



Mémoire de stage pour l’obtention du Diplôme Universitaire de Technologie Réseaux

Et Télécommunications

Département Réseaux et Télécommunications

Promotion 2020/2021

**Kajanthan SINNATHURAI**

**Mise en place d’une intrusion dans un système sécurisé :**

Sous la responsabilité de : Monsieur Brice AUGUSTIN

## 

## Remerciements :

Je tiens à remercier les professeurs de l’IUT Créteil-Vitry pour avoir pris le temps de rédiger des sujets de substitutions pour les étudiants qui n’avaient pas de stage et d’accompagner les étudiants afin obtenir leur DUT.

Je remercie Monsieur Samer MOHAMMED pour nous fournir les consignes et les matériels nécessaire afin de réaliser ce projet.

Je remercie fortement Monsieur Brice AUGUSTIN pour m’avoir guidé, conseillé sur la réalisation de ce projet et aussi pour l’écriture de ce rapport. Je le remercie pour sa confiance en moi car il me laissait travailler en autonomie et que je n’avais pas l’obligation de venir à l’IUT pour effectuer ce projet, je pouvais le faire à distance dans les horaires qui me convenaient. Il était toujours présent pour mes nombreuses questions concernant le sujet. De plus, merci pour vos conseils sur l’utilisation de certain logiciel en Réseau et aussi pour les explications.

Je remercie également Madame Anne-Paule SANTUCCI pour les cours qu’on a pu avoir avec vous et pour les conseils afin de rédiger un bon rapport de stage.

Je remercie aussi Amine ABDOUL-AZID, c’est un étudiant de Licence Pro à l’IUT de Créteil-Vitry. Il a apporté beaucoup d’explications sur mon projet et des conseils pour bien réaliser ce projet.

Je remercie aussi Mohammed DIABY, c’est un étudiant avec qui j’ai pu réaliser ce projet. J’ai pu travailler avec lui pour partager ma maquette et l’avancement du projet.

Je remercie l’ensemble des personnes qui liront dans le futur mon rapport.

## SOMMAIRE :

[Remerciements : 2](#_Toc76850692)

[SOMMAIRE : 3](#_Toc76850693)

[Glossaire des figures : 4](#_Toc76850694)

[Section n°1 : Introduction générale 5](#_Toc76850695)

[Section n°2 : Contexte et théorie liée au sujet, adéquation aux DUT 6](#_Toc76850696)

[Section n°3 : Présentation de la réalisation technique 9](#_Toc76850697)

[Section n°3 : PARTIE 1 : 9](#_Toc76850698)

[Section n°3 : Partie 2 : 11](#_Toc76850699)

[ROUTEUR : 11](#_Toc76850700)

[SERVEUR WEB : 12](#_Toc76850701)

[A6) 15](#_Toc76850702)

[A7) 18](#_Toc76850703)

[POSTE DE TRAVAIL : 18](#_Toc76850704)

[SERVEUR WWW : 20](#_Toc76850705)

[A8) 24](#_Toc76850706)

[POSTE DE TRAVAIL : 25](#_Toc76850707)

[FTP-PIRATE 25](#_Toc76850708)

[A9) 27](#_Toc76850709)

[SSH-PIRATE : 27](#_Toc76850710)

[POSTE : 27](#_Toc76850711)

[SSH-PIRATE : 28](#_Toc76850712)

[A10) 29](#_Toc76850713)

[POSTE : 29](#_Toc76850714)

[Glossaire : 33](#_Toc76850715)

[Conclusion 34](#_Toc76850716)

[TP Audit de sécurité : 35](#_Toc76850717)

[Sources*:* 36](#_Toc76850718)

## Glossaire des figures :

[Figure 1 : La maquette complexe de la situation mis en place 7](#_Toc76850648)

[Figure 2 : La maquette simplifié de la situation mis en place 8](#_Toc76850649)

[Figure 3 : Visa de sécurité proposée par l'ANSSI 10](#_Toc76850650)

[Figure 4 : VM mis en place 11](#_Toc76850651)

[Figure 5 : Transformer un PC en routeur 11](#_Toc76850652)

[Figure 6 : Mise en place du serveur web 12](#_Toc76850653)

[Figure 7 : Recherche de PHP7 13](#_Toc76850654)

[Figure 8 : Installation de PHP7.0 13](#_Toc76850655)

[Figure 9 : Configuration du serveur web 14](#_Toc76850656)

[Figure 10 : Vérification de la configuration du serveur web 14](#_Toc76850657)

[Figure 11 : Historique des commandes 15](#_Toc76850658)

[Figure 12 : Installation de NMAP 16](#_Toc76850659)

[Figure 13 : Exécution de la commande NMAP 16](#_Toc76850660)

[Figure 14 : Installation et exécution de la commande TCPDUMP 17](#_Toc76850661)

[Figure 15 : Analyse de Wireshark 17](#_Toc76850662)

[Figure 16 : Création du compte utilisateur Lorie 18](#_Toc76850663)

[Figure 17 : Connexion à distance 19](#_Toc76850664)

[Figure 18 : Fichier Hosts sur le poste 20](#_Toc76850665)

[Figure 19 : Connexion en SSH 20](#_Toc76850666)

[Figure 20 : Fichier Hosts sur le WEB 21](#_Toc76850667)

