Hackers Hiring Hackers: How to Do Things Better

Tottenkoph
IrishMASMS

Disclaimer

This presentation is intended for the attendees and may contain information that is privileged or unsuitable for overly sensitive persons with low self-esteem, no sense of humour, or irrational religious/political beliefs. Those of you with an overwhelming fear of the unknown will be gratified to learn that there is no intended hidden message revealed by reading this warning backwards, so just ignore that alert notice from Microsoft. However, by pouring a complete circle of salt around yourself and your computer, you can ensure that no harm will befall you or your pets. Your mileage & satisfaction may vary, not all warranties apply during all time frames. Confirm these statements with your management before approval & implementation.
No individuals or equipment were harmed while producing this presentation, but it was created with recycled electrons. No animals were harmed in the transmission of this document, although if the raccoons keep getting into the trash I may have to do something about it. No individual, organization, or entity can be held liable or be quoted without written consent of the presenters.

I speak for no one, no one speaks for me.

Who & What are we?

Who & What are you?

- Human
- Potentially a hiring manager
- Hacker with little to no work experience in the field
- Hacker with experience looking for their next opportunity

Why are we talking about this at DEFCON?

- Lots of talks about how to be a better pen tester and how to use all of the cool new tools, but only a few talks that address what some of us consider to be the hardest part of getting a job in InfoSec: the hiring process.
- We desperately need people with the technical skills hackers have
- Both sides of the table are doing horribly when it comes to hiring and interviewing for work.

Why are we talking about this at DEFCON?

This talk takes our experiences (and that of others in the community) as both interviewers and interviewees in order to help better prepare hackers to enter (or move within) “the industry”. We also want to let the people making hiring decisions know what they can do to get the people and experience they need.

Why are we talking about this at DEFCON?

- “It is hard to find people to hire”
- We scare and confuse some HR and recruiters
- We (hackers and hiring managers alike) keep shooting ourselves in this process
- Getting and retaining talent is in some ways a social engineering exercise

Social Engineering Exercise
(Hiring Manager's Perspective)

- Get individuals interested in applying
- Avoid bottlenecks at HR
- Finding an appropriate offer that upper management approves of
- The acceptance of the offer by the candidate
- Having the candidate show up on day one and onboarded
- Nurturing the candidate so they grow personally and professionally

Social Engineering Exercise
(Job Hunter's Perspective)

- Writing a convincing resume/cover letter to get past the HR gateway
- The interviewing process (hiring managers and beyond)
- Get (or negotiate) a suitable offer
- Show up on day one & onboarding

Core Problem aka Opportunity #1

EXPECTATIONS

Expectations

"Can't find anyone to hire!"

vs

"Must work in our corporate office in Wichita, initially on a six month contract to fire with rotating SOC shift cycle!"

Hiring the UnHireable

Winn Schwartau talks about “Hiring the UnHireable”

“... intentionally or not—is create a sub-category of talent whom we will never hire. The Unhireable. ...”

http://techspective.net/2015/07/06/hiring-the-unhireable-its-time-we-get-over-ourselves/

What do you want?

- Expectations for jobs can be unclear
  - The job title may say a “Junior” or “Entry-level”, but then it asks for CISSP certification or 5 years of experience
- Position Description (PD) could be all over the map, looking for jack of all trades (master of none)
- Folks looking to break into InfoSec end up either applying for everything or nothing
  - They honestly have no idea what hiring managers are looking for, but they want to try regardless.

Tell us what you want

What you really, really want?

- Be clear with what the job will entail
- If you want a log monkey, say you want a log monkey

What do you want?

- What really matters?
  - To your environment, your team, the biz?
- Experience?
  - Entry-level or someone more senior
- Certs and/or a degree?
- Do not ask for things “just because”
  - Limits your pool of applicants
- What level of experience can you afford?

Certifications? Degree?

- What really matters?
- What certifications can you afford?
- Discrimination?

Scope?

