Mr JACQUEMIN

18/11/2024

Compte rendu TP9

Attaque par DoS – Déni de service

GoldenEye

TEWES Arnaud
BTS SIO SISR 2EME ANNÉE

Introduction

Dans ce TP, nous avons expérimenté une attaque par DoS (déni de service) grâce à l'application GoldenEye sous Kali Linux. Une attaque par DoS simule des centaines ou milliers de connexions simultanément et fonctionne comme un embouteillage visant à rendre inaccessible un site internet, un équipement (un serveur) pour les utilisateurs.

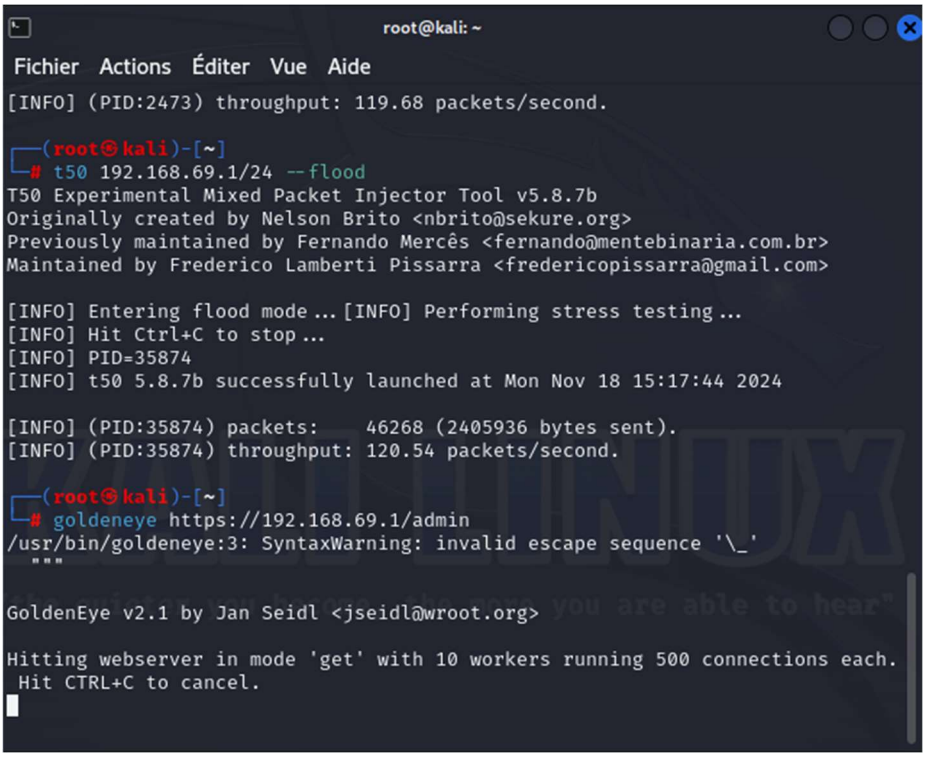
GoldenEye est utilisé pour test des serveur web (http/https) afin de tester leurs résistances, voici les tests que nous avons réalisé :

1. La machine répond encore correctement après avoir exécuté le programme ?

Je n'ai pas réussi à l'expérimenter directement car mon Kali Linux plantait à chaque fois que j'essayais de lancer le logiciel sur l'interface web de mon Stormshield.

GoldenEye est censé simuler énormément de connexions en même temps sur un serveur web pour tenter de faire tomber cet équipement et le rendre inutilisable (il teste la résistance d'un serveur web). Dans la pratique, l'interface web de mon Stormshield après l'attaque est censée être inaccessible à la connexion et ses performances (utilisations disque, CPU, RAM) en seraient grandement affecté provoquant un arrêt de ses fonctions

Ce dernier doit redémarrer pour retrouver un fonctionnement normal. Cela rendrait le service indisponible pendant un certain temps.



