ROADMAP TO OSCP

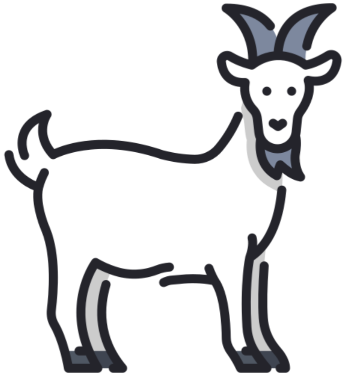
HEY THERE!

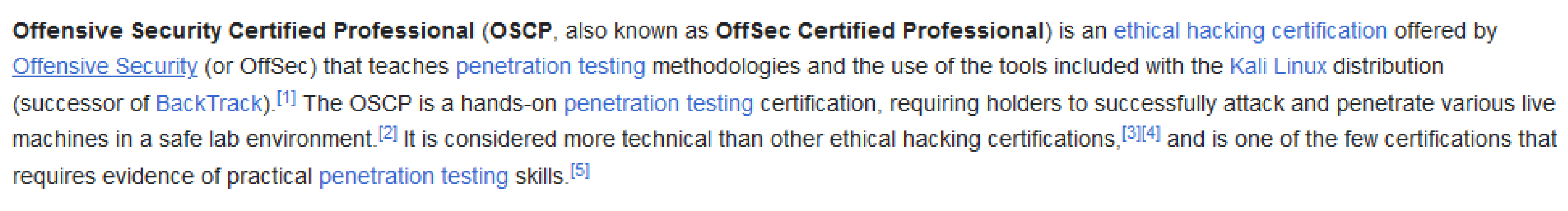
I am Ansh Bhawnani

I am here because I love to give presentations.

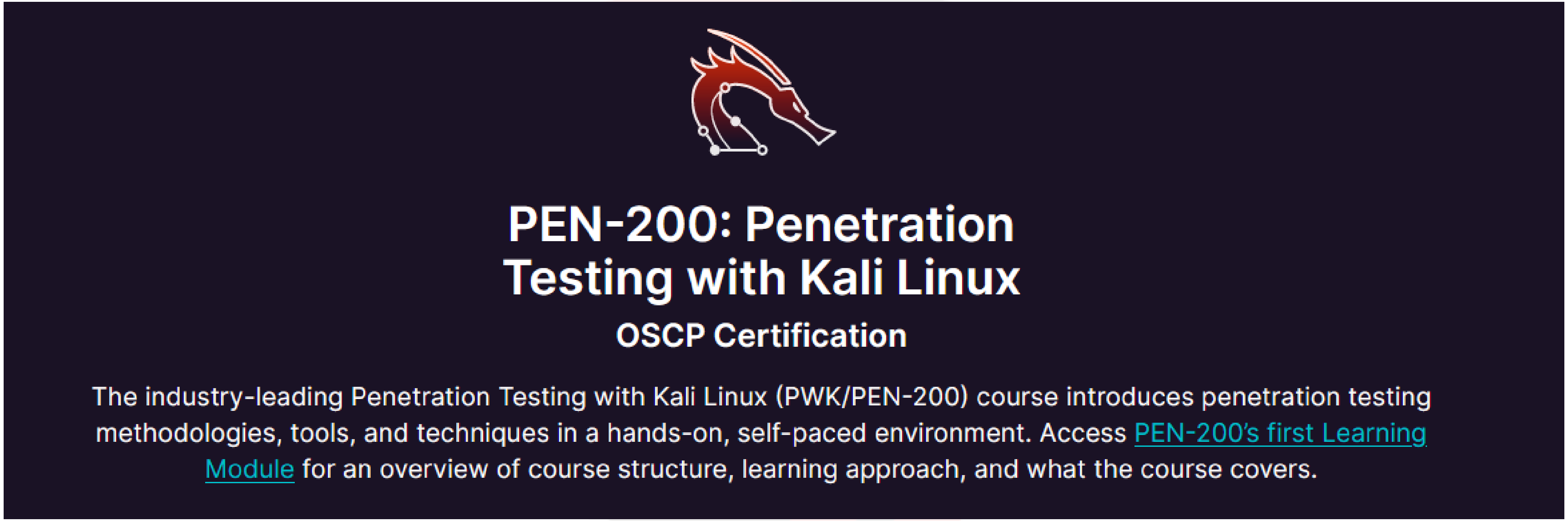
You can find me at @techhacker98

– WHAT IS OSCP?





