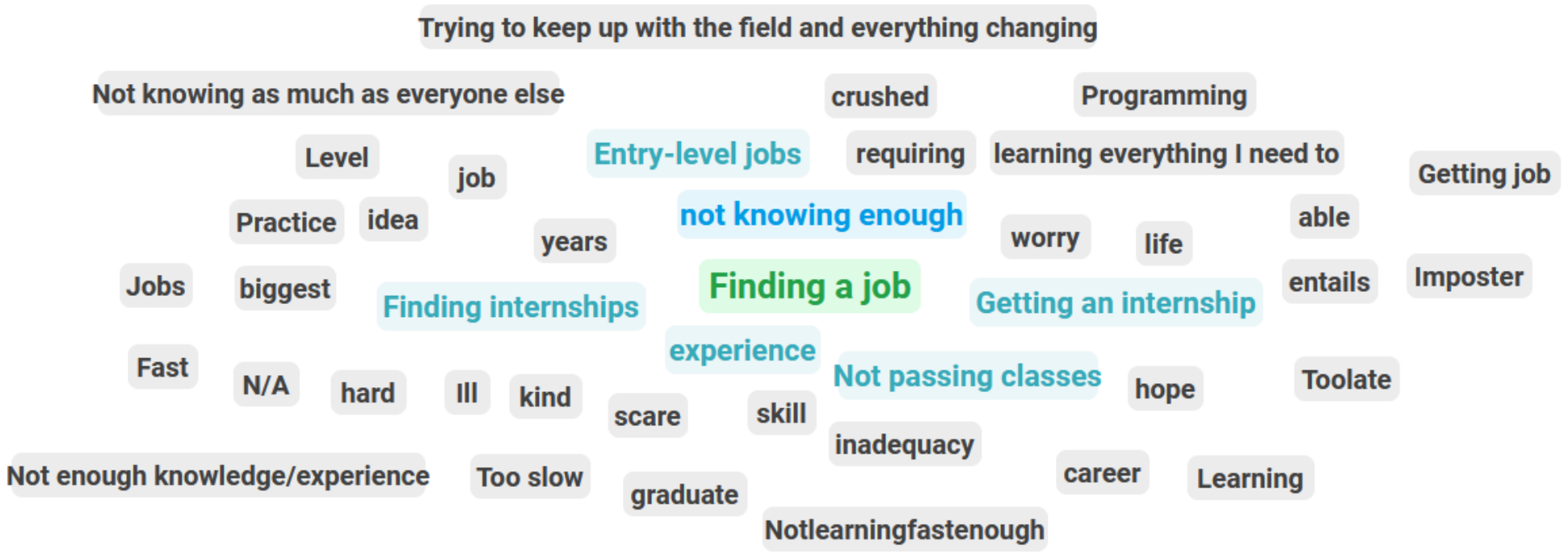
CREATE. DON'T CONSUME. & A WILD HACKING CASE STUDY

BYU IT&C 291R IAN COOK FEBRUARY 6TH, 2025

PARTICIPATE:

What is your biggest worry as a cybersecurity Student at BYU?

Review answers



TODAY

1. whoami
2. Life of a Researcher
3. BYU Advice & Career Advice
4. Cyber Case Study

Ask Questions at any time, email me questions afterward: cyber@ohcoz.com

1. WHOAMI

Senior Associate Research Scientist @ Peraton Labs in DC

(June 2023-Present)

BYU Cybersecurity Grad (2017-2023), former CSA president

Volunteer - World Team Lead at Collegiate Pentesting Competition

(Two seasons now)

The following presentation represents my personal views only.

RESEARCH VS DEVELOPMENT

1. Individually diving deep into technologies & topics
2. Day to day looks like:
    a. Technical Reading (RFCs, current academic landscape)
    b. Small proof of concepts at later stages
    c. Self-Driven learning and discovery, filling in gaps
3. Big Picture Task: Leverage expertise and analysis into a larger system to solve problems.

1. Working cross-team collaboratively, in Agile/SAFE SWE environment, Customer Input Driven
2. Day to day looks like:
    a. Feature Development
    b. Release Testing
    c. Development Cycle planning
    d. Rapid Proto-type to Production level
3. Big Picture: Delivering a resilient technical system

CAREER ADVICE

from someone just a little bit further down the road from y'all:

- Interview Tips.
- Create vs Consume
- BYU- Specific Advice
- General Career Advice
- Reach Out!

