

OSCP受験記

@salty_byte 2023/3/3

話すこと

- OSCPとは
- 受験前の知識
- PEN-200実施
- 試験
- 感想とか
- まとめ

OSCPとは

OSCPとは

- OffSec Certified Professionalの略
- OffSec (Offensive Security) が実施している、侵入テストの認定資格
- PEN-200コースで受けることができる
- 最終試験を合格すればOSCPとして認定される

<https://www.offsec.com/courses/pen-200/>

コース

	100 Level	200 Level	300 Level
Penetration Testing	PEN - 100	PEN - 200	PEN - 300
	PEN - 103	PEN - 210	
Web Application	WEB - 100	WEB - 200	WEB - 300
Exploit Development	EXP - 100		EXP - 301
			EXP - 312
Security Operations	SOC - 100	SOC - 200	
OffSec Academy		OSA - PEN - 200	
Cloud Security	CLD - 100		
Secure Software Development	SSD - 100		

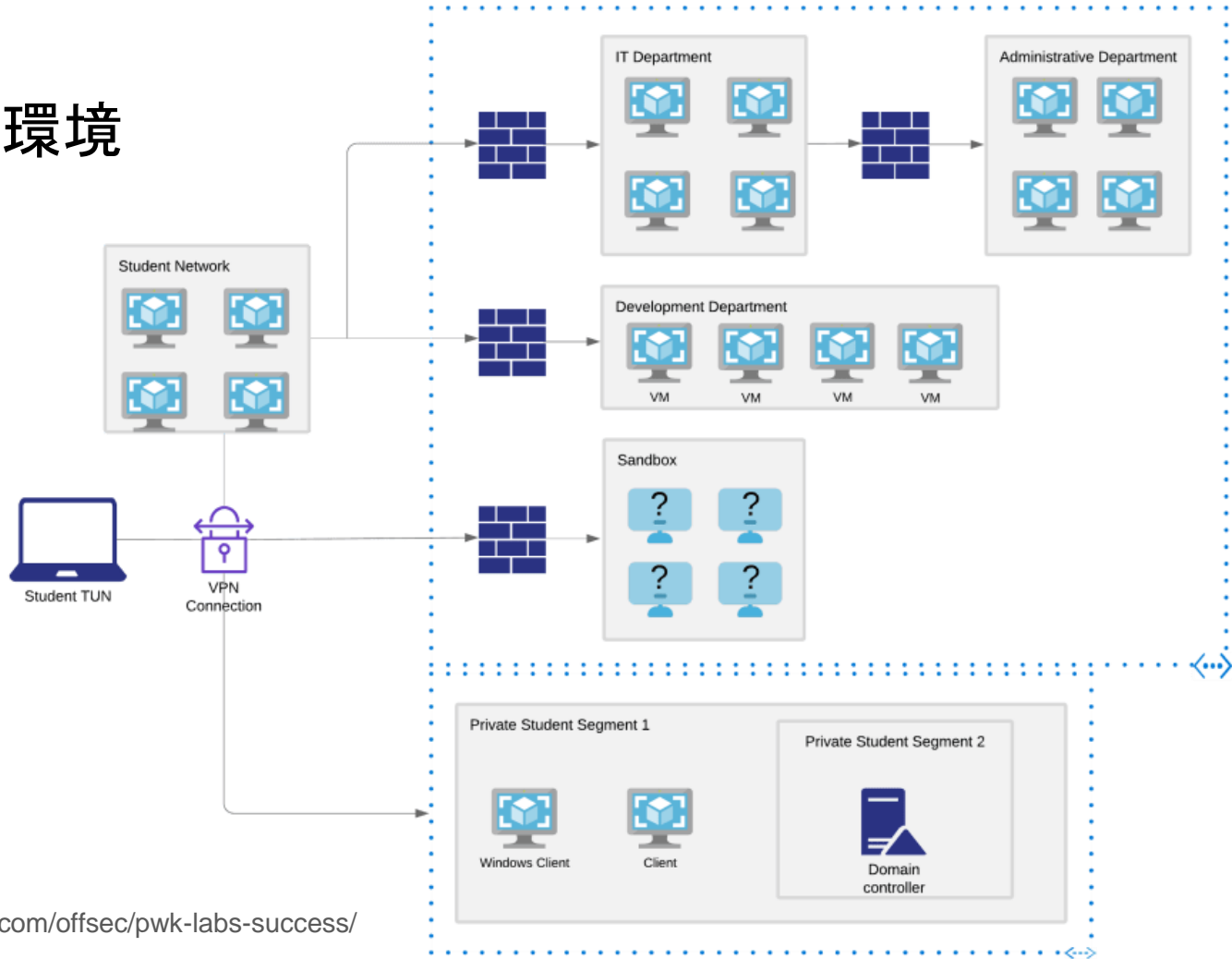
プラン（2023/03/03時点）

- Course & Cert Exam Bundle : \$1599
 - 1コース：ラボ環境3ヶ月
