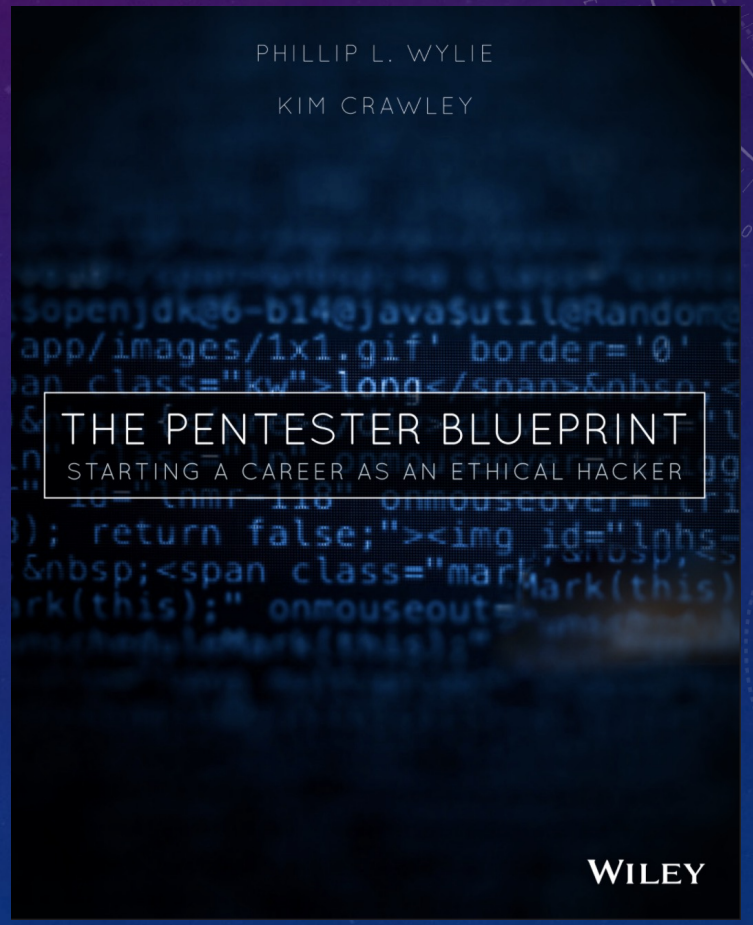
OFFENSIVE SECURITY FOR ALL

PHILLIP WYLIE, CISSP, OSCP, GWAPT

PHILLIP WYLIE, CISSP, OSCP, GWAPT

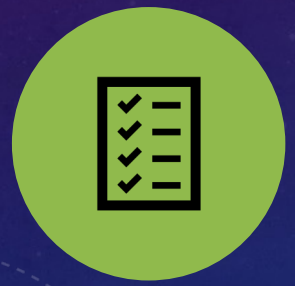
- Director of Security @ Alias Cybersecurity
- Cybersecurity 19+ Years & Offensive Security 10+ Years
- Former Adjunct Instructor @ Dallas College
- DEF CON 940 & The Pwn School Project Founder
- Concept creator & coauthor of “The Pentester Blueprint: Starting a Career as an Ethical Hacker”
- Featured in “Tribe of Hackers Red Team”
- Podcaster and Host of “Phillip Wylie Show” and previously “The Hacker Factory Podcast”



