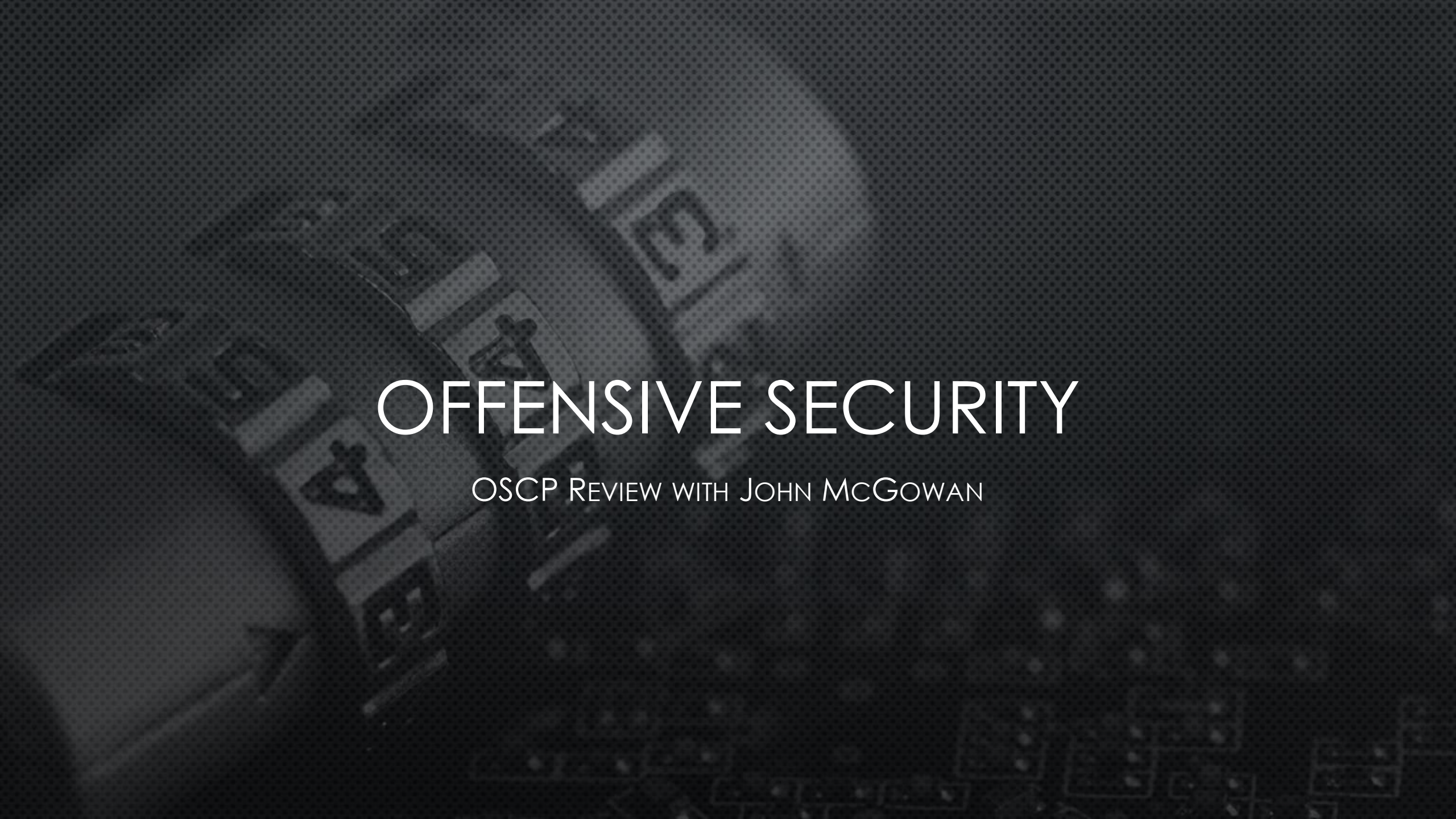


OFFENSIVE SECURITY

OSCP REVIEW WITH JOHN MCGOWAN

JOHN MCGOWAN

- Security Engineer
- OSCP,CISSP,CCNP,CCNA Security,GSEC,MCSA
- Telecoms
- Healthcare
- Finance
- Consulting
- 20 Years IT Engineering

