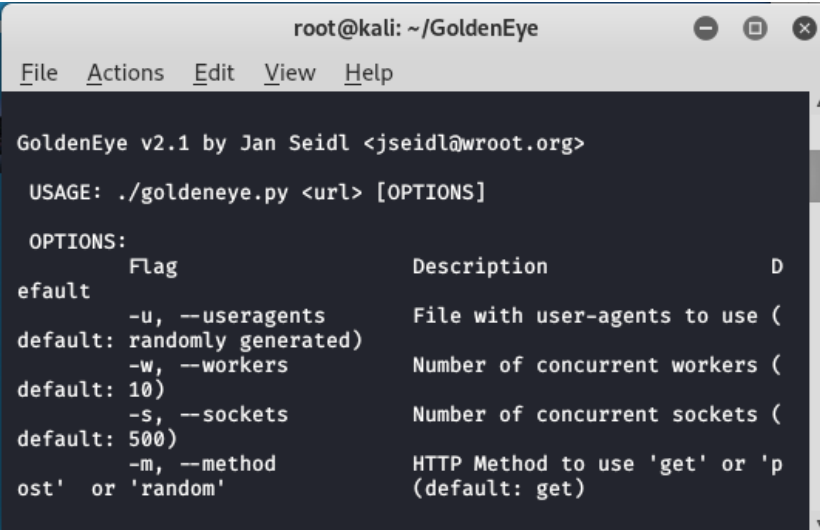


TP Découverte Kali Linux – Bloc 3 – GOMES Tiago – 2024/2025 – Mewo

L'outil Goldeneye n'est plus maintenue alors j'ai fait des recherches sur son fonctionnement pour répondre à la question ci-dessous.

On exécute le script py avec `./` suivi du nom du script dans notre cas `goldeneye.py`, on ajoute les paramètres `-h` pour comprendre comment utiliser le script.

```
./goldeneye.py -h
```



```
root@kali: ~/GoldenEye
File Actions Edit View Help

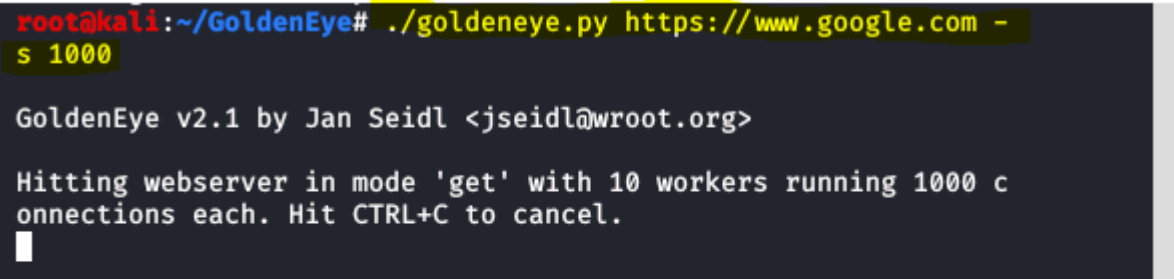
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

USAGE: ./goldeneye.py <url> [OPTIONS]

OPTIONS:
  Flag                Description
  default: randomly generated
  -u, --useragents      File with user-agents to use (
  default: 10)          Number of concurrent workers (
  -w, --workers          Number of concurrent sockets (
  default: 500)         HTTP Method to use 'get' or 'p
  -s, --sockets          (default: get)
  -m, --method
  ost' or 'random'
```

Sur le résultat de la commande nous comprenons que pour exécuter le script il faut utiliser la base `./goldeneye.py` plus le lien du site cible à la place de `<url>` avec l'option `-s` pour choisir le nombre de sockets (point de connexion entre deux machines dans notre cas réseaux) puis le nombre 1000 par exemple.

```
./goldeneye.py https://www.google.com -s 1000
```



```
root@kali: ~/GoldenEye# ./goldeneye.py https://www.google.com -
s 1000

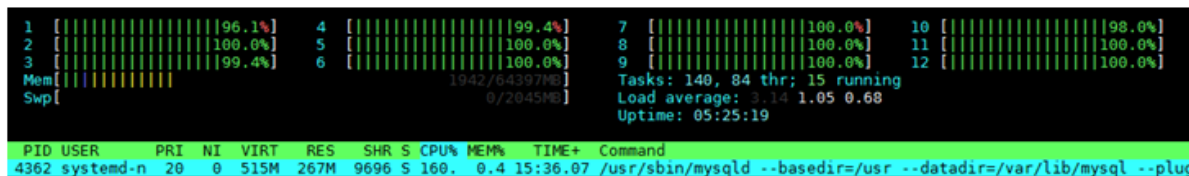
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 10 workers running 1000 c
onnections each. Hit CTRL+C to cancel.
█
```

