

Playzone 2021

Projet ethical hacking



17 décembre 2021

Technobel

Kools Ludovick

Table des matières

[Introduction 2](#_Toc90573645)

[Présentation de l’infrastructure 3](#_Toc90573646)

[Les projet ethical hacking 5](#_Toc90573647)

[ARP poisonning 5](#_Toc90573648)

[Procédure 5](#_Toc90573649)

[Utilisation de Metasploit 7](#_Toc90573650)

[Conclusion 11](#_Toc90573651)

# Introduction

Comme chaque année, arrive enfin la tant attendue Playzone de Technobel. Plus qu’un évènement, celle-ci va permettre à tous les étudiants de collaborer et d’avancer ensemble afin de démontrer l’étendue de leurs talents ainsi que le large éventail de compétences acquis lors de leur formation.

En effet, grâce à la mise en situation proposée lors de la Playzone, il nous est enfin donné d’appréhender, voir, expérimenter et comprendre les tenants et aboutissants de la création d’un projet. C’est dans ce genre de moments qu’il nous est enfin possible d’apercevoir ce que seront les réalités de notre métier de demain et de pouvoir nous construire un reflet de toutes les compétences qui seront nécessaires pour bien progresser tant au niveau hardskills que softskills.

Lors de cette Playzone, l’équipe SecOps a été divisée en trois teams distinctes :

1. L’équipe Audit : Cette équipe (composée de Corentin Goffin, Thomas Buscema et Gabriel Libert) avait pour but de réaliser un audit fonctionnel de l’infrastructure ainsi qu’un audit énergétique de celle-ci.
2. L’équipe SOC/NOC : Cette équipe (composée de Kevin Godefroid, François Lemaire et Nathan Ndjoni) avait pour but de déployer une solution SOC/NOC afin de monitorer l’ensemble de notre infrastructure.
3. L’équipe ethical hacking : Cette équipe (composée de Emmanuel Elsen, Brandon Billen et de moi-même) avait pour but de réaliser de l’ethical hacking et du pentesting sur l’infrastructure.

Afin de mener à bien les différentes missions qui nous ont été confiées, il a fallu en amont préparer une infrastructure sur laquelle évoluer tout au long de cet évènement où nous nous sommes isolés afin de ne pas déranger le bon fonctionnement de la Playzone des autres participants. Vous trouverez donc dans ces quelques pages le récit de ma Playzone.

# Présentation de l’infrastructure

Comme dit précédemment, afin de bien pouvoir commencer, il nous a été nécessaire de monter une infrastructure afin de pouvoir travailler dans les meilleures conditions. Sachant qu’il y avait une montagne de matériel à notre disposition, nous avons vu les choses en très (trop) grand et sommes partit sur une infrastructure qui, selon nous, pouvait se trouver le plus proche possible de ce qu’il serait disponible en production. Nous sommes donc partis sur, pour le côté « LAN » :

* Un routeur « core » servant de lien entre le Lan en lui-même, le datacenter et la couche backbone / agrégation.
* Un switch MLS qui permet de faire la jonction entre le routeur et les autres switchs.
* Deux switchs 2960 dont l’un PoE afin d’alimenter les téléphones VoIP et l’autre interconnectant les différents clients du réseau.

Dans ces différents clients se trouvait notamment une machine simulant une machine « vérolée » garantissant un accès au LAN à l’équipe d’ethical hacking, une machine servant de machine d’audit pour l’équipe d’audit ainsi que plusieurs machines servant de clients au LAN et servant de test pour le bon fonctionnement de serveur DHCP.

En ce qui concerne la téléphonie IP, manquant de temps et étant donné que l’infrastructure n’étant pas la priorité de notre Playzone, nous avons décidé de la mettre de côté.

Du côté du datacenter, se trouvent :

* Le routeur « core » cité précédemment.
* Un switch MLS servant de lien entre les différents serveurs.