[Figure 21 : Le fichier auth.log sur le Web 21](#_Toc76850668)

[Figure 22 : Le fichier Auth.log sur le poste 22](#_Toc76850669)

[Figure 23 : Identifier les utilisateurs 22](#_Toc76850670)

[Figure 24 : Installation Hydra 23](#_Toc76850671)

[Figure 25 : Téléchargement du fichier 500 pires MDP 23](#_Toc76850672)

[Figure 26 : Exécution de la commande HYDRA 24](#_Toc76850673)

[Figure 27 : Création des fichiers confidentiels 25](#_Toc76850674)

[Figure 28 : Connexion en FTP 25](#_Toc76850675)

[Figure 29 : Modification du fichier FTP 26](#_Toc76850676)

[Figure 30 : Redémarrage du service vsftpd 26](#_Toc76850677)

[Figure 31 : Liste des fichiers exfiltrés 26](#_Toc76850678)

[Figure 32 : Création du point de collecte 27](#_Toc76850679)

[Figure 33 : Création des fichiers confidentiel POT 27](#_Toc76850680)

[Figure 34 : Listes des fichiers récupérés 27](#_Toc76850681)

[Figure 35 : Le script mis en place pour transférer des fichiers 28](#_Toc76850682)

[Figure 36 : Le script est supprimé après l'exécution 28](#_Toc76850683)

[Figure 37 : Les fichiers "pots de vin" sur le PC pirate 28](#_Toc76850684)

[Figure 38 : Script pour une connexion TCP 29](#_Toc76850685)

[Figure 39 : Liste du répertoire des programmes 29](#_Toc76850686)

[Figure 40 : La tâche Crontab à 3h 30](#_Toc76850687)

[Figure 41 : Exécution de TCPDUMP 30](#_Toc76850688)

[Figure 42 : Analyse avec Wireshark 31](#_Toc76850689)

[Figure 43 : Message envoyé par le pirate 31](#_Toc76850690)

[Figure 44 : Usage du reverse-shell 32](#_Toc76850691)

## Section n°1 : Introduction générale

Arrivant à la fin de ma formation initiale de DUT Réseau & Télécommunications à l’IUT de Créteil-Vitry, pour obtenir le diplôme universitaire de technologie (DUT), je devais réaliser un stage de 10 semaines en entreprise du 19/04/2021 au 25/06/2021. Néanmoins l’IUT de Créteil -Vitry a mis en place des sujets de substitutions.

Après plusieurs propositions de sujet par Monsieur MOHAMMED, j’ai choisi de faire un sujet qui était de créer un bot qui est un agent virtuel programmé qui réalise des actions comme des réponses ou la possibilité d’afficher des informations avec mon tuteur était Monsieur AUGUSTIN.

Monsieur AUGUSTIN m’a informé que certains sujets n’étaient pas à jour et nous a proposé de nouveaux sujets.

J’ai donc choisi de faire un projet sur le thème de la sécurité car ce projet me permet de découvrir davantage sur le monde de l’informatique et de la sécurité.

De plus, ce projet répond aux critères de la formation cycle ingénieur Réseaux et Sécurité.

Le but de mon projet est de réaliser un travaux pratique pour les étudiants de 2e année qui prendra la forme d’une enquête informatique.

Je devais écrire un scénario avec une entreprise qui se fait pirater.

Donc le but de ce TP est de savoir comment le pirate est rentré dans le réseau de l’entreprise et aussi savoir ce qu’il a fait sur les ordinateurs et quelles sont les données qui ont été dérobées.

De plus, je devais faire rendre compréhensible ce sujet pour les étudiants de 2e année.

La question intéressante qui nous motive à travailler sur ces projets est la question suivante :

**Comment éviter de se faire pirater les données de l’entreprise ?**

## Section n°2 : Contexte et théorie liée au sujet, adéquation aux DUT

Pour commencer, j’ai mis en place la maquette qui résume bien le scénario du tuteur pour mieux visualiser et comprendre le scénario, savoir ce je dois faire, quel est le rôle de chaque équipement. Je peux mettre en évidence les erreurs telle qu’une mauvaise attribution d’adresses IP pour des équipements, je peux toujours revoir et corriger sur ma maquette.

D’abord j’ai fait une maquette un peu plus complexe qui résume bien le scénario.

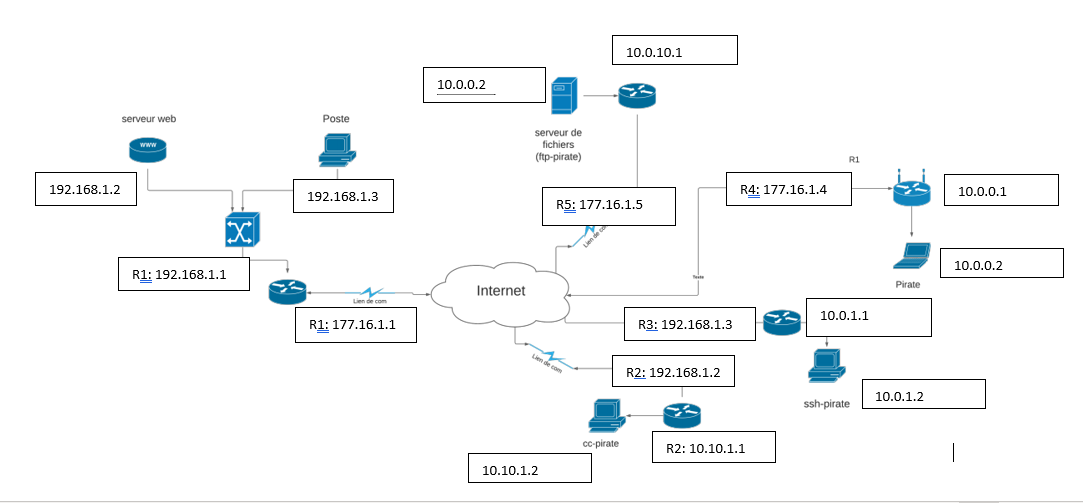
On a d’un côté l’entreprise avec un serveur WEB et un poste de travail.