Offensive Security Certified Professional (**OSCP**, also known as **OffSec Certified Professional**) is an ethical hacking certification offered by Offensive Security (or OffSec) that teaches penetration testing methodologies and the use of the tools included with the Kali Linux distribution (successor of BackTrack).[1] The OSCP is a hands-on penetration testing certification, requiring holders to successfully attack and penetrate various live machines in a safe lab environment.[2] It is considered more technical than other ethical hacking certifications,[3][4] and is one of the few certifications that requires evidence of practical penetration testing skills.[5]



PEN-200: Penetration Testing with Kali Linux

OSCP Certification

The industry-leading Penetration Testing with Kali Linux (PWK/PEN-200) course introduces penetration testing methodologies, tools, and techniques in a hands-on, self-paced environment. Access PEN-200's first Learning Module for an overview of course structure, learning approach, and what the course covers.

WHAT TO LEARN IN THE COURSE?

- Kali Linux Basics
- Command Line and Bash Scripting
- Essentials Tools
- Information Gathering
- Vulnerability Scanning
- Web Application Attacks
- Client Side Attacks
- ~~Buffer Overflows~~
- Finding and Fixing Public Exploits
- File Transfers
- Anti Virus Bypass
- Privilege Escalation
- Password Attacks
- Port Redirection and Tunneling
- Active Directory Attacks
- Metasploit Framework
- Powershell Empire
- Assembling the Pieces

FIRST THINGS FIRST

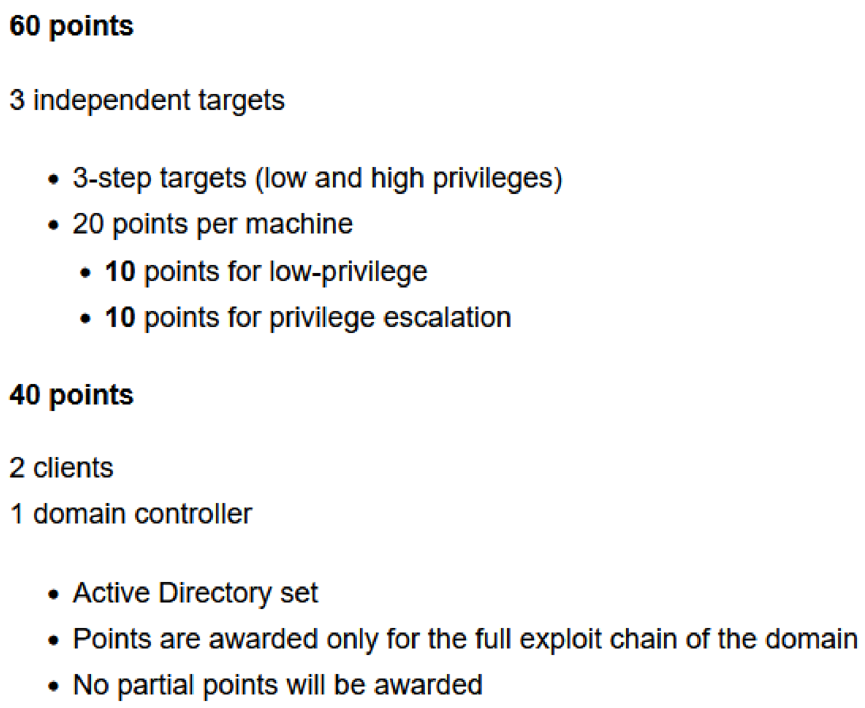
Who is this Course For?

- Infosec professionals transitioning to Pentesting
- People having basic Pentesting skills
- Security Professionals
- Not for absolute Beginners!

