours d'exécution, et automatisation de cette recherche sur toutes les machines virtuelles afin de détecter les processus en arrière-plan.

- **Découverte de sous-processus automatisés** : nombreux sont les serveurs qui utilisent de petits scripts au lancement automatique, et ces scripts, souvent écrits à la main, constituent fréquemment la clé pour atteindre l'objectif du projet. Cependant, il est rare de pouvoir les lister directement depuis leur dossier cible (CRON), ce qui ralentit considérablement la recherche d'informations.
  Solution : utilisation de *pspy64* pour identifier les processus en cours d'exécution, ainsi que l'automatisation de cette recherche sur l'ensemble des machines virtuelles, afin de détecter les processus tournant en arrière-plan.

Suggestion d'amélioration :

Les deux acteurs du projet soulignent que des leçons théoriques, dispensées avant la mise en pratique, auraient pu raccourcir davantage le temps de réalisation du projet.

Eléments réutilisables :

La formation étant complète, l'intégralité de son contenu pourra être réutilisée. En effet, les connaissances apportées sont suffisantes et permettent à la fois de maîtriser les fondamentaux du fonctionnement de Linux, ainsi que les bonnes pratiques en cybersécurité. Le projet en lui-même est donc de nouveau réalisable.

Organisation du projet Hydra

Pour l'organisation, nous sommes restés sur quelque chose de simple. Le projet se composant de sept machines virtuelles, nous avons décidé de nous les répartir équitablement, en fonction des difficultés des *rooms*. Cette organisation a permis de combler les lacunes en cas de prise de retard de l'un ou de l'autre des membres de l'équipe. Cela n'a toutefois pas été nécessaire, les deux agents ayant évolué au même rythme. Cette organisation s'est donc révélée optimale.

Appréciation globale

En tant que chef de projet, j'ai trouvé que ce projet apportait de nombreux bénéfices et un important bagage technique. Il permet de compléter des connaissances essentielles pour créer et concevoir les projets futurs de manière sécurisée. Nous tirons de ce projet des leçons précieuses pour les réalisations à venir. Il serait intéressant de le reproduire pour de futurs collaborateurs.