Ces deux équipements sont reliés sur un switch qui permet l’interconnexion d’appareils communicants. Et ce switch est connecté à un routeur qui permet d’accéder à internet mais aussi de communiquer à l’extérieur de l’entreprise.

On a l’autre côté des pirates qui sont connecter sur plusieurs routeurs dans des endroits différents pour dissimuler leur trace. On a plusieurs équipements côté pirate :

* Serveur de fichier (FTP-Pirate)
* PC Pirate
* SSH-Pirate
* CC-pirate

Ces différents équipements vont permettre au pirate de se connecter à distance, exfiltrer des fichiers et de récupérer ces fichiers sur son PC à lui.

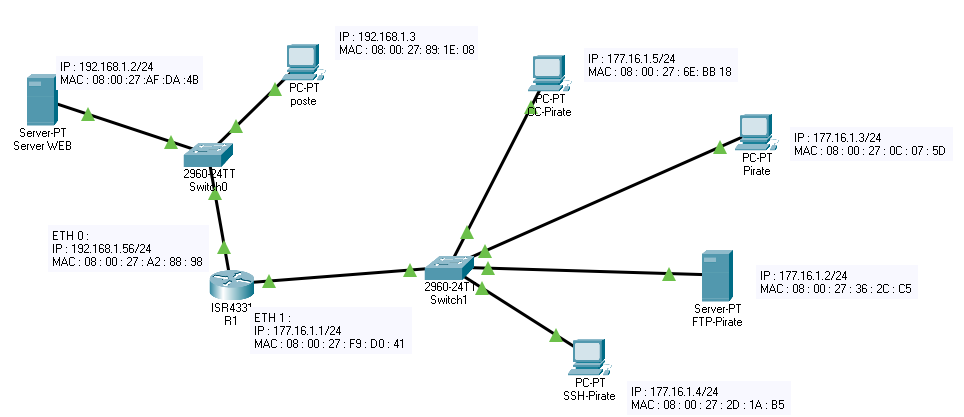


Pirate :

Entreprise :

Figure 1 : La maquette complexe de la situation mis en place

Dans cette deuxième maquette je décide de simplifier les choses après la demande de mon tuteur car cela va me faciliter la mise en place de cette maquette physiquement. Donc je décide d’enlever les routeurs du côté pirate et je les relie avec un switch.



Entreprise :

Pirate :

Figure 2 : La maquette simplifié de la situation mis en place

Pour chaque équipement, j’attribue des adresse IP, c’est un numéro d’identification qu’on attribue à une machine qui est connecté à un réseau. Cet identifiant permet de communiquer entre machine et échanger des données sur Internet.

On peut aussi voir qu’ils ont des adresses MAC, cela permet à identifier de manière unique, un périphérique réseau.

## Section n°3 : Présentation de la réalisation technique

## Section n°3 : PARTIE 1 :

Lors de la réalisation de mon projet, j’ai d’abord commencé par effectuer des recherches pour savoir comment une entreprise est sécurisée, comment elle se fait pirater, quelles sont les attaques les plus connus.

Ensuite, je voulais comprendre les notions de sécurité car sur le thème de sécurité, je n’avais pas de connaissance approfondie et c’est je souhaitais d’apprendre davantage. De plus, mon but premier était donc de m’imposer une routine de travail afin de respecter un quota d’heures et pouvoir faciliter ma motivation au travail.

J’ai donc choisi de mettre en place une routine qui était de venir à l’IUT de 9H à 12H et l’après-midi de 13H à 16H, tous les jours de la semaine, ainsi que le Week-end.

Une fois cette routine mise en place, les deux premières semaines de mon projet étaient dédiées aux recherches, ce qui m’as permis de me renseigner bien plus sur ce sujet que je ne maîtrisais pas.

Par la suite, j’ai pris contact avec M. AUGUSTIN afin de lui demander des conseils et de savoir quelles sont les consignes qu’on doit respecter pour la réalisation de ce projet.

J’ai donc reçu des conseils de la part de M. AUGUSTIN, de même il nous a conseillé de faire une formation sur le thème de sécurité en s’inscrivant sur un « MOOC ». C’est une formation mise en place par l’ANSSI, c’est un service français créé par décret qui est l’acteur majeur de la²cybersécurité²qui²apporte²son²expertise²pour²les²entreprises (<https://www.secnumacademie.gouv.fr/>).



