TP Découverte Kali Linux – Bloc 3 – AKALAN Selim – 2022/2023 – UFA Robert Schuman

SOMMAIRE

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..... 3

- Récupérez votre VM Kali, votre plan d'adressage et vérifiez que tout est opérationnel..... 3

- Sur votre machine Kali, allez dans le menu principal et cherchez l'application goldeneye. Notez dans quel dossier elle est rangée. Si elle n'est pas installée, lisez la documentation ci-dessous et faites le nécessaire..... 3

- Lisez la documentation qui s'affiche et utilisez le programme avec une machine de votre contexte. La machine répond encore correctement après avoir exécuté le programme ? 4

Quels sont les enjeux/dangers possibles avec une telle application ? Comment s'en protéger ? 5

Cette autre application fait-elle la même chose ? 5

- Sur votre machine Kali, allez dans le menu principal et cherchez l'application légion. Notez dans quel dossier elle est rangée. Si elle n'est pas installée, lisez la documentation ci-dessous et faites le nécessaire. 7

- Lisez la documentation, expérimentez là avec les machines de votre contexte. Quels sont les enjeux/dangers possibles avec une telle application ? 7

Quels sont les enjeux/dangers possibles avec une telle application ? 8

Conclusion : 9

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.

Pour redécouvrir le monde magique de Kali, mettons-nous en condition ;

- Récupérez votre VM Kali, votre plan d'adressage et vérifiez que tout est opérationnel.

- Information de la VM.

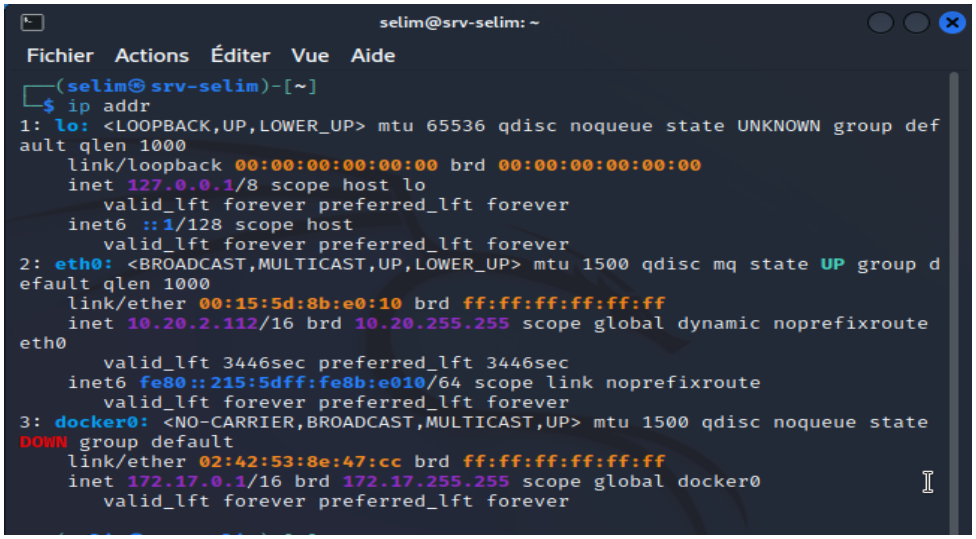

Figure 1: Info de notre vm

Continuons notre expérimentation ;

- Sur votre machine Kali, allez dans le menu principal et cherchez l'application goldeneye. Notez dans quel dossier elle est rangée. Si elle n'est pas installée, lisez la documentation ci-dessous et faites le nécessaire.

- Le dossier de GoldenEye est dans : /home/selim.