 - 試験1回まで
- Learn One : \$2499
 - 1コース：ラボ環境1年
 - 試験2回まで
 - Proving Groundsも使い放題
- Learn Unlimited : \$5499
 - 全部のコースが受けられる
 - 試験に回数制限なし
 - Proving Groundsも使い放題

ラボ環境

- 大きく分けて2種類ある
 - 教材/演習
 - テキストに従って学習する
 - テキストは英語だが、ブラウザの翻訳機能を使えば問題ないはず
 - 章ごとに手を動かして実施する演習がある
 - 申請すればPDFで教材をダウンロードできる
 - 練習用マシン
 - ひたすらネットワーク上のマシンを攻略していく

ラボVPN環境



コース申請に必要なもの

- パスポート
 - 持っていない人は発行に2～3週間とかかかるので注意
 - コース申し込みをすると、IDを送るように指示される
 - OpenPGPを使ってメールで送付する
 - PGPを使わなくても多分大丈夫

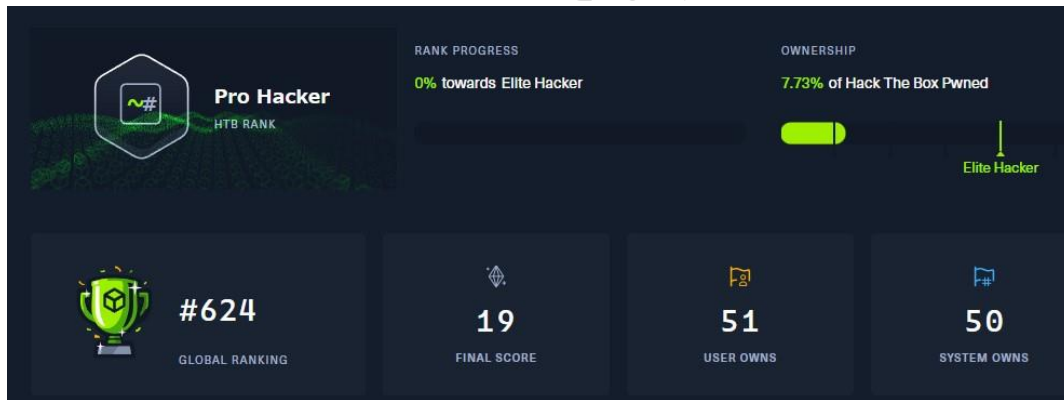
受験前の知識

受験前の知識（事前知識/経験）

- Web脆弱性診断経験3年半
 - Webアプリの脆弱性はある程度わかる
- その他セキュリティ
 - ペンテスト実務経験なし
 - HackTheBox 1年（独学）
 - CTF (2-3年前に少しやってたが、一緒にやる人がいないので今はやっていない)
- 開発言語
 - 読める/書ける：Java、TypeScript
 - 読める/ちょっと書ける：Python、PHP、Ruby
 - ちょっと読める/ほぼ書けない：C、C++