Figure 3 : Visa de sécurité proposée par l'ANSSI

Cette formation constitue à faire une bonne introduction à la sécurité et qu’on aura besoin pour notre projet.

Cette formation m’a permis aussi de développer des compétences et des connaissances sur le thème de sécurité. J’ai pu comprendre et apprendre les différents types de pirates qu’une entreprise ou un particulier peut avoir, mais aussi pour bien sécurisé son PC et d’éviter les pirates.

Ensuite notre tuteur, nous a partagé le descriptif du scénario qu’il avait imaginé.

Pour qu’on respecte les critères de stage, nous avons travaillé chacun de son côté, en effet il a divisé ce projet en deux sous-parties.

Mohammed DIABY s’occupait de la première partie tandis que moi je devais faire la deuxième partie.

## Section n°3 : Partie 2 :

Après avoir mis en place la maquette et les recherches que j’ai pu faire, je débute ce projet sur des machines virtuelles afin de mettre en place le scénario du tuteur.

J’utilise donc sept VM, je commence par configurer tous les équipements avec des adresses IP statiques comme sur la maquette :

Une image contenant texte

Description générée automatiquement

Figure 4 : VM mis en place

### ROUTEUR :

Dans le fichier « /etc/sysctl.conf » je décommente l’IPv4 pour rendre ma VM en tant que routeur, ce qui permettra de communiquer vers l’extérieur.

On utilise la commande « sysctl -p » pour voir et appliquer la modification qu’on a fait dans le fichier précédent :

Une image contenant texte

Description générée automatiquement

Figure 5 : Transformer un PC en routeur

### SERVEUR WEB :

Sur le serveur Web, j’installe *apache2* qui va permettre d'écouter en tant que serveur web ainsi que les requêtes émises par les navigateurs (qui demandent des pages web), de chercher la page demandée et de la renvoyer.

#### Installation de apache2 :

Une image contenant texte

Description générée automatiquement

Figure 6 : Mise en place du serveur web

J’essaie d’installer php7 mais la commande ne fonctionne pas sur les nouvelles versions de Debian donc je décide de vérifier toutes les versions disponibles de php avec la commande : « apt search php ».

Une image contenant texte

Description générée automatiquement

Figure 7 : Recherche de PHP7

J’ai remarqué que « le store » me propose d’installer php avec le paquet php-7.0.

#### J’installe php :

Une image contenant texte

Description générée automatiquement

Figure 8 : Installation de PHP7.0

La racine du serveur web avec apache2 est situé dans /var/www/html Je fais une copie du fichier index.html original en tant que index.html.copie (cette étape de sauvegarde est optionnel) .

Je supprime avec rm le fichier index.html ensuite je crée un nouveau fichier index.html

Puis je renomme index.html vers index.php avec index.php

Enfin, je teste la fonction phpinfo() dans ce fichier présent dans index.php

Une image contenant texte

Description générée automatiquement

Figure 9 : Configuration du serveur web

Je fais un « ls » dans le répertoire « /var/www/html » pour voir les fichiers présents.

Je renomme « index.html » en tant que « index.php » avec la commande « mv » car je souhaite utiliser le serveur php :

Une image contenant texte

Description générée automatiquement

Figure 10 : Vérification de la configuration du serveur web

Je fais un « history » pour voir toutes les commandes qui a été utilisé sur cette machine :

Une image contenant texte

Description générée automatiquement

Figure 11 : Historique des commandes

# A6)

Dans cette partie nous savons que le pirate a réussi à pénétrer dans le réseau de l’entreprise à cause une faille dans la page « ping.php » et « log.php » (la partie de MOHAMED).

Avec le fichier « log.php » le pirate découvre le mot de passe de www (web). Donc il a l’accès dans le réseau de l’entreprise et donc sur le serveur web de l’entreprise.

Le pirate va s’en servir d’une technique de scan de ports avec le logiciel « NMAP » qu’il va mettre en place sur le serveur Web. Par conséquent, NMAP est utilisé pour détecter les ports ouverts dans le réseau à distance.

Le pirate va utiliser ce logiciel pour découvrir s’il existe d’autres utilisateurs dans ce même réseau et s’il existe il va avoir l’adresse IP de cet utilisateur. Et par la suite, il pourra prendre le contrôle sur le pc de cet utilisateur et récupérer des documents confidentiels.

Le pirate installe le logiciel « nmap » qui va servir à scanner le réseau de l’entreprise :

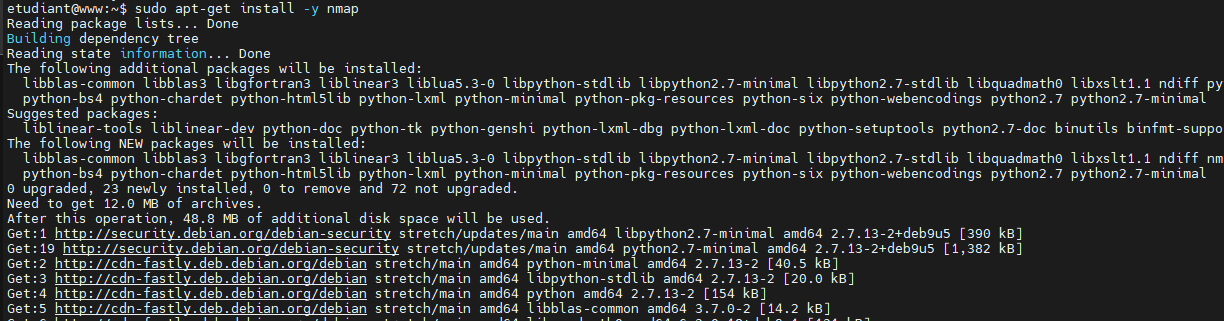


Figure 12 : Installation de NMAP

La commande qui va permettre au pirate de savoir l’existence des autres adresse IP de ce réseau est : « nmap -T4 -sP 192.168.1.0/24 | grep for »