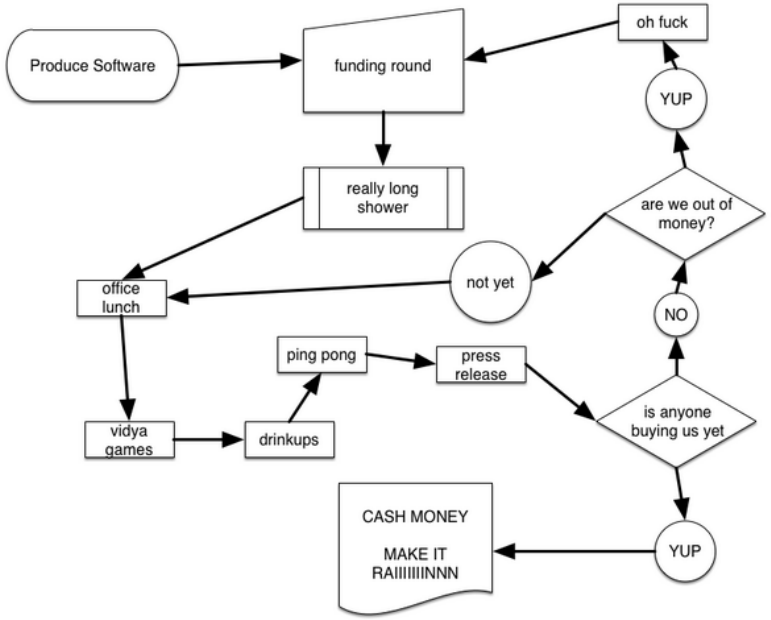
- Dedicated role
  - Analyst (Digging through the data)
  - Engineer (Running the toolsets)
  - Architect (Strategic view)
  - Forensics
  - Malware
  - Penetration tester
- Application vs Network/System Security
  - Vendor, developer of software/hardware

ALL THE THINGS!

- ‘Jack of all trades’?
  - Master of none
  - Consider career growth
  - Health and welfare of team
  - Burnout

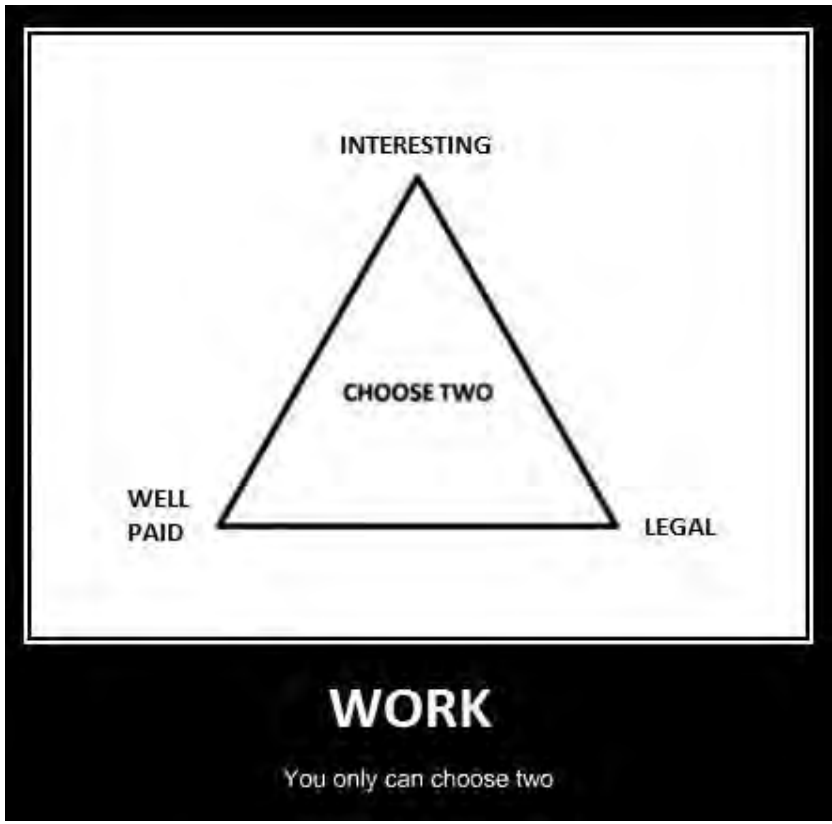
Where do they fit?

- Organizational fit
- Direct report
  - Reporting to IT? Legal?
    - Consider potential conflicts of interest
  - Startups: a Security Architect is not a replacement for a CISO



Hacker Expectations

- Apply, and the job is yours!
  - For as much money as you want!
  - With no bureaucracy to deal with!
  - All the tools you want - or the freedom to create your own!
  - With a free pass to hacker summer camp!



Core Problem aka Opportunity #2

THE APPLICATION PROCESS

The Application Process

- Preparation by both parties should be done before the first calls are made to set up an interview
  - Seldom done, let alone done well
- Timing is everything
  - Candidate could have finished the application process, hired, and started elsewhere before you send your first reply

How Do you Find Candidates?

- Involvement in
  - Local IT & InfoSec communities/Meetups
  - Mailing lists & forums
  - Local tech/college professional meetings
- Posting online
  - Monster, CareerBuilder, Beyond, etc.
  - Craigslist
  - Reddit
  - Closed IT/InfoSec communities & lists

How Do you Find Candidates?

- One of your obligations as a hiring manager, as a leader in InfoSec is to nurture talent in our field
- Your involvement in the local groups helps promote & screen


HELLO
IS IT LEADS
YOU'RE LOOKING FOR?