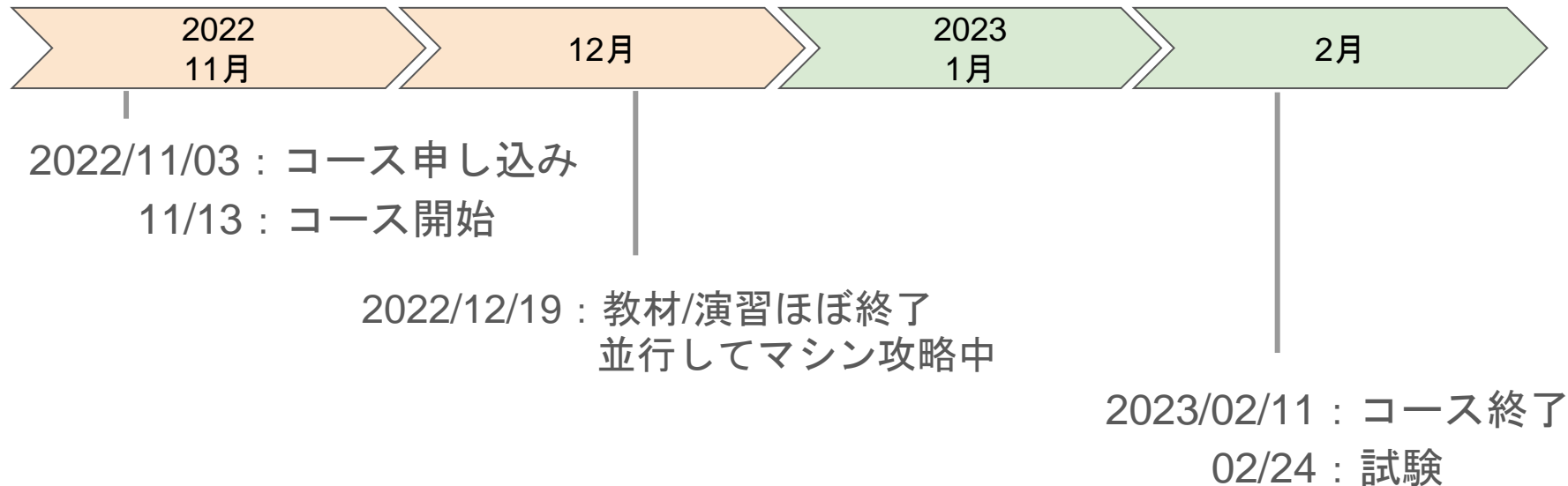
受験前の知識 (HackTheBox)

- 取り組み
 - 2021年2月から開始
 - 2022年2月まで毎週1台のマシン攻略
- ランク
 - Pro Hacker
 - EASY/MEDIUMマシンができるぐらい