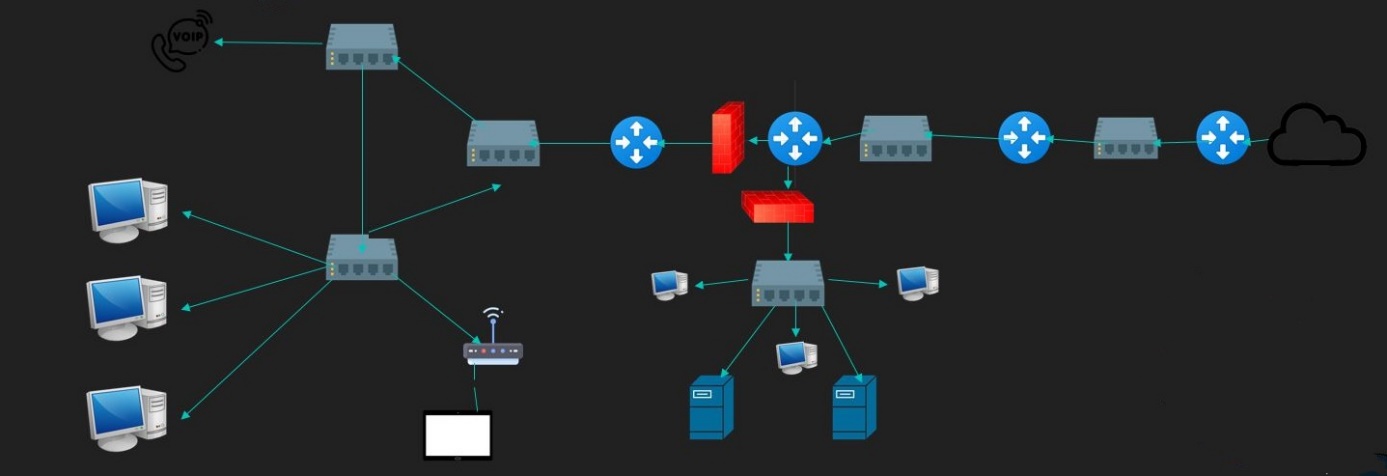
Afin de subvenir aux différents besoins, plusieurs machines serveur ont été déployées incluant :

* Un Radius
* Un DHCP
* Un TFTP
* Un NFS
* Deux serveur web dont un comportant des VHosts
* Un Active Directory
* Une machine SOC/NOC avec AlienVault et Nagioslog
* Une machine pour l’équipe d’audit
* Une machine « vérolée » servant de second point d’entrée pour l’équipe d’ethical hacking.

Enfin, la partie BBA / Agrégation était quant à elle composée d’un switch BBA, un routeur BBA, un switch agrégation et enfin le routeur agrégation qui se trouvait être notre point de sortie vers le WAN.

Il va sans dire que toutes les features de « base » ont été déployés tel que des VLAN, des Dot1q, loopback de test, ntp, stp, pat, IP helper, mot de passe sur les devices, adressage IP cohérent ainsi qu’une documentation claire afin de pouvoir se structurer et s’y retrouver.

Il peut sembler à ce point relativement difficile de s’y retrouver dans toutes ces explications, c’est pour ça que je vous propose en page suivante d’illustrer mes propos par un schéma.