AGENDA

Offensive Security Introduction

Security Assessment Types



Methodology and Standards

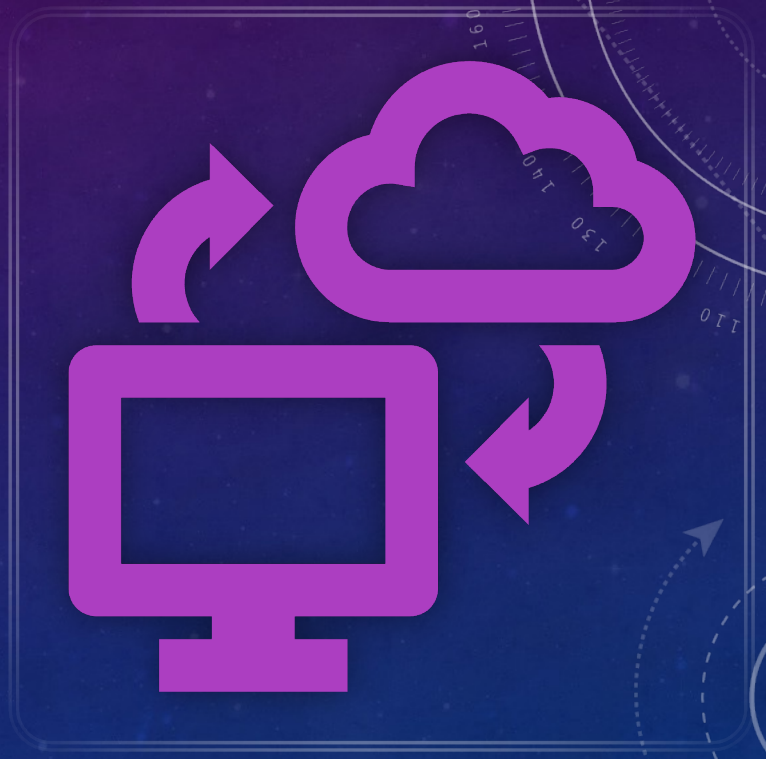
Security Assessment Tools

DEFINING OFFENSIVE SECURITY

•Offensive security, involves assessing the security of in scope targets from a threat attacker's perspective in order to identify vulnerabilities and weaknesses that could be exploited by threat actors. This can include techniques such as **hacking, social engineering**, and **physical breaches**, and is used to proactively identify and address security risks before they can be exploited. Offensive security is an important complement to vulnerability management, as it provides a way to validate the effectiveness of vulnerability management efforts and ensure that critical vulnerabilities are being prioritized and remediated.

OFFENSIVE SECURITY TARGETS

- Computers
- Networks
- Applications
- Cloud
- Hardware
- Transportation – Cars, aircraft, other multi passenger transportation types
- Physical Security – Assessing security of buildings
- People (Social Engineering)



OFFENSIVE SECURITY ASSESSMENT TYPES

- Vulnerability Management
- Vulnerability Assessments
- Penetration Testing aka Pentesting
- Red Teaming aka Adversary Emulation

VULNERABILITY MANAGEMENT

- Vulnerability management is the "cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating" system and software vulnerabilities. Vulnerability management is integral to computer security and network security and must not be confused with vulnerability assessment.

