TP découverte Kali / Linux 2

Installation de golden eye :

Pour installer golden eye il faut faire cette commande sur la machine Kali :

```
sudo apt install goldeneye
```

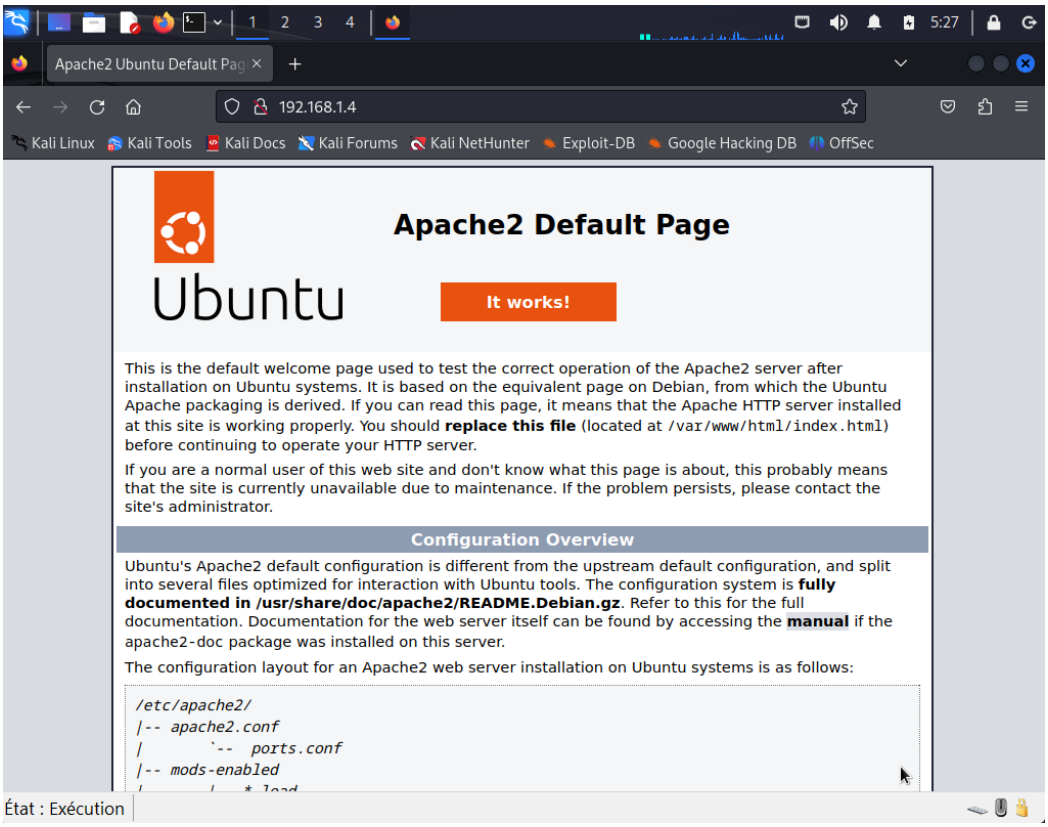
Si l'application ne s'installe pas correctement il faut récupérer le dossier d'installation sur ce site :

https://www.geeksforgeeks.org/goldeneye-ddos-tool-in-kali-linux/

Une fois goldeneye installé il faut avoir une VM Linux avec une page web, nous avons déjà une machine Linux de prête. Sur celle-ci on a installé apache avec cette commande :

