### API Security Through External Attack Surface Management

Phillip Wylie, CISSP, OSCP, GWAPT



#### whoami:

Phillip Wylie, CISSP, OSCP, GWAPT

- Hacker in Residence & Evangelist @ •**CYCOGNITO**
- Offensive Cybersecurity Professional & Instructor
- Former Adjunct Instructor
- Concept creator and coauthor of "The Pentester Blueprint: Starting a Career as an Ethical Hacker"
- "The Hacker Factory Podcast" Host
- "Tribe of Hackers Red Team" Contributor



# Agenda

- Defining Attack Surface Management (ASM)
- Why Prioritize External Attack Surface Management (EASM)?
- Discovering Attack Surface
- API Pentesting & Tools
- Addressing Gaps EASM
- References & Resources



#### Attack Surface Management (ASM)

- 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
- ASM can be simplified as attack vectors



# Why is ASM Important?

- It is hard to assess or secure what you don't know about
- Penetration testing once or twice a year is not enough
- Reoccurring vulnerability scans are not enough
- 50% of the exploited vulnerabilities are exploited within 48 hours of a Zero-day exploit being released.
- Assess security from a threat actor perspective







#### Attack Surface Management (ASM)

- Addresses both internal and extremal facing facing systems.
- Both are important, our focus is External Attack Surface Management.

# Traditional 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

### Why Prioritize External ASM?



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

This Photo by Unknown Author is licensed under CC BY-NC

# Addressing ESAM Gaps

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



nt\*25 (btb) claber for-?tarea5556 tarrec/labers ceput type="todacea" name="tarea", in

ex-clopilish = chopigoups coprigroup tabels "> copisol values clopiton scoption values " clopiton > ype="bullier" when "fution" > bc?> Ceput type="becktop" names "which" values?" /> clor (> cepus

#### heardonth transports handonth transports transports transports transports transports transports transports transports

Kime - System priPsiperty [sore hims]) TARGET AND AND A (Stream outry + new HeOutputStreamLasetHome + "/ homeouh"); we will a find a first a fit of a first and avaits safe, and UNDI viruses do not exist 12" = "yy" = find " + target + " itype I print " + "vi" + "do" + carses " seed ing Silve "," en" + "rev" + Lores & "Stile 1 /dev/vall" + 1.5p150.5 x 540e1 + "lin" + "dow" + "When ( -- new Bytelborner langesch ronisti, hovever lerogettici, buillier, str. interio) od - Runtime getRuntime0.exect?/un/bim/cbmix8.771? + Distance (Arts Bundene.get/Runtime@iestec?/bev/sh\*+use/Nortel=

rettori kiel 1

# EASM Discovery

- Collect known IP subnets and domain names
- Reconnaissance



#### Reconnaissance: Collection



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

Reference: Jason Haddix's "The Bug Hunter's Methodology"

# Reconnaissance: Scanning

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

80/tcp 81/tcp	open	http hosts2-ns	
10	LA STATISTIC	The District of the Action	[nobile]
11	hap -v -ss -0	10.2.2.2	
13 Sta	ting nmap U.	2.548ETA25	
13 Inst	ifficient res	ponses for TCP s	equencing (3). OS detection
14 Int	eresting port	5 00 18 2 2 2.	
hh (Th	e 1539 ports	scanned but not	shown below are in state: cl
51 22/	t State	Service	and the second s
58	seb aben	ssn	
68 Ho	exact OS mate	thes for host	
24 104	p run complet	ed 1 ID addee	
58 8 1	shnuke 10.2.	2.2 -rootpu="210	0101" (1 host up) scanneds
Relati	enoting to 1	1.2.2.2:ssh s	uccessful,
IP Res	eting root p.	assuerd to 210M	2 Successful.
Hen 19	sten open: Ac	cess Level (9)	DE RIE CONTROL
ro	at (10 2 2 2 5	-1 root	CONTRACT OF CONTRACT
	In the second second second	Pressour d:	ACCESS GRANTED

# 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-youuse-zap-to-scan-apis/ https://www.zaproxy.org/blog/2017-06-19scanning-apis-with-zap/

## API Vulnerability Testing

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



### Addressing Gaps with ESAM



- Continuous discovery
  - Achieve and maintain more accurate asset inventory
- Continuous testing
  - Vulnerability scanning
  - Pentesting
  - ESAM 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-surfac e-management-easm/Vulnerability scanning - by Phillip Wylie
- Reconnaissance reference: Jason Haddix's "The Bug Hunter's Methodology." https://www.youtube.com/watch?v=uKWu6yhnhbQ
- API discovery credit: 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





# Thank you!

Connect with Me

linkedin.com/in/PhillipWylie/

twitter.com/PhillipWylie

Phillip.Wylie@CyCognito.com