– ABOUT THE EXAM

- Yes, it’s a battlefield
  - 24 hour fully proctored
  - Exam time: **23 hour 45 minutes**
  - Another 24 hour for uploading documentation
  - Min 70 points for passing

Exam Structure



60 points

3 independent targets

- 3-step targets (low and high privileges)
- 20 points per machine
  - **10** points for low-privilege
  - **10** points for privilege escalation

40 points

2 clients

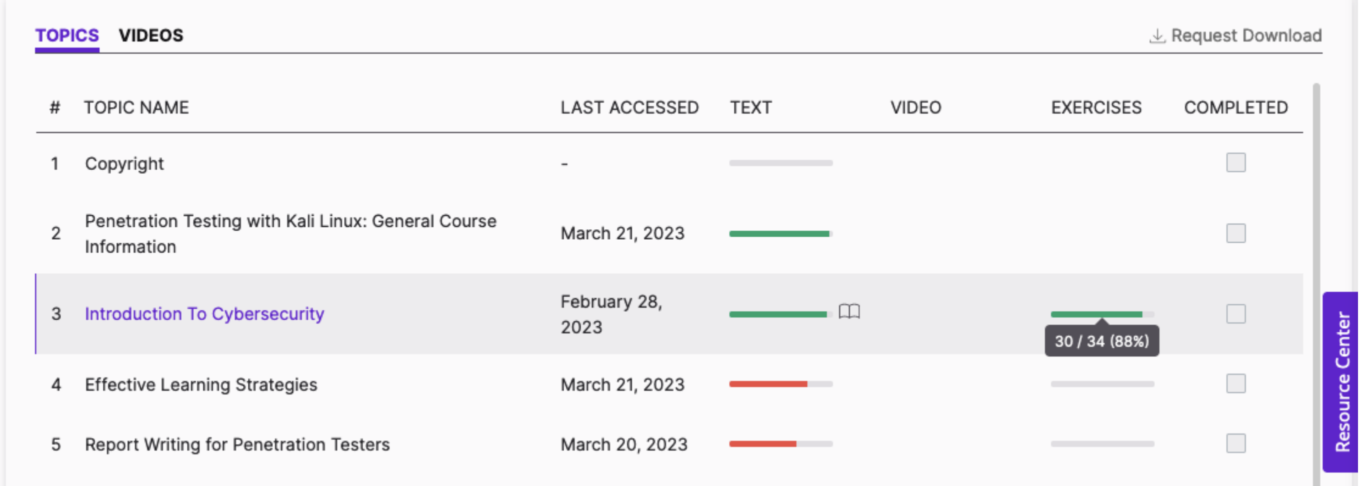
1 domain controller

- Active Directory set
- Points are awarded only for the full exploit chain of the domain
- No partial points will be awarded

Bonus Points (10)

- >= **80%** correct solutions for topic exercises in each topic
- **30** correct proof.txt hashes from challenge machines

Bonus Points (10)



#	TOPIC NAME	LAST ACCESSED	TEXT	VIDEO	EXERCISES	COMPLETED
1	Copyright	-				□
2	Penetration Testing with Kali Linux: General Course Information	March 21, 2023				□
3	Introduction To Cybersecurity	February 28, 2023			30 / 34 (88%)	□
4	Effective Learning Strategies	March 21, 2023				□
5	Report Writing for Penetration Testers	March 20, 2023				□

Passing Scenarios

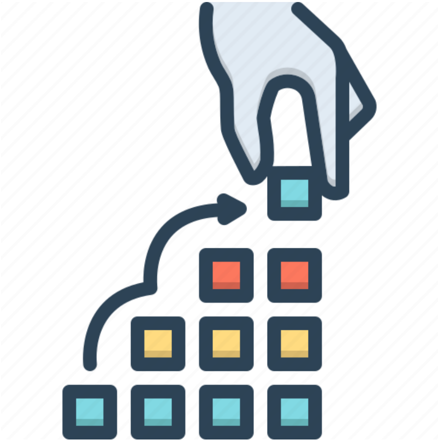
- (40) AD Set + (20) Non-AD + (10) Non-AD
- (10) BP + (40) AD Set + (20) Non-AD
- (10) BP + (40) AD Set + (10) Non-AD + (10) Non-AD
- (10) BP + (20) Non-AD + (20) Non-AD + (20) Non-AD

PWK COURSE

- PDF Book
- Videos
- Exercises
- Labs (now Challenges)

- **Lab Access**
  - 90 days voucher (1500$)
  - Costly, right?
  - Make sure you utilize those days!