- « T4 » : permet de définir le modèle de synchronisation, il est entre 0 et 5, plus le chiffre est proche de 5 plus ça va accélérer l’analyse de nmap dans le réseau.

- « sP » : Sweep Ping force à utiliser le protocole ARP

- « 192.168.1.0/20 » je défini l’adresse du réseau dans lequel nmap doit analyser, dans notre cas c’est l’adresse réseau de l’entreprise.

- « grep for » permet d’afficher toutes les lignes avec le mot « for »

Une image contenant texte

Description générée automatiquement

Figure 13 : Exécution de la commande NMAP

Par la suite, pour obtenir le détail du trafic depuis une interface réseau, je décide d’utiliser le logiciel « tcpdump ».

Tcpdump est un analyseur de paquets en ligne de commande ce qui va me permettre de voir les flux de réseau.

J’installe « tcpdump » et j’essaie de voir les flux de réseau en essayant de recharger les pages web.

Tcpdump va jouer le rôle de Wireshark en ligne de commande :

Une image contenant texte

Description générée automatiquement

Figure 14 : Installation et exécution de la commande TCPDUMP

Les fichiers «. pcap » peuvent être ouverts sur Wireshark ce qui permet d’avoir une interface graphique.

Voici l’analyse du paquet ssh entre le serveur et l’hôte, on voit l’adresse ip du serveur web :

Nmap n’utilise pas le protocole ICMP (qui simulerait des pings à toutes les adresses IP) pour analyser le réseau.

Une image contenant texte

Description générée automatiquement

Figure 15 : Analyse de Wireshark

En effet on constate qu’il utilise le protocole ARP, peut-être pour récupérer le nom d’hôte DNS et éviter de se faire détecter/bloquer par un pare-feu.

En effet le protocole ARP est utilisé car on a utilisé les options « -T4 **-sP** ».

# A7)

Dans cette partie, le pirate va découvrir l’existence du poste de travail via une attaque de type brute-force.

L’attaque par force brute est une méthode utilisée pour trouver un mot de passe ou une clé. Pour cela, on met en place un logiciel qui va permettre de tester, une à une, toutes les combinaisons possibles.

### POSTE DE TRAVAIL :

Je crée un utilisateur sur poste de travail qui est « lorie » avec la commande « adduser $name » et je lui attribue un mot de passe qui va être dans les 500 pire mots de passe. Je lui attribue le mot de passe : **coffee**

Ensuite je me connecte sur « lorie » avec la commande « su - lorie » et avec le mot de passe que je lui ai attribué :

Une image contenant texte

Description générée automatiquement

Figure 16 : Création du compte utilisateur Lorie

J’essaie de faire un SSH (connecter à distance) avec le compte de « lorie » vers le serveur Web avec la commande « ssh etudiant@www » mais malheureusement cette commande ne fonctionne pas car dans le fichier « hosts » je n’ai pas attribué le nom de domaine qui correspond à l’adresse IP.

Et le SSH fonctionne avec l’adresse IP du serveur.

Une image contenant texte

Description générée automatiquement

Figure 17 : Connexion à distance

Je modifie le fichier « hosts » en attribuant le nom de domaine qui correspond à l’adresse IP :

Une image contenant texte

Description générée automatiquement

Figure 18 : Fichier Hosts sur le poste

Après la modification du fichier « hosts » le SSH fonctionne avec le nom de domaine « www » :

Une image contenant texte

Description générée automatiquement

Figure 19 : Connexion en SSH

### SERVEUR WWW :

Je modifie également le fichier « hosts » sur le serveur web : Qui permet la résolution de nom en local c’est-à-dire lier une adresse IP, à un nom de domaine, une suite de lettre séparé par des points :

Une image contenant texte

Description générée automatiquement

Figure 20 : Fichier Hosts sur le WEB

Dans le fichier « auth.log » on peut voir les connexions effectuées sur cette machine et savoir quelle machine s’est connecté. Pour voir ce fichier, on utilise la commande « cat /var/log/auth.log » :

Par ailleurs, on peut observer qu’un utilisateur a déjà essayé de se connecter sur le web en SSH, l’utilisateur est « lorie » son adresse IP est « 192.168.1.3 ».

Donc le pirate est au courant un autre utilisateur dans le même réseau que serveur web et il a aussi le nom de cet utilisateur qui est « lorie ».

