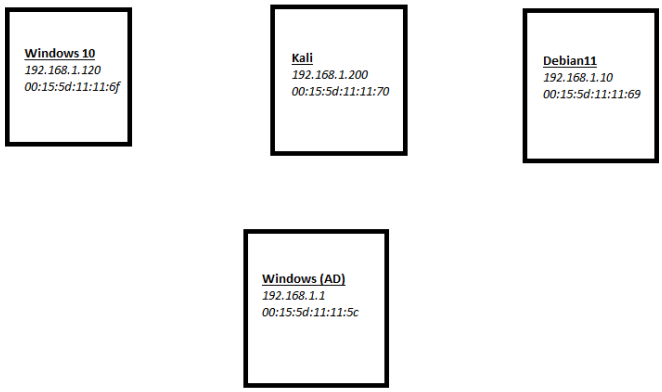
TP Découverte Kali Linux – Bloc 3 – JOBARD Guillaume – 2021/2022 – UFA Robert Schuman

De BARILLY Dylan.

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.



Introduction : Dans ce TP nous allons découvrir d'autres fonctionnalités de Kali, notamment avec l'application goldeneye et l'application legion que nous allons découvrir dans ce TP.

Installation de goldeneye :

GoldenEye est un outil de test HTTP DoS. Cet outil peut être utilisé pour tester si un site est sensible aux attaques par déni de service (DoS). Il est possible d'ouvrir plusieurs connexions parallèles sur une URL pour vérifier si le serveur Web peut être compromis.

```
└─$ sudo apt install goldeneye
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  goldeneye
0 upgraded, 1 newly installed, 0 to remove and 259 not upgraded.
Need to get 83.9 kB of archives.
After this operation, 986 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 goldeneye all 1.2.0+git2019123
0-2 [83.9 kB]
Fetched 83.9 kB in 1s (83.7 kB/s)
Selecting previously unselected package goldeneye.
(Reading database ... 397449 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 (2.11.2-2) ...
Processing triggers for kali-menu (2023.2.3) ...
```

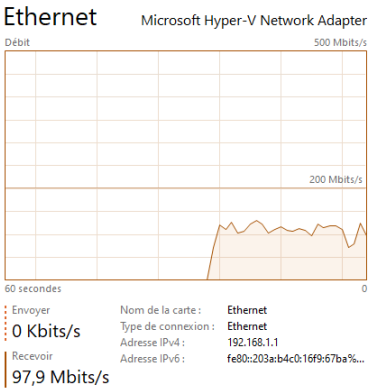
L'application goldeneye est installé.

T50 est une application sous Kali Linux qui a pour bu d'envoyer pleins de trafic sur un réseau défini afin d'essayer de boucher le trafic.

Passons à l'installation de T50 avec la commande « sudo apt install t50 », après l'installation, avec la commande « sudo t50 192.168.1.1 –flood » nous remarquons que sur la VM inscrite dans la commande, le reçu de Mbits/s devient tout de suite élevé avec des pics à plus de 100Mbits/s

```
┌──(kali㉿kali)-[~]
└─$ sudo t50 192.168.1.1 --flood
T50 Experimental Mixed Packet Injector Tool v5.8.7b
Originally created by Nelson Brito <nbrito@sekure.org>
Previously maintained by Fernando Mercês <fernando@mentebinaria.com.br>
Maintained by Frederico Lamberti Pissarra <fredericopissarra@gmail.com>

[INFO] Entering flood mode ... [INFO] Performing stress testing ...
[INFO] Hit Ctrl+C to stop ...
[INFO] PID=5176
[INFO] t50 5.8.7b successfully launched at Wed Jun 21 03:51:54 2023
```