PEN-200実施

PEN-200実施

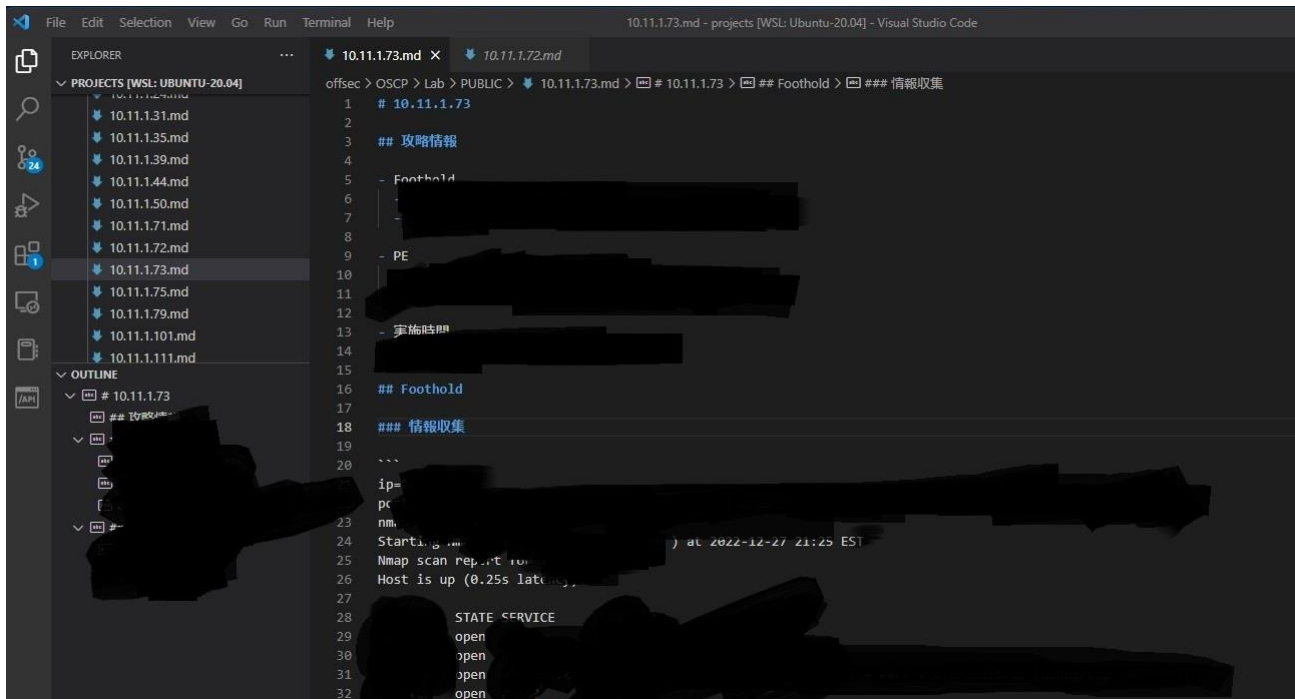


マシン攻略

- 平日は2~4時間ぐらい
- 休日は10時間ぐらい
- 年末年始もひたすらマシン攻略していた
 - 12/31の夜はUltimate Chicken Horseで遊んだ

PEN-200実施（進め方）

- 日記みたいな形で実施時間や何をやったか等をテキスト形式でまとめた
- マシン攻略の際は、該当のマシンの攻略情報を自分なりにまとめた



```
offsec > OSCP > Lab > PUBLIC > 10.11.1.73.md > 10.11.1.73 > ## Foothold > ### 情報収集
1  # 10.11.1.73
2
3  ## 攻略情報
4
5  - Foothold
6
7  [REDACTED]
8
9  - PE
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 - 実施時間
14 [REDACTED]
15
16 ## Foothold
17
18 ### 情報収集
19
20 ...
21 ip= [REDACTED]
22 pc [REDACTED]
23 nm [REDACTED]
24 Starting [REDACTED] at 2022-12-27 21:25 EST
25 Nmap scan report for [REDACTED]
26 Host is up (0.25s latency)
27
28 STATE SERVICE
29 open
30 open
31 open
32 open
```


