Computer Network Security

COMP 178 | Spring 2025 | University of the Pacific | Jeff Shafer

Closing Thoughts

Skills Power Up?

Penetration Testing – Next Steps

- **More Exploits**
- What *specifically* do you want to target?
  - Specialize in exploits for that!

Penetration Testing – Next Steps

- Target More Platforms?
  - Windows? Mac?
  - Mobile Devices? (Android? iOS?)
  - IOT devices?
  - ICS devices?
- Target Wireless Networks?
- Target Web Apps?
  - SQL injection
  - Cross-Site Scripting
- Target The Cloud?
  - Microservices
  - In-memory data stores
  - Kubernetes applications
  - Specifics for AWS
  - Specifics for Azure

Penetration Testing – Next Steps

- **More Exploits**
- Increasing Skills → Increasing Capabilities
  - Level 1: Fully functional exploits in Metasploit
  - Level 2: Proof of concept code at exploit-db.com, github, random links from Twitter, etc…
  - Level 3: Reverse engineer security patches to discover vulnerabilities (and write exploits)
  - Level 4: **Discover your *own* vulnerabilities and write exploits**

iOS Zero-Click Radio Proximity Exploit

https://www.youtube.com/watch?v=_sTw7GGoJ6g

iOS Zero-Click Radio Proximity Exploit

- Discovered by Ian Beer (Research, Google *Project Zero* group)
  - Had a lot of free time during COVID lockdown! ☺
- Buffer overflow bug in AWDL (Apple mesh networking protocol used for AirDrop over WiFi, etc..)
- **Extremely detailed (30k word)** description of how Ian went from nothing to a full proof of concept exploit
  - https://googleprojectzero.blogspot.com/2020/12/an-ios-zero-click-radio-proximity.html

Thomas Dullien – Love/Hate Offensive Work

https://www.youtube.com/watch?v=8QRnOpjmneo

- *"Why I Love Offensive Work, Why I Don't Love Offensive Work"*, Thomas Dullien (aka "Halvar Flake"), Keynote Talk @ OffensiveCon20
  - Security researcher with 20+ year background in offensive and defense techniques
  - Winner of *Pwnie Award*, 2015
  - Researcher at Google *Project Zero* (2016-2019)
  - https://thomasdullien.github.io/about/

Thomas Dullien – Love/Hate Offensive Work

Reasons to ♥ offensive work

Technical reasons:

1. Full-stack CS, across abstraction layers
2. Creativity
3. Scientific frontiers
4. Practical real-world effects

Economic reasons:

5. Incentive alignment
6. Mission-critical for customers
7. Not the customers money

Emotional reasons:

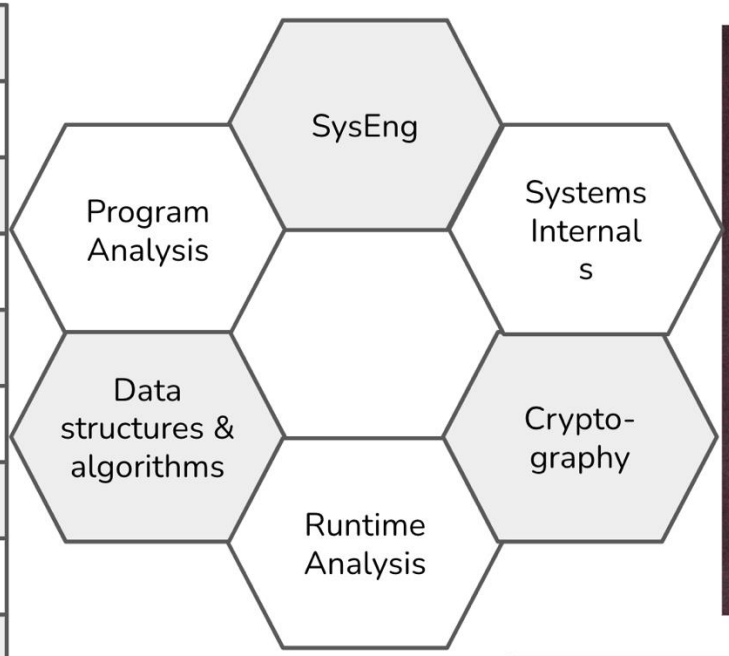
8. The “high” after success
9. Close to real-world magic
10. Interesting people

https://www.youtube.com/watch?v=8QRnOpjmneo

Thomas Dullien – Love/Hate Offensive Work

Technical ♥ 1: Full stack CS

- Interaction Software → World
- Higher Level Logic
- Software implementation
- Libraries
- Runtimes
- Operating System
- Firmware
- Hardware Spec
- Hardware Implementation



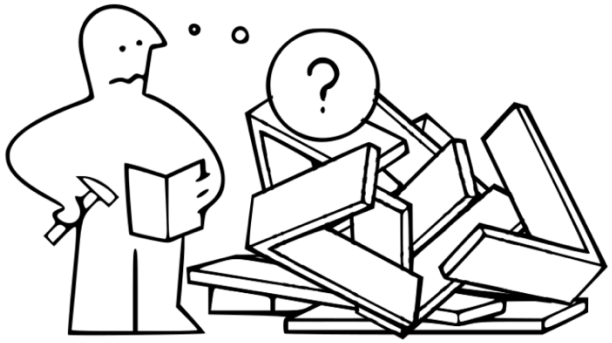
Spelunking in code caves & ruins

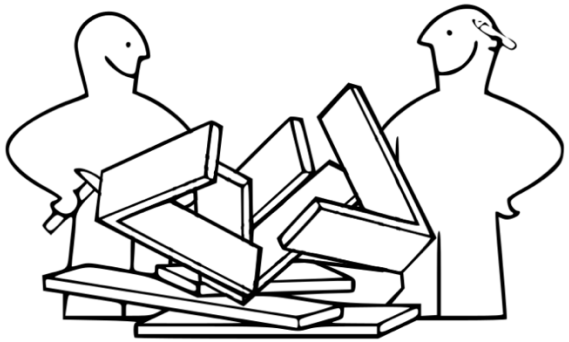
https://www.youtube.com/watch?v=8QRnOpjmneo

