So you wanna do OSCP?

or

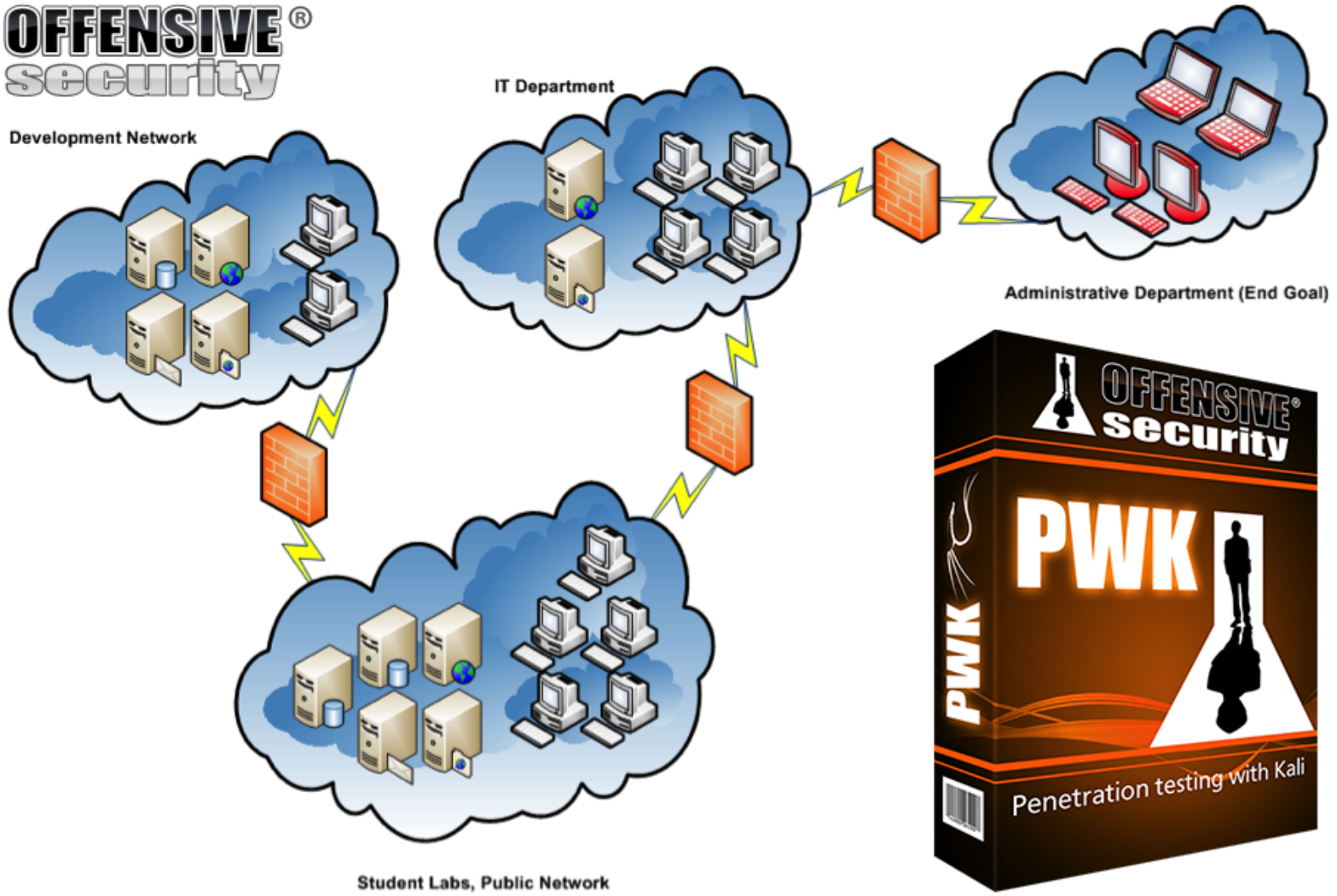
how I stopped being a miserable sysadmin and got a totally sweet job breaking other people's nice things.

or

(almost) everything I know about pentesting I learned from Hannibal Lecter.

What am I talking about?

- Penetration Testing With Kali Linux - PWK



What am I talking about?

- Offensive Security Certified Professional - OSCP

Who am I?