HR/recruiter teams

- Paid recruiters, overseas body shops
- Recruiter roadblocks
  - Sends the screening questionnaire, expecting the applicant to do their work
    - Starts off with a poor experience
    - Candidates will go elsewhere
- Your HR/recruiting staff and their initial contacts and conversations with candidates set the tone for the process, ensure they are good ones
  - Sets up expectations for the next step(s)

Consider the types of questions

- Carefully consider the types of questions you want to ask BEFORE the interview
- Respect the sensitivities of the applications in your questions
- Creating the interviews
  - Balancing fact based questions vs essay/short
  - Does your team share questions?
  - How do you divvy up who asks what
    - Do you avoid duplication?

Defining Key Areas

- How do you define key areas/topics?
- Testing/evaluating for specific skills? Or more General?
- How do you match up skills to the Position description, then the areas to question per candidate?

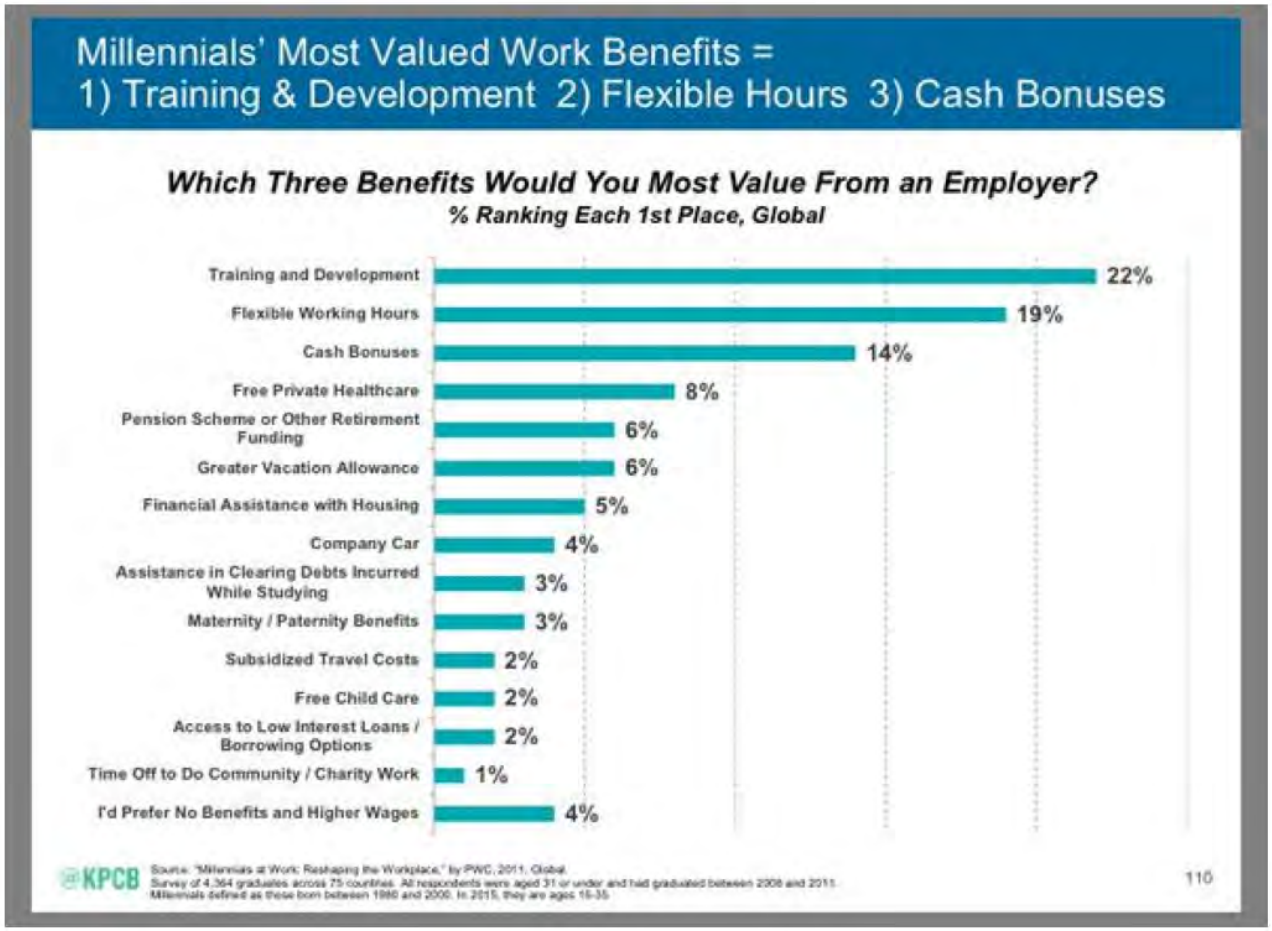
Questioning Compensation

- Salary history
  - You know the range, pay them what they are worth
  - Incentives
    - Flexible work schedule
    - Work from home
    - Training budget

Startup L. Jackson
@StartupLJackson

Follow

Your employees want professional development. A fun workplace, stock options, and free lunch won't cut it.