2. Quels sont les enjeux / dangers possibles avec une telle application ?

Avec une telle application, les enjeux / danger possibles sont :

Une indisponibilité d'un serveur web ou d'un équipement réseau : Les attaques DoS visent à rendre un site web ou un service indisponible, ce qui peut entrainer une perte de client et de revenu (par exemple pour un site de shopping).

Induire des couts de récupération : Restaurer le service après une attaque DoS peut entrainer des frais importants en termes de temps et de personnel requis et bloqué pour régler le souci.

Saturation de la bande passante : Une attaque DoS peut saturer la bande passante, affectant les autres services et utilisateurs du réseau.

Impact sur la réputation : Les interruptions de service fréquentes peuvent nuire à la réputation de l'entreprise et à la confiance des clients.

3. Comment s'en protéger ?

Pour s'en protéger, il existe plusieurs méthodes qui permettent de limiter l'impact de ce type d'attaque ou pour le bloquer complètement. Pour se protéger, nous pouvons utiliser :

Pare-feux avec IDS/IPS : Utiliser des pare-feux équipés de détection (IDS) et prévention d'intrusions (IPS) pour surveiller et bloquer les attaques par déni de service.

Rate Limiting : Mettre en place des limites de taux pour contrôler le nombre de requêtes qu'un serveur peut recevoir d'une même adresse IP dans un temps donné

HAProxy (répartition de charge) : Utiliser HAProxy pour répartir la charge entre plusieurs serveurs, assurant ainsi la continuité du service même en cas de fortes demandes (comme pour un DoS)

Surveillance active : Mettre en place des outils de monitoring (comme PRTG vu en cours avec Mr ROTH) pour détecter rapidement une activité suspecte.

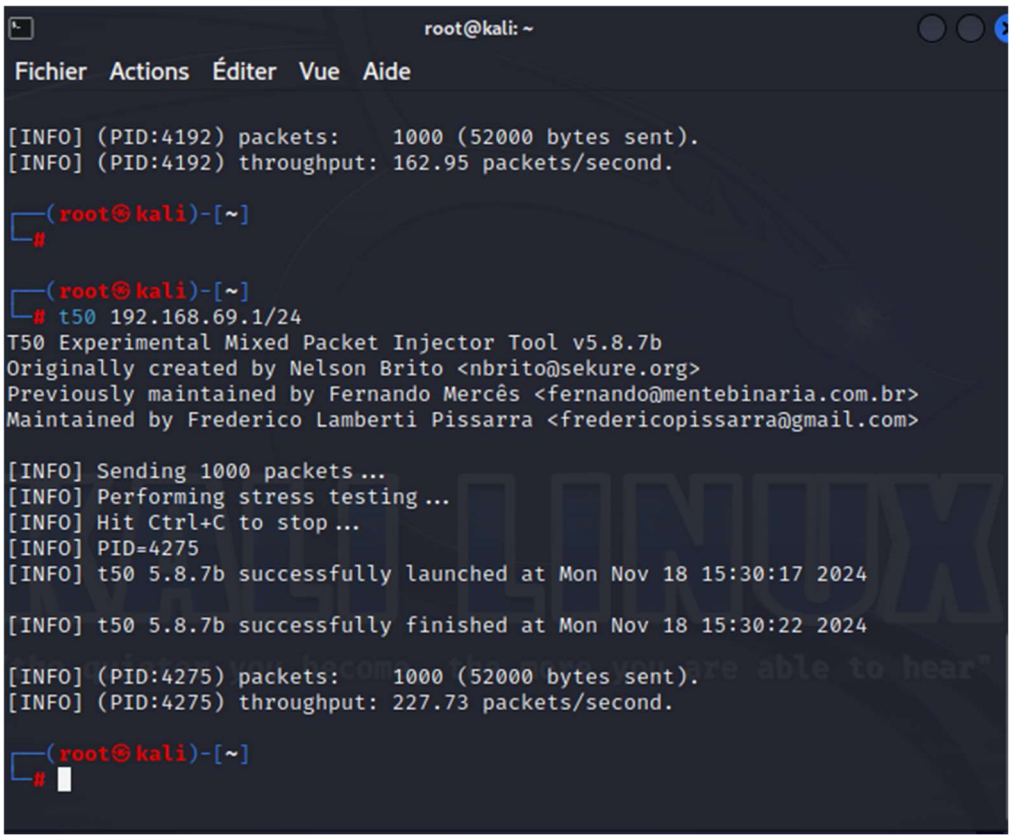
4. **L'application T50 fait-elle la même chose que l'application Goldeneye ? Expérimentez aussi avec cette application et décrivez-la brièvement**