COURSE CONTENT

STRUCTURE OF VERSION 1

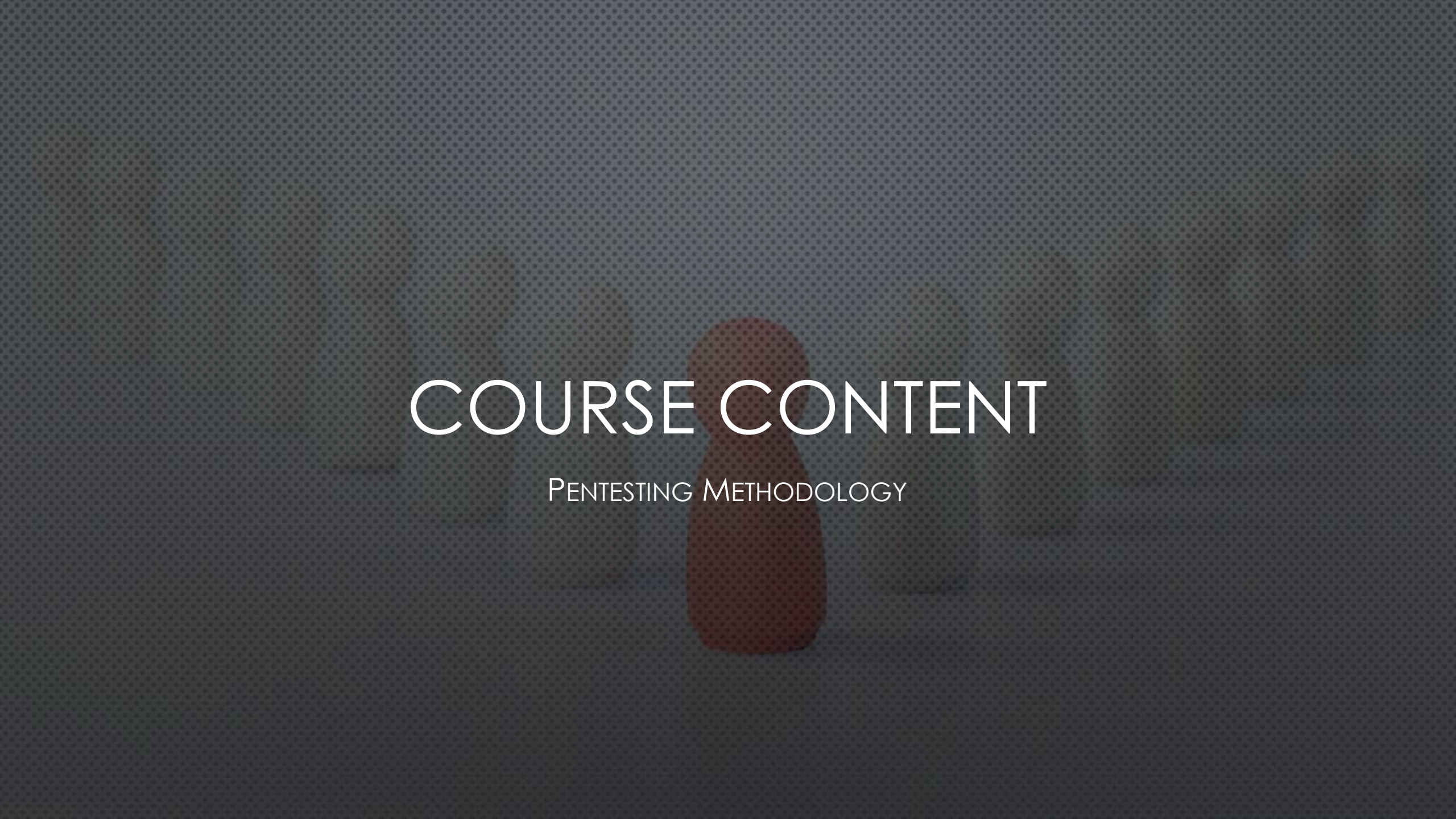
CHANGES IN VERSION 2

NOTES

RESOURCES

LESSONS LEARNED

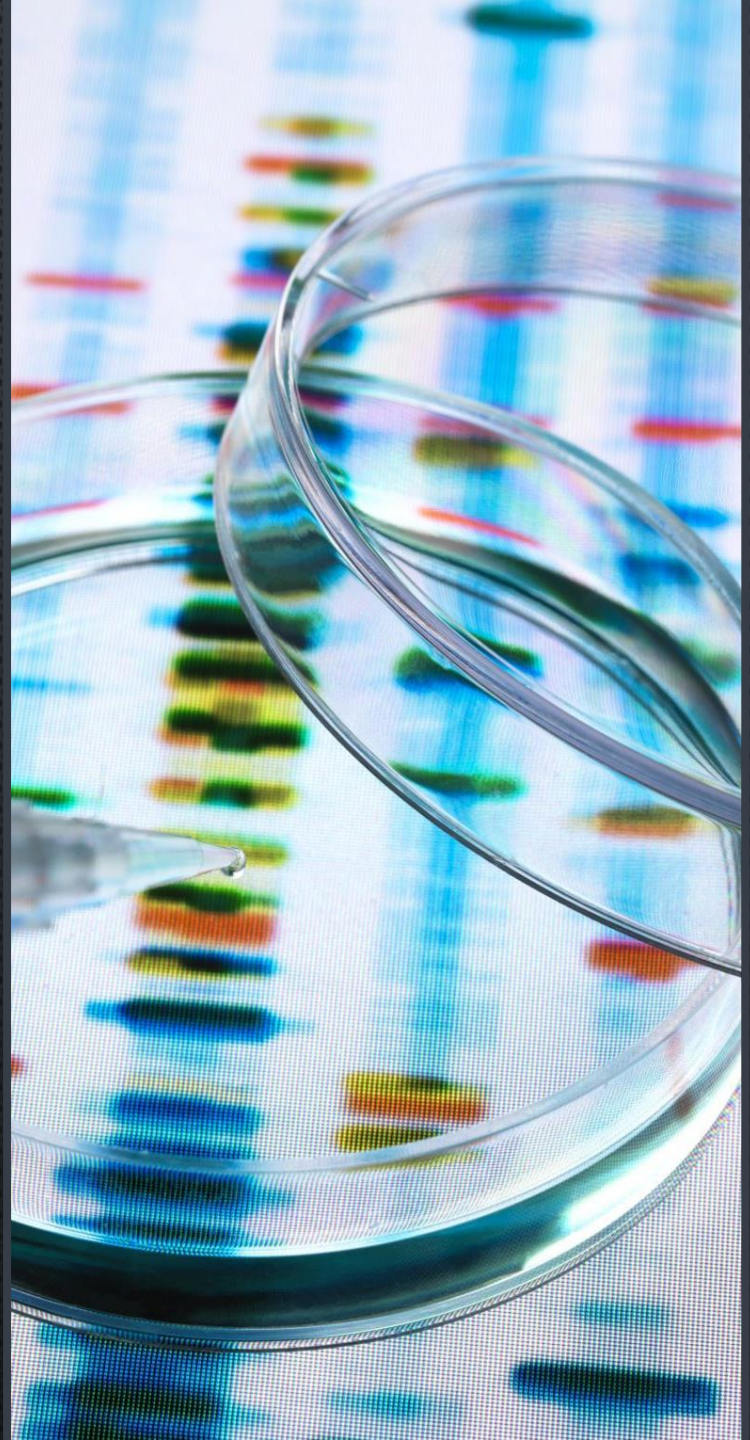
OFFENSIVE SECURITY COURSE BREAKDOWN



COURSE CONTENT

PENTESTING METHODOLOGY

CONCEPTS



- Vulnerability identification and analysis
- Pentester methodology
- Scanning
- Web Hacking
- File transfers
- CVE
- Service Misconfiguration
- Shells
- Payload obfuscation
- Local File Inclusion/Remote File inclusion
- Authentication Bypass
- Antivirus evasion
- Active Directory
- Pivoting and proxying
- Privilege Escalation
- Scripting & Automation

Methodology

Scanning

Enumeration

Exploitation

Privilege Escalation

Exam Objectives Shift – Jan 11, 2022

Version 1

- Buffer Overflow Machine (25)
- Windows/Linux Machine (25)
- 2xWindows/Linux Machines (20/25)
- Windows/Linux Machine (10)
- Course exercises & Lab Report (5)
- Emphasis on Binary Exploitation

Version 2

- Active Directory Set of 3 Machines (40)
- 3x Windows/Linux Machines (20)
- Buffer Overflow is possibly one of these machines, but counts for user shell.
- Course Exercises & Lab report (10)
- Emphasis on active directory exploitation and Kerberos

NOTES

Organizing Command Output to Efficiently produce Quality Reporting

Checks and Extended Notes

Obsidian Notebook

- Used to maintain notes on each box
- Templates for checks - each item I need to enumerate to get minimum baseline information
- Allows command output to be pasted directly to the notebook and export of pdfs
- Graphical view of inter-relation of notes
- Fast and Unintrusive
- Maintains Structured Enumeration Approach

