RetEx
OSCP 2024

Naullet Arthur @Fey

Sommaire

1. Introduction
2. Exercices
3. Lab
4. Exam
5. Avis
6. Conclusion

Introduction

Kezaco l'OSCP (Out standing Specialist Cat Professional)

Kezaco l'OSCP

La certification OSCP (OffSec Certified Professional) correspond à la réussite de l'examen associé au cours PEN-200 de chez OffSec*.

Le cours s'intitule « Penetration Testing with Kali Linux » et passe en revue toutes les bases du Pentest Réseau, Web, Linux, Windows, AD.**

L'Examen est réputé pour être assez complexe ce qui fait de la certification une des plus reconnues dans le milieu pour valider les acquis d'un *testeur de stylo* aka *pentester* aka *auditeur technique en cybersécurité*🥐🥖.

** OffSec ou Offensive Security est l'entreprise qui a créé Metasploit, exploitDB, Kali, etc.*

*** On peut tout de même faire l'exam sur l'OS de son choix. Ex: Personnellement, j'ai tout fait sur mon mac sans Kali.*

Kezaco l'OSCP

Accès aux cours + 3 mois de lab + 1 voucher d'exam

Selon moi, si on a le temps #PasDeVie et qu'on a déjà un peu d'experience type HTB, cela est suffisant. Avec obligation de vie de famille ou autre, la formule avec 6 mois de lab/exos est peut-être plus adapatée.

Les exercices et labs sont largement faisable mais peuvent être ~~très~~ chronofage.

Kezaco l'OSCP – L'exam

L'examen dure 24h (surveillé) puis sont accordées 24h supplémentaires pour l'écriture et l'envoi du rapport.

6 machines au total: 100 points:

- AD, 3 machines = 40 pts (Domaine Admin necessaire pour les pts)
- 3 machines StandAlone(Linux et/ou windows): = 60 pts
  - 10 pts shell with user privileges
  - 10 pts shell with root privileges

Points Bonus 10 pts:

- 80% d'exercice réussi dans chaque topic du PEN-200
- Minimum 30 proof (root privileges) flag envoyés sur les LAB. Correspond à environ 60% des lab flags

Prerequis pour avoir l'examen:

- 70 pts minimum
- soumission d'un rapport détaillé des étapes de compromission #ScreenshotsDansTousLesSens

Partie 1

Les Cours & Exercices

Les Cours & Exercices

Pen-200 Topic:

- ***Penetration Testing with Kali Linux: General Course Information***
- ***Introduction To Cybersecurity***
- ***Effective Learning Strategies***
- ***Report Writing for Penetration Testers***
- **Information Gathering**
- **Vulnerability Scanning**
- **Introduction to Web Application Attacks**
- **Common Web Application Attacks**
- **SQL Injection Attacks**
- **Client-side Attacks**
- **Locating Public Exploits**
- **Fixing Exploits**
- **Antivirus Evasion**
- **Password Attacks**
- **Windows Privilege Escalation**
- **Linux Privilege Escalation**
- **Port Redirection and SSH Tunneling**
- **Tunneling Through Deep Packet Inspection**
- **The Metasploit Framework**
- **Active Directory Introduction and Enumeration**
- **Attacking Active Directory Authentication**
- **Lateral Movement in Active Directory**
- **Assembling the Pieces**

Format: Vidéo + Texte sur Web Panel

Rappel: 80% d'exercice réussis dans chaque topic pour les 10 pts bonus

Les Cours & Exercices

Durée: environ 1 mois de travail à raison d'une séance d'1h (presque) tous les soirs.

Les exercices permettent de se familiariser avec les environnement d'OffSec.

Les thèmes qu'ils abordent couvrent les techniques necessaires à la réussite des labs.

Points clés:

- **Reparcourir toutes les techniques d'attaques de bases pour completer ses connaissances.**
- **Découvrir certaines nouvelles technique. Ex: technique de phishing avec les .Library-ms + .lnk**
- **Découvrir des nouveaux outils ou améliorer la maitrise de ceux déja connus.**
- **Se forcer à réaliser des montages un peu complexe. Ex: tunnelling avec 2+ rebonds + bypass de protection.**

Les exercices ne sont pas compliqués mais sont complets, variés, pas tricky sauf quelques execptions.