Rebecca Slatkin
@RebeccaSlatkin

Follow

What recruiters think I want: Beer cart, ping pong table
What I really want: Silence, coworkers with good table manners, attention to UX

Application Tracking Systems (ATS)

- Ensure the ATS you use doesn't require PII/NPPI
  - SSANs in BrassRing
- Test and validate your application process
  - Get a friend to apply, do they make it through the process? Past HR at least?
- Avoid the common application fails
  - The initial impressions last

[Insert ATS fail screenshot examples here]
[Redacted to protect the guilty]

Tyler Schmall
@tylerschmall

Follow

Got about 2/3 of the way through a job application and came across this question and x'd out of it.

Which meme do you most identify with and why? *


THE FAILBOAT
HAS ARRIVED

Hack your resume

- Experience reflects your background and the role
  - No BS, No stretching the truth
  - Careful on the buzzword bingo
    - Enough to match the role in the big HR
    - Know what the terms mean


The Official
BULLSHIT
FLAG™
www.BSFlag.com

Hack your Resume

- Tailor your resume to make it relevant to the employer/hiring manager
- Have your resume/CV as long as it needs to be.
  - Is your resume long enough so it reaches where it's supposed to go?
- 1 or 2 page resume, and a full CV
  - Different hiring managers, different preferences

Hack your Resume

- File names make a difference
  - Distinguish yourself from other candidates
  - Managers make mistakes, and lose documents; good labeling helps you out.
- Sanitize the metadata
  - The downloaded template has a surprise...

Application Tracking Systems

- There are different Application Tracking Systems (ATS)
  - Heavyweight application systems with data mining looking for keywords & the basic application management
    - Taleo, iCIMS, SuccessFactors, PeopleSoft, Bullhorn, Brassring
  - Lightweight application tracking
    - Workday, Jobvite, SilkRoad, LinkedIn, SmartRecruiters

Heavyweight ATS

- Be one of the first to apply
- Fill out every applicable text box
- Resume/CV formatting for computer readable
  - No graphics or special characters
  - Web safe fonts
  - Spell check
  - Skills section as complete and truthful as possible

Email Applications

- Quick and easy to apply, easy to get lost
- Subject line is important
- Include a cover letter in the body of the email
- Digital signature is a bonus

USAJobs Applications

- Government roles have dedicated websites for applications
  - For USA, USAJobs
    - Mostly, some .GOV still have their own
- Similar to the heavyweight ATS
  - Unwieldy
  - Be sure to answer the qualifier questions
  - Review the application process for the surprise essay questions

Customised Resumes

- The full CV with buzzword bingo for the heavyweight application systems
  - Import, then tweak details
- The 1 or 2 page resume for human digestion
  - Include with application as well

Don’t Hack With Your Resume

- Submit resumes as text, RTF, and/or PDF
- Do not insert malicious code or trackers into your resume or cover letter
  - Nor should you conduct a penetration test on the application systems

Security Clearances

- Do not belong on the resume
- Do not belong on your social media profiles
- This information makes you a bigger target
  - And look like a moron
- DSS/OPM does not look kindly on this
  - Read the NDA you signed
  - Does not matter that the APT$ stole it all
- The proper answer: “That information can be verified with a conversation with your Personal Security Officer.”

Time to Communicate (Hackers)

- Use a professional looking email address
  - Don’t send it from l33tH4x0rz666@caturday.net
  - Caution on Google data mining
  - Best keep personal & work email separate
    - GTFG email address

Time to Communicate (Hackers)

- Cover letter
  - Why do you want the role?
  - What role are you applying for?
  - No letter indicates you are not interested, or just spamming applications
  - Just five (5) minutes on why this role sounds interesting makes a difference

Use Your Network

- Reach out to your network regarding specific companies and roles
  - Social media
    - Even a short note to the recruiter has gotten the screening interview

How To Meet Hiring Managers

- Involvement in
  - Local IT & InfoSec communities/Meetups
  - Mailing lists & forums
  - Conferences
- Online communities
  - Reddit
  - Closed/vetted InfoSec and DFIR lists, SANS


