Coordinating Defense:

MY TAKE ON EFFECTIVE SECURITY TESTING STRATEGIES

OWASP Sofia Chapter
21.03.2025

c:\>whoami |

- Dimo Stankov
- linkedin.com/in/dimo-stankov
- Level: 25 cyber mage
- CEH, Security+, ITIL4

I am this old

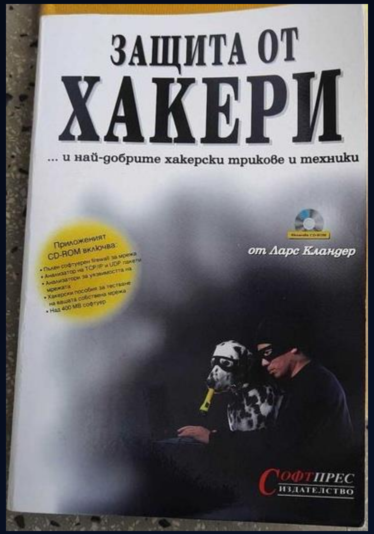


Image: Gemini

Agenda Items

- Security testing flavors
- Vulnerability assessments
- Penetration testing (vulnAss vs penetration)
- Red/Purple team
- Crowd testing
- Coordinating it all

Security testing flavors

- Static/Dynamic Application Security Testing out of scope
  - Methods for finding security vulnerabilities in applications
    - SAST finds vulnerabilities in the code itself
    - DAST finds vulnerabilities in the running application's behavior
- Vulnerability assessments
  - Identify security weaknesses within computer systems, networks, and applications
- Penetration Tests
  - Simulated cyber attack to find vulnerabilities and misconfigurations and test exploitability
- Red/Purple Team
  - Simulates advanced, real-world cyberattacks to test an organization's overall security posture
- Bug Bounty / Responsible Disclosure Program (crowd testing)
  - Work with the cyber-community to receive bug reports

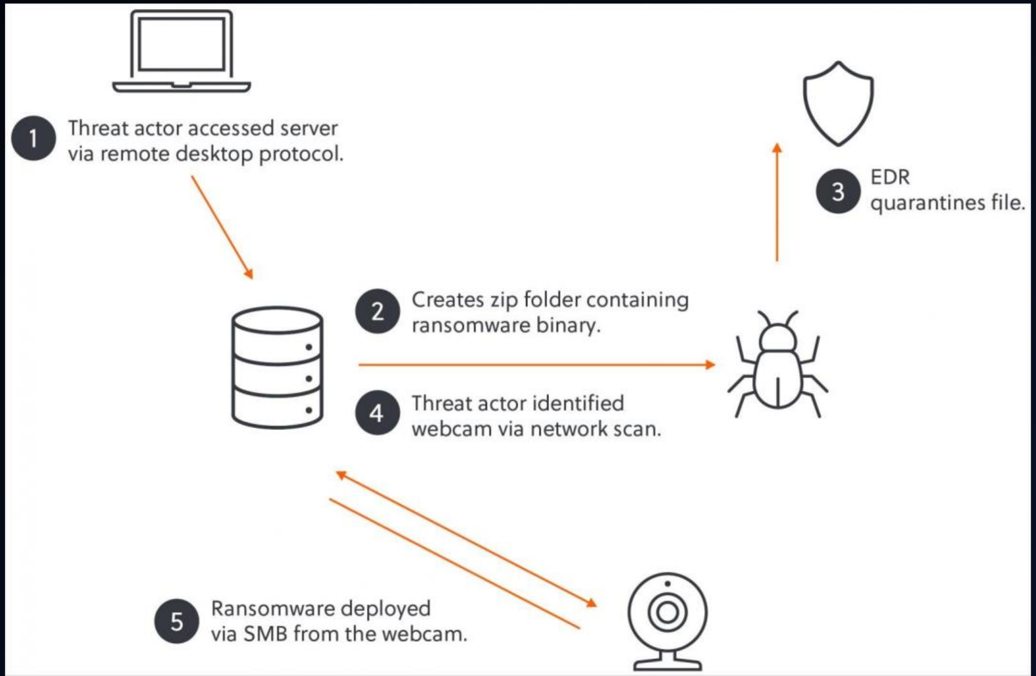
Vulnerability assessments

- Identify known security weaknesses within computer systems, networks, and applications via automated scans
- What CVEs exist for the software versions in use
- Can be Internal/External; Authenticated/Non-Authenticated
- Vulnerability scanning generates a large number of Findings (Vulnerability x Affected assets)
- Reported vulnerabilities may or may not be exploitable in the environment, so they need to be triaged and prioritized
- Regular patch cycles need to be in place
- Track, report, escalate – SLAs
- CMDB needs to be in place, all systems must be scanned

Asset	IP	Application	CVE	CVSSv3	…
DC-001	10.10.10.1	Windows Server 2012 R2	CVE-2017-0144 - EternalBlue	8,8	
WEB-003	172.217.20.78	Apache Log4j2 2.0	CVE-2021-44228 – Log4Shell	10	

…but why should we care if X is updated?