Partie 2

Les Labs

Les Labs

6 labs au total:

- **2 labs taille moyenne (10 – 15 machines)**
- **1 gros lab (3 réseaux, 20 machines)**
- **3 labs type OSCP (6 machine: 3 dans un AD et 3 standalone)**

Les Labs

Les points clés:

- Pleins d'envirronement AD rigolos à attaquer.
- Oblige le "try hard" pour réussir à flag.
- Découverte d'exploit sur pas mal de technos fun. *Ex: RCE sur serveur de remote mouse*
- Prépare bien à se mettre dans le moule d'OffSec pour l'exam.

Grosso modo, ça vaut carrément le coup !

Les conseils:

- Faire une grosse partie des exos avant.
- Utiliser un minimum le forum, try hard un maximum sur les exos.
- Se garder au moins 2 labs OSCP like pour faire des exams blancs.
- S'entrainer à bien faire les screens comme demander à l'exam. Il y'a beaucoup de retex relatant de mauvaises surprises.
- Faire un petit tableaux avec les différents flags obtenus pour mieux visualiser son avancée.

Partie 3

L’exam, le fameux

La préparation

Des fruits, du café, de quoi grignoter.

Une bonne nuit de sommeil la veille.

Un ou des petits jours de congé pour bien se détendre les jours qui précèdent.

Refaire une passe sur les lab OSCP like.

Relire ses penses bêtes et notes (Ex: chemin d'attaque type sur l'AD, tester les Brute Force débiles, etc.)

Faire ou Refaire une ou deux machines HackTheBox la veille histoire de s'échauffer.

Et c'est parti, début de l'exam à 7h…

Le jour J – Partie 1 – All is fine

6h45: Verification de l'ID, check webcam + partage des écrans.

Let's go !

7h00: Je commence l'AD rapidement

Je bloque… Ce n'est pas grave je passe aux Stand Alone pour sécuriser des points. *Un peu déçu quand même l'AD passait bien aux exams blancs.*

8h18: Shell user sur machine StandAlone1

8h48: Shell root sur machine StandAlone1

La StandAlone2 m'inspire pas, ce n'est pas grave je passe à la 3.

10h05: Shell user sur machine StandAlone3

10h37: Shell root sur machine StandAlone3

Super, ça fait 3h que ça ne fait que 3-4h que ça a commencé et j'ai 40 points.

Le jour J – Partie 2 – Le désespoir

11h00: début du passage à vide

..

.. Rien

.. Rien

12h00: toujours rien, aucuns points d'entrée sur l'AD.

.. Rien

.. Rien

16h00: une piste sur StandAlone2 mais impossible de l'exploiter.

..

.. Rien

.. Rien

.. Début du désespoir.

Ce qui me sauve du craquage c'est de faire BEAUCOUP de pauses, ouvrir la fenêtre , prendre l'air, s'allonger 5 min, refaire un bon café, etc.

Le jour J – Partie 3 - Remotivé

21h11: Bingo, une piste sur l'AD, un point d'entrée.

21h37: user sur machine1.

21h50: privesc, admin sur machine1.

On reprend espoir, j'essaye de rester concentrer au vu de la fatigue et du temps restant.

23h54: lateralization, shell user machine2.

00h20: privesc, shell admin machine2.

00h26: shell user DC.

On voit le bout du tunnel.

I am finally IN !

Le jour J – Partie 3 - Remotivé

Je galère un peu, une technique de LPE jamais expérimentée mais plutôt bien documentée donc ça roule finalement plutôt bien.

1h57: Domain admin.

```
C:\Users\Administrator\Desktop>whoami
[redacted]\administrator

C:\Users\Administrator\Desktop>
dc01
```

2h00: Profiter des dernières heures de l'exam pour reprendre les quelques Screenshots manquantes et rererere-vérifier qu'on n'a pas oublié des Screenshots, surtout celles des flags + checker qu'on a bien upload les flags sur le portail de l'exam.

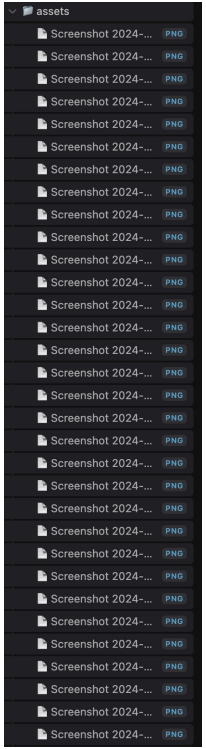
~4h00: un dodo bien mérité.

Le jour J+1 – Partie 4 - Rapport

C’est fatiguant de devoir faire un rapport quand on a très très peu dormi la veille même en aillant 24h.

Un petit tour au travail pour raconter ses aventures et manger avec les collègues !