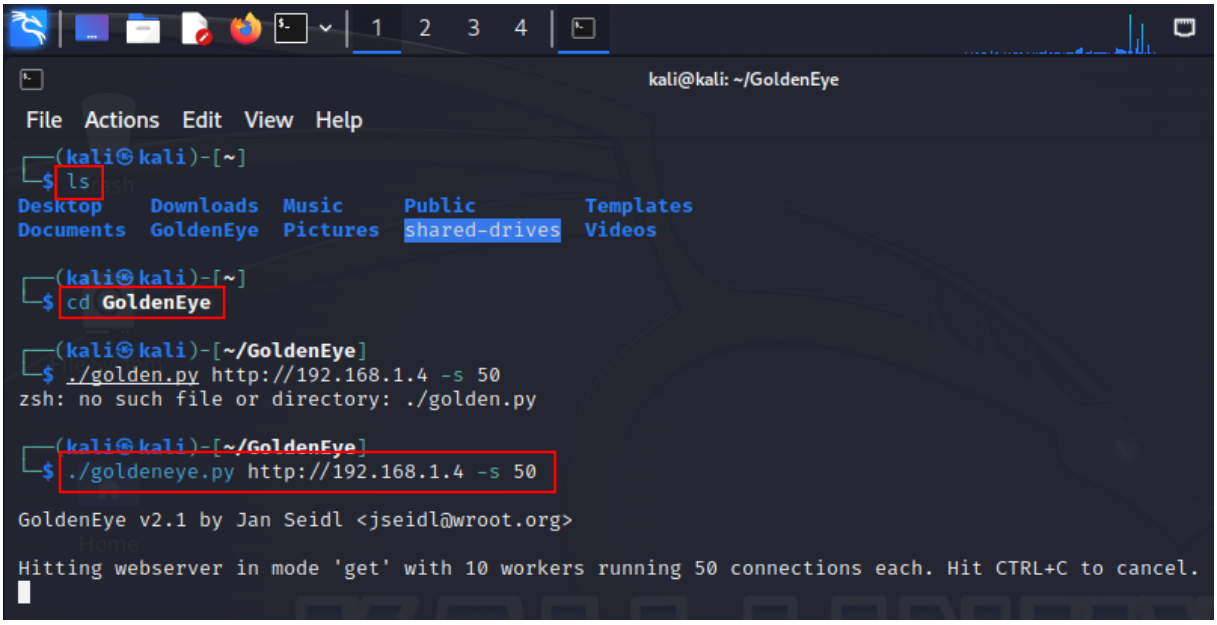
```
sudo apt install apache2
```

On voit que notre page Apache fonctionne.



On peut maintenant commencer à utiliser golden eye.

Pour utiliser Goldeneye on doit se rendre dans le dossier puis exécuter la commande :



A cette étape je me suis rendu compte que mes attaques ne donnaient rien de concluant. J'ai donc éteint :

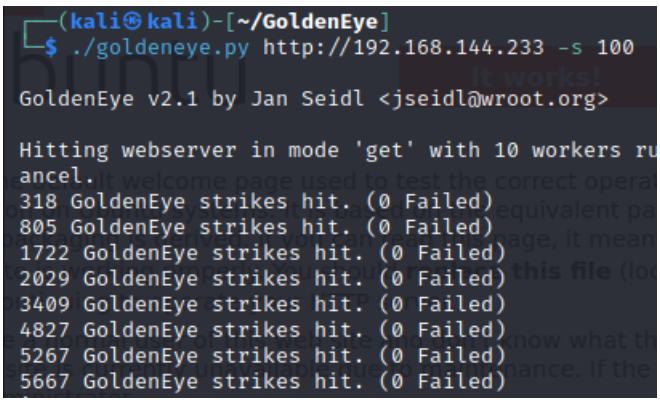
- Mon pare-feu
- Mon serveur Windows

J'ai mis mes VM Kali-Linux et Linux avec Apache2 en WAN (DHCP) pour qu'elles soient interconnectées. Ensuite j'ai réessayé mais aucunes des deux avaient internet. J'ai donc fait un :

```
Sudo dhclient eth0
```

Pour avoir une nouvelle IP sur les 2 machines. Une fois cela fait les 2 machines avaient internet et pouvaient communiquer.

J'ai donc relancé une attaque avec goldeneye.



Une fois l'attaque réalisée, la page apache met énormément de temps à recharger ou alors elle ne répond plus du tout.

L’utilisation de Goldeneye comporte des dangers et enjeux :

- Il permet de mener des attaques DoS contre des sites web ou des réseaux ne nous appartenant pas ce qui est illégal
- Les attaques menées par Goldeneye peuvent entraîner des pertes financières sur des sites de ventes ou autre.
- Goldeneye peut être utiliser pour compromettre la sécurité de la machine sur laquelle on s’attaque

- Les attaques DoS laissent des traces, l’utilisation de goldeneye peut conduire à une identification et à des poursuites judiciaires.

- L’utilisation de goldeneye sans autorisation va à l’encontre de l’éthique de la sécurité informatique.

On peut se protéger de Goldeneye de différentes façons :

1. Utilisez un pare-feu.
2. Considérez une solution anti-DDoS.
3. Configurez la répartition de la charge.
4. Surveillez le trafic réseau.
5. Gardez vos systèmes à jour.
6. Configurez le filtrage IP.
7. Limitez les erreurs de configuration.
8. Élaborez un plan de réponse aux incidents.
9. Utilisez la sauvegarde et la redondance.
10. Signalez aux autorités en cas d'attaque.