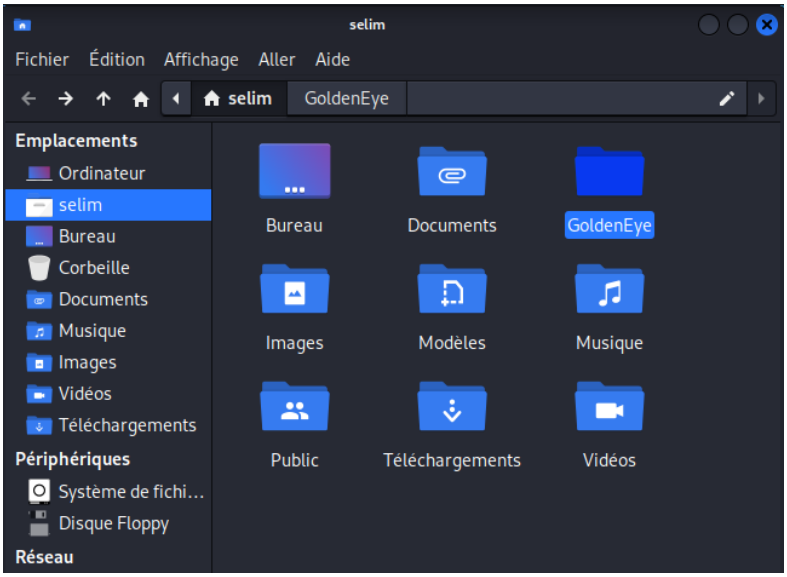

Figure 2: Le dossier GoldenEye

- Lisez la documentation qui s'affiche et utilisez le programme avec une machine de votre contexte. La machine répond encore correctement après avoir exécuté le programme ?

- Ma machine répond correctement après avoir exécuté le programme, mais j'ai vu des PC dans notre labo qui plantait après exécution de ce programme.

- Suite à l'accord de mon collègue, nous allons procéder à une attaque sur son WordPress. Une image de son site avant l'attaque.