- Ref: https://en.wikipedia.org/wiki/Vulnerability_management

VULNERABILITY MANAGEMENT

Asset Discovery and Inventory

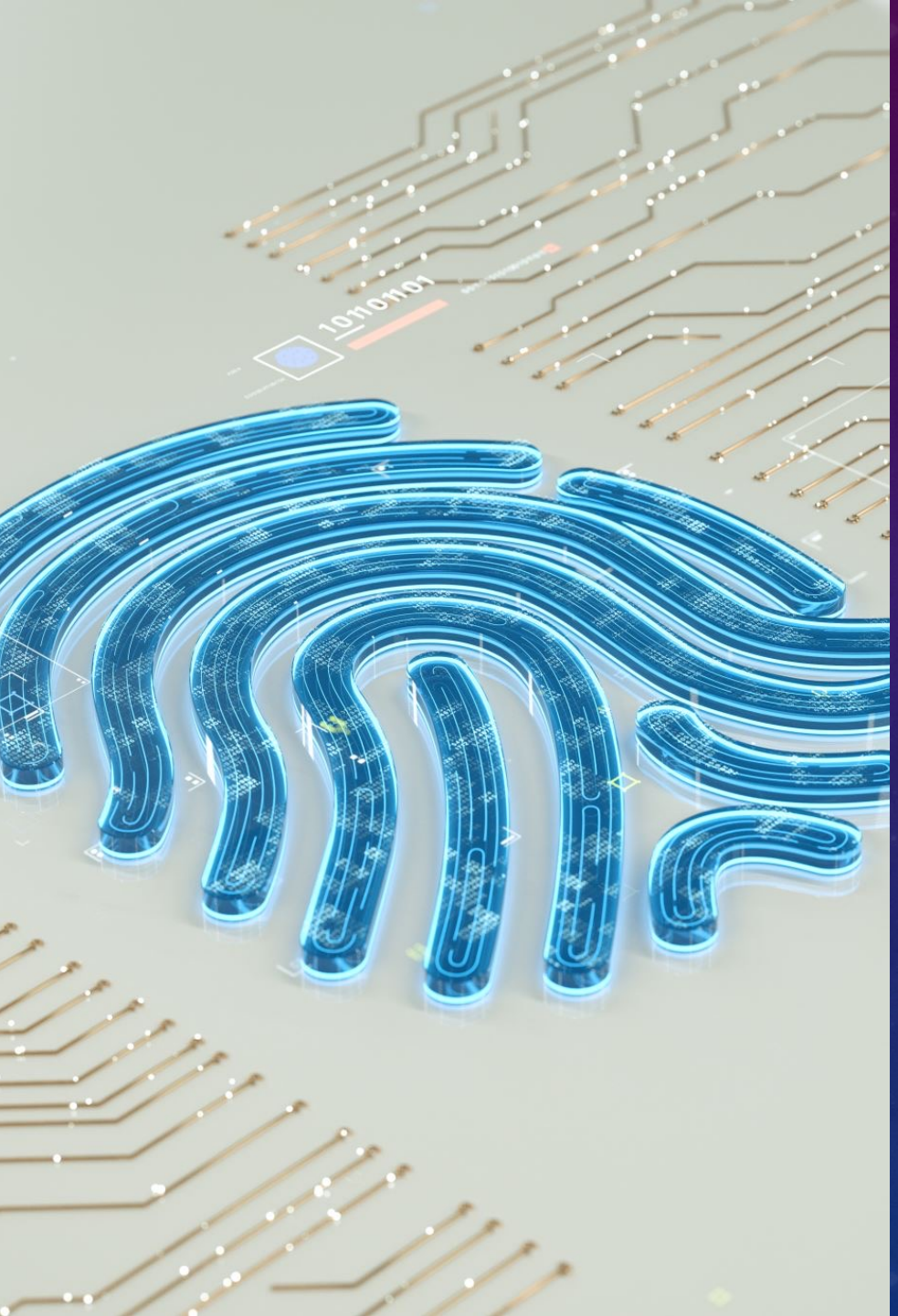
Vulnerability Scanning

Vulnerability Remediation (including patching)

