Rapport

Introduction

Nous sommes Christopher Hardeman et Léo Rouger, tous deux étudiants en Mastère 1 Cybersécurité à Bordeaux Ynov Campus.

Dans le cadre de notre YDay Labo SSI, nous avons choisi de vous présenter notre parcours d’apprentissage et notre réalisation du Pro Lab Dante de Hack The Box.

Pour ce YDay, nous avons un projet Fil Rouge à réaliser tout au long de l’année et à présenter en fin d’année. Au vu de nos bagages cyber respectifs, nous avons donc cherché un projet nous permettant de monter en compétence sur les sujets ou nous avions des lacunes. Après plusieurs réflexions, nous en sommes arrivés

au choix de monter en compétence sur la sécurité offensive, domaine dans lequel nous n'avions que peu de compétences. Ce domaine nous attirait également et nous avions envie de nous faire plaisir.

Au cours de nos recherches, nous nous sommes aperçus que la plateforme Hack The Box proposait des labo d'entrainement un peu plus poussés à réaliser : les **Pro Labs.**

Parmi ceux-ci, un lab est plutot orienté pentest junior : **Dante**.

Nous sommes donc partis sur l'idée de relever le défi du Pro Lab Dante, ce qui nous pousserait non seulement à travailler tout au long de l'année mais qui allait également nous permettre de monter en compétences. Ce labo étant un labo assez généraliste, il nous permettrait de progresser sur un large spectre de compétences cyber.

Cet objectif allait également nous permettre d'appuyer les compétences acquises lors de nos cours à YNOV mais également dans nos entreprises respectives.

Qui sommes-nous ?

Afin de remettre un peu de contexte sur nos profils respectifs, voici un peu plus de détails :

- Christopher est en alternance chez Sopra Steria en tant qu'ingénieur cybersécurité, il s'occupe de la partie Protect Identity pour un grand groupe toulousain. Avant Ynov, ses connaissances en cybersécurité étaient maigres et il a fallu (presque) partir de zéro. Il a néanmoins un bagage en développement Web (JS, React).

- Léo est en alternance chez Cheops Technology en tant qu'ingénieur cyber généraliste. Avant Ynov, il a travaillé en tant qu'administrateur système et réseau pendant 5 ans dans une petite ESN du secteur géographique de Poitiers.

Christopher a des compétences en Développement Front Web et un bagage léger en cybersécurité avec la remise à niveau d'Ynov.

Léo a lui un bagage un peu plus complet avec quelques années d'administrateur système et réseau, une bonne connaissance en réseau et déjà une bonne progression sur la plateforme Root-Me.

Dante ? Kezako ?

Le Pro Lab Dante se présente comme un défi de niveau **Intermédiaire** selon Hack The Box. Il est présenté comme un labo accessible aux pentesters junior et mobilisant un bon socle de compétences en matière de pentest.

Les compétences principales annoncées par Hack The Box pour ce lab sont les suivantes :

- Enumeration
- Développement d'exploits
- Mouvement latéral
- Elevation de privilèges
- Attaque d'applications Web

Il comporte 14 machines (13 sont seulement dans le scope du labo) et 27 flags sont à récupérer au total. Parmi ces machines, nous retrouvons 7 machines Linux et 6 machines Windows.

Nous avons également lu des retours d'expérience de personnes ayant réalisé le lab pour avoir une idée un peu plus précise des tâches à effectuer dans le labo. Nous ajouterons qu'une des compétences majeures à avoir pour ce labo est le pivoting, pour savoir rebondir d'un environnement (réseau, machine) à un autre.

D'après les revues des différents utilisateurs, le niveau de Dante correspond bien à celui annoncé par Hack The Box. Le labo mobilise beaucoup de compétences de bases attendues pour un pentest, toutefois sans trop rentrer dans les détails de chacune des dites compétences.