– BEFORE THE COURSE



– BASIC KNOWLEDGE

- **Fundamentals**
  - **Windows Basics**
    - System Administration
    - User Account Management
    - Good CMD
    - Powershell basics
    - Groups and Policies
    - Service Management

- **Fundamentals**
    - **Linux Basics**
        - File System and Directory Structure
        - System Administration
        - User and Group Management
        - File Management and Access Control
        - Service Management
        - Bash shell basics

- **Networking Basics**
  - TCP/IP protocol suite
  - Basic network communication
  - Layer 3/4 addressing
  - OSI Model
  - Subnetting and NAT
  - Proxies and Tunneling

- **Web Application Basics**
  - Client Server Architecture
  - HTTP and HTTPS (SSL)
  - Request Response Protocol
  - HTTP headers
  - Status Codes and Errors
  - URL Concepts

- **Programming (YES!)**
  - Basics Paradigms (if-else/loops/data types/functions/files)
  - Ability to read and modify code
  - Basics of Python
  - Exception and Error Handling

- **Cryptography**
  - Encryption/Decryption
  - Hashing algorithms (MD5/SHA)
  - Encoding/Decoding
  - Public Key Infrastructure
  - Crypto Applications: SSH/VPN/NTLM

– PRACTICE LABS

- TJNull NetSecFocus (do them all)
- VulnHub, no?
- Proving Grounds (Play and Practice)
  - Buy the subscription (worth it)
- Hack The Box
- THM Offensive Pentesting

- Stuck, need walkthroughs?
  - Videos
    - IppSec
    - S1REN
    - HackerSploit
  - Articles
    - Hacking Articles
    - 0xdf
    - Infosec Writeups

– START THE PWK!

- Videos > PDF > PWK Labs
- PDF > Videos > PWK Labs
- Videos > PWK Labs
- Only PWK labs (not recommended ☹)

– TOOLS

- **Pentesting = Human Expertise + Arsenal of tools**

- Scanning
  - nmap
  - wpscan
  - nikto

- Enumeration
  - smbclient
  - Dirbuster/gobuster
  - NSE
  - impacket

- Password Attacks
  - john
  - hashcat
  - hydra

- Web Attacks
  - Burp Suite
  - nikto
  - netcat

- Initial Access
  - searchsploit
  - msfvenom
  - cewl

- Privilege Escalation
  - *-privesc-check
  - linpeas
  - winpeas
  - pspy

- General
  - netcat
  - powershell
  - socat
- Active Directory
  - crackmapexec
  - enum4linux
  - impacket toolkit
  - Bloodhound
  - mimikatz
  - Adpeas
- Pivoting
  - Proxychains
  - ssh
  - chisel
  - plink