RECRUITER ADDED ME ON LINKEDIN
SO I GUESS YOU COULD SAY THINGS ARE GETTING PRETTY SERIOUS
makeameme.org

Working With Recruiters

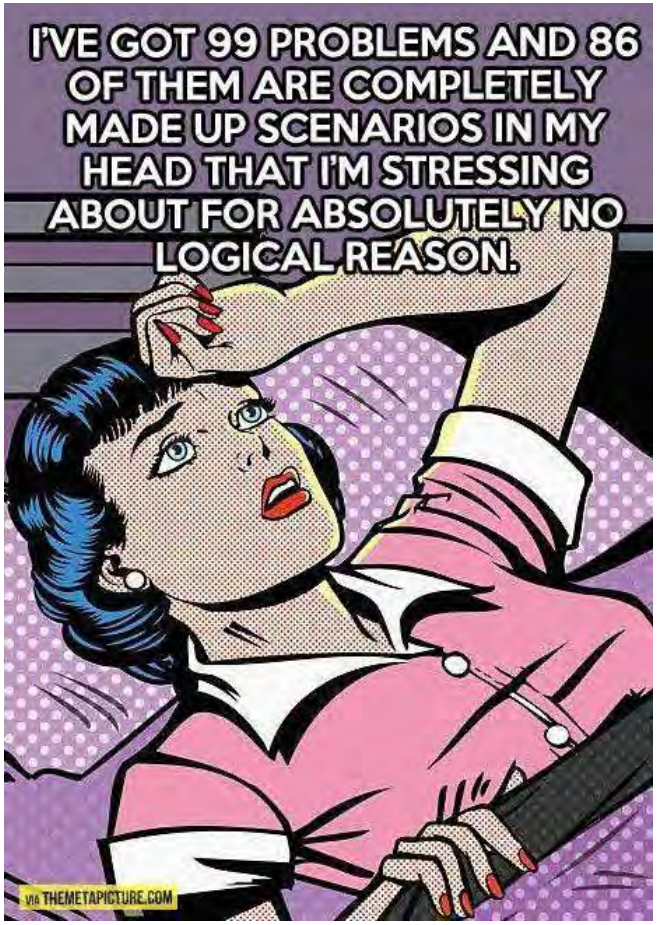
- There are different types of recruiters
  - Technical recruiters
    - Company
    - Agencies (boutique and otherwise)
  - Agencies just looking for a body to fill a seat
    - Spamming of the PDs
    - Unable to answer follow-up questions
- Do your research on recruiters like you would potential companies to work for
  - Build relationships with good ones

Understand the odds

- You could be one of tens or a hundred candidates
  - Connect with those involved before the search
  - Try to not get discouraged
  - Diversify your applications
  - Location
    - Depth of the labor pool
    - Who else applied for the role