Repeat

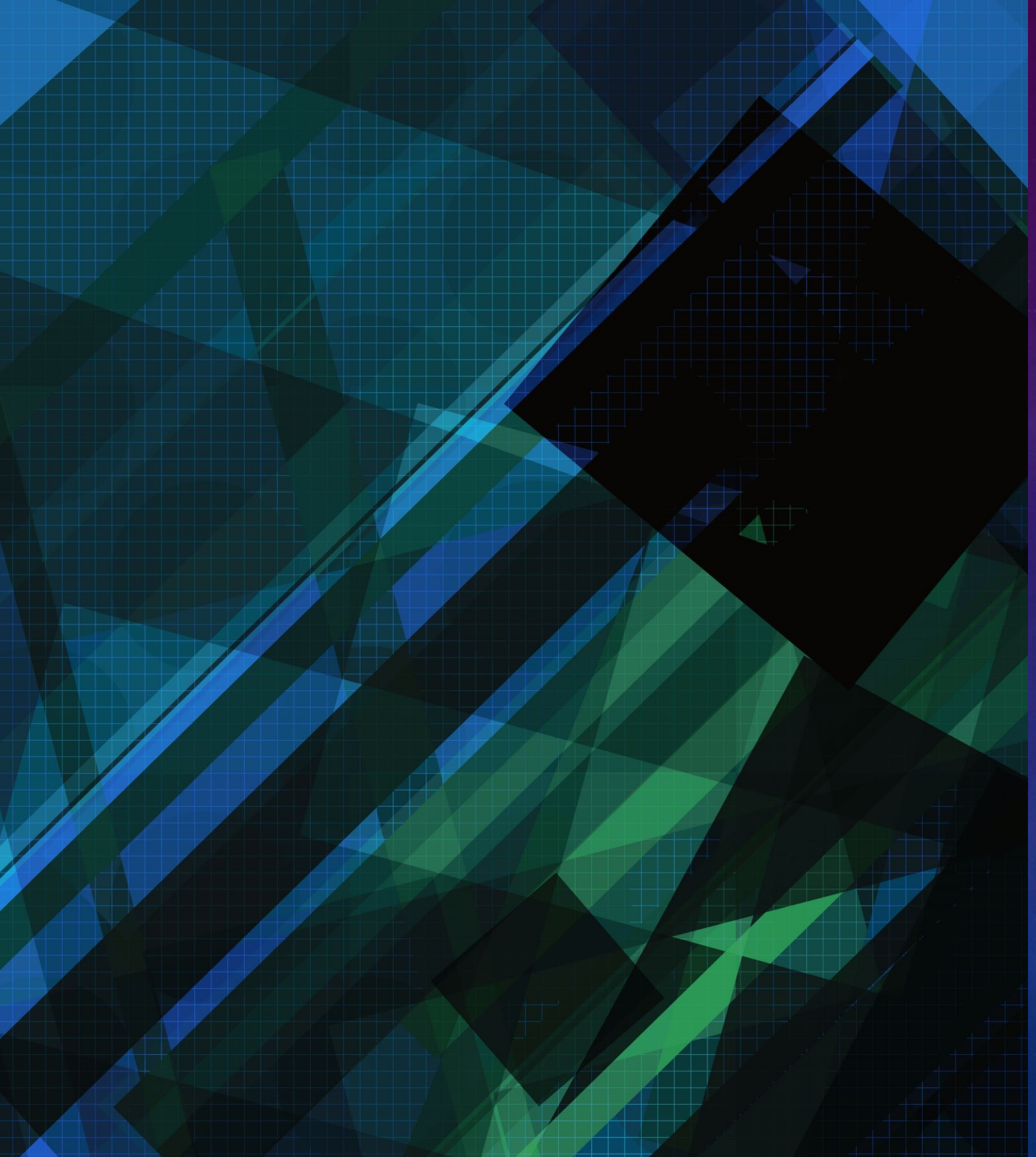
VULNERABILITY SCANNING

- A vulnerability scanner is a computer program designed to assess computers, networks, or applications for known weaknesses.
- Vulnerability scanning automates the process of detecting vulnerabilities by using a vulnerability scanner, which helps scale the amount of testing that can be done.



VULNERABILITY ASSESSMENTS

- Vulnerability assessments are similar to vulnerability scanning, since it is used to assess computers, networks, and applications for security flaws.
- Vulnerability assessments can be done manually without vulnerability scanners, but it takes more time, and is not as scalable.
- A combination of vulnerability scanning, and manual testing is most common and more effective and scalable for vulnerability assessments.
- A major difference between vulnerability assessments and vulnerability scanning, is that the findings are validated to ensure they are not false positives. They can be validated using tools or manual techniques.



PENETRATION TESTS

- Penetration Tests (pentests) similarly to vulnerability assessments are used to assess computers, networks, and applications for security flaws.
- Vulnerabilities are validated like in pentests vulnerability
  assessments, but exploitable vulnerabilities a re exploited if possible.
- Exploited vulnerabilities are taken a step further by using post exploitation techniques.

PENETRATION TYPES

Black Box (aka Blind) - Little to no details of the target in scope. More of a threat actor or malicious hacker approach.

Gray Box - Details such as IP addresses, domains, subdomains of in scope targets. Most pentests fall into this category.

White Box (aka Crystal Box, Assumed Breach) - More detailed information including IP address, domains, subdomains, documentation, accounts and password, and sometimes source code. Most thorough the three methods. When used in infrastructure pentests, it is sometimes referred to as the assumed breach method.

RED TEAMING

- Red Teaming is the process of using tactics, techniques and procedures (TTPs) to emulate a real-world threat actor with the goals of training and measuring the effectiveness of people, processes, and technology used to defend and environment.
- Also known as adversary emulation.