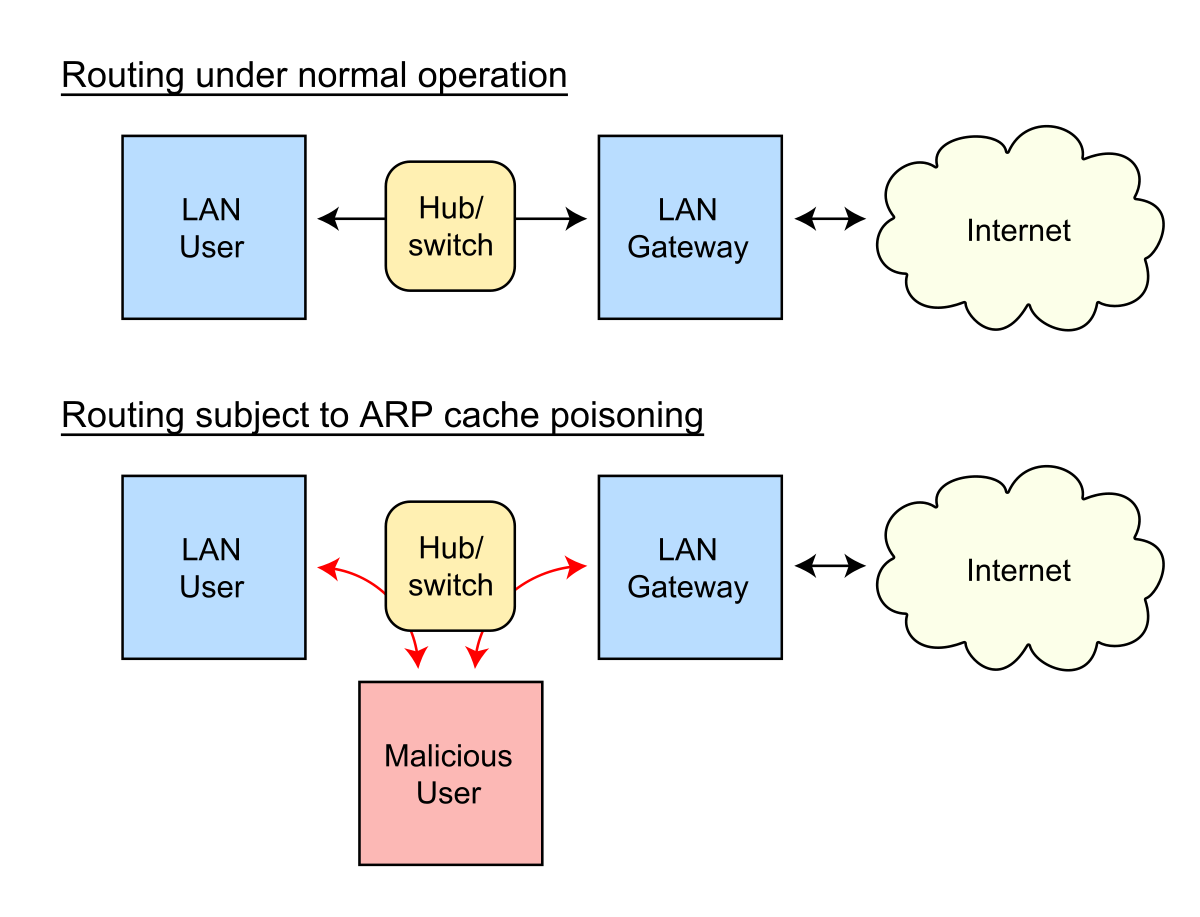
Vous pouvez donc retrouver ici en bleu la partie LAN, en rouge la partie datacenter et le reste qui est la sorte du réseau en passant par le BBA et l’agrégation.

Ceci conclut donc la partie de création du réseau. Il nous aura fallu une semaine et demi pour en arriver au bout car il y a eu beaucoup de digression lors de la création de celui-ci et du mal à se concentrer sur la partie vraiment importante de la Playzone, c’est-à-dire l’orientation des équipes car nous étions plus penchés sur la partie architecture qui n’est absolument pas le but ici.

