Roméo DERRUAU
Et Chat GPT

TP Découverte Kali Linux – Bloc 3 – JOBARD Guillaume – 2024/2025 – Mewo

Objectif : Découvrir l'intérêt de sécuriser correctement une machine sous Windows ou Linux et savoir se protéger en se mettant à la place de l'attaquant via Kali Linux.

Pour redécouvrir le monde magique de Kali, mettons-nous en condition ;

- Récupérez votre VM Kali, votre plan d'adressage et vérifiez que tout est opérationnel.

Continuons notre expérimentation ;

- Sur votre machine Kali, allez dans le menu principal et cherchez l'application goldeneye. Notez dans quel dossier elle est rangée. Si elle n'est pas installée, lisez la documentation ci-dessous et faites le nécessaire.

Lors de l'installation, j'ai saisi Golden Eye dans l'invite de commande et ça m'a proposé de l'installer.
Après l'installation, voici ce qu'il ce passe.

- Lisez la documentation qui s'affiche et utilisez le programme avec une machine de votre contexte. La machine répond encore correctement après avoir exécuté le programme ? Quels sont les enjeux/dangers possibles avec une telle application ? Comment s'en protéger ? Cette autre application fait-elle la même chose ?

A mon avis, Goldeneye peut être utilisé pour effectuer une attaque de type DOS ou DDOS. Des problèmes de sécurité se posent car l'outil est utilisé pour évaluer les défenses des entreprises et former des professionnels, mais il peut également être exploité à des fins illégales par les individus malveillants. Inconscients, risquant des conséquences pour les moins informés

T50 est similaire à Goldeneye, mais ce dernier fonctionne sur plusieurs protocoles et cible la couche réseau, tandis que T50 se concentre uniquement sur le HTTP et vise la couche application. Par conséquent, Goldeneye est utilisé spécifiquement pour tester les serveurs web, tandis que T50 est utilisé pour effectuer des tests plus généraux.

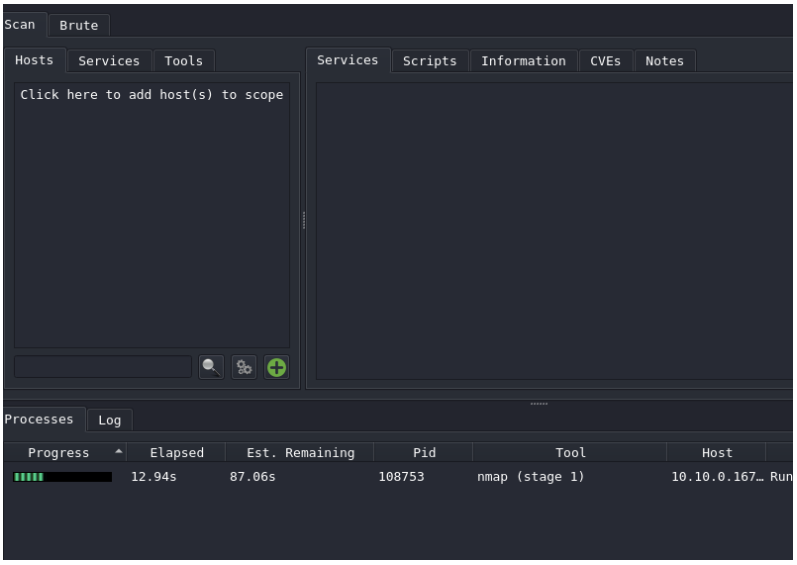
Essayons autre chose ;

- Sur votre machine Kali, allez dans le menu principal et cherchez l'application légion. Notez dans quel dossier elle est rangée. Si elle n'est pas installée, lisez la documentation ci-dessous et faites le nécessaire.

Légion est dans le dossier 1-information et gathering et 2-vulnérability analysis

- Lisez la documentation, expérimentez là avec les machines de votre contexte. Quels sont les enjeux/dangers

possibles avec une telle application ?



L'automatisation des tests de pénétration par Légion permet de gagner du temps pour les professionnels de la sécurité et de former les futurs experts. Cependant, comme tout outil, il comporte des risques, notamment celui d'être utilisé par des individus malveillants pour exploiter les vulnérabilités des systèmes tiers à des fins profitables.

Enfin ;

- Tirez des conclusions sur ce que vous venez de découvrir, documentez ce TP et rendez-le sur Moodle dans les délais indiqués. Le barème reposera sur la qualité de votre rendu, orthographe, rédaction, explications, illustration…

En conclusion, des outils dangereux pour les infrastructures informatiques sont facilement accessibles et simples à utiliser. Il est crucial de prendre conscience des risques et de mettre en place des mesures de protection, telles que mises à jour, pare-feu, proxy, etc. Mieux vaut prévenir que guérir, car la menace peut venir de partout.