PEN-200実施（可視化）

- コミットタイミングがproof.txtを提出した日なので、緑じゃない日も取り組んでいる



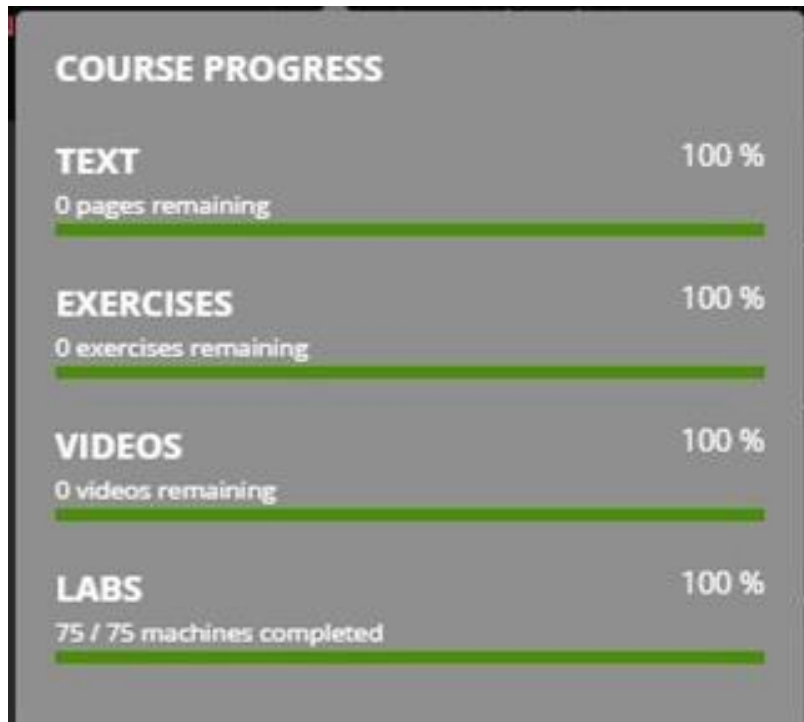
PEN-200実施時間

- 教材/演習
 - 130時間程
- 練習用マシン
 - 300時間程

これが多いか少ないか普通なのかどうかは不明

PEN-200実施

- 最終日に進捗が100%になった



試験

試験内容

- 100点満点中70点で合格
- 40点 : Active Directory Set完答
- 60点 : 独立マシン3台
 - ユーザアクセス (local.txt) : 10点
 - 権限昇格 (proof.txt) : 10点
- ボーナス10点 :
 - 教材/演習 80%完了
 - ラボマシン 30台 以上攻略

<https://help.offensive-security.com/hc/en-us/articles/4412170923924>

再受験時の注意点

- 再度受験したい場合は一定期間待たないといけない
 - 例) OffSec Course & Cert Exam Bundleの場合
 - 初回：前回の試験日から 6 週間以降
 - 2回目：前回の試験日から 8 週間以降
 - 3回目：前回の試験日から 12 週間以降
- 詳しくは以下のリンクから確認すること
 - <https://help.offensive-security.com/hc/en-us/articles/4406830092564-What-is-the-Exam-Retake-Policy-Staged>

試験スケジュール（JST）

- 試験開始：2023/02/24(金) 9:00
- 試験終了：2023/02/25(土) 8:45
- レポート提出期限：試験終了から24時間以内

試験前日

- 8割部屋の掃除
- 残りはADの復習

試験タイムライン（マシン攻略）

2023/02/24

- 08:45 試験用画面で待機
- 09:05 トラブルシューティング
- 09:15 試験前検査
- 09:35 試験開始
- ~10:00 AD1台目調査中断
- 11:00 独立1台目 local.txt提出
- 14:00 独立2台目 local.txt提出
- 15:10 独立2台目 proof.txt提出
- 15:30 独立1台目 proof.txt提出
- 17:20 独立3台目 local.txt提出
- 17:30 独立3台目 proof.txt提出
- ~20:15 レポート用の証跡集め
- 20:15 AD1台目続き開始

2023/02/25

- 02:00 終了宣言
- 04:00過ぎ 就寝

試験タイムライン（レポート作成）

2023/02/25

- 09:30 起床
- 09:30 レポート作成開始

2023/02/26

- 01:00 レポート完成
- 01:25 レポート提出

レポート作成

- 33ページぐらいになった
- ADがまるまる入っていないのでこんなもんだと思う

試験結果

- レポート提出から2日後にメールで合格通知が来た
- ギリギリ合格：70点
 - 独立マシン1：local.txt + proof.txt（20点）
 - 独立マシン2：local.txt + proof.txt（20点）
 - 独立マシン3：local.txt + proof.txt（20点）
 - ラボ：ボーナス点（10点）

感想

新しく学べたこと

- AD環境の攻略方法
- Windowsマシンの攻略方法
- いろんなツールの使い方
 - Mimikatz、CrackMapExecとか
- （すごく初歩だと思うが）アンチウイルス回避手法
- Shell
 - ワンライナーのコマンド実施とか

一番大変だったこと

- 3ヶ月で75台ラボマシン攻略
 - 正確には2ヶ月で70台
 - 最初の1ヶ月は教材/演習をゆっくりやってた（謎の余裕がこの時期にはあった）
 - ラボの利用可能最終日に全て完了した
 - 理解度を深めるため、攻略済マシンで他の手法確認に時間を使った方が良かったかも