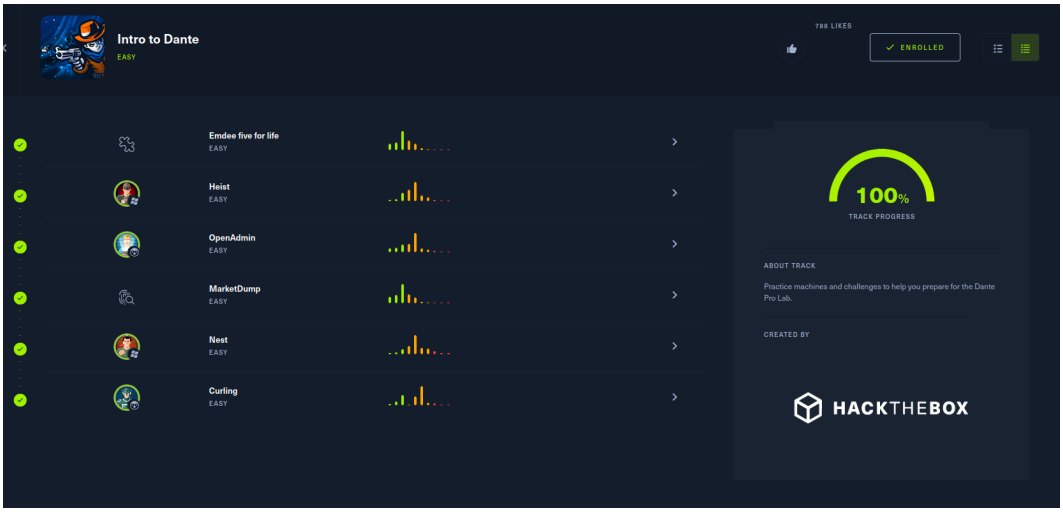
Parcours d'apprentissage

Track Dante — Le fil rouge de progression

Hack The Box fournit, pour s'entrainer, des "tracks".

Ce sont des parcours d'apprentissage qui permettent d'orienter et de travailler les connaissances nécessaires pour certains sujets.

En l'occurrence, pour notre cas il existe un track "Intro to Dante".



Les box proposées dans ce track nous permettent de nous concentrer sur les connaissances nécessaires pour pouvoir mener à bien notre mission et vaincre le boss final : Dante.

Les machines se présentent ainsi :

- **Emdee FIve for life - Ce n'est pas une box, plutôt un challenge à résoudre**
  - Compétences abordées : Attaques de webapp (Burp Suite), scripting (Python, BeautifulSoup), manipulation de hash MD5
- **Heist - Easy**
  - Compétences abordées : Enumeration (analyse de fichiers de config), Enumeration Windows (CrackMapExec, RID Bruteforce, Evil-WinRM...), Forensic mémoire (Dump de process, recherche d'informations dans ce dump)
- **OpenAdmin - Easy**
  - Compétences abordées : Exploitation d'une webapp vulnérable, Reverse Shell, Enumeration Linux, Mouvement latéral, Bruteforce d'identifiants,

Exploitation de sudo pour élévation de privilège

- **MarketDump - Idem que pour “Emdee Five for life”, il s’agit d’un challenge**
  - Compétences abordées : Analyse basique de capture réseau (Wireshark), décodage d’informations encodées en baseXX
- **Nest - Easy**
- **Curling - Easy**
  - Compétences abordées : Exploitation de CMS vulnérable (Joomla), énumération Web (Ffuf, dirbuster), Reverse Shell, Forensic sur fichiers (binwalk, foremost, xxd), Exploitation de cronjobs Linux

Concernant le timing de réalisation, malgré des disparités dans le rythme consacré à l’entrainement, le track a été réalisé par les deux membres de ce projet.

Nous avons réalisé la plupart des box de ce track sur les temps consacrés au YDay le mercredi.

La somme de nos bagages techniques nous a permis de résoudre ces box ensemble et ainsi de progresser individuellement sur les points suivants :

- Compétences techniques : Nous avons découvert de nouvelles manières d’exploiter, d’énumérer, mais également appris à utiliser plusieurs outils essentiels associés à ces techniques.
- Compétences méthodologiques : Les machines proposées sont prévues pour nous apprendre à créer notre propre méthodologie de pentest afin de gagner en efficacité et en pertinence.
- Compétences rédactionnelles : Nous nous sommes obligés à rédiger des write-up pour chacune de ces machines. Cela nous semblait essentiel car nous pensons que pour rédiger un write-up, il est nécessaire d’avoir bien compris les actions réalisées précédemment.

Cours HackTheBox Academy

En complément du track “Intro to Dante”, nous avons également suivi les cours proposés sur la plateforme Hack The Box Academy.

Christopher avait des lacunes en terme de réseau, n’ayant jamais pratiqué auparavant. Il avait également un contexte global en cybersécurité très peu défini. HackTheBox Academy a permis de résoudre pas mal de ces lacunes, via un suivi de ces cours tout au long de l’année.