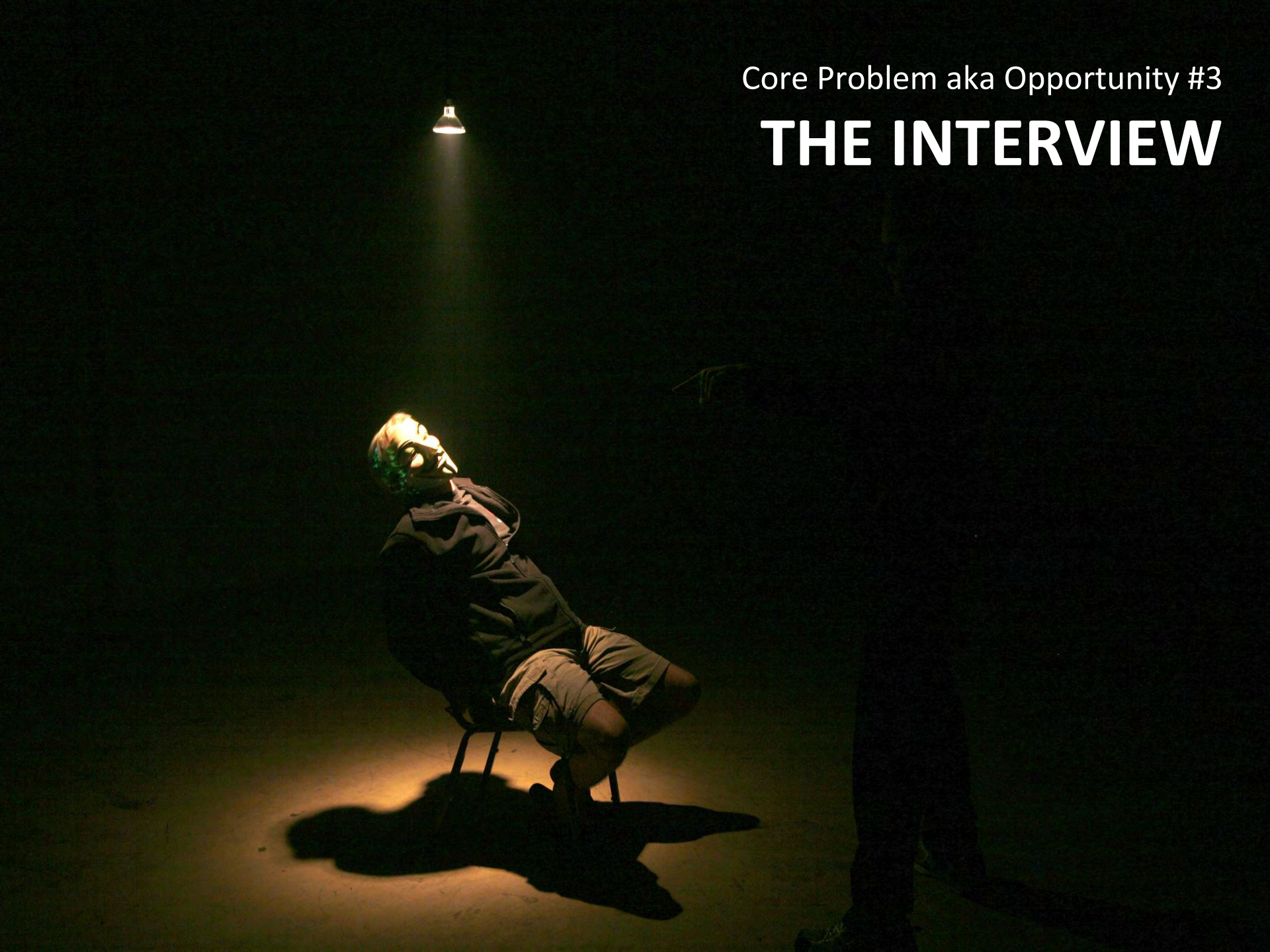
Keep Perspective

- Have patience
- Keep in mind the other requirements and stressors the hiring managers have
  - Outside influences on the process
- Get feedback from mentors & peers



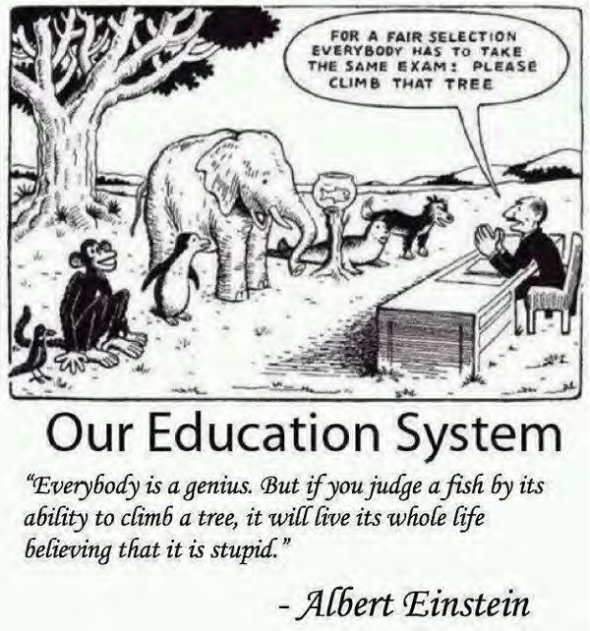
Core Problem aka Opportunity #3

THE INTERVIEW



The Interview

The interview process is hard. But when you compound that with the nervousness of trying to get a job in your "dream field" and the fact that most of us are weird shits who do weird shit during the day, the interview can be anxiety-inducing. There are a lot of little things that can be done by both sides to make it a little bit less awful.




ACTUALLY, IT IS ABOUT ETHICS
IN JOB INTERVIEWS
memegenerator.net

Hiring Managers

- “Stump the monkey” isn’t fun for anyone
  - Trick questions, the Google stumpers
  - Nor does it convey how good of an analyst they are or could be
    - How the candidate processing information to mitigate the threat/risk/vulnerability
    - Not how fast they can recite knowledge
  - Could dissuade a good candidate from accepting an offer

Stump the Monkey

- The intent is to find individuals for your team, not prove how smart you are - or how dumb they are
  - Lasting impression on you & company
    - See the Glassdoor Interview ratings & feedback
  - Sometimes there is more than one answer
    - With the answer different than yours
- See Wheaton's Law

https://dontbeadickday.com/

July 29

Question Bias

- So what if the candidate does not know how to work with oak
  - Can they learn to work with mahogany?
- Avoid close-ended questions
  - “Have you worked with Oak”?
  - “What is the UDP flag on a DNS request that fails”
  - “What protocol uses port 0”

Toolset Bias

- Best to use situational, exploratory conversations
- What are some of the ways you have used wood to address vulnerabilities?
- See: If Carpenters Were Hired Like Programmers

  http://www.jasonbock.net/jb/News/Item/7c334037d1a9437d9fa6506e2f35eaac

Hiring Bias

- Stop passing judgement
  - Piercings and tattoos no longer mean that they're ex-convicts
- Don't be a dick (Wheaton's Law)
  - People get nervous and forget things
  - So what if they self-identify as a hacker?

