HACKTHEBOX INTRO

How to get started

What we will cover today

_> WHOAMI

Intro to HTB
- Why do HTB?
- How do I get started?
  - I feel every box is super hard to approach, what do I do?
- Stuff you should know about before even attempting

Useful tools in HTB
- nmap (quick guide)
- Burpsuite
  - Different web requests

_> WHOAMI

- Emil Hørning
- 3rd semester Cybersec student
- Used to be #1 in the danish Leaderboards for HTB
- Work as penetration tester at TDC
- Also make challenges for haaukins
- Have 1 masters in computer science from ITU
  - Yes I am doing my 2nd masters
  - Yes I did it because I didn't want to move out of the dorm I live in (LOL)
- I love CTF and HTB.
- I started from basically no security knowledge ~2 years ago
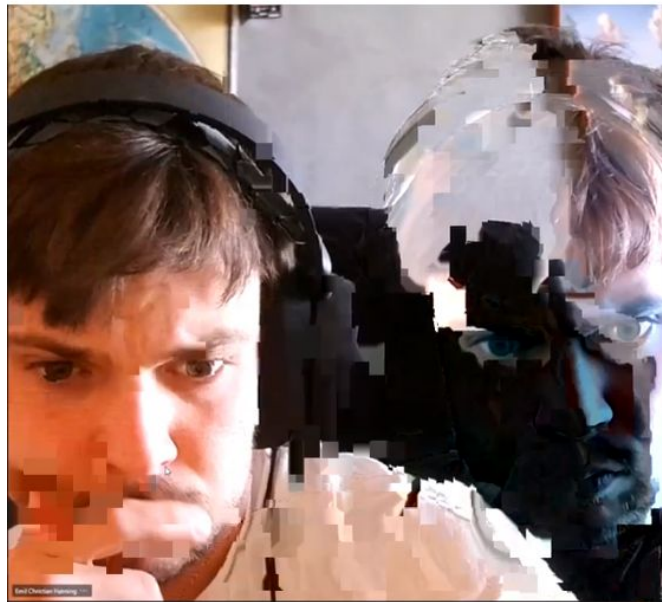
Why should I even do HTB???

Why should I even do HTB?

- It's super fun
  - When you get access you feel happy
- It enables creative thinking
  - Like solving puzzles, makes you happy!!!!!!!
- It feels cool to be a hacker
  - You can freeride how society views hackers and present yourself clever and mysterious, even if you just do basic shit
- Makes your profile more attractive in security, even if you don't want to be a pentester
- Lets you learn a lot of fundamental stuff about security.
- It is super fun, really.

But it is so hard to get started

# I feel every box is super hard to approach, what do I do?

- I understand this so well. I really do.
  - The learning curve is super fucking steep
- You sit and stare at each box and have no idea how to even progress?

- The answer is simple, but not very pleasant:
- ***You have to keep trying different stuff, just keep trying!***
  - With that said I do have some tips, otherwise this session would be stupid and worthless.
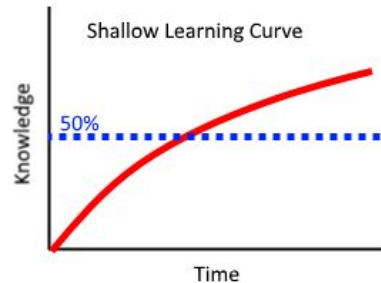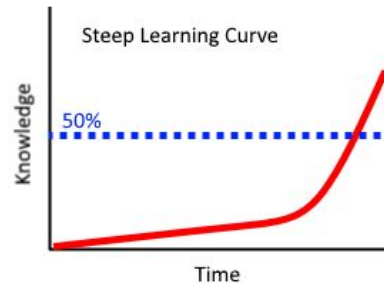
Kali linux (and offsec) motto