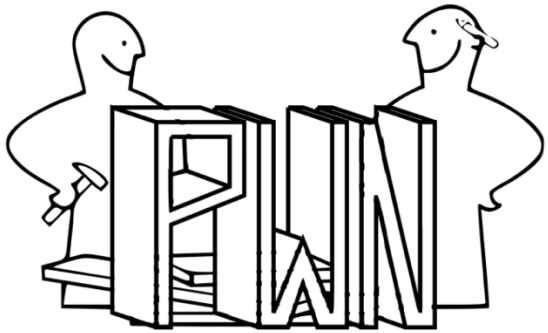
Thomas Dullien – Love/Hate Offensive Work

Technical ♥ 2: Creativity

- Analogy: Writing an exploit is like getting a random assortment of IKEA parts…
- … with the task of building a useful, sturdy, and comfortable chair out of it.







https://www.youtube.com/watch?v=8QRnOpjmneo

Thomas Dullien – Love/Hate Offensive Work

Technical  4: Practical effects

- Work on offensive technology is not theoretical.
- Contrary to work in (public) Cryptography, you can actually see the results: A root shell speaks to me differently than lowering the complexity of an attack from 2^128 to 2^110.
- Deeply satisfying to see the technology work.
- **Offensive tools are an outlier in the security (product) industry: They reliably do what they advertise they do.**

https://www.youtube.com/watch?v=8QRnOpjmneo

Thomas Dullien – Love/Hate Offensive Work

Reasons to  offensive work

Societal reasons:

1. "For whom" - you always pick a side
2. Non-optimal choices for employers
3. Limited societal value-add

Emotional reasons:

4. Every. Single. Moral. Question. Is. Complicated.
5. Economic incentives cloud judgement of one's actions.
6. Non-accumulative.

Technical reasons:

7. Repetitive when maximizing profit
8. Become the world's leading expert on obsolete technologies
9. Missing a huge technical transformation
10. The obituary test

https://www.youtube.com/watch?v=8QRnOpjmneo

Thomas Dullien – Love/Hate Offensive Work

Societal 1: "For whom?" - you pick a side

- Bob Morris Sr. asked me when I met what I do. "I study math." - "For whom?"
- All of security is fundamentally about **human power & conflict**. You always pick a side.
- Interestingly, both **defensive and offensive security tends to be on the side of the already-powerful.** I am running out of sides I like to pick.

https://www.youtube.com/watch?v=8QRnOpjmneo

Thomas Dullien – Love/Hate Offensive Work

Emotional  6: Non-accumulative

- **Offensive security** is much less accumulative than many other parts of engineering.
- Working on tooling means 10 years down the line your tools are better.
- Looking back at a long offensive career is often: “I found this OpenSSH remote …. and it is gone. I found this RDP remote … and it is gone. I developed this technique for exploiting 2006 kxmalloc, and it was replaced.”
- Even by tech standards, offensive work is particularly ephemeral.

https://www.youtube.com/watch?v=8QRnOpjmneo

Thomas Dullien – Love/Hate Offensive Work

Technical  8: Experts on obsolete tech

- **Obsolete technologies are where the bugs are.** There are more people that have deeply analyzed TrueType Font rendering virtual machines for vuln-dev than for typography.

- By definition, customers want to target “mass-market” tech. This is often much older than “emerging” tech.

- Eventually, obsolete tech ceases to be useful even for offensive purposes. At this point, you are stuck with an encyclopedic knowledge of how TrueType font rendering bugs evolved from 1995 to now.

https://www.youtube.com/watch?v=8QRnOpjmneo

Thomas Dullien – Love/Hate Offensive Work

Technical  9: Missing a huge tech transform

- **Computing is changing** more rapidly right now than in recent decades.
- **Datacenter-sized computing** is emerging, with emergent proto-OS's and nobody with any clue how to properly architect them. No full OS exists. No real debugging exists.
- **End-of-Moore** will reshape software deeply, and is already reshaping hardware deeply.
- **A lot of offensive work:** Another bug in Chrome plz kthxbai. Or perhaps "another Safari bug + iOS privesc plz kthxbai". Feels unimportant / unexciting.

https://www.youtube.com/watch?v=8QRnOpjmneo

Penetration Testing – Next Steps

- **Post-Exploit**
- What *specifically* do you want to target?
  - Specialize in understanding *how to use that system* after you gain access
  - *Once you have a shell, what do you do THEN?*
- Windows? Mac? Android? iOS? IOT? ICS?
  - *We barely talked about Windows - **PowerShell Kung-Fu?***

Fun Things

HACKTHEBOX

https://www.hackthebox.com/

- Virtual hacking labs at a variety of skill levels
  - 150+ machines!
  - 100+ challenges!
  - New labs introduced every week
- Capture The Flag (CTF) and Battleground challenges
- Free to get started
  - ($14/month for VIP access)

Fun Things

- Bash and PowerShell skills
- Windows and Linux memory forensics
- Web application challenges
- A "smart home" mobile application
- Insecure connected cameras
- Layer 2/DHCP attacks
- Injection attacks
- …

https://www.sans.org/cyber-ranges/

Fun Things

https://holidayhackchallenge.com/