Reviewing resumes & length of time in a role

- Why does the length of time in a role matter?
  - Why this concern on ‘job hopping’?
  - Most are out of the candidate's control
    - Startups
    - Company failure or change of direction
    - Contract work
    - Layoff, unemployment
- Put yourself in their place

Reviewing resumes & length of time in a role

- Just because unemployed does not make them untouchable
  - Put aside your bias
  - Listen to the reason(s) and don't assume they're excuses
- Discrimination

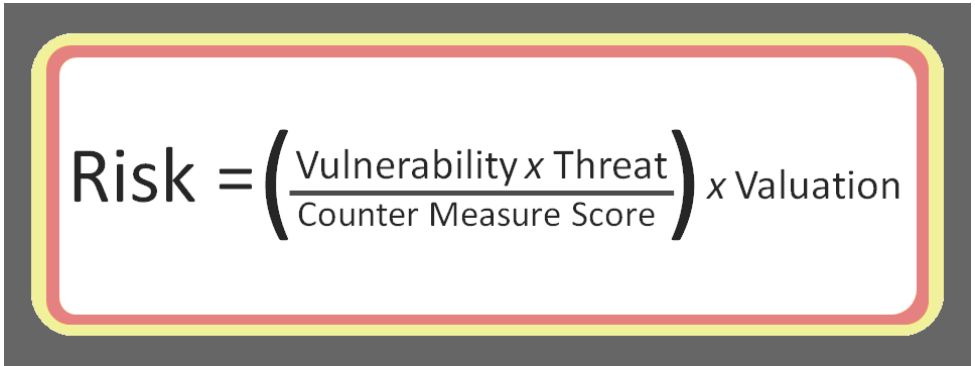
Reviewing resumes & length of time between roles

Not all gaps between jobs should be a (bad) reflection on the candidate

- Family illnesses
- School, personal development
- Recession (yes, there still is one)
- Personal time, recuperation from last role
  - Toxic work environment/manager
  - “Mourning period” after getting laid off from a job/company they really enjoyed being a part of (or needed)

The InfoSec Question

- Can the candidate explain how you can reduce Risk by affecting Vulnerability, Threat, Asset or Cost?
  - Most technical folk focus on Vulnerability.
  - Most nontechnical folk focus on Threat.
  - We need to reduce Vulnerability and Threat, but also work on Cost.



Hiring Excuses

Commonly heard excuses:

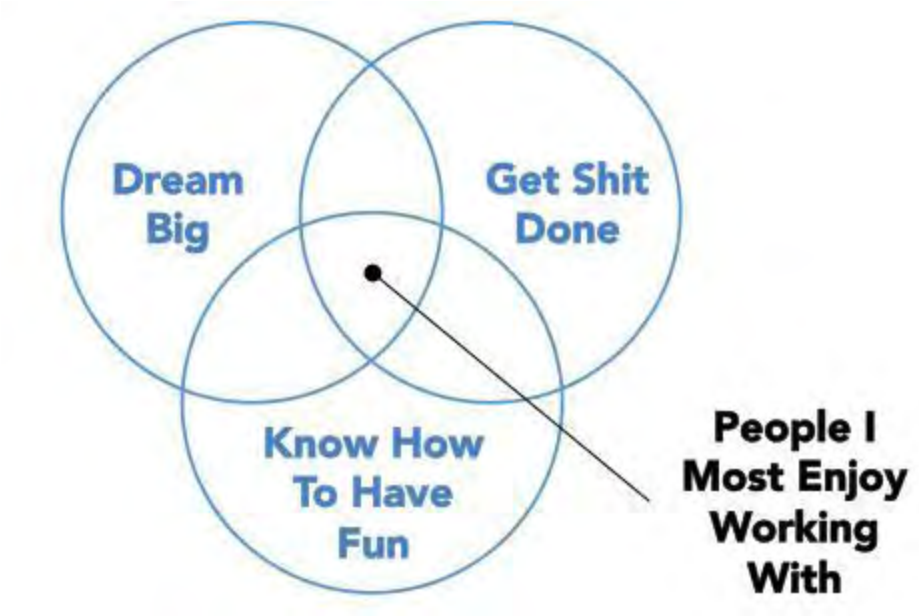
- “Not technical enough”
- “Not a cultural fit”

In your team interviews, use a scoring system and average the scores to help eliminate bias.

We need to stop using culture fit as a crutch for not hiring someone.

Culture Fit Excuse

- Think about whether you would want to work with this individual, but do not use it as an excuse when someone ”better” comes along.
- Do you think the person can do the job - or can learn?
- Diversity of the team
  - a good thing.



Trifecta

- Ability to learn (and want to learn skills)
  - This is critical
- Passion. What is this person passionate about?
  - Learning? Figuring things out? Solving problems? That is huge.
- Ability to be wrong/fail, and to do so well. We will all fail. The key is, if you fail, can you fail well? Can you learn and grow from it, or do you hide it and try to blame others?