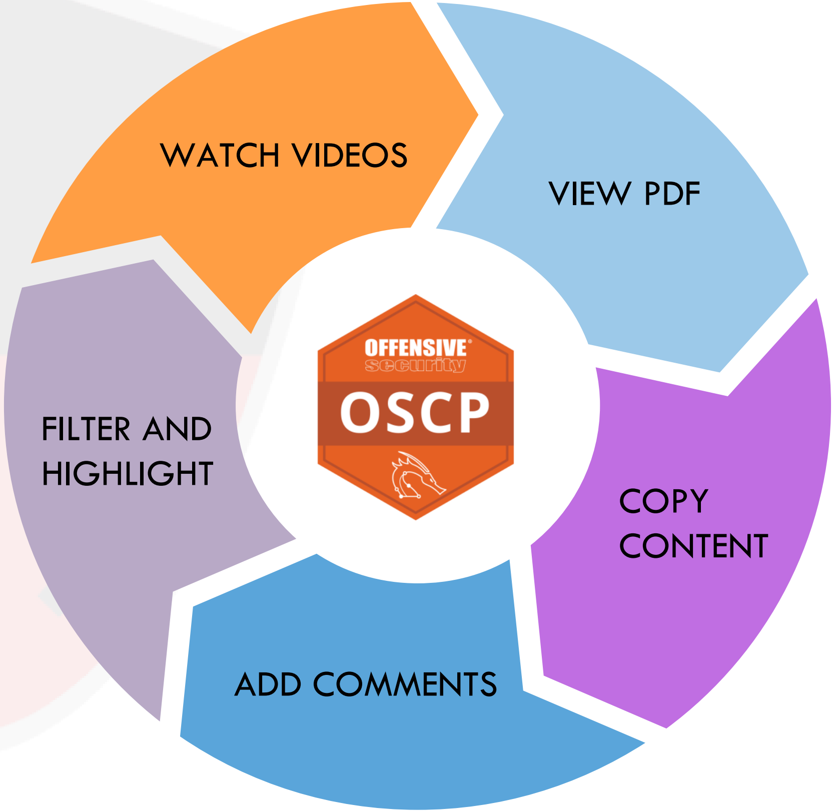
– NOTE MAKING

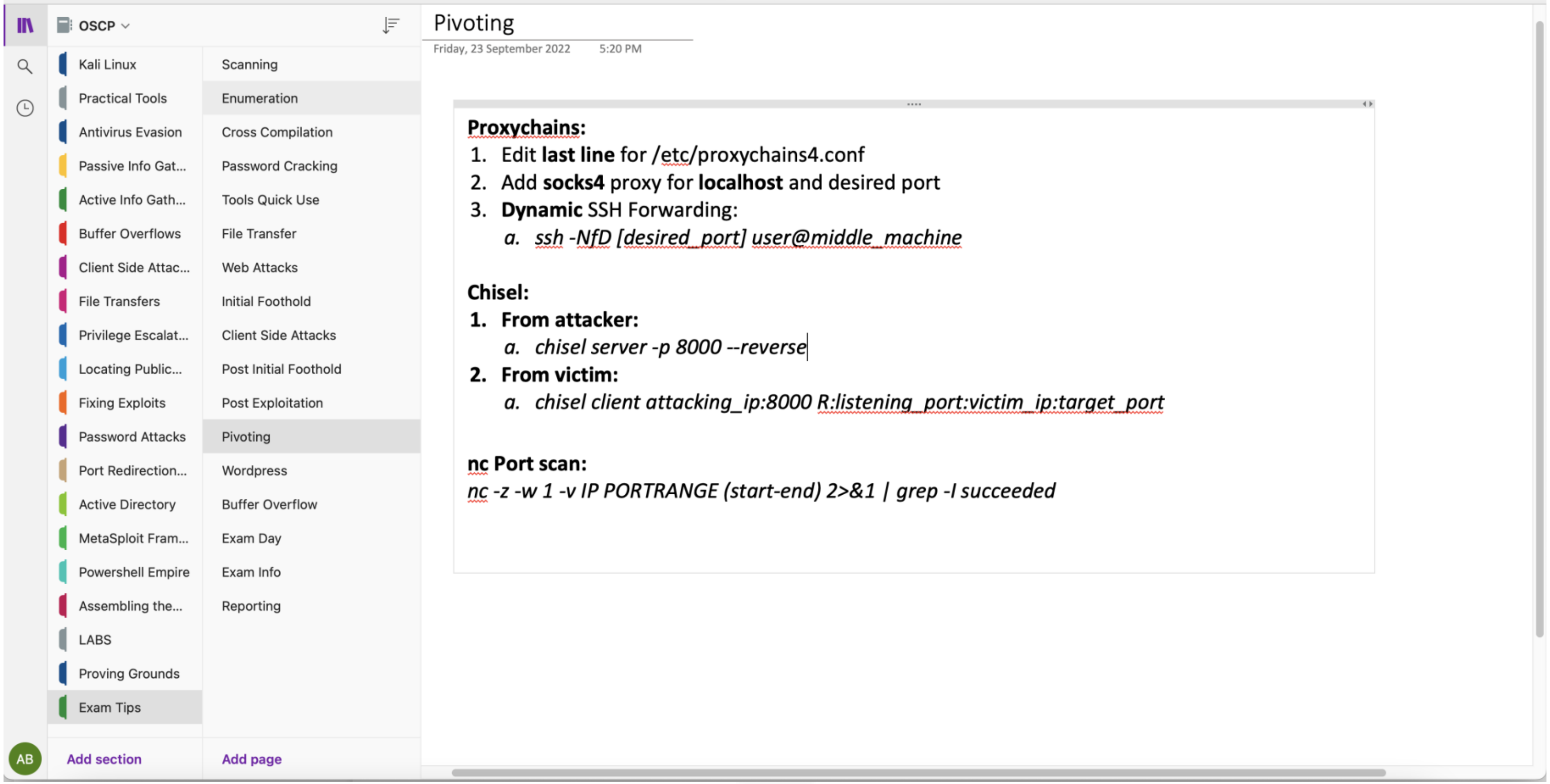
- **Tools?**
  - OneNote
  - CherryTree
  - KeepNote
  - Notion