Comme expliqué plus haut, Léo avait déjà un bon bagage en terme d’administration système et réseau, mais pas dans un contexte cyber. Ayant pour objectif de passer la certification Hack The Box CPTS l’année suivante, il s’est servi du path Pentester pour progresser également pour la réalisation de Dante.

Prérequis

Avant de commencer les cours, certaines bases sont nécessaires afin d'appréhender au mieux les différents concepts abordés. A notre sens, il est nécessaire d'avoir de bonnes bases dans les domaines suivants :

- Administration système (Windows/Linux)
- Administration réseau
- Fonctionnement des applications Web
- Connaitre au moins un langage de scripting (par exemple Python)
- Avoir une bonne "culture informatique" en général

Ces bases sont requises pour pouvoir effectuer les cours Hack The Box Academy de manière sereine.

Dans notre cas, comme expliqué précédemment Christopher avait un peu plus de lacunes sur les domaines du réseau et du système. Cela lui a donc demandé un peu plus de temps pour se remettre à niveau sur ces sujets.

Cours essentiels

Au vu des sujets abordés dans Dante, nous avons souhaité nous concentrer sur des cours pertinents dans ce contexte.

Voici les cours les plus importants, selon notre vision, pour réussir ce challenge :

- **Network Enumeration with Nmap** : Ce cours est assez exhaustif concernant l'outil de scan de port **nmap**. Il permet d'avoir une très bonne vue d'ensemble sur les possibilité offertes par cet outil puissant.

- **Attacking Web Applications with Ffuf** : Cours très complet sur l'utilisation de l'outil d'énumération web **ffuf**. Ce cours permet (en plus d'apprendre à utiliser ffuf de manière exhaustive) d'avoir de bonnes bases de méthodologie concernant le pentest d'applications Web.
- **Active Directory Enumeration & Attacks** : Dante étant un labo comportant beaucoup de machines Windows, il est important d'avoir une bonne vision des possibilités d'exploitation de ce type d'environnement. Le cours en question détaille le fonctionnement d'un Active Directory et les manières les plus communes d'exploitation Active Directory dans le cadre d'un pentest.
- **Pivoting, Tunneling and Port Forwarding** : Sûrement le cours le plus important pour la réalisation de Dante. Il permet de comprendre les différentes mécaniques permettant de passer d'un réseau à un autre via des serveurs de rebond par exemple ou bien d'accéder à des applications dont l'accès est restreint. Dante étant un labo avec plusieurs réseaux cloisonnés, il est essentiel de bien comprendre ces notions.
- **Shells & Payloads** : Permet de bien comprendre les différentes manipulations réalisables pour obtenir, générer, compromettre l'accès shell sur une machine dans le cadre d'un pentest.
- **File Transfers** : Ce cours permet d'avoir une bonne vision des différentes techniques permettant de télécharger des données vers une machine compromise ou bien de téléverser des fichiers vers celle-ci (par exemple des outils ou des fichiers nécessaires à l'exploitation).

Les machines HackTheBox

En complément du track Dante, des box Hack The Box hors track on également été réalisées par chacun d'entre nous :

Pour Christopher :

- CozyHosting
- Analytics
- Devvortex

- Perfection

Pour Léo :

- TwoMillion
- CozyHosting
- Sau
- Lame
- Devvortex
- Analytics
- Zipping
- Hospital
- Active
- Forrest

Ces machines, pour la plupart de niveau Easy voire Medium, nous ont permis de consolider notre base méthodologique. Cela a également été nécessaire pour bien s'imprégner de la "logique Hack The Box". En effet, chaque plateforme d'entrainement cyber a sa propre manière de résoudre les challenge, il nous semblait donc important de nous familiariser avec celle-ci.

Autres méthodes d'apprentissage

De manière annexe, nous avons utilisé d'autres plateformes pour compléter notre apprentissage, que ce soit via nos cours ou bien sur notre temps personnel.

Nous avons pu par exemple aborder des concepts d'attaque web avec les challenges **PortSwigger** dans le cadre de notre majeure **Vulnérabilités** à Ynov.

Nous avons également utilisé Root-Me pour aborder d'autres concepts non nécessairement liés à Dante. Cela avait pour but d'élargir notre panel de compétences générales mais également d'avoir une meilleure vision et culture du monde cyber en général.

Nous avons participé tous les deux au CTF de notre YDay Labo SSI.

