Day in the Life of a Cybersecurity Professional

Casaba | Slater Weinstock

About Me

- Graduated from WSU
  - Bachelor of Science in Chemistry (2015)
  - Bachelor of Science in Computer Science (2019)
- Areas
  - Mobile application security (iOS)
  - Desktop application security (macOS)
  - Web application security
  - AWS Infrastructure
  - Cryptography
  - Programming Languages: C, C++, Objective-C, Swift, Go, JavaScript

About Casaba

- Made in Seattle in 2002
- We have offices in Singapore, Malaysia, and Shanghai and are currently opening an office in the UK
- We have nearly 20 years of experience
- We are the lead security auditors for Microsoft Azure, Teams, Azure IoT, Facebook Messenger, and WhatsApp Business
- Work in a large variety of contexts including retail, manufacturing, financial, gaming, engineering, biotech, healthcare, software development, mobile, governments, etc

Some Companies We Work With

- Microsoft
- Meta
- Amazon
- GE Healthcare
- Costco Global
- Hasbro
- Electronic Arts

Why did I choose the cybersecurity space?

- Working with brand new tech each day
- No day is ever the same
- Problem solving and the research component is a large part of the industry
- Having the opportunity to work over a large range of the cybersecurity space

How do I stay up to date?

- r/netsec
- HackerNews
- Twitter
- The Daily Swig
- DarkReading
- Various Podcasts (Security. Cryptography. Whatever.)

What languages do we commonly encounter?

- JavaScript
- TypeScript
- C
- C++
- C#
- Go
- Rust
- Objective-C
- Swift
- Erlang
- PHP
- Assembly

What is a day like?

- This is a tough question
- I could be:
  - In a threat modeling discussion with a client on a new feature
  - Reviewing an implemented mitigation against a previous attack and discussing with a client how it could be more optimized
  - Penetration testing a new product:
    - Reviewing code and the architecture of a new product
    - Reading articles on the core framework a product uses
    - Messing around with a product, exploring use cases, etc
    - Hacking a product, writing exploit code, reverse engineering, fuzzing, etc

How does a pentesting engagement work?

- The length of time varies between a few days up to several months depending on the scope and size
- The codebases we work with are often extremely large (millions LOC)
- The team sizes vary based on the scope of the product and the areas of expertise, my typical team size is 2-3 people
- Starting an engagement:
  - Spend time reading documentation about the feature/product including internal documentation
  - There are times a client is worried about a specific attack vector (maybe a newly published attack against a similar product) so I will learn about that attack
  - Messing around with the product, getting a sense of how a customer or an attacker would use it. Here I am mainly looking for certain behavior which would make me believe an attack vector is present
  - Profile the codebase for hot spots using software component analysis tools (e.g., Snyk) and static analysis tools (e.g., Semmle, PVS-Studio)

What are some of the tools I use?

- Burp Suite, Proxyman – Intercepting proxies
- Ripgrep/Sift – Code searching tool
- Nmap – Network port scanning
- Xcode/Android Studio/Visual Studio – IDEs
- Semgrep – General purpose static analysis code tool
- Tcpdump/Wireshark – TCP/IP packet sniffer
- Snyk – Software component analysis tool
- Trufflehog – scanner for secrets in source code and git history
- AFL – a genetic algorithm based fuzzing tool

What skills do I need?

- Curious and research-oriented
- The “evil bit”
- Thriving in ambiguity
- Critical thinking/breaking down large projects
- Software development background
- Technical writing
- Public speaking

Do certifications matter?

- Yes, no, maybe?
  - Certifications are a great way to prove some technical knowledge. They can also get you through some HR barriers when interviewing at companies
  - Certifications are not a substitute for experience
  - What really matters is can you learn and do the work
- What are some good certifications to get?
  - CompTIA Security+, Network+
  - OSCP
  - Certificated Ethical Hacker

Interview Questions

- I take a broad approach when interviewing people, asking about a range of topics tailored to their resume
- Some questions will be definitions, such as define public-key cryptography
- Some questions will be about new attacks in the wild, such as describe to me what dependency confusion is. Can you think of when this attack was used or demonstrated?
- Some questions will be conversational, such as test plan creation around a given app on a given platform or designing a secure method

Cybersecurity Market Outlook

- There is an estimated 33% growth for infosec professionals between 2020-2030 (https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6)
- Tech is always changing, new features are being added, more services are being moved to the cloud, more open-source software is being developed and released, the rise of remote work, and these all lead to more attack vectors
- Security is iterative, there isn't a "one and done" approach. You always need to be reviewing features, even ones that have been previously reviewed to make sure a new attack vector is not present
- Cybercrime costs organizations a huge amount of money. It's estimated that cybercrime could cost the world over 10 trillion USD annually by 2025 (https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/)

Thank You

Slater Weinstock

slater@casaba.com