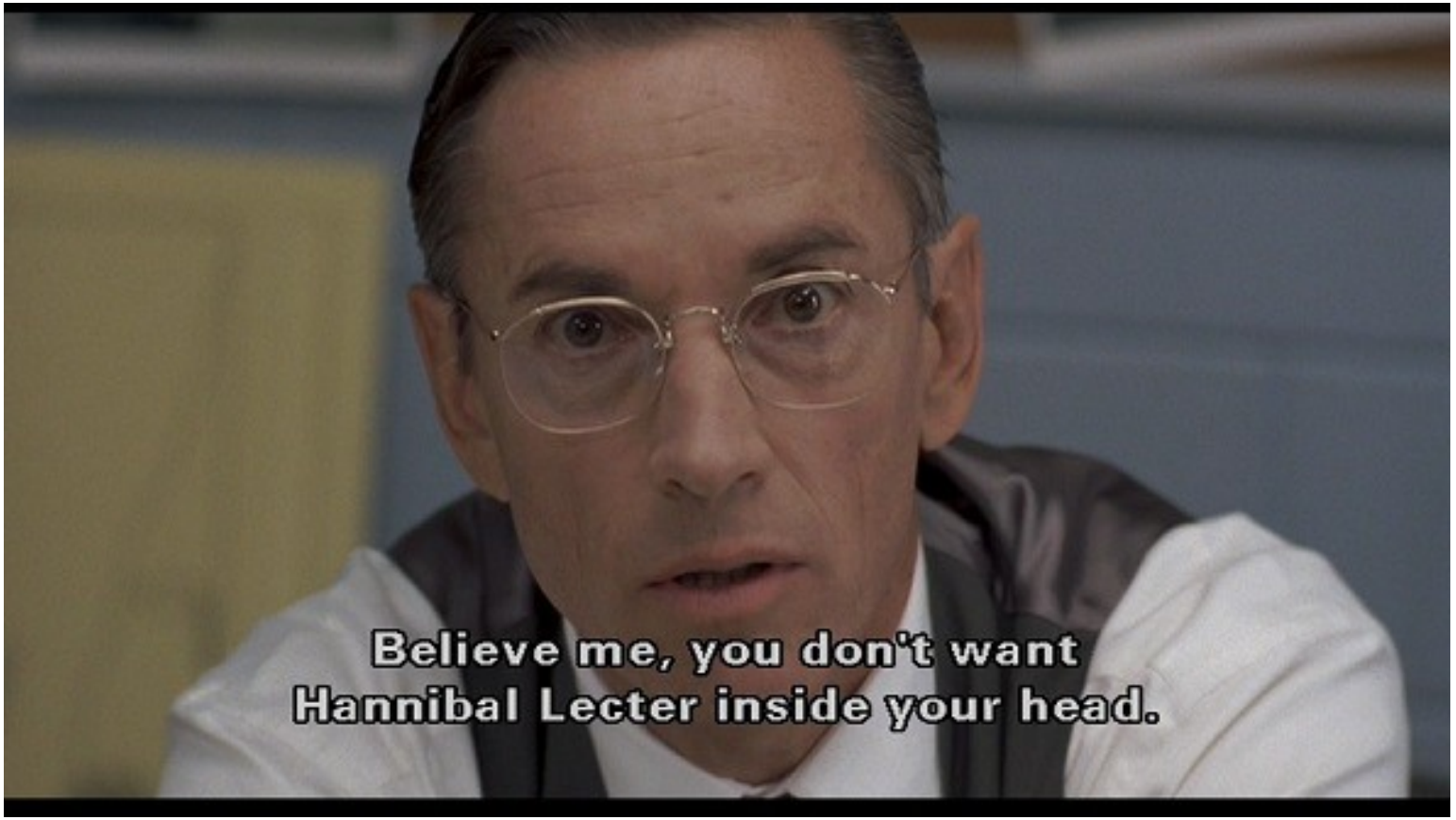
- Mike Loss
- Was a systems engineer at Curtin.
- Learned some stuff about info sec.
- Got frustrated not being able implement stuff I learned.

Who am I?

- Decided it would be more fun to learn to break stuff.
- Did OSCP.
- Now work at Asterisk as a tester.
- I don’t speak for them and my opinions are my own.

Why you shouldn’t listen to me.

- I’m not a rep of Offensive Security.
- My course experience is a year old.
- I’m just some guy.



Why you should listen to me.