Léo de son côté a également participé à plusieurs CTF présentiels parmi lesquels :

- CTF du département de la Gironde
- CTF European Cyber Cup 2 dans le cadre du FIC
- CTF Ynov x Seela

Ainsi qu'à des CTF online comme :

- HackDay CTF
- 1753 CTF
- Kalmar CTF
- Midnight Flag CTF

Bilan de l'apprentissage

Notre phase d'apprentissage et d'entrainement a duré du mois de novembre 2023 au mois de mars 2024.

Arrivé à cette date, nous devions commencer Dante afin d'avoir le temps suffisant de réaliser le labo, celui-ci étant relativement long à réaliser.

Au terme de cette période, nous avons fait le bilan sur notre progression.

Pour Léo :

- Bonne montée en compétence technique
- Méthodologie de pentest bien établie et intégrée
- Bonne vision de base de la sécurité offensive
- S’est senti plutôt à l’aise sur l’exercice

Pour Christopher :

- Une vision plus définie de la cybersécurité
- Une bonne connaissance de base
- Une montée en compétence technique (surtout en réseau)
- Méthodologie de pentest style ‘Hack The Box’
- Des difficultés sur la plupart des exercices

Ayant plus de lacunes sur les sujets de base, Christopher a mis plus de temps à rattraper son retard sur ces compétences. Nous avons donc pris la décision que Léo réaliserai le labo Dante sans Christopher.

En revanche, Christopher a continué son apprentissage avec les différentes méthodes citées précédemment, notamment sur les sujets suivants :

- Réalisation d’une box sans aucun soutien externe
- Quelques challenges Root-Me

Réalisation du Pro Lab Dante

Cette partie se concentrera uniquement sur le travail de Léo qui a réalisé le labo. Cette partie expliquera de façon globale le déroulé du labo. Il ne sera pas détaillé de manière exhaustive la méthodologie entière utilisée pour réaliser le labo qui serait trop chronophage.

Si besoin de consultation, un write-up a été rédigé.

Afin de ne pas rendre ce rapport trop long, il sera présenté 3 compétences jugées essentielles ayant permis la réussite du labo.

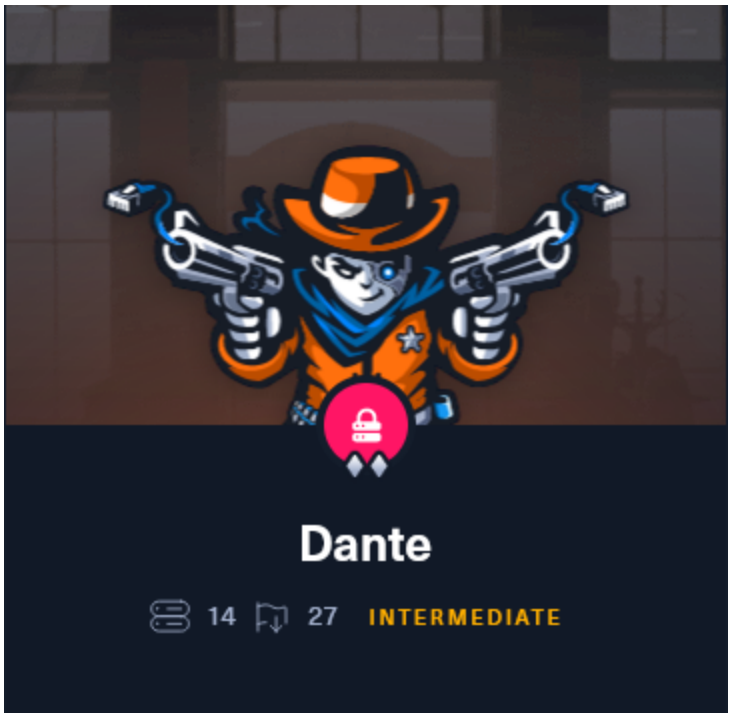
Scénario du labo

Voici le scénario du labo fourni par Hack The Box :

```
Dante LLC have enlisted your services to audit their network.
The company has not undergone a comprehensive penetration test :
They are concerned that any actual breach could lead to a loss c
```

Aucun doute, nous sommes explicitement placés dans la peau d'un pentester. Notre mission est d'auditer la sécurité de l'entreprise Dante LLC et de trouver le maximum de failles sur son système informatique.

Pour rappel, Dante comporte 14 machines (dont seulement 13 sont dans le périmètre réel d'attaque) et 27 flags sont à récupérer sur celles-ci.