kali lincox
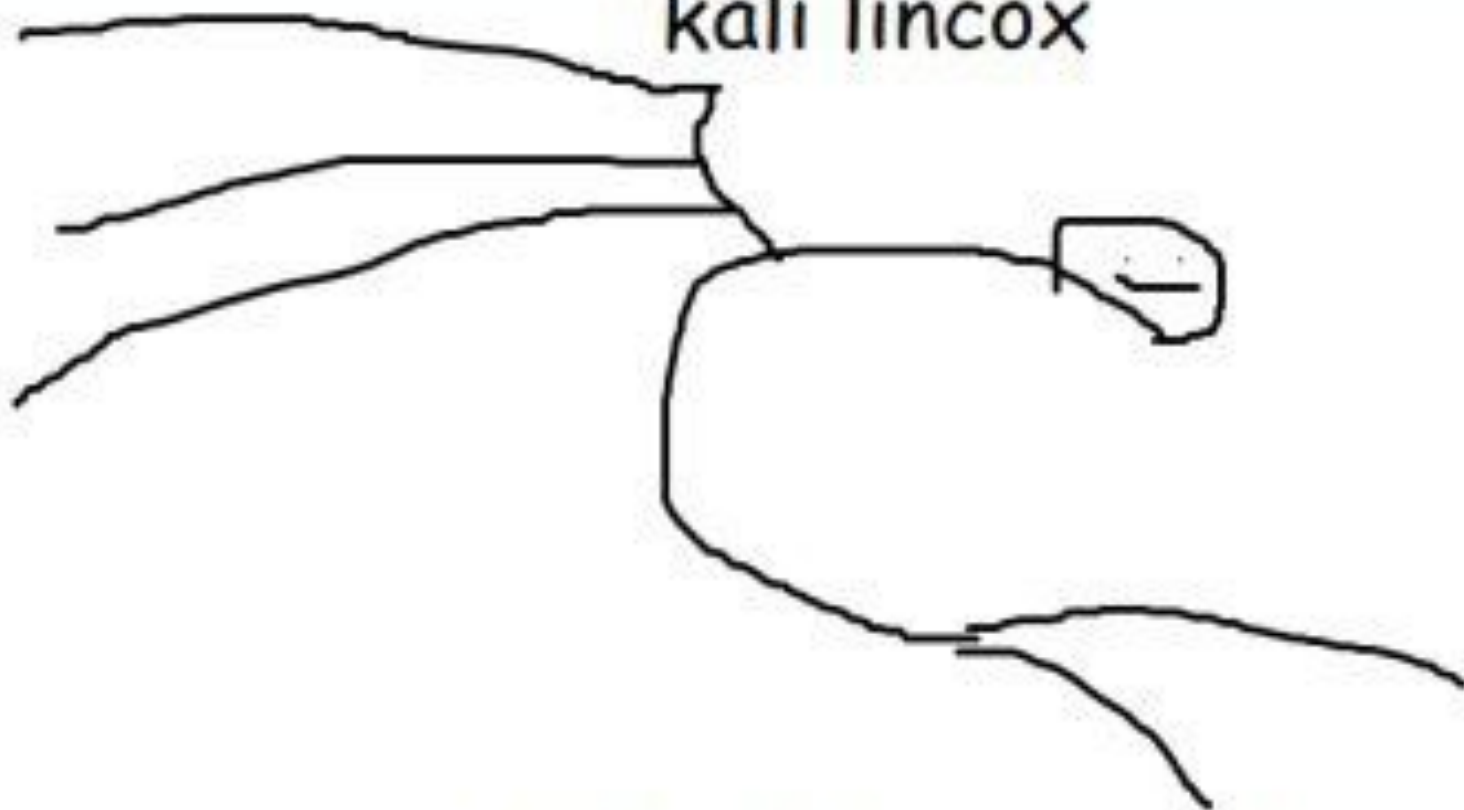
the louder u r the less u hear

1. Literal prerequisites for practicing ethical hacking and where to fulfill them (Excludes windows stuff)

Prerequisite	Where to learn it
Basic linux command line knowledge	overthewire.org or haaukins, Or the lost semester from MIT
Basic networking (ip addresses, TCP/IP stack, ports etc)	Revisit your networking course? youtube and the likes.
Basic programming in bash or python3	I learned it on uni, but you can learn it on youtube
Basic remote management over SSH	overthewire.org or haaukins

2. Stuff that will help you for sure if you know about it.

Prerequisite	Where to learn it
Basic web knowledge; requests (GET,POST), Anatomy of a request + hosts	HTB Academy has some good modules, or PORTSWIGGER web academy
Very basic encryption and hashing knowledge	Network security 1? Fundamentals. The lost semester at MIT
Encoding knowledge (Base64, URL-encoding, hex encoding)	This just comes with practice, but I would read up on these 3

TIER 0/1 MODULES

I really recommend doing all these on HTB Academy.

It will take a lot of time, but it's worth it

https://academy.hackthebox.com/

TIER 0
MODULES

I really recommend doing all these o[...]

It will take a lot of time, but it's worth [...]

https://academy.hackthebox.com/

HTB ACADEMY

1 more approach to getting started (paid :-s)

- Get HTB premium so you can access old retired machines.
- Start the latest easy retired machine and find a writeup
  - Good writeups are on the machine page
  - I also like Ippsec videos
- Try to do the box, if you are stuck for more than 10 minutes, consult the writeup.
- Whenever you read something in the writeup you don't know about it, you should go research it

Note: This is a tedious but effective approach.

Closing thoughts

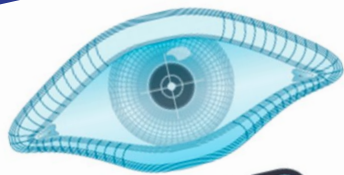Hackthebox and other ethical hacking platforms are hard to approach. It takes some dedication

SO WHAT NOW?!

Let us go through some tools together

- Nmap
- Gobuster
- Burpsuite + foxyproxy

Everyone please connect to BOUNTYHUNTER

Retired easy machine on HTB

(I will go through it slow)

BountyHunter

OS	RELEASE DATE	DIFFICULTY	MACHINE STATE
Linux	24 Jul 2021	Easy	Retired