T50 est un outil de stress test du réseau capable de lancer des attaques DoS en utilisant différents types de paquets (TCP, UDP, ICMP, etc...). Contrairement à GoldenEye, qui se concentre sur les attaques http/HTTPS, T50 peut créer un trafic malveillant plus diversifié, ciblant plusieurs couches du modèle OSI et pouvant cibler plusieurs hôtes d'un réseau en même temps en ciblant un port en particulier par exemple.

Comparaison :

GoldenEye : Principalement utilisé pour les tests de charge HTTP, visant à surcharger les serveurs web.

T50 : Plus polyvalent, capable de lancer des attaques DoS utilisant différents protocoles réseau pour tester la résistance d'un réseau



Je l'ai donc lancé sur une machine de mon réseau (ici mon Stormshield) pour voir ce que l'application peut engendrer comme souci.

Nous pouvons voir la courbe de performance lors du stress test qui augmente légèrement :

5) Quels sont les enjeux / dangers possibles avec une telle application ?

Legion est une application d'analyse de réseau utilisée pour effectuer des audits de sécurité afin de trouver des failles ou des services exposés dans un part informatique.

Les risques sont :

- Legion peut permettre à un attaquant de découvrir les machines actives et les services en cours d'exécution et vulnérables sur un réseau et d'en créer une cartographie (comme avec nmap, d'ailleurs l'application utilise nmap pour scanner le réseau) pour lui donner une vision claire de l'infrastructure

- Une fois les services identifiés (par un exemple un service FTP avec de faible mot de passe) un attaquant pourrait exploiter des vulnérabilités pour obtenir un accès non autorisé et induire à la compromission des données.

- Les informations collectées par Legion peuvent être utilisées pour lancer des attaques ciblées, comme l'exploitation d'une vulnérabilité.

Legion peut aussi être utiliser à des fins légitime pour effectuer des tests d'intrusion (ou pen-test) et de permettre aux administrateurs d'identifier les failles dans leurs propres parcs informatiques AVANT qu'elles ne soient exposées sur internet

Comme tout outil de ce type, Legion peut être utilisé de manière illégale pour mener des attaques contre des réseaux tiers. C'est pourquoi son usage doit être strictement limité à des environnements pour lesquels on a une autorisation explicite.

Conclusion

Ce TP a permis de se plonger dans l'utilisation de trois outils majeurs de tests réseau disponibles sur Kali Linux : GoldenEye, T50, et Legion. Ces outils, bien qu'efficaces dans un cadre légitime, montrent également l'importance de protéger les systèmes face aux menaces auxquels ils peuvent être contraint.

Pour se protéger efficacement, il est essentiel de configurer correctement ses équipements de sécurité (pare-feu avec IPS/IDS, limitations de connexions, mises à jour régulières) et de réaliser des audits réguliers pour essayer de résister à tous ces types d'attaques.

Cette exploration a aussi montré que ces outils sont à double tranchant. Bien qu'ils soient des alliés précieux dans un cadre pédagogique ou professionnel, leur puissance en fait également des armes redoutables entre les mains d'attaquants mal intentionnés. L'éthique et la légalité de leur utilisation est un impératif.