MY ONE SLIDE ON INTERVIEWS (NOT EXHAUSTIVE)

If it is a Cyber analyst or non-dev/engineering role:

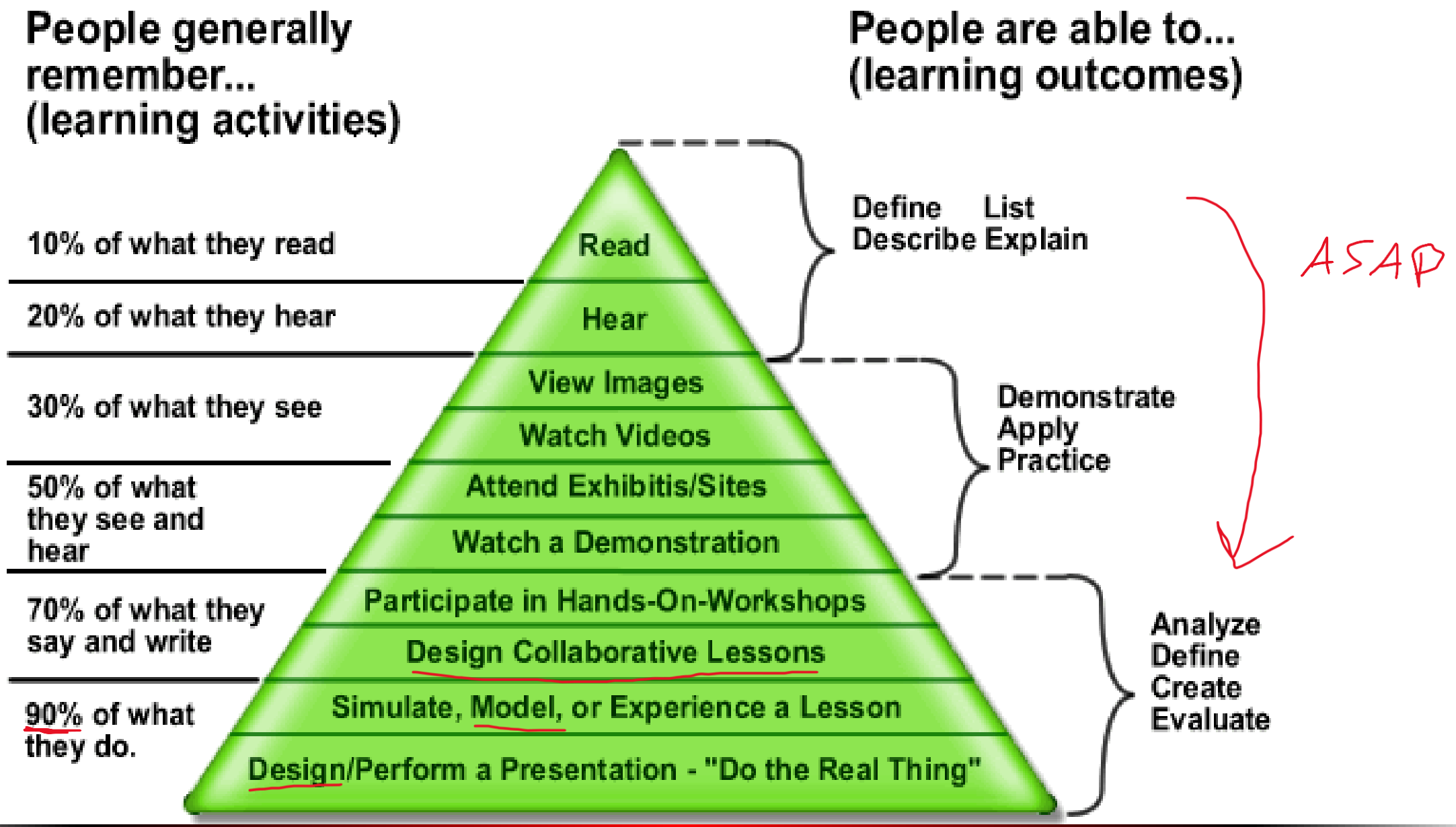
- Know exactly what happens when you open a browser and type in google.com. Know Buffer Overflow Attacks
- Know Asymmetric/Symmetric Encryption

If it is a Cyber Engineer/ Software Dev:

- Know your Data Structures (CS 235 wildly important actually)
- Know easy-medium Leetcode in Python (as a minimum)
- Build proficiency in a low-level language, and a scripting language

Other tips:

- Have 3-4 types of resumes depending on type of roles you are aiming for.
- A good Resume gets the interview, then it's all on your ability to communicate technical and nontechnical to survive and advance
- Take notes before and after every interview
- ASK QUESTIONS:
  - Personal favorite: What type of problems do you typically spend time on the most in this role? Is it design, troubleshooting, optimizing, time-management, politics etc.
- In the eyes of recruiters:
  Work Experience > Side Projects > Certifications > Degree.