Si l'on veut annuler ou arrêter l'attaque, il suffit de faire `CTRL+C`. Nous pouvons pour voir l'attaque utiliser un outil comme Wireshark.

La machine affectée voit ces ressources systèmes augmenter de manière significative comme sur l'exemple ci-dessous.

TP Découverte Kali Linux – Bloc 3 – GOMES Tiago – 2024/2025 – Mewo



Ce qui peut entraîner une indisponibilité voire une panne des services du serveur.

L'utilisation du script Goldeneye présente des enjeux et des dangers importants, surtout dans un contexte de cybersécurité. Installer ce genre de logiciel est à la portée de tout le monde, une simple commande dans un terminal suffit, accompagnée d'un tutoriel en ligne de quelques minutes. Cela signifie que même des utilisateurs peu expérimentés peuvent y avoir accès.

Pour une personne avec des compétences limitées en informatique, ces outils pourraient ne pas causer de dommages significatifs. Cependant, entre les mains d'un individu ayant une bonne maîtrise technique, ces logiciels peuvent devenir des armes redoutables, particulièrement contre des entreprises disposant de services en ligne. Un attaquant malveillant pourrait exploiter ces outils pour perturber des systèmes ou voler des données sensibles.

Pour se protéger de telles menaces, il est crucial d'utiliser des outils de surveillance et des logiciels de sécurité adaptés. Cela inclut des pare-feux, des systèmes de détection d'intrusion (IDS), ainsi que la mise à jour régulière des systèmes pour corriger les vulnérabilités potentielles.

T50 et GoldenEye sont tous deux des outils utilisés pour les tests de pénétration et les attaques par déni de service. T50 est destiné à tester la résilience des réseaux en simulant un trafic massif, tandis que GoldenEye se concentre sur les serveurs web et les applications web en générant un grand nombre de requêtes. Bien qu'ils aient des objectifs similaires, leur application est adaptée à des contextes légèrement différents. En résumé, T50 est plus général tandis que GoldenEye est spécialisé dans les attaques contre les serveurs web.

Legion est un outil de reconnaissance réseau grâce à certains modules complémentaires. Legion permet d'identifier les diverses failles sur la cible.

Les enjeux et dangers liés à l'utilisation de Legion sont significatifs. En premier lieu, si l'outil est utilisé de manière malveillante, il peut permettre des reconnaissances illégales sur des réseaux, violant ainsi la confidentialité des systèmes. De plus, Legion peut révéler des vulnérabilités qui, si exploitées par des attaquants, peuvent compromettre les données et la sécurité des systèmes. Les scans effectués peuvent aussi affecter les performances du réseau en générant un trafic important. Enfin, les informations collectées doivent être soigneusement protégées pour éviter les fuites de données sensibles. Pour minimiser ces risques, il est essentiel d'utiliser Legion dans un cadre légal et avec des autorisations appropriées.

TP Découverte Kali Linux – Bloc 3 – GOMES Tiago – 2024/2025 – Mewo

En conclusion, les outils comme Goldeneye, T50, GoldenEye et Legion, bien que puissants pour les tests de pénétration, peuvent poser des risques importants s'ils sont utilisés de manière malveillante. Ils peuvent révéler des vulnérabilités ou perturber les systèmes, mettant en danger la sécurité des données et des performances réseau. Pour minimiser ces risques, il est crucial d'utiliser ces outils de manière légale, avec des mesures de sécurité appropriées et une gestion rigoureuse des informations collectées.

TP Découverte Kali Linux – Bloc 3 – GOMES Tiago – 2024/2025 – Mewo

Liens :

- <https://www.geeksforgeeks.org/goldeneye-ddos-tool-in-kali-linux/>
- <https://www.youtube.com/watch?v=Zu5YTmwp2Ik>
- <https://www.chatgpt.com>