



OFFENSIVE SECURITY

OSCP REVIEW WITH JOHN MCGOWAN

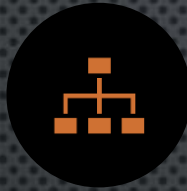
JOHN MCGOWAN

- 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

The background of the image consists of a dark gray, textured surface composed of interlocking puzzle pieces. These pieces are arranged in concentric circular patterns, creating a sense of depth and complexity. The lighting is subtle, highlighting the edges of the puzzle pieces and giving them a three-dimensional appearance.

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

Usage

The general structure of a call is this:

NOTES

---loglevel: ORGANIZING COMMAND OUTPUT TO EFFICIENTLY PRODUCE

specify a "log_level" with `--loglevel <level>`, where `<level>` can be `critical`, `error`, `warning`, `info` or `debug`. The `info` level is the default and does not fill the terminal with tons of output. You can set it to `debug` if you want to have more output and want to diagnose your triggers.

05000

- Subcommand: watch
- Name collections with `kscli`
- Subcommand: create
- How to evaluate?

docs

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

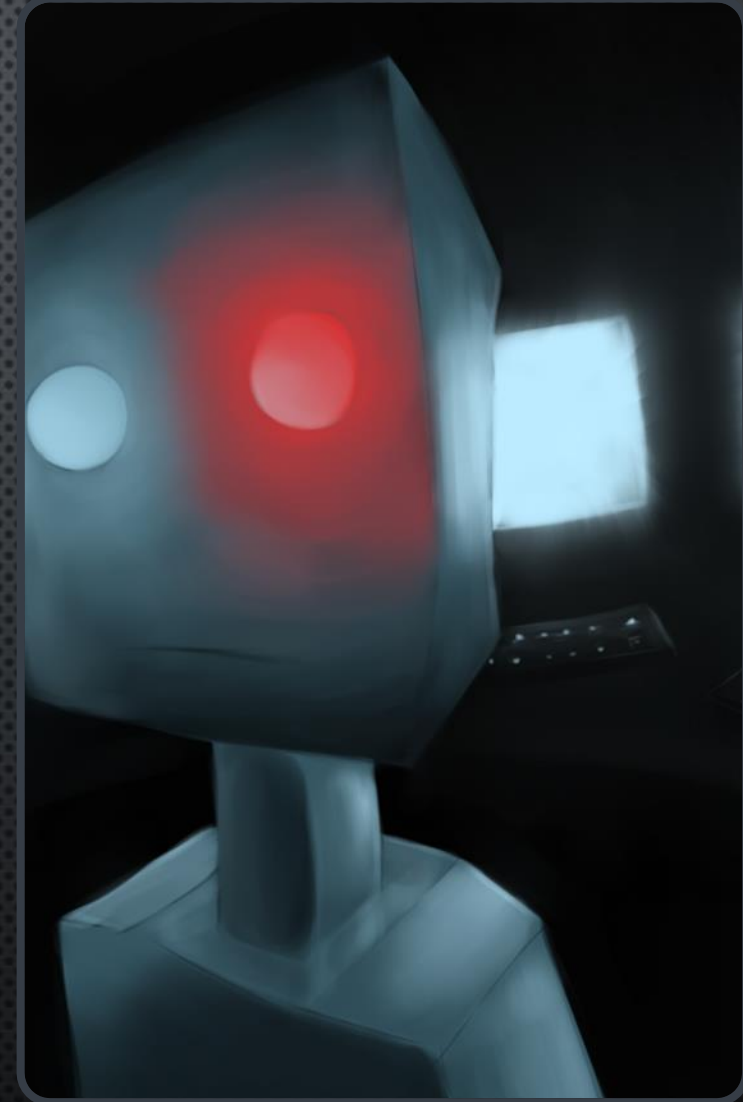
- KEEP MANY EXAMPLES OF COMMANDS RUN LIKE CURL, MIMIKATZ, OR CRACKMAPEXEC
- QUICK INSTRUCTIONS FOR COMPLICATED PROCESSES THAT I ONLY USE ONCE IN A WHILE
- COMMANDS THAT NEED TO BE USED AGAIN, BUT NOT NECESSARILY ON EVERY BOX
- ACTIVE DIRECTORY PROCESSES
- SHELLS
- CUSTOM SCRIPTS I'VE WRITTEN
- VERSIONING

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://ippsec.rocks/)
- [HTTPS://0XDF.GITLAB.IO/](https://0xdf.gitlab.io/)

PLATFORMS:

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

WEB RESOURCES

- [HTTPS://BOOK.HACKTRICKS.XYZ/](https://book.hacktricks.xyz/)
- [HTTPS://GITHUB.COM/SWISSKYREPO/PAYLOADSALLTHETHINGS](https://github.com/swisskyrepo/PayloadsAllTheThings)
- [HTTPS://GTFOBINS.GITHUB.IO/](https://gtfobins.github.io/)
- [HTTPS://LOLBAS-PROJECT.GITHUB.IO/](https://lolbas-project.github.io/)
- [HTTPS://PENTEST.WS/TOOLS/VENOM-BUILDER](https://pentest.ws/tools/venom-builder)
- [HTTPS://GITHUB.COM/HASAMBA/HACKING-AND-CTF-CHEAT-SHEET/BLOB/MAIN/HACKING%20CHEAT%20SHEET.MD](https://github.com/hasambha/Hacking-And-CTF-Cheat-Sheet/blob/main/Hacking%20Cheat%20Sheet.md)
- [HTTPS://BLOG.G0TM1K.COM/2011/08/BASIC-LINUX-PRIVILEGE-ESCALATION/](https://blog.g0tmilk.com/2011/08/basic-linux-privilege-escalation/)
- [HTTPS://SUSHANT747.GITBOOKS.IO/TOTAL-OSCP-GUIDE/CONTENT/](https://sushant747.gitbooks.io/total-osp-guiDe/content/)
- [HTTPS://DOCS.MICROSOFT.COM/EN-US/LEARN/?SOURCE=LEARN](https://docs.microsoft.com/en-us/learn/?source=learn)
- [HTTPS://GITHUB.COM/SWISSKYREPO/PAYLOADSALLTHETHINGS/BLOB/MASTER/METHODOLOGY%20AND%20RESOURCES/REVERSE%20SHELL%20CHEATSHEET.MD](https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20CheatSheet.md)



LESSONS LEARNED