- I did the course and popped 49.5/50 lab machines.
- I did the exam and popped 5/5 targets.

Why is PWK/OSCP great?

- Practical training.
- Practical exam.
  - Actually respected by some industry people unlike most ‘pentesting’ certs.
- Pretty cheap, esp compared to SANS.

Item	Price in USD
Penetration Testing with Kali + 30 days Lab access + Certification	USD 800.00
Penetration Testing with Kali + 60 days Lab access + Certification	USD 1000.00
Penetration Testing with Kali + 90 days Lab access + Certification	USD 1,150.00
PWK Lab access – extension of 90 days	USD 600.00
PWK Lab access – extension of 60 days	USD 450.00
PWK Lab access – extension of 30 days	USD 250.00
PWK Lab access – extension of 15 days	USD 150.00
Upgrade from PWB v.3.0 to PWK	USD 200.00
Upgrade from PWB v.2.0 to PWK	USD 300.00
Upgrade from PWB v.1.0 to PWK	USD 400.00
OSCP – Certification retake	USD 60.00

Why is PWK/OSCP not that great?

- There are some gaps in the course.
  - No social engineering/phishing
  - Very light on:
    - Network attacks like arp spoofing
    - Active Directory domains
    - Web testing
  - Some content can feel dated.
  - Emphasis on ‘poppin shellz’.

- Conditions you to think everything will be exploitable and ‘client side doesn’t count’.
- Can no longer talk about certificate revocation without double checking letter order.
- OSCP kind of sounds like it stands for ‘open source child porn’.

What is it?

- The Coursework
  - PDF and videos – approx 60hrs w/exercises

What is it?

- The Labs
  - VPN connection to simulated corp networks.
  - ~50 Vms in 4 interconnected networks.
  - Best Fun EVER.

What is it?

- The Exam
  - Like the labs in miniature.
  - 5 Targets, 24 hours.

What should I know beforehand?

- Google-Fu
- Super basic scripting/coding – bash/batch/python
- Basic windows and linux command line
  - How permissions work in each
- Network fundamentals e.g. basic TCP/IP, subnetting, etc.
- Really basic Active Directory/Kerberos
  - e.g. what is a token, what is a ticket, why time is important, etc.

What will I need to have?

- A computer capable of running a VM.
- A decent internet connection.
- Use the VM Offsec provide.

NOTES NOTES NOTES

- There’s no way you can remember everything.
- Find a system that works for you.

SCREENSHOTS SCREENSHOTS SCREENSHOTS

- Shutter is pretty good.

ENUMERATE ENUMERATE ENUMERATE

- Having more info is almost always good

NOTHING is ever too obvious or too easy.

Post-Exploitation

- File System
- Logged in users
- Sniff some traffic

Other students are jerks

- Revert before attacking, revert again.

When you get stuck...

When you get stuck...

- **Lecter:** First principles, Clarice. Read Marcus Aurelius. Of each particular thing ask: what is it in itself? What is its nature? What does he do, this man you seek?
- **Starling:** He kills women...
- **Lecter:** No! That is incidental. What is the first and principal thing he does, what need does he serve by killing?
- **Starling:** Anger, social resentment, sexual frustration...

What the hell does that mean?

- It’s easy to get tunnel vision.
- Go back to first principles

Exam Technique

- Choose an early morning start time
  - Recon/enumeration script, THEN smash coffee til the output makes sense.
- Metagaming the points system

Exam Restrictions

- Read them carefully, they are kind of complex.

Additional Study Resources

- windows privesc fundamentals from fuzzysecurity - http://www.fuzzysecurity.com/tutorials/16.html
- basic linux privesc from g0tmi1k - https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation
- corelan exploit dev - https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows
- Pentestmonkey's SQL injection cheat sheet - http://pentestmonkey.net/category/cheat-sheet/sql-injection
- Exploitdb – search 'buffer overflow poc' and look for examples that provide the vulnerable software.

Handy Downloads and Tools

- Powershell Post-exploitation tools https://github.com/PowerShellMafia/PowerSploit
- SecLists - wordlists, payloads, webshells, oh my. https://github.com/danielmiessler/SecLists
- Offsec exploit db binaries https://github.com/offensive-security/exploit-database-bin-sploits

Any Questions?

I do wish we could chat longer,
but I’m having an old friend for dinner.