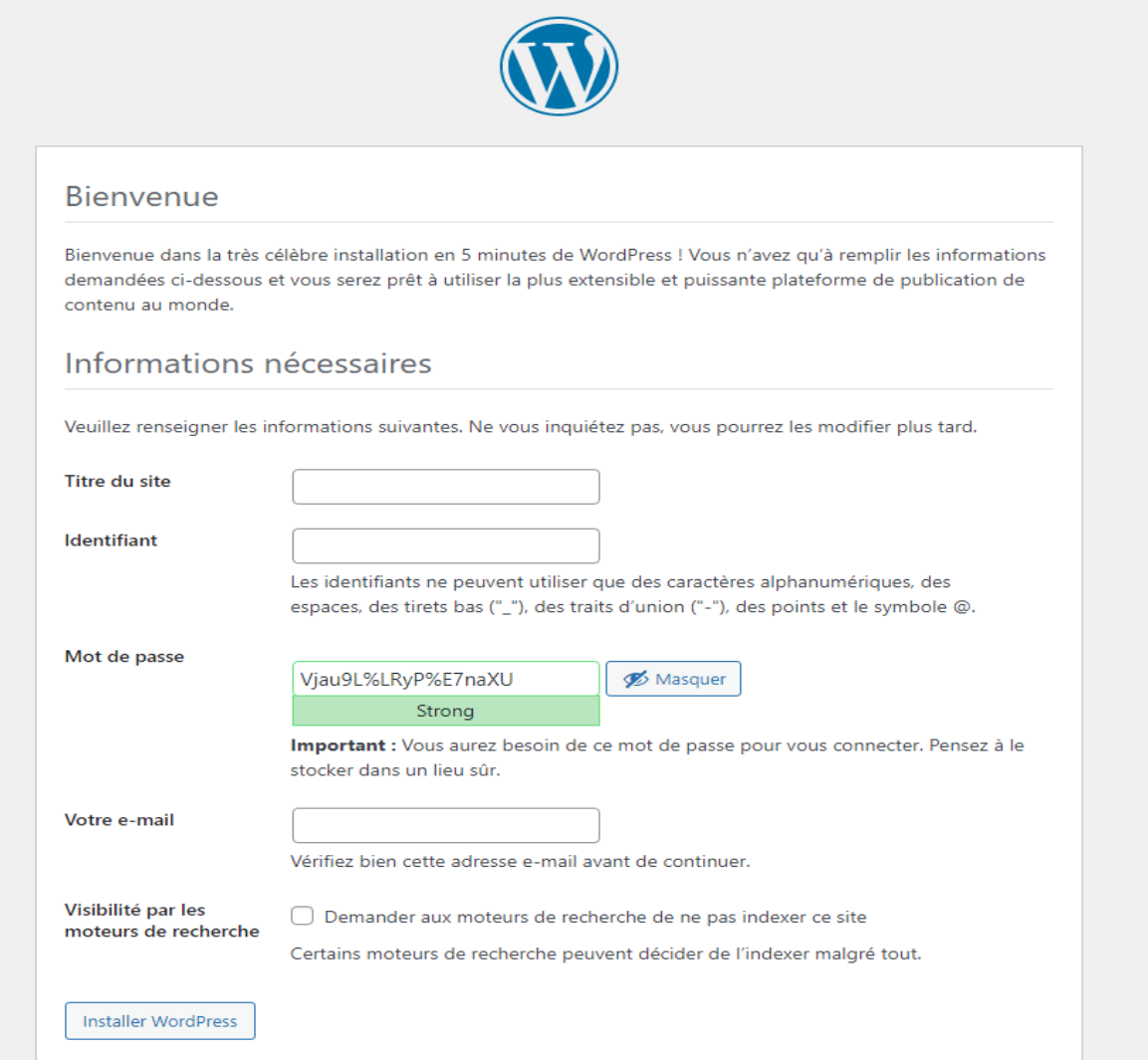

Figure 3: Le site avant l'attaque

- *On revient sur notre machine et nous procédons à l'attaque. L'attaque peut se faire via un nom de domaine ou une adresse IP. La commande : «./goldeneye.py nom de domaine ou IP -s 1000 » permet de faire l'attaque mais « -s 1000 » veut dire « s = socket » donc Le socket envoie 1000 requêtes.*
  - *Ps : Socket = communication entre client-serveur.*

```
┌──(selim㉿srv-selim)-[~/GoldenEye]
└─$ ./goldeneye.py http://10.20.2.219:8000 -s 1000

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

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

Figure 4: La commande pour envoyer l'attaque

-

- *Après l'attaque, le site n'est plus accessible en moins d'une minute.*

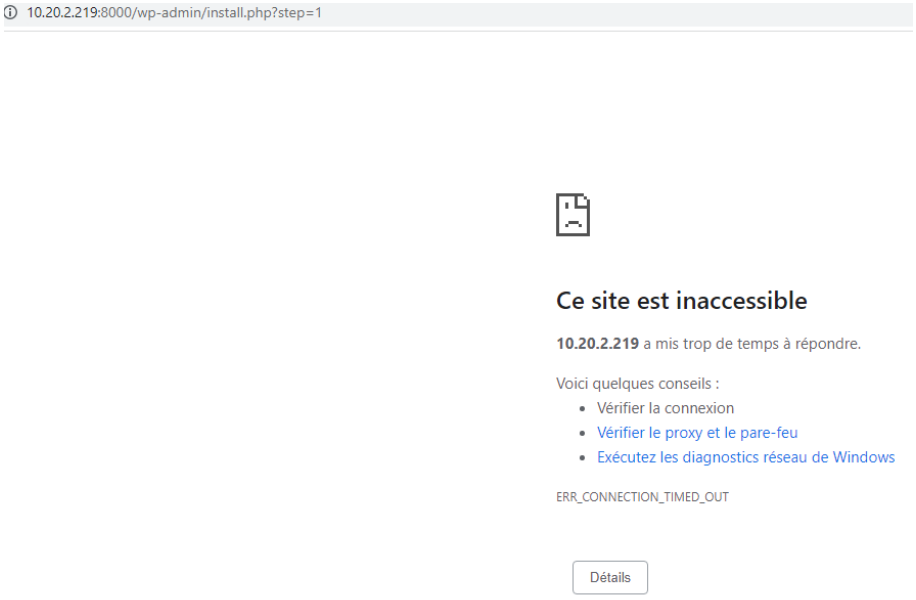

Figure 5 : Le site après l'attaque

Quels sont les enjeux/dangers possibles avec une telle application ? Comment s'en protéger ?

- *Les dangers possibles de telle application sont : facile d'utilisation, qu'une attaque peut se faire très rapidement, faire des tomber des serveurs web qui n'est pas protégé, elle envoie des centaines de requêtes donc elle casse le système en face rapidement*