- **OneNote**
  - Simple Interface
  - Cloud Sync
  - Free and feature-rich
  - Hierarchical Notebook structure

- **Lab Notes Format**
  - Recon
  - Initial Access
  - Priv Esc
  - Post Exploitation (if any)
  - Exploits Used
  - Tools Used
  - Other resources

— NOTE MAKING WORKFLOW





Pivoting

Friday, 23 September 2022 5:20 PM

Proxychains:

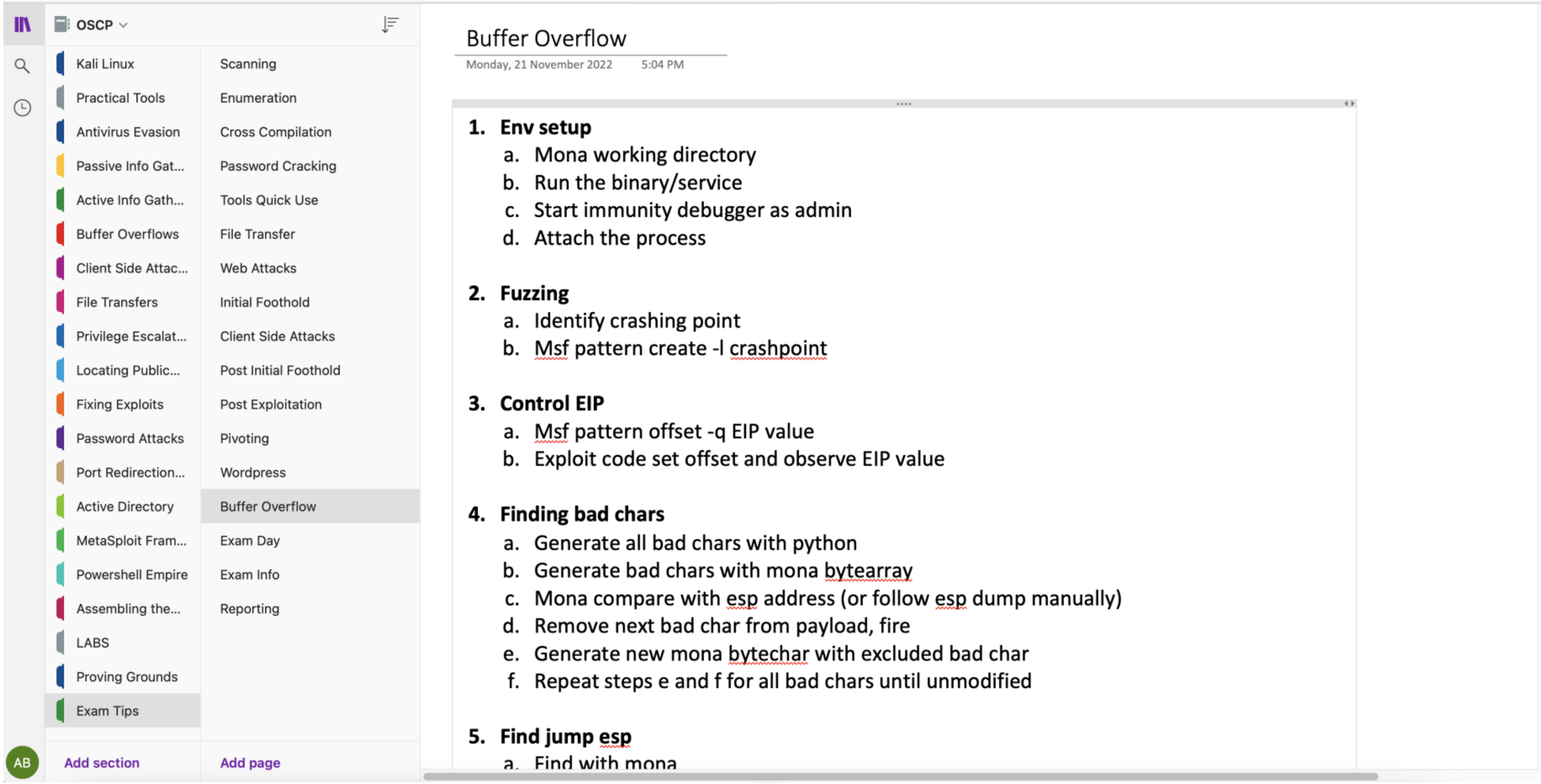
1. Edit **last line** for /etc/proxychains4.conf
2. Add **socks4** proxy for **localhost** and desired port
3. **Dynamic** SSH Forwarding:
   a. *ssh -NfD [desired_port] user@middle_machine*