Une image contenant texte

Description générée automatiquement

Figure 21 : Le fichier auth.log sur le Web

Depuis le poste :

Une image contenant texte

Description générée automatiquement

Figure 22 : Le fichier Auth.log sur le poste

Cette commande permet de voir l’utilisateur qui s’est connecté :



Figure 23 : Identifier les utilisateurs

Cette commande affiche le fichier auth.log pour l’adresse IP du poste

Nous avons le fichier, nous recherchons l’adresse ip de www, avec le mot user et le mot Invalid ensuite on récupère la 8ème colonne séparé par un espace, on trie en retirant les doublons.

Pour trouver le mot de passe de cet utilisateur Lorie, nous allons utiliser l’attaque par force brute. Pour effectuer cette attaque, je décide d’utiliser le logiciel « hydra ».

Hydra est un crackeur de mot de passe. Il permet de tester plusieurs mots de passe pour l’utilisateur Lorie et qu’il va essayer toutes les possibilités possibles.

Le pirate installe « hydra » sur le serveur Web qui va permettre de cracker les mots de passe :

Une image contenant texte

Description générée automatiquement

Figure 24 : Installation Hydra

Avec la commande « curl » je télécharge les 500 pires mots de passe et que le mot de passe « coffee » de Lorie il fait partie de cette liste :

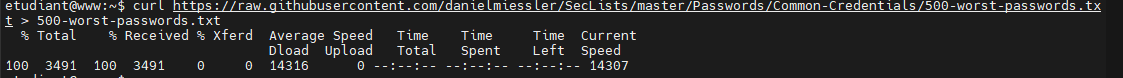


Figure 25 : Téléchargement du fichier 500 pires MDP

Avec la commande « hydra -l lorie -p 500-worst-passwords.txt poste ssh», on récupère le mot de passe de Lorie qui est « coffee » :

* « l » permet de définir l’identifiant de l’utilisateur qui est Lorie
* « p » c’est pour définir de tester les mots de passe dans le fichier suivant qui est les 500 pires mots de passe.
* « ssh poste » pour définir la connexion à distance sur le poste qui est l’hôte en SSH.

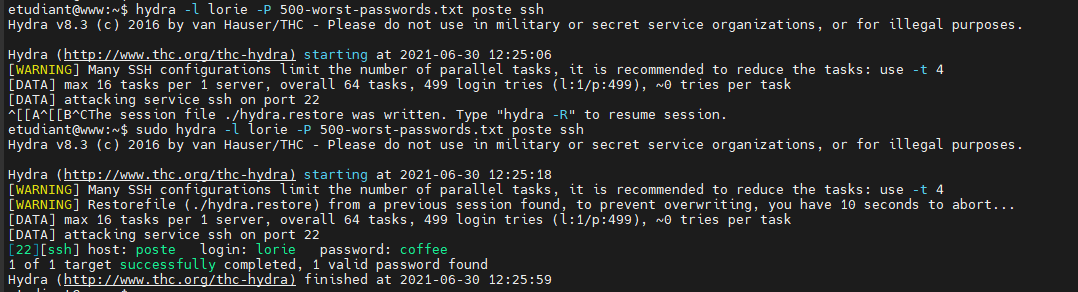


Figure 26 : Exécution de la commande HYDRA

On peut remarquer que sur l’hôte de poste pour l’identifiant Lorie on a un mot de passe qui est Coffee. Donc nous avons le mot de passe de l’autre utilisateur qui est connecté dans le même réseau que le serveur Web et qui est dans le réseau de l’entreprise.

Le pirate a donc accès à l’ensemble de l’entreprise (serveur Web et Poste de travail) et il peut récupérer les documents confidentiels ou mettre en panne les PC.

# A8)

Nous savons que le pirate a le contrôle sur le serveur Web et sur le poste de travail. Dans cette partie, le pirate va profiter de l’accès au réseau de l’entreprise pour exfiltrer des fichiers.

Sur le serveur web et poste j’installe FTP et le serveur VSFTPD qui va permettre d’exfiltrer les fichiers.

FTP (FILE TRANSFER PROTOCOL), est un protocole de communication qui permet de partager des fichiers sur un réseau TCP/IP.

VSFTPD est un serveur FTP qui est installé sur un ordinateur pour autoriser le téléchargement, la lecture, la modification ou la suppression à distance de fichiers par utilisateur.

### POSTE DE TRAVAIL :

Sur le poste de travail je crée les fichiers draft\_iphone30.docx et client\_database.sql :

Une image contenant texte

Description générée automatiquement

Figure 27 : Création des fichiers confidentiels

Je me connecte en ftp de poste vers le ftp-pirate ce qui va me permettre d’envoyer des fichiers de poste vers le ftp-pirate, j’utilise pour cela la commande MPUT.

La commande MPUT permet de transférer d’un PC à un serveur FTP vers le chemin indiqué.

MPUT \* permet d’envoyer tous les fichiers disponibles présent dans le répertoire du poste.

Une image contenant texte

Description générée automatiquement

Figure 28 : Connexion en FTP

### FTP-PIRATE

Après l’installation de FTP et VSFTPD, je dois donner l’accès en écriture et de lecture des fichiers car sinon le transfert de fichier ne fonctionnera pas.