Prise en main du labo

Un VPN nous est fourni par Hack The Box pour nous connecter au labo.

Notre point d'entrée se situe dans un réseau en **10.10.110.0/24.**

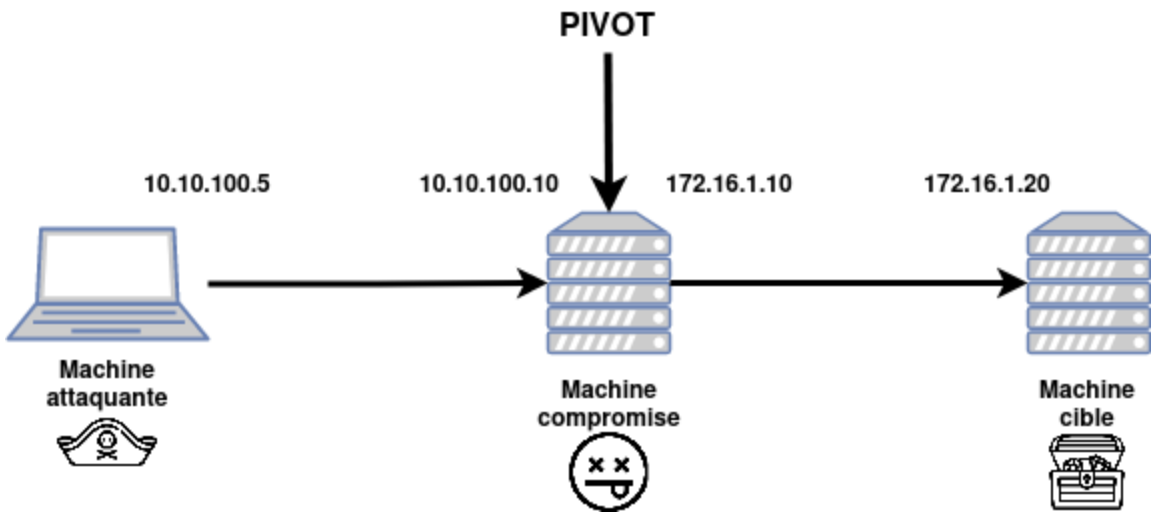
Dans ce réseau se trouvent deux machines. Parmi ces deux machines une est à exploiter, l'autre est le pare-feu du réseau, qui est hors périmètre (information donnée par Hack The Box).

La première machine à attaquer est une machine Linux, avec une exploitation web à réaliser puis une élévation de privilèges. Cette machine nous donne ensuite accès à un second réseau comportant une bonne partie des autres machines du labo.

Le nerf de la guerre : le pivoting

Comme expliqué, la machine point d'entrée nous donne accès à un second réseau. Afin de pouvoir attaquer les machines présentes dans ce réseau, il est nécessaire de savoir pivoter sur celui-ci à travers notre machine initiale.

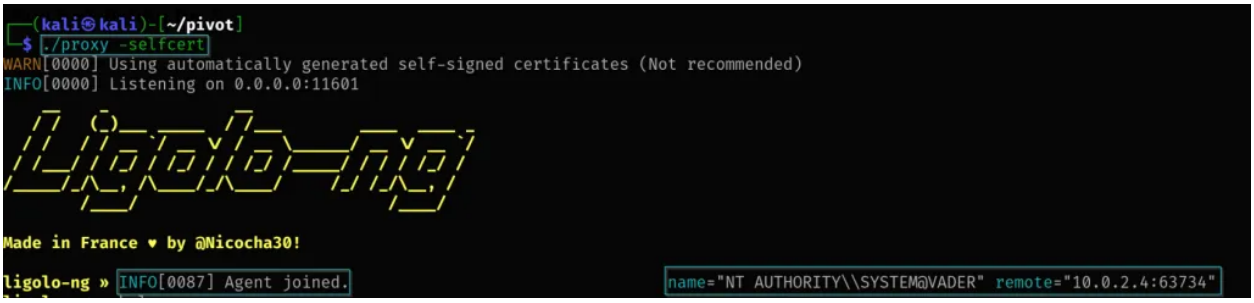
Pour rappel : Le pivoting (ou tunneling) consiste à utiliser une machine compromise afin d'accéder à des ressources non accessible depuis notre machine attaquante.