- *On peut se protéger en sécurisant notre site web en le mettant en https, car il est difficile d'attaquer un site sécurisé en https, les attaques DoS peuvent être contré, donc : de manière régulière faire les mises à jour de sécurité, un pare-feu correctement paramétré, mot de passe complexe et changé régulièrement. Fermé les ports inutiles. Mettre un Fail2ban en place.*

Cette autre application fait-elle la même chose ?

- *GoldenEye et t50 ont le même but, mais pas les mêmes fonctionnalités, ces deux applications permettent de faire une attaque DoS.*
- *GoldenEye fait des attaques DoS, il utilise un trafic HTTP parfaitement légitime. Cette application permet à une seule machine de désactiver le serveur Web d'une autre machine, il utilise un trafic HTTP parfaitement légitime. Il établit une connexion TCP complète et ne nécessite ensuite que quelques centaines de requêtes à intervalles réguliers et à long terme. Par conséquent, l'outil n'a pas besoin d'utiliser beaucoup de trafic pour épuiser les connexions disponibles sur un serveur.*
- *T50 effectue des attaques DoS, mais il utilise l'injection de paquets réseau en utilisant divers protocoles tels que TCP, UDP et ICMP. T50 est un programme d'injection de paquets très puissant, il peut envoyer jusqu'à 1.000.000 de paquets par seconde. Avec cette application, vous pouvez envoyer un nombre très élevé de*

demandes de paquets, de sorte que la cible ne peut pas répondre à toutes les demandes ou y répond lentement, de sorte que la cible peut devenir indisponible ou perdre ses performances.