Et par la suite je dois redémarrer le serveur FTP pour qu’il prenne en compte les modifications qu’on a effectuées dans le fichier /etc/vsftpd.conf :

Une image contenant texte

Description générée automatiquement

Figure 29 : Modification du fichier FTP



Figure 30 : Redémarrage du service vsftpd

Pour vérifier si les fichiers sont bien arrivés j’utilise la commande « ls » pour voir les fichiers présents sur le ftp-pirate et on peut remarquer que le transfert de fichier à bien marcher car on a les deux fichiers (draft\_iphone30.docx et client\_database.sql) qui étaient sur le poste et que on l’a maintenant sur le PC de pirate :

Une image contenant texte

Description générée automatiquement

Figure 31 : Liste des fichiers exfiltrés

# A9)

### SSH-PIRATE :

Je crée un répertoire « data » pour mettre les fichiers confidentiels cela va permettre au pirate de redirigé les fichiers directement vers « data » et les fichiers exfiltrer ne seront pas sur le répertoire courant :



Figure 32 : Création du point de collecte

### POSTE :

On a généré des fichiers confidentiels au format XLSX (EXCEL) :

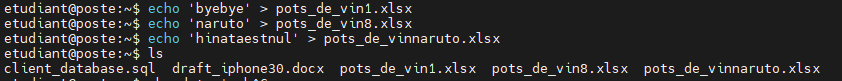


Figure 33 : Création des fichiers confidentiel POT

On affiche l’ensemble des fichiers liés à ce motif « pots\_de\_vin\*.xlsx », la commande avec une étoile permet de chercher tous les fichiers où il y a le nom « pots-de-vin » devant et **tout caractère qui suit** suivi du .xlsx:



Figure 34 : Listes des fichiers récupérés

Je crée un script « exfiltration.sh » qui va permettre de récupérer les fichier « pots de vin » et que je transfère vers le ssh-pirate dans le « data » :

Dans le script, je défini l’identifiant et le mot de passe (étudiant et vitrygtr), ensuite j’indique vers quel adresse IP les fichiers doit être envoyer (ssh-pirate), par la suite j’identifie quel fichier doit être envoyé. J’écris une ligne de commande en plus avec « sshpass » cette commande va permettre d’exécuter le fichier « exfiltration.sh » sans nous demander le mot de passe car je lui indique quel mot de passe utiliser.

Après que les fichiers sont envoyés je supprime le fichier « exfiltation.sh » donc ce script se supprime sur le poste pour pas laisser de trace pour l’administrateur de Réseau.

Une image contenant texte

Description générée automatiquement

Figure 35 : Le script mis en place pour transférer des fichiers

Je vois que le fichier est supprimé après son exécution comme j’ai demandé :

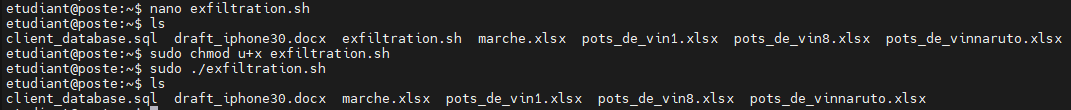


Figure 36 : Le script est supprimé après l'exécution

### SSH-PIRATE :

ssh-pirate récupère l’ensemble de l’information qui était dans le poste, donc les fichiers « pots de vin » ont bien été transféré de poste vers le ssh-pirate grâce au script que le pirate a mis en place :



Figure 37 : Les fichiers "pots de vin" sur le PC pirate

# A10)

### POSTE :

Je crée un script pour créer un « reverse-shell ».

Le paramètre -l permet de le démarrer en tant que serveur.

Tandis que l’option -p spécifie le port d’écoute 4242.

On redirige la commande dans /dev/null avec l’affichage de la sortie standard et d’erreur.

Ce qui permet d’éviter de voir le contenu taper à 3H du matin ou le lendemain à l’écran et d’effacer les traces de l’exécution de cette tâche planifiée. De plus, l’utilisateur de poste ne peut pas envoyer de message au pirate sans modifier le script.

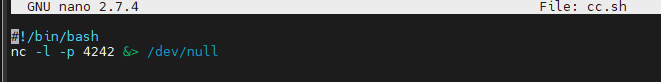


Figure 38 : Script pour une connexion TCP

Ce script pour éviter de se faire démasquer est placer dans le répertoire des programmes courants : /etc voire /usr/bin

Une image contenant texte, mur, moniteur, noir

Description générée automatiquement

Figure 39 : Liste du répertoire des programmes

On exécute crontab avec nano, il édite le fichier crontab

Ensuite on liste les tâches crons avec crontab -l

Une image contenant texte

Description générée automatiquement

Figure 40 : La tâche Crontab à 3h

Tout d’abord, je lance tous les jours tcpdump sur le poste.

Ensuite je récupère le fichier généré .pcap

Enfin, j’analyse le port d’écoute, et l’adresse IP, port dynamique (50616) de cc-pirate

Par ailleurs, je filtre sur l’heure et sur les adresses de destinations :

Une image contenant texte

Description générée automatiquement

Figure 41 : Exécution de TCPDUMP

Une image contenant texte

Description générée automatiquement

Figure 42 : Analyse avec Wireshark

On met un filtre qui filtre sur les adresses différentes de 192.168.1.3 (poste), on peut remarquer que le protocole TCP est utilisé sur le port 4242 et on peut voir le message envoyé par le pirate : ex : rm fichiers, « augustin is the best ».

On peut voir que le pirate a envoyé ces messages vers le poste de travail mais que les commandes ne sont pas exécutées.