La méthode initiale utilisée dans le cadre du labo a été d'utiliser un proxy SOCKS4 avec l'outil **proxychains**. Cette méthode a permis de réaliser une seconde machine, cependant elle a vite été limitante dû aux performances et à la stabilité des connexions au travers de proxychains.

Une méthode alternative a donc été recherchée et trouvée : il a été décidé d'utiliser l'outil **ligolo-ng** du français Nicocha30.

Ligolo-ng est un outil de tunneling fonctionnant à la manière d'un VPN. Un serveur ligolo-ng est lancé sur notre machine attaquante au travers d'une carte réseau virtuelle dédiée en écoute sur un port particulier. On lance ensuite l'agent sur la machine compromise en lui indiquant de se connecter à notre machine attaquante.



Nous pouvons voir sur la capture ci-dessus que le proxy reçoit bien la connexion de l'agent en question.

Une fois cette connexion reçue, nous lançons le tunnel et ajoutons une route statique sur la carte ligolo de notre machine attaquante vers le réseau cible pour que tout le traffic à destination du réseau cible passe par notre tunnel ligolo.

Cette technique a été essentielle pour la réalisation du labo. En effet, la grande majorité des machines se situent dans le second réseau.

Par la suite, il a même été nécessaire d'effectuer jusqu'à 4 pivotings simultanés afin d'atteindre les dernières machines du labo, situées dans d'autres réseaux.

Ligolo-ng a également été utilisé pour réaliser du forward de ports locaux (par exemple dans le cas d'une machine avec un service réseau accessible uniquement en local).

Le pivoting est donc la compétence majeure à détenir pour la réalisation de Dante.

L'énumération

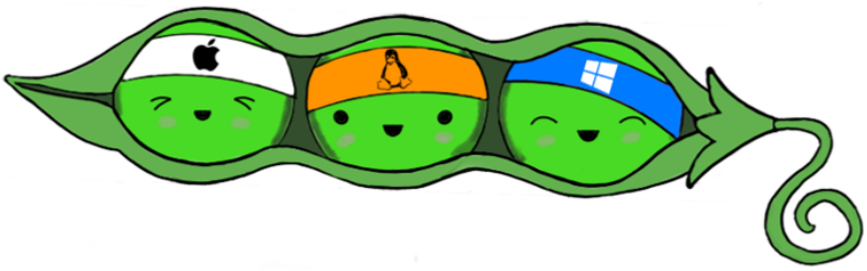
Au fil des machines compromises, nous avons besoin d'informations glanées sur les machines précédentes pour pouvoir avancer.

Il est également important d'avoir toutes les informations pour pouvoir réaliser, par exemple, une élévation de privilèges sur une machine.

Il est donc essentiel d'avoir une bonne méthodologie d'énumération pour pouvoir en tirer profit au maximum. Ces informations permettent essentiellement de pouvoir réaliser d'autres machines mais peuvent aussi nous faire gagner du temps dans le cadre de certaines machines (pas besoin de bruteforce un mot de passe si on l'a déjà récupéré avant dans un fichier .txt par exemple).

Pour ceci, il a été utilisé quelques outils permettant de gagner du temps, entre autres :

- LinEnum
- LinPEAS
- WinPEAS
- SharpHound
- BloodHound
- pspy



Ces outils ont été essentiels pour la réussite du lab et ont permis de découvrir de nouvelles manières d'exploiter des faiblesses de configuration par exemple.

Une partie de l'énumération était faite "à la main" également, les administrateurs HackTheBox ayant laissé des indices à divers endroits du labo (comme par exemple des fichiers Excel contenant des identifiants, des users sur les machines dont le mot de passe serait à réutiliser etc...)

Il est donc indispensable d'effectuer une énumération exhaustive dans le cadre de ce labo.

La prise de notes

Dante est impossible à réaliser sans une prise de notes efficace.

Celle-ci est indispensable sous plusieurs aspects :

- Il est impossible de se rappeler de tête des informations précédentes d'une session de travail à l'autre.
- Cela permet de remettre ses idées en place lorsque l'on est pris dans le feu de l'action. Cet aspect permet aussi souvent de repenser le pentest sous un nouvel angle, nous permettant d'éventuellement trouver d'autres solutions en cas de blocage
- Elle permet aussi de valider les connaissances acquises. Il n'est pas possible de décrire ce que l'on fait via des notes sans l'avoir réellement compris. Cet aspect permet de s'assurer d'un apprentissage continu tout au long de la réalisation du labo

Dans cet optique, un write-up a été rédigé sous la forme d'un document qui pourra être relu dans 6 mois, 1 an...et être toujours compréhensible.