# Les projet ethical hacking

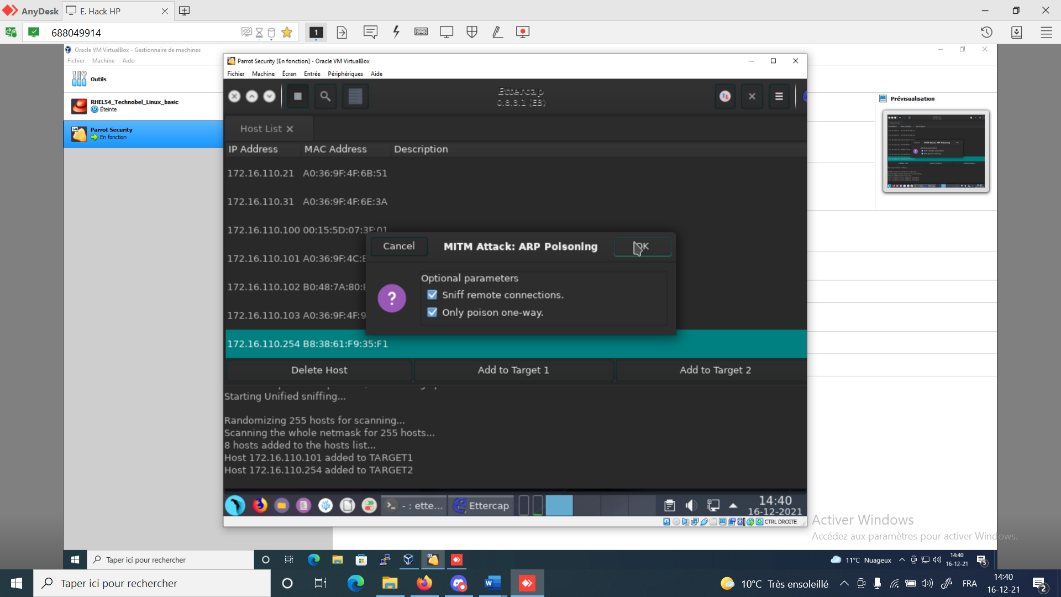
## ARP poisonning

La première manipulation qui a été réalisée dans le cadre de notre Playzone, nous avons décidé de faire un ARP poisonning envers le serveur web afin de prendre la place de celui-ci. Cette attaque est de type man in the middle (MitM) et, elle permet de modifier la table ARP des cibles afin de s’insérer dans les communications et, de facto, intercepter toutes les informations transitant entre celles-ci.

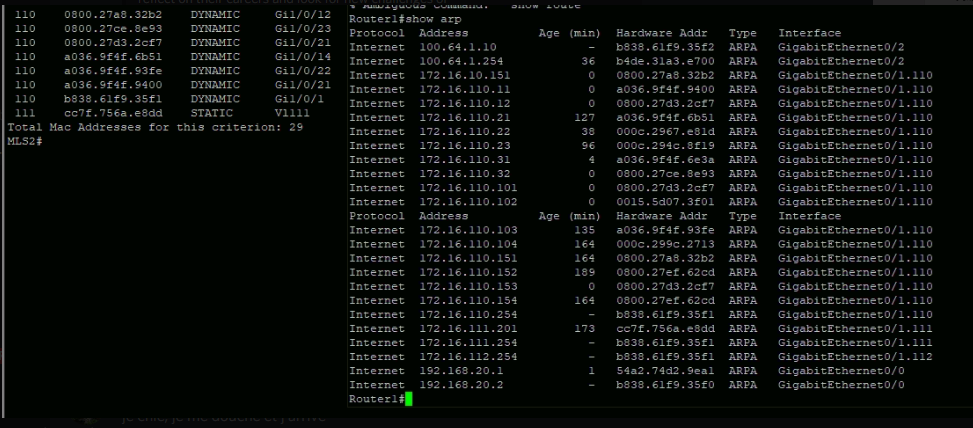


## Procédure

Dans un premier temps, il faudra mettre en place d’un alias sur la carte Ethernet grâce à la commande :  
*ifconfig eth0 :1 172.16.110.154 netmask 255.255.255.0*   
Ensuite nous utilisons Ettercap afin de réaliser le premier poisonning :



Lors de celui-ci, il faut en premier scanner les différents hosts sur le réseau afin de pouvoir les sélectionner. Dans un premier temps, nous allons sélectionner dans un premier temps le routeur et comme deuxième cible la machine physique qui héberge le serveur web. Cette opération va nous permettre de prendre la place du serveur web dans la CAM du switch afin de rediriger le tout vers notre machine de « piratage ».