```
┌──(selim㉿srv-selim)-[~]
└─$ sudo t50 10.20.1.11 --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=44812
[INFO] t50 5.8.7b successfully launched at Tue Oct 11 11:59:35 2022
```

Figure 6 : Utilisation de t50

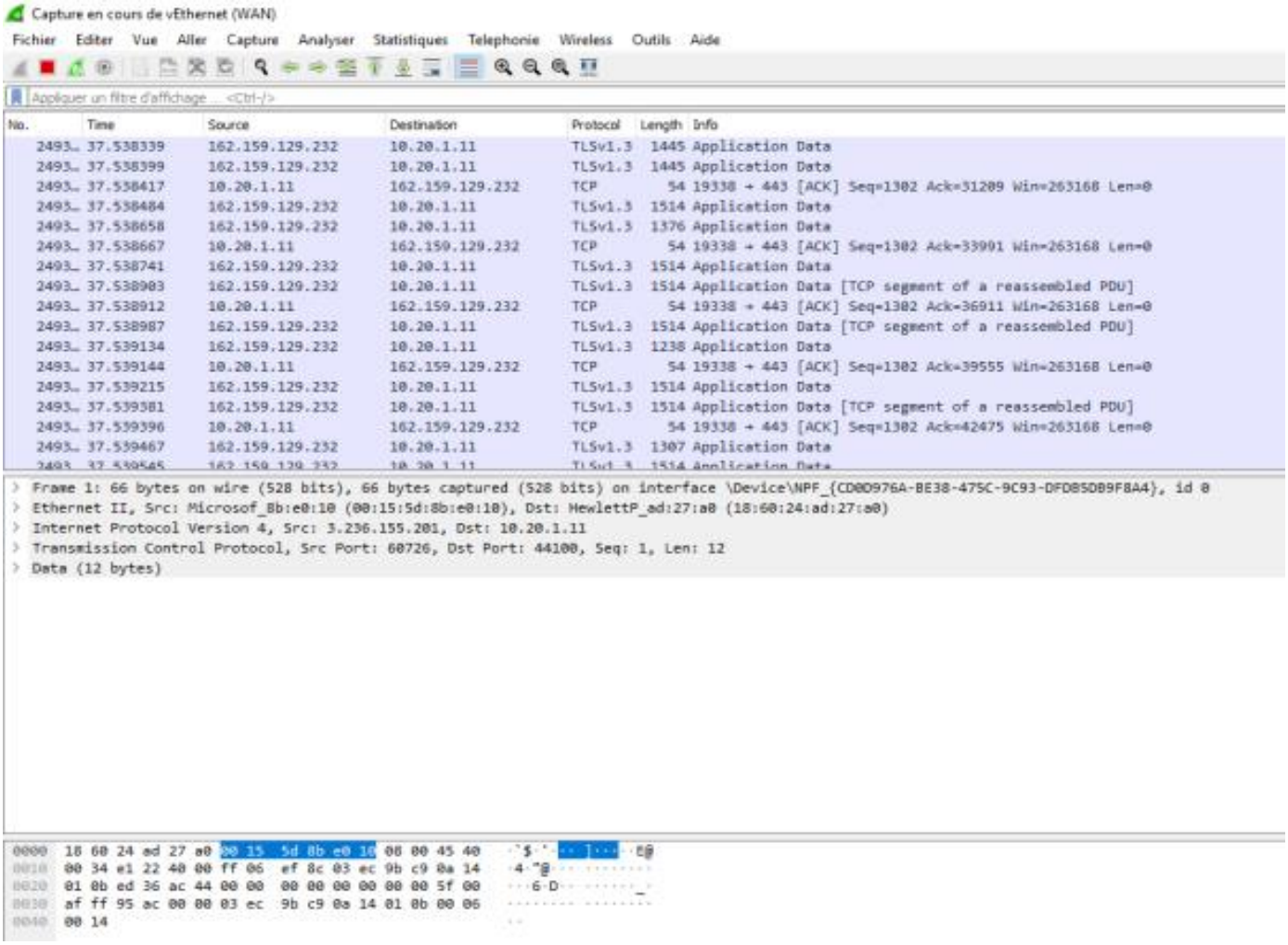

Figure 7 : Les requêtes envoyer par t50

Essayons autre chose ;

- Sur votre machine Kali, allez dans le menu principal et cherchez l'application légion. Notez dans quel dossier elle est rangée. Si elle n'est pas installée, lisez la documentation ci-dessous et faites le nécessaire.

- L'application « Légion » est rangé dans le dossier « 01 – Récupération d'informations ».

Figure 8 : Dossier légion

- Lisez la documentation, expérimentez là avec les machines de votre contexte. Quels sont les enjeux/dangers possibles avec une telle application ?

- On lance l'application Légion avec la commande « legion –h » dans le terminal.

Figure 9 : Ouvrir l'application légion

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

- *L'application Légion est un bon outil pour les tests d'intrusion. En utilisant cela, nous pouvons effectuer une analyse automatique et trouver des vulnérabilités sur les applications Web. Suite à mes recherches plus approfondies concernant cette application, nous allons voir qu'elle permet de faire énormément de taches, RIP au site qui se font attaquer par ce genre de logiciel. Je vous laisse découvrir la liste des taches que peut effectuer Légion est tous ces enjeux/dangers :*

