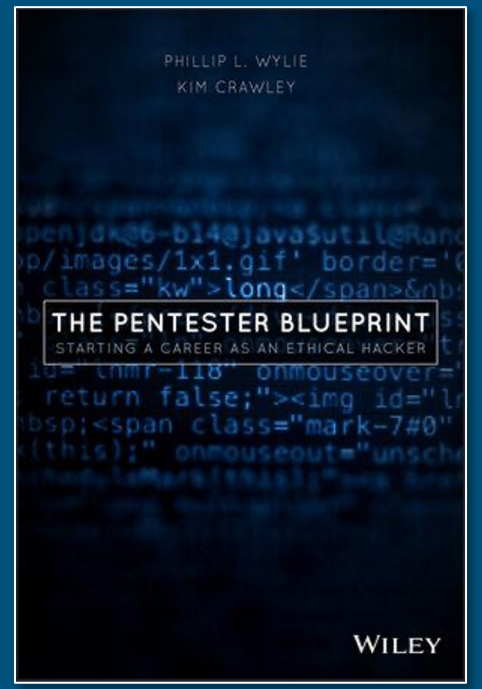
API Security Through External Attack Surface Management

Phillip Wylie, CISSP, OSCP, GWAPT

Phillip Wylie, CISSP, OSCP, GWAPT

- Security Solutions Specialist & Evangelist @ CYE
- Offensive Cybersecurity Professional & Instructor
- Former Adjunct Instructor @ Dallas College
- Concept creator and coauthor of “The Pentester Blueprint: Starting a Career as an Ethical Hacker”
- Featured in “Tribe of Hackers Red Team”
- “The Hacker Factory Podcast” Host
- DEF CON Group 940 Founder



My Offensive Security Career Journey & Fun Facts

Pro Wrestler > CAD Drafter > Sysadmin > Infosec > AppSec > Pentester

Agenda

- Defining Attack Surface Management
- Prioritizing External Attack Surface
- Risky Exposed Services & Protocols
- Risky API Exposures
- Discovering Attack Surface
- API Pentesting & Tools
- Addressing Gaps With External Attack Surface Management

Attack Surface Management

- To understand Attack Surface Management (ASM), we must first define Attack Surface.
- The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment.
  – NIST
- Attack Surface = attack vectors

ASM Importance

- Assess security from a threat actor perspective
- It is hard to assess and secure what you don’t know about
- Penetration testing once or twice a year is not enough
- Reoccurring vulnerability scans are not enough
- Threat actors are constantly scanning the Internet looking for vulnerabilities to exploit.

CISA: Reducing the Significant Risk of Known Exploited Vulnerabilities

Also, many vulnerabilities classified as “critical” are highly complex and have never been seen exploited in the wild—in fact, only 4% of the total number of CVEs have been publicly exploited. But threat actors are extremely fast to exploit their vulnerabilities of choice: of those 4% known exploited CVEs, 42% are being used on day 0 of disclosure; 50% within 2 days; and 75% within 28 days. Meanwhile, the CVSS scores some of these as “medium” or even “low” severity.

Reference: https://www.cisa.gov/sites/default/files/publications/Reducing_the_Significant_Risk_of_Known_Exploited_Vulnerabilities_211103.pdf

Attack Surface Management (ASM)

- ASM addresses both internal and external facing facing systems.
- While both are important, our focus is the **external attack surface**.

Elements of ASM

- Vulnerability Scanning
- Vulnerability Assessments & Penetration Testing
- Red Teaming aka Adversary Emulation
- Purple Teaming
- Bug Bounties
- Application Security & Testing Integrated in SDLC

Traditional ASM Gaps

- Compliance based penetration testing
- Narrow scopes – miss testing types, systems and whole environments
- Time and resource limitations
- Incomplete and inaccurate asset inventories

Prioritizing External Attack Surface

- Internet exposed and highly accessible to threat actors
- Internet exposed services and protocols are possible risks
- Penetration testing once or twice a year is not enough
- Reoccurring vulnerability scans are not enough

Risky Exposed Services & Protocols

- Remote Desktop Protocol (RDP)
- MS Windows Protocols
- SMB Protocols on UNIX or LINUX based systems
- Clear text protocols ie HTTP, FTP, Telnet

Risky API Exposures: What is Web API?

- API stands for Application Programming Interface.
- A Web API is an application programming interface for the Web.
- A Browser API can extend the functionality of a web browser.
- A Server API can extend the functionality of a web server.