**Ensuite, il faut effectuer un flood de la CAM du switch afin de faire réagir les administrateurs du réseau. En effet, une table CAM qui est remplie fait agir le switch comme un hub et pose donc un problème au niveau de la sécurité ainsi qu’au niveau des performances. Pour effectuer ce flood, nous utilisons la commande :   
*macof -i eth0*

*Illustration de la CAM du switch qui a été poisoned ainsi que le router qui nous prends pour la machine*

Nous attendons patiemment le rétablissement de la CAM pour pouvoir lancer la suite de notre attaque. Une fois celle-ci rétablie, nous pouvons relancer Ettercap afin de poison d’un côté le site web directement cette fois-ci et le routeur d’un autre côté.

Dans un même temps, nous démarrons un serveur Apache afin de mettre en place notre page qui a pour but de remplacer le vrai site web.

Une fois toute ces manipulations effectuées, notre page web va remplacer le site de l’intranet de façon transparente pour l’utilisateur.

Le poisonning étant réalisé avec succès, il soulève plusieurs questions sécuritaires. En effet avec une telle page, il va être possible de récupérer les informations de l’intranet de tous les utilisateurs. Pire encore, avec cette technique, il est possible de prendre la place d’un éventuel DNS et donc de remplacer les sites publics tel que Facebook ou autres afin de récupérer les données des utilisateurs du LAN.

Mais alors comment se protéger de cela dans mon infrastructure ? Et bien il existe un moyen extrêmement simple à mettre en place et très efficace qui s’appelle le DAI (Dynamic ARP Inspection) Lorsque DAI est activé, le switch abandonne le paquet ARP si l'adresse MAC et l'adresse IP de l'expéditeur ne correspondent pas à une entrée de la base de données des liaisons DHCP snooping. Toutefois, ce problème peut aussi être résolu grâce aux mappages statiques. Les mappages statiques sont utiles lorsque les hôtes configurent des adresses IP statiques, que DHCP snooping ne peut pas être exécuté ou que d'autres switch du réseau n'exécutent pas d'inspection ARP dynamique. Un mappage statique associe une adresse IP à une adresse MAC sur un VLAN.

## Utilisation de Metasploit

Dans un second temps, nous avons utilisé Metasploit afin de détecter des failles dans le réseau dans lesquelles nous pourrons nous engouffrer. En effet, le but de celui-ci est de fournir des informations sur les vulnérabilités de systèmes informatiques, d'aider à la pénétration et au développement de signatures pour les systèmes de détection d'intrusion. Il intègre une base de données très complète sur les CVE et les NVT permettant une pénétration plus aisée pour les initiés à la pratique.

Afin d’utiliser metasploit, il est plus intéressant d’y lier une base de données. Dans notre cas, nous avons utilisé PostgreSQL. Avant de lancer metasploit, nous lançons donc PostgreSQL avec la commande :

*systemctl start postgresql.service*

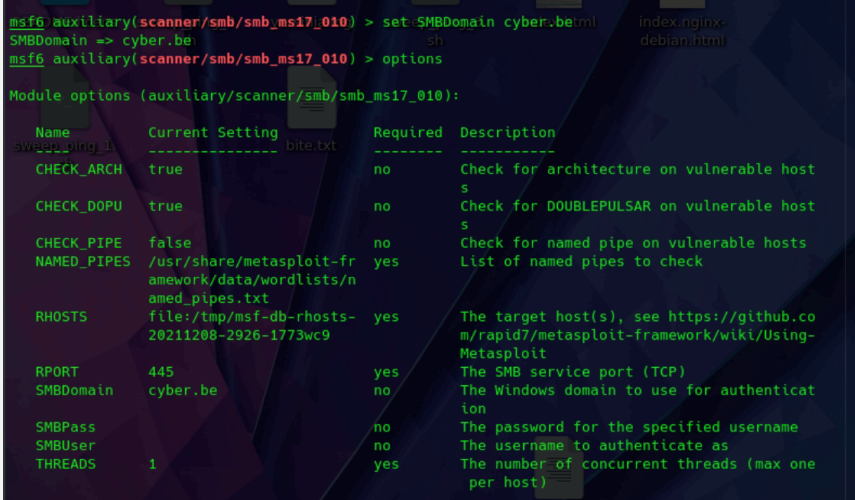
Ensuite, nous lançons *msfconsole* pour accéder à metasploit. Une fois celui-ci lancé nous faisons un *db\_status* pour savoir si la base de données est bien connectée. Une fois cette action vérifiée, nous allons initialiser un espace de travail avec *workspace -a pentest,* où pentest sera le nom de l’espace de travail et le -a montre qu’il faut le créer. Ceci effectué nous lançons un scan   
*db\_nmap -sV -O 172.16.110.0/24*Afin de connaitre les services et les O.S. du réseau dans lequel nous évoluons. Grace aux commandes *services* et *host* nous constatons qui y a un Active Directory disponible. Connaissant une faille SMB, nous décidons de prendre ce chemin pour nous infiltrer. Nous utilisons donc ce un script disponible via la commande :