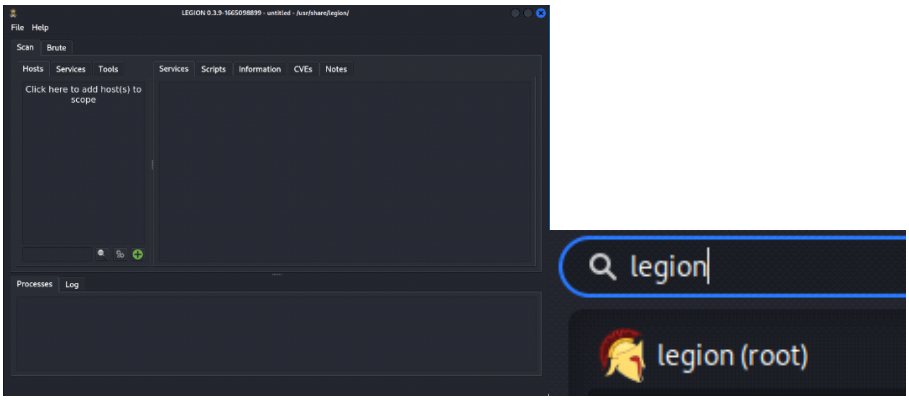


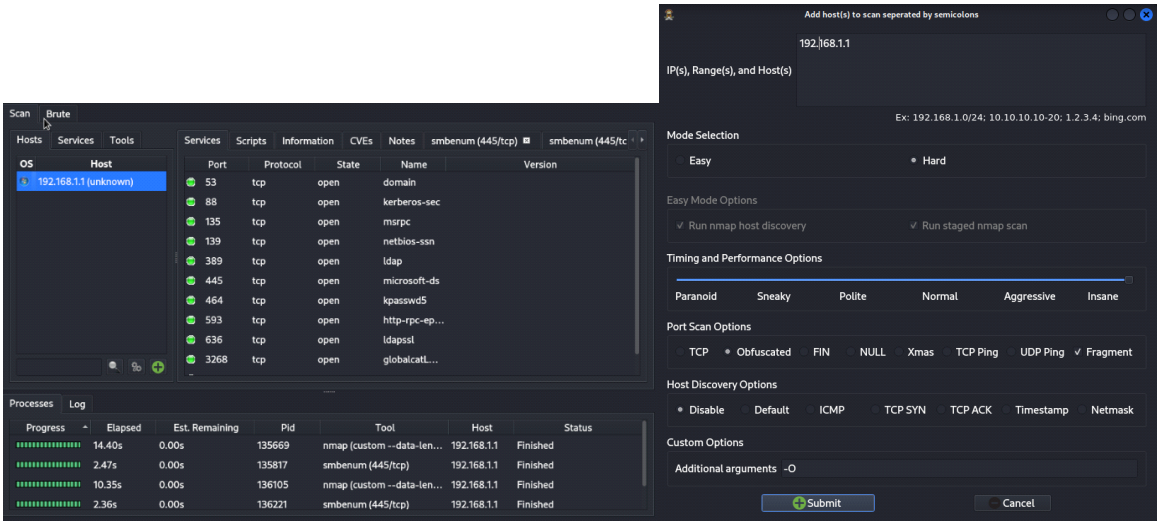
Les enjeux/dangers possibles avec une telle application sont dans un premier temps malveillant, les ransomwares sont possibles effectivement il est possible de crypter les fichiers afin de demander une rançon, la propagation est rapide au sein de l'entreprise est peut détruire les données de votre entreprise. Les entreprises les plus touchés sont les banques et les hôpitaux, cela peut-être très dangereux économiquement comme humainement. Cependant il peut être utilisé pour se protéger de ces attaques, en étant proactive et en prenant le temps de voir les failles de système que l'entreprise peut avoir afin de les rectifier.

La différence entre T50 et Goldeneye est que T50 attaque le réseau tandis que Goldeneye attaque les serveurs HHTP.

Il est possible de s'en protéger en mettant en place un filtrage des IP qui peuvent nous envoyer des paquets (Stormshield)

Passons à l'utilisation de l'application legion : C'est un outil de test de pénétration de réseau open source, facile à utiliser, super-extensible et semi-automatisé qui facilite la découverte, la reconnaissance et l'exploitation des systèmes d'information.





Legion est une application permettant de rendre visible tous les ports ouverts d'une adresse IP, en plus, il sait quel OS s'agit-il est le nom de celle-ci, sur les exemples ci-dessus j'ai fait une attaque sur mon AD (192.168.1.1), j'ai pu apercevoir les ports ouverts de mon AD, cela permet de voir les intrusions possibles sur son réseau afin de combler les failles sur celui-ci, cependant de façon malveillant il peut être vraiment dangereux pour les personnes qui veulent s'introduire dans le réseau.

Conclusion : Pour conclure ce TP, nous avons vu certaine application comme GoldenEye qui permet d'envoyer pleins de paquet sur la partie http, nous avons aussi vu T50 qui permet d'essayer de boucher le trafic réseau en envoyant pleins de paquets et pour finir nous avons vu Legion qui permet de rendre

visible tous les ports ouverts d'une adresse IP. Toutes les applications vus dans ce TP peuvent être utilisé de façon malveillante afin de nuire à une entreprise mais elles peuvent être aussi utilisé de façon pour combler les failles de l'entreprise, en effet en voyant les ports ouverts d'une adresse IP nous pouvons afin constater tous les ports ouverts et donc faire le nécessaire pour les fermer. De plus en cas d'attaque sur le trafic réseau ou HTTP il suffit de mettre en place un système de filtrage.