Une image contenant texte

Description générée automatiquement

Figure 43 : Message envoyé par le pirate

On peut utiliser des commandes à distances, ici on peut voir que whoami montre que l’attaquant utilise le compte étudiant.

Néanmoins étudiant pouvant utiliser sudo, il peut faire une élévation de privilèges.

De plus on peut voir que le répertoire courant sur le terminal, cependant le pirate doit visionner sur le terminal de poste sauf s’il transfère le résultat sur un de ces postes pirates…

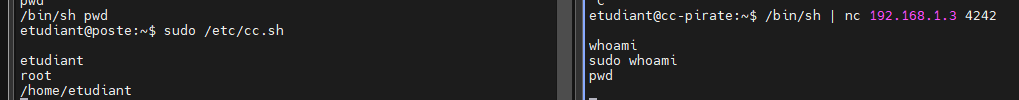


Figure 44 : Usage du reverse-shell

## Glossaire :

IUT : Institut Universitaire Technologique

DUT : Diplôme Universitaire Technologique

BAC : Baccalauréat

TP : Travaux pratique

ELEVATION DE PRIVILEGE : Un utilisateur normal gagne des droits d’accès c’est-à-dire devenir administrateur (root).

SWITCH : Commutateur

PC : Personal Computer

VM : Virtual Machine

SSH : Secure Shell

MAC : Media Access Control

MOOC : Formation en ligne

ANSSI : Agence nationale de la sécurité des systèmes d'information

Debian : Distribution simple pour le système d’exploitation Linux

Paquetage : Fichiers installables similaire à une application

Gestionnaire de paquets : APT Advanced package Tool est l’équivalent d’un Windows Store mais en ligne de commandes.

Réseau TCP/IP : Protocole utilisé pour un transfert de donnée sur internet

/dev/null : Est l’équivalent d’un trou-noir mais pour des fichiers par conséquent les fichiers sont supprimés dès qu’ils sont créées.

SSH :

Wireshark :

## Conclusion

Le sujet de substitution que M. AUGUSTIN nous a proposé, s’est bien très bien passé. C’était également l’occasion de travailler en autonomie sur un projet dans mon domaine d’études. Malgré que je n’ai pas pu réaliser un stage afin de valider mon DUT, de découvrir le monde de travail et de mettre en place ce que j’ai pu acquérir pendant ces deux années à IUT de Créteil-Vitry.

J’ai également pu à quelques reprises faire un lien direct entre mon projet et la formation que j’ai réalisé lors de cas pratiques, d’interventions ou de mon projet essentiellement sur Linux (debian).

Je suis également satisfait d’avoir réussi mon projet de migration vers le nouveau serveur web en autonomie. J’ai la sensation d’avoir contribué à mon échelle au futur du service. Le fait d’avoir réalisé ce projet est une bonne expérience que j’aimerais rééditer.

## TP Audit de sécurité :

*Nous vous proposons un sujet sur le thème de la sécurité : Pour cela vous répondrez à ces différentes questions lors de votre TP :*

*A6) Comment le pirate découvre l’existence du poste de travail dans l’entreprise ?*

***Indice :*** *Il faut utiliser un scanneur réseau et analysé le trafic réseau de l’entreprise.*

*A7) Comment le pirate découvre le nom et le mot de passe de l’utilisateur qui est connecté sur le poste ?*

***Indice :*** *Il regarde le fichier « auth.log » pour voir les connexions effectuées. Le pirate effectue une attaque par force-brute.*

*A8) Comment le pirate exfiltre les fichiers ?*

***Indice :*** *On vérifie l’historique des commandes pour savoir quel moyen utiliser pour exfiltrer les fichiers. On peut aussi utiliser les trafics et les flux du réseau.*

*A9) Quel autre moyen est utilisé par le pirate pour exfiltrer des fichiers ?*

***Indice :*** *Regarder le trafic réseau et les fichiers effacer.*

*A10) Comment le pirate a encore l’accès sur le PC poste lorsque la faille est résolue ?*

***Indice :*** *Voir les flux et le trafic du réseau dans des heures précises.*

*Lister les tâches planifiées.*

## Sources*:*

<https://www.makeuseof.com/tcpdump-examples/#:~:text=%20The%20tcpdump%20Output%20Format%20%201%20Timestamp,9%20Window%20size%2010%20Packet%20length%20More%20>

<https://www.youtube.com/watch?v=R-IE2j04Chc>

<https://www.youtube.com/watch?v=wJ6E1ndOooI>

<https://www.quennec.fr/trucs-astuces/syst%C3%A8mes/gnulinux/commandes/fichiers-dossiers/transfert-de-fichiers-scp>

<https://secnumacademie.gouv.fr/auth/login/fr>

<https://tech.korben.info/t/logiciel-hydra-avis/5414>

<https://www.youtube.com/watch?v=-4-xm7tk1pU&ab_channel=Archidote>

<https://fr.wikipedia.org/wiki/Nmap>

<https://www.youtube.com/watch?v=KizktyVDnEA&ab_channel=WakedXY>

<https://www.youtube.com/watch?v=uNgJJ-QeZpk&ab_channel=inceptor>

<https://www.journaldugeek.com/2008/12/30/les-pires-500-mots-de-passe-depuis-toujours/>