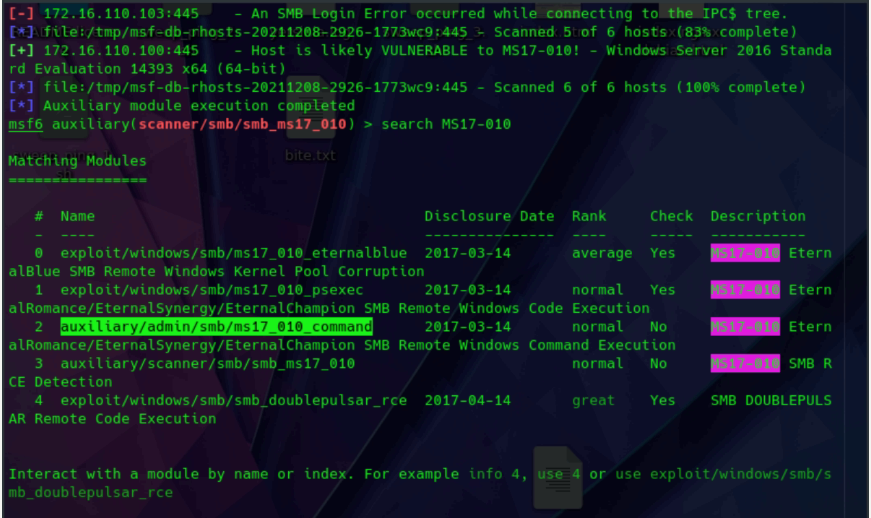
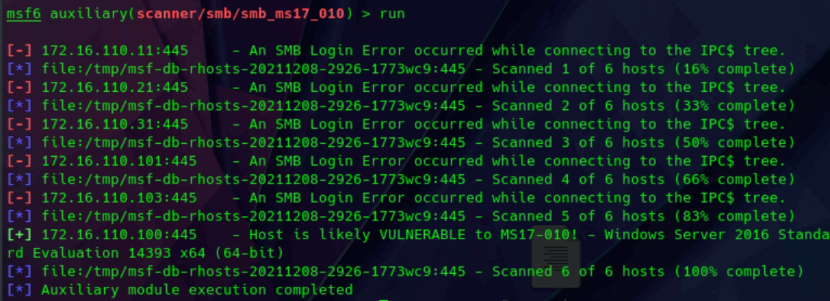
*Use auxiliary/scanner/smb/smb\_ms17\_010*

Grace à la commande *options,* Nous constatons que les options RHOSTS et RPORT sont indispensables. L’option RPORT étant renseignée par défaut, il ne reste plus qu’à spécifier l’option RHOSTS. Cependant, plutôt que de la renseigner à la main, nous allons utiliser la commande suivante pour mettre dans les RHOSTS (-R) tous les hosts qui ont le service 445 (-p) ouvert (-u).