De plus, cet exercice a permis d'emmagasiner beaucoup de connaissances techniques qui pourront re-servir par la suite. Il serait intéressant de réaliser des fiches méthodologie pentest basées sur l'expérience de Dante.

Éléments bloquants

Quelques difficultés ont tout de même été rencontrées au cours de la réalisation du labo. En effet, il est impossible de tout connaitre dans le cadre d'un pentest.

Voici une liste non exhaustive d'éléments qui ont pu être bloquants par moment :

- Le manque de connaissances web. Léo étant issu d'un passé orienté système/infra, le web n'était pas quelque chose de maitrisé. Cela a pu causer quelques ralentissement dans l'accomplissement de certaines tâches.
- Le manque de pratique sur les outils. Certains outils ont été testés pour la première fois dans le cadre de ce labo. Le manque de pratique obligeait à

revenir sans arrêt vers la documentation pour avoir les bonnes options par exemple.

- Le manque de pratique en scripting. Certaines tâches répétitives dans le labo auraient pu être automatisées avec des scripts. Par manque de pratique en scripting, ces tâches étaient réalisées à la main. Si un nouveau labo devait être effectué, ce serait l'axe principal d'amélioration.

Concernant les blocages que j'ai pu avoir, j'ai pu m'assister de différents supports pour m'aider à avancer :

- Le Discord Hack The Box avec le channel dédie à Dante m'ont aidé à me débloquer sur certains points. J'ai également pu aider d'autres participants.
- Les différents forums techniques ont pu m'aider sur certaines exploitations ou utilisations d'outils.
- Mon collègue Bryan Ferreras-Roca réalisait Dante en même temps que moi, nous avons donc pu échanger à de multiples reprises sur le labo et ainsi se faire avancer mutuellement.

Retour d'expérience

Initialement, Dante était un défi personnel pour se prouver que l'on était capable de réaliser notre premier Pro Lab après une année seulement à Ynov.

Bien que pour Léo, la tâche soit finalement accomplie, Christopher, au fil de cette année, a dévié de sa trajectoire pour se rendre compte que ce qui l'animait en cybersécurité, ce n'était pas la partie technique.

En effet, l'alternance de Christopher étant orienté plutôt blue team, il a commencé à développer une certaine affection, non pas pour le travail qu'il a effectué cette année car il y a eu pas mal de soucis, mais pour la gestion de projet et d'équipe notamment avec le onboarding d'un collègue arrivé plus tard. Cette expérience professionnelle, bien que mauvaise sur plusieurs aspects, lui a néanmoins permis de se rendre compte de ce qu'il voulait réellement faire. De la gestion de projet

cyber, lui permettant ainsi pour l'année prochaine, de pouvoir se réorienter sur de la **GRC pour commencer**.

Concernant Léo, il se sert de cette expérience comme d'un socle technique lui validant une base convenable en sécurité offensive. Ayant pour objectif le passage de la certification Hack The Box CPTS lors de l'année de Mastère 2, cela s'inscrit dans cette lignée.

L'objectif de l'année prochaine sera de réaliser toujours plus de box et de challenge sur les plateformes en ligne et en CTF jusqu'à avoir le niveau attendu.

D'un point de vue personnel, cela lui a permis de travailler la persévérance ainsi que le fait de se fixer un cadre de travail convenable afin de mener à bien la mission.

Dante est un bon lab tenant ses promesses, offrant un lab pour les juniors en cybersécurité. Même si nous n'avons pas pu compléter tous les deux le labo, cette expérience nous a permis d'approfondir notre projet professionnel et de le rendre plus précis.


HACKTHEBOX
HTBCERT-9951AAF1F1
PRO LABS
DANTE
CERTIFICATE OF COMPLETION
Léo Rouger
Is hereby granted this certificate on completion of the Hack The Box Pro Labs: Dante
Haralampos Pylarinos, CEO
Shaun Whorton
Shaun Whorton, Lab Master
Date 27 Apr 2024
CPE credits 40
Length 40 hours
Location Online
Subject areas covered
Enumeration, Exploit development, Lateral movement, Local privilege escalation, Situational awareness, Web application attacks
HACK THE BOX
CERTIFIED PRO LABS
SINCE 2017
SEAL OF APPROVAL