SECURITY ASSESSMENT TYPE COMPARISON

Vulnerability Management	**Vulnerability Assessment**	**Pentest**	**Red Team/Adversary Emulation**
• Asset Discovery/Inventory • Vulnerability Scanning *Not an assessment type.*	• Reconnaissance • Vulnerability Scanning • Vulnerability Validation	• Reconnaissance • Vulnerability Scanning • Vulnerability Validation • Exploitation • Post Exploitation	• Reconnaissance • Vulnerability Discovery • Exploitation • Post Exploitation

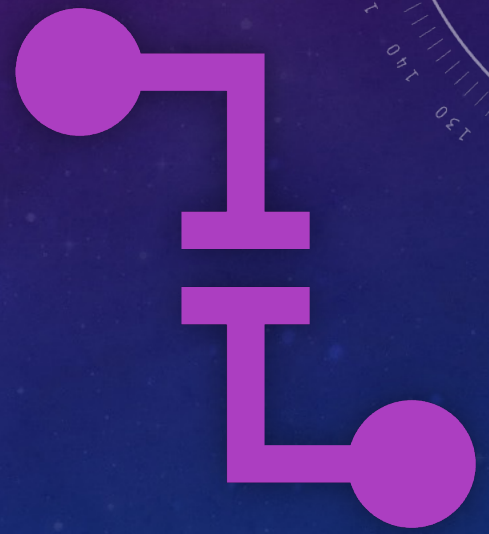
PENTESTING METHODOLOGY

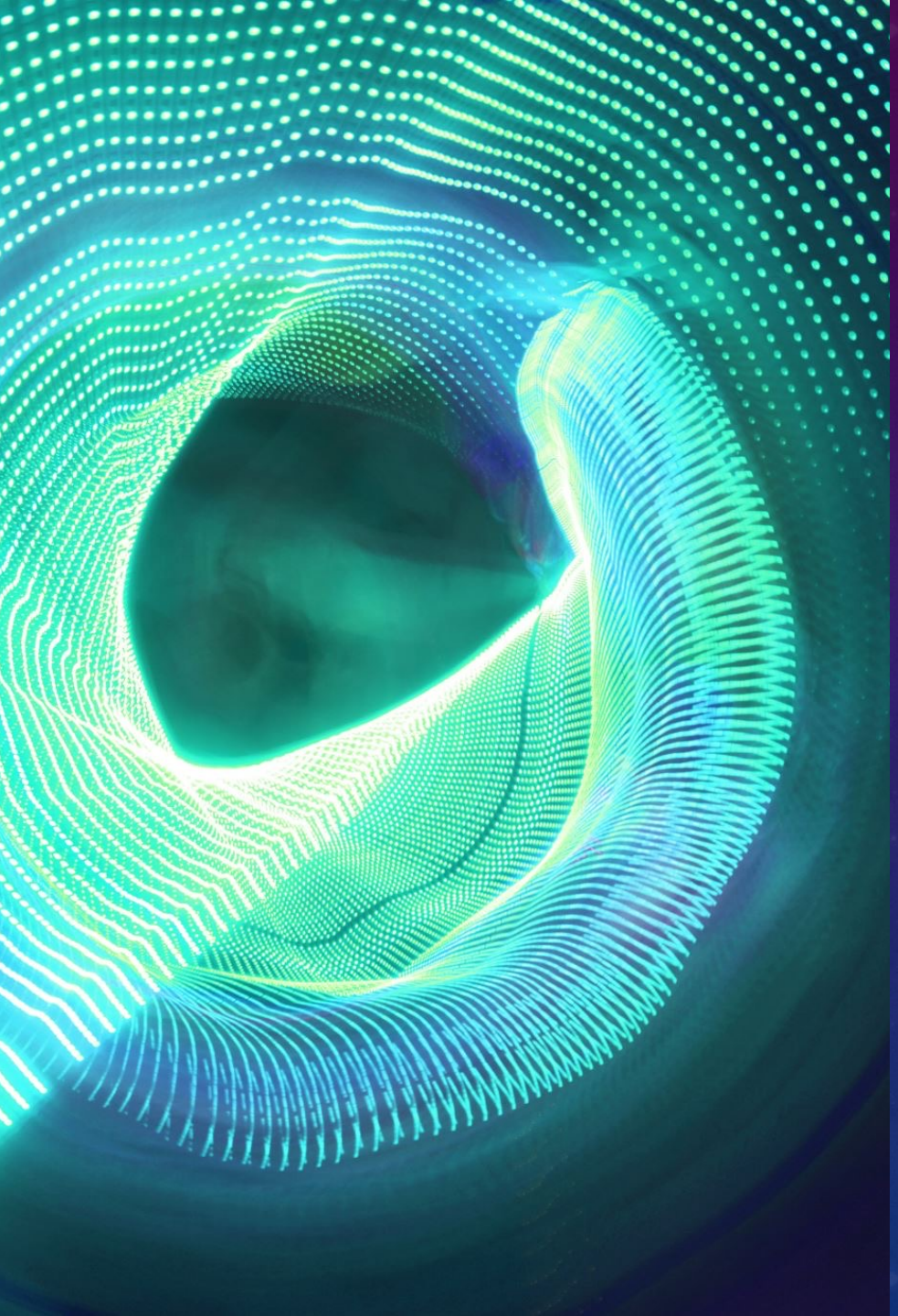
- Penetration Testing Execution Standard (PTES)
- Following are the main sections defined by the standard as the basis for penetration testing execution:
- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