Chisel:

1. **From attacker:**
   a. *chisel server -p 8000 --reverse*
2. **From victim:**
   a. *chisel client attacking_ip:8000 R:listening_port:victim_ip:target_port*

nc Port scan:

nc -z -w 1 -v IP PORTRANGE (start-end) 2>&1 | grep -I succeeded



Buffer Overflow

Monday, 21 November 2022 5:04 PM

1. **Env setup**
   a. Mona working directory
   b. Run the binary/service
   c. Start immunity debugger as admin
   d. Attach the process

2. **Fuzzing**
   a. Identify crashing point
   b. Msf pattern create -l crashpoint

3. **Control EIP**
   a. Msf pattern offset -q EIP value
   b. Exploit code set offset and observe EIP value

4. **Finding bad chars**
   a. Generate all bad chars with python
   b. Generate bad chars with mona bytearray
   c. Mona compare with esp address (or follow esp dump manually)
   d. Remove next bad char from payload, fire
   e. Generate new mona bytechar with excluded bad char
   f. Repeat steps e and f for all bad chars until unmodified

5. **Find jump esp**
   a. Find with mona

- PDF for note making
- Initial Access
- Priv Esc
- Post Exploitation (if any)
- Exploits Used
- Tools Used
- Other resources

– ACTIVE DIRECTORY

- **Courses:**
  - YouTube Playlist
  - Pentester Academy
  - Udemy
  - TCM Active Directory
  - **Bitten Tech**’s Active Directory for Pentesting ☺

- **Practice**
  - HTB Dante Pro Labs
  - HTB RastaLabs Pro Lab
  - THM Throwback
  - THM Attacktive Directory
  - THM Wreath

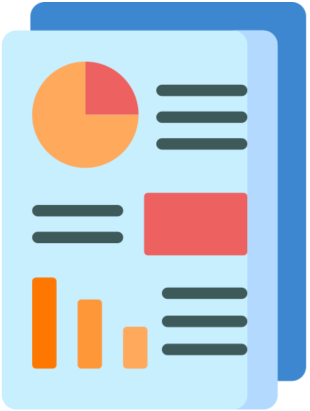
– BEYOND THE COURSE

- **Blogs:**
  - HackTricks
  - Hacking Articles
  - Ippsec.rocks

– GIVING THE EXAM

- **VMWare** > VirtualBox (you can use any)
- My Kali Specs:
  - 4 core CPU
  - 8 GB RAM
  - 128 MB Video Memory
- Have backups, snapshots
- Recon **parallely**, focus **manually**
- Don’t be **stuck**, and **don’t** keep switching

– REPORTING



- Use Official OffSec Report Template
- Just explain what you did, don't write too much
- Put as many screenshots as possible
- Proof read 2-3 times

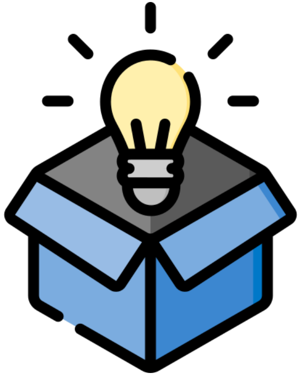
MY STRATEGY?

- Came with basic pentesting/CTF skills
- 1 year subscription
- Videos > PDF > PWK labs
- No exercises
- 1 month study, 4 months practice, 1 month note making
- HTB > PG >THM (~150 in total)
- 12 hour mock test – 3 random HTB machines
- Full day rest before exam
- Victory 🏆

ANY OTHER TIPS BRO?

- Have a **Plan**
- Have a **Dry Run** before the exam
- Practice Practice **PRACTICE**
- Create your **own notes/cheatsheet**
- Not about **how** to exploit, but **what** to exploit
- Take **Breaks**

- DON'T RELY ON TOOLS!
- Try Harder (but change)
- {Manual} Enumeration is the key
- Think out of the box
- Don't underestimate and overestimate



THANKS!