BleepingComputer: S-RM reports - AKIRA Ransomware gang encrypted network from a webcam to bypass EDR



1 Threat actor accessed server via remote desktop protocol.

2 Creates zip folder containing ransomware binary.

3 EDR quarantines file.

4 Threat actor identified webcam via network scan.

5 Ransomware deployed via SMB from the webcam.

bit.ly/4iCTHPf

"S-RM told BleepingComputer that there were patches available for the webcam flaws, meaning that the attack, or at least this vector, was avoidable."

Penetration Testing

- Simulated cyber attack to find and exploit vulnerabilities
- WebApplication, Infrastructure, API, Mobile, Physical
- Try every door and window, push all the buttons
- Pentests are “loud” AF, Speed not Stealth
- Follows a Methodology – OWASP, OSSTMM, PTES, NIST
- Can be Black/Grey/White box testing
  - Assumed breach, User Credentials
- Time boxed vs Scoped
- If outsourcing – NDA, Statement of Work, ROE, Authorization
- Quality Test = Quality Tester + Quality Report
- Report has to be well presented to the stakeholders or all is in vain

Image: Internet, Computer geek 80s

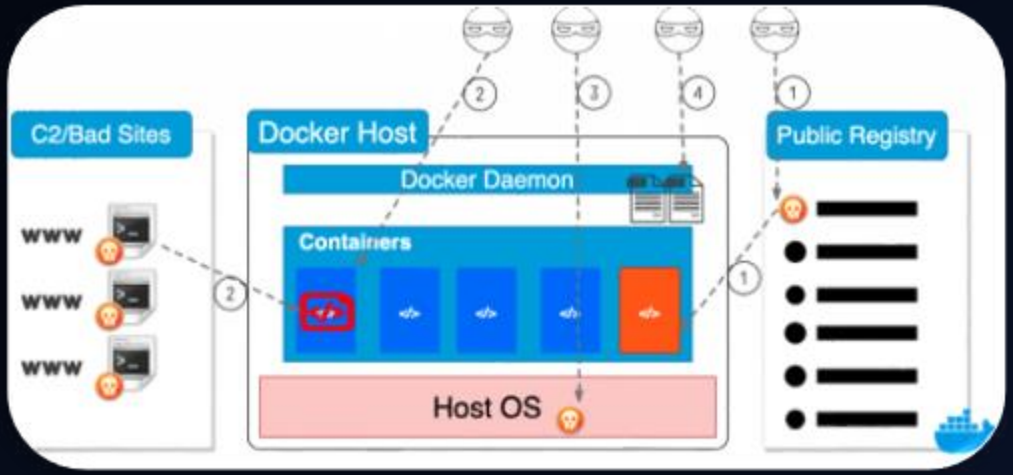
VS

Image: Internet, PTA

..but my vulnscan shows 0 vulns, why PenTest?

- PenTests confirm vulnerability exploitability
- Pentests may uncover misconfigurations
  - ex1: Exposed Docker server

Unit42: Attacker’s Tactics and Techniques in Unsecured Docker Daemons Revealed



bit.ly/4ikEh1S

  - ex2: Internal SMTP server without authentication 💌

…but do I need Physical PenTest?

- Wow can someone get in?
  - ex1. Basic RFID/NFC + Flipper0 = hello cloned card 💳 😈
- Yeah, but HR documents are in a separate room…
  - ex2. I don’t need a key, I have a laminated piece of paper 📄 😈
- You can’t clone our cards!
  - ex3. Covid friendly no-touch buttons VS peace of paper 🌡 😈

Red/Purple Team

- Simulates advanced, real-world cyberattacks to test an organization's overall security posture (MITRE ATT&CK®)
- They are after a main goal – The Crown Jewels 👑
- Shortest path with least resistance
- Custom payloads and tools, Stealth not Speed
- Testing Defenses and Blue team reactions
- Purple – Blue team knows and is involved

…but I did a pentest, why do a read-team?