Reference: http://www.pentest-standard.org/index.php/Main_Page

POST EXPLOITATION TECHNIQUES

- Lateral movement - The process by which attackers spread from an entry point to the rest of the network.
- Privilege escalation – The process of gaining elevated permissions on a system, or application.
- Accessing data – The process of trying to gain access to sensitive data.
- Data exfiltration – The process of trying to export data out of the network or environment.





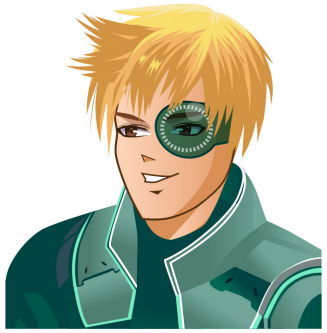
WEB APPLICATION PENTESTING

- OWASP (Open Web Application Security Project)
  - Web Security Testing Guide
  - OWASP Top 10
  - OWASP API Top 10

- References:
- https://owasp.org/www-project-web-security-testing-guide/v42/
- https://owasp.org/Top10/
- https://owasp.org/API-Security/editions/2023/en/0x11-t10/

TOOLS

- Port and service scanners – Nmap, Masscan
- Vulnerability scanners
- Exploit tools – Metasploit, Core Impact, Exploit Pack
- Command and Control (C2) Frameworks



FORTRA
Cobalt Strike

NMAP

Nessus

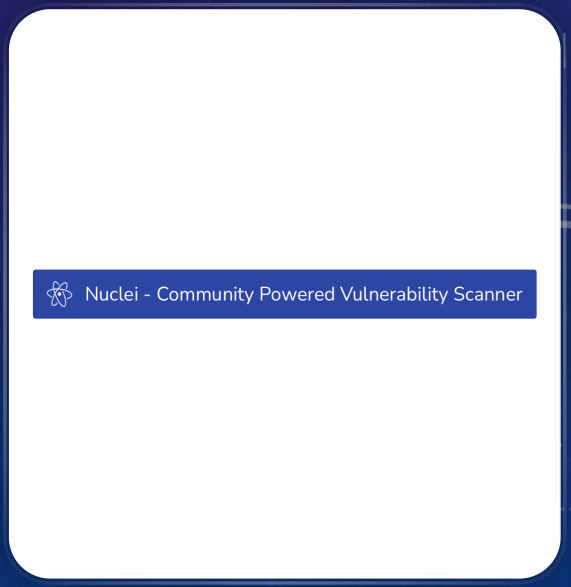
VULNERABILITY SCANNERS

Network Scanners

- Tenable Vulnerability Scanners – Nessus, Tenable Security Center
- Qualys
- Rapid7 Nexpose
- Greenbone OpenVAS – Commercial and free version
- Nuclei – Free command line scanner

Web Application Scanners

- AppScan
- Fortify DAST



LET’S CONNECT!

- LinkedIn: PhillipWylie
- Twitter (X): PhillipWylie
- Website: TheHackerMaker.com
- youtube.com/@PhillipWylie
- Podcast: PhillipWylieShow.com