People generally remember... (learning activities)
People are able to... (learning outcomes)
10% of what they read
20% of what they hear
30% of what they see
50% of what they see and hear
70% of what they say and write
90% of what they do.
Read
Hear
View Images
Watch Videos
Attend Exhibitis/Sites
Watch a Demonstration
Participate in Hands-On-Workshops
Design Collaborative Lessons
Simulate, Model, or Experience a Lesson
Design/Perform a Presentation - "Do the Real Thing"
Define List
Describe Explain
Demonstrate
Apply
Practice
Analyze
Define
Create
Evaluate
ASAP

Lessons I learned from BYU

1. Invest in each other's success.
2. Break out of silos (yes be friends with the CS students. They will most likely be your coworkers at some point)
3. Fail! College is a ball pit. Learn to flip there, before you must flip in the real world on concrete.
4. Get more out of class. Looking back, the only reason I didn't learn more was solely because I didn't try harder.
5. Find ways to build up the program as you go through it. This is your home for 4 years. Leave a mark.
6. Representing BYU is special. Do it exceptionally well.
7. Get work experience as soon as possible.
8. Pursue opportunities such as Scholarship For Service
9. Raise your standards. This is an insanely difficult field. The harder you work now, the higher your compounding trajectory will be.

General Lessons:

1. Figure out your optimal system of note-taking
2. If you work with other people, build relationships. Relationships can't help you if they don't exist.
3. Time spent problem solving is time spent learning at an exponential rate.
4. It's a marathon, not a sprint. You will go through cycles of loving and not loving your job. Work can be work.
5. First job out of college will not be your dream job- just means you have plenty of room to grow.
6. Before seriously job searching, rank the following in order of importance. As you job search, compare it to your list

NON-EXHAUSTIVE LIST OF JOB QUALITIES TO COMPARE & RANK

1. Day to day tasks are interesting
2. Pays well
3. Opportunities to interact with other teams
4. Opportunities to interact with customers or people outside company
5. Structured Advancement milestones
6. Challenging Technical Problems
7. Matches your Technical Talents
8. How does that industry view your team? (Cost Center or Revenue Center)
9. Opportunities to attain further education and training
10. PTO and Benefits are at or above industry standard
11. Work with people you have existing relationships with
12. Opportunities to lead
13. Work Life Balance. Expectation of 40 hours vs More.
14. Self Tasking Culture or Structured Playbook Culture
15. Fully-Remote vs Hybrid vs In Person- HIGHLY RECOMMEND IN PERSON to start
16. And more.

NETWORK

Networking is hard. But it truly is the "sudo" of career progression.

Some tips:

- Do your research
- Genuine Curiosity goes far- ask insightful questions.
- Don't go straight for the Big Ask

Just like learning- Can't cram.

- Spaced repetition. (online is amazing for this)
- Don't just consume relationships. Give value!

KEY POINTS

- Create, not just Consume
- BYU & College presents an abundance of doors. Open as many as you can!
- Seek the highest quality of Learning
- Resist the Path of Least Resistance

CYBER CASE STUDY:

Scenario:
Adversary has valid credentials to a target company but can't authenticate to any public service because of MFA. (i.e. gets to a valid duo prompt, but can't progress)

How did they breach Company XYZ?

CYBER CASE STUDY:

Scenario: Valid Creds but blocked by MFA

Q1: How did they breach Company XYZ?

- A: Social Engineer Helpdesk w/ use of valid creds
- B: Spam MFA prompts until user accepts
- C: Something wild

CYBER CASE STUDY:

Scenario: Valid Creds but blocked by MFA

- A: ~~Social Engineer Helpdesk w/ use of valid creds~~
- B: ~~Spam MFA prompts until user accepts~~ (Uber hack from 2022 by Lapsus$)
- C: Something wild

CYBER CASE STUDY:

Scenario: Valid Creds but blocked by MFA

Something wild:

Authenticating to the enterprise onsite WIFI requires no MFA.

Problem?

APT is halfway around the world. So now what?

CYBER CASE STUDY:

Enter Company B.

Company A's next-door neighbor.

Now Company B's security was less mature.

Company B gets breached.

Problem?

How do you get from Company B's infrastructure to Company A?

CYBER CASE STUDY:

Q: How do you get from Company B's infrastructure to Company A?

- A. Bluetooth Attack through thin walls
- B. Insecure Guest Wifi
- C. Something Wild

CYBER CASE STUDY:

Q: How do you get from Company B's infrastructure to Company A?

- A. ~~Bluetooth Attack through thin walls~~
- B. ~~Insecure Guest Wifi~~ (They used this on the 3rd time actually)
- C. Something Wild

CYBER CASE STUDY:

Q: How do you get from Company B's infrastructure to Company A?

Something Wild:

Breached Company B.

Scanned all hosts, found one that was dual-homed (open connections to both ethernet and wireless)

Connected to Company A's Enterprise Network with Compromised Credentials.

Also compromised Company B's VPN once Network Access was established, thus maintaining persistence.

CYBER CASE STUDY:

Moral of the story:

Security is really hard.

But we know what happened.

Which means defenses are getting better.

CYBER CASE STUDY:

For all the fun technical details:

https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/