- Red team engagement
  - very few people informed
  - sophisticated C2 tools
  - Clean payloads not listed in VirusTotal, able to bypass EDR
  - Generating real live ATP telemetry
  - Going all the way
    - pivoted to misconfigured server (Domain Users group member of Administrators)
    - dumped LSASS, LSA Secrets, KerbeRoasting, AS-REP Roasting (not all was detected)
  - Fine tune SIEM, EDR, XDR, update playbooks

Bug Bounty / Vulnerability Disclosure Policy

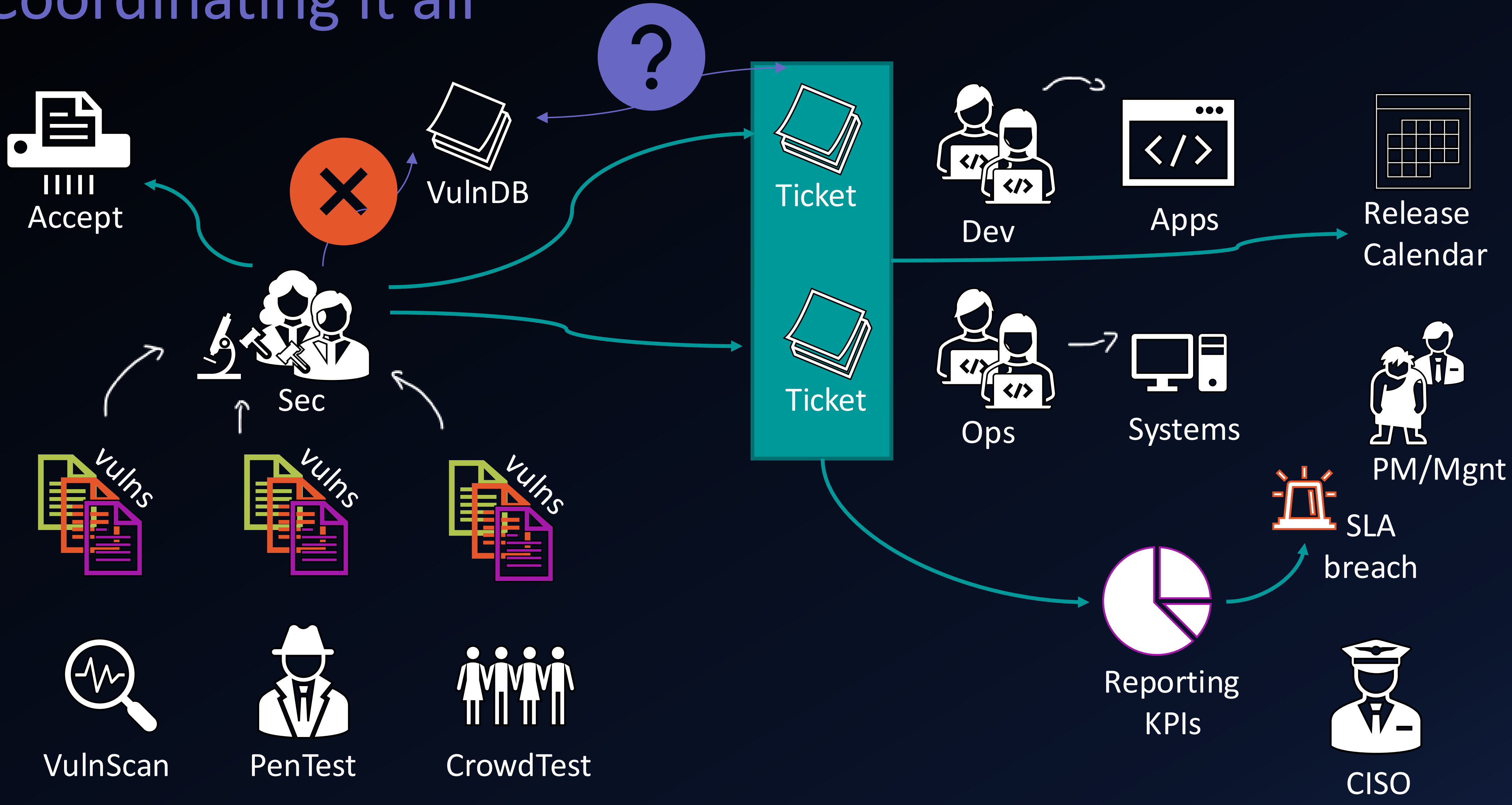
- Responsible Disclosure Program
  - Provide a way for researchers to disclose vulnerabilities responsibly
  - Can be self hosted or via Platform
  - More likely to find zeroDays
- Bug Bounty
  - Report a vulnerability – get ca$h
  - Clear program rules and guidelines
  - Can be self hosted or via Platform
  - More likely to find 0-Days

Coordinating it all

- Security testing as a service (internal)
  - Coordinating Pentest
  - Coordinating Vulnerability triaging
- Responsible Disclosure Program
  - Initial communication with Researchers
- Segregation of duties, avoid conflict of interests
- Proper reporting and escalation

Image: Gemini

Coordinating it all



Conclusion

- Security testing flavors
- VulnAss VS PenTest VS Red Team VS Crowd testing
- Coordinating Defense: My take

Q&A

THANKS AND HACK THE PLANET