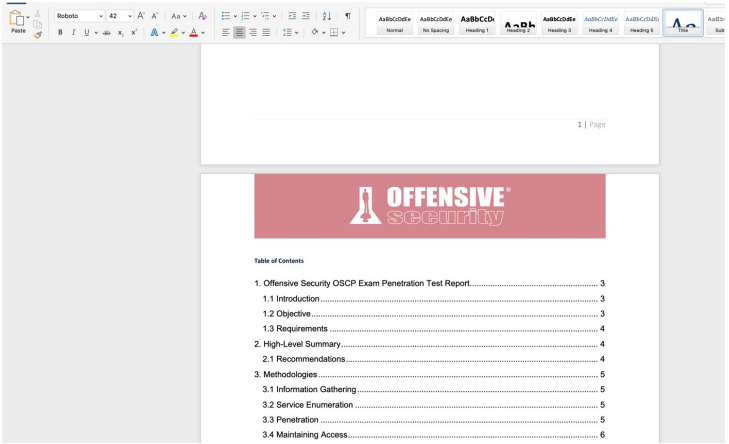
J’avance doucement dans la journée…



Quelques screenshots à integrer.

Le jour J+1 – Partie 4 - Rapport

20h00: je m'y remets sérieusement, je galère avec le template d'OffSec sur word #Beurk



1 | Page

OFFENSIVE security

Table of Contents

J'ai souffert

1h57: envoi du rapport.

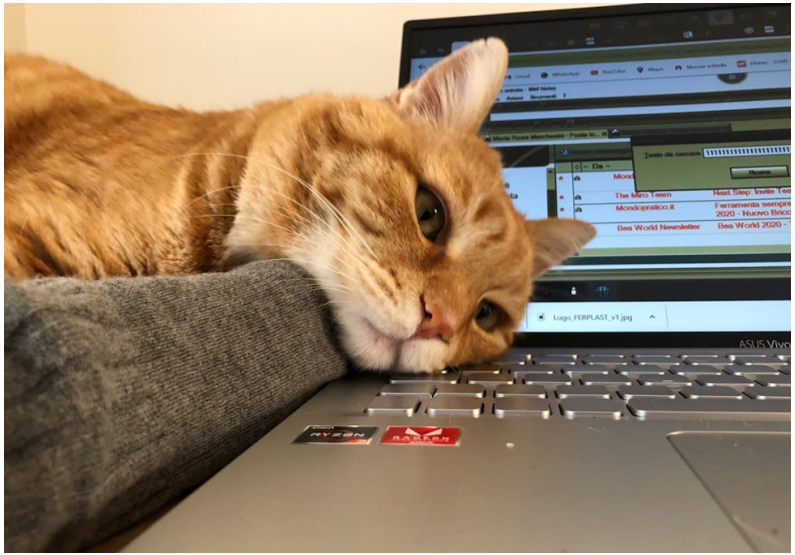
2h00: un autre dodo bien mérité.

L’attente

C’est long, très long…

OffSec indique une durée maximum de 10 jours ouvrés pour le résultat de l’exam.

J’essaye de pas y penser mais c’est compliqué.



Le résultat

Le week-end après l'exam (~6 jours après)

Dear Arthur,

We are happy to inform you that you have successfully completed the Penetration Testing with Kali Linux certification exam and have obtained your Offsec Certified Professional (OSCP) certification.

Your certification will be issued under the following name:

Arthur N[redacted]

Conclusion

Mon avis

Conclusion

Est-ce que L'OSCP est la meilleure certification de pentester qui ferra de moi un hacker hors pair en situation réelle ?

Conclusion

Est-ce que L'OSCP est une bonne certification pour:

- **Valider ses acquis et les compétences de bases du pentest Linux, AD/Windows.**
- **Découvrir quelques nouvelles techniques.**
- **Faire BEAUCOUP de mise en pratique avec des scénarios sympas.**
- **Travailler sur des labs plutôt complets & variés.**
- **Avoir un petit coup d'adrénaline pendant 24h.**

La suite…

Pour continuer chez Offsec:

- **Suite logique de l'OSCP**
- **Evasion avancé d'AV, latéralisation complexe dans un AD, etc.**
- **48h + 24h d'exam**

- **ça a l'air fun**
- **Orienté Wireless**

- **Full web et moi j'aime le web**
- **En 2 mots: from XSS to RCE**

La suite…

Chez HTB:

- **OSCP en mieux d'après les retours, en plus moderne, en plus complet.**
- **Moins chers, ~400$.**
- **~300 personnes seulement l'ont obtenu.**
- **EXAM SUR 10 JOURS. #LaFlemme**

Merci