Hacker Appearance

- Leave the ski mask at home
- Appropriateness
  - A bank vs. a startup?
  - East or West coast? Southwest?
- In your recon phase, determine the daily dress and take it up a notch

Hacker conduct in interview

- Don’t fucking swear
- Watch your personal sharing & stories
- Personal hygiene
- Personal space
- Manners still count
  - With everyone

#pantslessness

Hack the Interview

- Research on company and interviewees
  - Glassdoor
    - Help by leaving reviews, use Bugmenot & public WiFi
  - Wikipedia
  - Crunchbase
  - Social media
    - LinkedIn, with your alternate profile & proxy
  - Review rating Web sites, GTFG

Knowing Your Target

- Understand the target organization and hiring manager
  - Their product, values
- Able to explain why & how you are the best person for the role and the team at that company
- Have your three bullets and stick to them


QUESTION
EVERYTHING
WHY?

Hackers Question Everything

- From your research, have questions to ask them
  - Get them to sell you the role & the company
  - This is an interview on both sides of the table
    - Would you want to work for the manager?
    - Do you like the company, what they produce and stand for?

Question Everything

- Have appropriate answers for every InfoSec related interview question online
- “I don’t know” is not an answer
  - How would you figure it out?
- Your judgement call on calling out interviewers regarding inappropriate questions

A Question of Timing

- Did the interviewees give you enough time to ask questions?
  - Or was it the token five minutes at the end of their grilling?
  - Was it a conversation between peers, or individuals in the industry - or a grilling?

Core Problem aka Opportunity #4

POST-INTERVIEW

Post-Interview

A lot of folks can not seem to find the balance between being aloof about not getting the job and acting like overly attached girlfriend.

Hiring Managers

- Don’t leave people hanging
  - Send an email or call with status updates
  - Contact within 3-4 weeks at maximum
- Provide feedback
  - If HR will allow
  - Perhaps in a non-official capacity instead?
  - Builds relationships within the community
  - Helps improve the pool of candidates
    - Lets us determine what you need/want

Provide Feedback

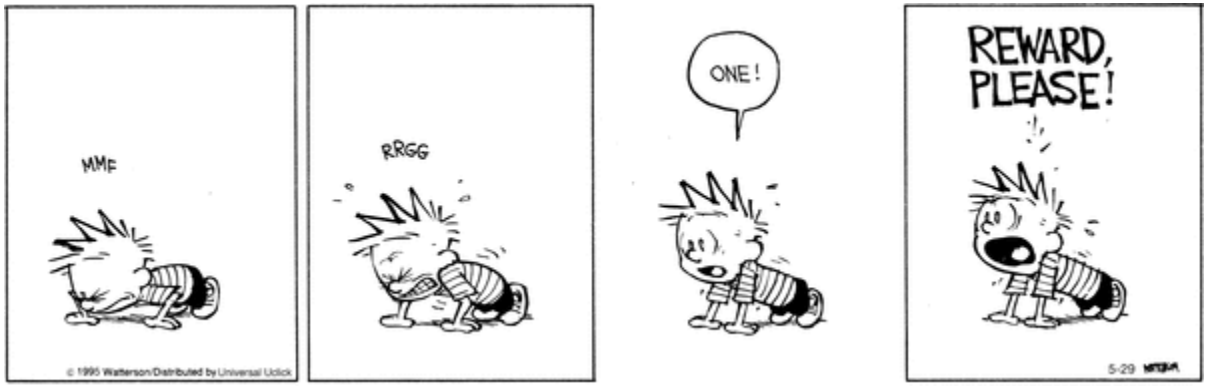
- Glaring resume issues/errors
- Topics to review
  - Tools, Techniques, Procedures (TTPs)
  - Protocols
- Interview tips
  - Talk more/don’t talk as much
  - Etiquette

Hackers, Follow Up

- Send a “thank you” email to all you talked and interacted with. Consider snail mail card
  - Best not send connection requests on social media

Hackers

- Follow-up
  - When should you reach out if you have not heard back?
  - Don’t panic
    - It may take a while to hear back
- Be realistic in your expectations
  - Know the local/regional/national market



Social Network

- Leverage your network to provide insight & potential references to the company/hiring manager
- How do you get previous supervisors as references?
- DO NOT send social media connection requests
  - Creeepy….
- Leave feedback on Glassdoor?

Employers forget that the impression they leave on their employees, past & present, influences income, rep and biz dev in ways unknown.
@kjvalentine

Thanks (Credits)

@StartUpJackson, @RebeccaSlatkin, @TylerSchmall

roadtociso.wordpress.com - Jesika McEvoy

jasonbock.net - Jason Bock

@kjvalentine

John Omernik aka Chief Ten Beers

Winn Schwartau

All those applications we submitted, those folks we interviewed with, and those we have interviewed.

Q&A

TUVM @AcademicsSay