Reference: https://www.w3schools.com/js/js_api_intro.asp

Risky API Exposures

- Insecure APIs
- Unintentionally exposed APIs

Addressing EASM Gaps

- EASM Discovery
- Reconnaissance Including OSINT (Open-Source Intelligence)

EASM Discovery

- Collect known IP subnets and domain name
- Reconnaissance

Reconnaissance: Collection

- IP address discovery
  - ASNs (Autonomous System Numbers)
  - ARIN & RIPE regional registrars
- Subdomain enumeration
  - Subfinder
  - OWASP AMASS
- Open-Source Intelligence (OSINT)
  - Shodan – locate unknown hosts
  - Crunchbase – mergers and acquisitions

Reference: Jason Haddix's "The Bug Hunter's Methodology"
https://www.youtube.com/watch?v=uKWu6yhnhbQ

Reconnaissance: Scanning

- Scan IP addresses & domains (including subdomains)
  - Nmap scan for live hosts
  - Nmap ports & service scans to identify web resources

API Endpoint Discovery

- API Enumeration Tools
  - Kiterunner – Restful API discovery
  - FUFF – Wordlist based API discovery

Reference:
Katie Paxton-Fear aka InsiderPhD - My API Testing Automated Toolbox
https://www.youtube.com/c/InsiderPhD

API Vulnerability Testing

- API Vulnerability Testing Tools
  - Autorize – Burp Suite extension for detecting IDOR
  - Logger++ - Multithreaded logging extension for Burp Suite
  - SQLMap – SQL injection testing tool
  - NoSQLMap – NoSQL testing tool
  - JWT_Tool – JSON Web Token testing tool
  - Burp Suite – Intercepting proxy and vulnerability testing tool

Reference:
Katie Paxton-Fear aka InsiderPhD - My API Testing Automated Toolbox
https://www.youtube.com/c/InsiderPhD

API Vulnerability Testing

- API Vulnerability Testing Tools
  - OWASP ZAP
    - OpenAPI add-on
    - GraphQL add-on
    - SOAP add-on
    - Import files containing URLs add-on

References:
https://www.zaproxy.org/faq/how-can-you-use-zap-to-scan-apis/
https://www.zaproxy.org/blog/2017-06-19-scanning-apis-with-zap/

API Vulnerability Testing

- OWASP API Security Top 10 & API Security Project
  - https://owasp.org/www-project-api-security/

Addressing Gaps with EASM

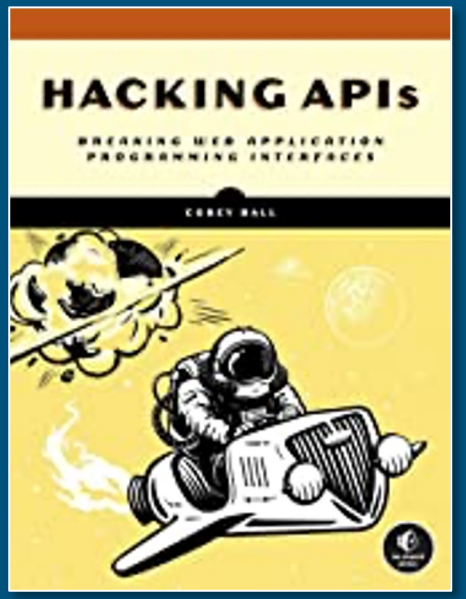
- Continuous discovery
  - Achieve and maintain a more accurate asset inventory
- Continuous testing
  - Vulnerability scanning
  - Pentesting
  - EASM platforms
- Automation
  - Improves scalability and resource limitations
  - Improves consistency
- Remediation
  - Timely and complete

References & Resources

- https://www.uscybersecurity.net/csmag/securing-apis-through-external-attack-surface-management-easm/ - by Phillip Wylie
- Reconnaissance reference: Jason Haddix's "The Bug Hunter's Methodology." https://www.youtube.com/watch?v=uKWu6yhnhbQ
- API discovery reference: Katie Paxton-Fear aka InsiderPhD – My API Testing Automated Toolbox https://www.youtube.com/c/InsiderPhD
- For further information on API penetration testing, get the new API hacking book by Corey Ball titled "Hacking APIs: Breaking Web Application Programming Interfaces."

  ISBN-13: 9781718502444

  Publisher: No Starch Press
- API Security Certified Expert by Corey Ball: https://university.apisec.ai/apisec-certified-expert



Thank you & let’s connect!

- linkedin.com/in/phillipwylie
- Twitter: PhillipWylie
- TheHackerMaker.com
- TheHackerFactory.simplecast.com
- YouTube: @PhillipWylie