Gitbook

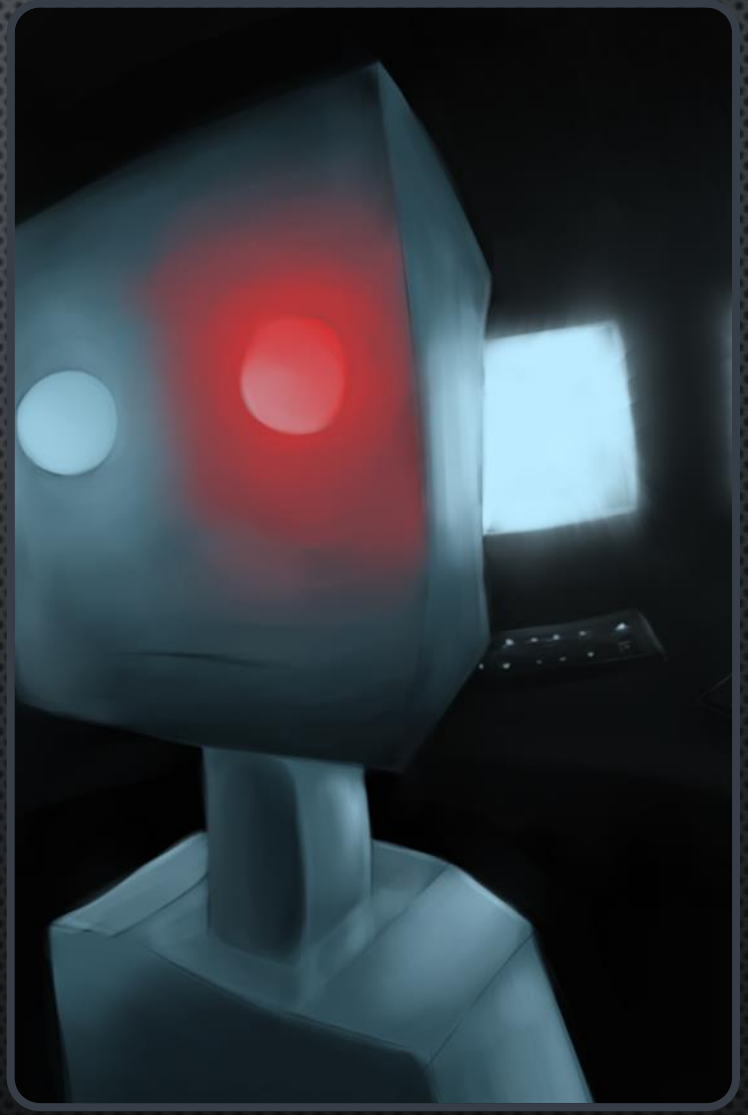
- Keep many examples of commands run like curl, mimikatz, or crackmapexec
- Quick instructions for complicated processes that I only use once in a while
- Commands that need to be used again, but not necessarily on every box
- Active Directory Processes
- Shells
- Custom Scripts I've written
- Versioning

AUTOMATION: REFINING THE PROCESS PRESENTS OPPORTUNITIES FOR AUTOMATION

Commands that are executed in specific situations (Gitbook)

Commands that need to be run on each box but are challenging to automate (Obsidian)

Commands that are the exact same on every box you run (Script)



RESOURCES

VIDEO & LABS

YOUTUBE:

- IPPSEC, 0XDF, XCT, JOHN HAMMOND, HACKERSPLOIT, COMPUTERFILE, RANA KHALIL, TIB3RIUS
- HTTPS://IPPSEC.ROCKS/
- HTTPS://0XDF.GITLAB.IO/

PLATFORMS:

- VIRTUAL HACKING LABS
- PWK LABS
- HACKTHEBOX
- TRYHACKME
- PROVING GROUNDS
- PENTESTERACADEMY
- PENTESTERLABS

WEB RESOURCES

- https://book.hacktricks.xyz/
- https://github.com/swisskyrepo/PayloadsAllTheThings
- https://gtfobins.github.io/
- https://lolbas-project.github.io/
- https://pentest.ws/tools/venom-builder
- https://github.com/hasamba/Hacking-and-CTF-Cheat-Sheet/blob/main/Hacking%20Cheat%20Sheet.md
- https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
- https://sushant747.gitbooks.io/total-oscp-guide/content/
- https://docs.microsoft.com/en-us/learn/?source=learn
- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md

LESSONS LEARNED