- *Reconnaissance et analyse automatiques avec NMAP, whataweb, nikto, Vulners, Hydra, SMBenum, dirbuster, sslyzer, webslayer et plus encore (avec près de 100 scripts auto-programmés).*
- *Interface graphique facile à utiliser avec des menus et des panneaux contextuels riches qui permettent aux pentesters de trouver et d'exploiter rapidement les vecteurs d'attaque sur les hôtes.*
- *La fonctionnalité modulaire permet aux utilisateurs de personnaliser facilement Legion et d'appeler automatiquement leurs propres scripts/outils.*
- *Analyse de scène hautement personnalisable pour une évasion IPS de type ninja.*
- *Détection automatique des CPE (Common Platform Enumeration) et des CVE (Common Vulnerabilities and Exposures).*
- *Lie les CVE aux exploits comme détaillés dans Exploit-Database.*
- *Enregistrement automatique en temps réel des résultats et des tâches du projet.*

- *Suite à l'accord d'un collègue de ma classe, j'ai effectué un scan via son IP.*
- *En "mode difficile", nous obtenons des options de personnalisation supplémentaires telles que l'analyse de port personnalisée, la découverte d'hôte et les options de découverte personnalisées.*
- *Dans les arguments supplémentaires, nous utilisons les options -sV et -O. L'indicateur -sV est utilisé pour la version du service et l'indicateur -O pour la détection du système d'exploitation. Ensuite, il nous suffit de cliquer sur "Soumettre".*

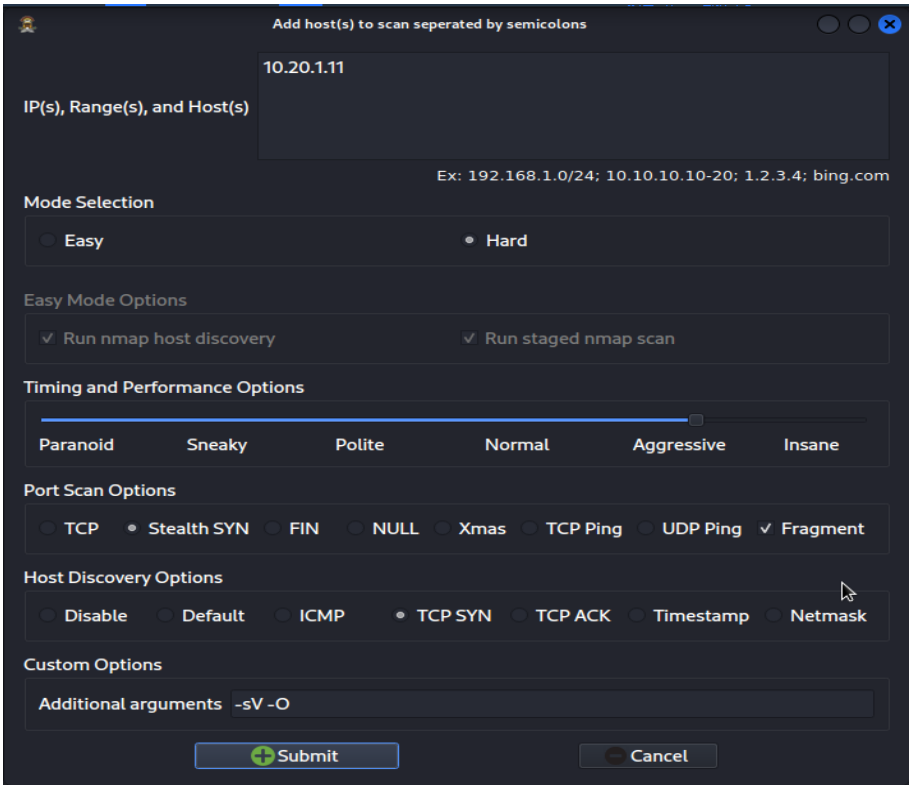