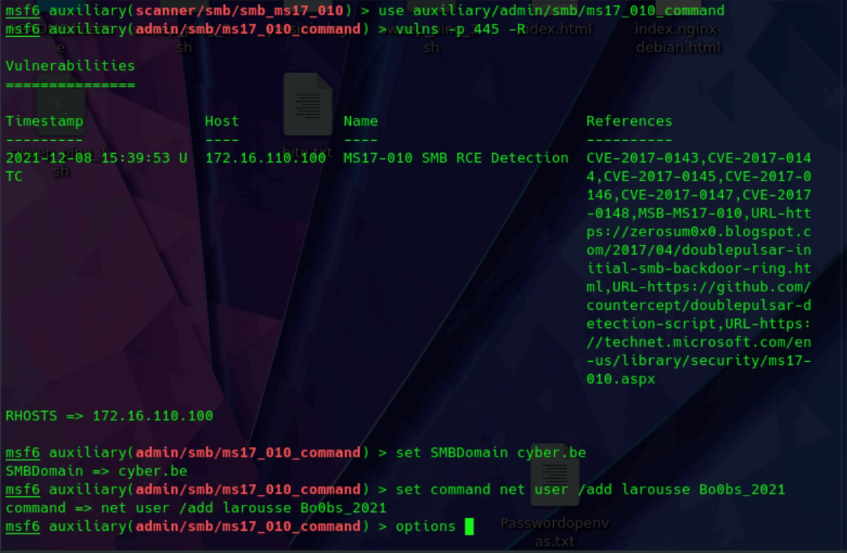
*Services -u -p 445 -R*

Grâce au scan nmap utilisé précédemment, nous connaissons aussi le domaine cyber.be que nous allons renseigner.



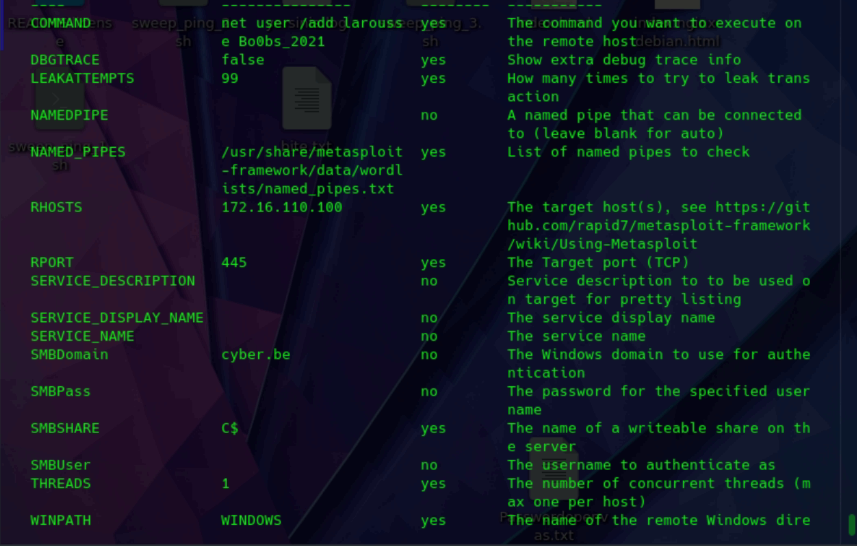


En lançant le script nous découvrons une faille MS17-010 sur le SMB nous permettant d’envoyer des commandes admin sur le serveur. Une aubaine pour nous, nous décidons de fait de l’utiliser.

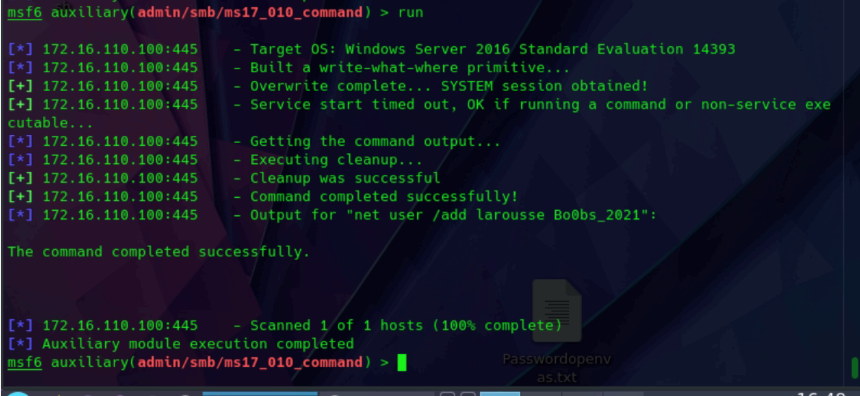


Nous paramétrons l’option RHOSTS du module grâce à la liste des machines et des services déjà identifiés comme vulnérables et nous paramétrons le domaine comme étant cyber.be. Nous utilisons ensuite l’option command pour nous ajouter un utilisateur dans l’Active Directory.