残念だったこと

- 試験でADができなかった
 - 正確には、ADの踏み台の取っ掛けりがわからなかった
 - 横展開部分は結構勉強したつもりだが、活かせなかったのは残念

やっておくべきこと

- ラボ環境の自分用攻略メモを作る
 - コピペで使えるコマンドメモを作っておくと、試験中に調べる必要がなくなりロスが減る
 - チェックリストを作って、確認漏れが内容にするのもあり
 - 基本的に情報収集（列挙）をしている時間の方が長い可能性もある
 - 手順を確立しておくと Good

やっておくべきこと

- レポート作成の練習
 - ほとんどやらずにいたので試験の時に後悔
 - 手順だけでなく、脆弱性の説明や対策も書く必要がある
 - サンプルレポートはあるのでラボのマシンで時間を図って書いてみるのはあり
 - いろんな人が書き方の動画を上げている

気を付けること

- Learn Oneで申し込むことを推奨
 - 3カ月のラボ環境だと期間的に結構辛い（精神的/身体的）
 - 仕事が忙しいと着手時間が減る
（12月～3月は診断の依頼が増えて忙しいのになぜかこの時期に受けた）
 - 75台のマシン攻略が人によってはギリギリ
 - プライベート時間をほぼOSCPの勉強に使うことになる
 - 1回試験に落ちてももう一回チャンスがある
 - Proving Groundsで他のマシンにも挑戦できる

=> 値段は上がるがそれ以上の価値はある（と思う）

気を付けること

- ラボの教材/演習はさっさと終わらせる
 - 座学の部分は手を動かさないと覚えられない（個人差あり）
 - ツールがいろいろ出てくるが、紹介されているのは機能の一部でしかない
 - 教材に時間を使うよりマシンに時間を使った方が有意義だと思う
 - わからなくなったら戻るぐらいが丁度いい

気を付けること

- 試験前にカメラを用意する
 - 試験時に部屋の周りやデスク周りを映すことになる
 - ノートPC等に付属するカメラだと映すのが大変と思われる

気を付けること

- 試験前日はしっかり寝る
 - 試験時間が24時間近くあるので寝ておかないと体力が持たない（かも）

気を付けること

- 試験を終了する場合は寝てからにすること
 - レポートの期限は試験が終了してから24時間までのため
 - 中断は試験画面で中断申請すれば可能（らしい）

気を付けること

- レポートの証跡

- Local.txt及びProof.txtのスクリーンショットを取る際は、IPアドレスも載せる
- 脆弱性のあるソフトウェアを見つけたら、そのバージョン情報がわかる画面をスクリーンショットする
- 使用したコマンドとその結果をログとして残せるようにしておく
 - 例) `script -a -f ~/oscp.log`

勉強に使った本

ミミミミミツミ（著者：Allsafe）

<https://allsafe.booth.pm/items/1861943>

- Mimikatzの使い方を学べて、内容も面白いので買って良かった
- 残念ながら試験では使う機会は無かった

参考になった記事

mimichanのブログ

<https://mimichan1533.hatenablog.com/entry/2022/10/23/114309>

- カメラ情報とか参考書籍とか助かりました

よく使ったツール

- Nmap
- Hydra
- MSFvenom
- Reverse Shell Generator (<https://www.revshells.com/>)
- NetCat (nc)
- SearchSploit
- Mimikatz
- CrackMapExec
- Impacket
- xfreerdp
- John the Ripper

ほとんど使わなかったツール

使わなくても何とかあったもの

- LinPEAS
- WinPEAS
- BloodHound
- Powershell Empire

まとめ

まとめ

- Learn Oneで申し込んで気持ちに余裕を持たせる（推奨）
- ラボでしっかり学ぶ
- ラボでやったことを自分用にまとめる
- レポートを書く練習をする
- 試験前はちゃんと寝る
- 試験でマシンを攻略しても安心せず、証跡をしっかりと残す

Try Harder!