Figure 10 : Attaque via Légion

- *Il analysera d'abord l'adresse IP ou Web avec nmap, puis exécutera Nikto sur l'adresse IP ou Web ciblée. Legion testera avec divers outils automatisés comme Shodan, whataweb, Vulners, Hydra, SMBenum, dirbuster, sslyzer, webslayer et plus (avec près de 100 scripts auto-programmés). Nous avons un onglet sur Légion pour chaque outil utilisé et il est également capable de trouver CVE. Il nous montrera le CVE s'il est disponible.*

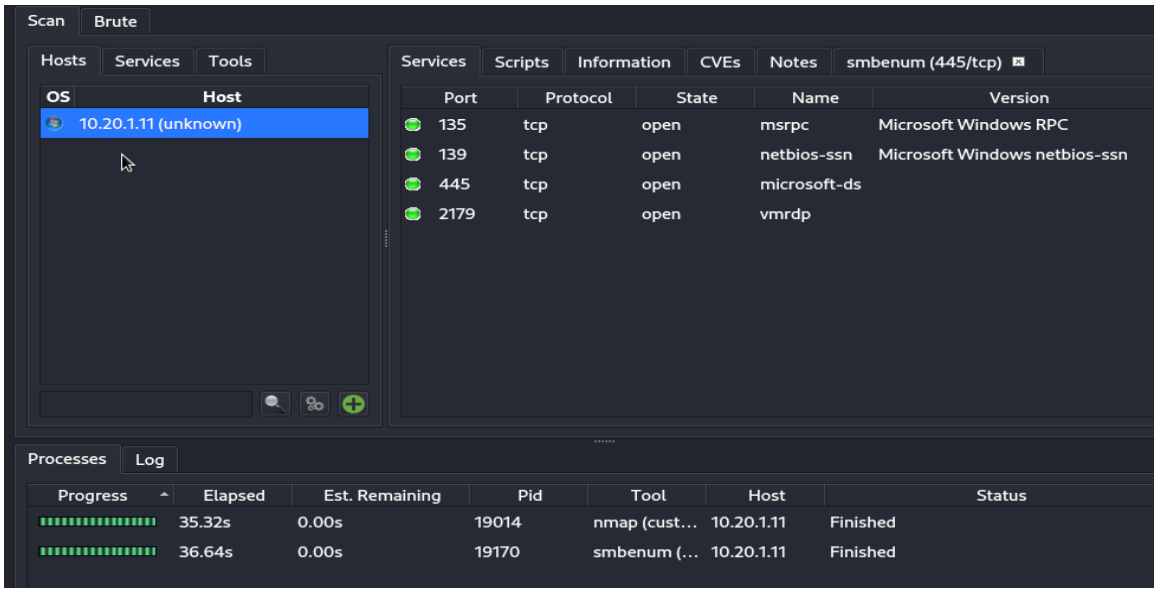

Figure 11 : Résultat Légion

Enfin ;

- Tirez des conclusions sur ce que vous venez de découvrir, documentez ce TP et rendez-le sur Moodle dans les délais indiqués. Le barème reposera sur la qualité de votre rendu, orthographe, rédaction, explications, illustration…

Conclusion : *Ce TP permet de pouvoir ce familiarisé sur la sécurité des serveurs Web. Suite à ce TP, nous pouvions voir qu'un site web non sécurisé peut être en 10 secondes cassé, et donc suite aux applications utilisées sur Kali, nous avions pu pratiquer des attaques sur des sites de nos collègues de la classe avec leur accord. Ces attaques ont durée des secondes et leur site n'était déjà plus en vie. Grâce à ce TP, nous avions pu nous enrichir sur la sécurité des sites internet et sur les attaques qui peuvent être pratiqué via des logiciels qui sont faciles d'utilisation.*

En espérant que ce TP vous sera utile pour la découverte de Kali et de ces applications.