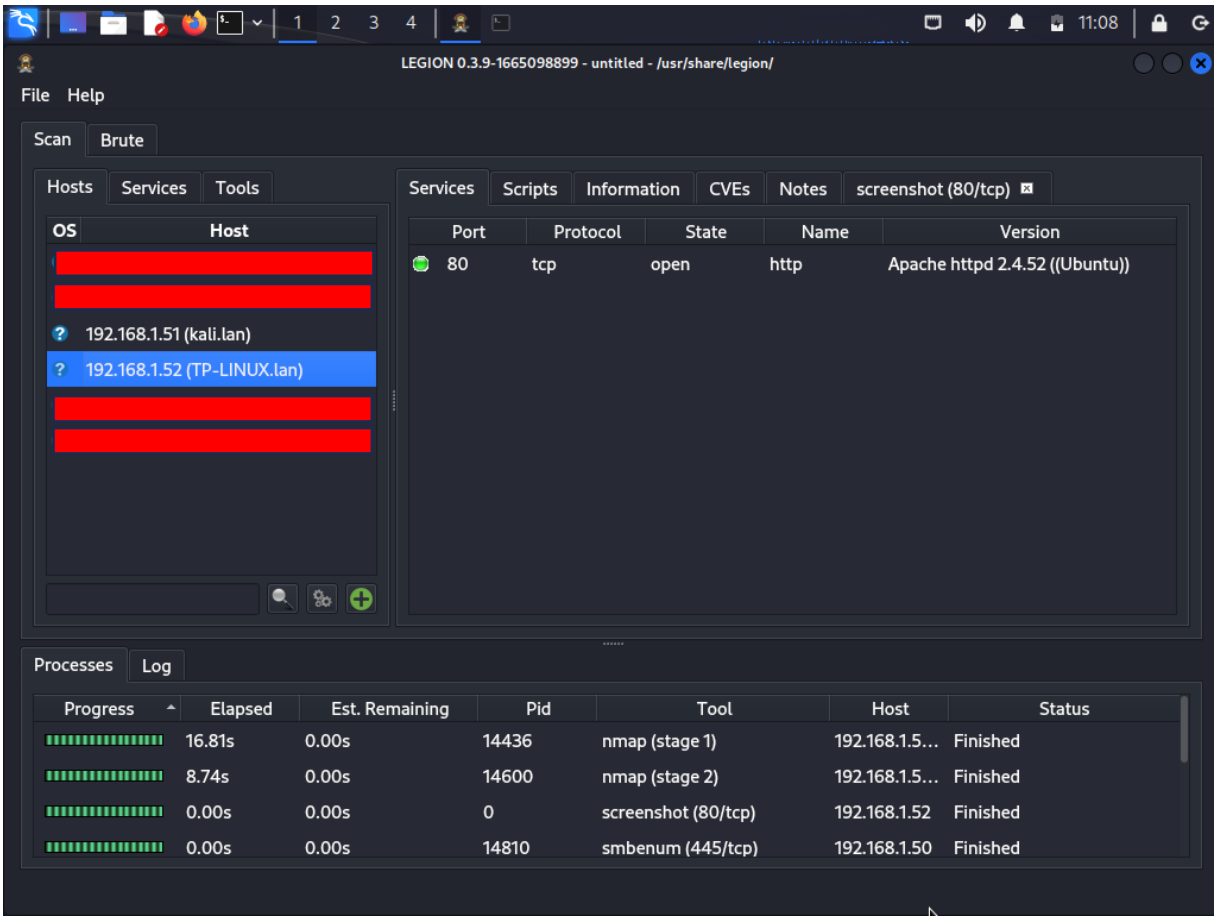
T50 n’est pas comme Goldeneye car T50 attaque avec différents protocoles.

T50 est plus flexible et est un outil plus polyvalent. Il est plus complexe que Goldeneye car il a davantage d’options avancées.

Utilisation de Legion :

J’ai rentré l’IP de ma machine Linux : 192.168.1.52

Legion a donc détecté mon port 80 qui est ouvert mais aussi il a cherché aussi toutes les IP connectées à mon PC dont l’IP de ma Box bouygues…



Legion représente une menace s’il n’est pas utilisé dans un cadre professionnel et sécurisé.

Si l’utilisation de ce logiciel se fait sur un réseau sans autorisation cela constitue une violation de la loi.

Si légion est utilisé de manière inappropriée il peut révéler des vulnérabilités sensibles ou des failles de sécurités qui peuvent être exploitées par des personnes malveillantes.

Si les tests réalisés avec Legion sont mal planifiés ou exécutés ils peuvent affecter le réseau.

En résumé, l'application Legion sur Kali Linux est un outil puissant pour les professionnels de la sécurité informatique, mais son utilisation doit être entreprise de manière légale, éthique et autorisée. Il est essentiel de respecter les lois locales et de maintenir des pratiques éthiques en matière de tests de sécurité. Si vous n'avez pas l'expertise nécessaire pour utiliser Legion de manière appropriée, il est recommandé de faire appel à des professionnels de la sécurité informatique qualifiés.

CONCLUSION :

En conclusion, ces outils, lorsqu'ils sont utilisés de manière légale, éthique et responsable, peuvent être précieux pour les professionnels de la sécurité informatique. Cependant, leur utilisation inappropriée peut avoir des conséquences légales, éthiques et techniques graves. Il est essentiel de respecter les lois locales, de garantir le consentement du propriétaire du système testé et de mettre en œuvre des pratiques de sécurité responsables lors de l'utilisation de ces outils. Si vous n'êtes pas sûr de la manière d'utiliser ces outils de manière appropriée, il est recommandé de faire appel à des professionnels de la sécurité informatique qualifiés.

STCHERBININE Mattéo SIO2