Nous vérifions que tous les paramètres ont bien été entrés dans le script avant de le lancer



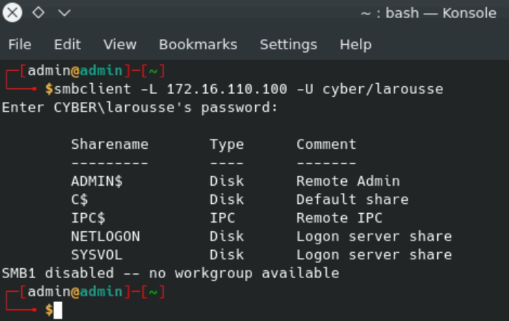
Et, enfin, nous lançons le script.



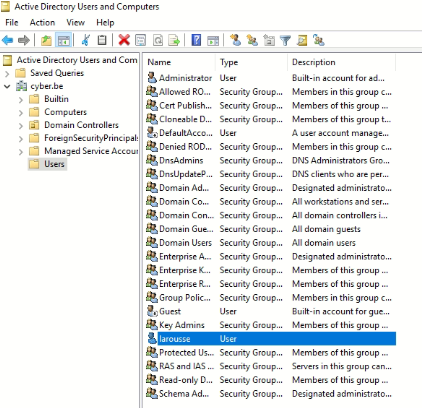
Metasploit nous confirme que la commande a bien été entrée, nous décidons donc de faire passer la commande

*Set COMMAND net group \ ‘’Domain Admins\’’ larousse /domain /add*

Afin de se garantir les droits administrateurs sur le domaine. Il nous est maintenant possible de nous connecter simplement sur le serveur via la Konsole de Parrot OS pour pouvoir visualiser tous les fichiers de l’Active Directory.



Et en se connectant sur l’Active Directory, nous pouvons constater notre présence dans la liste des utilisateurs.



Ceci n’est qu’une démonstration de ce qu’il est possible de faire grâce à metasploit et au script que nous avons utilisé. Il aurait été possible d’être beaucoup plus virulent lors de l’exécution de celui-ci, par exemple en récupérant toutes les données du serveur ou même en changeant le mot de passe administrateur, …

# Conclusion

Nous avons pu constater au cours de ces quatre semaines de Playzone, qu’avec des connaissances assez abouties en réseau et en sécurité de l’informatique, il est relativement aisé de pratiquer des pentest et du ethical hacking. Néanmoins, il est important de garder à l’esprit que toutes les manipulations faites dans le cadre d’ethical hacking sont approuvées par l’infrastructure qui se prête à celui-ci. Le piratage informatique est puni par la loi et il va donc en soit que les compétences obtenues dans ce domaine ne doivent servir en but que le test sur des infrastructures consciente du travail qui va être effectué derrière.

Je terminerai par un mot personnel simplement en remerciant le centre de formation Technobel ainsi que notre formateur Jean de nous avoir permis de développer de tels compétences durant l’année 2020, je peux vous assurer que malgré plusieurs échecs lors de nos phases de travail, nous avons su garder la tête sur les épaules et trouver toujours plus de manières d’avancer et de trouver de nouvelles manières d’agir. Et se faisant, certaines fonctionnaient nous refaisant monter en nous les étoiles dans les yeux et la joie d’un enfant ouvrant ses cadeaux de noël. Alors je ne dirai qu’une seule chose : Merci de votre temps et votre patience nous permettant d’avancer toujours plus vers notre futur métier.